(Q1) What is the purpose of the -sn option in nmap?

This **-sn** tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the host discovery probes. This is often known as a "ping scan", but you can also request that traceroute and NSE host scripts be run. This is by default one step more intrusive than the list scan, and can often be used for the same purposes. It allows light reconnaissance of a target network without attracting much attention. Knowing how many hosts are up is more valuable to attackers than the list provided by list scan of every single IP and host name.

(Q2) In the previous lab, you used nmap to find what services are running on what ports in the Metasploitable2 VM. Which nmap option gives you the version of those services? why is it important for vulnerability scanning?

Using the **-sV** option and specifying port 3306 with the option **-p3306** we can find the software using port 3306 and it's version.

It's important to check the version of software as outdated software likely has vulnerabilities that can be easily patched when updated to the newest version.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p3306 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-09 13:33 EST
Nmap scan report for 10.0.2.4
Host is up (0.0094s latency).

PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.0.51a-3ubuntu5

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
```

(Q3) Try scanning Metasploitable2 VM from your Kali machine using -A option with nmap. What additional information about the open ports on Metasploitable2 VM can you get by using this option? o Watch this video for more info

The option -A includes information like OS and version detection, script scanning, and traceroute. Notice the difference between the two screenshot when -A is provided.

```
┌──(kali㉿kali)-[~]
└─$ nmap  10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-16 12:58 EST
Nmap scan report for 10.0.2.4
Host is up (0.15s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-16 12:53 EST
Nmap scan report for 10.0.2.4
Host is up (0.28s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT   STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.15
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```

(Q4) What vulnerabilities did you find – both from Google and using the script?

From medium.com, FTP version 2.3.4 has known vulnerabilities that include “buffer overflows, format string vulnerabilities, and authentication bypass issues.”

Using vulners script, which checks for vulnerabilities by using CVSS scores. As you can see below the FTP received the highest score, confirming it’s known vulnerabilities that we googled earlier. Each URL provided is a known vulnerability on the vulners.com site.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script vulners -p21 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-16 13:33 EST
Nmap scan report for 10.0.2.4
Host is up (0.024s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
| vulners:
|   cpe:/a:vsftpd:vsftpd:2.3.4:
|       PRION:CVE-2011-2523     10.0    https://vulners.com/prion/PRION:CVE-2011-2523
|       EDB-ID:49757    10.0    https://vulners.com/exploitdb/EDB-ID:49757      *EXPLOIT*
|_      1337DAY-ID-36095        10.0    https://vulners.com/zdt/1337DAY-ID-36095        *EXPLOIT*
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.03 seconds
```

(Q5) Some of the information on a vulnerability scan report might be incorrect. What kind of potential errors should you be looking for on such a scan report?

Some errors to look out for include false positives and false negatives. These are crucial to be aware of as it gives users a false sense of the systems when the opposite may be occurring.

(Q6) Look at how found vulnerabilities were scored high, medium, and low using their CVSS score. Watch this video and list different parts of the CVSS Base Vector.

CVSS scores on a 10-point scale. A base CVSS score can be determined by combining the results of the eight different metrics, which include Attack Vector, referring to the type of access; Attack Complexity; the Privileges Required for the attacker; and the User Interaction an attacker needs. It also includes the Confidentiality impact, the Integrity impact, the Availability impact, and finally, the Scope, referring to whether other vulnerabilities can be impacted by the one vulnerability being focused on.

(Q7) List different solution types suggested in the report for found vulnerabilities.

Based on the extremely high CVSS rating of 9.8 received for the Backdoor Command Execution Vulnerability, network access should be restricted since the attack vector is network-based. The attack complexity is rated low, so security patches, software updates, and security configuration reviews should be completed immediately. Given that all the other metrics are at the highest possible risk, action should be taken for each category as comprehensively as possible. Overall, immediate action is imperative since the rating is extremely high, making it a top priority.

(Q8) Watch this video and list the factors to consider when prioritizing found vulnerabilities for remediation.

Vulnerabilities should be prioritized based on factors such as system criticality, information sensitivity, vulnerability severity, remediation difficulty, and vulnerability exposure.