SKILLCERTPRO
IT CERTIFICATION TRAININGS

0

Information Security / By SkillCertPro

Practice Set 20

Your results are here!! for" CEHv11 Practice Test 20 "

0 of 65 questions answered correctly

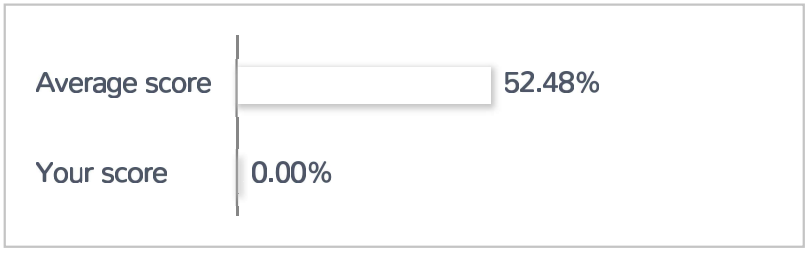
Your time: 00:00:02

Your Final Score is : 0

You have attempted : 0

Number of Correct Questions : 0 and scored 0

Number of Incorrect Questions : 0 and Negative marks 0



You can review your answers by clicking view questions.

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

Restart Test | View Answers

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

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

Correct Incorrect

Review Question Summary

1. Question

Which of the following attack is possible if a token and a 4-digit personal identification number (PIN) are used to access a computer system? The token performs off-line checking for the correct PIN.

- Brute force
- Smurf
- Man-in-the-middle
- Birthday

Unattempted

In a brute force attack, cybercriminals try every combination of characters until the password is broken. Even though all passwords will be found, this attack is very time-consuming.

2. Question

Just right after your lunch break, you received a suspicious email in your inbox. You are familiar with the sender but the subject line has strange characters in it. What is the best approach to this situation?

- Forward the email to your company's IT team and permanently delete the email.
- Reply to the sender and ask what is the email all about.
- Forward the email to your supervisor and ask how to handle the situation.
- Immediately delete the email and pretend that it never happened.

Unattempted

Forward the email to your IT/Security team so they can further investigate the email. Permanently delete the email to avoid possible damages.

3. Question

A large financial company recently requires its employees to perform file transfers using protocols that encrypts traffic. As a security analyst, you suspect that some of the employees are still performing file transfers using unencrypted protocols. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wire shark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

- tcp.port != 21
- tcp.port = 23
- **tcp.port ==21 || tcp.port ==22**
- tcp.port ==21

Unattempted

Wireshark filter “tcp.port ==21 || tcp.port ==22” will show traffic from ports 21 and 22 which is used for FTP.

4. Question

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

- Data integrity
- Key recovery
- Key discovery
- **Bulk data encryption**

Unattempted

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

5. Question

Which of the following statements describe an anomaly-based IDS?

- Cannot deal with encrypted network traffic
- Requires vendor updates for a new threat
- Produces fewer false positives

Can identify unknown attacks

Unattempted

Unlike signature-based IDS which can only detect known attacks for which a signature has previously been created, anomaly-based IDS can identify unknown attacks.

6. Question

Brian discovered an active server that is currently in the same network as the machine he recently exploited. He pings it but it did not respond. What could be the main issue?

The ARP is disabled on the target server.

The TCP/IP does not support ICMP.

The ping command requires root privileges

The ICMP is disabled on the target server

Unattempted

The ping command sends an ICMP echo request to a device on the network, and the device immediately responds with an ICMP echo reply. If there was no response after the ping, the ICMP may be disabled on the target server.

7. Question

This act addresses the rights and obligations of owners of copyrighted material who believe their rights under U.S. copyright law have been infringed, particularly but not limited to, on the Internet. It also addresses the rights and obligations of OSP / ISP (Internet Service Providers) on whose servers or networks the infringing material may be found.

SOX

HIPAA

GDPR

DMCA

Unattempted

The Digital Millennium Copyright Act or DMCA is a 1998 United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization. It penalizes the production and dissemination

of technology, devices, or services intended to circumvent measures that control access to copyrighted works.

8. Question

This is described as “Attempting an injection attack on a web server based on responses to True/False questions “

- Classic SQLi
- Compound SQLi
- **Blind SQLi**
- DMS-specific SQLi

Unattempted

Blind SQL (Structured Query Language) injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the application’s response. This attack is often used when the web application is configured to show generic error messages but has not mitigated the code that is vulnerable to SQL injection.

9. Question

In the context of Windows Security, what is a ‘null’ user?

- A pseudo account that was created for security administration purpose
- **A pseudo account that has no username and password**
- An account that has been suspended by the admin
- A user that has no skills

Unattempted

A null user is an account that has no username and password.

10. Question

Which of the following biometrics scan measures the geometry of the face through a digital video camera?

- **Facial recognition scan**

- Retinal scan
- Iris scan
- Signature kinetics 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.

11. Question

You want to evaluate several plain-text firewall logs that faster than usual. To do efficient searches of the logs you must use regular expressions. Which command-line utility are you most likely to use?

- Relational Database
- Notepad
- MS Excel
- **Grep**

Unattempted

Grep is a command-line utility for searching plain-text data sets for lines that match a regular expression.

12. Question

A recently hired SOC Analyst is searching for ways on how to mitigating Cross-site Scripting (XSS) flaws. Which advice can you give to the new SOC Analyst?

- Verify access right before allowing access to protected information and UI controls.
- **Validate and escape all information sent to a server.**
- Use digital certificates to authenticate a server before sending data.
- Verify access right before allowing access to protected information and UI controls.

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.

13. Question

This organization specifies the requirements for launching, instigating, keeping, and continually improving an organization's information security management system.

- SOX
- OWASP
- **ISO/IEC 27001**
- GDPR

Unattempted

International Organization for Standardization and International Electro-Technical Commission or ISO/IEC 27001:2013 specifies the requirements for launching, instigating, keeping, and continually improving an organization's information security management system. It also includes the requirements needed to assess and treat data security risks tailored to the organization's needs.

14. Question

This malicious software is designed to give continued, privileged access to a hacker over a host computer or a system while remaining undetected or hidden.

- Emotet
- Exploit
- Botnet
- **Rootkit**

Unattempted

A rootkit is a malicious software designed to give continued, privileged access to a hacker over a host computer or a system while remaining undetected or hidden. Once the rootkit has been installed, it will allow the hacker to remotely execute files as well as change the system configurations on the computer. This can give hackers easy access to the host computer and make it easy for them to steal the user's personal information.

15. Question

In this phase, the ethical hacker deletes all the traces of ethical hacking.

- Clearing and covering tracks
- Footprinting
- Scanning
- Enumeration

Unattempted

The last phase of ethical hacking is clearing and covering tracks. In this phase, the hacker will take all the necessary steps to delete and hide any hacking traces to avoid detection by the user or IT security personnel to avoid legal action.

16. Question

While conducting a Black box penetration testing via the TCP port (80), you noticed that the traffic gets blocked when you try to pass IRC traffic from a web enabled host. Upon further checking, you found out that outbound HTTP traffic is being allowed. What type of firewall is being utilized for the outbound traffic?

- Application
- Circuit
- Packet Filtering
- Stateful

Unattempted

An application firewall is an enhanced firewall that limits access by applications to the operating system (OS) of a computer. Conventional firewalls merely control the flow of data to and from the central processing unit (CPU), examining each packet and determining whether or not to forward it toward a particular destination. An application firewall offers additional protection by controlling the execution of files or the handling of data by specific applications.

17. Question

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

- single sign-on
- PKI

- biometrics
- SOA

Unattempted

PKI or Public Key Infrastructure is a security architecture developed to increase the 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.

18. Question

TCP/IP session hijacking is carried out in which of the following OSI layer?

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

Unattempted

TCP operates at the Transport layer or Layer 4 of the OSI model. TCP/IP session hijack occurs at the Transport layer.

19. Question

Which type of firewall only monitors TCP handshaking of packets at the session layer of the OSI model?

- Application-level firewall
- Stateful multilayer inspection firewall
- packet filtering firewall
- **circuit-level gateway firewall**

Unattempted

A circuit-level gateway is a firewall that provides User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) connection security and works between an Open Systems Interconnection (OSI) network model's transport and application layers such as the session layer. Unlike application gateways, circuit-level gateways monitor TCP data packet handshaking and session fulfillment of firewall rules and policies.

20. Question

Which of the following biometrics scan measures the unique fold of thread like muscles in the iris?

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

21. Question

This is a type of malware that self-replicates by copying itself into another program or file with the help of human interaction.

- Trojan
- **Virus**
- Worms

Unattempted

A virus is a type of malware that self-replicates by copying itself into another program or file with the help of human interaction. It is designed to delete or corrupt programs and files, slow down the machine, and infect other computers connected to the same network.

22. Question

This process can determine the possible effects when some of the company's critical business processes suddenly stop.

- Risk Mitigation
- **Business Impact Analysis (BIA)**
- Disaster Recovery Planning (DRP)

Emergency Plan Response (EPR)

Unattempted

A business impact analysis (BIA) predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies. Potential loss scenarios should be identified during a risk assessment.

23. Question

Which of the following best describes a Suicide hacker.

Someone who hacks just because they can.

Someone who hacks for a purpose and doesn't bother suffering imprisonment.

Someone who hacks for the safety of the company.

Someone who hacks in exchange of money.

Unattempted

Suicide hackers are those who hack for some purpose and even don't bother to suffer long-term jail due to their activities.

24. Question

Which of the following cryptography attack is an understatement for the extraction of cryptographic secrets (e.g. the password to an encrypted file) from a person by coercion or torture?

Ciphertext-only Attack

Chosen-Cipher text Attack

Timing Attack

Rubber Hose Attack

Unattempted

The rubber hose attack is extracting secrets from people by use of torture or coercion.

25. Question

This is considered the best way to protect Personally Identifiable Information (PII) from Web application vulnerabilities?

- **Using cryptographic storage to store all Personally Identifiable Information (PII)**
- Using encrypted communications protocols to transmit Personally Identifiable Information (PII)
- Using full disk encryption on all hard drives to protect Personally Identifiable Information (PII)
- Using a security token to log into all Web applications that use Personally Identifiable Information (PII)

Unattempted

It is a best practice that any Personally Identifiable Information (PII) must be encrypted

26. Question

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

- Curl
- **Traceroute**
- hping3
- Ping

Unattempted

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

27. Question

Which protocol will allow you to guess a sequence number when you are attempting to man-in-the-middle a session?

- UPD
- **TCP**
- ICMP
- UPX

Unattempted

To establish a TCP session, the client starts by sending a SYN packet with a sequence number. To hijack the session, it is required to send a packet with the right sequence number, otherwise, they are dropped.

28. Question

A compromised system is sometimes referred to as:

- Zombie Army
- Zombie
- Botnet
- **Zombie System**

Unattempted

The compromised system is sometimes referred to as a zombie system. It is called a zombie system because the computer's legitimate owner is unaware that the machine has already been compromised.

29. Question

Which of the following Web Application security risks happens when a certain application fails to secure the stored or in-transit user credentials against hackers.

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

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.

30. Question

This protocol is specifically designed for transporting event messages?

- SNMP

- SYSLOG
- ICMP
- SMS

Unattempted

Syslog or System Logging Protocol is a standard for message logging. It is a standard for sending and receiving notification messages from various network devices. The messages include time stamps, event messages, severity, host IP addresses, diagnostics, and more. Syslog was designed to monitor network devices and systems to send out notification messages if there are any issues with functioning. It also sends out alerts for pre-notified events and monitors suspicious activity via the change log/event log of participating network devices.

31. Question

A malicious software that 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.

- Ransomware
- Spyware
- Firmware
- 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.

32. Question

Incident management refers to logging, recording, and resolving events promptly. (True/False)

- FALSE
- TRUE

Unattempted

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

33. Question

What term is used in serving different types of web pages based on the user's IP address?

- **Website cloaking**
- IP access blockade
- Website filtering
- Mirroring website

Unattempted

Website cloaking is serving different web pages based on the source IP address of the user.

34. Question

This architecture is designed to verify and authenticate individuals taking part in a data exchange within an enterprise?

- Single-Sign-On
- Biometrics
- **Public Key Infrastructure (PKI)**
- Service Oriented Architecture (SOA)

Unattempted

PKI or Public Key Infrastructure is a security architecture developed to increase the 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.

35. Question

Which of the following options is the most secure way for storing backup tapes?

- It must be stored inside the data center for faster retrieval in a fireproof safe.
- **It must be stored in a climate-controlled facility offsite.**

- It must be stored in a cool dry environment
- It must be stored on a different floor in the same building.

Unattempted

An effective disaster data recovery strategy should consist of producing backup tapes and housing them in an offsite storage facility. This way the data isn't compromised if a natural disaster affects the business' office. It is highly recommended that the backup tapes be handled properly and stored in a secure, climate-controlled facility. This provides peace of mind and gives the business almost immediate stability after a disaster.

36. Question

Which of the following does not belong to the group?

- **Terminating**
- Footprinting
- Gaining Access
- Scanning

Unattempted

Phases of Ethical Hacking

1. Reconnaissance
2. Scanning and Enumeration
3. Gaining Access
4. Maintaining Access
5. Clearing and Covering Tracks

37. Question

Which of the following cipher encrypts the plain text digit (bit or byte) one by one?

- **Stream cipher**
- Modern cipher
- Block cipher
- Classical cipher

Unattempted

Stream ciphers are a type of encryption algorithm that processes an individual bit, byte, or character of plaintext at a time. Stream ciphers are often faster than block ciphers in hardware and require less complex circuitry.

38. Question

This virus tries to hide from antivirus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

- Cavity virus
- Tunneling virus
- Polymorphic virus
- **Stealth virus**

Unattempted

A stealth virus contains sophisticated means of avoiding antivirus detection software. After it manages to get into the now-infected machine a stealth virus hides by continually renaming and moving around the disc.

39. Question

In Wireshark, the packet bytes panes show the data of the current packet in which format?

- **Hexadecimal**
- ASCII only
- Binary
- Decimal

Unattempted

The packet bytes pane shows the data of the current packet in a hexdump style. Each line contains the data offset, sixteen hexadecimal bytes, and sixteen ASCII bytes.

40. Question

Which of the following statements is NOT true about ethical hacking?

- Ethical hacking should not involve writing to or modifying the target systems.
- Hire ethical hackers who do not sell vendor hardware/software or other consulting services.
- **Ethical hackers are not allowed to use any tools or methods that can exploit the vulnerabilities in an organization's systems.**
- Testing should be remotely performed offsite.

Unattempted

Ethical hackers use the same tools and methods done by cybercriminals. It includes methods that can exploit the system's vulnerabilities.

41. Question

Which of the following is the best approach for checking vulnerabilities on a Windows-based computer?

- Utilizing the built-in Windows Update tool
- Checking MITRE.org for the latest list of CVE findings
- **Using a scan tool such as Nessus**
- Creating a disk image of a clean Windows installation

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

42. Question

Every morning, the first thing that you do is check your email inbox. One morning, you received an email from a known person but the subject line is unusual. What is the best approach to this situation?

- Reply to the sender and ask what is the email all about.
- Immediately delete the email and pretend that it never happened.
- **Forward the email to your company's IT team and permanently delete the email.**
- Forward the email to your supervisor and ask how to handle the situation.

Unattempted

Forward the email to your IT/Security team so they can further investigate the email. Permanently delete the email to avoid possible damages.

43. Question

An ISP or Internet Service Provider needs to authenticate users connecting using 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 is most likely able to handle this requirement?

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

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 manage accounting.

44. Question

What type of jailbreaking is a userland exploit?

- Allows user-level access and iboot-level access.
- **Allows user-level access and not iboot-level access.**
- Allows access to the filesystem, iBoot, and NOR access.

Unattempted

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

45. Question

A type of penetration testing where the tester has no prior knowledge of the internal IT system.

- **Black box testing**

- Gray box testing
- Red box testing
- White box testing

Unattempted

A black-box tester is unaware of the internal structure of the application to be tested, while a white-box tester has access to the internal structure of the application. 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.

46. Question

Using a fingerprint and a PIN as a two-factor authentication satisfies which of the following?

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

Unattempted

Fingerprint = Something you are

PIN = Something you know

47. Question

This device is capable of searching for and locating rogue access points?

- HIDS
- NIDS
- **WIPS**
- WISS

Unattempted

A wireless intrusion prevention system (WIPS) is a dedicated security device or integrated software application that monitors a wireless LAN network's radio spectrum for rogue access points and other

wireless threats.

48. Question

What is the correct PCAP filter to capture all TCP traffic going to or from host 192.168.0.125 on port 25?

- tcp.src == 25 and ip.host == 192.168.0.125
- **tcp.port == 25 and ip.host == 192.168.0.125**
- port 25 and host 192.168.0.125
- host 192.168.0.125:25

Unattempted

The destination host and IP host must be configured.

49. Question

This is a legally binding contract that establishes a confidential relationship between the parties signing the agreement. This may also be referred to as a confidentiality agreement.

- Terms of Engagement
- **Non-disclosure Agreement**
- Contract
- Rules of Engagement

Unattempted

A non-disclosure agreement is a legally binding contract that establishes a confidential relationship. The party or parties signing the agreement agree that sensitive information they may obtain will not be made available to any others. An NDA may also be referred to as a confidentiality agreement.

50. Question

A digital signature is simply a message that is encrypted with the public key instead of the private key. (True/False)

- **TRUE**
- FALSE

Unattempted

A message is encrypted with a user's private key so that only the user's public key can decrypt the signature and the user's identity can be verified.

51. Question

An ethical hacker discovers a vulnerability on the website of a major company. What is the appropriate thing to do?

- Ignore it.
- Exploit the vulnerability without harming the website owner so that attention be drawn to the problem.
- **Notify the website owner to address the vulnerability.**
- Sell the information on the dark web.

Unattempted

Ethical hackers or white hat hackers do ethical hacking for the benefit of the company.

52. Question

Which of the following SHA or Secure Hashing Algorithm can produce a 160-bit digest from a message with a maximum length of (264-1) bits and resembles the MD5 algorithm?

- **SHA-1**
- SHA-2
- SHA-0
- SHA-3

Unattempted

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

53. Question

Which of the following can be done in OWASP Broken Web Applications Project?

- [ ] Hacking known websites
- [ ] **Testing manual assessment techniques**
- [ ] **Using of automated tools**
- [ ] **Testing source code analysis tools**

Unattempted

OWASP Broken Web Applications Project is a collection of vulnerable web applications available for testing on a virtual machine.

54. Question

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

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

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.

55. Question

Which of the following configuration allows NIC to pass all traffic it receives to the Central Processing Unit (CPU), instead of passing only the frames that the controller is intended to receive.

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

Unattempted

Promiscuous mode refers to the special mode of Ethernet hardware that allows a NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting.

56. Question

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

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

Unattempted

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

57. Question

Which of the following statements is TRUE about sniffers?

- **Sniffers operate on Layer 2 of the OSI model**
- Sniffers operate on both Layer 2 & Layer 3 of the OSI model.
- Sniffers operate on Layer 3 of the OSI model
- Sniffers operate on Layer 1 of the OSI model.

Unattempted

The OSI layer 2 is where packet sniffers collect their data.

58. Question

This property guarantees that no hash function will generate similar hashed value for two different messages?

- Bit Resistance
- **Collision resistance**
- Public Key strength
- Private Key strength

Unattempted

Collision resistance ensures that no hash function will produce the same value for two different inputs.

59. Question

It is very essential to employ a proxy tool when testing web applications to save every request and response. It allows you manually test every request and analyze the response to find vulnerabilities. It also allows you to test parameters and headers manually to get more precise results than when using web vulnerability scanners. What proxy tool will help you find web vulnerabilities?

- **Burpsuite**
- Dimitry
- Proxychains
- Maskgen

Unattempted

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, to finding and exploiting security vulnerabilities.

60. Question

This is a self-propagating botnet that has the capability of finding and infecting those vulnerable devices that are still using their factory default username and password.

- Monero
- Lemon Duck
- **Mirai**
- Prometei

Unattempted

One of the most familiar examples of a botnet is a Mirai botnet. Mirai botnet is a self-propagating botnet, which has the capability of finding and infecting those vulnerable devices that are still using their factory default username and password. Unfortunately, most IoT devices are still using their default credentials, thus they are being used as a part of DDOS attacks.

61. Question

Which of the following tool can be used in performing session splicing attacks?

- TCPsplice
- Hydra
- Burp
- **Whisker**

Unattempted

A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. A whisker is an evasion tool that crafts packets with small payloads referred to as session splicing.

62. Question

Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct Diffie-Hellman (DH) group for the 768-bit key?

- Diffie-Hellman (DH) group 2
- Diffie-Hellman (DH) group 14
- Diffie-Hellman (DH) group 5
- **Diffie-Hellman (DH) group 1**

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

63. Question

Which of the following is an IDS defeating technique?

- IDS spoofing or session assembly
- IP splicing or packet reassembly
- **IP fragmentation or session splicing**
- IP routing or packet dropping

Unattempted

IP fragmentation or session splicing is a way of defeating an IDS.

64. Question

These are hackers backed by the government to penetrate, gain top-secret information, and damage the information systems of other governments.

- Black Hat Hacker
- Spy Hacker
- Suicide Hacker
- **State-sponsored hacker**

Unattempted

State-sponsored hackers are individuals employed by the government to penetrate and gain top-secret information and to damage the information systems of other governments.

65. Question

An ethical hacker successfully gained access to his client's hybrid network. Which port should he listen to know which Microsoft Windows workstations have their file sharing enabled?

- 161
- 1433
- 3389

445

Unattempted

SMB has always been a network file-sharing protocol. As such, SMB requires network ports on a computer or server to enable communication to other systems. SMB uses either IP port 139 or 445.

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 →

Important Links

REFUND POLICY

REFUND REQUEST

TERMS & CONDITIONS

PRIVACY POLICY

Privacy Policy