

## **Phase 2. Identify Targets and Run Scans**

**Goal:** Identify the tools and techniques to be used to perform host discovery and enumeration.

**Procedure:** List out the tools you plan on using to perform network scans, the purpose for using them, and how you will use them. For example:

1. *Tool:* Nmap.

Purpose: Obtain information on hosts and the services and operating systems they are running.

*Commands:* <[List commands to be used for identifying live hosts, banner grabbing, OS fingerprinting, open ports, etc.](#)>

**Deliverable:** Provide a minimum 2-page description of the tools you plan on using for the network scans, your reasoning for selecting them, and how they will be used. Be sure to include any challenges and potential drawbacks or limitations. Deliverable should cover at least 5 tools/resources.

**Course content reference:** There are two optional labs, [Reconnaissance from the WAN](#) and [Scanning the Network on the LAN](#), that may help you with this step.

**NOTE:** Kali is **not** a tool; it is a Linux distribution or collection of tools, so do not include it in your list.

# **SOLUTION**

All of these tools are beneficial to scan the target network. The 5 tools that I chose are: Nmap, Wireshark, Zenmap, Metasploit, and OpenVAS.

## **1. Nmap**

- a. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. The primary objective of Nmap is to scan an entire network or single host rapidly. Nmap sends raw IP packets in a unique way to detect the hosts available on the network system. It can also detect the services which are being offered by these hosts, their operating system, and a bunch of other characteristics.
- b. **Benefits of Nmap include:**
  - i. It can discover the host connected to the network.
  - ii. It can discover the free ports on the target host.
  - iii. It can detect all the services running on the host along with the operating system and version.
  - iv. It can detect any loopholes or potential vulnerabilities in the Network system.
  - v. It can be used for auditing the Network system as it can detect the new servers.
  - vi. It can search subdomain and Domain Name system queries
  - vii. With the help of the Nmap scripting engine (NSE), interaction can be made with the target host.
  - viii. It can determine the nature of the service that the host is performing, like whether the host is a mail service or a web server or so on.
- c. **Drawbacks/limitations of Nmap**
  - i. The standard Nmap utility is that it does not come with a graphical user interface.
  - ii. Can be blocked by firewalls
  - iii. Can be blocked by antivirus software
  - iv. Port scan may trigger HIDS or IDS/IPS software
- d. **Commands**
  - i. Live host scan
  - ii. Port scan
  - iii. OS fingerprinting
  - iv. Banner Grabbing

## **2. Wireshark**

- a. Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Wireshark's core features include: capture live packet data, Import packets from text files, view packet data and protocol information, save captured packet data, display packets, filter packets, search packets, colorize packets and generate statistics. However, for the purposes of this assignment, we're only going to focus

on the following features: identifying hosts, services, port identification, and communication patterns.

**b. Benefits of Wireshark**

- i. With wireshark, you can see details about the packets coming in and going out your network card. This allows you to understand what other devices your computer is talking to, and what they are sending between each other.

**c. Drawbacks/limitations of Wireshark**

- i. Cannot run outside of the network
- ii. The packets are copied so another user cannot know that they are being monitored

**d. Commands**

- i. Live host scan
- ii. Port scan
- iii. OS fingerprinting
- iv. Banner Grabbing

**3. Zenmap**

- a. Zenmap is a graphical user interface (GUI) for Nmap, a free and open-source network scanning tool. It simplifies using Nmap by providing a user-friendly interface and additional features that enhance the scanning experience.

**b. Benefits of Zenmap**

- i. User-friendly graphical interface, provides a more accessible option for less experienced users

**c. Drawbacks/limitations of Zenmap**

- i. Nmap, the original command-line tool, offers extensive functionality and flexibility for advanced users; not so much as Zenmap.

**d. Commands**

- i. Live host scan
- ii. Port scan
- iii. OS fingerprinting
- iv. Banner Grabbing

**4. Metasploit**

- a. The Metasploit framework is a penetration testing tool for exploiting and validating vulnerabilities. It includes the fundamental architecture, particular content, and tools required for penetration testing and extensive security evaluation. It is a well-known exploitation framework that is routinely updated; new exploits are included as soon as they are announced.

**b. Benefits of Metasploit**

- i. Metasploit can run the same checks and scans from Nmap. This stage occurs first before developing and executing an exploit code.

**c. Drawbacks/limitations of Metasploit**

- i. Metasploit can be noisy and easily detected by security solutions, making it difficult to establish persistence on compromised systems

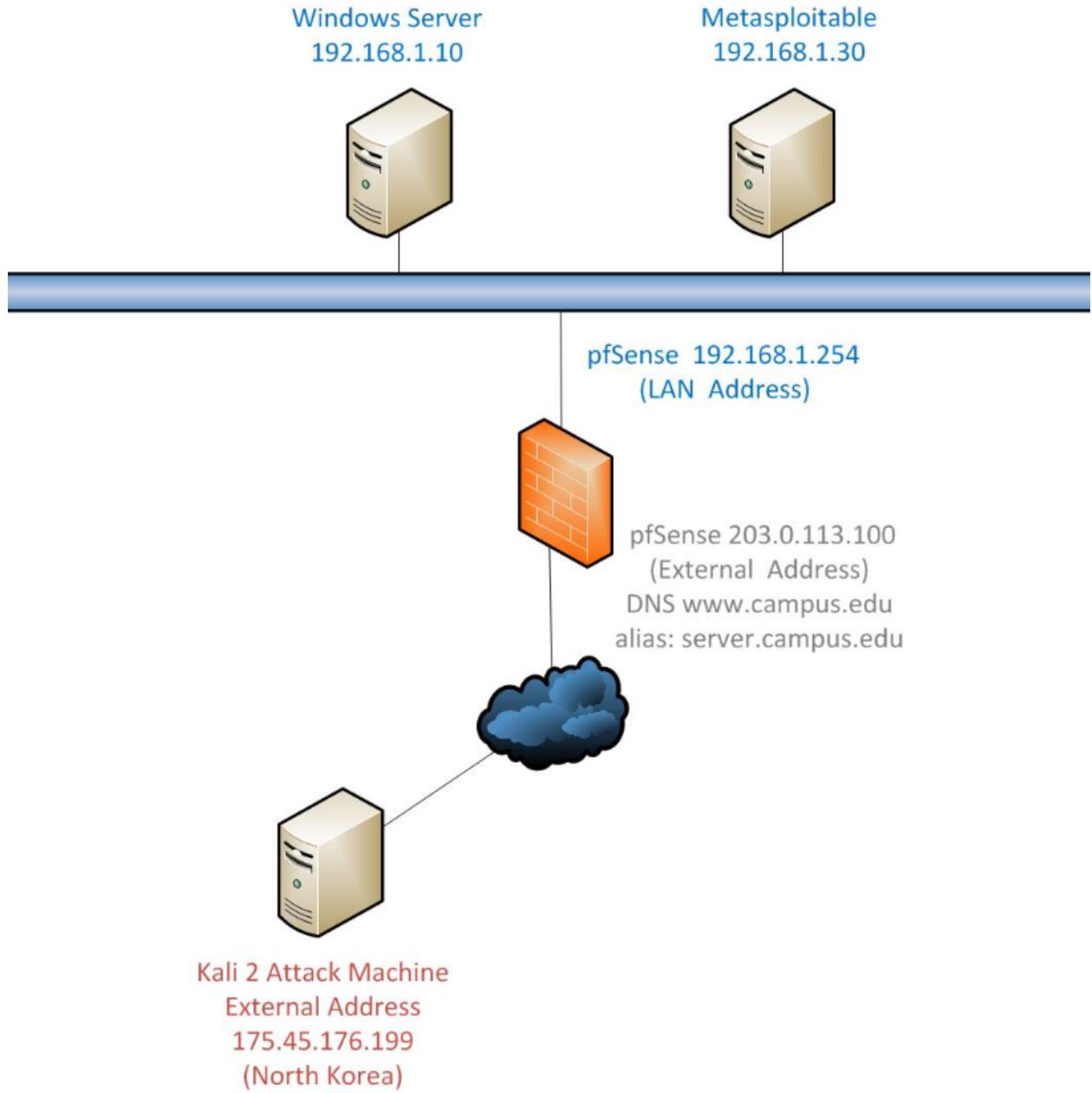
**d. Commands**

- i. Live host scan
- ii. Port scan

- iii. OS fingerprinting
- iv. Banner Grabbing

## 5. OpenVAS

- a. OpenVAS is a system vulnerability scanner that checks visible ports, services it can access for known exploits, and high level web threats. OpenVAS is an application firewall that web servers use to prevent unauthorized access to websites or servers.
- b. **Benefits of OpenVas**
  - i. Web-based GUI
- c. **Drawbacks/limitations of OpenVAS**
  - i. Not very accurate and contains many false–positives
- d. **Commands**
  - i. Live host scan
  - ii. Port scan
  - iii. OS fingerprinting
  - iv. Banner Grabbing



## 1. Nmap

### a. Finding live hosts in your network

- i. Example - # nmap -sP www.campus.edu
  - a. # nmap -sn www.campus.edu (sn = disable port)

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

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-07-07 00:21 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00050s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
root@kali2:~# nmap -sn www.campus.edu

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-07-07 00:21 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00039s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

n

b. Open ports

i. Example - # nmap www.campus.edu

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

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-07-07 00:21 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00046s 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

1. Nmap done: 1 IP address (1 host up) scanned in 21.96 seconds
```

c. OS Fingerprinting

i. Example - \$nmap -O [www.campus.edu](http://www.campus.edu)

```

root@kali2:~# nmap -O www.campus.edu

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-07-07 00:25 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00037s 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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running (JUST GUESSING): Microsoft Windows 2008|Phone|7|Vista (96%)
OS CPE: cpe:/o:microsoft:windows_server_2008::beta3 cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_7:::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_vista:::- cpe:/o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows Server 2008 or 2008 Beta 3 (96%), Microsoft Windows Phone 7.5 or 8.0 (89%), Windows Server 2008 R2 (89%), Microsoft Windows 7 Professional or Windows 8 (89%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (89%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (89%), Microsoft Windows 7 (88%), Microsoft Windows Server 2008 (86%), Microsoft Windows Server 2008 R2 or
ii.

Windows 8 (86%), Microsoft Windows 7 SP1 (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
iii.  Nmap done: 1 IP address (1 host up) scanned in 21.23 seconds

```

#### d. Banner Grabbing

- i. First we need to determine which ports are open \$nmap [www.campus.edu](http://www.campus.edu)

```

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

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-07-06 23:41 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00042s 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  closed rmiregistry
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
5432/tcp  open  postgresql
8180/tcp  closed sampleflag:999818

1. Nmap done: 1 IP address (1 host up) scanned in 18.62 seconds

```

```
root@kali2:~# nmap -sV --script=banner www.campus.edu

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-07-07 00:05 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00043s latency).
Not shown: 989 filtered ports
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              Microsoft ftpd
|_banner: 220 Microsoft FTP Service
23/tcp    open  telnet?
25/tcp    open  smtp             hMailServer smtpd
|_banner: 220 SERVER ESMTP
80/tcp    open  http             Apache httpd 2.2.14 ((Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1 )
|_http-server-header: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
110/tcp   open  pop3            hMailServer pop3d
|_banner: +OK POP3
443/tcp   open  ssl/http        Apache httpd 2.2.14 (DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1 )
|_http-server-header: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
1099/tcp  open  rmiregistry     GNU Classpath grmiregistry
3306/tcp  open  mysql           MySQL 5.0.51a-3ubuntu5
|_banner: >\x00\x00\x00\x0A5.0.51a-3ubuntu5\x00\x08\x00\x00\x00YcgYi%F\x
|_00,\xA4\x08\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00...
3389/tcp  open  ssl/ms-wbt-server?
5432/tcp  open  postgresql      PostgreSQL DB 8.3.0 - 8.3.7
```

2.

```
8180/tcp open  http          Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: SERVER, localhost; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org
/
Nmap done: 1 IP address (1 host up) scanned in 173.72 seconds
```

3.

e. Port Range

- i. Example - # nmap [www.campus.edu](http://www.campus.edu) -p <range>

```
root@kali2:~# nmap www.campus.edu -p 1-100
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-07-07 00:33 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00042s latency).
Not shown: 96 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 2.07 seconds
```

1.

## 2. Wireshark

#### a. Finding live hosts in your network

- i. First you will ping another host in your network. In my virtual network, my host IP address is 10.1.1.4 and I wish to ping 10.1.1.6.
  - ii. Example = “Ping 10.1.1.6”

```
C:\Users\ifyou>ping 10.1.1.6

Pinging 10.1.1.6 with 32 bytes of data:
Reply from 10.1.1.6: bytes=32 time=3ms TTL=128
Reply from 10.1.1.6: bytes=32 time=4ms TTL=128
Reply from 10.1.1.6: bytes=32 time=2ms TTL=128
Reply from 10.1.1.6: bytes=32 time=1ms TTL=128

Ping statistics for 10.1.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms
```

iii.

## b. Open Ports

- i. On the Statistics Tab, when you go to the Endpoints tab, you can inspect the UDP and TCP connections and all the open ports that are being utilized.

Endpoint Settings		Ethernet · 2	IPv4 · 49	IPv6	TCP · 106	UDP · 28			
	Protocol	Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
<input type="checkbox"/>	Name resolution	3.225.14.251	443	52	24.877 KiB	27	20.960 KiB	25	3.917
<input type="checkbox"/>	Limit to display filter	3.229.52.221	443	102	31.160 KiB	49	16.233 KiB	53	14.927
<input checked="" type="checkbox"/>	Ethernet	3.231.143.7	443	18	7.051 KiB	9	5.252 KiB	9	1.799
<input type="checkbox"/>	Bluetooth	3.234.97.112	443	22	12.137 KiB	11	6.262 KiB	11	5.875
<input type="checkbox"/>	DCCP	8.28.7.82	443	42	14.616 KiB	19	10.646 KiB	23	3.970
<input type="checkbox"/>	FC	10.1.1.4	61519	5	313 bytes	2	108 bytes	3	205 bytes
<input type="checkbox"/>	FDDI	10.1.1.4	61520	92	19.373 KiB	54	10.068 KiB	38	9.305
<input type="checkbox"/>	IEEE 802.11	10.1.1.4	61521	5	282 bytes	3	162 bytes	2	120 bytes
<input type="checkbox"/>	IEEE 802.15.4	10.1.1.4	61522	25	7.881 KiB	14	2.118 KiB	11	5.763
<input checked="" type="checkbox"/>	IPv4	10.1.1.4	61523	25	9.683 KiB	13	1.871 KiB	12	7.812
<input checked="" type="checkbox"/>	IPv6	10.1.1.4	61524	17	6.440 KiB	9	1.054 KiB	8	5.387
<input type="checkbox"/>	Filter list for specific type	10.1.1.4	61525	17	6.430 KiB	9	1.054 KiB	8	5.376
<input type="checkbox"/>		10.1.1.4	61526	25	12.123 KiB	12	1.770 KiB	13	10.354
<input type="checkbox"/>		10.1.1.4	61527	23	9.721 KiB	12	1.928 KiB	11	7.793
<input type="checkbox"/>		10.1.1.4	61528	94	100.486 KiB	21	6.362 KiB	73	94.124
<input type="checkbox"/>		10.1.1.4	61529	19	7.696 KiB	9	1.054 KiB	10	6.643
<input type="checkbox"/>		10.1.1.4	61530	24	9.091 KiB	12	1.944 KiB	12	7.146
<input type="checkbox"/>		10.1.1.4	61531	360	459.539 KiB	43	7.439 KiB	317	452.100 KiB

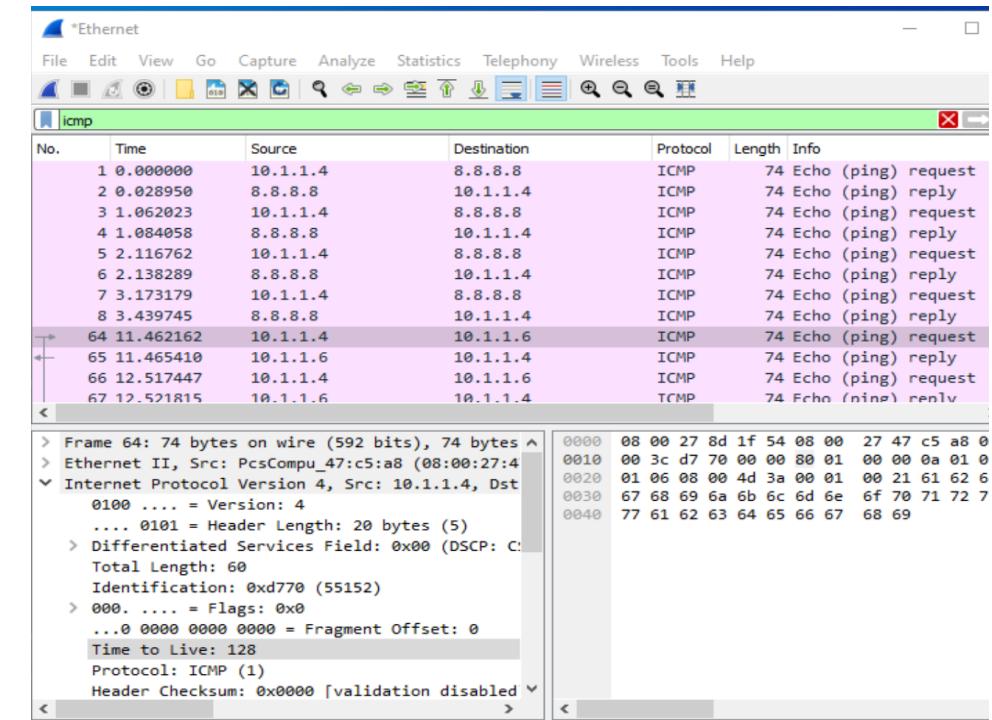
ii.

Endpoint Settings		Ethernet · 2	IPv4 · 49	IPv6	TCP · 106	UDP · 28			
	Protocol	Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
<input type="checkbox"/>	Name resolution	3.225.14.251	443	52	24.877 KiB	27	20.960 KiB	25	3.917
<input type="checkbox"/>	Limit to display filter	3.229.52.221	443	102	31.160 KiB	49	16.233 KiB	53	14.927
<input checked="" type="checkbox"/>	Ethernet	3.231.143.7	443	18	7.051 KiB	9	5.252 KiB	9	1.799
<input type="checkbox"/>	Bluetooth	3.234.97.112	443	22	12.137 KiB	11	6.262 KiB	11	5.875
<input type="checkbox"/>	DCCP	8.28.7.82	443	42	14.616 KiB	19	10.646 KiB	23	3.970
<input type="checkbox"/>	FC	10.1.1.4	61519	5	313 bytes	2	108 bytes	3	205 bytes
<input type="checkbox"/>	FDDI	10.1.1.4	61520	92	19.373 KiB	54	10.068 KiB	38	9.305
<input type="checkbox"/>	IEEE 802.11	10.1.1.4	61521	5	282 bytes	3	162 bytes	2	120 bytes
<input type="checkbox"/>	IEEE 802.15.4	10.1.1.4	61522	25	7.881 KiB	14	2.118 KiB	11	5.763
<input checked="" type="checkbox"/>	IPv4	10.1.1.4	61523	25	9.683 KiB	13	1.871 KiB	12	7.812
<input checked="" type="checkbox"/>	IPv6	10.1.1.4	61524	17	6.440 KiB	9	1.054 KiB	8	5.387
<input type="checkbox"/>	Filter list for specific type	10.1.1.4	61525	17	6.430 KiB	9	1.054 KiB	8	5.376
<input type="checkbox"/>		10.1.1.4	61526	25	12.123 KiB	12	1.770 KiB	13	10.354
<input type="checkbox"/>		10.1.1.4	61527	23	9.721 KiB	12	1.928 KiB	11	7.793
<input type="checkbox"/>		10.1.1.4	61528	94	100.486 KiB	21	6.362 KiB	73	94.124
<input type="checkbox"/>		10.1.1.4	61529	19	7.696 KiB	9	1.054 KiB	10	6.643
<input type="checkbox"/>		10.1.1.4	61530	24	9.091 KiB	12	1.944 KiB	12	7.146
<input type="checkbox"/>		10.1.1.4	61531	360	459.539 KiB	43	7.439 KiB	317	452.100 KiB

iii.

## c. OS Fingerprinting

- i. Line 64 and Internet Protocol Version 4 - Time to Live - 128. This chart shows the best guess is that this is a Windows based on OS



ii.

Operating System (OS)	Time To Live	TCP Window Size
Linux (Kernel 2.4 and 2.6) <sup>1</sup>	64	5840
Google Linux	64	5720
FreeBSD	64	65535
OpenBSD	64	16384
Windows 95	32	8192
Windows 2000	128	16384
Windows XP	128	65535
Windows 98, Vista and 7 (Server 2008)	128	8192
IOS 12.4 (Cisco Routers)	255	4128
Solaris 7	255	8760
AIX 4.3	64	16384

iii.

#### d. Banner Grabbing

- i. We can initiate a capture and then we can filter the “http” protocol and in the middle pane, we could get the banner on the Hypertext Transfer Protocol tab

ii.

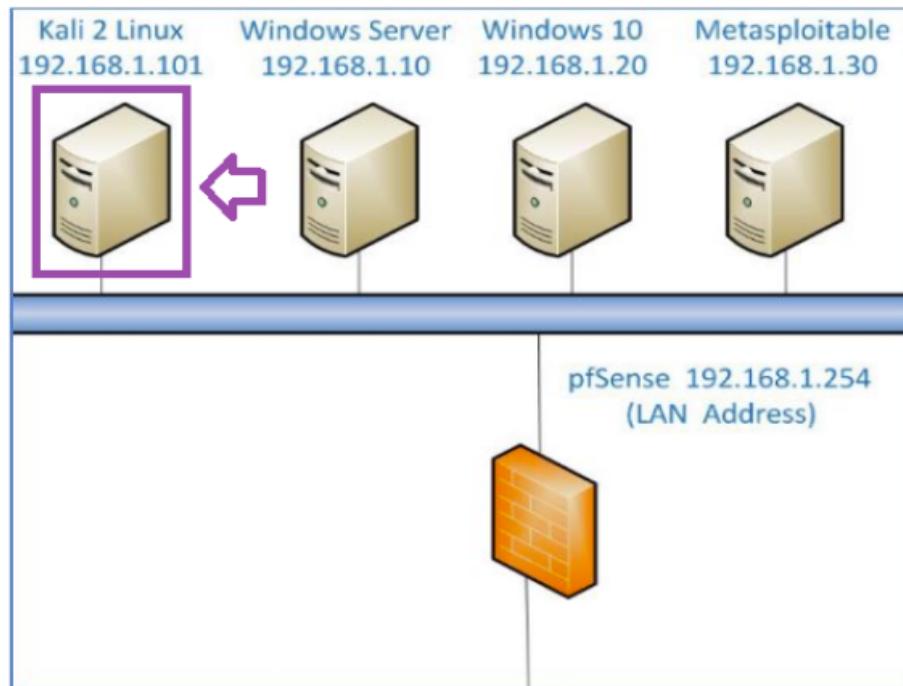
No.	Time	Source	Destination	Protocol	Length	Info
5609	78.109702	10.1.1.4	34.104.35.123	HTTP	333	HEAD /edged1/release2/
5612	78.466540	10.1.1.4	34.104.35.123	HTTP	384	GET /edged1/release2/c
5667	78.562124	34.104.35.123	10.1.1.4	HTTP	415	HTTP/1.1 200 OK
6455	92.887494	10.1.1.4	34.104.35.123	HTTP	355	HEAD /edged1/release2/
6457	92.913036	34.104.35.123	10.1.1.4	HTTP	644	HTTP/1.1 200 OK
6459	93.064958	10.1.1.4	34.104.35.123	HTTP	406	GET /edged1/release2/c
6468	93.092349	34.104.35.123	10.1.1.4	HTTP	844	HTTP/1.1 200 OK
9260	112.538402	10.1.1.4	34.104.35.123	HTTP	351	HEAD /edged1/release2/
9274	112.703351	10.1.1.4	34.104.35.123	HTTP	402	GET /edged1/release2/c
164...	142.233354	34.104.35.123	10.1.1.4	HTTP	1109	HTTP/1.1 200 OK
5610	78.136890	34.104.35.123	10.1.1.4	TCP	644	HTTP/1.1 200 OK [TCP
9261	112.564123	34.104.35.123	10.1.1.4	TCP	646	HTTP/1.1 200 OK ]TCP

```

> Transmission Control Protocol, Src Port: 80, Ds ^ 
> [8 Reassembled TCP Segments (11010 bytes): #646 
< Hypertext Transfer Protocol 
  > HTTP/1.1 200 OK\r\n 
    accept-ranges: bytes\r\n 
    content-disposition: attachment\r\n 
    content-security-policy: default-src 'none'\r\n 
    server: Google-Edge-Cache\r\n 
    <server: Google-Edge-Cache\r\n> 
    x-content-type-options: nosniff\r\n 
    x-frame-options: SAMEORIGIN\r\n 
    x-xss-protection: 0\r\n 
    x-request-id: aad27800-327a-46ea-8d3b-e3a5d9: 
< > 
0010 03 3e 82 bb 00 00 ff 06 e5 16 22 68 23 7b 6^ 
0020 01 04 00 50 f3 70 00 53 15 07 c4 e2 5a c4 5^ 
0030 7b 12 60 b6 00 00 11 5e b0 c7 d9 78 98 3b 8^ 
0040 0a d9 71 12 de 81 15 52 42 c5 0b e4 3d bd 7^ 
0050 ca 34 04 81 26 b4 dc d5 52 de e0 e4 1a fb 6^ 
0060 b0 58 aa a4 9c 53 69 40 7a c7 f8 a7 98 d7 e^ 
0070 5b 20 b3 2e 76 dd 88 96 8a b4 95 9e dd d6 6^ 
0080 c4 2e b4 1f 47 fe 89 45 bd 53 a4 a9 02 fd 9^ 
0090 80 d0 ad 37 fb a9 4e 6a 76 c7 ef 15 56 e0 1^ 
00a0 57 05 cd 3d 73 ca 99 97 f7 8e 0b 66 92 86 6^ 
00b0 db 60 aa 90 3d b9 99 b1 b6 ad 89 c3 24 54 8^ 
00c0 2f 9f 3f 62 77 e8 f5 e2 68 c7 d3 0b 97 53 3^ 
00d0 43 de 5a f9 fe 50 d4 19 d5 91 9b b1 2c 94 1^ 
< > 
Frame (844 bytes) Reassembled TCP (11010 bytes) 
|| Packets: 19047 · Displayed: 12 (0.1%) Profile: Default 

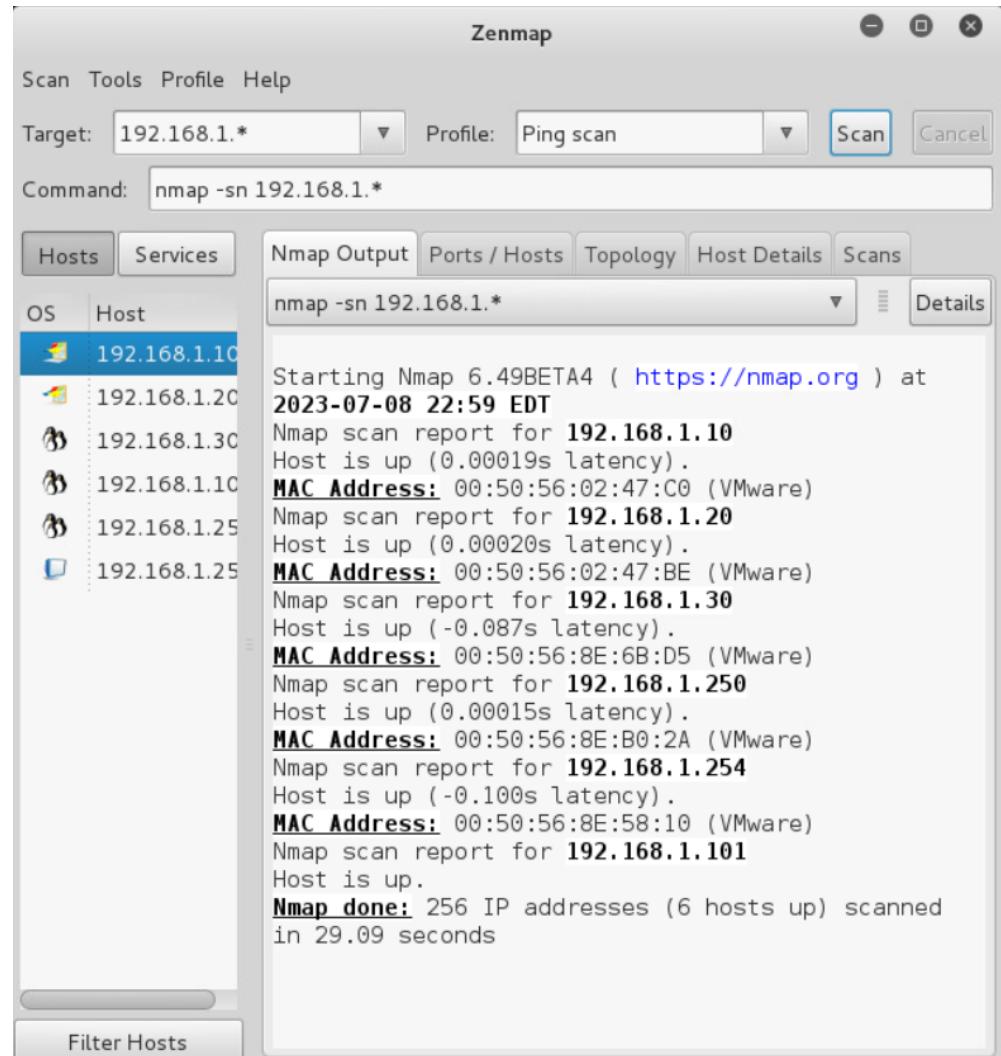
```

### 3. Zenmap



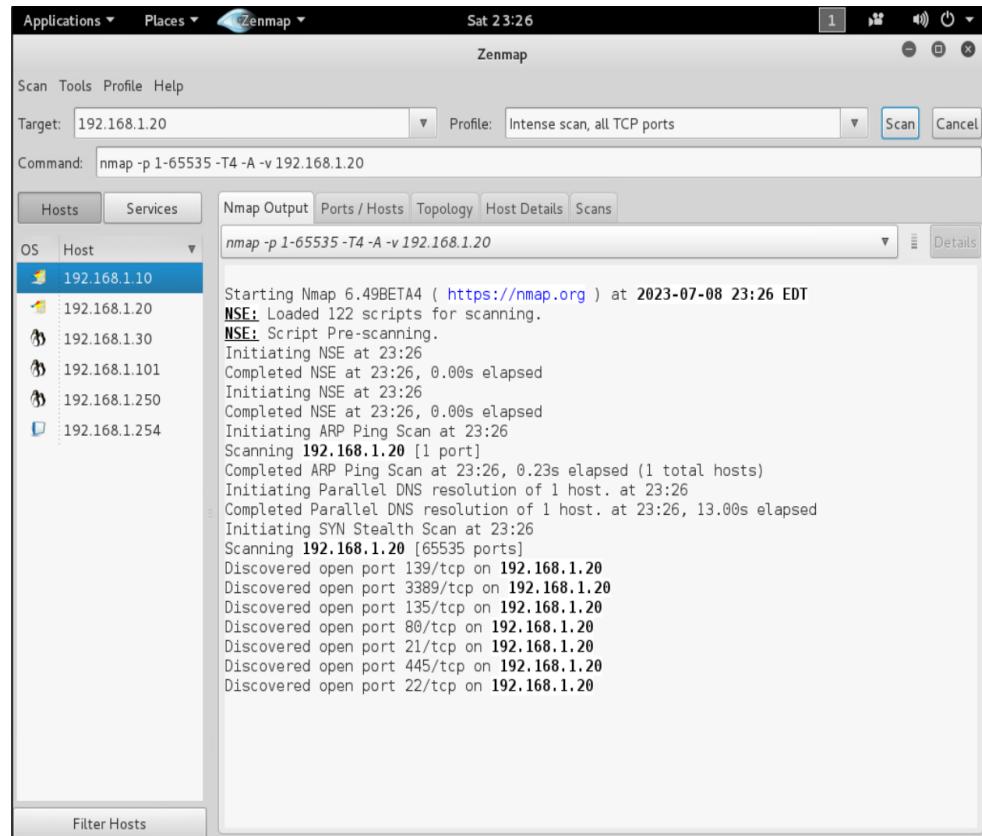
a.

b. **Finding live hosts in your network**



c. Open Ports

i.



ii.

#### d. OS Fingerprinting

Applications ▾ Places ▾ Zenmap ▾ Sat 23:44

Zenmap

Scan Tools Profile Help

Target: 192.168.1.20 Profile: Scan Cancel

Command: nmap -O 192.168.1.20

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

nmap -O 192.168.1.20

OS Host

OS	Host
	192.168.1.10
	192.168.1.20
	192.168.1.30
	192.168.1.101
	192.168.1.250
	192.168.1.254

Starting Nmap 6.49BETA4 ( <https://nmap.org> ) at 2023-07-08 23:29 EDT  
 Nmap scan report for 192.168.1.20  
 Host is up (0.00011s latency).  
**Not shown:** 992 filtered ports  
 PORT STATE SERVICE  
 21/tcp open ftp  
 22/tcp open ssh  
 80/tcp open http  
 135/tcp open msrpc  
 139/tcp open netbios-ssn  
 445/tcp open microsoft-ds  
 3389/tcp open ms-wbt-server  
 5357/tcp open wsdapi  
**MAC Address:** 00:50:56:02:47:BE (VMware)  
**Warning:** OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
**Device type:** general purpose|phone  
 Running (JUST GUESSING): Microsoft Windows 7|8|Vista|2008|Phone (93%)  
**OS CPE:** cpe:/o:microsoft:windows\_7:::-professional cpe:/o:microsoft:windows\_8 cpe:/o:microsoft:windows\_vista:::- cpe:/o:microsoft:windows\_vista:::sp1 cpe:/o:microsoft:windows\_server\_2008:::sp1 cpe:/o:microsoft:windows  
**Aggressive OS guesses:** Microsoft Windows 7 Professional or Windows 8 (93%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (93%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (91%), Microsoft Windows 7 (90%), Microsoft Windows Phone 7.5 or 8.0 (90%), Windows Server 2008 R2 (89%), Microsoft Windows Server 2008 R2 (88%), Microsoft Windows Server 2008 SP1 (88%), Microsoft Windows Vista SP0 - SP1 (87%), Microsoft Windows 7 SP 1 (86%)  
 No exact OS matches for host (test conditions non-ideal).

i. Filter Hosts

Network Distance: 1 hop  
 OS detection performed. Please report any incorrect results at <https://nmap.org/submit/>.  
**Nmap done:** 1 IP address (1 host up) scanned in 26.64 seconds

ii. Filter Hosts

Zenmap

Scan Tools Profile Help

Target: www.campus.edu Profile: Scan Cancel

Command: nmap -O www.campus.edu

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

www.campus.

```

Starting Nmap 6.49BETA4 ( https://nmap.org ) at
2023-07-08 02:46 EDT
Nmap scan report for www.campus.edu
(203.0.113.100)
Host is up (0.00028s latency).
Not shown: 990 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
8180/tcp  open  sampleflag:999818
Warning: OSScan results may be unreliable
because we could not find at least 1 open and 1
closed port
Aggressive OS guesses: HP 4000M ProCurve switch
(J4121A) (95%), Tomato 1.27 - 1.28 (Linux
2.4.20) (93%), Linux 2.6.18 - 2.6.22 (92%), D-
Link DWL-624+ or DWL-2000AP, or TRENDnet
TEW-432BRP WAP (90%), AVtech Room Alert 26W
environmental monitor (89%), Microsoft Windows

```

Filter Hosts

iii.

Server 2008 or 2008 Beta 3 (86%), Microsoft
Windows Vista Home Premium SP1 (86%)
No exact OS matches for host (test conditions
non-ideal).

OS detection performed. Please report any
incorrect results at <https://nmap.org/submit/>.
Nmap done: 1 IP address (1 host up) scanned in
34.15 seconds

Filter Hosts

iv.

#### e. Banner Grabbing

Applications ▾ Places ▾ Zenmap ▾ Sun 00:02

Scan Tools Profile Help

Target: 192.168.1.20 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.1.20

**Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans**

OS	Host	Port	Protocol	State	Service	Version
	192.168.1.10	21	tcp	open	ftp	Microsoft ftpd
	192.168.1.20	22	tcp	open	tcpwrapped	
	192.168.1.30	80	tcp	open	http	Microsoft IIS httpd 10.0
	192.168.1.101	135	tcp	open	msrpc	Microsoft Windows RPC
	192.168.1.250	139	tcp	open	netbios-ssn	Microsoft Windows 98 netbios-ssn
	192.168.1.254	445	tcp	open	microsoft-ds	(primary domain: WORKGROUP)
		3389	tcp	open	ms-wbt-server	
		5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
		1539	tcp	open	msrpc	Microsoft Windows RPC

i. Filter Hosts

ii.

#### 4. Metasploit

##### a. Finding live hosts in your network

```
http://metasploit.pro

Taking notes in notepad? Have Metasploit Pro track & report
your progress and findings -- learn more on http://rapid7.com/metasploit

=[ metasploit v4.11.5-2016010401 ]]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post      ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops        ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > nmap -sn www.campus.edu
[*] exec: nmap -sn www.campus.edu

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-07-08 03:04 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00032s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

i.

**b. Open Ports**

```
msf > nmap www.campus.edu
[*] exec: nmap www.campus.edu

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-07-09 01:01 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00051s 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

i.  Nmap done: 1 IP address (1 host up) scanned in 5.12 seconds
```

**c. OS Fingerprinting**

```
msf > nmap -O www.campus.edu
[*] exec: nmap -O www.campus.edu

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-07-08 03:08 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00035s 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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running (JUST GUESSING): Microsoft Windows 2008|Phone|7|Vista (96%)
OS CPE: cpe:/o:microsoft:windows_server_2008::beta3 cpe:/o:microsoft:windows_server_2008 cp
e:/o:microsoft:windows cpe:/o:microsoft:windows_7:::-:professional cpe:/o:microsoft:windows_
```

i.

```

8 cpe:/o:microsoft:windows_vista:: - cpe:/o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows Server 2008 or 2008 Beta 3 (96%), Microsoft Windows Phone 7.5 or 8.0 (89%), Windows Server 2008 R2 (89%), Microsoft Windows 7 Professional or Windows 8 (89%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (89%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (89%), Microsoft Windows 7 (88%), Microsoft Windows Server 2008 (86%), Microsoft Windows Server 2008 R2 or Windows 8 (86%), Microsoft Windows 7 SP1 (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.65 seconds
msf > 

```

#### d. Banner Grabbing

```

msf > nmap -sV -T4 -O -F --version-light www.campus.edu
[*] exec: nmap -sV -T4 -O -F --version-light www.campus.edu

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-07-08 03:11 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00046s latency).
Not shown: 91 filtered ports
PORT      STATE SERVICE          VERSION
21/tcp     open  ftp              Microsoft ftptd
23/tcp     open  telnet?
25/tcp     open  smtp             hMailServer smptd
80/tcp     open  http             Apache httpd 2.2.14 ((Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
110/tcp    open  pop3            hMailServer pop3d
443/tcp    open  ssl/http        Apache httpd 2.2.14 (DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
3306/tcp   open  mysql           MySQL 5.0.51a-Ubuntu5
3389/tcp   open  ssl/ms-wbt-server?
5432/tcp   open  postgresql       PostgreSQL DB 8.3.0 - 8.3.7
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|WAP
Running (JUST GUESSING): Microsoft Windows 2008|Vista|7|Phone (94%), FreeBSD 6.X (87%), AirSpan embedded (85%)
OS CPE: cpe:/o:microsoft:windows_server_2008::beta3 cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_vista:: - cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_cpe:/o:microsoft:windows_8 cpe:/o:freebsd:freebsd:6.3
Aggressive OS guesses: Microsoft Windows Server 2008 or 2008 Beta 3 (94%), Microsoft Window

```

i.

```

s Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (89%), Microsoft Windows Phone 7.5 or 8.0 (88%), Windows Server 2008 R2 (87%), Microsoft Windows 7 Professional or Windows 8 (87%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (87%), FreeBSD 6.3-RELEASE (87%), Microsoft Windows Server 2008 SP1 (87%), Microsoft Windows 7 (86%), AirSpan ProST WiMAX access point (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Hosts: SERVER, localhost; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.82 seconds
msf > 

```

### 5. OpenVAS

#### a. Finding live hosts in your network

 Greenbone Security Assistant	Logged in as Admin admin   Logout											
	Sun Jul 9 02:39:15 2023 UTC											
<a href="#">Scan Management</a> <a href="#">Asset Management</a> <a href="#">SecInfo Management</a> <a href="#">Configuration</a> <a href="#">Extras</a> <a href="#">Administration</a> <a href="#">Help</a>												
<b>Report: Hosts 1 - 1 of 1 (total: 1)</b> <a href="#">?</a> <a href="#">PDF</a> <a href="#">Done</a>												
Filter: <input checked="" type="checkbox"/> All results <a href="#">sort-reverse=severity result_hosts_only=1 min_cvss_base= levels=hmlg</a> <a href="#">?</a>												
Host	OS	Ports	Apps	Distance	Start	End	High	Medium	Low	Log	False Pos.	Total
203.0.113.100		10	6	1	Jul 9, 02:25:19	Jul 9, 02:38:35	8	19	5	40	0	72
Total: 1							8	19	5	40	0	72

i.

## b. Open Ports

 Greenbone Security Assistant	Logged in as Admin admin   Logout		
	Sun Jul 9 02:42:30 2023 UTC		
<a href="#">Scan Management</a> <a href="#">Asset Management</a> <a href="#">SecInfo Management</a> <a href="#">Configuration</a> <a href="#">Extras</a> <a href="#">Administration</a> <a href="#">Help</a>			
<b>Report: Ports 1 - 10 of 10 (total: 10)</b> <a href="#">?</a> <a href="#">PDF</a> <a href="#">Done</a>			
Filter: <input checked="" type="checkbox"/> All results <a href="#">sort-reverse=severity result_hosts_only=1 min_cvss_base= levels=hmlg</a> <a href="#">?</a>			
Port	IANA	Hosts	Severity
21/tcp		1	0.0
23/tcp		1	0.0
25/tcp		1	0.0
80/tcp		1	10.0
110/tcp		1	0.0
443/tcp		1	10.0
1099/tcp		1	0.0
3306/tcp		1	0.0
3389/tcp		1	5.0
5432/tcp		1	8.5

i.

## c. OS Fingerprinting

 Greenbone Security Assistant	Logged in as Admin admin   Logout		
	Sun Jul 9 02:43:18 2023 UTC		
<a href="#">Scan Management</a> <a href="#">Asset Management</a> <a href="#">SecInfo Management</a> <a href="#">Configuration</a> <a href="#">Extras</a> <a href="#">Administration</a> <a href="#">Help</a>			
<b>Report: Operating Systems 1 - 1 of 1 (total: 1)</b> <a href="#">?</a> <a href="#">PDF</a> <a href="#">Done</a>			
Filter: <input checked="" type="checkbox"/> All results <a href="#">sort-reverse=severity result_hosts_only=1 min_cvss_base= levels=hmlg</a> <a href="#">?</a>			
Operating System	CPE	Hosts	Severity
HP JetDirect [possible conflict]	cpe:/h:hp:jetdirect	1	10.0 (High)

i.

**Result Details**   

Task: Immediate scan of IP 203.0.113.100 ID: 997c8f64-203a-472a-be6d-13c1a7acbb0e

Vulnerability	Severity	Host	Location	Actions
OS fingerprinting	0.0 (Log)	203.0.113.100	general/tcp	 

**Summary**  
This script performs ICMP based OS fingerprinting (as described by Ofir Arkin and Fyodor Yarochkin in Phrack #57). It can be used to determine remote operating system version.

**Vulnerability Detection Result**  
ICMP based OS fingerprint results: (91% confidence)  
FreeBSD  
HP JetDirect

**Log Method**  
Details: OS fingerprinting (OID: 1.3.6.1.4.1.25623.1.0.102002)  
Version used: \$Revision: 43 \$

**References**  
Other: <http://www.phrack.org/issues.html?issue=57&id=7#article>

ii.

#### d. Banner Grabbing

 **Greenbone**  
Security Assistant Logged in as Admin admin | Logout  
Sun Jul 9 02:45:46 2023 UTC

[Scan Management](#) [Asset Management](#) [SecInfo Management](#) [Configuration](#) [Extras](#) [Administration](#) [Help](#)

**Result Details**   

Task: Immediate scan of IP 203.0.113.100 ID: 0f5a0e1b-7a21-4ae3-82e3-ed0ba3075b82

Vulnerability	Severity	Host	Location	Actions
FTP Banner Detection	0.0 (Log)	203.0.113.100	21/tcp	 

**Summary**  
This Plugin detects the FTP Server Banner

**Vulnerability Detection Result**  
Remote FTP server banner :  
220 Microsoft FTP Service

**Log Method**  
Details: [FTP Banner Detection \(OID: 1.3.6.1.4.1.25623.1.0.10092\)](#)  
Version used: \$Revision: 563 \$

i.

Greenbone Security Assistant

Logged in as Admin admin | Logout  
Sun Jul 9 02:46:23 2023 UTC

Scan Management Asset Management SecInfo Management Configuration Extras Administration Help

NVT Details ? 📈 📈 📈

**Name:** FTP Banner Detection  
**Config:**  
**Family:** General  
**OID:** 1.3.6.1.4.1.25623.1.0.10092  
**Version:** \$Revision: 563 \$  
**Notes:** 0  
**Overrides:** 0

**ID:** 1.3.6.1.4.1.25623.1.0.10092  
**Last modified:** Tue Jul 15 06:41:18 2014  
**Created:** Thu Nov 3 13:08:04 2005

**Summary**  
This Plugin detects the FTP Server Banner

**Vulnerability Scoring**  
CVSS base: **0.0**  
CVSS base vector: [AV:N|AC:L|Au:N|C:N|I:N|A:N](#)

**Preferences**

Name	Default Value	Actions
Timeout	default	

ii.

# REFERENCES

- <https://www.educba.com/what-is-nmap/>
- <https://community.tanium.com/s/article/Choosing-the-Right-Discovery-Method-NMAP-Pros-and-Cons>
- <https://www.comparitech.com/net-admin/how-to-use-wireshark/>
- <https://www.comparitech.com/net-admin/wireshark-review/#:~:text=It%20cannot%20run%20from%20outside,for%20those%20already%20passing%20by.>
- <https://www.quora.com/What-is-the-difference-between-NMAP-and-Wireshark>
- <https://www.geeksforgeeks.org/using-metasploit-and-nmap-to-scan-for-vulnerabilities-in-kali-linux/>
- <https://nextdoorsec.com/zenmap-vs-nmap/#:~:text=Nmap%2C%20the%20original%20command%2Dline,option%20for%20less%20experienced%20users.>
- <https://www.quora.com/What-is-the-difference-between-NMAP-and-Metasploit>
- <https://duanechambers77.medium.com/what-is-the-openvas-vulnerability-scanner-b51573052475>
- [https://www.tcg.com/blog/faster-openvas-vulnerability-scanning/#:~:text=OpenVAS%20is%20a%20system%20vulnerability,vulnerabilities%20and%20improper%20file%20access\).](https://www.tcg.com/blog/faster-openvas-vulnerability-scanning/#:~:text=OpenVAS%20is%20a%20system%20vulnerability,vulnerabilities%20and%20improper%20file%20access).)