SKILLCERTPRO
IT CERTIFICATION TRAININGS

0

Information Security / By SkillCertPro

Practice Set 19

Your results are here!! for" CEHv11 Practice Test 19 "

0 of 65 questions answered correctly

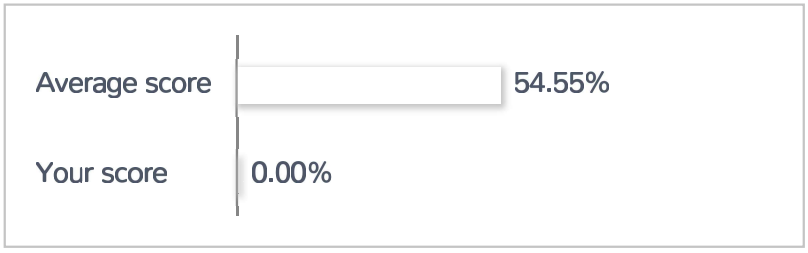
Your time: 00:00:01

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

Which of the following describes a denial-of-service (DoS) attack?

- A cybercriminal using every character, word, or letter to beat authentication.
- **A cybercriminal preventing legitimate users from accessing a website.**
- A cybercriminal trying to decipher a password by using a system, which subsequently crashes the network.
- A cybercriminal attempting to imitate a legitimate user by confusing a computer or even another person

Unattempted

Denial of service, or DoS, is an attack on a computer or network which makes it inaccessible to the user. In a DoS attack, a cybercriminal sends high volume traffic to a victim's system to overload its resources until the system crashes, preventing its users from accessing the network.

2. Question

This can be tagged as the critical phase of ethical hacking wherein the ethical hacker will spend a considerable amount of time?

- Escalating privileges
- **Reconnaissance**
- Network mapping
- Gaining access

Unattempted

In cybersecurity, reconnaissance is the preliminary phase or "information gathering" phase of ethical hacking. It is a crucial element of any successful cyberattack, as this is the phase in which the hacker collects all of the necessary information about the target before executing the attack.

3. Question

Which of the following is/are NOT an example of passive reconnaissance?

- Spyse
- Wireshark
- Shodan
- **Ping**

Unattempted

Passive reconnaissance is the process of gaining valuable information without alerting the potential victim. An example of passive reconnaissance is reviewing or checking the targeted company's website. Some good examples of passive reconnaissance are Shodan, Spyse, theHarvester, and Wireshark.

4. Question

MX record priority increases as the number increases.

- **FALSE**
- TRUE

Unattempted

The priority is used to determine which MX server to connect to first, in order to get to your inbox. The highest priority MX record has the lowest number.

5. Question

This vulnerability can be minimized by making sure that all data at rest and in-transit are well encrypted with strong, standard algorithms and uses up-to-date protocols such as transport layer security (TLS) with perfect forward secrecy (PFS) ciphers.

- Injection
- Broken Authentication
- Cross-site scripting
- **Sensitive data exposure**

Unattempted

Sensitive data exposure happens when an application fails to secure the stored or in-transit sensitive information such as account credentials, credit card numbers, Social Security Numbers, financial and healthcare information, and other personally identifiable information (PII) against hackers.

6. Question

Session hijacking is carried out in which of the following OSI layer?

- Datalink layer
- Physical layer
- Network layer
- **Transport layer**

Unattempted

Transmission Control Protocol (TCP) operates at the Transport layer, or Layer 4 of the OSI model. Session hijacking occurs at the Transport layer.

7. Question

Which of the following describes a zero-day attack?

- **If a hacker manages to exploit the vulnerability before software developers can find a fix.**
- If a hacker attacks the system simultaneously without the victim knowing.
- If a hacker manages to exploit a known vulnerability
- If a hacker finds a lot of vulnerability in less than 24 hours.

Unattempted

A zero-day attack is an attack that exploits a potentially serious software security weakness that the vendor or developer may be unaware of. The software developer must rush to resolve the weakness as soon as it is discovered to limit the threat to software users.

8. Question

This type of jailbreaking allows user-level access and not iboot-level access?

- Bootrom Exploit
- **Userland Exploit**
- Sandbox Exploit
- iBoot Exploit

Unattempted

A userland exploit is a jailbreak that allows user-level access without iBoot-level access.

9. Question

Therese is a network administrator of a startup company that is setting up an e-commerce website. The company is concerned about a possible packet sniffing because credit card information will be sent electronically over the Internet. Customers will need to encrypt the data with HTTPS while visiting the site. Which type of certificate will be used to encrypt and decrypt the data?

- **Asymmetric**
- Confidential
- Non-confidential
- Symmetric

Unattempted

Asymmetric encryption also known as public-key encryption is used as a method of assuring the confidentiality, authenticity, and non-repudiation of electronic communications and data storage.

10. Question

Which of the following offers non-repudiation when it comes to sending communications online?

- Hearsay
- Date and Time
- **Digital signatures**
- Name of sender

Unattempted

Digital signatures can offer non-repudiation when it comes to online transactions, where it is crucial to ensure that a party to a contract or a communication can't deny the authenticity of their signature on a document or sending the communication in the first place.

11. Question

Which component of IPsec performs protocol-level functions that are required to encrypt and decrypt the packets?

- IPsec Policy Agent
- **Internet Key Exchange (IKE)**
- Oakley
- IPsec driver

Unattempted

Internet Key Exchange (IKE) is the protocol used to set up a secure, authenticated communications channel between two parties. IKE typically uses X. 509 PKI certificates for authentication and the Diffie–Hellman key exchange protocol to set up a shared session secret.

12. Question

Which of the following is not a PCI compliance recommendation?

- **Rotating employees handling credit card transactions on a yearly basis to different departments.**
- Using a firewall between the public network and the payment card data.
- Limiting access to card holder data to as few individuals as possible.
- Using encryption to protect all transmission of card holder data over any public network.

Unattempted

The 12 requirements of PCI DSS that must be complied with are:

1. Installing, maintaining, and configuring your firewall.
2. Avoid using default passwords and settings.
3. Protect the stored cardholders' information.
4. Encrypt transmission of cardholder data across open, public networks.
5. Scan and update antivirus software regularly.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder information by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder information.
10. Track and monitor all access to network resources and cardholder information.
11. Regularly conduct a vulnerability scan and do penetration testing
12. Maintain a policy that addresses information security.

13. Question

A security engineer is conducting an internal security audit and wants to know what ports are open on all the servers. What is the best way to find out?

- Scan servers with MBSA
- **Scan servers with Nmap**
- Physically go to each server
- Telnet to every port on each server

Unattempted

Nmap or network mapper is a powerful reconnaissance tool. It is a free, open-source Linux command-line tool that can be used to gather lots of information about the target. This program can be used in finding active hosts on a network, perform port scanning, ping sweeps, and, OS and version detection.

14. Question

This refers to a newly discovered vulnerability or flaw in a software application.

- Time-to-check to a time-to-use flaw
- HTTP header injection vulnerability
- **0-day vulnerability**
- Input validation flaw

Unattempted

A zero-day vulnerability (also referred to as Day Zero) is an attack that exploits a potentially serious software security weakness that the vendor or developer may be unaware of. The software developer must rush to resolve the weakness as soon as it is discovered to limit the threat to software users.

15. Question

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

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

Unattempted

A bollard is a short post used to create a protective or architectural perimeter. When installed primarily as a visual guide, they guide traffic and mark boundaries.

16. Question

Paul performs a scan on his company's network. He discovered that TCP port 123 is open. What services by default run on TCP port 123?

- Telnet
- **Network Time Protocol**
- POP3
- DNS

Unattempted

Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network. NTP runs on TCP/UDP port 123.

17. Question

This network security technique uses multiple layers of security controls to be placed throughout an IT infrastructure. This helps the organization improve its security posture against malicious attacks or potential

vulnerabilities.

- Host-Based Intrusion Detection System
- **Defense in depth**
- Security through obscurity
- Network-Based Intrusion Detection System

Unattempted

Defense in Depth (DiD) is a series of defensive mechanisms that are layered in order to protect valuable data and information. If one mechanism fails, another steps up immediately to thwart an attack. This multi-layered approach with intentional redundancies increases the security of a system as a whole and addresses many different attack vectors.

18. Question

An IS auditor found out during the security audit that the company has no documented security procedures. What should the IS auditor do?

- Terminate the audit
- Create a procedures document
- **Identify and evaluate existing practices**
- Conduct compliance testing

Unattempted

The IS auditor must evaluate the existing policies and practices to identify problem areas and opportunities.

19. Question

What is the result of the following command:

```
nmap -sS -O -p 123-153 192.168.111.107
```

- Stealth scan, opening port 123 and 153
- **Stealth scan, determine operating system, and scanning ports 123 to 153.**
- Stealth scan, checking open ports 123 to 153

Stealth scan, checking all open ports excluding ports 123 to 153

Unattempted

-sS = Stealth scanning

-O = Operating System (OS) checking

-p = Scan fewer ports

-p 123-153 = Scanning ports 123 to 153

20. Question

Which of the following uses an Advanced encryption standard (AES) algorithm?

Key discovery

Data integrity

Bulk data encryption

Key recovery

Unattempted

AES is a symmetric encryption algorithm ideal for encrypting data in bulk.

21. Question

Which of the following virus attempts to install itself inside the file it is infecting?

Tunneling virus

Polymorphic virus

Polymorphic virus

Cavity virus

Unattempted

Cavity virus known as spacefiller virus is a rare type of computer virus that installs itself by filling in empty sections of a file. By only using empty sections of a file, the virus can infect a file without the size of the file changing, making it more difficult to detect.

22. Question

Which of the following vulnerability usually exposes sensitive files, databases, and passwords on a windows file servers?

- Cross-site scripting
- CRLF injection
- **Missing patches**
- SQL injection

Unattempted

Patch management fixes vulnerabilities on your software and applications that are susceptible to cyber-attacks, helping your organization reduce its security risk.

23. Question

Xanwyll is a senior colleague of Theon in a large financial company. He sent an email to Theon regarding a contract with one of the company's clients. Theon was obliged to accept the offer. After 2 days, Xanwyll denies that he had ever sent an email to Theon. What must Theon know to prove that it was Xanwyll who sent the email?

- Confidentiality
- Authentication
- **Non-Repudiation**
- Integrity

Unattempted

Non-repudiation is the assurance that someone cannot deny the validity of something. It is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data. In other words, non-repudiation makes it very difficult to successfully deny who/where a message came from as well as the authenticity and integrity of that message.

24. Question

Angel, a network administrator, noticed an Intrusion Detection System (IDS) alert of a possible malicious sequence of packets sent to a web server in the network's external DMZ. The packet was captured by the IDS and saved to a PCAP file. What type of tool can be used to investigate the captured packet?

- Vulnerability scanner
- **Protocol analyzer**
- Protocol analyzer
- Network sniffer

Unattempted

A packet analyzer is also known as a network analyzer/protocol analyzer/packet sniffer is a computer program that can intercept and log traffic that passes over a digital network or part of a network. A packet analyzer can analyze packet traffic saved in a PCAP file.

25. Question

This is a tool in Metasploit that helps the penetration tester in evading Anti-virus Systems.

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

Unattempted

Msfencode is a Metasploit framework tool that alters the code in an executable so that it looks different from antivirus software but will still run the same way.

26. Question

Which of the following problems can be solved by using Wireshark?

- Resetting the administrator password on multiple systems.
- Checking creation dates on all webpages on a server.
- **Troubleshooting communication resets between two systems.**
- Tracking version changes of source code.

Unattempted

WireShark is a utility that can sniff the network traffic to identify or troubleshoot a communication issue or allow you to monitor the functionality of communication processes.

27. Question

In Trojan terminology, what is a covert channel?

- **Channel that transfers information within a computer system or network in a way that violates the security policy.**
- Kernel operation that hides boot processes and services to mask detection
- Legitimate communication path within a computer system or network for transfer of data.
- Reverse tunneling technique that uses HTTPS protocol instead of HTTP protocol to establish connections.

Unattempted

Internet covert channel is the digital equivalent of a briefcase with a secret compartment that a spy might use to slip sensitive documents past security guards into or out of a secure facility. An attacker can use Internet covert channels to transmit sensitive documents unobserved, bypassing network security measures.

28. 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.
- Both are asymmetric algorithms, but RSA uses 1024-bit keys.
- Both are asymmetric algorithms, but RSA uses 1024-bit keys.
- **RSA is asymmetric, which is used to create a public/private key pair; AES is symmetric, which is used to encrypt data.**

Unattempted

RSA uses asymmetric encryption while AES uses symmetric encryption.

29. Question

This is the simplest way of gaining unauthorized access to a targeted system or network rather than breaking it?

- Packet sniffing
- Port Scanning
- **Social engineering**
- Eavesdropping

Unattempted

Social engineering is an act of using an individual to compromise an information system or to give access to a sensitive resource. It exploits human psychology that aims to manipulate the victim into divulging confidential information in the interest of cybercriminals.

30. Question

Which of the following account authentications is/are supported by SSH-1 protocol but not SSH-2 protocol?

- [ ] **TIS authentication**
- [ ] **Rhosts (RSH-style) authentication**
- [ ] Password-based authentication
- [ ] **Kerberos authentication**

Unattempted

SSH-2 protocol supports Publickey, Hostbased, and Password-based authentication types. SSH-1 supports a wider range of account authentication types, including RSA only, RhostsRSA, Rhosts (RSH-style), TIS, and Kerberos authentication types.

31. Question

A student from SIA University approached the University's network administrator asking for advice on how to send encrypted email from home. The student can't afford any license fees or services. Which of the following is the most secure encryption protocol that the network administrator should recommend?

- Multipurpose Internet Mail Extensions (MIME)
- IP Security (IPSec)

- Hyper Text Transfer Protocol with Secure Socket Layer (HTTPS)
- **Pretty Good Privacy (PGP)**

Unattempted

Pretty Good Privacy (PGP) is a specific implementation of asymmetric encryption used for both sending encrypted emails and encrypting sensitive files.

32. Question

Why should the security analyst disable/remove unnecessary ISAPI filters?

- To protect against social engineering attacks
- **To protect against webserver attacks**
- To protect against wireless attacks
- To protect against jailbreaking

Unattempted

Removing unnecessary ISAPI filters can enhance the security and steadiness of a server.

33. Question

This tool can hide processes from the process list. It can also hide files, registry entries, and intercept keystrokes.

- DoS tool
- **RootKit**
- Scanner
- Trojan

Unattempted

Rootkit is a type of malicious software that is designed to remain hidden on your computer.

34. Question

This Bluetooth hacking technique is used by an attacker to send messages to victims without the recipient's consent. This technique is similar to email spamming.

- Bluesnarfing
- **Bluejacking**
- Bluesniffing
- Bluesmacking

Unattempted

Bluejacking is the sending of unsolicited messages, anonymously, over a Bluetooth connection.

35. Question

A botnet can be managed through which of the following?

- E-Mail
- Linkedin and Facebook
- **IRC**
- FTP server

Unattempted

Botnets often use IRC as a command-and-control framework because the source code is readily available.

36. Question

Which of the following is/are an example of passive reconnaissance?

- [ ] **Traceroute**
- [ ] **Nmap**
- [ ] Spyse
- [ ] **Ping**

Unattempted

Active reconnaissance is the opposite of passive reconnaissance wherein the information is gathered by directly engaging with the potential target. This may be done via manual testing or automated scanning using tools such as Nmap, ping, traceroute, and netcat.

37. Question

This type of attack happens by manipulating the targeted network so the attacker's host appears to be the desired destination.

- Evil Twin AP
- Cracking WEP key
- **Session Hijacking**
- Eavesdropping

Unattempted

Session hijacking is an attack where cybercriminals take over a current session after the user has established an authenticated session.

38. Question

This is an IDS evasion technique in which an attacker delivers data in multiple, small-sized packets to the target computer, making it very difficult to detect.

- **Session Splicing**
- TCP cutting
- Port Evasion
- Burp

Unattempted

The idea behind session splicing is to split data between several packets, making sure that no single packet matches any patterns within an IDS signature to avoid detection.

39. Question

Which of the following does not belong to the group?

- **Mixed honeypots**
- High-interaction honeypots
- Low-interaction honeypots

- Pure honeypots

Unattempted

Pure, low-interaction, and high-interaction are types of honeypot deployments.

40. Question

Which of the following is an example of an asymmetric encryption implementation?

- MD5
- **PGP**
- 3DES
- SHA1

Unattempted

Pretty Good Privacy (PGP) is a specific implementation of asymmetric encryption used for both sending encrypted emails and encrypting sensitive files.

41. Question

Passwords stored using specialized encryption algorithms are known as hashes. Which of the following is an advantage of this method?

- Passwords can be easily retrieved using the hash key stored by administrators.
- **User passwords stored using hashes are non-reversible.**
- Hashing is faster compared to other encryption algorithms.
- Hashed user passwords is impossible to crack unless the key used to encrypt them is obtained.

Unattempted

Hash functions are not reversible.

42. Question

This security defense strategy requires using several or layered varying methods to protect IT systems against malicious attacks.

- Covert channels
- Exponential backoff algorithm
- Three-way handshake
- **Defense in depth**

Unattempted

Defense in Depth (DiD) is a series of defensive mechanisms that are layered in order to protect valuable data and information. If one mechanism fails, another steps up immediately to thwart an attack. This multi-layered approach with intentional redundancies increases the security of a system as a whole and addresses many different attack vectors.

43. Question

Which of the following virus is usually targeting Microsoft Office products?

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

Unattempted

A macro virus is a computer virus written in the same macro language used for software programs, including Microsoft Excel or word processors such as Microsoft Word. When a macro virus infects a software application, it causes a sequence of actions to begin automatically when the application is opened.

44. Question

This serves as a primary service of the U.S. Computer Security Incident Response Team (CSIRT).

- A. To provide a computer security surveillance service and supply the government with important intelligence information on individuals traveling abroad.
- A. To provide a risk assessment service and assist law enforcement agencies to profile an individual's or company's asset.
- **A. To provide an IR service and enable a reliable and trusted single POC for reporting computer security incidents worldwide.**

A. To provide a pen testing service and support exception reporting on incidents worldwide by individuals and multi-national corporations.

Unattempted

CSIRT provides 24x7 Computer Security Incident Response Services to any user, company, government agency, or organization. CSIRT provides a reliable and trusted single point of contact for reporting computer security incidents worldwide. CSIRT provides the means for reporting incidents and for disseminating important incident-related information.

45. Question

Which of the following is also known as the Spacefiller virus?

Stealth virus

Tunneling virus

Which of the following is also known as the Spacefiller virus?

Polymorphic virus

Unattempted

Cavity virus known as spacefiller virus is a rare type of computer virus that installs itself by filling in empty sections of a file.

46. Question

Axl has successfully compromised a server on a network and opened a shell. He wants to identify all operating systems running on the network. Unfortunately, as he attempts to fingerprint all machines in the network using the nmap syntax below, it is not going through. What seems to be wrong in his syntax?

```
invictus@victim_server:~$ nmap -T4 -O 10.10.0.0/24
TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx
QUITTING!
```

The outgoing TCP/IP fingerprinting is blocked by the host firewall.

The Nmap syntax is wrong.

This is a common behavior for a corrupted Nmap application.

OS Scan requires root privileges.

Unattempted

The requested scan type requires root privileges.

47. Question

The act that states that all medical practices must ensure that all necessary measures are in place while saving, accessing, and sharing any electronic medical data to keep patient data secure.

COBIT

HIPAA

ISO/IEC 27002

FISMA

Unattempted

Health Insurance Portability and Accountability Act (HIPAA) is a 1996 legislation in the United States that protects patients' health information from being disclosed without their consent or knowledge. It regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities" (generally, health care clearinghouses, employer-sponsored health plans, health insurers, and medical service providers that engage in certain transactions.)

48. Question

This act mandated several reforms to improve corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud.

DMCA

HIPAA

SOX

GDPR

Unattempted

Sarbanes Oxley Act (SOX), also known as "Public Company Accounting Reform and Investor Protection Act" aims to protect investors and the public from accounting errors and fraudulent practices in enterprises by

enhancing corporate disclosures' accuracy and reliability. This act mandated several reforms to improve corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud.

49. Question

Which of the following type of attacks target DNS servers directly?

- DNS reverse connection
- **DNS reflector and amplification**
- DNS forward lookup
- DNS cache poisoning

Unattempted

The DNS reflector and amplification type attack the DNS servers directly. By adding amplification to the attack, many hosts send the attack and result in a denial-of-service to the DNS servers.

50. Question

Which of the following commands will start the Nessus client in the background so that the Nessus server can be configured on a Linux device.

- **nessus &**
- nessus +
- nessus *s
- nessus -d

Unattempted

In Linux, to start a process in the background you will use &.

51. Question

Paul a penetration tester from SIA Global Security compromised a server with an IP address of 10.10.0.6. Which of the following Nmap commands must he use to quickly list all the machines in the same network?

- **nmap -T4 -F 10.10.0.0/24**
- nmap -T4 -O 10.10.0.0/24

- nmap -T4 -q 10.10.0.0/24
- nmap -T4 -r 10.10.1.0/24

Unattempted

The command “nmap -T4 -F” is used to scan faster than a normal scan because it uses the aggressive timing template and scans fewer ports.

52. Question

What risk is present if a recent Nmap scan shows that port 69 is open?

- Weak SSL version
- **Unauthenticated access**
- Active mail relay
- Clear text authentication

Unattempted

Trivial File Transfer Protocol (TFTP) runs on port 69. TFTP allows transferring of files without authentication.

53. Question

Which of the following can mitigate the risk of sensitive data exposure? Choose all that applies.

- [ ] **Encrypting data at rest and in-transit.**
- [ ] Enabling cache.
- [ ] **Using transport layer security (TLS) protocol.**
- [ ] **Disabling cache.**

Unattempted

The risks of sensitive data exposure can be minimized by making sure that all data at rest and in-transit are well encrypted with strong, standard algorithms and uses up-to-date protocols such as transport layer security (TLS) with perfect forward secrecy (PFS) ciphers. Another way is to disable the caching or the process of storing data temporarily to speed up future requests.

54. Question

What web browser-based vulnerability allows a cybercriminal to manipulate users in performing actions they do not intend to such as making a fund transfer?

- Webform input validation
- **Cross-Site Request Forgery**
- Cross-Site Scripting
- Clickjacking

Unattempted

Cross-site request forgery, also known as CSRF is a type of malicious exploit that allows an attacker to trick users to perform actions that they do not intend to. Some examples are changing the email address and/or password, or making a funds transfer. Depending on the nature of the action, the attacker might be able to gain full control over the user's account.

55. Question

Principle of Least Privilege (PoLP) is a security concept that requires a user/employee to:

- Be trusted to keep all data and access to that data under their sole control.
- **Have limited to those functions required to do the job.**
- Be given root or administrative privileges.
- Be given privileges equal to everyone else in the department.

Unattempted

The principle of least privilege (PoLP) refers to an information security concept in which a user is given the minimum levels of access – or permissions – needed to perform his/her job functions.

56. Question

XYZ company wants to test its security infrastructure by hiring elite pen testers like you. During the interview, they asked you to show sample reports from previous penetration tests. What is the best approach to this?

- Share reports, after NDA is signed.
- **Decline but, provide references.**
- Share full reports with redactions

- Share full reports, not redacted.

Unattempted

Penetration test data done from previous clients should not be disclosed to third parties.

57. Question

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

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

Unattempted

A gray-box tester partially knows the internal structure, which includes access to the documentation of internal data structures as well as the algorithms used.

58. Question

Which of the following tools can be used as a network intrusion prevention and intrusion detection, record network activity, and function as a network sniffer?

- Nessus
- Nmap
- Cain and Abel
- **Snort**

Unattempted

Snort is an open-source intrusion prevention and detection system that aims to provide the most effective and comprehensive real-time network defense. It can be used as a packet sniffer, a packet logger, and a network file logging device.

59. Question

This Web Application security risk is defined as the failure of properly implementing all the security controls of a server or web application.

- Security Misconfiguration
- Sensitive Data Exposure
- Cross-site scripting Attack (XSS)
- Broken Authentication Attack

Unattempted

Security misconfiguration is the failure to properly implement all the security controls for a server or web application. This vulnerability allows the hacker to use the default username and password of the system, which may lead to a data breach.

60. Question

This type of malware restricts the user from accessing their computer system and demands that the user pay a certain amount of money to the cybercriminal to remove the restriction.

- Spyware
- Ransomware
- Riskware
- Adware

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.

61. Question

A penetration tester was able to sniff packets on a company's wireless network. Using the XOR, what was the original message?

Key = 10110010 01001011
Cyphertext = 01100101 01011010

- 11110010 01011011
- 00101000 11101110
- **11010111 00010001**
- 00001101 10100100

Unattempted

XOR (eXclusive OR) is a boolean logic operation that is widely used in cryptography. It is used in generating parity bits for error checking and fault tolerance. The output is True (or 1) if and only if the two inputs are different. The output is false (or 0) if the two inputs have the same value.

62. Question

This is an IDS evasion technique in which an attacker delivers data in multiple, small-sized packets to the target computer, making it very difficult to detect.

- **Session Splicing**
- Burp
- Port Evasion
- TCP cutting

Unattempted

The idea behind session splicing is to split data between several packets, making sure that no single packet matches any patterns within an IDS signature to avoid detection.

63. Question

Which of the following can be used as a basic vulnerability scanner which can cover several vectors such as FTP, SMB, and HTTP?

- SAINT scripting
- Metasploit scripting engine
- Nessus scripting engine
- **NMAP scripting engine**

Unattempted

The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It is designed for network discovery, version detection, backdoor detection, and vulnerability detection and exploitation.

64. Question

Where are passwords kept in Linux?

- /etc/passwd
- **/etc/shadow**
- /bin/shadow
- /bin/password

Unattempted

In Linux, passwords are stored in the /shadow file.

65. 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 15?

- **3072 bit key**
- 1536 bit key
- 1025 bit key
- 2048 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

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 →

Privacy Policy