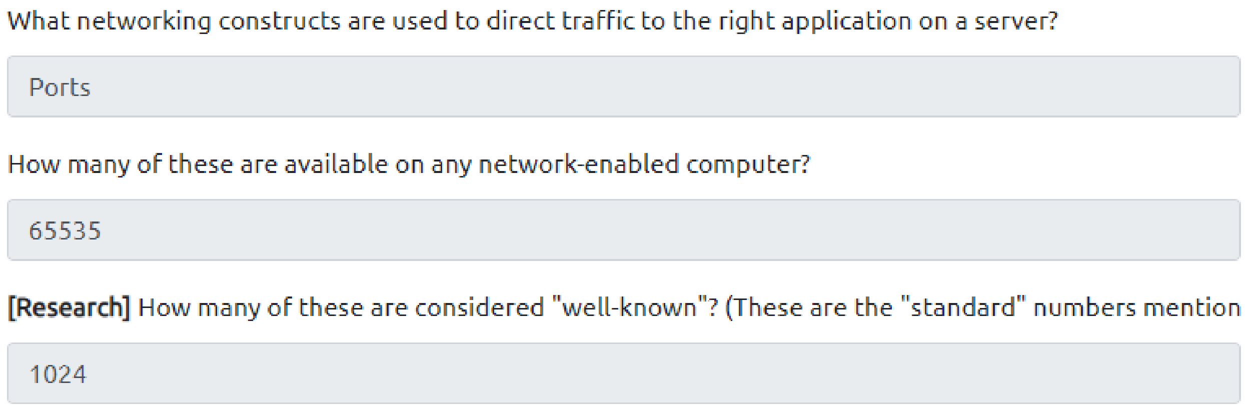
So welcome again….

Now with networking room https://tryhackme.com/room/furthernmap

So, starting with basic information in intro task


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

Ports

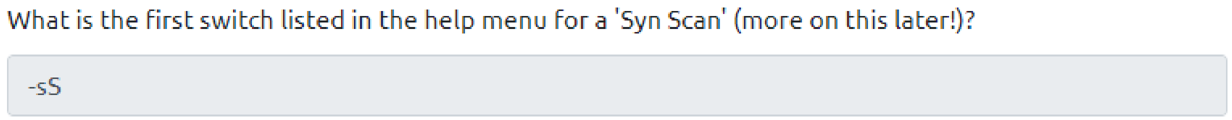
How many of these are available on any network-enabled computer?

65535

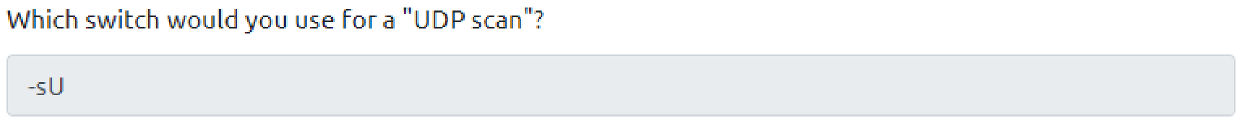
[Research] How many of these are considered "well-known"? (These are the "standard" numbers mention

1024

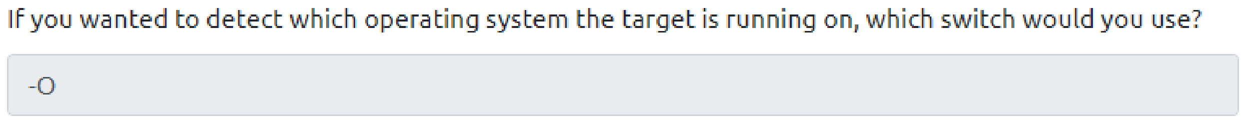
Task 3 nmap switches


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

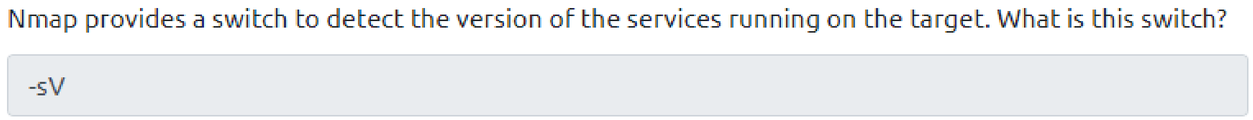
-sS


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

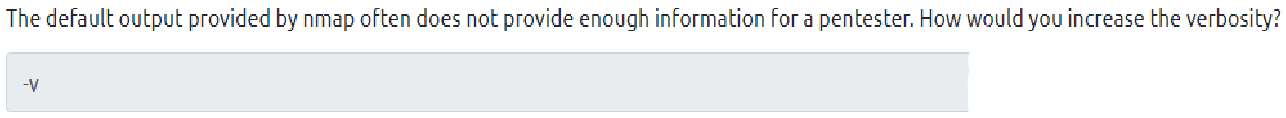
-sU


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

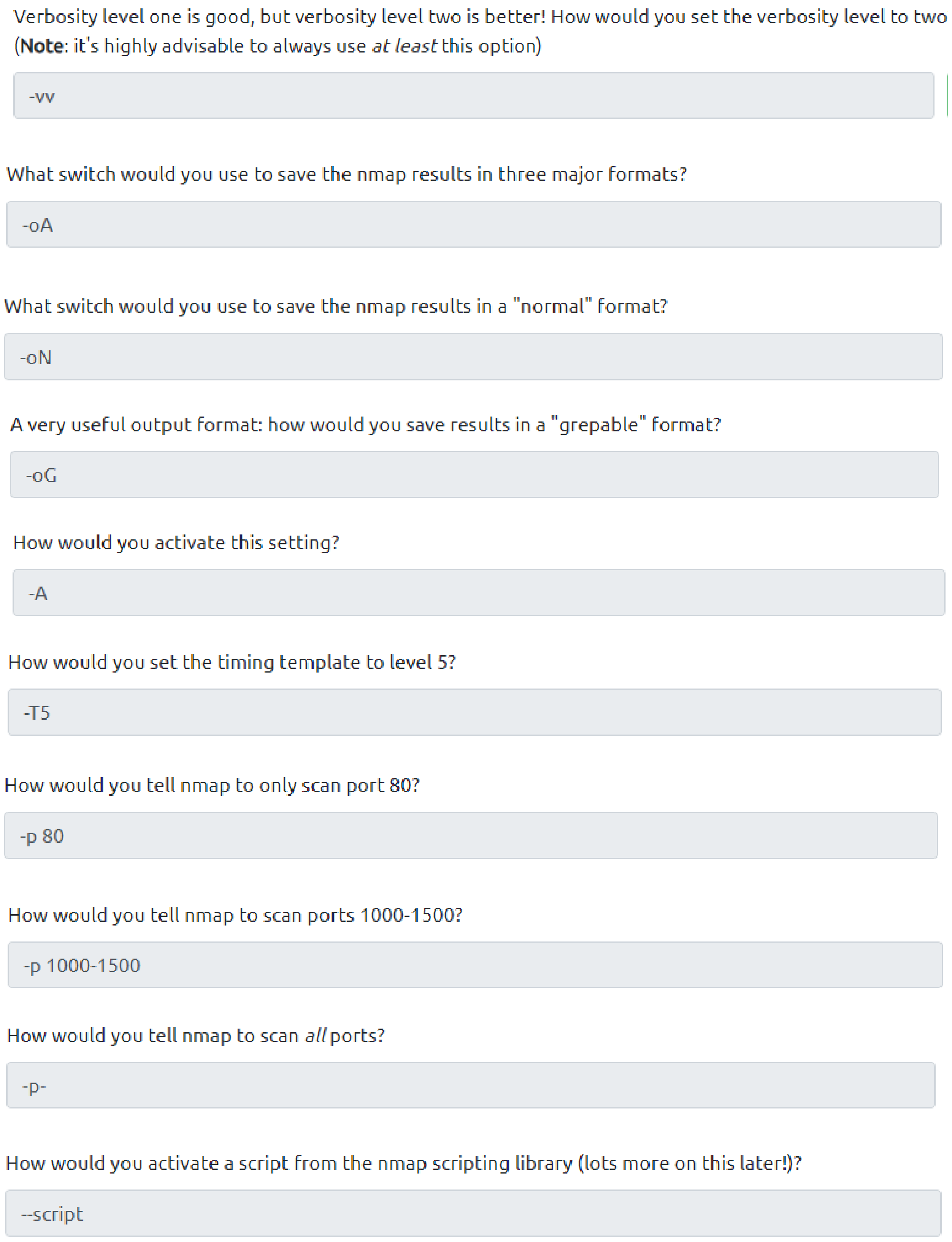
-O


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

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

How would you activate this setting?

-A

How would you set the timing template to level 5?

-T5

How would you tell nmap to only scan port 80?

-p 80

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

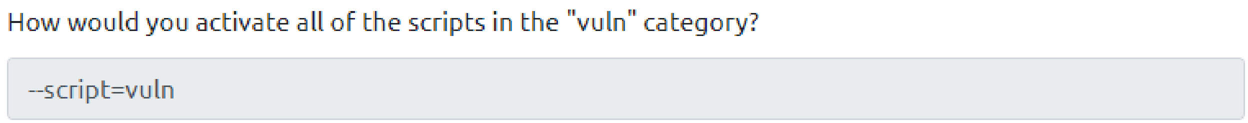
-p 1000-1500

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!)?

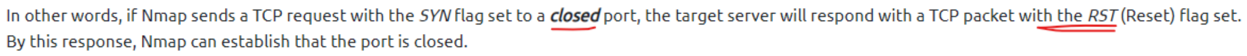
--script



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

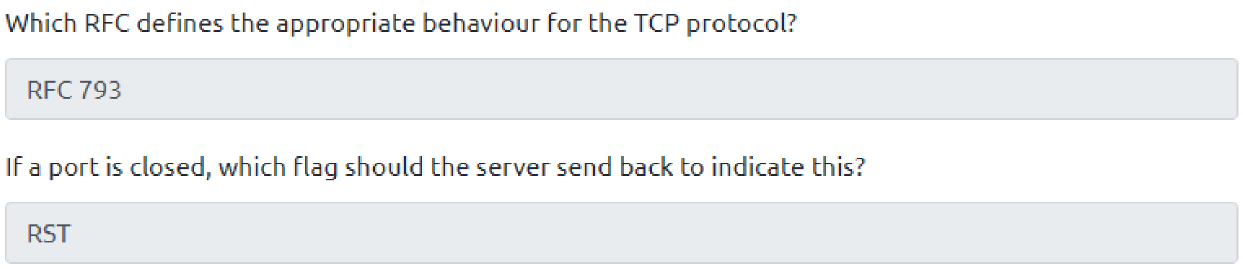
--script=vuln

Task 5 **Scan Types** TCP Connect Scans



In other words, if Nmap sends a TCP request with the *SYN* flag set to a ***closed*** port, the target server will respond with a TCP packet with the *RST* (Reset) flag set. By this response, Nmap can establish that the port is closed.

Which RFC defines the appropriate behaviour for the TCP protocol?



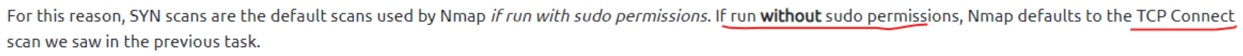
Which RFC defines the appropriate behaviour for the TCP protocol?

RFC 793

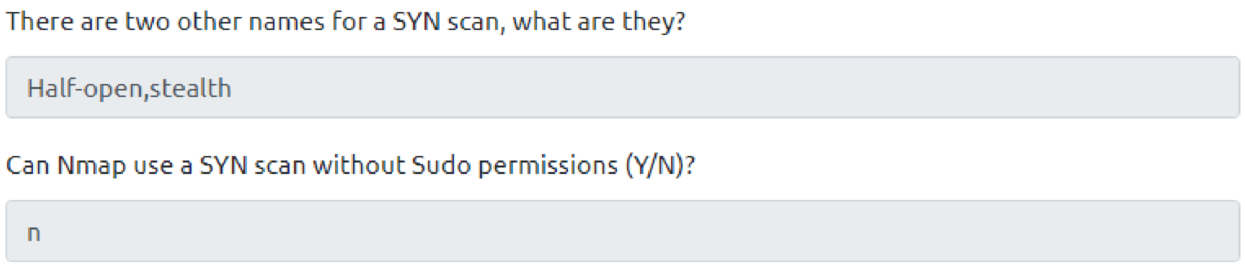
If a port is closed, which flag should the server send back to indicate this?

RST

Task 6 **Scan Types** SYN Scans



For this reason, SYN scans are the default scans used by Nmap *if run with sudo permissions*. If run **without** sudo permissions, Nmap defaults to the TCP Connect scan we saw in the previous task.



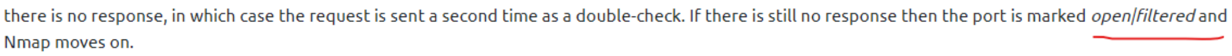
There are two other names for a SYN scan, what are they?

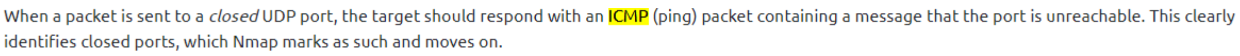
Half-open,stealth

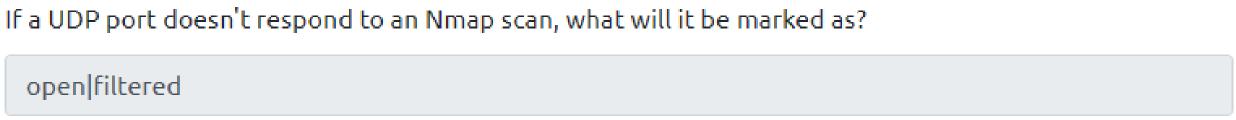
Can Nmap use a SYN scan without Sudo permissions (Y/N)?

n

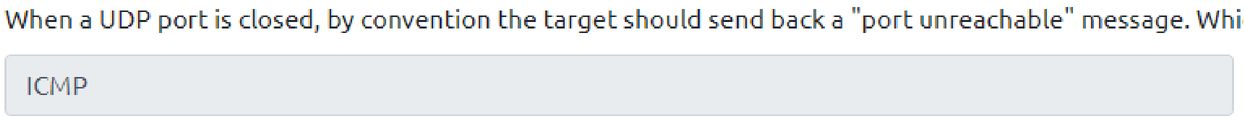
Task 7 **Scan Types** UDP Scans


there is no response, in which case the request is sent a second time as a double-check. If there is still no response then the port is marked *open|filtered* and Nmap moves on.


When a packet is sent to a *closed* UDP port, the target should respond with an ICMP (ping) packet containing a message that the port is unreachable. This clearly identifies closed ports, which Nmap marks as such and moves on.

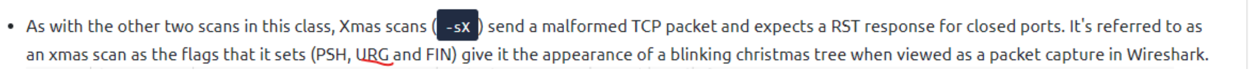

If a UDP port doesn't respond to an Nmap scan, what will it be marked as?

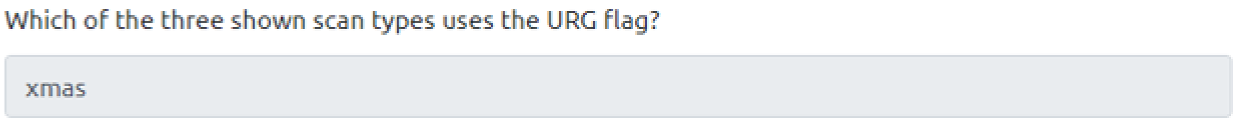
open|filtered


When a UDP port is closed, by convention the target should send back a "port unreachable" message. Whi

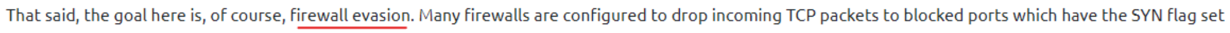
ICMP

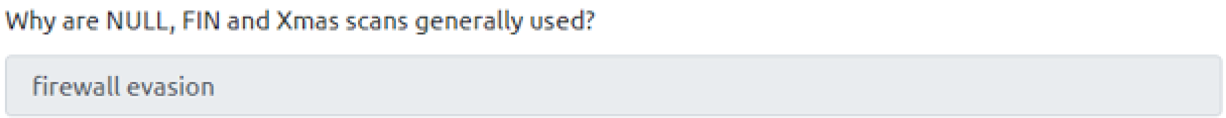
Task 8 **Scan Types** NULL, FIN and Xmas


- 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.

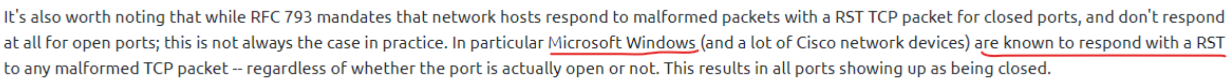

Which of the three shown scan types uses the URG flag?

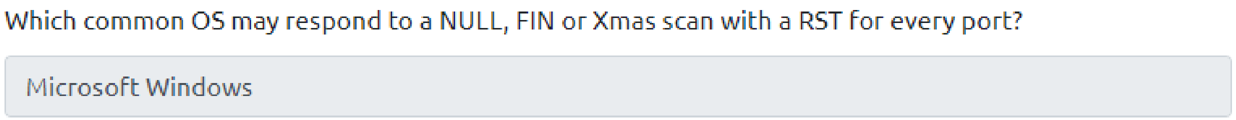
xmas


That said, the goal here is, of course, firewall evasion. Many firewalls are configured to drop incoming TCP packets to blocked ports which have the SYN flag set


Why are NULL, FIN and Xmas scans generally used?

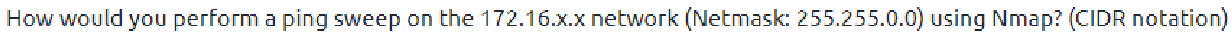
firewall evasion


It's also worth noting that while RFC 793 mandates that network hosts respond to malformed packets with a RST TCP packet for closed ports, and don't respond at all for open ports; this is not always the case in practice. In particular Microsoft Windows (and a lot of Cisco network devices) are known to respond with a RST to any malformed TCP packet -- regardless of whether the port is actually open or not. This results in all ports showing up as being closed.


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

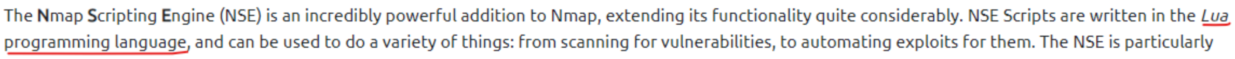
Microsoft Windows

Task 9 **Scan Types** ICMP Network Scanning

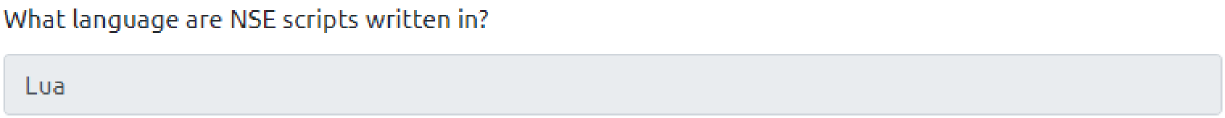

How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? (CIDR notation)

Since the netmask is 255.255.0.0 so that means the first 2 octets are constants and the rest are not so it's cleary they are 32 bits (the CIRD notation used with constant bits) so answer is: nmap -sn 172.16.0.0/16

Task 10 **NSE Scripts** Overview



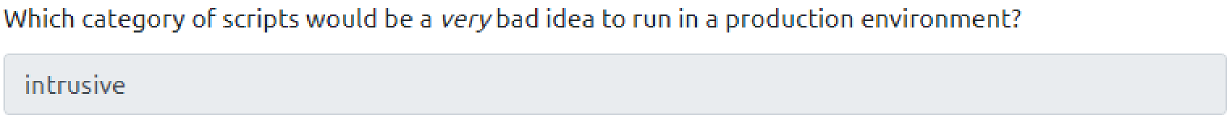
The **N**map **S**cripting **E**ngine (NSE) is an incredibly powerful addition to Nmap, extending its functionality quite considerably. NSE Scripts are written in the *Lua* programming language, and can be used to do a variety of things: from scanning for vulnerabilities, to automating exploits for them. The NSE is particularly



What language are NSE scripts written in?

Lua

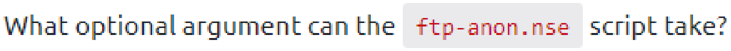
`intrusive` :- Not safe: likely to affect the target



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

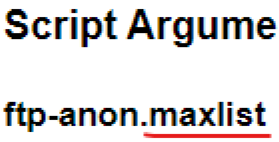
intrusive

Task 11 **NSE Scripts** Working with the NSE



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

Just little search I found that in https://nmap.org/nsedoc/scripts/ftp-anon.html

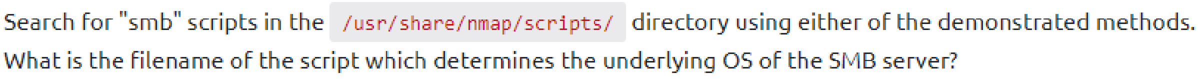


Script Arguments

ftp-anon.maxlist

Answer : maxlist

Task 12 **NSE Scripts** Searching for Scripts

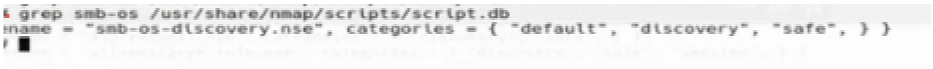


Search for "smb" scripts in the `/usr/share/nmap/scripts/` directory using either of the demonstrated methods. What is the filename of the script which determines the underlying OS of the SMB server?

Using grep as

grep smb-os /user/share/nmap/scripts/script.db

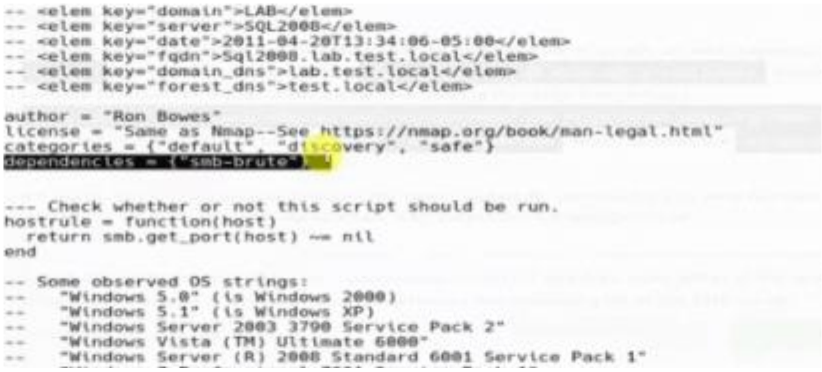
we got



```
$ grep smb-os /usr/share/nmap/scripts/script.db
Entry { filename = "smb-os-discovery.nse", categories = { "default", "discovery", "safe", } }
$ █
```

Answer : smb-os-discovery.nse

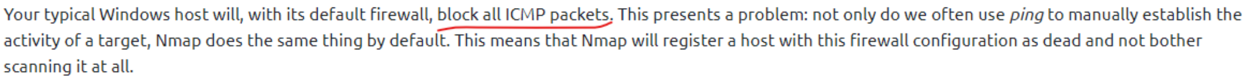
Read through this script. What does it depend on?



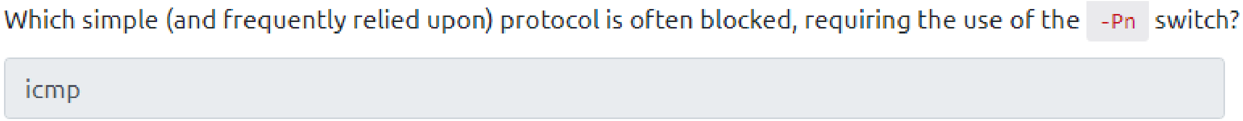
```
-- <elem key="domain">LAB</elem>
-- <elem key="server">SQL2008</elem>
-- <elem key="date">2011-04-20T13:34:06-05:00</elem>
-- <elem key="fqdn">Sql2008.lab.test.local</elem>
-- <elem key="domain_dns">lab.test.local</elem>
-- <elem key="forest_dns">test.local</elem>

author = "Ron Bowes"
license = "Same as Nmap--See https://nmap.org/book/man-legal.html"
categories = {"default", "discovery", "safe"}
dependencies = {"smb-brute"}


--- Check whether or not this script should be run.
hostrule = function(host)
  return smb.get_port(host) ~= nil
end

-- Some observed OS strings:
--    "Windows 5.0" (is Windows 2000)
--    "Windows 5.1" (is Windows XP)
--    "Windows Server 2003 3790 Service Pack 2"
--    "Windows Vista (TM) Ultimate 6000"
--    "Windows Server (R) 2008 Standard 6001 Service Pack 1"
```

Answer : smb-brute

Task 13 Firewall Evasion

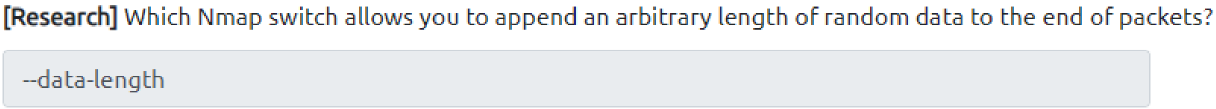


Your typical Windows host will, with its default firewall, block all ICMP packets. This presents a problem: not only do we often use *ping* to manually establish the activity of a target, Nmap does the same thing by default. This means that Nmap will register a host with this firewall configuration as dead and not bother scanning it at all.



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

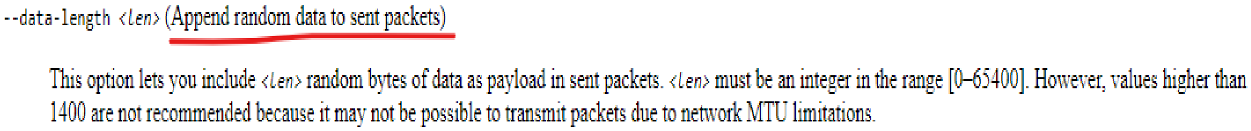
icmp



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

--data-length

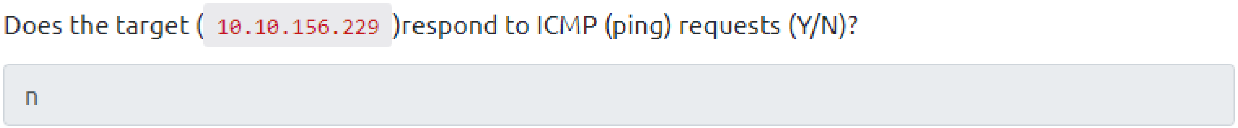
Just little search I found in https://nmap.org/book/nping-man-payload-options.html



`--data-length` *<len>* (Append random data to sent packets)

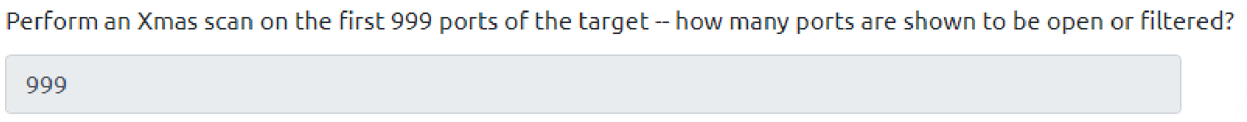
This option lets you include *<len>* random bytes of data as payload in sent packets. *<len>* must be an integer in the range [0–65400]. However, values higher than 1400 are not recommended because it may not be possible to transmit packets due to network MTU limitations.

Task 14 practical



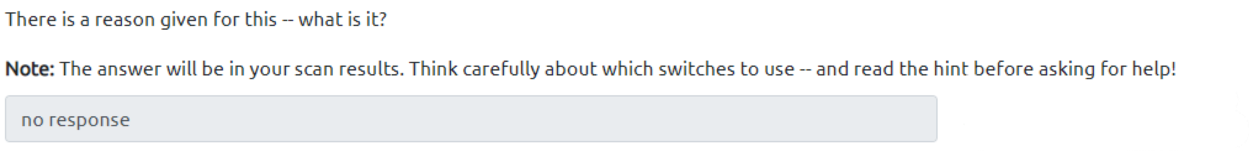
Does the target (`10.10.156.229`)respond to ICMP (ping) requests (Y/N)?

n



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

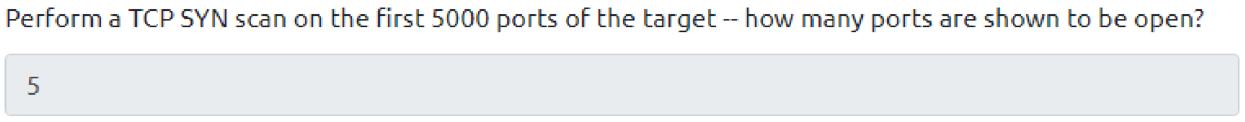
999



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!

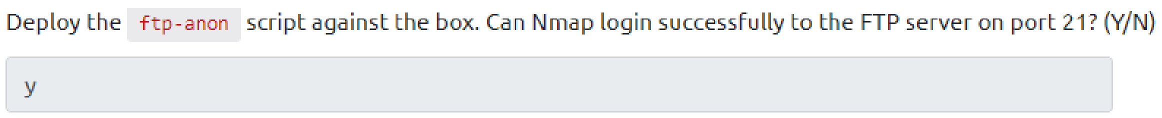
no response



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

5

Using nmap -p0-4999 -T4 -Pn 10.10.156.229



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

y

Using nmap -p 21 -Pn –script ftp-anon 10.10.156.229

Congratulations

You've completed the room!