Thm nmap

Does the target (`10.10.64.12`)respond to ICMP (ping) requests (Y/N)?

Answer format: *

Submit

On first connection to a target network in a black box assignment, our first objective is to obtain a "map" of the network structure -- or, in other words, we want to see which IP addresses contain active hosts, and which do not.

One way to do this is by using Nmap to perform a so called "ping sweep". This is exactly as the name suggests: Nmap sends an ICMP packet to each possible IP address for the specified network. When it receives a response, it marks the IP address that responded as being alive. For reasons we'll see in a later task, this is not always accurate; however, it can provide something of a baseline and thus is worth covering.

To perform a ping sweep, we use the `-sn` switch in conjunction with IP ranges which can be specified with either a hypen (`-`) or CIDR notation. i.e. we could scan the `192.168.0.x` network using:

- `nmap -sn 192.168.0.1-254`

or

- `nmap -sn 192.168.0.0/24`

The `-sn` switch tells Nmap not to scan any ports -- forcing it to rely primarily on ICMP echo packets (or ARP requests on a local network, if run with sudo or directly as the root user) to identify targets. In addition to the ICMP echo requests, the `-sn` switch will also cause nmap to send a TCP SYN packet to port 443 of the target, as well as a TCP ACK (or TCP SYN if not run as root) packet to port 80 of the target.

```
root@ip-10-10-229-189:~# nmap -sn 10.10.64.12

Starting Nmap 7.60 ( https://nmap.org ) at 2022-04-20 10:07 BST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.49 seconds
```

Does the target (`10.10.64.12`)respond to ICMP (ping) requests (Y/N)?

n

Correct Answer

==========
==========
==========
==========
==========

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

Answer format: ***

Submit

- As with the other two scans in this class, Xmas scans (`-sX`) send a malformed TCP packet and expects a RST response for closed ports. It's referred to as an xmas scan as the flags that it sets (PSH, URG and FIN) give it the appearance of a blinking christmas tree when viewed as a packet capture in Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	TCP	54	46664 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2	0.000100904	127.0.0.1	127.0.0.1	TCP	54	80 → 46664 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0

```
Acknowledgment number: 0
Acknowledgment number (raw): 0
0101 .... = Header Length: 20 bytes (5)
Flags: 0x029 (FIN, PSH, URG)
  000. .... .... = Reserved: Not set
  ...0 .... .... = Nonce: Not set
  .... 0... .... = Congestion Window Reduced (CWR): Not set
  .... .0.. .... = ECN-Echo: Not set
  .... ..1. .... = Urgent: Set
  .... ...0 .... = Acknowledgment: Not set
  .... .... 1... = Push: Set
  .... .... .0.. = Reset: Not set
  .... .... ..0. = Syn: Not set
  .... .... ...1 = Fin: Set
```

```
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
```

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

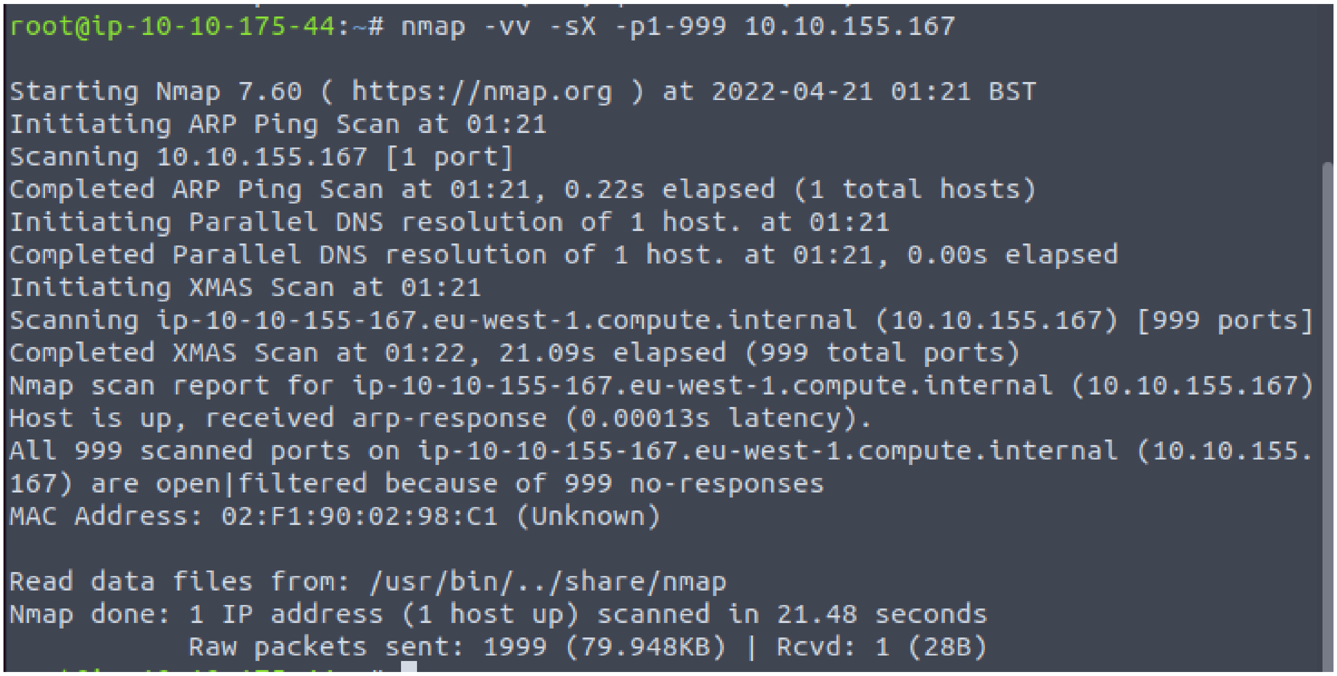
-v

Correct Answer

Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two?
(**Note**: it's highly advisable to always use *at least* this option)

-vv

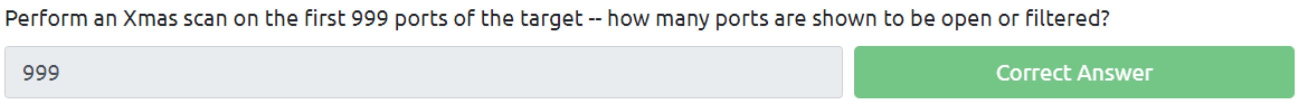
Correct Answer



```
root@ip-10-10-175-44:~# nmap -vv -sX -p1-999 10.10.155.167

Starting Nmap 7.60 ( https://nmap.org ) at 2022-04-21 01:21 BST
Initiating ARP Ping Scan at 01:21
Scanning 10.10.155.167 [1 port]
Completed ARP Ping Scan at 01:21, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:21
Completed Parallel DNS resolution of 1 host. at 01:21, 0.00s elapsed
Initiating XMAS Scan at 01:21
Scanning ip-10-10-155-167.eu-west-1.compute.internal (10.10.155.167) [999 ports]
Completed XMAS Scan at 01:22, 21.09s elapsed (999 total ports)
Nmap scan report for ip-10-10-155-167.eu-west-1.compute.internal (10.10.155.167)
Host is up, received arp-response (0.00013s latency).
All 999 scanned ports on ip-10-10-155-167.eu-west-1.compute.internal (10.10.155.
167) are open|filtered because of 999 no-responses
MAC Address: 02:F1:90:02:98:C1 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.48 seconds
           Raw packets sent: 1999 (79.948KB) | Rcvd: 1 (28B)
```



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

999

==

==

==

==

==

==

==

==

==

==

==

==

==

==

==

==

==

==

==

==

==

==

==

==

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

999 | Correct Answer

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!

no response | Correct Answer | Hint

```
root@ip-10-10-175-44:~# nmap -vv -sX -p1-999 10.10.155.167

Starting Nmap 7.60 ( https://nmap.org ) at 2022-04-21 01:21 BST
Initiating ARP Ping Scan at 01:21
Scanning 10.10.155.167 [1 port]
Completed ARP Ping Scan at 01:21, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:21
Completed Parallel DNS resolution of 1 host. at 01:21, 0.00s elapsed
Initiating XMAS Scan at 01:21
Scanning ip-10-10-155-167.eu-west-1.compute.internal (10.10.155.167) [999 ports]
Completed XMAS Scan at 01:22, 21.09s elapsed (999 total ports)
Nmap scan report for ip-10-10-155-167.eu-west-1.compute.internal (10.10.155.167)
Host is up, received arp-response (0.00013s latency).
All 999 scanned ports on ip-10-10-155-167.eu-west-1.compute.internal (10.10.155.
167) are open|filtered because of 999 no-responses
MAC Address: 02:F1:90:02:98:C1 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.48 seconds
           Raw packets sent: 1999 (79.948KB) | Rcvd: 1 (28B)
```

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

999 | Correct Answer

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!

no response | Correct Answer | Hint

==========
==========
==========
==========
==========
==========
==========
==========

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

Answer format: *

Submit

As with TCP scans, SYN scans (`-sS`) are used to scan the TCP port-range of a target or targets; however, the two scan types work slightly differently. SYN scans are sometimes referred to as "*Half-open*" scans, or "*Stealth*" scans.

Where TCP scans perform a full three-way handshake with the target, SYN scans sends back a RST TCP packet after receiving a SYN/ACK from the server (this prevents the server from repeatedly trying to make the request). In other words, the sequence for scanning an **open** port looks like this:

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

-v

Correct Answer

Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two?
(**Note**: it's highly advisable to always use *at least* this option)

-vv

Correct Answer

(10.10.182.131)

```
root@ip-10-10-213-222: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-213-222:~# nmap -vv -sS -p1-5000 10.10.182.131

Starting Nmap 7.60 ( https://nmap.org ) at 2022-04-21 07:07 BST
Initiating ARP Ping Scan at 07:07
Scanning 10.10.182.131 [1 port]
Completed ARP Ping Scan at 07:07, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:07
Completed Parallel DNS resolution of 1 host. at 07:07, 0.00s elapsed
Initiating SYN Stealth Scan at 07:07
Scanning ip-10-10-182-131.eu-west-1.compute.internal (10.10.182.131) [5000 ports
]
Discovered open port 80/tcp on 10.10.182.131
Discovered open port 53/tcp on 10.10.182.131
Discovered open port 21/tcp on 10.10.182.131
Discovered open port 3389/tcp on 10.10.182.131
Discovered open port 135/tcp on 10.10.182.131
Increasing send delay for 10.10.182.131 from 0 to 5 due to 11 out of 32 dropped
probes since last increase.
SYN Stealth Scan Timing: About 36.85% done; ETC: 07:09 (0:00:53 remaining)
SYN Stealth Scan Timing: About 65.24% done; ETC: 07:09 (0:00:33 remaining)
Increasing send delay for 10.10.182.131 from 5 to 10 due to 14 out of 46 dropped
 probes since last increase.
Completed SYN Stealth Scan at 07:09, 124.73s elapsed (5000 total ports)
Nmap scan report for ip-10-10-182-131.eu-west-1.compute.internal (10.10.182.131)
```

```
Completed SYN Stealth Scan at 07:09, 124.73s elapsed (5000 total ports)
Nmap scan report for ip-10-10-182-131.eu-west-1.compute.internal (10.10.182.131)
Host is up, received arp-response (0.00067s latency).
Scanned at 2022-04-21 07:07:40 BST for 125s
Not shown: 4995 filtered ports
Reason: 4995 no-responses
PORT     STATE SERVICE       REASON
21/tcp   open  ftp           syn-ack ttl 128
53/tcp   open  domain        syn-ack ttl 128
80/tcp   open  http          syn-ack ttl 128
135/tcp  open  msrpc         syn-ack ttl 128
3389/tcp open  ms-wbt-server syn-ack ttl 128
MAC Address: 02:EC:0E:D8:D7:E1 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 125.20 seconds
           Raw packets sent: 15090 (663.944KB) | Rcvd: 105 (4.604KB)
root@ip-10-10-213-222:~#
```

```
Reason: 4995 no-responses
PORT     STATE SERVICE       REASON
21/tcp   open  ftp           syn-ack ttl 128
53/tcp   open  domain        syn-ack ttl 128
80/tcp   open  http          syn-ack ttl 128
135/tcp  open  msrpc         syn-ack ttl 128
3389/tcp open  ms-wbt-server syn-ack ttl 128
MAC Address: 02:EC:0E:D8:D7:E1 (Unknown)
```

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

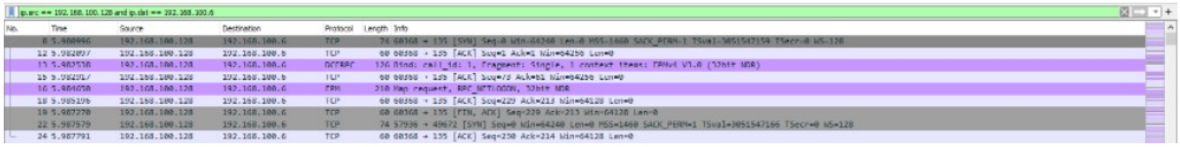
5

Correct Answer

==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========

Filtering by SRC and DST: The second filter will look at is two in one as well as a filter operator: ip.src and ip.dst. These filters allow us to filter the traffic by the source and destination from which the traffic is coming from.

Syntax: `ip.src == <SRC IP Address> and ip.dst == <DST IP Address>`

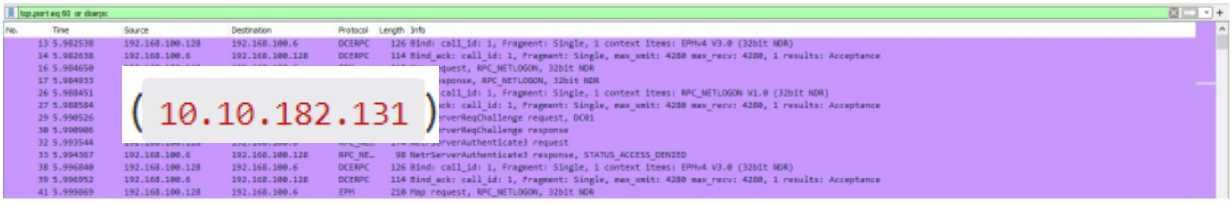


Similar to the first filter we can see that Wireshark is combing through the packets and filtering based on the source and destination we set.

Filtering by TCP Protocols: The last filter that we will be covering is the protocol filter, this allows you to set a port or protocol to filter by and can be handy when trying to keep track of an unusual protocol or port being used.

It is worthwhile to mention that Wireshark can filter by both port numbers as well as protocol names.

Syntax: `tcp.port eq <Port #> or <Protocol Name>`



(ip.src == 10.10.182.131 || ip.dst == 10.10.182.131) && tcp.port eq 80

*eth0 (tcp port http)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(ip.src == 10.10.182.131 || ip.dst == 10.10.182.131) && tcp.port eq 80 Expression… +

No.	Time	Source	Destination	Protocol	Length	Info

Capturing from eth0 (tcp port http)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(ip.src == 10.10.182.131 || ip.dst == 10.10.182.131) && tcp.port eq 80 Expression… +

No.	Time	Source	Destination	Protocol	Length	Info
2503	27.146957760	10.10.213.222	10.10.182.131	TCP	58	6157
2504	27.147603684	10.10.182.131	10.10.213.222	TCP	58	80 -
2505	27.147609995	10.10.213.222	10.10.182.131	TCP	54	6157

```
▸ Frame 2503: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interfac
▸ Ethernet II, Src: MS-NLB-PhysServer-19_9e:61:31:23 (02:13:9e:61:31:23), Dst: 02:e
▸ Internet Protocol Version 4, Src: 10.10.213.222, Dst: 10.10.182.131
▸ Transmission Control Protocol, Src Port: 61576, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  02 ec 0e d8 d7 e1 02 13  9e 61 31 23 08 00 45 00   ........ ·a1#··E·
0010  00 2c 49 1d 00 00 3a 06  97 39 0a 0a d5 de 0a 0a   ·,I···:· ·9......
0020  b6 83 f0 88 00 50 c6 13  d9 a3 00 00 00 00 60 02   ·····P·· ......`·
0030  04 00 63 20 00 00 02 04  05 b4                     ··c ···· ··
```

eth0: <live capture in p

0-255.1-254

orks

y to given ports
overy probes

ometimes]
vers

root@ip-10-10-213-222: ~

File Edit View Search Terminal Help

```
           Raw packets sent: 101 (4.428KB) | Rcvd: 3 (116B)
root@ip-10-10-213-222:~# nmap -vv -sS -p1-100 10.10.182.131

Starting Nmap 7.60 ( https://nmap.org ) at 2022-04-21 07:39 BST
Initiating ARP Ping Scan at 07:39
Scanning 10.10.182.131 [1 port]
Completed ARP Ping Scan at 07:39, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:39
Completed Parallel DNS resolution of 1 host. at 07:39, 0.00s elapsed
Initiating SYN Stealth Scan at 07:39
Scanning ip-10-10-182-131.eu-west-1.compute.internal (10.10.182.131) [100 ports]
Discovered open port 21/tcp on 10.10.182.131
Discovered open port 80/tcp on 10.10.182.131
Discovered open port 53/tcp on 10.10.182.131
Completed SYN Stealth Scan at 07:39, 1.95s elapsed (100 total ports)
Nmap scan report for ip-10-10-182-131.eu-west-1.compute.internal (10.10.182.131)
Host is up, received arp-response (0.00039s latency).
Scanned at 2022-04-21 07:39:09 BST for 2s
Not shown: 97 filtered ports
Reason: 97 no-responses
PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 128
53/tcp open  domain  syn-ack ttl 128
80/tcp open  http    syn-ack ttl 128
MAC Address: 02:EC:0E:D8:D7:E1 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.30 seconds
           Raw packets sent: 199 (8.740KB) | Rcvd: 5 (204B)
root@ip-10-10-213-222:~# nmap -vv -sS -p1-100 10.10.182.131
```

Applications Places System Thu 21 Apr, 07:41 AttackBox IP:10.10.213.222

Capturing from eth0 (tcp port http)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(ip.src == 10.10.182.131 || ip.dst == 10.10.182.131) && tcp.port eq 80 Expression… +

No.	Time	Source	Destination	Protocol	Length	Info
2503	27.146957760	10.10.213.222	10.10.182.131	TCP	58	61576 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2504	27.147603684	10.10.182.131	10.10.213.222	TCP	58	80 → 61576 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=8961
2505	27.147609995	10.10.213.222	10.10.182.131	TCP	54	61576 → 80 [RST] Seq=1 Win=0 Len=0

```
▸ Frame 2503: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0
▸ Ethernet II, Src: MS-NLB-PhysServer-19_9e:61:31:23 (02:13:9e:61:31:23), Dst: 02:ec:0e:d8:d7:e1 (02:ec:0e:d8:d7:e1)
▸ Internet Protocol Version 4, Src: 10.10.213.222, Dst: 10.10.182.131
▸ Transmission Control Protocol, Src Port: 61576, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  02 ec 0e d8 d7 e1 02 13  9e 61 31 23 08 00 45 00   ........ .a1#..E.
0010  00 2c 49 1d 00 00 3a 06  97 39 0a 0a d5 de 0a 0a   .,I...:. .9......
0020  b6 83 f0 88 00 50 c6 13  d9 a3 00 00 00 00 60 02   .....P.. ......`.
0030  04 00 63 20 00 00 02 04  05 b4                     ..c .... ..
```

```
Transmission Control Protocol, Src Port: 61576, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 61576
  Destination Port: 80
  [Stream index: 1]
  [TCP Segment Len: 0]
  Sequence number: 0    (relative sequence number)
  [Next sequence number: 0    (relative sequence number)]
  Acknowledgment number: 0
  0110 .... = Header Length: 24 bytes (6)
▸ Flags: 0x002 (SYN)
  Window size value: 1024
  [Calculated window size: 1024]
  Checksum: 0x6320 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
▸ Options: (4 bytes), Maximum segment size
▸ [Timestamps]
```

==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========
==========

Deploy the `ftp-anon` script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

Answer format: *

Submit

Script ftp-anon

Jump to:
- Script Arguments
- Example Usage
- Script Output

Script types: portrule
Categories: ***default***, ***auth***, ***safe***
Download: **https://svn.nmap.org/nmap/scripts/ftp-anon.nse**

Script Summary

Checks if an FTP server allows anonymous logins.

If anonymous is allowed, gets a directory listing of the root directory and highlights writeable files.

See also:

- **ftp-brute.nse**

Script Arguments

ftp-anon.maxlist

The maximum number of files to return in the directory listing. By default it is 20, or unlimited if verbosity is enabled. Use a negative number to disable the limit, or `0` to disable the listing entirely.

Example Usage

```
nmap -sV -sC <target>
```

Script Output

```
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--   1 1170     924            31 Mar 28  2001 .banner
| d--x--x--x   2 root     root         1024 Jan 14  2002 bin
| d--x--x--x   2 root     root         1024 Aug 10  1999 etc
| drwxr-srwt   2 1170     924          2048 Jul 19 18:48 incoming [NSE: writeable
| d--x--x--x   2 root     root         1024 Jan 14  2002 lib
| drwxr-sr-x   2 1170     924          1024 Aug  5  2004 pub
|_Only 6 shown. Use --script-args ftp-anon.maxlist=-1 to see all.
```

AttackBox IP:10.10.213.222

Task 11 NSE Scripts Working with the NSE

In Task 3 we looked very briefly at the `--script` switch for activating NSE scripts from the `vuln` category using `--script=vuln`. It should come as no surprise that the other categories work in exactly the same way. If the command `--script=safe` is run, then any applicable safe scripts will be run against the target (Note: only scripts which target an active service will be activated).

To run a specific script, we would use `--script=<script-name>`, e.g. `--script=http-fileupload-exploiter`.

Multiple scripts can be run simultaneously in this fashion by separating them by a comma. For example: `--script=smb-enum-users,smb-enum-shares`.

Some scripts require arguments (for example, credentials, if they're exploiting an authenticated vulnerability). These can be given with the `--script-args` Nmap switch. An example of this would be with the `http-put` script (used to upload files using the PUT method). This takes two arguments: the URL to upload the file to, and the file's location on disk. For example:

```
nmap -p 80 --script http-put --script-args http-put.url='/dav/shell.php',http-put.file='./shell.php'
```

Note that the arguments are separated by commas, and connected to the corresponding script with periods (i.e. `<script-name>.<argument>`).

A full list of scripts and their corresponding arguments (along with example use cases) can be found here.

Nmap scripts come with built-in help menus, which can be accessed using `nmap --script-help <script-name>`. This tends not to be as extensive as in the link given above, however, it can still be useful when working locally.

Answer the questions below

What optional argument can the `ftp-anon.nse` script take?

maxlist | Correct Answer

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

-v | Correct Answer

Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two?
(**Note**: it's highly advisable to always use *at least* this option)

-vv | Correct Answer

(10.10.202.6)

```
root@ip-10-10-213-180:~# nmap -vv -p21 --script=ftp-anon 10.10.202.6

Starting Nmap 7.60 ( https://nmap.org ) at 2022-04-21 22:25 BST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 22:25
Completed NSE at 22:25, 0.00s elapsed
Initiating ARP Ping Scan at 22:25
Scanning 10.10.202.6 [1 port]
Completed ARP Ping Scan at 22:25, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:25
Completed Parallel DNS resolution of 1 host. at 22:25, 0.00s elapsed
Initiating SYN Stealth Scan at 22:25
Scanning ip-10-10-202-6.eu-west-1.compute.internal (10.10.202.6) [1 port]
Discovered open port 21/tcp on 10.10.202.6
Completed SYN Stealth Scan at 22:25, 0.22s elapsed (1 total ports)
NSE: Script scanning 10.10.202.6.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 22:25
Completed NSE at 22:25, 30.01s elapsed
Nmap scan report for ip-10-10-202-6.eu-west-1.compute.internal (10.10.202.6)
Host is up, received arp-response (0.00025s latency).
Scanned at 2022-04-21 22:25:06 BST for 30s
```

```
root@ip-10-10-213-180: ~
File  Edit  View  Search  Terminal  Help
Discovered open port 21/tcp on 10.10.202.6
Completed SYN Stealth Scan at 22:25, 0.22s elapsed (1 total ports)
NSE: Script scanning 10.10.202.6.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 22:25
Completed NSE at 22:25, 30.01s elapsed
Nmap scan report for ip-10-10-202-6.eu-west-1.compute.internal (10.10.202.6)
Host is up, received arp-response (0.00025s latency).
Scanned at 2022-04-21 22:25:06 BST for 30s

PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 128
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
MAC Address: 02:57:1E:27:76:D3 (Unknown)

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 22:25
Completed NSE at 22:25, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 31.17 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)
root@ip-10-10-213-180:~#
```

```
PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 128
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
MAC Address: 02:57:1E:27:76:D3 (Unknown)
```

Deploy the `ftp-anon` script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

y

Correct Answer