SKILLCERTPRO
IT CERTIFICATION TRAININGS

0

Information Security / By SkillCertPro

Practice Set 13

Your results are here!! for" CEHv11 Practice Test 13 "

0 of 65 questions answered correctly

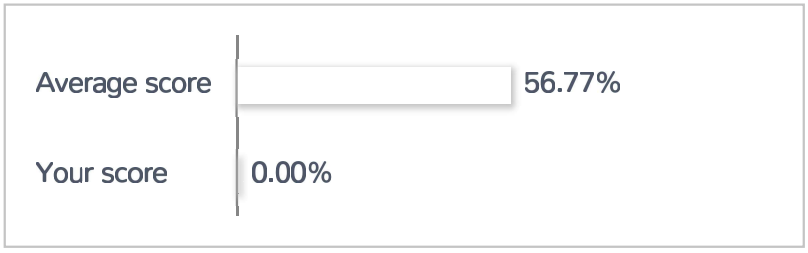
Your time: 00:00:01

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

A firewall is a software/hardware based system located at the network gateway that monitors and controls the traffic in the system. Which of the following firewalls can mitigate SQL injection attacks?

- Cloud firewall
- Packet filtering firewall
- **Web application firewall**
- Complete firewall

Unattempted

Web application firewall secures websites, web applications, and web services against known and unknown attacks such as SQL injection, path traversal, cross-site scripting, and others that result in web site defacement.

2. Question

You want to use NMAP to map domain names into IP addresses. Which of the following commands can make this possible?

- **>host -t a siaglobalsecurity.org**
- >host -t AXFR siaglobalsecurity.org
- >host -t ns siaglobalsecurity.org
- >host -t soa siaglobalsecurity.org

Unattempted

The A record is an Address record. It returns a 32-bit IPv4 address and is most commonly used to map hostnames to an IP address of the host.

3. Question

This command line switch can remotely detect the operating system of the targeted host.

- nmap -sS
- nmap -OS
- nmap -S
- **nmap -O**

Unattempted

-O is a command line switch used for OS detection in Nmap. For example, nmap -O 192.168.1.1.

4. Question

SIA Telco is planning for a company expansion this 2021. This big move will require their network to authenticate their users connecting via analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network. Which of the following AAA protocol should the chief network engineer implement?

- **RADIUS**
- TACACS+
- Kerberos
- DIAMETER

Unattempted

RADIUS is an AAA protocol that manages network access. RADIUS uses two packet types to manage the full AAA process: Access-Request, which manages authentication and authorization; and Accounting-Request, which manages accounting.

5. Question

It is an act that should be adhered to by anyone who handles any electronic medical data. This act states that all medical practices must ensure that all necessary measures in keeping the patients' medical information are in place.

- **Health Insurance Portability and Accountability Act (HIPAA)**

- Payment Card Industry Data Security Standard (PCI DSS)
- Fair and Accurate Credit Transactions Act (FACTA)
- Sarbanes-Oxley Act (SOX)

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.)

6. Question

An ethical hacker has successfully exploited a Linux server. The ethical hacker wants to make sure that outbound traffic from the server will not be detected by a Network-Based Intrusion Detection Systems (NIDS). Which of the following is the best way to avoid the NIDS?

- Protocol Isolation
- **Encryption**
- Use HTTP instead of HTTPS
- Steganography

Unattempted

NIDS is used to protect a system from network-based threats by monitoring and analyzing network traffic. When the traffic is encrypted, NIDS can only perform packet level analysis, since the contents in the application layer are inaccessible.

7. Question

Which of the following nmap commands should be used if a hacker wants to run a port scan on a web server but wants to lessen the amount of noise in order to evade IDS?

- nmap -sP -p
- **nmap -sT -O -T0**
- nmap -sS

map -A -Pn

Unattempted

-sT means TCP Connect scan

-O means Operating system (OS) detection

-T0 means Paranoid (0) Intrusion Detection System evasion

8. Question

Von is a security analyst from SIA Global Security. One of his tasks is to monitor and check the IDS logs. He noticed that an alert was triggered even though he found nothing malicious on a normal web application traffic. He can mark this alert as:

False Negative

True Negative

False Positive

True Positive

Unattempted

False positives are mislabeled security alerts. These alerts indicates that there is a threat when in reality no attack has taken place. For example, an alert was triggered indicating a brute force attack, but later on found out that it was just the user who mistyped the password a lot of times.

9. Question

Internet standards such as PGP, SSL, and IKE are all examples of which type of cryptography?

Public Key

Digest

Hash Algorithm

Secret Key

Unattempted

Public-key algorithms are fundamental security ingredients in cryptosystems, applications and protocols. They underpin various Internet standards, such as Secure Sockets Layer (SSL),Transport Layer Security (TLS), S/MIME, PGP, Internet Key Exchange (IKE or IKEv2), and GPG.

10. Question

It is a regulation that requires businesses to ensure the protection of personal data and privacy of European citizens.

- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Digital Millennium Copyright Act (DMCA)

Unattempted

General Data Protection Regulation or GDPR is a regulation that requires businesses to ensure the protection of personal data and privacy of European citizens. It establishes one law across the continent and a single set of rules which applies to companies doing business within EU member states.

11. Question

What are the three types of multi factor authentication?

- Something you are
- Something you have
- Something you remember
- Something you know

Unattempted

Multi-factor authentication (MFA) is a method of logon verification where at least two different factors of proof are required. The three authentication factors are: something you have, something you know, and something you are.

12. Question

Jen receives an unsuspicious email after accessing her bank account through a web browser. The email contains a very catchy image, and out of curiosity, she clicked it. She was then redirected to a website which shows an animated GIF of cat running around the park. After a few days, Jen noticed that all of her funds in her bank account was gone. Which of the following web browser-based security vulnerability got exploited by the hacker?

- Cross-Site Request Forgery
- Web Form Input Validation
- 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 perform. 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.

13. Question

Which of the following commands is used to find the number of hops to the target?

- Ping
- Curl
- Traceroute
- hping3

Unattempted

Traceroute is a network diagnostic command that displays the IP and hostname of the machines along the route taken by the packets.

14. Question

Which of the following best describes the role of the U.S. Computer Security Incident Response Team (CSIRT)?

- It registers critical penetration testing for the Department of Homeland Security and public and private sectors.
- It maintains, builds, and decommissions the nation's Internet infrastructure.
- It provides vulnerability assessments on behalf of the Department of Defense (DOD), and public and private sectors.

It provides incident response (IR) services to any user, company, government agency, or organization in partnership with the Department of Homeland Security.

Unattempted

Computer security incident response team or CSIRT's main responsibility is to expose and avert cyberattacks targeting an organization. It is important to have a security team that is solely focused on incident response (IR).

15. Question

Passive reconnaissance is the process of gathering information through which of the following?

- Network traffic sniffing
- Man in the middle attacks
- **Publicly accessible sources**
- Social engineering

Unattempted

Passive reconnaissance is the act of gathering information without alerting the potential victim. A hacker may use OSINT or Open Source Intelligence for gathering publicly available information of the targeted individual or organization.

16. Question

This tool is used on a Linux-based system as a passive wireless packet analyzer.

- Tshark
- Nessus
- Wireshark
- **Kismet**

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.

17. Question

Which of the following would you use in nmap if you want to perform a stealth scan?

- nmap -sT
- nmap -sC
- **nmap -sS**
- nmap -sU

Unattempted

#NAME?

18. Question

Upon getting unauthorized access to a Linux host, a hacker was able to steal the password file from /etc/passwd. What happens next?

- The hacker needs a key since the password file is encrypted.
- **Nothing. The stolen file does not contain any passwords.**
- The hacker uses the passwords for personal gain.
- Nothing. The password is encrypted.

Unattempted

The password file from /etc/passwd does not contain the passwords.

19. Question

This type of TCP scan is used to identify listening port by sending a series of packet with no set flags?

- **Null scan**
- Half scan
- Open scan
- Closed scan

Unattempted

Null scan is a type of scan that is used to identify listening TCP port. In a null scan, a series of packet is sent to a TCP port with zero bits or no flags set.

20. Question

Jane was hired as the Security Operation Center Analyst of SIA University. One of her tasks is to monitor all the incoming and outgoing traffic on SIA University's local network. Which of the following tool will help her in checking for suspicious activities and possible exploits in the network?

- Host-based Intrusion Detection System (HIDS)
- Intrusion Prevention System (IPS)
- Proxychains
- **Network-based Intrusion Detection System (NIDS)**

Unattempted

Network-based intrusion detection system (NIDS) is used to protect a system from network-based threats by monitoring and analyzing network traffic. NIDS scan all inbound packets and hunt for any suspicious patterns. When threats are discovered, the system takes action based on its severity. This includes notifying administrators, or blocking the source IP address from accessing the network.

21. Question

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

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

Unattempted

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

22. Question

What is the main difference between "Blind" SQL Injection to "Normal" SQL Injection vulnerability?

- The vulnerability is called "Blind" because it is still vulnerable to code injection even though the application properly filters the user input.
- **In Blind SQL Injection, the HTTP response of the vulnerable application such as the injection results and database errors is not visible to the attacker.**
- In normal SQL injection, the request to the web server is not shown to the administrator of the vulnerable application.
- In blind SQL injection, the successful attack does not show an error message to the administrator of the affected application.

Unattempted

Blind SQL injection is nearly identical to normal SQL injection, the only difference is the way the data is retrieved from the database.

23. Question

This program allows us to run more than one operating system (OS) inside our machine.

- **VirtualBox**
- Windows 10
- None of the Above
- Kali Linux

Unattempted

VirtualBox is a virtualization machine that will allow you to run more than one operating system (OS) inside a single machine. This is essential in ethical hacking when performing penetration testing in a virtual environment.

24. Question

Which of the following is the result of a NULL scan on an open port?

- **No response**
- FIN
- SYN

RST

Unattempted

Null scan is a type of scan that is used to identify listening TCP port. In a null scan, a series of packet is sent to a TCP port with zero bits or no flags set. If the target port is open, a null scan will result to a no response since the host will ignore the packet. If the target port is closed, it will respond a RST packet.

25. Question

Which of the following is designed to increase the confidentiality of information by implementing verification and authentication during a data exchange?

biometrics

single sign on

SOA

PKI

Unattempted

PKI or Public Key Infrastructure is a security architecture developed to increase secured transfer of information. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

26. Question

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

Nessus

Nmap

Snort

Cain and Abel

Unattempted

Snort is an open source intrusion prevention and detection system which 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.

27. Question

This act requires the standard national numbers of employers to be identified on standard transactions.

- Sarbanes-Oxley Act (SOX)
- Fair and Accurate Credit Transactions Act (FACTA)
- **Health Insurance Portability and Accountability Act (HIPAA)**
- Payment Card Industry Data Security Standard (PCI DSS)

Unattempted

Health Insurance Portability and Accountability Act (HIPAA) requires that employers have standard national numbers that identify them on standard transactions.

28. Question

Hashing algorithm is an algorithm developed by the National Institute of Standards and Technology to generate cryptographically secure one-way hash. Which of the following is being described?

- SSL
- **MD5**
- IKE
- PGP

Unattempted

Message Digest Algorithm 5 also known as MD5 is a cryptographic hash algorithm that can be used to create a 128-bit string value from an arbitrary length string.

29. Question

This can be simply defined as the collection publicly available information:

- Social intelligence
- Human intelligence
- Real intelligence

Open-source intelligence

Unattempted

OSINT or Open-source intelligence refers to any available information that can be accessed from free public sources such as the internet.

30. Question

Angel is the current Chief Security Officer at SIA University. During their meeting with a Security consultant, Angel explains that there might be a conflict with their existing security controls. She discussed that their Network Administrator is the only one responsible for the approval and issuance of RFID card access to their server room, and monitoring/reviewing the weekly access logs. SIA University is currently facing which of the following issue?

Overworked employee

Lack of working experience

Poor employee utilization

Segregation of Duties

Unattempted

The concept of delegating more than one person to complete a task is called Separation of duties. Separation of duties, also known as Segregation of duties has two primary goal. First is to prevent the conflict of interest, and reduce the risk of unauthorized access and fraudulent activity. Second is to identify and mitigate control failures such as security breaches, information theft and circumvention of security controls.

31. Question

This tool is used for checking network vulnerabilities and compliance assessment.

Nessus

Hashcat

Wireshark

Network Mapping

Unattempted

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

32. Question

It is an act of gathering information without engaging with the system or the individual itself.

- None of the Above
- Network Mapping
- **Passive Reconnaissance**
- Active Reconnaissance

Unattempted

Passive reconnaissance is the process of gaining valuable information without being noticed by the potential victim. It is also an act of gathering information without engaging with the system or the individual

33. Question

A start-up company hired a penetration tester to conduct a security audit on their network. Upon investigating, it was discovered that a breach to the company's network had happened a lot of times because the IDS is not configured properly. This is why no alarms were triggered during the attack. What type of alert is the IDS giving?

- False Positive
- **False Negative**
- True Positive
- True Negative

Unattempted

False negative happens when no alarm was raised even though an attack has taken place.

34. Question

Which of the following command line switches in Nmap is used for detecting operating system?

- **#NAME?**
- #NAME?
- #NAME?
- #NAME?

Unattempted

-O is a command line switch used for OS detection in Nmap. For example, nmap -O 192.168.1.1.

35. Question

Jane is a network security officer at SIA Global Security. She has a machine installed with a snort and another machine installed with kiwi Syslog. She performed a SYN scan and wants to check if the messages sent from the snort machine (10.172.0.18) are received by the kiwi Syslog machine (10.172.0.150). What Wireshark filter will show that there is a connection between the two machines?

- tcp.srcport==514 && ip.src==10.172.0.150
- tcp.srcport==514 && ip.src==10.172.0.18
- **tcp.dstport==514 && ip.dst==10.172.0.150**
- tcp.dstport==514 && ip.dst==10.172.0.0/24

Unattempted

To check the connections between two machines, the destination port at destination IP must be configured. The destination IP is 10.172.0.150, where the kiwi Syslog is installed.

36. Question

This standard is associated with the credit card industry?

- Health Insurance Portability and Accountability Act (HIPAA)
- Control Objectives for Information and Related Technology (COBIT)
- **Payment Card Industry Data Security Standards (PCI DSS)**
- Sarbanes-Oxley Act (SOX)

Unattempted

Payment Card Industry Data Security Standard (PCI DSS) is a global information security standard by "PCI Security Standards Council" that handles cardholders' data for debit, credit, prepaid, e-purse, ATM, and POS cards. This offers a comprehensive and robust standard and supporting materials to improve payment card information security. This include an outline of specifications, tools, measurements, and support resources to help organizations protect the cardholder's information.

37. Question

This is a powerful framework commonly used by ethical hackers in performing automated attacks on a network in order to check its security vulnerabilities.

- Hashcat
- **Metasploit**
- Maltego
- Bruteforce

Unattempted

Metasploit framework is a very powerful tool which can be used by penetration testers to check vulnerabilities on networks and servers. It provides exploits, payloads, auxiliary functions, encoders, listeners, shellcode, post-exploitation code and nops.

38. Question

Which of the following is/are an example(s) of a Botnet? (Select all that apply.)

- Stuxnet
- **Lemon Duck**
- **Mirai**
- **Prometei**

Unattempted

Botnets are used to carry out malicious activities such as account credential leakage, unauthorized access and clicking of ads, sending spam emails, and participating in a DDoS (Distributed Denial of Service) attacks. Some of the most familiar examples of a botnets are mirai, lemon duck, and prometei.

39. Question

Which type of SQL injection attack is being used if the attacker uses the command:

- SELECT*FROM user WHERE name = 'Angelica' AND UserID IS NULL; --';
- **End of line comment**
- Tautology
- Incorrect query
- Logical query

Unattempted

In this type of SQL Injection Attack, the cybercriminal uses SQL comment operator "- – " to ignore part from SQL query search.

40. Question

Which of the following algorithm was tagged as useless way back in 2007, after discovering that the passkeys can be easily uncovered in less than a minute?

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

Unattempted

WEP or Wired Equivalent Privacy is currently the most widely used Wi-Fi security protocol for securing 802.11 networks. In 2007, a new attack on WEP, the PTW attack, was discovered, which allows an attacker to recover the secret key in less than 60 seconds in some cases.

41. Question

Which of the following best describes Code injection?

- Code injection is a form of cyberattack where the cybercriminal gains access to the server and adds a new code.

Code injection is a form of cyberattack where the cybercriminal commands the server to perform a buffer overflow.

Code injection is a form of cyberattack where the cybercriminal injects malicious data into the code interpreter.

Code injection is a form of cyberattack where the cybercriminal injects additional javascript code running on the website.

Unattempted

Injection flaws are commonly found in SQL, LDAP, XPath, NoSQL, OS commands, XML parsers, SMTP headers, expression languages (EL), and Object Relational Mapping (ORM) queries.
The hacker injects malicious SQL code or query into the user input form to manipulate and control the database, allowing them to access and delete modify information and change other applications' behavior.

42. Question

The goal of this type of malware is not to steal confidential information, but rather, to restrict the user from using the system.

Denial of Service

Ransomware

Virus

Trojan

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.

43. Question

You were hired to do a web application security test. You noticed that the site is dynamic and must make use of a back end database. In order to check if SQL injection is possible, what is the first character that you should use to attempt breaking a valid SQL request?

Semicolon

Double quote

- Single quote
- Backlash

Unattempted

Injection attacks can be prevented by doing a source code validation or review. This will allow you to determine the injection flaws and mitigate them before deploying the code into production.

44. Question

This tool performs comprehensive tests against web servers, including potentially dangerous files/programs, and version specific problems.

- Nikto
- Dsniff
- John the Ripper
- Snort

Unattempted

Nikto is an Open Source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software.

45. Question

This type of malware can remain dormant in a victim's computer and will trigger only when the programmed condition is met.

- Botnet
- Ransomware
- Trojan
- Logic Bomb

Unattempted

A logic bomb is a malicious program that has been inserted into the victims' computer network, operating system, or software application. Unlike other malware attacks, logic bombs can remain dormant in a victims' computer unless the programmed condition that will trigger it is met.

46. Question

Which of the following refers to the group of hijacked or infected computers, servers, mobile, and IoT devices that is being controlled by a hacker.

- Trojan
- Virus
- Logic Bomb
- **Botnet**

Unattempted

Botnet refers to the group of hijacked or infected computers, servers, mobile devices, and IoT (Internet of Things) devices that are being controlled by a hacker. Botnets are used to carry out malicious activities such as account credential leakage, unauthorized access and clicking of ads, sending spam emails, and participating in a DDoS (Distributed Denial of Service) attacks.

47. Question

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

- **Kismet**
- Netstumbler
- Abel
- Nessus

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.

48. Question

This is an environment where we can practice ethical hacking without the fear of compromising a legitimate network.

- Sand environment
- Practice Environment
- Safe Environment
- **Sandboxed Environment**

Unattempted

Sandboxed environment, also known as hacking environment, is where we can practice and explore a variety of hacking techniques without compromising other legitimate systems or networks.

49. Question

Jane, a freelance CEH, is bidding for a security audit contract on a large company. This job contract involves penetration testing and reporting. The company is asking for a proof of work so Jane prints out several audits that she has performed from other companies. Which of the following is likely to occur?

- The company will ask the same type of format of testing.
- **Jane may expose the vulnerabilities of her previous company.**
- Jane will ask for above average payment on the bid because of her great work.
- The company will hire Jane because of her previous experiences.

Unattempted

Ethical hackers must maintain the confidentiality of a sensitive data. Do not disclose any sensitive information obtained from your ethical hacking to other third parties unless authorized by the owner.

50. Question

Which of the following command line switches in Nmap is used for scanning fewer ports.

- #NAME?
- #NAME?
- **#NAME?**

- #NAME?

Unattempted

-P command line switch is used for scanning fewer ports other than the default scanning using Nmap tool. For example, nmap -p 80 192.168.1.1 will scan port 80.

51. Question

Which of the following is an architectural pattern that aims to provide application functionality as services to other applications?

- Object Oriented Architecture
- Lean Development
- **Service Oriented Architecture (SOA)**
- Agile Software Development

Unattempted

A service-oriented architecture (SOA) is an architectural pattern in computer software design in which application components provide services to other components via a communications protocol, typically over a network.

52. Question

Which of the following DNS record types can specify how long does a DNS poisoning will last?

- Name Server (NS)
- Pointer (PTR)
- **Start of Authority (SOA)**
- Address Record (A)

Unattempted

The Start of Authority (SOA) record stores important information about a domain or zone such as the primary name server of the domain, the email address of the admin, the last update of domain, the time the server should wait before the refresh.

53. Question

As an ethical hacker, you are tasked to perform a penetration test in XY company. While performing the first step, which is the information gathering, you found the list of employees along with their emails posted on the internet. Using an email spoofing technique, you sent an email to one of the employees while pretending to be his supervisor. In this email you asked him to open the pdf links and print it. Believing you were his supervisor, he read your email and opens the malicious link which infected his machine. What testing method was used in this attack?

- Social Engineering
- Tailgating
- Eavesdropping
- Piggybacking

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.

54. Question

It is an adaptive SQL Injection testing technique that is used to identify coding errors and security loopholes by inputting huge amounts of random data against the targeted application.

- Fuzz testing
- Dynamic testing
- Function testing
- Static testing

Unattempted

Fuzz testing is a quality and assurance checking technique that is used to identify coding errors and security loopholes in a targeted web applications. Huge amounts of random data called 'Fuzz' will be generated by the fuzz testing tools (Fuzzers) and be used against the target web application to discover vulnerabilities that can be exploited by various attacks.

55. Question

Which of the following keys are shared during the process of encryption and decryption?

- Owner's keys
- Private keys
- Public and private keys
- **Public keys**

Unattempted

In asymmetric key system, public keys are shared or available to anyone, while private keys are held only by the key owner.

56. Question

This is a form of Penetration Testing or Ethical Hacking which relies on exploiting human psychology to manipulate the victim into divulging confidential information in the interest of cybercriminals.

- Piggybacking
- Tailgating
- Eavesdropping
- **Social Engineering**

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.

57. Question

Which of the following statements best describes Social Engineering?

- Social Engineering is the practice of studying sociology.
- Social Engineering is a technique of disclosing information publicly.
- **Social Engineering is an act of using an individual to gather sensitive information without breaking into the system.**
- Social Engineering is used to perform time accounting.

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.

58. Question

It is the process of identifying, analyzing, prioritizing, and resolving security events in an organization.

- Service Level Agreement
- Incident Metrics
- Security Policy
- **Incident Management Process**

Unattempted

Incident management is a set of defined processes to identify, analyze, prioritize, and resolve security incidents to restore and prevent further damage in service operations.

59. Question

Which of the following is used to indicate a single-line or nested comment in structured query language (SQL)?

- –
- %%
- '
- ||

Unattempted

SQL Comment uses the two hyphens (–) for single-line or nested comments. Comments inserted with –– are terminated by a new line, which is specified with a carriage return.

60. Question

Which type of hackers are often referred to as the "good guys" or those who exploit security vulnerabilities for the benefit of the company?

- Yellow Hat Hacker
- **White Hat Hacker**
- Grey Hat Hacker
- Black Hat Hacker

Unattempted

White hat hackers or "the good guys" are often referred to as ethical hackers. They are authorized persons or individuals specializing in ethical hacking tools, techniques, and methodologies to strengthen an organization's information systems.

61. Question

Bluetooth uses which of the following digital modulation technique to exchange information between paired devices?

- **Phase-shift keying (PSK)**
- Amplitude-shift keying (ASK)
- Quadrature amplitude modulation (QAM)
- Frequency-shift keying (FSK)

Unattempted

Phase shift keying is the form of Bluetooth modulation used to enable the higher data rates achievable with Bluetooth 2 EDR (Enhanced Data Rate). Two forms of PSK are used: /4 DQPSK, and 8DPSK

62. Question

A network administrator uncovers several unfamiliar files such as a tarball and nc files in the root directory of his Linux FTP server. Upon further checking, the FTP server's access logs show that an anonymous user was able to log in to the server, uploaded the unfamiliar 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 a process, and the netstat command shows that the nc process is listening on a network port. What kind of vulnerability made this remote attack possible?

- **File system permissions**
- Privilege escalation

- Brute force login
- Directory traversal

Unattempted

To upload files the user must have proper write file permissions.

63. Question

Which of the following is/are not passive reconnaissance tools? Choose all that applies.

- Wireshark
- **Nmap**
- The Harvester
- Shodan

Unattempted

Nmap is a powerful active reconnaissance tool. This tool can be used to gather lots of information about the target. Let's see how we can use Nmap in our favor.

64. Question

A future client wants to see sample reports from previous penetration tests. What should you do next?

- Share full reports with redactions.
- Share full reports, not redacted.
- Share reports, after NDA is signed.
- **Decline but, provide references.**

Unattempted

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

65. Question

The amount of risk that remains after all the countermeasures have been exhausted is called?

- Impact Risk

- Inherent Risk
- **Residual Risk**
- Deferred Risk

Unattempted

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

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 →

CONTACT FORM

Important Links

REFUND POLICY

REFUND REQUEST

TERMS & CONDITIONS

PRIVACY POLICY

Privacy Policy