



Enumerating Hosts Using Wireshark, Windows, and Linux Commands

ETHICAL HACKING & Lab # 2

Student Info

Name: SRIJA PABBA

Student ID: 00866719

Email:

spabb6@unh.newhaven.edu

Table of Contents

I.	Executive Summary	2
	Highlights	
	Objectives	
II.	Lab Description Details	2
	Include Steps Taken, Notes, & Screen Shots demonstrating completion of lab objectives	
III.	Supporting Evidence.....	12
IV.	Conclusion & Wrap-Up	14
	Summary with observations, Success & Failures, Challenges	

Executive Summary

Highlights

In this lab, I explored system enumeration using various tools, including command line utilities like db_nmap, net, nbtstat, and ifconfig, as well as GUI tools like Wireshark and Armitage. I learned about active scanning techniques that are detectable on the network, alongside passive scanning methods that allow for stealthy data collection. This hands-on experience enhanced my skills in identifying network services and vulnerabilities, providing me with a comprehensive understanding of effective network analysis and security assessment.

Objectives

The objective of this lab is to explore system enumeration techniques using command line and GUI tools on Linux and Windows. I aim to identify network services and vulnerabilities through tools like db_nmap, net, nbtstat, ifconfig, Wireshark, and Armitage. Additionally, I will differentiate between active scanning, which is detectable, and passive scanning, which allows for stealthy data collection, to enhance my understanding of network analysis and security.

Lab Description Details

Ifconfig

Ifconfig > ip1.txt

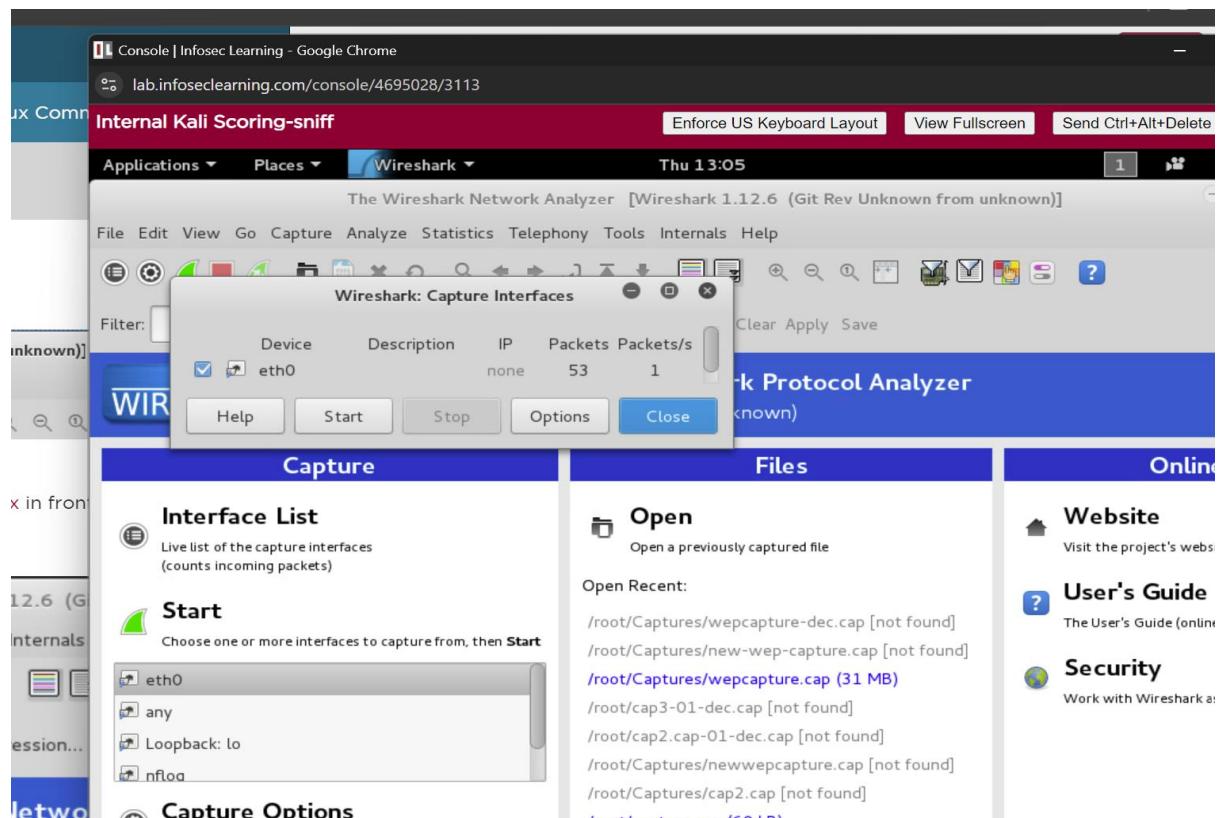
The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the output of the 'ifconfig' command being redirected to a file named 'ip1.txt'. The file content is then viewed using the 'cat' command. The terminal window title is 'Internal Kali Scoring-sniff' and the prompt is 'root@kali2:~#'. The desktop background shows a dark theme with icons for various applications like terminal, file manager, and browser.

```
root@kali2:~# ifconfig > ip1.txt
root@kali2:~# cat ip1.txt
root@kali2:~#
```

The terminal output shows the configuration for several interfaces:

- 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:22 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1358 (1.3 KiB) TX bytes:1358 (1.3 KiB)
- eth0**: Link encap:Ethernet HWaddr 00:50:56:8e:e9:ae
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::250:56ff:fe8e:e9ae/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:405 errors:0 dropped:11 overruns:0 frame:0
TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:38756 (37.8 KiB) TX bytes:13281 (12.9 KiB)
- eth1**: 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:34 errors:0 dropped:0 overruns:0 frame:0
TX packets:34 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:2152 (2.1 KiB) TX bytes:2152 (2.1 KiB)

Interface window in Wireshark



Packets appearing list

No.	Time	Source	Destination	Protocol	Length	Info
29	5.624982000	192.168.1.20	192.168.1.10	DNS	84	Standard query 0x6204 A sls.update.microsoft
30	5.732213000	192.168.1.10	128.9.0.107	DNS	84	Standard query 0xa51f A sls.update.microsoft
31	5.732425000	192.168.1.10	192.33.4.12	DNS	84	Standard query 0xa51f A sls.update.microsoft
32	5.773508000	192.168.1.10	192.112.36.4	DNS	81	Standard query 0x4094 A update.googleapis.co
33	6.240435000	ac:7a:56:49:bf:bb	PVST+	STP	64	RST. Root = 32768/1528/ac:7a:56:49:bf:80 Cos
34	6.573899000	Vmware_0e:7b:1a	Broadcast	ARP	60	Who has 203.0.113.254? Tell 203.0.113.100
35	6.683778000	Vmware_02:47:c0	Vmware_8e:f7:8a	ARP	60	Who has 192.168.1.254? Tell 192.168.1.10
36	6.683815000	Vmware_0e:f7:8a	Vmware_02:47:c0	ARP	60	192.168.1.254 is at 00:50:56:8e:f7:8a
37	6.746430000	192.168.1.10	128.9.0.107	DNS	93	Standard query 0x93c8 A v10.vortex-win.data.
38	6.746538000	192.168.1.10	192.33.4.12	DNS	93	Standard query 0x93c8 A v10.vortex-win.data.
39	7.000017000	192.168.1.20	192.168.1.10	DNS	93	Standard query 0xb7c A v10.vortex-win.data.

Frame 29: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
Ethernet II, Src: Vmware_02:47:be (00:50:56:02:47:be), Dst: Vmware_02:47:c0 (00:50:56:02:47:c0)
Internet Protocol Version 4, Src: 192.168.1.20 (192.168.1.20), Dst: 192.168.1.10 (192.168.1.10)
User Datagram Protocol, Src Port: 58042 (58042), Dst Port: 53 (53)
Domain Name System (query)

net view

Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/4695028/3115
Internal Windows 10 Scoring-sniff Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete
Administrator: cmd - Shortcut
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.
C:\windows\system32>net view
Server Name Remark

\\CONCORD
\\METASPOITABLE metasploitable server (samba 3.0.20-debian)
The command completed successfully.
C:\windows\system32>_

Net view /domain

Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/4695028/3115
Internal Windows 10 Scoring-sniff Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete F
Administrator: cmd - Shortcut
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.
C:\windows\system32>net view
Server Name Remark

\\CONCORD
\\METASPOITABLE metasploitable server (samba 3.0.20-debian)
The command completed successfully.
C:\windows\system32>net view /domain
Domain

CAMPUS
WORKGROUP
The command completed successfully.
C:\windows\system32>_

Net view /domain:campus

lab.infoseclearning.com/console/4695028/3115
Internal Windows 10 Scoring-sniff Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete
Administrator: cmd - Shortcut WORKGROUP The command completed successfully.
C:\windows\System32>netview /domain:campus 'netview' is not recognized as an internal or external command,
operable program or batch file.
C:\windows\System32>net view /domain:campus Server Name Remark

\\SERVER
The command completed successfully.
C:\windows\System32>

Net view /domain:workgroup

C:\windows\System32>net view /domain:workgroup Server Name Remark

\\CONCORD
\\METASPLOITABLE metasploitable server (Samba 3.0.20-Debian)
The command completed successfully.
C:\windows\System32>

Net view \\server

```
C:\windows\System32>net view \\server
Shared resources at \\server

share name  Type  Used as  Comment

-----
NETLOGON    Disk      Logon server share
share        Disk
SYSVOL      Disk      Logon server share
The command completed successfully.
```

Net view \\metasploitable

```
Administrator: cmd - Shortcut
Enforce US Keyboard Layout  View Fullscreen  Send Ctrl+Alt+De

C:\Windows\Scoring-sniff>
MAC Address = 00-50-56-02-47-C0

C:\Windows\System32>nbtstat -a METASPLOITABLE
Ethernet0:
Node IpAddress: [192.168.1.20] scope Id: []
          NetBIOS Remote Machine Name Table

          Name        Type      Status
-----
METASPLOITABLE <00>  UNIQUE   Registered
METASPLOITABLE <03>  UNIQUE   Registered
METASPLOITABLE <20>  UNIQUE   Registered
@@__MSBROWSE__@<01> GROUP    Registered
WORKGROUP     <00>  GROUP    Registered
WORKGROUP     <1D>  UNIQUE   Registered
WORKGROUP     <1E>  GROUP    Registered

MAC Address = 00-00-00-00-00-00
```

```
nbstat -a server
```

Internal Windows 10 Scoring-sniff

Administrator: cmd - Shortcut

```
flag5      Disk          flag5:571444
flag6      Disk          flag6:333459
share      Disk
The command completed successfully.

C:\Windows\System32>nbtstat -a server

Ethernet0:
NodeIpAddress: [192.168.1.20] scope Id: []

      NetBIOS Remote Machine Name Table

      Name           Type        Status
-----  
 SERVER         <00>    UNIQUE    Registered
 CAMPUS         <00>    GROUP     Registered
 CAMPUS         <1C>    GROUP     Registered
 SERVER         <20>    UNIQUE    Registered
 CAMPUS         <1E>    GROUP     Registered
 CAMPUS         <1B>    UNIQUE    Registered
 CAMPUS         <1D>    UNIQUE    Registered
 @@_MSBROWSE_@<01> GROUP     Registered

MAC Address = 00-50-56-02-47-C0
```

Nbstat -a METASPLOITABLE

```
 SERVER         <20>    UNIQUE    Registered
 CAMPUS         <1E>    GROUP     Registered
 CAMPUS         <1B>    UNIQUE    Registered
 CAMPUS         <1D>    UNIQUE    Registered
 @@_MSBROWSE_@<01> GROUP     Registered

MAC Address = 00-50-56-02-47-C0

C:\Windows\System32>nbtstat -a METASPLOITABLE

Ethernet0:
NodeIpAddress: [192.168.1.20] Scope Id: []

      NetBIOS Remote Machine Name Table

      Name           Type        Status
-----  
 METASPLOITABLE <00>    UNIQUE    Registered
 METASPLOITABLE <03>    UNIQUE    Registered
 METASPLOITABLE <20>    UNIQUE    Registered
 WORKGROUP       <00>    GROUP     Registered
 WORKGROUP       <1E>    GROUP     Registered

MAC Address = 00-00-00-00-00-00
```

Service postgresql start

msfconsole

The terminal window is titled "internal Kali Scoring-sniff". The command history shows:

```
root@kali2:~# service postgresql start
root@kali2:~# cd armitage
root@kali2:~/armitage# msfconsole
```

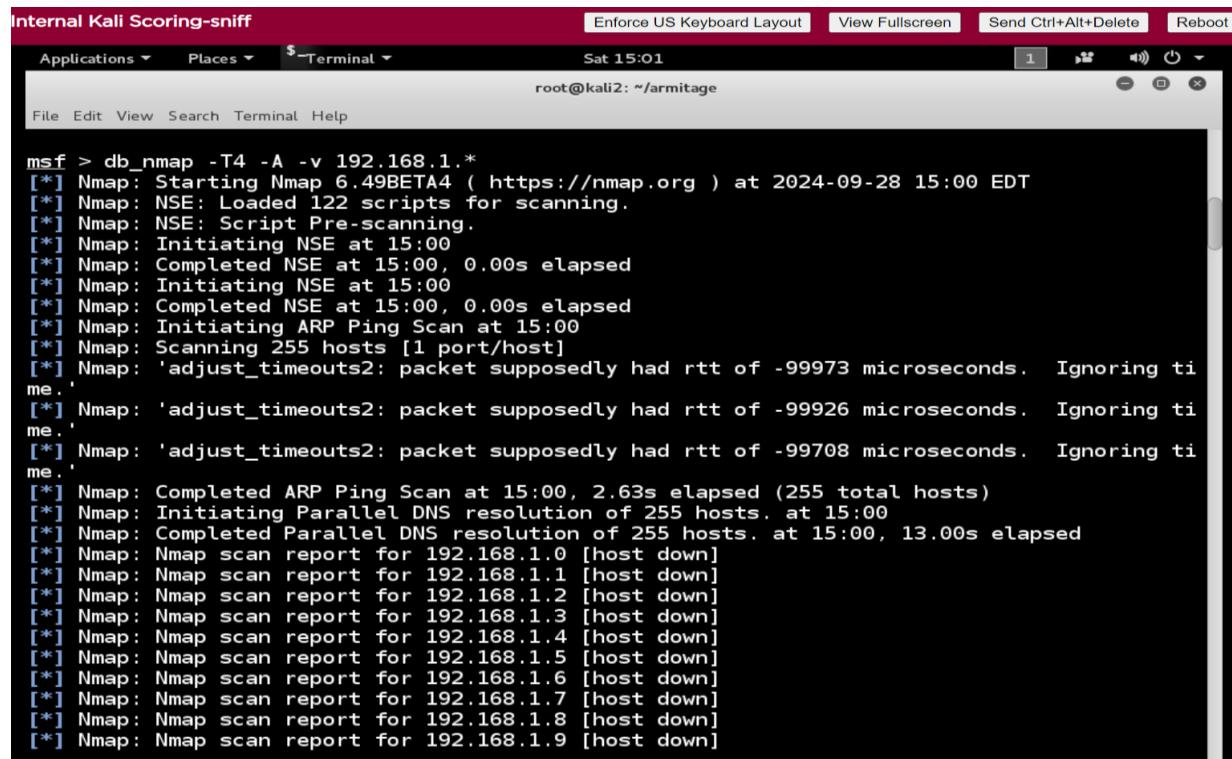
The terminal then displays a series of ASCII characters forming the text:

```
wake up, Neo...
the matrix has you
follow the white rabbit.

knock, knock, Neo.
```

Below this text is a large, stylized ASCII representation of the Matrix code, consisting of various symbols like parentheses, slashes, and underscores. At the bottom of the terminal window, the URL <http://metasploit.pro> is visible.

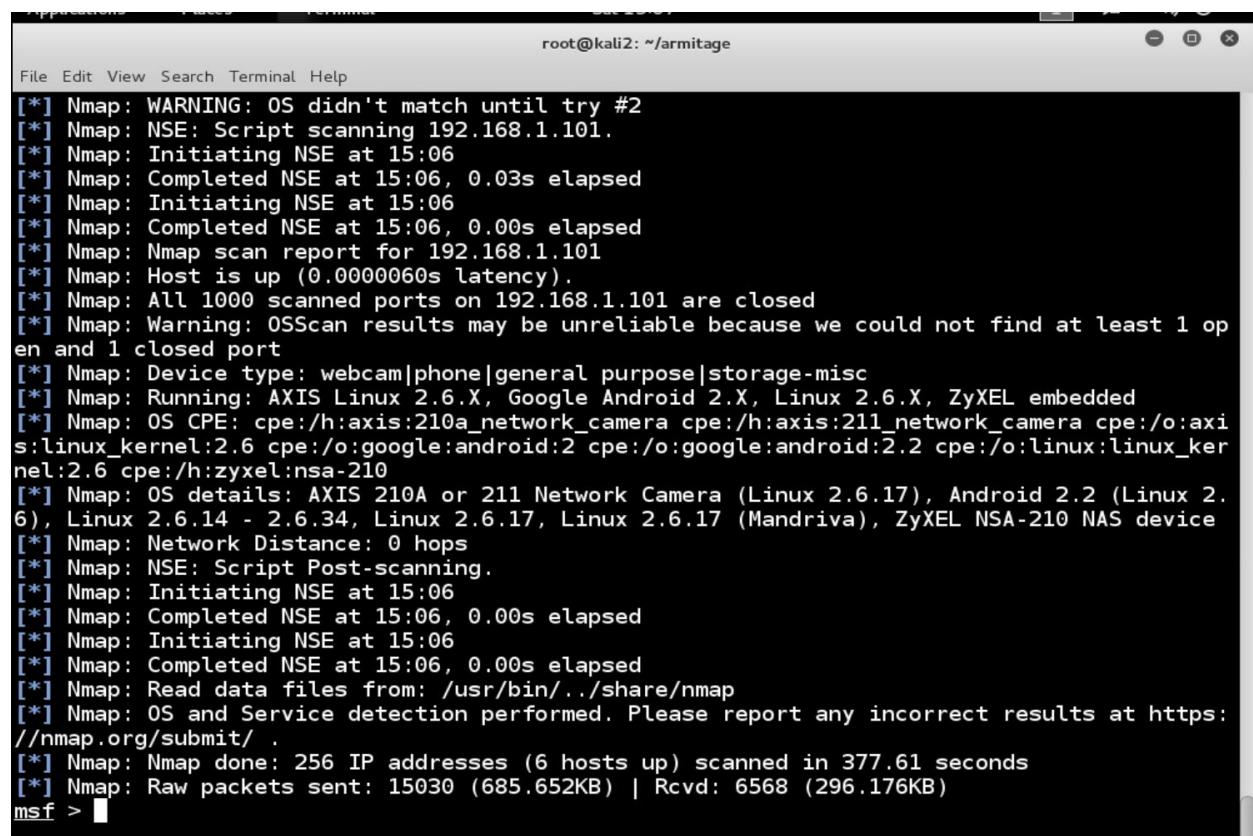
Db_nmap -T4 -A -v 192.168.1.*



The screenshot shows a terminal window titled "Internal Kali Scoring-sniff" with a red header bar. The window title bar includes "Enforce US Keyboard Layout", "View Fullscreen", "Send Ctrl+Alt+Delete", and "Reboot". The terminal window itself has a dark background and displays the following nmap command and its output:

```
msf > db_nmap -T4 -A -v 192.168.1.*  
[*] Nmap: Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2024-09-28 15:00 EDT  
[*] Nmap: NSE: Loaded 122 scripts for scanning.  
[*] Nmap: NSE: Script Pre-scanning.  
[*] Nmap: Initiating NSE at 15:00  
[*] Nmap: Completed NSE at 15:00, 0.00s elapsed  
[*] Nmap: Initiating NSE at 15:00  
[*] Nmap: Completed NSE at 15:00, 0.00s elapsed  
[*] Nmap: Initiating ARP Ping Scan at 15:00  
[*] Nmap: Scanning 255 hosts [1 port/host]  
[*] Nmap: 'adjust_timeouts2: packet supposedly had rtt of -99973 microseconds. Ignoring time.'  
[*] Nmap: 'adjust_timeouts2: packet supposedly had rtt of -99926 microseconds. Ignoring time.'  
[*] Nmap: 'adjust_timeouts2: packet supposedly had rtt of -99708 microseconds. Ignoring time.'  
[*] Nmap: Completed ARP Ping Scan at 15:00, 2.63s elapsed (255 total hosts)  
[*] Nmap: Initiating Parallel DNS resolution of 255 hosts. at 15:00  
[*] Nmap: Completed Parallel DNS resolution of 255 hosts. at 15:00, 13.00s elapsed  
[*] Nmap: Nmap scan report for 192.168.1.0 [host down]  
[*] Nmap: Nmap scan report for 192.168.1.1 [host down]  
[*] Nmap: Nmap scan report for 192.168.1.2 [host down]  
[*] Nmap: Nmap scan report for 192.168.1.3 [host down]  
[*] Nmap: Nmap scan report for 192.168.1.4 [host down]  
[*] Nmap: Nmap scan report for 192.168.1.5 [host down]  
[*] Nmap: Nmap scan report for 192.168.1.6 [host down]  
[*] Nmap: Nmap scan report for 192.168.1.7 [host down]  
[*] Nmap: Nmap scan report for 192.168.1.8 [host down]  
[*] Nmap: Nmap scan report for 192.168.1.9 [host down]
```

The time of Scan and no .of hosts up are displayed



The screenshot shows a terminal window titled "Internal Kali Scoring-sniff" with a red header bar. The terminal window displays the following nmap command and its output:

```
[*] Nmap: WARNING: OS didn't match until try #2  
[*] Nmap: NSE: Script scanning 192.168.1.101.  
[*] Nmap: Initiating NSE at 15:06  
[*] Nmap: Completed NSE at 15:06, 0.03s elapsed  
[*] Nmap: Initiating NSE at 15:06  
[*] Nmap: Completed NSE at 15:06, 0.00s elapsed  
[*] Nmap: Nmap scan report for 192.168.1.101  
[*] Nmap: Host is up (0.0000060s latency).  
[*] Nmap: All 1000 scanned ports on 192.168.1.101 are closed  
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
[*] Nmap: Device type: webcam|phone|general purpose|storage-misc  
[*] Nmap: Running: AXIS Linux 2.6.X, Google Android 2.X, Linux 2.6.X, ZyXEL embedded  
[*] Nmap: OS CPE: cpe:/h:axis:210a_network_camera cpe:/h:axis:211_network_camera cpe:/o:axis:linux_kernel:2.6 cpe:/o:google:android:2 cpe:/o:google:android:2.2 cpe:/o:linux:linux_kernel:2.6 cpe:/h:zyxel:nsa-210  
[*] Nmap: OS details: AXIS 210A or 211 Network Camera (Linux 2.6.17), Android 2.2 (Linux 2.6), Linux 2.6.14 - 2.6.34, Linux 2.6.17, Linux 2.6.17 (Mandriva), ZyXEL NSA-210 NAS device  
[*] Nmap: Network Distance: 0 hops  
[*] Nmap: NSE: Script Post-scanning.  
[*] Nmap: Initiating NSE at 15:06  
[*] Nmap: Completed NSE at 15:06, 0.00s elapsed  
[*] Nmap: Initiating NSE at 15:06  
[*] Nmap: Completed NSE at 15:06, 0.00s elapsed  
[*] Nmap: Read data files from: /usr/bin/../share/nmap  
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
[*] Nmap: Nmap done: 256 IP addresses (6 hosts up) scanned in 377.61 seconds  
[*] Nmap: Raw packets sent: 15030 (685.652KB) | Rcvd: 6568 (296.176KB)
```

```
msf > hosts
```

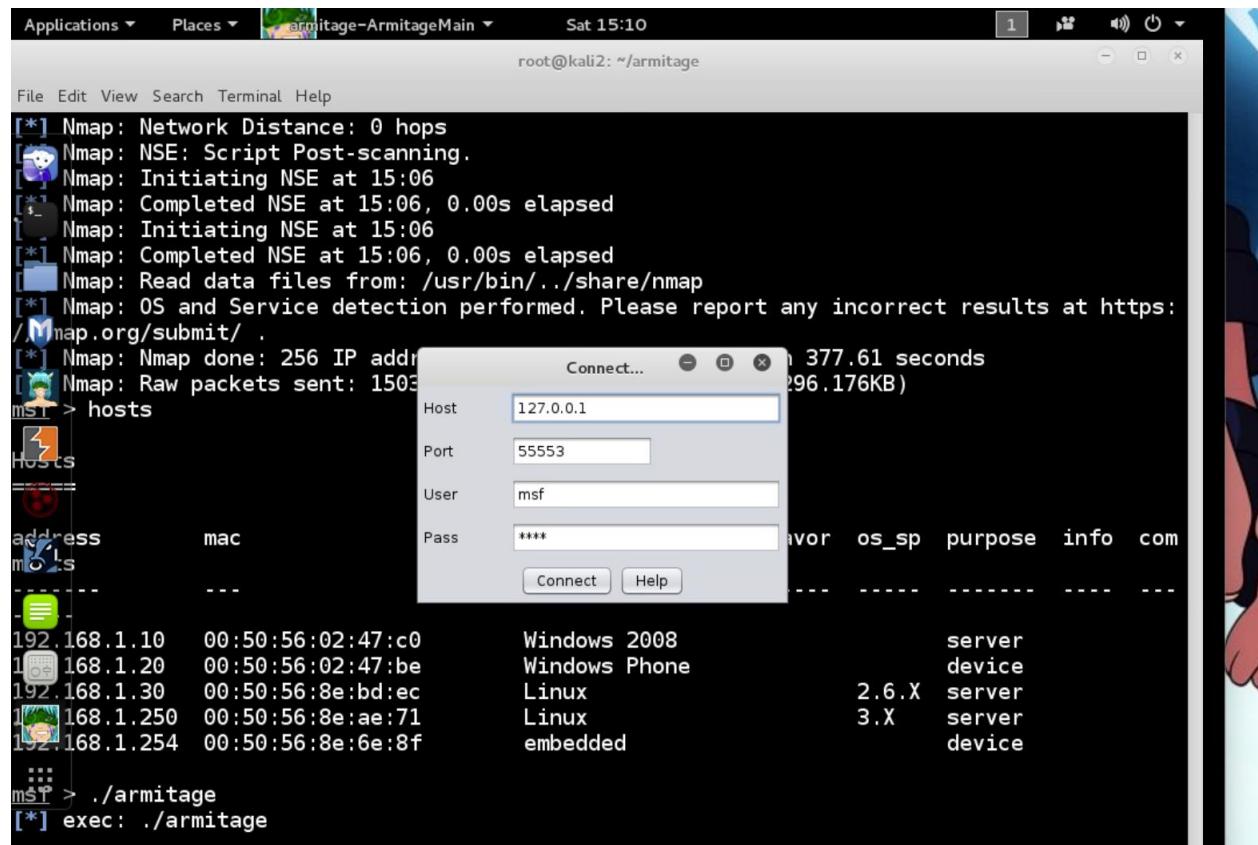
```
[*] Nmap: Raw packets sent: 15030 (685.652KB) | Rcvd: 6568 (296.176KB)
msf > hosts

Hosts
=====

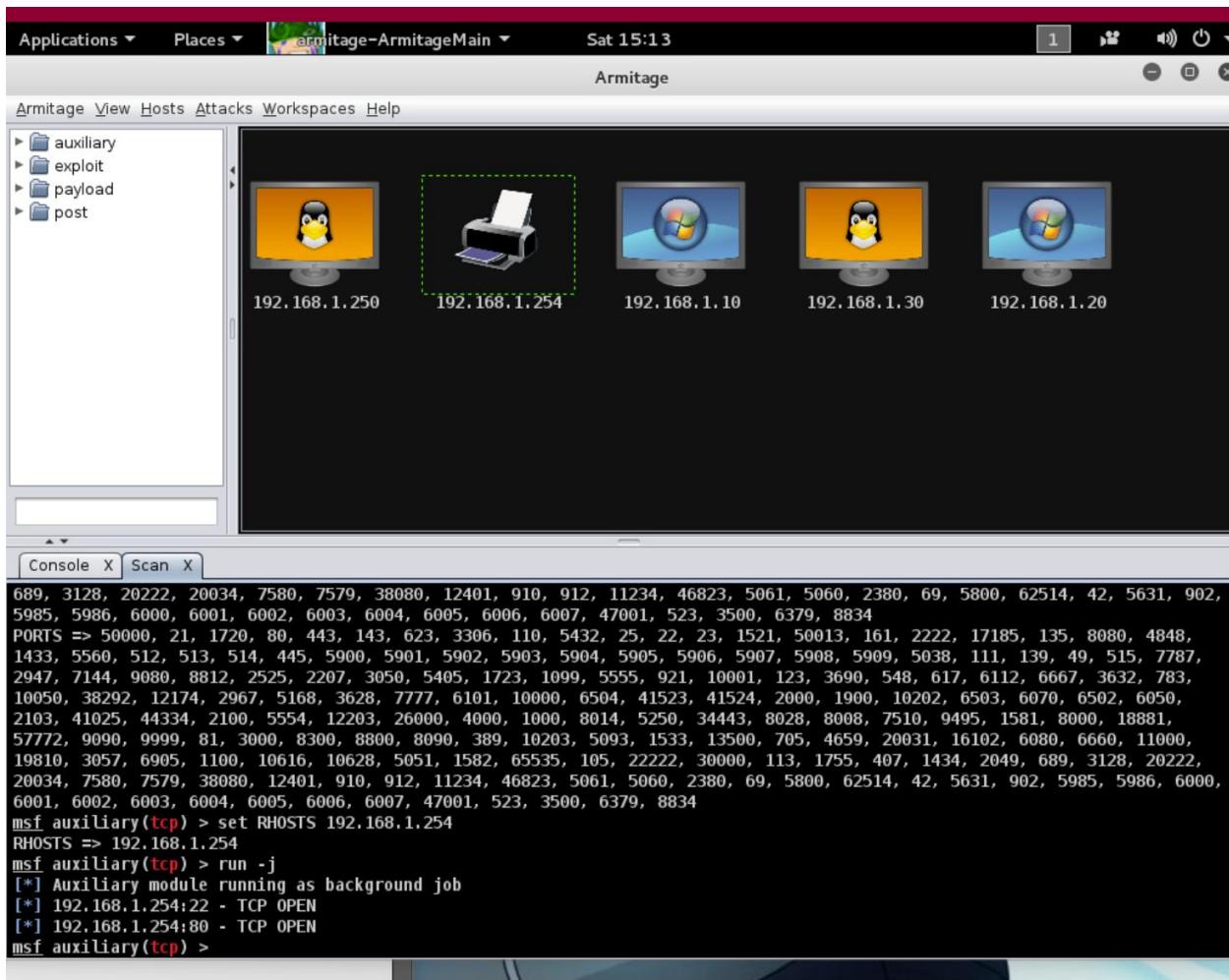
address      mac          name  os_name      os_flavor  os_sp   purpose  info  com
ments
-----  -----
192.168.1.10 00:50:56:02:47:c0    Windows 2008           server
192.168.1.20 00:50:56:02:47:be    Windows Phone        device
192.168.1.30 00:50:56:8e:bd:ec    Linux            2.6.X  server
192.168.1.250 00:50:56:8e:ae:71    Linux            3.X   server
192.168.1.254 00:50:56:8e:6e:8f    embedded          device

msf >
```

To start Armitage and click connect button to start Metasploit



Scanning the hosts



Supporting Evidence

Capturing the Challenge Flag and cat ip2.txt

The screenshot shows a web browser with two tabs open. The left tab is titled 'Ethical Hacking and Systems Defense' and contains a command-line interface for Wireshark, Windows, and Linux. It shows network interface details and a sample flag '999818'. Below the interface are two buttons: 'SAMPLE CHALLENGE' and 'CHALLENGE #1'. The right tab is titled 'Internal Kali Scoring-sniff' and shows a terminal window with root privileges. The terminal displays the output of the 'cat ip2.txt' command, which is identical to the content shown in the left tab. The terminal window has a standard Linux desktop environment with icons for various applications like Leafpad and Nautilus.

```
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe07:71c/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:7439 errors:0 dropped:0 overruns:0 frame:0
TX packets:49 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:827225 (807.8 KiB) TX bytes:8005 (7.8 KiB)

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
sample flag: 999818
TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1200 (1.1 KiB) TX bytes:1200 (1.1 KiB)

e the sample flag of 999818. Click on the Challenge icon and type the
ver box. This is just to show you how to capture Challenge Flags you
his lab.

SAMPLE CHALLENGE

CHALLENGE #1

root@kali2:~# cat ip2.txt
eth0      Link encap:Ethernet HWaddr 00:0c:29:07:07:1c
          inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe07:71c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:7439 errors:0 dropped:0 overruns:0 frame:0
          TX packets:49 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:827225 (807.8 KiB) TX bytes:8005 (7.8 KiB)

          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
          sample flag: 999818
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1200 (1.1 KiB) TX bytes:1200 (1.1 KiB)

root@kali2:~#
```

the following command and press Enter, so your system will not have

cat /etc/resolv.conf.backup2

The screenshot shows a terminal window with root privileges. The user runs the command 'cp /etc/resolv.conf /etc/resolv.conf.' followed by 'cat /etc/resolv.conf.backup1'. The terminal then displays the contents of the backup file, which includes a comment '# Generated by NetworkManager' and a 'nameserver 172.16.200.2' entry. The user then runs 'ifconfig eth0 192.168.1.101 netmask 255.255.255.0', 'route add default gw 192.168.1.254', and 'cp /etc/resolv.conf /etc/resolv.conf.backup1'. When attempting to run 'cat /etc.resolv.conf.backup1', the terminal returns an error message: 'cat: /etc.resolv.conf.backup1: No such file or directory'. The user then runs 'cat /etc/resolv.conf.backup2', which also includes the '# Generated by NetworkManager' comment and the 'nameserver 172.16.200.2' entry. The terminal window has a standard Linux desktop environment with icons for various applications like Leafpad and Nautilus.

```
root@kali2:~# cp /etc/resolv.conf /etc/resolv.conf.
root@kali2:~# cat /etc/resolv.conf.backup1
# Generated by NetworkManager
search localdomain
nameserver 172.16.200.2

root@kali2:~# ifconfig eth0 192.168.1.101 netmask 255.255.255.0
root@kali2:~# route add default gw 192.168.1.254
root@kali2:~# cp /etc/resolv.conf /etc/resolv.conf.backup1
root@kali2:~# cat /etc.resolv.conf.backup1
cat: /etc.resolv.conf.backup1: No such file or directory
root@kali2:~# cat /etc/resolv.conf.backup1
# Generated by NetworkManager
search localdomain
nameserver 172.16.200.2

root@kali2:~# cat /etc/resolv.conf.backup2
# Generated by NetworkManager
search localdomain
nameserver 172.16.200.2
flag:334451
root@kali2:~#
```

the following command and press Enter, to set the DNS server.

```
echo nameserver 192.168.1.10 > /etc/resolv.conf
```

```
kali2:~# echo nameserver 192.168.1.10 > /etc/resolv.conf
```

`cat /etc/resolv.flag`

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "Internal Kali Scoring-Shell". The terminal content shows the following session:

```
root@kali2:~# cat /etc/resolv.conf
nameserver 192.168.1.10
root@kali2:~# ifconfig eth0 192.168.1.101 netmask 255.255.255.0
root@kali2:~# route add default gw 192.168.1.254
root@kali2:~# cp /etc/resolv.conf /etc/resolv.conf.backup1
root@kali2:~# cat /etc/resolv.conf.backup1
cat: /etc/resolv.conf.backup1: No such file or directory
root@kali2:~# cat /etc/resolv.conf.backup1
# Generated by NetworkManager
search localdomain
nameserver 172.16.200.2
root@kali2:~# cat /etc/resolv.conf.backup2
# Generated by NetworkManager
search localdomain
nameserver 172.16.200.2
flag:334451
root@kali2:~# echo nameserver 192.168.1.10 > /etc/resolv.conf
root@kali2:~# cat /etc/resolv.conf
nameserver 192.168.1.10
root@kali2:~# cat /etc/resolv.flag
flag:888999
root@kali2:~#
```

To the left of the terminal window, there is a sidebar with various icons and a "CHALLENGE #3" button.

Captured the Flag 5 and 6 from the net view \\localhost

The screenshot shows a Windows terminal window titled "Administrator: cmd - Shortcut" with the following command history:

```
C:\Windows\System32>net view \\metasploitable
Shared resources at \\metasploitable
metasploitable server (Samba 3.0.20-Debian)
Share name      Type  Used as  Comment
-----
administrator  Disk   Home Directories
opt            Disk
tmp            Disk   oh noes!
The command completed successfully.

C:\Windows\System32>net view \\localhost
Shared resources at \\localhost

Share name      Type  Used as  Comment
-----
flag5          Disk   flag5:571444
flag6          Disk   flag6:333459
share          Disk
The command completed successfully.
```

To the left of the terminal window, there is a sidebar with various icons and two "CHALLENGE" buttons: "CHALLENGE #4" and "CHALLENGE #5".

Conclusion & Wrap-Up

Summary with:

Observations

In this lab, I explored system enumeration using various command line and GUI tools, including db_nmap, net, nbtstat, ifconfig, Wireshark, and Armitage. I noted that active scanning techniques revealed significant information about network services and devices, but they also increased the risk of detection. In contrast, passive scanning provided insights without alerting network defenses, demonstrating its value for stealthy assessments.

Identified risks

The main risk was how easily the Postgres service could be exploited, giving unauthorized access. Once inside, the ability to escalate privileges meant full control of the system was possible. Also, using scanning tools like Nmap could alert the target, increasing the chance of being detected.

Suggested recommendations

To avoid this type of attack, it's important to keep services like Postgres updated and secured with strong passwords and configurations. Firewalls and access controls should be in place. Regular vulnerability scans can help detect and fix these issues before attackers find them.

Your successes & failures

I successfully exploited the Postgres service and gained higher privileges, showing how a simple vulnerability can lead to complete system takeover. However, I struggled with setting up openVAS at first, which slowed down the scanning process.

Challenges

I faced challenges in analyzing large volumes of data from Wireshark, requiring more time and focus for effective interpretation. Variations in network configurations complicated the enumeration process, making it difficult to draw clear conclusions. Additionally, generating Nmap scans for hosts took a long time, and balancing thorough scanning with stealth remained a constant challenge, especially with active techniques.