Further Nmap Room Write up

The FurtherNmap room on TryHackMe is designed to deepen understanding of the Nmap tool beyond basic scans.

It covers scanning types (TCP SYN, UDP, connect scans), timing templates, verbosity levels, output options, and basic NSE (Nmap Scripting Engine) usage.

In a real-world scenario, these techniques allow penetration testers to discover open ports, identify running services, detect the operating system, and automate vulnerability checks.

For this write-up, I applied the commands on a Metasploitable2 virtual machine to illustrate realistic results.

Introduction:

1. What networking constructs are used to direct traffic to the right application on a server?

Answer:

Ports

Ports are numerical identifiers used in networking to direct traffic to specific applications or services running on a server

2. How many of these are available on any network-enabled computer?

Answer:

65535

This is the total number of ports available, ranging from 0 to 65535

3- How many of these are considered “well-known”?

Answer:

1024

Ports 0 to 1023 are considered "well-known" ports and are typically assigned to widely used services and application

Note : this is metasploitable ip address which we woll be doing several nmap command on so if you see the ip changes don’t worry we still on metasploitable.

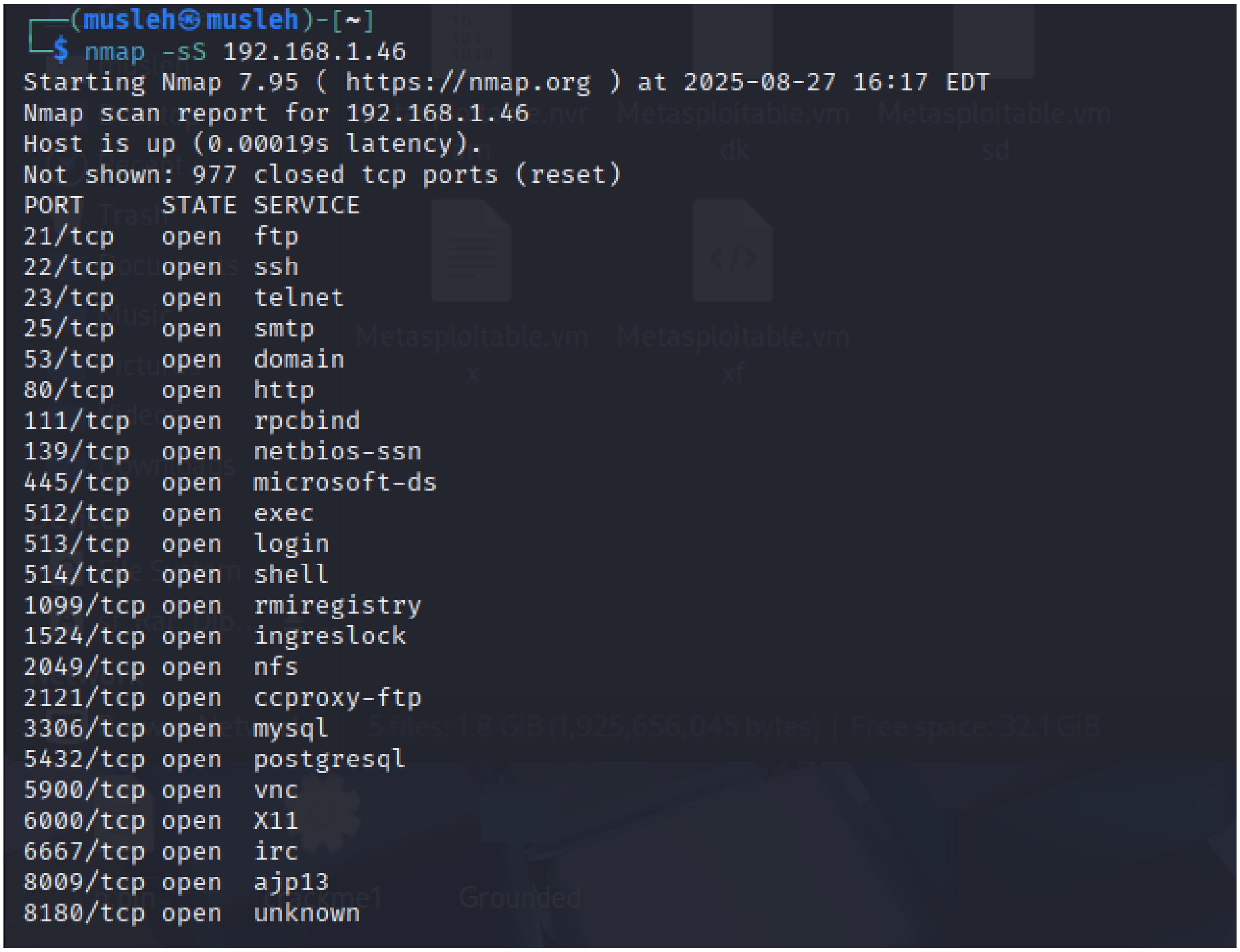
Nmap Switches

1. What is the first switch listed in the help menu for a ‘Syn Scan’?

Answer:

-sS

The -sS switch initiates a SYN scan, which is a stealthy scan method that sends SYN packets and analyzes the responses to determine open ports.



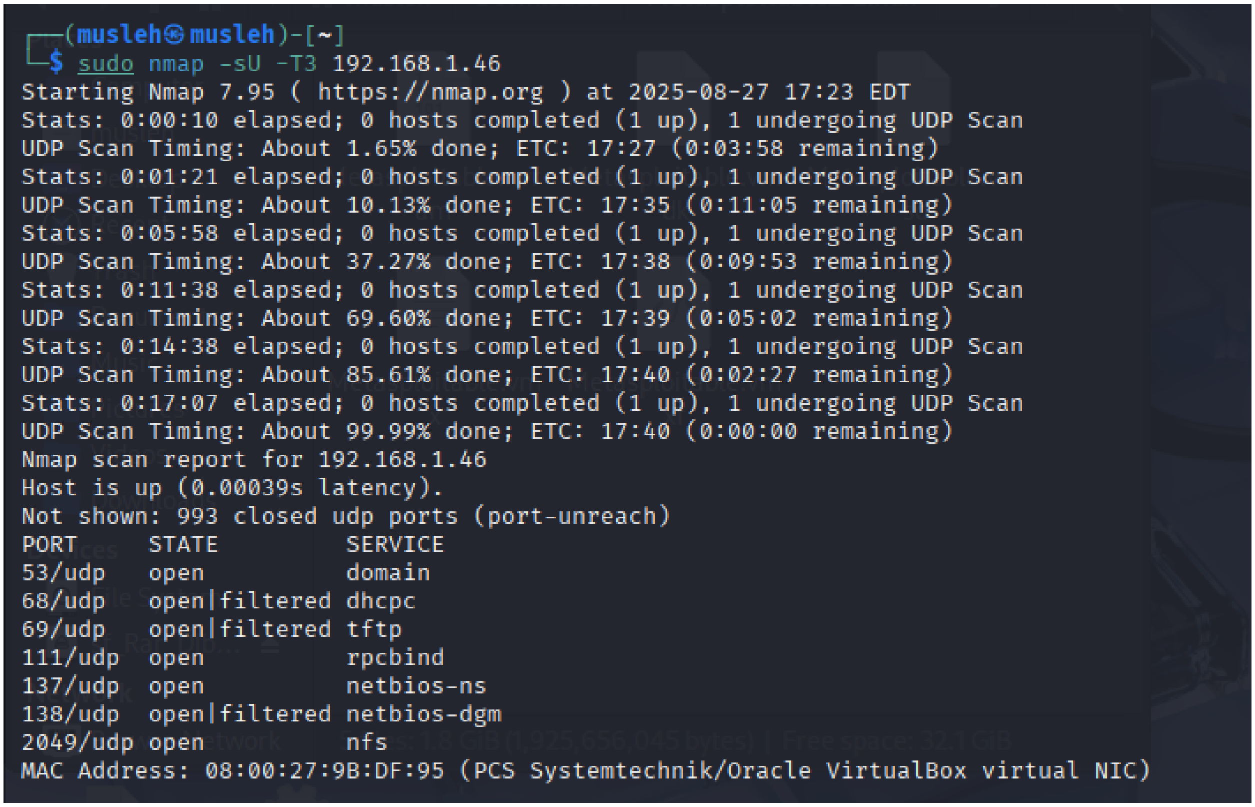
```
┌──(musleh㉿musleh)-[~]
└─$ nmap -sS 192.168.1.46
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-27 16:17 EDT
Nmap scan report for 192.168.1.46
Host is up (0.00019s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

2. Which switch would you use for a “UDP scan”?

Answer:

-sU

The -sU switch is used to perform a UDP scan, which checks for open UDP ports on the target system.



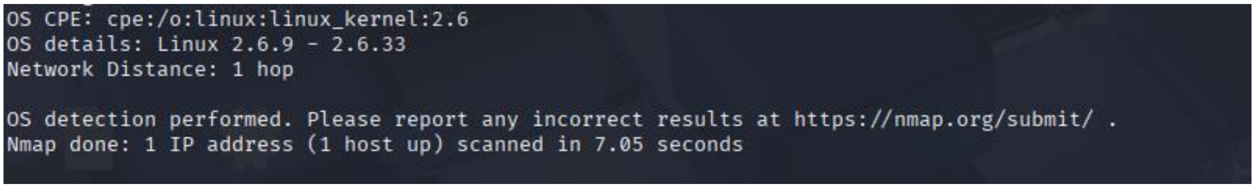
```
┌──(musleh㉿musleh)-[~]
└─$ sudo nmap -sU -T3 192.168.1.46
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-27 17:23 EDT
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 1.65% done; ETC: 17:27 (0:03:58 remaining)
Stats: 0:01:21 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 10.13% done; ETC: 17:35 (0:11:05 remaining)
Stats: 0:05:58 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 37.27% done; ETC: 17:38 (0:09:53 remaining)
Stats: 0:11:38 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 69.60% done; ETC: 17:39 (0:05:02 remaining)
Stats: 0:14:38 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 85.61% done; ETC: 17:40 (0:02:27 remaining)
Stats: 0:17:07 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 17:40 (0:00:00 remaining)
Nmap scan report for 192.168.1.46
Host is up (0.00039s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT     STATE         SERVICE
53/udp   open          domain
68/udp   open|filtered dhcpc
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open          nfs
MAC Address: 08:00:27:9B:DF:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

3. If you wanted to detect which operating system the target is running on, which switch would you use?

Answer:

-O

The -O switch enables OS detection, allowing Nmap to attempt to determine the operating system of the target host.



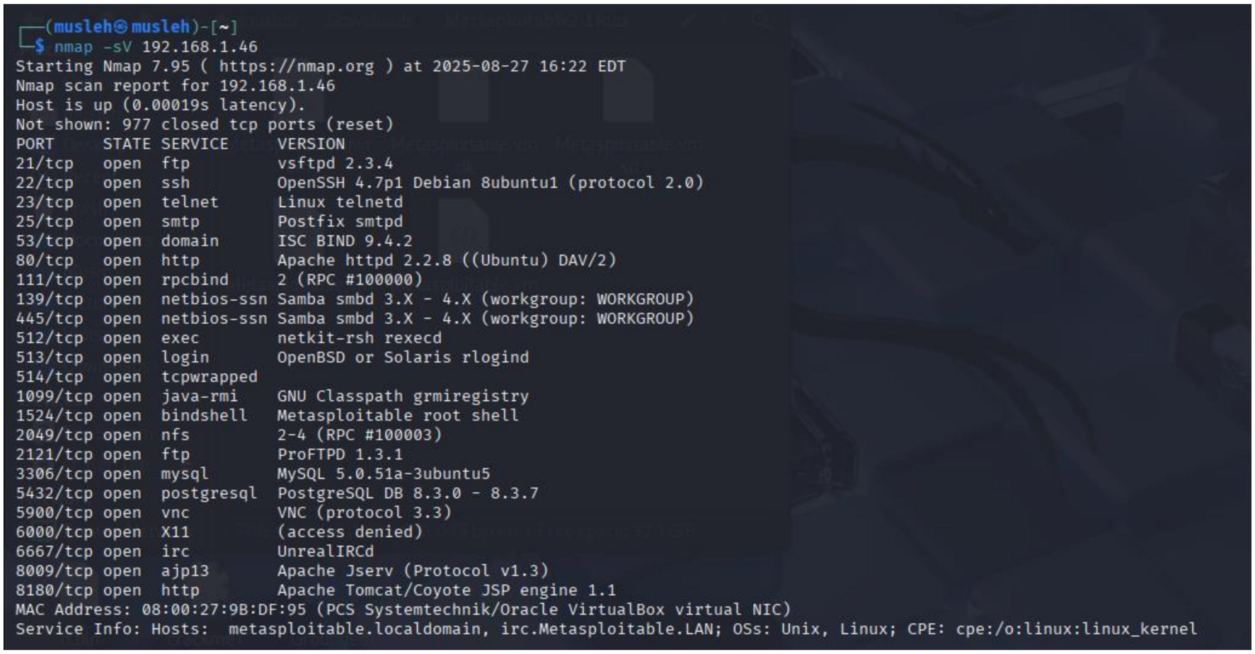
```
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.05 seconds
```

4. Nmap provides a switch to detect the version of the services running on the target. What is this switch?

Answer:

-sV

The -sV switch enables version detection, which attempts to determine the versions of services running on open ports.



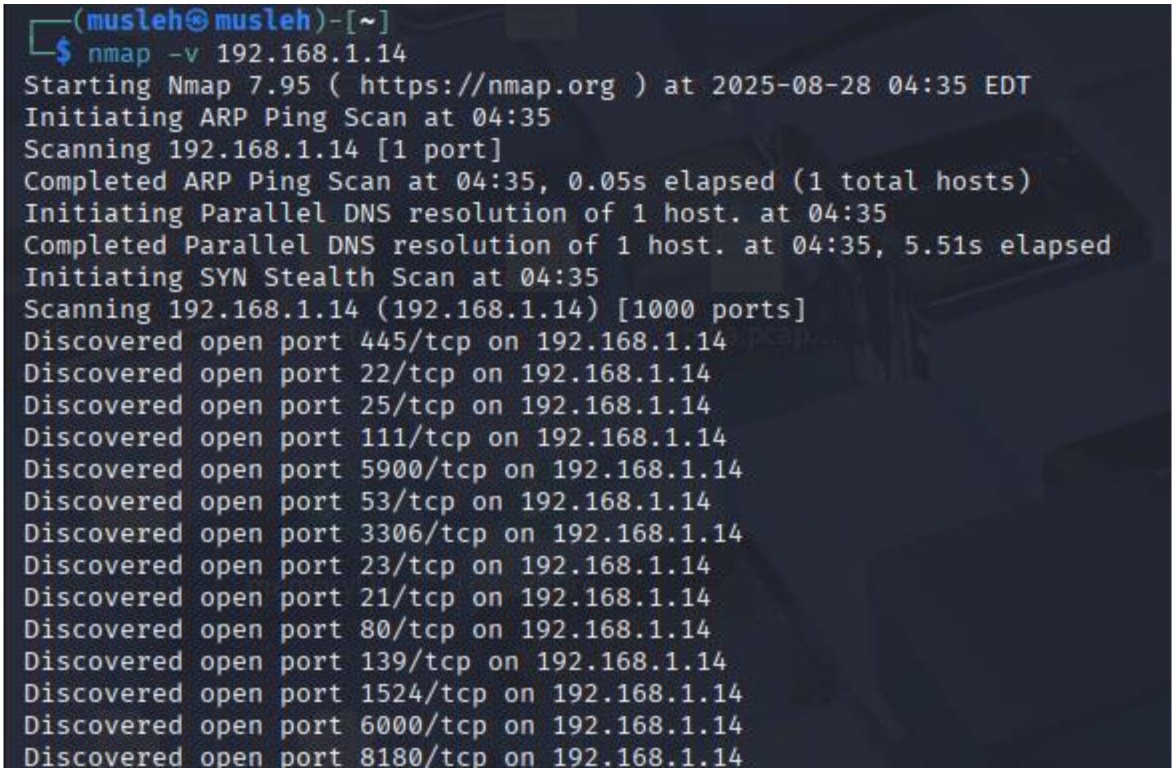
```
┌──(musleh㉿musleh)-[~]
└─$ nmap -sV 192.168.1.46
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-27 16:22 EDT
Nmap scan report for 192.168.1.46
Host is up (0.00019s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:9B:DF:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

5. The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity?

Answer:

-v

The -v switch increases the verbosity level, providing more detailed information during the scan process.



```
┌──(musleh㉿musleh)-[~]
└─$ nmap -v 192.168.1.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-28 04:35 EDT
Initiating ARP Ping Scan at 04:35
Scanning 192.168.1.14 [1 port]
Completed ARP Ping Scan at 04:35, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:35
Completed Parallel DNS resolution of 1 host. at 04:35, 5.51s elapsed
Initiating SYN Stealth Scan at 04:35
Scanning 192.168.1.14 (192.168.1.14) [1000 ports]
Discovered open port 445/tcp on 192.168.1.14
Discovered open port 22/tcp on 192.168.1.14
Discovered open port 25/tcp on 192.168.1.14
Discovered open port 111/tcp on 192.168.1.14
Discovered open port 5900/tcp on 192.168.1.14
Discovered open port 53/tcp on 192.168.1.14
Discovered open port 3306/tcp on 192.168.1.14
Discovered open port 23/tcp on 192.168.1.14
Discovered open port 21/tcp on 192.168.1.14
Discovered open port 80/tcp on 192.168.1.14
Discovered open port 139/tcp on 192.168.1.14
Discovered open port 1524/tcp on 192.168.1.14
Discovered open port 6000/tcp on 192.168.1.14
Discovered open port 8180/tcp on 192.168.1.14
```

6. Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two?

Answer:

-vv

The -vv switch sets the verbosity level to two, offering even more detailed output than the -v switch.

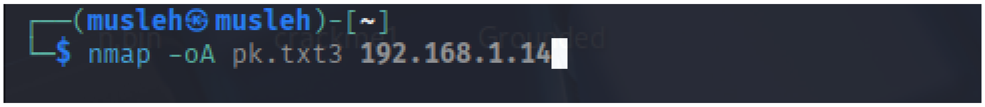
***same as above but with more scanning details.**

7. What switch would you use to save the nmap results in three major formats?

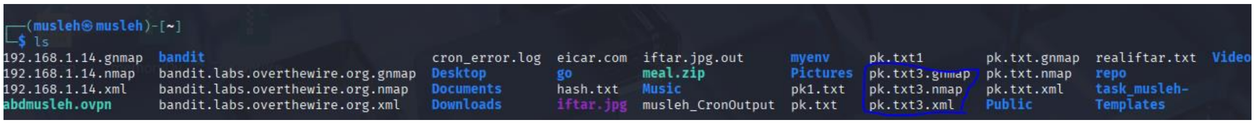
Answer:

-oA

The -oA switch saves the scan results in all three major formats: normal, XML, and greppable



```
┌──(musleh㉿musleh)-[~]
└─$ nmap -oA pk.txt3 192.168.1.14
```



```
┌──(musleh㉿musleh)-[~]
└─$ ls
192.168.1.14.gnmap  bandit                              cron_error.log  eicar.com  iftar.jpg.out       myenv     pk.txt1          pk.txt.gnmap  realiftar.txt  Videos
192.168.1.14.nmap   bandit.labs.overthewire.org.gnmap   Desktop         go         meal.zip            Pictures  pk.txt3.gnmap    pk.txt.nmap   repo
192.168.1.14.xml    bandit.labs.overthewire.org.nmap    Documents       hash.txt   Music               pk1.txt   pk.txt3.nmap     pk.txt.xml    task_musleh-
abdmusleh.ovpn      bandit.labs.overthewire.org.xml     Downloads       iftar.jpg  musleh_CronOutput   pk.txt    pk.txt3.xml      Public        Templates
```

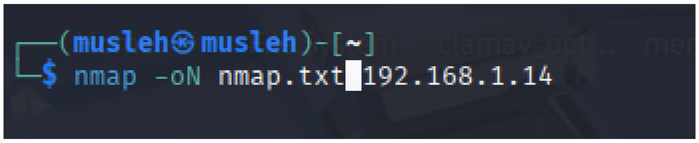
As you see the out put is the scanning result in three diffrenet file format based on the file I chose which was pk.txt3

8. What switch would you use to save the nmap results in a "normal" format?

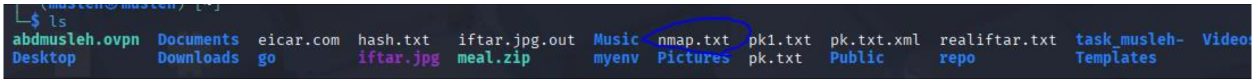
Answer:

-oN

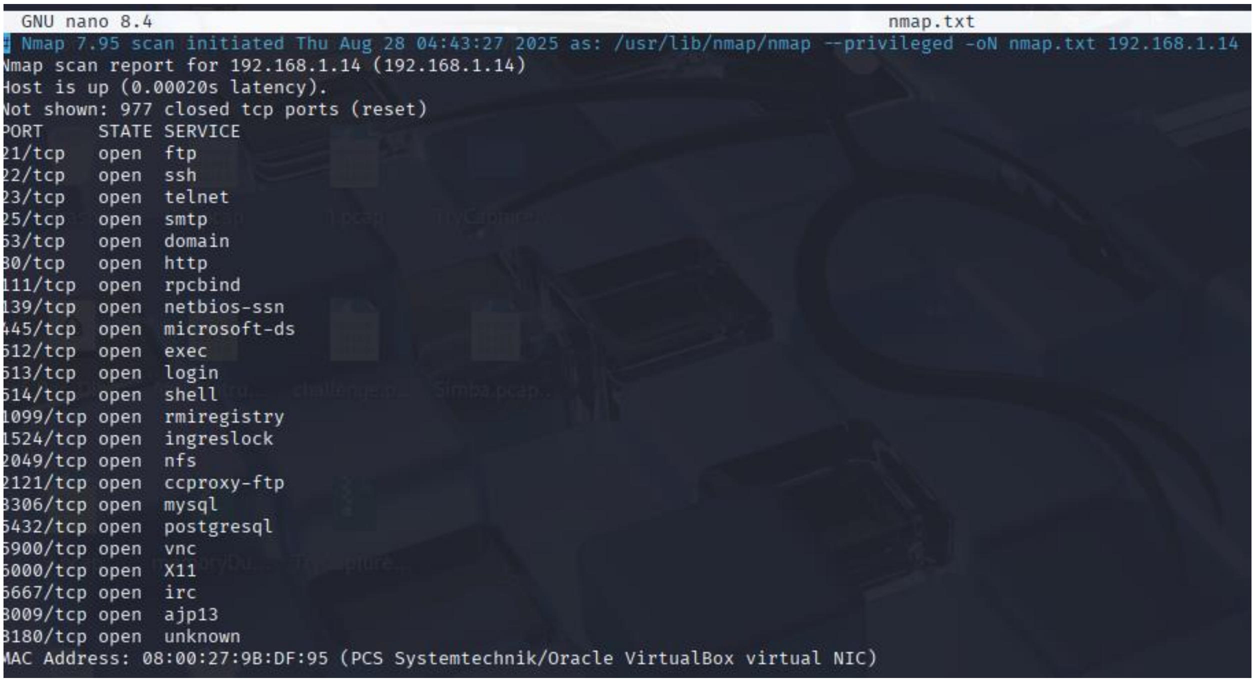
The -oN switch saves the scan results in a human-readable "normal" format.



```
┌──(musleh㉿musleh)-[~]
└─$ nmap -oN nmap.txt 192.168.1.14
```



```
└─$ ls
abdmusleh.ovpn  Documents  eicar.com  hash.txt   iftar.jpg.out  Music  nmap.txt  pk1.txt  pk.txt.xml  realiftar.txt  task_musleh-  Videos
Desktop         Downloads  go         iftar.jpg  meal.zip       myenv  Pictures  pk.txt   Public      repo           Templates
```



```
 GNU nano 8.4                                                        nmap.txt
# Nmap 7.95 scan initiated Thu Aug 28 04:43:27 2025 as: /usr/lib/nmap/nmap --privileged -oN nmap.txt 192.168.1.14
Nmap scan report for 192.168.1.14 (192.168.1.14)
Host is up (0.00020s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:9B:DF:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

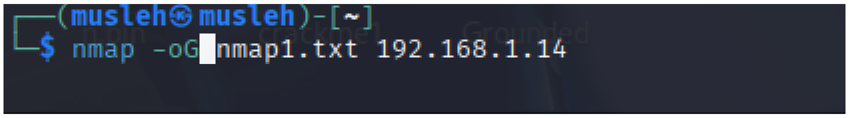
***this is how the file look like inside.**

9. A very useful output format: how would you save results in a “grepable” format?

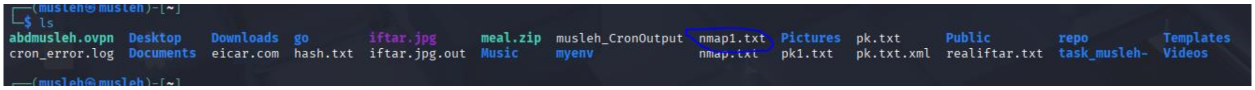
Answer:

-oG

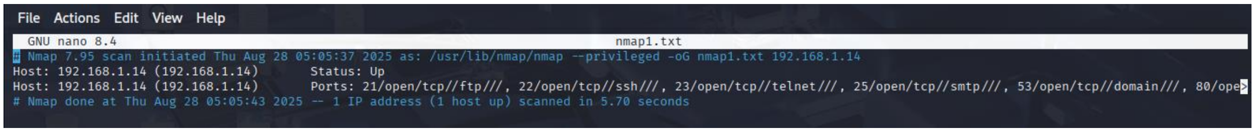
The -oG switch saves the scan results in a format that is easy to parse with tools like grep.



```
┌──(musleh㉿musleh)-[~]
└─$ nmap -oG nmap1.txt 192.168.1.14
```



```
┌──(musleh㉿musleh)-[~]
└─$ ls
abdmusleh.ovpn  Desktop    Downloads  go        iftar.jpg      meal.zip  musleh_CronOutput  nmap1.txt  Pictures  pk.txt      Public           repo          Templates
cron_error.log  Documents  eicar.com  hash.txt  iftar.jpg.out  Music     myenv              nmap.txt   pk1.txt   pk.txt.xml  realiftar.txt  task_musleh-  Videos

┌──(musleh㉿musleh)-[~]
```



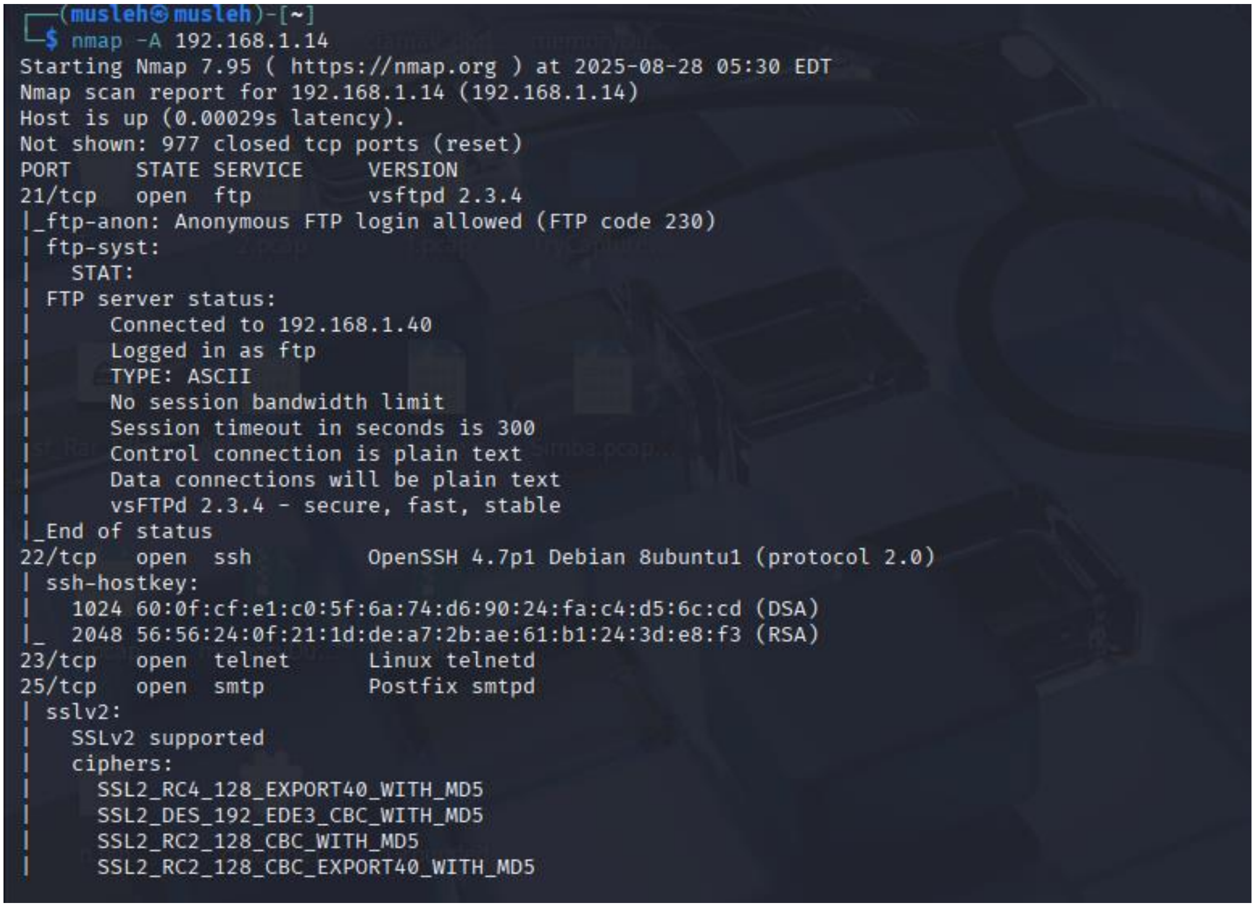
```
 GNU nano 8.4                                   nmap1.txt
# Nmap 7.95 scan initiated Thu Aug 28 05:05:37 2025 as: /usr/lib/nmap/nmap --privileged -oG nmap1.txt 192.168.1.14
Host: 192.168.1.14 (192.168.1.14)       Status: Up
Host: 192.168.1.14 (192.168.1.14)       Ports: 21/open/tcp//ftp///, 22/open/tcp//ssh///, 23/open/tcp//telnet///, 25/open/tcp//smtp///, 53/open/tcp//domain///, 80/ope>
# Nmap done at Thu Aug 28 05:05:43 2025 -- 1 IP address (1 host up) scanned in 5.70 seconds
```

10. Sometimes the results we're getting just aren't enough. If we don't care about how loud we are, we can enable "aggressive" mode. This is a shorthand switch that activates service detection, operating system detection, a traceroute and common script scanning. How would you activate this setting?

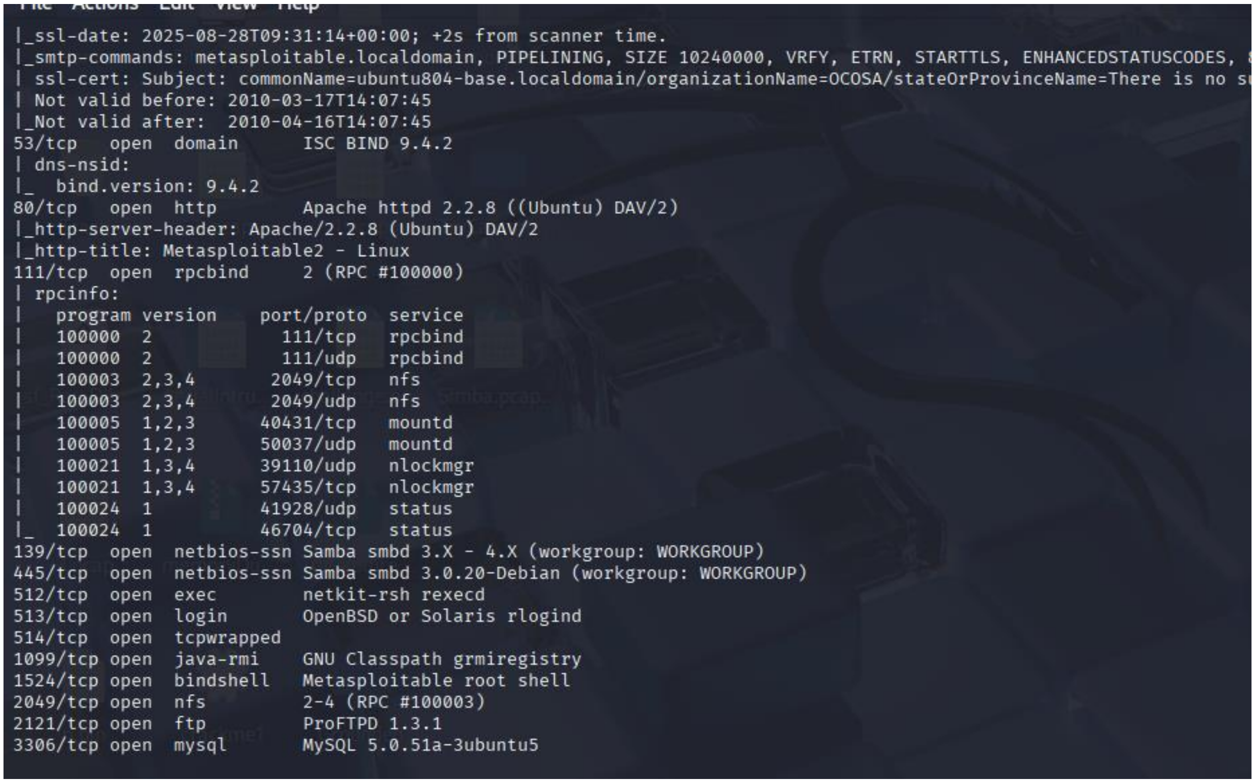
Answer:

-A

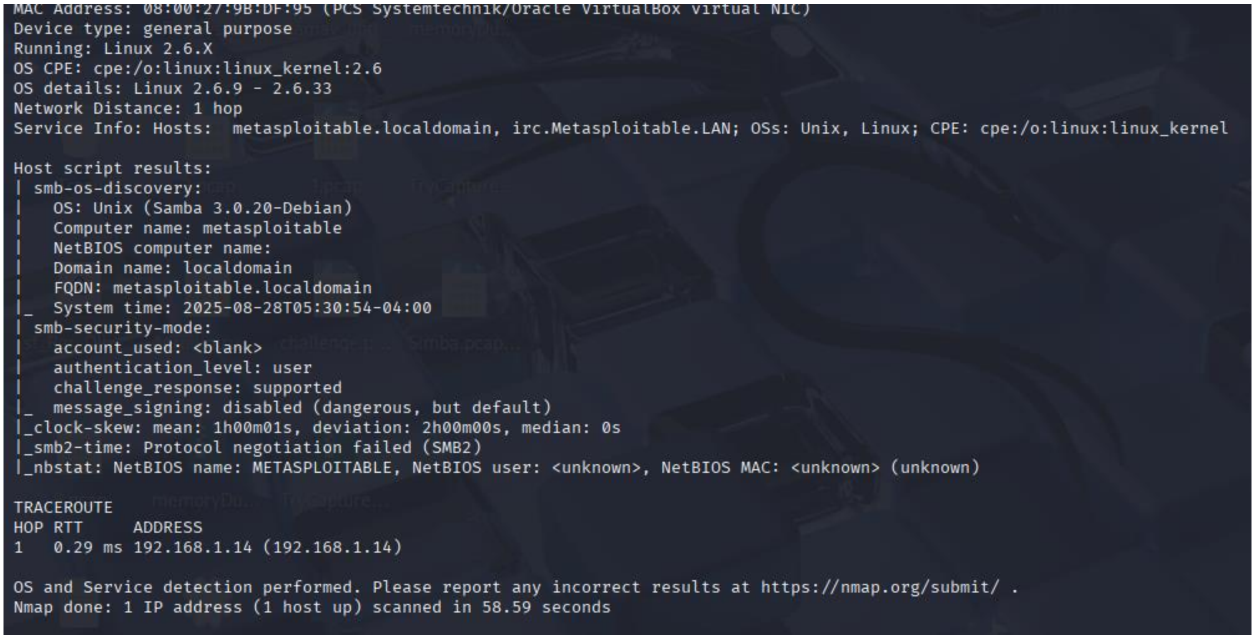
The -A switch enables aggressive scanning, which includes OS detection, version detection, script scanning, and traceroute



```
┌──(musleh㉿musleh)-[~]
└─$ nmap -A 192.168.1.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-28 05:30 EDT
Nmap scan report for 192.168.1.14 (192.168.1.14)
Host is up (0.00029s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.40
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
```



```
|_ssl-date: 2025-08-28T09:31:14+00:00; +2s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no su
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      40431/tcp   mountd
|   100005  1,2,3      50037/udp   mountd
|   100021  1,3,4      39110/udp   nlockmgr
|   100021  1,3,4      57435/tcp   nlockmgr
|   100024  1          41928/udp   status
|_  100024  1          46704/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
```



```
MAC Address: 08:00:27:9B:DF:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-08-28T05:30:54-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h00m01s, deviation: 2h00m00s, median: 0s
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT     ADDRESS
1   0.29 ms 192.168.1.14 (192.168.1.14)

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 58.59 seconds
```

- **-A gets you a lot of stuff right? Well be carefull it is very loud and noisy (aggressive)**

11. How would you set the timing template to level 5?

Answer:

-T5

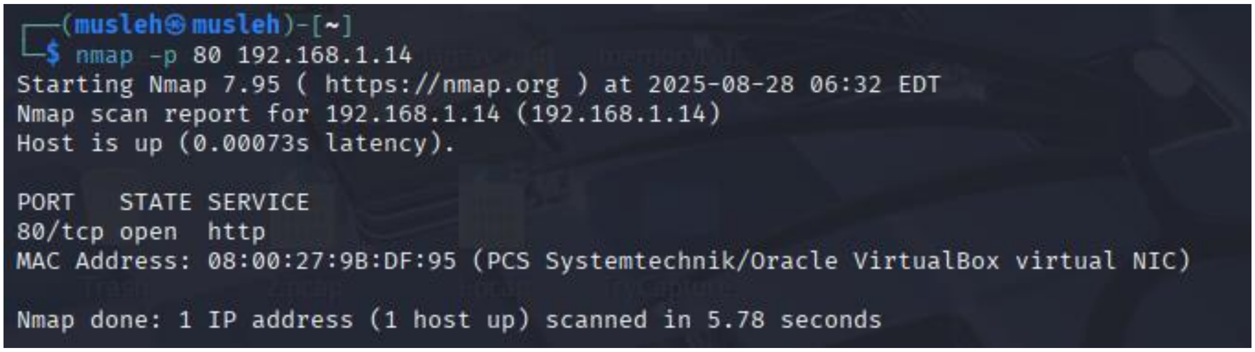
The -T5 switch sets the timing template to level 5, which is the fastest and most aggressive scan timing.

12. How would you tell nmap to only scan port 80?

Answer:

-p 80

The -p 80 switch tells Nmap to scan only port 80, commonly used for HTTP services.



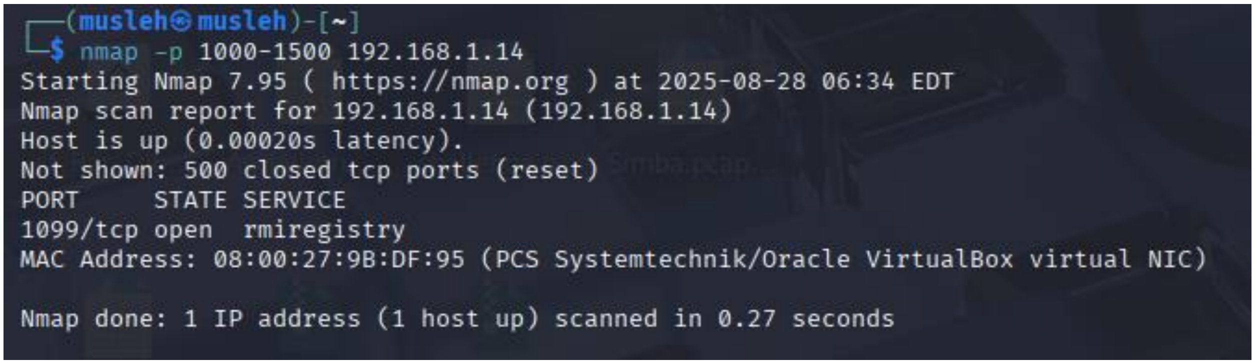
```
┌──(musleh㉿musleh)-[~]
└─$ nmap -p 80 192.168.1.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-28 06:32 EDT
Nmap scan report for 192.168.1.14 (192.168.1.14)
Host is up (0.00073s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:9B:DF:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.78 seconds
```

13. How would you tell nmap to scan ports 1000–1500?

Answer:

-p 1000-1500

The -p 1000-1500 switch specifies a range of ports to scan, in this case, ports 1000 through 1500.



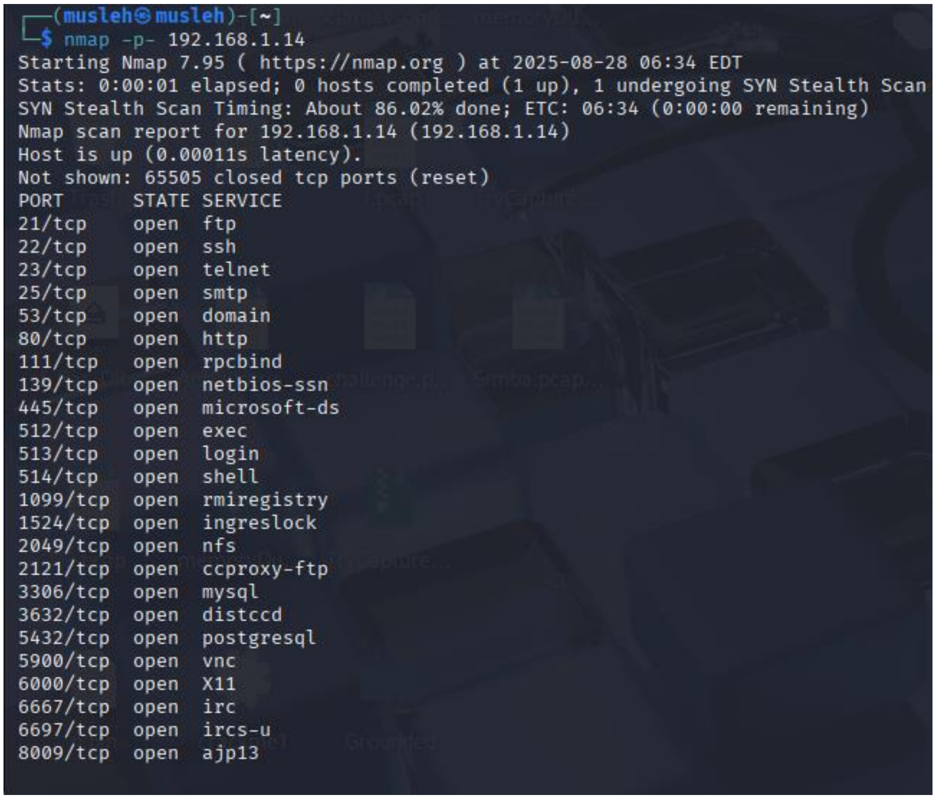
```
┌──(musleh㉿musleh)-[~]
└─$ nmap -p 1000-1500 192.168.1.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-28 06:34 EDT
Nmap scan report for 192.168.1.14 (192.168.1.14)
Host is up (0.00020s latency).
Not shown: 500 closed tcp ports (reset)
PORT     STATE SERVICE
1099/tcp open  rmiregistry
MAC Address: 08:00:27:9B:DF:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

14. How would you tell nmap to scan all ports?

Answer:

-p-

The -p- switch tells Nmap to scan all 65535 ports



```
┌──(musleh㉿musleh)-[~]
└─$ nmap -p- 192.168.1.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-28 06:34 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 86.02% done; ETC: 06:34 (0:00:00 remaining)
Nmap scan report for 192.168.1.14 (192.168.1.14)
Host is up (0.00011s latency).
Not shown: 65505 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
3632/tcp open  distccd
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
6697/tcp open  ircs-u
8009/tcp open  ajp13
```

15. How would you activate a script from the nmap scripting library (lots more on this later!)?

Answer:

--script

The --script switch allows you to specify a particular Nmap Scripting Engine (NSE) script to run during the scan.

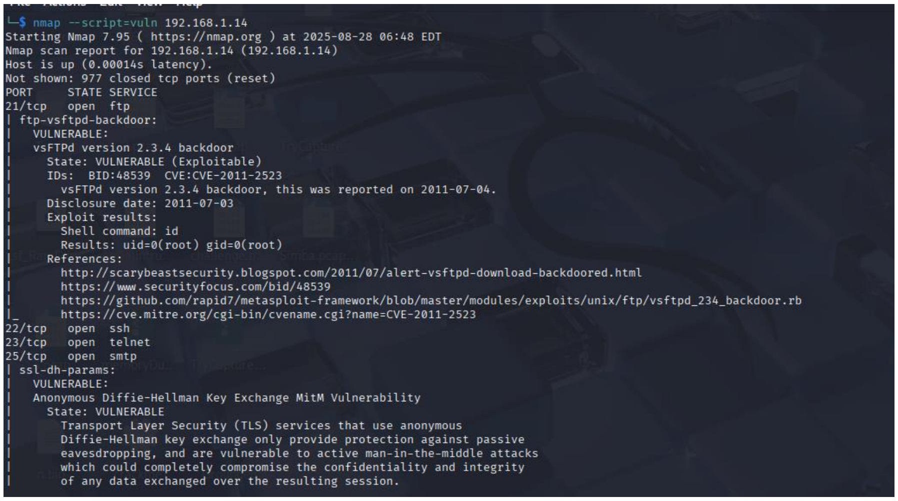
16. How would you activate all of the scripts in the “vuln” category?

Answer:

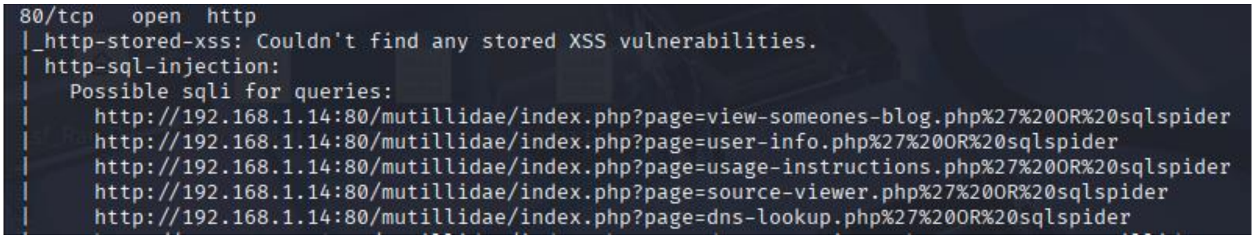
--script=vuln

The --script=vuln switch tells Nmap to run all scripts in the "vuln" category, which are designed to detect vulnerabilities.

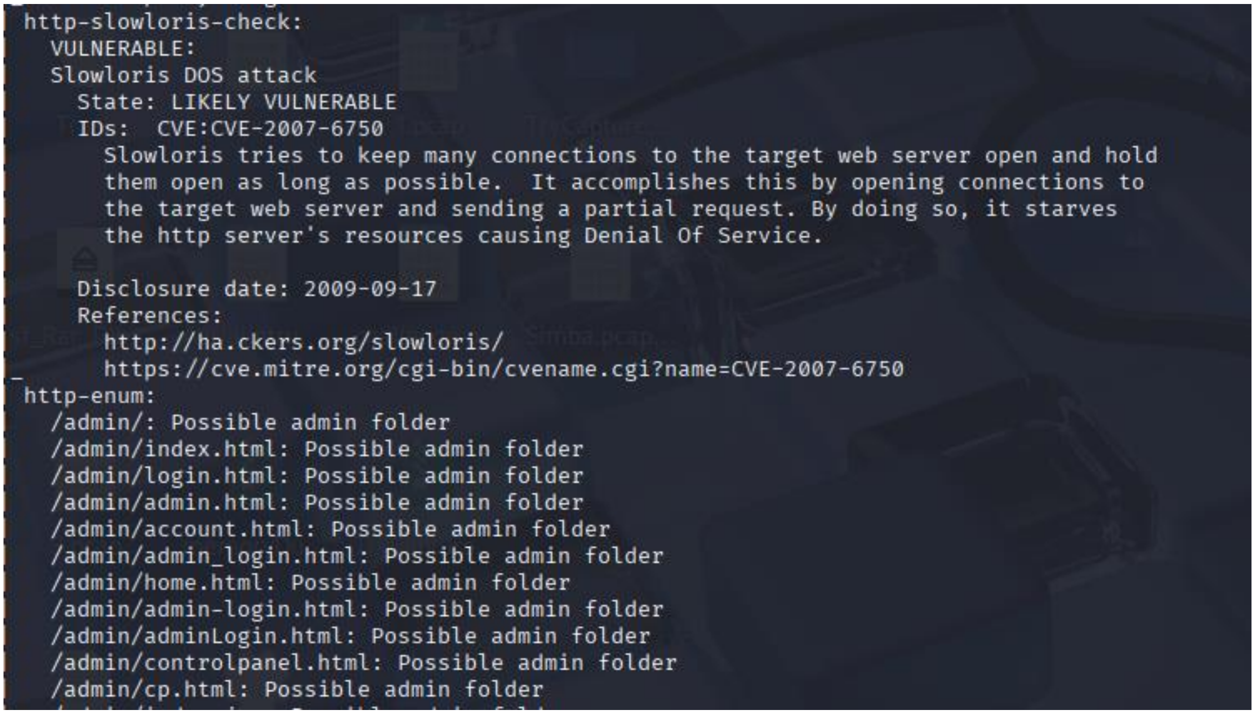
***now vuln scanning on metasploitable are very intresting lets take a look on there:**



```
└─$ nmap --script=vuln 192.168.1.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-28 06:48 EDT
Nmap scan report for 192.168.1.14 (192.168.1.14)
Host is up (0.00014s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://www.securityfocus.com/bid/48539
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
```



```
80/tcp   open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.1.14:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.14:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.14:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
|     http://192.168.1.14:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.14:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
```



```
 http-slowloris-check:
   VULNERABLE:
   Slowloris DOS attack
     State: LIKELY VULNERABLE
     IDs:  CVE:CVE-2007-6750
       Slowloris tries to keep many connections to the target web server open and hold
       them open as long as possible.  It accomplishes this by opening connections to
       the target web server and sending a partial request. By doing so, it starves
       the http server's resources causing Denial Of Service.

     Disclosure date: 2009-09-17
     References:
       http://ha.ckers.org/slowloris/
_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
 http-enum:
   /admin/: Possible admin folder
   /admin/index.html: Possible admin folder
   /admin/login.html: Possible admin folder
   /admin/admin.html: Possible admin folder
   /admin/account.html: Possible admin folder
   /admin/admin_login.html: Possible admin folder
   /admin/home.html: Possible admin folder
   /admin/admin-login.html: Possible admin folder
   /admin/adminLogin.html: Possible admin folder
   /admin/controlpanel.html: Possible admin folder
   /admin/cp.html: Possible admin folder
```

Task 4: Scan Types Overview

Read the Scan Types Introduction.

Answer:

No answer needed.

Task 5: Scan Types TCP Connect Scans

1. Which RFC defines the appropriate behaviour for the TCP protocol?

Answer:

RFC 793

RFC 793 defines the Transmission Control Protocol (TCP) and its behavior, including how connections are established and terminated.

2. If a port is closed, which flag should the server send back to indicate this?

Answer:

RST

If a port is closed, the server should respond with a TCP packet containing the RST (Reset) flag to indicate that the connection is not allowed.

Task 6: SYN Scans

1. There are two other names for a SYN scan, what are they?

Answer:

Half-open, Stealth

SYN scans are sometimes referred to as "Half-open" scans or "Stealth" scans because they don't complete the full TCP handshake, making them less detectable.

2. Can Nmap use a SYN scan without Sudo permissions (Y/N)?

Answer:

N

Nmap requires root (sudo) privileges to send raw packets necessary for SYN scans. Without these privileges, Nmap defaults to a TCP connect scan.

Task 7: UDP Scans:

1. If a UDP port doesn’t respond to an Nmap scan, what will it be marked as?

Answer:

open|filtered

If a UDP port doesn't respond, Nmap marks it as "open|filtered" because it's unclear whether the port is open or the response was filtered by a firewall

2. When a UDP port is closed, by convention the target should send back a “port unreachable” message. Which protocol would it use to do so?

Answer:

ICMP

When a UDP port is closed, the target should respond with an ICMP "port unreachable" message to indicate that the port is not available.

Task 8: NULL, FIN, Xmas Scans

1- Which scan uses the URG flag?

Answer: Xmas scan

Xmas scans set FIN, PSH, and URG flags, making packets appear “decorated” like a Christmas tree.

2- Why use NULL, FIN, Xmas scans?

Answer: To evade firewall/IDS detection

Some firewalls/IDS ignore these unusual packets, making them useful for stealth scanning.

3- Which OS responds with RST for these scans?

Answer: Microsoft Windows

Explanation: Windows responds with RST on closed ports for these unusual packets, limiting the scan’s effectiveness.

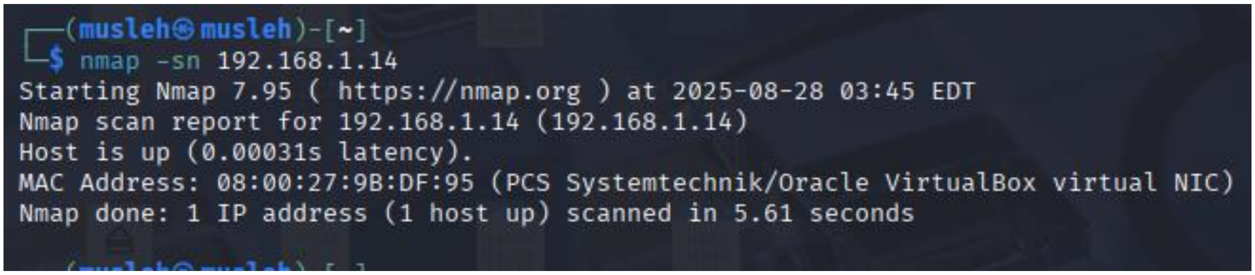
Task 9: ICMP Network Scanning

1. How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? (CIDR notation)

Answer:

nmap -sn 172.16.0.0/16

The -sn switch tells Nmap to perform a ping sweep (host discovery) without port scanning. The /16 CIDR notation specifies the 172.16.x.x network with a netmask of 255.255.0.0



```
┌──(musleh㉿musleh)-[~]
└─$ nmap -sn 192.168.1.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-28 03:45 EDT
Nmap scan report for 192.168.1.14 (192.168.1.14)
Host is up (0.00031s latency).
MAC Address: 08:00:27:9B:DF:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 5.61 seconds

┌──(musleh㉿musleh)-[~]
```

Task 10: NSE Scripts Overview

1- What language are NSE scripts written in?

Answer: Lua

2- Which categories are considered safe?

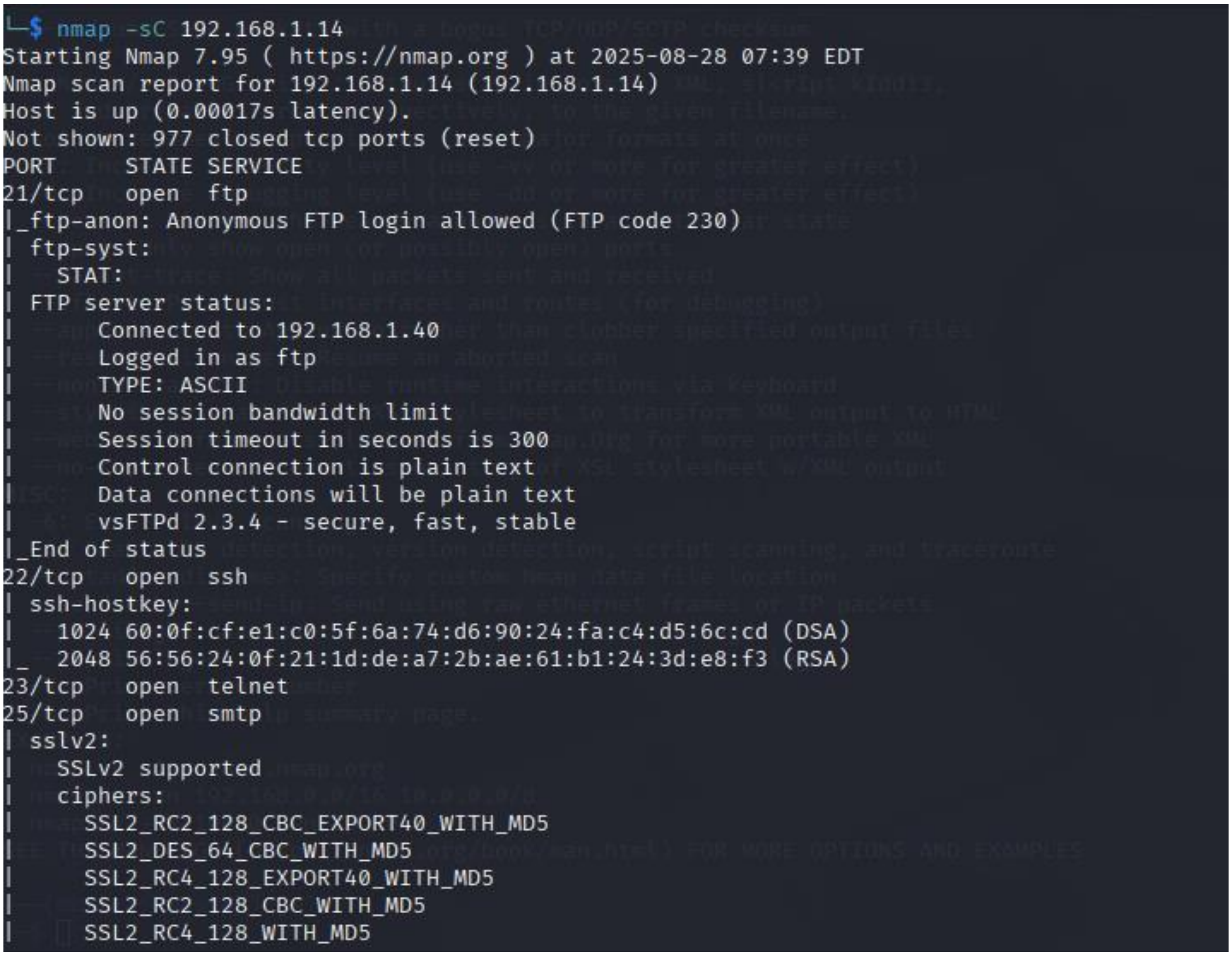
Answer: safe

3- Which categories may be intrusive or dangerous?

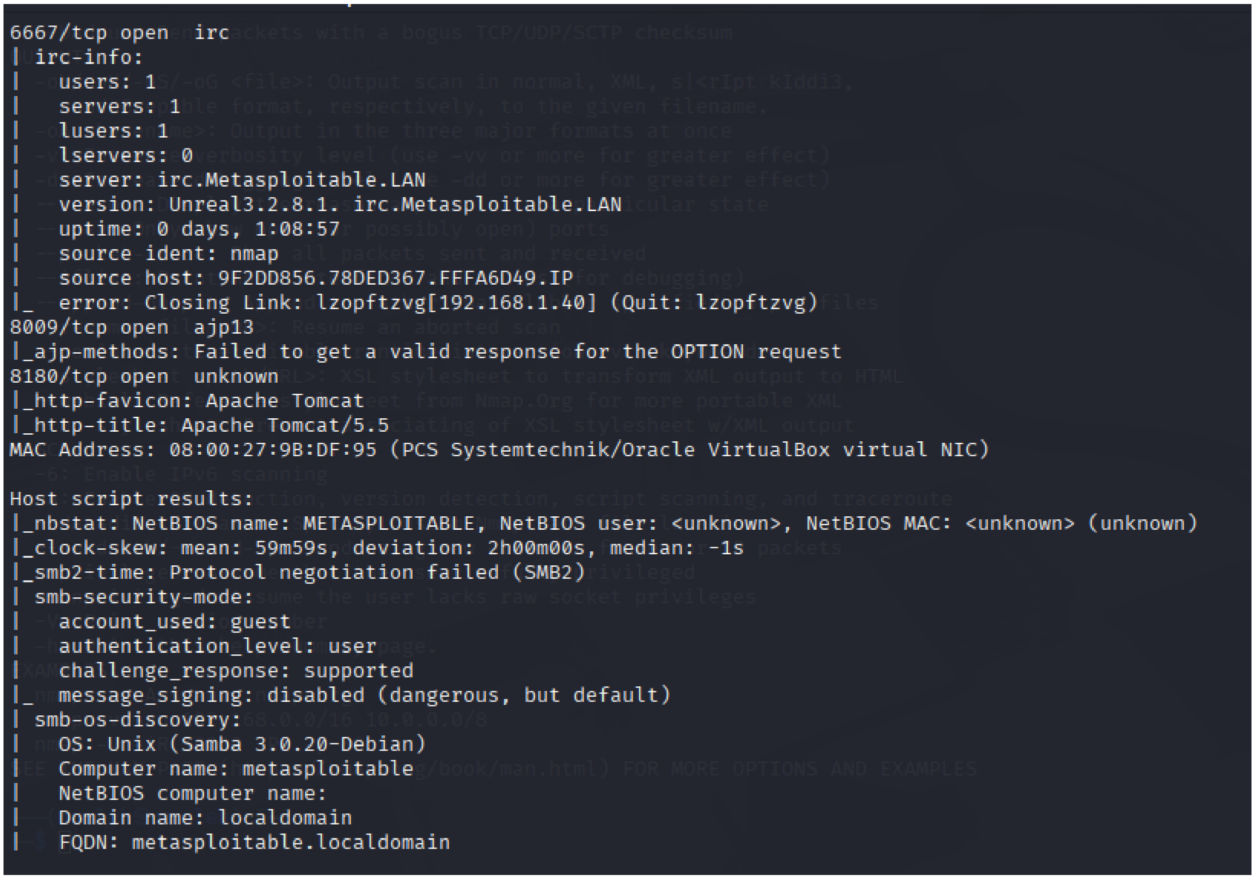
Answer: intrusive, exploit, dos

4- How to run default scripts?

Answer: -sC or --script=default



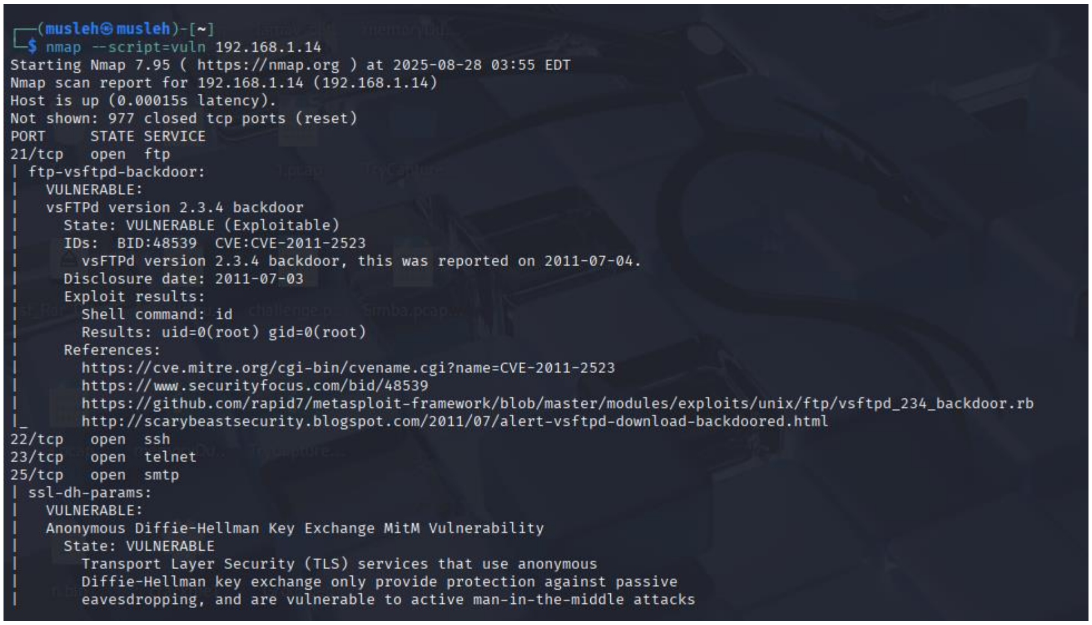
```
└─$ nmap -sC 192.168.1.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-28 07:39 EDT
Nmap scan report for 192.168.1.14 (192.168.1.14)
Host is up (0.00017s latency).
Not shown: 977 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.40
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp  open  ssh
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp  open  telnet
25/tcp  open  smtp
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
```



```
6667/tcp open  irc
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 1:08:57
|   source ident: nmap
|   source host: 9F2DD856.78DED367.FFFA6D49.IP
|_  error: Closing Link: lzopftzvg[192.168.1.40] (Quit: lzopftzvg)
8009/tcp open  ajp13
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  unknown
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:9B:DF:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 59m59s, deviation: 2h00m00s, median: -1s
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
```

5- How to run a specific category, like vuln?

Answer: --script=vuln



```
┌──(musleh㉿musleh)-[~]
└─$ nmap --script=vuln 192.168.1.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-28 03:55 EDT
Nmap scan report for 192.168.1.14 (192.168.1.14)
Host is up (0.00015s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://www.securityfocus.com/bid/48539
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
```

Task 11 : Working With NSE:

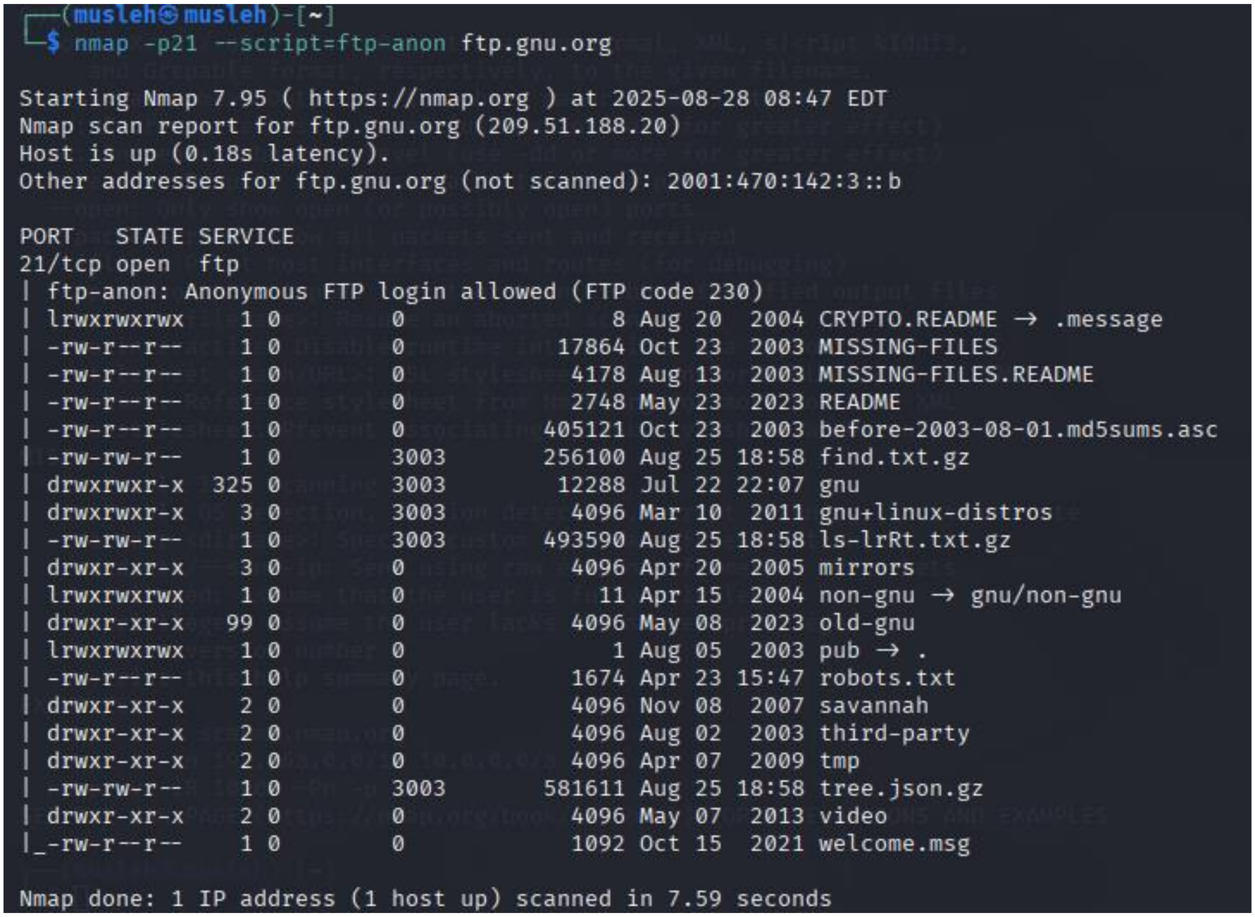
Question: what optional argument can the ftp-anon.nse script take?

Answer: maxlist

The ftp-anon.nse script in Nmap checks if an FTP server allows anonymous logins and retrieves a directory listing of the root directory. It highlights writable files if anonymous access is permitted.

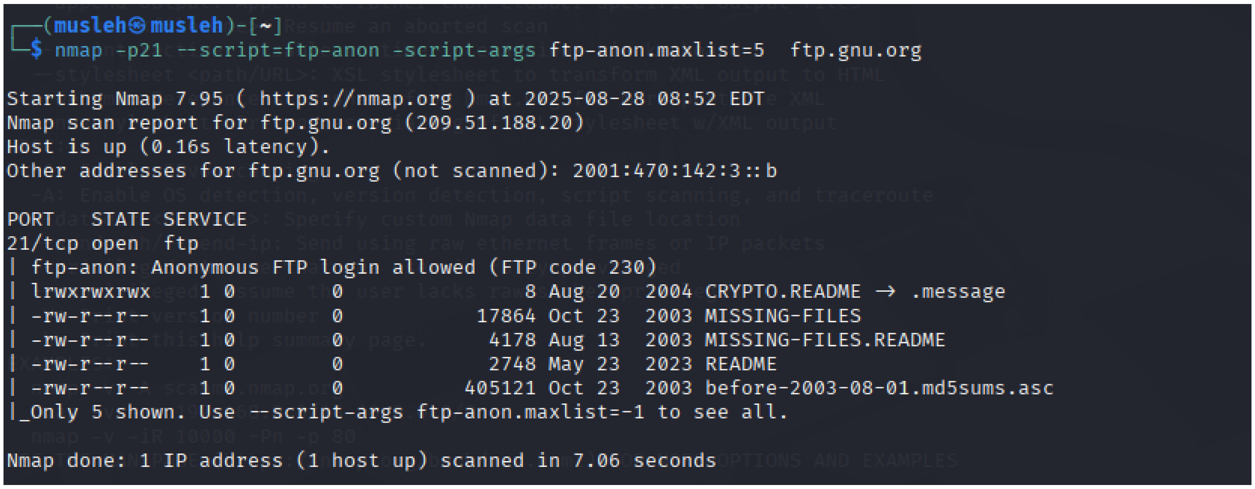
maxlist: Specifies the maximum number of files to return in the directory listing

***here is an example for ftp-anon:**



```
┌──(musleh㉿musleh)-[~]
└─$ nmap -p21 --script=ftp-anon ftp.gnu.org

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-28 08:47 EDT
Nmap scan report for ftp.gnu.org (209.51.188.20)
Host is up (0.18s latency).
Other addresses for ftp.gnu.org (not scanned): 2001:470:142:3::b

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| lrwxrwxrwx    1 0        0               8 Aug 20  2004 CRYPTO.README → .message
| -rw-r--r--    1 0        0           17864 Oct 23  2003 MISSING-FILES
| -rw-r--r--    1 0        0            4178 Aug 13  2003 MISSING-FILES.README
| -rw-r--r--    1 0        0            2748 May 23  2023 README
| -rw-r--r--    1 0        0          405121 Oct 23  2003 before-2003-08-01.md5sums.asc
| -rw-rw-r--    1 0        3003       256100 Aug 25 18:58 find.txt.gz
| drwxrwxr-x  325 0        3003        12288 Jul 22 22:07 gnu
| drwxrwxr-x    3 0        3003         4096 Mar 10  2011 gnu+linux-distros
| -rw-rw-r--    1 0        3003       493590 Aug 25 18:58 ls-lrRt.txt.gz
| drwxr-xr-x    3 0        0            4096 Apr 20  2005 mirrors
| lrwxrwxrwx    1 0        0              11 Apr 15  2004 non-gnu → gnu/non-gnu
| drwxr-xr-x   99 0        0            4096 May 08  2023 old-gnu
| lrwxrwxrwx    1 0        0               1 Aug 05  2003 pub → .
| -rw-r--r--    1 0        0            1674 Apr 23 15:47 robots.txt
| drwxr-xr-x    2 0        0            4096 Nov 08  2007 savannah
| drwxr-xr-x    2 0        0            4096 Aug 02  2003 third-party
| drwxr-xr-x    2 0        0            4096 Apr 07  2009 tmp
| -rw-rw-r--    1 0        3003       581611 Aug 25 18:58 tree.json.gz
| drwxr-xr-x    2 0        0            4096 May 07  2013 video
|_-rw-r--r--    1 0        0            1092 Oct 15  2021 welcome.msg

Nmap done: 1 IP address (1 host up) scanned in 7.59 seconds
```

And here if we want to use the optional argument:



```
┌──(musleh㉿musleh)-[~]
└─$ nmap -p21 --script=ftp-anon -script-args ftp-anon.maxlist=5  ftp.gnu.org

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-28 08:52 EDT
Nmap scan report for ftp.gnu.org (209.51.188.20)
Host is up (0.16s latency).
Other addresses for ftp.gnu.org (not scanned): 2001:470:142:3::b

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| lrwxrwxrwx    1 0        0               8 Aug 20  2004 CRYPTO.README -> .message
| -rw-r--r--    1 0        0           17864 Oct 23  2003 MISSING-FILES
| -rw-r--r--    1 0        0            4178 Aug 13  2003 MISSING-FILES.README
| -rw-r--r--    1 0        0            2748 May 23  2023 README
| -rw-r--r--    1 0        0          405121 Oct 23  2003 before-2003-08-01.md5sums.asc
|_Only 5 shown. Use --script-args ftp-anon.maxlist=-1 to see all.

Nmap done: 1 IP address (1 host up) scanned in 7.06 seconds
```

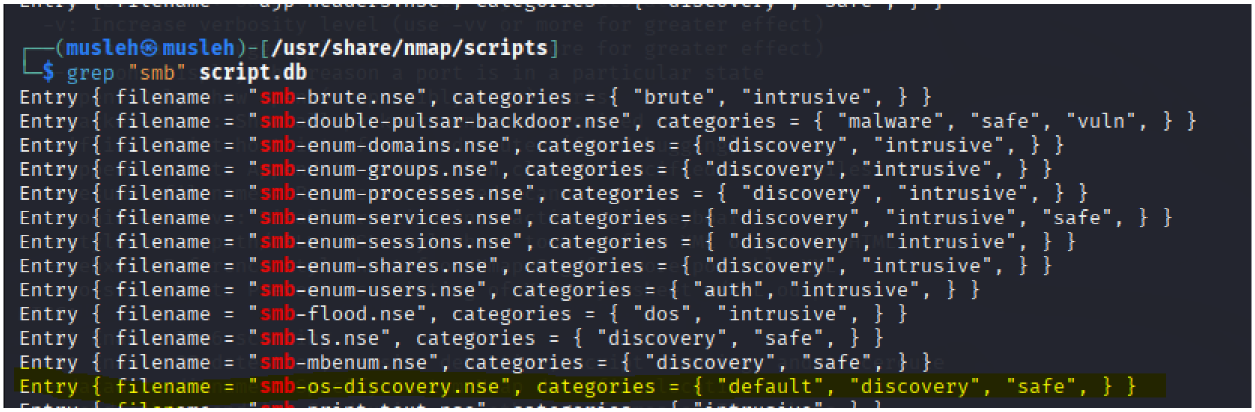
Task 12 : Searching for a Script:

Question: Search for "smb" scripts in the /usr/share/nmap/scripts/ directory using either of the demonstrated methods.

What is the filename of the script which determines the underlying OS of the SMB server?

Answer:

smb-os-discovery.nse



```
┌──(musleh㉿musleh)-[/usr/share/nmap/scripts]
└─$ grep "smb" script.db
Entry { filename = "smb-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "smb-double-pulsar-backdoor.nse", categories = { "malware", "safe", "vuln", } }
Entry { filename = "smb-enum-domains.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-groups.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-processes.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-services.nse", categories = { "discovery", "intrusive", "safe", } }
Entry { filename = "smb-enum-sessions.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-shares.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-users.nse", categories = { "auth", "intrusive", } }
Entry { filename = "smb-flood.nse", categories = { "dos", "intrusive", } }
Entry { filename = "smb-ls.nse", categories = { "discovery", "safe", } }
Entry { filename = "smb-mbenum.nse", categories = { "discovery", "safe", } }
Entry { filename = "smb-os-discovery.nse", categories = { "default", "discovery", "safe", } }
```

Question :

Read through this script. What does it depend on?

Answer:

Smb-Brute

Task 13 : Firewall evasion

Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the -Pn switch?

Answer: ICMP

Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?

Answer: --data-length

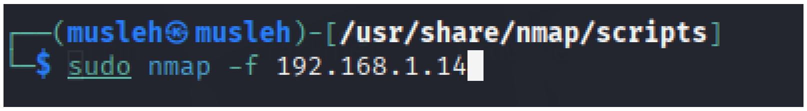
Nmap has a feature that lets you pad out packets with random data. This is achieved with the --data-length switch. By default, Nmap probes are relatively

small, which makes them easy to fingerprint by intrusion detection systems (IDS) or firewalls. When you add random padding, the packets become larger and more irregular, making it harder for security devices to distinguish them from normal network traffic

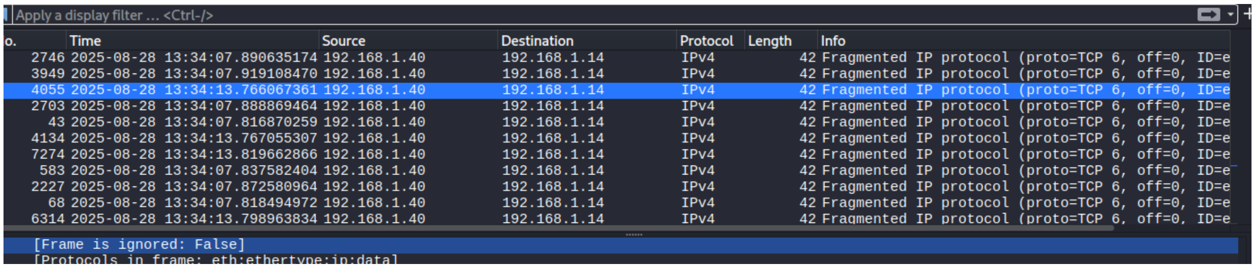
***now lets do a little experiment to actually showcase the difference between -f, mtu <number> , -badsum.**

The most practical why is by analyzing packets using wireshark

1- (-f)



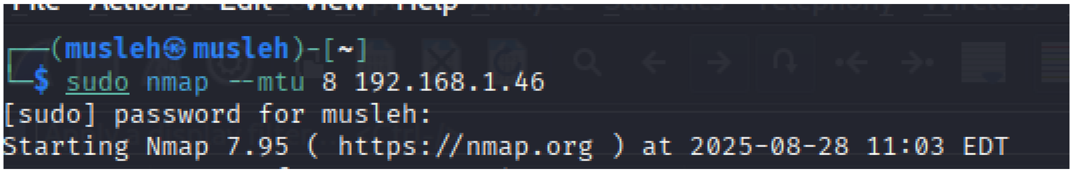
```
┌──(musleh㉿musleh)-[/usr/share/nmap/scripts]
└─$ sudo nmap -f 192.168.1.14
```



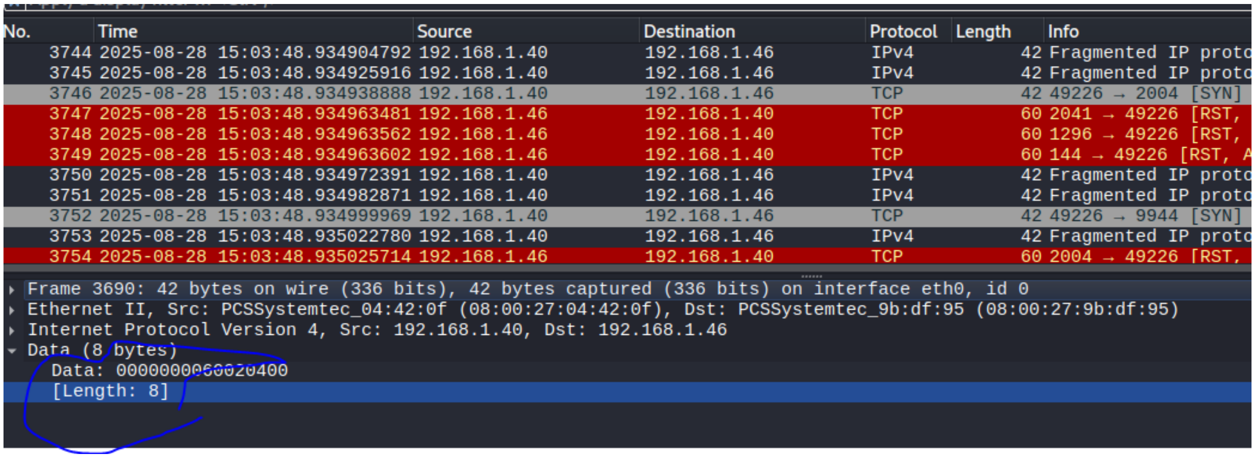
o.	Time	Source	Destination	Protocol	Length	Info
2746	2025-08-28 13:34:07.890635174	192.168.1.40	192.168.1.14	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=e
3949	2025-08-28 13:34:07.919108470	192.168.1.40	192.168.1.14	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=e
4055	2025-08-28 13:34:13.766067361	192.168.1.40	192.168.1.14	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=e
2703	2025-08-28 13:34:07.888869464	192.168.1.40	192.168.1.14	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=e
43	2025-08-28 13:34:07.816870259	192.168.1.40	192.168.1.14	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=e
4134	2025-08-28 13:34:13.767055307	192.168.1.40	192.168.1.14	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=e
7274	2025-08-28 13:34:13.819662866	192.168.1.40	192.168.1.14	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=e
583	2025-08-28 13:34:07.837582404	192.168.1.40	192.168.1.14	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=e
2227	2025-08-28 13:34:07.872580964	192.168.1.40	192.168.1.14	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=e
68	2025-08-28 13:34:07.818494972	192.168.1.40	192.168.1.14	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=e
6314	2025-08-28 13:34:13.798963834	192.168.1.40	192.168.1.14	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=e

```
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:data]
```

2- mtu + number

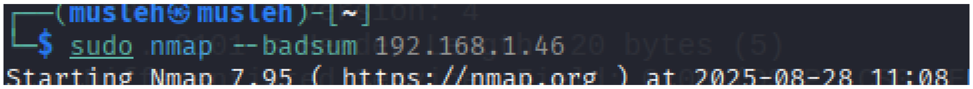


```
┌──(musleh㉿musleh)-[~]
└─$ sudo nmap --mtu 8 192.168.1.46
[sudo] password for musleh:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-28 11:03 EDT
```

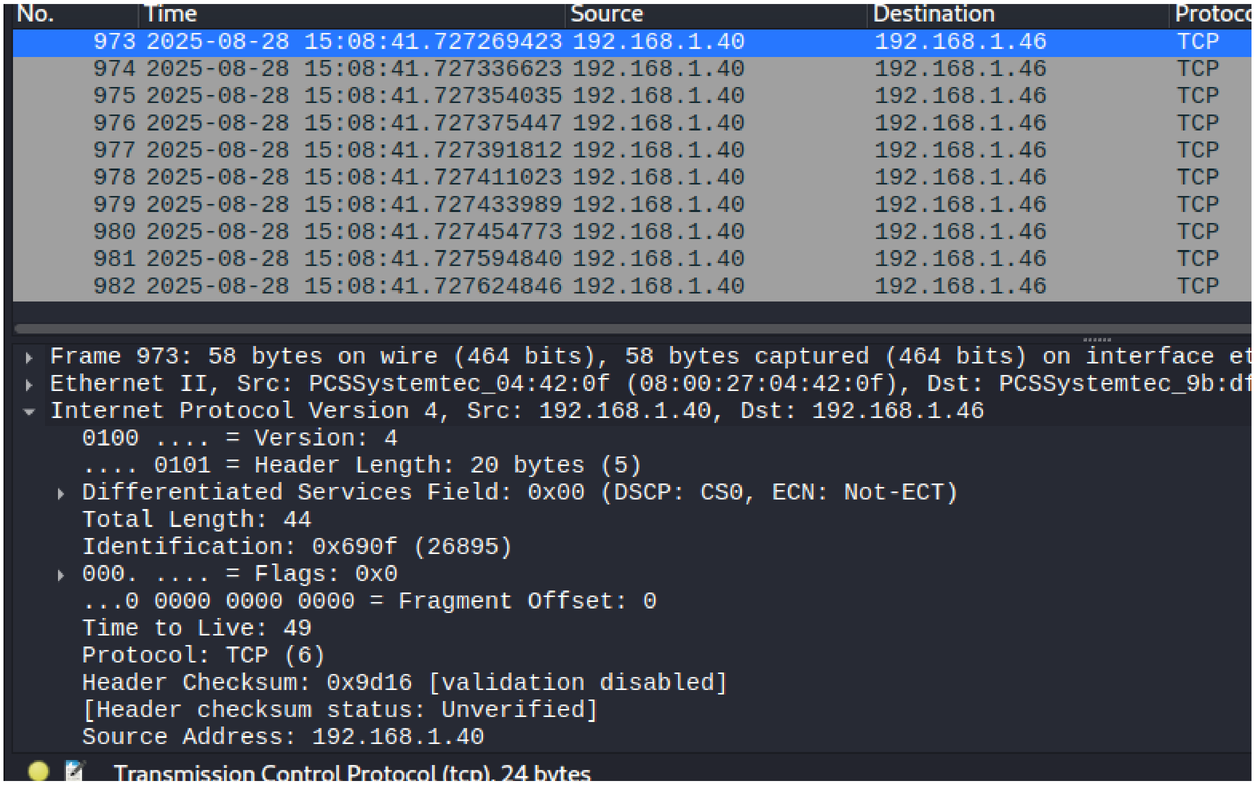


```
No.  Time                           Source        Destination   Protocol Length Info
3744 2025-08-28 15:03:48.934904792 192.168.1.40  192.168.1.46  IPv4         42 Fragmented IP proto
3745 2025-08-28 15:03:48.934925916 192.168.1.40  192.168.1.46  IPv4         42 Fragmented IP proto
3746 2025-08-28 15:03:48.934938888 192.168.1.40  192.168.1.46  TCP          42 49226 → 2004 [SYN]
3747 2025-08-28 15:03:48.934963481 192.168.1.46  192.168.1.40  TCP          60 2041 → 49226 [RST,
3748 2025-08-28 15:03:48.934963562 192.168.1.46  192.168.1.40  TCP          60 1296 → 49226 [RST,
3749 2025-08-28 15:03:48.934963602 192.168.1.46  192.168.1.40  TCP          60 144 → 49226 [RST, A
3750 2025-08-28 15:03:48.934972391 192.168.1.40  192.168.1.46  IPv4         42 Fragmented IP proto
3751 2025-08-28 15:03:48.934982871 192.168.1.40  192.168.1.46  IPv4         42 Fragmented IP proto
3752 2025-08-28 15:03:48.934999969 192.168.1.40  192.168.1.46  TCP          42 49226 → 9944 [SYN]
3753 2025-08-28 15:03:48.935022780 192.168.1.40  192.168.1.46  IPv4         42 Fragmented IP proto
3754 2025-08-28 15:03:48.935025714 192.168.1.46  192.168.1.40  TCP          60 2004 → 49226 [RST,

▸ Frame 3690: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
▸ Ethernet II, Src: PCSSystemtec_04:42:0f (08:00:27:04:42:0f), Dst: PCSSystemtec_9b:df:95 (08:00:27:9b:df:95)
▸ Internet Protocol Version 4, Src: 192.168.1.40, Dst: 192.168.1.46
▾ Data (8 bytes)
    Data: 0000000060020400
    [Length: 8]
```

3- badsum:



```
┌──(musleh㉿musleh)-[~]
└─$ sudo nmap --badsum 192.168.1.46
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-28 11:08
```



```
No.  Time                           Source        Destination   Protoco
973 2025-08-28 15:08:41.727269423 192.168.1.40  192.168.1.46  TCP
974 2025-08-28 15:08:41.727336623 192.168.1.40  192.168.1.46  TCP
975 2025-08-28 15:08:41.727354035 192.168.1.40  192.168.1.46  TCP
976 2025-08-28 15:08:41.727375447 192.168.1.40  192.168.1.46  TCP
977 2025-08-28 15:08:41.727391812 192.168.1.40  192.168.1.46  TCP
978 2025-08-28 15:08:41.727411023 192.168.1.40  192.168.1.46  TCP
979 2025-08-28 15:08:41.727433989 192.168.1.40  192.168.1.46  TCP
980 2025-08-28 15:08:41.727454773 192.168.1.40  192.168.1.46  TCP
981 2025-08-28 15:08:41.727594840 192.168.1.40  192.168.1.46  TCP
982 2025-08-28 15:08:41.727624846 192.168.1.40  192.168.1.46  TCP

▸ Frame 973: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface et
▸ Ethernet II, Src: PCSSystemtec_04:42:0f (08:00:27:04:42:0f), Dst: PCSSystemtec_9b:df
▾ Internet Protocol Version 4, Src: 192.168.1.40, Dst: 192.168.1.46
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 44
    Identification: 0x690f (26895)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 49
    Protocol: TCP (6)
    Header Checksum: 0x9d16 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.40
Transmission Control Protocol (tcp), 24 bytes
```

Task 14: Practical:

Question: Does the target ip respond to ICMP echo (ping) requests (Y/N)?

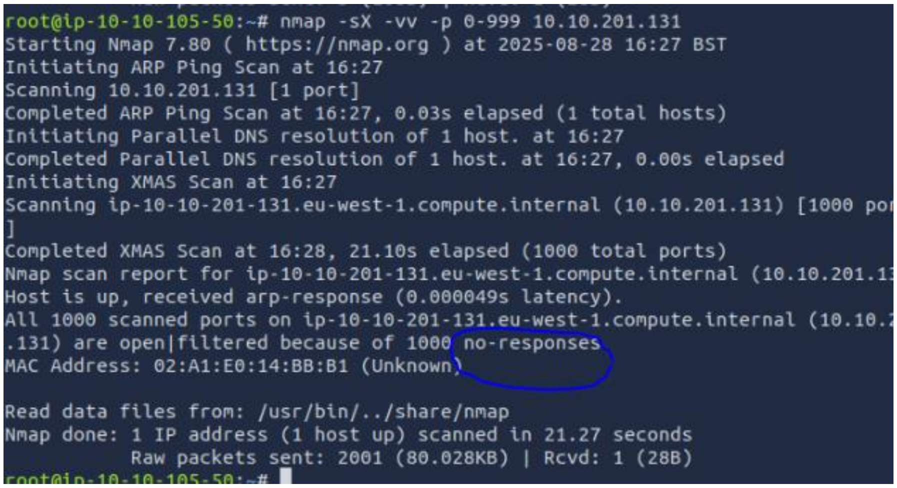
Answer : N

Perform an Xmas scan on the first 999 ports of the target -- how many ports are shown to be open or filtered?

Answer: 999

There is a reason given for this -- what is it?

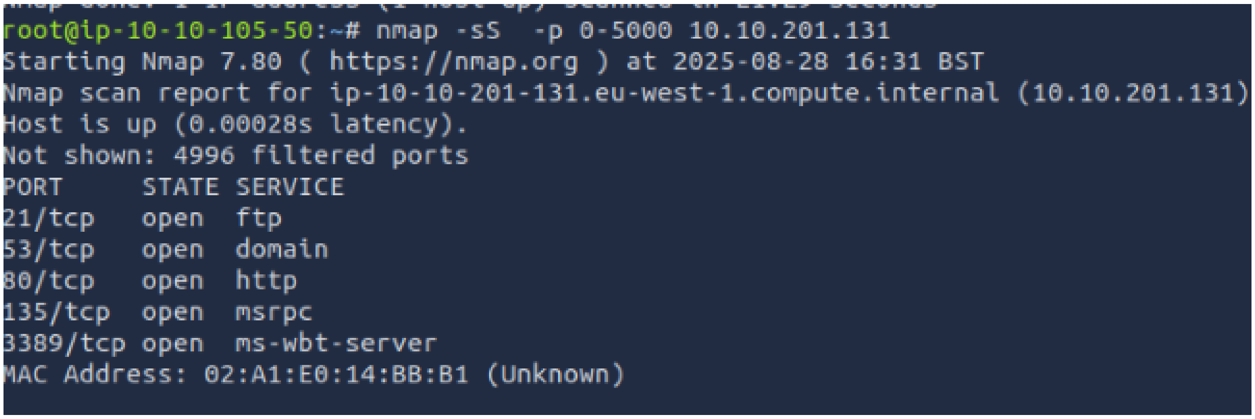
Note: The answer will be in your scan results. Think carefully about which switches to use -- and read the hint before asking for help!



```
root@ip-10-10-105-50:~# nmap -sX -vv -p 0-999 10.10.201.131
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-28 16:27 BST
Initiating ARP Ping Scan at 16:27
Scanning 10.10.201.131 [1 port]
Completed ARP Ping Scan at 16:27, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:27
Completed Parallel DNS resolution of 1 host. at 16:27, 0.00s elapsed
Initiating XMAS Scan at 16:27
Scanning ip-10-10-201-131.eu-west-1.compute.internal (10.10.201.131) [1000 po
]
Completed XMAS Scan at 16:28, 21.10s elapsed (1000 total ports)
Nmap scan report for ip-10-10-201-131.eu-west-1.compute.internal (10.10.201.1
Host is up, received arp-response (0.000049s latency).
All 1000 scanned ports on ip-10-10-201-131.eu-west-1.compute.internal (10.10.
.131) are open|filtered because of 1000 no-responses
MAC Address: 02:A1:E0:14:BB:B1 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.27 seconds
           Raw packets sent: 2001 (80.028KB) | Rcvd: 1 (28B)
root@ip-10-10-105-50:~#
```

Question: Perform a TCP SYN scan on the first 5000 ports of the target -- how many ports are shown to be open?

Answer: 5



```
root@ip-10-10-105-50:~# nmap -sS  -p 0-5000 10.10.201.131
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-28 16:31 BST
Nmap scan report for ip-10-10-201-131.eu-west-1.compute.internal (10.10.201.131)
Host is up (0.00028s latency).
Not shown: 4996 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
3389/tcp open  ms-wbt-server
MAC Address: 02:A1:E0:14:BB:B1 (Unknown)
```

Question :Open Wireshark (see Cryillic's Wireshark Room for instructions) and perform a TCP Connect scan against port 80 on the target, monitoring the results. Make sure you understand what's going on. Deploy the ftp-anon script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

Answer: Y

Thank You