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 use 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 experience 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 check 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

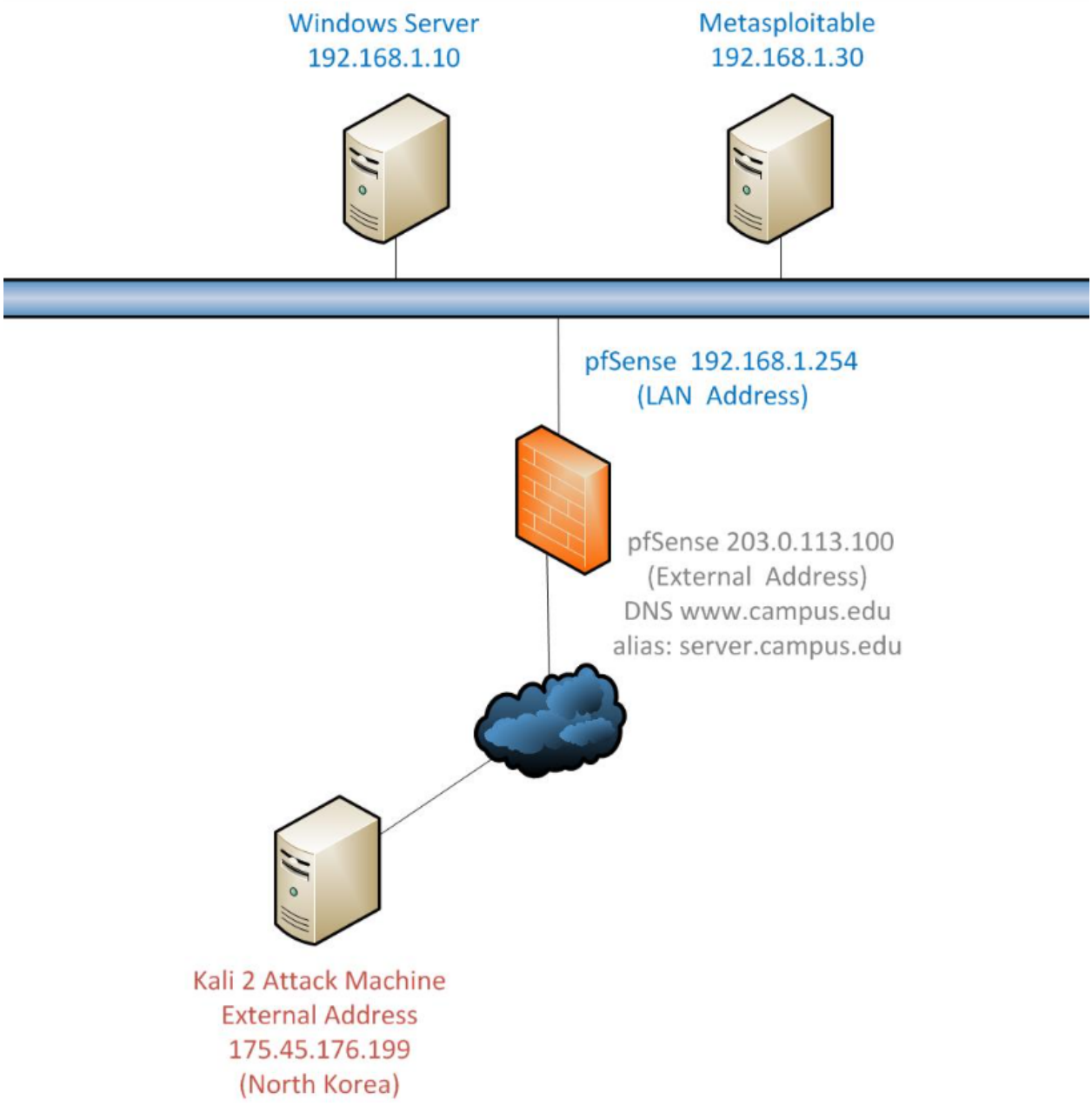
d. Commands

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)

b.

```
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`

1.

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

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-07-07 00
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

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

c. OS Fingerprinting

i. Example - $nmap -O 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 c
losed 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_
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 Window
s 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/ .
Nmap done: 1 IP address (1 host up) scanned in 21.23 seconds
```

iii.

d. **Banner Grabbing**

i. **First we need to determine which ports are open $nmap 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

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

1.

2.
```
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_autoind
ex_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_autoind
ex_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%vF\x
|_00,\xAA\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
```

3.
```
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/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 173.72 seconds
```

e. **Port Range**

i. **Example - # nmap www.campus.edu -p <range>**

1.
```
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
```

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”**

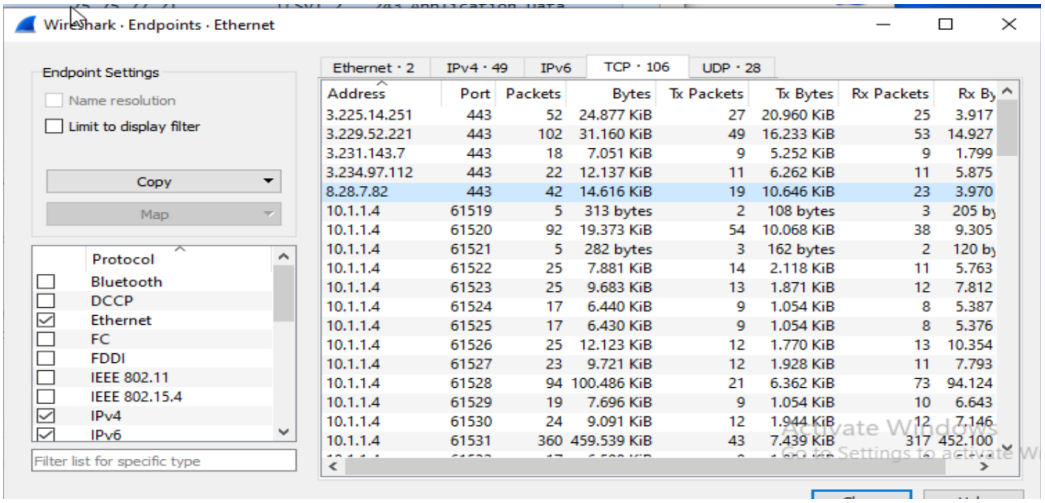
iii.

```
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
```

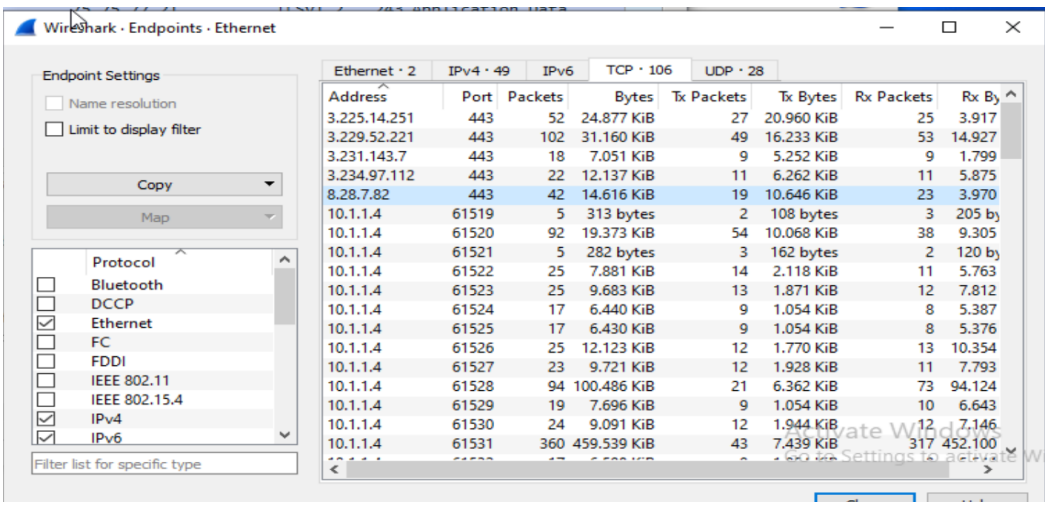
b. **Open Ports**

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.**

ii.



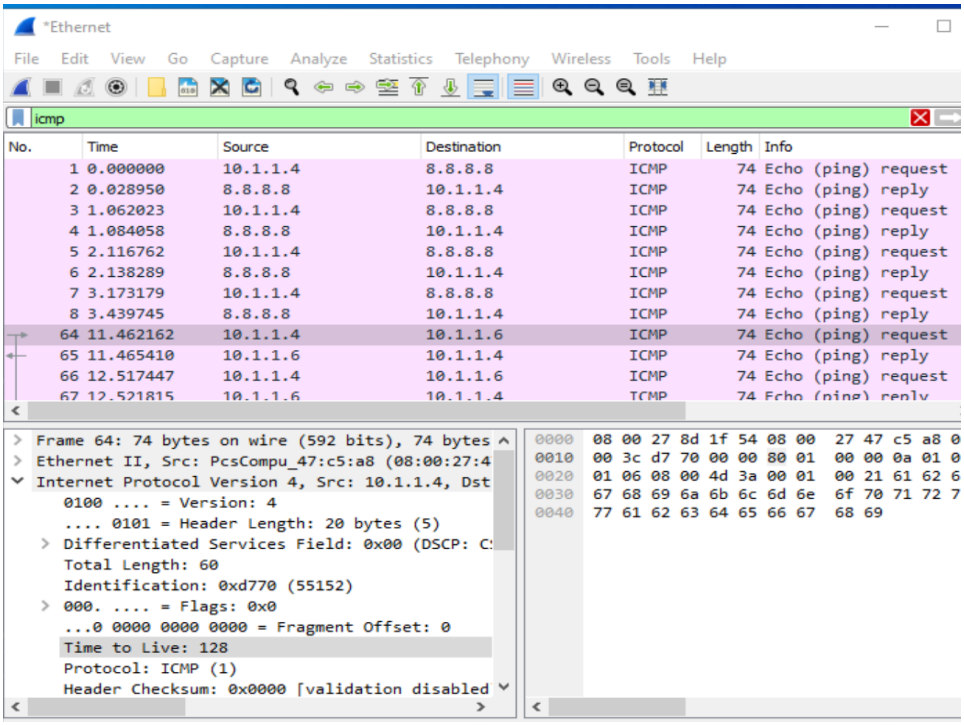
iii.



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.



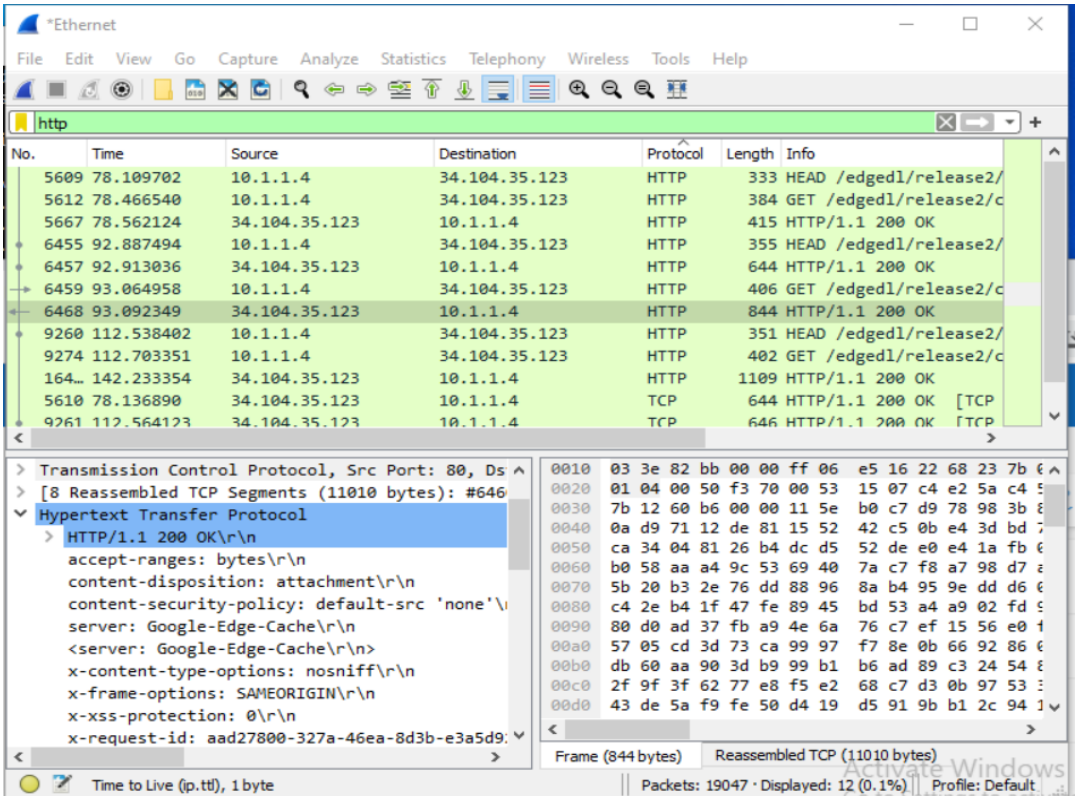
iii.

Operating System (OS)	Time To Live	TCP Window Size
Linux (Kernel 2.4 and 2.6)	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

d. Banner Grabbing

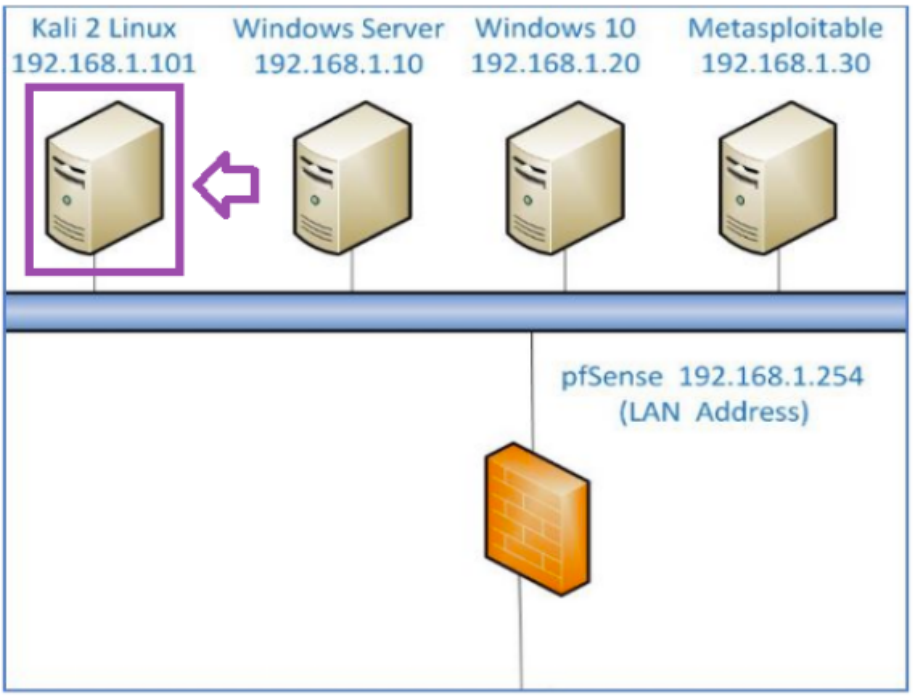
i. We can initiate a capture and then we can filter the “http” protocol and in the middle pane, we could get the banner on the Hypertext Transfer Protocol tab

ii.



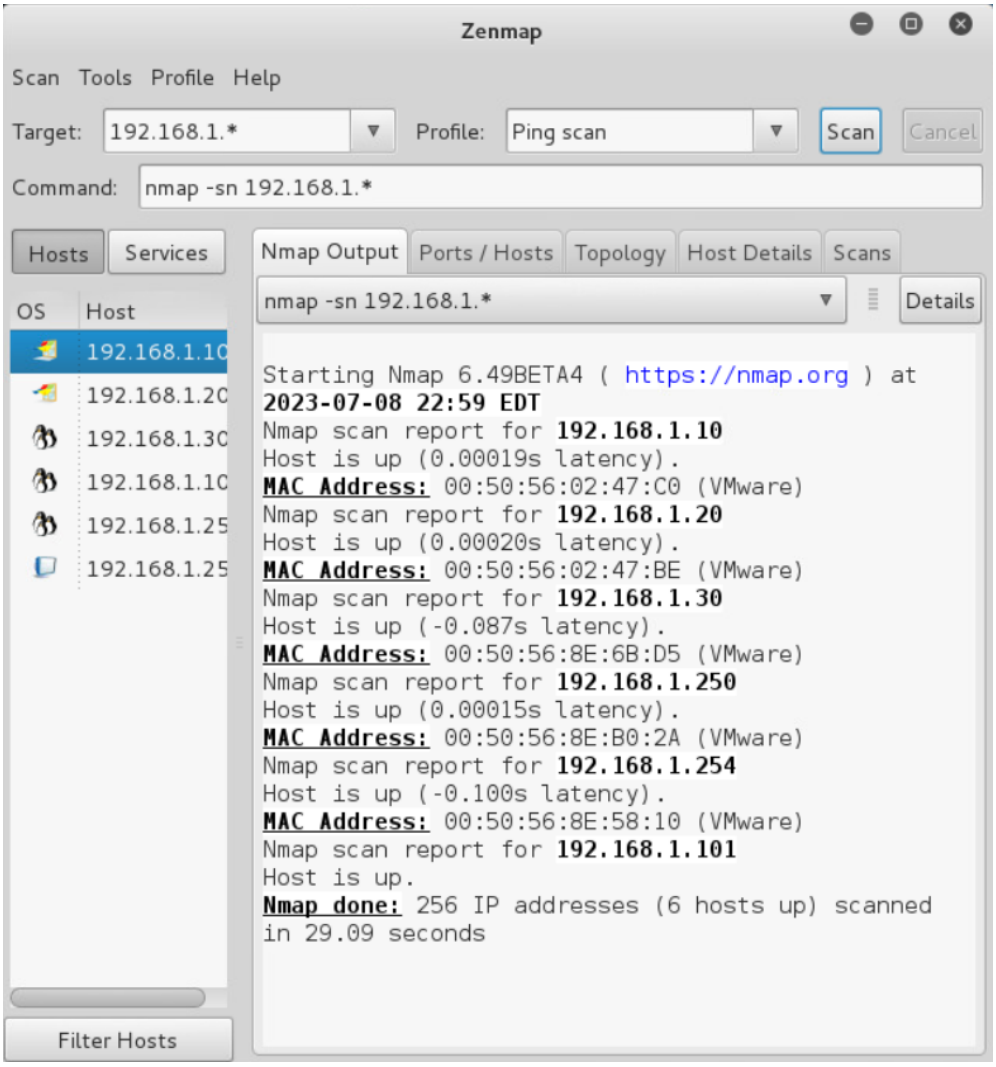
3. Zenmap

a.



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

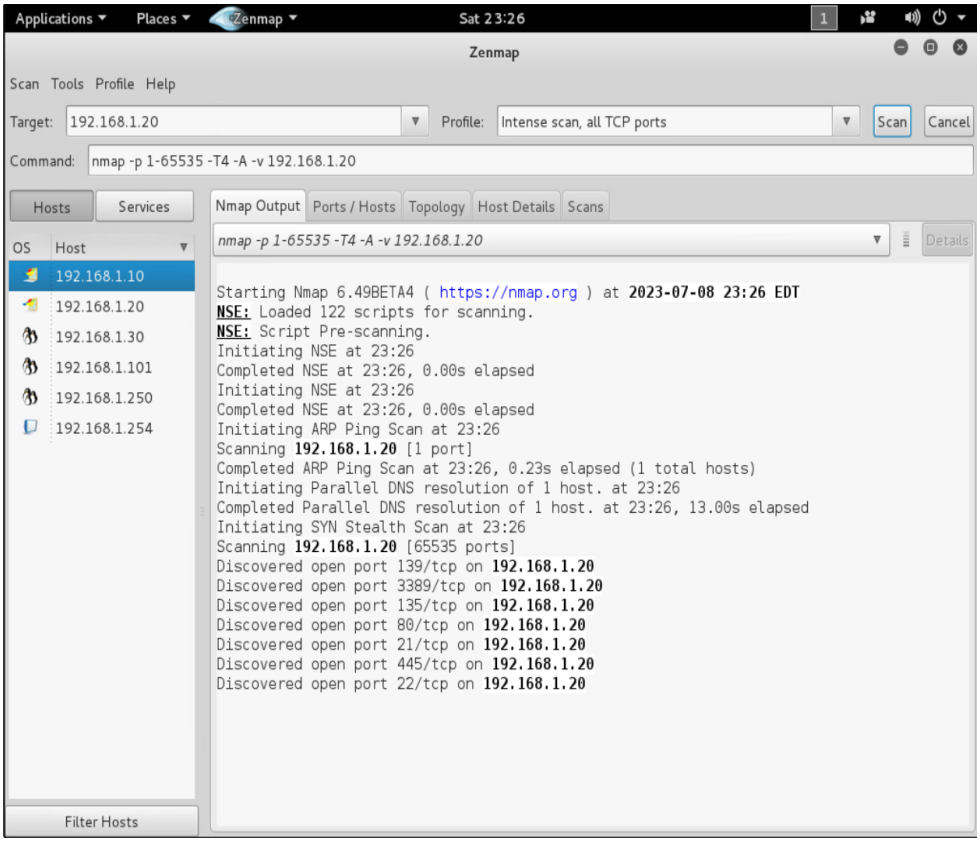
i.



c. **Open Ports**

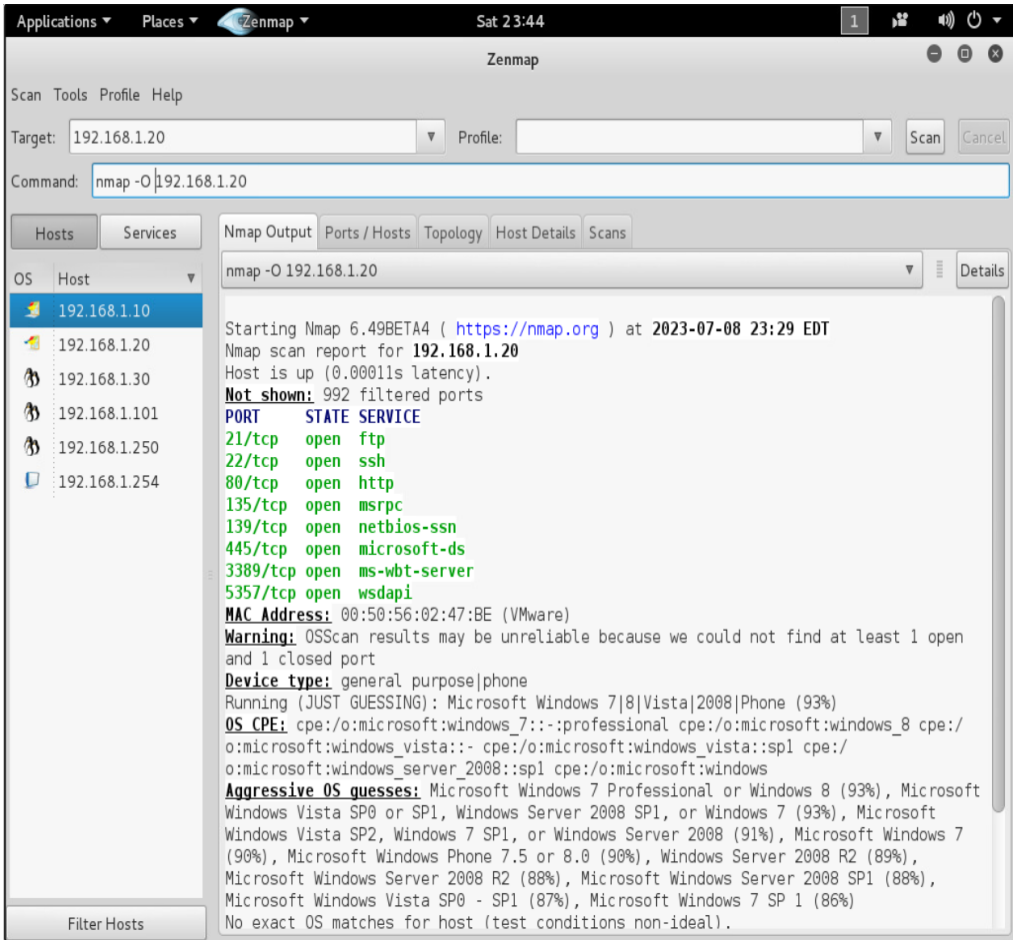
i.

ii.

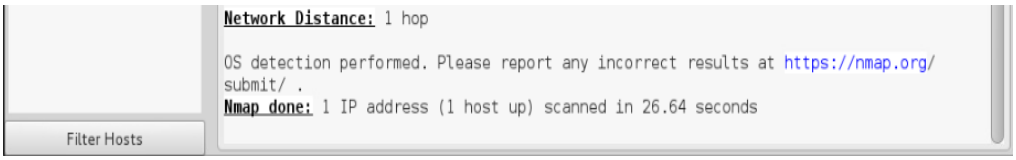


d. OS Fingerprinting

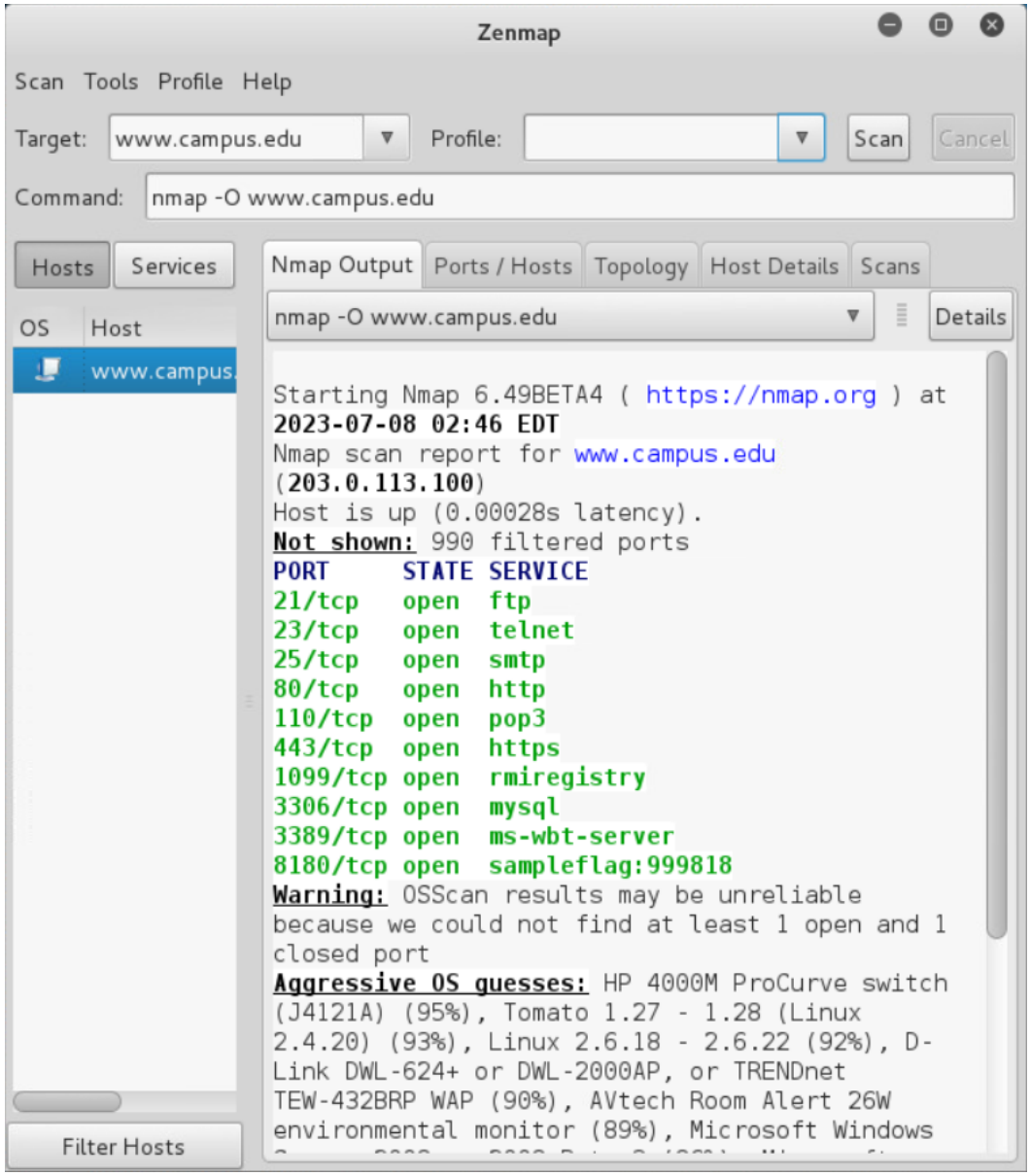
i.


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
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
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -O 192.168.1.20
Details
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).

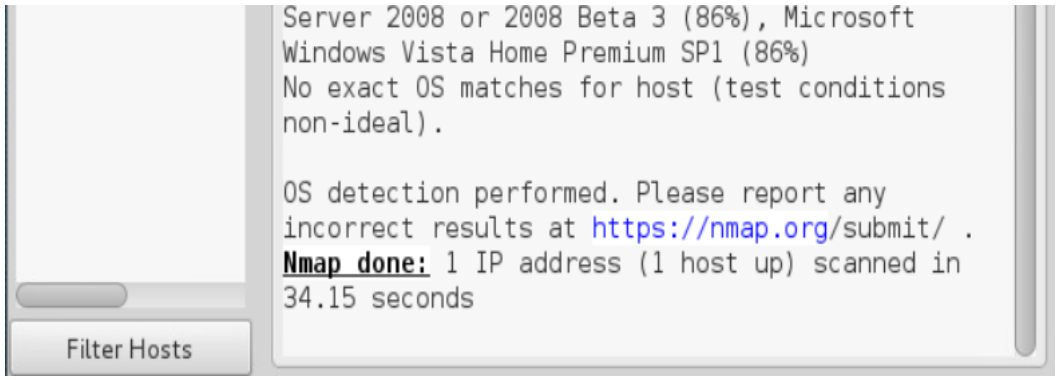
ii.


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
Filter Hosts

iii.

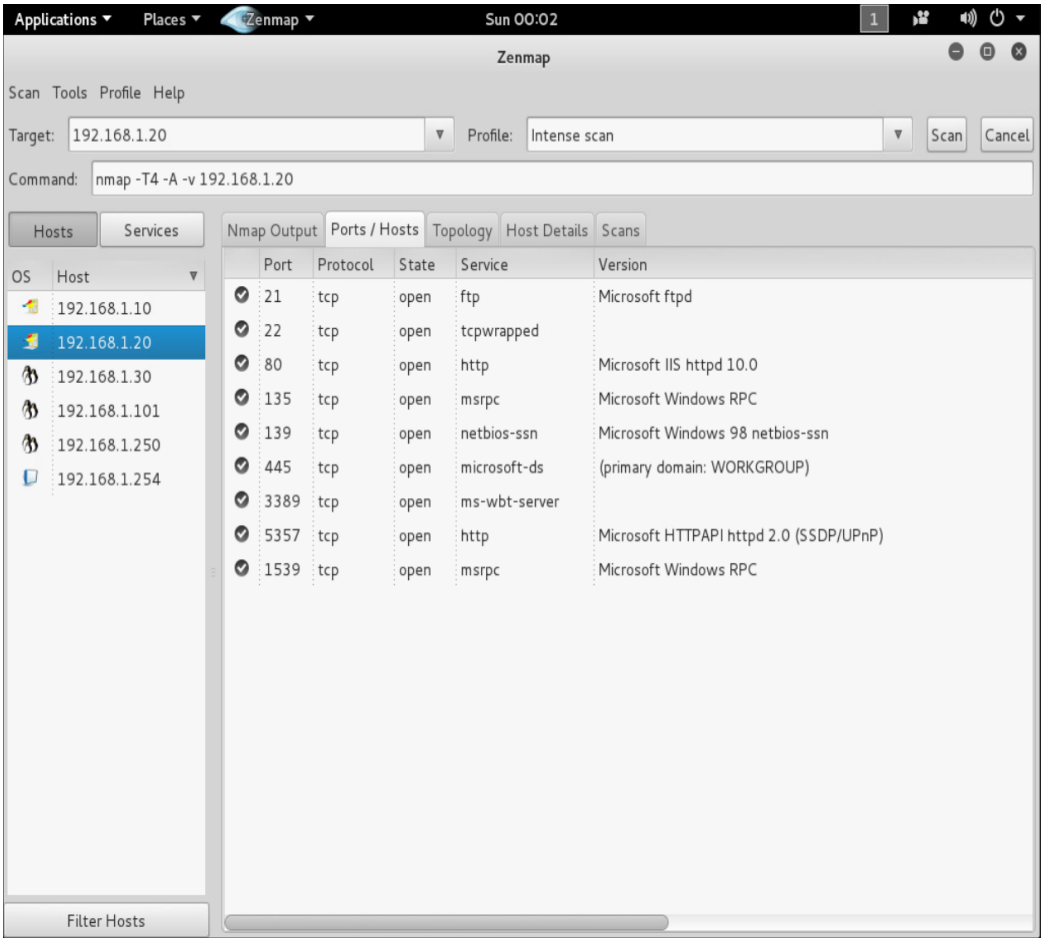


iv.



e. **Banner Grabbing**

i.



ii.

4. Metasploit
    a. **Finding live hosts in your network**

i.

```
       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
```

b. **Open Ports**

i.

```
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

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

c. **OS Fingerprinting**

i.

```
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 c
losed 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_
```

```
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 Window
s 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 >
```

ii.

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 ftpd
23/tcp   open  telnet?
25/tcp   open  smtp               hMailServer smtpd
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-3ubuntu5
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 c
losed port
Device type: general purpose|phone|WAP
Running (JUST GUESSING): Microsoft Windows 2008|Vista|7|Phone (94%), FreeBSD 6.X (87%), Air
Span embedded (85%)
OS CPE: cpe:/o:microsoft:windows_server_2008::beta3 cpe:/o:microsoft:windows_server_2008 cp
e:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:window
s_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
```

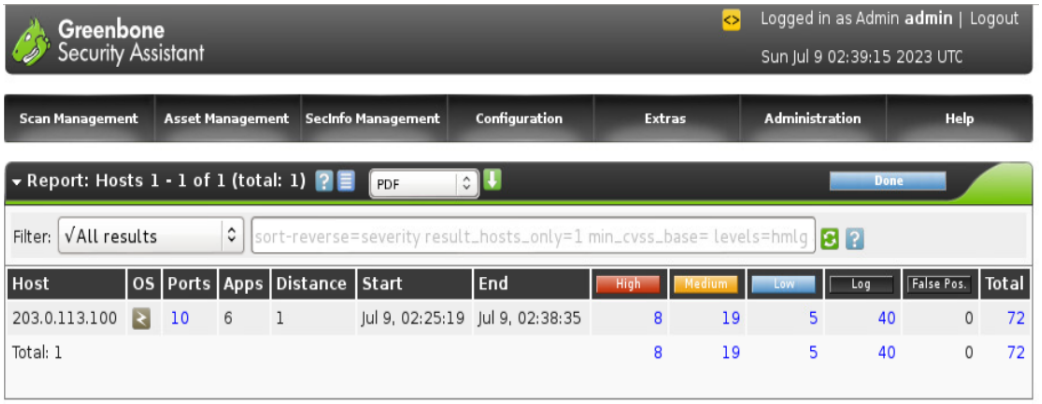
i.

```
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%), AirSp
an 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 >
```

ii.

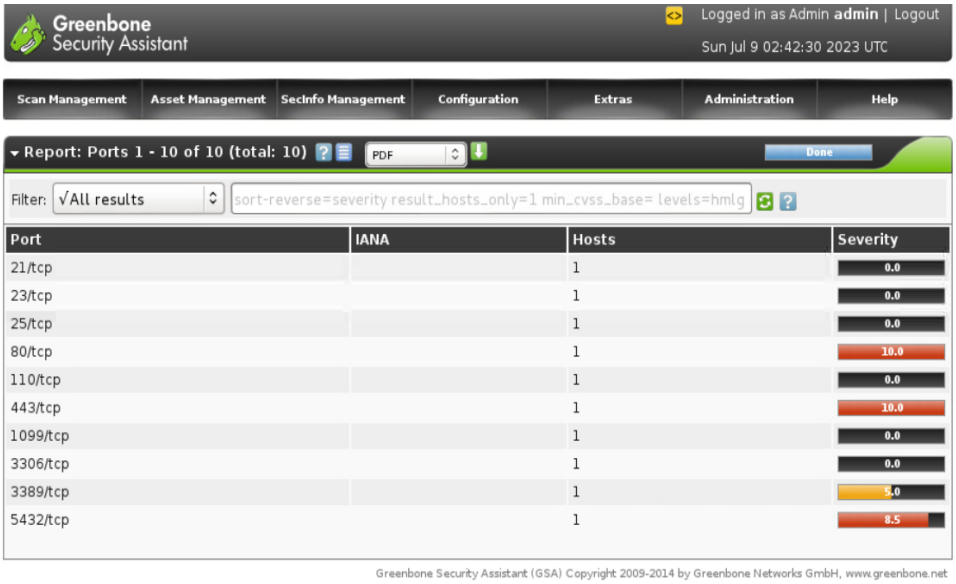
5. OpenVAS
   a. Finding live hosts in your network

i.



b. Open Ports

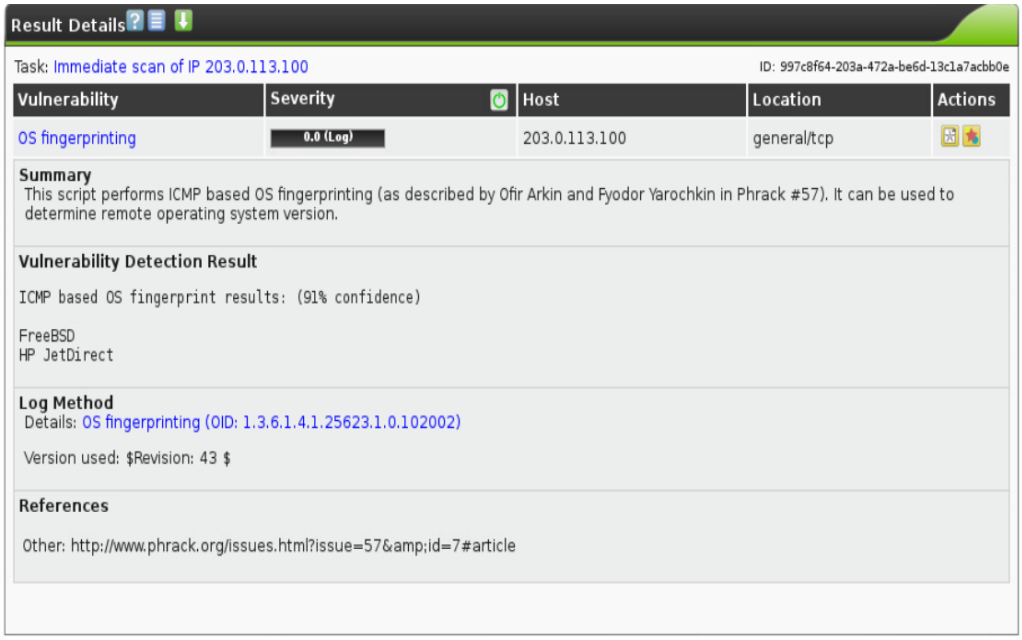
i.



c. OS Fingerprinting

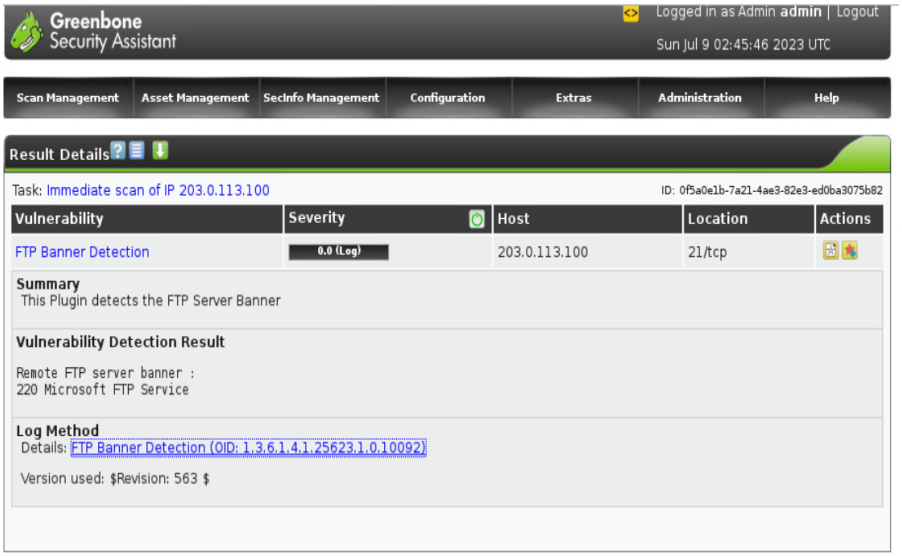
i.

ii.

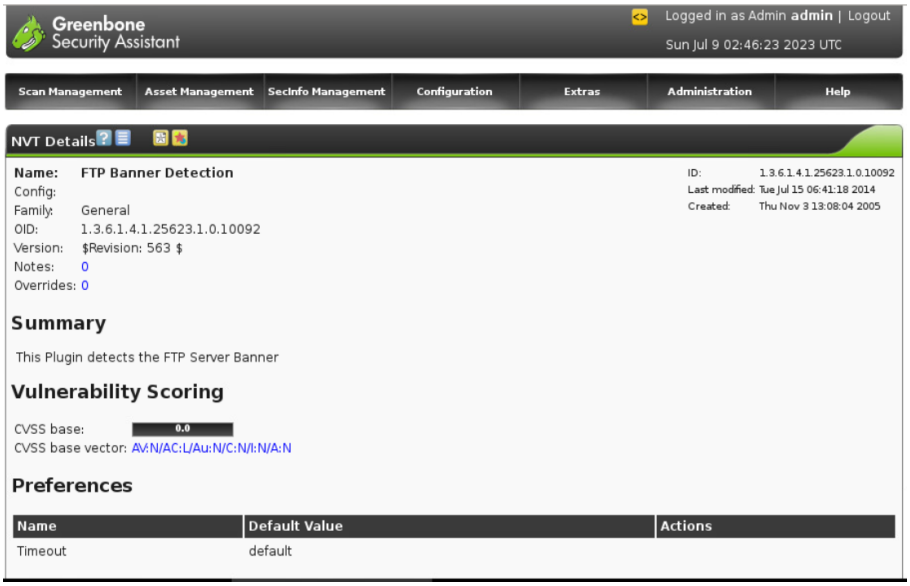


d. Banner Grabbing

i.



ii.


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

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).