SKILLCERTPRO
IT CERTIFICATION TRAININGS

0

Information Security / By SkillCertPro

Practice Set 17

Your results are here!! for" CEHv11 Practice Test 17 "

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

Average score	57.55%
Your score	0.00%

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

Which of the following is a strong post designed to stop a car?

- Fence
- Gate
- Reinforced rebar
- **Bollard**

Unattempted

A bollard is a sturdy, short, vertical post.

2. Question

Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 1?

- 2048 bit key
- 1025 bit key
- 1536 bit key
- **768 bit key**

Unattempted

DH Group 1: 768-bit group

DH Group 2: 1024-bit group

DH Group 5: 1536-bit group

DH Group 14: 2048-bit group

DH Group 15: 3072-bit group

3. Question

A three-way handshake is a process used in establishing a TCP connection. What type of message is used when terminating the connection?

- SYN
- ACK
- **FIN**
- SYN-ACK

Unattempted

TCP traffic begins with a three-way handshake. In this TCP handshake process, a client needs to initiate the conversation by requesting a communication session with the Server.

SYN — Used to initiate and establish a connection. It also helps you to synchronize sequence numbers between devices.

ACK — Helps to confirm to the other side that it has received the SYN.

SYN-ACK — SYN message from local device and ACK of the earlier packet.

FIN — Used to terminate a connection.

4. Question

What hacking attack is challenge/response authentication used to prevent?

- **Replay attacks**
- Scanning attacks
- Session hijacking attacks
- Password cracking attacks

Unattempted

Challenge-response authentication can defend against session replay attacks, in which an attacker listens to previous messages and resends them later to get the same credentials as the original message. Challenge-response systems defend against replay attacks because each challenge and response is unique.

5. Question

A cybercriminal who uses rogue wireless AP performed a MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections. When users accessed any page, the applet ran and exploited many machines. Which of the following tools did the cybercriminal used to inject HTML code?

- Tcpdump
- Aircrack-ng
- Wireshark
- **Ettercap**

Unattempted

Ettercap is a comprehensive suite for man-in-the-middle attacks. It features sniffing of live connections, content filtering on the fly, and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.

6. Question

This is a type of network attack which relies on sending an abnormally large packet size that exceeds TCP/IP specifications?

- TCP hijacking
- SYN flooding
- Smurf attack
- **Ping of death**

Unattempted

Ping of Death is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.

7. Question

What are the three types of compliance that the Open Source Security Testing Methodology Manual (OSSTMM) recognizes?

- Regulatory

- [ ] Standards based
- [ ] Legislative
- [ ] Contractual

Unattempted

The OSSTMM recognizes three types of compliance:

A. Legislative. Compliance with legislation is in accordance to the region where the legislation can be enforced. The strength and commitment to the legislation comes from previously successful legal arguments and appropriately set and just enforcement measures. Examples are Sarbanes-Oxley, HIPAA, and the various Data Protection and Privacy legislation.

B. Contractual. Compliance to contractual requirements are in accordance to the industry or within the group that requires the contract and may take action to enforce compliance. An example is the payment card industry data security standard (PCI DSS) promoted and required by VISA and MasterCard.

C. Standards based. Compliance to standards is in accordance with the business or organization where the compliance to standards is enforced as policy. Examples are the OSSTMM, ISO 27001/5, and ITIL.

8. Question

A website is vulnerable to XSS and SQL injection attack due to:

- ○ Broken Authentication
- ○ Weak Password
- ○ Improper Output Validation
- ○ **Improper input Validation**

Unattempted

Cross-site scripting or XSS flaws occur whenever an application allows users to add custom code that includes data from untrusted sources without proper validation. Hackers inject malicious scripts into a victim's system by hiding them within legitimate requests.

9. Question

A security engineer wants to map the company's internal network. What type of scan is being used if she enters the following nmap command:

```
nmap -n -sS -P0 -p
```

- Scheduled scan
- Full scan
- **Stealth scan**
- Quick scan

Unattempted

-sS is a command line switch used for finding out the most commonly used TCP port using TCP SYN scan or stealth scan.

10. Question

This is the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

- Deferred risk
- Impact risk
- Inherent risk
- **Residual risk**

Unattempted

According to ISO 27001, residual risk is “the risk remaining after risk treatment”.

11. Question

This tool is used to collect wireless packet data?

- Nessus
- **NetStumbler**
- Netcat
- John the Ripper

Unattempted

The NetStumbler application is a Windows-based tool generally used to discover WLAN networks running on 802.11 a/b/g standards. It helps detect other networks that may cause interference to your network, and is

generally used for war driving purposes by attackers. It can also find out poor coverage areas in the WLAN network, and helps the administrator set up the network the way it is intended to be.

12. Question

This is a web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed by other users.

- SQL injection attack
- DAP Injection attack
- Cross-Site Request Forgery (CSRF)
- **Cross-Site Scripting (XSS)**

Unattempted

Cross-site scripting or XSS flaws occur whenever an application allows users to add custom code that includes data from untrusted sources without proper validation. Hackers inject malicious scripts into a victim's system by hiding them within legitimate requests. Hackers can also bypass authentication mechanisms, gain privileges, and then inject malicious scripts into specific web pages. These malicious scripts can hijack user sessions, deface websites, or redirect the user to malicious sites.

13. Question

Which of the following malware allows cybercriminals to remotely access the victim's computer and lock it once installed. This malware generates a pop-up window, webpage, or email warning telling the victim that they've been hacked and then demands a ransom payment before they can access their files and programs again.

- Adware
- Firmware
- Spyware
- **Ransomware**

Unattempted

Ransomware is a form of malware that restricts the user from accessing their infected computer system or files and then asks for a ransom payment to regain user access. The main goal of a ransomware attack is to extort money from its victims.

14. Question

Which of the following are well known password-cracking programs?

- [ ] Jack the Ripper
- [ ] NetCat
- [ ] **John the Ripper**
- [ ] **L0phtcrack**

Unattempted

L0phtcrack and John the Ripper are two well know password-cracking programs. While netcat is considered the Swiss-army knife of hacking tools, it is not used for password cracking.

15. Question

Medusa can be used to carry:

- ○ Vulnerability Scanning
- ○ Ping Flood Attack
- ○ **Brute-Force Attack**
- ○ Passive Reconnaissance

Unattempted

Medusa is intended to be a speedy, massively parallel, modular, login brute-forcer.

16. Question

What could be done next if the final set of security controls did not eliminate all the risk in a system?

- ○ Remove current controls since they are not completely effective.
- ○ Continue applying controls until there is zero risk.
- ○ Ignore the remaining risk.
- ○ **Check the residual risk, if it is low enough, it can be accepted.**

Unattempted

According to ISO 27001, residual risk is "the risk remaining after risk treatment".

17. Question

Which of the following tools are you going to use in order to remain undetected by an IDS while pivoting and passing traffic over a server you have just compromised and gained root access to?

- None of the above.
- Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.
- Use Alternate Data Streams to hide the outgoing packets from this server.
- **Install Cryptcat and encrypt outgoing packets from this server.**

Unattempted

Cryptcat is a tool used for moving data off the victim's system across the normal open ports without any of the security devices detecting it.

18. Question

SIA Global Security's policy states that all web browsers must automatically delete their HTTP browser cookies upon terminating. Which of the following security breach will be mitigated by this policy?

- Cybercriminals accessing passwords stored on the user's computer without the user's knowledge.
- Cybercriminals accessing the user and password information stored in the company's SQL database.
- Cybercriminals determining the user's web browser usage patterns, including when sites were visited and for how long.
- **Cybercriminals stealing the user's authentication details to access websites that trust the web browser.**

Unattempted

Cookies can store passwords and form content a user has previously entered, such as a credit card number or an address. Cookies can be stolen using a technique called cross-site scripting. This occurs when an attacker takes advantage of a website that allows its users to post unfiltered HTML and JavaScript content.

19. Question

A network security admin is concerned that Address Resolution Protocol (ARP) spoofing or poisoning might occur on his network. Which of the following will help the network security admin mitigate this attack? Choose all that apply.

- [ ] **Use static ARP entries (for small network).**
- [ ] Use firewall between all LAN segments.
- [ ] **Use ARPwatch to monitor for strange ARP activity.**
- [ ] **Use port security on switches.**

Unattempted

Using port security on switches will only allow the first MAC address that is connected to the switch to use that port, thus preventing ARP spoofing. ARPwatch monitors strange ARP activity that can help identify ARP spoofing. On a very small network, static ARP entries are a possibility. However, on a large network, this is not an realistic option.

20. Question

This algorithm provides better protection against brute force attacks by using a 160-bit message digest.

- ( ) MD4
- ( ) MD5
- ( ) RC4
- ( ) **SHA-1**

Unattempted

Secure Hash Algorithm 1 or SHA-1 is a cryptographic hash function that produces a 160-bit (20-byte) hash value.

21. Question

Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

- ( ) etherea
- ( ) Nessus
- ( ) Jack the ripper

Tcpdump

Unattempted

Tcpdump is a command line utility that allows user to capture and analyze network traffic going through the user's system. It is often used to help troubleshoot network issues, as well as a security tool. It can also be launched in the background or as a scheduled job using tools like cron.

22. Question

Anna is attempting to use nslookup to query the Domain Name Service (DNS). She uses the nslookup interactive mode for the search. Which of the following command should she type into the command shell to request the appropriate records?

Transfer type=ns

Set type=ns

Request type=ns

Locate type=ns

Unattempted

"set type=ns" specifies a DNS name server for the named zone.

23. Question

Which system consists of a publicly available set of databases that contain domain name registration contact information?

IETF

IANA

CAPTCHA

WHOIS

Unattempted

WHOIS is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system, but is also used for a wider range of other information.

24. Question

A penetration tester from SIA Global Security was contacted to scan a server. She needs to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for. Which of the below scanning technique will she use?

- TCP Scanning
- **IP Fragment Scanning**
- Inverse TCP flag scanning
- ACK flag scanning

Unattempted

IP fragmentation occurs when packets are broken up into smaller pieces (fragments) so they can pass through a link at a smaller maximum transmission unit than the original or larger packet size. IP fragmentation can cause problems when fragments are affected by packet loss and cause excessive retransmissions. This can cause performance issues. To recover the loss of a fragment, protocols, like TCP, retransmit fragments in order to reassemble them. Fragmented traffic can also be crafted to evade intrusion detection systems and be used maliciously.

25. Question

Which of the following biometrics scan is most commonly used for liveness detection?

- Facial recognition scan
- Retinal scan
- Signature kinetics scan
- **Iris scan**

Unattempted

The iris, or the colored part of the eye, consists of thick, thread-like muscles. By measuring the unique folds of these muscles, biometric authentication tools can confirm identity with incredible accuracy. Iris scan is also used for liveness detection such as requiring the user to blink for the scan.

26. Question

A three-way handshake is a process used in establishing a TCP connection. What type of message is sent by the server to the client to confirm that the message has been received?

- ACK
- FIN
- SYN-ACK
- SYN

Unattempted

TCP traffic begins with a three-way handshake. In this TCP handshake process, a client needs to initiate the conversation by requesting a communication session with the Server.

SYN — Used to initiate and establish a connection. It also helps you to synchronize sequence numbers between devices.

ACK — Helps to confirm to the other side that it has received the SYN.

SYN-ACK — SYN message from local device and ACK of the earlier packet.

FIN — Used to terminate a connection.

27. Question

This tool is used to attack web applications by starvation of available sessions on the web server. It keeps the sessions at halt using never-ending POST transmissions and sending an arbitrarily large content-length header value.

- My Doom
- LOIC
- **R-U-Dead-Yet?(RUDY)**
- Astacheldraht

Unattempted

'R U Dead Yet?' or R.U.D.Y. is a denial-of-service attack tool that aims to keep a web server tied up by submitting form data at an absurdly slow pace. A R.U.D.Y. exploit is categorized as a low-and-slow attack, since it focuses on creating a few drawn-out requests rather than overwhelming a server with a high volume of quick requests. A successful R.U.D.Y. attack will result in the victim's origin server becoming unavailable to legitimate traffic.

28. Question

Which of the following does not describe Simple Object Access Protocol (SOAP)? Choose all that applies.

- Only compatible with the application protocol HTTP
- Exchanges data between web services
- Based on XML
- Provides a structured model for messaging

Unattempted

A SOAP client formulates a request for a service. This involves creating a conforming XML document, either explicitly or using Oracle SOAP client API. A SOAP client sends the XML document to a SOAP server. This SOAP request is posted using HTTP or HTTPS to a SOAP Request Handler running as a servlet on a Web server.

29. Question

It is a wireless network detector, packet sniffer, and intrusion detection system (IDS) and is commonly found on Linux-based system.

- Kismet
- Netstumbler
- Nessus
- Abel

Unattempted

Kismet is a wireless network detector, packet sniffer, and intrusion detection system (IDS) that works with any wireless card supporting raw monitoring (rfmon) mode. It can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic and works on Linux, Mac OSX, and Windows 10 under the WSL framework.

30. Question

Iya received an email with an attachment labeled "Updated_Scholarship_0321" which she thought came from her school. Inside the zip file is a file named "Updated_Scholarship_0321.docx.exe" disguised as a word document. Upon execution, a window appears stating, "This word document is corrupt." In the background, the file copies itself to Iya's APPDATA\local directory and begins to beacon to a C2 server to download additional malicious binaries. Iya encountered which type of malware?

- Macro Virus

- Trojan
- Worm
- Key-Logger

Unattempted

A Trojan is a type of malware in which it disguises itself as something that it isn't. Trojans often masquerades as a legitimate application, file, or seemingly harmless program to trick its victims into installing it.

31. Question

In Windows Operating System, where can you see the event logs?

- Control Panel
- Services
- Event Viewer
- Task Manager

Unattempted

Event Viewer is a component of Microsoft's Windows NT operating system that lets administrators and users view the event logs on a local or remote machine.

32. Question

Which of the following vulnerability has been detected in the web application if the tester attempts to insert the below test script into the search area on the company's web site:

```
< script>alert("This is a test")</script>
```

The result of this test script is a pop-up box that appears on the screen with the text: "This is a test".

- Cross-site scripting
- Cross-site request forgery
- Buffer overflow
- Distributed denial of service

Unattempted

Cross-site scripting or XSS flaws occur whenever an application allows users to add custom code that includes data from untrusted sources without proper validation. Hackers inject malicious scripts into a victim's system by hiding them within legitimate requests. Hackers can also bypass authentication mechanisms, gain privileges, and then inject malicious scripts into specific web pages. These malicious scripts can hijack user sessions, deface websites, or redirect the user to malicious sites.

33. Question

How can a rootkit bypass Windows 7 operating system's kernel mode, code signing policy?

- Performing common services for the application process and replacing real applications with fake ones.
- **Attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/options**
- Defeating the scanner from detecting any code change at the kernel.
- Replacing patch system calls with its own version that hides the rootkit (attacker's) actions.

Unattempted

By attaching itself to the master boot record in a hard drive and changing the machines boot sequence/options Windows 7 boot record never has the opportunity to determine something is wrong.

34. Question

This is an effective way to prevent Cross-site Scripting (XSS) flaws in software applications?

- Verify access right before allowing access to protected information and UI controls.
- **Validate and escape all information sent to a server.**
- Use security policies and procedures to define and implement proper security settings.
- Use digital certificates to authenticate a server before sending data.

Unattempted

Minimizing cross-site scripting flaws includes escaping suspicious HTTP requests, validating or sanitizing user-generated content, and enabling content security policy (CSP) as an added layer of in-depth defense in mitigating XSS.

35. Question

Which of the following toolkit contains different modules that have prepackaged exploits for a variety of vulnerabilities. This provides a higher chance of breaking into a wide range of vulnerable devices.

- **Metasploit**
- Bug Exploit
- Phishing
- Vulnerability kit

Unattempted

Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it can be easily customized and used with most operating systems.

36. Question

Which of the following biometrics scan measures a person's external features through a digital video camera?

- **Facial recognition scan**
- Iris scan
- Signature kinetics scan
- Retinal scan

Unattempted

A facial recognition scan measures the geometry of the face, including the distance between the eyes, the distance from the chin to the forehead, and multiple other points on a person's face.

37. Question

A security policy will be more accepted by employees if it is consistent and has the support of

- Supervisor
- Coworkers
- Security officer

Executive management

Unattempted

Everyone including the CEO down to the new hires must comply with security policies. If the executive management does not comply with the security policies and the consequences of non-compliance with the policy are not enforced, then mistrust and apathy toward compliance with the policy can affect your organization.

38. Question

It is an organization's established protocol for retaining information for operational or regulatory compliance needs.

Acceptable Use Policy

Data Retention Policy

Password Policy

Media Disposal Policy

Unattempted

Data Retention Policy is an organization's established protocol for retaining information for operational or regulatory compliance needs.

39. Question

Angel is an expert when it comes to password weaknesses and key loggers. She was then assigned to conduct a password assessment to XYZ company. She suspects that password policies are not in place and weak passwords are the norm throughout the company. Which of the following will she use to get the password from the company's hosts and servers?

Software only, they are the most effective.

Hardware and Software Keyloggers.

Passwords are always best obtained using Hardware key loggers.

Hardware, Software, and Sniffing.

Unattempted

All loggers will work as long as he has physical access to the computers.

40. Question

Which of the following tools can be used for passive OS fingerprinting?

- **Tcpdump**
- ping
- tracert
- Nmap

Unattempted

The passive operating system fingerprinting is a feature built into both the pf and tcpdump tools.

41. Question

Which of the following represents the initial two commands that an IRC client sends to join an IRC network?

- LOGIN, NICK
- LOGIN, USER
- **USER, NICK**
- USER, PASS

Unattempted

A “PASS” command is not required for either client or server connection to be registered, but it must precede the server message or the latter of the NICK/USER combination.

42. Question

A three-way handshake is a process used in establishing a TCP connection. What type of message is sent by the client to the server to begin this negotiation?

- **SYN**
- SYN-ACK
- ACK
- FIN

Unattempted

TCP traffic begins with a three-way handshake. In this TCP handshake process, a client needs to initiate the conversation by requesting a communication session with the Server.

SYN — Used to initiate and establish a connection. It also helps you to synchronize sequence numbers between devices.

ACK — Helps to confirm to the other side that it has received the SYN.

SYN-ACK — SYN message from local device and ACK of the earlier packet.

FIN — Used to terminate a connection.

43. Question

This tool is best used to achieve compliance with PCI Requirement 11?

- **Nessus**
- Clamwin
- Sub7
- Truecrypt

Unattempted

Nessus performs vulnerability, configuration, and compliance assessments. It supports various technologies such as operating systems, network devices, hypervisors, databases, tablets/phones, web servers, and critical infrastructure.

44. Question

Which of the following is an incorrect definition or characteristics of Simple Object Access Protocol (SOAP)?

- Provides a structured model for messaging
- Exchanges data between web services
- **Only compatible with the application protocol HTTP**
- Based on XML

Unattempted

A SOAP client formulates a request for a service. This involves creating a conforming XML document, either explicitly or using Oracle SOAP client API. A SOAP client sends the XML document to a SOAP server. This

SOAP request is posted using HTTP or HTTPS to a SOAP Request Handler running as a servlet on a Web server.

45. Question

Which of the following requires a host application for replication?

- Virus
- Micro
- Worm
- Trojan

Unattempted

Computer viruses can spread across the network only with the help of human intervention while worms do it independently.

46. Question

Which of the following programming languages have a built-in-bounds checking mechanism?

- C++
- Python
- Java
- C#

Unattempted

Programming languages such as C#, Java, Python have built-in inbound checking.

47. Question

Which of the following have the capability to check if the computer files have been changed or not?

- Firewall alerts
- Network sniffing
- Integrity checking hashes

Permission sets

Unattempted

Integrity checking is the process of comparing the current state of stored data and/or programs to a previously recorded state in order to detect any changes.

48. Question

Which of the following has the purpose of denying network access to local area networks and other information assets by unauthorized wireless devices.

Wireless Access Control List

Wireless Access Point

Wireless Analyzer

Wireless Intrusion Prevention System

Unattempted

A wireless intrusion prevention system (WIPS) operates at the Layer 2 (data link layer) level of the Open Systems Interconnection model. WIPS can detect the presence of rogue or misconfigured devices and can prevent them from operating on wireless enterprise networks by scanning the network's RFs for denial of service and other forms of attack.

49. Question

Which of the following virus infects the system boot sector and the executable files at the same time?

Stealth virus

Macro

Multipartite Virus

Polymorphic virus

Unattempted

A multipartite virus is a fast-moving virus that uses file infectors or boot infectors to attack the boot sector and executable files simultaneously. Most viruses either affect the boot sector, the system or the program files. The multipartite virus can affect both the boot sector and the program files at the same time, thus causing more damage than any other kind of virus.

50. Question

Which of the following policy contains guidelines for employees regarding what is allowed to use, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to the employee as soon as they join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms.

- **Information Security Policy (ISP)**
- Penetration Testing Policy (PTP)
- Information Audit Policy (IAP)
- Company Compliance Policy (CCP)

Unattempted

An information security policy (ISP) is a set of rules, policies , and procedures designed to ensure all users and networks within an organization meet minimum IT security and data protection security requirements.

51. Question

Which of the following is the reason why a cybercriminal wants to perform a scan on port 137?

- To check for file and print sharing on Windows systems.
- To disrupt the NetBIOS SMB service on the target host.
- To discover proxy servers on a network.
- **To discover information about a target host using NBTSTAT**

Unattempted

Microsoft encapsulates NetBIOS information within TCP/IP using port 135 to port 139.

52. Question

Which of the following is not a Bluetooth attack?

- Bluesmacking
- Bluesnarfing

- **Bluedriving**
- Bluejacking

Unattempted

Bluedriving is a bluetooth wardriving utility. It can capture bluetooth devices, lookup their services, get GPS information and present everything in a nice web page.

53. Question

What type of breach has the cybercriminal just performed in this scenario:

- An unauthorized individual enters a building following an employee through the employee's entrance after their break time.
- Announced
- **Tailgating**
- Piggybacking
- Reverse Social Engineering

Unattempted

Tailgating is a social engineering attack by cybercriminals in which they trick employees into helping them gain unauthorized access to the company premises.

54. Question

The security engineers and web development team of XYZ company have become aware of a certain type of security vulnerability in their web software. To prevent the possibility of being exploited, they want to modify the software requirements by disallowing users from entering HTML as input into their web application. Which of the following application vulnerability is being described in the scenario?

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

Unattempted

Cross-site scripting or XSS flaws occur whenever an application allows users to add custom code that includes data from untrusted sources without proper validation. Hackers inject malicious scripts into a victim's system by hiding them within legitimate requests.

55. Question

Which of the following is the correct process for the TCP three-way handshake connection termination?

- ACK, ACK-SYN, SYN
- **FIN, ACK-FIN, ACK**
- SYN, SYN-ACK, ACK
- ACK, ACK-FIN, FIN

Unattempted

Connection Establishment: SYN, SYN-ACK, ACK

Connection Termination: FIN, ACK-FIN, ACK

56. Question

Which of the following tools can be used in Fingerprinting VPN firewalls?

- **Ike-scan**
- Angry IP
- Arp-scan
- Nikto

Unattempted

ike-scan is a command-line tool that uses the IKE protocol to discover, fingerprint, and test IPsec VPN servers. It scans IP addresses for VPN servers by sending a specially crafted IKE packet to each host within a network.

57. Question

Which of the following best describes the Address Resolution Protocol (ARP)?

- It sends a reply packet to all the network elements, asking for the MAC address from a specific IP.

- **It sends a request packet to all the network elements, asking for the MAC address from a specific IP.**
- It sends a request packet to all the network elements, asking for the domain name from a specific IP.
- It sends a reply packet for a specific IP, asking for the MAC address.

Unattempted

Address Resolution Protocol (ARP) is one protocol of the TCP/IP protocol suite that is used to resolve an IP address to its matching MAC address.

58. Question

Which solution can be used to emulate computer services, such as mail and FTP, and to capture information related to logins or actions?

- Core server
- **Honeypot**
- Firewall
- Layer 4 switch

Unattempted

Honeypots are a type of deception technology that allows you to understand cybercriminals' behavior patterns. Security teams can use honeypots to investigate cybersecurity breaches to collect intel on how cybercriminals operate. They also reduce the risk of false positives, when compared to traditional cybersecurity measures, because they are unlikely to attract legitimate activity.

59. Question

Which of the following vulnerability in GNU's bash shell gives the cybercriminals access to run remote commands on a vulnerable system. The malicious software takes control of an infected machine, launches a denial-of-service attack to disrupt websites, and scans for other vulnerable devices?

- Rootshell
- Shellbash
- Rootshock
- **Shellshock**

Unattempted

Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell.

60. Question

Which of the following password cracking method uses word lists in combination with numbers and special characters?

- Hybrid
- Symmetric
- Linear
- Brute Force

Unattempted

A hybrid attack is a type of password attack that uses a combination of brute force and dictionary attacks such that it adds simple numbers or symbols to the passwords from a world list as it attempts to crack a password.

61. Question

Which mode of IPSec should be used to assure the security and confidentiality of data within the same LAN?

- AH promiscuous
- ESP transport mode
- ESP confidential
- AH Tunnel mode

Unattempted

Encapsulating Security Payload (ESP) provides confidentiality (in addition to authentication, integrity, and anti-replay protection) for the IP payload.

62. Question

Which of the following is the best countermeasure to a ransomware attack?

- Pay a ransom

- Use multiple antivirus software.
- **Keep some generation of off-line backup.**
- Analyze the ransomware to get the decryption key of encrypted data.

Unattempted

The best defense against any malware attack is having backup files.

63. Question

This refers to logging, recording, and resolving events promptly.

- Internal Procedure
- **Incident Management Process**
- Metrics
- Security Policy

Unattempted

Incident management is the process of managing IT service disruptions and restoring services within agreed service level agreements (SLAs).

64. Question

During a vulnerability testing, the penetration tester conducts an ACK scan using Nmap against the external interface of the DMZ firewall. The reports said that port 80 is unfiltered. Based on the response, which type of packet inspection is the firewall conducting?

- Stateful
- Host
- **Stateless**
- Application

Unattempted

Stateless firewalls watch network traffic and restrict or block packets based on source and destination addresses or other static values. They're not 'aware' of traffic patterns or data flows.

65. Question

Which of the following processes evaluates the adherence of an organization to its stated security policy?

- Vulnerability assessment
- **Security auditing**
- Penetration testing
- Risk assessment

Unattempted

A security audit is a systematic evaluation of the security of a company's information system by measuring how well it conforms to a set of established criteria.

Click Below to go to Next Practice Set

Pages: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

← Previous Post

Next Post →

Quick Links

ABOUT US

FAQ

BROWSE ALL PRACTICE TESTS

CONTACT FORM

Important Links

REFUND POLICY

REFUND REQUEST

TERMS & CONDITIONS

PRIVACY POLICY

Privacy Policy