Colby Heilner

Professor Torres

2/19

IT 145

Lab 4

Part A:

- (Run Part A on **NISGTC Network Security Lab 01** -Backtrack Internal and Backtrack External host)

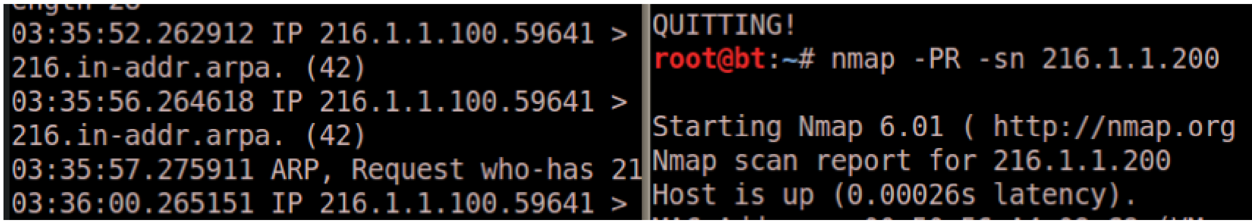
1. Launch tcpdump as you did in the class (with the host destinations)
2. Run the below scans as you did in class against **Each** of the IP's in this lab as well as the **Network** from both the external Backtrack and the Internal Backtrack:

–Discovery scans

- ○ Describe and perform a Layer 2 scan

  Detecting a live host with ARP.

  Tcpdump left

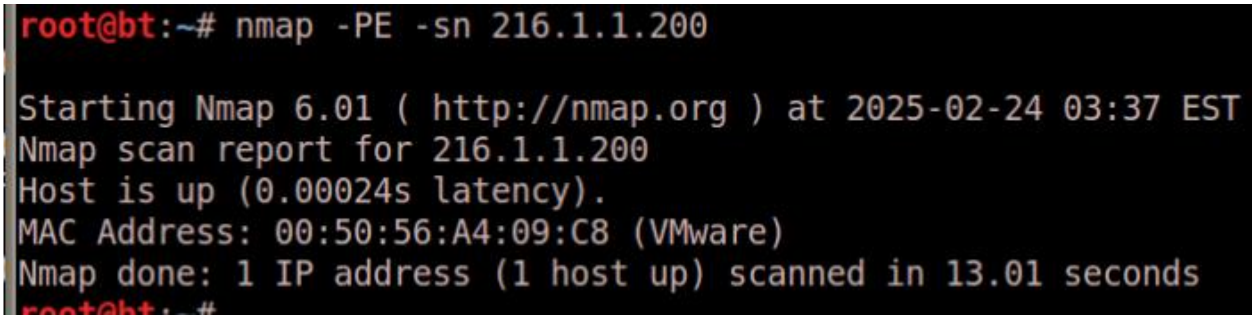


```
03:35:52.262912 IP 216.1.1.100.59641 >
216.in-addr.arpa. (42)
03:35:56.264618 IP 216.1.1.100.59641 >
216.in-addr.arpa. (42)
03:35:57.275911 ARP, Request who-has 21
03:36:00.265151 IP 216.1.1.100.59641 >
```

```
QUITTING!
root@bt:~# nmap -PR -sn 216.1.1.200

Starting Nmap 6.01 ( http://nmap.org
Nmap scan report for 216.1.1.200
Host is up (0.00026s latency).
```

- ○ Describe and perform a Layer 3 scan

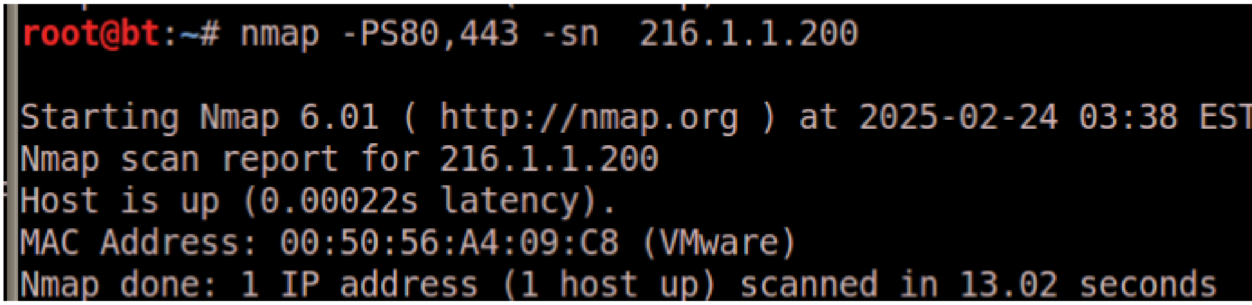
  Host discovery with ICMP



```
root@bt:~# nmap -PE -sn 216.1.1.200

Starting Nmap 6.01 ( http://nmap.org ) at 2025-02-24 03:37 EST
Nmap scan report for 216.1.1.200
Host is up (0.00024s latency).
MAC Address: 00:50:56:A4:09:C8 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 13.01 seconds
root@bt:~#
```

- Describe and perform a Layer 4 scan

SYN scans for host if up

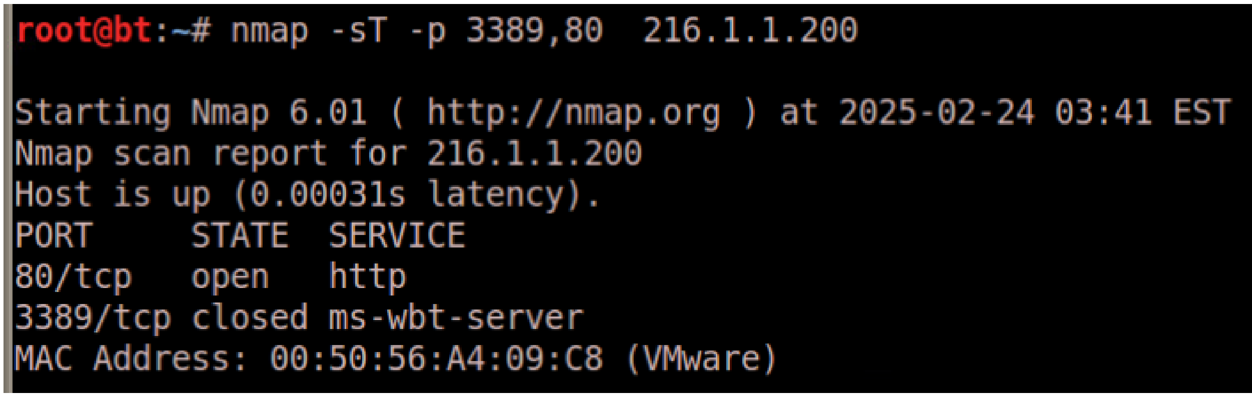


```
root@bt:~# nmap -PS80,443 -sn  216.1.1.200

Starting Nmap 6.01 ( http://nmap.org ) at 2025-02-24 03:38 EST
Nmap scan report for 216.1.1.200
Host is up (0.00022s latency).
MAC Address: 00:50:56:A4:09:C8 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 13.02 seconds
```

–Port Scans

- Describe and perform a TCP scan

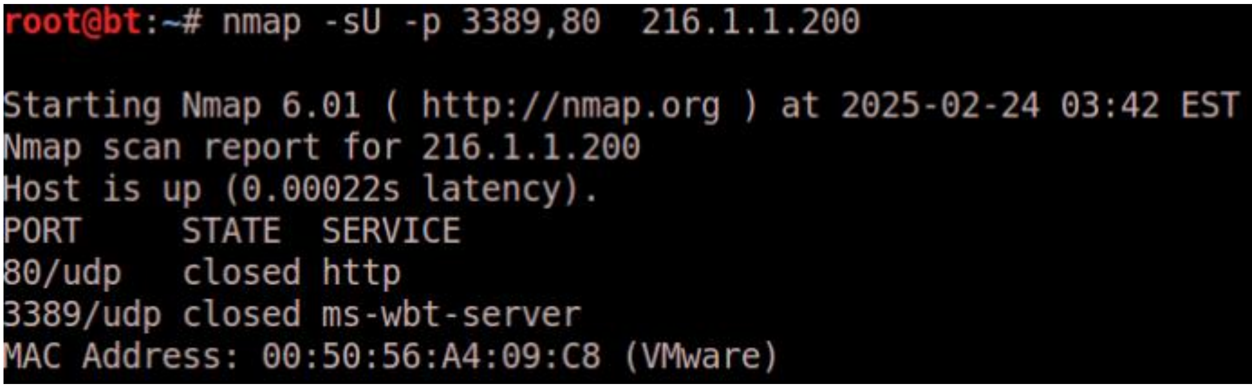
-sT is tcp connect



```
root@bt:~# nmap -sT -p 3389,80  216.1.1.200

Starting Nmap 6.01 ( http://nmap.org ) at 2025-02-24 03:41 EST
Nmap scan report for 216.1.1.200
Host is up (0.00031s latency).
PORT     STATE  SERVICE
80/tcp   open   http
3389/tcp closed ms-wbt-server
MAC Address: 00:50:56:A4:09:C8 (VMware)
```

- Describe and perform a UDP scan

-sU is a udp scan



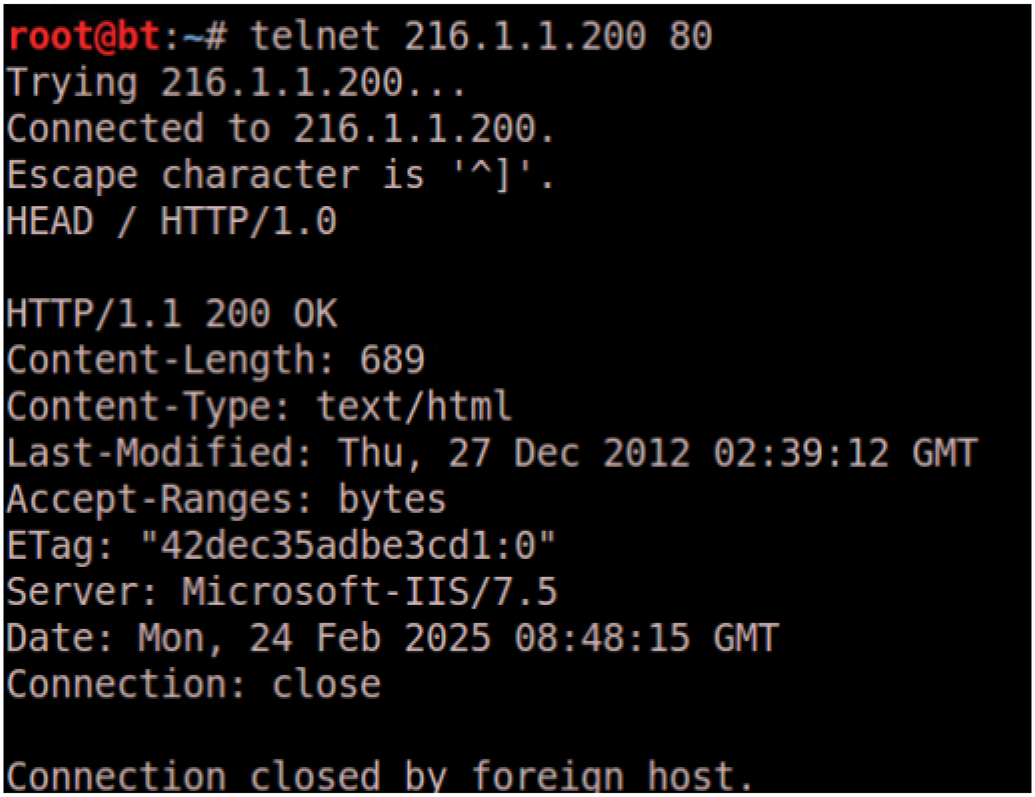
```
root@bt:~# nmap -sU -p 3389,80  216.1.1.200

Starting Nmap 6.01 ( http://nmap.org ) at 2025-02-24 03:42 EST
Nmap scan report for 216.1.1.200
Host is up (0.00022s latency).
PORT     STATE  SERVICE
80/udp   closed http
3389/udp closed ms-wbt-server
MAC Address: 00:50:56:A4:09:C8 (VMware)
```

Make sure you know what you are scanning for!

–Fingerprint Scans

- Describe and perform a Banner Grabbing (use netcat or telnet)

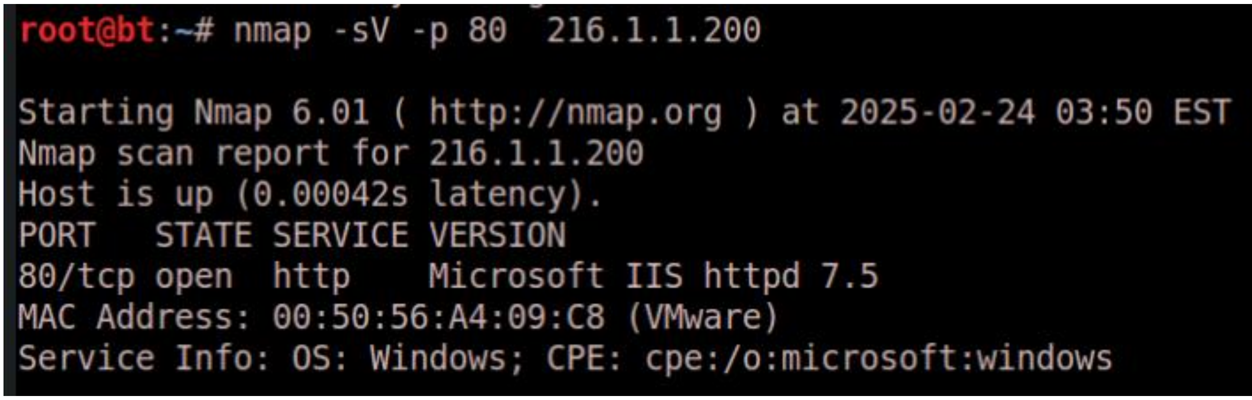
  I requested to view port 80 and its banner by writing HEAD / HTTP/1.0



```
root@bt:~# telnet 216.1.1.200 80
Trying 216.1.1.200...
Connected to 216.1.1.200.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Content-Length: 689
Content-Type: text/html
Last-Modified: Thu, 27 Dec 2012 02:39:12 GMT
Accept-Ranges: bytes
ETag: "42dec35adbe3cd1:0"
Server: Microsoft-IIS/7.5
Date: Mon, 24 Feb 2025 08:48:15 GMT
Connection: close

Connection closed by foreign host.
```

- Describe and perform a Service ID (Version Scanning)

  -sV scans for version of service

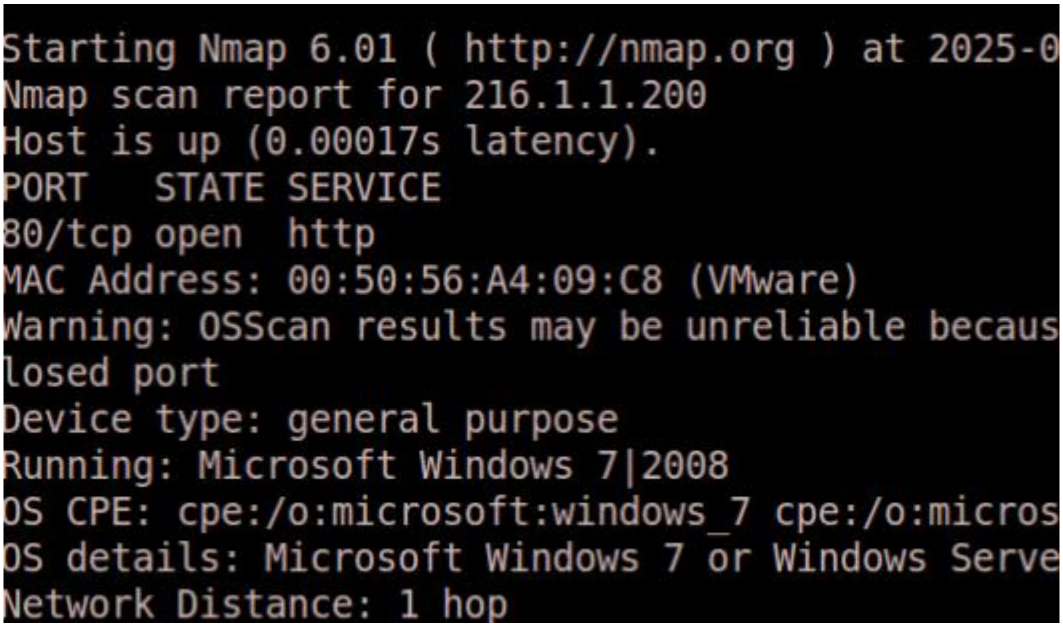


```
root@bt:~# nmap -sV -p 80  216.1.1.200

Starting Nmap 6.01 ( http://nmap.org ) at 2025-02-24 03:50 EST
Nmap scan report for 216.1.1.200
Host is up (0.00042s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 7.5
MAC Address: 00:50:56:A4:09:C8 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Same version as the banner grab!

- Describe and perform a OS scan

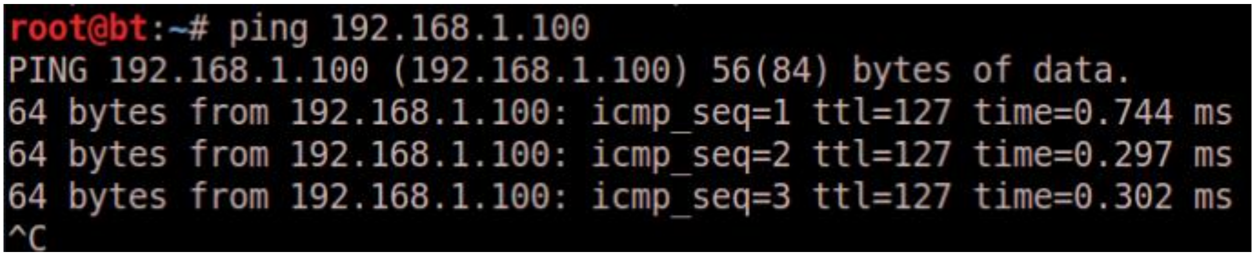
  -O is the flag for operating system check



```
Starting Nmap 6.01 ( http://nmap.org ) at 2025-0
Nmap scan report for 216.1.1.200
Host is up (0.00017s latency).
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:50:56:A4:09:C8 (VMware)
Warning: OSScan results may be unreliable becaus
losed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:micros
OS details: Microsoft Windows 7 or Windows Serve
Network Distance: 1 hop
```

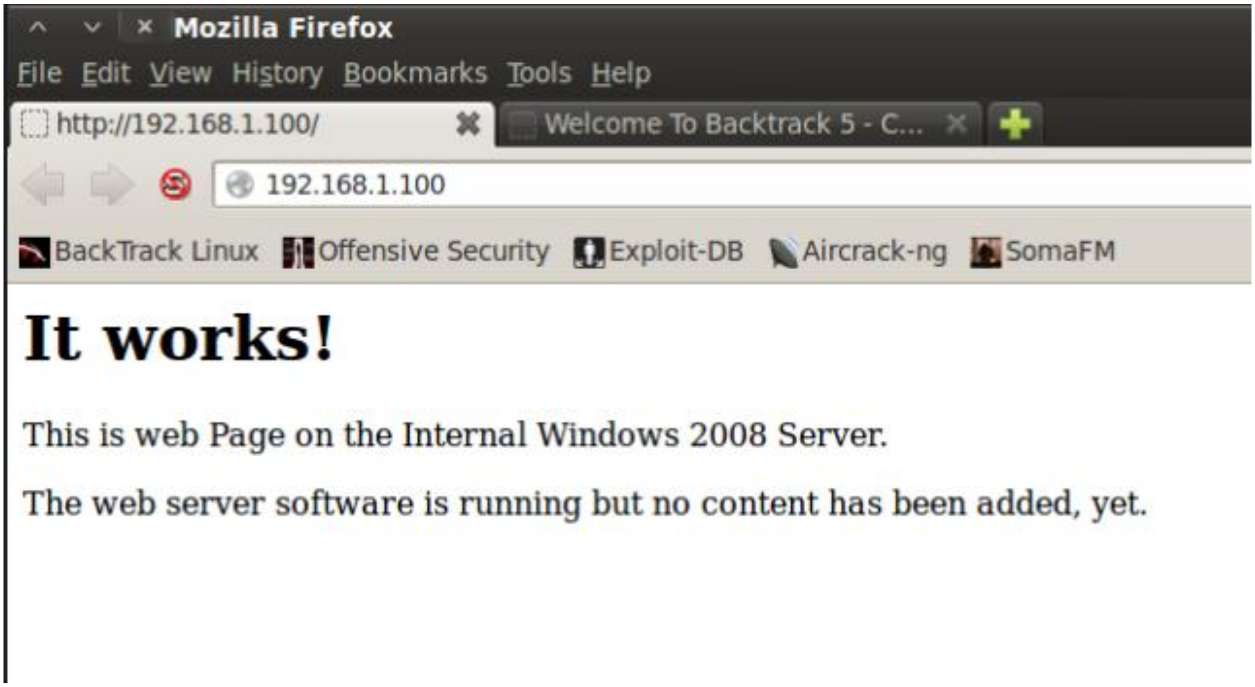
After finishing this section, briefly discuss what is wrong with the security on this network

Not sure why external can directly connect to internal.



```
root@bt:~# ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_seq=1 ttl=127 time=0.744 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=127 time=0.297 ms
64 bytes from 192.168.1.100: icmp_seq=3 ttl=127 time=0.302 ms
^C
```

I can access the internal website from external and I don’t believe it is port forwarded.



It works!

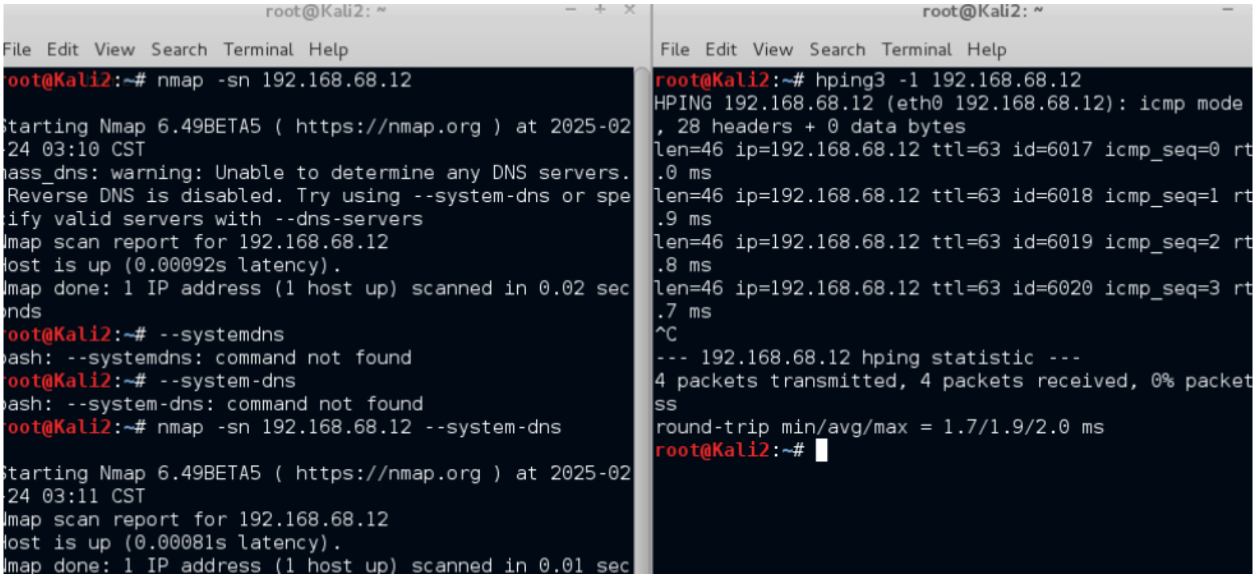
This is web Page on the Internal Windows 2008 Server.

The web server software is running but no content has been added, yet.

Part B:

-
    - Capture a screen shot of the results of each major command. Research what the below scans do, how to do the below scans with Nmap and Hping, and run the commands in the **NetLab NDG Ethical Hacking- Lab 01** from the Kali Box, screenshot your results. Run Tcpdump or Wireshark while you are running the below scans so that you can view and understand the traffic on the network. Run all scans with NMAP and Hping against 192.168.68.12 ONLY
        -
            - Describe and perform a ping sweep

              -sn and -1 detect is host is alive via ping

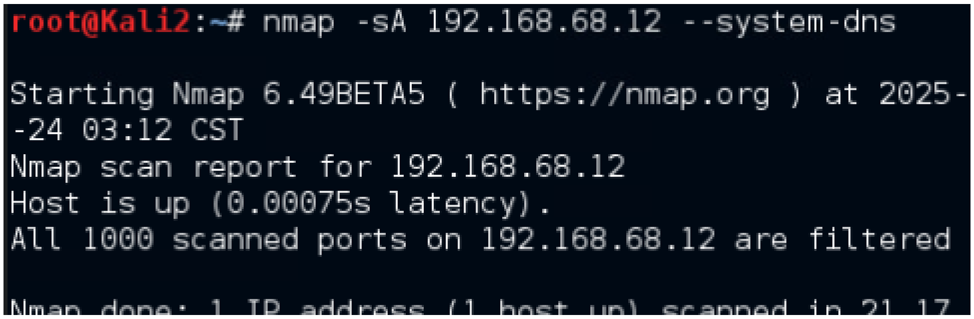

root@Kali2: ~
File Edit View Search Terminal Help
root@Kali2: ~
File Edit View Search Terminal Help

```
oot@Kali2:~# nmap -sn 192.168.68.12

tarting Nmap 6.49BETA5 ( https://nmap.org ) at 2025-02
24 03:10 CST
ass_dns: warning: Unable to determine any DNS servers.
 Reverse DNS is disabled. Try using --system-dns or spe
ify valid servers with --dns-servers
map scan report for 192.168.68.12
ost is up (0.00092s latency).
map done: 1 IP address (1 host up) scanned in 0.02 sec
nds
oot@Kali2:~# --systemdns
ash: --systemdns: command not found
oot@Kali2:~# --system-dns
ash: --system-dns: command not found
oot@Kali2:~# nmap -sn 192.168.68.12 --system-dns

tarting Nmap 6.49BETA5 ( https://nmap.org ) at 2025-02
24 03:11 CST
map scan report for 192.168.68.12
ost is up (0.00081s latency).
map done: 1 IP address (1 host up) scanned in 0.01 sec
```

```
root@Kali2:~# hping3 -1 192.168.68.12
HPING 192.168.68.12 (eth0 192.168.68.12): icmp mode
, 28 headers + 0 data bytes
len=46 ip=192.168.68.12 ttl=63 id=6017 icmp_seq=0 rt
.0 ms
len=46 ip=192.168.68.12 ttl=63 id=6018 icmp_seq=1 rt
.9 ms
len=46 ip=192.168.68.12 ttl=63 id=6019 icmp_seq=2 rt
.8 ms
len=46 ip=192.168.68.12 ttl=63 id=6020 icmp_seq=3 rt
.7 ms
^C
--- 192.168.68.12 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet
ss
round-trip min/avg/max = 1.7/1.9/2.0 ms
root@Kali2:~#
```

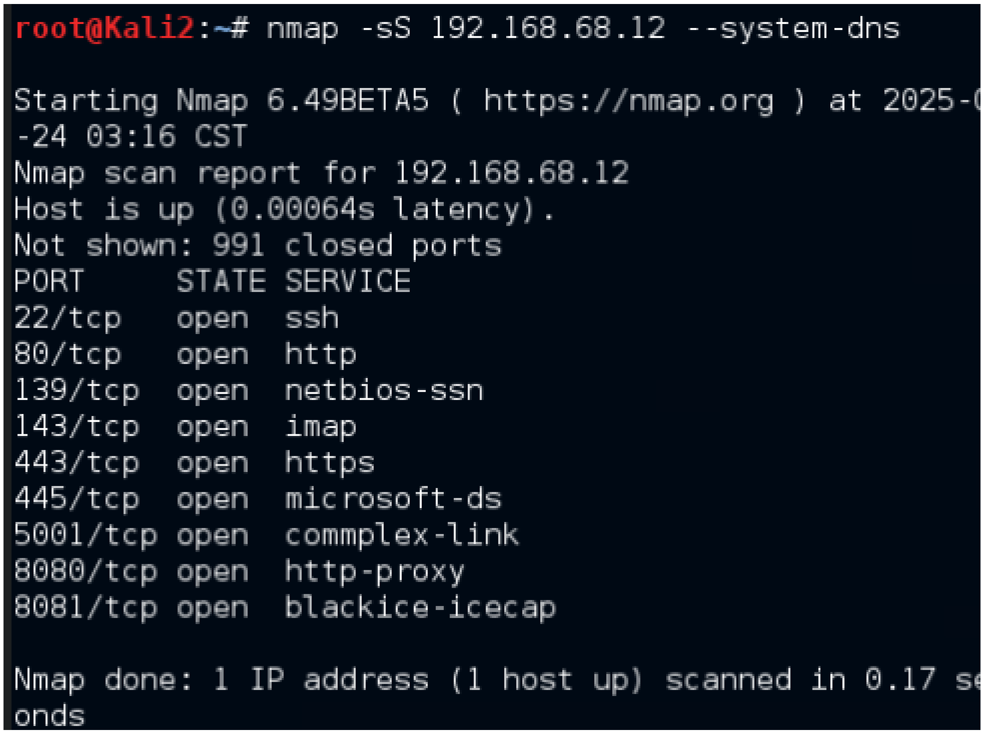
- Describe and perform a Ack scan

  -sA and -A



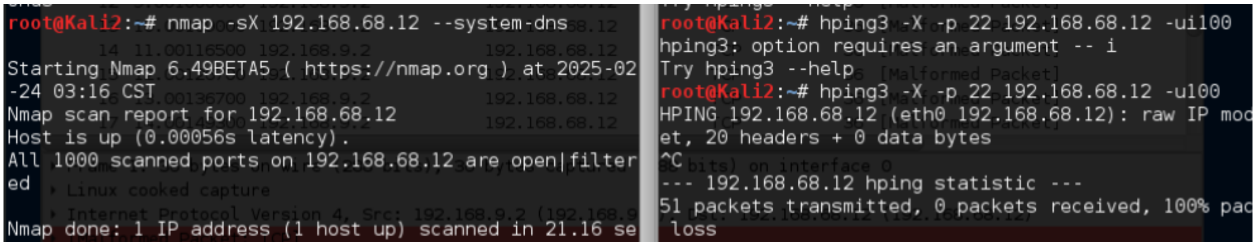
```
root@Kali2:~# nmap -sA 192.168.68.12 --system-dns

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2025-
-24 03:12 CST
Nmap scan report for 192.168.68.12
Host is up (0.00075s latency).
All 1000 scanned ports on 192.168.68.12 are filtered

Nmap done: 1 IP address (1 host up) scanned in 21.17
```

- Describe and perform a Syn scan



```
root@Kali2:~# nmap -sS 192.168.68.12 --system-dns

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2025-0
-24 03:16 CST
Nmap scan report for 192.168.68.12
Host is up (0.00064s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 0.17 se
onds
```

- Describe and perform a Xmas scan



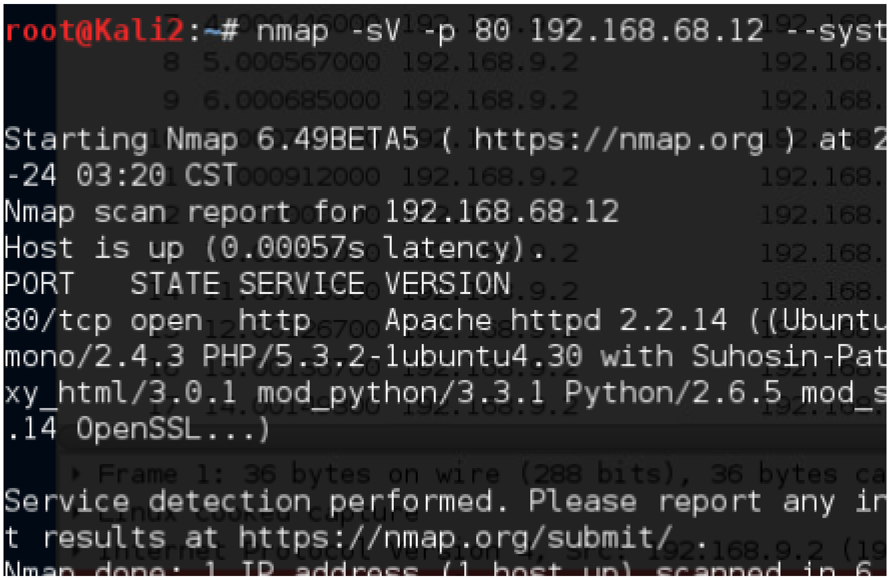
```
root@Kali2:~# nmap -sX 192.168.68.12 --system-dns

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2025-02
-24 03:16 CST
Nmap scan report for 192.168.68.12
Host is up (0.00056s latency).
All 1000 scanned ports on 192.168.68.12 are open|filter
ed

Nmap done: 1 IP address (1 host up) scanned in 21.16 se
```

```
root@Kali2:~# hping3 -X -p 22 192.168.68.12 -ui100
hping3: option requires an argument -- i
Try hping3 --help
root@Kali2:~# hping3 -X -p 22 192.168.68.12 -u100
HPING 192.168.68.12 (eth0 192.168.68.12): raw IP mod
et, 20 headers + 0 data bytes
^C
--- 192.168.68.12 hping statistic ---
51 packets transmitted, 0 packets received, 100% pac
 loss
```

  - Describe and perform a Version scan

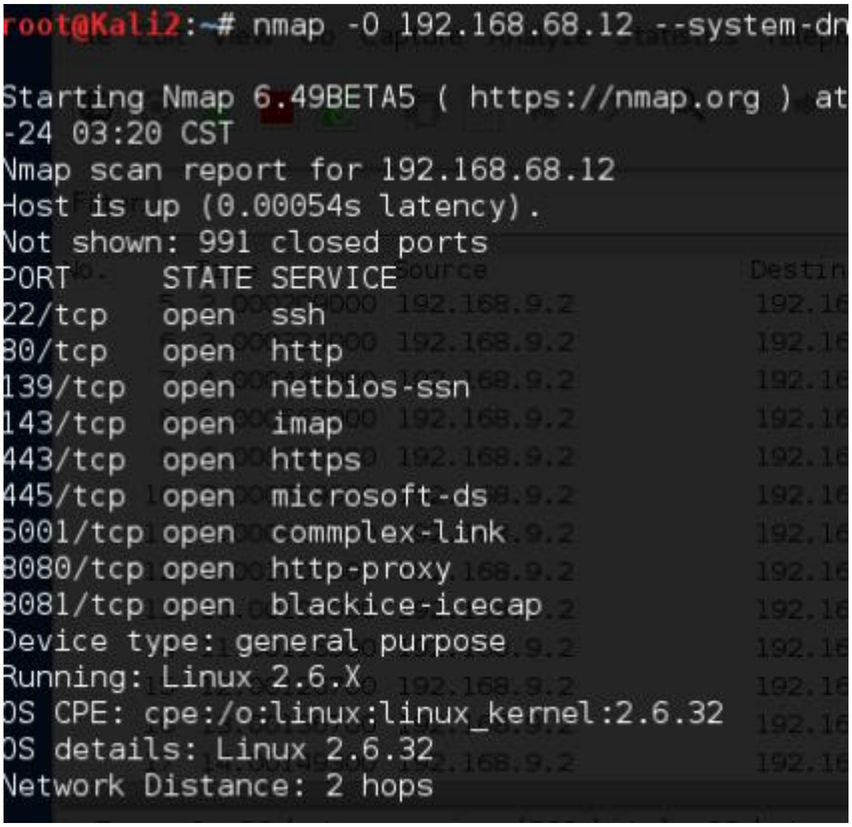
    -sV

    Gets version of service scanned.



```
root@Kali2:~# nmap -sV -p 80 192.168.68.12 --syst


Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2
-24 03:20 CST
Nmap scan report for 192.168.68.12
Host is up (0.00057s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.14 ((Ubuntu
mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Pat
xy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_s
.14 OpenSSL...)

Service detection performed. Please report any in
t results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6
```

- Describe and perform a OS scan



```
root@Kali2:~# nmap -O 192.168.68.12 --system-dn

Starting Nmap 6.49BETA5 ( https://nmap.org ) at
-24 03:20 CST
Nmap scan report for 192.168.68.12
Host is up (0.00054s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 2 hops
```

- Which scan created the most traffic on Tcpdump/Wireshark?

XMAS this is because it is named after making every light turn on in a switch when ran against it.

It does a lot of different tests.

- After finishing this section, briefly discuss what is wrong with the security on this network

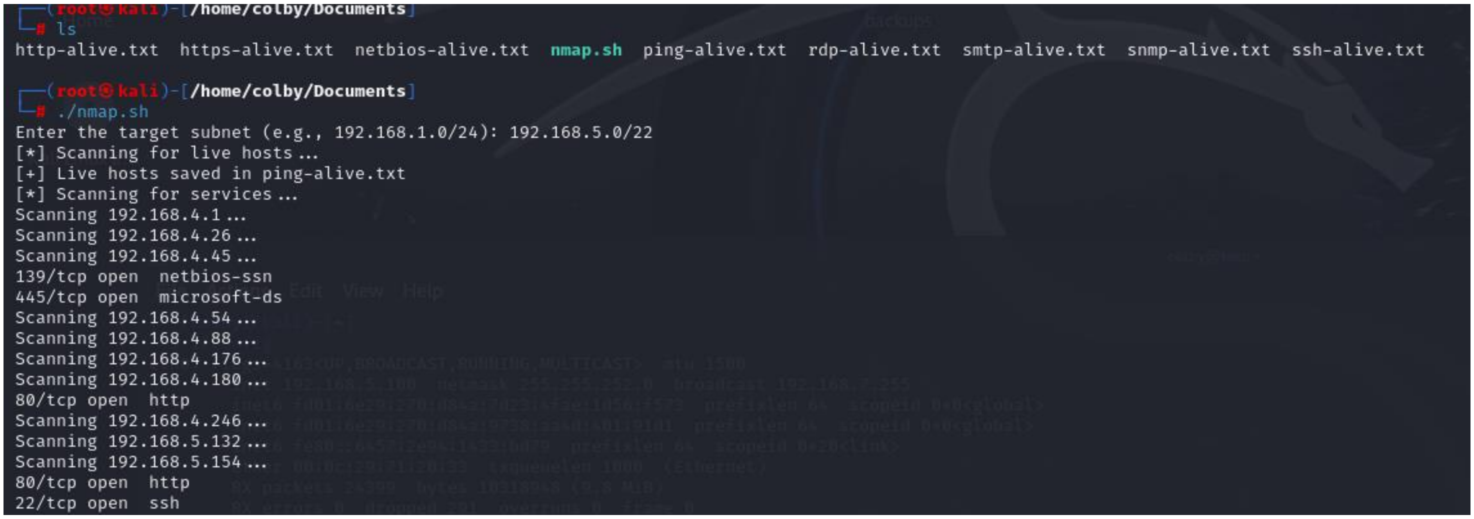
  DMZ →LAN not good

  also **Wan → Lan** not usually good.

  Make firewall rules to only allow wan to dmz and do not all dmz traffic to get into lan "lateral movement!"

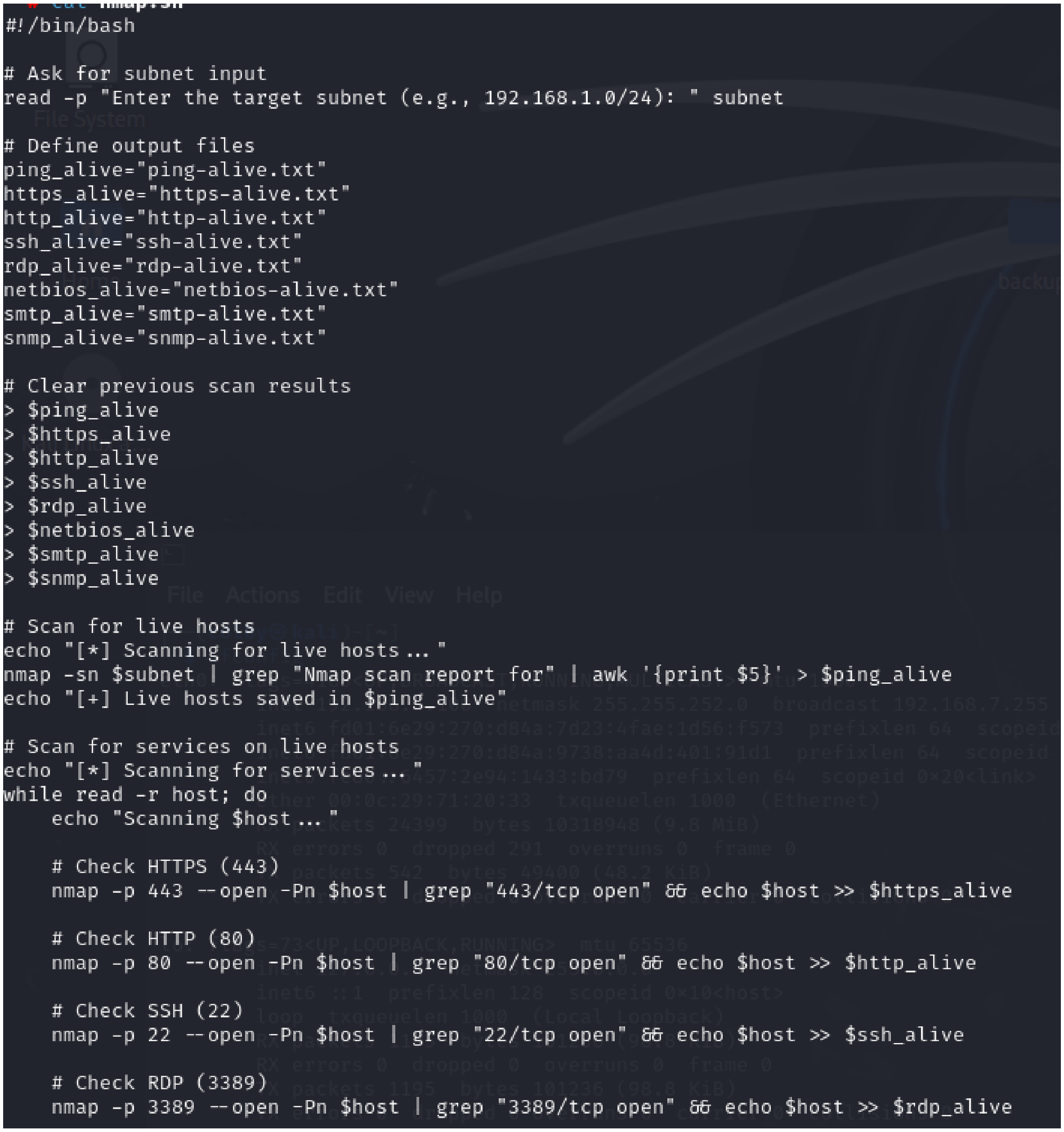
- **Create an interactive bash script. When you run the script it should ask for your target subnet to scan, it will run a scan and create the below files:**
- **ping-alive.txt**
- **https-alive.txt**
- **http-alive.txt**
- **ssh-alive.txt**
- **rdp-alive.txt**
- **netbios-alive.txt**
- **smtp-alive.txt**
- **snmp-alive.txt**

It updates me with verbose during the scan

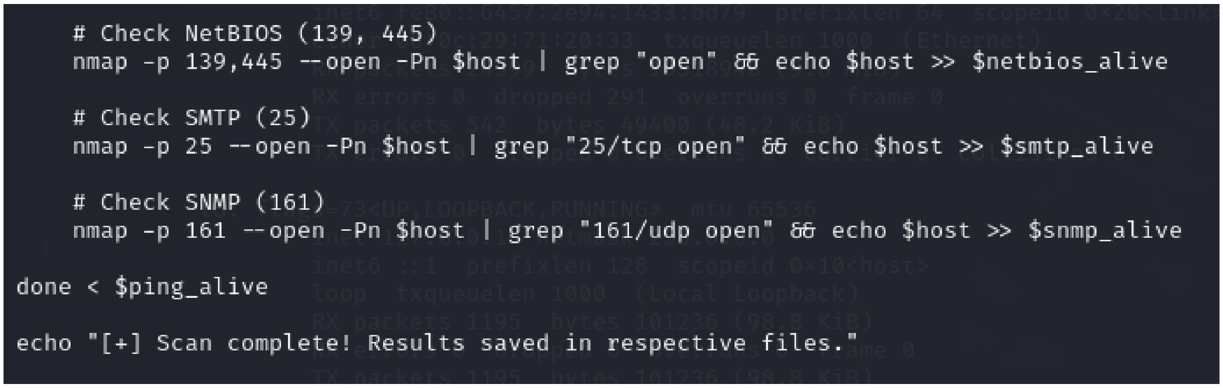


```
┌──(root㉿kali)-[/home/colby/Documents]
└─# ls
http-alive.txt  https-alive.txt  netbios-alive.txt  nmap.sh  ping-alive.txt  rdp-alive.txt  smtp-alive.txt  snmp-alive.txt  ssh-alive.txt

┌──(root㉿kali)-[/home/colby/Documents]
└─# ./nmap.sh
Enter the target subnet (e.g., 192.168.1.0/24): 192.168.5.0/22
[*] Scanning for live hosts ...
[+] Live hosts saved in ping-alive.txt
[*] Scanning for services ...
Scanning 192.168.4.1 ...
Scanning 192.168.4.26 ...
Scanning 192.168.4.45 ...
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
Scanning 192.168.4.54 ...
Scanning 192.168.4.88 ...
Scanning 192.168.4.176 ...
Scanning 192.168.4.180 ...
80/tcp open  http
Scanning 192.168.4.246 ...
Scanning 192.168.5.132 ...
Scanning 192.168.5.154 ...
80/tcp open  http
22/tcp open  ssh
```

Here is the clear



```
#!/bin/bash

# Ask for subnet input
read -p "Enter the target subnet (e.g., 192.168.1.0/24): " subnet

# Define output files
ping_alive="ping-alive.txt"
https_alive="https-alive.txt"
http_alive="http-alive.txt"
ssh_alive="ssh-alive.txt"
rdp_alive="rdp-alive.txt"
netbios_alive="netbios-alive.txt"
smtp_alive="smtp-alive.txt"
snmp_alive="snmp-alive.txt"

# Clear previous scan results
> $ping_alive
> $https_alive
> $http_alive
> $ssh_alive
> $rdp_alive
> $netbios_alive
> $smtp_alive
> $snmp_alive

# Scan for live hosts
echo "[*] Scanning for live hosts..."
nmap -sn $subnet | grep "Nmap scan report for" | awk '{print $5}' > $ping_alive
echo "[+] Live hosts saved in $ping_alive"

# Scan for services on live hosts
echo "[*] Scanning for services..."
while read -r host; do
    echo "Scanning $host..."

    # Check HTTPS (443)
    nmap -p 443 --open -Pn $host | grep "443/tcp open" && echo $host >> $https_alive

    # Check HTTP (80)
    nmap -p 80 --open -Pn $host | grep "80/tcp open" && echo $host >> $http_alive

    # Check SSH (22)
    nmap -p 22 --open -Pn $host | grep "22/tcp open" && echo $host >> $ssh_alive

    # Check RDP (3389)
    nmap -p 3389 --open -Pn $host | grep "3389/tcp open" && echo $host >> $rdp_alive
```



```
    # Check NetBIOS (139, 445)
    nmap -p 139,445 --open -Pn $host | grep "open" && echo $host >> $netbios_alive

    # Check SMTP (25)
    nmap -p 25 --open -Pn $host | grep "25/tcp open" && echo $host >> $smtp_alive

    # Check SNMP (161)
    nmap -p 161 --open -Pn $host | grep "161/udp open" && echo $host >> $snmp_alive

done < $ping_alive

echo "[+] Scan complete! Results saved in respective files."
```

NetLabs is timed, so the last one above should be created outside of NetLabs and tested within NetLabs once complete.

Part C:

- Which scan gave you the best results?

  I prefer -sS or -sT as they provide a more reliant connection-oriented scan.

- Did any one scan provide all or more information than all of the other scans combined?

  Just use the **-A** with speed -T1-5 flag for Nmap this pretty much does it all if stealth is not a concern

- Use the internet and state some scanning techniques you would have to do to bypass firewalls and/or trick IDS/IPS systems

  I have down tons of looking into this! Lots being my own tests. I have out some of these results in a IT-140 lab as well.

  I have learned that snort and other rules-based IDS and IPS like to look for really fast connections to ports. This usually indicated port scanners because services do not normally need to make 1000+ requests in a few seconds all in the same context. So you can bounce around with fancy Nmap flags and come to limiting parallels and rate of connections. On top of that you can match your source and dst port to make it look like normal traffic flow.

  Here is one I have shared before.

  ```
  nmap -sS -T2 --scan-delay 1000ms --max-rate 1 --min-parallelism 1 --max-retries 2 -g 4567 -vv 192.168.5.201 -p 4567
  ```

  I think you could also use hping3 to act as a Ip inside of the network or inside of a ip pass list but I have yet to get this to work due to hpings slow port scanning speeds.

  ```
  Hping3 -S -a x.x.x.x -p 22 -c 10 x.x.x.x
  ```

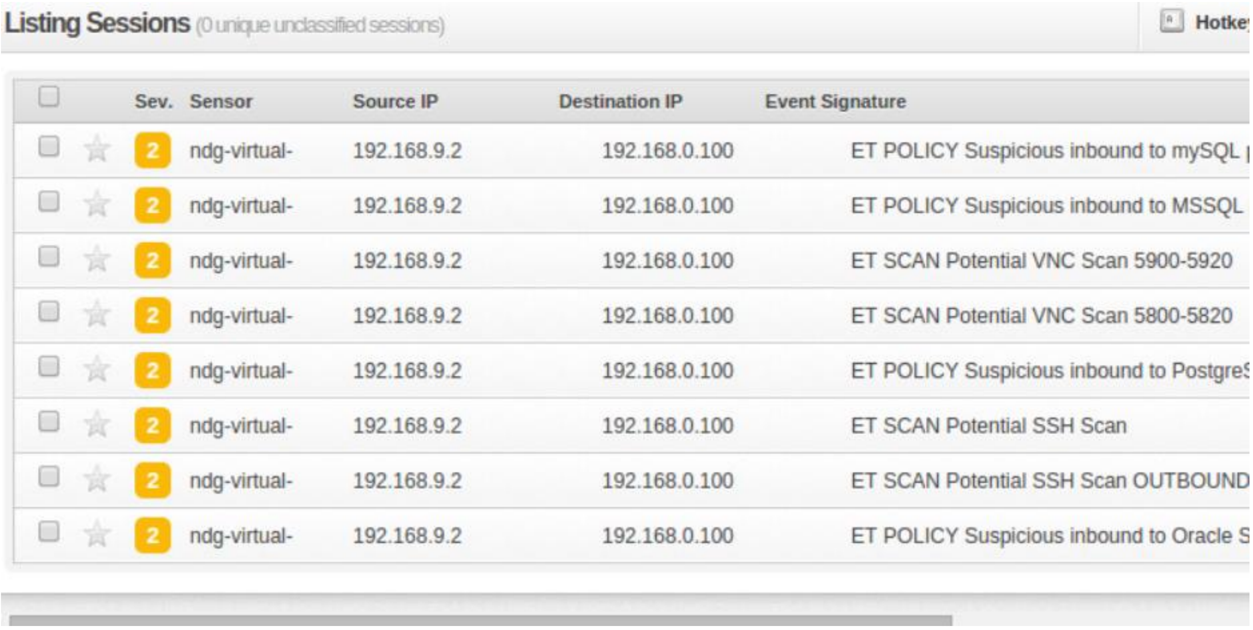
  The -a flag spoofs the source port for scan.

Extra Credit (5 points):

- One of the host in **NDG Ethical Hacking Lab 01** has a blocking/firewall/IPS rule, try some of the techniques that you have researched to bypass the blocks against this secured host (you may have to restart/reset this host -several times-hint hint)

  It took me going into another lab for this netlab (Evading IDS) but I found that sec onion has a IDS

  I ran a standard Nmap scan against seconion and it showed these



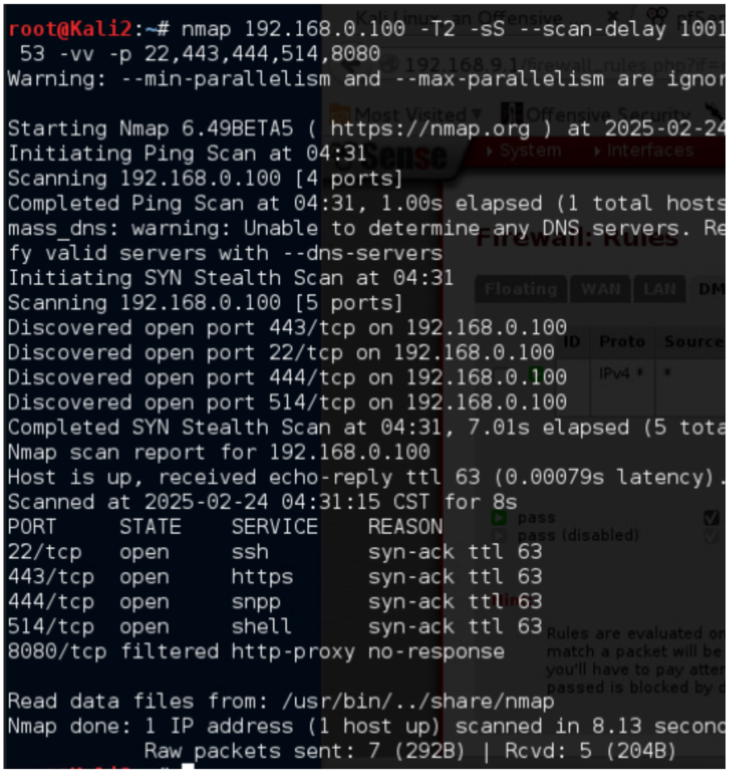
Listing Sessions (0 unique unclassified sessions)

Hotke

☐		Sev.	Sensor	Source IP	Destination IP	Event Signature
☐	☆	2	ndg-virtual-	192.168.9.2	192.168.0.100	ET POLICY Suspicious inbound to mySQL
☐	☆	2	ndg-virtual-	192.168.9.2	192.168.0.100	ET POLICY Suspicious inbound to MSSQL
☐	☆	2	ndg-virtual-	192.168.9.2	192.168.0.100	ET SCAN Potential VNC Scan 5900-5920
☐	☆	2	ndg-virtual-	192.168.9.2	192.168.0.100	ET SCAN Potential VNC Scan 5800-5820
☐	☆	2	ndg-virtual-	192.168.9.2	192.168.0.100	ET POLICY Suspicious inbound to PostgreS
☐	☆	2	ndg-virtual-	192.168.9.2	192.168.0.100	ET SCAN Potential SSH Scan
☐	☆	2	ndg-virtual-	192.168.9.2	192.168.0.100	ET SCAN Potential SSH Scan OUTBOUND
☐	☆	2	ndg-virtual-	192.168.9.2	192.168.0.100	ET POLICY Suspicious inbound to Oracle S

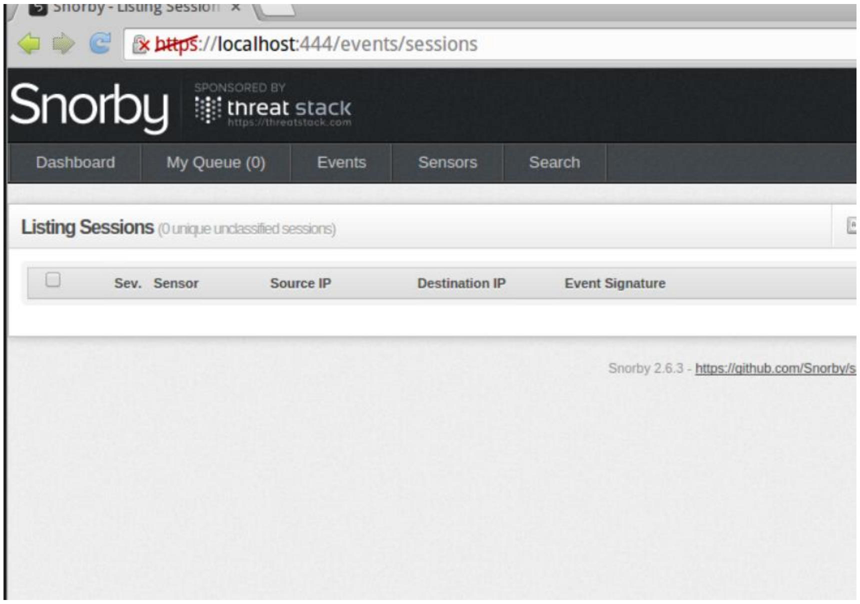
  Then I ran it with the command I showed just above

  nmap -sS -T2 --scan-delay 1000ms --max-rate 1 --min-parallelism 1 --max-retries 2 -g 4567 -vv 192.168.5.201 -p 4567



```
root@Kali2:~# nmap 192.168.0.100 -T2 -sS --scan-delay 1001
 53 -vv -p 22,443,444,514,8080
Warning: --min-parallelism and --max-parallelism are ignor

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2025-02-24
Initiating Ping Scan at 04:31
Scanning 192.168.0.100 [4 ports]
Completed Ping Scan at 04:31, 1.00s elapsed (1 total hosts
mass_dns: warning: Unable to determine any DNS servers. Re
fy valid servers with --dns-servers
Initiating SYN Stealth Scan at 04:31
Scanning 192.168.0.100 [5 ports]
Discovered open port 443/tcp on 192.168.0.100
Discovered open port 22/tcp on 192.168.0.100
Discovered open port 444/tcp on 192.168.0.100
Discovered open port 514/tcp on 192.168.0.100
Completed SYN Stealth Scan at 04:31, 7.01s elapsed (5 tota
Nmap scan report for 192.168.0.100
Host is up, received echo-reply ttl 63 (0.00079s latency).
Scanned at 2025-02-24 04:31:15 CST for 8s
PORT     STATE    SERVICE    REASON
22/tcp   open     ssh        syn-ack ttl 63
443/tcp  open     https      syn-ack ttl 63
444/tcp  open     snpp       syn-ack ttl 63
514/tcp  open     shell      syn-ack ttl 63
8080/tcp filtered http-proxy no-response

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 8.13 second
           Raw packets sent: 7 (292B) | Rcvd: 5 (204B)
```

No new events!



Listing Sessions (0 unique unclassified sessions)

☐	Sev.	Sensor	Source IP	Destination IP	Event Signature

Snorby 2.6.3 - https://github.com/Snorby/s

And again, it has eluded another IDS!

I tried this scan with a -p 1-1000 and it got caught

Best to limit the number of ports scanned at once.