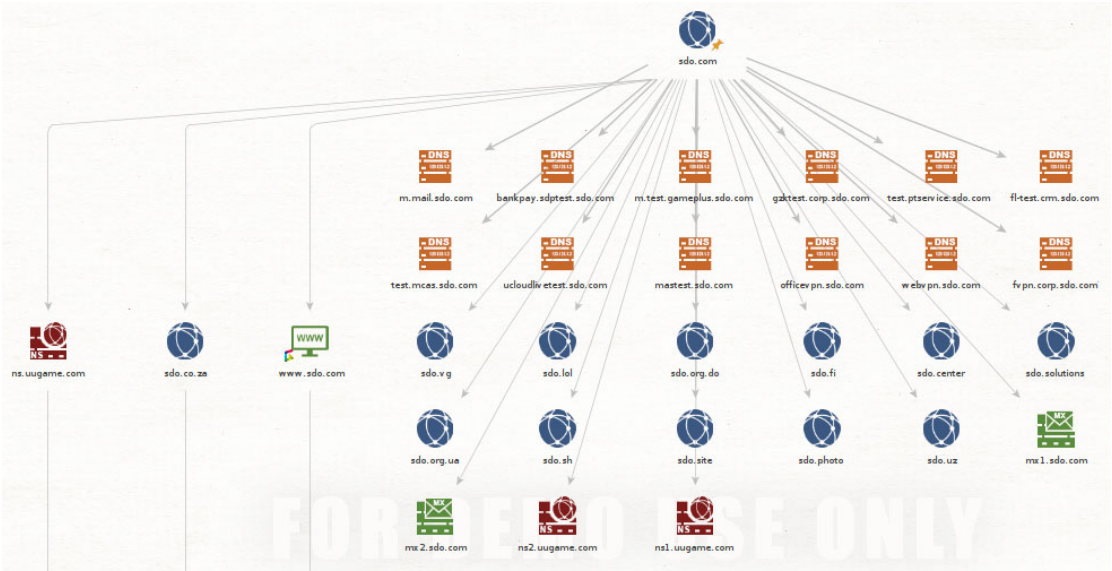
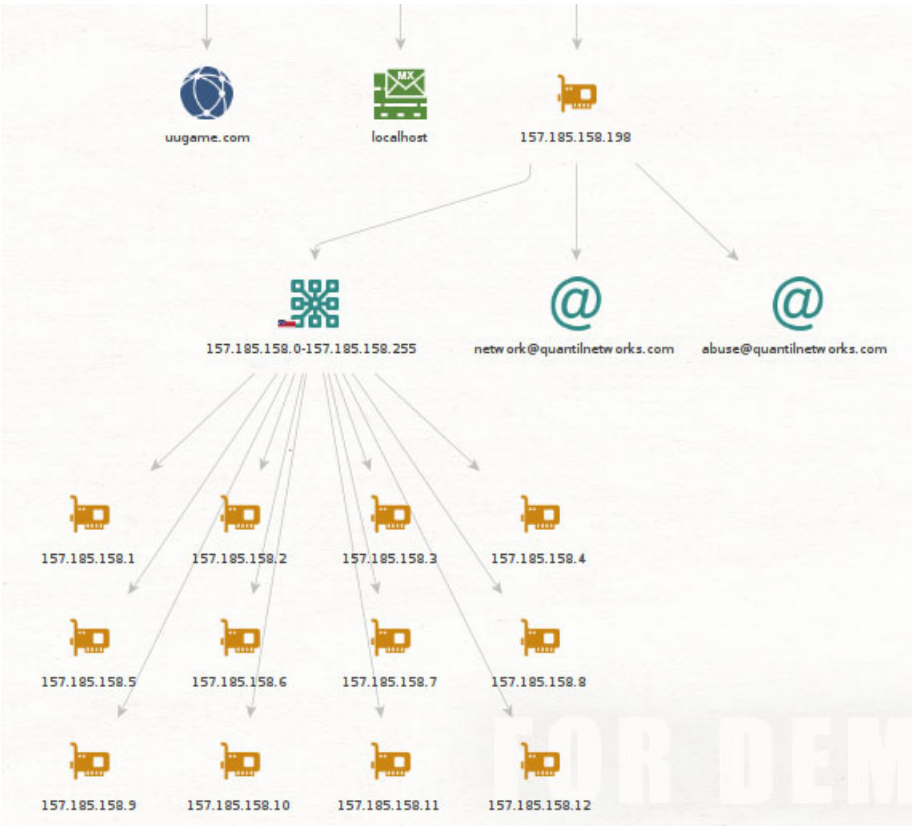
Task 1: Select a technology company that you have never heard of. Perform a thorough passive information gathering on the selected company and present your results in a brief report. Include your methodology and rationale in information gathering. Report the results of using at least two open source intelligence tools such as Maltego and theHarvester in your information gathering process.

The company that I selected is Shengqu Games. I just searched "Chinese game company" in google and randomly picked one from the search results, of which the main webpage is "www.sdo.com".
At first, I used the command "theHarvester -d www.sdo.com -b all". Then I got its ASNS information (AS45090, AS4809, AS4812, AS54994), email (info@sdo.com), and thirty IP addresses.
After that, I used the tool Maltego. I added the domain "www.sdo.com" firstly and performed a quick lookup to get the website. And then, I clicked "To Domain (find other TLDs)" on the domain and got twelve domains (sdo.vg, sdo.center, sdo.one, sdo.lol, sdo.ninja, sdo.org.do, sdo.solutions, sdo.org.ua, sdo.tw, sdo.fi, sdo.sh, sdo.bj.cn) that are related to the subdomains or associated with the hosting company. Then I clicked "To IP Address (DNS)" and got the IP address (157.185.158.198) of the website, from which people can interact with the target actively. And then I just clicked "To Email address (from whois info)" and got two Email addresses (abuse@quantilnetworks.com and network@quantilnetworks.com), which gave the information in regards to the hosting company behind the IP address or the server. Then I went back to the initial domain "www.sdo.com", and got the name server (ns.uugame.com, ns1.uugame.com and ns2.uugame.com) and the mail server (mx1.sdo.com and mx2.sdo.com) from the DNS record. Then I went to the IP address and clicked "To netblock (using routing info)" and got the net block (157.185.158.0-157.185.158.255) and clicked "To IP address (Found in Netblock)" and got all the IP addressed (157.185.158.1-12) of devices.
Through the tools Maltego and theHarvester, I really gathered so much information of the company Shengqu Games. And the screenshots of results are as follows:

Maltego:





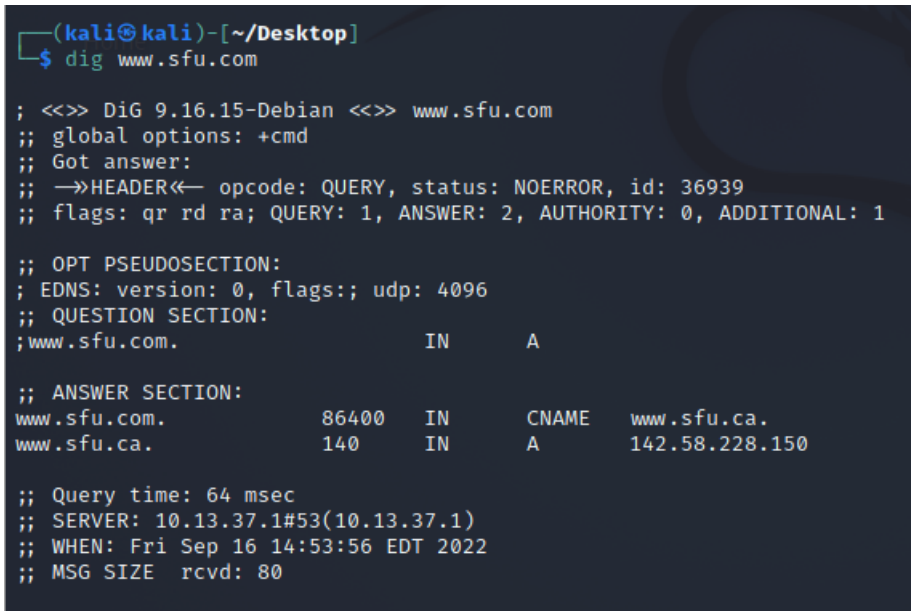
theHarvester:

```
[*] IPs found: 30
-------------------
61.172.242.20
61.172.242.23
61.172.242.29
61.172.249.231
61.172.249.232
61.172.249.233
61.172.249.234
61.172.249.235
101.227.2.32
106.39.255.185
114.80.132.136
114.80.132.185
116.211.3.39
124.223.124.47
150.138.167.194
157.185.145.91
163.171.128.148
163.171.132.119
183.134.11.86
203.130.59.29
220.243.235.203
220.243.237.152
222.73.2.76
222.73.13.118
222.246.232.153

[*] Emails found: 1
-------------------
info@sdo.com
```

```
[*] ASNS found: 4
-----------------
AS45090
AS4809
AS4812
AS54994

[*] Interesting Urls found: 2
-----------------------------
http://www.sdo.com/
https://www.sdo.com/

[*] No Twitter users found.


[*] No LinkedIn users found.


[*] LinkedIn Links found: 0
---------------------------

[*] No Trello URLs found.
```

Task 2: Using dig find the IP address of www.sfu.com (Links to an external site.). What is the IP address?

The IP address is 142.58.228.150



Task 3: The returned answer from the previous task includes a CNAME part.

What does this mean?

This means that the domain name “www.sfu.com” points to the domain name “www.sfu.ca”.

Task 4: Run a query to ask a root server about **mail.sfu.ca** without using recursion (Hint use the @ for directing the query to a specific root server).

What command did you use? What is the result of the query?

I used the command “dig -t NS” first to get the root server.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig -t NS

; <<>> DiG 9.16.15-Debian <<>> -t NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62478
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       86400   IN      NS      a.root-servers.net.
.                       86400   IN      NS      b.root-servers.net.
.                       86400   IN      NS      c.root-servers.net.
.                       86400   IN      NS      d.root-servers.net.
.                       86400   IN      NS      e.root-servers.net.
.                       86400   IN      NS      f.root-servers.net.
.                       86400   IN      NS      g.root-servers.net.
.                       86400   IN      NS      h.root-servers.net.
.                       86400   IN      NS      i.root-servers.net.
.                       86400   IN      NS      j.root-servers.net.
.                       86400   IN      NS      k.root-servers.net.
.                       86400   IN      NS      l.root-servers.net.
.                       86400   IN      NS      m.root-servers.net.

;; Query time: 15 msec
;; SERVER: 10.13.37.1#53(10.13.37.1)
;; WHEN: Fri Sep 16 19:59:30 EDT 2022
;; MSG SIZE  rcvd: 239
```

And I used the command “dig @c.root-servers.net mail.sfu.ca”.
The result is:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig @c.root-servers.net mail.sfu.ca

; <<>> DiG 9.16.15-Debian <<>> @c.root-servers.net mail.sfu.ca
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58462
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: f38d685a651bb6130100000063250efc1b3cd8089432994a (good)
;; QUESTION SECTION:
;mail.sfu.ca.                   IN      A

;; AUTHORITY SECTION:
ca.                     172800  IN      NS      x.ca-servers.ca.
ca.                     172800  IN      NS      j.ca-servers.ca.
ca.                     172800  IN      NS      c.ca-servers.ca.
ca.                     172800  IN      NS      any.ca-servers.ca.

;; ADDITIONAL SECTION:
any.ca-servers.ca.      172800  IN      A       199.4.144.2
x.ca-servers.ca.        172800  IN      A       199.253.250.68
j.ca-servers.ca.        172800  IN      A       198.182.167.1
c.ca-servers.ca.        172800  IN      A       185.159.196.2
any.ca-servers.ca.      172800  IN      AAAA    2001:500:a7::2
x.ca-servers.ca.        172800  IN      AAAA    2620:10a:80ba::68
j.ca-servers.ca.        172800  IN      AAAA    2001:500:83::1
c.ca-servers.ca.        172800  IN      AAAA    2620:10a:8053::2

;; Query time: 51 msec
;; SERVER: 192.33.4.12#53(192.33.4.12)
;; WHEN: Fri Sep 16 20:04:10 EDT 2022
;; MSG SIZE  rcvd: 325
```

Task 5: The answer to the previous task will not give you the IP address of **mail.sfu.ca**. Instead, follow the “path” down in the hierarchy of the nameservers to find the address of **mail.sfu.ca** without using recursion. What commands did you use? What is the IP you found?

I used the command “dig @x.ca-servers.ca mail.sfu.ca”.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig @x.ca-servers.ca mail.sfu.ca

; <<>> DiG 9.16.15-Debian <<>> @x.ca-servers.ca mail.sfu.ca
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49356
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 4
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;mail.sfu.ca.                   IN      A

;; AUTHORITY SECTION:
sfu.ca.                 86400   IN      NS      ns2.sfu.ca.
sfu.ca.                 86400   IN      NS      ns3.sfu.ca.
sfu.ca.                 86400   IN      NS      whistler.sfu.ca.

;; ADDITIONAL SECTION:
ns2.sfu.ca.             86400   IN      A       142.58.103.2
ns3.sfu.ca.             86400   IN      A       142.58.190.2
whistler.sfu.ca.        86400   IN      A       142.58.103.1

;; Query time: 191 msec
;; SERVER: 199.253.250.68#53(199.253.250.68)
;; WHEN: Fri Sep 16 20:05:36 EDT 2022
;; MSG SIZE  rcvd: 147
```

Then I used the command “dig @ns2.sfu.ca mail.sfu.ca”.
And the IP I found is 142.58.225.1.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig @ns2.sfu.ca mail.sfu.ca

; <<>> DiG 9.16.15-Debian <<>> @ns2.sfu.ca mail.sfu.ca
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42675
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 17dfc9f87e5859fd4fad2e7563250fb1fbfc21fb19513842 (good)
;; QUESTION SECTION:
;mail.sfu.ca.                   IN      A

;; ANSWER SECTION:
mail.sfu.ca.            300     IN      A       142.58.225.1

;; AUTHORITY SECTION:
sfu.ca.                 300     IN      NS      ns3.sfu.ca.
sfu.ca.                 300     IN      NS      ns2.sfu.ca.
sfu.ca.                 300     IN      NS      ns1.sfu.ca.

;; ADDITIONAL SECTION:
ns2.sfu.ca.             300     IN      A       142.58.103.2
ns1.sfu.ca.             300     IN      A       142.58.103.1
ns3.sfu.ca.             300     IN      A       142.58.103.140

;; Query time: 3 msec
;; SERVER: 142.58.103.2#53(142.58.103.2)
;; WHEN: Fri Sep 16 20:07:11 EDT 2022
;; MSG SIZE  rcvd: 186
```

Task 6: What is the IP address of the local network in the form of IP/netmask? What command did you use to find this?

The IP address of the local network is 10.13.37.0/24.
I used the command "ifconfig".

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.13.37.100  netmask 255.255.255.0  broadcast 10.13.37.255
        inet6 fe80::a00:27ff:fef1:baf9  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:f1:ba:f9  txqueuelen 1000  (Ethernet)
        RX packets 150  bytes 22617 (22.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 46  bytes 3934 (3.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1068 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1068 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Task 7: Perform a **full ping** scan in the local network using Nmap and identify all potential targets. Report the results of the scan and point to the IPs of the potential target machines. What commands did you use to scan the network?

I used the command "nmap -sP 10.13.37.0/24".
And the results are: 10.13.37.1, 10.13.37.100, 10.13.37.103, 10.13.37.104

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sP 10.13.37.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-16 20:55 EDT
Nmap scan report for pfSense.localdomain (10.13.37.1)
Host is up (0.0030s latency).
Nmap scan report for 10.13.37.100
Host is up (0.00017s latency).
Nmap scan report for 10.13.37.103
Host is up (0.0050s latency).
Nmap scan report for 10.13.37.104
Host is up (0.0046s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 3.28 seconds
```

Task 8: Perform a TCP SYN scan on a specific target using Nmap. Report the result. What command did you use to perform the scan? Perform a TCP full

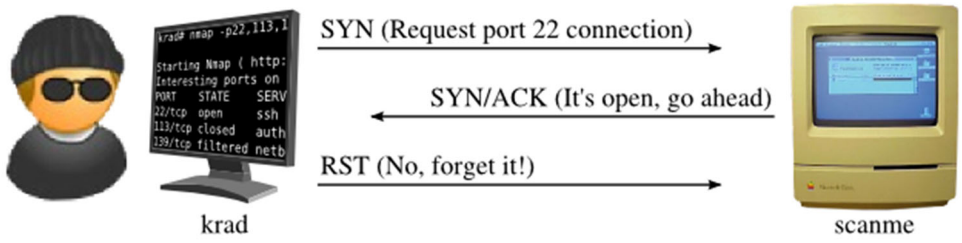
scan in a specific target **different** from the target you used for TCP SYN scan. Report the result. What command did you use to perform the scan? What is the difference between this method of scanning and the one that you used for the TCP SYN scan.

For TCP SYN scan, I used the command “sudo nmap -sS 10.13.37.104”.
And the result is:

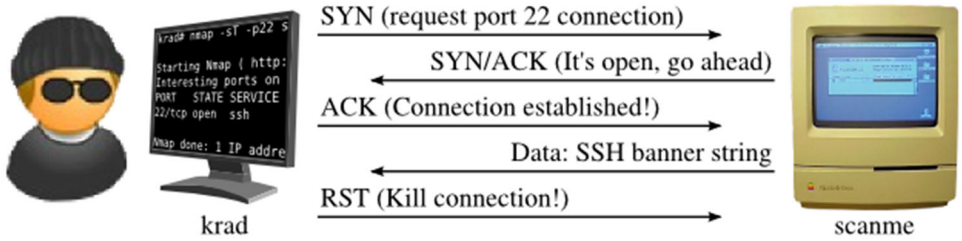
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sS 10.13.37.104
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-16 21:20 EDT
Nmap scan report for 10.13.37.104
Host is up (0.00062s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:76:DD:39 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.65 seconds
```

For TCP full scan, I used the command “nmap -sT 10.13.37.103”.
And the result is:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sT 10.13.37.103
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-16 21:24 EDT
Nmap scan report for 10.13.37.103
Host is up (0.0026s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 1.27 seconds
```



SYN scan of open port 22 *("TCP Connect Scan (-sT) | Nmap Network Scanning")*



Connect scan of open port 22 *("TCP SYN (Stealth) Scan (-sS) | Nmap Network Scanning")*

The difference between TCP full scan and TCP SYN scan is:
The TCP SYN scan only establish a half connection with the target machine, but the TCP full scan will establish a full TCP connection with the target machine.

Task 9: Perform two full port scanning on two different targets separately.

Report the results. Can you infer the operating system from these results? If

yes, indicate how. If not explain why.

All TCP and UDP ports of the first target (IP: 10.13.37.103)

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -n -PN -sS -sU -p- 10.13.37.103
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-20 14:00 EDT
Nmap scan report for 10.13.37.103
Host is up (0.00060s latency).
Not shown: 131060 closed ports
PORT     STATE         SERVICE
135/tcp  open          msrpc
139/tcp  open          netbios-ssn
445/tcp  open          microsoft-ds
123/udp  open|filtered ntp
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
445/udp  open|filtered microsoft-ds
500/udp  open|filtered isakmp
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
MAC Address: 08:00:27:56:ED:66 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 27.37 seconds
```

All TCP and UDP ports of the second target (IP: 10.13.37.104):

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -n -PN -sS -sU -p- 10.13.37.104
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-20 14:01 EDT
Stats: 0:20:05 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 1.11% done; ETC: 10:49 (20:27:51 remaining)
Stats: 0:20:19 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
```

The former command will cost too much time, so I just scan all TCP ports and 1000 UDP ports of the second target (IP: 10.13.37.104):

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -p- -sS 10.13.37.104
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-20 14:30 EDT
Nmap scan report for 10.13.37.104
Host is up (0.00023s latency).
Not shown: 65522 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49158/tcp open  unknown
MAC Address: 08:00:27:76:DD:39 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.56 seconds
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sU 10.13.37.104
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-20 14:31 EDT
Stats: 0:01:03 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 16.64% done; ETC: 14:37 (0:05:21 remaining)
Nmap scan report for 10.13.37.104
Host is up (0.00095s latency).
Not shown: 992 closed ports
PORT      STATE         SERVICE
137/udp   open|filtered netbios-ns
138/udp   open|filtered netbios-dgm
500/udp   open|filtered isakmp
1900/udp  open|filtered upnp
3702/udp  open|filtered ws-discovery
4500/udp  open|filtered nat-t-ike
5355/udp  open|filtered llmnr
49152/udp open|filtered unknown
MAC Address: 08:00:27:76:DD:39 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1124.70 seconds
```

I think I cannot infer the operating system from these results. The results only show the open state of the port of the target machine, but the different operating system may run the same service on the same port, so I think these results is not enough to infer the operation system.

Task 10: There are different ways to identify a target's operating system.

Using Nmap show **two** different ways to do that. Execute these for both of the target machines. In total there should be **four** results (two for the first target and two for the second). Report the results and associate the IPs with the operating systems.

The results of the first target:

nmap -A 10.13.37.104

```
└─$ sudo nmap -A 10.13.37.104
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-18 18:35 EDT
Nmap scan report for 10.13.37.104
Host is up (0.0014s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:76:DD:39 (Oracle VirtualBox virtual NIC)
Device type: general purpose|media device
Running: Microsoft Windows 2008|10|7|8.1, Microsoft embedded
OS CPE: cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_10 cpe:/h:microsoft:xbox_one cpe:/o:micro
OS details: Microsoft Windows Server 2008 SP2 or Windows 10 or Xbox One, Microsoft Windows 7 SP0 - SP1, Windows Serv
Network Distance: 1 hop
Service Info: Host: ADMIN-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h20m05s, deviation: 4h02m29s, median: 5s
|_nbstat: NetBIOS name: ADMIN-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:76:dd:39 (Oracle VirtualBox virtual
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: admin-PC
|   NetBIOS computer name: ADMIN-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-09-18T15:36:58-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-09-18T22:36:58
|_  start_date: 2022-09-18T22:34:52

TRACEROUTE
HOP RTT     ADDRESS
1   1.39 ms 10.13.37.104
```

nmap -O 10.13.37.104

```
┌──(kali㉿kali)-[/opt/nessus/sbin]
└─$ sudo nmap -O 10.13.37.104
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-18 18:40 EDT
Nmap scan report for 10.13.37.104
Host is up (0.00098s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49158/tcp open  unknown
MAC Address: 08:00:27:76:DD:39 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:
/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.
1 Update 1
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 2.63 seconds
```

The results of the second target:

nmap -A 10.13.37.103

```
┌──(kali㉿kali)-[/opt/nessus/sbin]
└─$ sudo nmap -A 10.13.37.103
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-18 18:40 EDT
Nmap scan report for 10.13.37.103
Host is up (0.0020s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows XP microsoft-ds
MAC Address: 08:00:27:56:ED:66 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 3h30m06s, deviation: 4h56m59s, median: 6s
|_nbstat: NetBIOS name: ADMIN-2BDBD2BA8, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:56:ed:66 (Oracle VirtualBox
virtual NIC)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: admin-2bdbd2ba8
|   NetBIOS computer name: ADMIN-2BDBD2BA8\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-09-18T15:41:04-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   1.96 ms 10.13.37.103

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 58.95 seconds
```

nmap -A 10.13.37.103

```
┌──(kali㉿kali)-[/opt/nessus/sbin]
└─$ sudo nmap -O 10.13.37.103
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-18 18:45 EDT
Nmap scan report for 10.13.37.103
Host is up (0.0018s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:56:ED:66 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
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 2.87 seconds
```

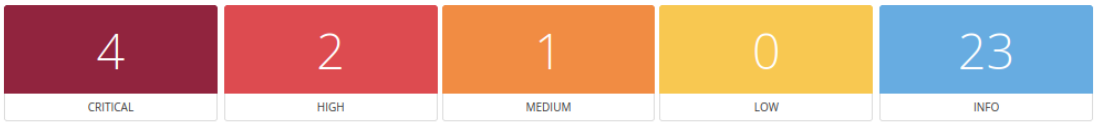
The operating system of the first target (IP:10.13.37.104) may be Win7, Win2008 or Win8.1.
The operating system of the second target (IP:10.13.37.103) may be Win XP SP2 or SP3.

Task 11: Perform an advanced scan on the Windows XP target machine.

Report the high/critical vulnerabilities of the system. Which of these could be

used directly to exploit and gain access to the target system and which to gain more info or perform a denial of service attack according to your opinion?

10.13.37.103



Severity	CVSS v3.0	Plugin	Name
CRITICAL	9.8	34477	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)
CRITICAL	10.0	73182	Microsoft Windows XP Unsupported Installation Detection
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
HIGH	8.1	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	7.3	26920	SMB NULL Session Authentication
MEDIUM	5.3	57608	SMB Signing not required
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

There are **four critical** vulnerabilities:

(1) MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)
(2) MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
(3) Microsoft Windows XP Unsupported Installation Detection
(4) Unsupported Windows OS (remote)

There are **two high** vulnerabilities:

(1) MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
(2) SMB NULL Session Authentication

MS08-067, MS09-001, MS17-010 could be used directly to exploit and gain access to the

target system.
SMB NULL Session Authentication could be used to gain more info.
MS09-001 could be used to perform a denial of service against the remote host.