SKILLCERTPRO
IT CERTIFICATION TRAININGS

0

Information Security / By SkillCertPro

Practice Set 8

Your results are here!! for" CEHv11 Practice Test 8 "

0 of 65 questions answered correctly

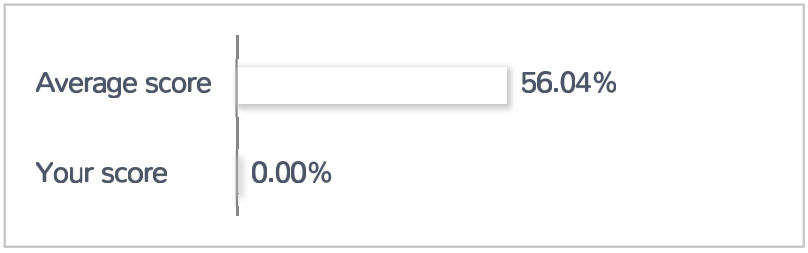
Your time: 00:00:02

Your Final Score is : 0

You have attempted : 0

Number of Correct Questions : 0 and scored 0

Number of Incorrect Questions : 0 and Negative marks 0



You can review your answers by clicking view questions.

Important Note : Open Reference Documentation Links in New Tab (Right Click and Open in New Tab).

Restart Test | View Answers

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34

35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51
52 53 54 55 56 57 58 59 60 61 62 63 64 65

Correct Incorrect

Review Question Summary

1. Question

Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drown based on these scan results? TCP port 21 "" no response – TCP port 22 "" no response – TCP port 23 "" Time-to-live exceeded

- The lack of response from ports 21 and 22 indicate that those services are not running on the destination server
- The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host
- **The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall**
- The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error

Unattempted

2. Question

If there is an Intrusion Detection System (IDS) in intranet, which port scanning technique cannot be used?

- Idle scan
- Spoof Scan
- TCP Connect scan
- **TCP SYN**

Unattempted

3. Question

Bob finished a C programming course and created a small C application to monitor the network traffic and produce alerts when any origin sends "many" IP packets, based on the average number of packets sent by all origins and using some thresholds. In concept, the solution developed by Bob is actually:

- A signature-based IDS
- A behavior-based IDS
- A hybrid IDS
- **Just a network monitoring tool**

Unattempted

4. Question

Internet Protocol Security IPSec is actually a suite of protocols. Each protocol within the suite provides different functionality. Collective IPSec does everything except.

- **Work at the Data Link Layer**
- Encrypt
- Authenticate
- Protect the payload and the headers

Unattempted

5. Question

What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?

- Announced
- Black-box
- **Grey-box**
- White-box

Unattempted

6. Question

Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

- Parabolic grid antenna
- Dipole antenna
- **Yagi antenna**
- Omnidirectional antenna

Unattempted

7. Question

Which regulation defines security and privacy controls for Federal information systems and organizations?

- EU Safe Harbor
- PCI-DSS
- HIPAA
- **NIST-800-53**

Unattempted

8. Question

Bob received this text message on his mobile phone: "Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com". Which statement below is true?

- **This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.**
- This is a scam because Bob does not know Scott.
- This is probably a legitimate message as it comes from a respectable organization.
- Bob should write to scottmelby@yahoo.com to verify the identity of Scott.

Unattempted

9. Question

During the process of encryption and decryption, what keys are shared?

- Public and private keys
- Private keys
- User passwords
- **Public keys**

Unattempted

10. Question

The company ABC recently contract a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. What is the following options can be useful to ensure the integrity of the data?

- The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure is the same document
- The document can be sent to the accountant using an exclusive USB for that document
- **The CFO can use a hash algorithm in the document once he approved the financial statements**
- The CFO can use an excel file with a password

Unattempted

11. Question

There are several ways to gain insight on how a cryptosystem works with the goal of reverse engineering the process. A term describes when two pieces of data result in the value is?

- Polymorphism
- **Collision**
- Escrow

Collusion

Unattempted

12. Question

A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering that NMAP result below, which of the following is likely to be installed on the target machine by the OS? Starting NMAP 5.21 at 2011-03-15 11:06 NMAP scan report for 172.16.40.65 Host is up (1.00s latency). Not shown: 993 closed ports PORT STATE SERVICE 21/tcp open ftp 23/tcp open telnet 80/tcp open http 139/tcp open netbios-ssn 515/tcp open 631/tcp open ipp 9100/tcp open MAC Address: 00:00:48:0D:EE:8

The host is likely a printer.

The host is likely a Linux machine.

The host is likely a Windows machine.

The host is likely a router.

Unattempted

13. Question

You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line. Which command would you use?

c:\services.msc

c:\ncpa.cp

c:\compmgmt.msc

c:\gpedit

Unattempted

14. Question

Which of the following is the best countermeasure to encrypting ransomwares?

- Use multiple antivirus softwares
- Pay a ransom
- **Keep some generation of off-line backup**
- Analyze the ransomware to get decryption key of encrypted data

Unattempted

15. Question

An attacker changes the profile information of a particular user (victim) on the target website. The attacker uses this string to update the victim's profile to a text file and then submit the data to the attacker's database.

What is this type of attack (that can use either HTTP GET or HTTP POST) called?

- SQL Injection
- Browser Hacking
- **Cross-Site Request Forgery**
- Cross-Site Scripting

Unattempted

16. Question

Emil uses nmap to scan two hosts using this command:

nmap -sS -T4 -O 192.168.99.1 192.168.99.7

He receives this output:

```
Nmap scan report for 192.168.99.1
Host is up (0.00082s latency).
Not shown: 994 filtered ports
PORT STATE SERVICE
21/tcp open ftp
23/tcp open telnet
53/tcp open domain
80/tcp open http
161/tcp closed snmp
MAC Address: B0:75:D5:33:57:74 (ZTE)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

Nmap scan report for 192.168.99.7
Host is up (0.000047s latency).
All 1000 scanned ports on 192.168.99.7 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
```

What is his conclusion?

- Host 192.168.99.1 is the host that he launched the scan from.
- Host 192.168.99.7 is an iPad.
- Host 192.168.99.7 is down.
- **He performed a SYN scan and OS scan on hosts 192.168.99.1 and 192.168.99.7**

Unattempted

17. Question

A large mobile telephony and data network operator has a data center that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems. What is the best security policy concerning this setup?

- As long as the physical access to the network elements is restricted, there is no need for additional measures.
- **Network elements must be hardened with user ids and strong passwords. Regular security tests and audits should be performed.**
- The operator knows that attacks and down time are inevitable and should have a backup site.

There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.

Unattempted

18. Question

Which tier in the N-tier application architecture is responsible for moving and processing data between the tiers?

Application Layer

Presentation tier

Data tier

Logic tier

Unattempted

19. Question

Which service in a PKI will vouch for the identity of an individual or company?

CBC

KDC

CR

CA

Unattempted

20. Question

A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The "ps" command shows that the "nc" file is running as process, and the netstat command shows the "nc" process is listening on a network port. What kind of vulnerability must be present to make this remote attack possible?

- Brute force login
- Directory traversal
- **File system permissions**
- Privilege escalation

Unattempted

21. Question

PGP, SSL, and IKE are all examples of which type of cryptography?

- Hash Algorithm
- **Public Key**
- Digest
- Secret Key

Unattempted

22. Question

You want to analyze packets on your wireless network. Which program would you use?

- **Wireshark with Airpcap**
- Ethereal with Winpcap
- Airsnort with Airpcap
- Wireshark with Winpcap

Unattempted

23. Question

What does a firewall check to prevent particular ports and applications from getting packets into an organization?

- Network layer headers and the session layer port numbers
- Application layer port numbers and the transport layer headers
- **Transport layer port numbers and application layer headers**
- Presentation layer headers and the session layer port numbers

Unattempted

24. Question

Seth is starting a penetration test from inside the network. He hasn't been given any information about the network. What type of test is he conducting?

- External, Whitebox
- Internal, Whitebox
- **Internal, Blackbox**
- External, Blackbox

Unattempted

25. Question

Which of the following is the BEST way to defend against network sniffing?

- Register all machines MAC Address in a Centralized Database
- **Using encryption protocols to secure network communications**
- Use Static IP Address
- Restrict Physical Access to Server Rooms hosting Critical Servers

Unattempted

26. Question

Look at the following output. What did the hacker accomplish?

```
; <<>> DiG 9.7.-P1 <<>> axfr domam.com @192.168.1.105
;; global options: +cmd
domain.com. 3600 IN SOA srv1.domain.com. hostsrv1.d
omain.com. 131 900 600 86400 3600
domain.com. 600 IN A 192.168.1.102
domain.com. 600 IN A 192.168.1.105
domain.com. 3600 IN NS srv1.domain.com.
domain.com. 3600 IN NS srv2.domain.com.
vpn.domain.com. 3600 IN A 192.168.1.1
server.domain.com. 3600 IN A 192.168.1.3
office.domain.com. 3600 IN A 192.168.1.4
remote.domain.com. 3600 IN A 192.168. 1.48
support.domain.com. 3600 IN A 192.168.1.47
ns1.domain.com. 3600 IN A 192.168.1.41
ns2.domain.com. 3600 IN A 192.168.1.42
ns3.domain.com. 3600 IN A 192.168.1.34
ns4.domain.com. 3600 IN A 192.168.1.45
srv1.domain.com. 3600 IN A 192.168.1.102
srv2.domain.com. 1200 IN A 192.168.1.105
domain.com. 3600 INSOA srv1.domain.com. hostsrv1.do
main.com. 131 900 600 86400 3600
;; Query time: 269 msec
;; SERVER: 192.168.1.105#53(192.168.1.105)
;; WHEN: Sun Aug 11 20:07:59 2013
;; XFR size: 65 records (messages 65, bytes 4501)
```

- The hacker listed DNS records on his own domain.
- **The hacker successfully transferred the zone and enumerated the hosts.**
- The hacker used who is to gather publicly available records for the domain.
- The hacker used the "fierce" tool to brute force the list of available domains.

Unattempted

27. Question

Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?

- Containment phase
- **Preparation phase**
- Identification phase

Recovery phase

Unattempted

28. Question

As an Ethical Hacker you are capturing traffic from your customer network with Wireshark and you need to find and verify just SMTP traffic. What command in Wireshark will help you to find this kind of traffic?

smtp port

tcp.port eq 25

tcp.contains port 25

request smtp 25

Unattempted

29. Question

You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping it but you didn't get any response back. What is happening?

You need to run the ping command with root privileges.

ICMP could be disabled on the target server.

TCP/IP doesn't support ICMP.

The ARP is disabled on the target server.

Unattempted

30. Question

What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?

Use a strong logon password to the operating system.

Back up everything on the laptop and store the backup in a safe place.

- Encrypt the data on the hard drive.
- Set a BIOS password

Unattempted

31. Question

Which of the following Nmap commands will produce the following output?

Output:

```
Staring Nmap 6.47 (http://nmap.org) at 2015-05-26 12:50 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00042s latency).
Not shown: 65530 open | filtered ports, 65529 filtered ports
PORT STATE SERVICE
111/tcp open rpcbind
999/tcp open garcon
1017/tcp open unknown
1021/tcp open exp1
1023/tcp open netvenuechat
2049/tcp open nfs
17501/tcp open unknown
111/udp open rpcbind
123/udp open ntp
137/udp open netbios-ns
2049/udp open zeroconf
17501/udp open|filtered unknown
51857/udp open|filtered unknown
54358/udp open|filtered unknown
56228/udp open|filtered unknown
57598/udp open|filtered unknown
59488/udp open|filtered unknown
60027/udp open|filtered unknown
```

- nmap ""sS ""sU ""Pn ""p 1-65535 192.168.1.1
- nmap ""sS ""Pn 192.168.1.1
- nmap ""sN ""Ps ""T4 192.168.1.1
- nmap ""sT ""sX ""Pn ""p 1-65535 192.168.1.1

Unattempted

32. Question

By using a smart card and pin, you are using a two-factor authentication that satisfies

- Something you have and something you are
- **Something you have and something you know**
- Something you know and something you are
- Something you are and something you remember

Unattempted

33. Question

When conducting a penetration test, it is crucial to use all means to get all available information about the target network. One of the ways to do that is by sniffing the network. Which of the following cannot be performed by the passive network sniffing?

- Capturing a network traffic for further analysis
- Identifying operating systems, services, protocols and devices
- **Modifying and replaying captured network traffic**
- Collecting unencrypted information about usernames and passwords

Unattempted

34. Question

Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

- **An authentication system that creates one-time passwords that are encrypted with secret keys.**
- An authentication system that uses passphrases that are converted into virtual passwords.
- A biometric system that bases authentication decisions on physical attributes.
- A biometric system that bases authentication decisions on behavioral attributes.

Unattempted

35. Question

John the Ripper is a technical assessment tool used to test the weakness of which of the following?

- Firewall rulesets
- File permissions
- **Passwords**
- Usernames

Unattempted

36. Question

The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the Central Processing Unit (CPU), rather than passing only the frames that the controller is intended to receive. Which of the following is being described?

- WEM
- Multi-cast mode
- Port forwarding
- **Promiscuous mode**

Unattempted

37. Question

What is the purpose of a demilitarized zone on a network?

- To contain the network devices you wish to protect
- To scan all traffic coming through the DMZ to the internal network
- **To only provide direct access to the nodes within the DMZ and protect the network behind it**
- To provide a place to put the honeypot

Unattempted

38. Question

A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

- Perform a vulnerability scan of the system.
- Perform a cost/benefit analysis of the audit feature.
- Allocate funds for staffing of audit log review.
- **Determine the impact of enabling the audit feature.**

Unattempted

39. Question

Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?

- msfd
- **msfencode**
- msfpayload
- msfcli

Unattempted

40. Question

In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known as wardriving. Which Algorithm is this referring to?

- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA2)
- Temporal Key Integrity Protocol (TKIP)
- **Wired Equivalent Privacy (WEP)**

Unattempted

41. Question

Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications an unpatched security flaws in a computer system?

- Wireshark
- **Metasploit**
- Nessus
- Maltego

Unattempted

42. Question

The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124. An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap 192.168.1.64/28 Why he cannot see the servers?

- The network must be down and the nmap command and IP address are ok
- **He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range.**
- He needs to add the command ""ip address"" just before the IP address.
- He needs to change the address to 192.168.1.0 with the same mask

Unattempted

43. Question

Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close. What just happened?

- Phishing
- **Tailgating**

- Masquerading
- Whaling

Unattempted

44. Question

A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed. Which security policy must the security analyst check to see if dial-out modems are allowed?

- Permissive policy
- Acceptable-use policy
- Firewall-management policy
- **Remote-access policy**

Unattempted

45. Question

Scenario: 1. Victim opens the attacker's web site. 2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make $1000 in a day?'. 3. Victim clicks to the interesting and attractive content URL. 4. Attacker creates a transparent 'iframe' in front of the URL which victim attempts to click, so victim thinks that he/she clicks to the 'Do you want to make $1000 in a day?' url but actually he/she clicks to the content or UPL that exists in the transparent 'iframe' which is setup by the attacker. What is the name of the attack which is mentioned in the scenario?

- **Clickjacking Attack**
- HTML Injection
- Session Fixation
- HTTP Parameter Pollution

Unattempted

46. Question

What is correct about digital signatures?

- Digital signatures are issued once for each user and can be used everywhere until they expire.
- **A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.**
- A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.
- Digital signatures may be used in different documents of the same type.

Unattempted

47. Question

You have successfully gained access to a Linux server and would like to ensure that the succeeding outgoing traffic from this server will not be caught by Network-Based Intrusion Detection Systems (NIDS). What is the best way to evade the NIDS?

- **Encryption**
- Out of band signaling
- Protocol Isolation
- Alternate Data Streams

Unattempted

48. Question

The following is part of a log file taken from the machine on the network with the IP address of 192.168.1.106:

```
Time:Mar 13 17:30:15 Port:20 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:17 Port:21 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:19 Port:22 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:21 Port:23 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:22 Port:25 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:23 Port:80 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:30 Port:443 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
```

What type of activity has been logged?

- Port scan targeting 192.168.1.103
- **Port scan targeting 192.168.1.106**
- Denial of service attack targeting 192.168.1.103
- Teardrop attack targeting 192.168.1.106

Unattempted

49. Question

Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in bounds checking mechanism? Code: #include int main(){ char buffer[8]; strcpy(buffer, “”11111111111111111111111111111111″”); } Output: Segmentation fault –

- Python
- C#
- **C++**
- Java

Unattempted

50. Question

In many states sending spam is illegal. Thus, the spammers have techniques to try and ensure that no one knows they sent the spam out to thousands of users at a time. Which of the following best describes what spammers use to hide the origin of these types of e-mails?

- Tools that will reconfigure a mail server's relay component to send the e-mail back to the spammers occasionally.
- A blacklist of companies that have their mail server relays configured to be wide open.
- **Mail relaying, which is a technique of bouncing e-mail from internal to external mails servers continuously.**
- A blacklist of companies that have their mail server relays configured to allow traffic only to their specific domain name.

Unattempted

51. Question

What is the difference between the AES and RSA algorithms?

- AES is asymmetric, which is used to create a public/private key pair; RSA is symmetric, which is used to encrypt data
- **RSA is asymmetric, which is used to create a public/private key pair; AES is symmetric, which is used to encrypt data**
- Both are asymmetric algorithms, but RSA uses 1024-bit keys
- Both are symmetric algorithms, but AES uses 256-bit keys

Unattempted

52. Question

Which type of security feature stops vehicles from crashing through the doors of a building?

- Turnstile
- Receptionist
- **Bollards**
- Mantrap

Unattempted

53. Question

Which of the following programs is usually targeted at Microsoft Office products?

- Polymorphic virus
- Stealth virus
- **Macro virus**
- Multipart virus

Unattempted

54. Question

An enterprise recently moved to a new office and the new neighborhood is a little risky. The CEO wants to monitor the physical perimeter and the entrance doors 24 hours. What is the best option to do this job?

- Use lights in all the entrance doors and along the company's perimeter.
- **Install a CCTV with cameras pointing to the entrance doors and the street.**
- Use fences in the entrance doors.
- Use an IDS in the entrance doors and install some of them near the corners.

Unattempted

55. Question

What mechanism in Windows prevents a user from accidentally executing a potentially malicious batch (.bat) or PowerShell (.ps1) script?

- **Data Execution Prevention (DEP)**
- User Access Control (UAC)
- Address Space Layout Randomization (ASLR)
- Windows firewall

Unattempted

56. Question

Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms?

- Security
- **Speed**
- Key distribution
- Scalability

Unattempted

57. Question

In which phase of the ethical hacking process can Google hacking be employed? This is a technique that involves manipulating a search string with specific operators to search for vulnerabilities. Example: allintitle: root passwd

- Gaining Access
- **Reconnaissance**
- Scanning and Enumeration
- Maintaining Access

Unattempted

58. Question

Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

- Cavity virus
- Macro virus
- **Stealth/ Tunneling virus**
- Polymorphic virus

Unattempted

59. Question

Which of the following is a passive wireless packet analyzer that works on Linux-based systems?

- **Kismet**
- Burp Suite
- tshark

OpenVAS

Unattempted

60. Question

You are an Ethical Hacker who is auditing the ABC company. When you verify the NOC one of the machines has 2 connections, one wired and the other wireless. When you verify the configuration of this Windows system you find two static routes. route add 10.0.0.0 mask 255.0.0.0 10.0.0.1 route add 0.0.0.0 mask 255.0.0.0 199.168.0.1 What is the main purpose of those static routes?

The first static route indicates that the internal addresses are using the internal gateway and the second static route indicates that all the traffic that is not internal must go to an external gateway.

Both static routes indicate that the traffic is external with different gateway.

The first static route indicates that the internal traffic will use an external gateway and the second static route indicates that the traffic will be rerouted.

Both static routes indicate that the traffic is internal with different gateway.

Unattempted

61. Question

An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up. What is the most likely cause?

The network devices are not all synchronized.

Proper chain of custody was not observed while collecting the logs.

The security breach was a false positive.

The attacker altered or erased events from the logs.

Unattempted

62. Question

A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application. What kind of Web application vulnerability likely exists in their software?

- Web site defacement vulnerability
- Cross-site Request Forgery vulnerability
- SQL injection vulnerability
- **Cross-site scripting vulnerability**

Unattempted

63. Question

What is the role of test automation in security testing?

- **It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.**
- Test automation is not usable in security due to the complexity of the tests.
- It is an option but it tends to be very expensive.
- It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies.

Unattempted

64. Question

In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?

- Both pharming and phishing attacks are identical.
- In a phishing attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name.

Both pharming and phishing attacks are purely technical and are not considered forms of social engineering

In a pharming attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name.

Unattempted

65. Question

Which of the following scanning method splits the TCP header into several packets and makes it difficult for packet filters to detect the purpose of the packet?

SYN/FIN scanning using IP fragments

IPID scanning

ICMP Echo scanning

ACK flag probe scanning

Unattempted

Click Below to go to Next Practice Set

We help you to succeed in your certification exams

We have helped over thousands of working professionals to achieve their certification goals with our practice tests.

Skillcertpro

Quick Links

ABOUT US
FAQ
BROWSE ALL PRACTICE TESTS
CONTACT FORM

Important Links

REFUND POLICY
REFUND REQUEST
TERMS & CONDITIONS
PRIVACY POLICY

Privacy Policy