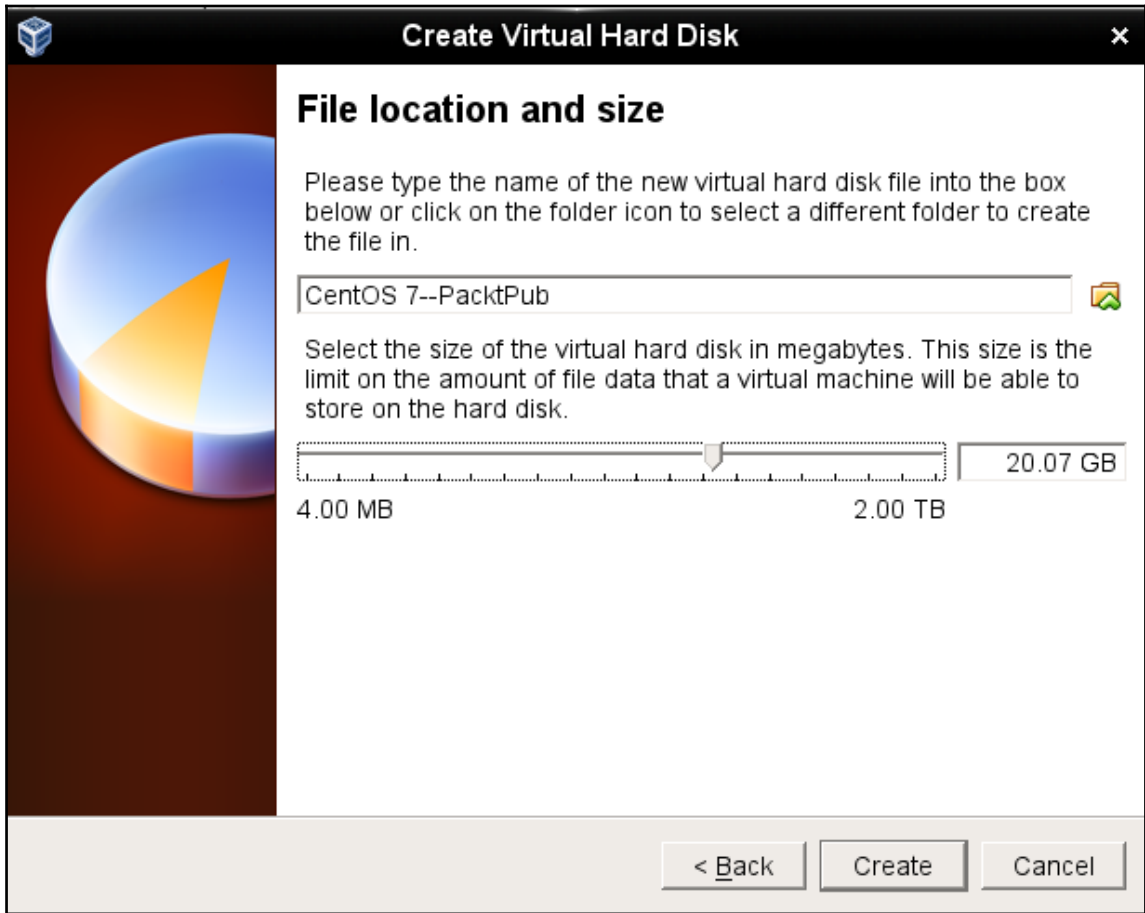
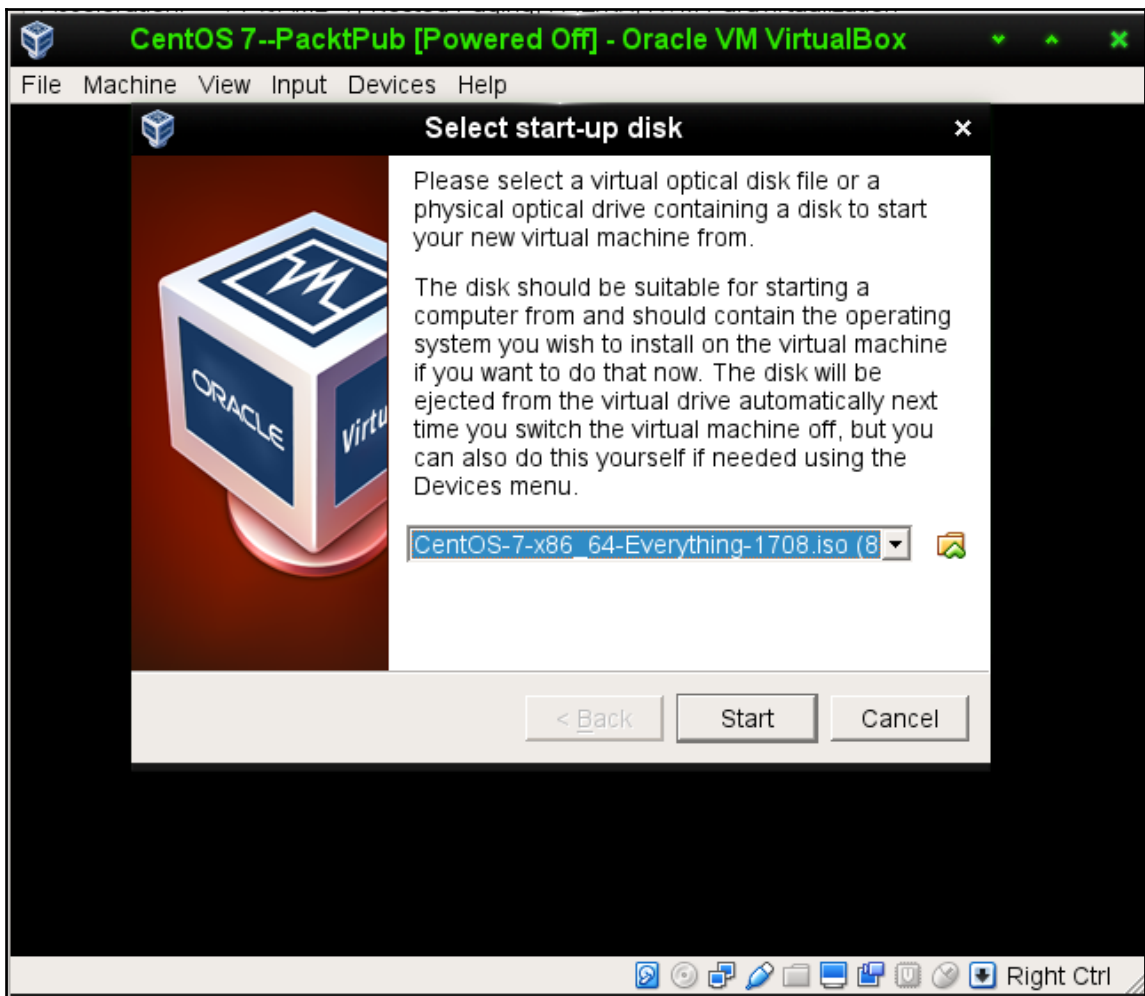


# Chapter 1: Running Linux in a Virtual Environment





**CREATE USER** CENTOS 7 INSTALLATION

us

Full name:

User name:

Tip: Keep your user name shorter than 32 characters and do not use spaces.

Make this user administrator

Require a password to use this account

Password:

Strong

Confirm password:

**CentOS 7--PacktPub - Settings** [X]

- General
- System
- Display
- Storage
- Audio
- Network**
- Serial Ports
- USB
- Shared Folders
- User Interface

**Network**

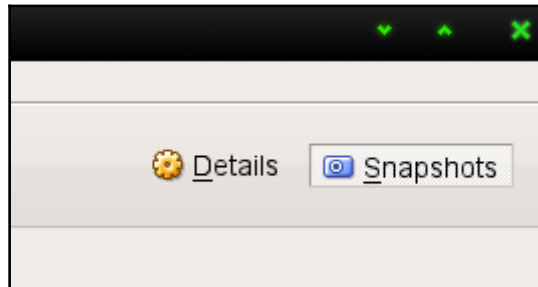
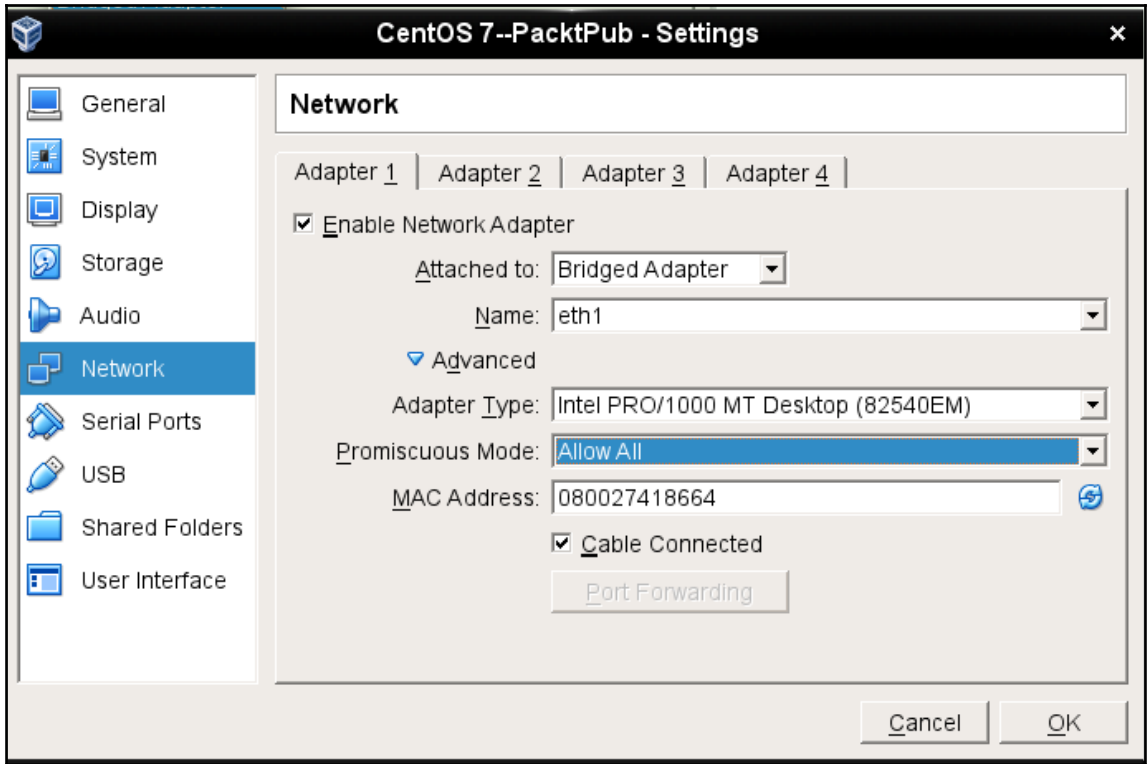
Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

Enable Network Adapter

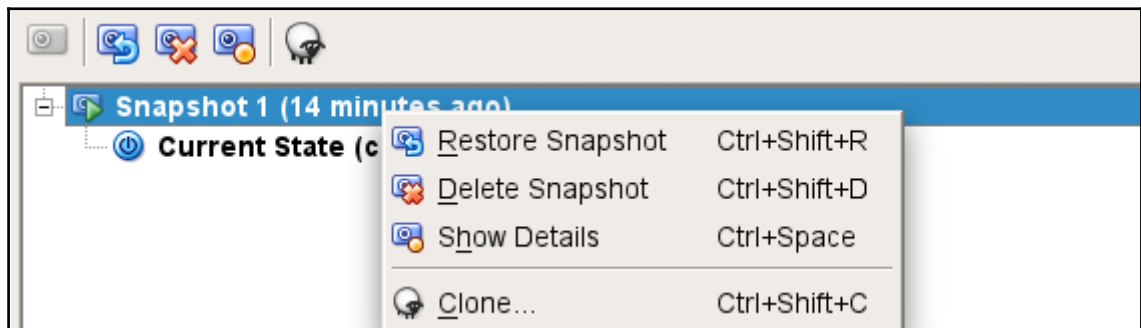
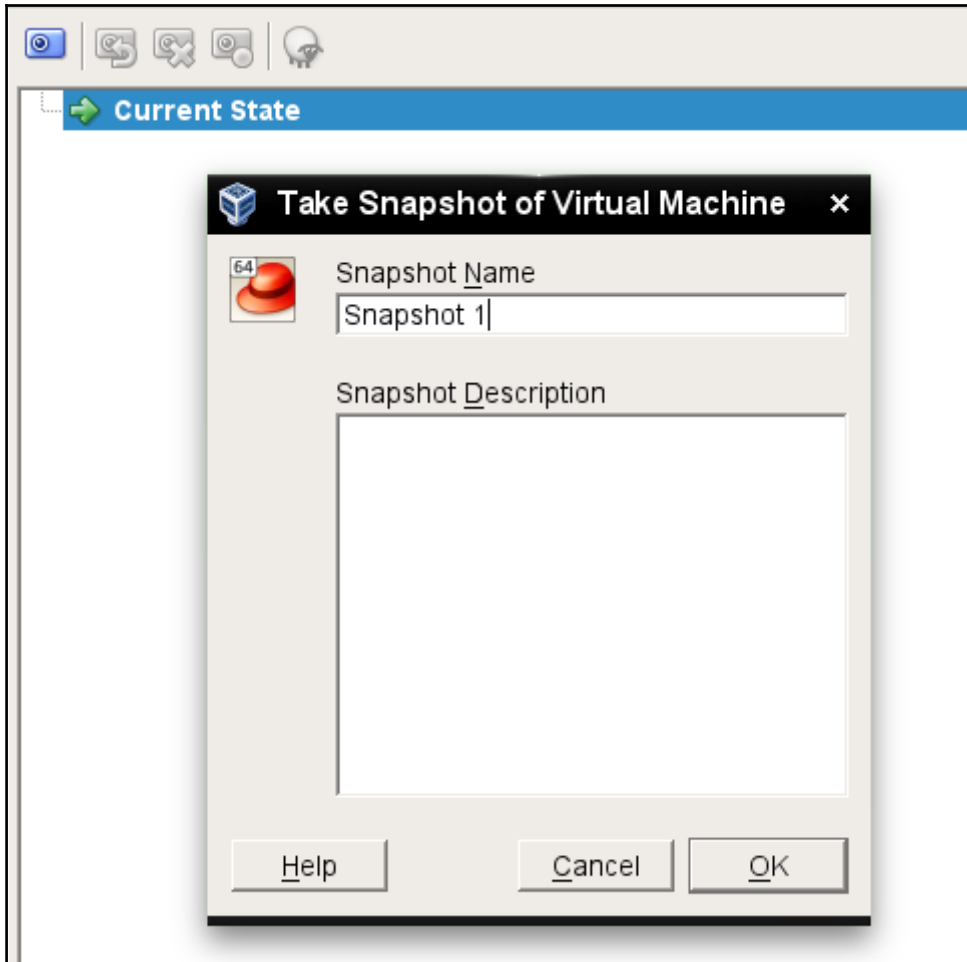
Attached to:

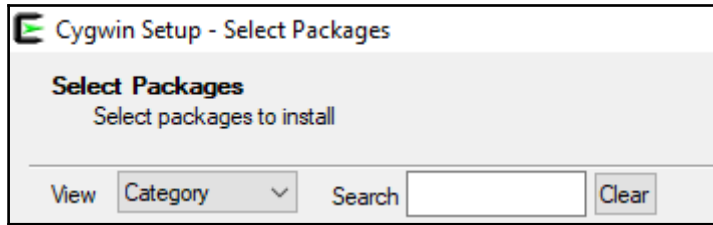
Name:

- Not attached
- NAT
- NAT Network
- Bridged Adapter**
- Internal Network
- Host-only Adapter
- Generic Driver





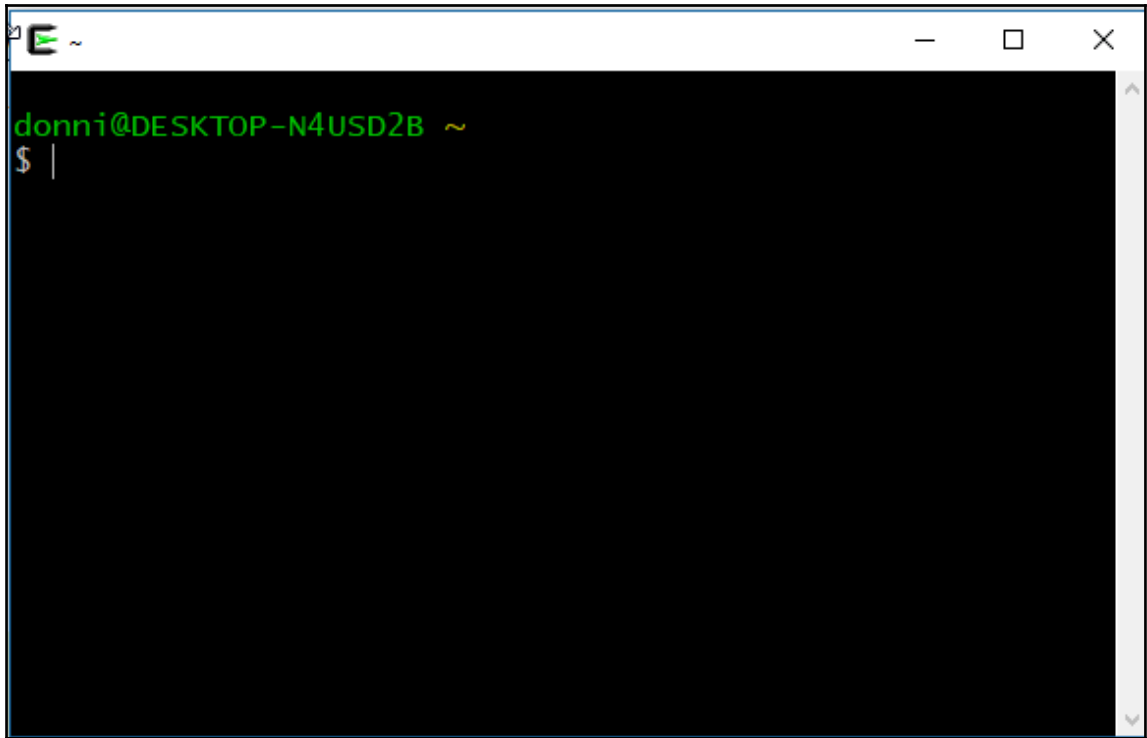




<input type="checkbox"/> Net <input checked="" type="checkbox"/> Default		<input checked="" type="checkbox"/> Skip	n/a	n/a	1,071k	aria2: Download utility for HTTP/HTTPS, FTP, BitTorrent and Metalink
		<input checked="" type="checkbox"/> Skip	n/a	n/a	24k	autossh: Automatically restart SSH sessions and tunnels

<input checked="" type="checkbox"/> Skip	n/a	n/a	1,898k	openldap-server: Lightweight Directory Access Protocol suite (server)
<input checked="" type="checkbox"/> Skip	n/a	n/a	750k	openssh: The OpenSSH server and client programs
<input checked="" type="checkbox"/> Skip	n/a	n/a	570k	openssl: A general purpose cryptography toolkit with TLS implementation
<input checked="" type="checkbox"/> Skip	n/a	n/a	4,693k	openssl-devel: A general purpose cryptography toolkit with TLS implementation (development)

<input checked="" type="checkbox"/> Skip	n/a	n/a	1,898k	openldap-server: Lightweight Directory Access Protocol suite (server)
<input checked="" type="checkbox"/> 7.5p1-1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	750k	openssh: The OpenSSH server and client programs
<input checked="" type="checkbox"/> Skip	n/a	n/a	570k	openssl: A general purpose cryptography toolkit with TLS implementation
<input checked="" type="checkbox"/> Skip	n/a	n/a	4,693k	openssl-devel: A general purpose cryptography toolkit with TLS implementation (development)



## Chapter 2: Securing User Accounts

```
Ubuntu 16.04.3 LTS ubuntu-steemnode tty1
ubuntu-steemnode login: _
```

```
CentOS Linux 7 (Core)
Kernel 3.10.0-693.2.2.el7.x86_64 on an x86_64
localhost login: _
```

```
Warning! Authorized Users Only!

CentOS Linux 7 (Core)
Kernel 3.10.0-693.2.2.el7.x86_64 on an x86_64
localhost login: _
```

## Chapter 3: Securing Your Server with a Firewall

```
Configuring iptables-persistent
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-to-date.
Save current IPv4 rules?
<Yes>                                     <No>
```

## Chapter 4: Encrypting and SSH Hardening

**Other Storage Options**

**Partitioning**

Automatically configure partitioning.  I will configure partitioning.

I would like to make additional space available.


**Encryption**

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


**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.

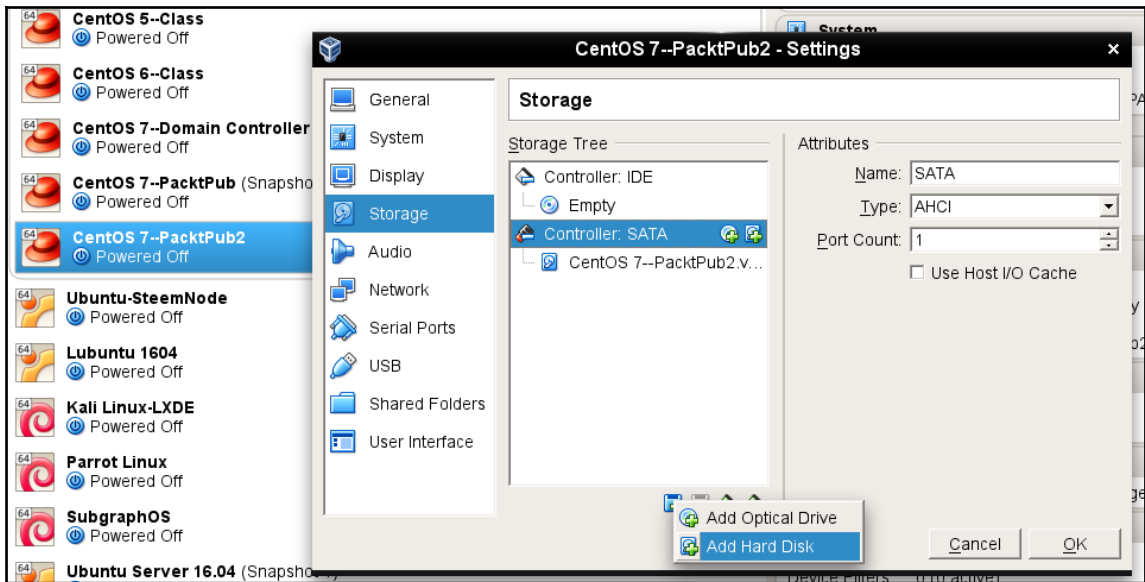
Passphrase:

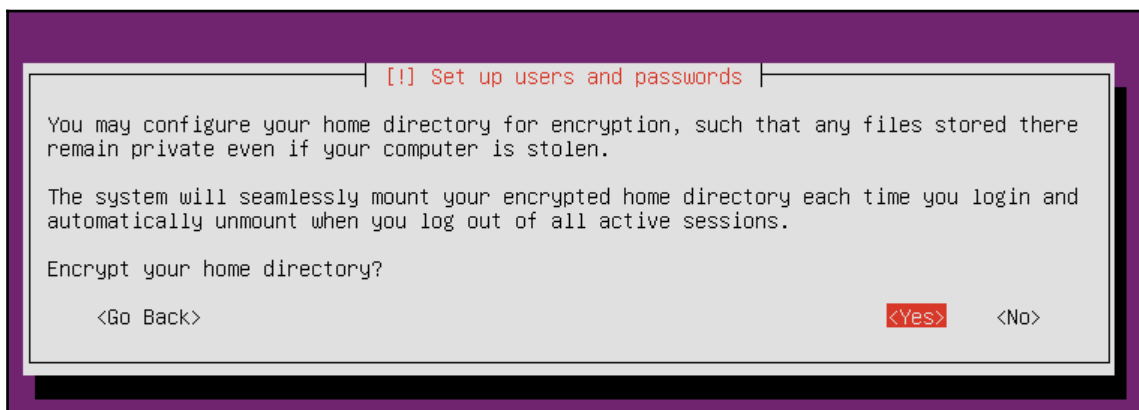
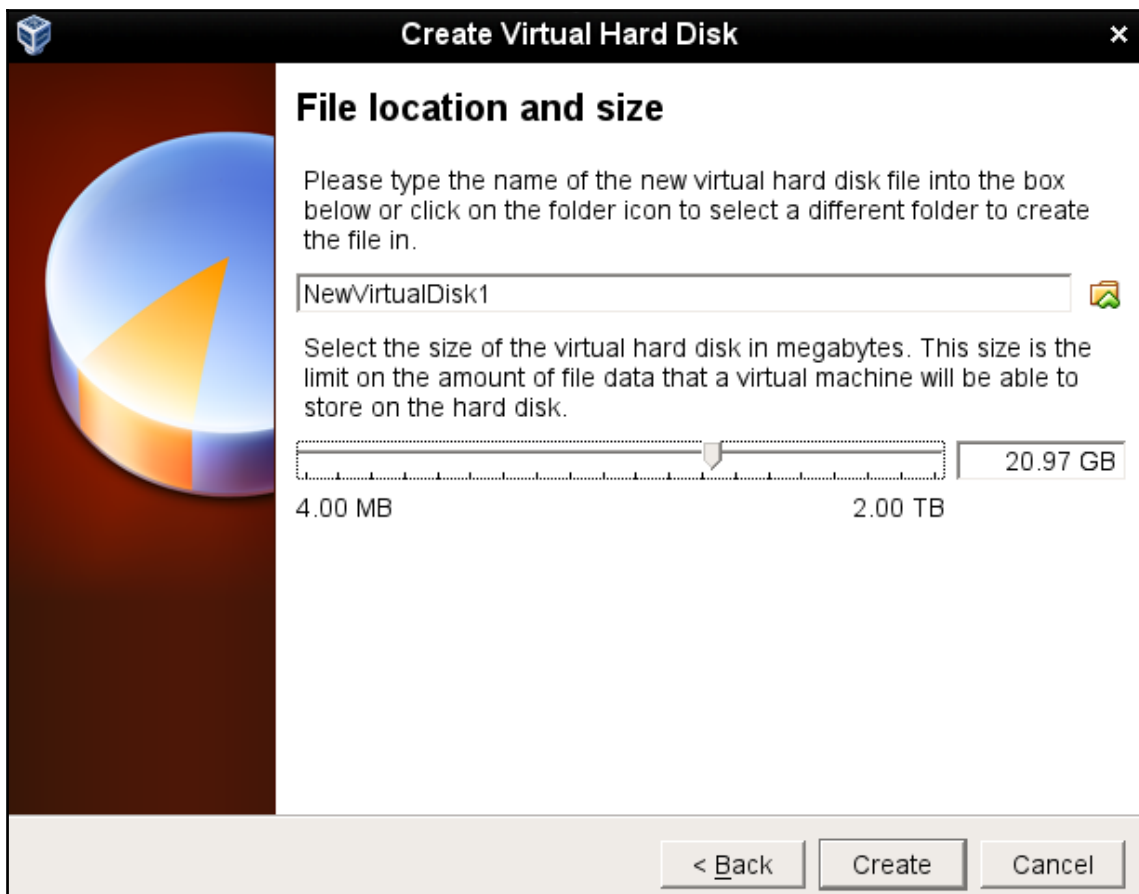
 **us**  Strong

Confirm:

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

```
Please enter passphrase for disk UBOX_HARDDISK (luks-2d7f02c7-864f-42ce-b362-50d
d830d9772)!:_
```







[!] Partition disks

The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

Partitioning method:

- Guided - use entire disk
- Guided - use entire disk and set up LVM
- Guided - use entire disk and set up encrypted LVM**
- Manual

<Go Back>

[!] Partition disks

You need to choose a passphrase to encrypt SCSI3 (0,0,0), partition #5 (sda).

The overall strength of the encryption depends strongly on this passphrase, so you should take care to choose a passphrase that is not easy to guess. It should not be a word or sentence found in dictionaries, or a phrase that could be easily associated with you.

A good passphrase will contain a mixture of letters, numbers and punctuation. Passphrases are recommended to have a length of 20 or more characters.

There is no way to recover this passphrase if you lose it. To avoid losing data, you should normally write down the passphrase and keep it in a safe place separate from this computer.

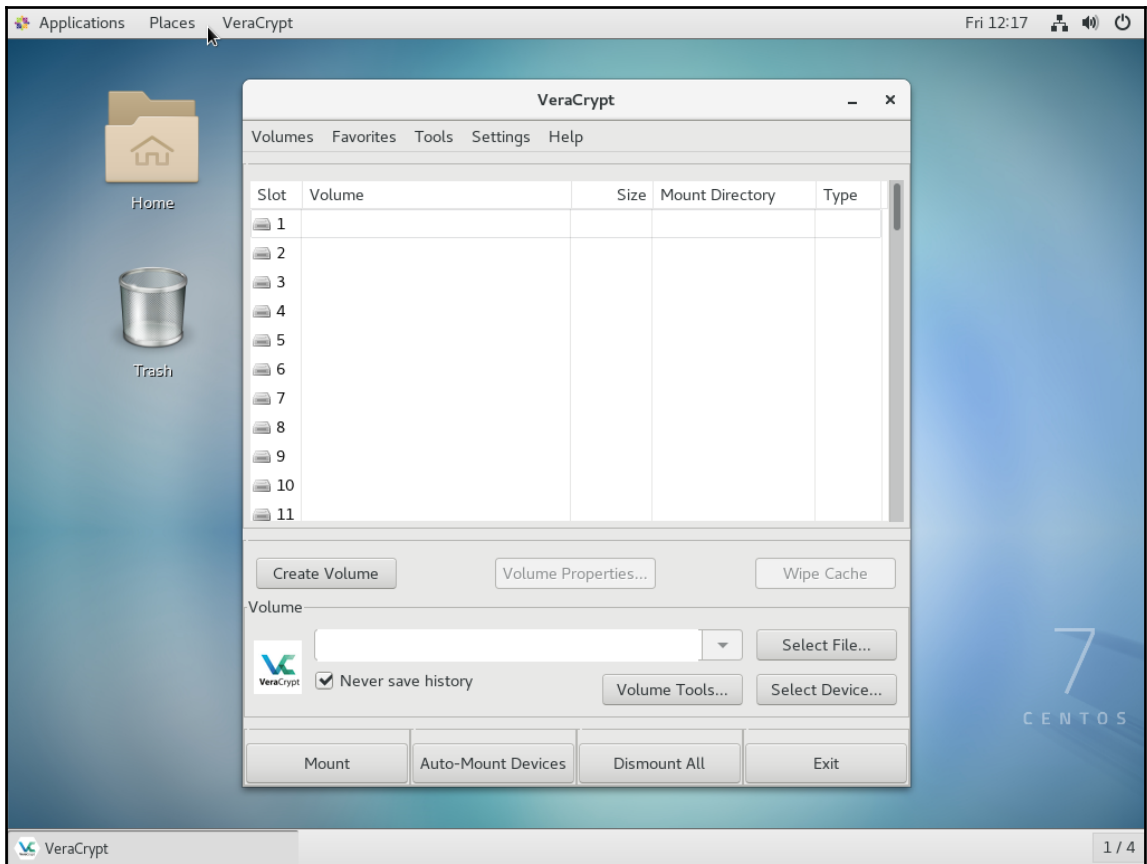
Encryption passphrase:

\_\_\_\_\_

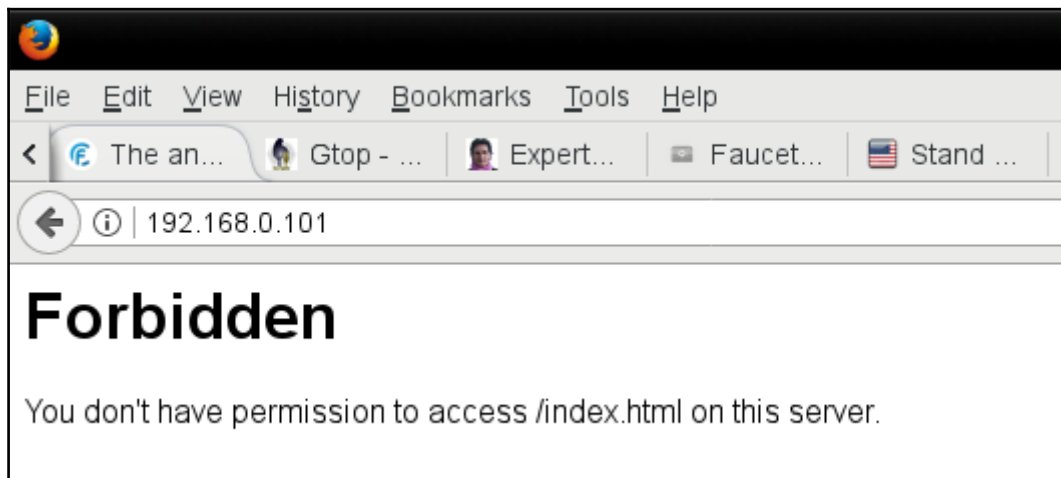
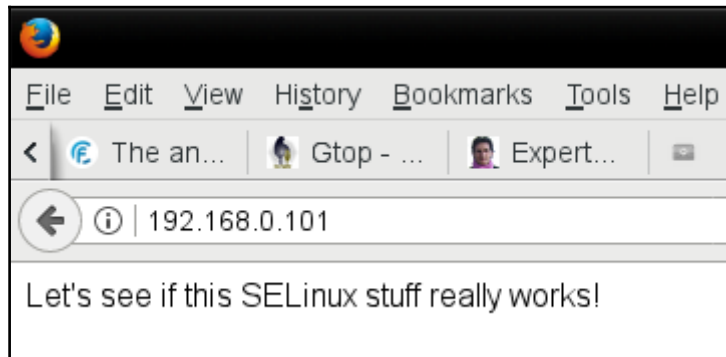
Show Password in Clear

<Go Back>

<Continue>



## Chapter 7: Implementing Mandatory Access Control with SELinux and AppArmor



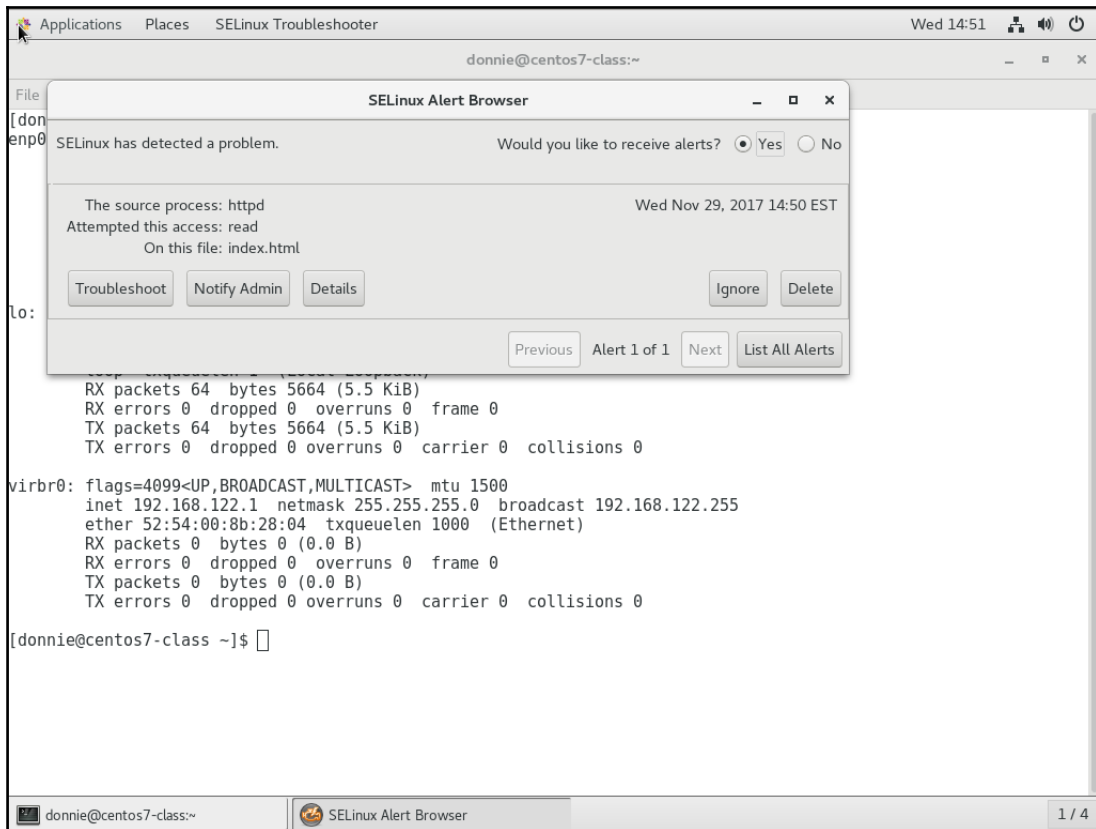
```
File Edit View Search Terminal Help
donnie@cent New SELinux security alert
AVC denial, click icon to view

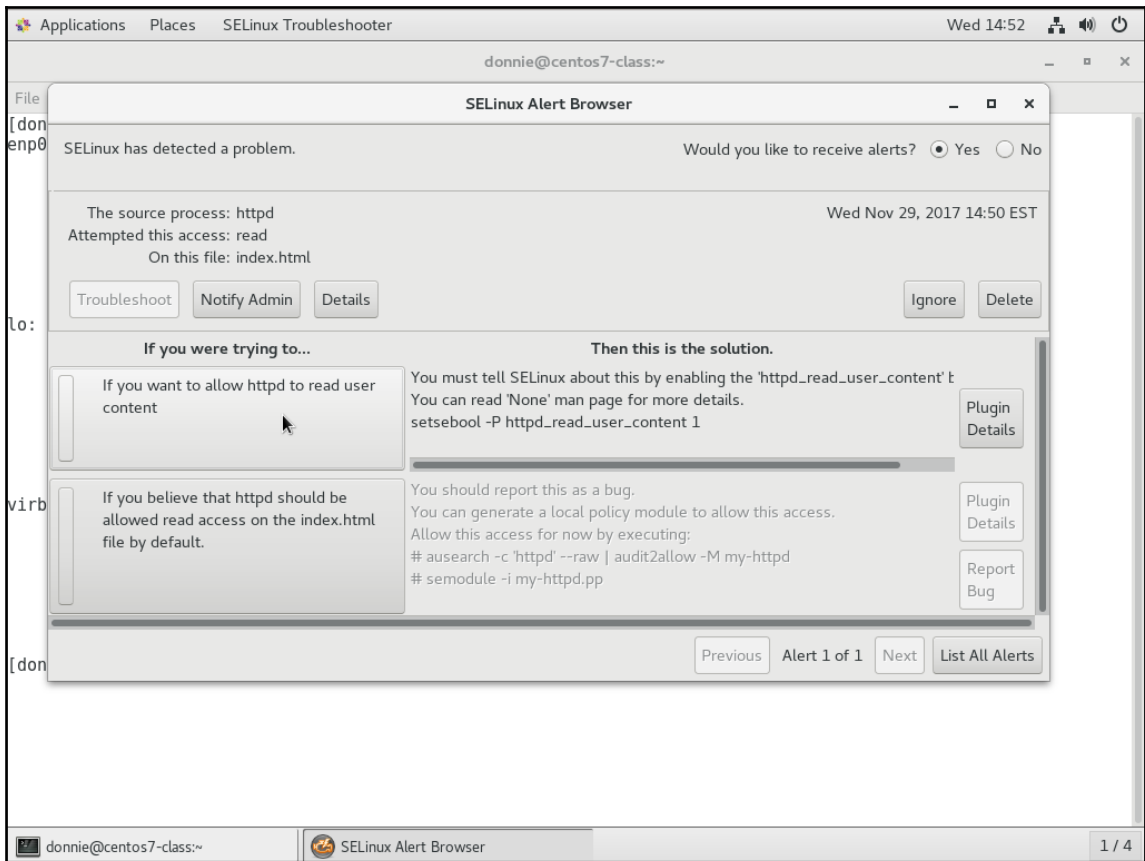
[donnie@centos7-class ~]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.4 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::a00:27ff:fe19:64d6 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:19:64:d6 txqueuelen 1000 (Ethernet)
    RX packets 240 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

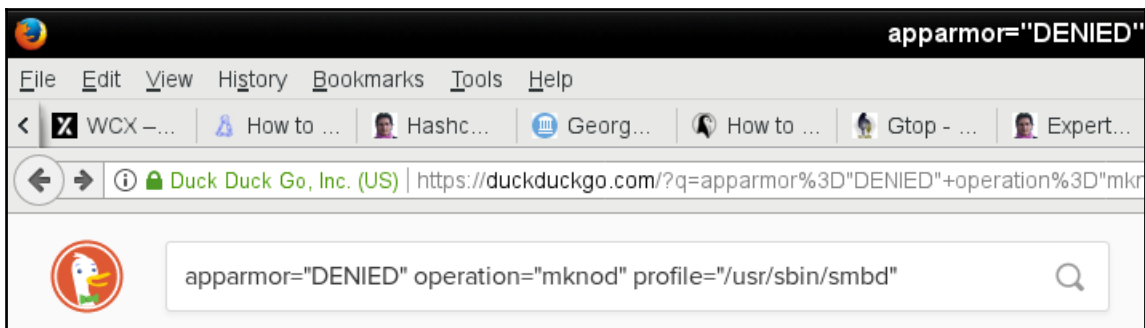
[donnie@centos7-class ~]$
```



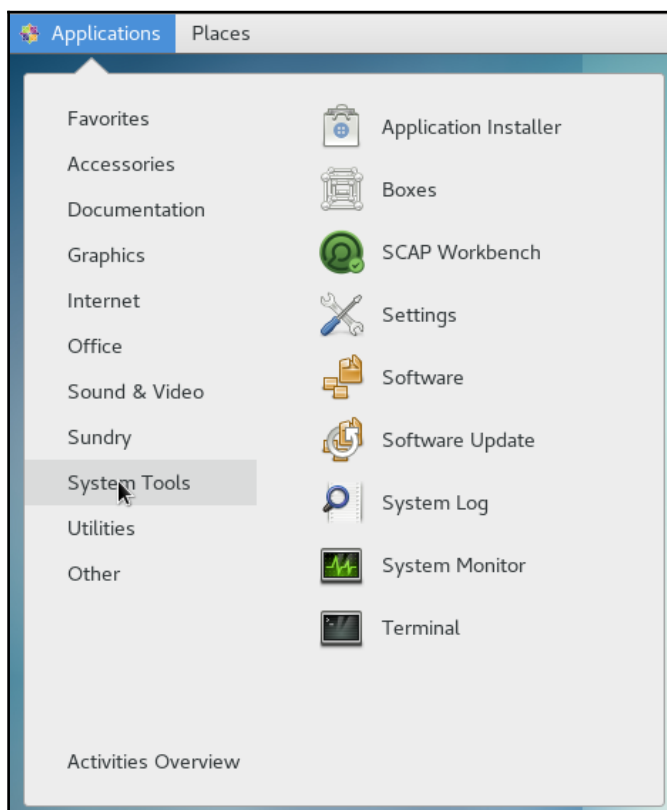


```
SELinux is preventing /usr/libexec/dovecot/dict from read access on the file .
**** Plugin catchall (100. confidence) suggests ****

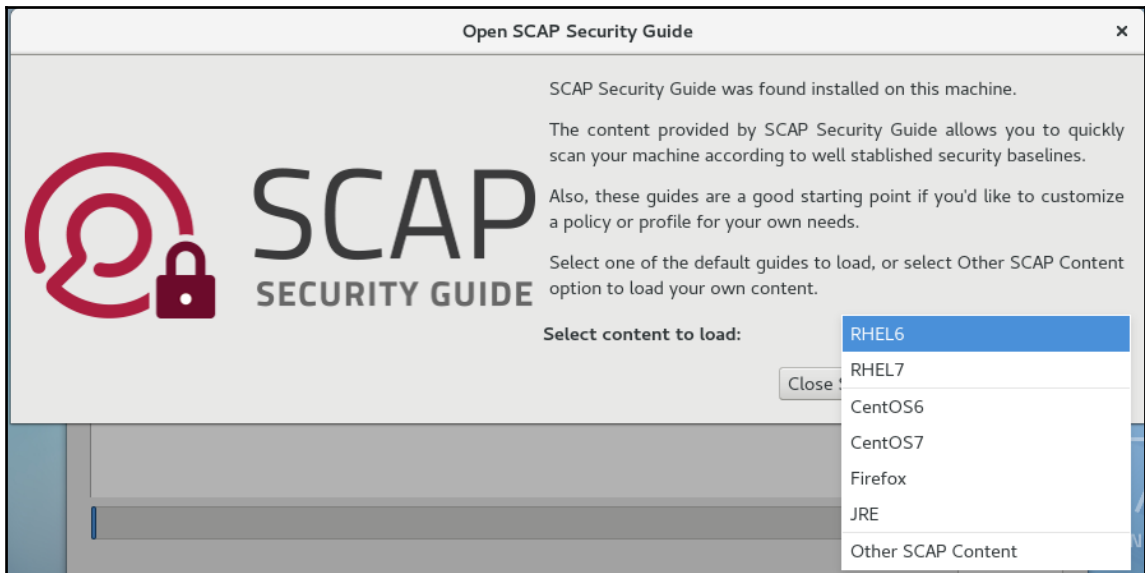
If you believe that dict should be allowed read access on the file by default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
# grep dict /var/log/audit/audit.log | audit2allow -M mypol
# semodule -i mypol.pp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

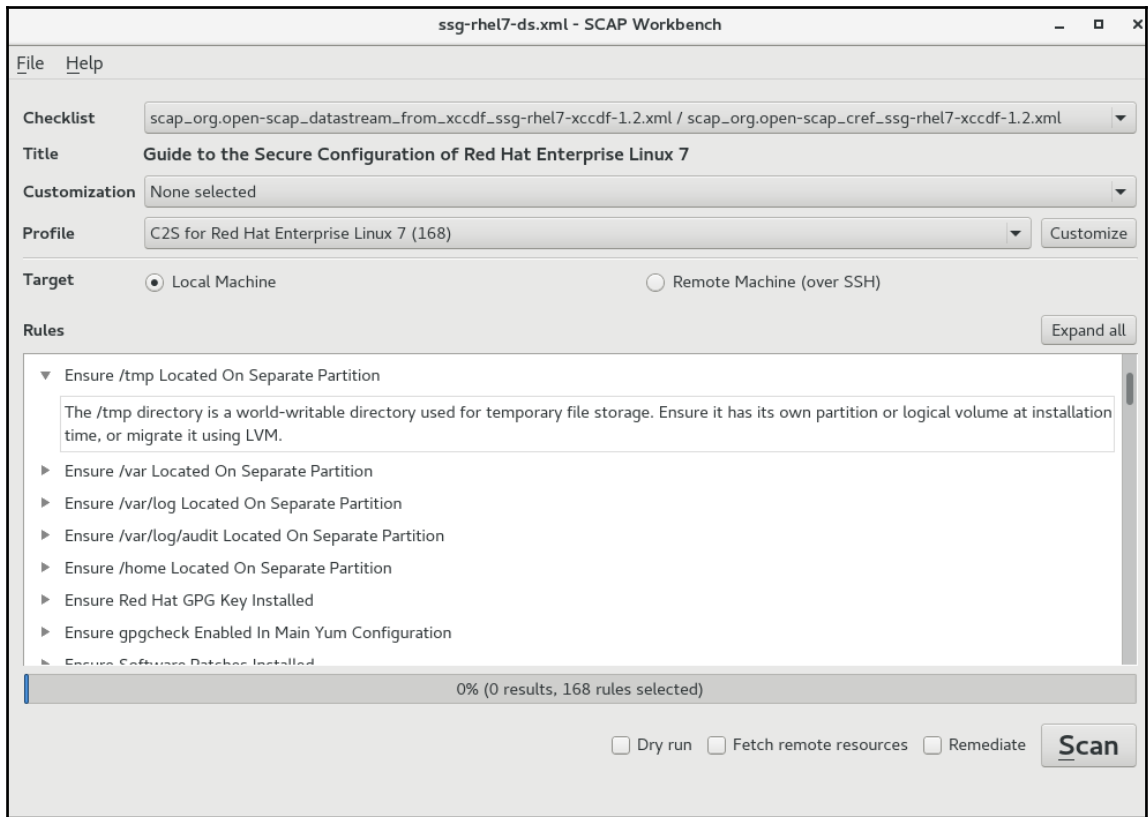


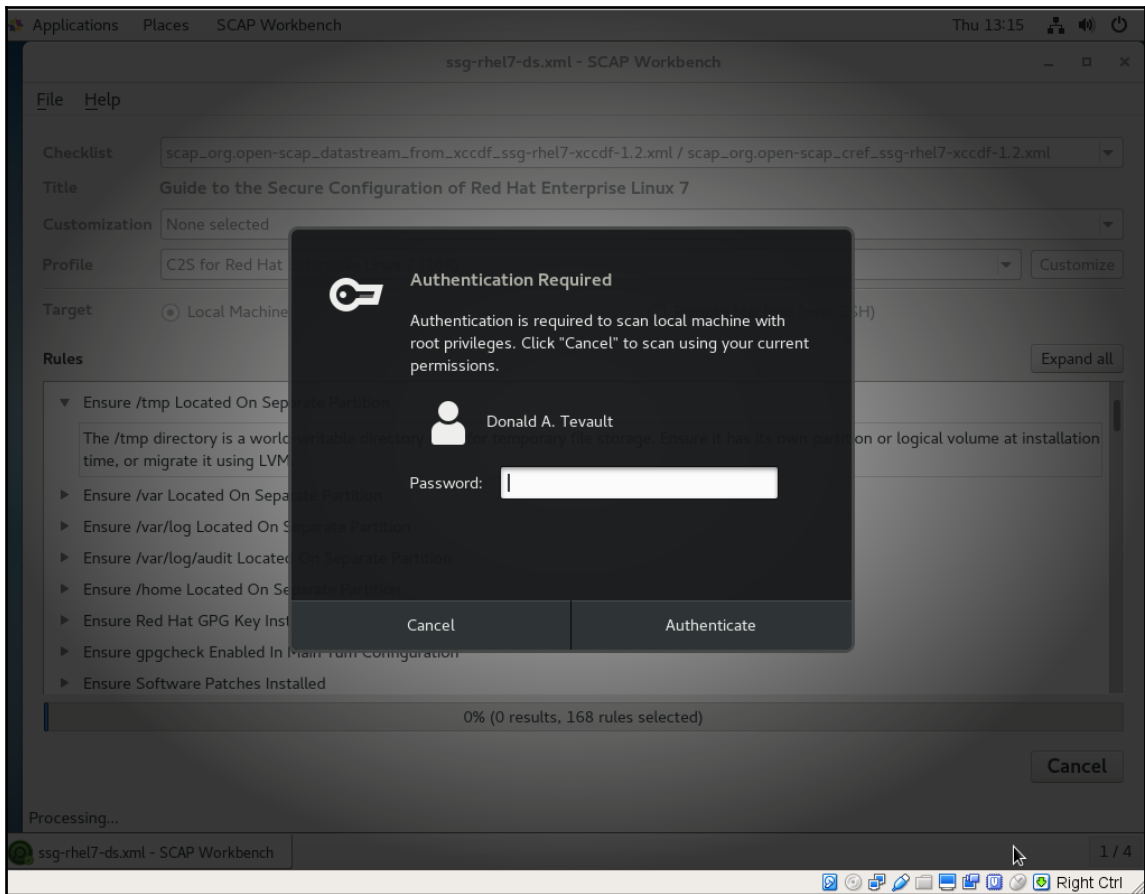
## Chapter 8: Scanning, Auditing, and Hardening











Suse 12 ▾

Ubuntu 14.04 ▾

Ubuntu 16.04 ▾

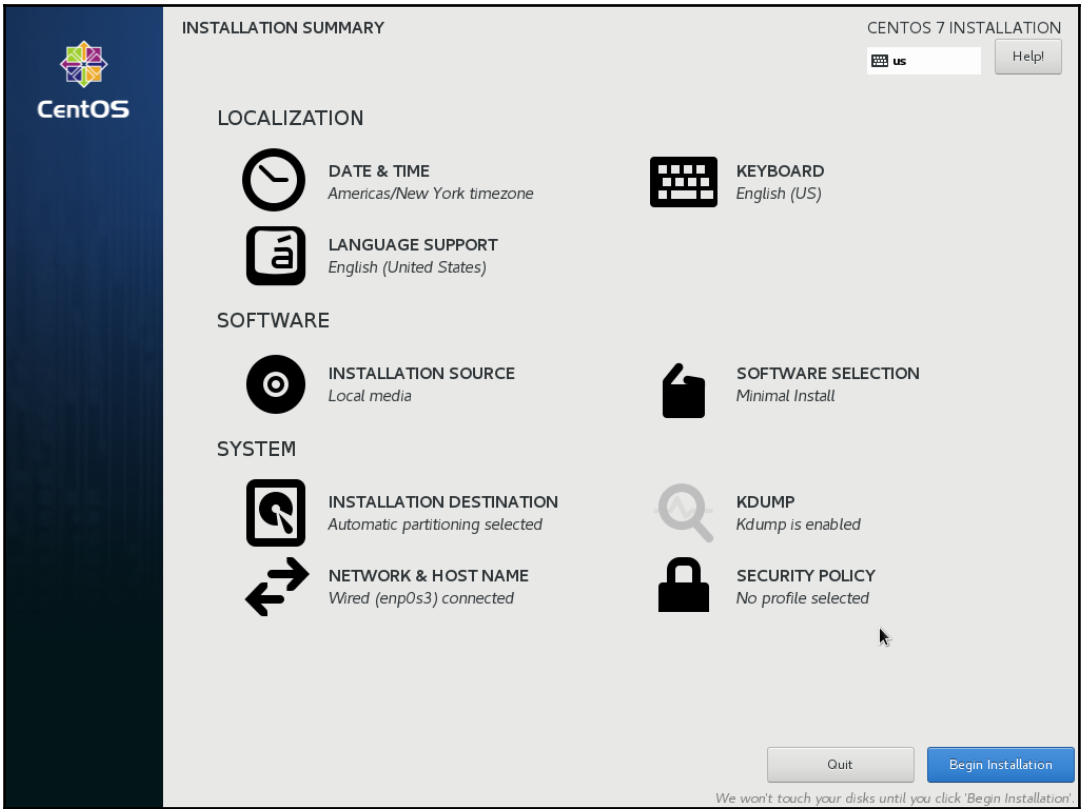
Common Profile for General-Purpose Ubuntu Systems

Profile for ANSSI DAT-NT28 Average (Intermediate) Level

Profile for ANSSI DAT-NT28 High (Enforced) Level

Profile for ANSSI DAT-NT28 Minimal Level

Profile for ANSSI DAT-NT28 Restrictive Level



**SECURITY POLICY** CENTOS 7 INSTALLATION

Done US Help!

Change content Apply security policy:  ON

Choose profile below:

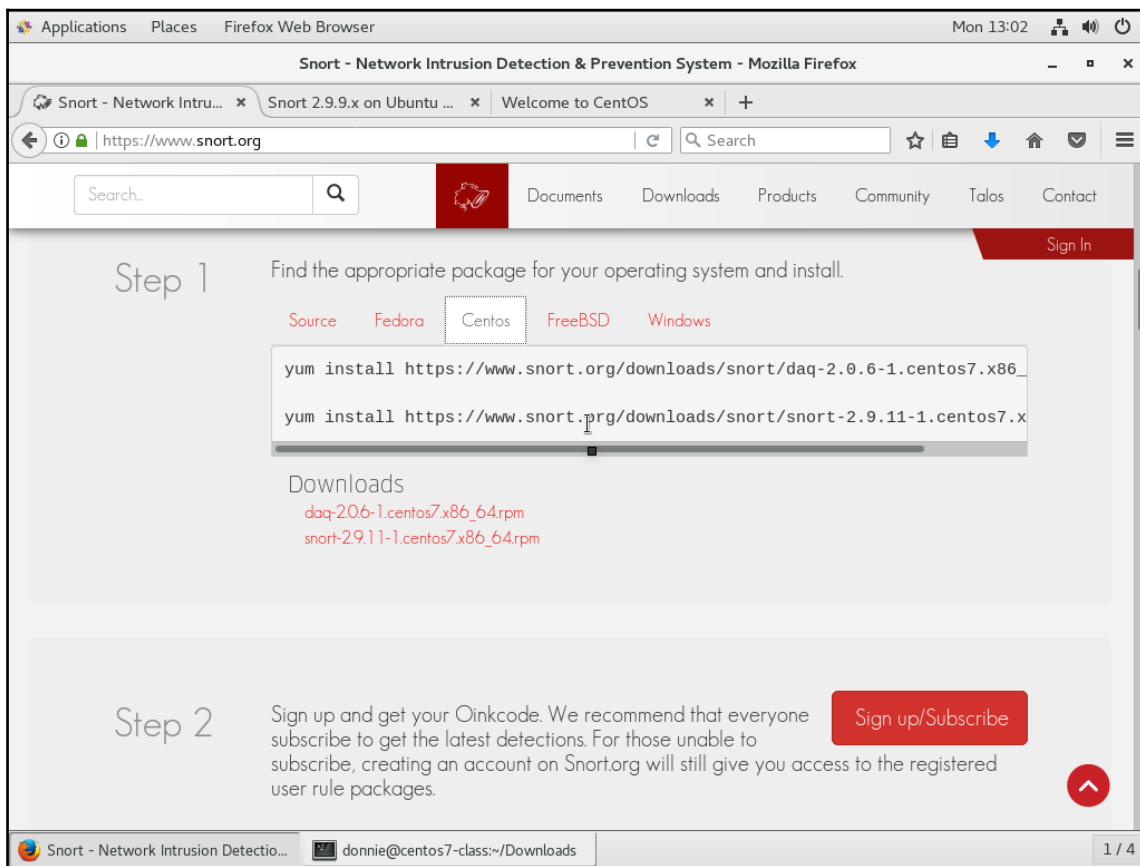
- Default**  
The implicit XCCDF profile. Usually, the default contains no rules.
- Standard System Security Profile**  
This profile contains rules to ensure standard security baseline of CentOS Linux 7 system. Regardless of your system's workload all of these checks should pass.
- PCI-DSS v3 Control Baseline for CentOS Linux 7**  
This is a \*draft\* profile for PCI-DSS v3.
- C2S for CentOS Linux 7**  
This profile demonstrates compliance against the U.S. Government Commercial Cloud Services (C2S) baseline.  
  
This baseline was inspired by the Center for Internet Security (CIS) CentOS Linux 7 Benchmark, v1.1.0 - 04-02-2015. For the SCAP Security Guide project to remain in compliance with CIS' terms and conditions, specifically Restrictions(8), note there is no representation or claim that the C2S profile will ensure a system is in compliance or consistency with the CIS baseline.

Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)

Select profile

Changes that were done or need to be done:  
💡 No profile selected

# Chapter 9: Vulnerability Scanning and Intrusion Detection



The screenshot shows a web browser window with the title "Snort - Network Intrusion Detection & Prevention System - Mozilla Firefox". The address bar shows "https://www.snort.org". The page content includes a search bar, navigation links (Documents, Downloads, Products, Community, Talos, Contact), and a "Sign In" button. The main content area is divided into steps:

**Step 2** Sign up and get your Oinkcode. We recommend that everyone subscribe to get the latest detections. For those unable to subscribe, creating an account on Snort.org will still give you access to the registered user rule packages. [Sign up/Subscribe](#) [Sign In](#)

**Step 3** Stay current with the latest updates using [PulledPork](#)

Community rules [Registered rules](#) [Subscriber rules](#)

```
wget https://www.snort.org/downloads/community/community-rules.tar.gz -O c
```

```
tar -xvfz community.tar.gz -C /etc/snort/rules
```

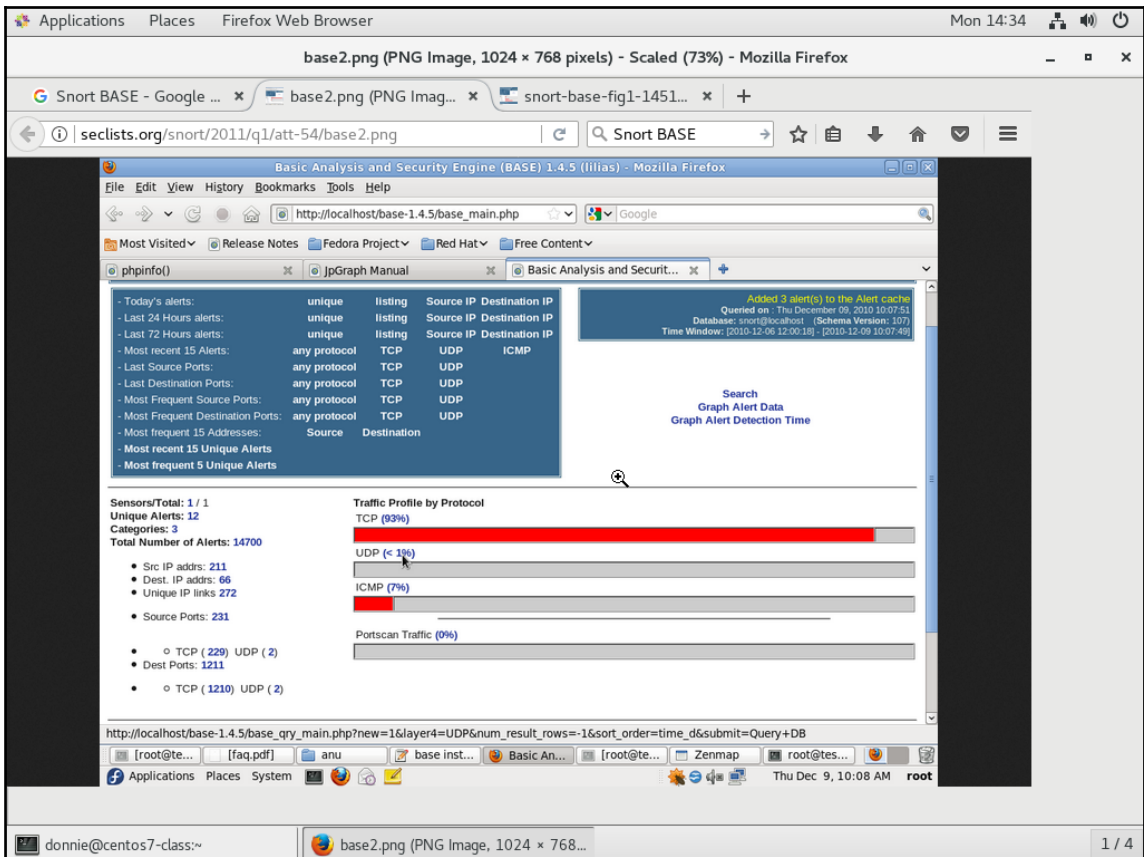
Downloads

- [community-rulestar.gz](#)
- [snort3-community-rulestar.gz](#)

The browser's status bar at the bottom shows the terminal prompt "donnie@centos7-class:~" and the page number "1 / 4".

**Step 4** For more details please reference our install guides on the documents page. [Read Docs](#)







The screenshot shows the IPFire web interface for configuring the Intrusion Detection System (IDS). The page title is "ipfire.localdomain". The navigation menu includes System, Status, Network, Services, Firewall, IPFire, and Logs. The traffic status shows "In 0.00 bit/s" and "Out 0.00 bit/s".

The main content area is titled "Intrusion Detection System". It features a section for "Intrusion Detection System" with two radio buttons: "GREEN Snort" (checked) and "RED Snort". Below this is a "Snort rules update" section with a dropdown menu currently set to "No". The dropdown menu is open, showing the following options: "No", "Emergingthreats.net Community Rules", "Snort/VRT GPLv2 Community Rules" (highlighted), "Sourcefire VRT rules for registered users", and "Sourcefire VRT rules with subscription".

Text on the page indicates that users need to register on [www.snort.org](http://www.snort.org) and provide a link code to activate the rules. A "Save" button is located at the bottom right of the configuration area.

The footer of the page displays "IPFire 2.19 (x86\_64) - Core Update 116" and "IPFire.org • Support the IPFire project with your donation".

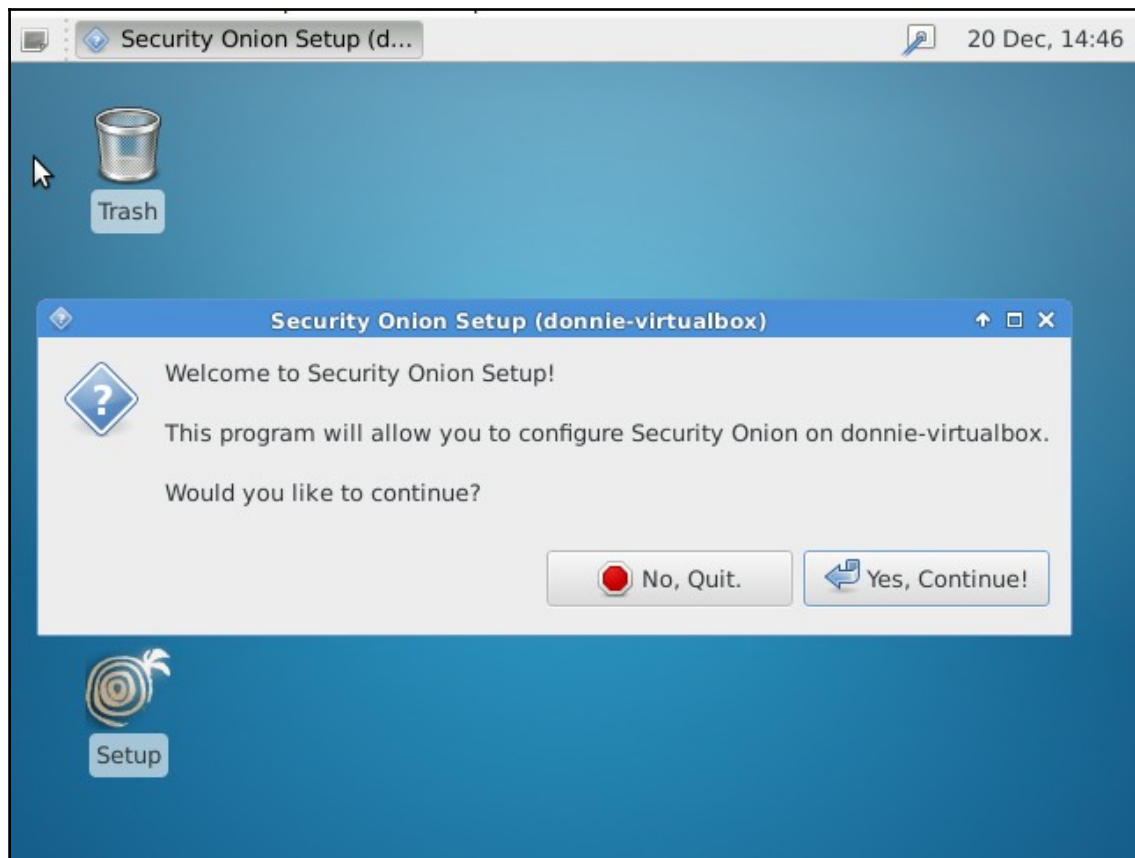
The screenshot shows the IPFire web interface for the "IDS log viewer". The page title is "ipfire.localdomain". The navigation menu includes System, Status, Network, Services, Firewall, IPFire, and Logs. The traffic status shows "In 0.00 bit/s" and "Out 0.00 bit/s".

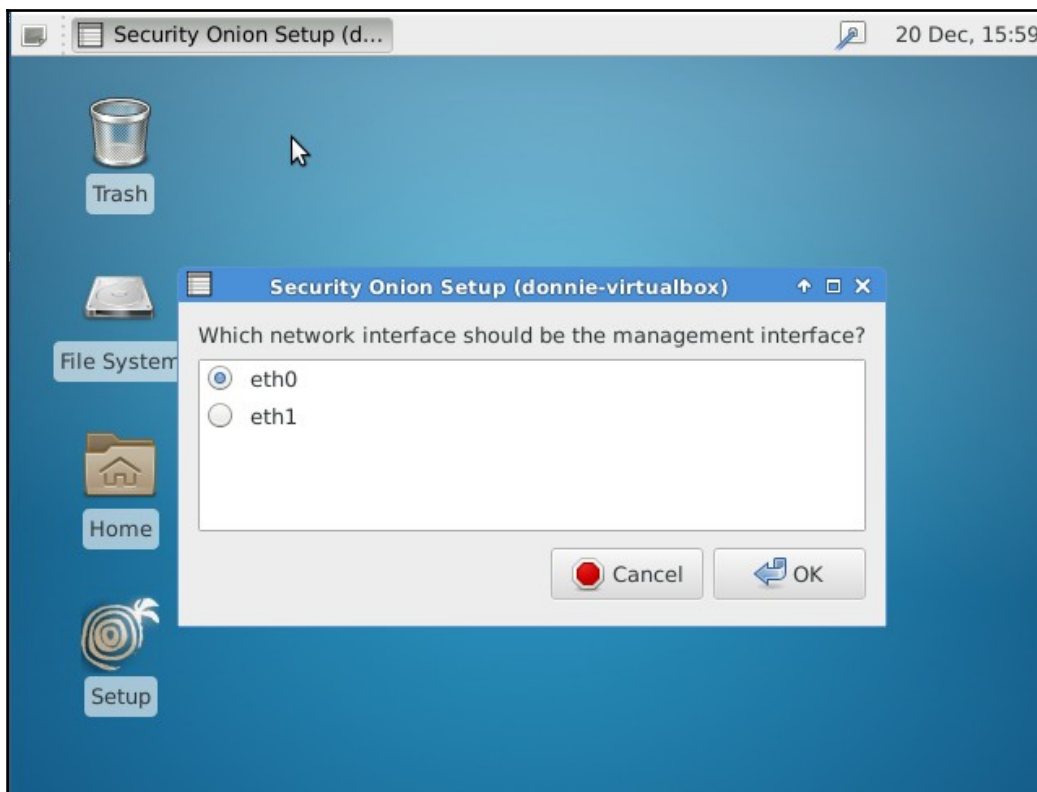
The main content area is titled "IDS log viewer". It features a "Settings:" section with a "Month:" dropdown set to "December" and a "Day:" dropdown set to "20". Below this is a "Log" section with the text "Total of number of Intrusion rules activated for December 20:" and a "Older" link.

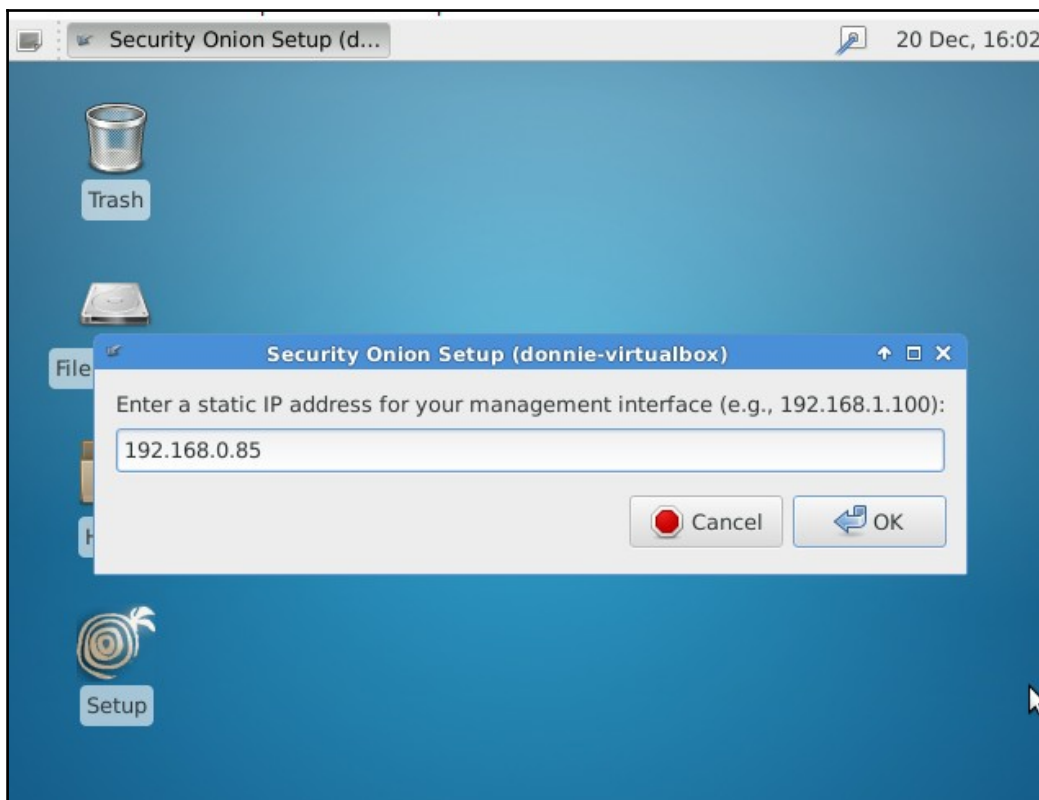
A vertical sidebar on the right side of the page contains a list of log categories: "Log Summary", "Log Settings", "Proxy Logs", "Proxy Reports", "Firewall Logs", "Fw-Loggraphs (IP)", "Fw-Loggraphs (Port)", "Fw-Loggraphs (Country)", "IDS Logs" (highlighted), "URL Filter Logs", and "System Logs".

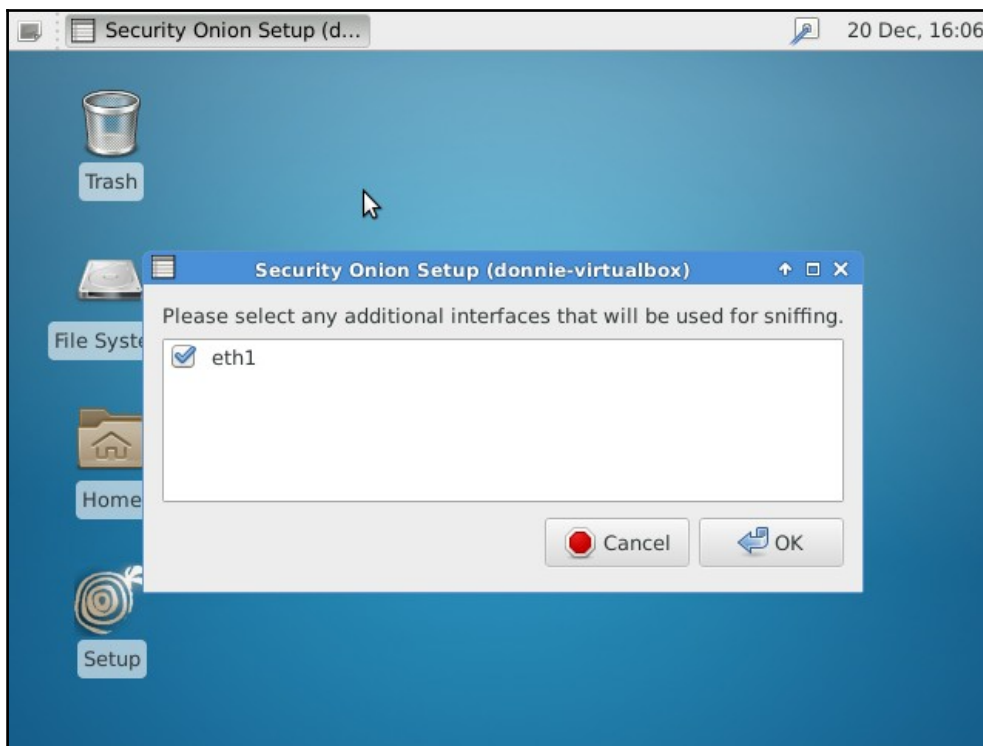
At the bottom of the sidebar, there are navigation buttons: "<<", ">>", "Update", and "Export". The text "Newer" is visible below the sidebar.

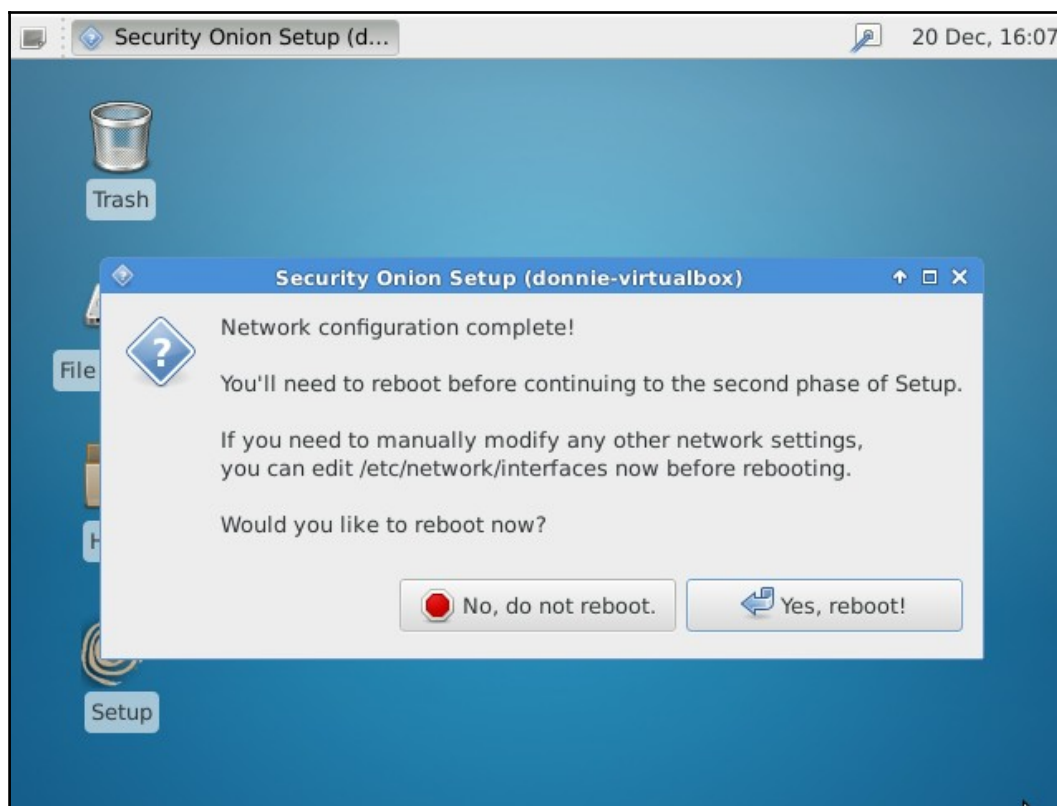
The footer of the page displays "IPFire 2.19 (x86\_64) - Core Update 116" and "IPFire.org • Support the IPFire project with your donation".



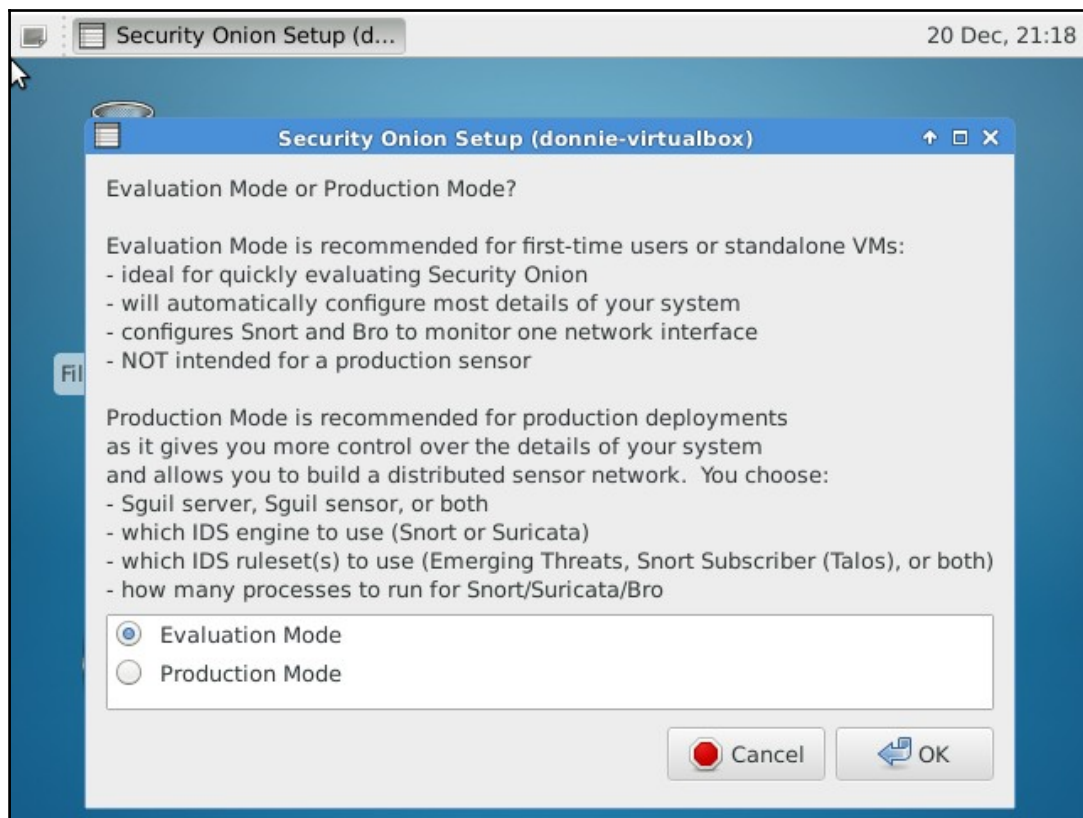








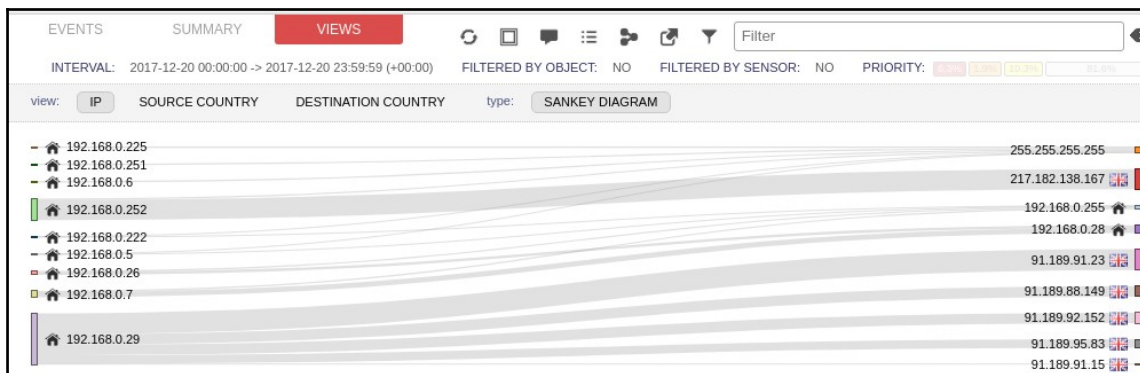




The screenshot shows a web browser window titled "squert (82) - donnie - Chromium" displaying a security dashboard. The dashboard has a navigation bar with "EVENTS", "SUMMARY", and "VIEWS" tabs. Below the navigation bar is a filter input field and a refresh button. A progress bar indicates 28.6% (red) and 71.4% (grey). The main content area shows a table of events with columns for time, description, sensor ID, count, and priority. A sidebar on the left provides filters for priority (high, medium, low, other) and classification (compromised L1, compromised L2). The footer includes "WELCOME donnie | LOGOUT" and "UTC 22:03:20".

Interval	Filtered by Object	Filtered by Sensor	Priority
2017-12-20 00:00:00 -> 2017-12-20 23:59:59 (+00:00)	NO	NO	
21:50:47	ET POLICY Request for Coinhive Browser Monero Miner M2	2024786	6 4.762%
21:50:22	ET POLICY Dropbox DNS Lookup - Possible Offsite File Backup in Use	2020565	17 4.762%
21:49:45	ET POLICY Dropbox Client Broadcasting	2012648	17 19.048%
21:49:38	[OSSEC] Integrity checksum changed.	550	0 54.762%
	[OSSEC] Integrity		

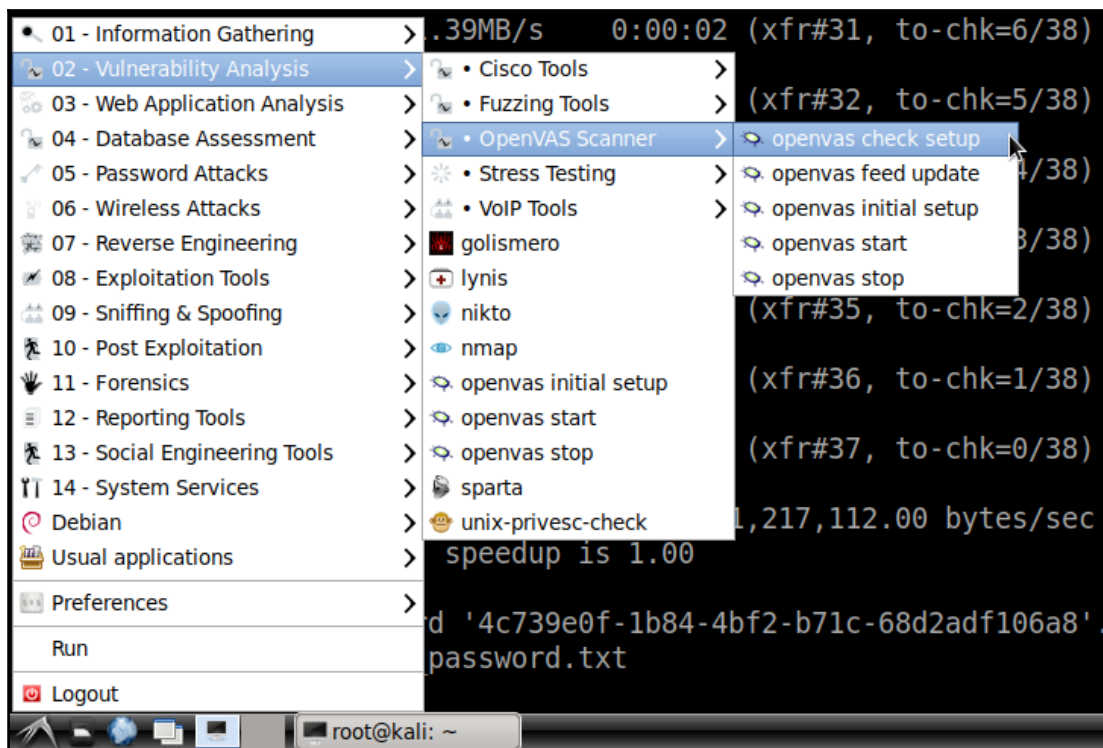
This block shows a detailed view of a security event. At the top, there are summary statistics: 18 (red), 2 (grey), 2 (red), 1 (red), and a grid icon. The event description is "ET POLICY Request for Coinhive Browser Monero Miner M2" with sensor ID 2024786, count 6, and priority 4.762%. Below the description is an alert message: "alert tcp \$EXTERNAL\_NET 443 -> \$HOME\_NET any (msg:'ET POLICY Request for Coinhive Browser Monero Miner M2'; flow:established,from\_server; content:'16']; content:'0b]"; within:8; content:'[0a e1 e6 bd 51 fb 3d 8f 06 be 0d b5 5e bd e9 df]"; within:100; metadata: former\_category POLICY; classtype:policy-violation; sid:2024786; rev:2; metadata:affected\_product Web\_Browsers, attack\_target Client\_Endpoint, deployment Perimeter, signature\_severity Minor, created\_at 2017\_09\_29, updated\_at 2017\_09\_29;)" and a file path "file: downloaded.rules:11411". At the bottom, there are options to "CATEGORIZE 18 EVENT(S)" and "CREATE FILTER: src dst both".

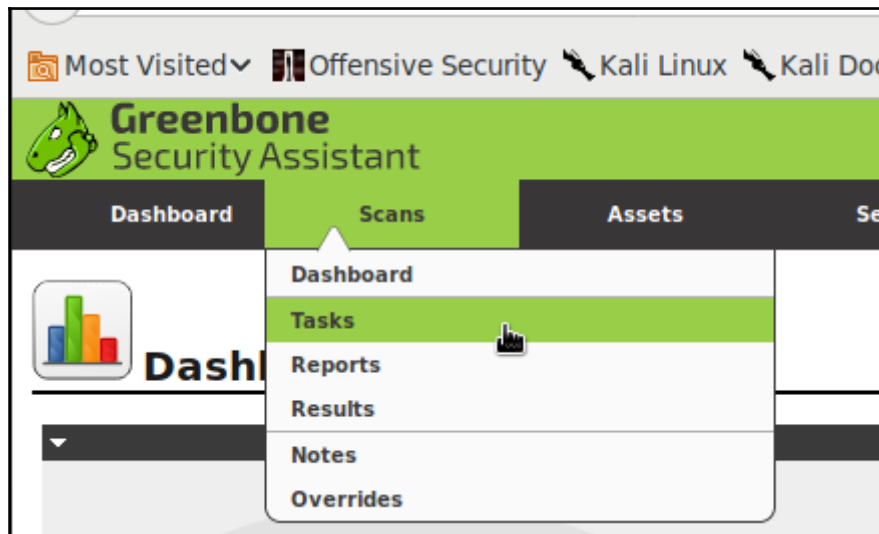
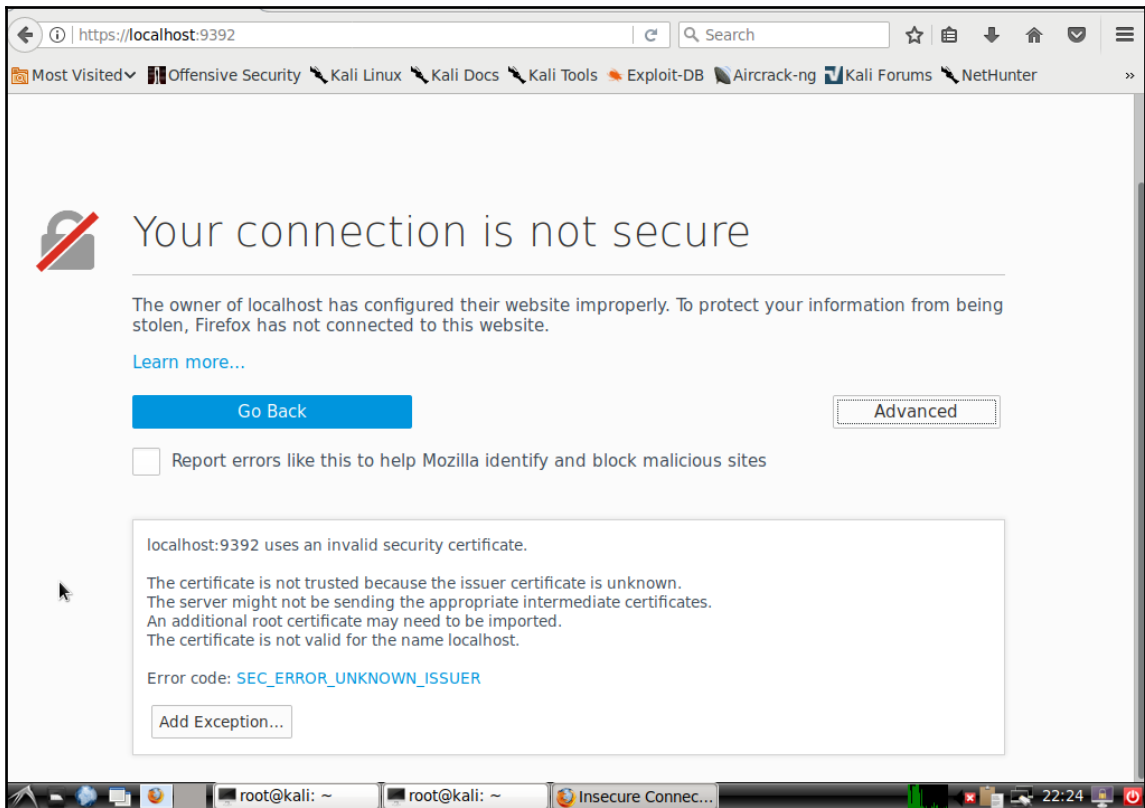


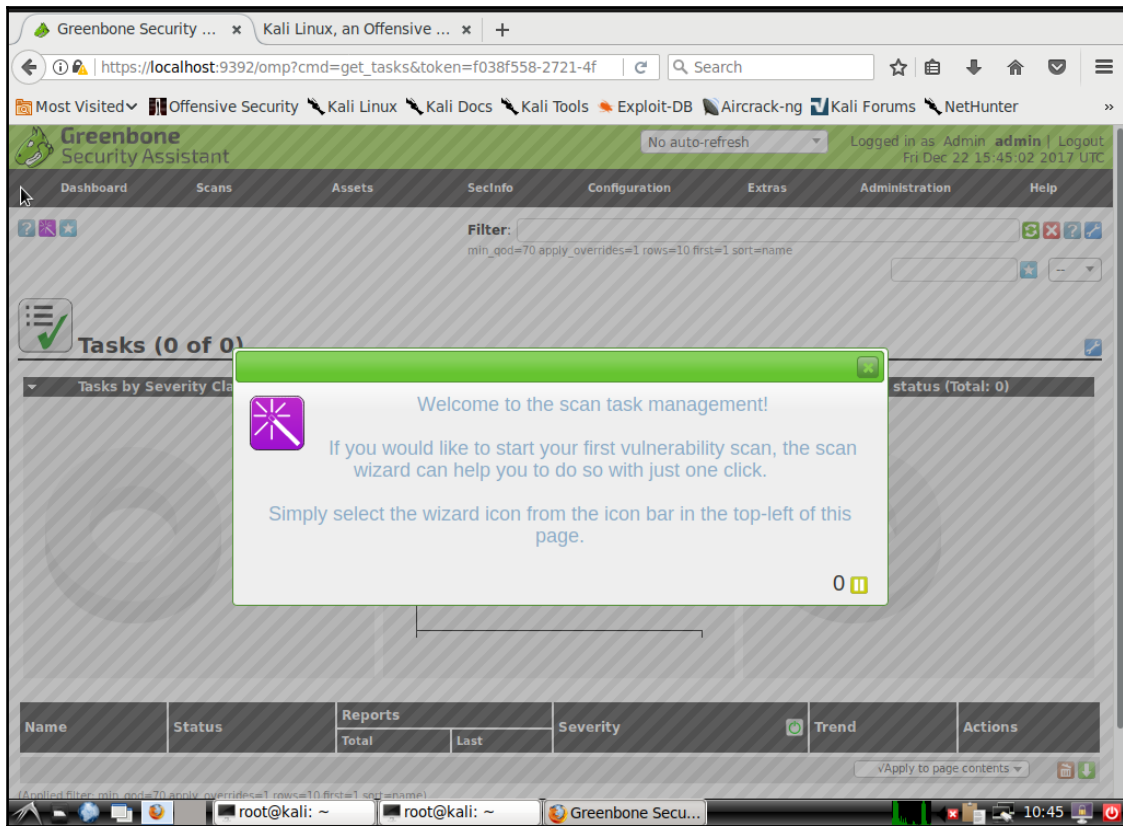
SaaS Basic	SaaS Premium	Self-Hosted
<p><b>\$ 1.5</b> / system / month</p> <p><b>Modules:</b></p> <ul style="list-style-type: none"> <li>✓ Security Auditing</li> <li>✓ Dashboard and Reporting</li> <li>✓ Implementation Plan</li> <li>✓ Hardening Advice</li> </ul> <p><a href="#">Purchase (1 year)</a></p>	<p><b>Full package</b></p> <p><b>\$ 3</b> / system / month</p> <p><b>Modules:</b></p> <ul style="list-style-type: none"> <li>✓ Security Auditing</li> <li>✓ Dashboard and Reporting</li> <li>✓ Implementation Plan</li> <li>✓ Hardening Advice</li> <li>✓ File Integrity Monitoring</li> <li>✓ Intrusion Detection</li> <li>✓ Configuration Management</li> <li>✓ Compliance and Policies</li> <li>✓ Programming Interface (API)</li> </ul> <p><a href="#">Purchase (1 year)</a></p>	<p><i>Tailored to your needs</i></p> <p><b>Customization options:</b></p> <ul style="list-style-type: none"> <li>More than 100 systems?</li> <li>Prefer the <a href="#">self-hosted version</a>?</li> <li>Managed service provider?</li> <li>Performing 3rd party audits?</li> </ul> <p><a href="#">Receive Custom Quote</a></p>

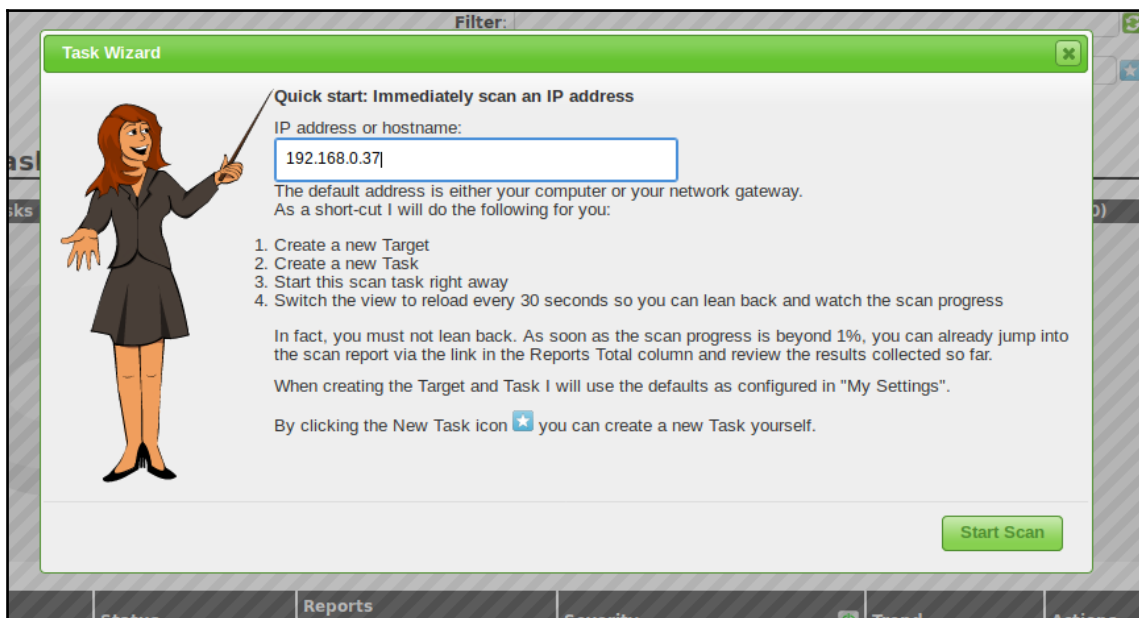
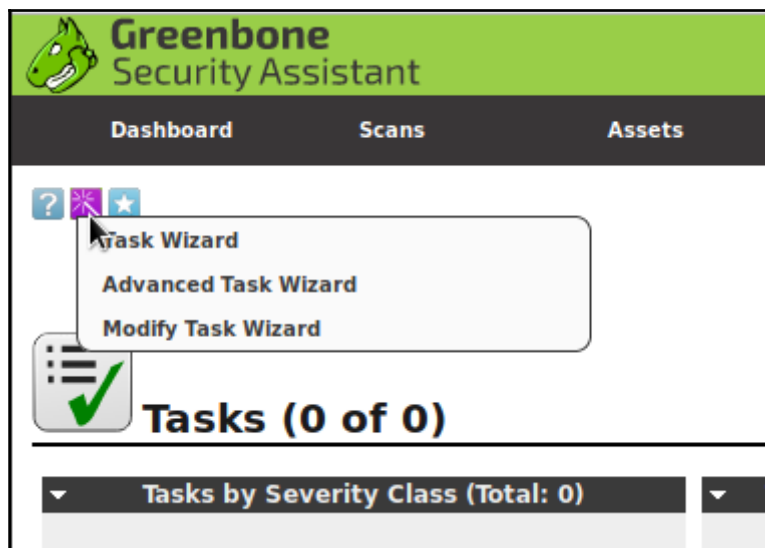
Kali 64 bit LXDE	HTTP   Torrent	2.7G	2017.3	4dd54f9aeecebec612af3dab581485415d817ddd6db251c9c880ff2d14657497e
------------------	-------------------	------	--------	---

```
sent 757 bytes received 46,858,055 bytes 1,217,112.00 bytes/sec
total size is 46,844,168 speedup is 1.00
/usr/sbin/opensvamd
User created with password '4c739e0f-1b84-4bf2-b71c-68d2adf106a8'.
root@kali:~#
```









Greenbone Security Assistant - Mozilla Firefox

Greenbone Security ... x Kali Linux, an Offensive ... x +

https://localhost:9392/omp?cmd=get\_tasks&token=f038f558-2721-4f

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

### Tasks (1 of 1)

Tasks by Severity Class (Total: 1)

■ N/A

1

Tasks with most High results per host

No Tasks with High severity found

Tasks by status (Total: 1)

■ Running

1

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
<a href="#">Immediate scan of IP 192.168.0.37</a>	1 %	0	(1)			

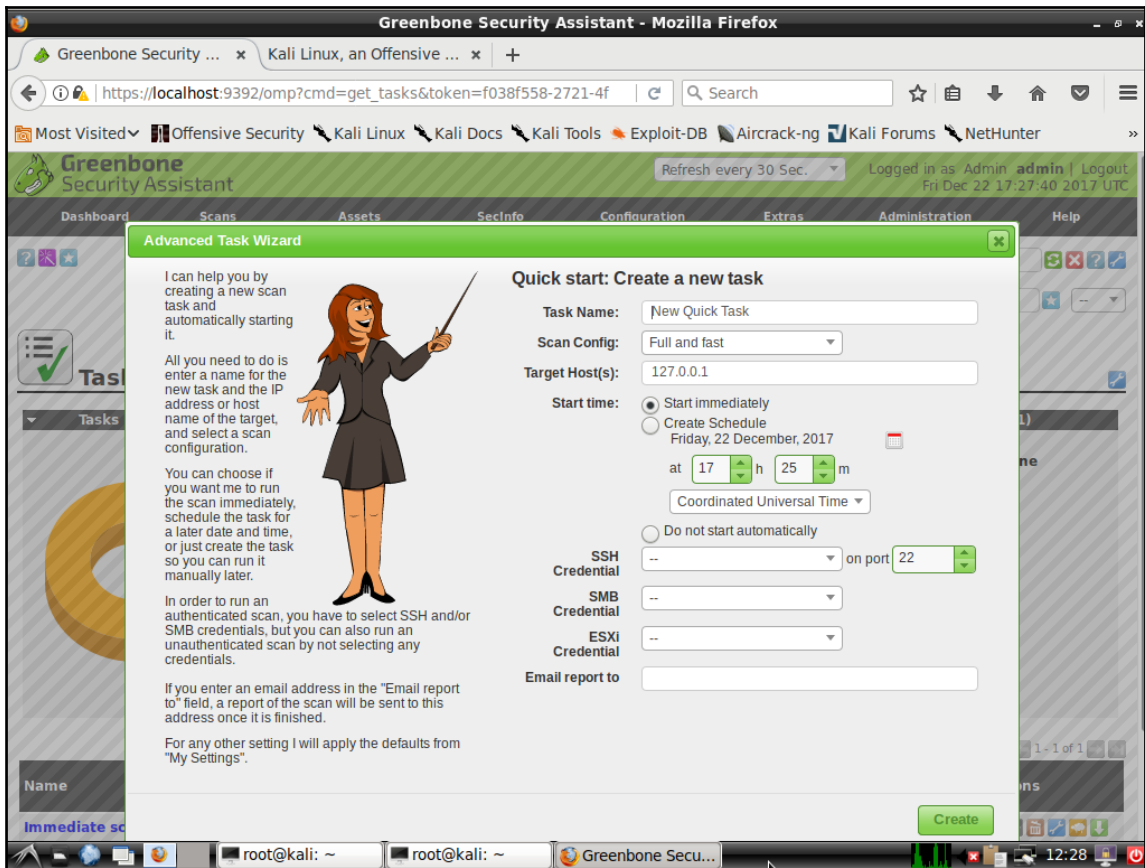
(Applied filter: min\_qod=70 apply\_overrides=1 rows=10 first=1 sort=name)

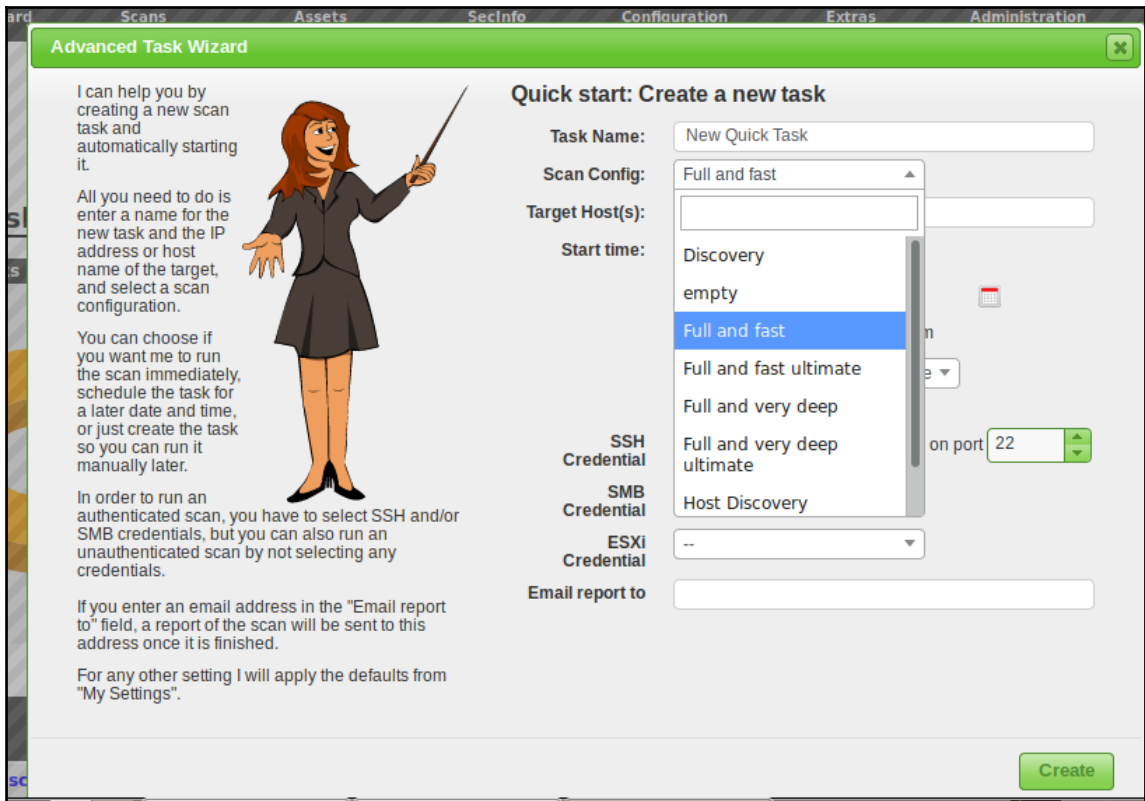
Backend operation: 0.12s

Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

root@kali: ~ root@kali: ~ Greenbone Secu... 10:49







Greenbone Security Assistant - Mozilla Firefox

Greenbone Security ... x Kali Linux, an Offensive ... x +

https://localhost:9392/omp?cmd=get\_reports&replace\_task\_id=1&filt

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

### Reports (1 of 2)

Reports by Severity Class (Total: 1)

High

Reports: High results timeline

Reports by CVSS (Total: 1)

Date	Status	Task	Severity	Scan Results	Actions
Fri Dec 22 17:29:22 2017	Done	New Quick Task	7.5 (High)	High: 1, Medium: 1, Low: 1, Log: 18, False Pos.: 0	[Log] [False Pos.] [X]

(Applied filter: task\_id=d23f4e16-4acd-43e0-9714-e6ac159dfe03 apply\_overrides=1 min\_qod=70 sort-reverse=date first=1 rows=10)

Backend operation: 0.34s Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

Vulnerability	Severity	QoD	Host	Location	Created
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95%	192.168.0.37	22/tcp	Fri Dec 22 17:42:07 2017
OS Detection Consolidation and Reporting	0.0 (Log)	80%	192.168.0.37	general/tcp	Fri Dec 22 17:39:56 2017
CGI Scanning Consolidation	0.0 (Log)	80%	192.168.0.37	631/tcp	Fri Dec 22 17:39:53 2017
HTTP Security Headers Detection	0.0 (Log)	80%	192.168.0.37	631/tcp	Fri Dec 22 17:42:17 2017
NIPrint LPD-LPR Print Server	7.5 (High)	99%	192.168.0.37	515/tcp	Fri Dec 22 17:47:35 2017
Service Detection with 'GET' Request	0.0 (Log)	80%	192.168.0.37	5900/tcp	Fri Dec 22 17:39:33 2017
VNC security types	0.0 (Log)	95%	192.168.0.37	5900/tcp	Fri Dec 22 17:42:06 2017
Traceroute	0.0 (Log)	80%	192.168.0.37	general/tcp	Fri Dec 22 17:39:01 2017
Service Detection with nmap	0.0 (Log)	80%	192.168.0.37	515/tcp	Fri Dec 22 17:44:32 2017
CPE Inventory	0.0 (Log)	80%	192.168.0.37	general/CPE-T	Fri Dec 22 17:50:51 2017

(Applied filter: first=11 rows=10 apply\_overrides=0 min\_qod=70 severity>Error and task\_id=d23f4e16-4acd-43e0-9714-e6ac159dfe03 sort=nvt)

The screenshot shows the Greenbone Security Assistant web interface in a Mozilla Firefox browser. The page displays a vulnerability report for 'NIPrint LPD-LPR Print Server'. The interface includes a navigation menu at the top with options like Dashboard, Scans, Assets, Secinfo, Configuration, Extras, Administration, and Help. The main content area shows the following details:

- Result: NIPrint LPD-LPR Print Server**
- ID:** d584b0e4-d5a6-4642-91fc-909c0a794210
- Created:** Fri Dec 22 17:47:35 2017
- Modified:** Fri Dec 22 17:47:35 2017
- Owner:** admin

Vulnerability	Severity	QoD	Host	Location	Actions
NIPrint LPD-LPR Print Server	7.5 (High)	99%	192.168.0.37	515/tcp	

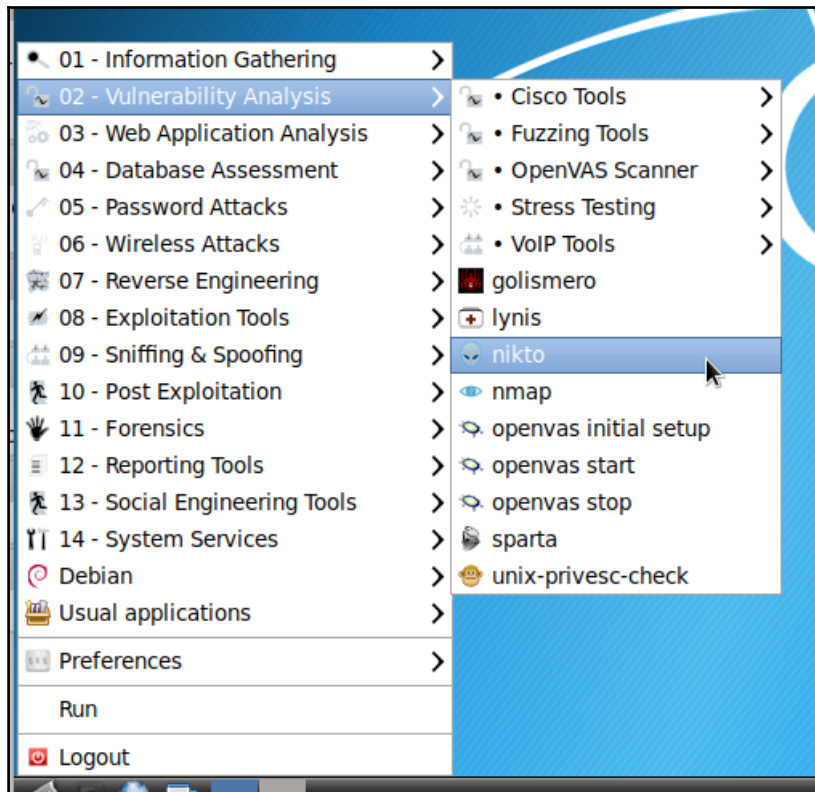
**Summary**  
A vulnerability in the NIPrint could allow an attacker to remotely overflow an internal buffer which could allow code execution.

**Vulnerability Detection Result**  
Vulnerability was detected according to the Vulnerability Detection Method.

**Solution**  
None, Contact the vendor <http://www.networkinstruments.com/products/niprint.html>

**Vulnerability Detection Method**  
Details: [NIPrint LPD-LPR Print Server \(OID: 1.3.6.1.4.1.25623.1.0.11926\)](#)  
Version used: \$Revision: 6053 \$

**References**  
CVE: [CVE-2003-1141](#)  
BID: 8968  
Other: OSVDB:2774



```
root@kali: ~  
File Edit Tabs Help  
-Format+      save file (-o) format  
-Help         Extended help information  
-host+        target host  
-id+          Host authentication to use, format is id:pass or id:p  
ass:realm  
-list-plugins List all available plugins  
-output+      Write output to this file  
-nossl        Disables using SSL  
-no404        Disables 404 checks  
-Plugins+     List of plugins to run (default: ALL)  
-port+        Port to use (default 80)  
-root+        Prepend root value to all requests, format is /direct  
ory  
-ssl          Force ssl mode on port  
-Tuning+     Scan tuning  
-timeout+    Timeout for requests (default 10 seconds)  
-update      Update databases and plugins from CIRT.net  
-Version     Print plugin and database versions  
-vhost+     Virtual host (for Host header)  
            + requires a value  
  
Note: This is the short help output. Use -H for full help text.  
root@kali:~#
```

# Chapter 10: Security Tips and Tricks for the Busy Bee

**WhatPortIs** [Browse Ports](#) [Submit New Port](#) [Statistics](#) [Blog](#)

## 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 <b>902</b>	<b>UDP</b>	ideafarm-door
Port <b>902</b>	<b>TCP</b>	ideafarm-door 902/tcp self documenting Door: send 0x...
Port <b>902</b>	<b>TCP</b>	VMware Server Console (TCP from management console t...
Port <b>902</b>	<b>UDP</b>	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-root ro crashkernel=auto rd.lvm.lv=centos/root rd.luks.uuid=luks-2d7f02c7-864f-42ce-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 2.02~beta2-36ubuntu3.14

*Ubuntu
Advanced options for Ubuntu

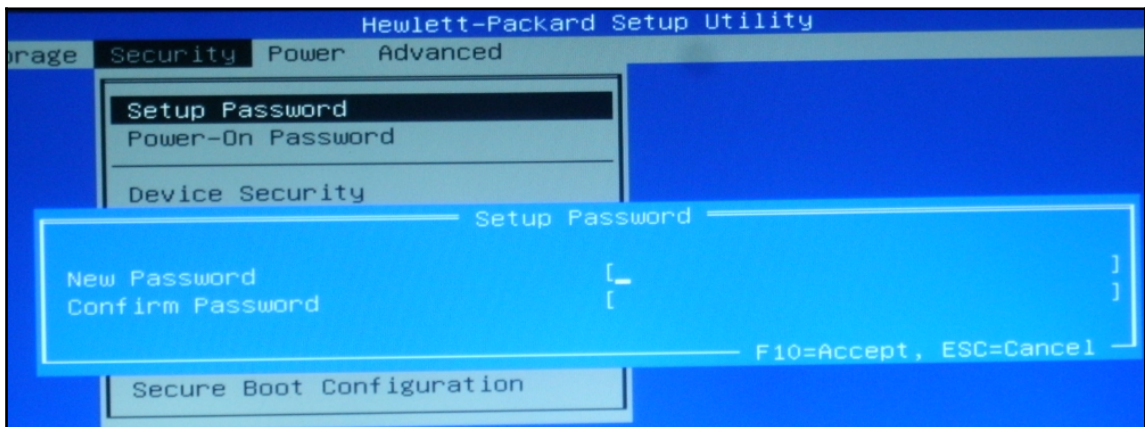
Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line.
```

```
linux /vmlinuz-4.4.0-104-generic root=/dev/mapper/ubuntu3\
--vg-root ro _
linux /vmlinuz-4.4.0-104-generic root=/dev/mapper/ubuntu3\
-vg-root rw init=/bin/bash_
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/# _
```

```
Enter username:
root
Enter password:
_
```

```
Enter username:  
donnie  
Enter password:  
_
```





The screenshot shows a Mozilla Firefox browser window displaying a Confluence page. The browser's address bar shows the URL `https://wikis.utexas.edu/display/`. The page title is "Red Hat Enterprise Linux 7 Hardening Checklist - ISO - Information Security Office - UT Austin Wikis - Mozilla Firefox".

The page content includes the following elements:

- Header:** "Information Security Office" with the motto "SECURUS // VIGILARE // INSANUS".
- Breadcrumbs:** "ISO - Information Security Office / Operating System Hardening Checklists".
- Section Title:** "Red Hat Enterprise Linux 7 Hardening Checklist".
- Metadata:** "Created by Jason M Ragland, last modified on Jun 23, 2015".
- Text:** "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."
- Section: 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.
- Section: How to read the checklist**

At the bottom of the page, it says "Powered by Atlassian Confluence 5.10.8 · Report a bug · Atlassian News" and "Confluence Documentation | Web Privacy Policy | Web Accessibility". The browser's taskbar at the bottom shows "Red Hat Enterprise Linux 7 Hardenin..." and a page indicator "1 / 4".

