Assignment #2 (21st Dec 2020)

2.1 Performing Passive Reconnaissance

The best way to learn passive information gathering is to use the tools. In this exercise, you will perform reconnaissance on several organizations. Acquire only the information requested.

Estimated Time: 20 minutes.

Domain Name	IP Address	Domain Expiration	Location	Registrar	Contact Person	Phone Number	Address
iisc.ac.in							
rutgers.edu							
drdo.gov.in							
bbc.com							

1. Review Table to determine the target of your passive information gathering. **2.** You can use a tool such as *Whois* or any of the other tools mentioned throughout the chapter. Some of these include:

- www.betterwhois.com
- www.allwhois.com
- http://geektools.com
- www.all-nettools.com
- www.dnsstuff.com
- www.samspade.org
- https://talosintelligence.com/

3. To verify the location of the organization, perform a *traceroute* or a ping with the –r option.

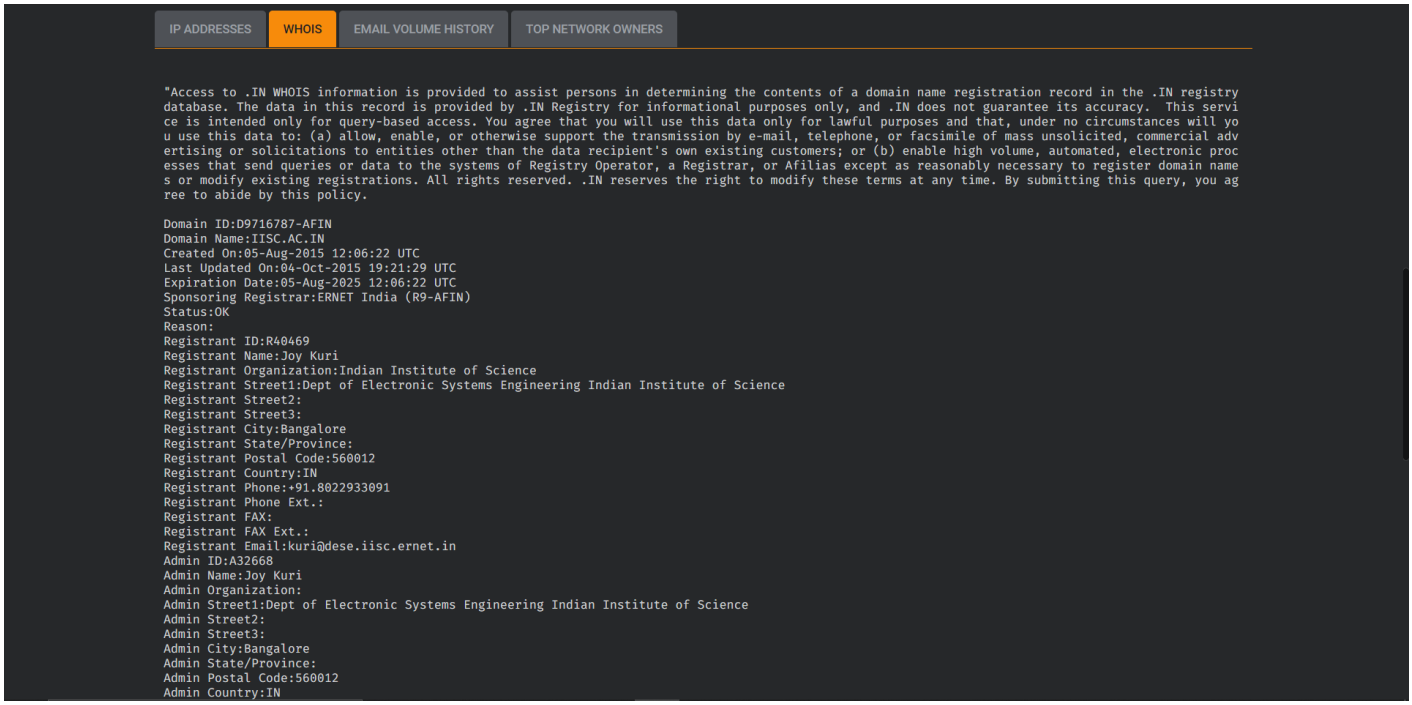
Answer:

Domain Name	IP Address	Domain Expiration	Location	Registrar	Contact Person	Phone Number	Address
iisc.ac.in	52.172.211.104	5/8/2025	INDIA	ERNET.India	Kuri@dese.iisc.emet.in	+91 8022933091	0 91 Indian Institute of Science, Dept of Electronic Systems Engineering, Postal Code:560 012 Country: India
rutgers.edu	128.6.46.111	31/7/2023	United States	Rutgers, The State University of New Jersey, Office of Information Technology	netmanager@rutgers.edu	+1 848445754	Rutgers, The State University of New Jersey, Office of Information Technology 96 Davidson Road Piscataway, NJ 08854-8096
drdo.gov.in	164.100.77.87	30/4/2021	India	National Informatics Centre	NA	NA	Defence Research & Development Organisation (DRDO), Delhi
bbc.com	107.178.239.195	14/7/2021	Great Britain UK	Tucows Domains INC	domainabuse@tucows.com	+1416530 123	British Broadcasting Corporation,

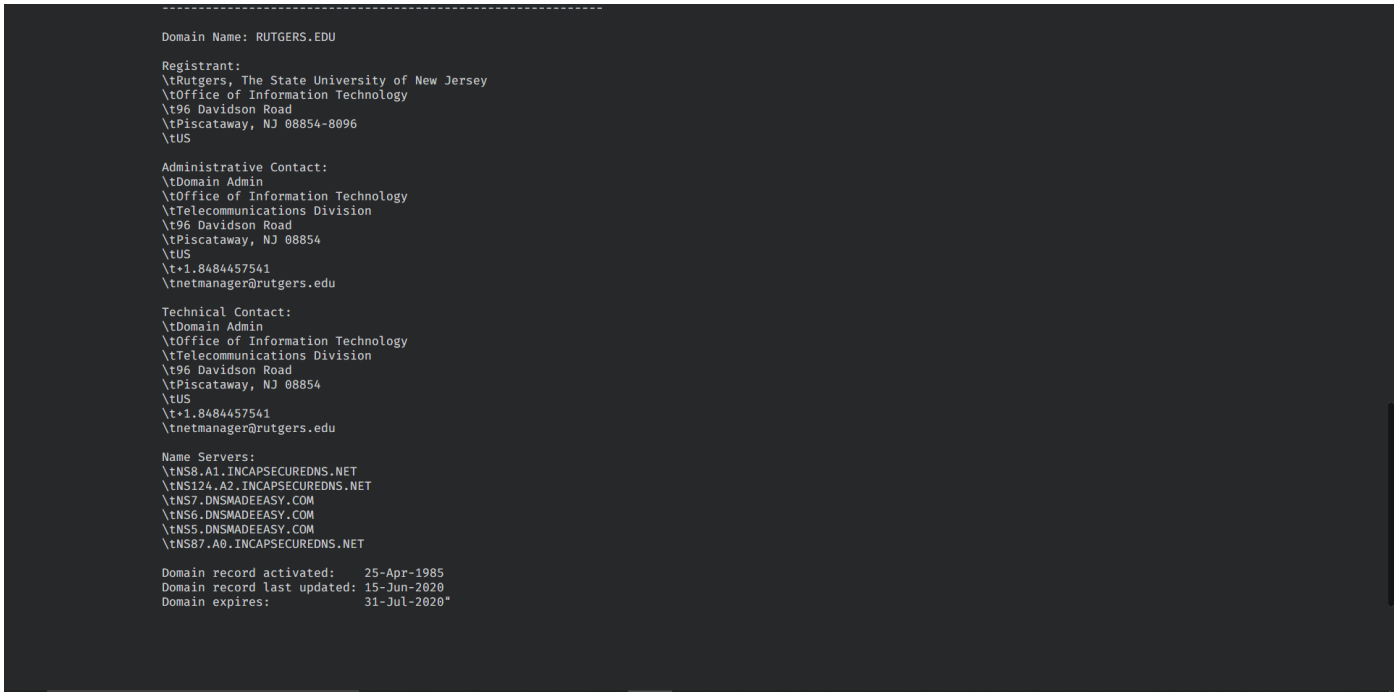
							London

Screenshots

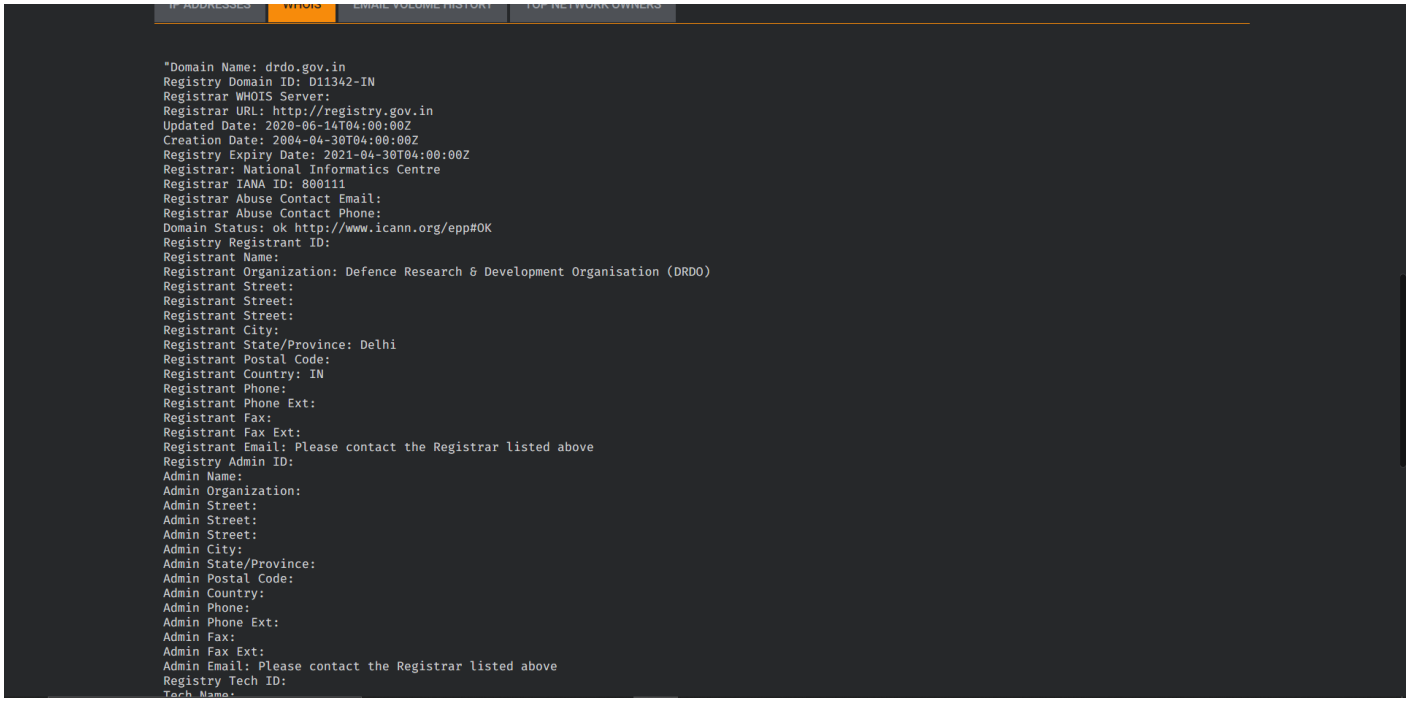
1) iisc.ac.in



2) rutgers.edu

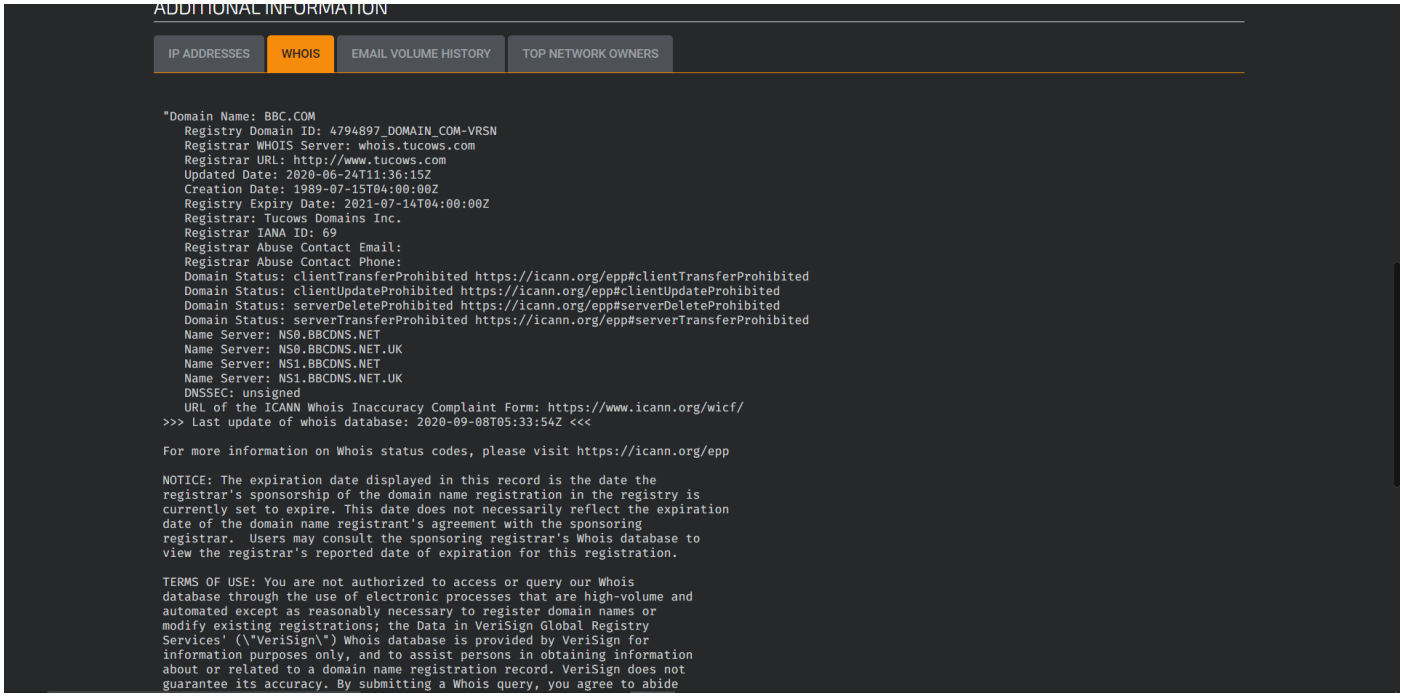


3) drdo.gov.in



```
"Domain Name: drdo.gov.in
Registry Domain ID: D11342-IN
Registrar WHOIS Server:
Registrar URL: http://registry.gov.in
Updated Date: 2020-06-14T04:00:00Z
Creation Date: 2004-04-30T04:00:00Z
Registry Expiry Date: 2021-04-30T04:00:00Z
Registrar: National Informatics Centre
Registrar IANA ID: 800111
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID:
Registrant Name:
Registrant Organization: Defence Research & Development Organisation (DRDO)
Registrant Street:
Registrant Street:
Registrant Street:
Registrant City:
Registrant State/Province: Delhi
Registrant Postal Code:
Registrant Country: IN
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Please contact the Registrar listed above
Registry Admin ID:
Admin Name:
Admin Organization:
Admin Street:
Admin Street:
Admin Street:
Admin City:
Admin State/Province:
Admin Postal Code:
Admin Country:
Admin Phone:
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: Please contact the Registrar listed above
Registry Tech ID:
Tech Name:
```

4) bbc.com



ADDITIONAL INFORMATION

IP ADDRESSES | WHOIS | EMAIL VOLUME HISTORY | TOP NETWORK OWNERS

```
"Domain Name: BBC.COM
   Registry Domain ID: 4794897_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.tucows.com
   Registrar URL: http://www.tucows.com
   Updated Date: 2020-06-24T11:36:15Z
   Creation Date: 1989-07-15T04:00:00Z
   Registry Expiry Date: 2021-07-14T04:00:00Z
   Registrar: Tucows Domains Inc.
   Registrar IANA ID: 69
   Registrar Abuse Contact Email:
   Registrar Abuse Contact Phone:
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Name Server: NS0.BBCDNS.NET
   Name Server: NS0.BBCDNS.NET.UK
   Name Server: NS1.BBCDNS.NET
   Name Server: NS1.BBCDNS.NET.UK
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-09-08T05:33:54Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' (\"VeriSign\") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
```

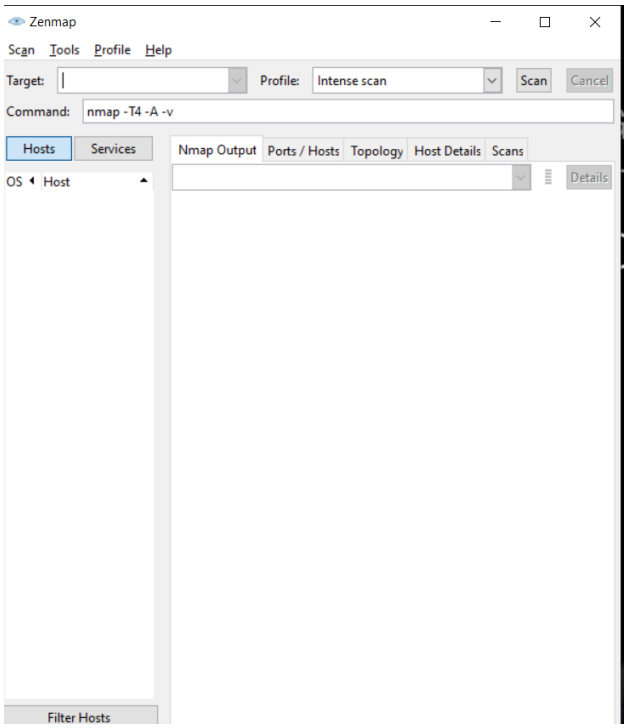
2.2 Performing Active Reconnaissance

The best way to learn active information gathering is to use the tools. In this exercise, you will perform reconnaissance on your own internal network. If you are not on a test network make sure you have permission before scanning or it may be seen as the precursor of an attack.

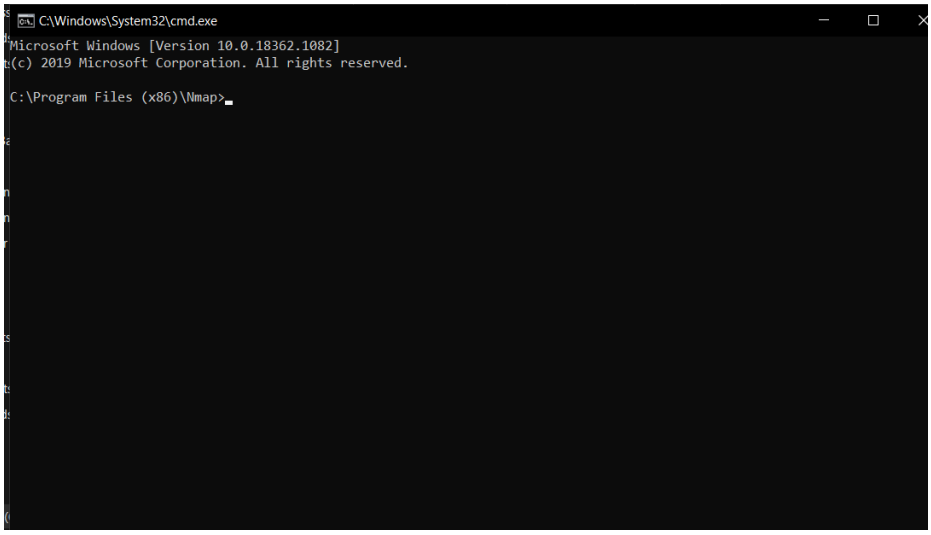
Estimated Time: 20 minutes

1. Download the most current version of Nmap from www.insecure.org/nmap/download.html.

- Downloaded Nmap Version 7.91



2. Open a command prompt and go to the directory that you have installed Nmap in.



3. Run *Nmap –h* from the command line to see the various options.

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18362.1082]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Nmap>Nmap -h
Nmap 7.91 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
```

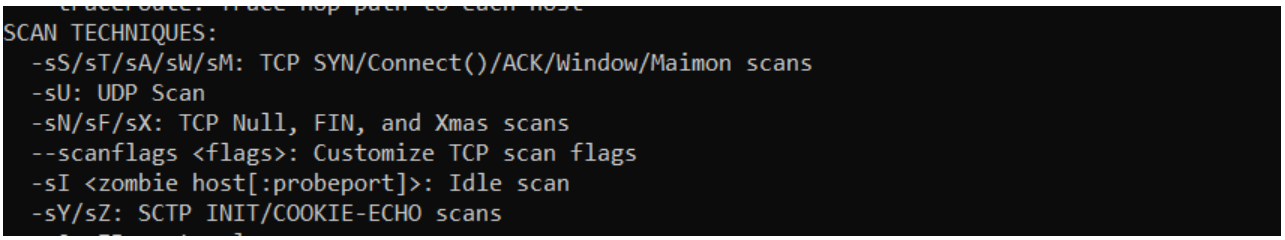
4. You'll notice that Nmap has many different options. Review and find the option for a full connect scan. Enter your result here: _____

Answer **–sT**

```
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
```

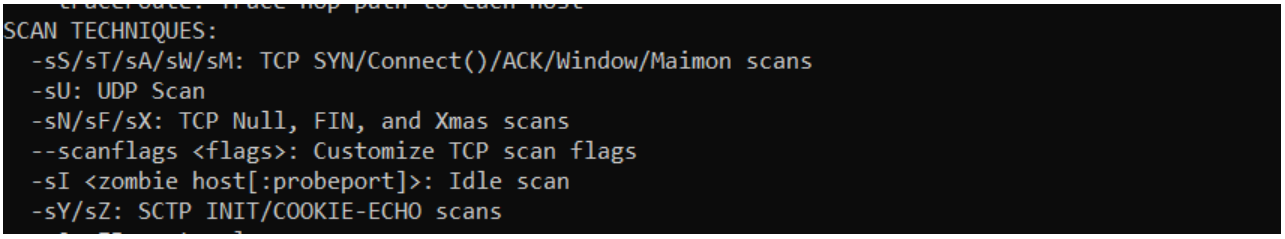
5. Review and find the option for a stealth scan. Enter your result here: ____

Answer **–sS**



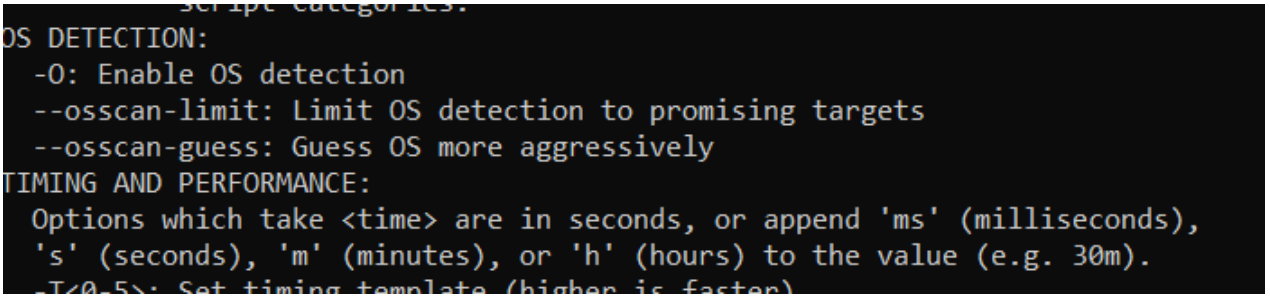
6. Review and find the option for a UDP scan. Enter your result here: ____

Answer: **-sU**



7. Review and find the option for a fingerprint scan. Enter your result here: ____

Answer: **-O**



8. Perform a full connect scan on one of the local devices you have identified on your network. The syntax is *Nmap -sT IP_Address.*

9. Perform a stealth scan on one of the local devices you have identified on your network. The syntax is *Nmap -sS IP_Address.*

10. Perform a UDP scan on one of the local devices you have identified on your network. The syntax is *Nmap -sU IP_Address.*

11. Perform a fingerprint scan on one of the local devices you have identified on your network. The syntax is *Nmap -O IP_Address.*

12. Observe the results of each scan. Was Nmap capable of successfully identifying the system? Were the ports it identified correct?

Yes, Nmap was able to successfully identify the system, and also all the ports were identified correctly, none of them were unknown or unidentified.
