Dear HAMDI SEVBEN,

You have passed the 'CPEH Practice Test'.

Exam Results

Result :	40.00 / 50.00
Percentage :	80.00 %
Passed :	Passed
Start Date :	2019-07-19 08:21:59
End Date :	2019-07-19 09:08:53
Spent Time :	46 min 54 sec
Passed Percentage :	70.00

Question 1 Cryptography refers to

Choice a ○ the study of cryptology

Choice b ○ the study of clustering

Choice c ● the science of studying and converting plain text to cipher text.

Choice d ○ hiding plain readable text.

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 51 sec.

#	Answer	Correct answer	Your answer
a.	the study of cryptology		
b.	the study of clustering		
c.	the science of studying and converting plain text to cipher text.		
d.	hiding plain readable text.		

Question 2 When establishing a Secure Shell (SSH), the client must provide the server with its public key to make the connection secure.

Choice a ● True

Choice b ○ False

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 56 sec.

#	Answer	Correct answer	Your answer
a.	True		
b.	False		

Question 3 The Metasploit Framework is an advanced commercial platform for developing, testing, and using exploit code.

Choice a ● True

Choice b ○ False

The answer is incorrect

Score is 0.00 out of 1.00. **Elapsed time** is 15 sec.

#	Answer	Correct answer	Your answer
a.	True		
b.	False		

Question 4 A Threat Agent/Source can best be described as what?

Choice a ○ The actual jurisdiction for which the hacker is located at the time of the attack.

Choice b ○ The legal jurisdiction for which the hacker was born.

Choice c ○ Both the legal and actual jurisdiction for which the hacker is located and was born.

Choice d ● An entity that can adversely act on assets.

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 34 sec.

#	Answer	Correct answer	Your answer
a.	The actual jurisdiction for which the hacker is located at the time of the attack.		
b.	The legal jurisdiction for which the hacker was born.		
c.	Both the legal and actual jurisdiction for which the hacker is located and was born.		
d.	An entity that can adversely act on assets.		

Question 5 What is a password salt?

Choice a ○ A password salt is a trick used by penetration testers to confuse network security personnel.

Choice b ○ A password salt is used by hackers and penetration testers to cover their tracks.

Choice c ● A password salt is random data unique to each user added to their password.

Choice d ○ A password salt is unique information added to a user’s password to make it easier to find on the network.

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 24 sec.

#	Answer	Correct answer	Your answer
a.	A password salt is a trick used by penetration testers to confuse network security personnel.		
b.	A password salt is used by hackers and penetration testers to cover their tracks.		
c.	A password salt is random data unique to each user added to their password.		
d.	A password salt is unique information added to a user’s password to make it easier to find on the network.		

Question 6 It is NOT possible to conduct a proper penetration test and not find an exploitable vulnerability.

Choice a ● True

Choice b ○ False

The answer is incorrect

Score is 0.00 out of 1.00. **Elapsed time** is 2 min 12 sec.

#	Answer	Correct answer	Your answer
a.	True		
b.	False		

Question 7 ________is a command-line utility that shows file version number, timestamp information, and digital signature details, including certificate chains.

Choice a ○ HijackThis

Choice b ○ Adaptive DarkNet

Choice c ● SigCheck

Choice d ○ Cain and Abel

The answer is incorrect

Score is 0.00 out of 1.00. **Elapsed time** is 30 sec.

#	Answer	Correct answer	Your answer
a.	HijackThis		
b.	Adaptive DarkNet		
c.	SigCheck		
d.	Cain and Abel		

Question 8 NMAP is a tool designed to scan very small networks. It doesn’t have the database capability to scan networks larger than 500 devices.

Choice a ○ True

Choice b ● False

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 1 min 4 sec.

#	Answer	Correct answer	Your answer
a.	True		
b.	False		

Question 9 If an employee uses a DNS that is poisoned, what has occurred?

Choice a ○ The employee’s packets will go to the wrong switch port on the destination end.

Choice b ● The employee will be sent to a website other than the one for which they intended to go.

Choice c ○ The employee will have to select a new DNS to access the Internet.

Choice d ○ The employee will not be able to access the Internet.

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 1 min 31 sec.

#	Answer	Correct answer	Your answer
a.	The employee’s packets will go to the wrong switch port on the destination end.		
b.	The employee will be sent to a website other than the one for which they intended to go.		
c.	The employee will have to select a new DNS to access the Internet.		
d.	The employee will not be able to access the Internet.		

Question 10 Next Generation Firewalls (NGF) provide the same features of congressional firewalls but can often provide new capabilities such as:

Choice a ● IDS, IPS, SSL, and SSH

Choice b ○ ARP/RARP table management, SSL, SSH, VPN termination, VLAN, and DHCP.

Choice c ○ ARP/RARP table management, VPN termination, VLAN, and DHCP.

Choice d ○ ARP/RARP table management, VLAN, and DHCP.

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 7 min 7 sec.

#	Answer	Correct answer	Your answer
a.	IDS, IPS, SSL, and SSH		
b.	ARP/RARP table management, SSL, SSH, VPN termination, VLAN, and DHCP.		
c.	ARP/RARP table management, VPN termination, VLAN, and DHCP.		
d.	ARP/RARP table management, VLAN, and DHCP.		

Question 11 A user creates a hash of a 235-page document using SHA-1. Later in the day, the same user creates a hash of a 9-page document, again using SHA-1. What will the size be of these two hashes?

Choice a ○ 128 bits/160 bits

Choice b ○ 160 bits/800 bits

Choice c ○ 128 bits/640 bits

Choice d ● 160 bits/160 bits

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 19 sec.

#	Answer	Correct answer	Your answer
a.	128 bits/160 bits		
b.	160 bits/800 bits		
c.	128 bits/640 bits		
d.	160 bits/160 bits		

Question 12 An Intrusion Prevention System (IPS) uses two main modes of detection. The two main modes are Signature-based and Anomaly-based.

Choice a ● True

Choice b ○ False

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 16 sec.

#	Answer	Correct answer	Your answer
a.	True		
b.	False		

Question 13 __________is a logical grouping of workstations, servers, and network devices on one LAN, despite their physical or geographical location.

Choice a ○ A Trivial File Transfer platform (TFTP)

Choice b ● A Virtual Local Area Network (VLAN)

Choice c ○ An Internet Group Management Protocol (IGMP)group

Choice d ○ An ARP/RARP table

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 30 sec.

#	Answer	Correct answer	Your answer
a.	A Trivial File Transfer platform (TFTP)		
b.	A Virtual Local Area Network (VLAN)		
c.	An Internet Group Management Protocol (IGMP)group		
d.	An ARP/RARP table		

Question 14 The software program Maltego is an extremely powerful tool that is used to gather information that will later be used to/for?

Choice a ○ Conduct cryptanalysis

Choice b ● Social engineering

Choice c ○ Brute force password attacks

Choice d ○ Man-in-the-Middle attacks

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 16 sec.

#	Answer	Correct answer	Your answer
a.	Conduct cryptanalysis		
b.	Social engineering		
c.	Brute force password attacks		
d.	Man-in-the-Middle attacks		

Question 15 TCP uses a three-way handshake.

Choice a ○ False

Choice b ● True

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 7 sec.

#	Answer	Correct answer	Your answer
a.	False		
b.	True		

Question 16 Penetration testers must know the law of the country for which the network is located before beginning any testing. Within the United States, which of the following is true?

Choice a ○ In Germany, the Penetration Tester could be prosecuted for creating a hacking tool.

Choice b ○ Civil law prevents all port scanning of US-based networks.

Choice c ○ A port scan is deemed an attempt to break in.

Choice d ● No federal law prohibits port scanning.

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 26 sec.

#	Answer	Correct answer	Your answer
a.	In Germany, the Penetration Tester could be prosecuted for creating a hacking tool.		
b.	Civil law prevents all port scanning of US-based networks.		
c.	A port scan is deemed an attempt to break in.		
d.	No federal law prohibits port scanning.		

Question 17 Security Information and Event Management (SIEM) combines security information and security event management (SIM, SEM). Why might the IT security department be using this product on the network?

Choice a ○ Provide real-time monitoring and analysis of alerts generated by network devices and applications.

Choice b ○ To store daily backups.

Choice c ○ To perform NAT/PAT functionality.

Choice d ● To manage all the log files in a single place where they cannot be altered by the system admins.

The answer is incorrect

Score is 0.00 out of 1.00. **Elapsed time** is 53 sec.

#	Answer	Correct answer	Your answer
a.	Provide real-time monitoring and analysis of alerts generated by network devices and applications.		
b.	To store daily backups.		
c.	To perform NAT/PAT functionality.		
d.	To manage all the log files in a single place where they cannot be altered by the system admins.		

Question 18 A unique characteristic of a virus is that it is self-executing and needs user action to initiate.

Choice a ● True

Choice b ○ False

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 17 sec.

#	Answer	Correct answer	Your answer
a.	True		
b.	False		

Question 19 Which of the following is most correct?

Choice a ○ All ports on the perimeter firewall should remain open, but within the network, unnecessary ports should be closed.

Choice b ● All ports within the network should be closed unless needed for operational requirements.

Choice c ○ All TCP ports should be closed throughout the network, and all protocols should operate off UDP ports only.

Choice d ○ All ports within the network should remain open to reduce helpdesk calls and to ensure maximum interoperability between applications.

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 54 sec.

#	Answer	Correct answer	Your answer
a.	All ports on the perimeter firewall should remain open, but within the network, unnecessary ports should be closed.		
b.	All ports within the network should be closed unless needed for operational requirements.		
c.	All TCP ports should be closed throughout the network, and all protocols should operate off UDP ports only.		
d.	All ports within the network should remain open to reduce helpdesk calls and to ensure maximum interoperability between applications.		

Question 20 Which of the following is LEAST true?

Choice a ○ A successful social engineering attack could be costly to an organization.

Choice b ○ Social engineering attacks rarely result in a significant financial loss.

Choice c ● A successful social engineering attack cannot result in a loss of privacy or loss of customer trust.

Choice d ○ Social engineering attacks rarely are successful because employees are smart, well-trained, and are difficult to trick.

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 1 min 17 sec.

#	Answer	Correct answer	Your answer
a.	A successful social engineering attack could be costly to an organization.		
b.	Social engineering attacks rarely result in a significant financial loss.		
c.	A successful social engineering attack cannot result in a loss of privacy or loss of customer trust.		
d.	Social engineering attacks rarely are successful because employees are smart, well-trained, and are difficult to trick.		

Question 21 You have just gained unauthorized access to a Linux server. Which directory would you most likely find the password file?

Choice a ○ /

Choice b ● /etc/passwd

Choice c ○ /passwd

Choice d ○ /usr/log/passwd

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 14 sec.

#	Answer	Correct answer	Your answer
a.	/		
b.	/etc/passwd		
c.	/passwd		
d.	/usr/log/passwd		

Question 22 Port scanning is considered

Choice a ● active reconnaissance

Choice b ○ a form of social engineering

Choice c ○ passive reconnaissance

Choice d ○ attacking a network

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 11 sec.

#	Answer	Correct answer	Your answer
a.	active reconnaissance		
b.	a form of social engineering		
c.	passive reconnaissance		
d.	attacking a network		

Question 23 This is the code which triggers the exploit. If it's related to string functions, then scripting languages are generally preferred.

Choice a ○ Injection vector

Choice b ○ Shellcode

Choice c ○ Handler routine

Choice d ● Request builder

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 10 min 46 sec.

#	Answer	Correct answer	Your answer
a.	Injection vector		
b.	Shellcode		
c.	Handler routine		
d.	Request builder		

Question 24 Managed switches can be used to provide which security feature?

Choice a ○ IP forwarding

Choice b ○ TCP/IP protocol blocking

Choice c ● Dynamic ARP inspection

Choice d ○ Drop packets not intended for this network.

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 9 sec.

#	Answer	Correct answer	Your answer
a.	IP forwarding		
b.	TCP/IP protocol blocking		
c.	Dynamic ARP inspection		
d.	Drop packets not intended for this network.		

Question 25 Which layer of the OSI model is responsible for packet sequencing?

Choice a ○ Layer 1 Physical

Choice b ○ Layer 7 Application

Choice c ○ Layer 2 Datalink

Choice d ● Layer 3 Network

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 21 sec.

#	Answer	Correct answer	Your answer
a.	Layer 1 Physical		
b.	Layer 7 Application		
c.	Layer 2 Datalink		
d.	Layer 3 Network		

Question 26 Windows and Linux both use one-way passwords.

Choice a ● True

Choice b ○ False

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 9 sec.

#	Answer	Correct answer	Your answer
a.	True		
b.	False		

Question 27 Which of the following is true?

Choice a ○ Nessus is a commercial tool designed for UNIX that will perform brute force attacks on firewalls as well as scanning.

Choice b ○ Nexus is a commercial Windows-based tool designed for vulnerability scanning of Windows and UNIX networks.

Choice c ○ Retina is a commercial vulnerability scanning tool for UNIX.

Choice d ● Qualys is a commercial cloud-based tool designed for scanning for vulnerabilities.

The answer is incorrect

Score is 0.00 out of 1.00. **Elapsed time** is 2 min 8 sec.

#	Answer	Correct answer	Your answer
a.	Nessus is a commercial tool designed for UNIX that will perform brute force attacks on firewalls as well as scanning.		
b.	Nexus is a commercial Windows-based tool designed for vulnerability scanning of Windows and UNIX networks.		
c.	Retina is a commercial vulnerability scanning tool for UNIX.		
d.	Qualys is a commercial cloud-based tool designed for scanning for vulnerabilities.		

Question 28 An SYN flood attack is accomplished when the sender sends ACK to the victim machine without sending an ACK.

Choice a ● True

Choice b ○ False

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 58 sec.

#	Answer	Correct answer	Your answer
a.	True		
b.	False		

Question 29 One of the many benefits of a vulnerability assessment is

Choice a ○ A detailed list of the access controls within the network.

Choice b ○ A detailed list of the users within the network.

Choice c ○ A detailed list of all the policies and procedures established for securing the network.

Choice d ● A detailed inventory of the vulnerabilities related to the assets in the network.

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 1 min 4 sec.

#	Answer	Correct answer	Your answer
a.	A detailed list of the access controls within the network.		
b.	A detailed list of the users within the network.		
c.	A detailed list of all the policies and procedures established for securing the network.		
d.	A detailed inventory of the vulnerabilities related to the assets in the network.		

Question 30 A vulnerability scan is NOT the same as a network penetration test.

Choice a ● True

Choice b ○ False

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 20 sec.

#	Answer	Correct answer	Your answer
a.	True		
b.	False		

Question 31 DNS databases contain information about fully qualified domain names (FQDN) and

Choice a ● IP addresses

Choice b ○ Location of servers

Choice c ○ Physical location of an organization's headquarters

Choice d ○ The date the IP addresses were assigned

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 22 sec.

#	Answer	Correct answer	Your answer
a.	IP addresses		
b.	Location of servers		
c.	Physical location of an organization's headquarters		
d.	The date the IP addresses were assigned		

Question 32 What are the four parts of the Information Systems Security Assessment Framework (ISSAF)?

Choice a ● Planning, Assurance, Controls, and Accreditation

Choice b ○ Planning, Assessment, Treatment, and Accreditation

Choice c ○ The process, Assurance, Testing, and Controls

Choice d ○ Planning, Assessment, Testing, and Accreditation

The answer is incorrect

Score is 0.00 out of 1.00. **Elapsed time** is 46 sec.

#	Answer	Correct answer	Your answer
a.	Planning, Assurance, Controls, and Accreditation		
b.	Planning, Assessment, Treatment, and Accreditation		
c.	The process, Assurance, Testing, and Controls		
d.	Planning, Assessment, Testing, and Accreditation		

Question 33 Why might a penetration tester use the Google Hacking Database (GHDB)?

Choice a ● It focuses on finding security weaknesses, and in some cases, provides the exploit for testing to see if that weakness exists within the target network.

Choice b ○ It contains a copy of all the malware found on the Internet.

Choice c ○ It contains all the IP addresses assigned to a particular company.

Choice d ○ It contains a copy of all the misconfigured web pages on the Internet.

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 31 sec.

#	Answer	Correct answer	Your answer
a.	It focuses on finding security weaknesses, and in some cases, provides the exploit for testing to see if that weakness exists within the target network.		
b.	It contains a copy of all the malware found on the Internet.		
c.	It contains all the IP addresses assigned to a particular company.		
d.	It contains a copy of all the misconfigured web pages on the Internet.		

Question 34 Which of the following is considered passive Information gathering?

Choice a ○ Social engineering a physical security guard to gain access to the parking lot but not contacting any other employee.

Choice b ● Gathering as much information as possible without contacting the target.

Choice c ○ Conducting a Denial of Service (DOS) probe on the target DMZ without getting access into the network itself.

Choice d ○ Probing the target network firewall to determine which ports are open without making direct contact with the target organization.

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 40 sec.

#	Answer	Correct answer	Your answer
a.	Social engineering a physical security guard to gain access to the parking lot but not contacting any other employee.		
b.	Gathering as much information as possible without contacting the target.		
c.	Conducting a Denial of Service (DOS) probe on the target DMZ without getting access into the network itself.		
d.	Probing the target network firewall to determine which ports are open without making direct contact with the target organization.		

Question 35 Which of the following is most secure and can be used with wireless communications?

Choice a ● WPA2

Choice b ○ IDEA

Choice c ○ Triple DES

Choice d ○ WPA

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 11 sec.

#	**Answer**	**Correct answer**	**Your answer**
a.	WPA2		
b.	IDEA		
c.	Triple DES		
d.	WPA		

Question 36 Wireshark cannot re-assemble TCP sessions.

Choice a ● True

Choice b ○ False

The answer is incorrect

Score is 0.00 out of 1.00. **Elapsed time** is 34 sec.

#	Answer	Correct answer	Your answer
a.	True		
b.	False		

Question 37 Several types of vulnerability assessments can be conducted. Which of the following is NOT a vulnerability assessment routinely conducted?

Choice a ● Open source intelligence available from the Internet.

Choice b ○ Database assessment

Choice c ○ Web Application assessment

Choice d ○ Vulnerability scanning

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 50 sec.

#	Answer	Correct answer	Your answer
a.	Open source intelligence available from the Internet.		
b.	Database assessment		
c.	Web Application assessment		
d.	Vulnerability scanning		

Question 38 Routers can provide which of the following security features?

Choice a ○ MAC Filtering

Choice b ○ When connected to active directory (AD), routers can manage QoS based on their access control lists which are stored in the active directory force controller.

Choice c ● Drop packets not intended for this network

Choice d ○ Password management

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 32 sec.

#	Answer	Correct answer	Your answer
a.	MAC Filtering		
b.	When connected to active directory (AD), routers can manage QoS based on their access control lists which are stored in the active directory force controller.		
c.	Drop packets not intended for this network		
d.	Password management		

Question 39 In _____________attacks, there will be some type of infusion of malicious client-side scripts into the website pages.

Choice a ● Cross-site script

Choice b ○ SYN Flood

Choice c ○ Man-in-the-Middle

Choice d ○ Man-in-the-Browser

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 14 sec.

#	Answer	Correct answer	Your answer
a.	Cross-site script		
b.	SYN Flood		
c.	Man-in-the-Middle		
d.	Man-in-the-Browser		

Question 40 Which of these commands will clear ARP cache?

Choice a ○ arp -c

Choice b ● arp -d

Choice c ○ arp -a

Choice d ○ arp -clear

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 15 sec.

#	Answer	Correct answer	Your answer
a.	arp -c		
b.	arp -d		
c.	arp -a		
d.	arp -clear		

Question 41 Electronic Codebook (ECB) is the least secure implementation of AES.

Choice a ○ True

Choice b ● False

The answer is incorrect

Score is 0.00 out of 1.00. **Elapsed time** is 13 sec.

#	Answer	Correct answer	Your answer
a.	True		
b.	False		

Question 42 Open-Source Intelligence (OSINT) is data that is collected using covert methods and confidential sources.

Choice a ○ True

Choice b ● False

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 13 sec.

#	Answer	Correct answer	Your answer
a.	True		
b.	False		

Question 43 Newer versions of Windows, such as Windows Server 2016, uses a stronger method to store passwords than previous versions.

Choice a ● True

Choice b ○ False

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 11 sec.

#	**Answer**	**Correct answer**	**Your answer**
a.	True		
b.	False		

Question 44 Web Scanners cannot test applications for known coding flaws such as injection issues or Cross-site Scripting vulnerabilities. The only way these errors can be found is by doing code reviews.

Choice a ○ True

Choice b ● False

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 23 sec.

#	Answer	Correct answer	Your answer
a.	True		
b.	False		

Question 45 Wireshark can be used in

Choice a ● both Windows and Unix environments.

Choice b ○ Unix networks.

Choice c ○ cloud computing environments.

Choice d ○ Windows networks.

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 22 sec.

#	Answer	Correct answer	Your answer
a.	both Windows and Unix environments.		
b.	Unix networks.		
c.	cloud computing environments.		
d.	Windows networks.		

Question 46 Which layer of the OSI model determines network topology?

Choice a ○ Layer 2 Datalink

Choice b ○ Layer 4 Transport

Choice c ○ Layer 5 Session

Choice d ● Layer 1 Physical

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 17 sec.

#	Answer	Correct answer	Your answer
a.	Layer 2 Datalink		
b.	Layer 4 Transport		
c.	Layer 5 Session		
d.	Layer 1 Physical		

Question 47 A Linux shell is

Choice a ○ A server running Linux that has all the ports closed and protocols removed.

Choice b ○ A hardened Linux distribution.

Choice c ● A Linux command language interpreter that executes commands.

Choice d ○ A Linux, bastion host.

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 15 sec.

#	Answer	Correct answer	Your answer
a.	A server running Linux that has all the ports closed and protocols removed.		
b.	A hardened Linux distribution.		
c.	A Linux command language interpreter that executes commands.		
d.	A Linux, bastion host.		

Question 48 Features exploit tunneling that allows you to run penetration tests from an exploited target.

Choice a ○ PcPdump

Choice b ○ Windump

Choice c ○ Nexus

Choice d ● Saint

The answer is correct

Score is 1.00 out of 1.00. **Elapsed time** is 57 sec.

#	Answer	Correct answer	Your answer
a.	PcPdump		
b.	Windump		
c.	Nexus		
d.	Saint		

Question 49 Why is NSlookup used?

Choice a ○ To adjust the TTL number prior to it reaching the DNS.

Choice b ○ To assign IP addresses in Windows Server 2016/Windows 10.

Choice c ● To query domain name servers.

Choice d ○ To check the lease time of an IP address on a workstation.

The answer is incorrect

Score is 0.00 out of 1.00. **Elapsed time** is 1 min.

#	Answer	Correct answer	Your answer
a.	To adjust the TTL number prior to it reaching the DNS.		
b.	To assign IP addresses in Windows Server 2016/Windows 10.		
c.	To query domain name servers.		
d.	To check the lease time of an IP address on a workstation.		

Question 50 “Bug Bounty Program” rewards ethical hackers based on the number of vulnerabilities found.

Choice a ○ True

Choice b ● False

The answer is incorrect

Score is 0.00 out of 1.00. **Elapsed time** is 18 sec.

#	Answer	Correct answer	Your answer
a.	True		
b.	False		