Question 1

5 out of 5 points

Which switch would you use to run a SYN scan?

Selected Answer: ✓ -sS

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	sS	*Case Sensitive*
✓ *Exact Match*	-sS	*Case Sensitive*

Question 2

5 out of 5 points

Which switch would you use to perform a connect scan?

Selected Answer: ✓ -sT

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	-sT	*Case Sensitive*
✓ *Exact Match*	sT	*Case Sensitive*

Question 3

5 out of 5 points

Which switch would you use to perform an XMAS tree scan?

Selected Answer: ✓ -sX

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	sX	*Case Sensitive*
✓ *Exact Match*	-sX	*Case Sensitive*

Question 4

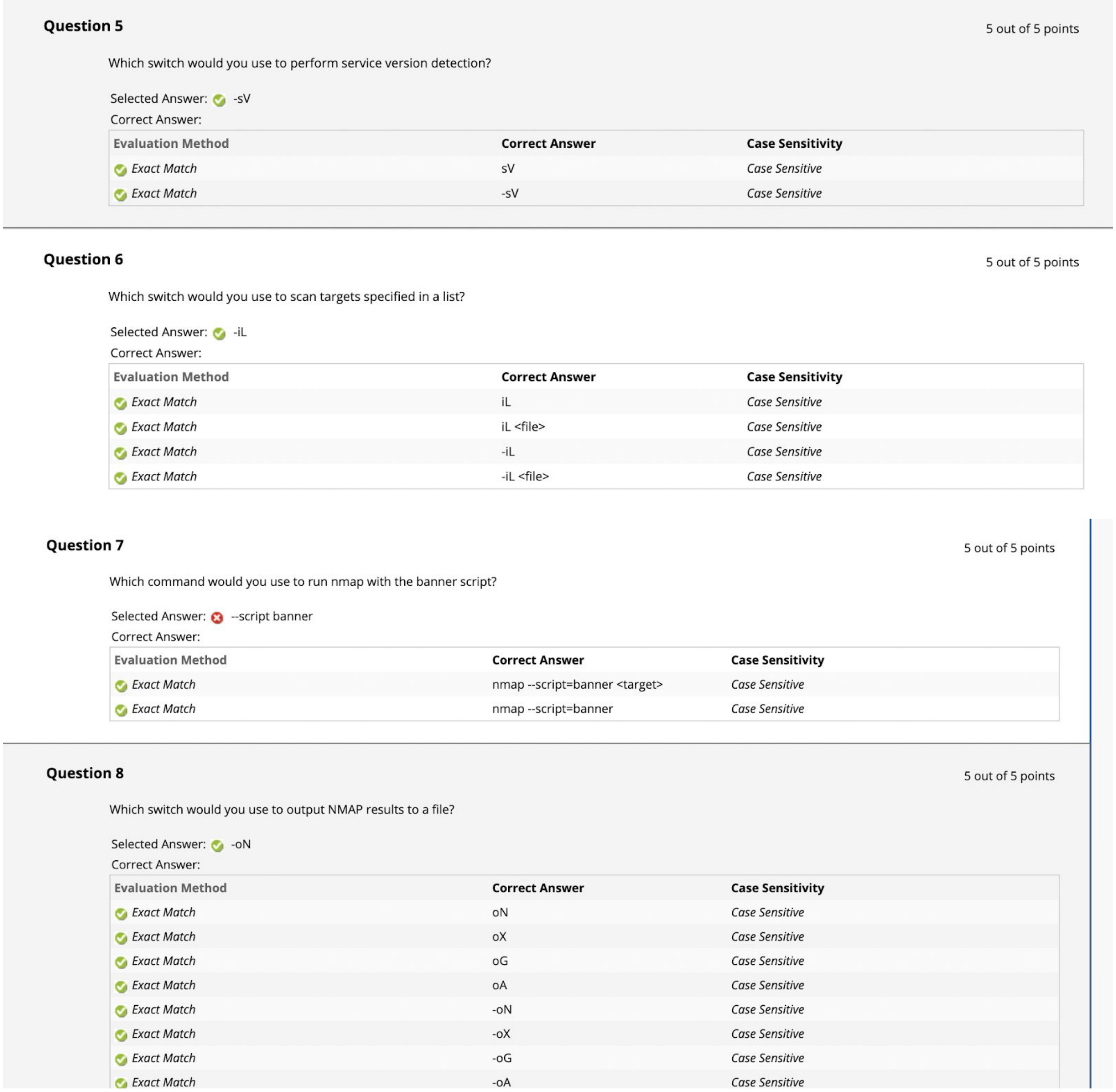
5 out of 5 points

Which switch would you use to perform operating system (OS) detection?

Selected Answer: ✓ -O

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	O	*Case Sensitive*
✓ *Exact Match*	-O	*Case Sensitive*



Question 5 5 out of 5 points

Which switch would you use to perform service version detection?

Selected Answer: ✓ -sV
Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	sV	*Case Sensitive*
✓ *Exact Match*	-sV	*Case Sensitive*

Question 6 5 out of 5 points

Which switch would you use to scan targets specified in a list?

Selected Answer: ✓ -iL
Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	iL	*Case Sensitive*
✓ *Exact Match*	iL <file>	*Case Sensitive*
✓ *Exact Match*	-iL	*Case Sensitive*
✓ *Exact Match*	-iL <file>	*Case Sensitive*

Question 7 5 out of 5 points

Which command would you use to run nmap with the banner script?

Selected Answer: ✗ --script banner
Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	nmap --script=banner <target>	*Case Sensitive*
✓ *Exact Match*	nmap --script=banner	*Case Sensitive*

Question 8 5 out of 5 points

Which switch would you use to output NMAP results to a file?

Selected Answer: ✓ -oN
Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	oN	*Case Sensitive*
✓ *Exact Match*	oX	*Case Sensitive*
✓ *Exact Match*	oG	*Case Sensitive*
✓ *Exact Match*	oA	*Case Sensitive*
✓ *Exact Match*	-oN	*Case Sensitive*
✓ *Exact Match*	-oX	*Case Sensitive*
✓ *Exact Match*	-oG	*Case Sensitive*
✓ *Exact Match*	-oA	*Case Sensitive*

Question 9

0 out of 5 points

What command would you use if you wanted to grep those results to find the open ports?

Selected Answer: ✗ -oG

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	cat <file> | grep open	*Case Sensitive*

Question 10

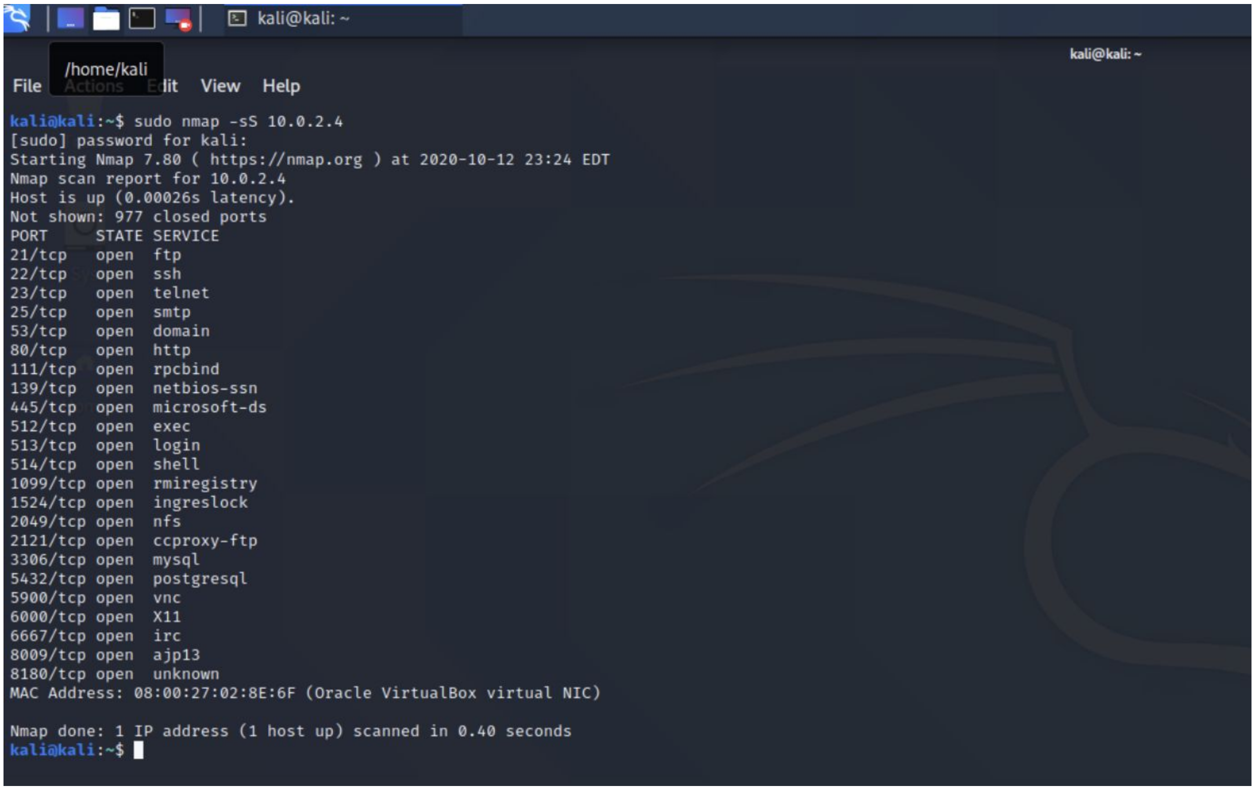
5 out of 5 points

Run 3 different NMAP scans. List the scan type, its intended purpose, and the command executed.

Selected Answer:

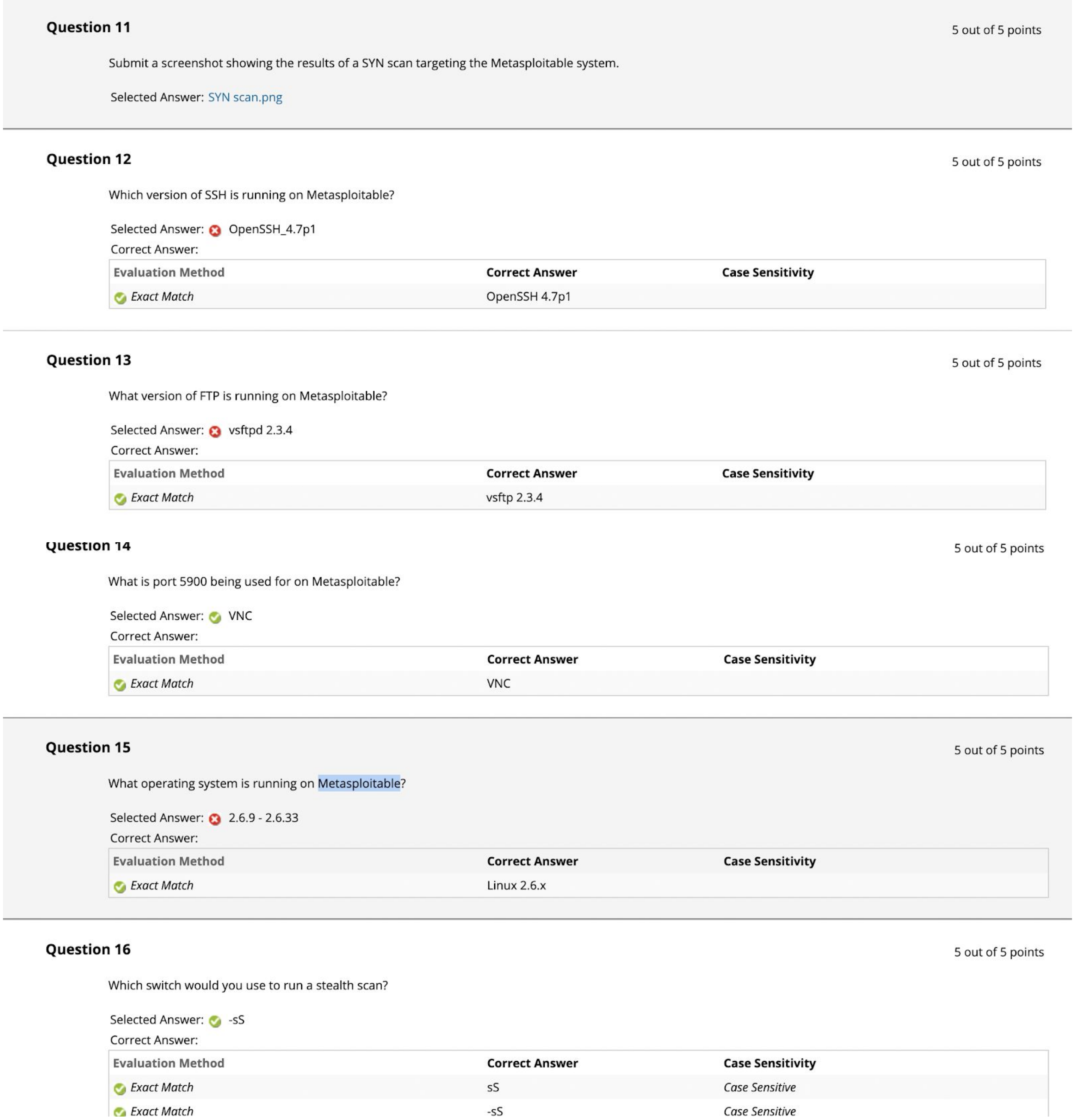
The first scan that I ran was a SYN scan (also called a stealth scan). The SYN scan sends fewer packets than other scans and sends them less frequently. The reason for doing this is to allow for the ability to perform a quick scan of lots of ports and this scan is not slowed by firewalls. This scan is called stealthy because it does not complete the TCP connections. The command that I used to execute the SYN scan was this: sudo nmap -sS 10.0.2.4
The second scan that I ran was a TCP connect scan. This scan is used to look for open port connections that can be used to communicate with. This is the only scan that can be done without full root privileges. The command that I used was: nmap -sT 10.0.2.4
The third scan that I ran was a UDP scan. The purpose of this scan is to locate UDP ports. TCP is the most common protocol used, but UDP ports are still used frequently enough that they deserve to have some scanning done. This scan is slower than a TCP scan, but it's important to do a UDP scan because these ports are still vulnerable to threat actors. The command that I used was: sudo nmap -sU 10.0.2.4

Correct Answer: [None]



```
kali@kali:~$ sudo nmap -sS 10.0.2.4
[sudo] password for kali:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-12 23:24 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00026s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:02:8E:6F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
kali@kali:~$
```



Question 11

5 out of 5 points

Submit a screenshot showing the results of a SYN scan targeting the Metasploitable system.

Selected Answer: SYN scan.png

Question 12

5 out of 5 points

Which version of SSH is running on Metasploitable?

Selected Answer: ✗ OpenSSH_4.7p1

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	OpenSSH 4.7p1	

Question 13

5 out of 5 points

What version of FTP is running on Metasploitable?

Selected Answer: ✗ vsftpd 2.3.4

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	vsftp 2.3.4	

Question 14

5 out of 5 points

What is port 5900 being used for on Metasploitable?

Selected Answer: ✓ VNC

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	VNC	

Question 15

5 out of 5 points

What operating system is running on Metasploitable?

Selected Answer: ✗ 2.6.9 - 2.6.33

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	Linux 2.6.x	

Question 16

5 out of 5 points

Which switch would you use to run a stealth scan?

Selected Answer: ✓ -sS

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	sS	*Case Sensitive*
✓ *Exact Match*	-sS	*Case Sensitive*

Question 17

0 out of 5 points

Why would you want to detect NMAP activity on your network?

Selected Answer: We want to use NMAP to detect activity on a network to ensure that only approved users have access to the network. Because NMAP can detect activity on a network it can also detect potential security vulnerabilities and threats. NMAP can also be used to troubleshoot a network.

Correct Answer: [None]

Question 18

5 out of 5 points

How can NMAP be used to troubleshoot?

Selected Answer: NMAP can be used to troubleshoot because it can deliver relevant results about a network. These results can help us learn more about a network so that troubleshooting actually addresses problems. Some of the ways that NMAP does this include the following: providing users with lists of the open ports, NMAP tells us the operating system and version of devices on a network, we can view routes to and from our server.

Correct Answer: [None]

Question 19

5 out of 5 points

Why is this tool useful from a network perspective?

Selected Answer: NMAP is useful from a networking perspective because it can provide information about a network, it can tell us about every active IP on a network, and it can also identify all of the devices on a network. Some of the specific things that NMAP provides include open ports, live hosts, and NMAP can even identify the operating systems of devices on the network.

Correct Answer: [None]

Question 20

5 out of 5 points

Why is this tool useful from a security perspective?

Selected Answer: NMAP is useful from a security perspective because companies and individual users can use it to ensure the security of their networks. NMAP allows the user to scan their network for vulnerabilities as if they were a hacker. Basically it can be used to test a network the way that a potential threat actor might attack the network and exploit vulnerabilities. Some of the specific functions include security scans, checking Firewall rules, asset discovery, and security security profiling.

Correct Answer: [None]

Tuesday, December 8, 2020 2:05:59 PM EST