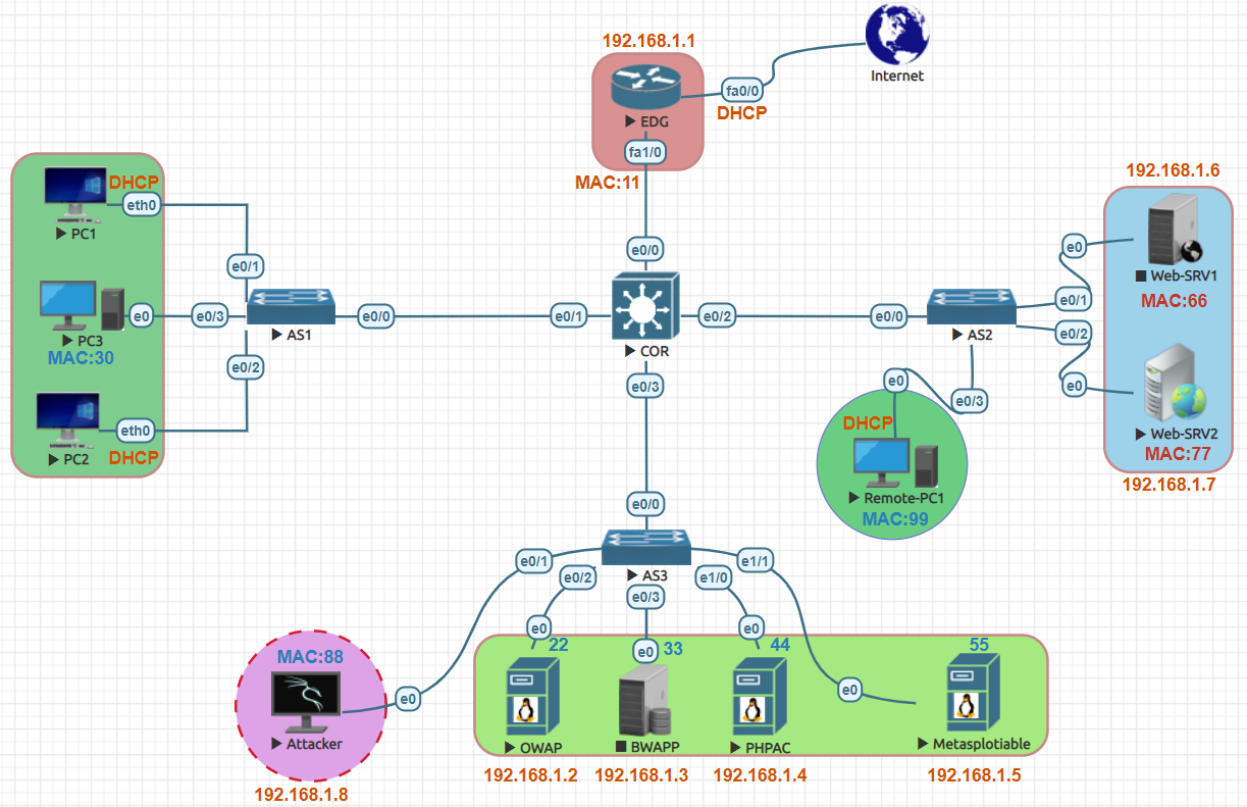
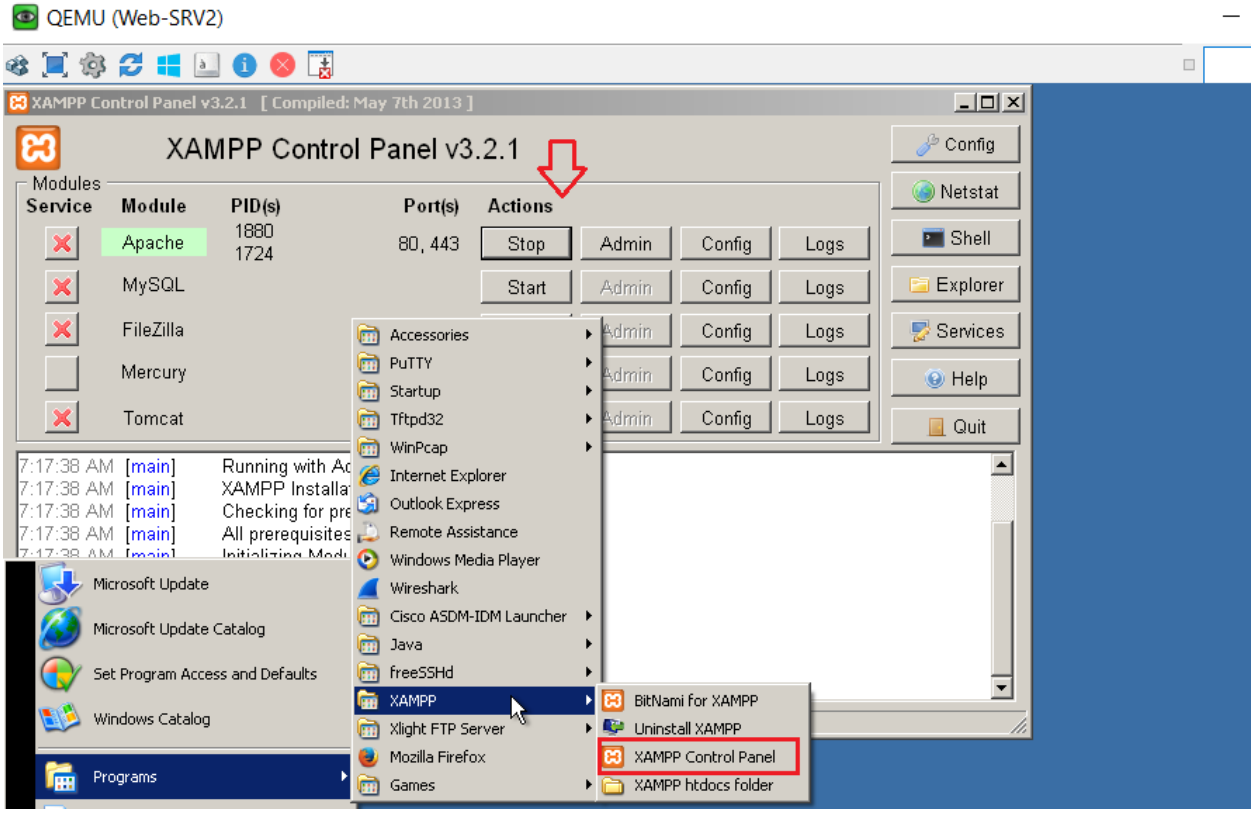
Reconnaissance Attack:



Network Subnet
192.168.1.0/24
Attacker IP Address
192.168.1.8

Attacker
nmap 192.168.1.0/24
nmap -sP 192.168.1.0/24
nmap -O 192.168.1.7
nmap -sV 192.168.1.7
nmap -O 192.168.1.5
hping3 --scan 1-65535 192.168.1.7 -S --rand-source
nmap -p 80 192.168.1.7
nmap -F 192.168.1.7
nmap -f 192.168.1.7
nmap 192.168.1.7
fping 192.168.1.7
whatweb 192.168.1.7
nikto -host 192.168.1.7

In Web-SRV2 navigate to Start go to XAMPP>XAMPP Control Panel start the web services.



Let's start Reconnaissance attack from Kali Linux Attacker using different tools & Commands.

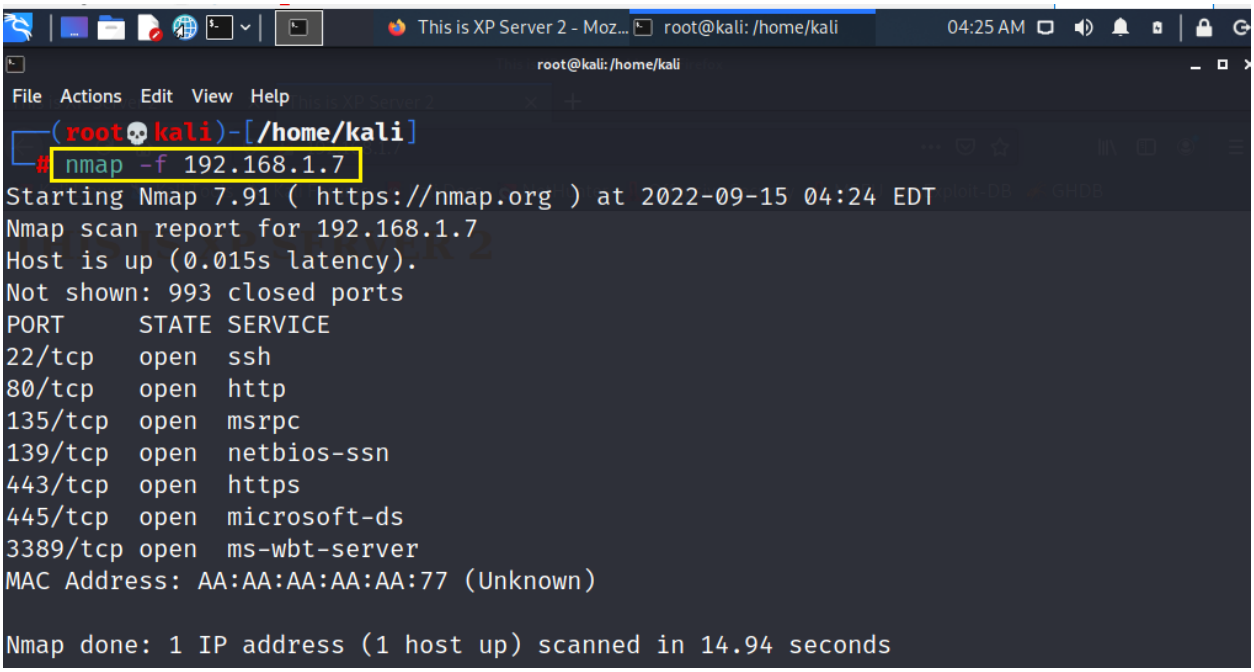
nmap -sP 192.168.1.0/24
nmap -O 192.168.1.7
nmap -sV 192.168.1.7
nmap -O 192.168.1.5
hping3 --scan 1-65535 192.168.1.7 -S --rand-source
nmap -p 80 192.168.1.7
nmap -F 192.168.1.7
nmap -f 192.168.1.7
nmap 192.168.1.0/24
nmap 192.168.1.7
fping 192.168.1.7
whatweb 192.168.1.7
whatweb 192.168.1.5
nikto -host 192.168.1.7

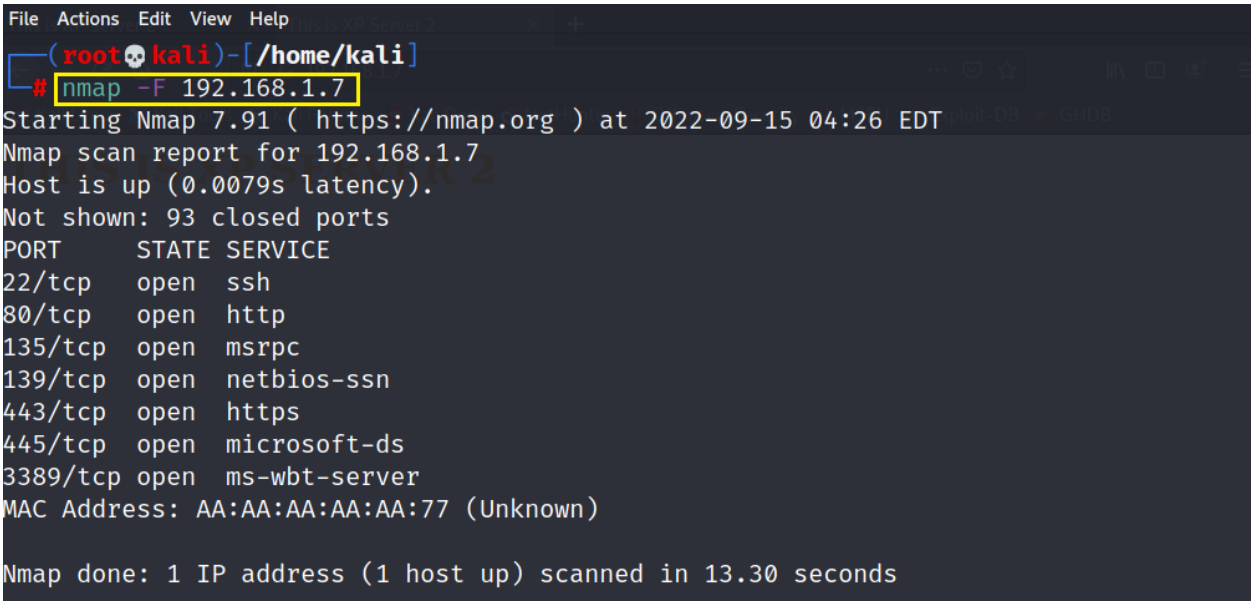
Scan the network for hosts and port open.

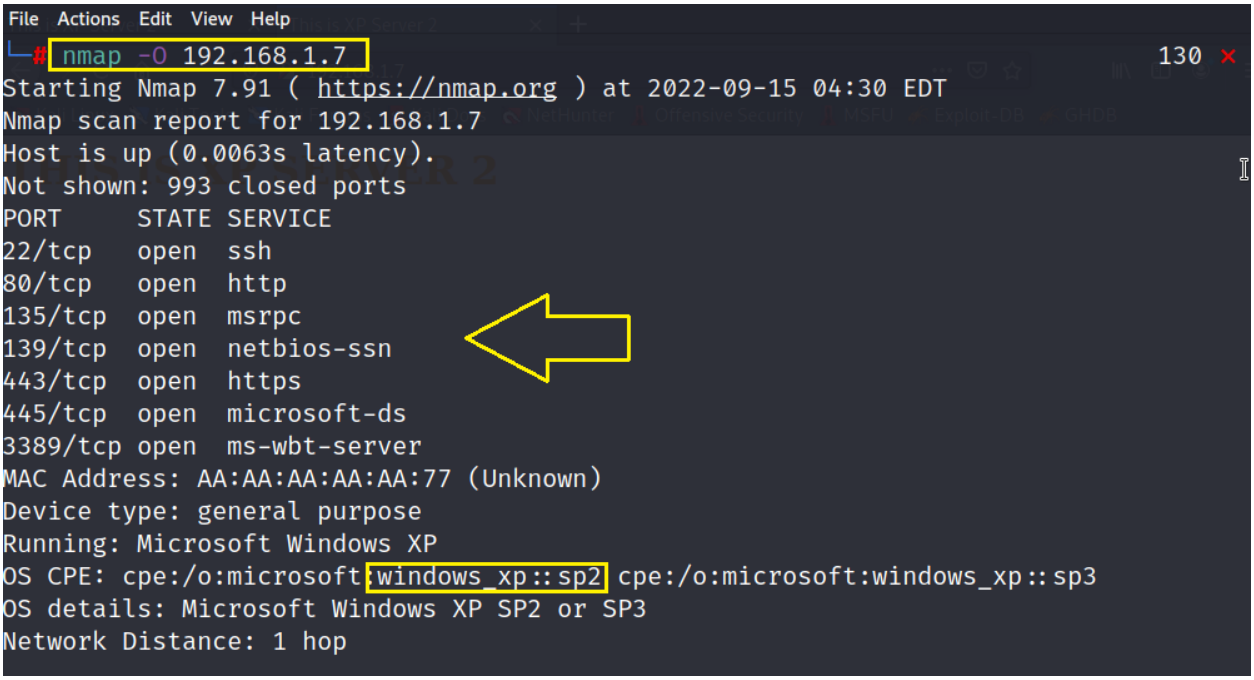
```
File  Actions  Edit  View  Help
┌──(root💀kali)-[/home/kali]
└─# nmap 192.168.1.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-15 04:27 EDT
Nmap scan report for 192.168.1.1
Host is up (0.019s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: AA:AA:AA:AA:AA:11 (Unknown)

Nmap scan report for 192.168.1.2
Host is up (0.0031s 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
MAC Address: AA:AA:AA:AA:AA:22 (Unknown)
```

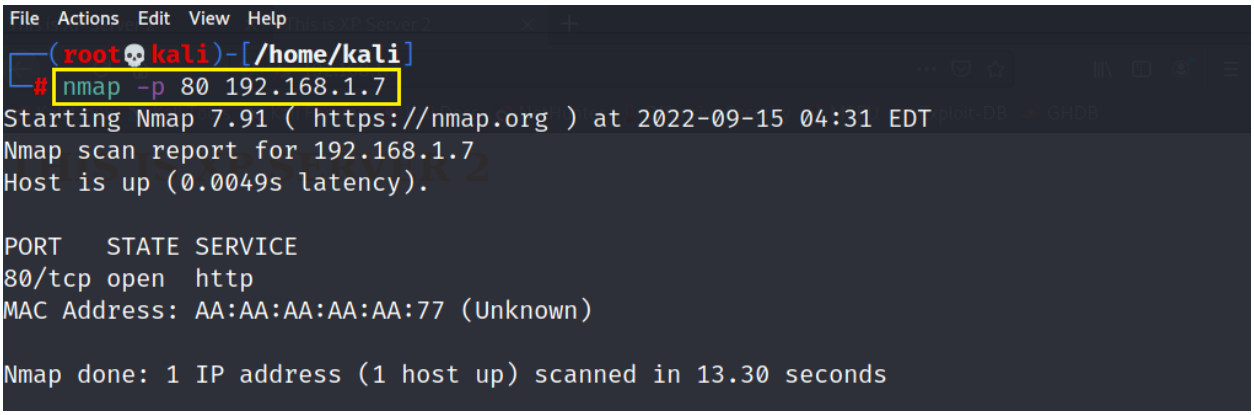
```
File  Actions  Edit  View  Help

Nmap scan report for 192.168.1.6
Host is up (0.0090s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: AA:AA:AA:AA:AA:66 (Unknown)

Nmap scan report for 192.168.1.7
Host is up (0.0082s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: AA:AA:AA:AA:AA:77 (Unknown)
```

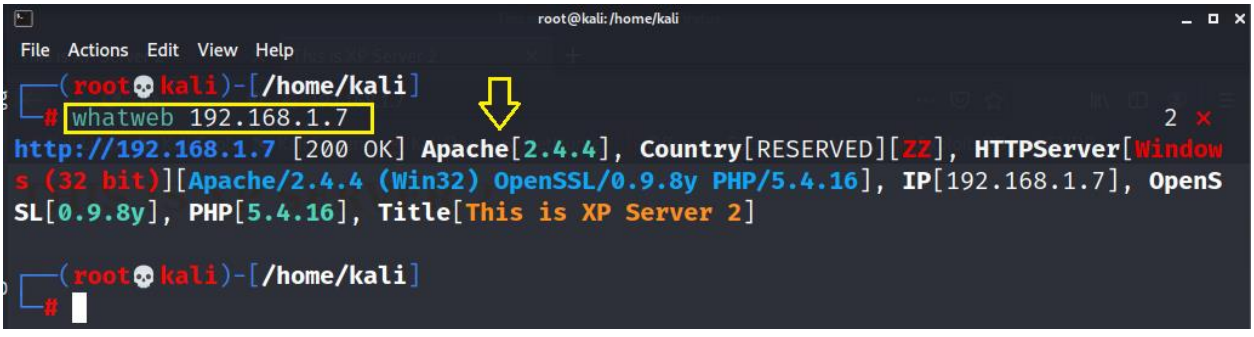
Scan the specific host for well-known open ports.

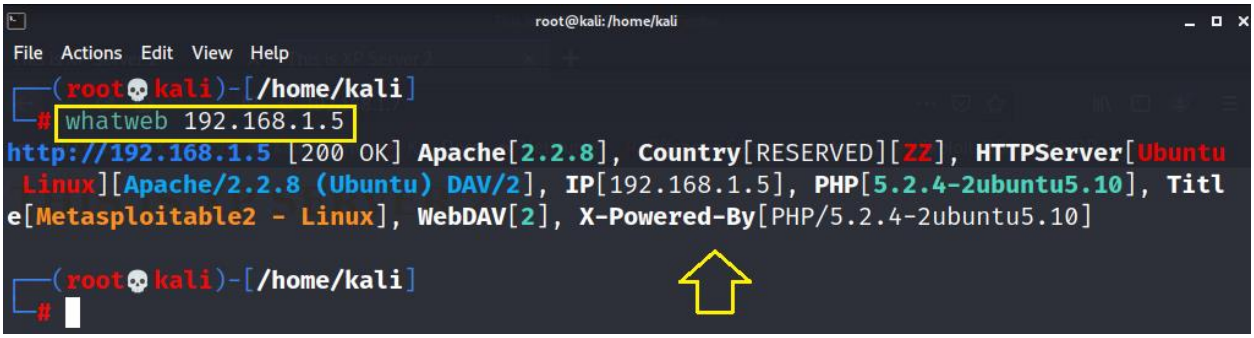


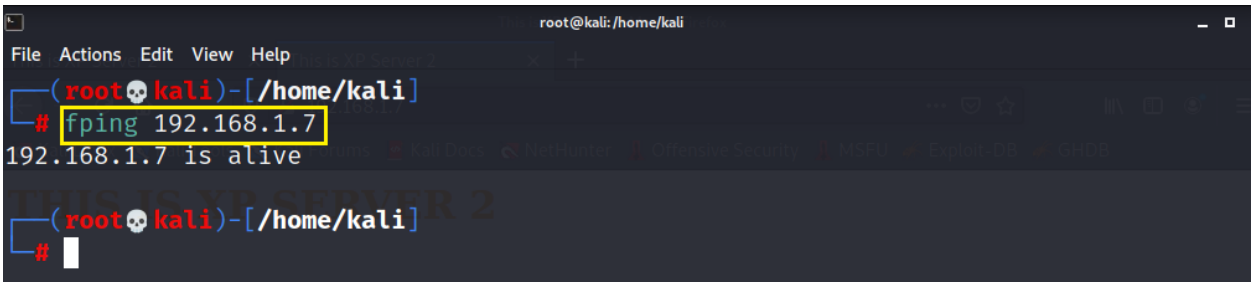


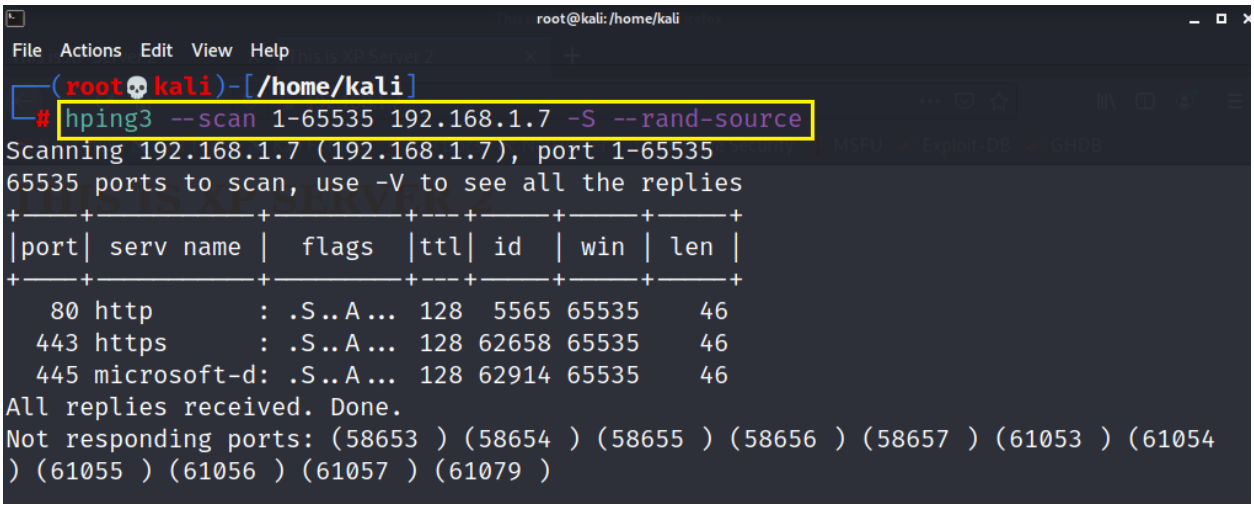

File Actions Edit View Help
nmap -O 192.168.1.7
130
Starting Nmap 7.91 (https://nmap.org) at 2022-09-15 04:30 EDT
Nmap scan report for 192.168.1.7
Host is up (0.0063s latency).
Not shown: 993 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
MAC Address: AA:AA:AA:AA:AA:77 (Unknown)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop


File Actions Edit View Help
(root kali)-[/home/kali]
nmap -p 80 192.168.1.7
Starting Nmap 7.91 (https://nmap.org) at 2022-09-15 04:31 EDT
Nmap scan report for 192.168.1.7
Host is up (0.0049s latency).
PORT STATE SERVICE
80/tcp open http
MAC Address: AA:AA:AA:AA:AA:77 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds


root@kali: /home/kali
File Actions Edit View Help
(root kali)-[/home/kali]
whatweb 192.168.1.7
2
http://192.168.1.7 [200 OK] Apache[2.4.4], Country[RESERVED][ZZ], HTTPServer[Windows (32 bit)][Apache/2.4.4 (Win32) OpenSSL/0.9.8y PHP/5.4.16], IP[192.168.1.7], OpenSSL[0.9.8y], PHP[5.4.16], Title[This is XP Server 2]
(root kali)-[/home/kali]
#

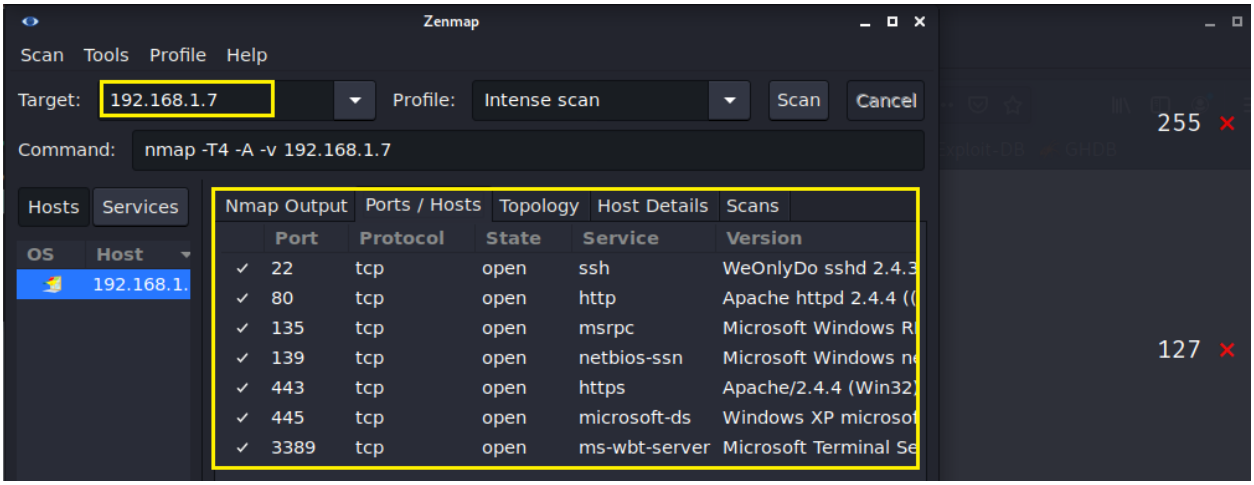

root@kali: /home/kali
File Actions Edit View Help
(root kali)-[/home/kali]
whatweb 192.168.1.5
http://192.168.1.5 [200 OK] Apache[2.2.8], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) DAV/2], IP[192.168.1.5], PHP[5.2.4-2ubuntu5.10], Title[Metasploitable2 - Linux], WebDAV[2], X-Powered-By[PHP/5.2.4-2ubuntu5.10]
(root kali)-[/home/kali]
#

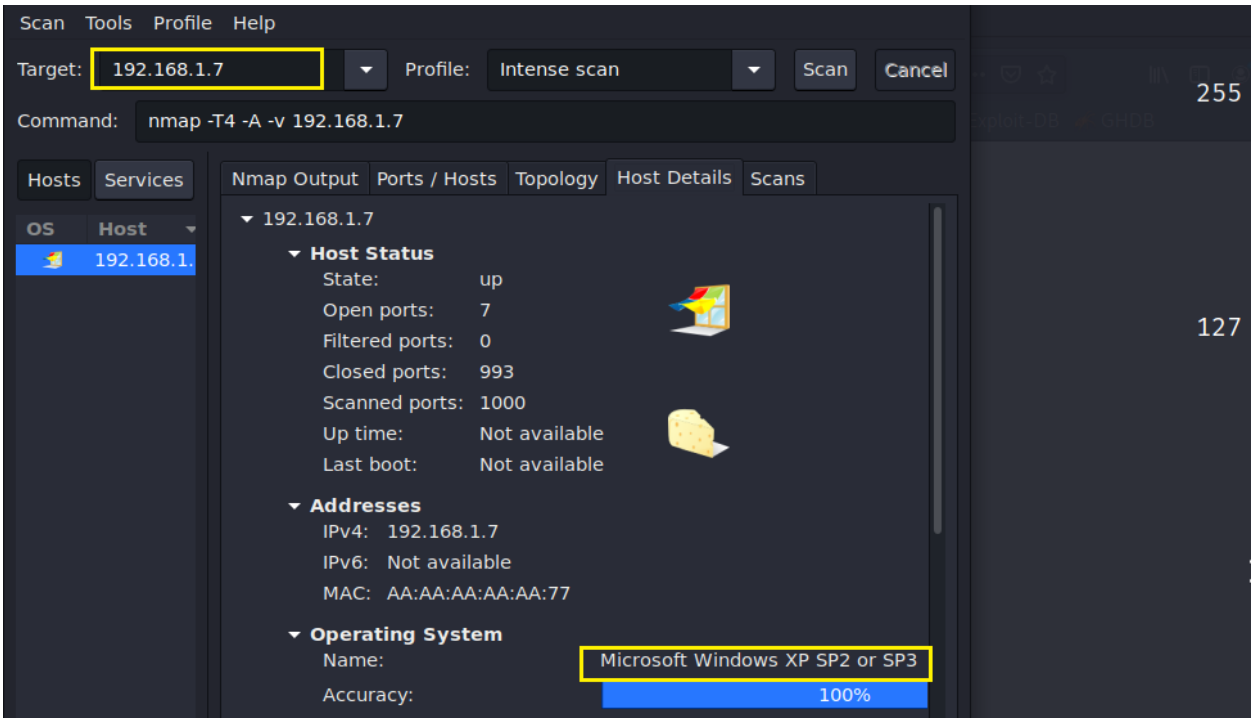

root@kali: /home/kali
File Actions Edit View Help
(root kali)-[/home/kali]
fping 192.168.1.7
192.168.1.7 is alive
(root kali)-[/home/kali]
#


root@kali: /home/kali
File Actions Edit View Help
(root kali)-[/home/kali]
hping3 --scan 1-65535 192.168.1.7 -S --rand-source
Scanning 192.168.1.7 (192.168.1.7), port 1-65535
65535 ports to scan, use -V to see all the replies
+----+------------+---------+---+-----+-----+-----+
|port| serv name | flags |ttl| id | win | len |
+----+------------+---------+---+-----+-----+-----+
80 http : .S..A... 128 5565 65535 46
443 https : .S..A... 128 62658 65535 46
445 microsoft-d: .S..A... 128 62914 65535 46
All replies received. Done.
Not responding ports: (58653) (58654) (58655) (58656) (58657) (61053) (61054) (61055) (61056) (61057) (61079)

```
File  Actions  Edit  View  Help
┌──(root💀kali)-[/home/kali]
└─# nmap -sV 192.168.1.7
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-15 05:02 EDT
Nmap scan report for 192.168.1.7
Host is up (0.013s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           WeOnlyDo sshd 2.4.3 (protocol 2.0)
80/tcp   open  http          Apache httpd 2.4.4 ((Win32) OpenSSL/0.9.8y PHP/5.4.16)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp  open  ssl/http      Apache httpd 2.4.4 ((Win32) OpenSSL/0.9.8y PHP/5.4.16)
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: AA:AA:AA:AA:AA:77 (Unknown)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:micro
soft:windows_xp
```

```
File  Actions  Edit  View  Help
┌──(root💀kali)-[/home/kali]
└─# nikto -host 192.168.1.7
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.7
+ Target Hostname:    192.168.1.7
+ Target Port:        80
+ Start Time:         2022-09-15 05:06:36 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.4 (Win32) OpenSSL/0.9.8y PHP/5.4.16
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agen
t to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to
render the content of the site in a different fashion to the MIME type
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easi
ly brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The
 following alternatives for 'index' were found: HTTP_NOT_FOUND.html.var, HTTP_NOT_F
OUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.htm
l.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, H
TTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_
FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.ht
ml.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var
+ OpenSSL/0.9.8y appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o
 and 0.9.8zc are also current.
+ Apache/2.4.4 appears to be outdated (current is at least Apache/2.4.37). Apache 2
```


Zenmap
Scan Tools Profile Help
Target: 192.168.1.7
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.1.7
Hosts
Services
OS
Host
192.168.1.
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Port
Protocol
State
Service
Version
22 tcp open ssh WeOnlyDo sshd 2.4.3
80 tcp open http Apache httpd 2.4.4 ((
135 tcp open msrpc Microsoft Windows R
139 tcp open netbios-ssn Microsoft Windows n
443 tcp open https Apache/2.4.4 (Win32)
445 tcp open microsoft-ds Windows XP microsof
3389 tcp open ms-wbt-server Microsoft Terminal Se
255
127


Scan Tools Profile Help
Target: 192.168.1.7
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.1.7
Hosts
Services
OS
Host
192.168.1.
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
192.168.1.7
Host Status
State: up
Open ports: 7
Filtered ports: 0
Closed ports: 993
Scanned ports: 1000
Up time: Not available
Last boot: Not available
Addresses
IPv4: 192.168.1.7
IPv6: Not available
MAC: AA:AA:AA:AA:AA:77
Operating System
Name: Microsoft Windows XP SP2 or SP3
Accuracy: 100%
255
127