NMAP - 06_10_2024

```
1. Which port scan method is also known as a half-open scan that never establishes a true connection with the target host over the network?
```

- A. TCP scan
- B. UDP scan
- C. SYN ACK
- D. SYN scan

> Ans : SYN scan

---

2. Which Nmap flag was likely used to determine the state of each port?

- A. -sV
- B. –T5
- C. –reason
- D. -sT

> Ans : -reason

```
  -sV: Probe open ports to determine service/version info
┌[user@parrot]-[~]
└─ $nmap --help | grep reason
  --reason: Display the reason a port is in a particular state
┌[user@parrot]-[~]
└─ $namp --reason skilldisk.com
bash: namp: command not found
┌[✗]-[user@parrot]-[~]
└─ $nmap --reason skilldisk.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-12 13:53 UTC
Nmap scan report for skilldisk.com (139.59.24.250)
Host is up, received syn-ack (0.014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE REASON
22/tcp  open  ssh     syn-ack
80/tcp  open  http    syn-ack
443/tcp open  https   syn-ack

Nmap done: 1 IP address (1 host up) scanned in 11.70 seconds
```

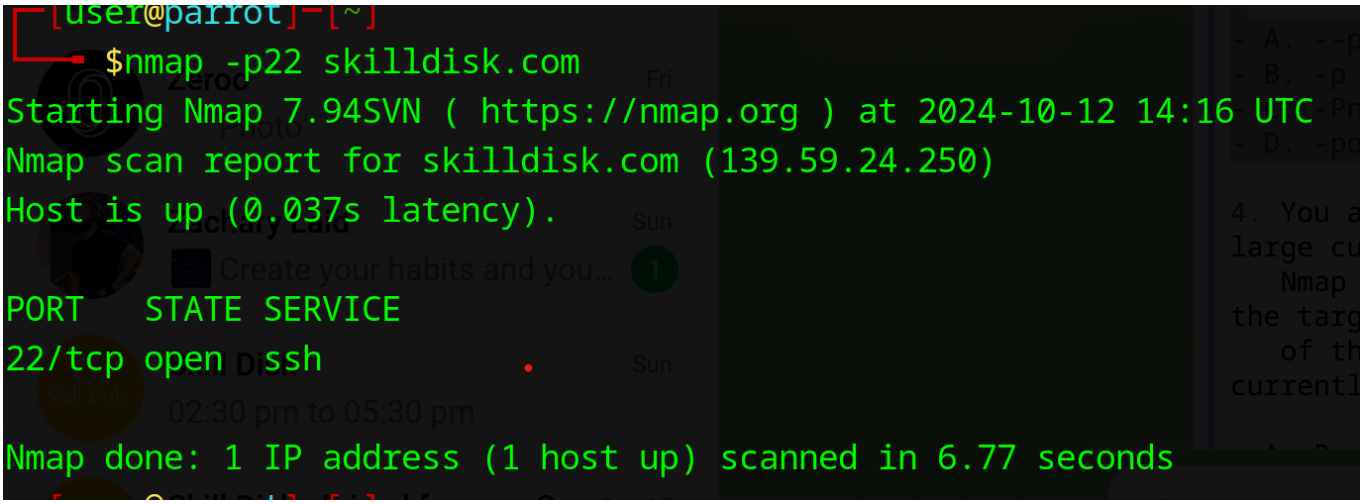
---

3. When conducting a port scan against a target, which Nmap flag is used to specify a port range?

- A. --p
- B. -p
- C. -Pn
- D. -ports

> Ans : -p

```
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
```



---

4. You are performing a penetration test for a large customer. You are using Nmap to determine the ports that are open on the target systems. What phase of the penetration testing process are you currently on?

- A. Reporting and communication
- B. Attacks and exploits
- C. Planning and scoping
- D. Information gathering and vulnerability identification

> Ans : information gathering and vulnerability Indentification

---

5. ou are in the discovery phase of a penetration test and would like to do a port scan on the network, but not perform a ping operation with the port scan. What Nmap switch would you use to disable pings with the port scan?

- A. -Pn
- B. -p
- C. -sP
- D. -sT

> Ans : -Pn

```
┌──[user@parrot]─[~]
└──╼ $nmap --help | grep Pn
  -Pn: Treat all hosts as online -- skip host discovery
  nmap -v -iR 10000 -Pn -p 80
┌──[user@parrot]─[~]
└──╼ $
```

```
┌──[user@parrot]─[~]
└──╼ $nmap -Pn skilldisk.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-13 03:03 UTC
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 99.45% done; ETC: 03:03 (0:00:00 remaining)
Nmap scan report for skilldisk.com (139.59.24.250)
Host is up (0.0077s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 11.41 seconds
```

---

6. Bob is using nmap to discover ports that are open on the systems. What form of information gathering is Bob performing?

- A. Vulnerability identification
- B. Active information gathering
- C. Vulnerability scanning
- D. Passive information gathering

> Ans : Active information gathering

---

7. You are starting your host discovery stage of the information gathering process and would like to identify the systems that are running on the network 10.1.0.0/24. What command would you use?

- A. nmap -sT 10.1.0.0/24

- B. nmap -sV 10.1.0.0/24
- C. nmap -sS 10.1.0.0/24
- D. nmap -sP 10.1.0.0/24

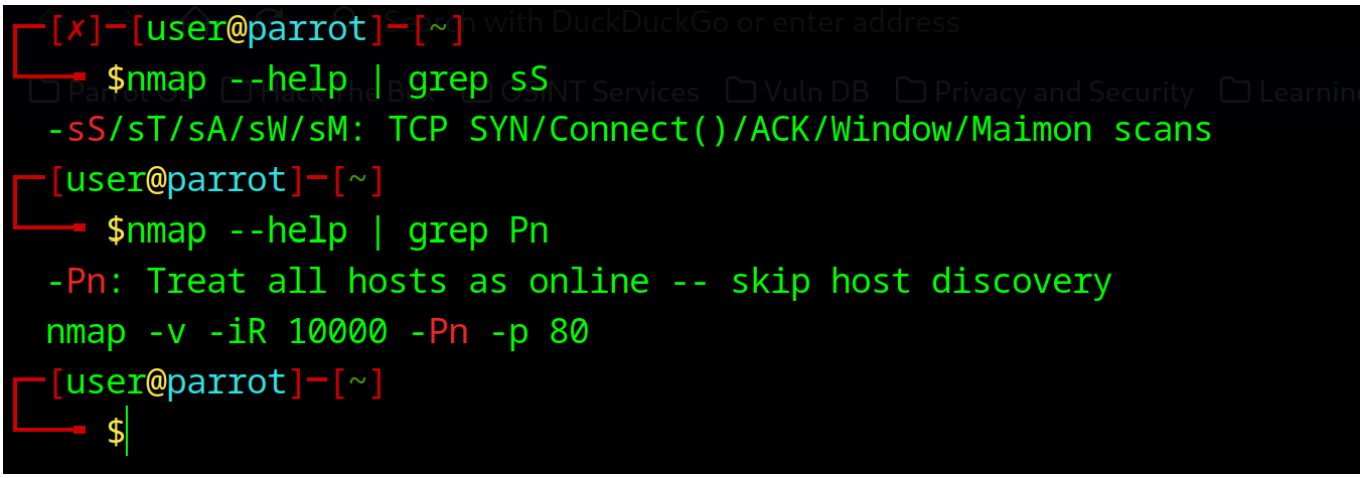
> Ans : nmap -sP 10.1.0.0/24

---

8. You are performing a SYN port scan on a customer's network that falls into the scope of the pentest. You would like to disable pings before enumerating the ports on each of the systems. What command would you use?

- A. nmap -sS 10.1.0.0/24 -p 80
- B. nmap -sS 10.1.0.0/24 -T0
- C. nmap -sS 10.1.0.0/24 -Pn
- D. nmap -sS 10.1.0.0/24 -oX

> Ans : nmap -sS 10.1.0.0/24 -Pn



---

9. You are performing a penetration test for one of your customers and you are familiar with an exploit against Remote Desktop Services. What command would you use to identify any systems that have Remote Desktop Services running? -
-A. nmap -sS 10.1.0.0/24 -p 1433

- B. nmap -sS 10.1.0.0/24 -p 3389
- C. nmap -sS 10.1.0.0/24 -Pn
- D. nmap -sS 10.1.0.0/24 -oX

> Ans : nmap -sS 10.1.0.0/24 -p 3389

```
┌──[user@parrot]─[/etc]
└──╼ $cat services | grep 3389
ms-wbt-server   3389/tcp
┌──[user@parrot]─[/etc]
```

wbt: This could refer to "Web-Based Terminal," which is sometimes used in the context of remote access

---

10. You are performing a black box pen test and would like to discover the public IP ranges used by an organization. What tool would you use?

- A. the Harvester
- B. nmap
- C. Whois
- D. hping3

> Ans : whois

```
┌──[user@parrot]─[~]
└──╼ $whois skilldisk.com
   Domain Name: SKILLDISK.COM
   Registry Domain ID: 2440937522_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2024-10-03T08:05:28Z
   Creation Date: 2019-10-07T01:17:48Z
   Registry Expiry Date: 2025-10-07T01:17:48Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
```

---

11. You are performing a penetration test to identify the network 192.168.1.0/24 those are running RDP services. Which command you will use ? -

- A. nmap -sS 192.168.1.0/24 -p 22
- B. nmap -sS 192.168.1.0/24 -Pn
- C. nmap -sS 192.168.1.0/24 -p 3389

- D. nmap -sS 192.168.1.0/24 -p 3306

> Ans : nmap -sS 192.168.1.0/23 -p 3389

---

12. List out the common 1000 ports scanned by nmap using the command

```
sudo nmap –sU 192.168.2.5
```