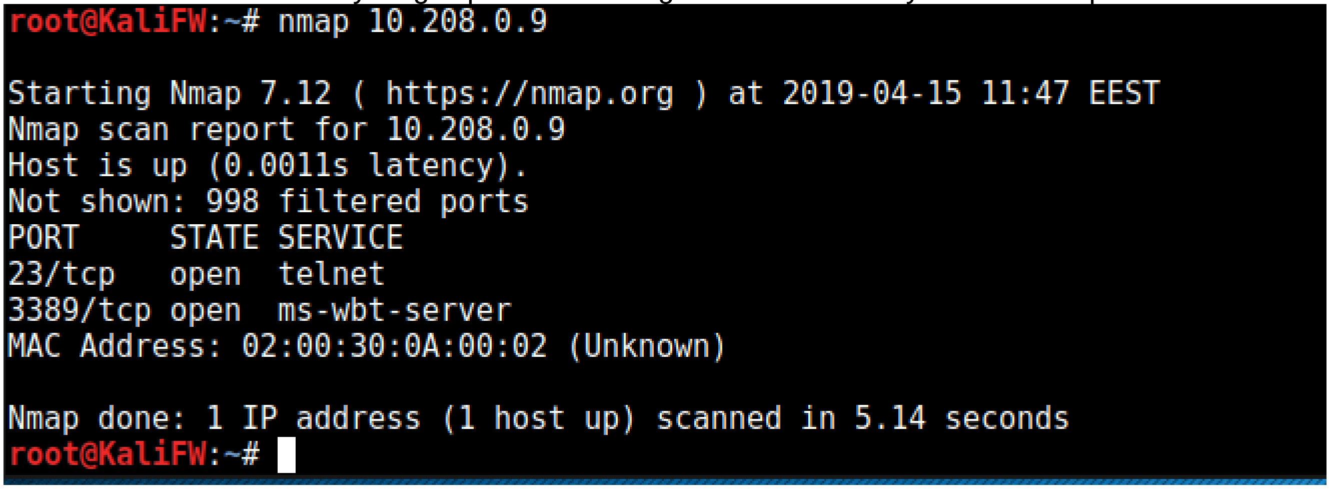
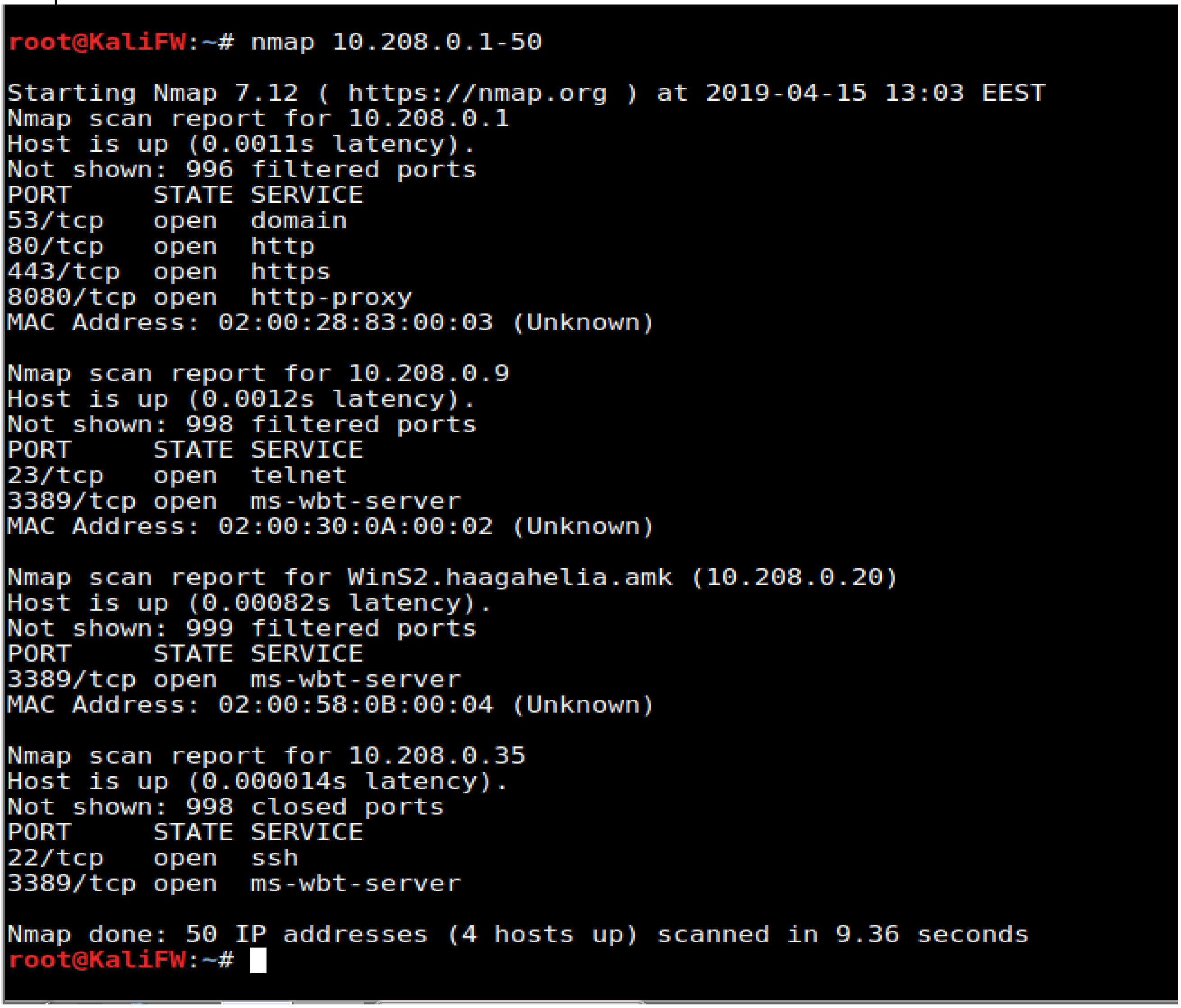
1. **How/why administrators are using it?**
   Administrators are using Kali Linux as to specifically to meet the requirements of professional penetration testing, monitor network, scan ports and security auditing so as a complete toolbox for penetration testing.
   There is wide array of reasons as to why one should use Kali Linux. Here I've listed some of them.
    1. As free as it can get – Kali Linux has been and will always be free to use.
    2. More tools than we could think of - Kali Linux comes with over 600 different penetration testing and security analytics related tools.
    3. Open-source - Kali, being a member of the Linux family, follows the widely appreciated open-source model. Their development tree is publicly viewable on Git and all the code is available for our tweaking purposes.
    4. Multi-language support – Although penetration tools tend to be written in English, it has been ensured that Kali includes true multilingual support, allowing more users to operate in their native language and locate the tools they need for the job.
    5. Completely customizable – The developers at offensive security understand that not everyone will agree with their design model, so they have made it as easy as possible for the more adventurous user to customizable Kali Linux to their liking, all the way down to the Kernel.
    6. A Live System: It can be used as a bootable live system means we can use Kali Linux without installing it, just by booting the ISO image.
    7. Forensics mode: Kali Linux has a forensics mode that can be enabled from the boot menu that helps to avoid any activity that would alter the data on the analyzed system when doing forensics work on a system.
    8. Usable on a Wide range of ARM Devices: Kali Linux provides binary packages for the armel, armhf and arm64 ARM architectures. Kali Linux can be deployed on many interesting devices, from smartphones and tables to Wi-Fi routers and computers of various shapes and sizes.
    9. A Trustable Operating System: As source code is easily being visible on Git repositories.

2. **How you scan your (vdi-lab project) host(s) availability?**
   Try nmap!
   Scan a single IP address/host; syntax when you use; IP address/hostname
   E.g nmap 10.208.x.xxx
   E.g nmap hostname
   Ans: Using Kali Linux tool nmap in Information gathering I can map network with IP address or host name we can scan any single ip address using this command. My scanned output:



```
root@KaliFW:~# nmap 10.208.0.9

Starting Nmap 7.12 ( https://nmap.org ) at 2019-04-15 11:47 EEST
Nmap scan report for 10.208.0.9
Host is up (0.0011s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
23/tcp   open  telnet
3389/tcp open  ms-wbt-server
MAC Address: 02:00:30:0A:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 5.14 seconds
root@KaliFW:~#
```

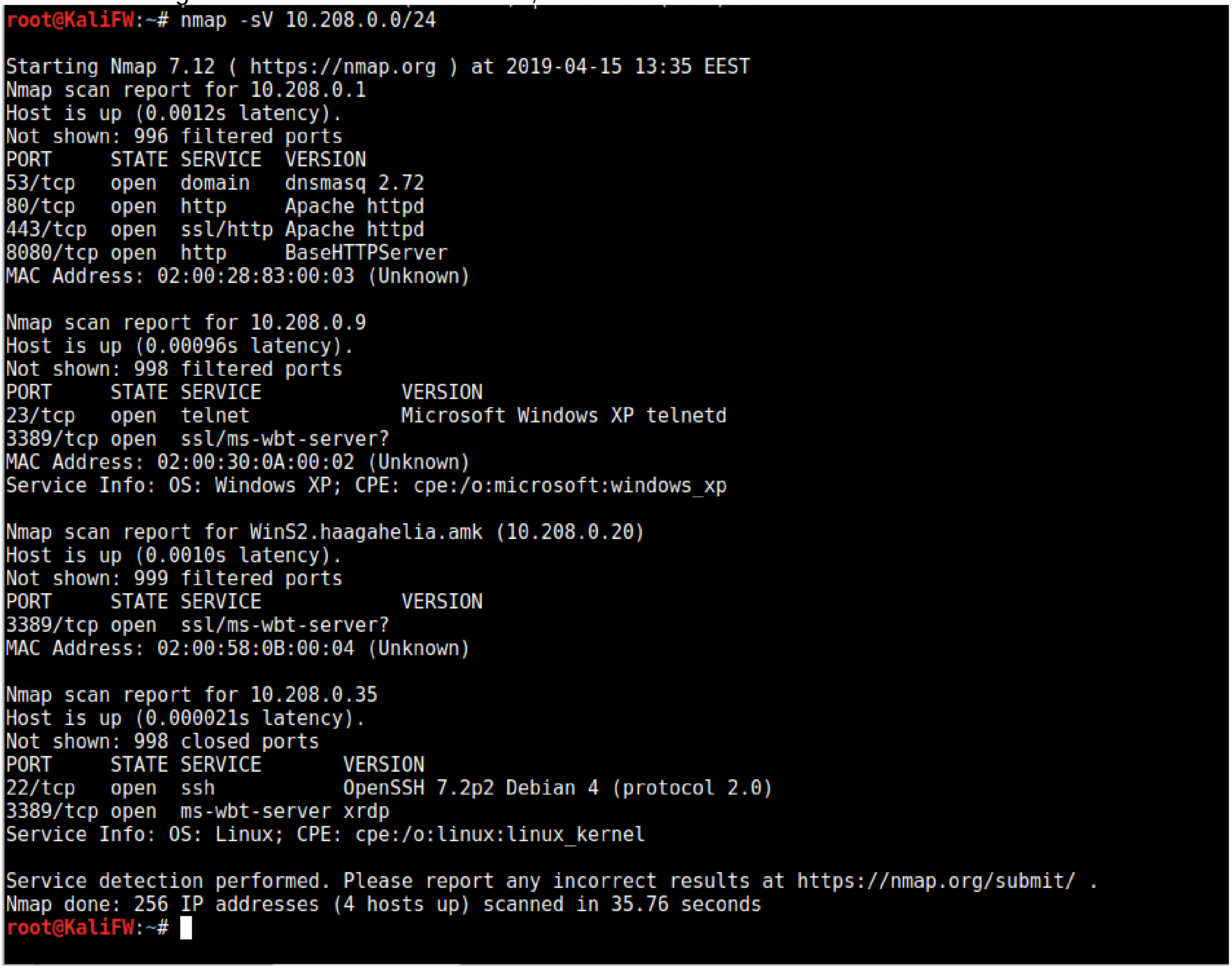
3. **Scan multiple IP address (a range of IP address) all your hosts (instances in vdi-lab).**
   Ans: We can scan multiple IP using command:
   Nmap 10.208.0.1-50
   This shows our host has quite bit of open network ports. These ports all indicate some sort of listening service on this machine.
   But having this many port open on most machines on real world environment is highly abnormal so it may be a wise idea to investigate those machines which has become very easy due to use of nmap to scan.



```
root@KaliFW:~# nmap 10.208.0.1-50

Starting Nmap 7.12 ( https://nmap.org ) at 2019-04-15 13:03 EEST
Nmap scan report for 10.208.0.1
Host is up (0.0011s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
MAC Address: 02:00:28:83:00:03 (Unknown)

Nmap scan report for 10.208.0.9
Host is up (0.0012s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
23/tcp   open  telnet
3389/tcp open  ms-wbt-server
MAC Address: 02:00:30:0A:00:02 (Unknown)

Nmap scan report for WinS2.haagahelia.amk (10.208.0.20)
Host is up (0.00082s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
MAC Address: 02:00:58:0B:00:04 (Unknown)

Nmap scan report for 10.208.0.35
Host is up (0.000014s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server

Nmap done: 50 IP addresses (4 hosts up) scanned in 9.36 seconds
root@KaliFW:~# █
```

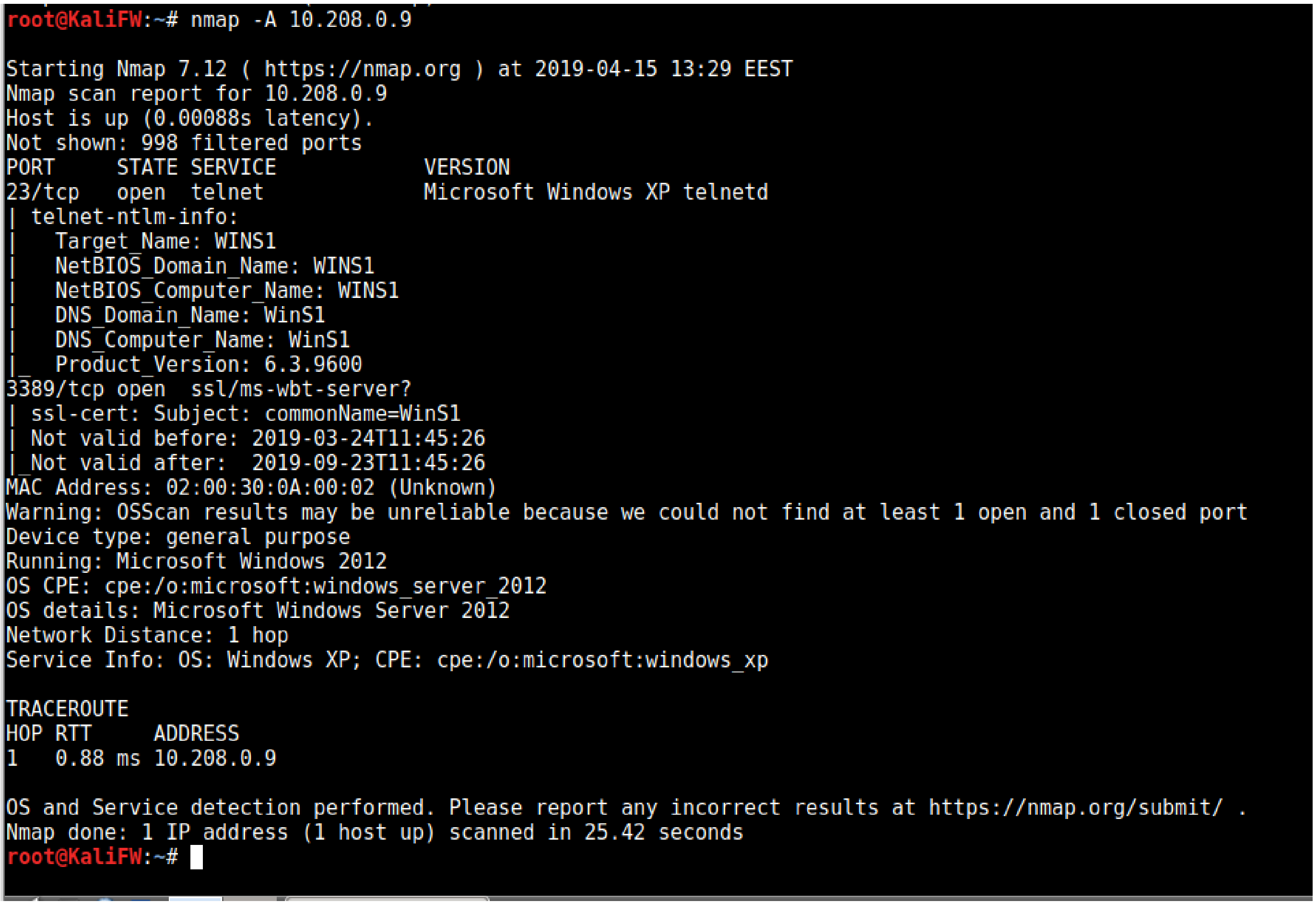
4. **What command Nmap -sV 10.208.0.0/24 does?**
   Ans: This command is used to perform service scan and is often used to try to determine what service may be listening on a port on a server.
   Using this command with Nmap will probe all the open ports and attempt to banner grab information from the service running on each port.
   Also, nmap also tried to determine information about the operating system running on this machine as well as its hostname.
   The main purpose of this command is to scan a target and work as version detection to determine service/version info showing following information available on entire subnet:
   - Using this command, we can scan entire subnet.

- It shows details of all the instances available on this subnet.
- It shows all the ports on this network their status of opening or closed.
- It shows all the available services.
- It shows versions of all available server versions.
- It is showing all the instance details wins1, wins2 and kali Linux.

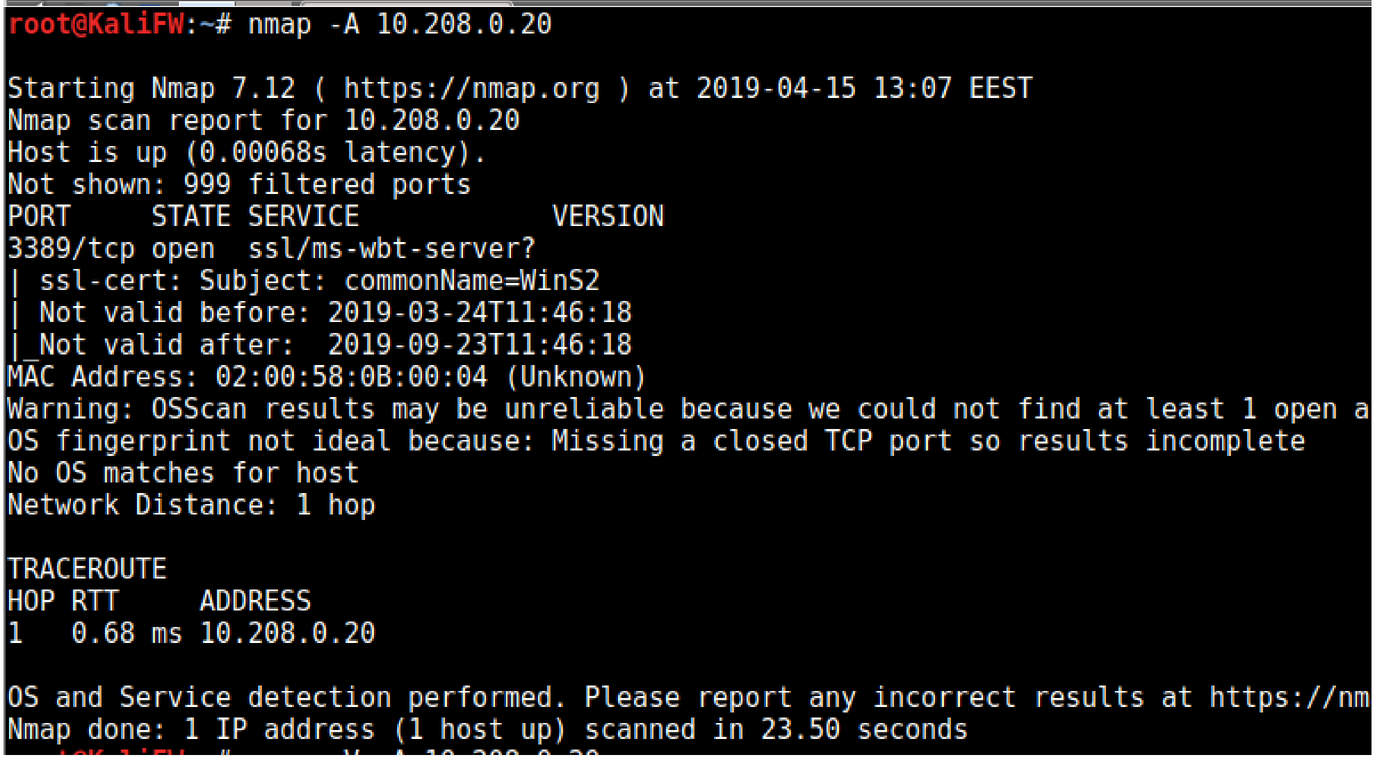


```
root@KaliFW:~# nmap -sV 10.208.0.0/24

Starting Nmap 7.12 ( https://nmap.org ) at 2019-04-15 13:35 EEST
Nmap scan report for 10.208.0.1
Host is up (0.0012s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE  VERSION
53/tcp   open  domain   dnsmasq 2.72
80/tcp   open  http     Apache httpd
443/tcp  open  ssl/http Apache httpd
8080/tcp open  http     BaseHTTPServer
MAC Address: 02:00:28:83:00:03 (Unknown)

Nmap scan report for 10.208.0.9
Host is up (0.00096s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE           VERSION
23/tcp   open  telnet            Microsoft Windows XP telnetd
3389/tcp open  ssl/ms-wbt-server?
MAC Address: 02:00:30:0A:00:02 (Unknown)
Service Info: OS: Windows XP; CPE: cpe:/o:microsoft:windows_xp

Nmap scan report for WinS2.haagahelia.amk (10.208.0.20)
Host is up (0.0010s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE           VERSION
3389/tcp open  ssl/ms-wbt-server?
MAC Address: 02:00:58:0B:00:04 (Unknown)

Nmap scan report for 10.208.0.35
Host is up (0.000021s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 7.2p2 Debian 4 (protocol 2.0)
3389/tcp open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 35.76 seconds
root@KaliFW:~# 
```

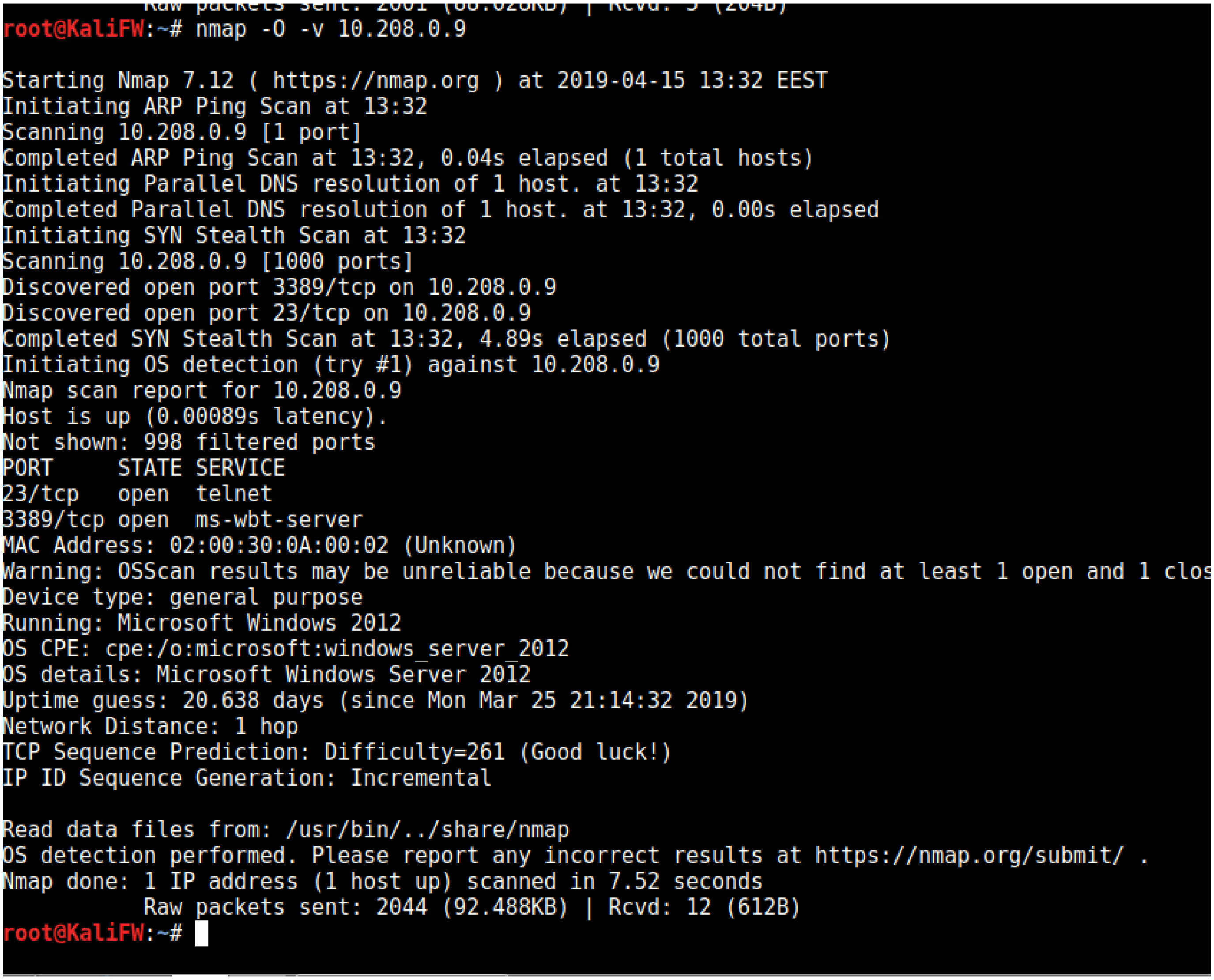
5. **How you can scan network operating systems and their versions?**
Here these snippets show network operating systems and their versions:



```
root@KaliFW:~# nmap -A 10.208.0.9

Starting Nmap 7.12 ( https://nmap.org ) at 2019-04-15 13:29 EEST
Nmap scan report for 10.208.0.9
Host is up (0.00088s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE            VERSION
23/tcp   open  telnet             Microsoft Windows XP telnetd
| telnet-ntlm-info:
|   Target_Name: WINS1
|   NetBIOS_Domain_Name: WINS1
|   NetBIOS_Computer_Name: WINS1
|   DNS_Domain_Name: WinS1
|   DNS_Computer_Name: WinS1
|_  Product_Version: 6.3.9600
3389/tcp open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=WinS1
| Not valid before: 2019-03-24T11:45:26
|_Not valid after:  2019-09-23T11:45:26
MAC Address: 02:00:30:0A:00:02 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012
OS details: Microsoft Windows Server 2012
Network Distance: 1 hop
Service Info: OS: Windows XP; CPE: cpe:/o:microsoft:windows_xp

TRACEROUTE
HOP RTT     ADDRESS
1   0.88 ms 10.208.0.9

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 25.42 seconds
root@KaliFW:~#
```



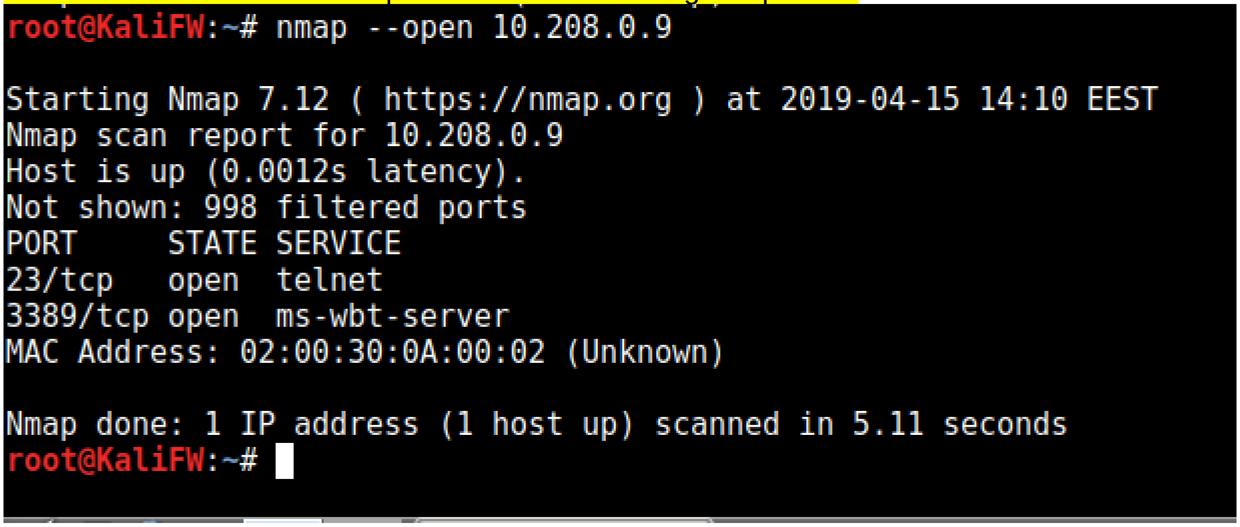
```
root@KaliFW:~# nmap -A 10.208.0.20

Starting Nmap 7.12 ( https://nmap.org ) at 2019-04-15 13:07 EEST
Nmap scan report for 10.208.0.20
Host is up (0.00068s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE            VERSION
3389/tcp open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=WinS2
| Not valid before: 2019-03-24T11:46:18
|_Not valid after:  2019-09-23T11:46:18
MAC Address: 02:00:58:0B:00:04 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open a
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.68 ms 10.208.0.20

OS and Service detection performed. Please report any incorrect results at https://nm
Nmap done: 1 IP address (1 host up) scanned in 23.50 seconds
```



```
           Raw packets sent: 2001 (88.028KB) | Rcvd: 5 (204B)
root@KaliFW:~# nmap -O -v 10.208.0.9

Starting Nmap 7.12 ( https://nmap.org ) at 2019-04-15 13:32 EEST
Initiating ARP Ping Scan at 13:32
Scanning 10.208.0.9 [1 port]
Completed ARP Ping Scan at 13:32, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:32
Completed Parallel DNS resolution of 1 host. at 13:32, 0.00s elapsed
Initiating SYN Stealth Scan at 13:32
Scanning 10.208.0.9 [1000 ports]
Discovered open port 3389/tcp on 10.208.0.9
Discovered open port 23/tcp on 10.208.0.9
Completed SYN Stealth Scan at 13:32, 4.89s elapsed (1000 total ports)
Initiating OS detection (try #1) against 10.208.0.9
Nmap scan report for 10.208.0.9
Host is up (0.00089s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
23/tcp   open  telnet
3389/tcp open  ms-wbt-server
MAC Address: 02:00:30:0A:00:02 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 clos
Device type: general purpose
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012
OS details: Microsoft Windows Server 2012
Uptime guess: 20.638 days (since Mon Mar 25 21:14:32 2019)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.52 seconds
           Raw packets sent: 2044 (92.488KB) | Rcvd: 12 (612B)
root@KaliFW:~#
```

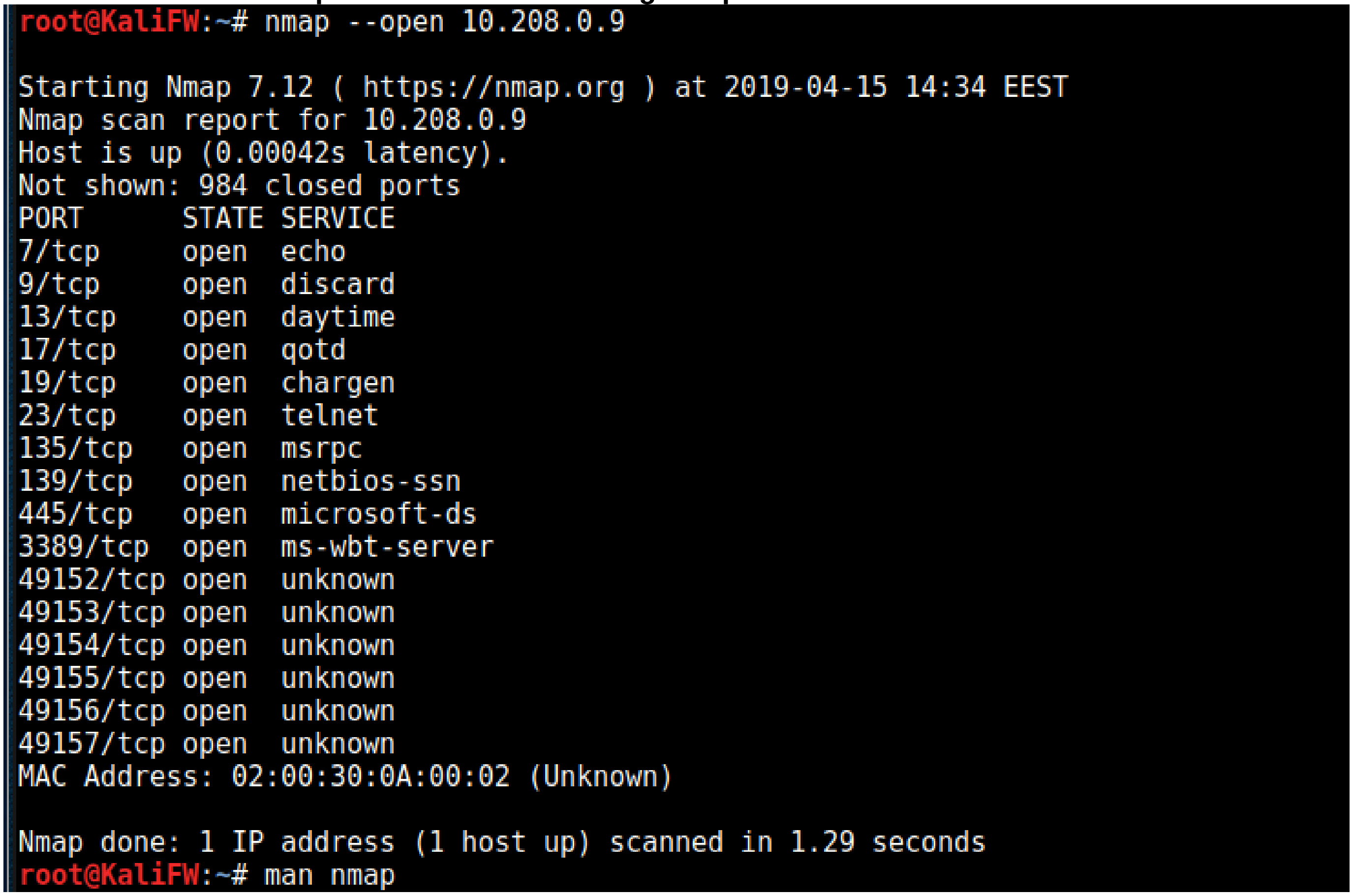
6. **Windows workstation and windows server installations (test them) check which ports are open?**
Is the situation different when (Windows server / workstation) firewalls are on and off?

When Windows firewall is on port status is shown in given picture:



```
root@KaliFW:~# nmap --open 10.208.0.9

Starting Nmap 7.12 ( https://nmap.org ) at 2019-04-15 14:10 EEST
Nmap scan report for 10.208.0.9
Host is up (0.0012s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
23/tcp   open  telnet
3389/tcp open  ms-wbt-server
MAC Address: 02:00:30:0A:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 5.11 seconds
root@KaliFW:~#
```

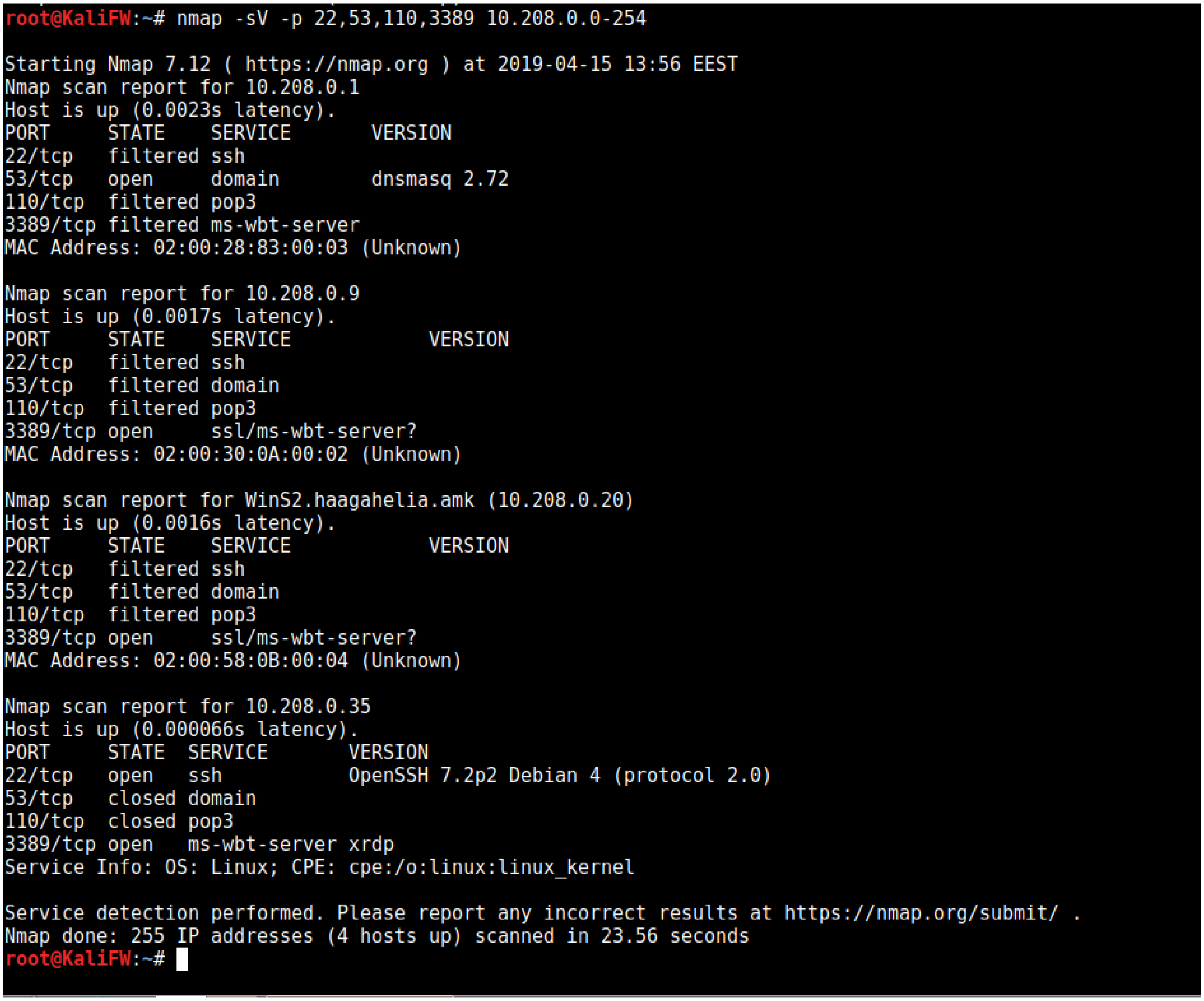
When Windows firewall is off port status in shown in given picture:



```
root@KaliFW:~# nmap --open 10.208.0.9

Starting Nmap 7.12 ( https://nmap.org ) at 2019-04-15 14:34 EEST
Nmap scan report for 10.208.0.9
Host is up (0.00042s latency).
Not shown: 984 closed ports
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
23/tcp    open  telnet
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 02:00:30:0A:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
root@KaliFW:~# man nmap
```

7. **What does command: nmap -sV -p 22,53,110,3389 10.208.0.0-254?**

   This command open ports to determine service/version info to specified ports.



```
root@KaliFW:~# nmap -sV -p 22,53,110,3389 10.208.0.0-254

Starting Nmap 7.12 ( https://nmap.org ) at 2019-04-15 13:56 EEST
Nmap scan report for 10.208.0.1
Host is up (0.0023s latency).
PORT     STATE    SERVICE       VERSION
22/tcp   filtered ssh
53/tcp   open     domain        dnsmasq 2.72
110/tcp  filtered pop3
3389/tcp filtered ms-wbt-server
MAC Address: 02:00:28:83:00:03 (Unknown)

Nmap scan report for 10.208.0.9
Host is up (0.0017s latency).
PORT     STATE    SERVICE            VERSION
22/tcp   filtered ssh
53/tcp   filtered domain
110/tcp  filtered pop3
3389/tcp open     ssl/ms-wbt-server?
MAC Address: 02:00:30:0A:00:02 (Unknown)

Nmap scan report for WinS2.haagahelia.amk (10.208.0.20)
Host is up (0.0016s latency).
PORT     STATE    SERVICE            VERSION
22/tcp   filtered ssh
53/tcp   filtered domain
110/tcp  filtered pop3
3389/tcp open     ssl/ms-wbt-server?
MAC Address: 02:00:58:0B:00:04 (Unknown)

Nmap scan report for 10.208.0.35
Host is up (0.000066s latency).
PORT     STATE  SERVICE       VERSION
22/tcp   open   ssh           OpenSSH 7.2p2 Debian 4 (protocol 2.0)
53/tcp   closed domain
110/tcp  closed pop3
3389/tcp open   ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 255 IP addresses (4 hosts up) scanned in 23.56 seconds
root@KaliFW:~# 
```

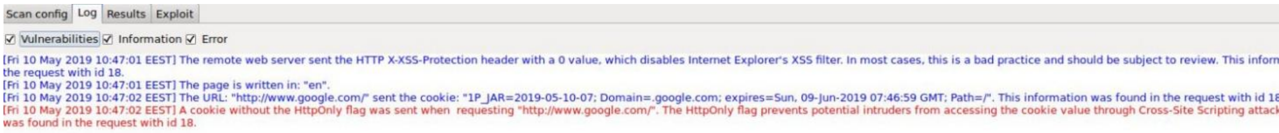
8. **What or which tools are appropriate for testing web server vulnerabilities? What tool(s) and how to test?**

Ans: Some of the tools for webserver testing are:

1. Detectify
2. Netsparker cloud
3. Grabber
4. Zed Attack proxy
5. Wapiti
6. W3af
7. WebScarab
8. SQLMap and a lot more

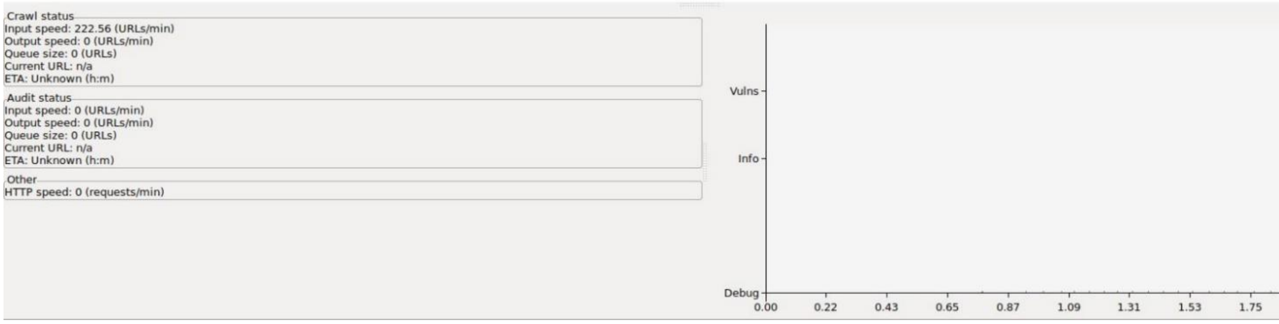
Among these tools I used W3af for vulnerabilities testing in Kali Linux. ‘
After I opened it I choosed fast scan profile for fast scanning.
Various information tell us about how scanning is going on. The information is giving basically what crawling is doing at current time. What audit is doing current time? Also, we have log showing what it found while it is scanning. Https speed shows how many requests per minuting is going on.

The graph is showing the debug information that’s giving as well as the information also vulnerabilities that it found in red colore-coded text and blue the other scanning information.



☑ Vulnerabilities ☑ Information ☑ Error

```
[Fri 10 May 2019 10:47:01 EEST] The remote web server sent the HTTP X-XSS-Protection header with a 0 value, which disables Internet Explorer's XSS filter. In most cases, this is a bad practice and should be subject to review. This inform
the request with id 18.
[Fri 10 May 2019 10:47:01 EEST] The page is written in: "en".
[Fri 10 May 2019 10:47:02 EEST] The URL: "http://www.google.com/" sent the cookie: "1P_JAR=2019-05-10-07; Domain=.google.com; expires=Sun, 09-Jun-2019 07:46:59 GMT; Path=/". This information was found in the request with id 18
[Fri 10 May 2019 10:47:02 EEST] A cookie without the HttpOnly flag was sent when  requesting "http://www.google.com/". The HttpOnly flag prevents potential intruders from accessing the cookie value through Cross-Site Scripting attack
was found in the request with id 18.
```

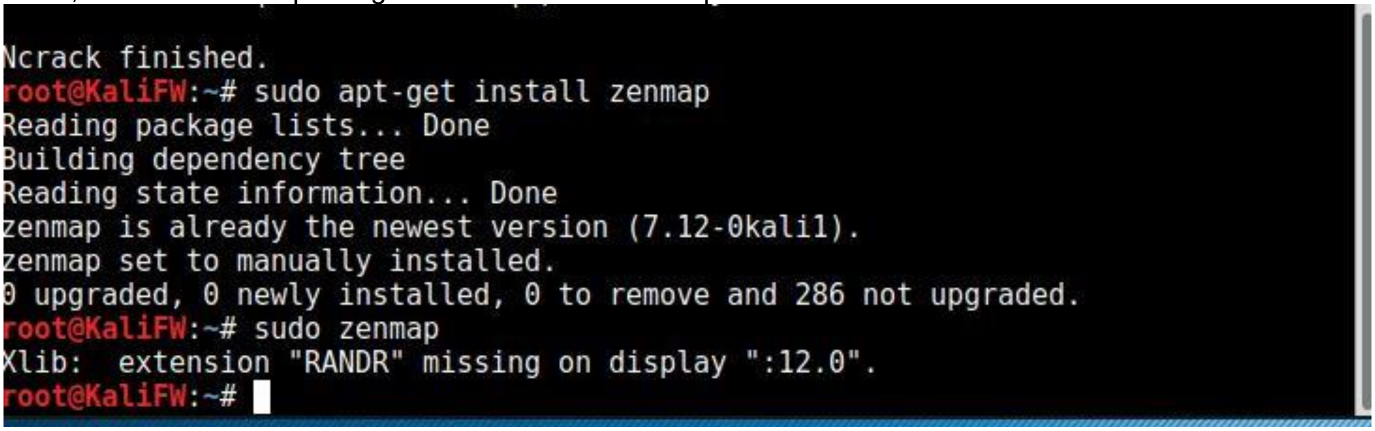


```
Crawl status
Input speed: 222.56 (URLs/min)
Output speed: 0 (URLs/min)
Queue size: 0 (URLs)
Current URL: n/a
ETA: Unknown (h:m)
Audit status
Input speed: 0 (URLs/min)
Output speed: 0 (URLs/min)
Queue size: 0 (URLs)
Current URL: n/a
ETA: Unknown (h:m)
Other
HTTP speed: 0 (requests/min)
```

9. Zenmap? What it is! How you can use it?

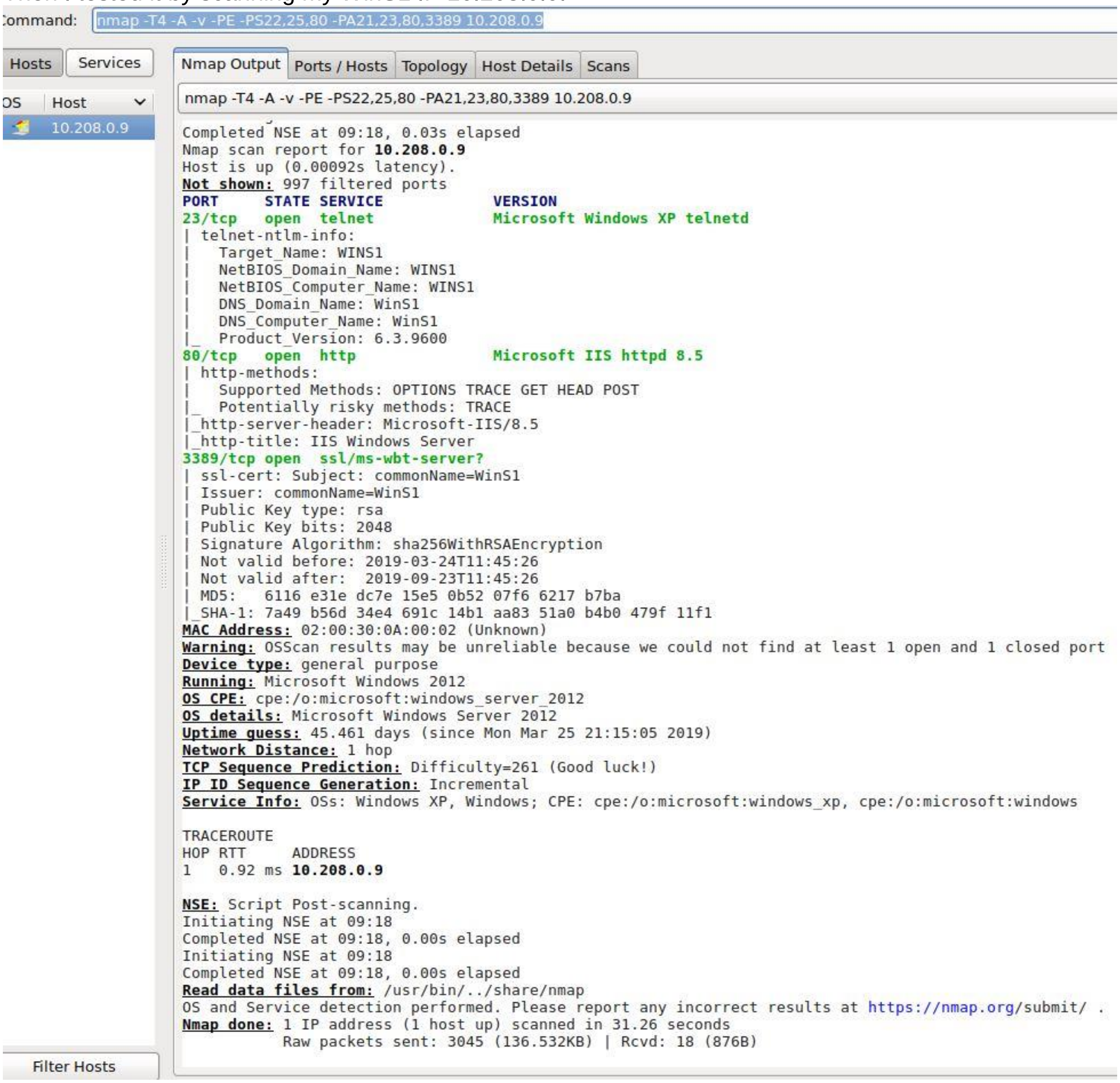
Zenmap is the official Nmap Security Scanner GUI which is multi-platform free and opensource application. It can be installed in any of the operating system and environment and monitor securities and performance our environment and its connections. Frequently used scans can be saved as profiles to make them easy to run repeatedly. Scans results can be compared with one another to see how they differ, and the result of recent scans are stored in a searchable database.

I used Zenmap by installing in Kali Linux using command: sudo apt-get install zenmap but in this case it was default installed.
Then, I started Zenmap using command: sudo Zenmap.



```
Ncrack finished.
root@KaliFW:~# sudo apt-get install zenmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
zenmap is already the newest version (7.12-0kali1).
zenmap set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 286 not upgraded.
root@KaliFW:~# sudo zenmap
Xlib:  extension "RANDR" missing on display ":12.0".
root@KaliFW:~# 
```

Then I tested it by scanning my WinS1 IP 10.208.0.9.



```
nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 10.208.0.9
```

```
Completed NSE at 09:18, 0.03s elapsed
Nmap scan report for 10.208.0.9
Host is up (0.00092s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE            VERSION
23/tcp   open  telnet             Microsoft Windows XP telnetd
| telnet-ntlm-info:
|   Target_Name: WINS1
|   NetBIOS_Domain_Name: WINS1
|   NetBIOS_Computer_Name: WINS1
|   DNS_Domain_Name: WinS1
|   DNS_Computer_Name: WinS1
|_  Product_Version: 6.3.9600
80/tcp   open  http               Microsoft IIS httpd 8.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.5
|_http-title: IIS Windows Server
3389/tcp open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=WinS1
| Issuer: commonName=WinS1
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2019-03-24T11:45:26
| Not valid after:  2019-09-23T11:45:26
| MD5:   6116 e31e dc7e 15e5 0b52 07f6 6217 b7ba
|_SHA-1: 7a49 b56d 34e4 691c 14b1 aa83 51a0 b4b0 479f 11f1
MAC Address: 02:00:30:0A:00:02 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012
OS details: Microsoft Windows Server 2012
Uptime guess: 45.461 days (since Mon Mar 25 21:15:05 2019)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows XP, Windows; CPE: cpe:/o:microsoft:windows_xp, cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT     ADDRESS
1   0.92 ms 10.208.0.9

NSE: Script Post-scanning.
Initiating NSE at 09:18
Completed NSE at 09:18, 0.00s elapsed
Initiating NSE at 09:18
Completed NSE at 09:18, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 31.26 seconds
           Raw packets sent: 3045 (136.532KB) | Rcvd: 18 (876B)
```