Comptia Security Plus Paper 1

1 UDP port 69 is assigned to:

SELECT THE CORRECT ANSWER

- A. TFTP ✔
- B. SNMP
- C. DHCP
- D. LDAP

Correct Option: A

EXPLANATION

UDP port 69 is assigned to TFTP

2

Which encryption technique used to access the database?

SELECT THE CORRECT ANSWER

- A. Symmetric key encryption
- B. Application-level encryption ✔
- C. Homomorphic encryption
- D. Transparent encryption

Correct Option: B

EXPLANATION

Application-level encryption is used to access the database.

3 What specific aspect of the CPU enables the microprocessor to handle running numerous operating systems simultaneously?

SELECT THE CORRECT ANSWER

- A. Clock multiplying
- B. Caching
- C. Pipelining
- D. Virtualization support ✔

Correct Option: D

EXPLANATION

Virtualization support

4 MD5, RIPEMD, SHA are types of

SELECT THE CORRECT ANSWER

- A. Encryption Algorithm
- B. Hashing Algorithm ✔
- C. Decryption Algorithm
- D. Sorting Algorithm

Correct Option: B

EXPLANATION

MD5, RIPEMD, SHA are types of Hashing algorithm.

5 Which of the following platforms is commonly used by the Watering Hole attacks?

SELECT THE CORRECT ANSWER

- A. Website ✔
- B. Web Browser
- C. Web Server
- D. Web Services

Correct Option: A

EXPLANATION

Website is commonly used for Watering hole attack.

6 Domain name to IP address mapping can be done by

SELECT THE CORRECT ANSWER

- A. tracert ✓
- B. nslookup
- C. nmap
- D. netstart

Correct Option: A

EXPLANATION

Domain name to IP address mapping can be done by tracert.

7 What type of address is falsified by MAC Spoofing and IP Spoofing?

SELECT THE CORRECT ANSWER

- A. Destination address
- B. Loopback Address
- C. MAC Address
- D. Source Address ✔

Correct Option: D

EXPLANATION

MAC Spoofing and IP Spoofing rely on falsifying the source address.

8 Secure transmission of HTTP traffic is possible because of

SELECT THE CORRECT ANSWER

- A. L2TP
- B. Secure Remote Protocol
- C. Transport Layer Security ✔
- D. Encryption

Correct Option: C

EXPLANATION

Secure transmission of HTTP traffic is possible because of Transport Layer Security.

9 Which type of network device is a Context Box Access Control?

SELECT THE CORRECT ANSWER

- A. VLAN
- B. VPN
- C. Stateful inspection firewall ✔
- D. IDS/IPS

Correct Option: C

EXPLANATION

Context Box Access Control is a type of Stateful inspection firewall.

10 What type of virtualization uses a host operating system?

SELECT THE CORRECT ANSWER

- A. Type-I
- B. Type-II ✔
- C. Open source
- D. Native Hypervisor

Correct Option: B

EXPLANATION

Type-II runs on a host operating system.

11 Who is responsible for data categorization and security?

SELECT THE CORRECT ANSWER

- A. COO
- B. CTO
- C. Security Officer ✔
- D. End User

Correct Option: C

EXPLANATION

A security officer is responsible for data categorization and security.

12 Session hijacking can be mitigated by

SELECT THE CORRECT ANSWER

- A. IDS
- B. Anti Virus
- C. IPSec ✓
- D. UDP

Correct Option: C

EXPLANATION

Session hijacking can be mitigated by IPSec.

13 Smart Card Reader used in laptop is a type of

SELECT THE CORRECT ANSWER

- A. New feature
- B. Data access Panel
- C. Access Control ✓
- D. Data Encryption

Correct Option: C

EXPLANATION

Smart Card Reader used in laptop is a type of access control.

14 Cold Sites are the most expensive form of data backup.

SELECT THE CORRECT ANSWER

- A. TRUE
- B. FALSE ✔

Correct Option: B

EXPLANATION

Cold sites are not the most expensive form of back up.The cost is based on the site size and the monthly rent may vary from $500 to $15k.

15 Which incident response process is involved to secure critical systems during business operations management?

SELECT THE CORRECT ANSWER

A. Recovery

B. Containment ✓

C. Research

D. Investigate

Correct Option: B

EXPLANATION

Containment secures critical systems during business operations management.

16 When a hypervisor is targeted from guest OS, it can be reported as

SELECT THE CORRECT ANSWER

- A. VM Escape ✓
- B. VM Nested
- C. VM Routing
- D. VM Mounting

Correct Option: A

EXPLANATION

When a hypervisor is targeted from guest OS, it can be reported as VM Escape.

17 A company recently changed its BYOD policy and asked the employees to bring the required devices for official use. Which is the best-suited method for protecting data?

SELECT THE CORRECT ANSWER

- A. Full-Disk Encryption ✔
- B. Biometric Authentication
- C. Geofencing
- D. GPS Tags

Correct Option: A

EXPLANATION

A full-disk encryption can be used to protect data on devices.

18 During a security audit in your organization, you identify vulnerability due to a software installation on process controller terminal. This terminal cannot be upgraded and hence has been put into isolated zone. As an auditor, what will you suggest for mitigating this risk?

SELECT THE CORRECT ANSWER

- A. Application Whitelisting ✓
- B. IP Blacklist
- C. DNS Spoofing
- D. IP Shadow

Correct Option: A

EXPLANATION

Application whitelisting will help mitigating these vulnerabilities.

19 Analyzed the following script Hello Dear I am looking for some online product but my wallet is blocked due to wrong credentials. Thank you What type of attack was attempted against the forum readers?

SELECT THE CORRECT ANSWER

- A. SQL Attack
- B. DLL Attack
- C. XSS Attack ✓
- D. API Attack

Correct Option: C

EXPLANATION

An XSS attack was attempted against the forum readers.

20 Which tool would a security administrator use to conduct a comprehensive stock level of all the encryption protocols and cipher suites?

SELECT THE CORRECT ANSWER

- A. tcpdump
- B. Protocol analyzer ✔
- C. netstat
- D. Nmap

Correct Option: B

EXPLANATION

Protocol analyzer will be used to check the encryption protocols and cipher suites.

21 A company is seeing an increase in the number of systems that lock up upon Windows startup. The security analyst clones a machine, boots it into safe mode, and discovers a file in the startup process that runs user start.bat. @echo off dbcfcssaaaandfkj start notepad. exe start notepad. exe start calculator.exe start calculator.exe start paint.exe start chrome.exe start efe.exe goto dbcfcssaaaandfkj Which of the following types of malware is present based on the file contents and the system issues?

SELECT THE CORRECT ANSWER

- A. Rootkit
- B. Logic bomb
- C. Worm
- D. Virus ✔

Correct Option: D

22 The security director of an organization recommends the use of newly installed SaaS application and plans to map this new SaaS application with the organization's Identity and Access Management (IAM) process. Which of the following will help complete this mapping?

SELECT THE CORRECT ANSWER

- A. LDAP
- B. RADIUS
- C. SAML ✔
- D. NTLM

Correct Option: C

23 To which of the following scenarios is the application of Faraday's cage best suited?

SELECT THE CORRECT ANSWER

A. To control emanation to thwart credential harvesting

B. To increase signal strength

C. To reduce external radio frequency (RF) interference with embedded processors ✔

D. To safeguard the audit logs' integrity against malicious modification

Correct Option: C

EXPLANATION

Faraday cages contribute to the prevention of electromagnetic interference.

24 An attacker motivated by political objectives who works for a short period but possesses virtually unlimited resources can be classified as a

SELECT THE CORRECT ANSWER

- A. Hacktivist. ✓
- B. Nation-state
- C. Script child
- D. APT

Correct Option: A

EXPLANATION

Politically driven threat actors are referred to as hacktivists.

25 What differentiates an intrusive and a non-intrusive vulnerability scanning?

SELECT THE CORRECT ANSWER

- A. Intrusive scanning uses credentials, non-intrusive do not require credentials ✓
- B. Intrusive scanning has a higher potential for disrupting system operations
- C. Non-intrusive scanning are not allowed to activate firewall counters
- D. Both intrusive and non-intrusive scanning are the same

Correct Option: A

EXPLANATION

Use of credential is the most significant difference

26 Your organization's Chief Information Officer (CIO) has determined that due to the new Public Key Infrastructure (PKI), the company will not use OCSP. However, the purpose of replacing OCSP remains unclear. Which of the following suggestions should be implemented?

SELECT THE CORRECT ANSWER

- A. Build an online intermediate CA
- B. Implement a key escrow
- C. Implement stapling
- D. Install a CRL ✓

Correct Option: D

EXPLANATION

CRL has the same functionality as OCSP.

27 Which of the following provides Perfect Forward Secrecy?

SELECT THE CORRECT ANSWER

- A. AES
- B. RC4
- C. DHE ✓
- D. HMAC

Correct Option: C

EXPLANATION

Diffie-Hellman protocol provides PFS.

28 Which among the following is used to outline the role and responsibility of data controller and processor?

SELECT THE CORRECT ANSWER

- A. GDPR ✔
- B. ISO 31000
- C. PCI DSS
- D. ISO 21000

Correct Option: A

EXPLANATION

A GDPR is a statement used for controlling and processing data.

29

A network administrator expressed concern during an audit that users continued to use the same passwords the day after a password change policy went into effect. Currently, the users must change their passwords every 30 days and are not allowed to reuse their last ten passwords. Which of the following options would enforce this?

SELECT THE CORRECT ANSWER

- A. The password should be older than 10 days. ✔
- B. Password history containing recently used passwords
- C. A password longer than ten characters
- D. Use of complex passwords

Correct Option: A

30 Which of the following methods should a technician employ to protect a cellular phone utilized in an investigation, so that the data isn't remotely deleted?

SELECT THE CORRECT ANSWER

A. Gap in the air

B. Locked cabinet

C. Cage de Faraday ✔

D. Safe

Correct Option: C

EXPLANATION

The technician should use the Cage de Faraday method to disable all radio connections to the phone.

31 A security analyst observes traffic on port 443 from an external IP address to an internal business network IP address while monitoring the SIEM. Which of the following protocol is probably the source of this traffic?

SELECT THE CORRECT ANSWER

- A. HTTP
- B. SSH
- C. SSL ✓
- D. DNS

Correct Option: C

EXPLANATION

443 is the port for HTTPS (HTTP+SSL).

32 Lateral movement within a network after using an initial exploit to gain persistent access with the intent of gaining further control of a system is referred to as:

SELECT THE CORRECT ANSWER

- A. Pivoting
- B. Persistence ✔
- C. Active reconnaissance
- D. backdoor

Correct Option: B

EXPLANATION

Lateral movement within a network after using an initial exploit to gain persistent access with the intent of gaining further control of a system is called persistence.

33

The perimeter UTM sends alerts to the security administrator. When the administrator examines the logs, he finds the following output: Time: 04:00:01 From Untrust Zone To DMZ Zone povnode.com is the perpetrator. Victim: 19.168.10.248 Destination: 80 What action should the security administrator take?

SELECT THE CORRECT ANSWER

A. Upload the PCAP to the IDS to generate a blocking signature to block the traffic.

B. Manually copy the <script> data from the PCAP file and generate a blocking signature in the HIDS to block the traffic for future events. ✔

C. Implement a host-based firewall rule to block future events of this type from occurring.

D. Submit a change request to modify the XSS vulnerability signature to TCP reset on future attempts.

Correct Option: B

34 Which of the following serves as a warning to the users about the dangers associated with the installation of pirated software on company-owned devices?

SELECT THE CORRECT ANSWER

- A. AUP ✔
- B. NDA
- C. ISA
- D. BPA

Correct Option: A

EXPLANATION

Acceptable use policy serves as a warning to users about pirated softwares.

35 Name the encryption algorithms which necessitates the use of a single encryption key. (Choose TWO.)

SELECT THE CORRECT ANSWER(S)

- ✓ A. MD5 ✓
- B. 3DES
- C. BCRYPT
- ✓ D. RC4 ✓

Correct Option: A, D

EXPLANATION

MD5 and RC4 are symmetric algorithms with single encryption key.

36 The incident response team found recently that one of the system passwords has been compromised and an unexpected login activity for one of the programs was detected. It was then discovered that users who were on vacation tried logging into their accounts. According to company rules, users must create passwords that contain an uppercase letter, a lowercase letter, a number, and a special symbol. This policy is enforced using technical controls, which also prevents users from using any of their previous eight passwords. The quantization does not employ single sign-on or password centralised storage.

SELECT THE CORRECT ANSWER

- A. Some users are meeting password complexity requirements but not password length requirements
- B. The password history enforcement is insufficient and old passwords are still valid across many different systems
- C. Some users are reusing passwords and some of the compromised passwords are valid on multiple systems ✓
- D. The compromised password file has been brute-force hacked, and the complexity requirements are not adequate to mitigate this risk

Correct Option: C

EXPLANATION

Some users are reusing passwords which are valid on multiple systems enabling them to access certain programs.

What authentication factor is this example referring to- the use of a one-time code texted to a smartphone?

SELECT THE CORRECT ANSWER

- A. Something you have ✓
- B. Something you are
- C. Something you know.
- D. Something you do

Correct Option: A

EXPLANATION

It is one of the examples of what you have authentication factor

38 COPE devices are being distributed to all account executives. Name the mobile device security practices that should be enabled to protect company data on these devices. (Choose TWO)

SELECT THE CORRECT ANSWER(S)

- A. Screen locks
- B. Remote wipe ✓
- C. Containerization ✓
- D. Full device encryption

Correct Option: B, C

EXPLANATION

Remote wipe and containerization are the two measures to be taken for COPE (Company Owned Personally Enabled device).

39 Attempting to exploit a buffer-overrun vulnerability in a system will most likely result in

SELECT THE CORRECT ANSWER

A. Arbitrary code execution

B. Resource exhaustion

C. Exposure of authentication credentials

D. Dereferencing of memory pointers ✔

Correct Option: D

EXPLANATION

Buffer overflow (overrun) is a part of memory pointers dereferencing.

40 A business recently bought a new application and wishes to prompt LDAP-based authentication for all staff members who will use it. What should be configured to securely connect the application to the company's LDAP server? (Choose TWO)

SELECT THE CORRECT ANSWER(S)

A. A. LDAP Path: ou-users,dc=company dc=com

B. B. LDAP Path: dc=com.dc=company, ou=users ✓

C. C. Port 88

D. D. Port 636 ✓

Correct Option: B, D

EXPLANATION

The admin should first configure LDAP path for enabling the domain and then configure port 638 for communication to securely connect the application to the company's LDAP server.

41 A company's network is under attack. Despite the fact that security controls are in place to thwart these attacks, the security administrator requires more information about the types of attacks that are being used. Which of the following network types would be the most helpful in assisting the security administrator?

SELECT THE CORRECT ANSWER

- A. DMZ
- B. Guest network
- C. Ad hoc
- D. Honeynet ✔

Correct Option: D

EXPLANATION

Honeypot helps to gather information about attack and the attacker.

42 Workstations in an air-gapped network are used by an organization's research department. Based on files from the research department, a competitor has created some products. Which of the following actions should management take to ensure that research files are secure and confidential?

SELECT THE CORRECT ANSWER

A. Implement multi factor authentication on the workstations.

B. Configure removable media controls on the workstations. ✔

C. Install a web application firewall in the research department.

D. Install HIDS on each of the research workstations.

Correct Option: B

EXPLANATION

Configuring removable media controls on the workstations will help secure the files.

43 A user complaint about one of the websites obtaining a 503: Service Unavailable message is being investigated by a security analyst. To check if the web server is up and running, the analyst runs the netstat-an command. The following outcomes are presented to the analyst: TCP 100.10.52.255: 80 192.168.2.112: 60973 TIME WAIT TCP 100.10.52.255: 80 192.168.2.112: 60974 TIME WAIT TCP 100.10.52.255: 80 192.168.2.112: 60975 TIME WAIT TCP 100.10.52.255: 80 192.168.2.112: 60976 TIME WAIT TCP 100.10.52.255: What type of an attack is this?

SELECT THE CORRECT ANSWER

A. Buffer overflow

B. Domain hijacking

C. Denial of Service ✔

D. ARP poisoning

Correct Option: C

EXPLANATION

This is a type of Denial of Service attack.

44 On a network, a security technician discovered an infected machine. What should the technician do?

SELECT THE CORRECT ANSWER

A. Power off the machine for loss prevention

B. Isolate the machine ✔

C. Report the incident

D. Gather more Information

Correct Option: B

EXPLANATION

The technician should isolate the machine.

45 A multifactor authentication system is represented by:

SELECT THE CORRECT ANSWER

A. An iris scanner coupled with a palm print reader and fingerprint scanner with liveness detection.

B. A secret passcode that prompts the user to enter a secret key if entered correctly

C. A digital certificate on a physical token that is unlocked with a secret passcode ✓

D. A one-time password token combined with a proximity badge

Correct Option: C

EXPLANATION

A multifactor authentication system is represented by a digital certificate on a physical token that is unlocked with a secret passcode.

46 A company's president, who is also a defence contract expert, was interviewed. The interviewer was more interested in the president's personal life and fact-figures, rather than his business success and his experiences. What kind of threat does it indicate?

SELECT THE CORRECT ANSWER

- A. Insider threat
- B. Social engineering ✔
- C. Passive reconnaissance
- D. Phishing

Correct Option: B

EXPLANATION

This is a kind of social engineering.

47 A company shifts its server farm next to a cotton mill and they share a common wall which is already damaged by the cotton mill's transportation activities. Moisture begins to seep in to the server room which causes equipment failure. What kind of threat is the server farm facing?

SELECT THE CORRECT ANSWER

- A. Foundational
- B. Man-made ✓
- C. Environmental
- D. Natural

Correct Option: B

EXPLANATION

This is a type of man-made threat

48 A sports equipment e-commerce company wants to collaborate with a clothing e-commerce company by providing authenticated users with access to the second company's products. Name the authentication method that the sports equipment company should use to connect and integrate the two environments.

SELECT THE CORRECT ANSWER

- A. SAML ✓
- B. LDAP
- C. Kerberos
- D. TACACS+

Correct Option: A

EXPLANATION

Security Assertion Markup Language can be used to integrate the two environments.

49 To identify potentially vulnerable systems, a security analyst wants to scan the network in a similar way that an attacker would. Which of the following solutions will help analysts to complete the target in the most effective manner?

SELECT THE CORRECT ANSWER

- A. Carry out a non-credentialed scan ✔
- B. Perform an intrusive scan
- C. Try escalation of privilege
- D. Perform a credentialed scan

Correct Option: A

EXPLANATION

Carrying out a non-credentialed scan of the network will help the analysts.

50 Which of the following risk management strategies makes use of cybersecurity insurance?

SELECT THE CORRECT ANSWER

A. Avoidance

B. Acceptance

C. Mitigation

D. Transference ✔

Correct Option: D

EXPLANATION

Transference is the shifting of risk load to a third-party.

51 Which of the following item should the first responder get FIRST as part of digital evidence from a compromised site?

SELECT THE CORRECT ANSWER

A. Virtual memory

B. BIOS configuration

C. Snapshot ✔

D. RAM

Correct Option: C

EXPLANATION

A first responder should collect snapshot as part of digital evidence collection.

52 A major security concern for IoT devices is:

SELECT THE CORRECT ANSWER

A. Many IoT devices include built-in accounts that users rarely use.

B. IoT devices have limited processing power. ✔

C. IoT devices are physically separated from one another.

D. IoT devices have pre-programmed applications.

Correct Option: B

EXPLANATION

IoT devices have limited processing power due to which they are unable to process a strong encryption.

53 A company employee recently retired, causing a delay in the schedule since no one could fill the employee's position. Which one of the following measures would be the most important in preventing a recurrence of this situation?

SELECT THE CORRECT ANSWER

- A. Mandatory vacation
- B. Separation of duties
- C. Job rotation ✓
- D. Exit interviews

Correct Option: C

EXPLANATION

Job rotation is a feasible solution for such a situation.

54 A business is putting in place a strategy to encrypt and sign all proprietary data in transit. To support this strategy, the company recently deployed PKI services. Name the protocols that support this strategy and make use of PKI-generated certificates?

SELECT THE CORRECT ANSWER

- A. S/MIME
- B. HTTP-Digest
- C. IPSec
- D. All of the above ✓

Correct Option: D

EXPLANATION

S/MIME, HTTP-Digest, IPSec will support this strategy.

55 A security analyst wishes to install an intrusion detection system to monitor the company's network. The analyst has been assured that there will be no network downtime during the implementation of the solution, but the IDS must capture all the network traffic. Which of the following should be used to put the IDS in place?

SELECT THE CORRECT ANSWER

- A. Network tap ✓
- B. Honeypot
- C. Aggregation
- D. Port mirror

Correct Option: A

EXPLANATION

Network tap should be used to put the IDS in place.

56 A worker fires up a web browser and types in a URL in the address bar. Instead of navigating to the specified site, the browser goes to a completely different one. Name the attacks that would have most likely occurred. (Select TWO.)

SELECT THE CORRECT ANSWER(S)

- A. DNS hijacking ✓
- B. Cross-site scripting
- C. Domain hijacking
- D. Man-in-the-browser ✓

Correct Option: A, D

EXPLANATION

DNS hijacking and man-in-the-browser attacks are most likely to have happened.

57 Read the following information: | MD5 HASH document.doc 049eab40 fd36caad1fab10b3cdf4a883 jpg 049eab40fd36caad1fab0b3cdf4a883, MD5 HASH image 049eab40fd36caad1fab0b3cdf4a883. Which of the below concepts describes the situation? (Select TWO)

SELECT THE CORRECT ANSWER(S)

- A. Salting
- B. Collision ✓
- C. Steganography
- D. Hashing ✓

Correct Option: B, D

EXPLANATION

The situation can be associated with Collision and Hashing

58 A technician executes a command and examines the following data: TCP 0.0.0.0: 445 Listening RpcSs TCP 0.0.0.0: 80 Listening httpd. exe TCP 0.0.0.0: 443192. 168.10.20: 1301 Established httpd. exe TCP 0.0.0.0: 90328 172.55.180.22: 9090 Established notepad.exe Which of the following types of malware should the technician report based on the aforementioned information??

SELECT THE CORRECT ANSWER

A. Spyware

B. Rootkit

C. RATE ✔

D. Logic bomb

Correct Option: C

EXPLANATION

RATE is the type of malware.

59 An organization is worried that if a mobile device is lost, any confidential material on the device could be retrieved by unauthorized individuals. Which of the following is the most effective way to avoid this? (Select TWO.)

SELECT THE CORRECT ANSWER(S)

- A. Initiate remote wiping on lost mobile devices. ✓
- B. Use FDE and require PINs on all mobile devices.
- C. Install antivirus on mobile endpoints.
- D. Require biometric logins on all mobile devices. ✓

Correct Option: A, D

EXPLANATION

To avoid such situation, initiate remote wiping on lost mobile devices and make biometric logins mandatory.

60 A company's IRP prioritises containment over elimination. An incident has been discovered in which an intruder from outside the organisation configured cryptocurrency mining software on the organization's web servers. What next step should the organization take?

SELECT THE CORRECT ANSWER

A. Decommission the affected servers from the network.

B. Examine firewall and intrusion detection system logs for possible source IPs. ✓

C. Locate and install any missing software updates.

D. Remove the malicious software and determine whether the servers need to be reimaged.

Correct Option: B

EXPLANATION

Examining firewall and intrusion detection system will provide more information about the attack, if not eliminate it.

61 Which of the following ensures security for a program while allowing it to access only the resources it needs to function and prohibiting it from operating at the system level?

SELECT THE CORRECT ANSWER

- (●) A. Sandbox ✓
- ( ) B. Honeypot
- ( ) C. GPO
- ( ) D. DMZ

Correct Option: A

EXPLANATION

The sandbox ensures a secure environment.

62 Insecure protocols were discovered during a security audit of a company's network. What protocols should be implemented to ensure that browser-based access to company switches uses the safest protocol possible?

SELECT THE CORRECT ANSWER

- A. SSH2
- B. TLS1.2 ✓
- C. SSL1.3
- D. SNMPv3

Correct Option: B

EXPLANATION

TLS1.2 will ensure that the browser-based access to company switches uses the safest protocol

63 Which of the following is MOST LIKELY to be the result of improper input handling?

SELECT THE CORRECT ANSWER

- A. Database table loss ✔
- B. Untrusted certificate alert
- C. Reboot loop after power off
- D. Violation of firewall ACLs

Correct Option: A

EXPLANATION

Database table loss could be the result of improper input handling.

64 A company wants to give its users the opportunity to choose which devices they want to use for business. Which of the following deployment models should the company employ such that these needs to do not overload the service desk?

SELECT THE CORRECT ANSWER

A. VDI environment

B. CYOD model ✓

C. DAC model

D. BYOD model

Correct Option: B

EXPLANATION

CYOD (Choose Your Own Device) model will help the company implement these requirements.

65 What is the name of the physical device used to ensure the safety of onsite backup tapes?

SELECT THE CORRECT ANSWER

- A. Fireproof Safe or Vault ✔
- B. Frade Cage
- C. Concrete Vault
- D. Cold Chamber

Correct Option: A

EXPLANATION

Fireproof cage or vault is the physical security device used to ensure the safety of the backup tapes.

66 The CISO of your organization wants to implement a policy which follows international standards for data privacy and sharing. Which of the following will help in understanding and writing these policies?

SELECT THE CORRECT ANSWER

- A. GDPR ✓
- B. NIST
- C. ISO 31000
- D. PCI DSS

Correct Option: A

EXPLANATION

GDPR helps in writing and understanding of policies.

67 Post a ransomware attack, the forensics expert wants to review digital currency transactions between the attacker and the victim. Which of the following is suitable for tracing transactions?

SELECT THE CORRECT ANSWER

- A. Public Ledger
- B. Event Log ✔
- C. NetFlow Data
- D. Checksum

Correct Option: B

EXPLANATION

Event Logs have all possible activities with time stamp and statements.

68 Which plan assists in determining how to relocate from a disaster site?

SELECT THE CORRECT ANSWER

- A. Disaster recovery plan ✓
- B. A backup site plan
- C. A privilege management policy
- D. A privacy plan

Correct Option: A

EXPLANATION

A disaster recovery plan helps in determining how to relocate from a disaster site.

69 What type of backup is used for immediate recovery of a file?

SELECT THE CORRECT ANSWER

A. Storage on-site

B. Working duplicates ✓

C. Backup in increments

D. Backup differential

Correct Option: B

EXPLANATION

Working duplicates helps in immediate recovery of files.

70 The company wants to reorganize backup procedures to reduce the time taken every evening. The company wants backups to be completed as soon as possible for each week. Which backup system can be used to save modified files since the last backup?

SELECT THE CORRECT ANSWER

A. Full backup

B. Incremental backup

C. Differential backup ✔

D. Backup server

Correct Option: C

EXPLANATION

Differential backup is used to save modified files since the last backup

71 You've been approached as a consultant to assist XYZ Corp with its backup procedures. One of the things you notice is that the company doesn't have a good tape-rotation system. To ensure long-term data storage, which backup method employs a revolving schedule of backup media?

SELECT THE CORRECT ANSWER

- A. Grandfather-Father-Son method ✔
- B. Full Archival method
- C. Backup Server method
- D. Differential Backup method

Correct Option: A

EXPLANATION

Grandfather-Father-Son method will ensure revolving schedule of backup media.

72 In the event of a disaster, which site gives the best-limited capabilities for restoring services?

SELECT THE CORRECT ANSWER

- A. Hot site
- B. Warm site ✔
- C. Cold site
- D. Backup site

Correct Option: B

EXPLANATION

A warm site gives the best-limited capabilities for restoring services.

73 You are the head of Information Technology for XYZ, and your cousin is the same for ABC. The companies are similar in size and are located hundreds of miles apart. You want to put in place an agreement that allows either company to use resources at the other site in the event that a disaster renders a building unusable. Both companies will benefit from this. What kind of agreement exists between two organisations to use each other's sites in the event of an emergency?

SELECT THE CORRECT ANSWER

A. Backup-site contract

B. Warm-site contract

C. Hot-site contract

D. Mutual understanding (Reciprocal Agreement) ✓

Correct Option: D

EXPLANATION

Mutual understanding will help both the companies have this agreement in place.

74 Which process automatically switches from a malfunctioning system to another system?

SELECT THE CORRECT ANSWER

A. Fail safe

B. Redundancy

C. Failover ✓

D. Hot site

Correct Option: C

EXPLANATION

A failover process automatically switches a malfunctioning system to another system.

75 Which agreement specifies a vendor's performance requirements?

SELECT THE CORRECT ANSWER

- A. MTBF
- B. MTTR
- C. SLA ✔
- D. BCP

Correct Option: C

EXPLANATION

An SLA specifies a vendor's performance requirements.

76 Your organisation is almost certain to invest capital in a new startup's application. You express your concern regarding the new firm's sustainability and the risk that this firm is taking because it is such a large investment. You recommend that the new firm agrees to keep its source code available for customers to use in the event that it goes out of business. What would you call this model?

SELECT THE CORRECT ANSWER

- (●) A. Code escrow ✓
- ( ) B. SLA
- ( ) C. BCP
- ( ) D. CA

Correct Option: A

EXPLANATION

With code escrow, the source code of a software is deposited with a third-party escrow agent as a security against an investment.

77 Which of the following is not included in an incident response policy?

SELECT THE CORRECT ANSWER

A. External agencies (that require status)

B. Experts from outside (to resolve the incident)

C. Plan for contingencies ✓

D. Procedures for gathering evidence

Correct Option: C

EXPLANATION

An incient response does not contain plans for contingencies.

78 Which of the following is a metric for a system's or component's expected failure rate?

SELECT THE CORRECT ANSWER

- A. CIBR
- B. AIFS
- C. MTBF ✔
- D. MTTR

Correct Option: C

EXPLANATION

MTBF or Mean Time Between Failures is the metric used for a system's expected failure rate.

79 Which of the following best describes those within the organization who possess the ability to step into positions as they become available?

SELECT THE CORRECT ANSWER

- A. Planning for succession ✓
- B. Planned progression
- C. Preparing for emergencies
- D. Planning for eventuality

Correct Option: A

EXPLANATION

Planning for succession enables those within the organization to step into positions when available.

80 What other term would you use to refer to working copies?

SELECT THE CORRECT ANSWER

- A. Functional equivalents
- B. Copies in circulation
- C. Copies for operational use
- D. Copies in shadow ✔

Correct Option: D

EXPLANATION

Working copies are also called copies in shadow.

81 Which of the following is performed to retract a change that resulted in a negative outcome?

SELECT THE CORRECT ANSWER

A. A. Redundancy

B. B. ERD

C. C. Reversal ✔

D. D. DISTRICT

Correct Option: C

EXPLANATION

Reversal is performed to retract a change that resulted in a negative outcome.

82 Which of the following describes data that is too large for a traditional database to handle?

SELECT THE CORRECT ANSWER

A. Information technology

B. Big-Data data sets ✔

C. Binary data stream

D. Warehouse of data

Correct Option: B

EXPLANATION

Big-Data data sets describes large data.

83 As per CERT, which of the following is a structured or ad hoc team that you can call to address the risks after it occurs?

SELECT THE CORRECT ANSWER

- A. CSIRT ✔
- B. CIRT
- C. IRT
- D. RT

Correct Option: A

EXPLANATION

CSIRT address the risks after it occurs.

84 Which of the following is a concept based on the assumption that all data created on any system is stored indefinitely?

SELECT THE CORRECT ANSWER

A. Cloud computing

B. Warm site

C. Big data

D. Full archival ✓

Correct Option: D

EXPLANATION

Full archival is based on the assumption that all data created on any system is stored indefinitely.

85 Which of the following backup type provides continuous online backup with optical or tape jukeboxes and allows for the closest version of an available real-time backup?

SELECT THE CORRECT ANSWER

- A. TPMB.
- B. HSM ✓
- C. SAN
- D. NAS

Correct Option: B

EXPLANATION

HSM provides continuous online backup and allows for the closest version of an available real-time backup.

86 Which type of penetration testing entails attempting to get access to a network?

SELECT THE CORRECT ANSWER

A. Discreet

B. Indiscreet

C. Non-intrusive

D. Intrusive ✔

Correct Option: D

EXPLANATION

Intrusive testing entails attempting to get access to a network.

87 While educating users about the importance of security as part of a training programme, you demonstrate that not all attacks require the use of advanced technological methods. Certain attacks take advantage of human frailties to obtain entry to areas that should be denied. What term do you use to refer to these types of attacks?

SELECT THE CORRECT ANSWER

- A. Social engineering ✓
- B. Intrusion detection systems
- C. Perimeter security
- D. Biometrics

Correct Option: A

EXPLANATION

These types of attacks are called Social engineering.

88 What is another term for social engineering?

SELECT THE CORRECT ANSWER

A. Disguise socially

B. Social hacking

C. Wetware ✓

D. Wetfire

Correct Option: C

EXPLANATION

Wetware is another term for social engineering.

89 Which statement most accurately describes tailgating?

SELECT THE CORRECT ANSWER

- A. Following someone through an unlocked door ✓
- B. Determining how to unlock a secured area
- C. Sitting in close proximity to another person during a meeting
- D. Stealing information from another person's desk

Correct Option: A

EXPLANATION

Tailgating is following someone through an unlocked door.

90 What is the type of social engineering in which you ask someone for the information you want while making it appear as if the request is legitimate?

SELECT THE CORRECT ANSWER

- A. Phishing ✔
- B. Hoaxing
- C. Swimming
- D. Spamming

Correct Option: A

EXPLANATION

A phishing attempt makes the request look legitimate.

Comptia Security Plus Paper 2

1 Who runs the department responsible for the overall internal security of an organization?

SELECT THE CORRECT ANSWER

- A. CEO
- B. COO
- C. CISO ✓
- D. Hacker

Correct Option: C

EXPLANATION

The Chief Information Security Officer is responsible for the overall internal security of an organization.

2 A location from where security team performs monitoring and protection of assets is known as

SELECT THE CORRECT ANSWER

- A. Security Operation Center ✔
- B. Local Security Post
- C. Security Service Station
- D. Security Alert Control Center

Correct Option: A

EXPLANATION

A security team performs monitoring and protection of assets from a security operation center.

3 Who is the single point of communication (SPOC) for notifying security incidence?

SELECT THE CORRECT ANSWER

- A. NIIT
- B. NIST
- C. CIRT ✔
- D. CIOT

Correct Option: C

EXPLANATION

CIRT is the SPOC for notifying security incidence.

4 An attribute of a secure network where a sender cannot deny having sent a message is called

SELECT THE CORRECT ANSWER

A. Confidentiality

B. Integrity

C. Non-Repudiation ✔

D. Availability

Correct Option: C

EXPLANATION

Non-Repudiation ensures that a sender cannot deny sending a message.

5 An organization is about to establish a new division that will collaborate between software developer and system management team. What type of division can this be?

SELECT THE CORRECT ANSWER

- A. DevOps ✔
- B. DevSecOps
- C. DevOS
- D. DevNetwork

Correct Option: A

EXPLANATION

Development and operations or DevOps will help in the collaboration between developers and system administrators. It also helps embed the security function within these teams.

6 A company wants a Enterprise Risk Framework (ERM) in place. Which of the following ISO framework can be used for this?

SELECT THE CORRECT ANSWER

- A. ISO27001
- B. ISO9001
- C. ISO 31000 ✓
- D. ISO 21000

Correct Option: C

EXPLANATION

ISO 31000 is an overall framework for ERM.

7 Someone who performs hacking activity with the help of internet resources or tutorials but without proper knowledge of its working is known as a

SELECT THE CORRECT ANSWER

- A. Hacker
- B. Hackevist
- C. Script Kiddie ✔
- D. Cracker

Correct Option: C

EXPLANATION

A script kiddie uses hacker tools without necessarily understanding its.

8 What type of threat actors are involved in huge financial funding?

SELECT THE CORRECT ANSWER

A. State Actors

B. Criminal Syndicates

C. Competitors

D. All of the above ✓

Correct Option: D

EXPLANATION

State actors, criminal syndicate, and competitors are involved in huge financial funding.

9 What framework would you suggest your CEO as an effective threat intelligence platform?

SELECT THE CORRECT ANSWER

- A. IETE
- B. OSINT ✔
- C. ISO21K
- D. AIS

Correct Option: B

EXPLANATION

OSINT can be suggested as an effective threat intelligence platform.

10 Which command can be used to scan host request connection without acknowledging it?

SELECT THE CORRECT ANSWER

- A. nmap -sS IP address ✓
- B. nmap -s U IP address
- C. nmap -p IP address
- D. nmap IP address

Correct Option: A

EXPLANATION

nmap -sS IP address can be used to scan host request connection without acknowledging it.

11 A system administrator wants to connect the HTTP port on a server and return any banner by sending the head HTTP keyword. Which of the following command can be used for this?

SELECT THE CORRECT ANSWER

- (●) A. echo "head" | nc IP address -v 80 ✔
- ( ) B. echo "head" | nc IP address -v 22
- ( ) C. echo "head" | IP address -v 80
- ( ) D. echo "head" IP address -v 8080

Correct Option: A

EXPLANATION

The command that can be used is, echo "head" | nc IP address -v 80

12 A Linux server is reported to generate suspicious network traffic at TCP port. Which tool could you use in the terminal on the server to check which process is using a given TCP port?

SELECT THE CORRECT ANSWER

- A. netstat command
- B. netstat command ✓
- C. newton command
- D. netflip command

Correct Option: B

EXPLANATION

The netstat command helps identify the process which is using a given TCP port.

13 A dictionary of vulnerability in released softwares and operating systems is defined as

SELECT THE CORRECT ANSWER

A. Common Vulnerability Score

B. Common Vulnerabilities and Exposures ✓

C. Common Vulnerabilities Score Record

D. Common Vulnerabilities System

Correct Option: B

EXPLANATION

Common Vulnerabilities and Exposures is the dictionary of vulnerability in released softwares and operating systems.

14 A threat actor triggers a DDoS attack to distract security team and attempts to accelerate plans to achieve the objectives. What would you define this attempt by the threat actor as?

SELECT THE CORRECT ANSWER

- A. Maneuver ✔
- B. Containment
- C. Erection
- D. DDoS attack

Correct Option: A

EXPLANATION

This type of an attack can be termed as Maneuver.

15 A vulnerability scan reports that a CVE associated with CentOS Linux is present on a host, but you have established that the host is not running CentOS. What type of scanning error event is this?

SELECT THE CORRECT ANSWER

- A. False Negative
- B. True Positive
- C. True Negative
- D. False Positive ✔

Correct Option: D

EXPLANATION

A vulnerability scan reporting that a CVE associated with CentOS Linux is present on a host is false and that the host is not running CentOS is positive.

16 Your company designed a new game and released its beta version. It then asked the users to identify bugs or vulnerabilities in the game. One of the beta users identified that a new level is added right after the user loses in the current level. Procedurally, it's a false process, and the user reports this to the company. What is this process called?

SELECT THE CORRECT ANSWER

- A. Bug Hunting
- B. Bug Bounty ✔
- C. Bug Removal
- D. Bug Tracer

Correct Option: B

17 During a train journey, you meet a stranger, and both of you become friends. You share your date of birth, profession, contact no., and email ID. A few days after your journey, you find out that there were three unsuccessful attempts for changing your email password. What type of attack could it be?

SELECT THE CORRECT ANSWER

- A. Meeting Attack
- B. Social Engineering Attack ✓
- C. Foot Printing
- D. Tailgating

Correct Option: B

EXPLANATION

This type of attack is called Social Engineering.

18 The other day you found that your terminal was logged in without your knowledge, and some information related to your current project was truncated and altered. During the investigation, a video record showed that a few days back, the security camera position was changed and focused on your terminal. What type of attack is this?

SELECT THE CORRECT ANSWER

- (●) A. Shoulder Surfing ✓
- ( ) B. Social Engineering
- ( ) C. Sniffing
- ( ) D. Foot printing

Correct Option: A

EXPLANATION

This type of attack is called Shoulder surfing where the attacker can use high-powered lenses or cameras to observe the target without being nearby.

19 Persistences in context of pentest is known as

SELECT THE CORRECT ANSWER

- (●) A. Use of remote access tool ✓
- ( ) B. Use of secure trap door
- ( ) C. Use on anti virus
- ( ) D. Use of smart devices

Correct Option: A

EXPLANATION

Remote Access Tool (RAT) are used to perform pentest.

20 You receive the following email from your CEO. Dear employee, please share your account details to verify your account. Please transfer $500 to the following company link; this amount will be reverted to you after successfully confirming your account details. Regards, CEO XYZ Corp. What type of an attack is this?

SELECT THE CORRECT ANSWER

- A. Spam
- B. Whaling ✓
- C. Vishing
- D. SMIShing

Correct Option: B

EXPLANATION

Whaling is directed at higher management in the organization. The reluctance of the upper management to learn basic security procedures makes them vulnerable to these kinds of attacks.

21 You receive anonymous banking service calls where the caller asks for your credit card CVV or OTP or, at times even your debit card PIN. What are such attempts called?

SELECT THE CORRECT ANSWER

- A. Spear Phishing
- B. Vishing ✓
- C. Whaling
- D. Hacking

Correct Option: B

EXPLANATION

These types of attacks are called Vishing.

22 An email alert claims to have found some sort of security issues, such as a virus or malware, and offer a tool to fix the issue. What would you call this type of an email?

SELECT THE CORRECT ANSWER

- A. Hoaxes ✓
- B. Horcruxes
- C. dejavu
- D. Pharming

Correct Option: A

EXPLANATION

This type of emails are called hoaxes.

23 An activity in which a threat actor registers a domain name similar to a real one, sometimes with a minor change in spelling or shuffling of alphabets. For example, Original: www.simplilearn.com Fake: www.simplylearn.com What would you call this type of attack?

SELECT THE CORRECT ANSWER

- A. Pharming
- B. Typosquatting ✓
- C. Watering Hole attack
- D. Hoaxes

Correct Option: B

EXPLANATION

This type of an attack is called Typosquatting.

24 While drafting an IRP, the organization must determine which employees have the power to shut down systems in the event of a crisis. Which of the following assertions is being made here?

SELECT THE CORRECT ANSWER

A. Reporting and escalation procedures

B. Permission auditing

C. Roles and responsibilities ✓

D. Communication methodologies

Correct Option: C

EXPLANATION

Roles and responsibilities define the authority and responsibilities of employees in an organization.

25 A computer forensics analyst recovers a flash drive containing a single 500-page text file. Which of the following algorithms should be used by the analyst to verify the file's integrity?

SELECT THE CORRECT ANSWER

- A. 3DES
- B. AES
- C. MD5 ✓
- D. RSA

Correct Option: C

EXPLANATION

MD5 is a hash-algorithm to validate the integrity of the file.

26 To ascertain a malware's impact, a security manager wishes to conduct a test on a piece of it that has been isolated on a user's computer. Which of the following should be the security professional's first step?

SELECT THE CORRECT ANSWER

- A. Create a sandbox on the machine. ✔
- B. Open the file and run it.
- C. Create a secure baseline of the system state.
- D. Harden the machine.

Correct Option: A

EXPLANATION

Create a sandbox on the machine as the malware should be inspected only in isolated environment.

27

A system administrator wishes to deactivate usernames and passwords for SSH authentication and substituting them with key-based authentication. Which of the following measures should the administrator take next to authorize the new design?

SELECT THE CORRECT ANSWER

A. Issue a public/private key pair for each user and securely distribute a private key to each employee.

B. Instruct users on how to create a public/private key pair and install users' public keys on the server. ✔

C. Disable the username and password authentication and enable TOTP in the sshd.conf file.

D. Change the default SSH port, enable TCP tunneling, and provide a pre-configured SSH client.

Correct Option: B

28 During penetration test of a network, which of the following tools an administrator can use to identify potential attacks?

SELECT THE CORRECT ANSWER

- A. Netstat
- B. Honeypot
- C. Company directory
- D. Nmap ✓

Correct Option: D

EXPLANATION

Nmap is used for tracing all the footprints over a network.

29 On a Windows host, a security analyst is running a credential-based vulnerability scanner. The vulnerability scanner connects to various systems via the NetBIOS over TCP/IP protocol. However, one of the default ports on the system is open, due to which the scan produces no results. Identify that port.

SELECT THE CORRECT ANSWER

- A. 135
- B. 137 ✔
- C. 3389
- D. 5060

Correct Option: B

EXPLANATION

Port 137 is open, causing the scan to fail.

30

A hacker breaks into a network and contaminates many systems with various malware. The hacker then contacts the network admin and demands money to clean the contamination from the files. If the demand is not addressed, the hacker threatens to make the information about the breach public. What type of an attack best describes this?

SELECT THE CORRECT ANSWER

A. Gray hat hackers

B. Organized crime ✔

C. Insiders

D. Hacktivists

Correct Option: B

EXPLANATION

It is an organized crime where the hacker demands money and uses ransomware.

31 Which of the following is an algorithm family that was developed for use cases requiring low power consumption and processing power?

SELECT THE CORRECT ANSWER

- A. Elliptic curve ✔
- B. RSA
- C. Diffie-Hellman
- D. SHA

Correct Option: A

EXPLANATION

Elliptic curve algorithm is used in cases which require low power consumption and processing power.

32 A systems administrator is enhancing the security settings on a virtual host to ensure that users on one virtual machine cannot access data on another virtual machine. Which of the following vulnerability is being taken care of by the administrator?

SELECT THE CORRECT ANSWER

A. VM sprawl

B. VM escape ✔

C. VM migration

D. VM sandboxing

Correct Option: B

EXPLANATION

The administrator is taking care of the VM escape vulnerability.

33 During an incident response process, an administrator disables all unnecessary services which resulted in a data breach. What best describes this action?

SELECT THE CORRECT ANSWER

- A. Containment
- B. Eradication ✔
- C. Recovery
- D. Identification

Correct Option: B

EXPLANATION

Administrator has eradicated the weak services

34 Live acquisition of data in Forensic analysis is dependent on which of the following? (Select two)

SELECT THE CORRECT ANSWER(S)

A. Data Accessibility

B. Hash Algorithms

C. Value and volatility of data ✓

D. Right to audit clauses ✓

Correct Option: C, D

EXPLANATION

Live acquisition of data is dependent on value and volatility of data and the right to audit clause.

35 Which of the following is the main disadvantage of using SSO?

SELECT THE CORRECT ANSWER

- A. The architecture can introduce a single point of failure ✓
- B. Users need to authenticate for each resource they access
- C. It requires an organization to configure federation.
- D. The authentication is transparent to the user.

Correct Option: A

EXPLANATION

Single point of failure is the main disadvantage because when SSO fails, access to all related systems is lost.

36 Which of the following types of attack is used when an attacker responds by sending the attacking machine's MAC address in order to resolve the MAC address of the attacking machine to the IP address of a valid server?

SELECT THE CORRECT ANSWER

- A. Session hijacking
- B. IP spoofing
- C. Evil twin
- D. ARP poisoning ✓

Correct Option: D

EXPLANATION

ARP poisoning is used when an attacker responds by sending the attacking machine's MAC address in order to resolve the MAC address of the attacking machine to the IP address of a valid server.

37 The ability of a code to target a hypervisor from inside a guest OS is defined as

SELECT THE CORRECT ANSWER

- A. Fog Computing
- B. SDN
- C. Container and Docking
- D. VM escape ✔

Correct Option: D

EXPLANATION

VM escape allows a code to target a hypervisor from inside a guest OS.

38 You instruct the network administrator of your company to improve the security posture of the company. To comply with this, the network administrator installs an IDS. Which of the following control does an IDS provide?

SELECT THE CORRECT ANSWER

A. Physical

B. Detective ✔

C. Administrative

D. Corrective

Correct Option: B

EXPLANATION

An Intrusion Detection Systems (IDS) is used to search or detect any unwanted activity in a network.

39 The IT department of an organization processes sensitive data and not all employees have access to that. Since all the employees of the company share the same office space, what controls should be put in place to reduce the risk of accidental spillage of sensitive information?

SELECT THE CORRECT ANSWER

- A. Fix screen filters. ✔
- B. Place locks for computer cables
- C. Have an IDS within the office premises
- D. Use a DLP solution.

Correct Option: A

EXPLANATION

Screen filters will protect data from shoulder surfing.

40

A network system is used to store proprietary information and thus requires the highest level of security possible. Which of the following should be implemented by a security administrator to ensure that the system cannot be accessed via the Internet?

SELECT THE CORRECT ANSWER

- A. VLAN
- B. Air gap ✓
- C. NAT
- D. Firewall

Correct Option: B

EXPLANATION

Air gap ensures that the system cannot be access via the Internet.

41 A security administrator receives a request for certificates from a customer in order to securely access the servers. The customer wishes to receive a single encrypted file that is PKCS compatible and contains the private key. Which of the following formats is appropriate for the technician?

SELECT THE CORRECT ANSWER

- A. PEM ✓
- B. DER
- C. P12
- D. PFX

Correct Option: A

EXPLANATION

The PEM format contains meets the user needs.

42 A penetration tester is determining the vulnerability of an internal system to an attack via a remote listener. Which of the following commands should the penetration tester execute to determine the existence of this vulnerability? (Choose TWO).

SELECT THE CORRECT ANSWER(S)

- ✓ A. tcpdump ✓
- ✓ B. nc ✓
- C. nmap
- D. nslookup

Correct Option: A, B

EXPLANATION

The tcpdump command checks traffic to the listener and nc command checks services.

43 Which of the following attacks can be mitigated by proper data retention policies?

SELECT THE CORRECT ANSWER

- A. Dumpster diving ✓
- B. Man-in-the-browser
- C. Spear phishing
- D. Watering hole

Correct Option: A

EXPLANATION

Dumpster diving is fully mitigated by data retention policy.

44

A technician is performing a network security audit by connecting a laptop to open hardwired jacks throughout the facility to ensure they are inaccessible. Which of the following is under examination?

SELECT THE CORRECT ANSWER

- A. Layer 3 routing
- B. Port security ✔
- C. Secure IMAP
- D. S/MIME

Correct Option: B

EXPLANATION

Port security is under examination during this audit.

45 What should be the top priority for a CISO while conducting a business impact analysis (BIA) in the event of a natural disaster?

SELECT THE CORRECT ANSWER

A. Identify redundant and high-availability systems

B. Identify mission-critical applications and systems

C. Identify the single point of failure in the system

D. Identify the impact on safety of the property ✔

Correct Option: D

EXPLANATION

The CISO should identify the impact of the event on the safety of the property.

46 Perfect Forward Secrecy (PFS) ensures that a compromise of a server's private key does not result in the decryption of the traffic sent in the past to that server. True or False?

SELECT THE CORRECT ANSWER

- (●) A. TRUE ✔
- ( ) B. FALSE

Correct Option: A

EXPLANATION

True as PFS ensures that the keys used to encrypt each session are destroyed after use.

47 Which mode of operation for bulk encryption ciphers provides the highest level of security?

SELECT THE CORRECT ANSWER

- A. Authentication Encryption with Additional Data (AEAD) ✓
- B. Systematic Data Encryption (SDE)
- C. Authentication and Trust Data (ATD)
- D. Perfect Forward Policy (PFP)

Correct Option: A

EXPLANATION

Counter modes implementing AEAD provides highest level of security

48 What type of brute attack focuses on exploiting collisions in a hash function?

SELECT THE CORRECT ANSWER

- A. DDoS
- B. Birthday attack ✔
- C. Target Attack
- D. Passive Attack

Correct Option: B

EXPLANATION

Birthday attack focuses on exploiting collisions in a hash function

49 Your company develops software that requires a database of encrypted passwords to be stored. What security controls can be put in place to increase the database's resistance to brute force attacks?

SELECT THE CORRECT ANSWER

- A. Using a key stretching password storage library ✓
- B. Using a key Encryption
- C. Using a PKI
- D. Using DES

Correct Option: A

EXPLANATION

Using a key stretching password storage library can increase the database's resistance to brute force attack.

50 Which cryptographic technology is used to share medical records with a data analytics firm?

SELECT THE CORRECT ANSWER

A. Isomorphic encryption

B. Homomorphic encryption ✔

C. DES

D. 3-DES

Correct Option: B

EXPLANATION

Homomorphic encryption performs calculations while preserving privacy and confidentiality with encrypted data.

51 In a simple model, which CA issues certificates to users and users only trust certificates issued by this CA?

SELECT THE CORRECT ANSWER

A. Intermediate CA

B. Single CA ✓

C. Self Certificate

D. Online CA

Correct Option: B

EXPLANATION

Single CA issues certificates and users only trust these certificates in a simple model.

52 Which CA supports access permissions for each certificate type such that you can choose which accounts are able to issue them?

SELECT THE CORRECT ANSWER

A. Linux CA

B. Mac CA

C. Windows CA ✔

D. Offline CA

Correct Option: C

EXPLANATION

Windows CA supports access permissions for each certificate type.

53 Which of the following is a weakness of a hierarchical trust model?

SELECT THE CORRECT ANSWER

- A. The structure depends on the integrity of the root CA. ✓
- B. The structure depends on the self-signed CA.
- C. Only code signing CA is possible for issue.
- D. Does not support Email/User certificate

Correct Option: A

EXPLANATION

Hierarchical trust model structure depends on the integrity of the root CA.

54 A three-factor authentication requires a password, PIN, and smart card. True or False?

SELECT THE CORRECT ANSWER

- (●) A. FALSE ✓
- ( ) B. TRUE

Correct Option: A

EXPLANATION

Three-factor authentication includes a biometric-, behavioral-, or location-based element. The password and PIN elements belong to the same factor (something that you know).

55 Which method implements location-based authentication?

SELECT THE CORRECT ANSWER

- A. Geolocation by IP ✓
- B. Geotagging
- C. Geofencing
- D. Geo Mapping

Correct Option: A

EXPLANATION

IP queries the location service running on a device or geolocation.

56 Is this true or false? Kerberos authenticates the user by passing the user's password to the target application server.

SELECT THE CORRECT ANSWER

A. TRUE

B. FALSE ✓

Correct Option: B

EXPLANATION

KDC verifies the user credential. The Ticket Granting Service (TGS) sends the user's account details (SID) to the target application for authorization.

57 Client authentication to the server is done using:

SELECT THE CORRECT ANSWER

- A. EDUS
- B. RADIUS ✓
- C. KERBEROS
- D. NAS

Correct Option: B

EXPLANATION

RADIUS allows client authentication to the server.

58 How do you implement a fingerprint reader as hardware?

SELECT THE CORRECT ANSWER

- A. As a resistive cell
- B. As a capacitive cell ✔
- C. As a RFID tag
- D. Aa a bluetooth receiver

Correct Option: B

EXPLANATION

A fingerprint reader is implemented as a hardware in the form of a capacitive cell.

59 One of your employee is leaving your organization. You ask your HR manager to conduct an exit meeting to ensure that the employee leaves the company gracefully. This act is known as:

SELECT THE CORRECT ANSWER

A. Exit Procedure

B. Offboarding policies ✓

C. Termination procedure

D. Farewell

Correct Option: B

EXPLANATION

Offboarding policies ensure that an employee leaves a company gracefully.

60 Secure Shell (SSH) protocol is very likely to be used to manage devices and services. What are the two types of key pairs used by SSH?

SELECT THE CORRECT ANSWER

- A. Host and User Key Pair ✔
- B. Client and Service Key
- C. Public and Private Key
- D. Symmetric and Asymmetric Key

Correct Option: A

EXPLANATION

Host and user key pair are the two types of key pairs used by SSH to manage devices and services.

61 What is the step-by-step listing of actions that must be completed for any given task?

SELECT THE CORRECT ANSWER

- A. ROP
- B. SOP ✓
- C. TOP
- D. POP

Correct Option: B

EXPLANATION

A Standard Operating Procedure (SOP) is the step-by-step listing of actions.

62 What procedure is followed to ensure that accounts are created for valid users, appropriate privileges are assigned, and only the valid user is aware of the credentials?

SELECT THE CORRECT ANSWER

- A. Offboarding
- B. Onboarding ✔
- C. Resource Privileges
- D. SOP

Correct Option: B

EXPLANATION

Onboarding ensures that accounts are created for valid users, they are provided with appropriate privileges, and only valid users are aware of their credentials.

63 Which container applies different security policies to a subset of objects within the same domain?

SELECT THE CORRECT ANSWER

A. Structured Unit (SU)

B. Process Unit (PU)

C. Organization Unit (OU) ✓

D. Terminal Unit (TU)

Correct Option: C

EXPLANATION

Organization unit applies different security policies to a subnet of objects within the same domain.

64 Which policy prevents users from selecting old passwords?

SELECT THE CORRECT ANSWER

A. Local data policy

B. Enforce password history ✓

C. Password encryption

D. Hash function

Correct Option: B

EXPLANATION

Enforce password history policy prevents users from selecting or choosing old passwords.

65 For a firm, which system implementation restricts a visitor's access to the firm's network infrastructure when the visitor agrees to the AUP?

SELECT THE CORRECT ANSWER

A. WiFi-protected setup

B. Password authentication protocol

C. Captive portal ✓

D. RADIUS

Correct Option: C

EXPLANATION

Captive portal restricts a visitor's access to the firm's network infrastructure when the visitor agrees to the AUp.

66 Which of the following explains the implementation of enterprise DMZ?

SELECT THE CORRECT ANSWER(S)

A. Using 1 firewall

B. Using 2 firewall ✓

C. Using triple-homed firewall ✓

D. Using honey pot

Correct Option: B, C

EXPLANATION

You can either use two firewalls (one external and one internal) around a screened subnet, or use a triple-homed firewall (one with three network interfaces) to implement an enterprise DMZ.

67 Which of the following option prevents an attacker from engineering a switching loop from a host connected to a standard switch port?

SELECT THE CORRECT ANSWER

- A. Using portfast and BPDU guard ✓
- B. Using EGP guard
- C. Using terminal protection procedure
- D. Mitigating MiTM attack

Correct Option: A

EXPLANATION

Using portfast and BPDU guard prevents an attacker from engineering a switching loop from a host connected to a standard switch port.

68

Ben is on a business trip with company owned laptop for official use. When he checks into his hotel, he turns on his laptop and discovers a wireless access point bearing the hotel's name, which he uses to send official communications. Which wireless threat is he at risk of becoming a victim of?

SELECT THE CORRECT ANSWER

- A. Ransomware
- B. Birthday Attack
- C. Evil Twin ✔
- D. MiTM

Correct Option: C

EXPLANATION

Ben is at risk of becoming a victim of Evil Twin attack when he uses a wireless access point to send official communications.

69 True or false? A virtual IP allows two appliances to be in a fault tolerant configuration to respond to requests of the same IP address.

SELECT THE CORRECT ANSWER

- (●) A. TRUE ✔
- ( ) B. FALSE

Correct Option: A

EXPLANATION

Virtual IP doesn't correspond to an actual physical network interface

70 What purpose does the default rule on a firewall have?

SELECT THE CORRECT ANSWER

- (●) A. Block traffic that is not specifically allowed ✓
- ( ) B. Block any traffic specifically allowed
- ( ) C. Not block any traffic specifically allowed
- ( ) D. Not block any traffic not specifically allowed

Correct Option: A

EXPLANATION

The default rule on a firewall blocks all traffic that is not specifically allowed.

71 Which of the following is a security protocol that protects HTTP and HTTPS applications and can be configured to include signatures for known application-level attacks, such as injection-based or scanning attacks?

SELECT THE CORRECT ANSWER

- A. Web Application Firewall (WAF) ✓
- B. Web Service Firewall (WSF)
- C. Data Protection Firewall (APF)
- D. IDS/IPS

Correct Option: A

EXPLANATION

WAF is a security protocol used to protect HTTP and HTTPS applications.

72 Which product collects IDS alerts and host logs from multiple sources and then performs correlation analysis on the observables to detect indicators of compromise and inform administrators of potential incidents?

SELECT THE CORRECT ANSWER

A. Product Information and Event Management (PIEM)

B. Security Information and Event Management (SIEM) ✔

C. Data and Event Management (DEM)

D. Event and Security Management (ESM)

Correct Option: B

EXPLANATION

Security Information and Event Management collects IDS alerts and host logs from multiple sources and then performs correlation analysis.

73 What are the vulnerabilites exposed by a rogue DHCP server?

SELECT THE CORRECT ANSWER

- A. DoS and Spoofing ✓
- B. Phishing and Masking
- C. Spamming and Flooding
- D. DOS and Flooding

Correct Option: A

EXPLANATION

Denial of service (DoS) and spoofing are the vulnerabilities exposed by a rogue DHCP server.

74 What is the key strength of the symmetric encryption algorithm if a cipher suite ECDHE-ECDSA AES256-GCM-SHA384 is used for the TLS session?

SELECT THE CORRECT ANSWER

- A. AES
- B. 128 Bit AES
- C. 256 Bit AES ✔
- D. 512 Bit AES

Correct Option: C

EXPLANATION

256 Bit AES is the key strength of the symmetric encryption algorithm for a cipher suite of ECDHE-ECDSA AES256-GCM-SHA384 for a TLS session.

75 Which security protocol and port is used by the SFTP to secure the connection and listen by default?

SELECT THE CORRECT ANSWER

- A. Secure Shell (SSH) over TCP port 128.
- B. Secure Shell (SSH) over TCP port 22. ✔
- C. Secure Shell (SSH) over TCP port 80
- D. Secure Shell (SSH) over TCP port 100.

Correct Option: B

EXPLANATION

Secure Shell over TCP Port 22 is used by the SFTP to secure the connection and listen by default.

76 True or false? A TLS VPN provideS access to web-based network resources.

SELECT THE CORRECT ANSWER

A. TRUE

B. FALSE ✓

Correct Option: B

EXPLANATION

Encapsulation of private network data is done by TLS (Transport Layer Security) VPN using TLS. This data can be frames or IP-level packets. it is not constrained by application-layer protocol.

77 Which is the appropriate interoperability agreement at the outset of two companies agreeing to work together?

SELECT THE CORRECT ANSWER

A. LOR

B. SLR

C. SLM

D. MOU ✓

Correct Option: D

EXPLANATION

MOU is the interoperability agreement used at the outset of two companies working together.

78 Which analysis tool is used to detect a process that is performing data exfiltration without being detected as a malware by the antivirus software?

SELECT THE CORRECT ANSWER

A. Local Anti Virus Tool

B. Windows Defender

C. Sandbox with Monitoring tool ✓

D. APT Scanner

Correct Option: C

EXPLANATION

A sandbox with monitoring tools is used to detect a process that is performing data exfiltration without being detected as a malware by the antivirus software.

79 It is a good practice to secure your smartphone from unauthorized access if it is stolen. Which is the best security control that can be implemented for this purpose?

SELECT THE CORRECT ANSWER

- (●) A. Screen Lock ✓
- ( ) B. App Lock
- ( ) C. Sim Lock
- ( ) D. Power Lock

Correct Option: A

EXPLANATION

Screen lock is the best security control used to prevent unauthorized access to your stolen smartphone.

80

Donald is a sales executive who attends professional conferences with representatives from competitor companies. He connects with the clients at the conference using his smartphone and a Bluetooth headset. It came to his notice that competitors' sales representatives are influencing his key connections by revealing private information from his email and calendar. Which is the wireless threat involved here?

SELECT THE CORRECT ANSWER

A. Bluejacking

B. Bluesnarfing ✓

C. Session Overloading

D. Sniffing and Flooding

Correct Option: B

EXPLANATION

Bluesnarfing refers to the stealing of confidential information from bluetooth devices without the

81 What general class of attack is designed to mitigate security issues and ensure that the requests from front-end web servers are authenticated?

SELECT THE CORRECT ANSWER

- A. XSS Attack
- B. SSRF ✔
- C. DoS
- D. Session Hijacking

Correct Option: B

EXPLANATION

Server-Side Request Forgery (SSRF) makes an arbitrary request to a back-end server using the public server. If the threat actor must defeat an authentication or authorization mechanism between a web server and a database server, then this made more complex.

82 If you have Microsoft Office Desktop app, you don't have to address the document security and the risks posed by the embedded macros and scripts.

SELECT THE CORRECT ANSWER

- A. Yes
- B. No ✔
- C. May be

Correct Option: B

EXPLANATION

Visual Basic for Applications (VBA) is used only with Microsoft Office. For macros, OpenOffice and LibreOffice use scripting language.

83 You are a policy writer for cloud resources. Which format will you use to write PaaS policies?

SELECT THE CORRECT ANSWER

- A. Java
- B. Go
- C. Python
- D. JSON ✓

Correct Option: D

EXPLANATION

JSON is used to write PaaS policies.

84

For customer management, a company is using a custom-developed client-server application that can be accessed from remote sites via a VPN. Rapid overseas expansion has resulted in numerous employee complaints, such as the system experiencing frequent outages and not being able to handle the increased number of users and access via client devices like smartphones. What kind of architecture could result in a more scalable solution?

SELECT THE CORRECT ANSWER

- A. Microservices ✓
- B. PaaS
- C. AaaS
- D. API
- E. IaaS

85 You're applying a solution overview on privacy-enhancing technologies based on the CompTIA Security+ syllabus objectives. You've finished taking notes under the following headings; which other report section do you need? Anonymization, Pseudo-Anonymization, Data Masking, Aggregation/Banding

SELECT THE CORRECT ANSWER

A. Containerization

B. Tokenization ✓

C. Aggregation

D. Hashing and Salting

Correct Option: B

EXPLANATION

Replacement of data with a randomly generated token from a separate token server or vault is know as tokenization. It reconstructs the original data when combined with the token vault.

86 Consider that you are providing security consulting to a company to improve their incident response procedures. The business manager is curious on the use of a out-of-band contact mechanism for responders. What is the reason for this?

SELECT THE CORRECT ANSWER

- A. The response team needs a secure channel to communicate over without alerting the threat actor. ✓
- B. The response team uses the Create Action Building plan.
- C. The response team needs forensic cover.
- D. The third party suggestions are marked for solutions.

Correct Option: A

87 Which software tool is used to forward Windows event logs to Syslog-compatible server

SELECT THE CORRECT ANSWER

A. Nmap tool

B. BeIFF tool

C. Nxlog tool ✓

D. Oven tool

Correct Option: C

EXPLANATION

Nxlog is the software tool used to forward Windows event logs to Syslog-compatible server.

88 If you want to recover the contents of the ARP cache as vital evidence of a man-in- the-middle attack. Is it the right option to shutdown the PC and image the hard drive to safeguard these contents?

SELECT THE CORRECT ANSWER

- A. Yes
- B. No ✓
- C. May Be

Correct Option: B

EXPLANATION

Shutting down the system will discard ARP cache contents as these are stored in the memory. It is a good option to dump the system memory or execute the ARP utility and taking a screenshot.

89

A mail server is being configured by an email systems administrator to prevent spear phishing attacks via email messages. Which of the following options illustrates the administrator's actions?

SELECT THE CORRECT ANSWER

A. Risk avoidance

B. Risk mitigation ✔

C. Risk transference

D. Risk acceptance

Correct Option: B

EXPLANATION

An administrator configuring a mail server to prevent spear phishing attacks via email messages is referred to as risk mitigation.

90 The junior systems administrator observed a red error notification on one of the two hard drives in a server room. The administrator replaced the hard drive but was unaware that the server was set up in an array. Which of the following configurations would ensure no data loss?

SELECT THE CORRECT ANSWER

A. RAID 0

B. RAID 1 ✔

C. RAID 2

D. RAID 3

Correct Option: B

EXPLANATION

RAID 1 configuration would ensure no data loss when there is an error notification from the hardware that was set up in an array.