SKILLCERTPRO
IT CERTIFICATION TRAININGS

0

Information Security / By SkillCertPro

Practice Set 14

Your results are here!! for" CEHv11 Practice Test 14 "

0 of 65 questions answered correctly

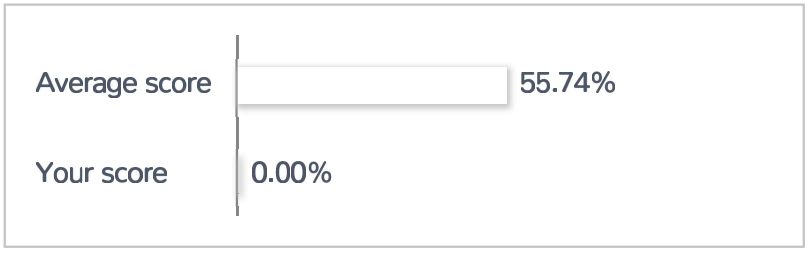
Your time: 00:00:02

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

This application allows developers to test vulnerabilities commonly found in Java-based applications.

- WebTest
- **WebGoat**
- WebBugs
- WebScript

Unattempted

WebGoat is a deliberately insecure application that allows interested developers to test vulnerabilities commonly found in Java-based applications that uses common and popular open-source components.

2. Question

In user authentication, which of the following is/are considered as “something you are”?

- **Iris scan**
- **Facial Recognition**
- **Fingerprint**
- PIN

Unattempted

Iris scan, fingerprint, and facial recognition are all considered as “something you are”, while PIN is “something you know”.

3. Question

XOR is a common cryptographical tool. What will be the result if you apply XOR in the following binary values: 11001100, 01101010?

- 11001100
- 1011001
- **10100110**
- 1101010

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.

4. Question

This analysis provides the possible consequences when one of company's critical processes were disrupted.

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

5. Question

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

- Internet Control Message Protocol
- **Transmission Control Protocol**
- Universal Protocol

- User Datagram Protocol

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.

6. Question

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

- Logic Bomb
- Trojan
- **Ransomware**
- Botnet

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.

7. Question

Which of the following architecture is designed to verify and authenticate individuals taking part in a data exchange within an enterprise?

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

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.

8. Question

The NMAP command "nmap -sn 192.32.111.107" performs which of the following?

- Trace sweep
- Port scan
- Operating system detect
- **Ping scan**

Unattempted

"nmap-sn" means no port scan. This means that Nmap will not do a port scan after the host discovery and only prints out the available hosts that responded to the host discovery probes. This is often known as a "ping scan".

9. Question

Which of the following does not belong to the group?

- Facial Recognition
- Fingerprint
- Iris scan
- **PIN**

Unattempted

Iris scan, fingerprint, and facial recognition are all considered as "something you are", while PIN is "something you know".

10. Question

It is a comprehensive tool for man-in-the-middle (MITM) attacks that can be used for computer network protocol analysis and security auditing.

- Tcpdump
- **Ettercap**
- Wireshark

- Aircrack-ng

Unattempted

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

11. Question

Which of the following restriction does a “white box testing ” methodology enforces?

- Only the internal operation of a system is known to the tester.
- The internal operation of a system is only partly accessible to the tester.
- Only the external operation of a system is accessible to the tester.
- **The internal operation of a system is completely known to the tester.**

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.

12. Question

Wireless intrusion prevention system (WIPS) operates at what layer of the Open Systems Interconnection (OSI) model?

- **Data Link Layer**
- Network Layer
- Session Layer
- Physical Layer

Unattempted

Wireless intrusion prevention system (WIPS) works at the data link layer (Layer 2) of the Open Systems Interconnection (OSI) model. It has the capability of discovering the presence of misconfigured devices and mitigating them from operating on wireless enterprise networks.

13. Question

A security audit of network systems must be performed to determine compliance with security policies. Which of the following tools would most likely be used in such an audit?

- Intrusion Detection System
- Protocol analyzer
- **Vulnerability scanner**
- Port scanner

Unattempted

Vulnerability scanning is a method used to check whether a system is exploitable by identifying its vulnerabilities. A vulnerability scanner consists of a scanning engine and a catalog. These tools generally target vulnerabilities that secure host configurations can fix easily, updated security patches, and a clean Web document.

14. Question

This is a fast-moving virus that can affect both the boot sector and the program files at the same time, thus causing more damage than any other kind of virus

- Stealth virus
- Polymorphic virus
- **Multipartite Virus**
- Macro virus

Unattempted

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

15. Question

Which definition among those given below best describes a covert channel?

- It is one of the weak channels used by WEP which makes it insecure
- A server program using a port that is not well known.
- It is the multiplexing taking place on a communication link.
- **Making use of a protocol in a way it is not intended to be used.**

Unattempted

An 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.

16. Question

A cybercriminal uses a communication channel within an operating system that is neither designed nor intended to transfer information. What communications channel is described here?

- **Covert**
- Classified
- Encrypted
- Overt

Unattempted

An 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.

17. Question

This type of hacker refers to an individual who works both offensively and defensively at various times. Their intention can either be to simply gain knowledge or to illegally make changes.

- Black Hat
- **Gray Hat**
- Suicide Hacker
- White Hat

Unattempted

Gray hat hackers are a mixture of white hat hackers and black hat hackers. They exploit a network's vulnerability without the owner's permission with no malicious intent. They usually do this for fun and because they can.

18. Question

This tool is used to analyze the files produced by packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

- Tcptraceroute
- Nessus
- **Tcptrace**
- OpenVAS

Unattempted

Tcptrace is a tool for the analysis of TCP dump files. It can take as input the files produced by several popular packet-capture programs, including tcpdump/WinDump/Wireshark, snoop, EtherPeek, and Agilent NetMetrix.

19. Question

Which of the following describes the Connection Stream Parameter Pollution (CSPP) attack?

- Insertion of malicious Javascript code into input parameters.
- Setting the user's SID to an explicit known value.
- Addition of multiple parameters with the same name in HTTP requests.
- **Injection of parameters into a connection string using semicolons as a separator.**

Unattempted

The so-called Connection String Parameter Pollution (CSPP) attack exploits poorly secured dynamic connections between Web apps and databases, namely ones that still use semicolons as separators between data such as the data source, user ID, and password associated with a connection to the database, for instance.

20. Question

This high-level programming language is vulnerable to buffer overflow attacks.

- Perl
- Java
- **C++**
- Python

Unattempted

C/C++ are high-level programming languages that are vulnerable to buffer overflow attacks.

21. Question

This type of attack targets a groups of users by infecting websites that they commonly visit.

- Heartbleed Attack
- **Watering Hole Attack**
- Shellshock Attack
- Spear Phishing Attack

Unattempted

A watering hole attack is a targeted attack designed to compromise users within a specific industry or group of users by infecting websites they typically visit and luring them to a malicious site. The end goal is to infect the users computer and gain access to the organizations network.

22. Question

This phase is critical as it will greatly affect the success of a penetration testing. This is also the most important phase of ethical hacking in which you need to spend a considerable amount of time.

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

Unattempted

Footprinting or reconnaissance is the first step in ethical hacking. The penetration tester will use this to evaluate the security of any IT infrastructure. Footprinting also means gathering all information about the computer system or a network and all the devices that are attached to this.

23. Question

XYZ company hired Jane, a security consultant, to do a physical penetration testing. On the first day of her assessment, she goes to the company`s building dressed like housekeeping. She waited in the lobby for any unsuspecting employee to pass through the main access gate, then followed the employee behind to get into the restricted area. What type of attack was performed by Jane?

- Social engineering
- Mantrap
- **Tailgating**
- Shoulder surfing

Unattempted

Tailgaiting is an act where the unauthorized person was able to enter the premises without the authorized person's knowledge. To avoid Tailgating, employees should be wary of their surroundings.

24. Question

Cross-site request forgery involves which of the following:

- A request sent by a cybercriminal from a browser to a serve
- **A browser making a request to a server without the user's knowledge**
- Modification of a request by a proxy between client and server
- A server making a request to another server without the user's knowledge

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.

25. Question

What do you call an attack which uses a combination of brute force and dictionary methods to have a variation of words?

- Massive attack
- Brute-Dictionary
- **Hybrid attack**
- Full blown attack

Unattempted

Hybrid Attacks are a kind of cyberattack where the perpetrator blends two or more kinds of tools to carry out the assault. A typical hybrid attack is one that merges a dictionary attack and a brute-force attack.

26. Question

This is defined as a short-range wireless communication technology replacing the cables connecting portable devices while maintaining high levels of security. It allows mobile phones, computers, and other devices to connect and communicate using a short-range wireless connection.

- **Bluetooth**
- Radio-Frequency Identification
- InfraRed
- WLAN

Unattempted

Bluetooth is a standard for the short-range wireless interconnection of mobile phones, computers, and other electronic devices.

27. Question

Theon logged in as an admin account. He wants to know what to type on the windows command line to launch the Group Policy Editor.

- compmgmt.msc
- **gpedit.msc**

- services.msc
- ncpa.cpl

Unattempted

To open the Group Policy Editor from the command line just type gpedit.msc in your run box or at the command line.

28. Question

Which of the following restriction does a “black box testing” methodology enforces?

- **Only the external operation of a system is accessible to the tester.**
- The internal operation of a system is only partly accessible to the tester.
- The internal operation of a system is completely known to the tester.
- Only the internal operation of a system is known to the tester.

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.

29. Question

SIA Global Security decides to implement a risk management strategy. Which of the following belongs to the five basic responses to risk?

- **Avoid**
- **Accept**
- **Mitigate**
- Delegate

Unattempted

There are five main ways to manage risks. These are acceptance, avoidance, transference, mitigation, or exploitation.

30. Question

Which of the following is a widely used standard for message logging. It also permits the separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Which of the following is being described?

- SMS
- SNMP
- ICMP
- **SYSLOG**

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

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.

32. Question

You received an email with an attachment labeled “Holiday_Sale_2021” which you thought came from your favorite shop. Inside the zip file is a file named “Holiday_Sale_2021.docx.exe” disguised as a word document.

Upon execution, a window appears stating, “This word document is corrupt.” In the background, the file copies itself to your APPDATA\local directory and begins to beacon to a C2 server to download additional malicious binaries. You encountered which type of malware?

- Trojan
- Keylogger
- Macro
- Worm

Unattempted

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

33. Question

Iya received an email attachment named “YouWonGrandPrize.zip.” The zip file contains a file named “ClaimYourPrize.docx.exe.” Out of excitement and curiosity, Iya immediately opened the said file. Without her knowledge, the file copies itself to Iya’s APPDATA\local directory and begins to beacon to a Command-and-control server to download additional malicious binaries. Iya encountered which type of malware?

- Key-logger
- Macro Virus
- Trojan
- Worm

Unattempted

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

34. 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 2048-bit key?

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

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

35. Question

This protocol is specifically designed for transporting event messages?

- SNMP
- SMS
- **SYSLOG**
- ICMP

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.

36. Question

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

- Public Key Strength
- Bit Resistance

- Collision resistance
- Private Key Strength

Unattempted

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

37. Question

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

- Shodan
- Wireshark
- Spyse
- 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.

38. Question

A hacker wants to leak classified information. For him to defeat a multi-level security solution, he can use:

- A covert channel
- Bypass regulator
- Asymmetric routing
- Steganography

Unattempted

An 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 – in this case, bypassing network security measures rather than bypassing security guards.

39. Question

Van, a security analyst in an insurance company, is assigned to test a new web application that will be used by clients in choosing and applying for an insurance plan. He discovered that the application was developed in ASP scripting language and it uses MSSQL as a database backend. He locates the application's search form and sends the following code in the search input field:

When Van submits the form, the browser returns a pop-up window that says "Vulnerable". Which of the following web applications vulnerability did Van discover?

- SQL injection
- Command injection
- Cross-site request forgery
- **Cross-site scripting**

Unattempted

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

40. Question

Which of the following protocol is used for setting up secure channels between two devices, typically in VPNs?

- Point to Point Protocol
- Secure Electronic Transaction
- **Internet Protocol Security**
- Privacy Enhanced Mail

Unattempted

IPsec is a group of networking protocols used for setting up secure encrypted connections, such as VPNs, across publicly shared networks.

41. Question

This method provides a thorough and comprehensive assessment of organizational security covering policy, procedure design, and implementation.

- Social engineering
- Access control list reviews
- **Penetration testing**
- Vulnerability scanning

Unattempted

Penetration testing is a methodological approach to security assessment that encompasses the security audit and vulnerability assessment and demonstrates if the vulnerabilities in the system can be successfully exploited by attackers.

42. Question

A hacker was able to install a sniffer program in a switched environment network. Which attack could he use to sniff all of the packets in the network?

- Smurf
- Tear Drop
- Fraggle
- **MAC Flood**

Unattempted

MAC flooding is a technique used to compromise the security of network switches that connect network segments or network devices. Attackers use the MAC flooding technique to force a switch to act as a hub so that they can easily sniff the traffic.

43. Question

This outlines the procedures that help protect the organizational resources and the rules that control access to them.

- Acceptable Use Policy
- User Account Policy

- Access Control Policy
- Data Retention Policy

Unattempted

Access Control Policy (ACP) outlines the procedures that help in protecting organizational resources and the rules that control access to them. It enables organizations to track their assets.

44. Question

This software is used to detect weak passwords that could put network security at risk.

- Jack the Ripper
- Netcat
- Cain and Abel
- John the Ripper

Unattempted

John the Ripper is often used in the enterprise to detect weak passwords that could put network security at risk, as well as other administrative purposes. The software can run a wide variety of password-cracking techniques against the various user accounts on each operating system and can be scripted to run locally or remotely.

45. Question

This security operation is used to determine the attack surface of an organization

- Run a network scan to detect network services in the corporate DMZ
- Train employees on the security policy regarding social engineering
- Review the need for a security clearance for each employee
- Use configuration management to determine when and where to apply security patches

Unattempted

For a network scan, the goal is to document the exposed attack surface along with any easily detected vulnerabilities.

46. Question

The following is a sample of output from an ethical hacker's machine targeting a machine with an IP address of 192.32.111.107. What is most likely taking place?

- Denial of service attack on 192.32.111.107
- Ping sweep of the 192.32.111.107 network
- **Remote service brute force attempt**
- Port scan of 192.32.111.107

Unattempted

The given output can be seen from a penetration tester's machine while attempting to brute force the targeted machine

47. 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.

- Riskware
- Adware
- Spyware
- **Ransomware**

Unattempted

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

48. Question

Which of the following is considered a brute force attack?

- You create hashes of a large number of words and compare them with the encrypted passwords
- **You attempt every single possibility until you exhaust all possible combinations or discover the password**
- You load a dictionary of words into your cracking program

- You threaten to use the rubber hose on someone unless they reveal their password

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.

49. Question

Which of the following cipher encrypts a block of plain text rather than one by one?

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

Unattempted

Block cipher converts the plain text into cipher text by taking plain text's block at a time.

50. Question

Andrea is the security administrator of a large financial company. One day she notices that the company's Oracle database server has been compromised, and customer information along with financial data has been stolen. She wants to report the crime immediately. Which organization coordinates computer crime investigations throughout the United States?

- National Institute of Crime Prevention (NICP)
- National Defense Cyber Alliance (NDCA)
- Cyber Incident Response Plan (CIRP)
- **National Infrastructure Protection Center (NIPC)**

Unattempted

The National Infrastructure Protection Center (NIPC) was a unit of the United States federal government charged with protecting computer systems and information systems critical to the United States' infrastructure.

51. 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-2
- SHA-3
- SHA-0
- **SHA-1**

Unattempted

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

52. Question

Which of the following physical characteristics is/are ideal to be used in a biometric control for a start-up and stable company?

- **Fingerprints**
- **Voice**
- Height and Weight
- **Iris patterns**

Unattempted

Height and weight are NOT ideal choices for biometric controls. Even though these provide some information about the user, they lack distinctiveness and permanence to sufficiently differentiate the user from each other.

53. 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 1024 bit key?

- Diffie-Hellman (DH) group 14
- Diffie-Hellman (DH) group 1

Diffie-Hellman (DH) group 5

Diffie-Hellman (DH) group 2

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

54. Question

It is critical to know the HTTP Methods that are available when getting information about a web server. The two important methods are PUT and DEL. PUT can upload a file to the server and DELETE can delete a file from the server. These methods (GET, POST, HEAD, PUT, DELETE, TRACE) can be detected by using which of the following Nmap script?

http-git

http enum

http-methods

http-headers

Unattempted

HTTP method vulnerability can be checked using NMAP. Example: #nmap -script=http-methods.nse 192.168.0.50

55. Question

Which of the following is the BEST approach in mitigating Cross-site Scripting (XSS) flaws?

Verifying access right before allowing access to protected information and UI controls.

Using digital certificates to authenticate a server prior to sending data.

Verifying access right before allowing access to protected information and UI controls.

Validating and escaping all information sent to a server.

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.

56. Question

This 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.

- Secret Channel
- **Covert Channel**
- Defense Channel

Unattempted

An 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.

57. Question

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

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

58. Question

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

- port 25 and host 192.168.0.125

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

Unattempted

The destination host and IP host must be configured.

59. Question

Just before you logged out, you received a suspicious email in your inbox. You are not familiar with the sender but the subject line is appealing. What is the best approach to this situation?

- Forward the email to your supervisor and ask how to handle the situation.
- Immediately delete the email and pretend that it never happened.
- **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.

Unattempted

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

60. Question

These are valid data-gathering activities that are associated with a risk assessment? Choose all that applies.

- Mitigation identification
- **Threat identification**
- **Control Analysis**
- **Vulnerability identification**

Unattempted

The most common way to describe risk is through the Risk equation. This equation is fundamental to all information security. Risk = Threat x Vulnerability x Control

61. Question

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

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

62. 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
- Kerberos
- TACACS+
- **RADIUS**

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.

63. Question

Which of the following restriction does a “gray box testing ” methodology enforces?

- The internal operation of a system is completely known to the tester
- **The internal operation of a system is only partly accessible to the tester.**

- Only the external operation of a system is accessible to the tester.
- Only the internal operation of a system is known to the tester.

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.

64. Question

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

- Presentation tier
- Application Layer
- **Logic tier**
- Data tier

Unattempted

Logic tier coordinates the application, processes command, makes logical decisions and evaluations, and performs calculations. It also moves and processes data between the two surrounding layers.

65. Question

It is implemented to ensure the safety of organizational computer systems and physical resources on company premises.

- Media Disposal Policy
- **Physical Security Policy**
- User Account Policy
- Data Retention Policy

Unattempted

Physical Security Policy is implemented to ensure the safety of the organizational computer systems and physical resources on company premises.

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

Privacy Policy