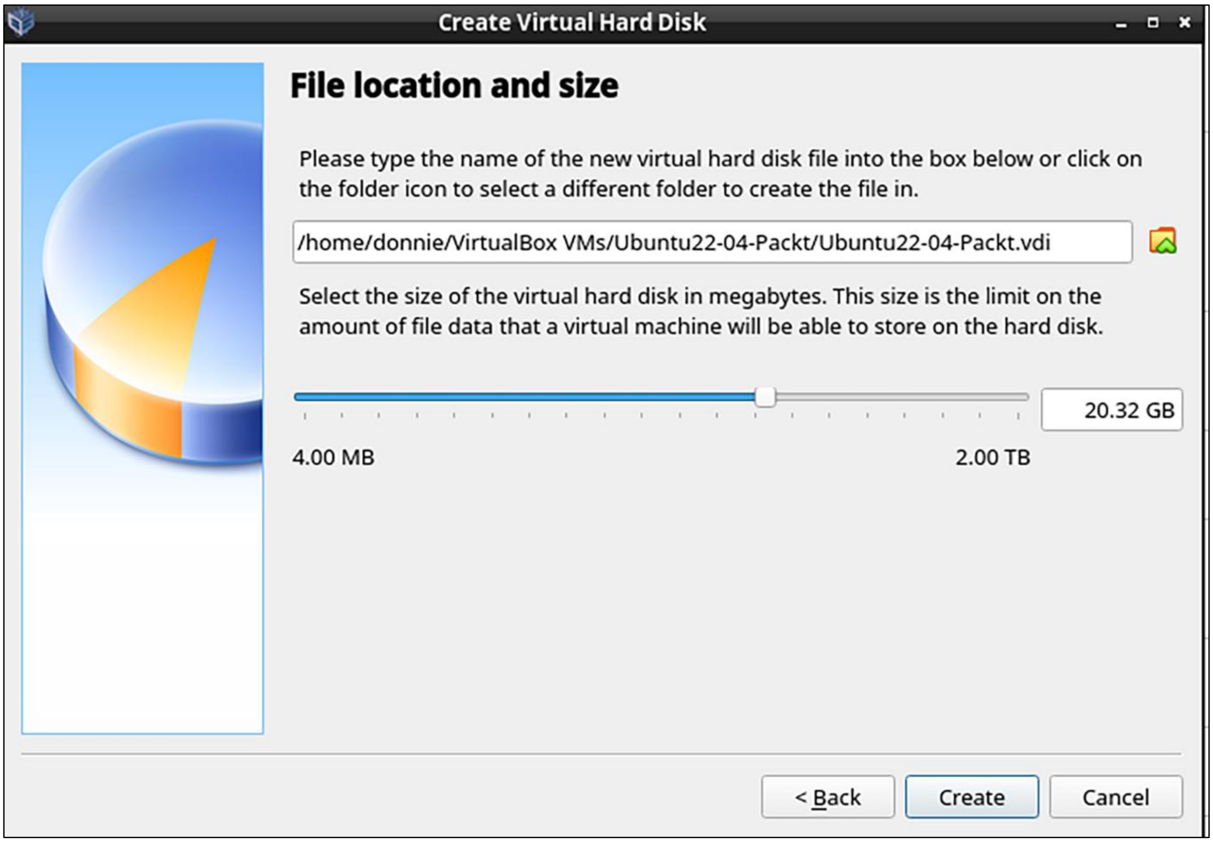
Chapter 1: Running Linux in a Virtual Environment



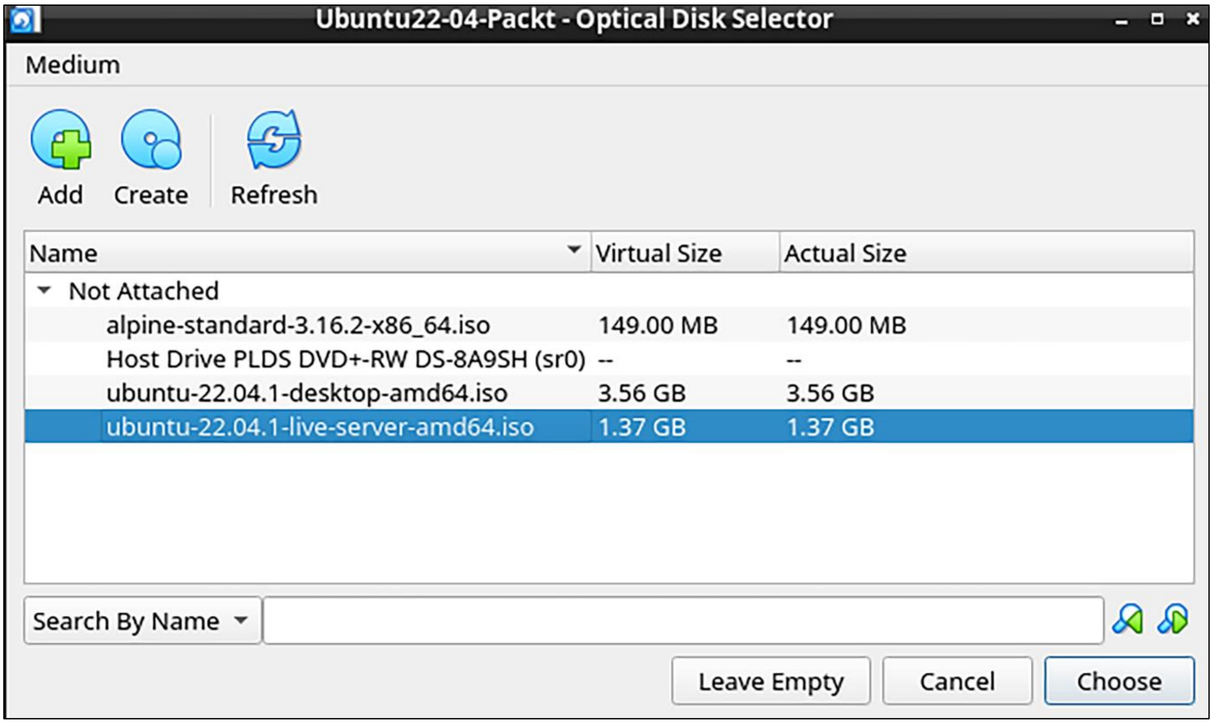
File location and size

Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

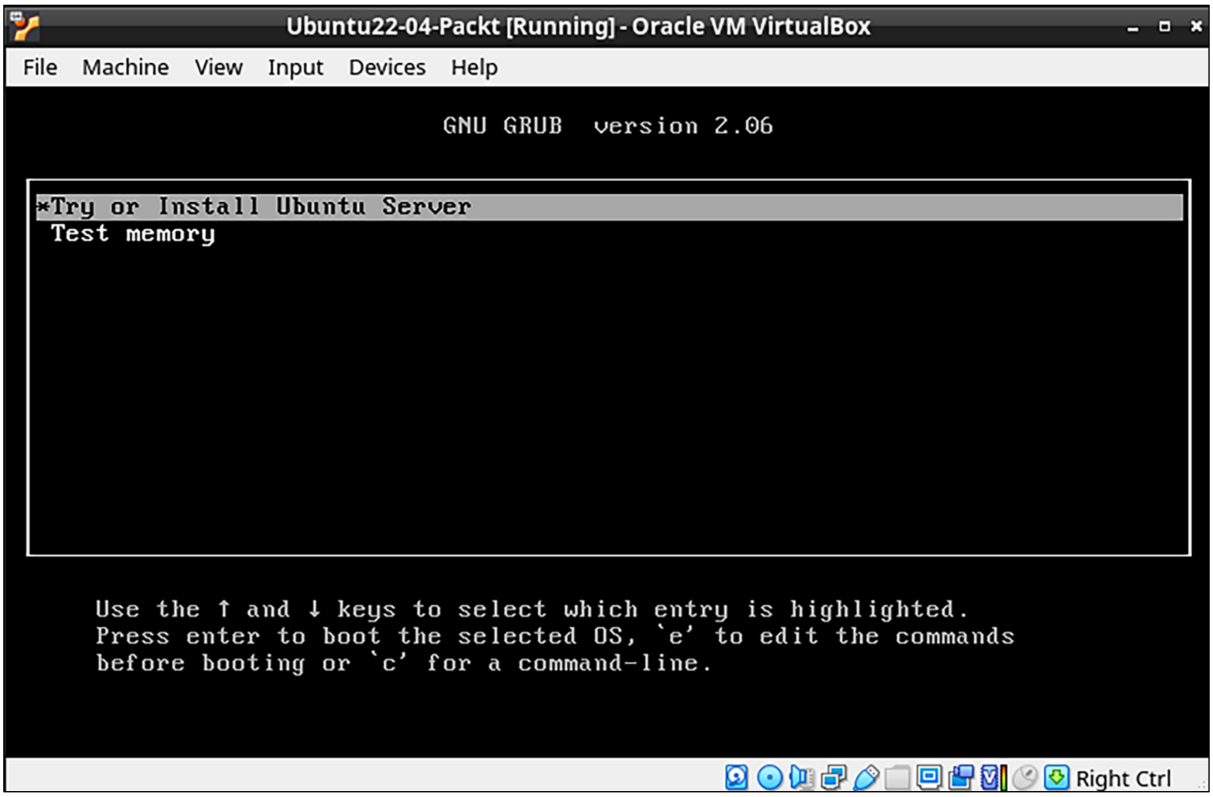
/home/donnie/VirtualBox VMs/Ubuntu22-04-Packt/Ubuntu22-04-Packt.vdi

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

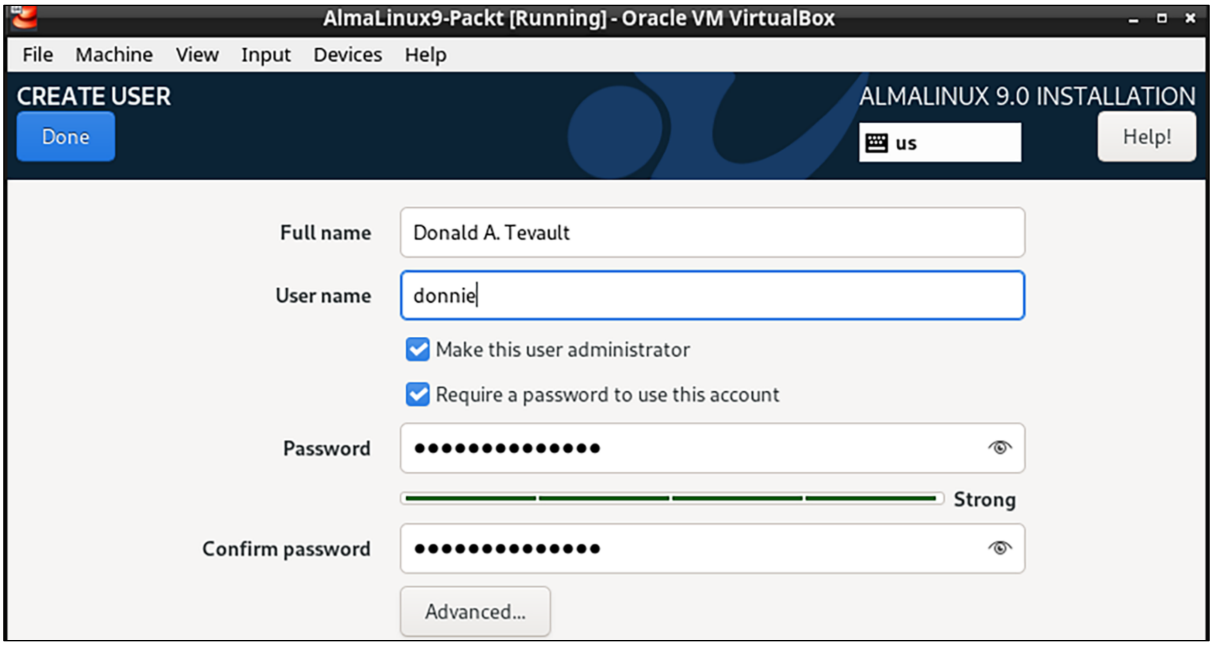
20.32 GB



Name	Virtual Size	Actual Size
Not Attached		
alpine-standard-3.16.2-x86_64.iso	149.00 MB	149.00 MB
Host Drive PLDS DVD+-RW DS-8A9SH (sr0)	--	--
ubuntu-22.04.1-desktop-amd64.iso	3.56 GB	3.56 GB
ubuntu-22.04.1-live-server-amd64.iso	1.37 GB	1.37 GB


Ubuntu22-04-Packt [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
GNU GRUB  version 2.06

*Try or Install Ubuntu Server
 Test memory

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line.
```


AlmaLinux9-Packt [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
CREATE USER
Done
ALMALINUX 9.0 INSTALLATION
us
Help!
Advanced...

Full name: Donald A. Tevault

User name: donnie

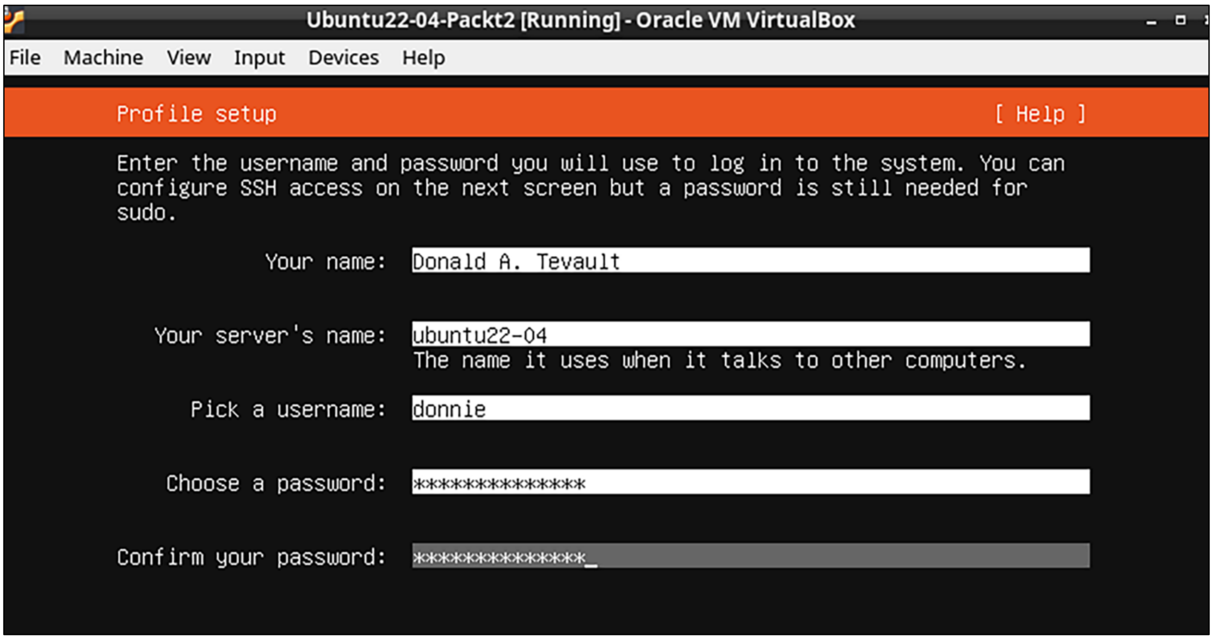
☑ Make this user administrator

☑ Require a password to use this account

Password: ••••••••••••••

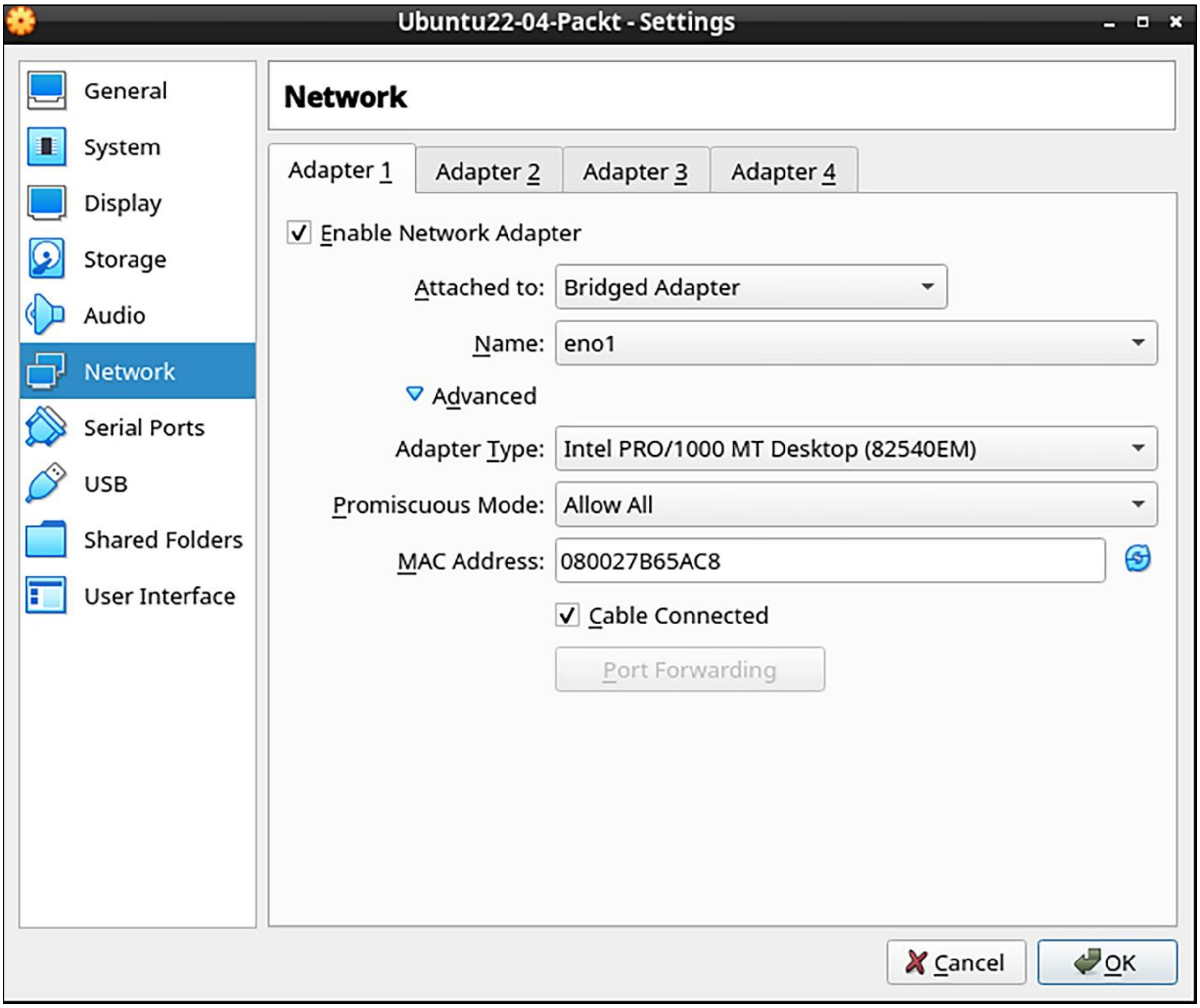
Strong

Confirm password: ••••••••••••••



Ubuntu22-04-Packt2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Profile setup
[Help]

```
Enter the username and password you will use to log in to the system. You can
configure SSH access on the next screen but a password is still needed for
sudo.

            Your name:  Donald A. Tevault

     Your server's name:  ubuntu22-04
                          The name it uses when it talks to other computers.

        Pick a username:  donnie

      Choose a password:  ***************

   Confirm your password:  ***************_
```



Network

☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: eno1

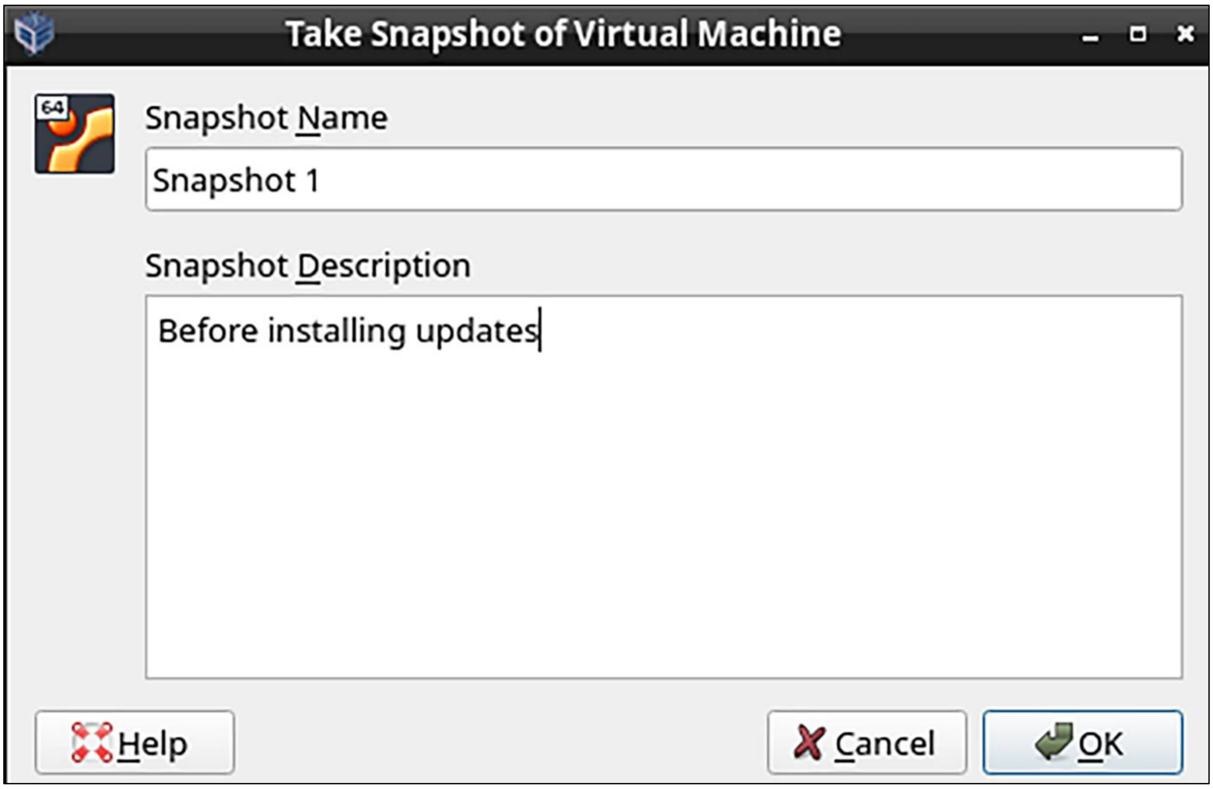
▽ Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

MAC Address: 080027B65AC8

☑ Cable Connected

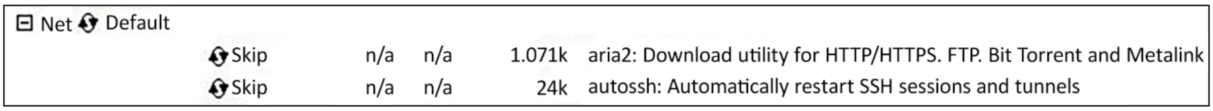


Snapshot Name

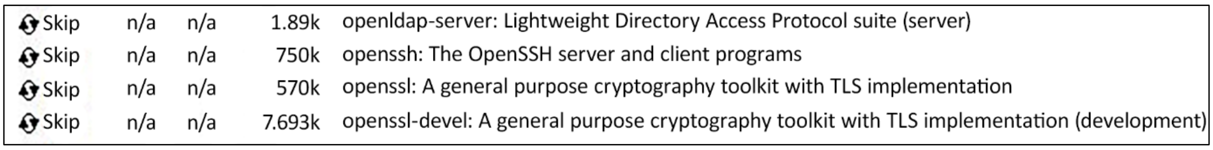
Snapshot 1

Snapshot Description

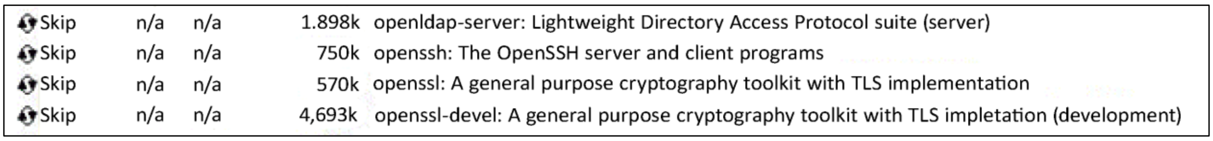
Before installing updates



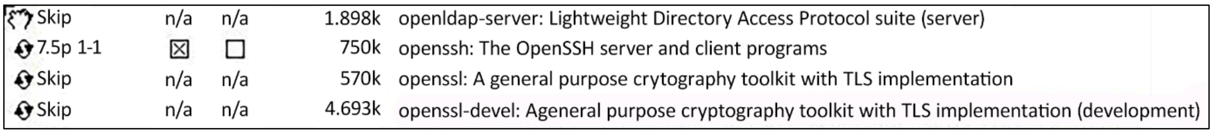
```
⊟ Net Default
                  Skip          n/a   n/a    1.071k  aria2: Download utility for HTTP/HTTPS. FTP. Bit Torrent and Metalink
                  Skip          n/a   n/a       24k  autossh: Automatically restart SSH sessions and tunnels
```



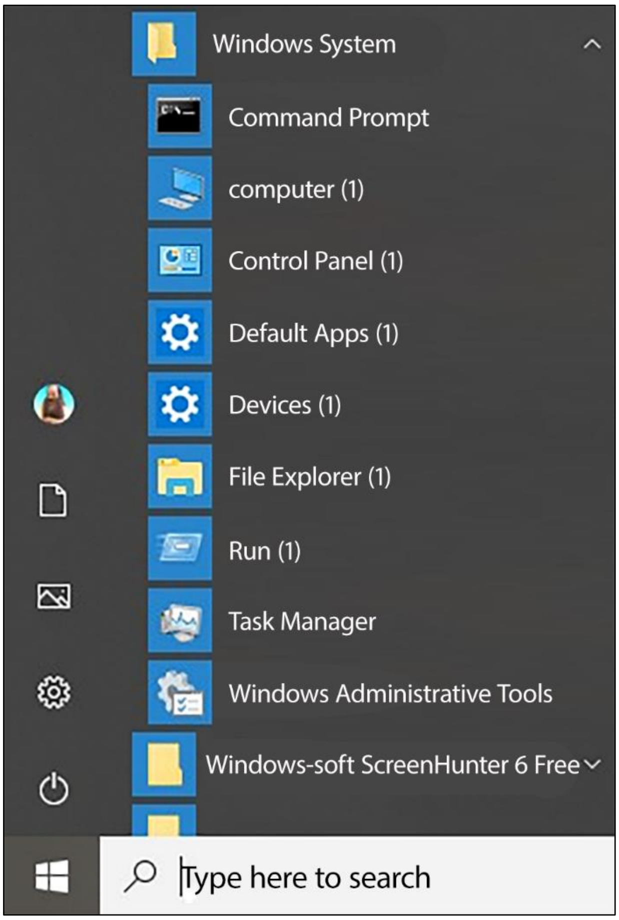
```
Skip   n/a   n/a    1.89k  openldap-server: Lightweight Directory Access Protocol suite (server)
Skip   n/a   n/a     750k  openssh: The OpenSSH server and client programs
Skip   n/a   n/a     570k  openssl: A general purpose cryptography toolkit with TLS implementation
Skip   n/a   n/a   7.693k  openssl-devel: A general purpose cryptography toolkit with TLS implementation (development)
```

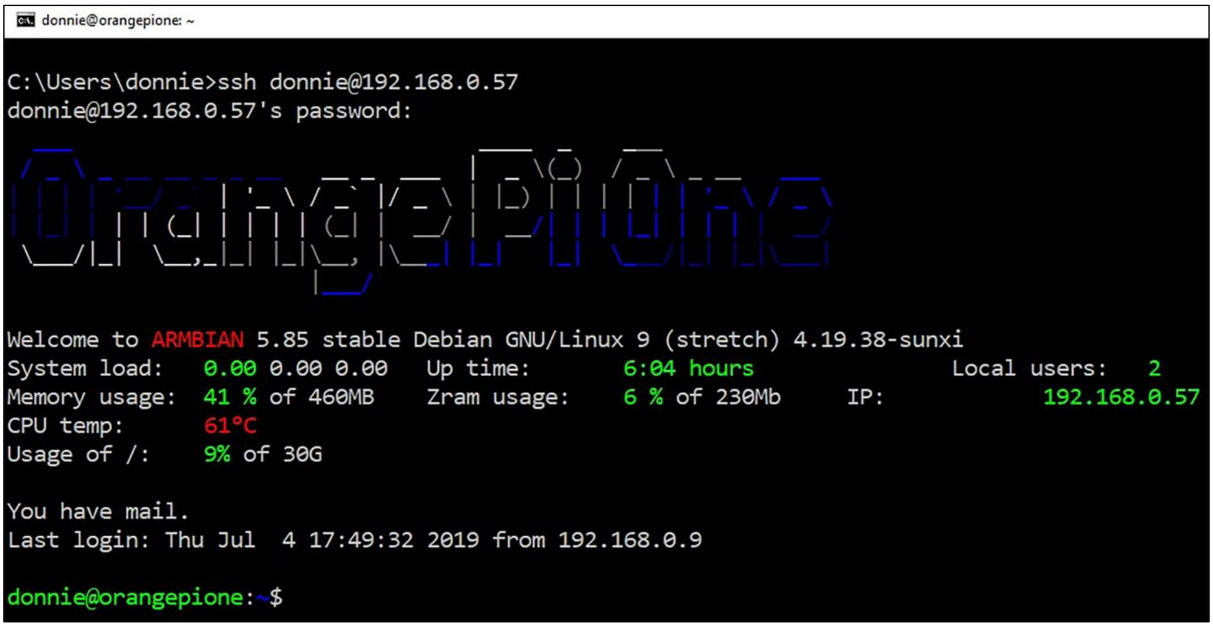


```
Skip    n/a   n/a     1.898k  openldap-server: Lightweight Directory Access Protocol suite (server)
Skip    n/a   n/a       750k  openssh: The OpenSSH server and client programs
Skip    n/a   n/a       570k  openssl: A general purpose cryptography toolkit with TLS implementation
Skip    n/a   n/a     4,693k  openssl-devel: A general purpose cryptography toolkit with TLS impletation (development)
```

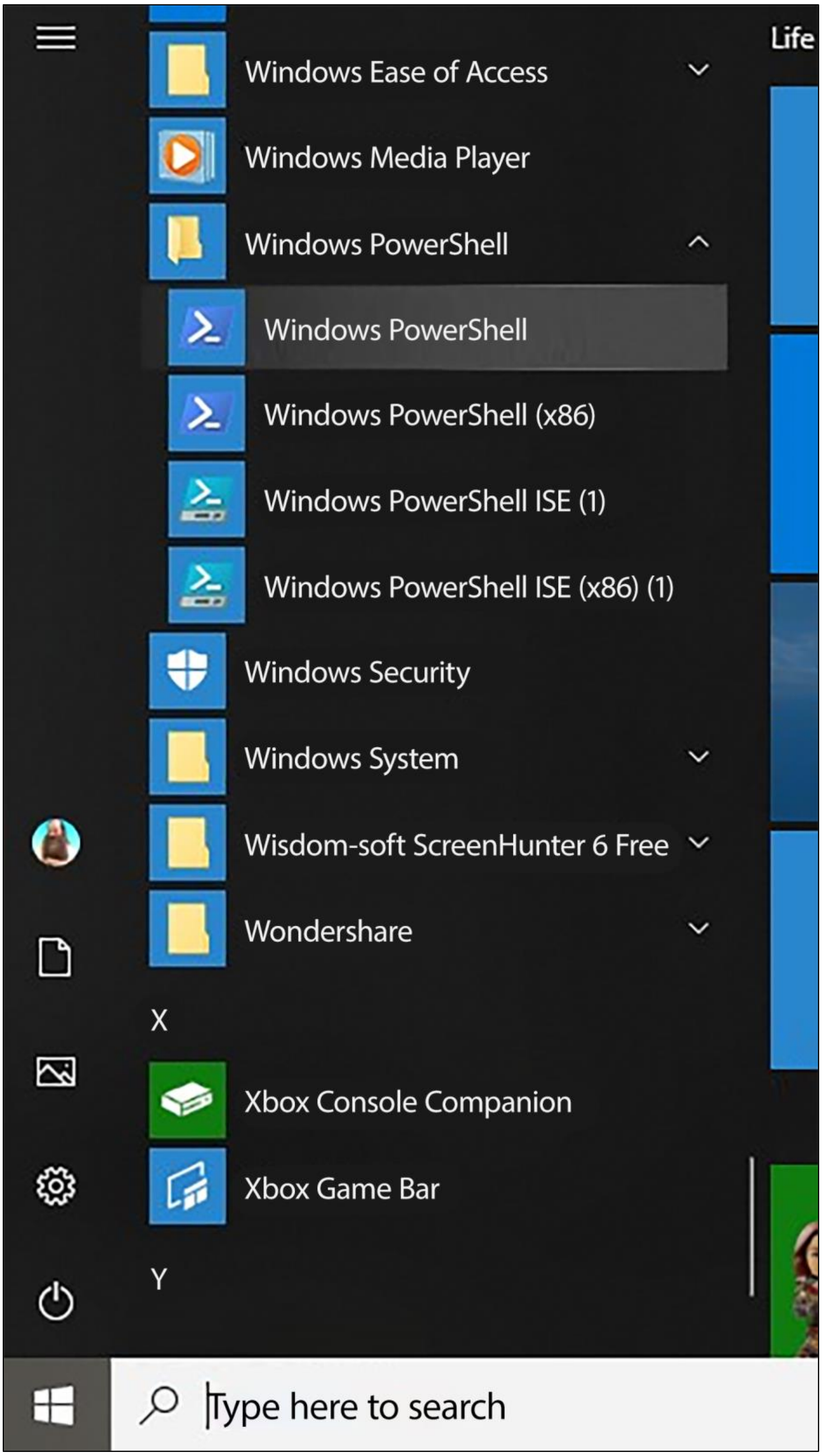


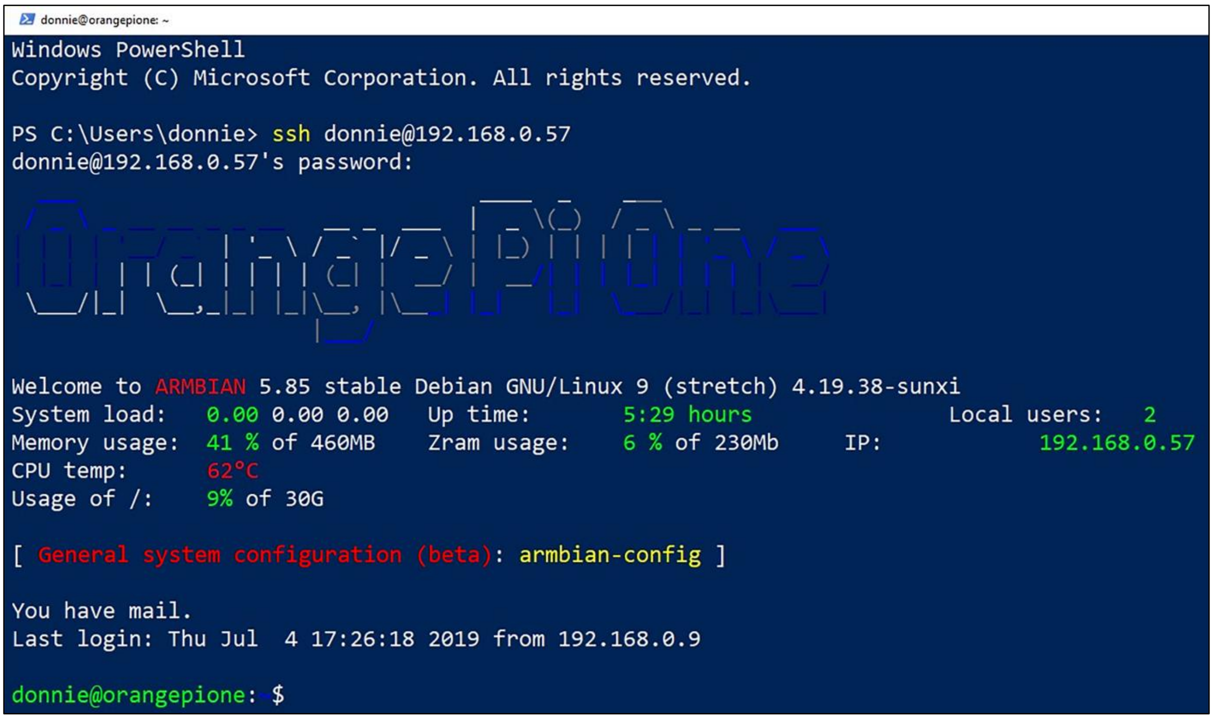
```
Skip       n/a   n/a     1.898k  openldap-server: Lightweight Directory Access Protocol suite (server)
7.5p 1-1   ☒     □         750k  openssh: The OpenSSH server and client programs
Skip       n/a   n/a       570k  openssl: A general purpose crytography toolkit with TLS implementation
Skip       n/a   n/a     4.693k  openssl-devel: Ageneral purpose cryptography toolkit with TLS implementation (development)
```



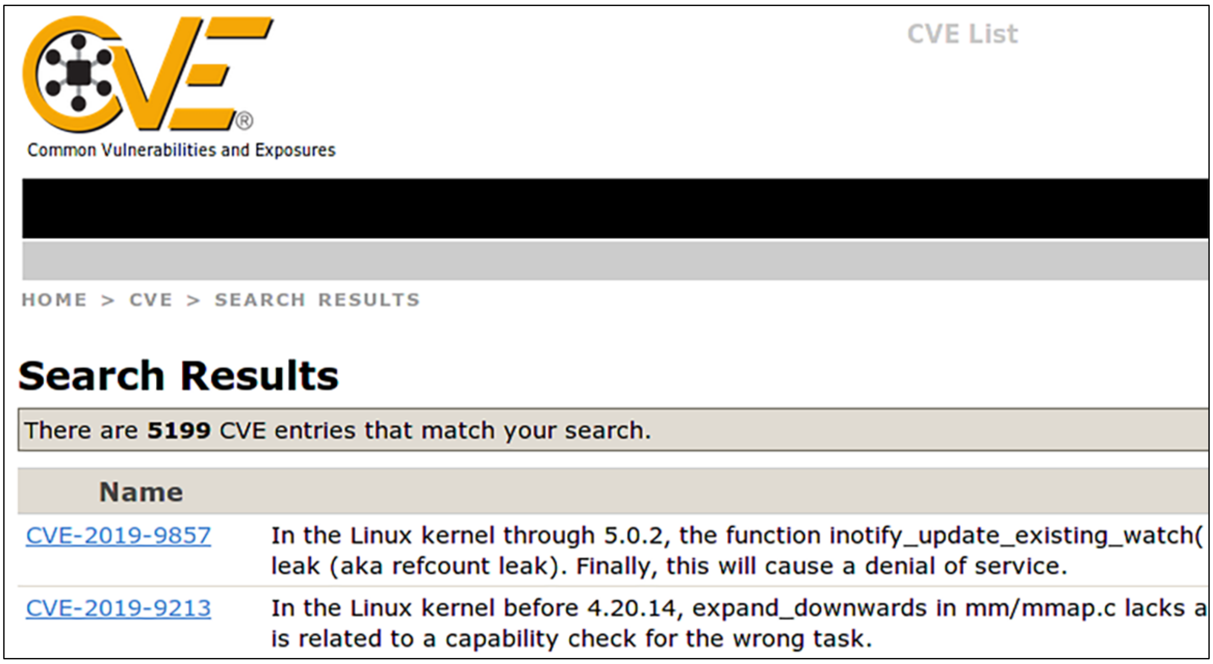


```
C:\Users\donnie>ssh donnie@192.168.0.57
donnie@192.168.0.57's password:

Welcome to ARMBIAN 5.85 stable Debian GNU/Linux 9 (stretch) 4.19.38-sunxi
System load:   0.00 0.00 0.00   Up time:       6:04 hours              Local users:   2
Memory usage:  41 % of 460MB    Zram usage:    6 % of 230Mb     IP:            192.168.0.57
CPU temp:      61°C
Usage of /:    9% of 30G

You have mail.
Last login: Thu Jul  4 17:49:32 2019 from 192.168.0.9

donnie@orangepione:~$
```


Life
Windows Ease of Access
Windows Media Player
Windows PowerShell
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE (1)
Windows PowerShell ISE (x86) (1)
Windows Security
Windows System
Wisdom-soft ScreenHunter 6 Free
Wondershare
X
Xbox Console Companion
Xbox Game Bar
Y
Type here to search



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\donnie> ssh donnie@192.168.0.57
donnie@192.168.0.57's password:

Welcome to ARMBIAN 5.85 stable Debian GNU/Linux 9 (stretch) 4.19.38-sunxi
System load:   0.00 0.00 0.00   Up time:       5:29 hours            Local users:   2
Memory usage:  41 % of 460MB    Zram usage:    6 % of 230Mb     IP:            192.168.0.57
CPU temp:      62°C
Usage of /:    9% of 30G

[ General system configuration (beta): armbian-config ]

You have mail.
Last login: Thu Jul  4 17:26:18 2019 from 192.168.0.9

donnie@orangepione:~$
```

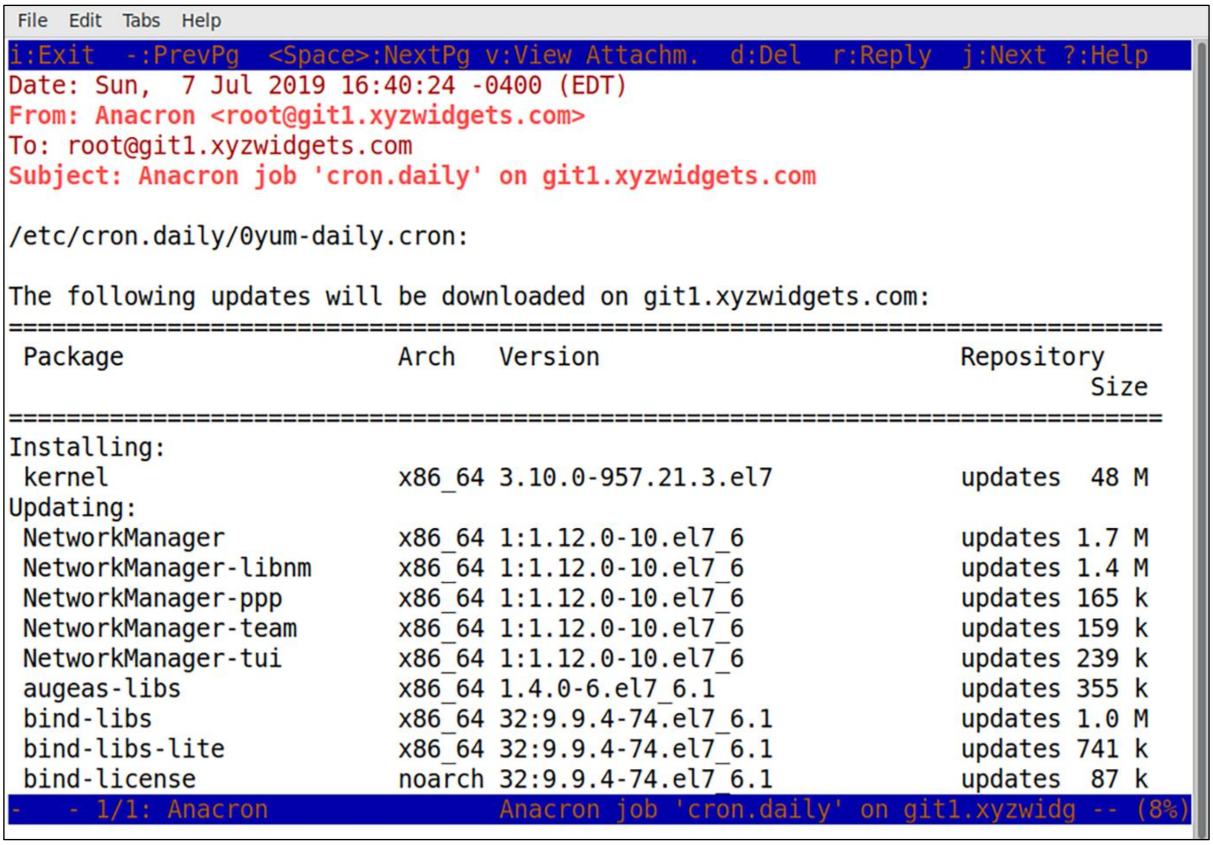


Common Vulnerabilities and Exposures
CVE List
HOME > CVE > SEARCH RESULTS

Search Results

There are **5199** CVE entries that match your search.

Name	
CVE-2019-9857	In the Linux kernel through 5.0.2, the function inotify_update_existing_watch(leak (aka refcount leak). Finally, this will cause a denial of service.
CVE-2019-9213	In the Linux kernel before 4.20.14, expand_downwards in mm/mmap.c lacks a is related to a capability check for the wrong task.

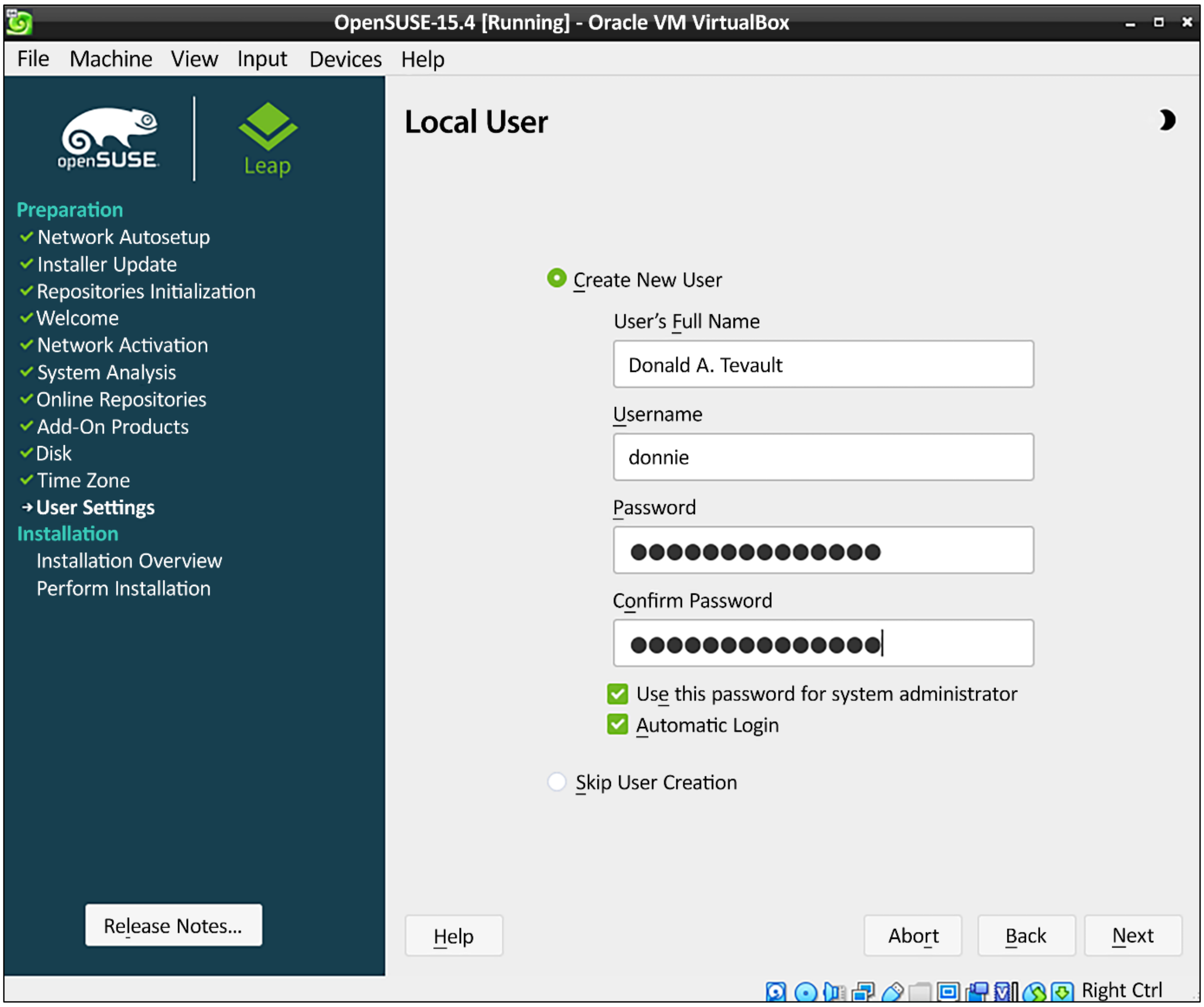


```
i:Exit  -:PrevPg  <Space>:NextPg v:View Attachm.  d:Del  r:Reply  j:Next ?:Help
Date: Sun,  7 Jul 2019 16:40:24 -0400 (EDT)
From: Anacron <root@git1.xyzwidgets.com>
To: root@git1.xyzwidgets.com
Subject: Anacron job 'cron.daily' on git1.xyzwidgets.com

/etc/cron.daily/0yum-daily.cron:

The following updates will be downloaded on git1.xyzwidgets.com:
================================================================================
 Package                    Arch   Version                         Repository
                                                                         Size
================================================================================
Installing:
 kernel                     x86_64 3.10.0-957.21.3.el7             updates   48 M
Updating:
 NetworkManager             x86_64 1:1.12.0-10.el7_6               updates 1.7 M
 NetworkManager-libnm       x86_64 1:1.12.0-10.el7_6               updates 1.4 M
 NetworkManager-ppp         x86_64 1:1.12.0-10.el7_6               updates 165 k
 NetworkManager-team        x86_64 1:1.12.0-10.el7_6               updates 159 k
 NetworkManager-tui         x86_64 1:1.12.0-10.el7_6               updates 239 k
 augeas-libs                x86_64 1.4.0-6.el7_6.1                 updates 355 k
 bind-libs                  x86_64 32:9.9.4-74.el7_6.1             updates 1.0 M
 bind-libs-lite             x86_64 32:9.9.4-74.el7_6.1             updates 741 k
 bind-license               noarch 32:9.9.4-74.el7_6.1             updates  87 k
-   - 1/1: Anacron                 Anacron job 'cron.daily' on git1.xyzwidg -- (8%)
```

Chapter 2: Securing Administrative User Accounts

How do I use RaspEX?

When you start up your Raspberry Mini computer with RaspEX you will (after a few seconds) end up in X and LXDE as the ordinary user **raspex**. The password for raspex is raspex. When logged in as raspex you can use Sudo to become root. Example: *sudo su* and *sudo pcmanfm*. The password for **root** superuser) is *root*. You can log out from LXDE and log in again as root (if you want). This is how it looks at SLiM's login page.



Local User

● Create New User

User's Full Name

Donald A. Tevault

Username

donnie

Password

●●●●●●●●●●●●●●

Confirm Password

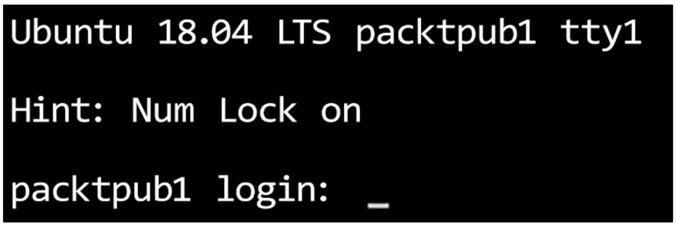
●●●●●●●●●●●●●●

☑ Use this password for system administrator

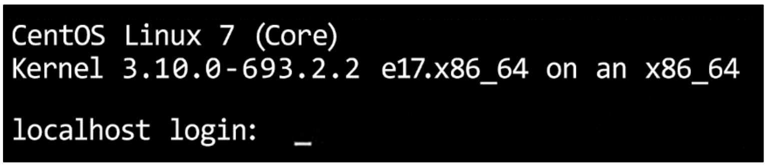
☑ Automatic Login

○ Skip User Creation

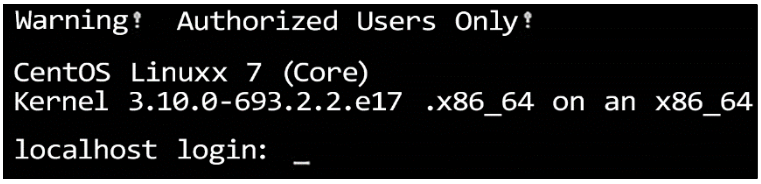
Chapter 3: Securing Normal User Accounts



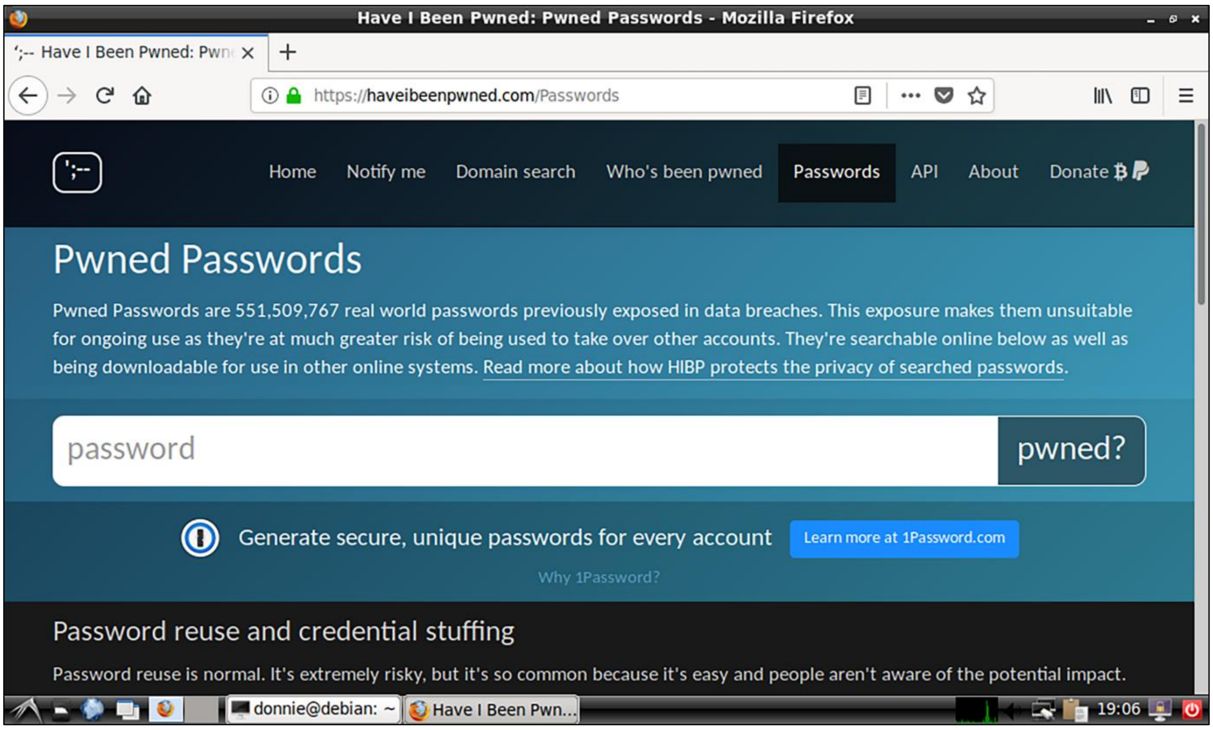
```
Ubuntu 18.04 LTS packtpub1 tty1

Hint: Num Lock on

packtpub1 login: _
```



```
CentOS Linux 7 (Core)
Kernel 3.10.0-693.2.2 e17.x86_64 on an x86_64

localhost login:  _
```



```
Warning!  Authorized Users Only!

CentOS Linuxx 7 (Core)
Kernel 3.10.0-693.2.2.e17 .x86_64 on an x86_64

localhost login: _
```



Have I Been Pwned: Pwned Passwords - Mozilla Firefox
';-- Have I Been Pwned: Pwn
https://haveibeenpwned.com/Passwords
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
password
pwned?
Learn more at 1Password.com
Why 1Password?
donnie@debian: ~
Have I Been Pwn...
19:06

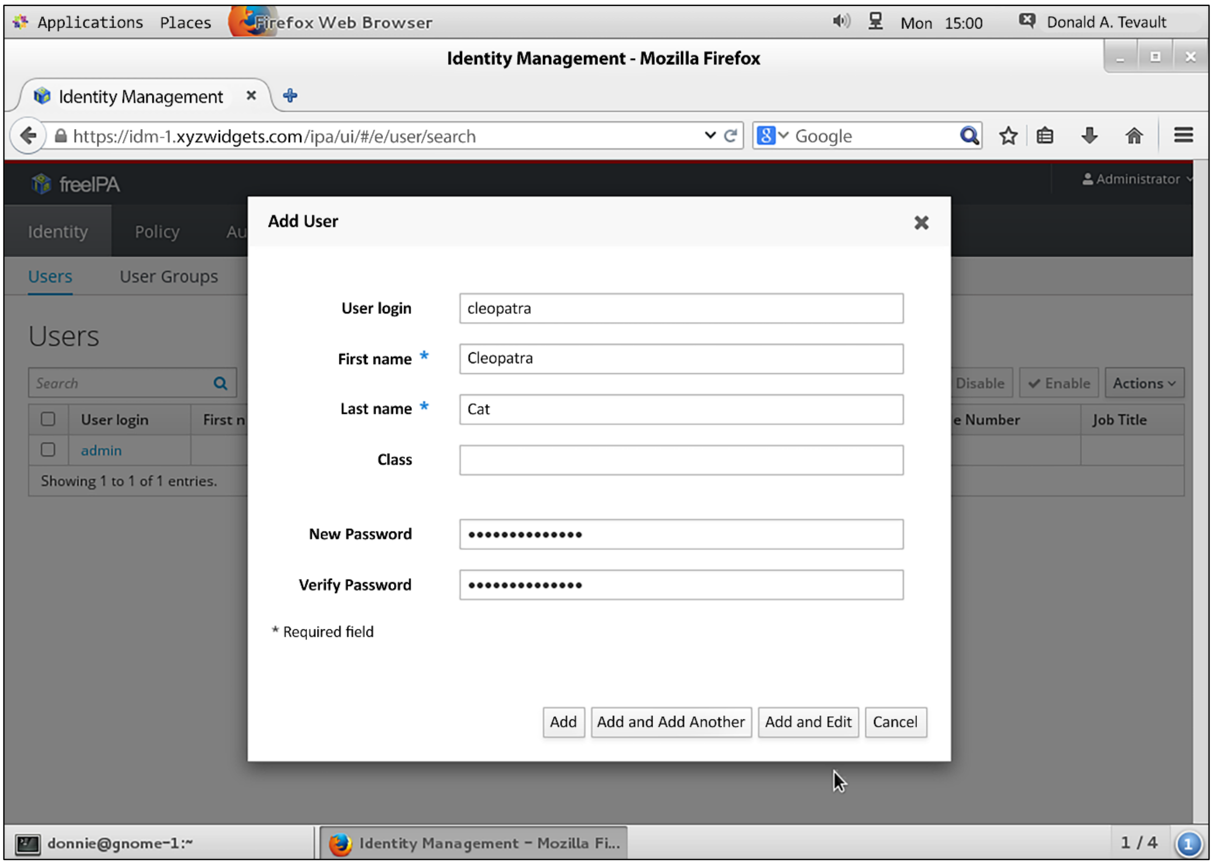
Pwned Passwords

Pwned Passwords are 551,509,767 real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. Read more about how HIBP protects the privacy of searched passwords.

Generate secure, unique passwords for every account

Password reuse and credential stuffing

Password reuse is normal. It's extremely risky, but it's so common because it's easy and people aren't aware of the potential impact.



Add User

User login: cleopatra

First name *: Cleopatra

Last name *: Cat

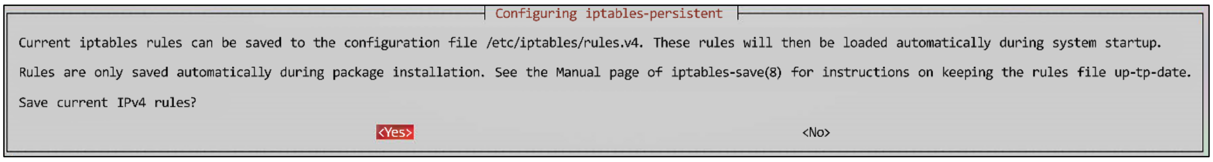
Class:

New Password: ••••••••••••••

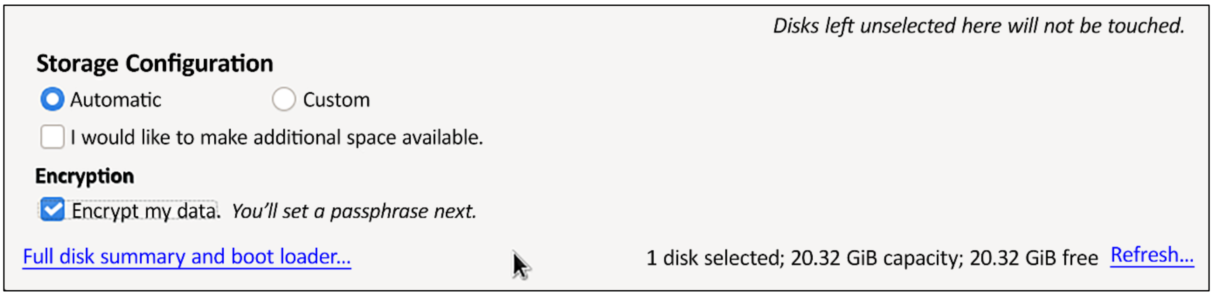
Verify Password: ••••••••••••••

* Required field

Chapter 4: Securing Your Server with a Firewall - Part 1



```
Current iptables rules can be saved to the configuration file /etc/iptables/rules.v4. These rules will then be loaded automatically during system startup.

Rules are only saved automatically during package installation. See the Manual page of iptables-save(8) for instructions on keeping the rules file up-tp-date.

Save current IPv4 rules?
```



Disks left unselected here will not be touched.

Storage Configuration

● Automatic ○ Custom

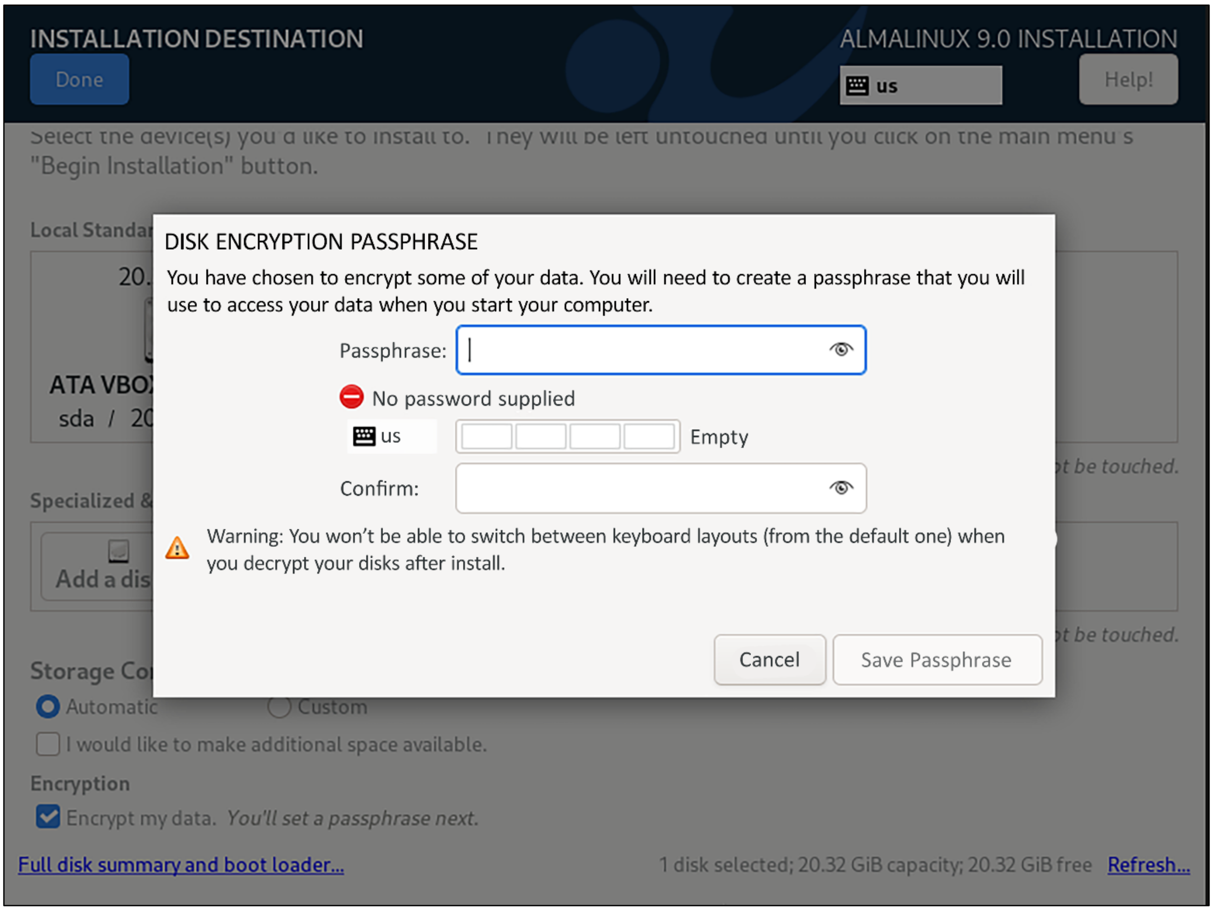
□ I would like to make additional space available.

Encryption

☑ Encrypt my data. *You'll set a passphrase next.*

Full disk summary and boot loader...

1 disk selected; 20.32 GiB capacity; 20.32 GiB free Refresh...



Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

DISK ENCRYPTION PASSPHRASE

You have chosen to encrypt some of your data. You will need to create a passphrase that you will use to access your data when you start your computer.

Passphrase:

No password supplied

us Empty

Confirm:

Warning: You won't be able to switch between keyboard layouts (from the default one) when you decrypt your disks after install.

Storage Configuration

● Automatic ○ Custom

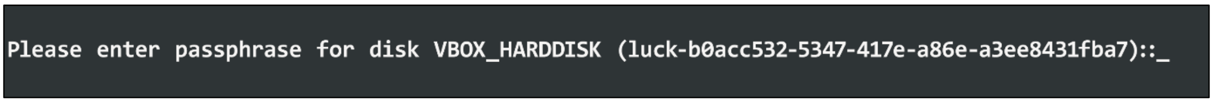
□ I would like to make additional space available.

Encryption

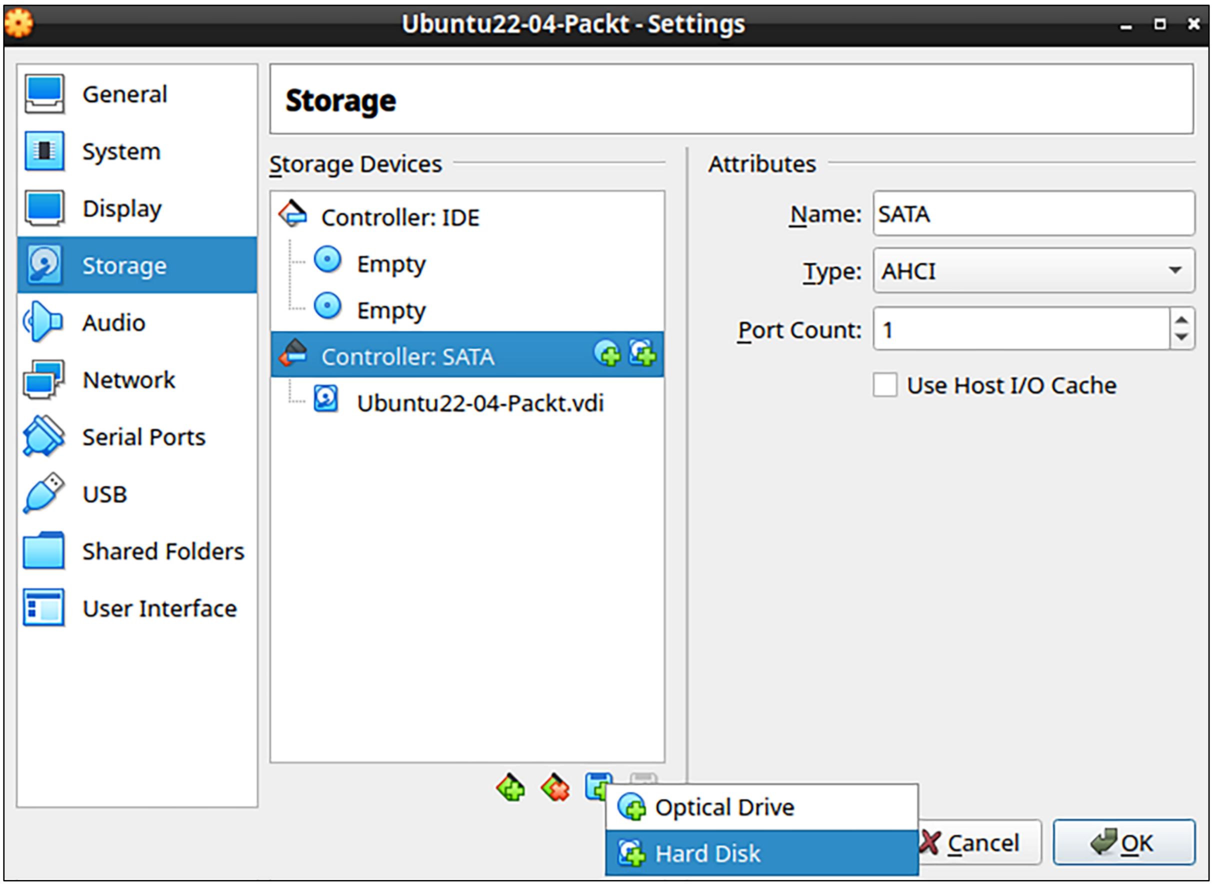
☑ Encrypt my data. *You'll set a passphrase next.*

Full disk summary and boot loader...

1 disk selected; 20.32 GiB capacity; 20.32 GiB free Refresh...



```
Please enter passphrase for disk VBOX_HARDDISK (luck-b0acc532-5347-417e-a86e-a3ee8431fba7)::_
```



Ubuntu22-04-Packt - Settings

Storage

Storage Devices

- Controller: IDE
  - Empty
  - Empty
- Controller: SATA
  - Ubuntu22-04-Packt.vdi

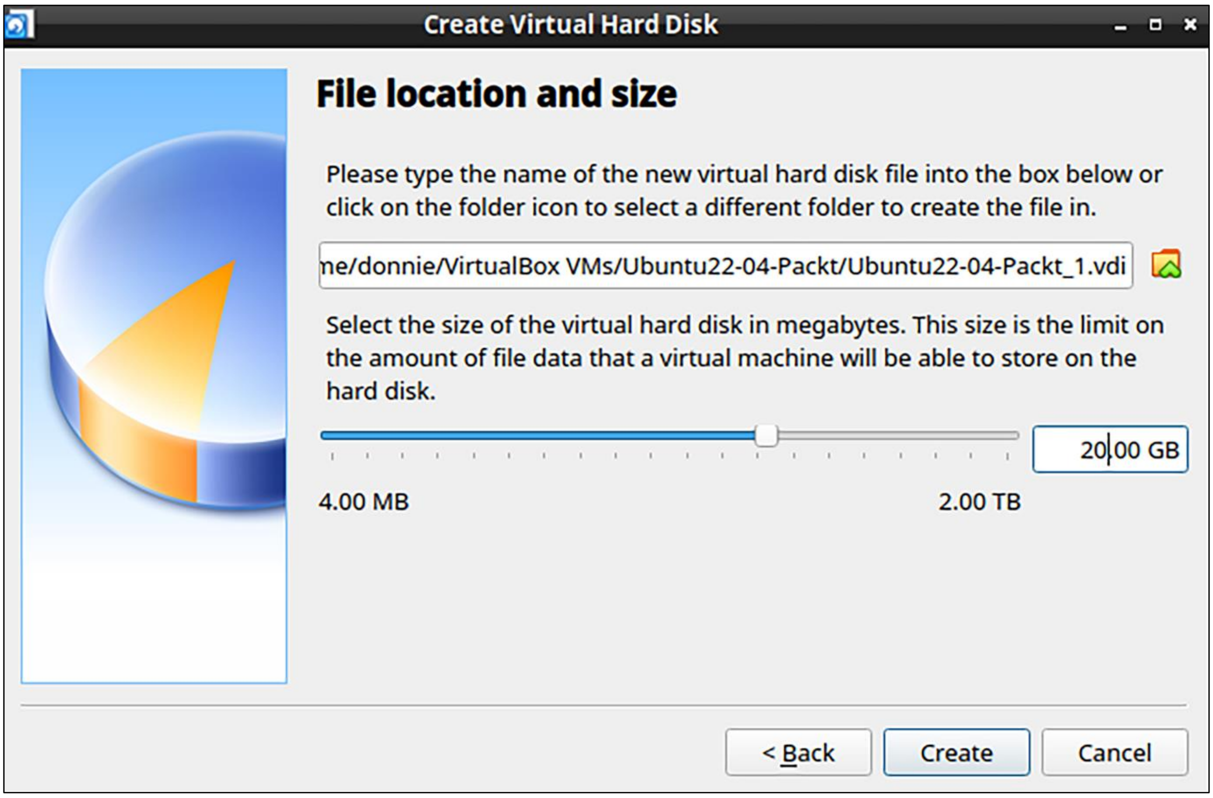
Attributes

Name: SATA

Type: AHCI

Port Count: 1

□ Use Host I/O Cache



Create Virtual Hard Disk

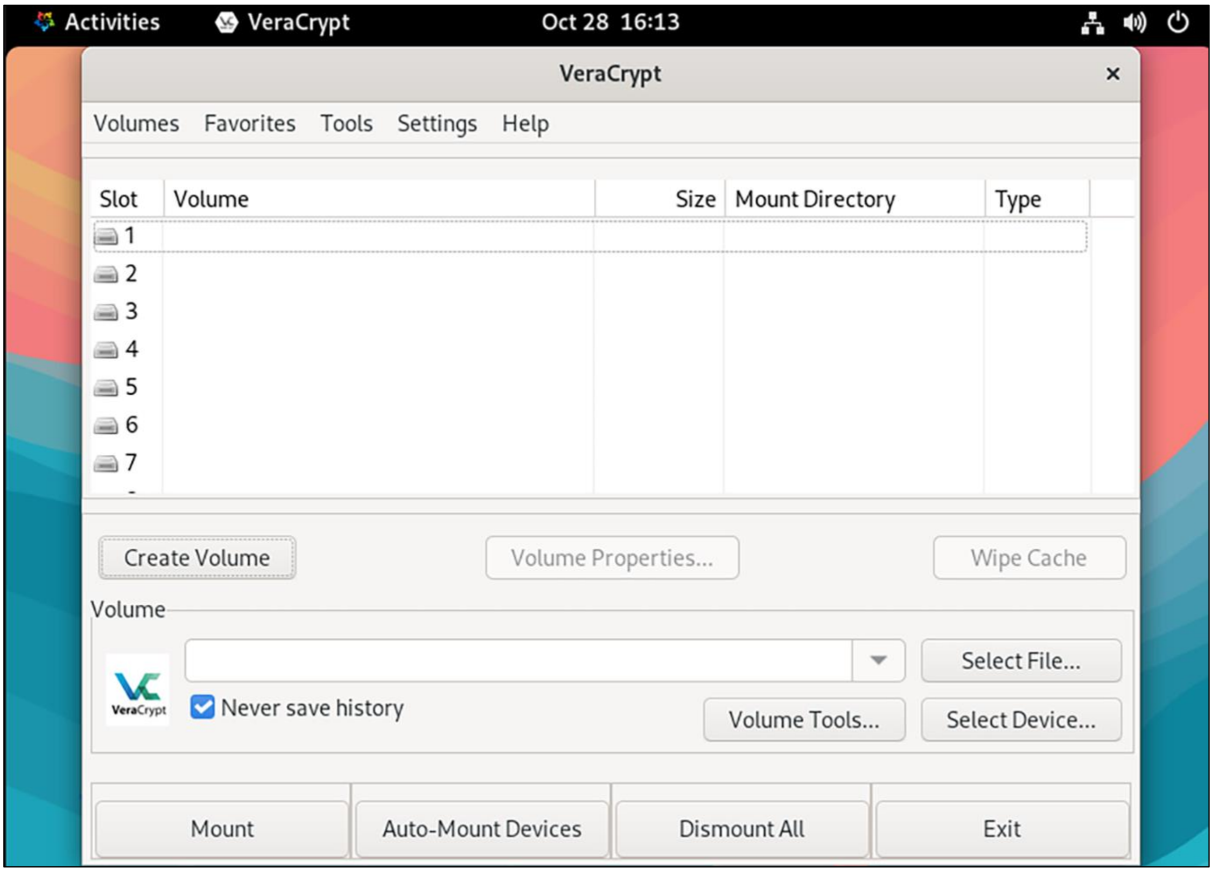
File location and size

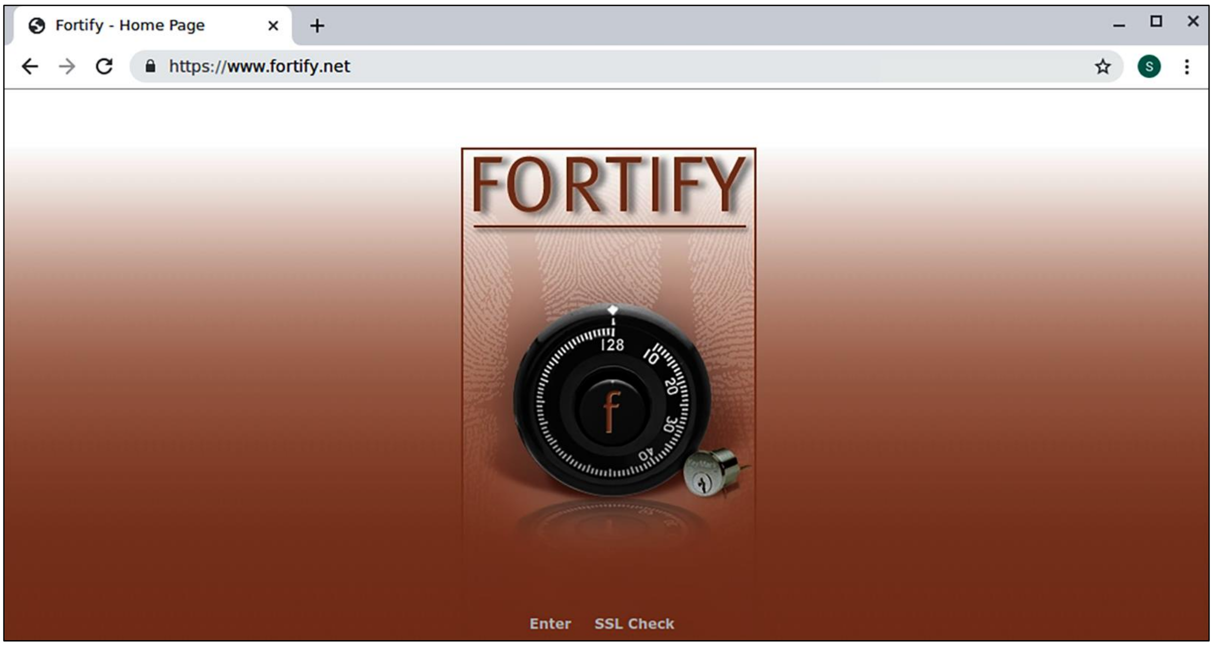
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

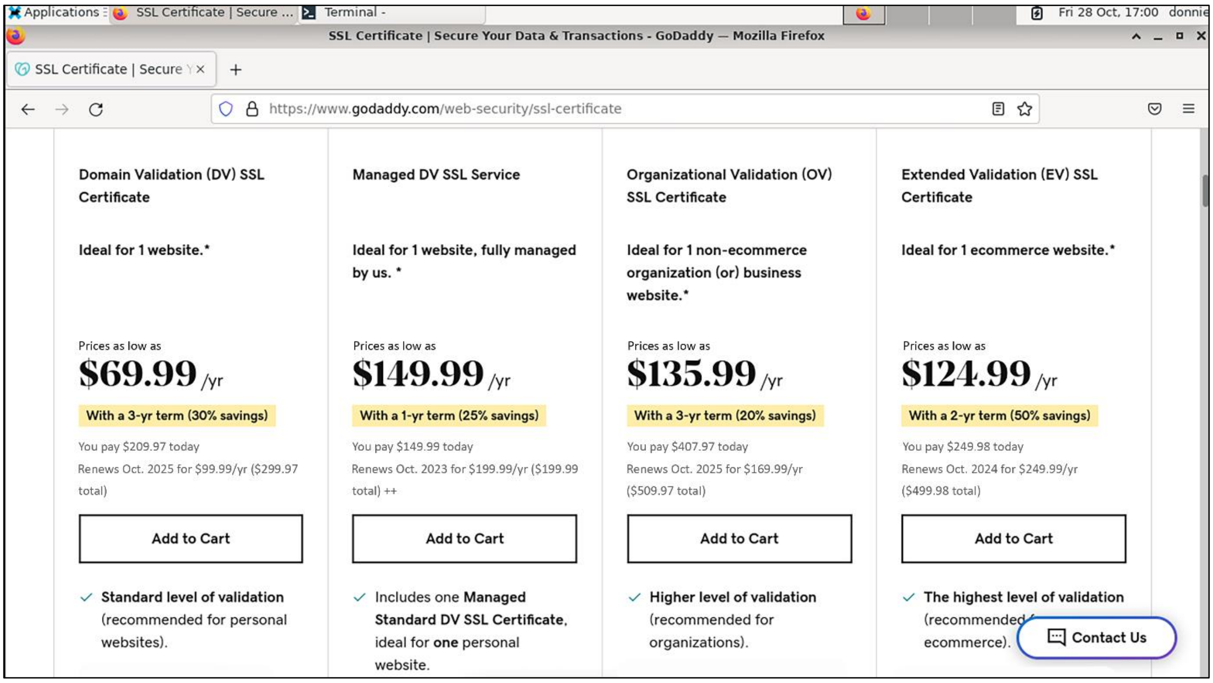
ne/donnie/VirtualBox VMs/Ubuntu22-04-Packt/Ubuntu22-04-Packt_1.vdi

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

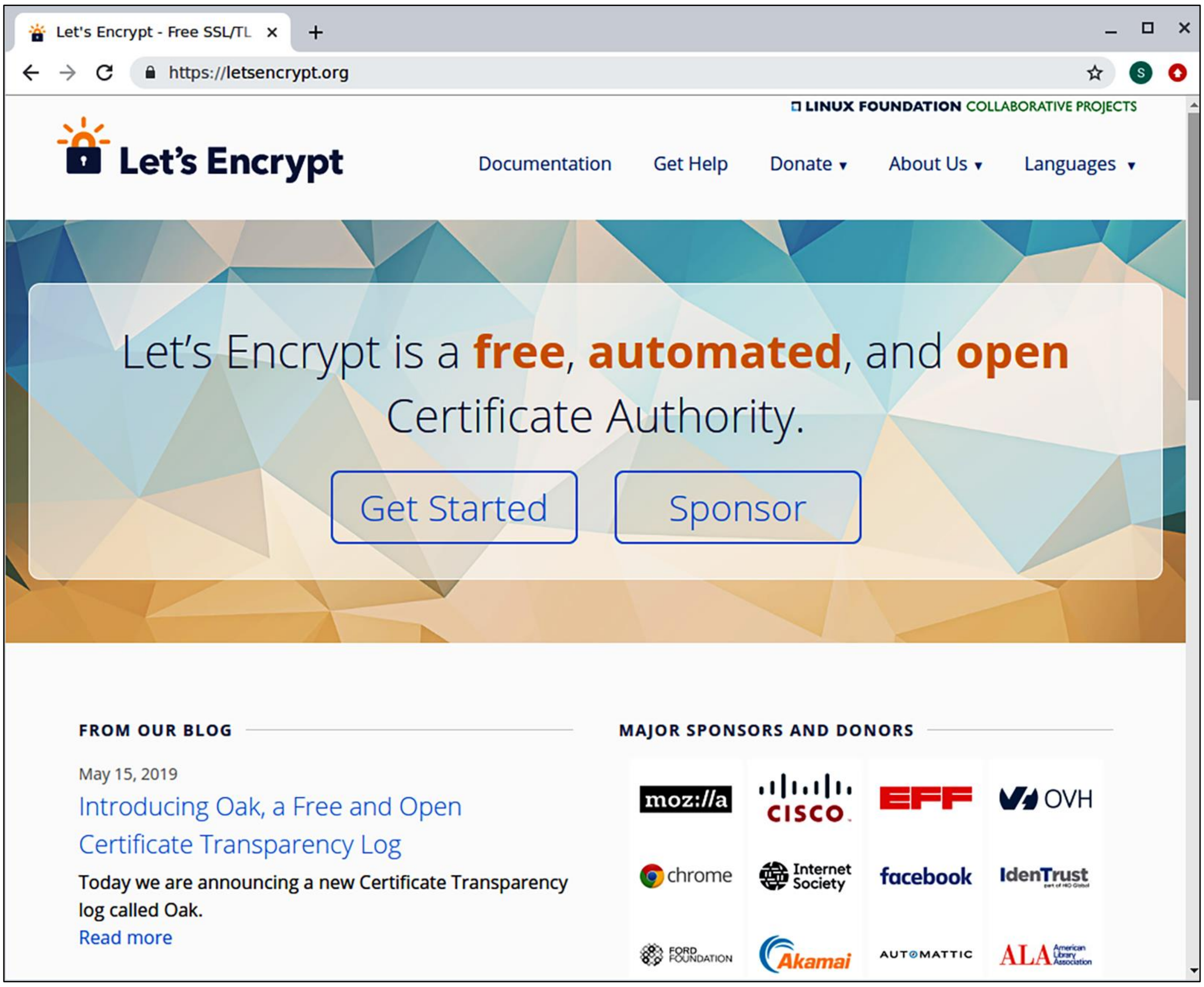
20.00 GB


Activities
VeraCrypt
Oct 28 16:13
VeraCrypt
Volumes Favorites Tools Settings Help
Slot Volume Size Mount Directory Type
1
2
3
4
5
6
7
Create Volume
Volume Properties...
Wipe Cache
Volume
VeraCrypt
☑ Never save history
Select File...
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit


Fortify - Home Page
https://www.fortify.net
FORTIFY
128
10
20
30
40
f
Enter
SSL Check


Applications
SSL Certificate | Secure ...
Terminal -
Fri 28 Oct, 17:00 donnie
SSL Certificate | Secure Your Data & Transactions - GoDaddy — Mozilla Firefox
SSL Certificate | Secure Y
https://www.godaddy.com/web-security/ssl-certificate
Contact Us

Domain Validation (DV) SSL Certificate	Managed DV SSL Service	Organizational Validation (OV) SSL Certificate	Extended Validation (EV) SSL Certificate
Ideal for 1 website.*	Ideal for 1 website, fully managed by us. *	Ideal for 1 non-ecommerce organization (or) business website.*	Ideal for 1 ecommerce website.*
Prices as low as **$69.99** /yr	Prices as low as **$149.99** /yr	Prices as low as **$135.99** /yr	Prices as low as **$124.99** /yr
With a 3-yr term (30% savings)	With a 1-yr term (25% savings)	With a 3-yr term (20% savings)	With a 2-yr term (50% savings)
You pay $209.97 today Renews Oct. 2025 for $99.99/yr ($299.97 total)	You pay $149.99 today Renews Oct. 2023 for $199.99/yr ($199.99 total) ++	You pay $407.97 today Renews Oct. 2025 for $169.99/yr ($509.97 total)	You pay $249.98 today Renews Oct. 2024 for $249.99/yr ($499.98 total)
Add to Cart	Add to Cart	Add to Cart	Add to Cart
✓ **Standard level of validation** (recommended for personal websites).	✓ Includes one **Managed Standard DV SSL Certificate**, ideal for **one** personal website.	✓ **Higher level of validation** (recommended for organizations).	✓ **The highest level of validation** (recommended f ecommerce).



Let's Encrypt is a **free**, **automated**, and **open** Certificate Authority.

FROM OUR BLOG

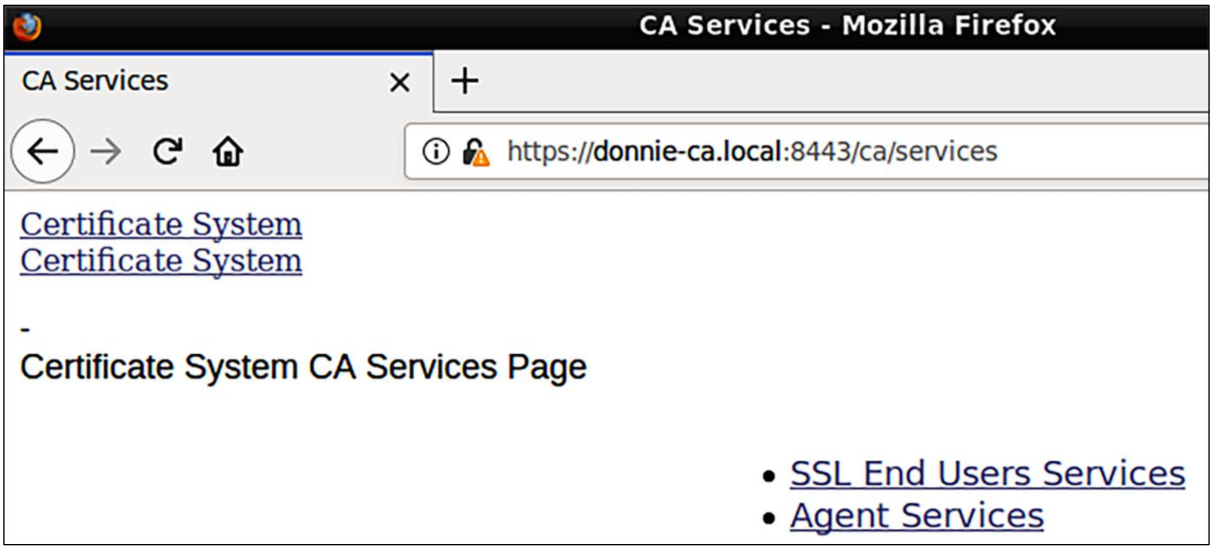
May 15, 2019

Introducing Oak, a Free and Open Certificate Transparency Log

Today we are announcing a new Certificate Transparency log called Oak.

Read more

MAJOR SPONSORS AND DONORS

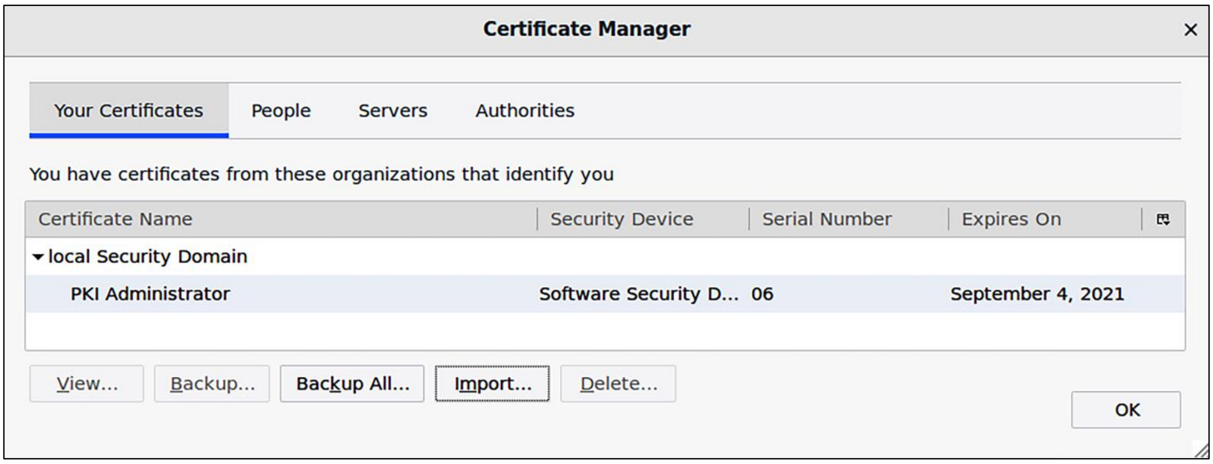


https://donnie-ca.local:8443/ca/services

Certificate System
Certificate System

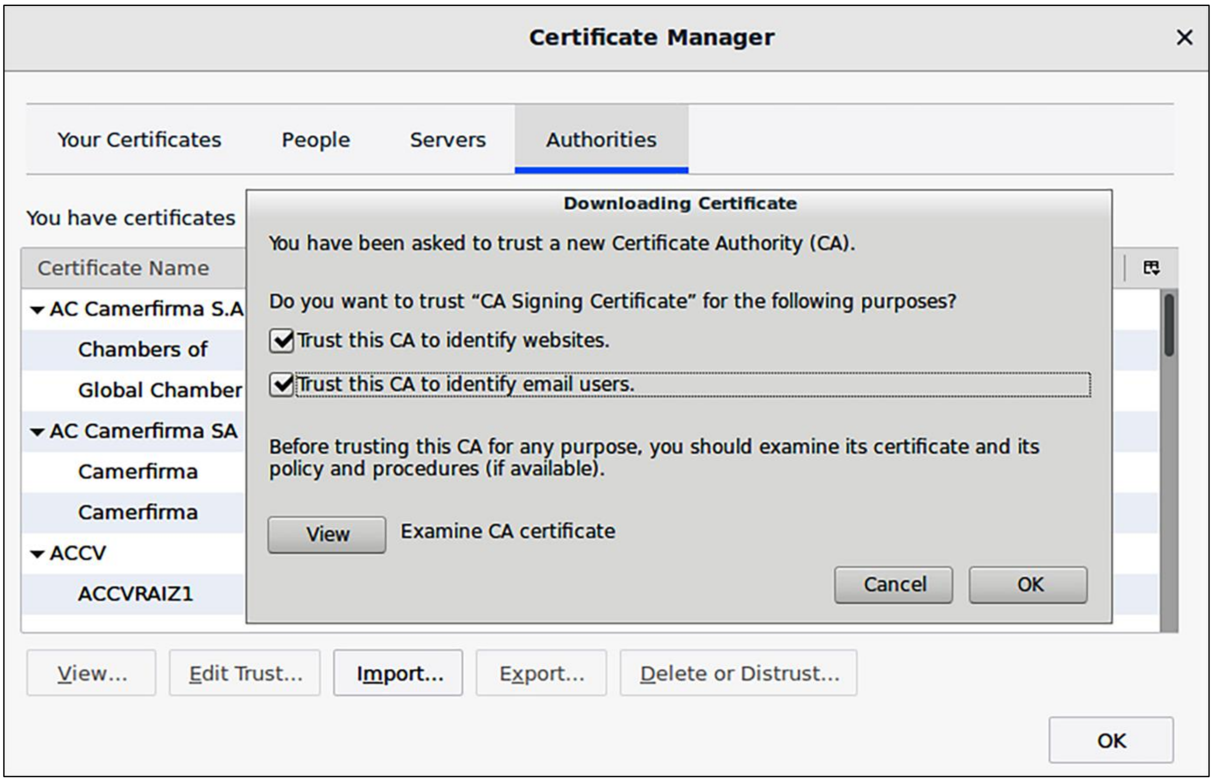
-
Certificate System CA Services Page

- SSL End Users Services
- Agent Services



You have certificates from these organizations that identify you

Certificate Name	Security Device	Serial Number	Expires On
▾ local Security Domain			
PKI Administrator	Software Security D...	06	September 4, 2021



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

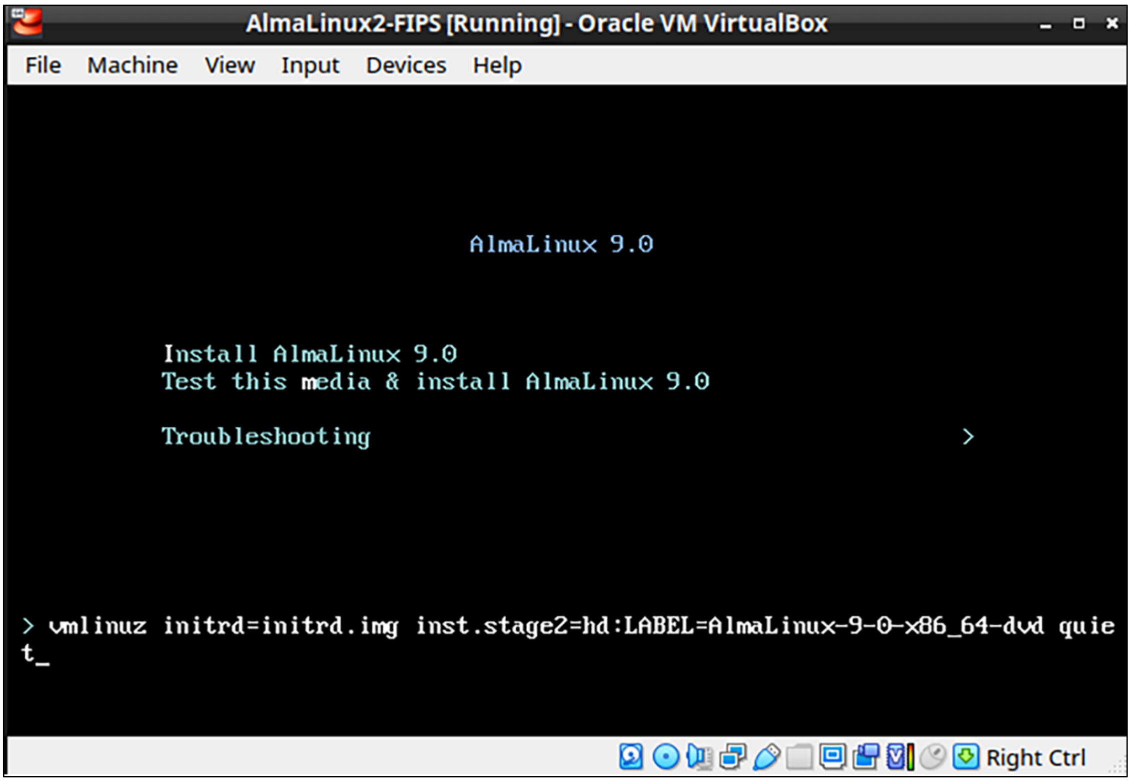
Do you want to trust "CA Signing Certificate" for the following purposes?

☑ Trust this CA to identify websites.

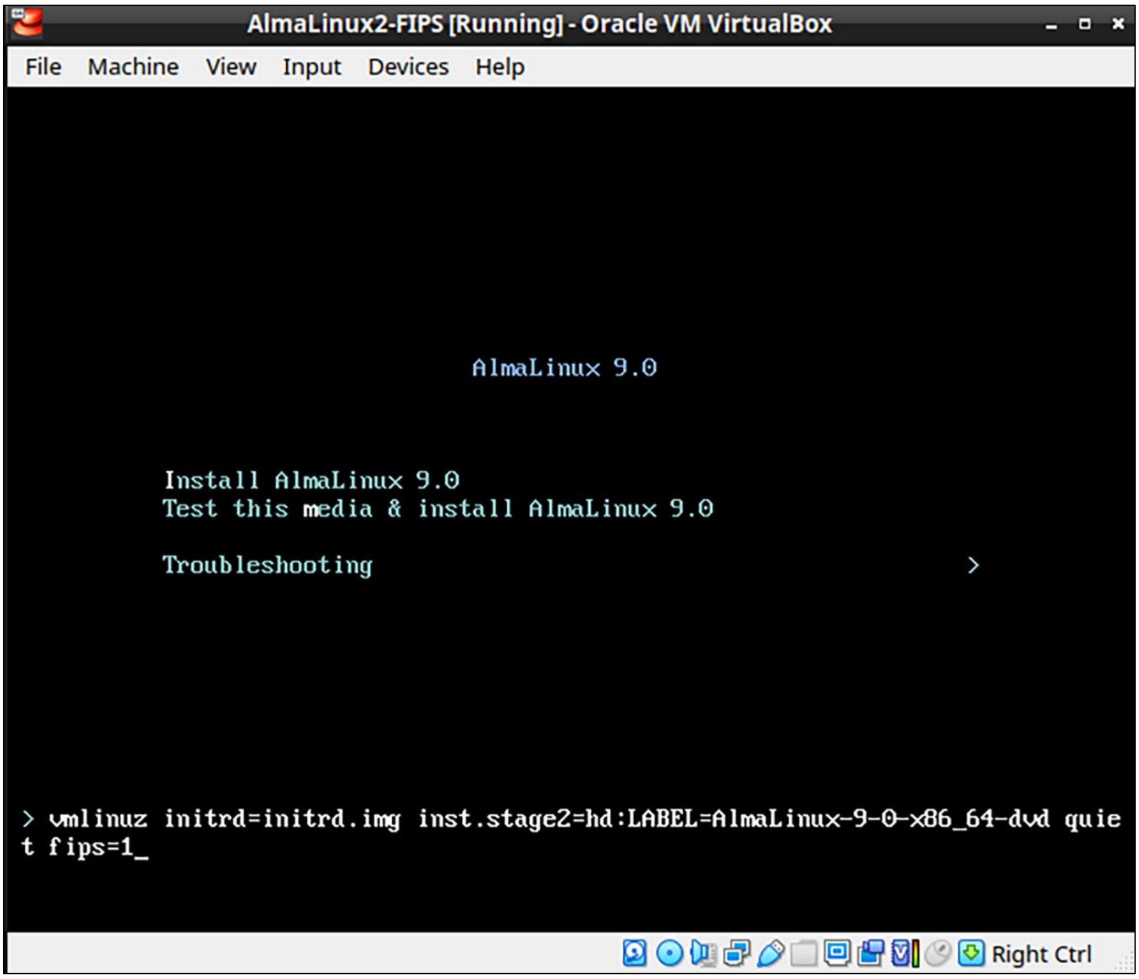
☑ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View Examine CA certificate

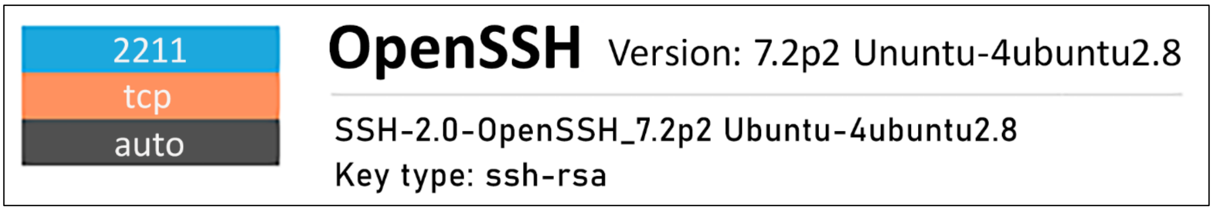

AlmaLinux2-FIPS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
AlmaLinux 9.0

Install AlmaLinux 9.0
Test this media & install AlmaLinux 9.0

Troubleshooting                                          >

> vmlinuz initrd=initrd.img inst.stage2=hd:LABEL=AlmaLinux-9-0-x86_64-dvd quie
t_
```


AlmaLinux2-FIPS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
AlmaLinux 9.0

Install AlmaLinux 9.0
Test this media & install AlmaLinux 9.0

Troubleshooting                                          >

> vmlinuz initrd=initrd.img inst.stage2=hd:LABEL=AlmaLinux-9-0-x86_64-dvd quie
t fips=1_
```

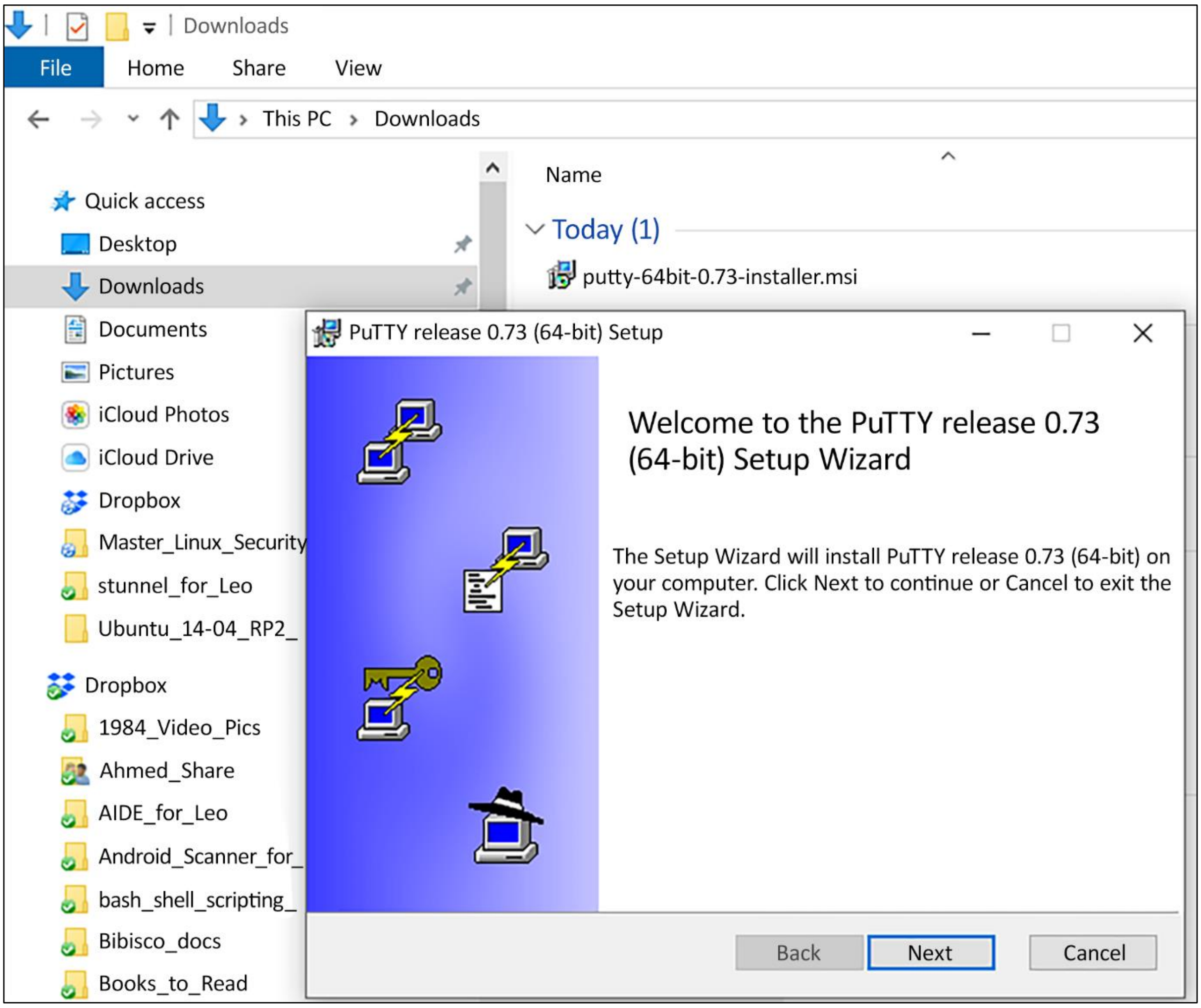
Chapter 7: SSH Hardening



OpenSSH Version: 7.2p2 Ununtu-4ubuntu2.8

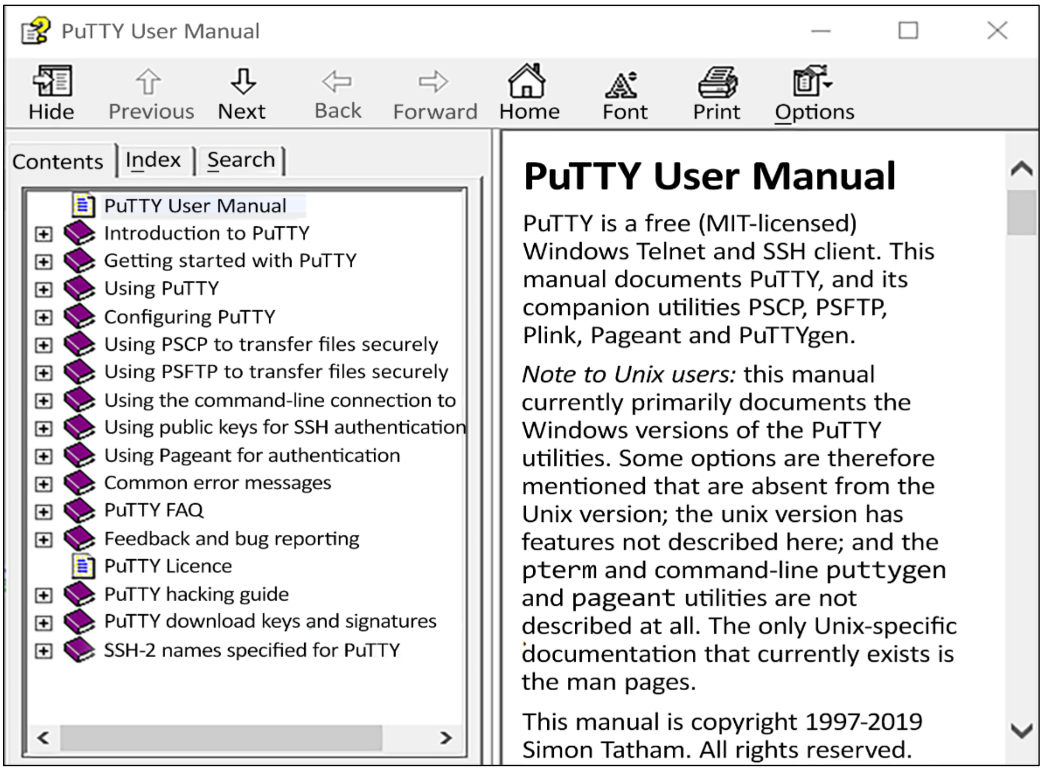
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8

Key type: ssh-rsa



Welcome to the PuTTY release 0.73 (64-bit) Setup Wizard

The Setup Wizard will install PuTTY release 0.73 (64-bit) on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

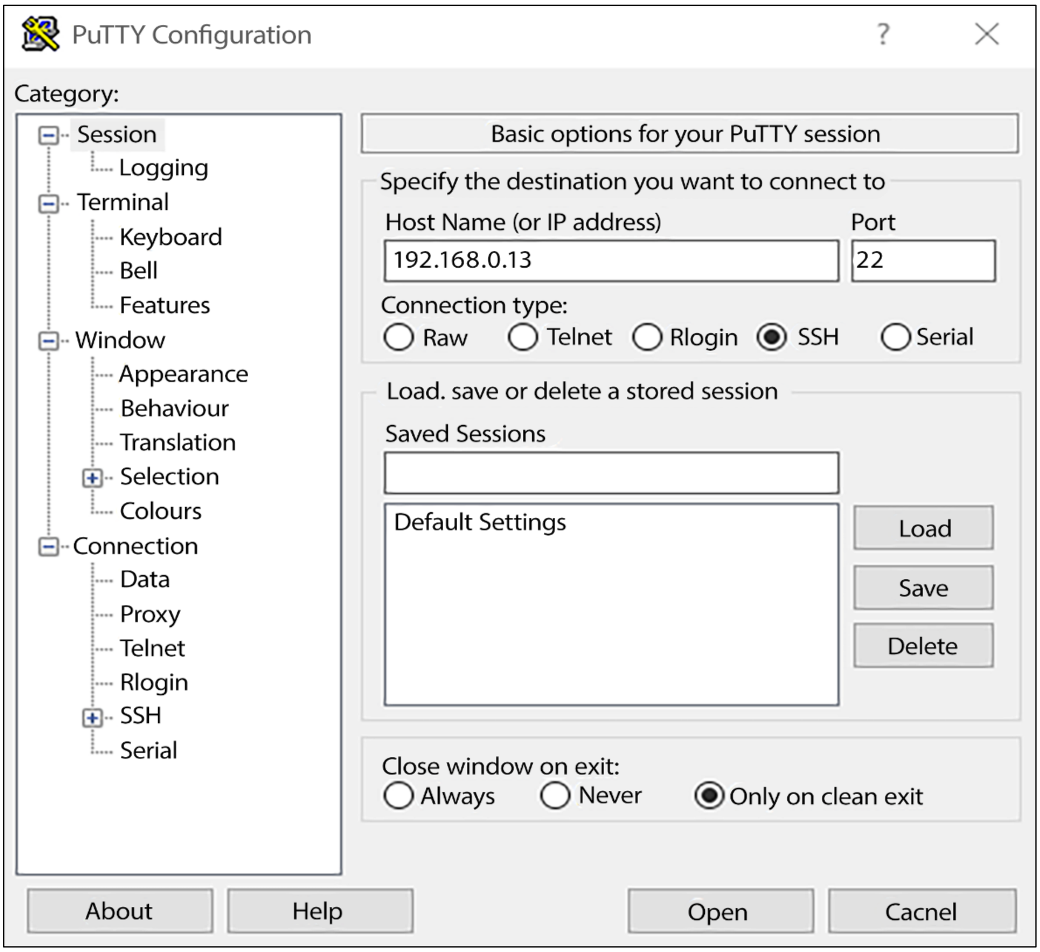

PuTTY User Manual
Hide
Previous
Next
Back
Forward
Home
Font
Print
Options
Contents
Index
Search
PuTTY User Manual
Introduction to PuTTY
Getting started with PuTTY
Using PuTTY
Configuring PuTTY
Using PSCP to transfer files securely
Using PSFTP to transfer files securely
Using the command-line connection to
Using public keys for SSH authentication
Using Pageant for authentication
Common error messages
PuTTY FAQ
Feedback and bug reporting
PuTTY Licence
PuTTY hacking guide
PuTTY download keys and signatures
SSH-2 names specified for PuTTY

PuTTY User Manual

PuTTY is a free (MIT-licensed) Windows Telnet and SSH client. This manual documents PuTTY, and its companion utilities PSCP, PSFTP, Plink, Pageant and PuTTYgen.

Note to Unix users: this manual currently primarily documents the Windows versions of the PuTTY utilities. Some options are therefore mentioned that are absent from the Unix version; the unix version has features not described here; and the `pterm` and command-line `puttygen` and `pageant` utilities are not described at all. The only Unix-specific documentation that currently exists is the man pages.

This manual is copyright 1997-2019 Simon Tatham. All rights reserved.



Specify the destination you want to connect to

Host Name (or IP address): 192.168.0.13

Port: 22

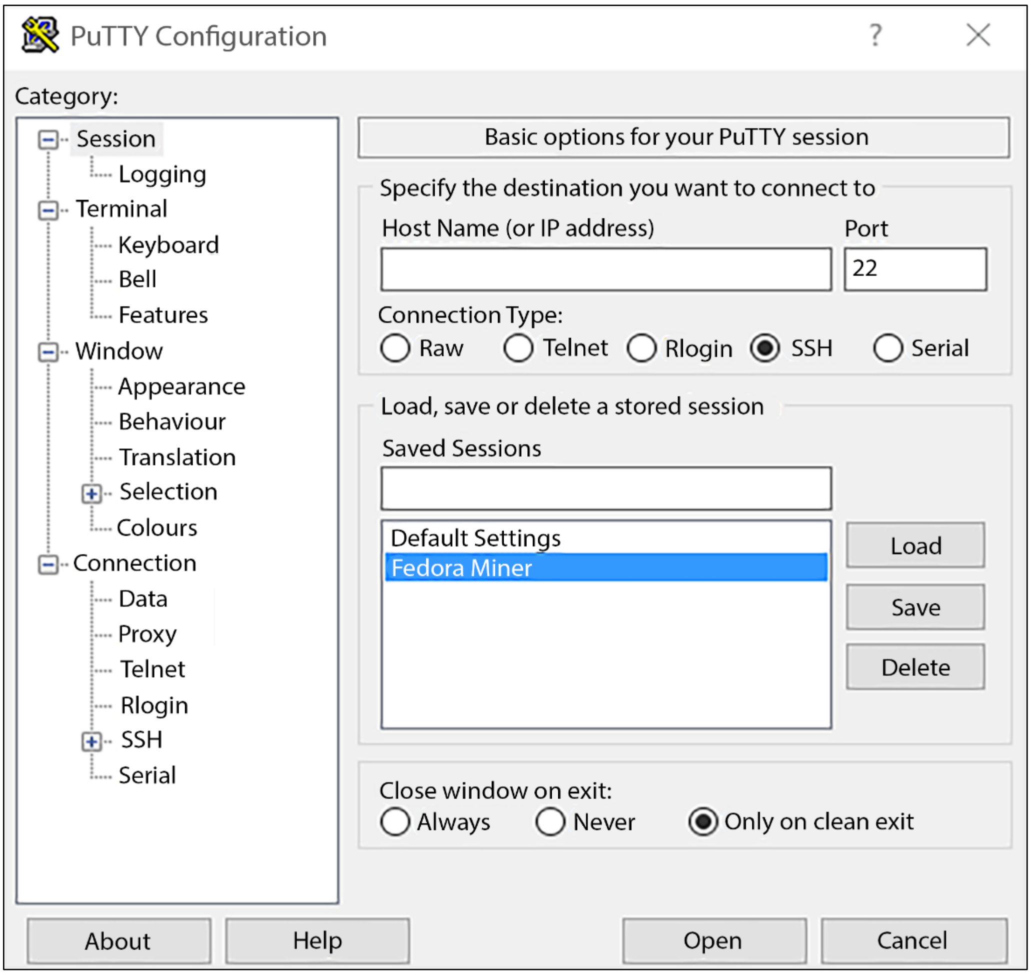
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load. save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit



Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

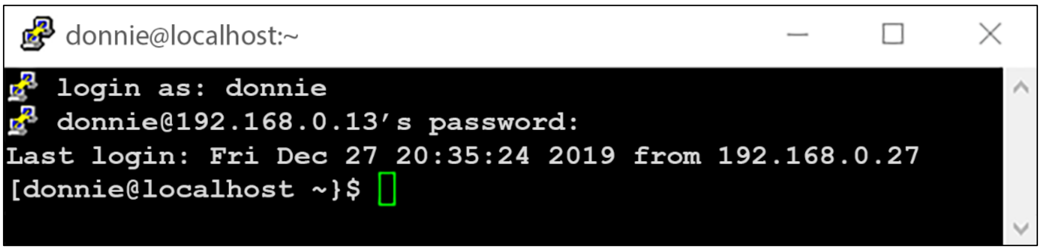
Connection Type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

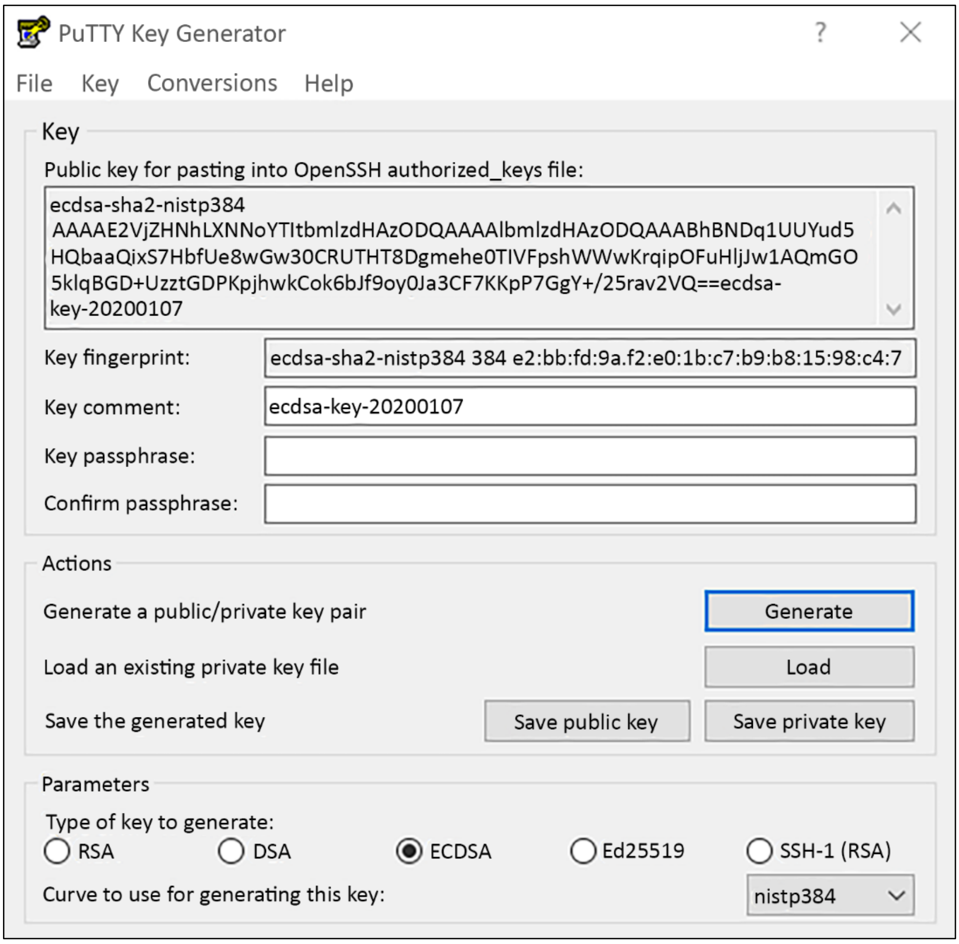
Saved Sessions

Default Settings
Fedora Miner

Close window on exit: ○ Always ○ Never ● Only on clean exit



```
login as: donnie
donnie@192.168.0.13's password:
Last login: Fri Dec 27 20:35:24 2019 from 192.168.0.27
[donnie@localhost ~}$
```



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ecdsa-sha2-nistp384
 AAAAE2VjZHNhLXNNoYTItbmlzdHAzODQAAAAlbmlzdHAzODQAAABhBNDq1UUYud5
HQbaaQixS7HbfUe8wGw30CRUTHT8Dgmehe0TIVFpshWWwKrqipOFuHljJw1AQmGO
5klqBGD+UzztGDPKpjhwkCok6bJf9oy0Ja3CF7KKpP7GgY+/25rav2VQ==ecdsa-
key-20200107
```

Key fingerprint: ecdsa-sha2-nistp384 384 e2:bb:fd:9a.f2:e0:1b:c7:b9:b8:15:98:c4:7

Key comment: ecdsa-key-20200107

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

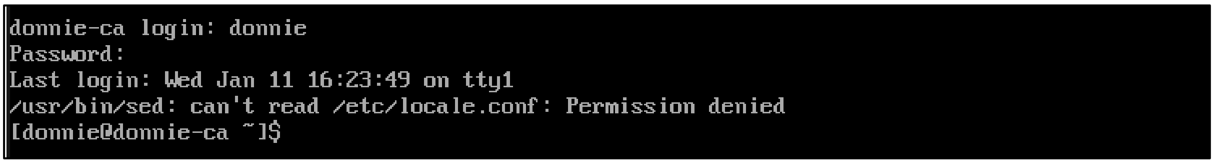
Parameters

Type of key to generate:

○ RSA ○ DSA ● ECDSA ○ Ed25519 ○ SSH-1 (RSA)

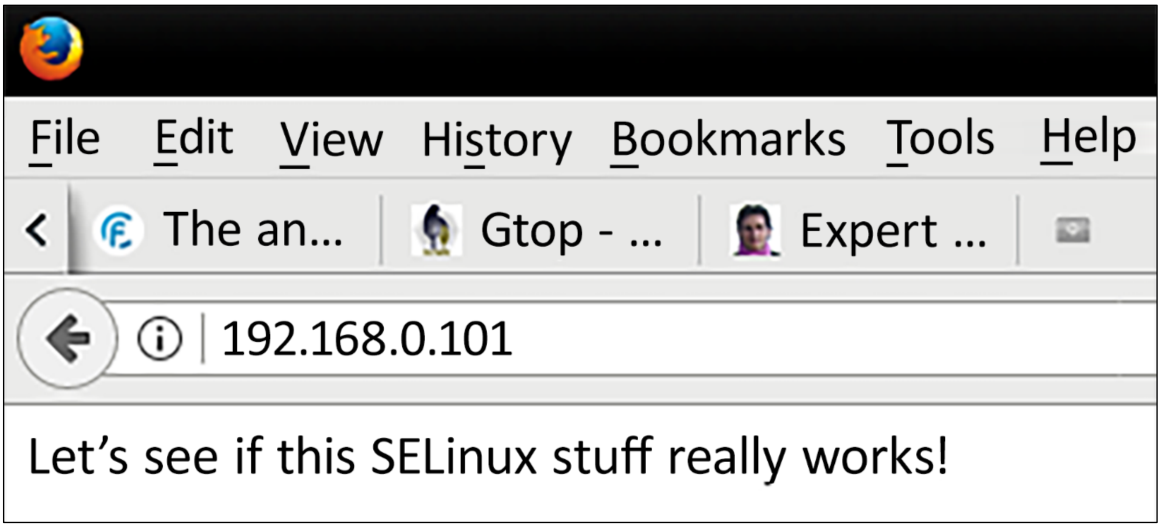
Curve to use for generating this key: nistp384

Chapter 8: Mastering Discretionary Access Control

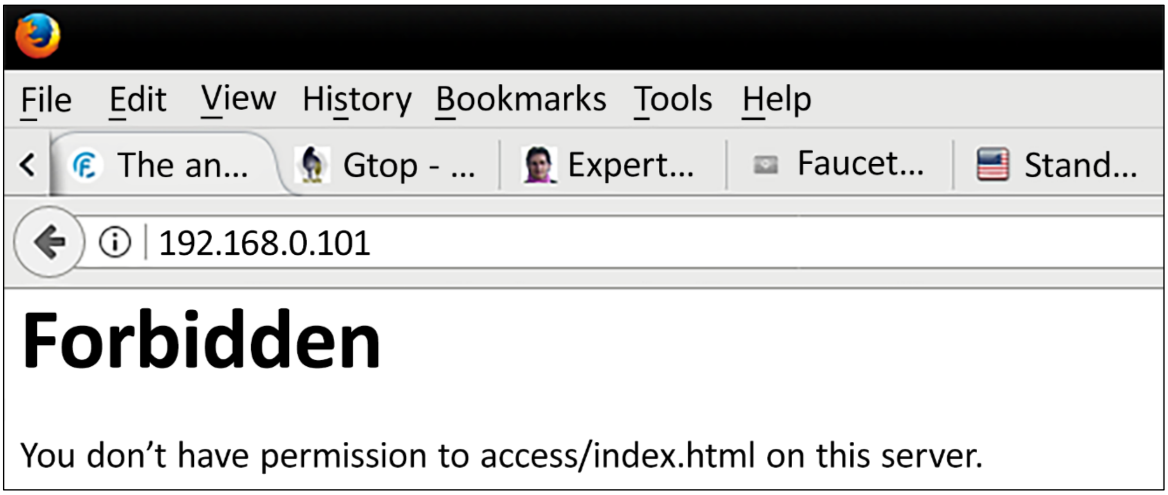


```
donnie-ca login: donnie
Password:
Last login: Wed Jan 11 16:23:49 on tty1
/usr/bin/sed: can't read /etc/locale.conf: Permission denied
[donnie@donnie-ca ~]$
```

Chapter 10: Implementing Mandatory Access Control with SELinux and AppArmor

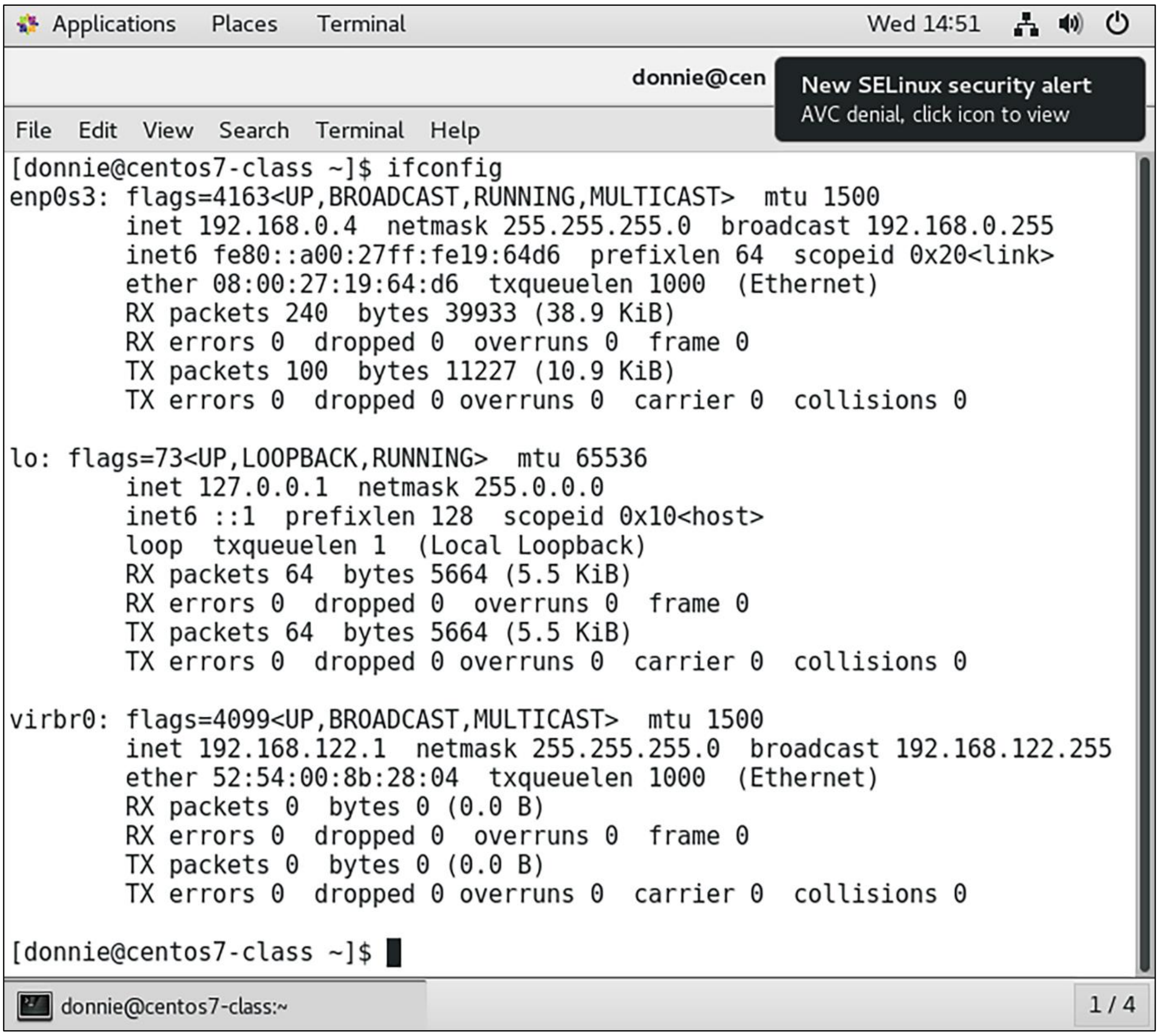


Let’s see if this SELinux stuff really works!

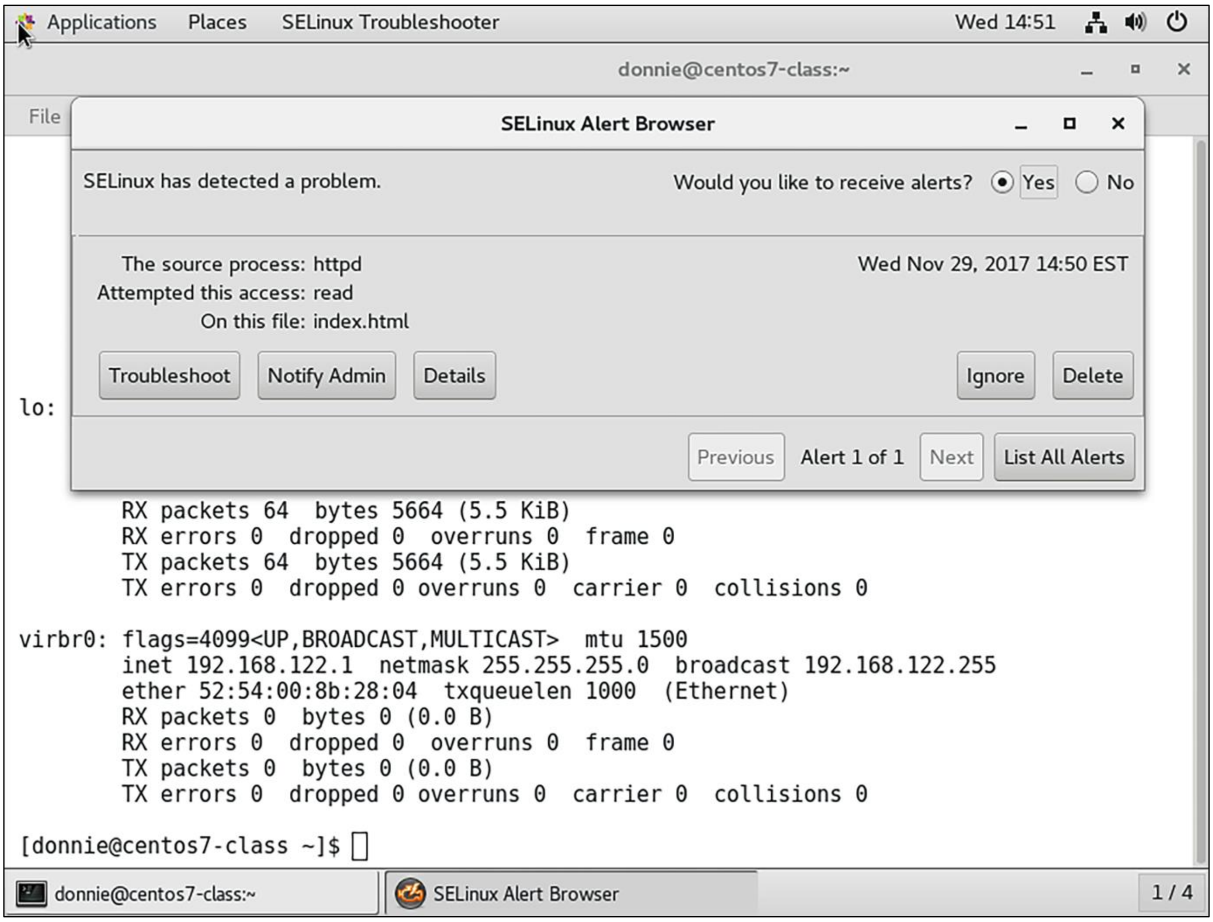


Forbidden

You don’t have permission to access/index.html on this server.



```
[donnie@centos7-class ~]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.4  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe19:64d6  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:19:64:d6  txqueuelen 1000  (Ethernet)
        RX packets 240  bytes 39933 (38.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 100  bytes 11227 (10.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 64  bytes 5664 (5.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 64  bytes 5664 (5.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 52:54:00:8b:28:04  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[donnie@centos7-class ~]$ 
```



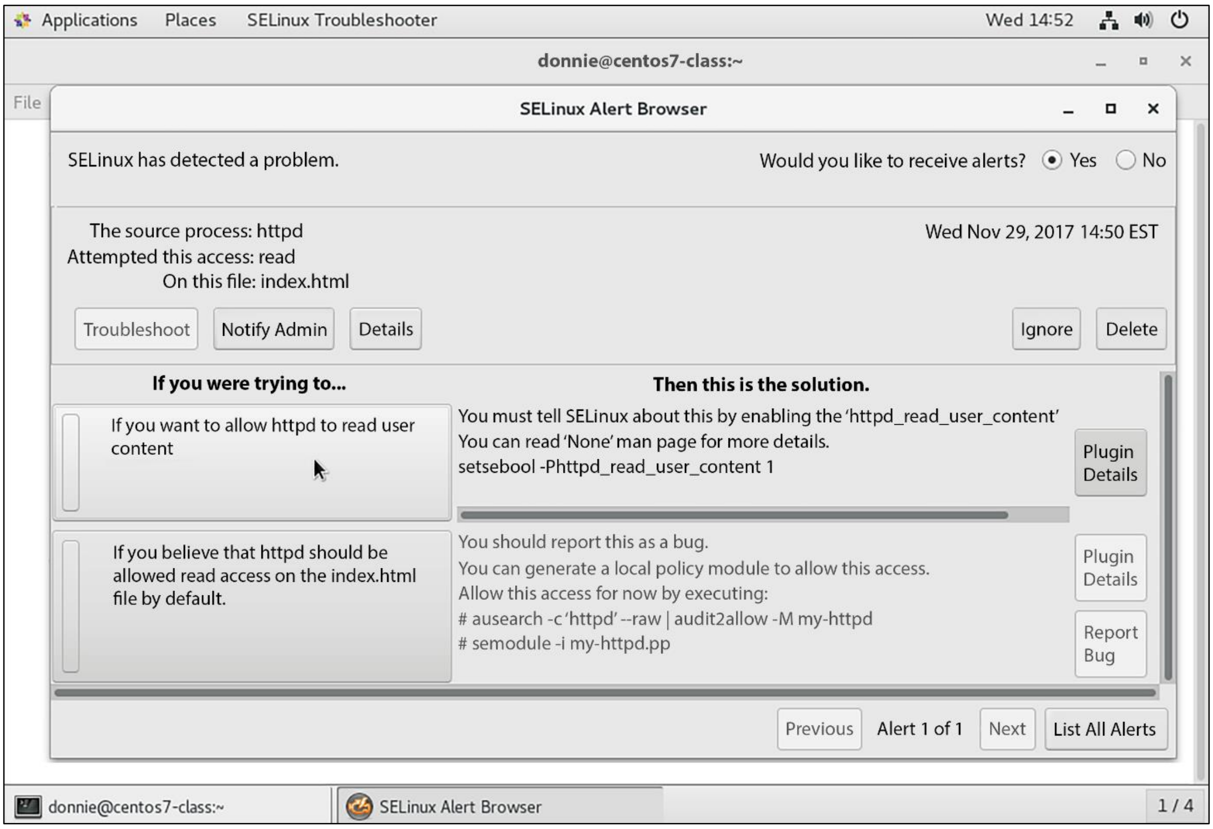
SELinux has detected a problem.

Would you like to receive alerts? ● Yes ○ No

The source process: httpd
Attempted this access: read
On this file: index.html

Wed Nov 29, 2017 14:50 EST

```
lo:
        RX packets 64  bytes 5664 (5.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 64  bytes 5664 (5.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 52:54:00:8b:28:04  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[donnie@centos7-class ~]$
```



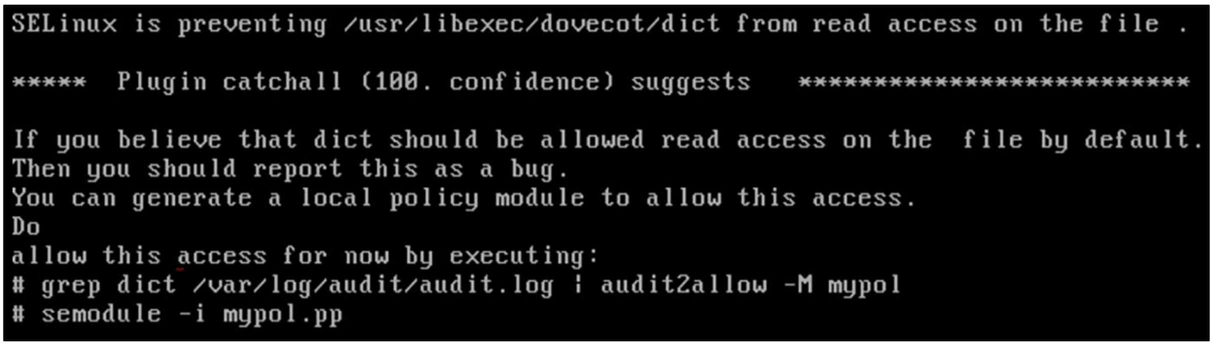
SELinux has detected a problem.

Would you like to receive alerts? ● Yes ○ No

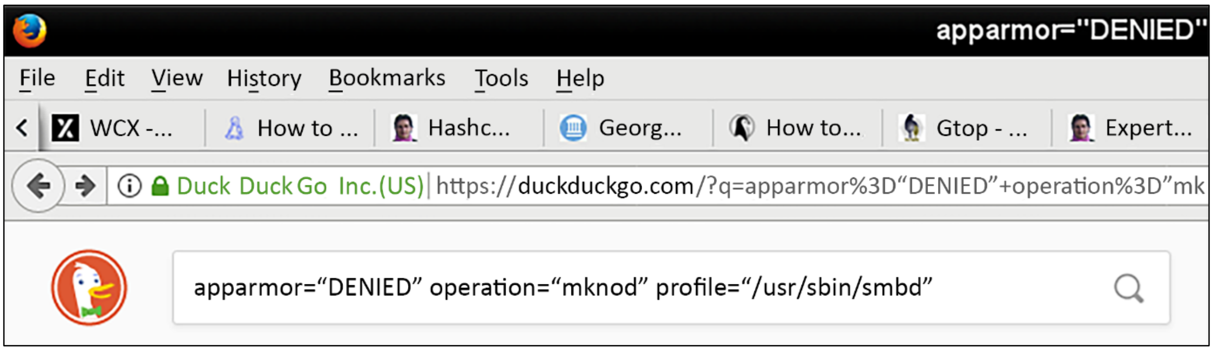
The source process: httpd
Attempted this access: read
On this file: index.html

Wed Nov 29, 2017 14:50 EST

If you were trying to...	Then this is the solution.
If you want to allow httpd to read user content	You must tell SELinux about this by enabling the 'httpd_read_user_content' You can read 'None' man page for more details. setsebool -Phttpd_read_user_content 1
If you believe that httpd should be allowed read access on the index.html file by default.	You should report this as a bug. You can generate a local policy module to allow this access. Allow this access for now by executing: # ausearch -c 'httpd' --raw | audit2allow -M my-httpd # semodule -i my-httpd.pp

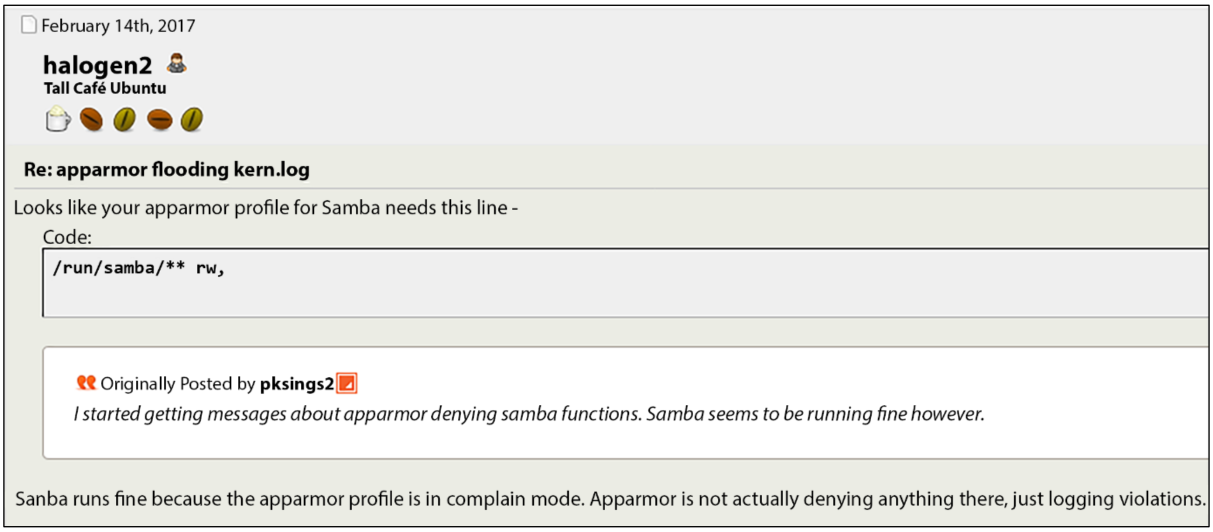


```
SELinux is preventing /usr/libexec/dovecot/dict from read access on the file .

*****  Plugin catchall (100. confidence) suggests   **************************

If you believe that dict should be allowed read access on the  file by default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
# grep dict /var/log/audit/audit.log | audit2allow -M mypol
# semodule -i mypol.pp
```



https://duckduckgo.com/?q=apparmor%3D“DENIED”+operation%3D”mk

apparmor=“DENIED” operation=“mknod” profile=“/usr/sbin/smbd”



February 14th, 2017

halogen2
Tall Café Ubuntu

Re: apparmor flooding kern.log

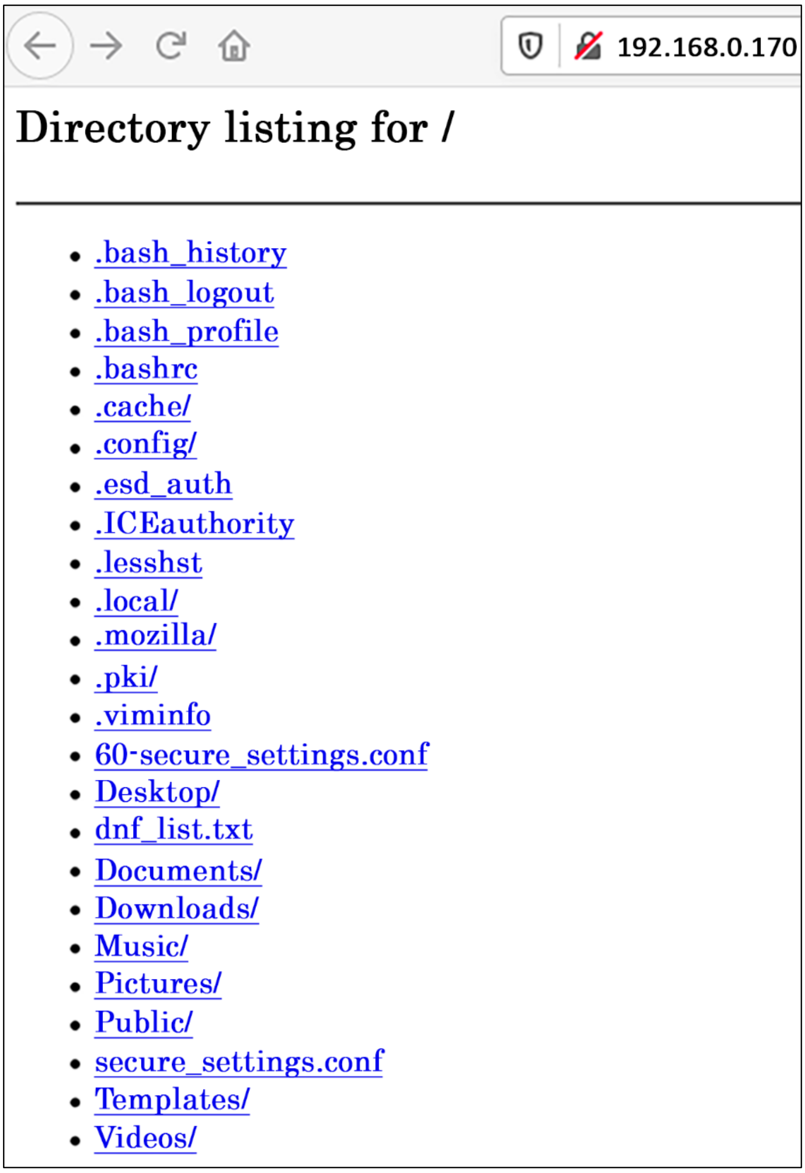
Looks like your apparmor profile for Samba needs this line -

Code:

```
/run/samba/** rw,
```

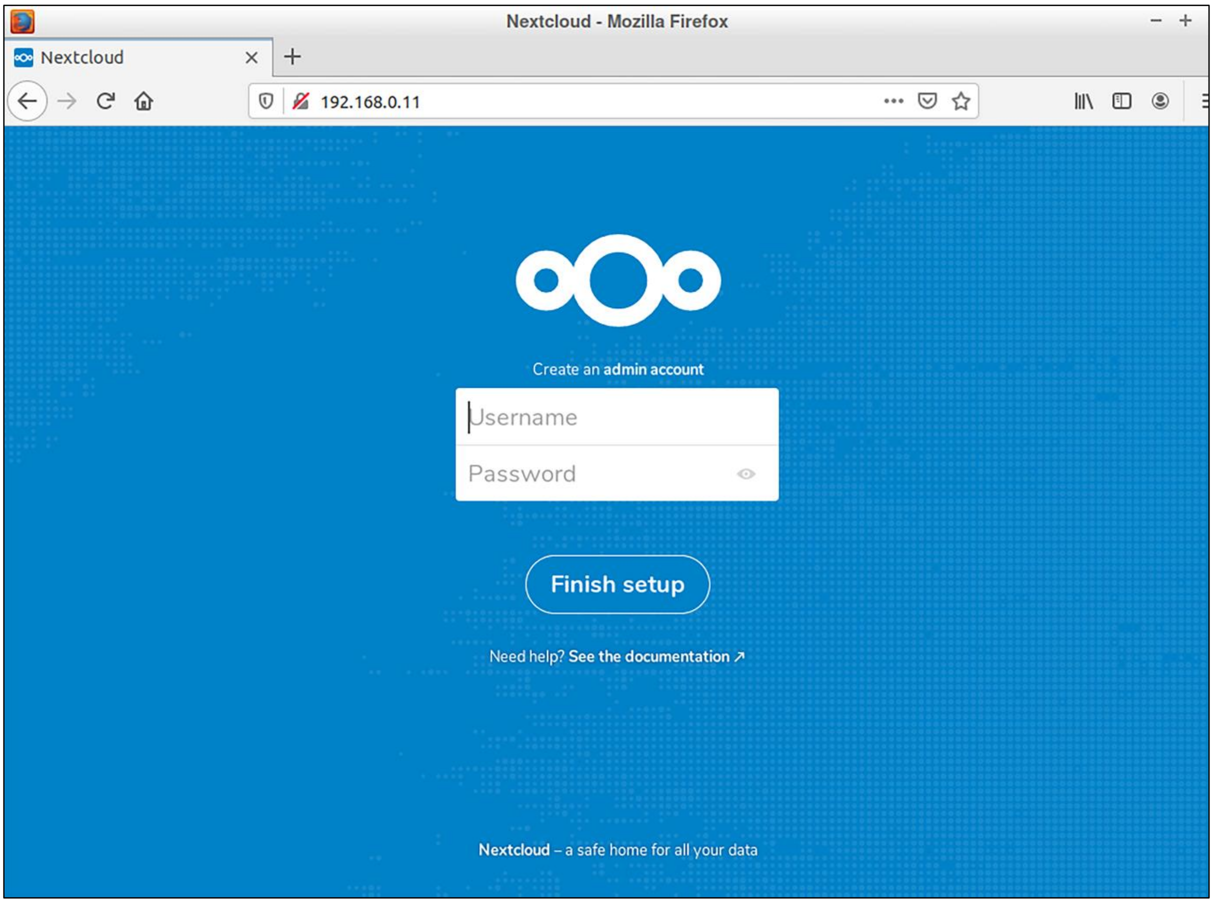
> Originally Posted by **pksings2**
> *I started getting messages about apparmor denying samba functions. Samba seems to be running fine however.*

Sanba runs fine because the apparmor profile is in complain mode. Apparmor is not actually denying anything there, just logging violations.



Directory listing for /

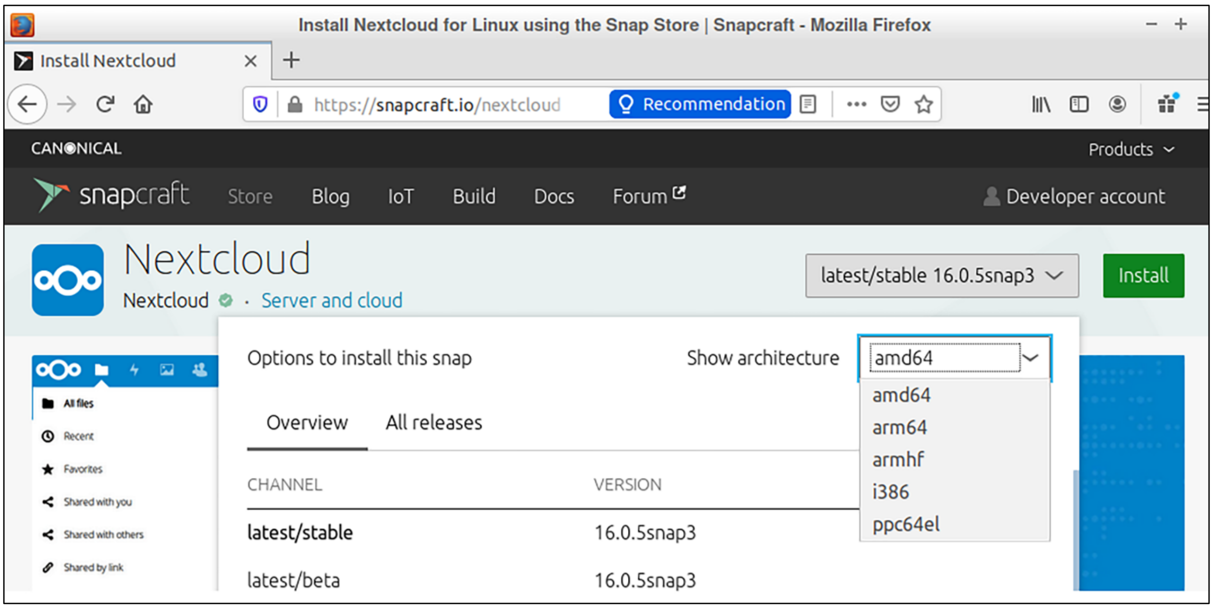
- .bash_history
- .bash_logout
- .bash_profile
- .bashrc
- .cache/
- .config/
- .esd_auth
- .ICEauthority
- .lesshst
- .local/
- .mozilla/
- .pki/
- .viminfo
- 60-secure_settings.conf
- Desktop/
- dnf_list.txt
- Documents/
- Downloads/
- Music/
- Pictures/
- Public/
- secure_settings.conf
- Templates/
- Videos/



Create an admin account

Need help? See the documentation ↗

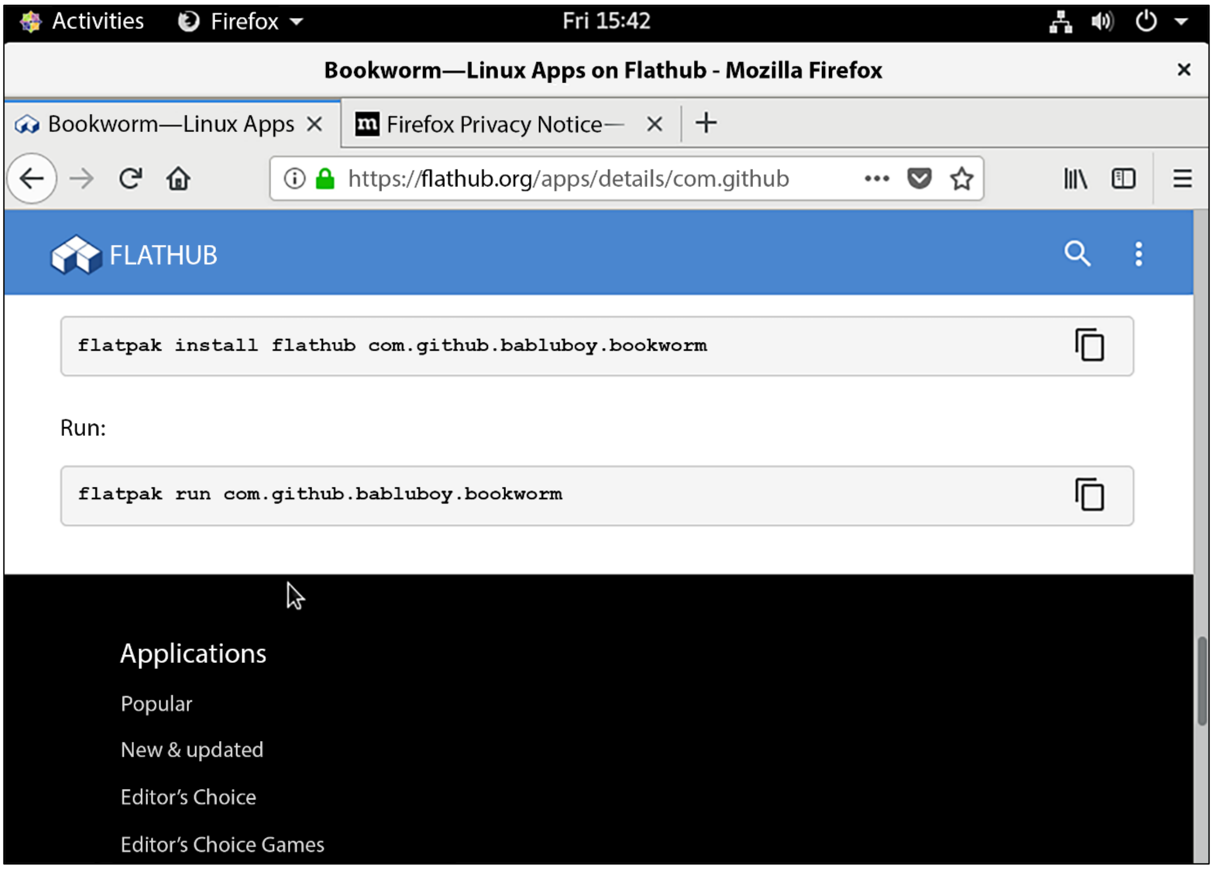
Nextcloud – a safe home for all your data



Options to install this snap

Show architecture: amd64

CHANNEL	VERSION
latest/stable	16.0.5snap3
latest/beta	16.0.5snap3



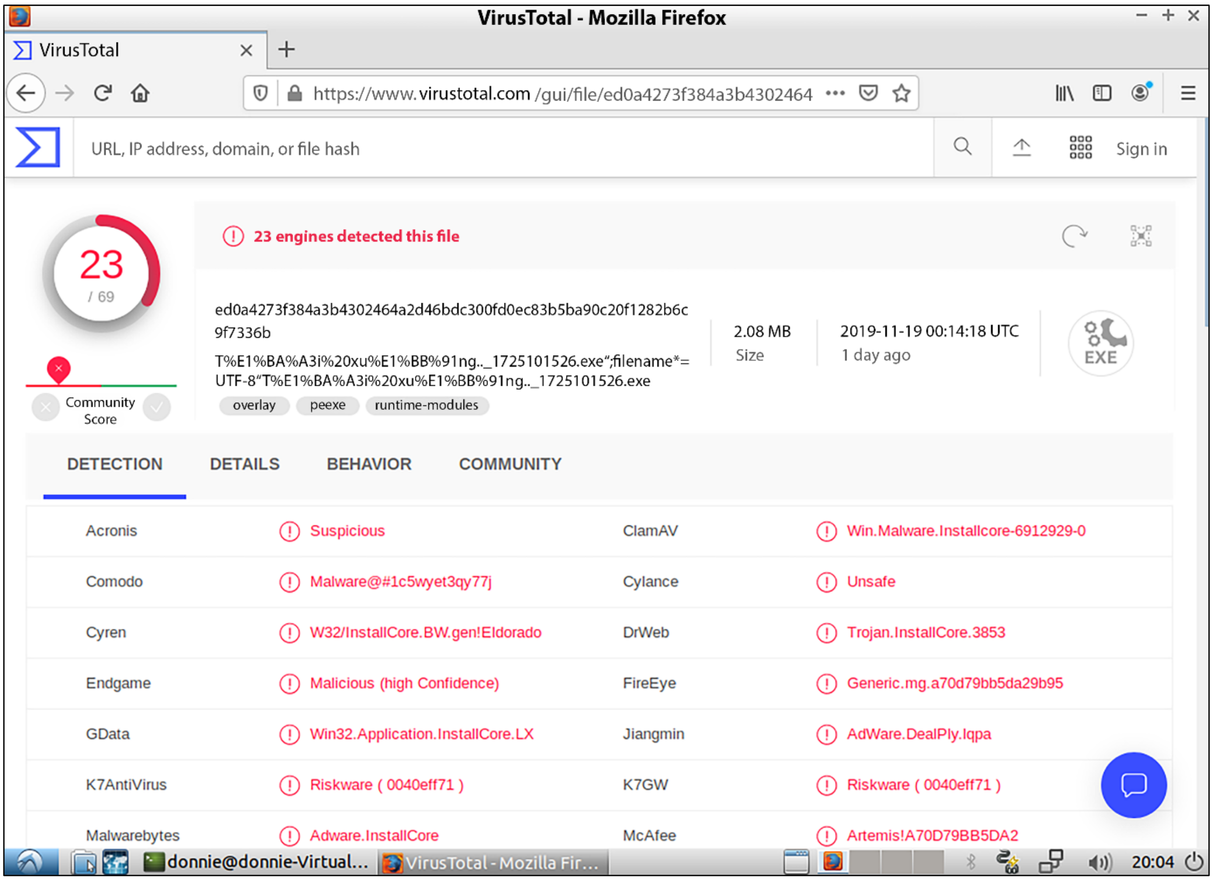
Activities
Firefox
Fri 15:42
Bookworm—Linux Apps on Flathub - Mozilla Firefox
Bookworm—Linux Apps
Firefox Privacy Notice—
https://flathub.org/apps/details/com.github
FLATHUB

```
flatpak install flathub com.github.babluboy.bookworm
```

Run:

```
flatpak run com.github.babluboy.bookworm
```

Chapter 12: Scanning, Auditing, and Hardening



VirusTotal - Mozilla Firefox
VirusTotal
https://www.virustotal.com/gui/file/ed0a4273f384a3b4302464
URL, IP address, domain, or file hash
Sign in
23
/ 69
Community Score

23 engines detected this file

ed0a4273f384a3b4302464a2d46bdc300fd0ec83b5ba90c20f1282b6c9f7336b

T%E1%BA%A3i%20xu%E1%BB%91ng.._1725101526.exe";filename*=UTF-8"T%E1%BA%A3i%20xu%E1%BB%91ng.._1725101526.exe

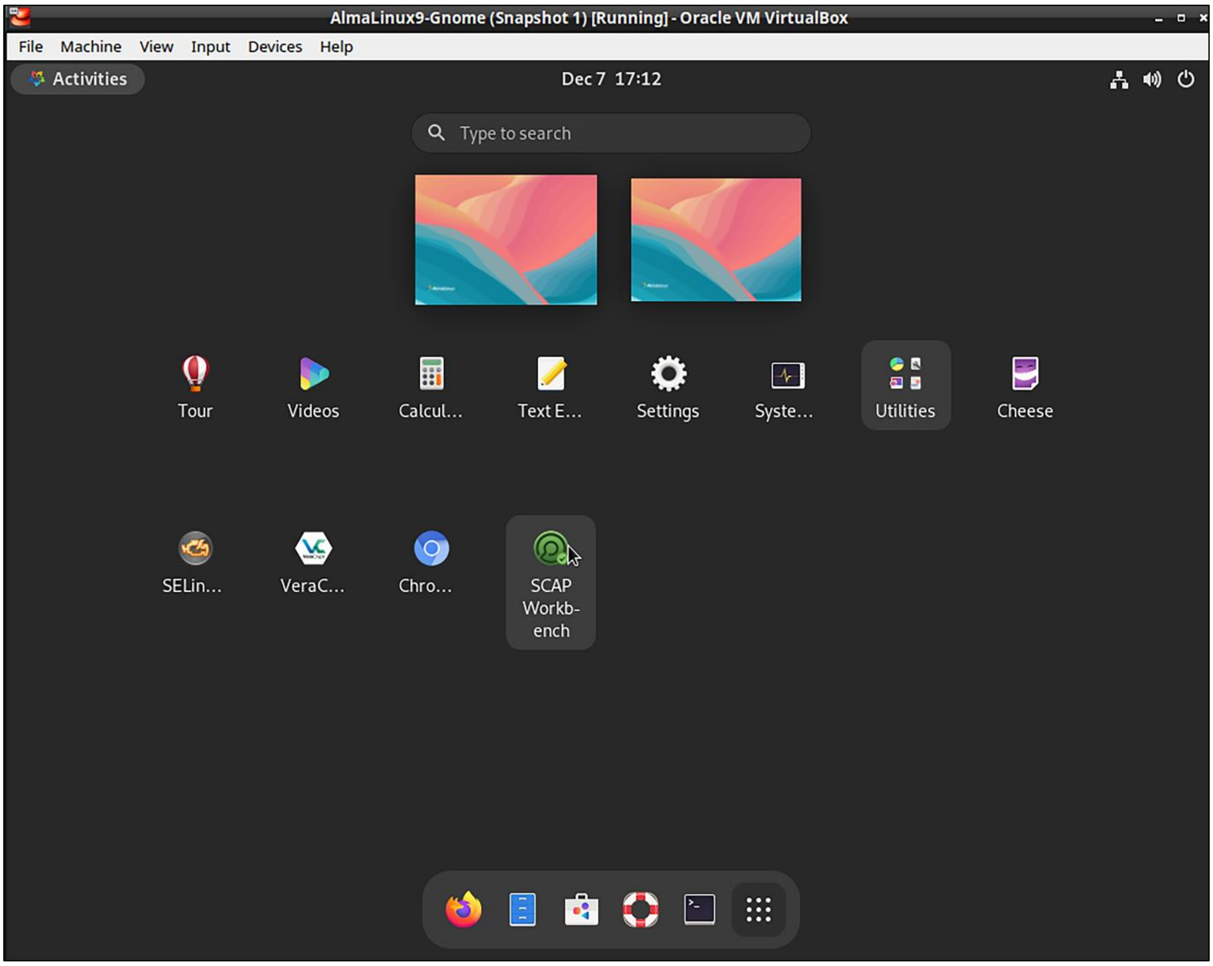
overlay peexe runtime-modules

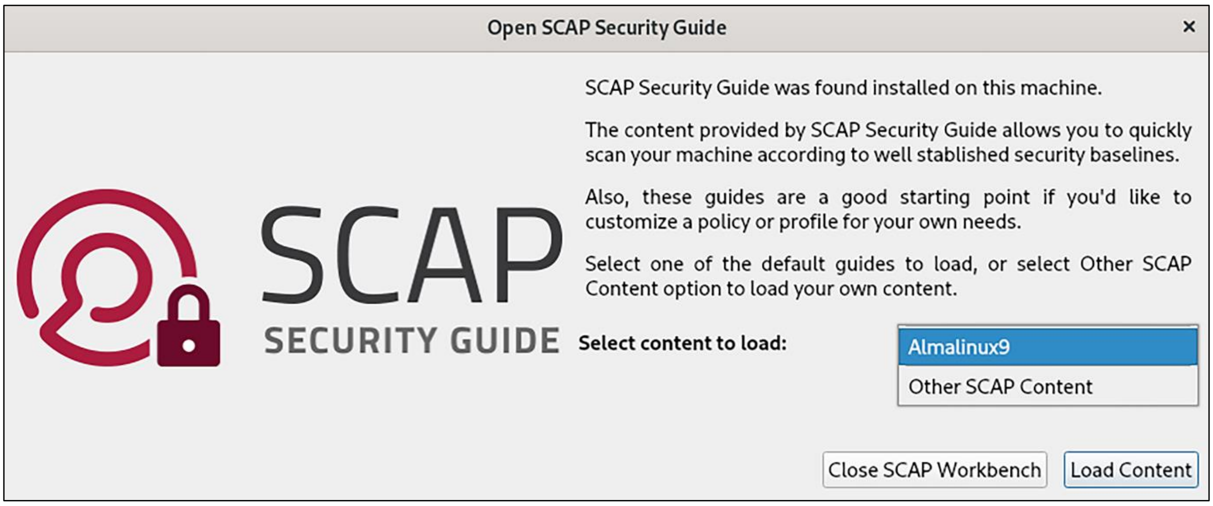
2.08 MB
Size

2019-11-19 00:14:18 UTC
1 day ago

EXE
DETECTION
DETAILS
BEHAVIOR
COMMUNITY

Acronis	Suspicious	ClamAV	Win.Malware.Installcore-6912929-0
Comodo	Malware@#1c5wyet3qy77j	Cylance	Unsafe
Cyren	W32/InstallCore.BW.gen!Eldorado	DrWeb	Trojan.InstallCore.3853
Endgame	Malicious (high Confidence)	FireEye	Generic.mg.a70d79bb5da29b95
GData	Win32.Application.InstallCore.LX	Jiangmin	AdWare.DealPly.lqpa
K7AntiVirus	Riskware (0040eff71)	K7GW	Riskware (0040eff71)
Malwarebytes	Adware.InstallCore	McAfee	Artemis!A70D79BB5DA2





SCAP Security Guide was found installed on this machine.

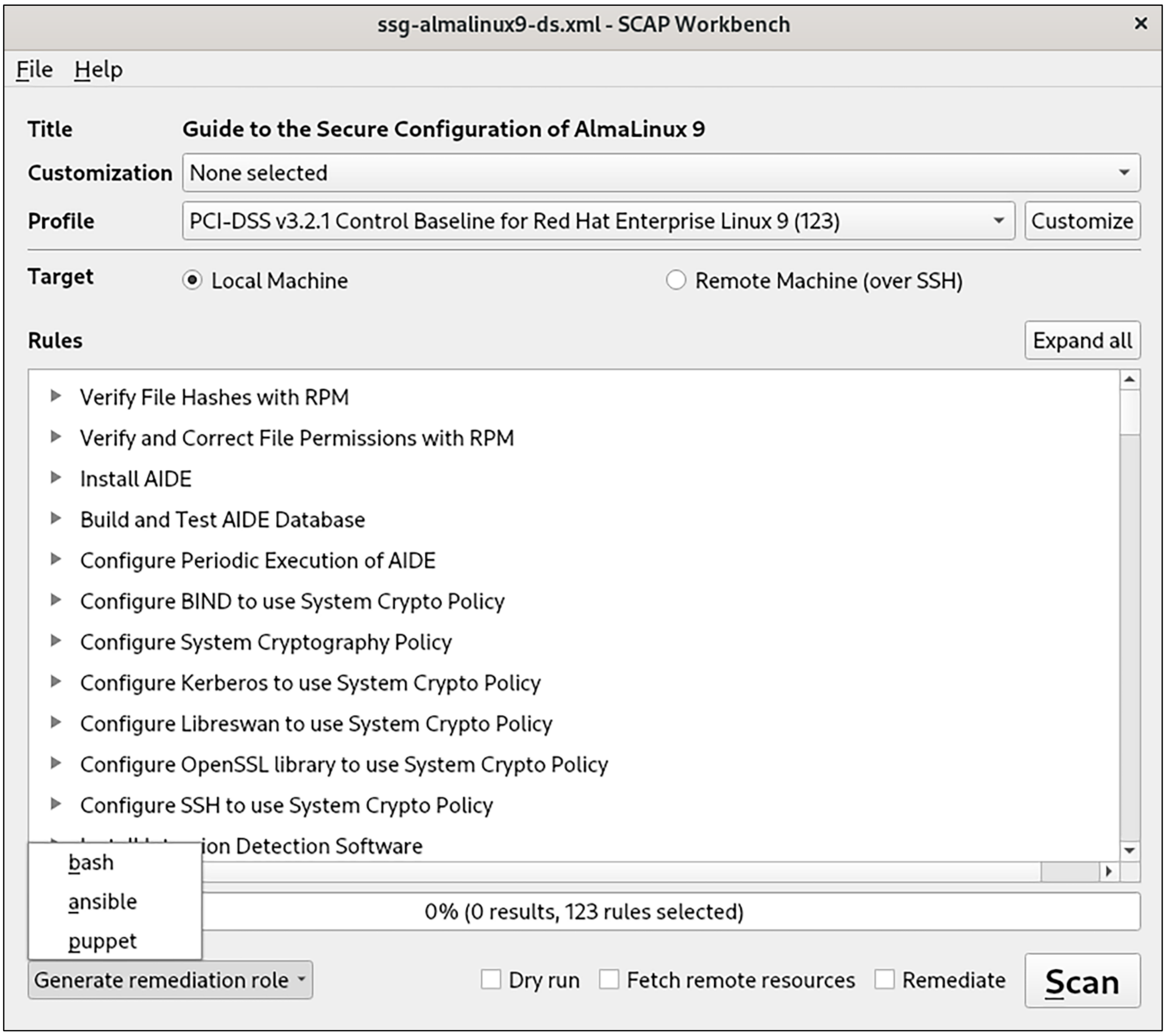
The content provided by SCAP Security Guide allows you to quickly scan your machine according to well stablished security baselines.

Also, these guides are a good starting point if you'd like to customize a policy or profile for your own needs.

Select one of the default guides to load, or select Other SCAP Content option to load your own content.

Select content to load: Almalinux9

Other SCAP Content



ssg-almalinux9-ds.xml - SCAP Workbench

Title: Guide to the Secure Configuration of AlmaLinux 9

Customization: None selected

Profile: PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 9 (123)

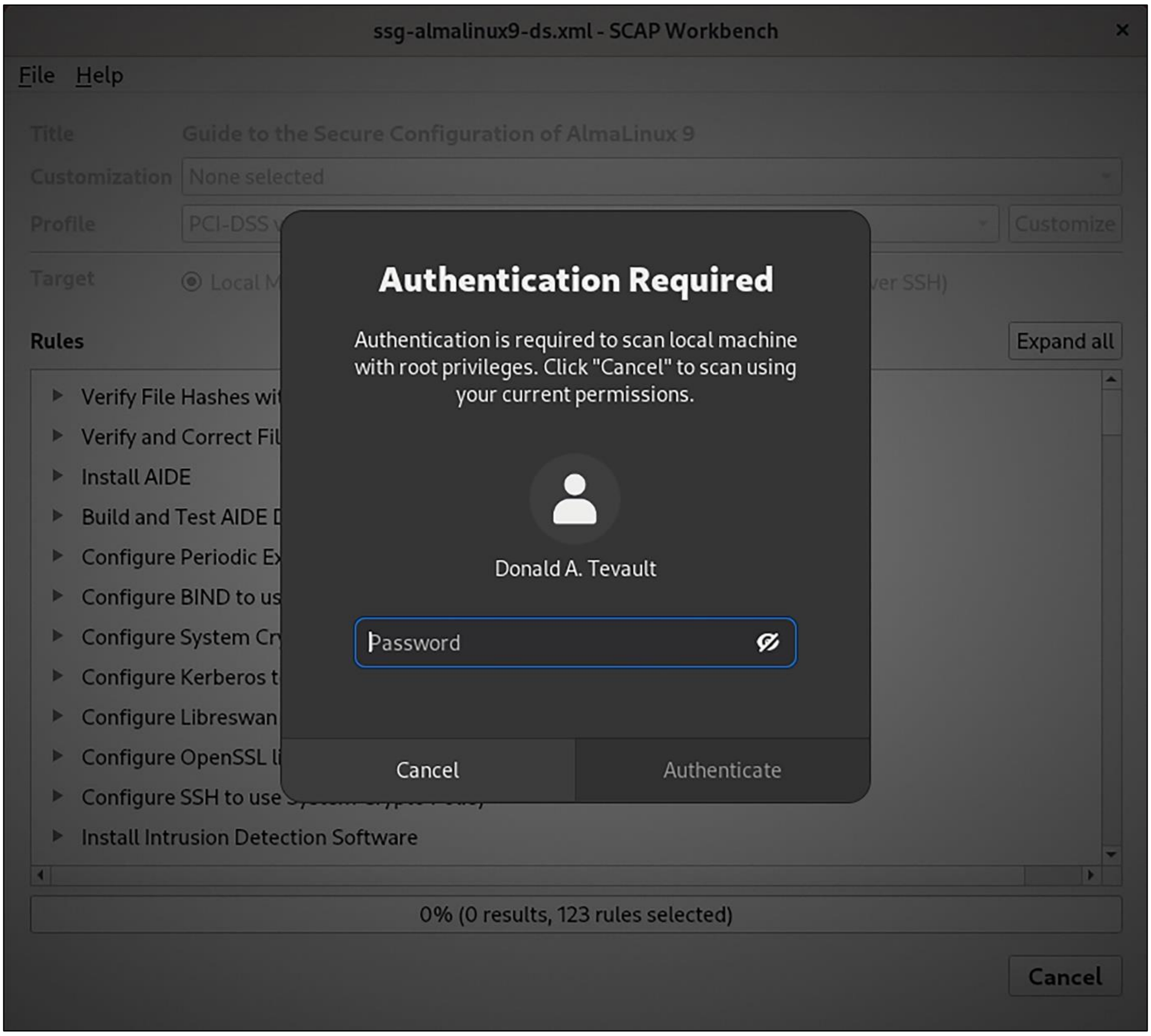
Target: ● Local Machine ○ Remote Machine (over SSH)

Rules

- Verify File Hashes with RPM
- Verify and Correct File Permissions with RPM
- Install AIDE
- Build and Test AIDE Database
- Configure Periodic Execution of AIDE
- Configure BIND to use System Crypto Policy
- Configure System Cryptography Policy
- Configure Kerberos to use System Crypto Policy
- Configure Libreswan to use System Crypto Policy
- Configure OpenSSL library to use System Crypto Policy
- Configure SSH to use System Crypto Policy
- ion Detection Software

0% (0 results, 123 rules selected)

□ Dry run □ Fetch remote resources □ Remediate



ssg-almalinux9-ds.xml - SCAP Workbench

Title: Guide to the Secure Configuration of AlmaLinux 9

Customization: None selected

Profile: PCI-DSS v

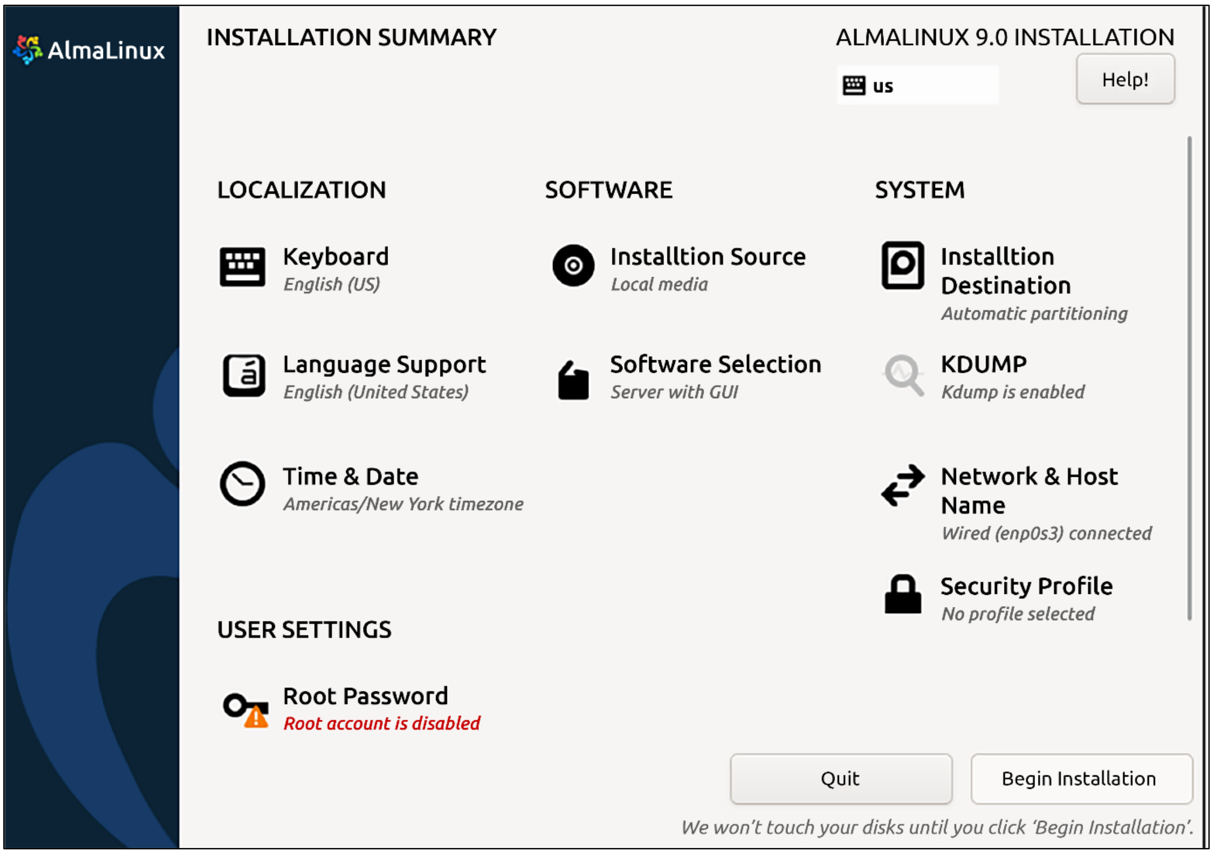
Target: ● Local M… …ver SSH)

Authentication Required

Authentication is required to scan local machine with root privileges. Click "Cancel" to scan using your current permissions.

Donald A. Tevault

0% (0 results, 123 rules selected)



INSTALLATION SUMMARY

ALMALINUX 9.0 INSTALLATION

LOCALIZATION

Keyboard
English (US)

Language Support
English (United States)

Time & Date
Americas/New York timezone

SOFTWARE

Installtion Source
Local media

Software Selection
Server with GUI

SYSTEM

Installtion Destination
Automatic partitioning

KDUMP
Kdump is enabled

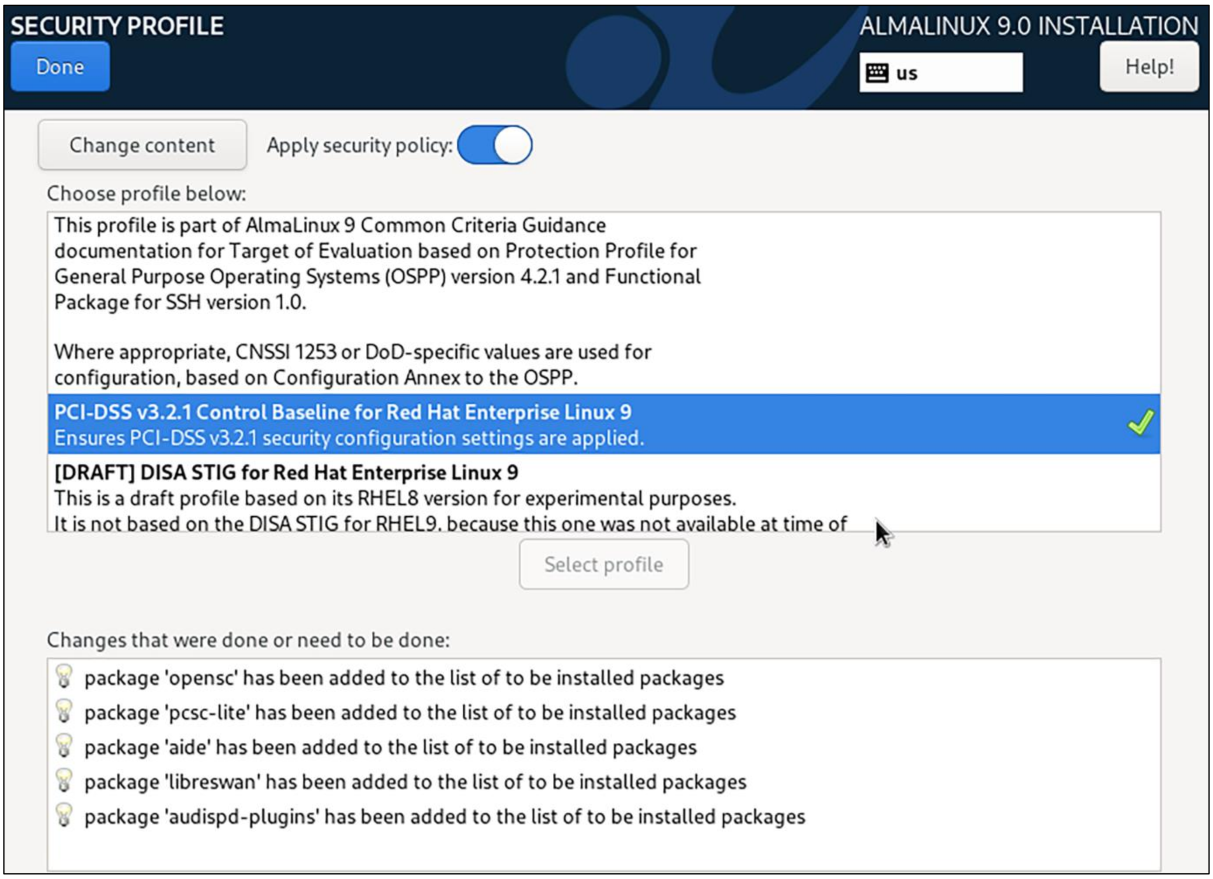
Network & Host Name
Wired (enp0s3) connected

Security Profile
No profile selected

USER SETTINGS

Root Password
Root account is disabled

We won't touch your disks until you click 'Begin Installation'.



SECURITY PROFILE

ALMALINUX 9.0 INSTALLATION

Apply security policy: ●

Choose profile below:

This profile is part of AlmaLinux 9 Common Criteria Guidance documentation for Target of Evaluation based on Protection Profile for General Purpose Operating Systems (OSPP) version 4.2.1 and Functional Package for SSH version 1.0.

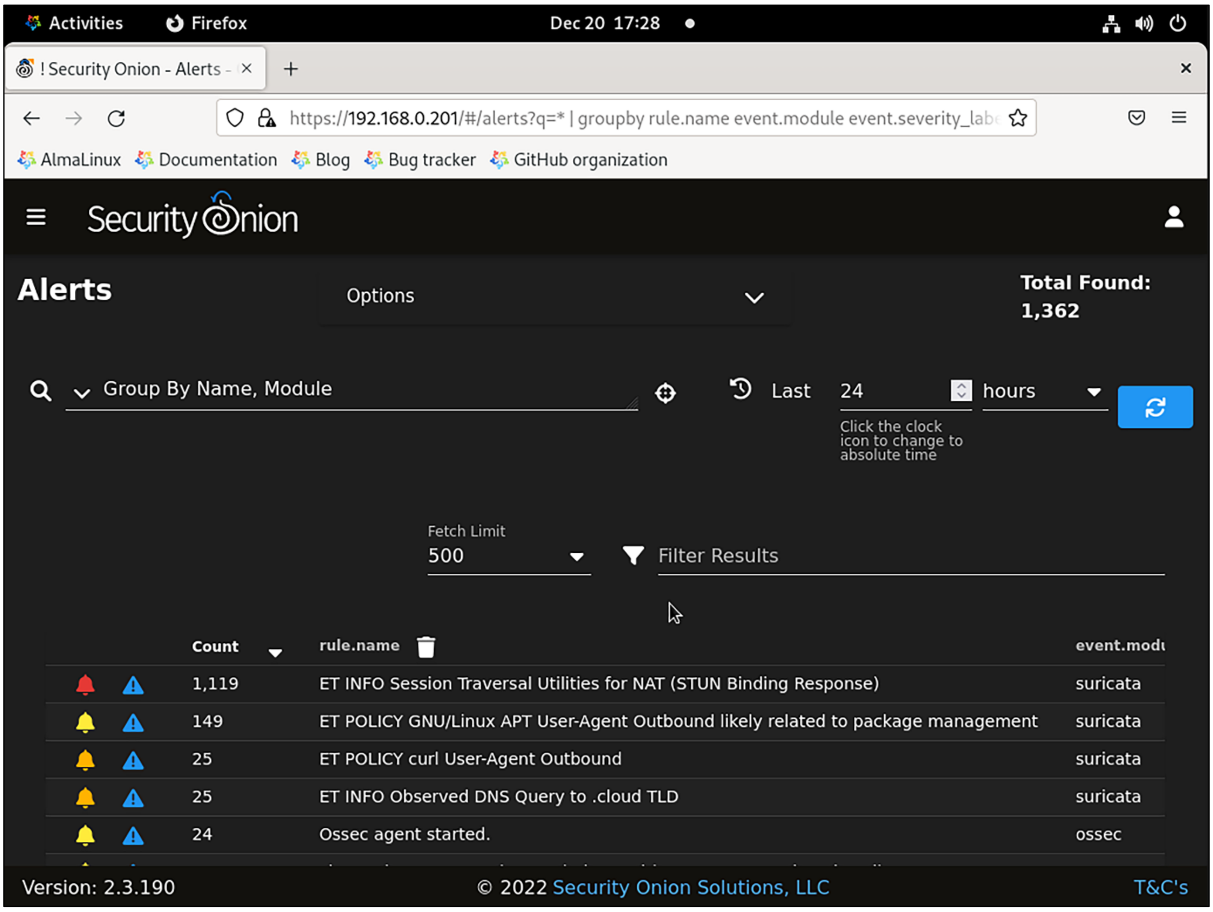
Where appropriate, CNSSI 1253 or DoD-specific values are used for configuration, based on Configuration Annex to the OSPP.

PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 9 ✓
Ensures PCI-DSS v3.2.1 security configuration settings are applied.

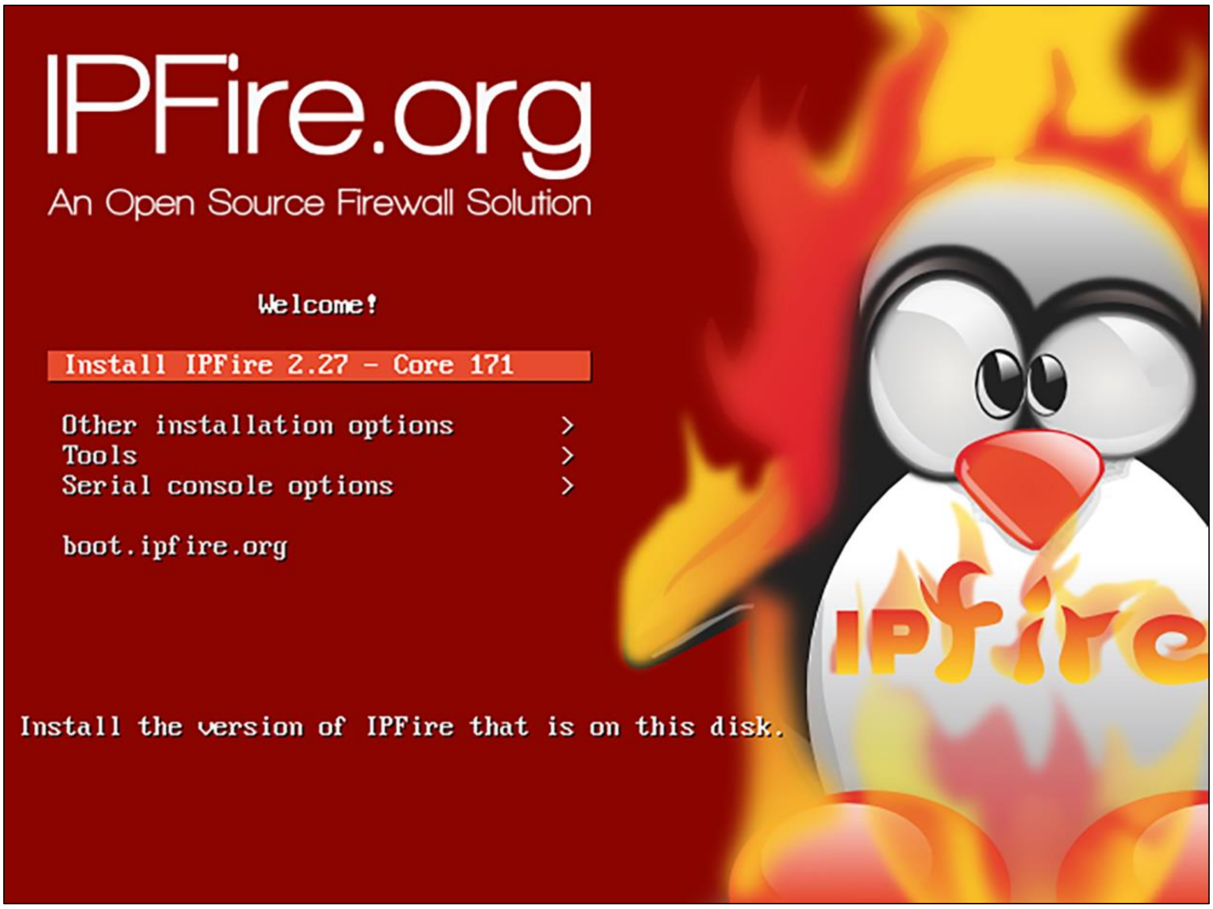
[DRAFT] DISA STIG for Red Hat Enterprise Linux 9
This is a draft profile based on its RHEL8 version for experimental purposes.
It is not based on the DISA STIG for RHEL9, because this one was not available at time of

Changes that were done or need to be done:

- package 'opensc' has been added to the list of to be installed packages
- package 'pcsc-lite' has been added to the list of to be installed packages
- package 'aide' has been added to the list of to be installed packages
- package 'libreswan' has been added to the list of to be installed packages
- package 'audispd-plugins' has been added to the list of to be installed packages



Count	rule.name	event.modu
1,119	ET INFO Session Traversal Utilities for NAT (STUN Binding Response)	suricata
149	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management	suricata
25	ET POLICY curl User-Agent Outbound	suricata
25	ET INFO Observed DNS Query to .cloud TLD	suricata
24	Ossec agent started.	ossec



IPFire.org

An Open Source Firewall Solution

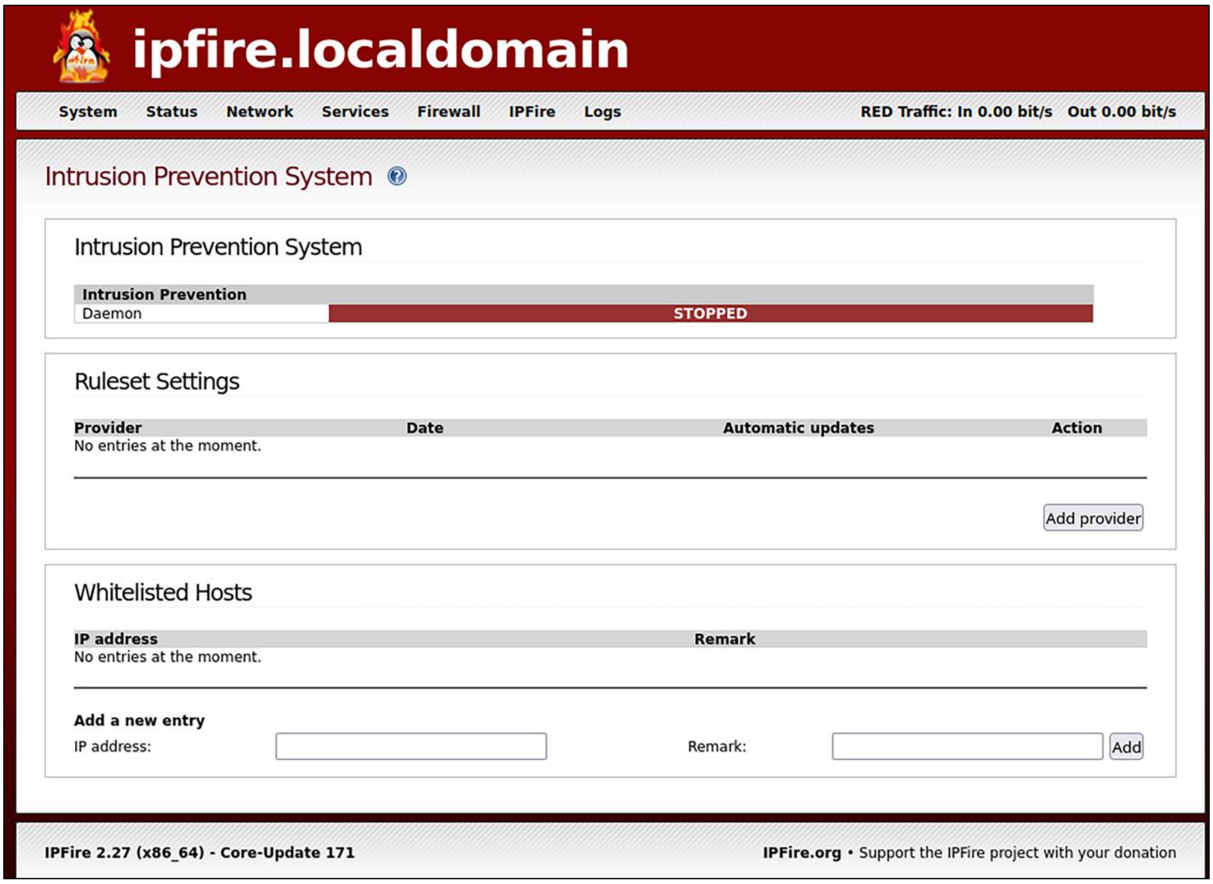
Welcome!

Install IPFire 2.27 - Core 171

Other installation options >
Tools >
Serial console options >

boot.ipfire.org

Install the version of IPFire that is on this disk.



RED Traffic: In 0.00 bit/s Out 0.00 bit/s

Intrusion Prevention System

Intrusion Prevention System

Intrusion Prevention	
Daemon	STOPPED

Ruleset Settings

Provider	Date	Automatic updates	Action
No entries at the moment.			

Whitelisted Hosts

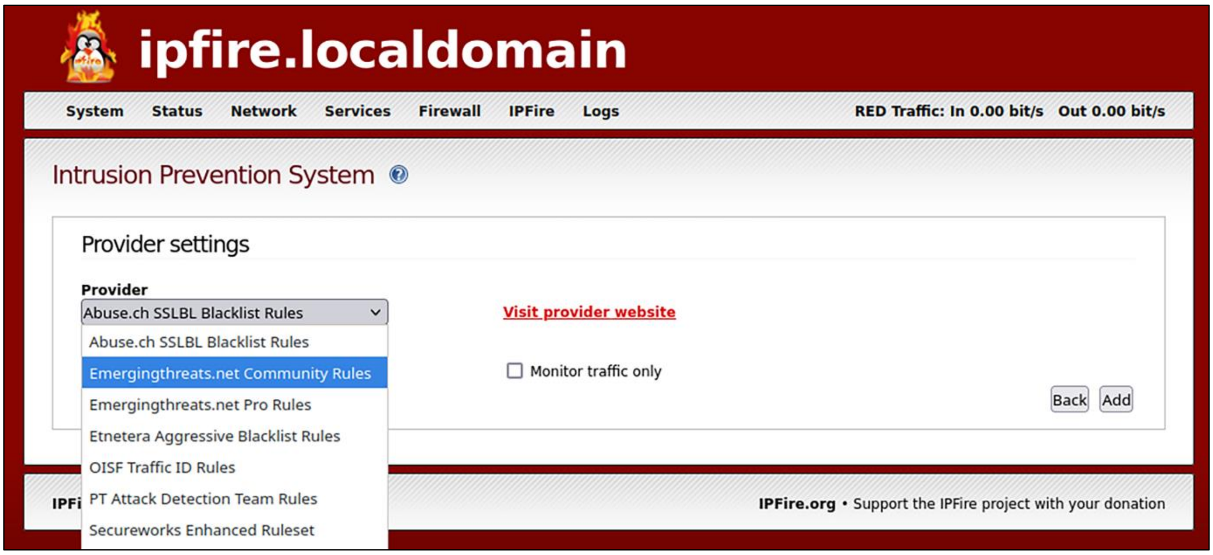
IP address	Remark
No entries at the moment.	

Add a new entry

IP address: Remark:

IPFire 2.27 (x86_64) - Core-Update 171

IPFire.org • Support the IPFire project with your donation


ipfire.localdomain
System
Status
Network
Services
Firewall
IPFire
Logs
RED Traffic: In 0.00 bit/s Out 0.00 bit/s

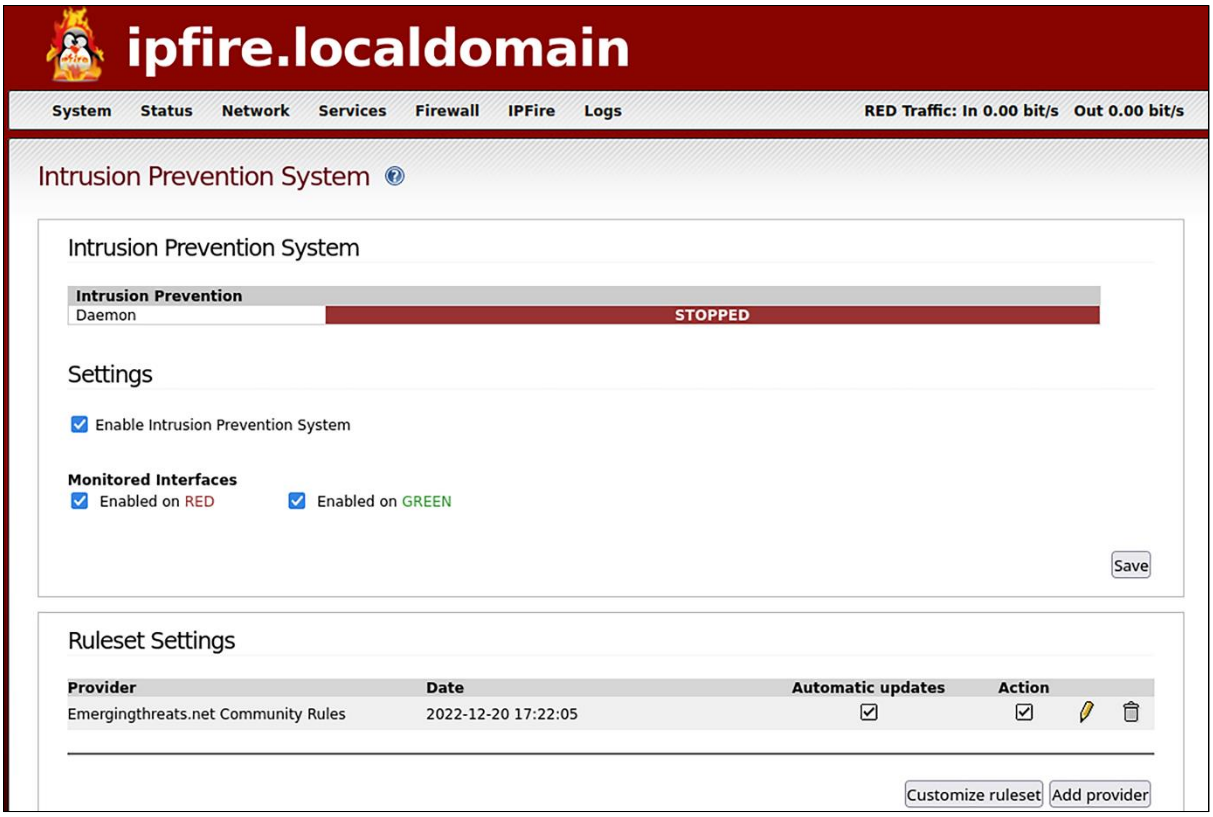
Intrusion Prevention System

Provider settings

Provider
Abuse.ch SSLBL Blacklist Rules

Abuse.ch SSLBL Blacklist Rules
Emergingthreats.net Community Rules
Emergingthreats.net Pro Rules
Etnetera Aggressive Blacklist Rules
OISF Traffic ID Rules
PT Attack Detection Team Rules
Secureworks Enhanced Ruleset
Visit provider website
Back
Add
IPFi
IPFire.org • Support the IPFire project with your donation

☐ Monitor traffic only



Intrusion Prevention System

Intrusion Prevention System

Intrusion Prevention	
Daemon	STOPPED

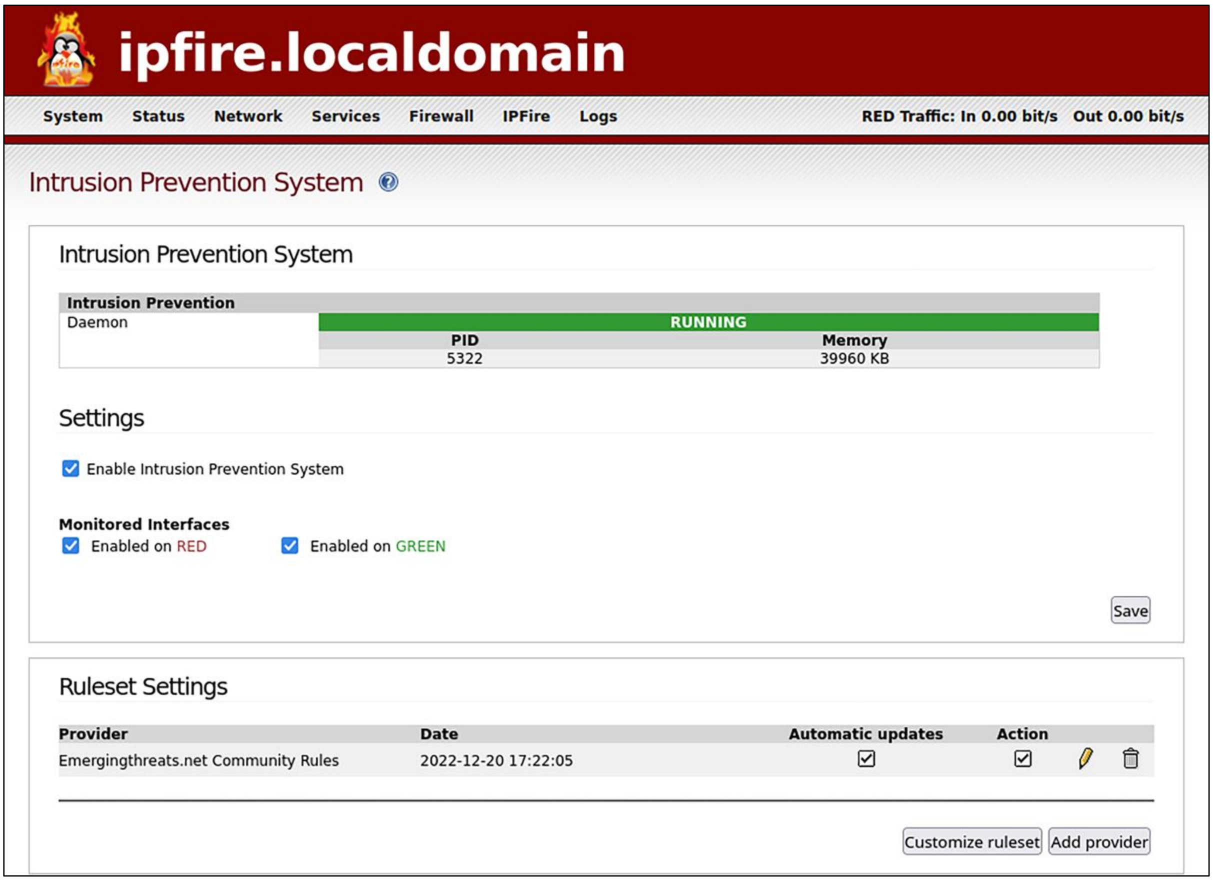
Settings

☑ Enable Intrusion Prevention System

Monitored Interfaces
☑ Enabled on RED ☑ Enabled on GREEN

Ruleset Settings

Provider	Date	Automatic updates	Action		
Emergingthreats.net Community Rules	2022-12-20 17:22:05	☑	☑	✎	🗑



Intrusion Prevention System

Intrusion Prevention System

Intrusion Prevention		
Daemon	RUNNING	
	PID	Memory
	5322	39960 KB

Settings

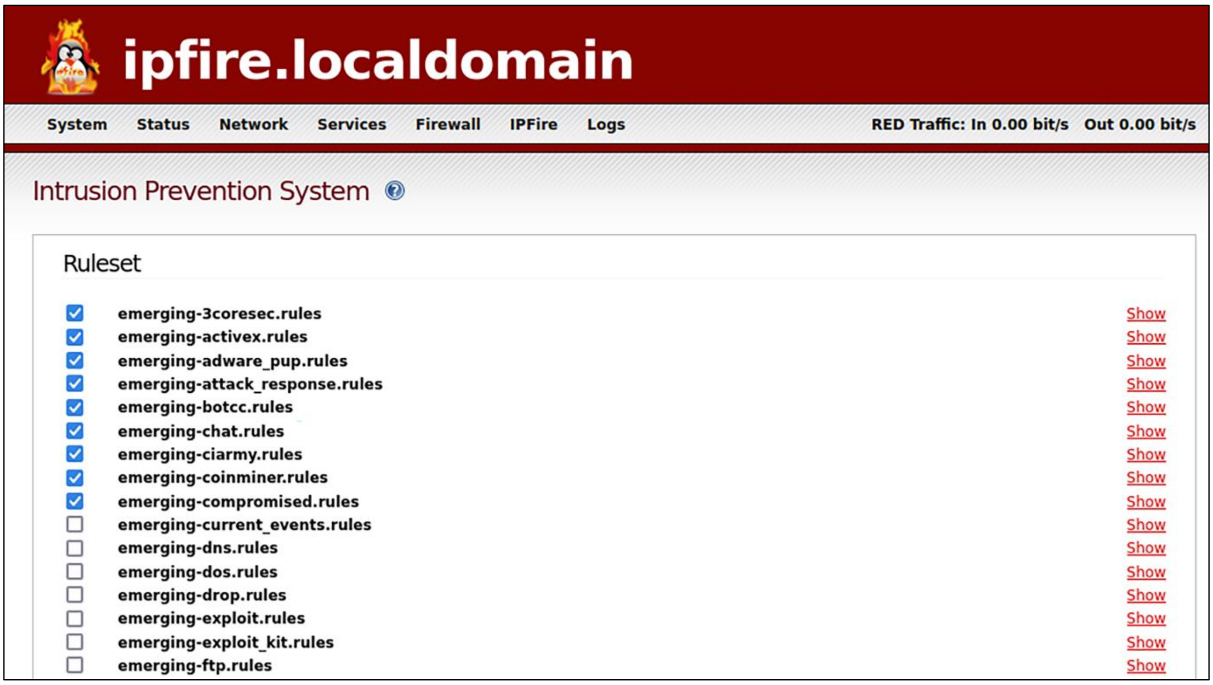
☑ Enable Intrusion Prevention System

Monitored Interfaces

☑ Enabled on RED ☑ Enabled on GREEN

Ruleset Settings

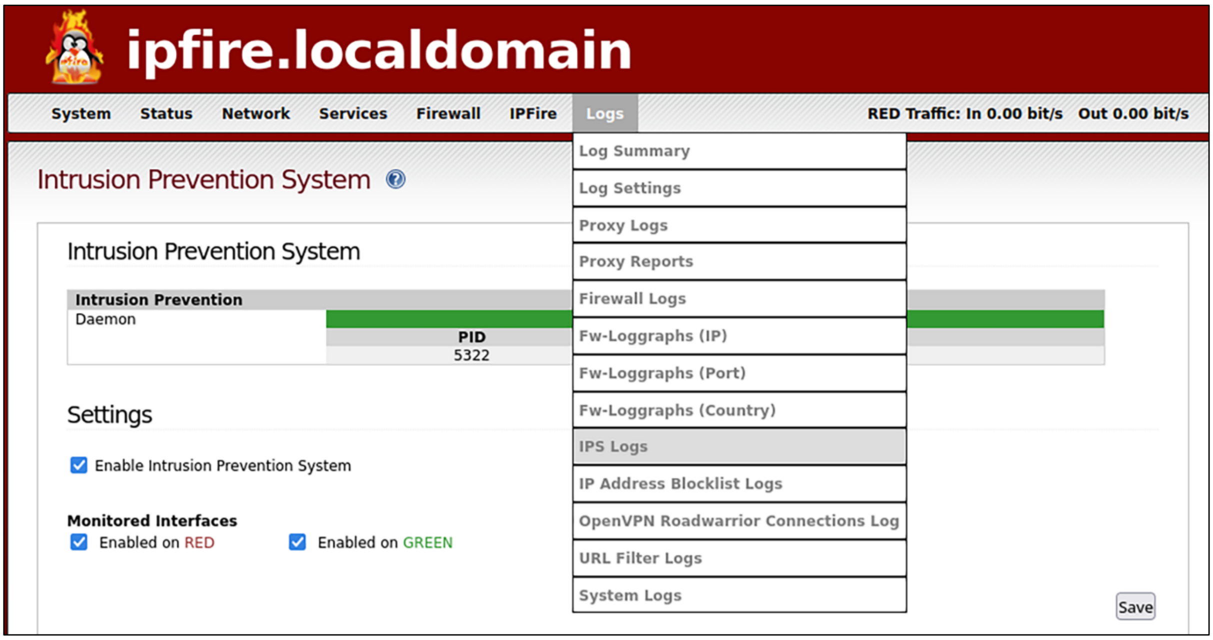
Provider	Date	Automatic updates	Action		
Emergingthreats.net Community Rules	2022-12-20 17:22:05	☑	☑	✎	🗑



Intrusion Prevention System

Ruleset

☑	emerging-3coresec.rules	Show
☑	emerging-activex.rules	Show
☑	emerging-adware_pup.rules	Show
☑	emerging-attack_response.rules	Show
☑	emerging-botcc.rules	Show
☑	emerging-chat.rules	Show
☑	emerging-ciarmy.rules	Show
☑	emerging-coinminer.rules	Show
☑	emerging-compromised.rules	Show
☐	emerging-current_events.rules	Show
☐	emerging-dns.rules	Show
☐	emerging-dos.rules	Show
☐	emerging-drop.rules	Show
☐	emerging-exploit.rules	Show
☐	emerging-exploit_kit.rules	Show
☐	emerging-ftp.rules	Show



Intrusion Prevention System

Intrusion Prevention System

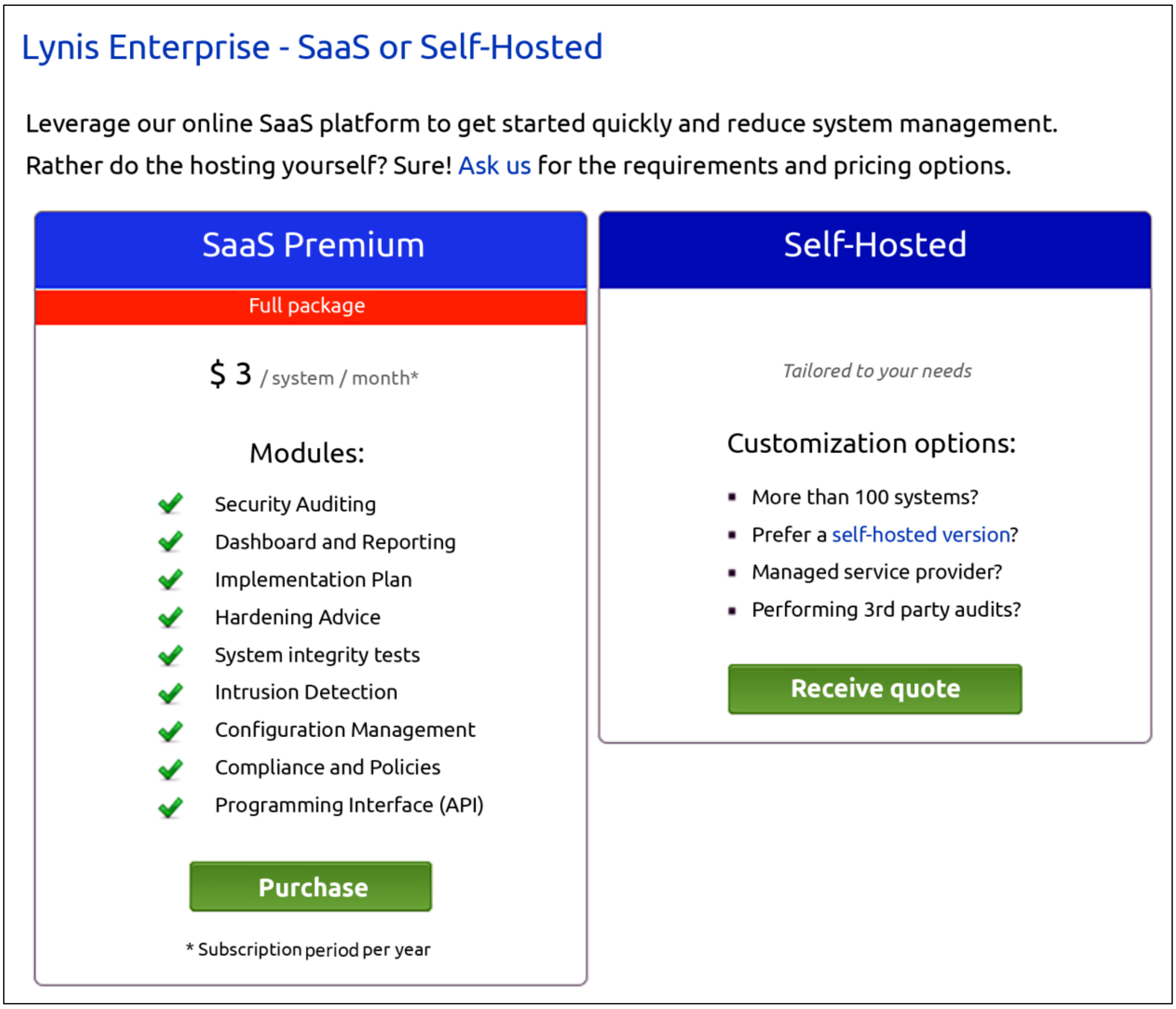
Intrusion Prevention	
Daemon	PID 5322

Settings

☑ Enable Intrusion Prevention System

Monitored Interfaces

☑ Enabled on RED ☑ Enabled on GREEN



Lynis Enterprise - SaaS or Self-Hosted

Leverage our online SaaS platform to get started quickly and reduce system management.
Rather do the hosting yourself? Sure! Ask us for the requirements and pricing options.

SaaS Premium

Full package

$ 3 / system / month*

Modules:

- ✓ Security Auditing
- ✓ Dashboard and Reporting
- ✓ Implementation Plan
- ✓ Hardening Advice
- ✓ System integrity tests
- ✓ Intrusion Detection
- ✓ Configuration Management
- ✓ Compliance and Policies
- ✓ Programming Interface (API)

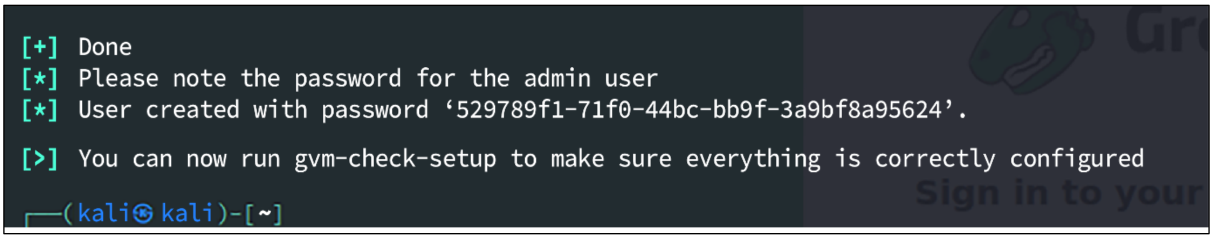
* Subscription period per year

Self-Hosted

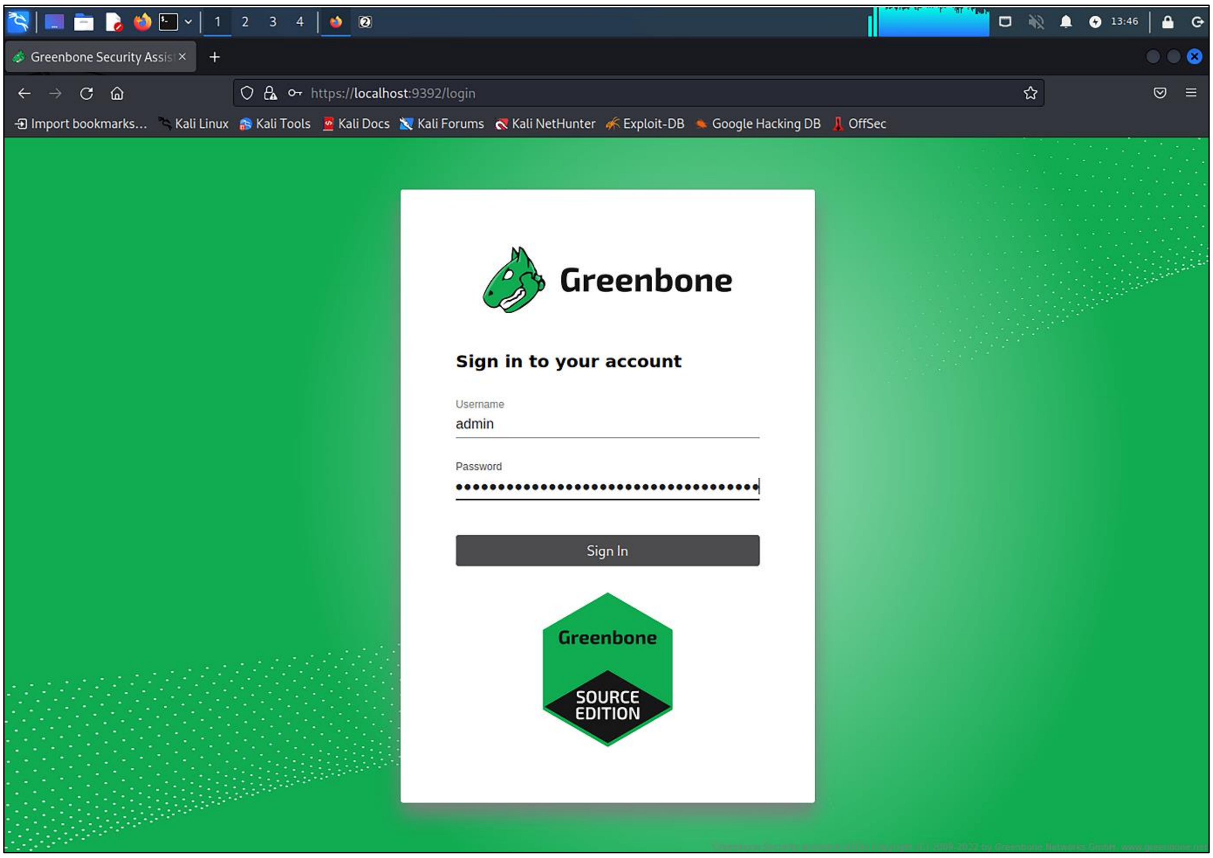
Tailored to your needs

Customization options:

- More than 100 systems?
- Prefer a self-hosted version?
- Managed service provider?
- Performing 3rd party audits?



```
[+] Done
[*] Please note the password for the admin user
[*] User created with password ‘529789f1-71f0-44bc-bb9f-3a9bf8a95624’.

[>] You can now run gvm-check-setup to make sure everything is correctly configured

┌──(kali㉿kali)-[~]
```

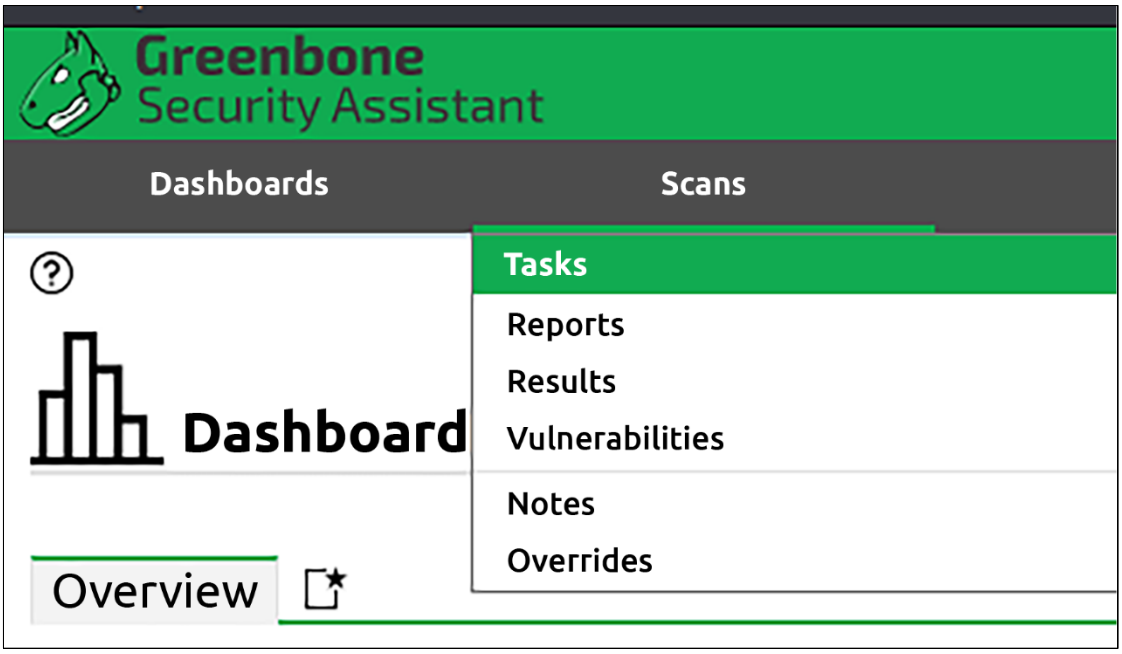


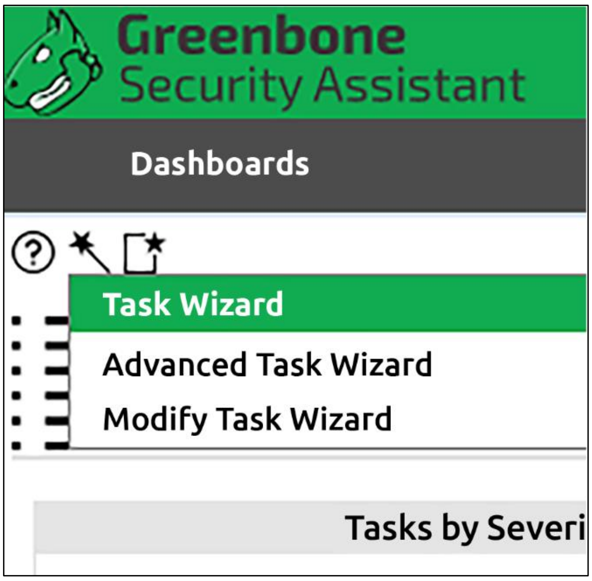
https://localhost:9392/login

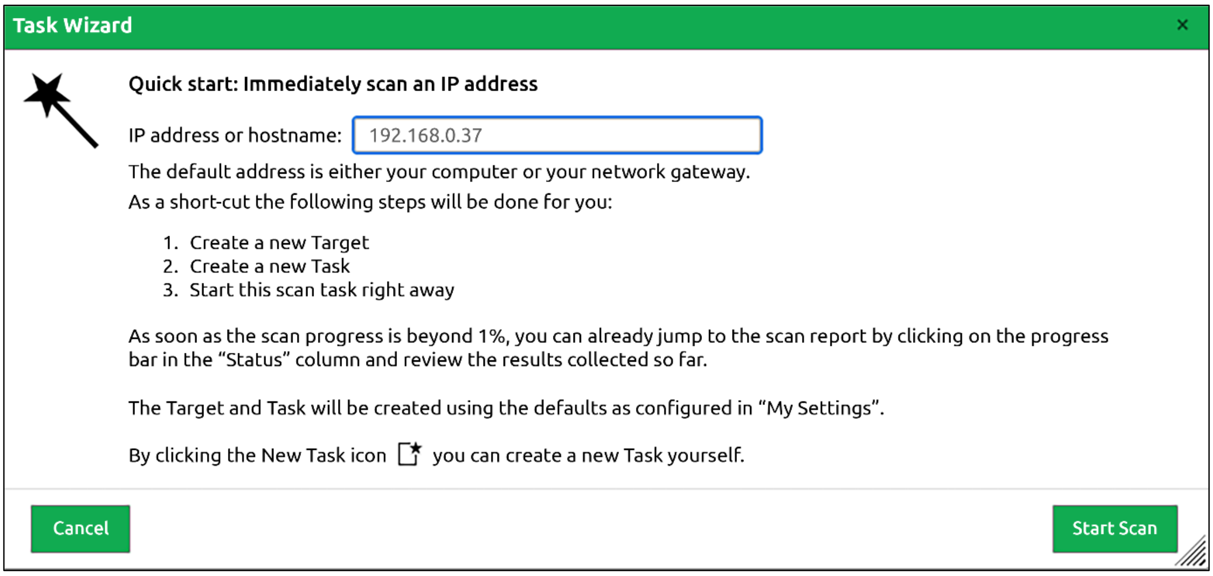
Sign in to your account

Username: admin

Password: ••••••••••••••••••••••••••••••••••••







Quick start: Immediately scan an IP address

IP address or hostname: 192.168.0.37

The default address is either your computer or your network gateway.

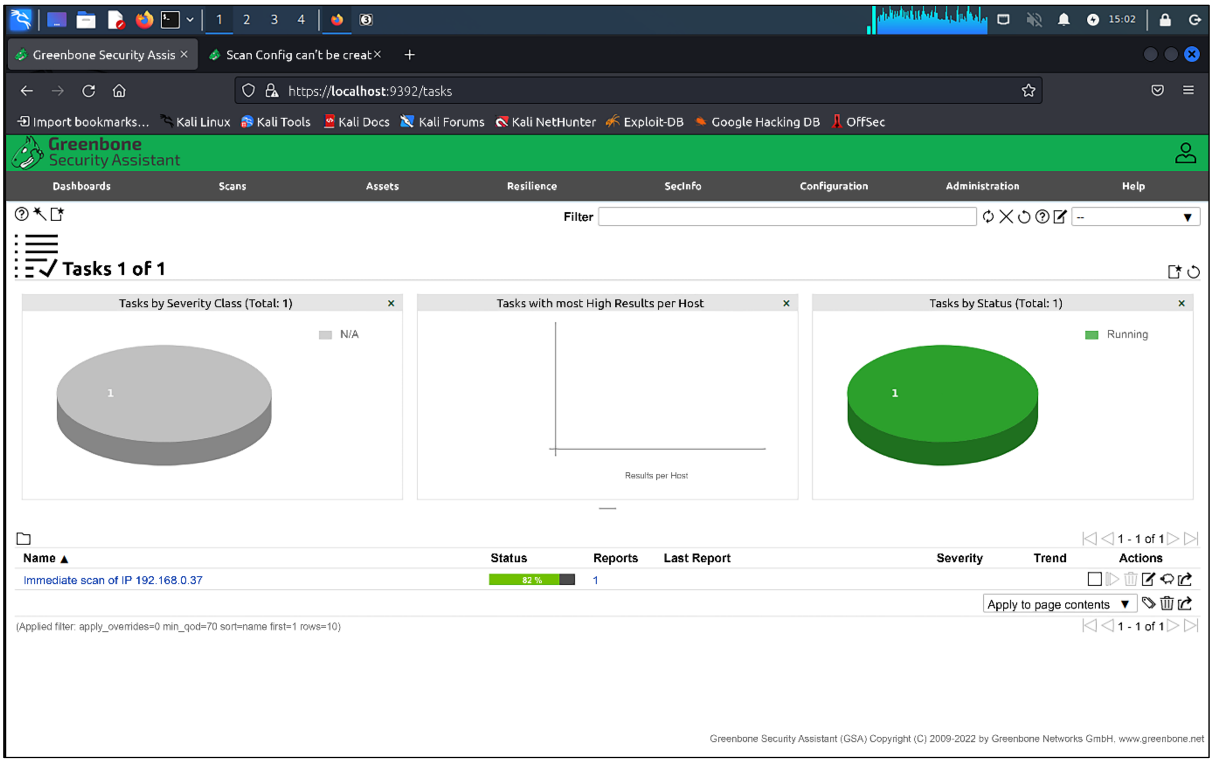
As a short-cut the following steps will be done for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away

As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progress bar in the "Status" column and review the results collected so far.

The Target and Task will be created using the defaults as configured in "My Settings".

By clicking the New Task icon you can create a new Task yourself.

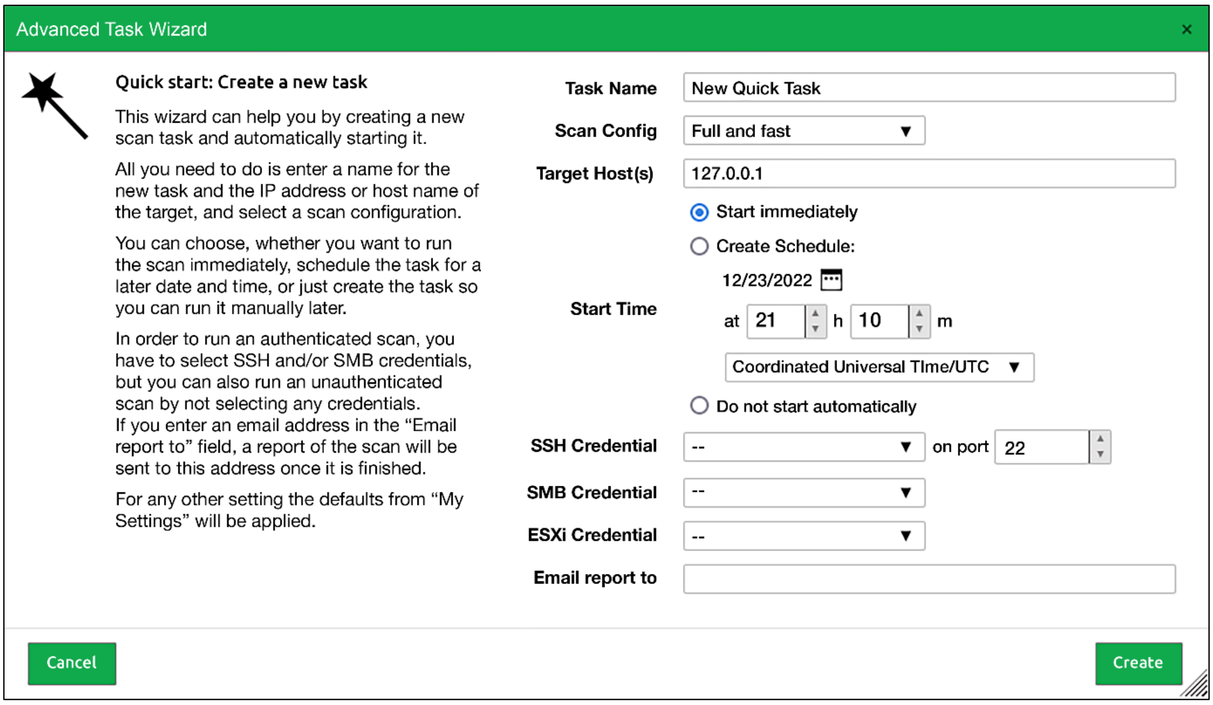


Greenbone Security Assis ×
Scan Config can't be creat ×
https://localhost:9392/tasks
Import bookmarks... Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Greenbone
Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
Tasks 1 of 1
Tasks by Severity Class (Total: 1)
N/A
1
Tasks with most High Results per Host
Results per Host
Tasks by Status (Total: 1)
Running
1
1 - 1 of 1
Apply to page contents

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Immediate scan of IP 192.168.0.37	82 %	1				

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net



Advanced Task Wizard

Quick start: Create a new task

This wizard can help you by creating a new scan task and automatically starting it.

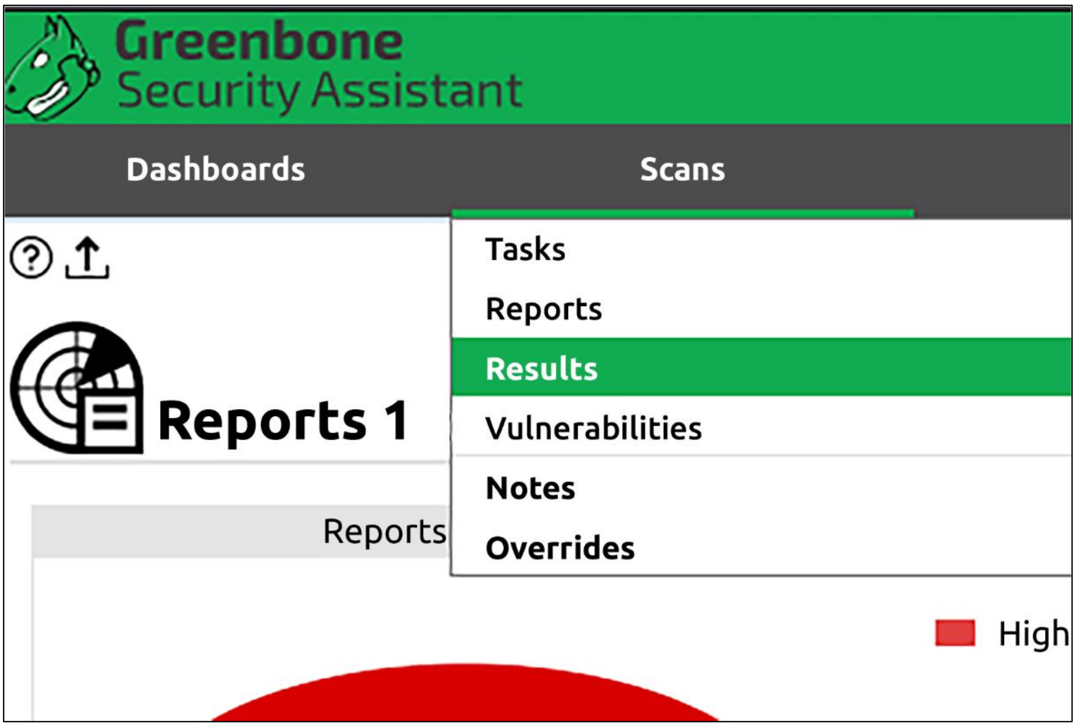
All you need to do is enter a name for the new task and the IP address or host name of the target, and select a scan configuration.

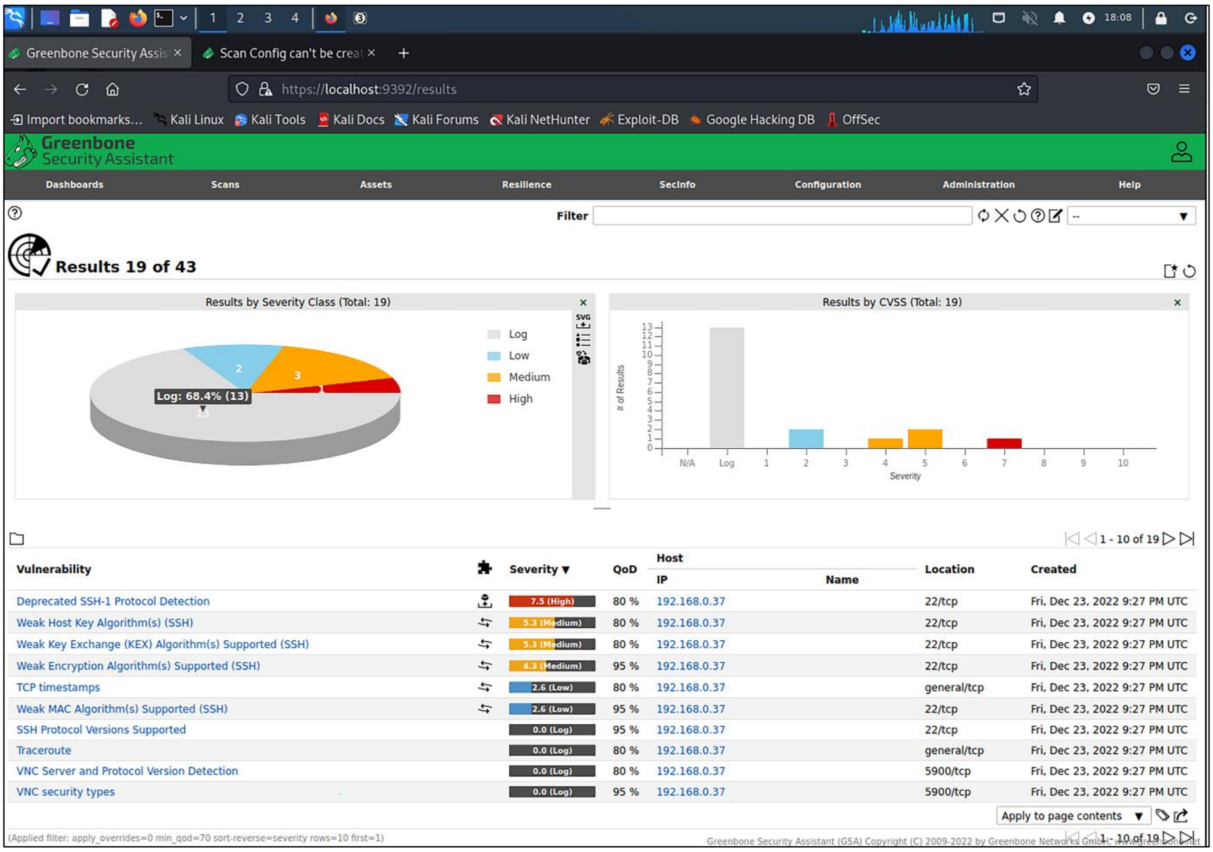
You can choose, whether you want to run the scan immediately, schedule the task for a later date and time, or just create the task so you can run it manually later.

In order to run an authenticated scan, you have to select SSH and/or SMB credentials, but you can also run an unauthenticated scan by not selecting any credentials.
If you enter an email address in the "Email report to" field, a report of the scan will be sent to this address once it is finished.

For any other setting the defaults from "My Settings" will be applied.

Task Name	New Quick Task
Scan Config	Full and fast ▼
Target Host(s)	127.0.0.1
	● Start immediately
	○ Create Schedule:
	12/23/2022
Start Time	at 21 h 10 m
	Coordinated Universal TIme/UTC ▼
	○ Do not start automatically
SSH Credential	-- ▼ on port 22
SMB Credential	-- ▼
ESXi Credential	-- ▼
Email report to	



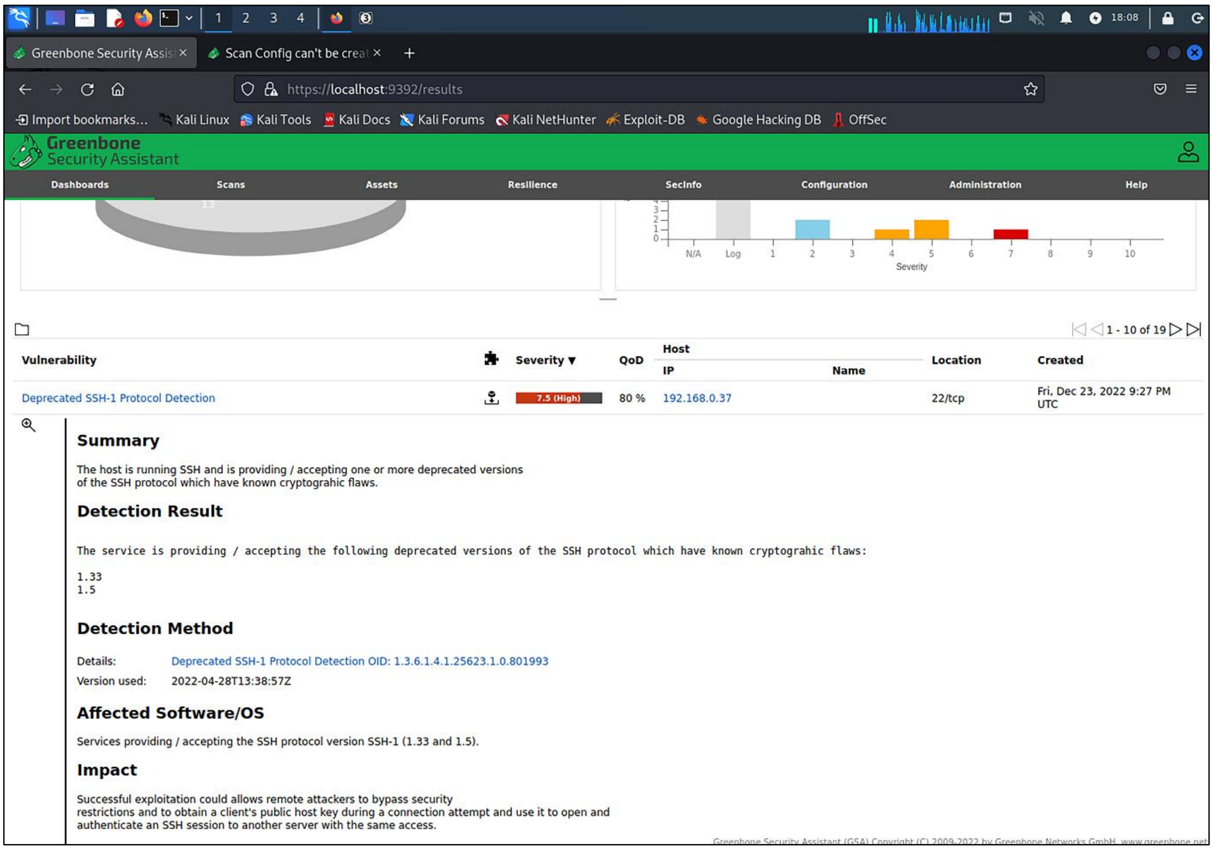


Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Deprecated SSH-1 Protocol Detection		7.5 (High)	80 %	192.168.0.37		22/tcp	Fri, Dec 23, 2022 9:27 PM UTC
Weak Host Key Algorithm(s) (SSH)		5.3 (Medium)	80 %	192.168.0.37		22/tcp	Fri, Dec 23, 2022 9:27 PM UTC
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)		5.3 (Medium)	80 %	192.168.0.37		22/tcp	Fri, Dec 23, 2022 9:27 PM UTC
Weak Encryption Algorithm(s) Supported (SSH)		4.3 (Medium)	95 %	192.168.0.37		22/tcp	Fri, Dec 23, 2022 9:27 PM UTC
TCP timestamps		2.6 (Low)	80 %	192.168.0.37		general/tcp	Fri, Dec 23, 2022 9:27 PM UTC
Weak MAC Algorithm(s) Supported (SSH)		2.6 (Low)	95 %	192.168.0.37		22/tcp	Fri, Dec 23, 2022 9:27 PM UTC
SSH Protocol Versions Supported		0.0 (Log)	95 %	192.168.0.37		22/tcp	Fri, Dec 23, 2022 9:27 PM UTC
Traceroute		0.0 (Log)	80 %	192.168.0.37		general/tcp	Fri, Dec 23, 2022 9:27 PM UTC
VNC Server and Protocol Version Detection		0.0 (Log)	80 %	192.168.0.37		5900/tcp	Fri, Dec 23, 2022 9:27 PM UTC
VNC security types		0.0 (Log)	95 %	192.168.0.37		5900/tcp	Fri, Dec 23, 2022 9:27 PM UTC

Apply to page contents ▼

(Applied filter: apply_overrides=0 min_qod=70 sort-reverse=severity rows=10 first=1)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net



Vulnerability		Severity ▼	QoD	Host IP	Host Name	Location	Created
Deprecated SSH-1 Protocol Detection		7.5 (High)	80 %	192.168.0.37		22/tcp	Fri, Dec 23, 2022 9:27 PM UTC

Summary

The host is running SSH and is providing / accepting one or more deprecated versions of the SSH protocol which have known cryptographic flaws.

Detection Result

```
The service is providing / accepting the following deprecated versions of the SSH protocol which have known cryptograhic flaws:

1.33
1.5
```

Detection Method

Details: Deprecated SSH-1 Protocol Detection OID: 1.3.6.1.4.1.25623.1.0.801993

Version used: 2022-04-28T13:38:57Z

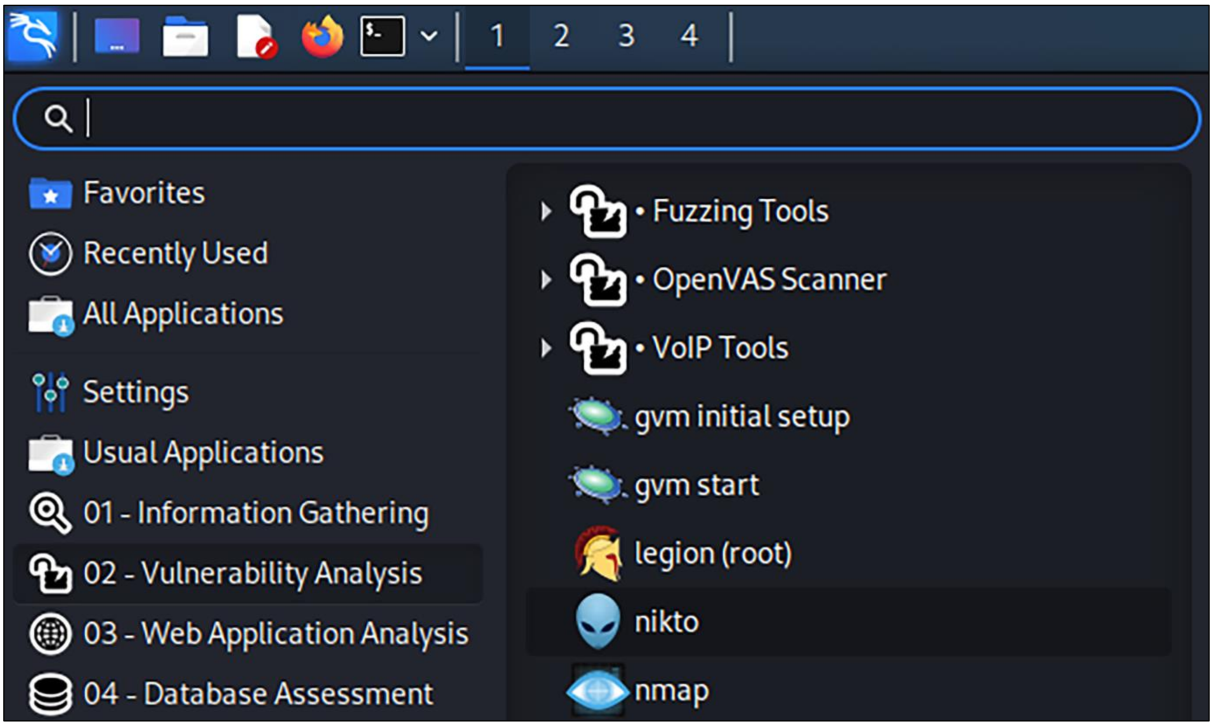
Affected Software/OS

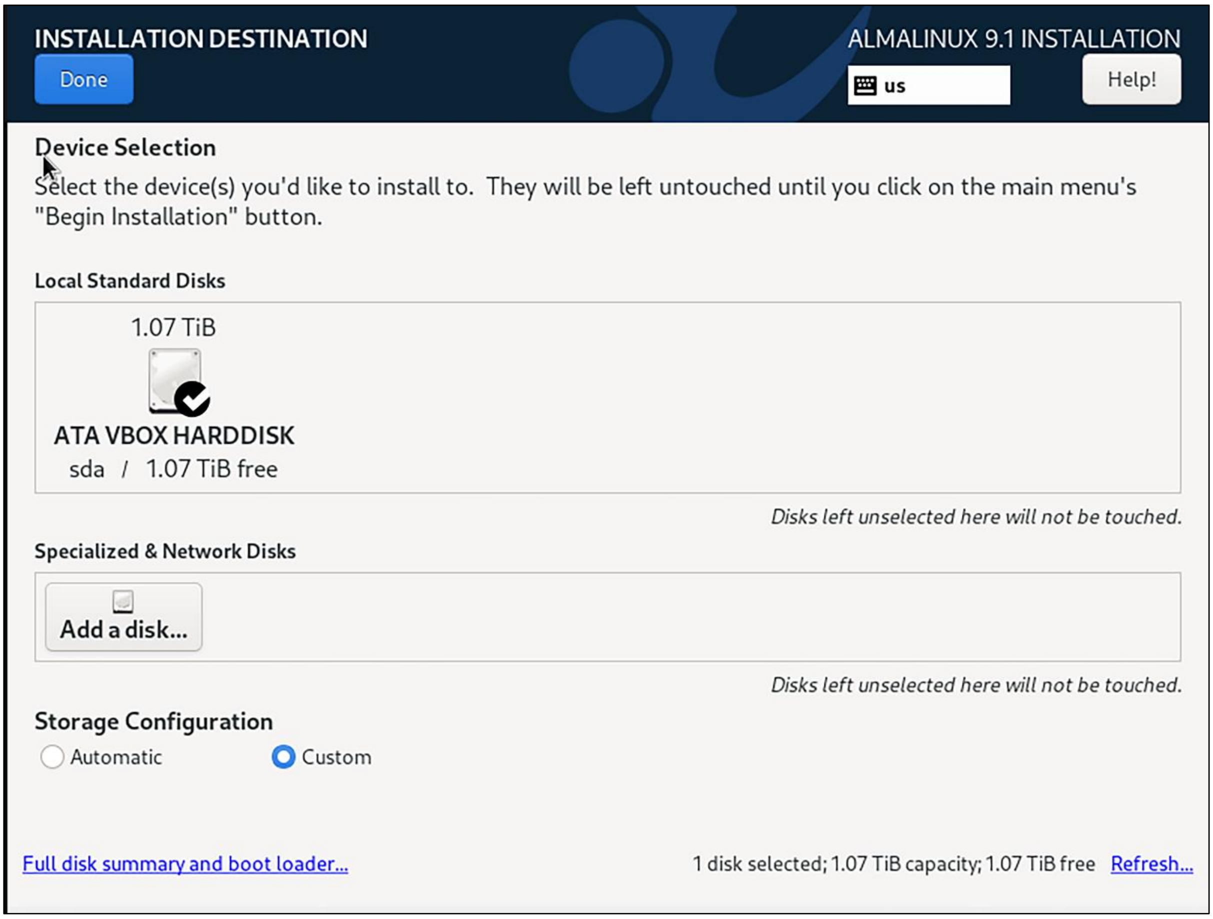
Services providing / accepting the SSH protocol version SSH-1 (1.33 and 1.5).

Impact

Successful exploitation could allows remote attackers to bypass security restrictions and to obtain a client's public host key during a connection attempt and use it to open and authenticate an SSH session to another server with the same access.

Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net





Device Selection

Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

Local Standard Disks

1.07 TiB

ATA VBOX HARDDISK

sda / 1.07 TiB free

Disks left unselected here will not be touched.

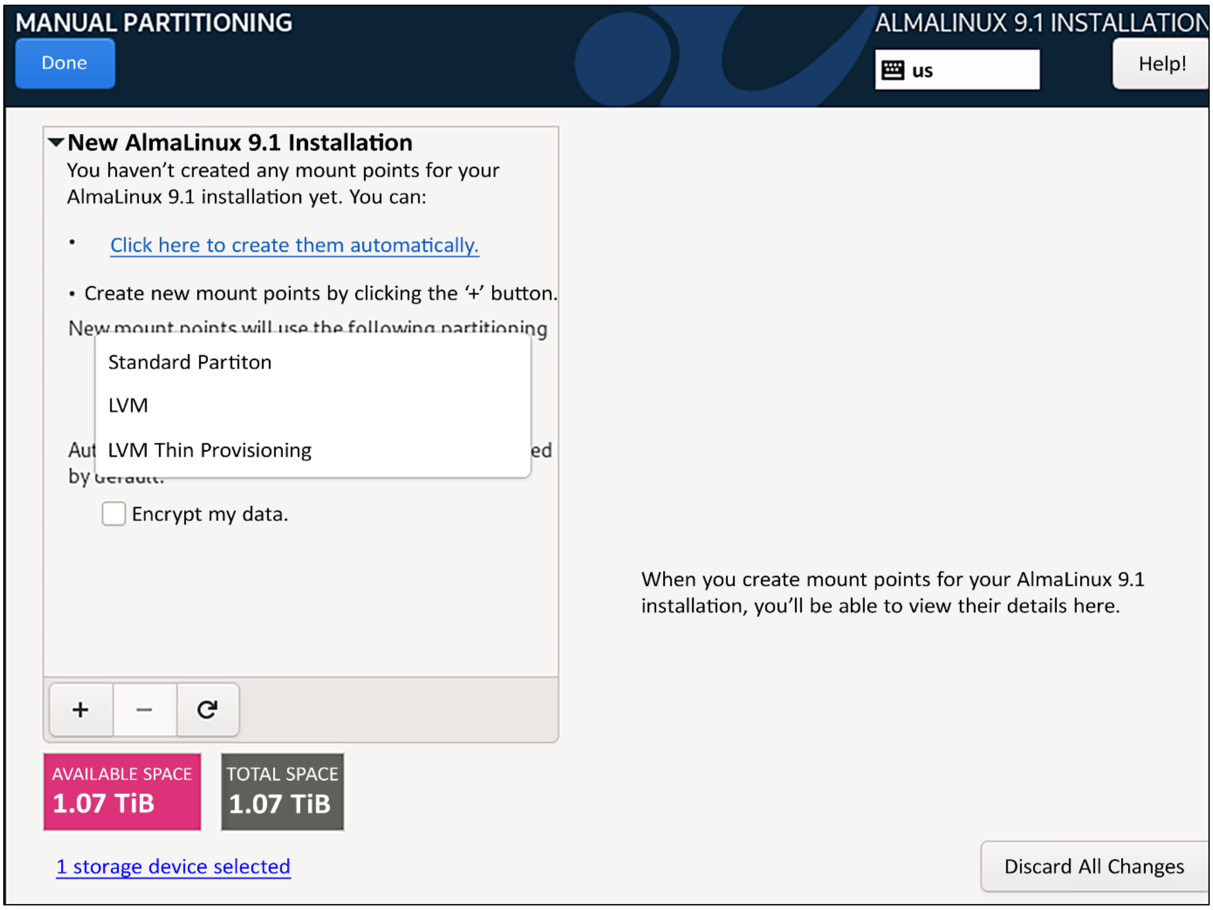
Specialized & Network Disks

Disks left unselected here will not be touched.

Storage Configuration

○ Automatic ● Custom

1 disk selected; 1.07 TiB capacity; 1.07 TiB free



New AlmaLinux 9.1 Installation

You haven't created any mount points for your AlmaLinux 9.1 installation yet. You can:

- Click here to create them automatically.
- Create new mount points by clicking the '+' button.

New mount points will use the following partitioning

Standard Partiton

LVM

LVM Thin Provisioning

Aut ... ed by default:

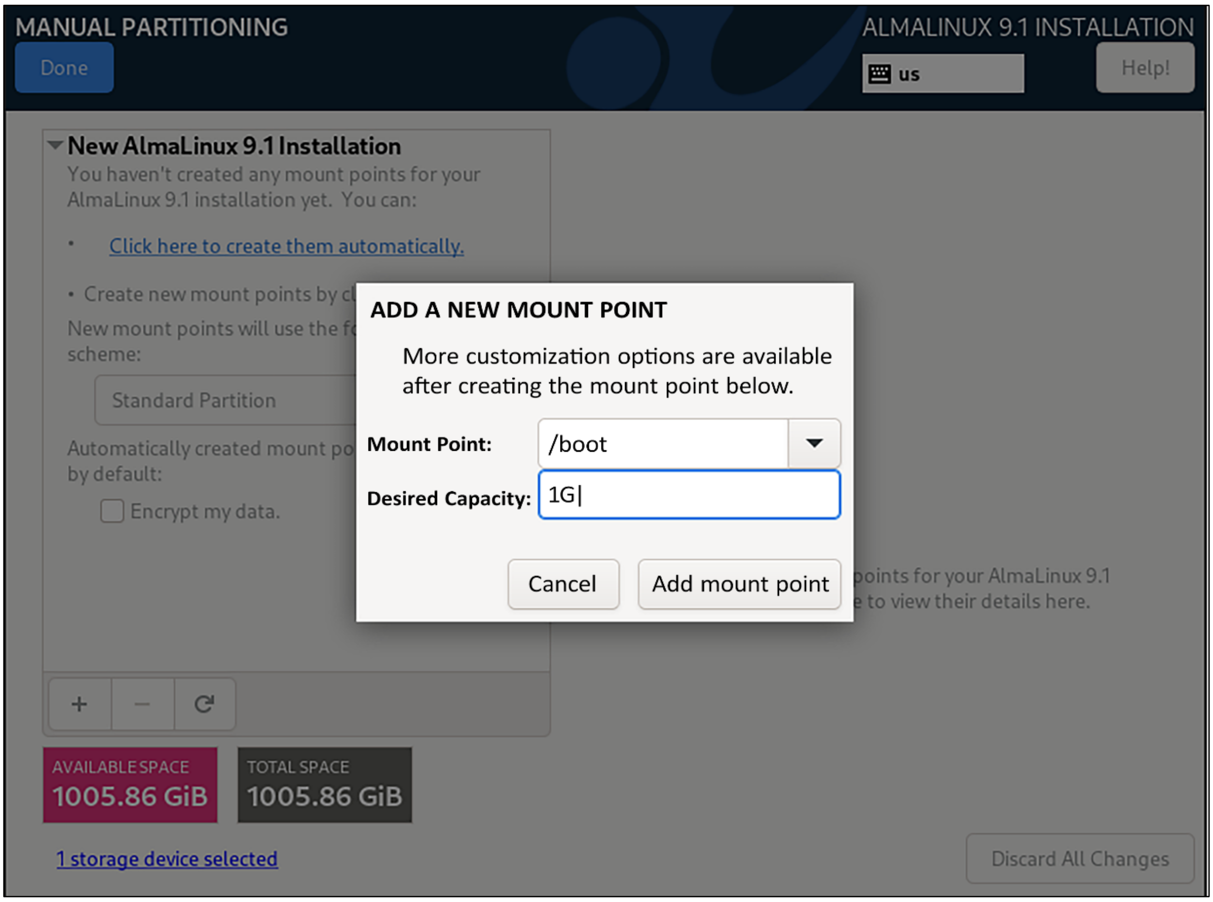
□ Encrypt my data.

When you create mount points for your AlmaLinux 9.1 installation, you'll be able to view their details here.

AVAILABLE SPACE 1.07 TiB

TOTAL SPACE 1.07 TiB

1 storage device selected



New AlmaLinux 9.1 Installation

You haven't created any mount points for your AlmaLinux 9.1 installation yet. You can:

- Click here to create them automatically.
- Create new mount points by cl

New mount points will use the f scheme:

Standard Partition

Automatically created mount po by default:

□ Encrypt my data.

points for your AlmaLinux 9.1 e to view their details here.

ADD A NEW MOUNT POINT

More customization options are available after creating the mount point below.

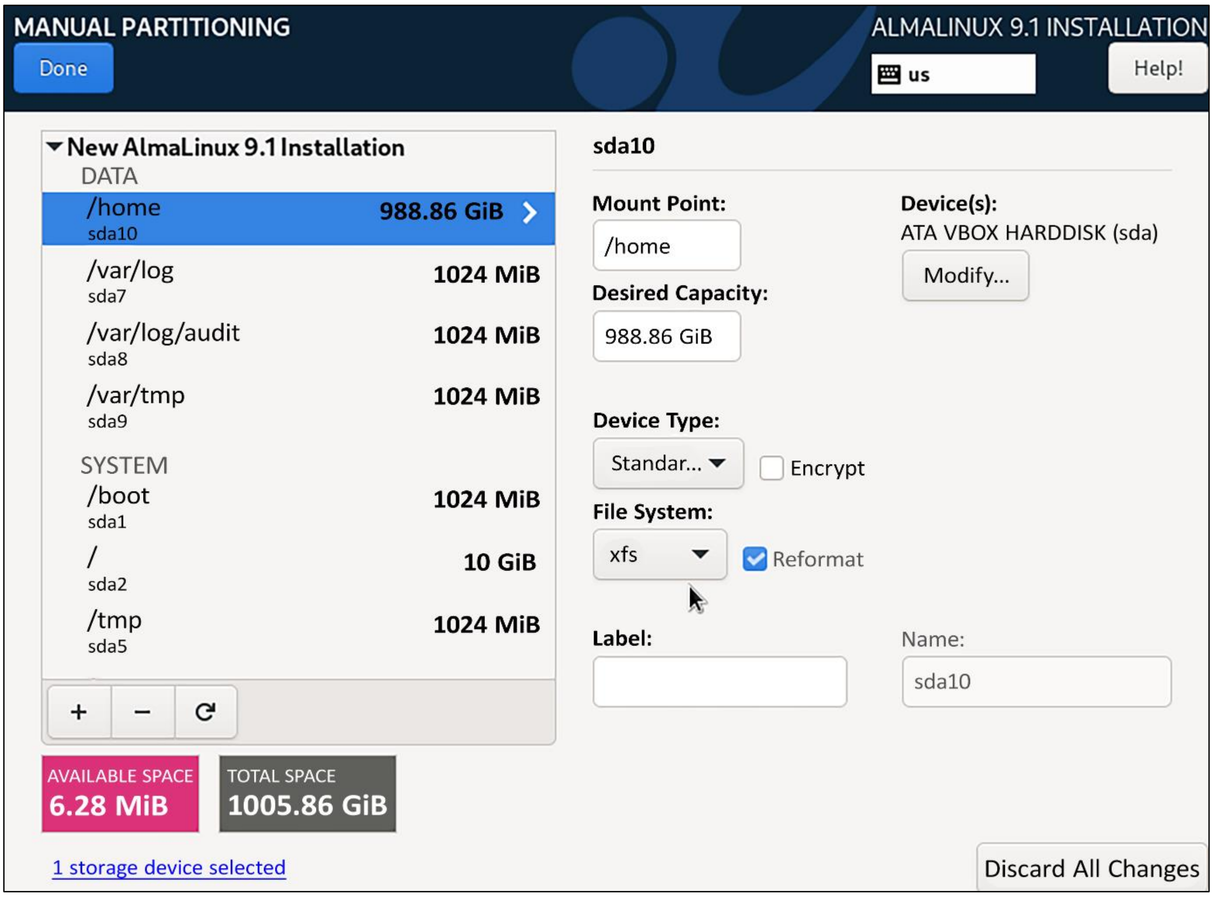
Mount Point: /boot

Desired Capacity: 1G

AVAILABLE SPACE 1005.86 GiB

TOTAL SPACE 1005.86 GiB

1 storage device selected



New AlmaLinux 9.1 Installation

DATA

/home sda10	988.86 GiB
/var/log sda7	1024 MiB
/var/log/audit sda8	1024 MiB
/var/tmp sda9	1024 MiB

SYSTEM

/boot sda1	1024 MiB
/ sda2	10 GiB
/tmp sda5	1024 MiB

AVAILABLE SPACE 6.28 MiB

TOTAL SPACE 1005.86 GiB

sda10

Mount Point: /home

Desired Capacity: 988.86 GiB

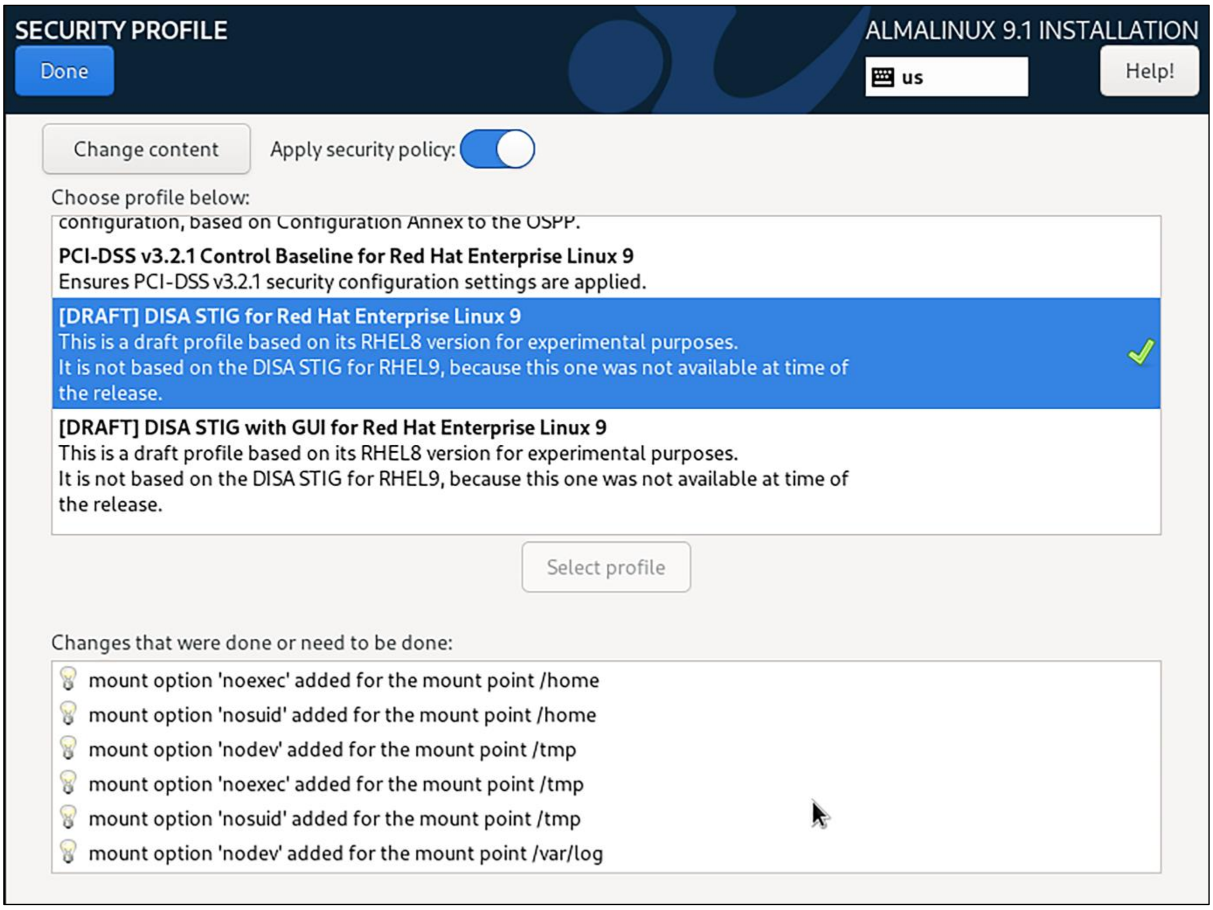
Device(s): ATA VBOX HARDDISK (sda)

Device Type: Standar... □ Encrypt

File System: xfs ☑ Reformat

Label:

Name: sda10



Apply security policy: ● (on)

Choose profile below:

configuration, based on Configuration Annex to the OSPP.

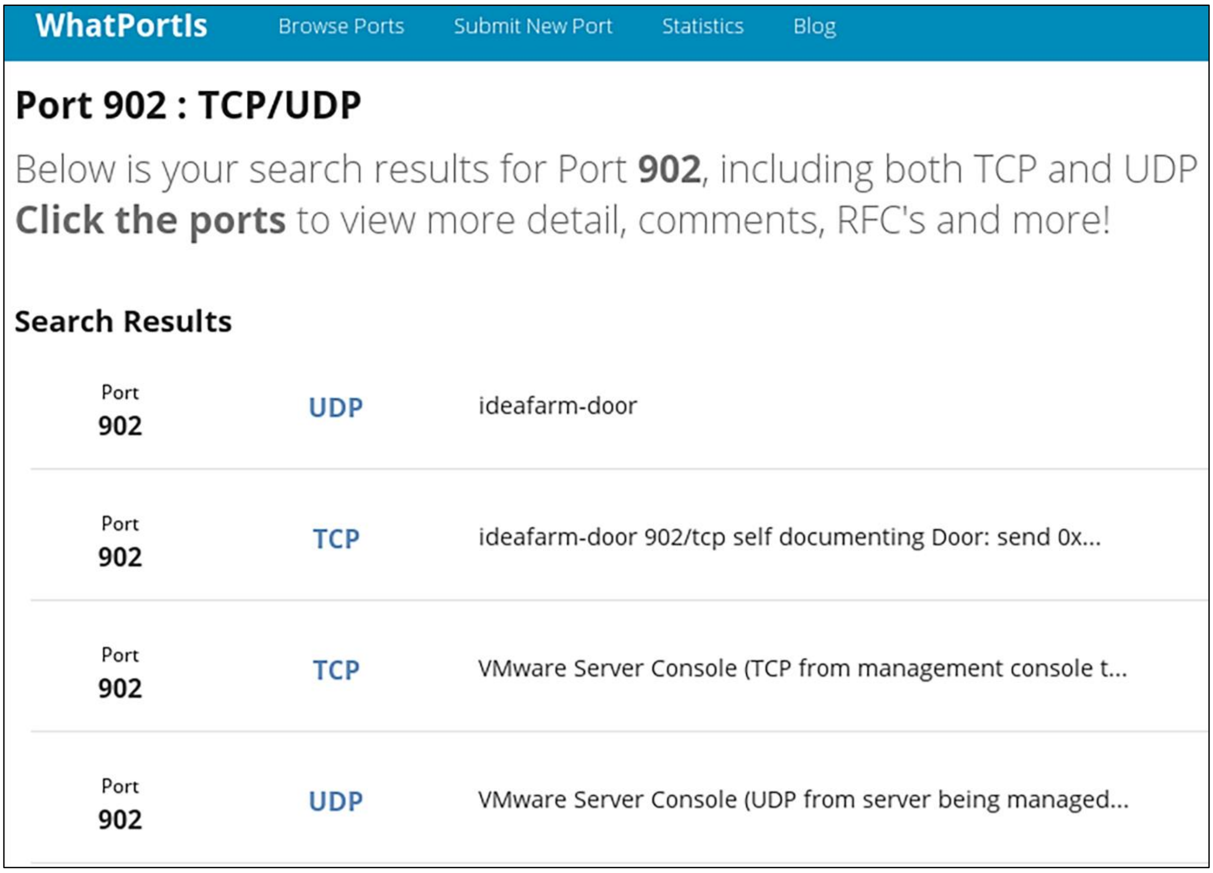
PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 9
Ensures PCI-DSS v3.2.1 security configuration settings are applied.

[DRAFT] DISA STIG for Red Hat Enterprise Linux 9 ✓
This is a draft profile based on its RHEL8 version for experimental purposes.
It is not based on the DISA STIG for RHEL9, because this one was not available at time of the release.

[DRAFT] DISA STIG with GUI for Red Hat Enterprise Linux 9
This is a draft profile based on its RHEL8 version for experimental purposes.
It is not based on the DISA STIG for RHEL9, because this one was not available at time of the release.

Changes that were done or need to be done:

- mount option 'noexec' added for the mount point /home
- mount option 'nosuid' added for the mount point /home
- mount option 'nodev' added for the mount point /tmp
- mount option 'noexec' added for the mount point /tmp
- mount option 'nosuid' added for the mount point /tmp
- mount option 'nodev' added for the mount point /var/log

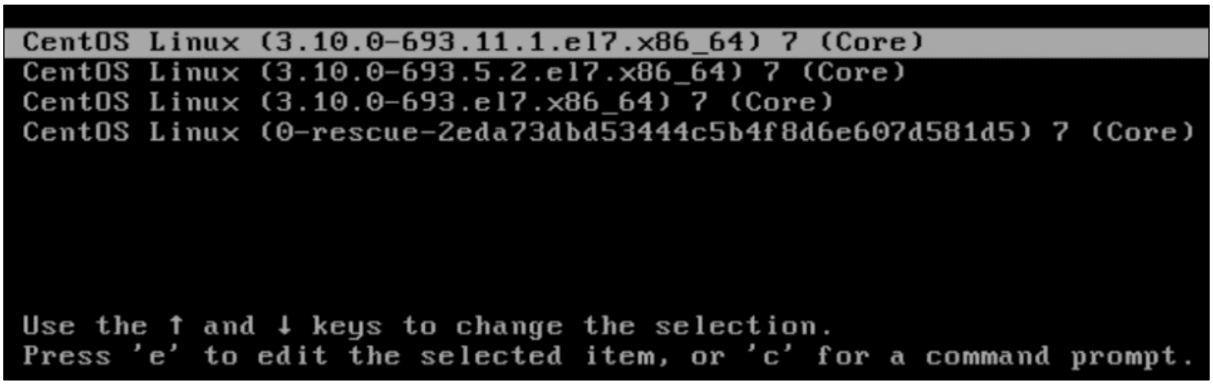


Port 902 : TCP/UDP

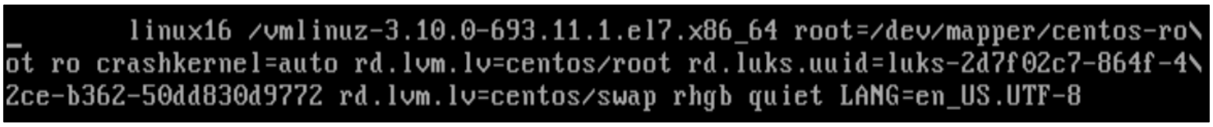
Below is your search results for Port **902**, including both TCP and UDP
Click the ports to view more detail, comments, RFC's and more!

Search Results

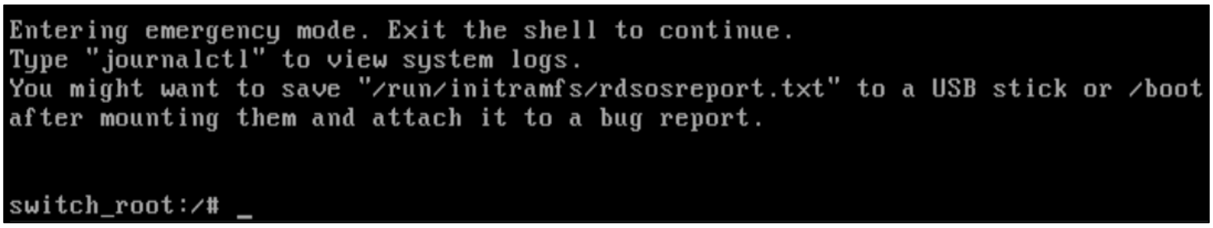
Port 902	UDP	ideafarm-door
Port 902	TCP	ideafarm-door 902/tcp self documenting Door: send 0x...
Port 902	TCP	VMware Server Console (TCP from management console t...
Port 902	UDP	VMware Server Console (UDP from server being managed...



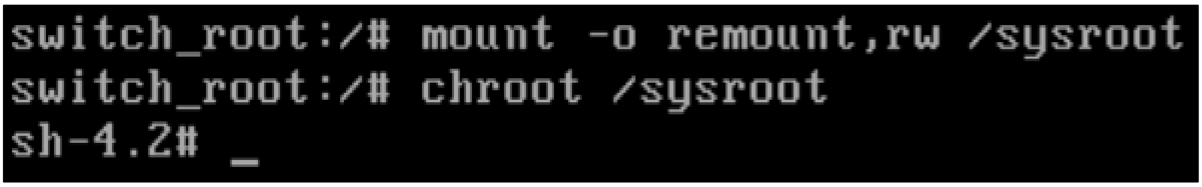
```
 CentOS Linux (3.10.0-693.11.1.el7.x86_64) 7 (Core)
 CentOS Linux (3.10.0-693.5.2.el7.x86_64) 7 (Core)
 CentOS Linux (3.10.0-693.el7.x86_64) 7 (Core)
 CentOS Linux (0-rescue-2eda73dbd53444c5b4f8d6e607d581d5) 7 (Core)






 Use the ↑ and ↓ keys to change the selection.
 Press 'e' to edit the selected item, or 'c' for a command prompt.
```



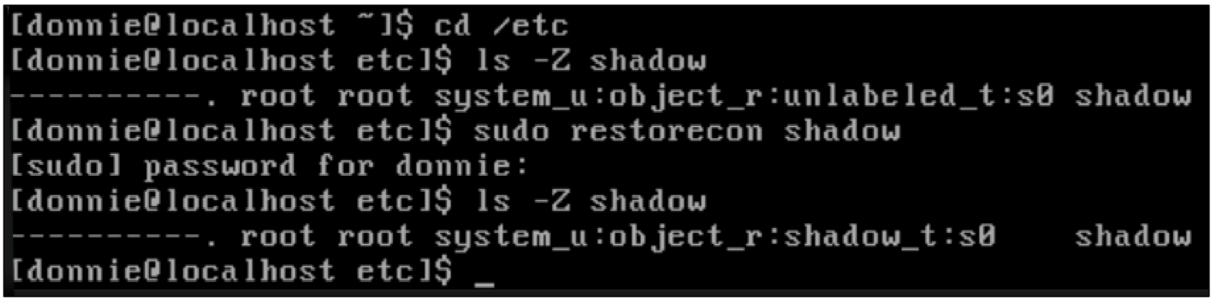
```
_       linux16 /vmlinuz-3.10.0-693.11.1.el7.x86_64 root=/dev/mapper/centos-ro\
ot ro crashkernel=auto rd.lvm.lv=centos/root rd.luks.uuid=luks-2d7f02c7-864f-4\
2ce-b362-50dd830d9772 rd.lvm.lv=centos/swap rhgb quiet LANG=en_US.UTF-8
```



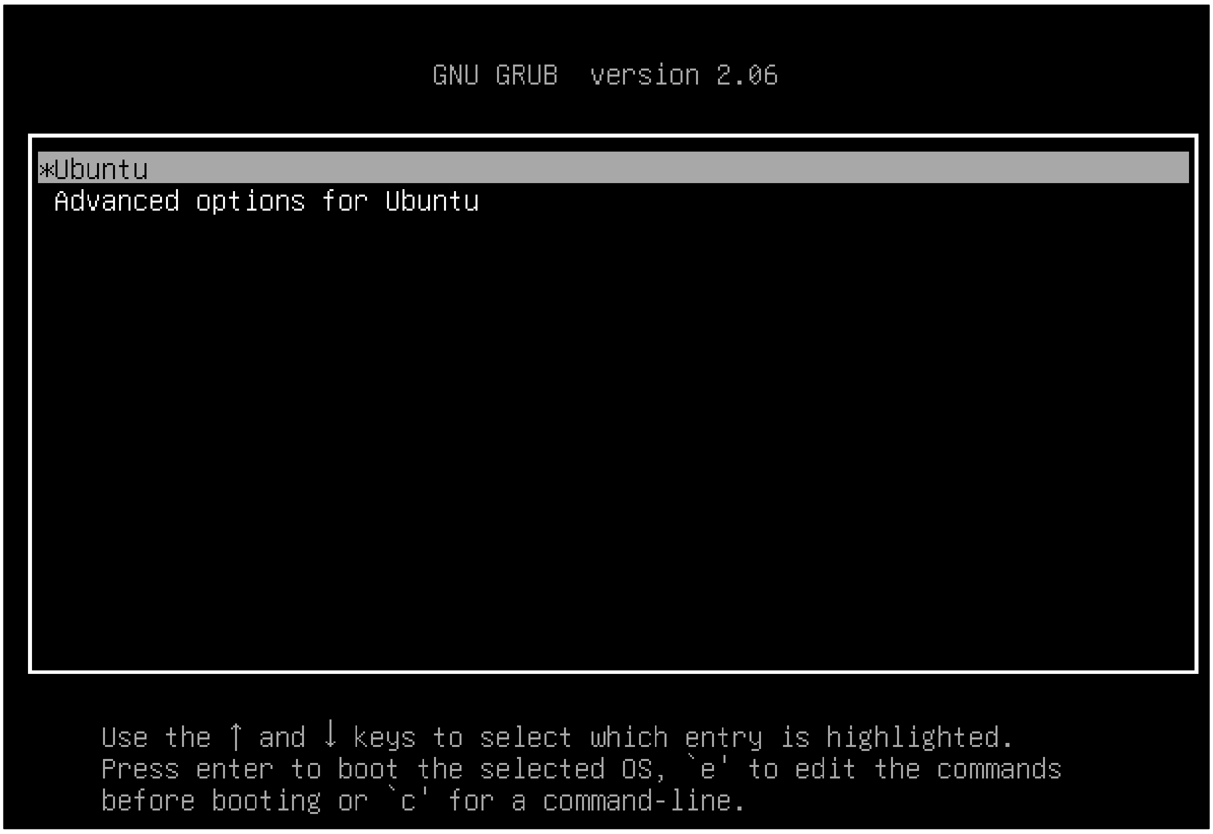
```
Entering emergency mode. Exit the shell to continue.
Type "journalctl" to view system logs.
You might want to save "/run/initramfs/rdsosreport.txt" to a USB stick or /boot
after mounting them and attach it to a bug report.


switch_root:/# _
```



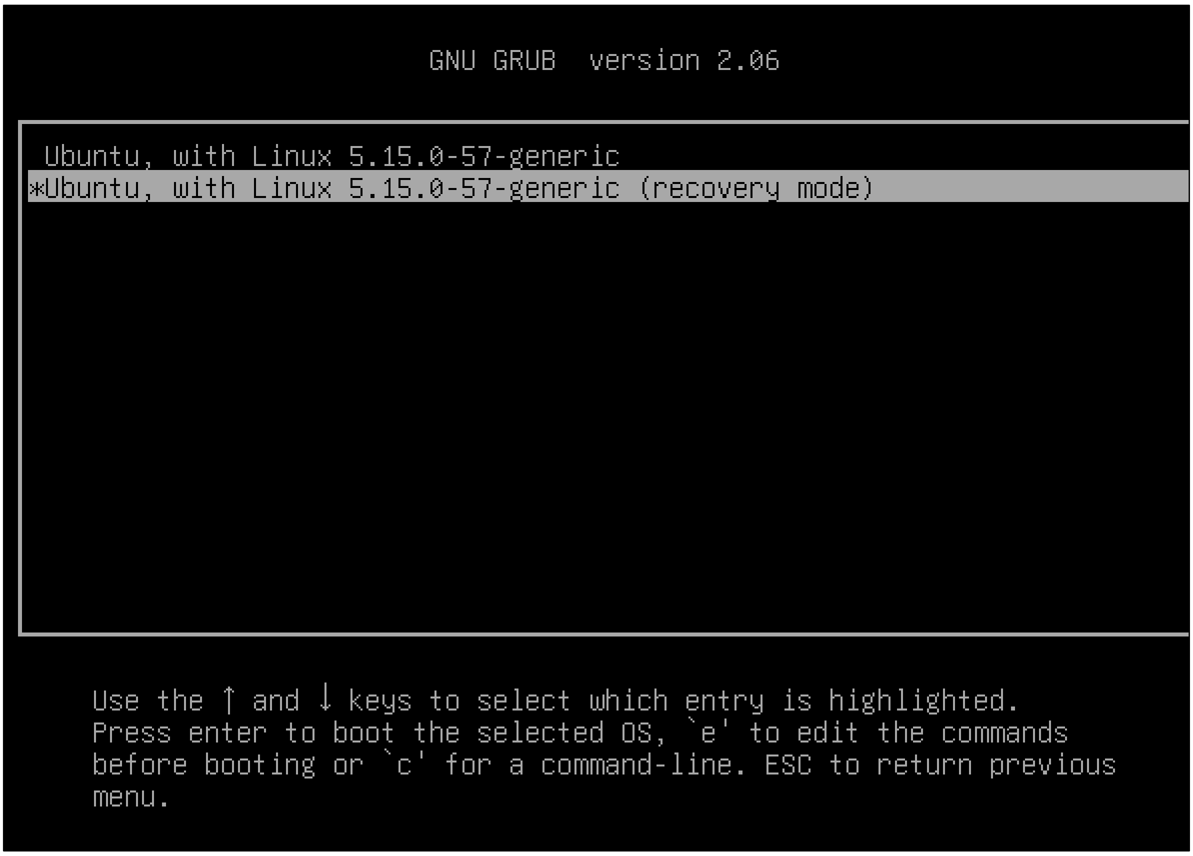
```
switch_root:/# mount -o remount,rw /sysroot
switch_root:/# chroot /sysroot
sh-4.2# _
```



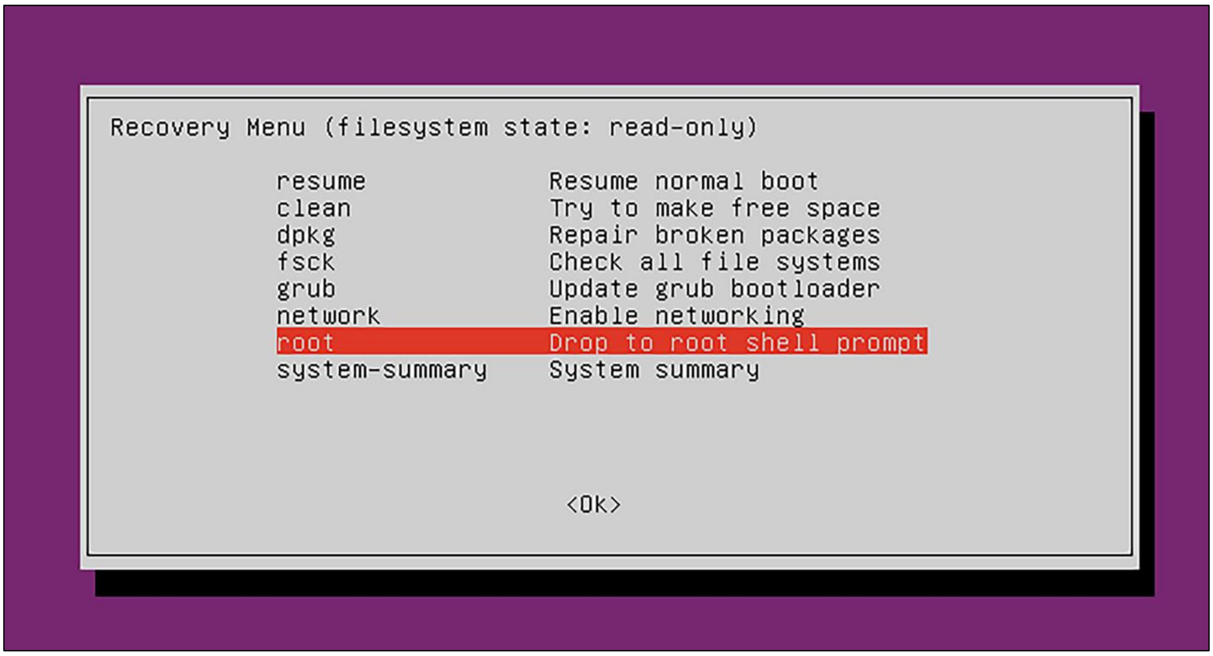
```
[donnie@localhost ~]$ cd /etc
[donnie@localhost etc]$ ls -Z shadow
----------. root root system_u:object_r:unlabeled_t:s0 shadow
[donnie@localhost etc]$ sudo restorecon shadow
[sudo] password for donnie:
[donnie@localhost etc]$ ls -Z shadow
----------. root root system_u:object_r:shadow_t:s0    shadow
[donnie@localhost etc]$ _
```



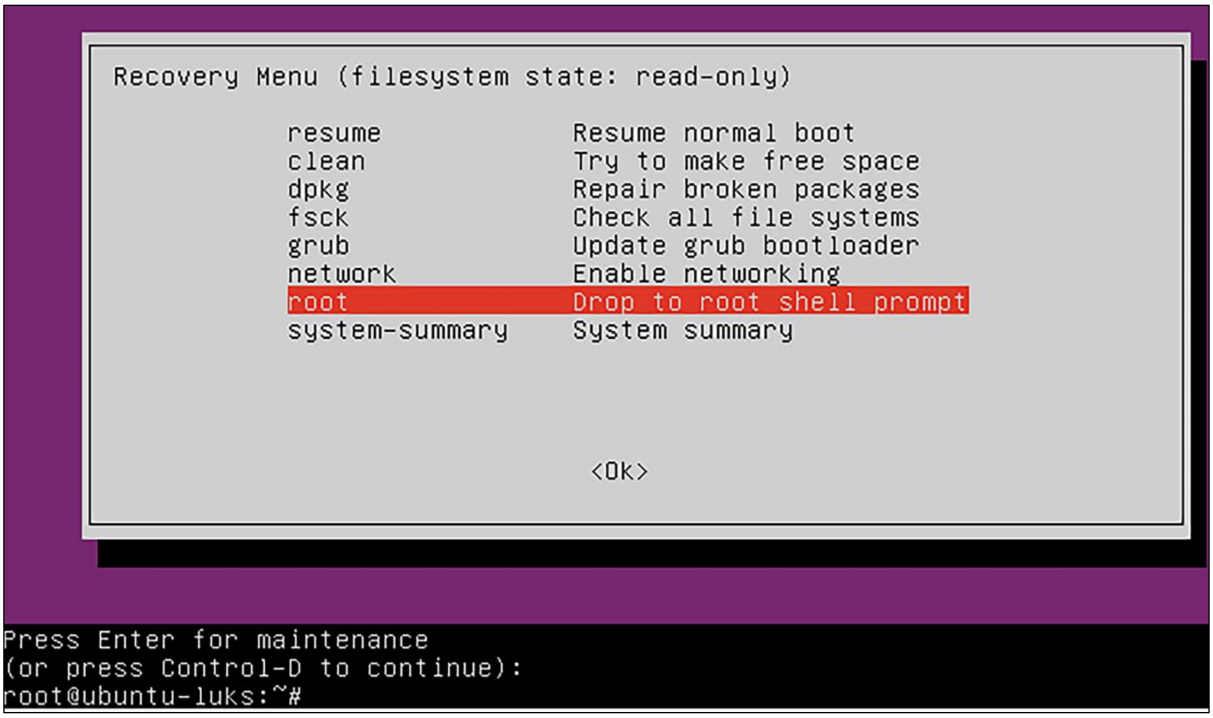
```
                    GNU GRUB  version 2.06

*Ubuntu
 Advanced options for Ubuntu




     Use the ↑ and ↓ keys to select which entry is highlighted.
     Press enter to boot the selected OS, `e' to edit the commands
     before booting or `c' for a command-line.
```



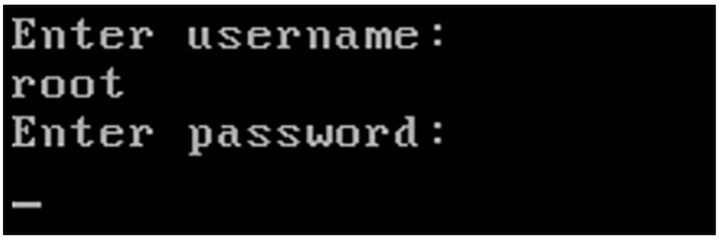
```
                     GNU GRUB  version 2.06

 Ubuntu, with Linux 5.15.0-57-generic
*Ubuntu, with Linux 5.15.0-57-generic (recovery mode)

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, `e' to edit the commands
    before booting or `c' for a command-line. ESC to return previous
    menu.
```



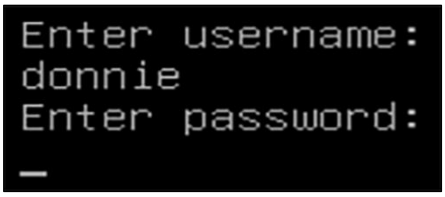
```
Recovery Menu (filesystem state: read-only)

           resume                  Resume normal boot
           clean                   Try to make free space
           dpkg                    Repair broken packages
           fsck                    Check all file systems
           grub                    Update grub bootloader
           network                 Enable networking
           root                    Drop to root shell prompt
           system-summary          System summary


                              <Ok>
```



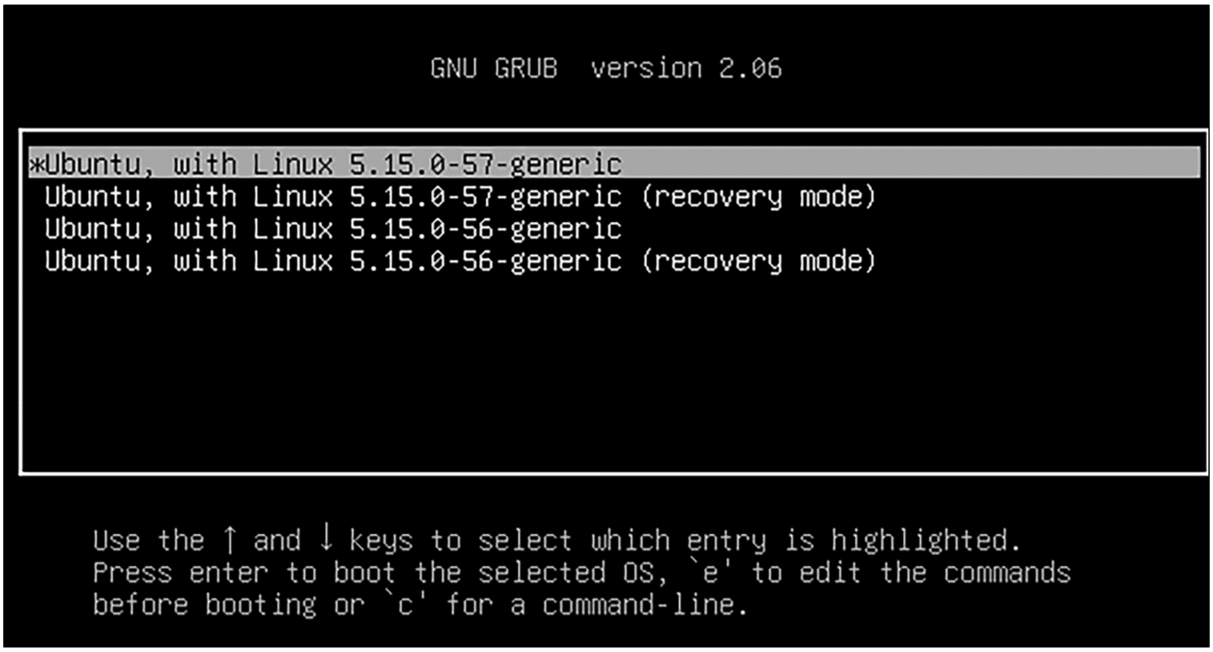
```
Recovery Menu (filesystem state: read-only)

              resume             Resume normal boot
              clean              Try to make free space
              dpkg               Repair broken packages
              fsck               Check all file systems
              grub               Update grub bootloader
              network            Enable networking
              root               Drop to root shell prompt
              system-summary     System summary




                                  <Ok>

Press Enter for maintenance
(or press Control-D to continue):
root@ubuntu-luks:~#
```



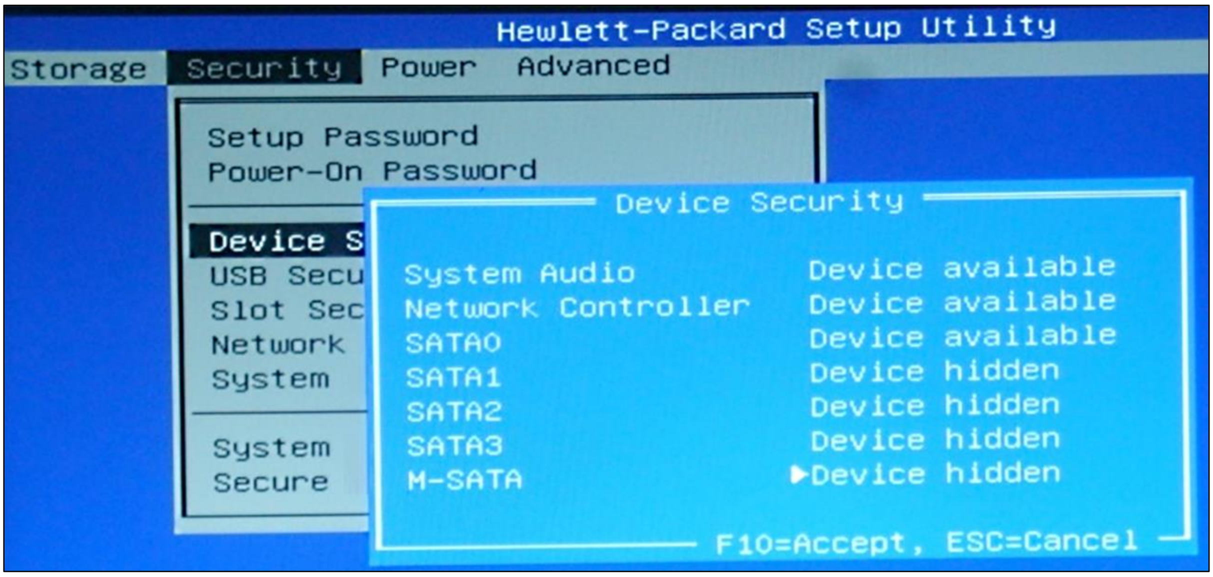
```
Enter username:
root
Enter password:

_
```



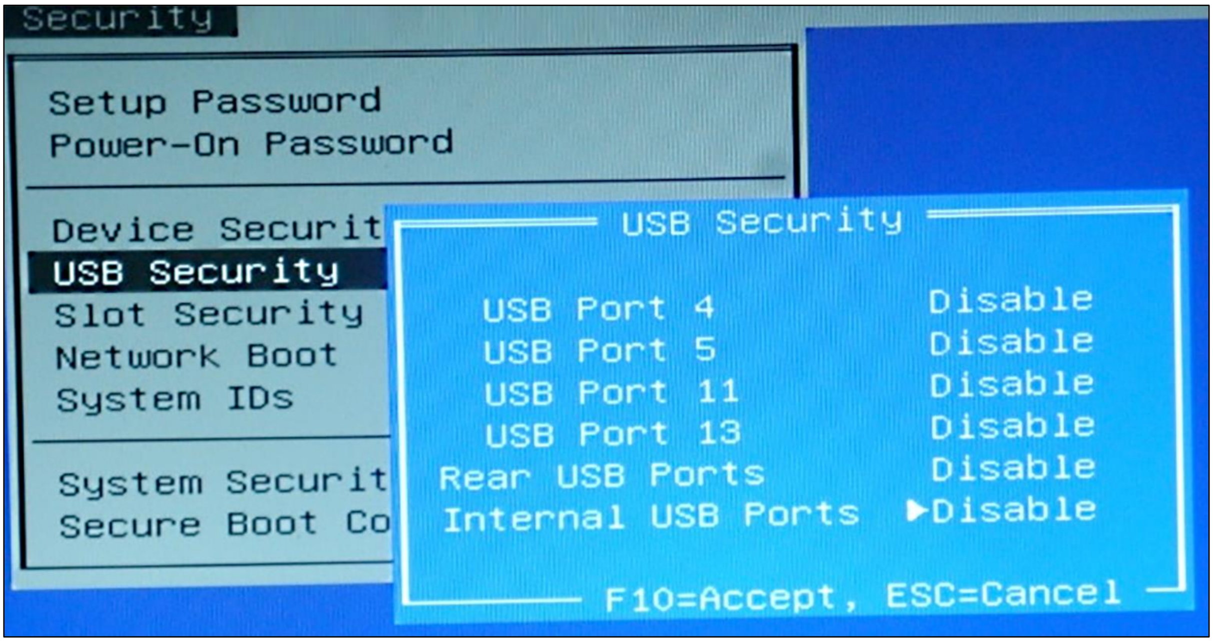
```
Enter username:
donnie
Enter password:

_
```



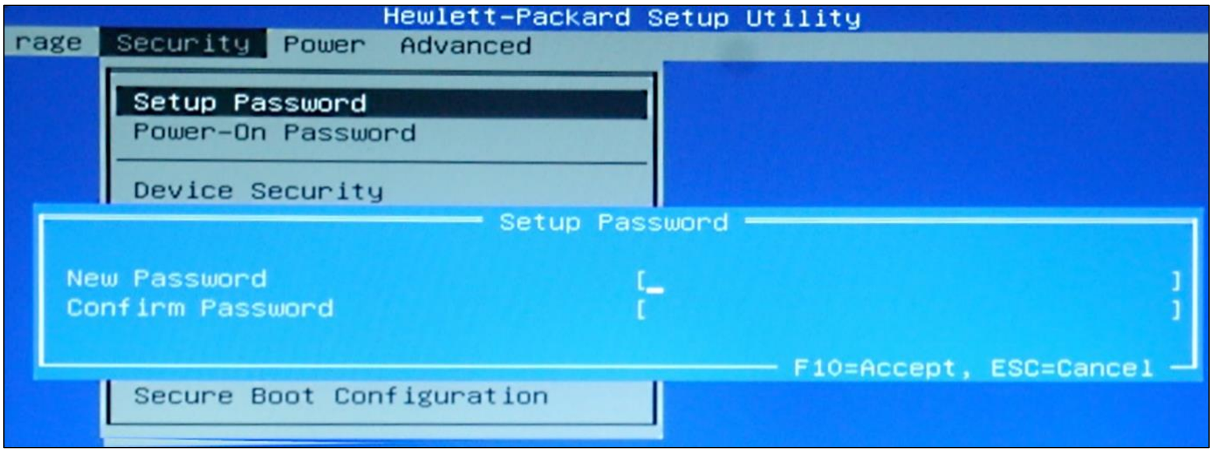
```
                    GNU GRUB  version 2.06

*Ubuntu, with Linux 5.15.0-57-generic
 Ubuntu, with Linux 5.15.0-57-generic (recovery mode)
 Ubuntu, with Linux 5.15.0-56-generic
 Ubuntu, with Linux 5.15.0-56-generic (recovery mode)






     Use the ↑ and ↓ keys to select which entry is highlighted.
     Press enter to boot the selected OS, `e' to edit the commands
     before booting or `c' for a command-line.
```



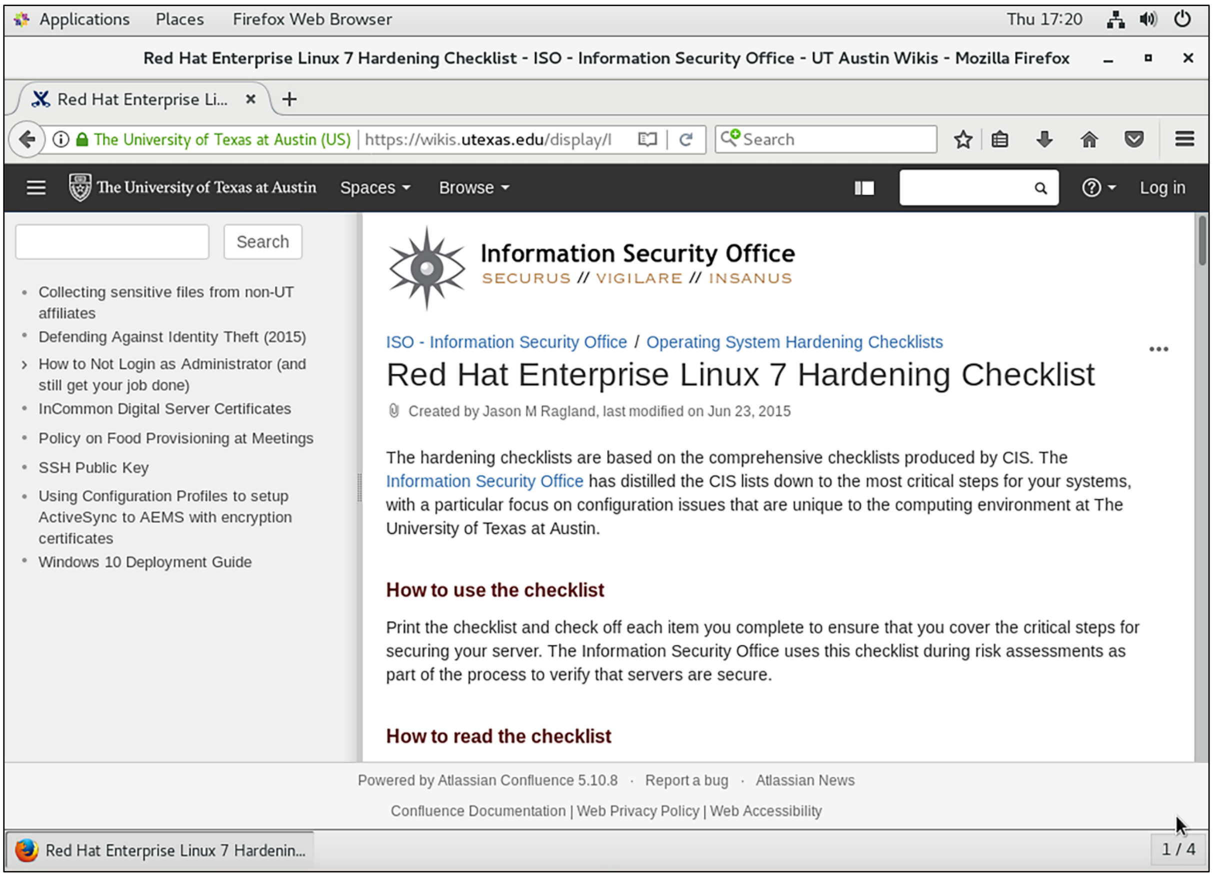
```
                          Hewlett-Packard Setup Utility
Storage  Security  Power  Advanced

      Setup Password
      Power-On Password

      Device S         Device Security
      USB Secu
      Slot Sec         System Audio             Device available
      Network          Network Controller       Device available
      System           SATA0                    Device available
                       SATA1                    Device hidden
      System           SATA2                    Device hidden
      Secure           SATA3                    Device hidden
                       M-SATA                  ▶Device hidden

                                        F10=Accept, ESC=Cancel
```



```
Security

  Setup Password
  Power-On Password

  Device Securit          USB Security
  USB Security
  Slot Security       USB Port 4              Disable
  Network Boot        USB Port 5              Disable
  System IDs          USB Port 11             Disable
                      USB Port 13             Disable
  System Securit    Rear USB Ports            Disable
  Secure Boot Co    Internal USB Ports       ▶Disable

                         F10=Accept, ESC=Cancel
```



```
                    Hewlett-Packard Setup Utility
rage  Security  Power  Advanced

     Setup Password
     Power-On Password

     Device Security
                            Setup Password

  New Password                              [_                              ]
  Confirm Password                          [                               ]

                                                  F10=Accept, ESC=Cancel
     Secure Boot Configuration
```



Red Hat Enterprise Linux 7 Hardening Checklist - ISO - Information Security Office - UT Austin Wikis - Mozilla Firefox

https://wikis.utexas.edu/display/I

Information Security Office
SECURUS // VIGILARE // INSANUS

ISO - Information Security Office / Operating System Hardening Checklists

Red Hat Enterprise Linux 7 Hardening Checklist

Created by Jason M Ragland, last modified on Jun 23, 2015

The hardening checklists are based on the comprehensive checklists produced by CIS. The Information Security Office has distilled the CIS lists down to the most critical steps for your systems, with a particular focus on configuration issues that are unique to the computing environment at The University of Texas at Austin.

How to use the checklist

Print the checklist and check off each item you complete to ensure that you cover the critical steps for securing your server. The Information Security Office uses this checklist during risk assessments as part of the process to verify that servers are secure.

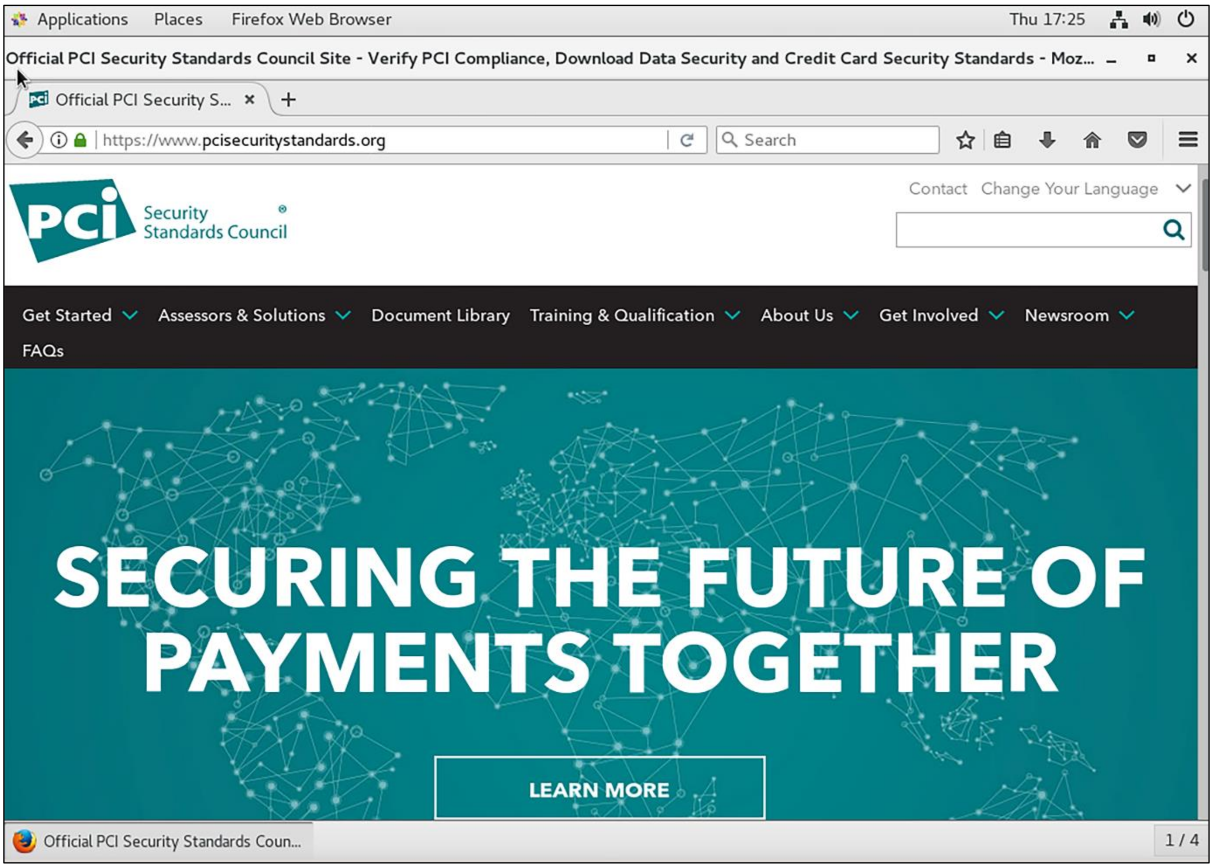
How to read the checklist

- Collecting sensitive files from non-UT affiliates
- Defending Against Identity Theft (2015)
- How to Not Login as Administrator (and still get your job done)
- InCommon Digital Server Certificates
- Policy on Food Provisioning at Meetings
- SSH Public Key
- Using Configuration Profiles to setup ActiveSync to AEMS with encryption certificates
- Windows 10 Deployment Guide

Powered by Atlassian Confluence 5.10.8 · Report a bug · Atlassian News

Confluence Documentation | Web Privacy Policy | Web Accessibility

Applications
Places
Firefox Web Browser
Thu 17:20
Red Hat Enterprise Li...
The University of Texas at Austin (US)
Search
The University of Texas at Austin
Spaces
Browse
Log in
Search
Red Hat Enterprise Linux 7 Hardenin...
1 / 4



Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards - Moz...

https://www.pcisecuritystandards.org

SECURING THE FUTURE OF PAYMENTS TOGETHER