Lab Report No.4

Advanced Scanning using Nmap

Ethical Hacking

Submitted By: Raghad Alharthi 2210003220

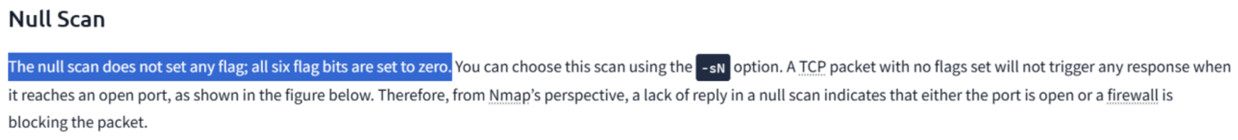
Section: CS Group no. 2

Contents

Room: Nmap Advanced Port Scans

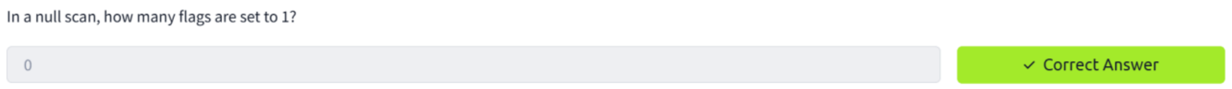
Task 2

Q1



Null Scan

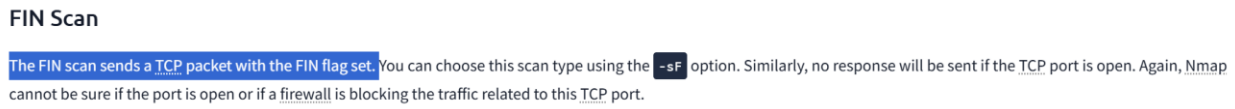
The null scan does not set any flag; all six flag bits are set to zero. You can choose this scan using the `-sN` option. A TCP packet with no flags set will not trigger any response when it reaches an open port, as shown in the figure below. Therefore, from Nmap's perspective, a lack of reply in a null scan indicates that either the port is open or a firewall is blocking the packet.



In a null scan, how many flags are set to 1?

0

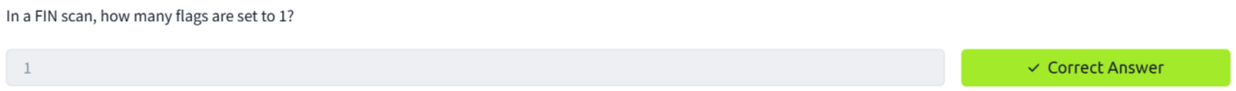
Q2



FIN Scan

The FIN scan sends a TCP packet with the FIN flag set. You can choose this scan type using the `-sF` option. Similarly, no response will be sent if the TCP port is open. Again, Nmap cannot be sure if the port is open or if a firewall is blocking the traffic related to this TCP port.

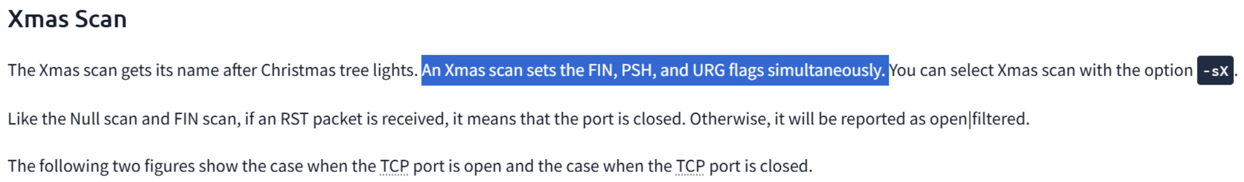
Only the FIN flag is 1.



In a FIN scan, how many flags are set to 1?

1

Q3



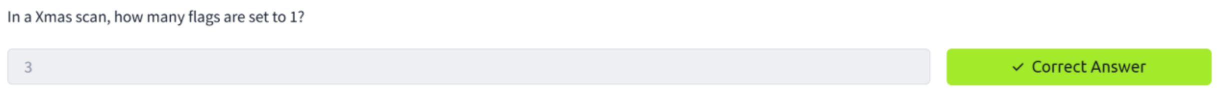
Xmas Scan

The Xmas scan gets its name after Christmas tree lights. An Xmas scan sets the FIN, PSH, and URG flags simultaneously. You can select Xmas scan with the option `-sX`.

Like the Null scan and FIN scan, if an RST packet is received, it means that the port is closed. Otherwise, it will be reported as open|filtered.

The following two figures show the case when the TCP port is open and the case when the TCP port is closed.

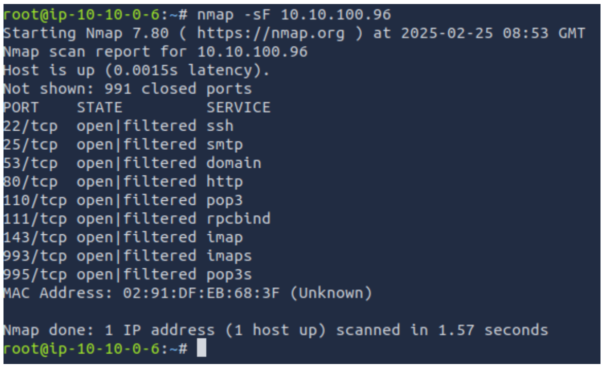
3 flags (FIN, PSH, and URG)



In a Xmas scan, how many flags are set to 1?

3

Q4



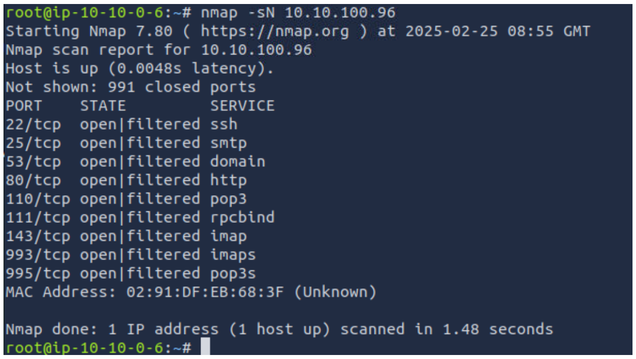
```
root@ip-10-10-0-6:~# nmap -sF 10.10.100.96
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-25 08:53 GMT
Nmap scan report for 10.10.100.96
Host is up (0.0015s latency).
Not shown: 991 closed ports
PORT    STATE         SERVICE
22/tcp  open|filtered ssh
25/tcp  open|filtered smtp
53/tcp  open|filtered domain
80/tcp  open|filtered http
110/tcp open|filtered pop3
111/tcp open|filtered rpcbind
143/tcp open|filtered imap
993/tcp open|filtered imaps
995/tcp open|filtered pop3s
MAC Address: 02:91:DF:EB:68:3F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
root@ip-10-10-0-6:~# 
```

Start the VM and load the AttackBox. Once both are ready, open the terminal on the AttackBox and use nmap to launch a FIN scan against the target VM. How many ports appear as open|filtered?

9

✓ Correct Answer

Q4



```
root@ip-10-10-0-6:~# nmap -sN 10.10.100.96
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-25 08:55 GMT
Nmap scan report for 10.10.100.96
Host is up (0.0048s latency).
Not shown: 991 closed ports
PORT    STATE         SERVICE
22/tcp  open|filtered ssh
25/tcp  open|filtered smtp
53/tcp  open|filtered domain
80/tcp  open|filtered http
110/tcp open|filtered pop3
111/tcp open|filtered rpcbind
143/tcp open|filtered imap
993/tcp open|filtered imaps
995/tcp open|filtered pop3s
MAC Address: 02:91:DF:EB:68:3F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds
root@ip-10-10-0-6:~# 
```

Repeat your scan launching a null scan against the target VM. How many ports appear as open|filtered?

9

✓ Correct Answer

Task 3

Q1

Uriel Maimon first described this scan in 1996. In this scan, the FIN and ACK bits are set. The target should send an RST packet as a response. However, certain BSD-derived systems drop the packet if it is an open port exposing the open ports. This scan won't work on most targets encountered in modern networks; however, we include it in this room to better understand the port scanning mechanism and the hacking mindset. To select this scan type, use the `-sM` option.

2 flags (FIN and ACK)

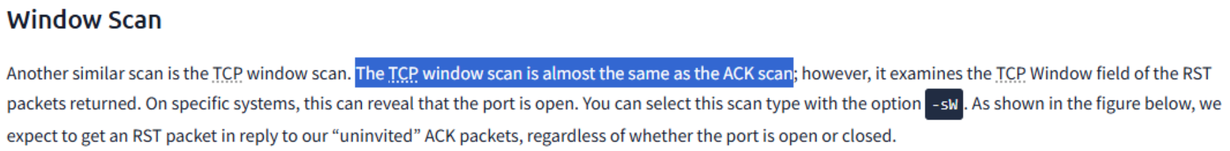
In the Maimon scan, how many flags are set?

2

✓ Correct Answer

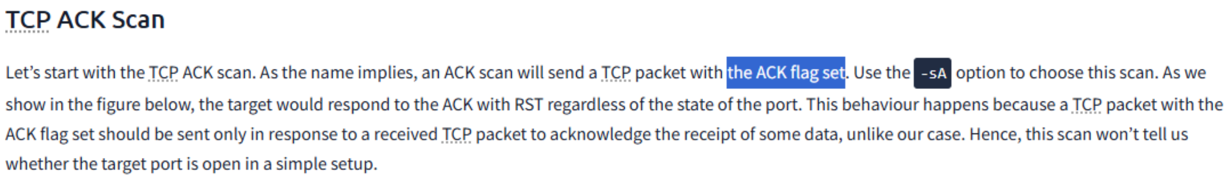
Task 4

Q1



Window Scan

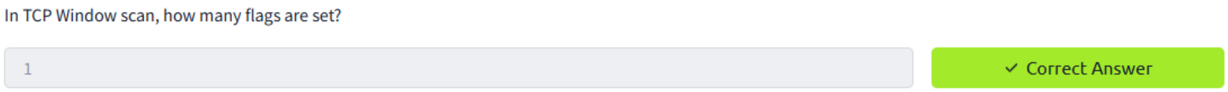
Another similar scan is the TCP window scan. The TCP window scan is almost the same as the ACK scan; however, it examines the TCP Window field of the RST packets returned. On specific systems, this can reveal that the port is open. You can select this scan type with the option `-sW`. As shown in the figure below, we expect to get an RST packet in reply to our "uninvited" ACK packets, regardless of whether the port is open or closed.



TCP ACK Scan

Let's start with the TCP ACK scan. As the name implies, an ACK scan will send a TCP packet with the ACK flag set. Use the `-sA` option to choose this scan. As we show in the figure below, the target would respond to the ACK with RST regardless of the state of the port. This behaviour happens because a TCP packet with the ACK flag set should be sent only in response to a received TCP packet to acknowledge the receipt of some data, unlike our case. Hence, this scan won't tell us whether the target port is open in a simple setup.

Knowing that we come to a conclusion that the flag set is only one which is the ACK flag



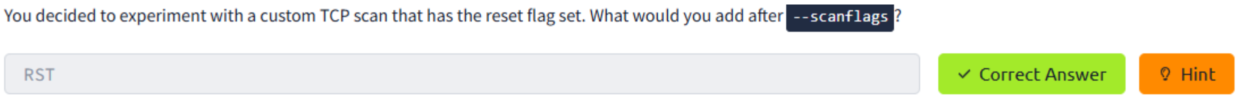
In TCP Window scan, how many flags are set?

1

Q2

We know from previous labs that reset flag is RST

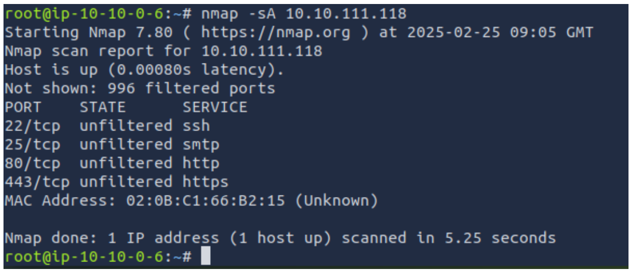
```
nmap --scanflags CUSTOM_FLAGS TARGET
```



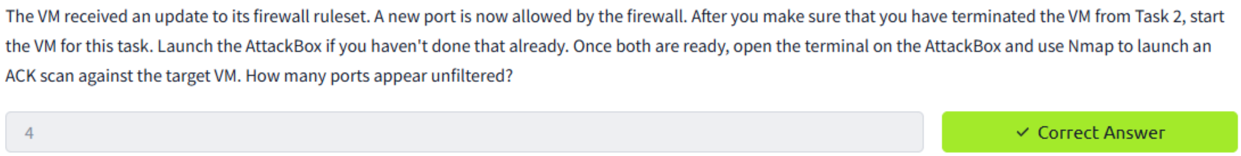
You decided to experiment with a custom TCP scan that has the reset flag set. What would you add after `--scanflags`?

RST

Q3



```
root@ip-10-10-0-6:~# nmap -sA 10.10.111.118
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-25 09:05 GMT
Nmap scan report for 10.10.111.118
Host is up (0.00080s latency).
Not shown: 996 filtered ports
PORT    STATE      SERVICE
22/tcp  unfiltered ssh
25/tcp  unfiltered smtp
80/tcp  unfiltered http
443/tcp unfiltered https
MAC Address: 02:0B:C1:66:B2:15 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 5.25 seconds
root@ip-10-10-0-6:~#
```



The VM received an update to its firewall ruleset. A new port is now allowed by the firewall. After you make sure that you have terminated the VM from Task 2, start the VM for this task. Launch the AttackBox if you haven't done that already. Once both are ready, open the terminal on the AttackBox and use Nmap to launch an ACK scan against the target VM. How many ports appear unfiltered?

4

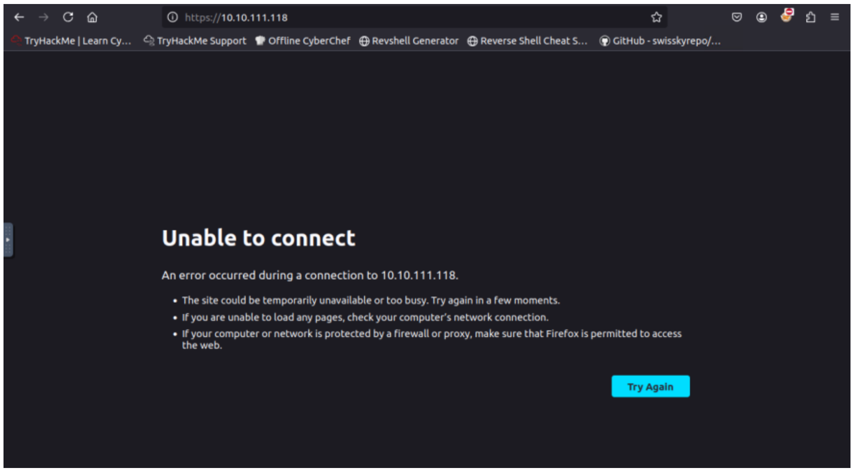
Q4

https port (443)

What is the new port number that appeared?

443 ✓ Correct Answer

Q5



Unable to connect

An error occurred during a connection to 10.10.111.118.

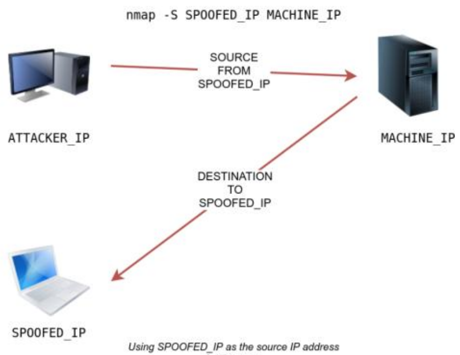
- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Is there any service behind the newly discovered port number? (Y/N)

N ✓ Correct Answer 💡 Hint

Task 5

Q1



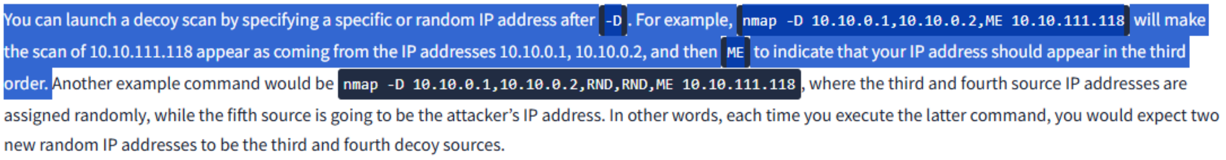
```
nmap -S SPOOFED_IP MACHINE_IP
```

Using SPOOFED_IP as the source IP address for the scan.

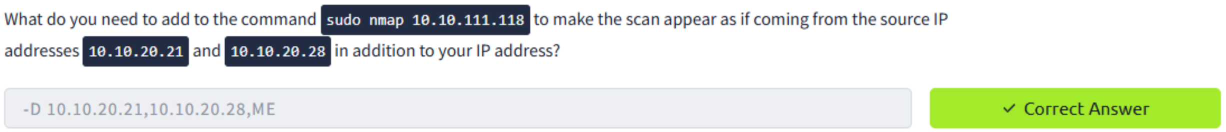
What do you need to add to the command `sudo nmap 10.10.111.118` to make the scan appear as if coming from the source IP address `10.10.10.11` instead of your IP address?

-S 10.10.10.11 ✓ Correct Answer

Q2



You can launch a decoy scan by specifying a specific or random IP address after `-D`. For example, `nmap -D 10.10.0.1,10.10.0.2,ME 10.10.111.118` will make the scan of 10.10.111.118 appear as coming from the IP addresses 10.10.0.1, 10.10.0.2, and then `ME` to indicate that your IP address should appear in the third order. Another example command would be `nmap -D 10.10.0.1,10.10.0.2,RND,RND,ME 10.10.111.118`, where the third and fourth source IP addresses are assigned randomly, while the fifth source is going to be the attacker's IP address. In other words, each time you execute the latter command, you would expect two new random IP addresses to be the third and fourth decoy sources.



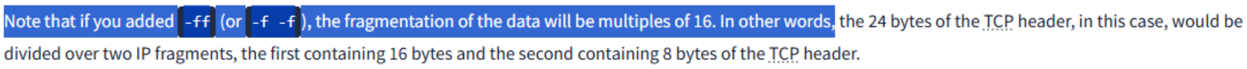
What do you need to add to the command `sudo nmap 10.10.111.118` to make the scan appear as if coming from the source IP addresses `10.10.20.21` and `10.10.20.28` in addition to your IP address?

-D 10.10.20.21,10.10.20.28,ME

✓ Correct Answer

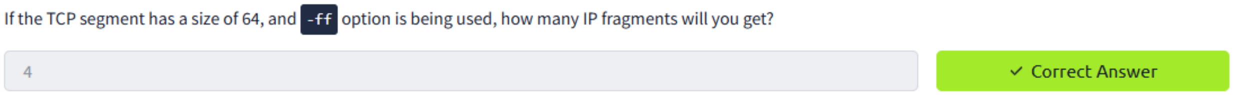
Task 6

Q1



Note that if you added `-ff` (or `-f -f`), the fragmentation of the data will be multiples of 16. In other words, the 24 bytes of the TCP header, in this case, would be divided over two IP fragments, the first containing 16 bytes and the second containing 8 bytes of the TCP header.

64 / 16 = 4



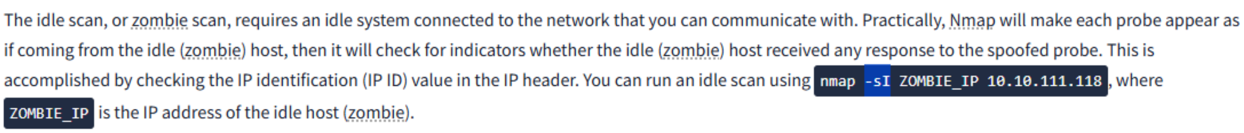
If the TCP segment has a size of 64, and `-ff` option is being used, how many IP fragments will you get?

4

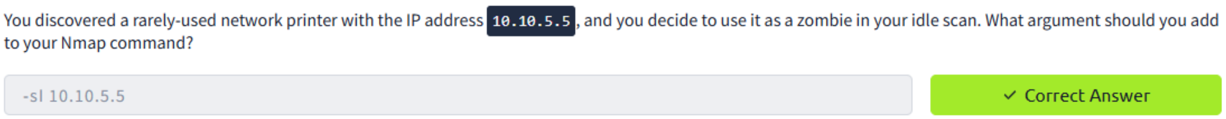
✓ Correct Answer

Task 7

Q1



The idle scan, or zombie scan, requires an idle system connected to the network that you can communicate with. Practically, Nmap will make each probe appear as if coming from the idle (zombie) host, then it will check for indicators whether the idle (zombie) host received any response to the spoofed probe. This is accomplished by checking the IP identification (IP ID) value in the IP header. You can run an idle scan using `nmap -sI ZOMBIE_IP 10.10.111.118`, where `ZOMBIE_IP` is the IP address of the idle host (zombie).



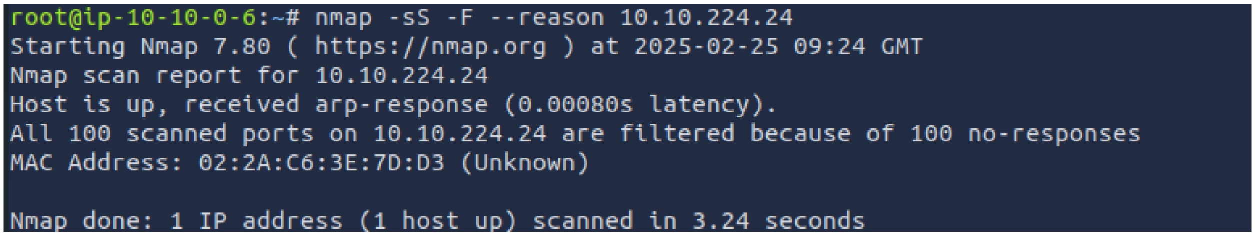
You discovered a rarely-used network printer with the IP address `10.10.5.5`, and you decide to use it as a zombie in your idle scan. What argument should you add to your Nmap command?

-sI 10.10.5.5

✓ Correct Answer

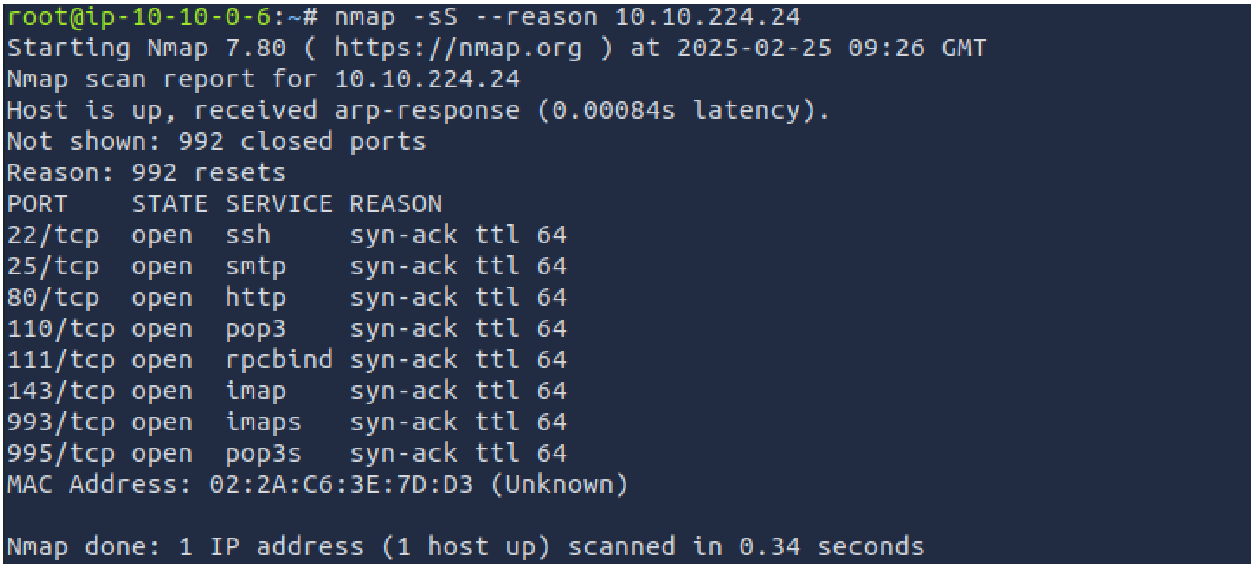
Task 8

Q1



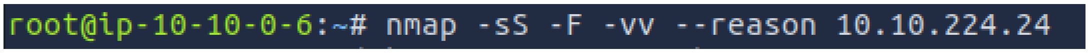
```
root@ip-10-10-0-6:~# nmap -sS -F --reason 10.10.224.24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-25 09:24 GMT
Nmap scan report for 10.10.224.24
Host is up, received arp-response (0.00080s latency).
All 100 scanned ports on 10.10.224.24 are filtered because of 100 no-responses
MAC Address: 02:2A:C6:3E:7D:D3 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.24 seconds
```

Not a telling output, so I changed command to:



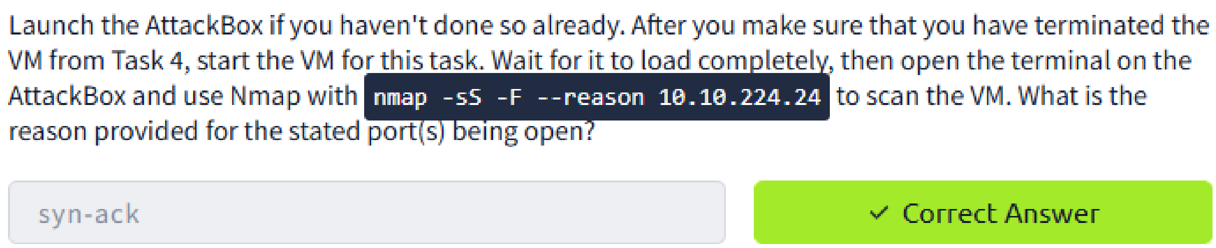
```
root@ip-10-10-0-6:~# nmap -sS --reason 10.10.224.24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-25 09:26 GMT
Nmap scan report for 10.10.224.24
Host is up, received arp-response (0.00084s latency).
Not shown: 992 closed ports
Reason: 992 resets
PORT    STATE SERVICE REASON
22/tcp  open  ssh     syn-ack ttl 64
25/tcp  open  smtp    syn-ack ttl 64
80/tcp  open  http    syn-ack ttl 64
110/tcp open  pop3    syn-ack ttl 64
111/tcp open  rpcbind syn-ack ttl 64
143/tcp open  imap    syn-ack ttl 64
993/tcp open  imaps   syn-ack ttl 64
995/tcp open  pop3s   syn-ack ttl 64
MAC Address: 02:2A:C6:3E:7D:D3 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

Or this command:



```
root@ip-10-10-0-6:~# nmap -sS -F -vv --reason 10.10.224.24
```

Both of these commands gave the answer.



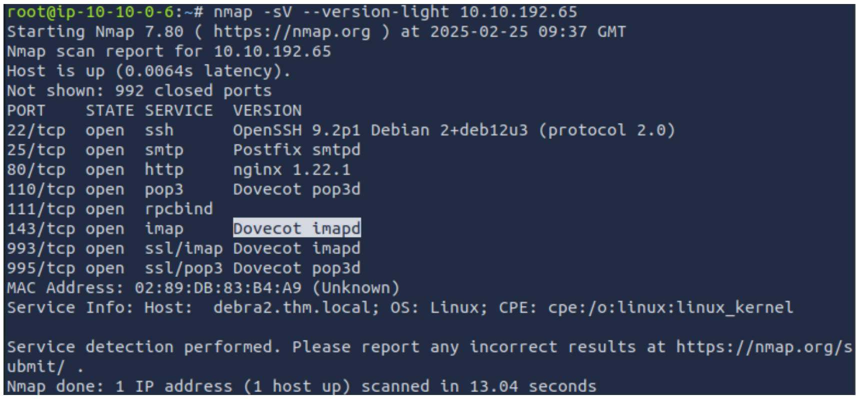
Launch the AttackBox if you haven't done so already. After you make sure that you have terminated the VM from Task 4, start the VM for this task. Wait for it to load completely, then open the terminal on the AttackBox and use Nmap with `nmap -sS -F --reason 10.10.224.24` to scan the VM. What is the reason provided for the stated port(s) being open?

syn-ack

Room: Nmap Post Port Scans

Task 2

Q1



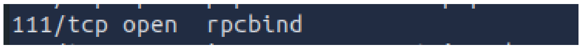
```
root@ip-10-10-0-6:~# nmap -sV --version-light 10.10.192.65
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-25 09:37 GMT
Nmap scan report for 10.10.192.65
Host is up (0.0064s latency).
Not shown: 992 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
25/tcp  open  smtp     Postfix smtpd
80/tcp  open  http     nginx 1.22.1
110/tcp open  pop3     Dovecot pop3d
111/tcp open  rpcbind
143/tcp open  imap     Dovecot imapd
993/tcp open  ssl/imap Dovecot imapd
995/tcp open  ssl/pop3 Dovecot pop3d
MAC Address: 02:89:DB:83:B4:A9 (Unknown)
Service Info: Host:  debra2.thm.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.04 seconds
```

Start the target machine for this task and launch the AttackBox. Run `nmap -sV --version-light 10.10.192.65` via the AttackBox. What is the detected version for port 143?

Dovecot imapd

✓ Correct Answer

Q2



```
111/tcp open  rpcbind
```

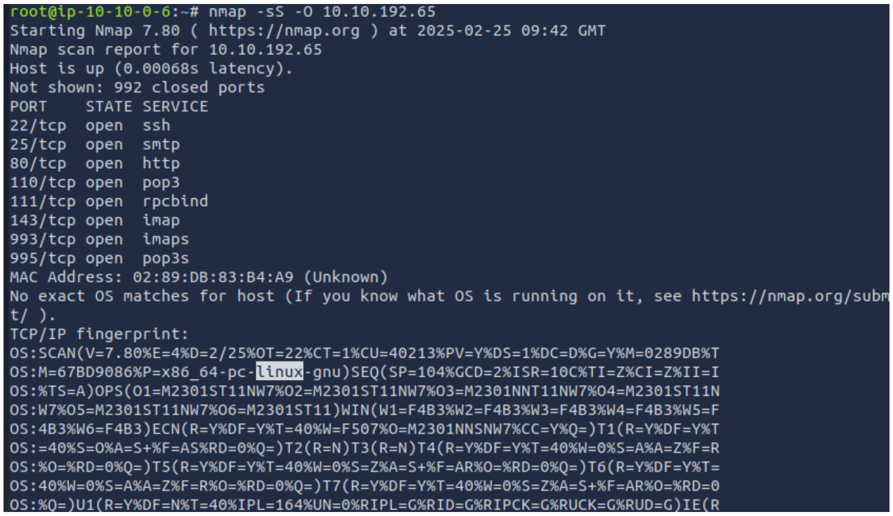
Which service did not have a version detected with `--version-light`?

rpcbind

✓ Correct Answer

Task 3

Q1



```
root@ip-10-10-0-6:~# nmap -sS -O 10.10.192.65
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-25 09:42 GMT
Nmap scan report for 10.10.192.65
Host is up (0.00068s latency).
Not shown: 992 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
111/tcp open  rpcbind
143/tcp open  imap
993/tcp open  imaps
995/tcp open  pop3s
MAC Address: 02:89:DB:83:B4:A9 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/subm
t/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=2/25%OT=22%CT=1%CU=40213%PV=Y%DS=1%DC=D%G=Y%M=0289DB%T
OS:M=67BD9086%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=2%ISR=10C%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M2301ST11NW7%O2=M2301ST11NW7%O3=M2301NNT11NW7%O4=M2301ST11N
OS:W7%O5=M2301ST11NW7%O6=M2301ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F
OS:4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M2301NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T
OS:=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R
OS:%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=
OS:40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0
OS:%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R
```

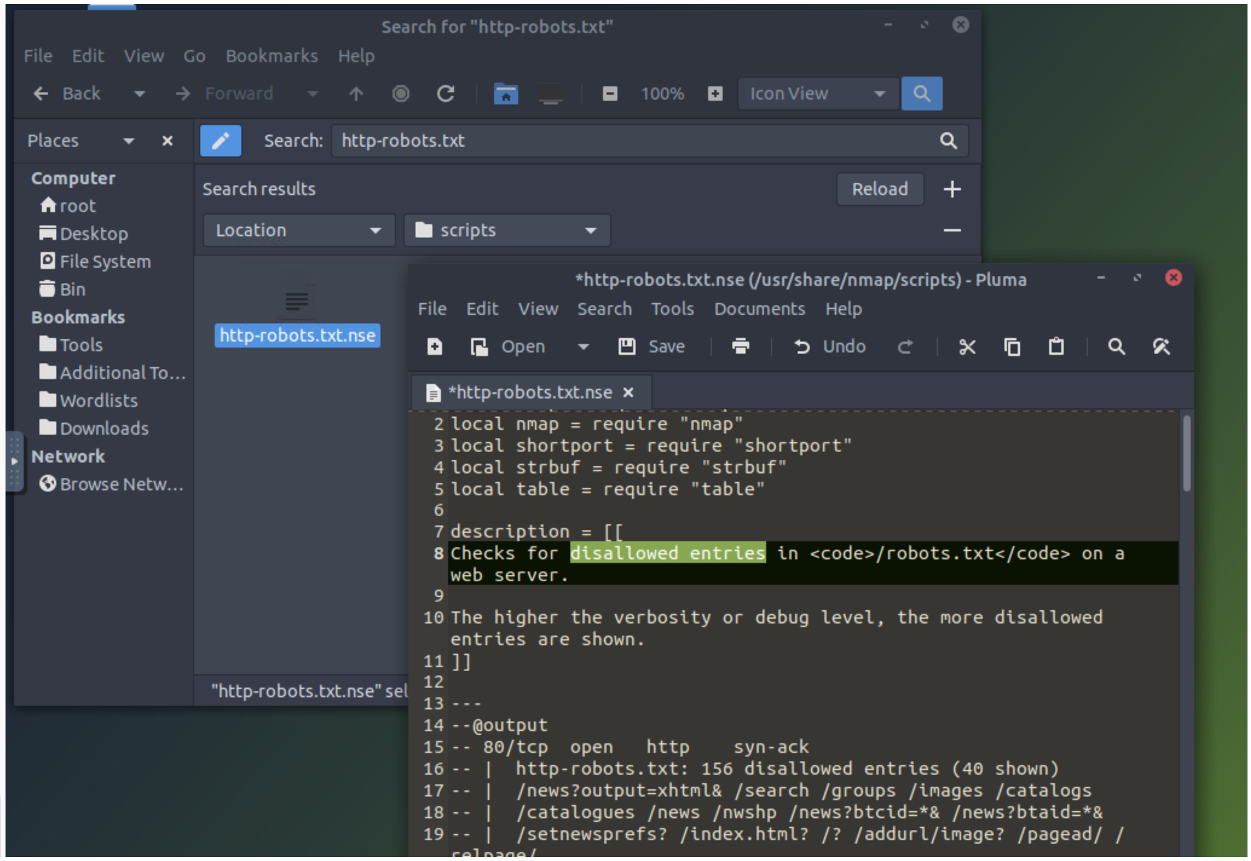
Run `nmap` with `-O` option against `10.10.192.65`. What OS did Nmap detect?

Linux

✓ Correct Answer

Task 4

Q1



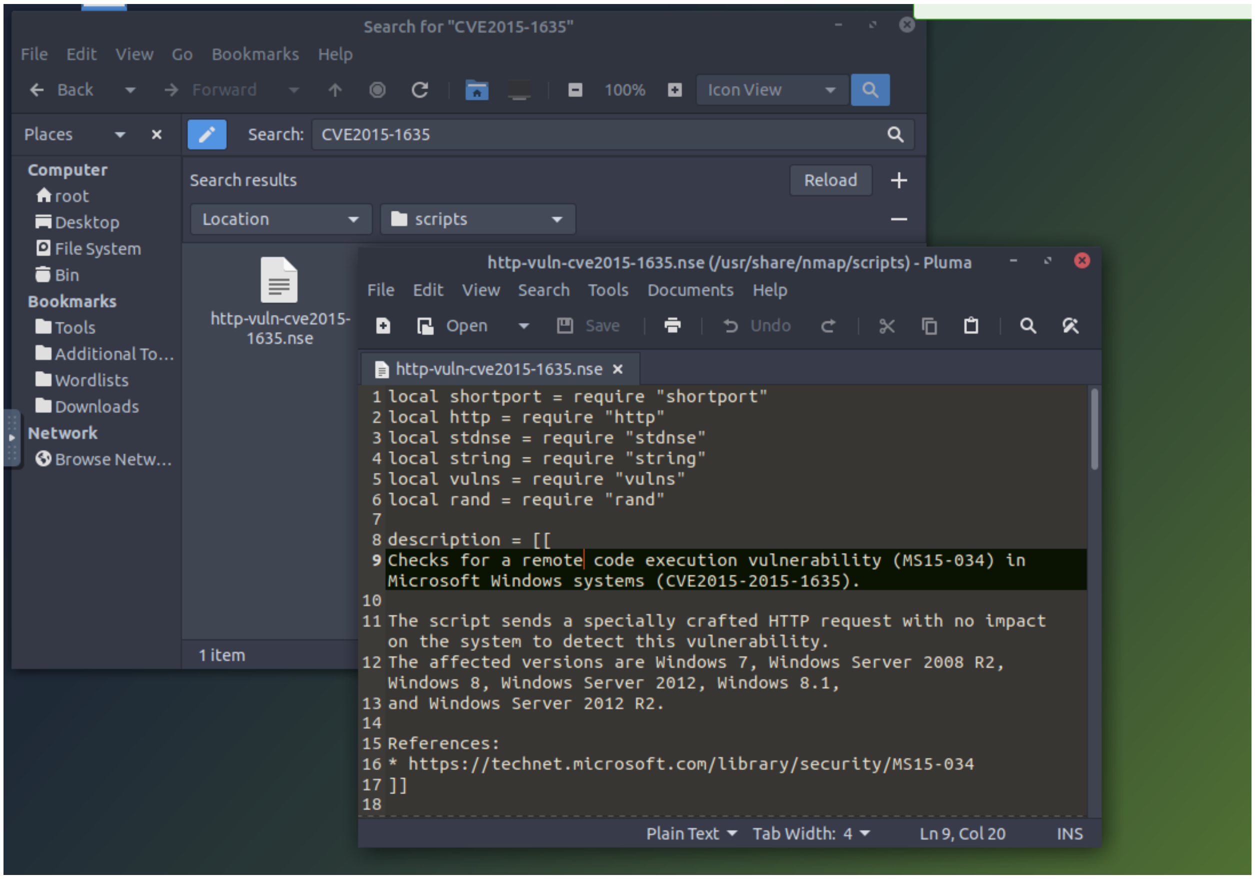
```
local nmap = require "nmap"
local shortport = require "shortport"
local strbuf = require "strbuf"
local table = require "table"

description = [[
Checks for disallowed entries in <code>/robots.txt</code> on a web server.

The higher the verbosity or debug level, the more disallowed entries are shown.
]]

---
--@output
-- 80/tcp  open   http    syn-ack
-- |  http-robots.txt: 156 disallowed entries (40 shown)
-- |  /news?output=xhtml& /search /groups /images /catalogs
-- |  /catalogues /news /nwshp /news?btcid=*& /news?btaid=*&
-- |  /setnewsprefs? /index.html? /? /addurl/image? /pagead/ /
relpage/
```

Knowing that Nmap scripts are saved in `/usr/share/nmap/scripts` on the AttackBox. What does the script `http-robots.txt` check for?

disallowed entries

✓ Correct Answer

Q2

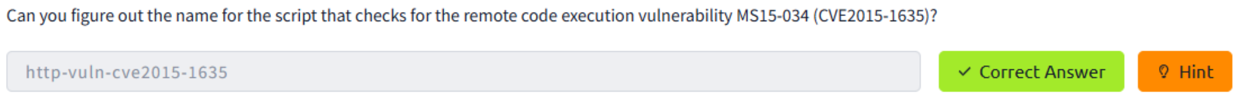


Search for "CVE2015-1635"
File Edit View Go Bookmarks Help
Back Forward 100% Icon View
Places
Computer
root
Desktop
File System
Bin
Bookmarks
Tools
Additional To…
Wordlists
Downloads
Network
Browse Netw…
Search results
Reload
Location
scripts
http-vuln-cve2015-1635.nse
1 item
http-vuln-cve2015-1635.nse (/usr/share/nmap/scripts) - Pluma
File Edit View Search Tools Documents Help
Open Save Undo
http-vuln-cve2015-1635.nse
Plain Text Tab Width: 4 Ln 9, Col 20 INS

Search: CVE2015-1635

```
local shortport = require "shortport"
local http = require "http"
local stdnse = require "stdnse"
local string = require "string"
local vulns = require "vulns"
local rand = require "rand"

description = [[
Checks for a remote code execution vulnerability (MS15-034) in Microsoft Windows systems (CVE2015-2015-1635).

The script sends a specially crafted HTTP request with no impact on the system to detect this vulnerability.
The affected versions are Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1,
and Windows Server 2012 R2.

References:
* https://technet.microsoft.com/library/security/MS15-034
]]

```

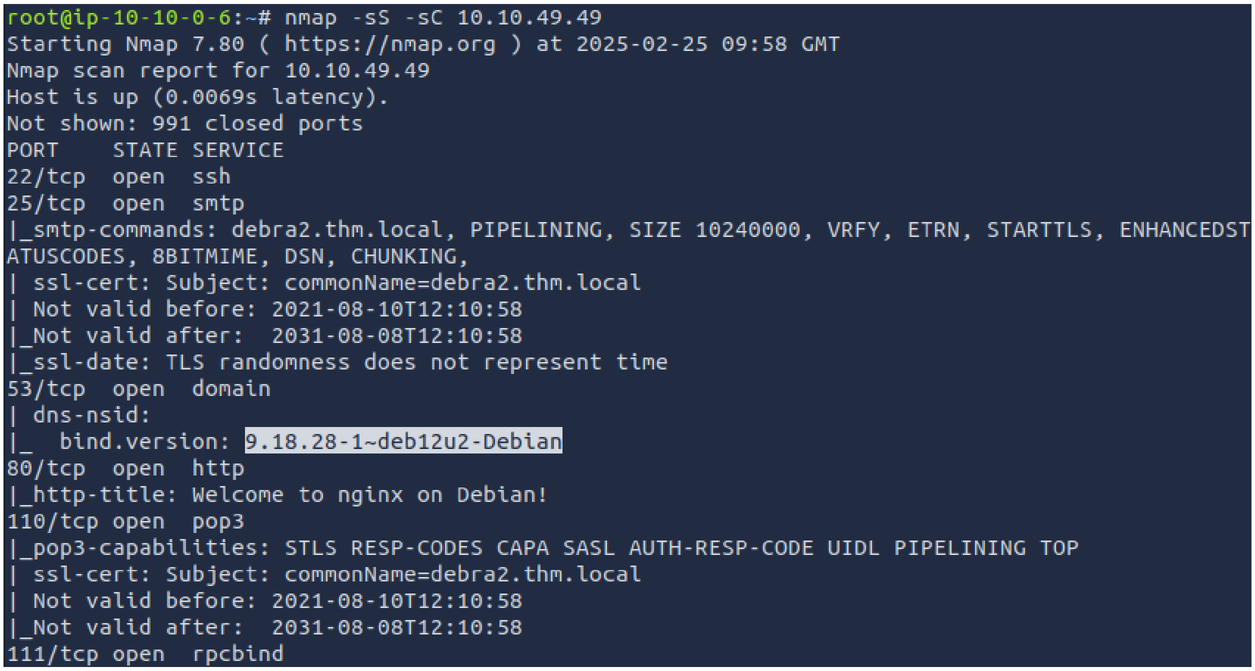
Searched “CVE2015-1635” and it appears right away



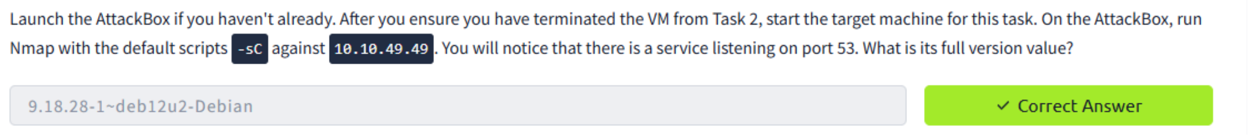
Can you figure out the name for the script that checks for the remote code execution vulnerability MS15-034 (CVE2015-1635)?

http-vuln-cve2015-1635

Q3



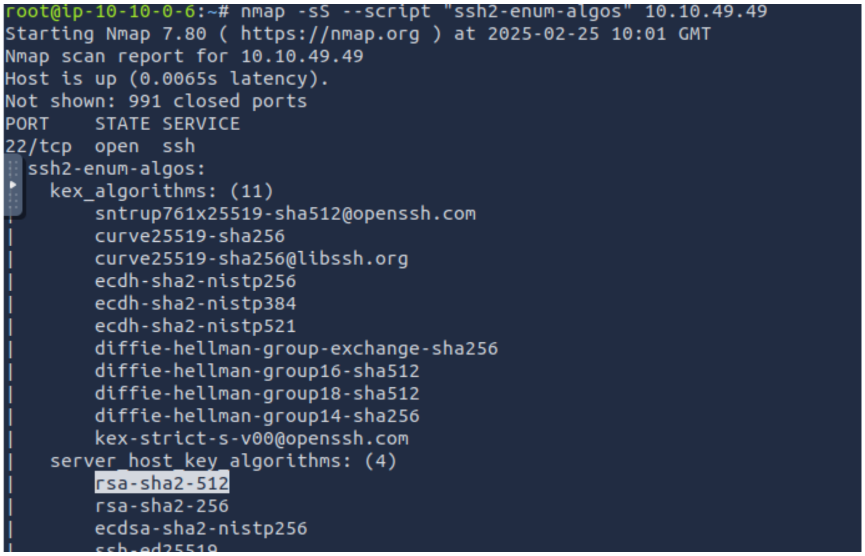
```
root@ip-10-10-0-6:~# nmap -sS -sC 10.10.49.49
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-25 09:58 GMT
Nmap scan report for 10.10.49.49
Host is up (0.0069s latency).
Not shown: 991 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
|_smtp-commands: debra2.thm.local, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDST
ATUSCODES, 8BITMIME, DSN, CHUNKING,
| ssl-cert: Subject: commonName=debra2.thm.local
| Not valid before: 2021-08-10T12:10:58
|_Not valid after:  2031-08-08T12:10:58
|_ssl-date: TLS randomness does not represent time
53/tcp  open  domain
| dns-nsid:
|_  bind.version: 9.18.28-1~deb12u2-Debian
80/tcp  open  http
|_http-title: Welcome to nginx on Debian!
110/tcp open  pop3
|_pop3-capabilities: STLS RESP-CODES CAPA SASL AUTH-RESP-CODE UIDL PIPELINING TOP
| ssl-cert: Subject: commonName=debra2.thm.local
| Not valid before: 2021-08-10T12:10:58
|_Not valid after:  2031-08-08T12:10:58
111/tcp open  rpcbind
```



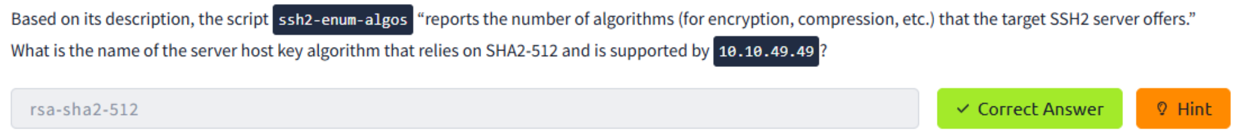
Launch the AttackBox if you haven't already. After you ensure you have terminated the VM from Task 2, start the target machine for this task. On the AttackBox, run Nmap with the default scripts `-sC` against `10.10.49.49`. You will notice that there is a service listening on port 53. What is its full version value?

9.18.28-1~deb12u2-Debian

Q4



```
root@ip-10-10-0-6:~# nmap -sS --script "ssh2-enum-algos" 10.10.49.49
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-25 10:01 GMT
Nmap scan report for 10.10.49.49
Host is up (0.0065s latency).
Not shown: 991 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
  ssh2-enum-algos:
    kex_algorithms: (11)
|       sntrup761x25519-sha512@openssh.com
|       curve25519-sha256
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group16-sha512
|       diffie-hellman-group18-sha512
|       diffie-hellman-group14-sha256
|       kex-strict-s-v00@openssh.com
|   server_host_key_algorithms: (4)
|       rsa-sha2-512
|       rsa-sha2-256
|       ecdsa-sha2-nistp256
|       ssh-ed25519
```

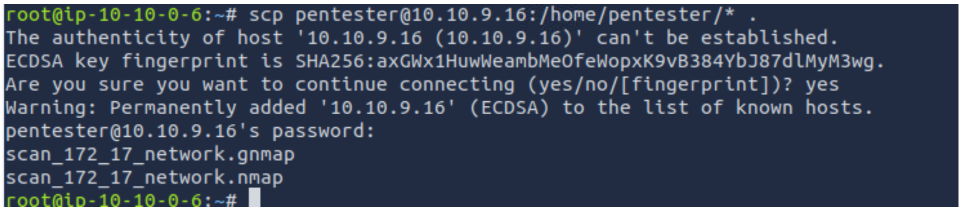


Based on its description, the script `ssh2-enum-algos` "reports the number of algorithms (for encryption, compression, etc.) that the target SSH2 server offers." What is the name of the server host key algorithm that relies on SHA2-512 and is supported by `10.10.49.49`?

rsa-sha2-512

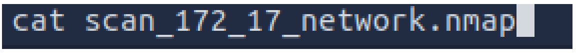
Task 5

Downloading reports:

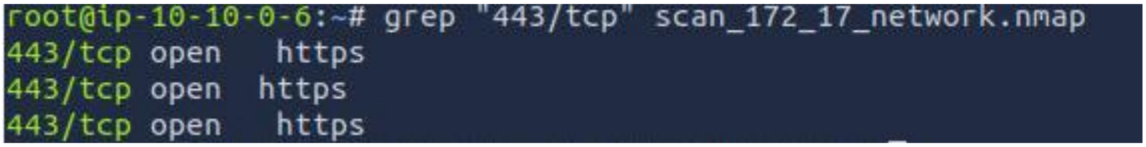


```
root@ip-10-10-0-6:~# scp pentester@10.10.9.16:/home/pentester/* .
The authenticity of host '10.10.9.16 (10.10.9.16)' can't be established.
ECDSA key fingerprint is SHA256:axGWx1HuwWeambMeOfeWopxK9vB384YbJ87dlMyM3wg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.9.16' (ECDSA) to the list of known hosts.
pentester@10.10.9.16's password:
scan_172_17_network.gnmap
scan_172_17_network.nmap
root@ip-10-10-0-6:~#
```

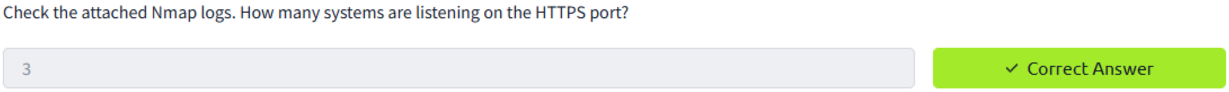
Q1



I tried running : “`cat scan_172_17_network.nmap`” but the output was so long that the terminal cuts it off, therefore I couldn’t count. I searched and found that I can use grep to specify the string Im looking for and used this command to have my answer:



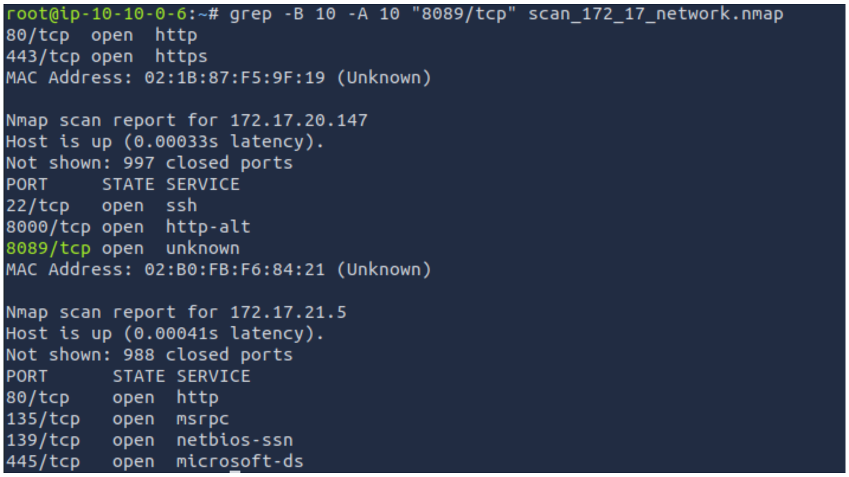
```
root@ip-10-10-0-6:~# grep "443/tcp" scan_172_17_network.nmap
443/tcp open   https
443/tcp open  https
443/tcp open   https
```



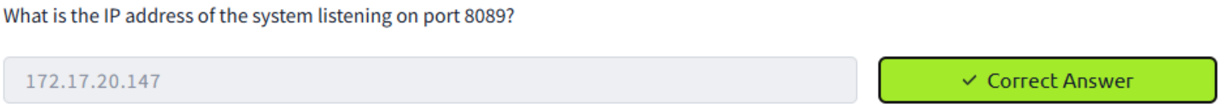
Check the attached Nmap logs. How many systems are listening on the HTTPS port?

3

Q2



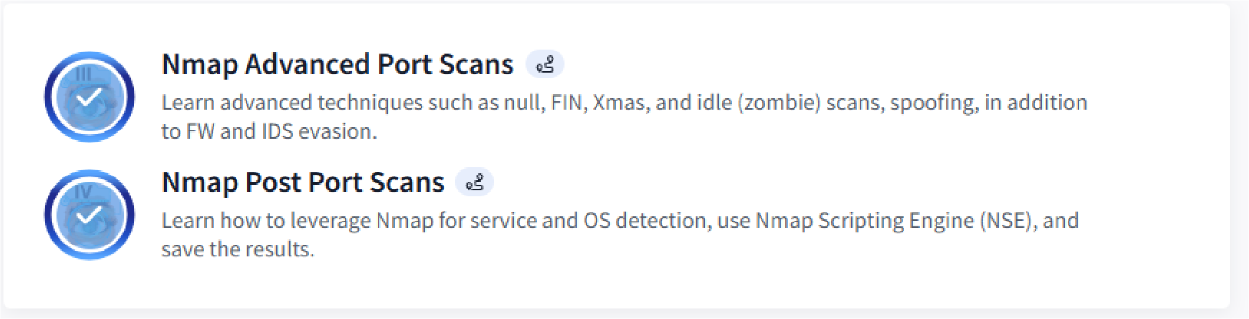
```
root@ip-10-10-0-6:~# grep -B 10 -A 10 "8089/tcp" scan_172_17_network.nmap
80/tcp  open  http
443/tcp open  https
MAC Address: 02:1B:87:F5:9F:19 (Unknown)

Nmap scan report for 172.17.20.147
Host is up (0.00033s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
8000/tcp open  http-alt
8089/tcp open  unknown
MAC Address: 02:B0:FB:F6:84:21 (Unknown)

Nmap scan report for 172.17.21.5
Host is up (0.00041s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
```



What is the IP address of the system listening on port 8089?

172.17.20.147

Rooms Completed!!



Nmap Advanced Port Scans

Learn advanced techniques such as null, FIN, Xmas, and idle (zombie) scans, spoofing, in addition to FW and IDS evasion.

Nmap Post Port Scans

Learn how to leverage Nmap for service and OS detection, use Nmap Scripting Engine (NSE), and save the results.