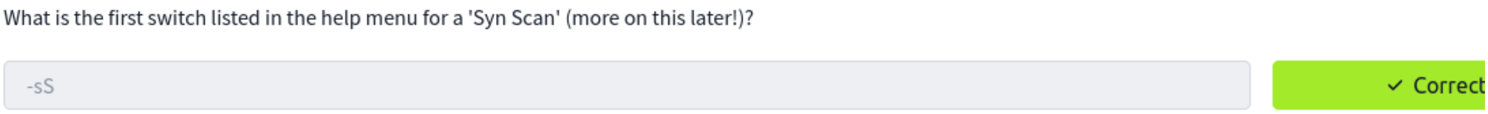
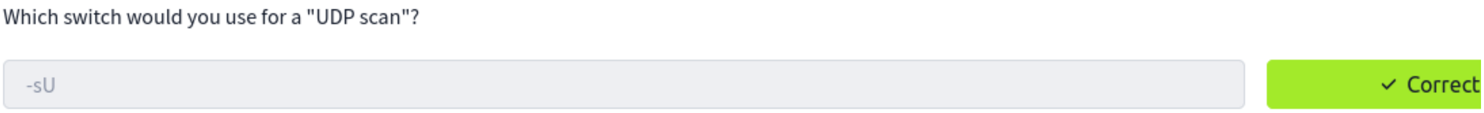
Network Mapper (NMAP)

This is a simple nmap room from tryhackme.
Can access the room from this link TryHackMe



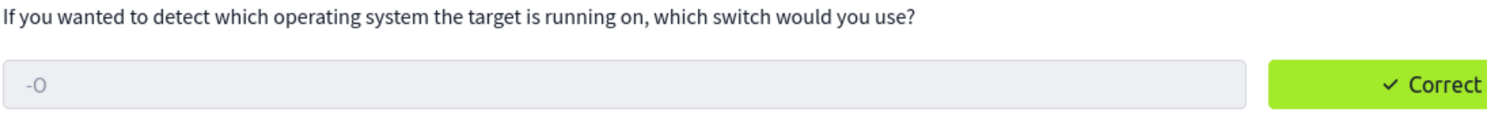
What is the first switch listed in the help menu for a 'Syn Scan' (more on this later!)?

-sS



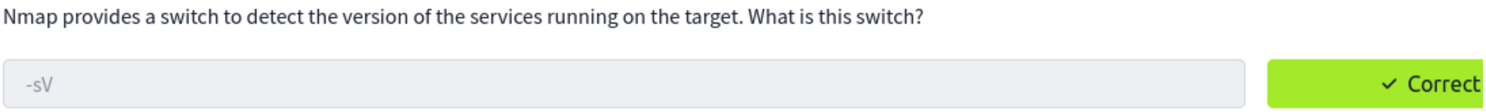
Which switch would you use for a "UDP scan"?

-sU



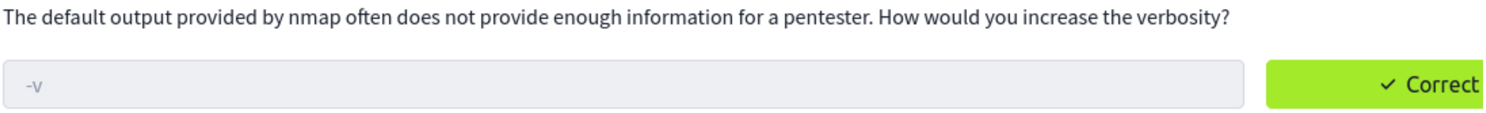
If you wanted to detect which operating system the target is running on, which switch would you use?

-O



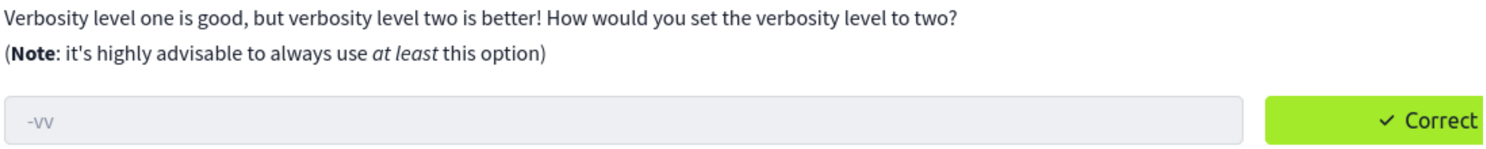
Nmap provides a switch to detect the version of the services running on the target. What is this switch?

-sV



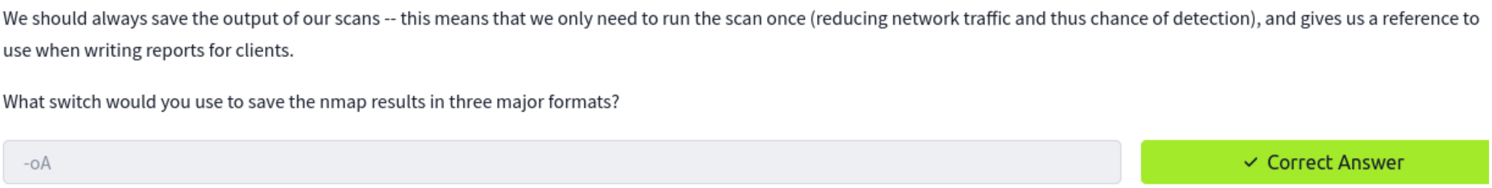
The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity?

-v



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)

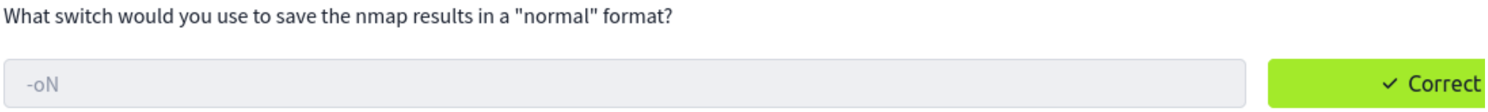
-vv



We should always save the output of our scans -- this means that we only need to run the scan once (reducing network traffic and thus chance of detection), and gives us a reference to use when writing reports for clients.

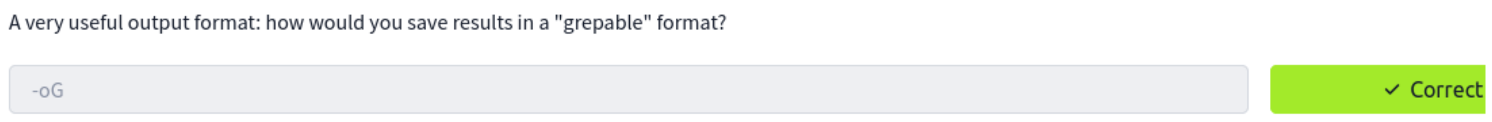
What switch would you use to save the nmap results in three major formats?

-oA

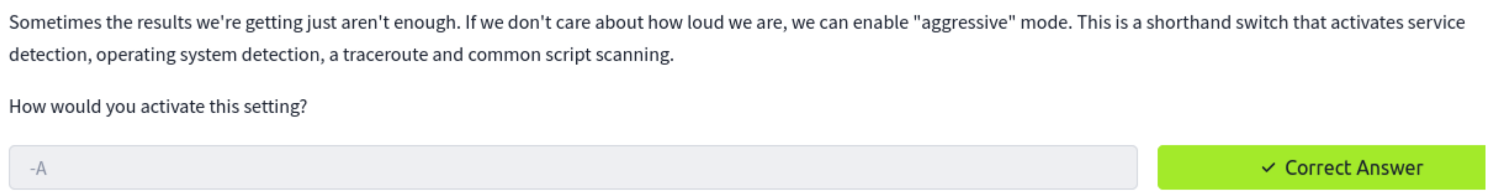


What switch would you use to save the nmap results in a "normal" format?

-oN

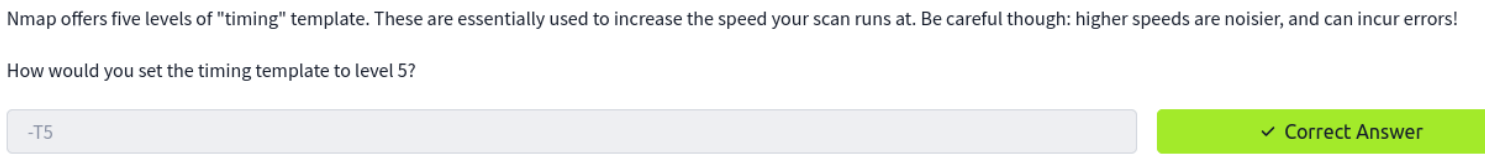

A very useful output format: how would you save results in a "grepable" format?

-oG


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.

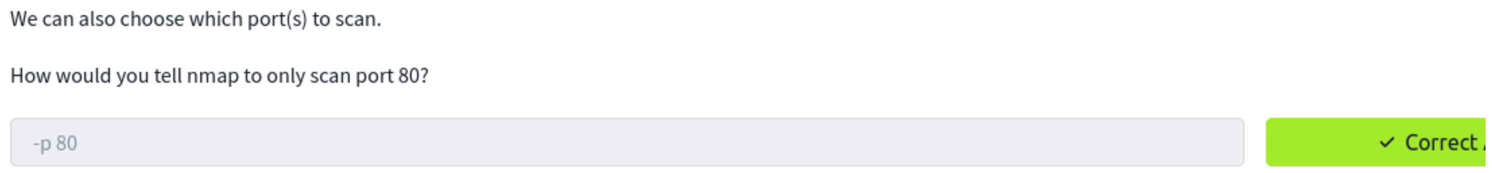
How would you activate this setting?

-A


Nmap offers five levels of "timing" template. These are essentially used to increase the speed your scan runs at. Be careful though: higher speeds are noisier, and can incur errors!

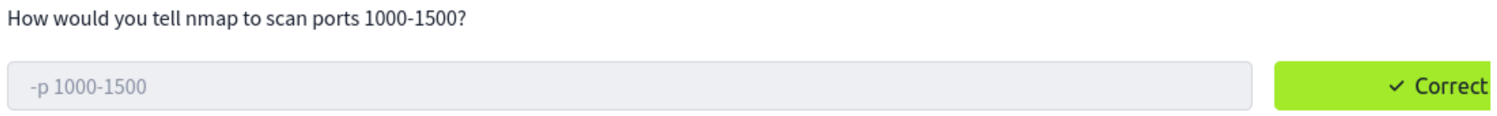
How would you set the timing template to level 5?

-T5

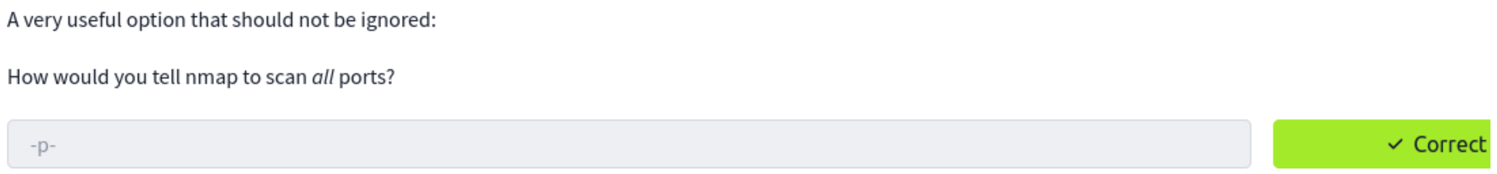

We can also choose which port(s) to scan.

How would you tell nmap to only scan port 80?

-p 80

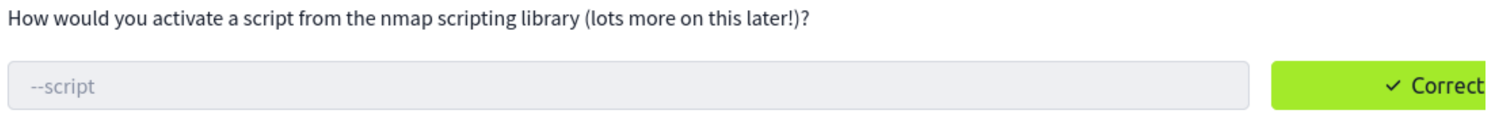

How would you tell nmap to scan ports 1000-1500?

-p 1000-1500

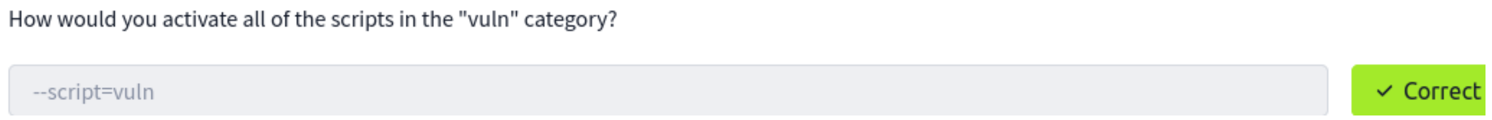

A very useful option that should not be ignored:

How would you tell nmap to scan *all* ports?

-p-


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

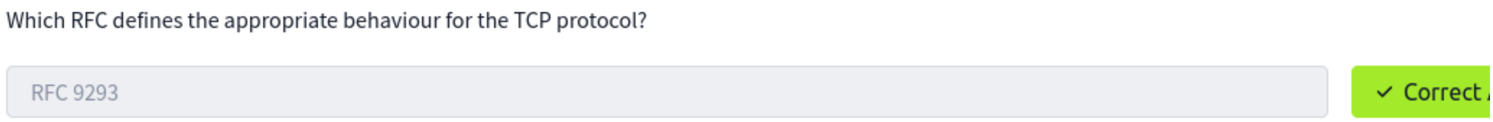
--script


How would you activate all of the scripts in the "vuln" category?

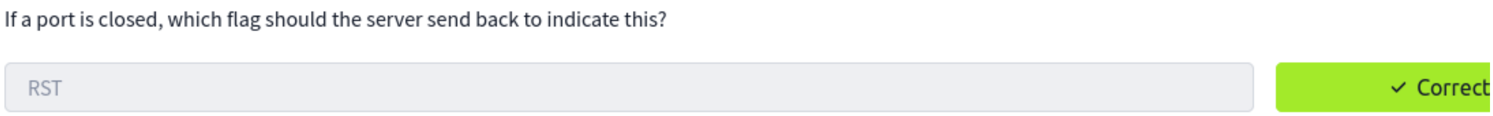
--script=vuln

When port scanning with Nmap, there are three basic scan types. These are:

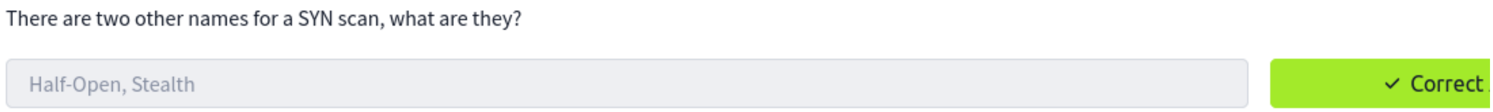
- TCP Connect Scans (`-sT`)
- SYN "Half-open" Scans (`-sS`)
- UDP Scans (`-sU`)


Which RFC defines the appropriate behaviour for the TCP protocol?

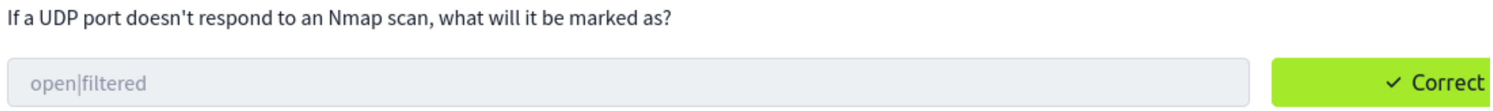
RFC 9293


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

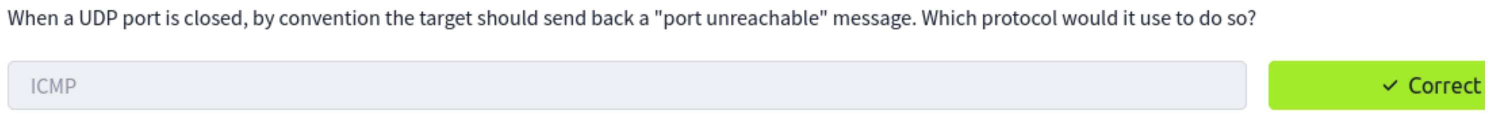
RST


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

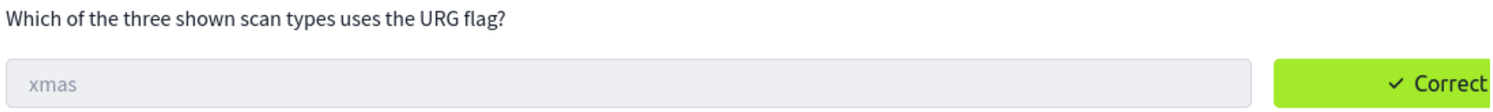
Half-Open, Stealth


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

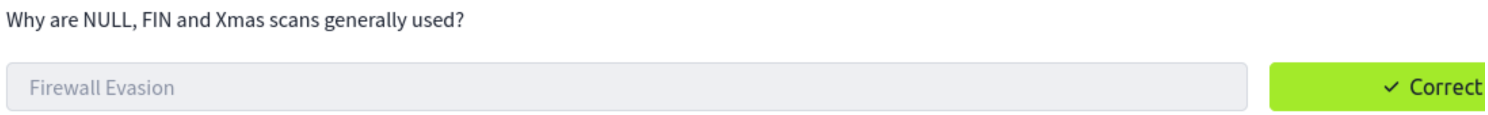
open|filtered


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?

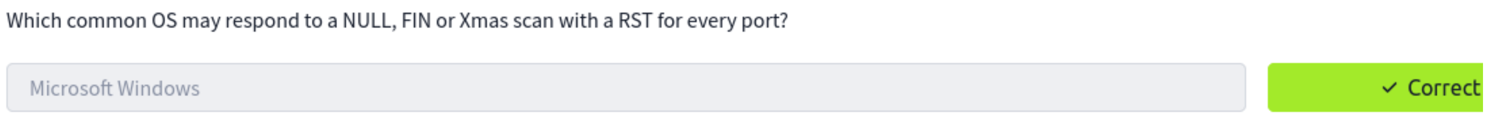
ICMP


Which of the three shown scan types uses the URG flag?

xmas


Why are NULL, FIN and Xmas scans generally used?

Firewall Evasion


Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port?

Microsoft Windows

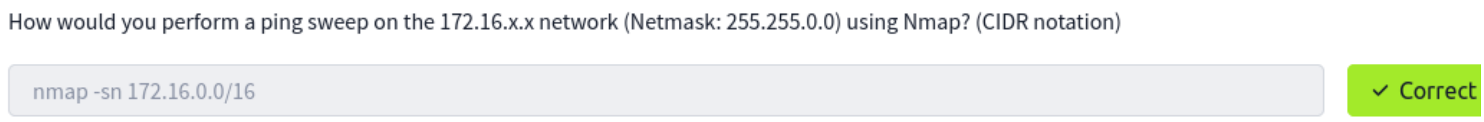
On first connection to a target network in a black box assignment, our first objective is to obtain a "map" of the network structure -- or, in other words, we want to see which IP addresses contain active hosts, and which do not. One way to do this is by using Nmap to perform a so called "ping sweep". 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`



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

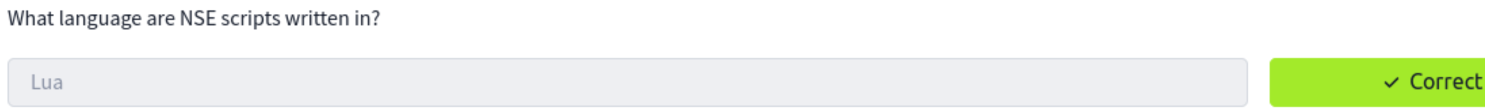
nmap -sn 172.16.0.0/16

There are many categories available. Some useful categories include:

- `safe`:- Won't affect the target
- `intrusive`:- Not safe: likely to affect the target

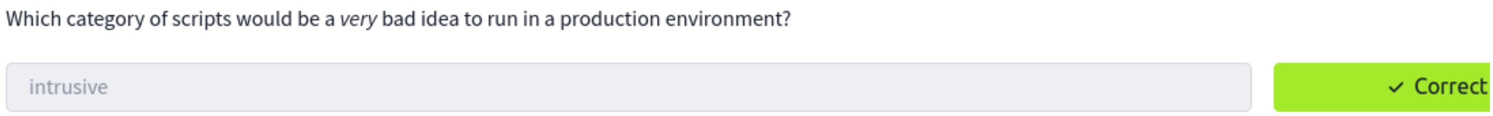
- `vuln`:- Scan for vulnerabilities
- `exploit`:- Attempt to exploit a vulnerability
- `auth`:- Attempt to bypass authentication for running services (e.g. Log into an FTP server anonymously)
- `brute`:- Attempt to bruteforce credentials for running services
- `discovery`:- Attempt to query running services for further information about the network (e.g. query an SNMP server).

A more exhaustive list can be found here.



What language are NSE scripts written in?

Lua



Which category of scripts would be a *very* bad idea to run in a production environment?

intrusive

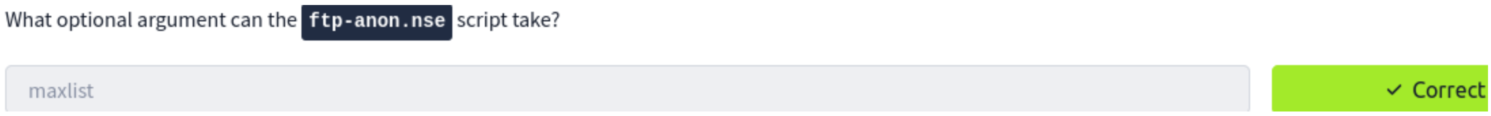
To run a specific script, we would use `--script=<script-name>` , e.g. `--script=http-fileupload-exploiter`. Multiple scripts can be run simultaneously in this fashion by separating them by a comma. For example: `--script=smb-enum-users,smb-enum-shares`.

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'
```

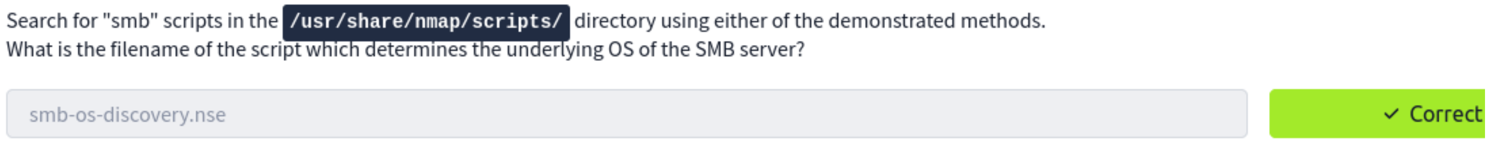
Note that the arguments are separated by commas, and connected to the corresponding script with periods (i.e. `<script-name>.<argument>`).

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



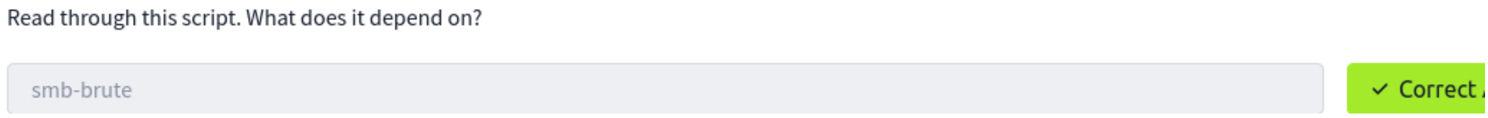
What optional argument can the `ftp-anon.nse` script take?

maxlist


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?

smb-os-discovery.nse

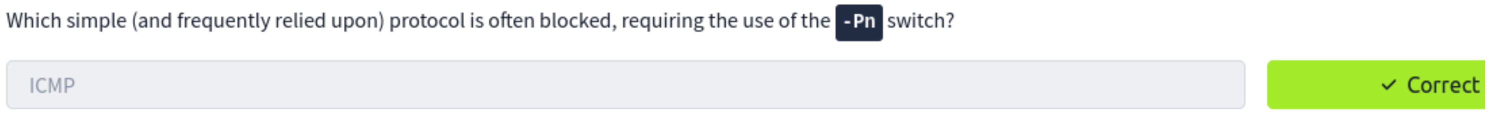
✓ Correct


Read through this script. What does it depend on?

smb-brute

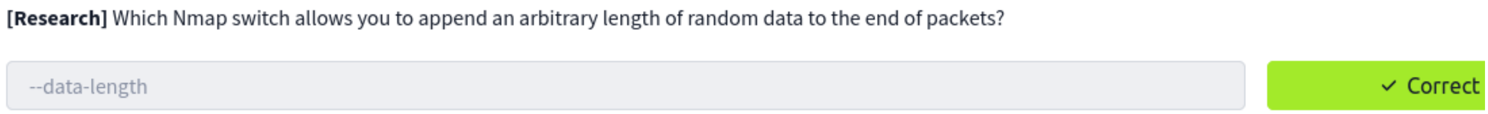
✓ Correct

There are a variety of other switches which Nmap considers useful for firewall evasion. We will not go through these in detail, however, they can be found here.


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

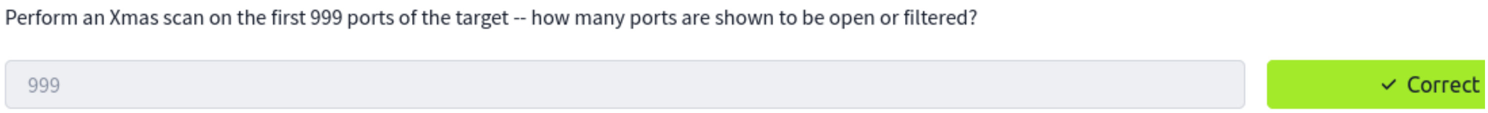
ICMP

✓ Correct


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

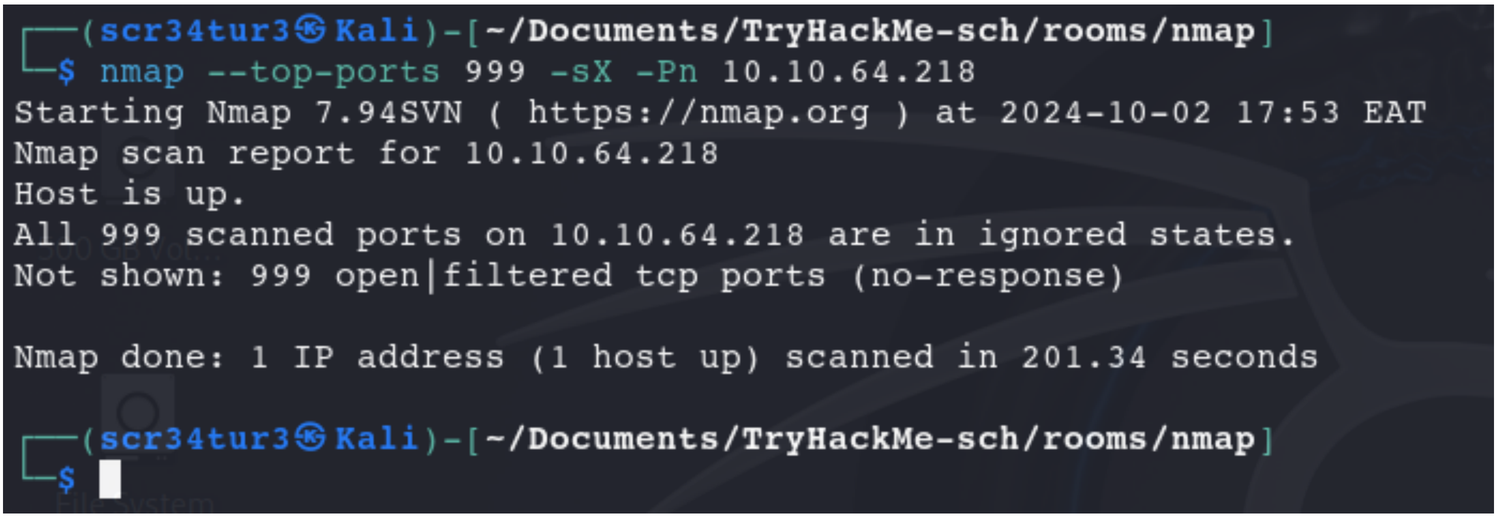
--data-length

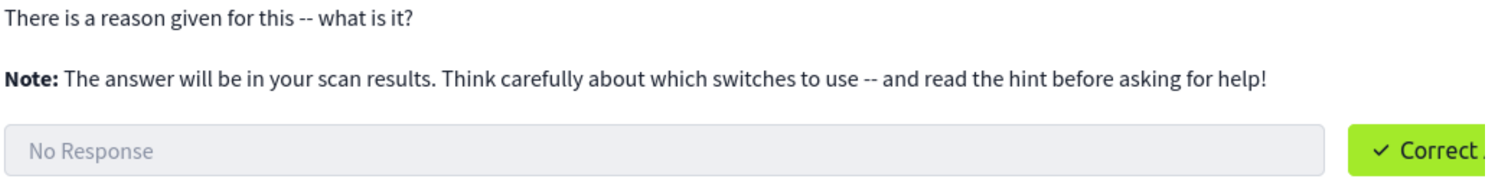
✓ Correct


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

999

✓ Correct

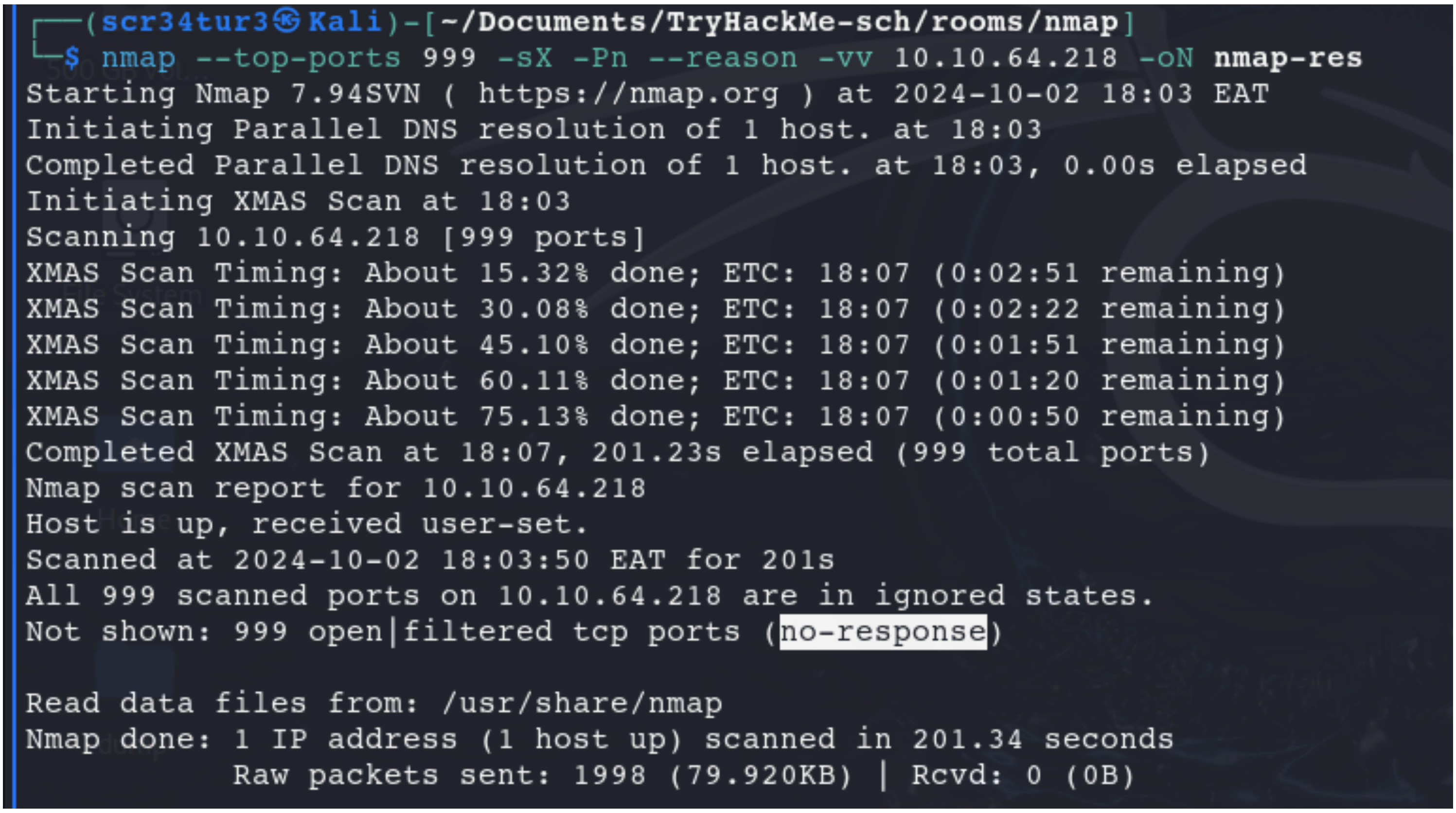

```
┌──(scr34tur3㉿Kali)-[~/Documents/TryHackMe-sch/rooms/nmap]
└─$ nmap --top-ports 999 -sX -Pn 10.10.64.218
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-02 17:53 EAT
Nmap scan report for 10.10.64.218
Host is up.
All 999 scanned ports on 10.10.64.218 are in ignored states.
Not shown: 999 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 201.34 seconds

┌──(scr34tur3㉿Kali)-[~/Documents/TryHackMe-sch/rooms/nmap]
└─$ 
```


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

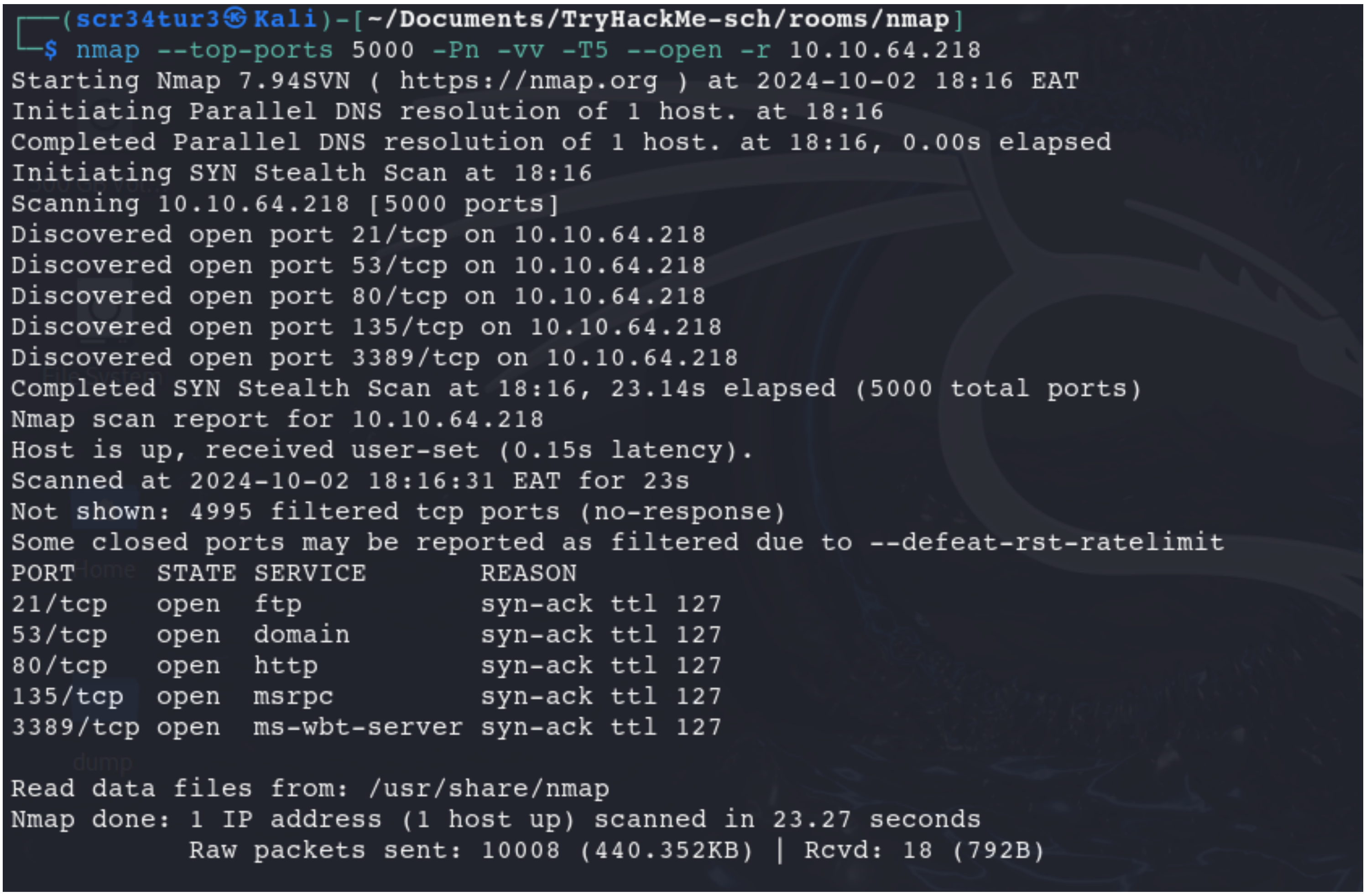


```
┌──(scr34tur3㉿Kali)-[~/Documents/TryHackMe-sch/rooms/nmap]
└─$ nmap --top-ports 999 -sX -Pn --reason -vv 10.10.64.218 -oN nmap-res
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-02 18:03 EAT
Initiating Parallel DNS resolution of 1 host. at 18:03
Completed Parallel DNS resolution of 1 host. at 18:03, 0.00s elapsed
Initiating XMAS Scan at 18:03
Scanning 10.10.64.218 [999 ports]
XMAS Scan Timing: About 15.32% done; ETC: 18:07 (0:02:51 remaining)
XMAS Scan Timing: About 30.08% done; ETC: 18:07 (0:02:22 remaining)
XMAS Scan Timing: About 45.10% done; ETC: 18:07 (0:01:51 remaining)
XMAS Scan Timing: About 60.11% done; ETC: 18:07 (0:01:20 remaining)
XMAS Scan Timing: About 75.13% done; ETC: 18:07 (0:00:50 remaining)
Completed XMAS Scan at 18:07, 201.23s elapsed (999 total ports)
Nmap scan report for 10.10.64.218
Host is up, received user-set.
Scanned at 2024-10-02 18:03:50 EAT for 201s
All 999 scanned ports on 10.10.64.218 are in ignored states.
Not shown: 999 open|filtered tcp ports (no-response)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 201.34 seconds
           Raw packets sent: 1998 (79.920KB) | Rcvd: 0 (0B)
```

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

5

✓ Correct

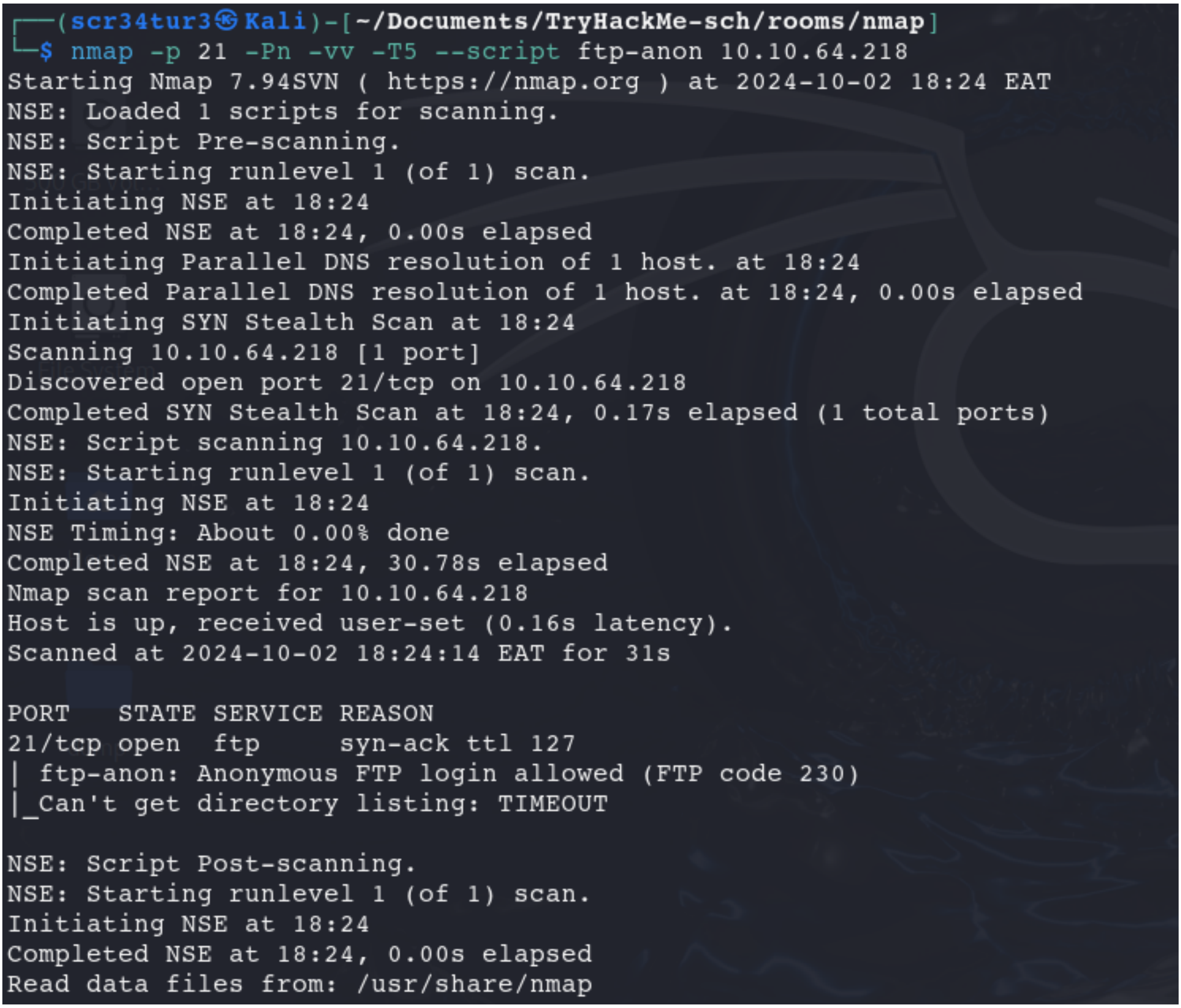


```
┌──(scr34tur3㉿Kali)-[~/Documents/TryHackMe-sch/rooms/nmap]
└─$ nmap --top-ports 5000 -Pn -vv -T5 --open -r 10.10.64.218
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-02 18:16 EAT
Initiating Parallel DNS resolution of 1 host. at 18:16
Completed Parallel DNS resolution of 1 host. at 18:16, 0.00s elapsed
Initiating SYN Stealth Scan at 18:16
Scanning 10.10.64.218 [5000 ports]
Discovered open port 21/tcp on 10.10.64.218
Discovered open port 53/tcp on 10.10.64.218
Discovered open port 80/tcp on 10.10.64.218
Discovered open port 135/tcp on 10.10.64.218
Discovered open port 3389/tcp on 10.10.64.218
Completed SYN Stealth Scan at 18:16, 23.14s elapsed (5000 total ports)
Nmap scan report for 10.10.64.218
Host is up, received user-set (0.15s latency).
Scanned at 2024-10-02 18:16:31 EAT for 23s
Not shown: 4995 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE       REASON
21/tcp   open  ftp           syn-ack ttl 127
53/tcp   open  domain        syn-ack ttl 127
80/tcp   open  http          syn-ack ttl 127
135/tcp  open  msrpc         syn-ack ttl 127
3389/tcp open  ms-wbt-server syn-ack ttl 127

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 23.27 seconds
           Raw packets sent: 10008 (440.352KB) | Rcvd: 18 (792B)
```

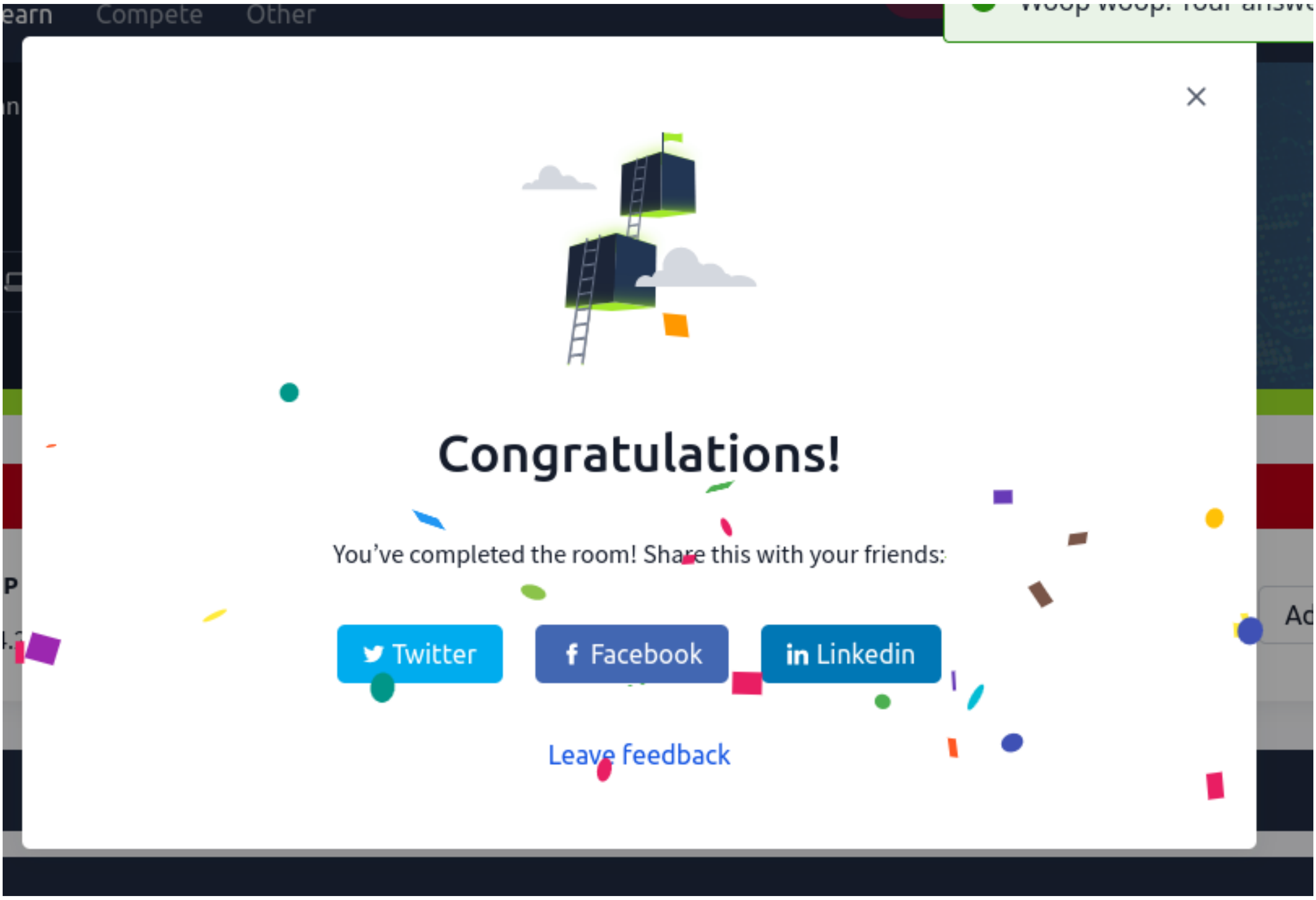
Open Wireshark (see Cryillic's Wireshark Room for instructions) and perform a TCP Connect scan against port 80 on the target, monitoring the results. Make sure you understand what's going on. Deploy the `ftp-anon` script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

Y

✓ Correct Answer



```
┌──(scr34tur3㉿Kali)-[~/Documents/TryHackMe-sch/rooms/nmap]
└─$ nmap -p 21 -Pn -vv -T5 --script ftp-anon 10.10.64.218
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-02 18:24 EAT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 18:24
Completed NSE at 18:24, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 18:24
Completed Parallel DNS resolution of 1 host. at 18:24, 0.00s elapsed
Initiating SYN Stealth Scan at 18:24
Scanning 10.10.64.218 [1 port]
Discovered open port 21/tcp on 10.10.64.218
Completed SYN Stealth Scan at 18:24, 0.17s elapsed (1 total ports)
NSE: Script scanning 10.10.64.218.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 18:24
NSE Timing: About 0.00% done
Completed NSE at 18:24, 30.78s elapsed
Nmap scan report for 10.10.64.218
Host is up, received user-set (0.16s latency).
Scanned at 2024-10-02 18:24:14 EAT for 31s

PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 127
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 18:24
Completed NSE at 18:24, 0.00s elapsed
Read data files from: /usr/share/nmap
```



Congratulations!

You’ve completed the room! Share this with your friends: