CompTIA Security+ SY0-601 Practice Questions

August 2021

Questions 238

Exam A

QUESTION 1
A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?

A. Nmap
B. Wireshark
C. Autopsy
D. DNSEnum

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 2
A network administrator has been asked to design a solution to improve a company's security posture The administrator is given the following, requirements?
* The solution must be inline in the network
* The solution must be able to block known malicious traffic
* The solution must be able to stop network-based attacks Which of the following should the network administrator implement to BEST meet these requirements?

A. HIDS
B. NIDS
C. HIPS
D. NIPS

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 3
A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?

A. A non-disclosure agreement
B. Least privilege
C. An acceptable use policy
D. Offboarding

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 4
A network engineer needs to build a solution that will allow guests at the company's headquarters to access the Internet via WiFi. This solution should not allow access to the internal corporate network, but it should require guests to sign off on the acceptable use policy before accessing the Internet. Which of the following should the

engineer employ to meet these requirements?

A. Implement open PSK on the APs
B. Deploy a WAF
C. Configure WIPS on the APs
D. Install a captive portal

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 5
Which of the following will provide the BEST physical security countermeasures to stop intruders? (Select TWO.)

A. Alarms
B. Signage
C. Lighting
D. Mantraps
E. Fencing
F. Sensors

Correct Answer: DE
Explanation

Explanation/Reference:
Section:

QUESTION 6
Under GDPR, which of the following is MOST responsible for the protection of privacy and website user rights?

A. The data protection officer
B. The data processor
C. The data owner
D. The data controller

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 7
An analyst needs to identify the applications a user was running and the files that were open before the user's computer was shut off by holding down the power button. Which of the following would MOST likely contain that information?

A. NGFW
B. Pagefile
C. NetFlow
D. RAM

Correct Answer: B

Explanation

Explanation/Reference:
Section:

QUESTION 8
A user enters a password to log in to a workstation and is then prompted to enter an authentication code. Which of the following MFA factors or attributes are being utilized in the authentication process? (Select TWO).

A. Something you know
B. Something you have
C. Somewhere you are
D. Someone you are
E. Something you are
F. Something you can do

Correct Answer: AB
Explanation

Explanation/Reference:
Section:

QUESTION 9
A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Choose two.)

A. Perform a site survey
B. Deploy an FTK Imager
C. Create a heat map
D. Scan for rogue access points
E. Upgrade the security protocols
F. Install a captive portal

Correct Answer: AC
Explanation

Explanation/Reference:
Section:

QUESTION 10
A security analyst is using a recently released security advisory to review historical logs, looking for the specific activity that was outlined in the advisory. Which of the following is the analyst doing?

A. A packet capture
B. A user behavior analysis
C. Threat hunting
D. Credentialed vulnerability scanning

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 11
An organization's help desk is flooded with phone calls from users stating they can no longer access certain websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command: ipconfig /flushdns, but the issue persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away. Which of the following attacks MOST likely occurred on the original DNS server?

A. DNS cache poisoning
B. Domain hijacking
C. Distributed denial-of-service
D. DNS tunneling

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 12
In which of the following risk management strategies would cybersecurity insurance be used?

A. Transference
B. Avoidance
C. Acceptance
D. Mitigation

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 13
The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve in the environment patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have been provided to frontline staff, and a risk analysis has not been performed. Which of the following is the MOST likely cause of the CRO's concerns?

A. SSO would simplify username and password management, making it easier for hackers to pass guess accounts.
B. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.
C. SSO would reduce the password complexity for frontline staff.
D. SSO would reduce the resilience and availability of system if the provider goes offline.

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 14
A security engineer is reviewing log files after a they discovered usernames and passwords for the organization's accounts are being offered on the dark web for sale. The engineer sees there was a change in the IP address for a vendor website than what was there earlier. This change lasted eight hours. Which of the following attacks was MOST likely used?

A. Man-in- the middle
B. Spear-phishing
C. Evil twin
D. DNS poisoning

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 15
A user recent an SMS on a mobile phone that asked for bankdetails. Which of the following social-engineering techniques was used in this case?

A. SPIM
B. Vishing
C. Spear phishing
D. Smishing

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 16
A consultant is configuring a vulnerability scanner for a large, global organization in multiple countries. The consultant will be using a service account to scan systems with administrative privileges on a weekly basis, but there is a concern that hackers could gain access to the account and pivot through the global network. Which of the following would be BEST to help mitigate this concern?

A. Create consultant accounts for each region, each configured with push MFA notifications.
B. Create one global administrator account and enforce Kerberos authentication
C. Create different accounts for each region. limit their logon times, and alert on risky logins
D. Create a guest account for each region. remember the last ten passwords, and block password reuse

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 17
A Chief Security Office's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?

A. Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.
B. Purchase cyber insurance from a reputable provider to reduce expenses during an incident.
C. Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.
D. Implement application whitelisting and centralized event-log management, and perform regular testing and

validation of full backups.

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 18
A security analyst is investigation an incident that was first reported as an issue connecting to network shares and the internet, While reviewing logs and tool output, the analyst sees the following:

IP address Physical addess
10.0.0.1 00-18-21-ad-24-bc
10.0.0.114 01-31-a3-ad-23-ab
10.0.0.115 00-18-21-ad-24-bc
10.0.0.116 00-19-08-ba-07-da
10.0.0.117 01-12-21-ca-11-ad

Which of the following attacks has occurred?

A. IP conflict
B. Pass-the-hash
C. MAC flooding
D. Directory traversal
E. ARP poisoning

Correct Answer: E
Explanation

Explanation/Reference:
Section:

QUESTION 19
The IT department's on-site developer has been with the team for many years. Each time an application is released, the security team is able to identify multiple vulnerabilities. Which of the following would BEST help the team ensure the application is ready to be released to production?

A. Limit the use of third-party libraries.
B. Prevent data exposure queries.
C. Obfuscate the source code.
D. Submit the application to QA before releasing it.

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 20
A software developer needs to perform code-execution testing, black-box testing, and non- functional testing on a new product before its general release. Which of the following BEST describes the tasks the developer is conducting?

A. Verification
B. Validation

C. Normalization
D. Staging

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 21
An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state?

A. The system was configured with weak default security settings.
B. The device uses weak encryption ciphers.
C. The vendor has not supplied a patch for the appliance.
D. The appliance requires administrative credentials for the assessment.

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 22
A cybersecurity analyst needs to implement secure authentication to third-party websites without users' passwords. Which of the following would be the BEST way to achieve this objective?

A. OAuth
B. SSO
C. SAML
D. PAP

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 23
A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company information on user devices. Which of the following solutions would BEST support the policy?

A. Mobile device management
B. Full-device encryption
C. Remote wipe
D. Biometrics

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 24

An organization is concerned that its hosted web servers are not running the most updated version of the software. Which of the following would work BEST to help identify potential vulnerabilities?

A. Hping3 -s comptia.org -p 80
B. Nc -1 -v comptia.org -p 80
C. nmap comptia.org -p 80 -AV
D. nslookup -port=80 comptia.org

Correct Answer: C
Explanation

Explanation/Reference:
Section:
Explanation:

nc & namp both would have worked. But only Nmap command is correcty formatted to be useful.
-V shows the current version; -A shows all info

QUESTION 25
A researcher has been analyzing large data sets for the last ten months. The researcher works with colleagues from other institutions and typically connects via SSH to retrieve additional data. Historically, this setup has worked without issue, but the researcher recently started getting the following message:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@   WARNING:  REMOTE HOST IDENTIFICATION HAS CHANGED!    @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
The fingerprint for the RSA key sent by the remote host is
SHA256:cBqYjal6ToV3jEIJHUSKtjjVziqnVd4Cz+1fhTM6+k4.
Please contact your system administrator.
RSA host key for 18.231.33.78 has changed and you have reque
Host key verification failed.
```

Which of the following network attacks is the researcher MOST likely experiencing?

A. MAC cloning
B. Evil twin
C. Man-in-the-middle
D. ARP poisoning

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 26
An employee has been charged with fraud and is suspected of using corporate assets. As authorities collect evidence, and to preserve the admissibility of the evidence, which of the following forensic techniques should be used?

A. Order of volatility
B. Data recovery
C. Chain of custody
D. Non-repudiation

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 27
A company has limited storage available and an online presence that cannot be interrupted for more than four hours. Which is the FASTEST database restore time in the event of a failure, which being mindful of the limited available storage space?

A. Implement fulltape backup every Sunday at 8:00 p.m and perform nightly tape rotations.
B. Implement differential backups every Sunday at 8:00 and nightly incremental backups at 8:00 p.m
C. Implement nightly full backups every Sunday at 8:00 p.m.
D. Implement full backups every Sunday at 8:00 p.m and nightly differential backups at 8:00 p.m.

Correct Answer: D
Explanation

Explanation/Reference:
Section:

Explanation:
Best possible answer. Shortest Recovery Time Objective.

QUESTION 28
Users have been issued smart cards that provide physical access to a building. The cards also contain tokens that can be used to access information systems. Users can log in to any thin client located throughout the building and see the same desktop each time. Which of the following technologies are being utilized to provide these capabilities? (Select TWO)

A. COPE
B. VDI
C. GPS
D. TOTP
E. RFID
F. BYOD

Correct Answer: BE
Explanation

Explanation/Reference:
Section:

QUESTION 29
The SOC is reviewing process and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected host was the best course of action. The allowed the malware to spread to additional hosts before it was contained. Which of the following would be BEST to improve the incident response process?

A. Updating the playbooks with better decision points
B. Dividing the network into trusted and untrusted zones
C. Providing additional end-user training on acceptable use
D. Implementing manual quarantining of infected hosts

Correct Answer: A
Explanation

Explanation/Reference:
Section:

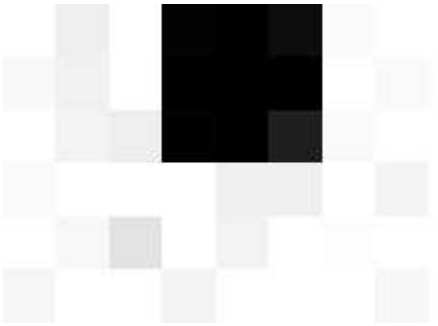
QUESTION 30
A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicates a directory-traversal attack has occurred. Which of the following is the analyst MOST likely seeing?

Option A: http://sample.url.com/<script>Please -Visit-Our-Phishing-Site</script>

Option B: http://sample.url.com/someotherpage onsite/../../../etc/shadow

Option C: http://sample.url.com/select-from-database-where-password-null

Option D:http://redirect.sample.url.sampleurl.com/malicios-dns-redirect



A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 31
A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

A. Segmentation
B. Firewall whitelisting
C. Containment
D. isolation

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 32
A manufacturer creates designs for very high security products that are required to be protected and controlled by the government regulations. These designs are not accessible by corporate networks or the Internet. Which of the following is the BEST solution to protect these designs?

A. An air gap
B. A Faraday cage
C. A shielded cable
D. A demilitarized zone

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 33
A security analyst is reviewing the following attack log output:
user comptia\john.smith attempted login with password123
user comptia\jane.doe attempted login with password123
user comptia\user.one attempted login with password123
user comptia\user.two attempted login with password123
user comptia\user.three attempted login with password123
user comptia\john.smith attempted login with password234
user comptia\jane.doe attempted login with password234
user comptia\user.one attempted login with password234
user comptia\user.two attempted login with password234
user comptia\user.three attempted login with password234

Which of the following types of attacks does this MOST likely represent?

A. Rainbow table
B. Brute-force
C. Password-spraying
D. Dictionary

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 34
A security auditor is reviewing vulnerability scan data provided by an internal security team. Which of the following BEST indicates that valid credentials were used?

A. The scan identified expired SSL certificates
B. The scan enumerated software versions of installed programs
C. The scan produced a list of vulnerabilities on the target host
D. The scan results show open ports, protocols, and services exposed on the target host

Correct Answer: B
Explanation

Explanation/Reference:
Section:
Explanations:
Enumerating software versions takes more permissions to run.

QUESTION 35
An organization hired a consultant to assist with an active attack, and the consultant was able to identify the compromised accounts and computers. Which of the following is the consultant MOST likely to recommend to prepare for eradication?

A. Quarantining the compromised accounts and computers, only providing them with network access
B. Segmenting the compromised accounts and computers into a honeynet so as to not alert the attackers.
C. Isolating the compromised accounts and computers, cutting off all network and internet access.
D. Logging off and deleting the compromised accounts and computers to eliminate attacker access.

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 36
The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

A. Install a NIDS device at the boundary.
B. Segment the network with firewalls.
C. Update all antivirus signatures daily.
D. Implement application blacklisting.

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 37
An organization suffered an outage and a critical system took 90 minutes to come back online. Though there was no data loss during the outage, the expectation was that the critical system would be available again within 60 minutes Which of the following is the 60-minute expectation an example of:

A. MTBF
B. RPO
C. MTTR
D. RTO

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 38
Which of the following will MOST likely adversely impact the operations of unpatched traditional programmable-logic controllers, running a back-end LAMP server and IOT systems with human-management interfaces that are accessible over the Internet via a web interface? (Choose two.)

A. Cross-site scripting
B. Data exfiltration
C. Poor system logging
D. Weak encryption
E. SQL injection
F. Server-side request forgery

Correct Answer: CD
Explanation

Explanation/Reference:
Section:

QUESTION 39
Which of the following BEST describes a security exploit for which a vendor patch is not readily available?

A. Integer overflow
B. Zero-day
C. End of life
D. Race condition

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 40
A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers the company is unable to upgrade the encryption standard. Which of the following types of controls should be used to reduce the risk created by this scenario?

A. Physical
B. Detective
C. Preventive
D. Compensating

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 41
While checking logs, a security engineer notices a number of end users suddenly downloading files with the .tar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?

A. A RAT was installed and is transferring additional exploit tools.
B. The workstations are beaconing to a command-and-control server.
C. A logic bomb was executed and is responsible for the data transfers.
D. A fileless virus is spreading in the local network environment.

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 42
A security auditor is reviewing vulnerability scan data provided by an internal security team. Which of the following BEST indicates that valid credentials were used?

A. The scan results show open ports, protocols, and services exposed on the target host
B. The scan enumerated software versions of installed programs
C. The scan produced a list of vulnerabilities on the target host
D. The scan identified expired SSL certificates

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 43
The IT department at a university is concerned about professors placing servers on the university network in an attempt to bypass security controls. Which of the following BEST represents this type of threat?

A. A script kiddie
B. Shadow IT
C. Hacktivism
D. White-hat

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 44
A security analyst is preparing a threat for an upcoming internal penetration test. The analyst needs to identify a method for determining the tactics, techniques, and procedures of a threat against the organization's network. Which of the following will the analyst MOST likely use to accomplish the objective?

A. A table exercise
B. NST CSF
C. MITRE ATT&CK
D. OWASP

Correct Answer: C
Explanation

Explanation/Reference:

Section:
Explanation:
MITRE ATT&CK, an open framework and knowledge base of adversary tactics and techniques based on real-world observations, provides a structured method to help you answer these questions.
ATT&CK is a powerful way to classify and study adversary techniques and understand their intent. You can use it to enhance, analyze, and test your threat hunting and detection efforts.

QUESTION 45
A company wants to deploy PKI on its Internet-facing website. The applications that are currently deployed are:
* www.company.com (main website)
* contactus.company.com (for locating a nearby location)
* quotes.company.com (for requesting a price quote)
The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com. Which of the following certificate types would BEST meet the requirements?

A. SAN
B. Wildcard
C. Extended validation
D. Self-signed

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 46
A company recently moved sensitive videos between on-premises. Company-owned websites. The company then learned the videos had been uploaded and shared to the internet. Which of the following would MOST likely allow the company to find the cause?

A. Checksums
B. Watermarks
C. Oder of volatility
D. A log analysis
E. A right-to-audit clause

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 47
A network engineer notices the VPN concentrator overloaded and crashes on days when there are a lot of remote workers. Senior management has placed greater importance on the availability of VPN resources for the remote workers than the security of the end users' traffic. Which of the following would be BEST to solve this issue?

A. iPSec
B. Always On
C. Split tunneling
D. L2TP

Correct Answer: C

Explanation

Explanation/Reference:
Section:

QUESTION 48
A security analyst has been asked to investigate a situation after the SOC started to receive alerts from the SIEM. The analyst first looks at the domain controller and finds the following events:

Keywords	Date and time	Source	Event ID
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:22 PM	Microsoft Windows security auditing	4771

To better understand what is going on, the analyst runs a command and receives the following output:

name	lastbadpasswordattempt	badpwdcount
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst's findings, which of the following attacks is being executed?

A. Credential harvesting
B. Keylogger
C. Brute-force
D. Spraying

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 49
A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices. Which of the following technologies would be BEST to balance the BYOD culture while also protecting the company's data?

A. Containerization
B. Geofencing
C. Full-disk encryption
D. Remote wipe

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 50
Which of the following BEST explains the reason why a server administrator would place a document named password.txt on the desktop of an administrator account on a server?

A. The document is a honeyfile and is meant to attract the attention of a cyberintruder.
B. The document is a backup file if the system needs to be recovered.
C. The document is a standard file that the OS needs to verify the login credentials.
D. The document is a keylogger that stores all keystrokes should the account be compromised.

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 51
A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts ineffective. Which of the following would BEST detect the presence of a rootkit in the future?

A. FDE
B. NIDS
C. EDR
D. DLP

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 52
Company engineers regularly participate in a public Internet forum with other engineers throughout the industry. Which of the following tactics would an attacker MOST likely use in this scenario?

A. Watering-hole attack
B. Credential harvesting
C. Hybrid warfare
D. Pharming

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 53
Which of the following refers to applications and systems that are used within an organization without consent or approval?

A. Shadow IT
B. OSINT
C. Dark web
D. Insider threats

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 54
In the middle of a cybersecurity incident, a security engineer removes the infected devices from the network and lock down all compromised accounts. In which of the following incident response phases is the security engineer currently operating?

A. Identification
B. Preparation
C. Eradiction
D. Recovery
E. Containment

Correct Answer: E
Explanation

Explanation/Reference:
Section:

QUESTION 55
Which of the following is the purpose of a risk register?

A. To define the level or risk using probability and likelihood
B. To register the risk with the required regulatory agencies
C. To identify the risk, the risk owner, and the risk measures
D. To formally log the type of risk mitigation strategy the organization is using

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 56
A pharmaceutical sales representative logs on to a laptop and connects to the public WiFi to check emails and update reports. Which of the following would be BEST to prevent other devices on the network from directly accessing the laptop? (Choose two.)

A. Trusted Platform Module

B. A host-based firewall
C. A DLP solution
D. Full disk encryption
E. A VPN
F. Antivirus software

Correct Answer: BE
Explanation

Explanation/Reference:
Section:

QUESTION 57
In which of the following common use cases would steganography be employed?

A. Obfuscation
B. Integrity
C. Non-repudiation
D. Blockchain

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 58
A company's bank has reported that multiple corporate credit cards have been stolen over the past several weeks. The bank has provided the names of the affected cardholders to the company's forensics team to assist in the cyber-incident investigation. An incident responder learns the following information:
* The timeline of stolen card numbers corresponds closely with affected users making Internet-based purchases from diverse websites via enterprise desktop PCs.
* All purchase connections were encrypted, and the company uses an SSL inspection proxy for the inspection of encrypted traffic of the hardwired network.
* Purchases made with corporate cards over the corporate guest WiFi network, where no SSL inspection occurs, were unaffected.
Which of the following is the MOST likely root cause?

A. HTTPS sessions are being downgraded to insecure cipher suites
B. The SSL inspection proxy is feeding events to a compromised SIEM
C. The payment providers are insecurely processing credit card charges
D. The adversary has not yet established a presence on the guest WiFi network

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 59
After a ransomware attack a forensics company needs to review a cryptocurrency transaction between the victim and the attacker. Which of the following will the company MOST likely review to trace this transaction?

A. The public ledger
B. The NetFlow data

C. A checksum
D. The event log

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 60
During an incident response, a security analyst observes the following log entry on the web server:

GET http://www.companysite.com/product_info.phy?show=../../../../etc/password HTTP/1.1 Host: www.companysite.com

Which of the following BEST describes the type of attack the analyst is experiencing?

A. SQL injection
B. Cross-site scripting
C. Pass-the-hash
D. Directory traversal

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 61
A remote user recently took a two-week vacation abroad and brought along a corporate- owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN. Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN?

A. Due to foreign travel, the user's laptop was isolated from the network.
B. The user's laptop was quarantined because it missed the latest patch update.
C. The VPN client was blacklisted.
D. The user's account was put on a legal hold.

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 62
A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent the issue from reoccurring?

A. CASB
B. SWG
C. Containerization
D. Automated failover

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 63
A user recently entered a username and password into a recruiting application website that had been forged to look like the legitimate site Upon investigation, a security analyst the identifies the following:
* The legitimate websites IP address is 10.1.1.20 and eRecruit local resolves to the IP
* The forged website's IP address appears to be 10.2.12.99. based on NetFlow records
* AH three at the organization's DNS servers show the website correctly resolves to the legitimate IP
* DNS query logs show one of the three DNS servers returned a result of 10.2.12.99 (cached) at the approximate time of the suspected compromise.
Which of the following MOST likely occurred?

A. A reverse proxy was used to redirect network traffic
B. An SSL strip MITM attack was performed
C. An attacker temporarily pawned a name server
D. An ARP poisoning attack was successfully executed

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 64
Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?

A. DLP
B. HIDS
C. EDR
D. NIPS

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 65
A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk. Which of the following should the administrator use?

A. logger
B. chmod
C. dd
D. dnsenum

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 66
A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security assessment. The analyst redirects the output to a file After the capture is complete, the analyst needs to review the first transactions quickly and then search the entire series of requests for a particular string Which of the following would be BEST to use to accomplish the task? (Select TWO).

A. head
B. Tcpdump
C. grep
D. rail
E. curl
F. openssi
G. dd

Correct Answer: AC
Explanation

Explanation/Reference:
Section:

QUESTION 67
A security analyst needs to generate a server certificate to be used for 802.1X and secure RDP connections. The analyst is unsure what is required to perform the task and solicits help from a senior colleague. Which of the following is the FIRST step the senior colleague will most likely tell the analyst to perform to accomplish this task?

A. Create an OCSP
B. Generate a CSR
C. Create a CRL
D. Generate a .pfx file

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 68
Which of the following describes the BEST approach for deploying application patches?

A. Apply the patches to systems in a testing environment then to systems in a staging environment, and finally to production systems.
B. Test the patches in a staging environment, develop against them in the development environment, and then apply them to the production systems
C. Test the patches in a test environment apply them to the production systems and then apply them to a staging environment
D. Apply the patches to the production systems apply them in a staging environment, and then test all of them in a testing environment

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 69
When selecting a technical solution for identity management, an architect chooses to go from an in-house to a third-party SaaS provider. Which of the following risk management strategies is this an example of?

A. Acceptance
B. Mitigation
C. Avoidance
D. Transference

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 70
A cybersecurity administrator has a reduced team and needs to operate an on-premises network and security infrastructure efficiently. To help with the situation, the administrator decides to hire a service provider. Which of the following should the administrator use?

A. SDP
B. AAA
C. IaaS
D. MSSP
E. Microservices

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 71
A security analyst is looking for a solution to help communicate to the leadership team the severity levels of the organization's vulnerabilities. Which of the following would BEST meet this need?

A. CVE
B. SIEM
C. SOAR
D. CVSS

Correct Answer: D
Explanation

Explanation/Reference:
Section:
Explanation:
The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat

QUESTION 72
A workwide manufacturing company has been experiencing email account compromise. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would BEST prevent this type of attack?

A. Network location
B. Impossible travel time
C. Geolocation
D. Geofencing

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 73
A global pandemic is forcing a private organization to close some business units and reduce staffing at others. Which of the following would be BEST to help the organization's executives determine the next course of action?

A. An incident response plan
B. A communications plan
C. A disaster recovery plan
D. A business continuity plan

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 74
Several employees return to work the day after attending an industry trade show. That same day, the security manager notices several malware alerts coming from each of the employee's workstations. The security manager investigates but finds no signs of an attack on the perimeter firewall or the NIDS. Which of the following is MOST likely causing the malware alerts?

A. A worm that has propagated itself across the intranet, which was initiated by presentation media
B. A fileless virus that is contained on a vCard that is attempting to execute an attack
C. A Trojan that has passed through and executed malicious code on the hosts
D. A USB flash drive that is trying to run malicious code but is being blocked by the host firewall

Correct Answer: B
Explanation

Explanation/Reference:
Section:
Explanation:
WhatsApp Web logic and allow attackers to trick victims into executing arbitrary code on their machines in a new and sophisticated way. All an attacker needed to do to exploit the vulnerability was to send a user a seemingly innocent vCard containing malicious code. Once opened, the alleged contact is revealed to be an executable file, further compromising computers by distributing bots, ransomware, RATs, and other malwares.
https://blog.checkpoint.com/2015/09/08/whatsapp-maliciouscard-vulnerabilities-allowed-attackers-to-compromise-hundreds-of-millions-of-whatsapp-users/

QUESTION 75
Which of the following would MOST likely support the integrity of a voting machine?

A. Asymmetric encryption
B. Blockchain

C. Transport Layer Security
D. Perfect forward secrecy

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 76
A cybersecurity administrator needs to add disk redundancy for a critical server. The solution must have a two-drive failure for better fault tolerance. Which of the following RAID levels should the administrator select?

A. 0
B. 1
C. 5
D. 6

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 77
A security incident may have occurred on the desktop PC of an organization's Chief Executive Officer (CEO) A duplicate copy of the CEO's hard drive must be stored securely to ensure appropriate forensic processes and the chain of custody are followed. Which of the following should be performed to accomplish this task?

A. Install a new hard drive in the CEO's PC, and then remove the old hard drive and place it in a tamper-evident bag
B. Connect a write blocker to the hard drive Then leveraging a forensic workstation, utilize the dd command m a live Linux environment to create a duplicate copy
C. Remove the CEO's hard drive from the PC, connect to the forensic workstation, and copy all the contents onto a remote fileshare while the CEO watches
D. Refrain from completing a forensic analysts of the CEO's hard drive until after the incident is confirmed, duplicating the hard drive at this stage could destroy evidence

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 78
A Chief Information Security Officer (CISO) needs to create a policy set that meets international standards for data privacy and sharing. Which of the following should the CISO read and understand before writing the policies?

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

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 79
A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Choose two.)

A. Dual power supply
B. Off-site backups
C. Automatic OS upgrades
D. NIC teaming
E. Scheduled penetration testing
F. Network-attached storage

Correct Answer: AD
Explanation

Explanation/Reference:
Section:

QUESTION 80
A company recently experienced a data breach and the source was determined to be an executive who was charging a phone in a public area. Which of the following would MOST likely have prevented this breach?

A. A firewall
B. A device pin
C. A USB data blocker
D. Biometrics

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 81
An organization has a growing workforce that is mostly driven by additions to the sales department. Each newly hired salesperson relies on a mobile device to conduct business. The Chief Information Officer (CIO) is wondering if the organization may need to scale down just as quickly as it scaled up. The CIO is also concerned about the organization's security and customer privacy. Which of the following would be BEST to address the CIO's concerns?

A. Disallow new hires from using mobile devices for six months
B. Select four devices for the sales department to use in a CYOD model
C. Implement BYOD for the sales department while leveraging the MDM
D. Deploy mobile devices using the COPE methodology

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 82
A company has drafted an insider-threat policy that prohibits the use of external storage devices. Which of the

following would BEST protect the company from data exfiltration via removable media?

A. Monitoring large data transfer transactions in the firewall logs
B. Developing mandatory training to educate employees about the removable media policy
C. Implementing a group policy to block user access to system files
D. Blocking removable-media devices and write capabilities using a host-based security tool

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 83
A system administrator needs to implement an access control scheme that will allow an object's access policy be determined by its owner. Which of the following access control schemes BEST fits the requirements?

A. Role-based access control
B. Discretionary access control
C. Mandatory access control
D. Attribute-based access control

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 84
A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

A. perform attribution to specific APTs and nation-state actors.
B. anonymize any PII that is observed within the IoC data.
C. add metadata to track the utilization of threat intelligence reports.
D. assist companies with impact assessments based on the observed data.

Correct Answer: B
Explanation

Explanation/Reference:
Section:
Explanation:
ndicator of compromise (IoC) in computer forensics is an artifact observed on a network or in an operating system that, with high confidence, indicates a computer intrusion.

QUESTION 85
A Chief Security Officer (CSO) is concerned about the amount of PII that is stored locally on each salesperson's laptop. The sales department has a higher-than-average rate of lost equipment. Which of the following recommendations would BEST address the CSO's concern?

A. Deploy an MDM solution.
B. Implement managed FDE.
C. Replace all hard drives with SEDs.

D. Install DLP agents on each laptop.

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 86
An analyst visits an internet forum looking for information about a tool. The analyst finds a threat that appears to contain relevant information. One of the posts says the following:

Hello everyone,
I am having the same problem with my server. Can you help me?

<script type="text/javascript" src=http://src=http://website.com/user.js> Onload=sqlexec();
</script>

Thanks you,

Joe

Which of the following BEST describes the attack that was attempted against the forum readers?

A. SOU attack
B. DLL attack
C. XSS attack
D. API attack

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 87
Which of the following is a team of people dedicated testing the effectiveness of organizational security programs by emulating the techniques of potential attackers?

A. Red team
B. White team
C. Blue team
D. Purple team

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 88
An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the MOST acceptable?

A. SED
B. HSM

C. DLP
D. TPM

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 89
A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems. Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization's security posture?

A. Configure the DLP policies to allow all PII
B. Configure the firewall to allow all ports that are used by this application
C. Configure the antivirus software to allow the application
D. Configure the DLP policies to whitelist this application with the specific PII
E. Configure the application to encrypt the PII

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 90
Which of the following cloud models provides clients with servers, storage, and networks but nothing else?

A. SaaS
B. PaaS
C. IaaS
D. DaaS

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 91
A network administrator would like to configure a site-to-site VPN utilizing iPSec. The administrator wants the tunnel to be established with data integrity encryption, authentication and anti- replay functions Which of the following should the administrator use when configuring the VPN ?

A. AH
B. EDR
C. ESP
D. DNSSEC

Correct Answer: C
Explanation

Explanation/Reference:

Section:

QUESTION 92
Which of the following job roles would sponsor data quality and data entry initiatives that ensure business and regulatory requirements are met?

A. The data owner
B. The data processor
C. The data steward
D. The data privacy officer.

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 93
A small company that does not have security staff wants to improve its security posture. Which of the following would BEST assist the company?

A. MSSP
B. SOAR
C. IaaS
D. PaaS

Correct Answer: B
Explanation

Explanation/Reference:
Section:
Explantion:
SOAR (Security Orchestration, Automation and Response).
They combine the following functions.
• Threat and vulnerability management
• Security incident response
• Security operations automation

QUESTION 94
A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

A. SIEM
B. DLP
C. CASB
D. SWG

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 95
The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work

from home anytime during business hours, incident during a pandemic or crisis, However, the CEO is concerned that some staff members may take advantage of the of the flexibility and work from high-risk countries while on holidays work at a third-party organization in another country. The Chief information Officer (CIO) believes the company can implement some basic controls to mitigate the majority of the risk. Which of the following would be BEST to mitigate CEO's concern? (Select TWO).

A. Geolocation
B. Time-of-day restrictions
C. Certificates
D. Tokens
E. Geotagging
F. Role-based access controls

Correct Answer: AB
Explanation

Explanation/Reference:
Section:

QUESTION 96
After entering a username and password, and administrator must gesture on a touch screen. Which of the following demonstrates what the administrator is providing?

A. Multifactor authentication
B. Something you can do
C. Biometric
D. Two-factor authentication

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 97
Joe, an employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm Joe's identity before sending him the prize. Which of the following BEST describes this type of email?

A. Spear phishing
B. Whaling
C. Phishing
D. Vishing

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 98
A security administrator checks the table of a network switch, which shows the following output:

VLAN Physical Address Type Port
1 001a:42ff:5113 Dynamic GE0/5
1 0faa:abcf:ddee Dynamic GE0/5

1 c6a9:6616:758e Dynamic GE0/5
1 a1a3:b6a3:1212 Dynamic GE0/5
1 6025:2ad8:bca2 Dynamic GE0/5
1 b935:f995:b00b Dynamic GE0/5

Which of the following is happening to this switch?

A. MAC Flooding
B. DNS poisoning
C. MAC cloning
D. ARP poisoning

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 99
A company uses wireless for all laptops and keeps a very detailed record of its assets, along with a comprehensive list of devices that are authorized to be on the wireless network. The Chief Information Officer (CIO) is concerned about a script kiddie potentially using an unauthorized device to brute force the wireless PSK and obtain access to the internal network. Which of the following should the company implement to BEST prevent this from occurring?

A. BDU guard
B. WPA-EAP
C. IP filtering
D. A WIDS

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 100
An organization is developing an authentication service for use at the entry and exit ports of country borders. The service will use data feeds obtained from passport systems, passenger manifests, and high- definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them. Which of the following biometrics will MOST likely be used, without the need for enrollment? (Choose two.)

A. Voice
B. Gait
C. Vein
D. Facial
E. Retina
F. Fingerprinting

Correct Answer: BD
Explanation

Explanation/Reference:

Section:

QUESTION 101
A user contacts the help desk to report the following:
* Two days ago, a pop-up browser window prompted the user for a name and password after connecting to the corporate wireless SSID. This had never happened before, but the user entered the information as requested.
* The user was able to access the Internet but had trouble accessing the department share until the next day.
* The user is now getting notifications from the bank about unauthorized transactions. Which of the following attack vectors was MOST likely used in this scenario?

A. Rogue access point
B. Evil twin
C. DNS poisoning
D. ARP poisoning

Correct Answer: B
Explanation

Explanation/Reference:
Section:

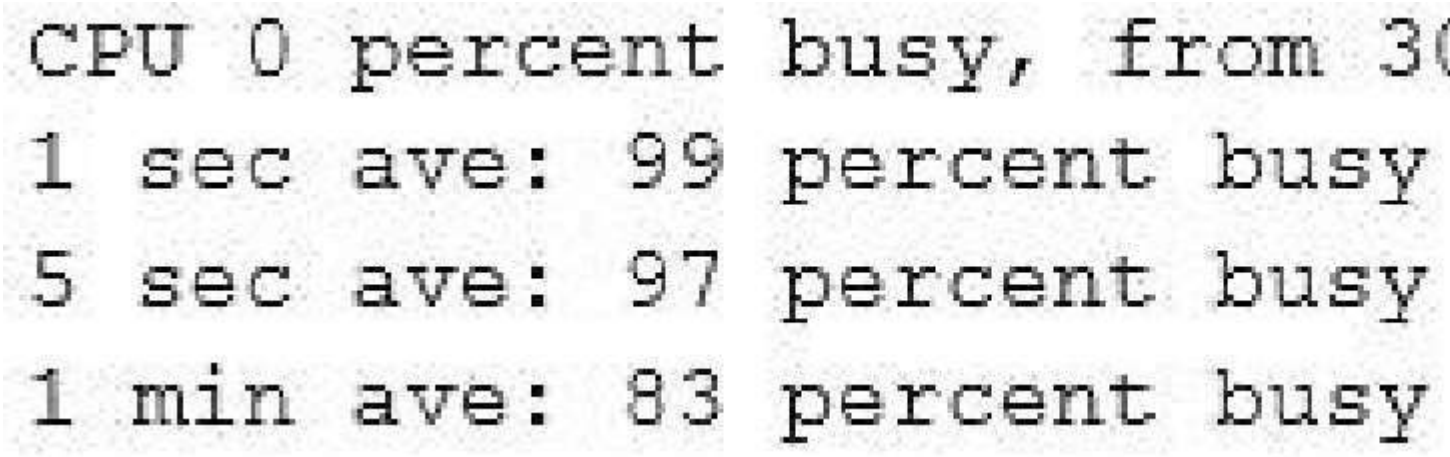
QUESTION 102
A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better.

A. validate the vulnerability exists in the organization's network through penetration testing
B. research the appropriate mitigation techniques in a vulnerability database
C. find the software patches that are required to mitigate a vulnerability
D. prioritize remediation of vulnerabilities based on the possible impact.

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 103
A network administrator has been alerted that web pages are experiencing long load times. After determining it is not a routing or DNS issue, the administrator logs in to the router, runs a command, and receives the following output:



Which of the following is the router experiencing?

A. DDoS attack
B. Memory leak
C. Buffer overflow
D. Resource exhaustion

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 104
A security analyst receives a SIEM alert that someone logged in to the appadmin test account, which is only used for the early detection of attacks. The security analyst then reviews the following application log:

```
...
[03/06/20xx:17:20:18] system 127.0.0.1 FindXPath=//User[Username/text()='foo' or 7=7 or
[03/06/20xx:17:21:18] appadmin 194.28.114.102 action:login result:success
[03/06/20xx:17:22:18] appadmin 194.28.114.102 action:open.account(12345) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(45678) result:fail
```

Which of the following can the security analyst conclude?

A. A replay attack is being conducted against the application.
B. An injection attack is being conducted against a user authentication system.
C. A service account password may have been changed, resulting in continuous failed logins within the application.
D. A credentialed vulnerability scanner attack is testing several CVEs against the application.

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 105
Joe, a user at a company, clicked an email link led to a website that infected his workstation. Joe, was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and It has continued to evade detection. Which of the following should administrator implement to protect the environment from this malware?

A. Install a definition-based antivirus.
B. Implement an IDS/IPS
C. Implement a heuristic behavior-detection solution.
D. Implement CASB to protect the network shares.

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 106
A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate device using PKI. Which of the following should the administrator configure?

A. A captive portal
B. PSK
C. 802.1X
D. WPS

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 107
A company processes highly sensitive data and senior management wants to protect the sensitive data by utilizing classification labels. Which of the following access control schemes would be BEST for the company to implement?

A. Discretionary
B. Rule-based
C. Role-based
D. Mandatory

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 108
A website developer is working on a new e-commerce website and has asked an information security expert for the most appropriate way to store credit card numbers to create an easy reordering process. Which of the following methods would BEST accomplish this goal?

A. Salting the magnetic strip information
B. Encrypting the credit card information in transit.
C. Hashing the credit card numbers upon entry.
D. Tokenizing the credit cards in the database

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 109
Which of the following ISO standards is certified for privacy?

A. ISO 9001
B. ISO 27002

C. ISO 27701
D. ISO 31000

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 110
An organization wants to implement a third factor to an existing multifactor authentication. The organization already uses a smart card and password. Which of the following would meet the organization's needs for a third factor?

A. Date of birth
B. Fingerprint
C. PIN
D. TPM

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 111
An organization that is located in a flood zone is MOST likely to document the concerns associated with the restoration of IT operation in a:

A. business continuity plan
B. communications plan.
C. disaster recovery plan.
D. continuity of operations plan

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 112
A university with remote campuses, which all use different service providers, loses Internet connectivity across all locations. After a few minutes, Internet and VoIP services are restored, only to go offline again at random intervals, typically within four minutes of services being restored. Outages continue throughout the day, impacting all inbound and outbound connections and services. Services that are limited to the local LAN or WiFi network are not impacted, but all WAN and VoIP services are affected. Later that day, the edge-router manufacturer releases a CVE outlining the ability of an attacker to exploit the SIP protocol handling on devices, leading to resource exhaustion and system reloads. Which of the following BEST describe this type of attack? (Choose two.)

A. DoS
B. SSL stripping
C. Memory leak
D. Race condition
E. Shimming

F. Refactoring

Correct Answer: AC
Explanation

Explanation/Reference:
Section:

QUESTION 113
A security analyst discovers that a company username and password database was posted on an Internet forum. The username and passwords are stored in plain text. Which of the following would mitigate the damage done by this type of data exfiltration in the future?

A. Create DLP controls that prevent documents from leaving the network
B. Implement salting and hashing
C. Configure the web content filter to block access to the forum.
D. Increase password complexity requirements

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 114
A host was infected with malware. During the incident response, Joe, a user, reported that he did not receive any emails with links, but he had been browsing the Internet all day. Which of the following would MOST likely show where the malware originated?

A. The DNS logs
B. The web server logs
C. The SIP traffic logs
D. The SNMP logs

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 115
A smart switch has the ability to monitor electrical levels and shut off power to a building in the event of power surge or other fault situation. The switch was installed on a wired network in a hospital and is monitored by the facilities department via a cloud application. The security administrator isolated the switch on a separate VLAN and set up a patch routine. Which of the following steps should also be taken to harden the smart switch?

A. Set up an air gap for the switch.
B. Change the default password for the switch.
C. Place the switch In a Faraday cage.
D. Install a cable lock on the switch

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 116
Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?

A. Least privilege
B. Awareness training
C. Separation of duties
D. Mandatory vacation

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 117
In which of the following situations would it be BEST to use a detective control type for mitigation?

A. A company implemented a network load balancer to ensure 99.999% availability of its web application.
B. A company designed a backup solution to increase the chances of restoring services in case of a natural disaster.
C. A company purchased an application-level firewall to isolate traffic between the accounting department and the information technology department.
D. A company purchased an IPS system, but after reviewing the requirements, the appliance was supposed to monitor, not block, any traffic.
E. A company purchased liability insurance for flood protection on all capital assets.

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 118
An organization's RPO for a critical system is two hours. The system is used Monday through Friday, from 9:00 am to 5:00 pm. Currently, the organization performs a full backup every Saturday that takes four hours to complete. Which of the following additional backup implementations would be the BEST way for the analyst to meet the business requirements?

A. Incremental backups Monday through Friday at 6:00 p.m and differential backups hourly
B. Full backups Monday through Friday at 6:00 p.m and incremental backups hourly.
C. incremental backups Monday through Friday at 6:00 p.m and full backups hourly.
D. Full backups Monday through Friday at 6:00 p.m and differential backups hourly.

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 119
On which of the following is the live acquisition of data for forensic analysis MOST dependent? (Choose two.)

A. Data accessibility

B. Legal hold
C. Cryptographic or hash algorithm
D. Data retention legislation
E. Value and volatility of data
F. Right-to-audit clauses

Correct Answer: AE
Explanation

Explanation/Reference:
Section:

QUESTION 120
An organization just experienced a major cyberattack. The attack was well coordinated sophisticated and highly skilled. Which of the following targeted the organization?

A. Shadow IT
B. An insider threat
C. A hacktivist
D. An advanced persistent threat

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 121
Which of the following describes the ability of code to target a hypervisor from inside

A. Fog computing
B. VM escape
C. Software-defined networking
D. Image forgery
E. Container breakout

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 122
A security analyst discovers several .jpg photos from a cellular phone during a forensics investigation involving a compromised system. The analyst runs a forensics tool to gather file metadata. Which of the following would be part of the images if all the metadata is still intact?

A. The GPS location
B. When the file was deleted
C. The total number of print jobs
D. The number of copies made

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 123
Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases? (Select TWO.)

A. Unsecure protocols
B. Use of penetration-testing utilities
C. Weak passwords
D. Included third-party libraries
E. Vendors/supply chain
F. Outdated anti-malware software

Correct Answer: DE
Explanation

Explanation/Reference:
Section:

QUESTION 124
A small business just recovered from a ransomware attack against its file servers by purchasing the decryption keys from the attackers. The issue was triggered by a phishing email and the IT administrator wants to ensure it does not happen again. Which of the following should the IT administrator do FIRST after recovery?

A. Scan the NAS for residual or dormant malware and take new daily backups that are tested on a frequent basis
B. Restrict administrative privileges and patch ail systems and applications.
C. Rebuild all workstations and install new antivirus software
D. Implement application whitelisting and perform user application hardening

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 125
A company recently set up an e-commerce portal to sell its product online. The company wants to start accepting credit cards for payment, which requires compliance with a security standard. Which of the following standards must the company comply with before accepting credit cards on its e-commerce platform?

A. PCI DSS
B. ISO 22301
C. ISO 27001
D. NIST CSF

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 126
A forensics investigator is examining a number of unauthorized payments the were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a

link to attempt to unsubscribe. One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:

<a=href="https://www.company.com/payto.do?/routing=00001111&account=22223334&amount=250">click here to unsubscribe

Which of the following will the forensics investigator MOST likely determine has occurred?

A. SQL injection
B. CSRF
C. XSS
D. XSRF

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 127
A financial analyst is expecting an email containing sensitive information from a client. When the email arrives, the analyst receives an error and is unable to open the encrypted message. Which of the following is the MOST likely cause of the issue?

A. The S/MIME plug-in is not enabled.
B. The SLL certificate has expired.
C. Secure IMAP was not implemented
D. POP3S is not supported.

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 128
A security analyst sees the following log output while reviewing web logs:

[02/Feb/2019:03:39:21 -0000 23.35.212.99 12.59.34.88 -"GET /uri/input.action?query=%2f..%2f..%..2fetc%2fpasswd HTTP/1.0" 80 200 200
[02/Feb/2019:03:39:21 -0000 23.35.212.99 12.59.34.88 -"GET /uri/input.action?query=/../../../etc/fpasswd HTTP/1.0" 80 200 200

Which of the following mitigation strategies would be BEST to prevent this attack from being successful?

A. Secure cookies
B. Input validation
C. Code signing
D. Stored procedures

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 129
A security administrator needs to create a RAID configuration that is focused on high read speeds and fault tolerance. It is unlikely that multiple drivers will fail simultaneously. Which of the following RAID configurations should the administration use?

A. RAID 0
B. RAID1
C. RAID 5
D. RAID 10

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 130
A recently discovered zero-day exploit utilizes an unknown vulnerability in the SMB network protocol to rapidly infect computers. Once infected, computers are encrypted and held for ransom. Which of the following would BEST prevent this attack from reoccurring?

A. Configure the perimeter firewall to deny inbound external connections to SMB ports.
B. Ensure endpoint detection and response systems are alerting on suspicious SMB connections.
C. Deny unauthenticated users access to shared network folders.
D. Verify computers are set to install monthly operating system, updates automatically.

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 131
Which of the following BEST explains the difference between a data owner and a data custodian?

A. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data
B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protection to the data
C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data
D. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 132
A user reports constant lag and performance issues with the wireless network when working at a local coffee shop. A security analyst walks the user through an installation of Wireshark and get a five-minute pcap to analyze. The analyst observes the following output:

No. Time Source Destination Protocol Length Info

1234 9.1195665 Sagemcon_87:9fa3 Broadcast 802.11 38 Deauthentication, SN=655, FN=0 1235 9.1265649 Sagemcon_87:9fa3 Broadcast 802.11 39 Deauthentication, SN=655, FN=0 1236 9.2223213 Sagemcon_87:9fa3 Broadcast 802.11 38 Deauthentication, SN=657, FN=0

What type of attack will most likely be attempted next?

A. Session replay
B. Evil twin
C. Bluejacking
D. ARP poisoning

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 133
A security audit has revealed that a process control terminal is vulnerable to malicious users installing and executing software on the system. The terminal is beyond end-of-life support and cannot be upgraded, so it is placed on a protected network segment. Which of the following would be MOST effective to implement to further mitigate the reported vulnerability?

A. DNS sinkholeing
B. DLP rules on the terminal
C. An IP blacklist
D. Application whitelisting

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 134
A network administrator has been asked to install an IDS to improve the security posture of an organization. Which of the following control types is an IDS?

A. Corrective
B. Physical
C. Detective
D. Administrative

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 135
Which of the following would be BEST to establish between organizations to define the responsibilities of each party and outline the key deliverables and include monetary penalties for breaches to manage third-party risk?

A. An ARO
B. An MOU

C. An SLA
D. A BPA

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 136
An organization has hired a security analyst to perform a penetration test. The analyst captures 1Gb worth of inbound network traffic to the server and transfer the pcap back to the machine for analysis. Which of the following tools should the analyst use to further review the pcap?

A. Nmap
B. cURL
C. Netcat
D. Wireshark

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 137
An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:
* Check-in/checkout of credentials
* The ability to use but not know the password
* Automated password changes
* Logging of access to credentials
Which of the following solutions would meet the requirements?

A. OAuth 2.0
B. Secure Enclave
C. A privileged access management system
D. An OpenID Connect authentication system

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 138
A security analyst needs to be proactive in understand the types of attacks that could potentially target the company's execute. Which of the following intelligence sources should to security analyst review?

A. Vulnerability feeds
B. Trusted automated exchange of indicator information
C. Structured threat information expression
D. Industry information-sharing and collaboration groups

Correct Answer: C
Explanation

Explanation/Reference:
Section:
Explanation:
The Structured Threat Information eXpression, or STIX, is an XML structured language for expressing and sharing threat intelligence.
STIX is a community-driven project currently led and sponsored by the office of Cybersecurity and Communications at the United States DHS.

QUESTION 139
A critical file server is being upgraded and the systems administrator must determine which RAID level the new server will need to achieve parity and handle two simultaneous disk failures. Which of the following RAID levels meets this requirements?

A. RAID 0+1
B. RAID 2
C. RAID 5
D. RAID 6

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 140
A database administrator needs to ensure all passwords are stored in a secure manner, so the administrator adds randomly generated data to each password before string. Which of the following techniques BEST explains this action?

A. Predictability
B. Key stretching
C. Salting
D. Hashing

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 141
A development team employs a practice of bringing all the code changes from multiple team members into the same development project through automation. A tool is utilized to validate the code and track source code through version control. Which of the following BEST describes this process?

A. Continuous delivery
B. Continuous integration
C. Continuous validation
D. Continuous monitoring

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 142
A company is implementing MFA for all applications that store sensitive data. The IT manager wants MFA to be non-disruptive and user friendly. Which of the following technologies should the IT manager use when implementing MFA?

A. One-time passwords
B. Email tokens
C. Push notifications
D. Hardware authentication

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 143
A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL:
http://dev-site.comptia.org/home/show.php?sessionID=77276554&loc=us
See Image:

The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:
http://dev-site.comptia.org/home/show.php?sessionID=98988475&loc=us
See Image:

Which of the following application attacks is being tested?

A. Pass-the-hash
B. Session replay
C. Object deference
D. Cross-site request forgery

Correct Answer: D
Explanation

Explanation/Reference:
Section:
Explanation:
Information is missing in this question to form an intelligent answer.

QUESTION 144
Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

A. SSAE SOC 2
B. PCI DSS
C. GDPR
D. ISO 31000

Correct Answer: C
Explanation

Explanation/Reference:

Section:

QUESTION 145
A company's Chief Information Office (CIO) is meeting with the Chief Information Security Officer (CISO) to plan some activities to enhance the skill levels of the company's developers. Which of the following would be MOST suitable for training the developers'?

A. A capture-the-flag competition
B. A phishing simulation
C. Physical security training
D. Basic awareness training

Correct Answer: A
Explanation

Explanation/Reference:
Section:
Explanation:
Capture The Flag (CTF) hacking events that are usually hosted at information security conferences, including the various BSides events. These events consist of a series of challenges that vary in their degree of difficulty, and that require participants to exercise different skillsets to solve. Once an individual challenge is solved, a "flag" is given to the player and they submit this flag to the CTF server to earn points. Players can be lone wolves who attempt the various challenges by themselves, or they can work with others to attempt to score the highest number of points as a team.

CTF events are usually timed, and the points are totaled once the time has expired. The winning player / team will be the one that solved the most challenges and thus secured the highest score.

QUESTION 146
A security analyst has received an alert about being sent via email. The analyst's Chief information Security Officer (CISO) has made it clear that PII must be handled with extreme care From which of the following did the alert MOST likely originate?

A. S/MIME
B. DLP
C. IMAP
D. HIDS

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 147
A public relations team will be taking a group of guests on a tour through the facility of a large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboards are cleaned and all desks are cleared. The company is MOST likely trying to protect against.

A. Loss of proprietary information
B. Damage to the company's reputation
C. Social engineering
D. Credential exposure

Correct Answer: A
Explanation

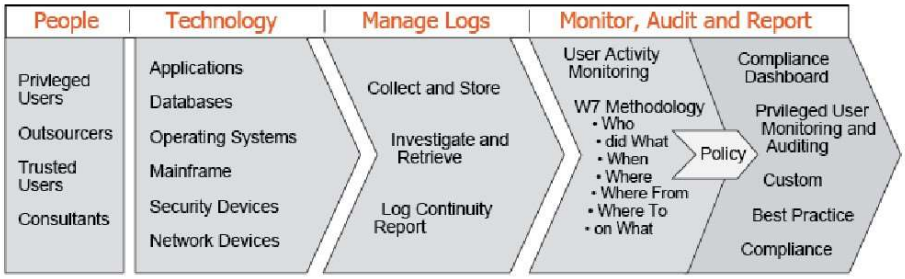
Explanation/Reference:
Section:

QUESTION 148
After reading a security bulletin, a network security manager is concerned that a malicious actor may have breached the network using the same software flaw. The exploit code is publicly available and has been reported as being used against other industries in the same vertical. Which of the following should the network security manager consult FIRST to determine a priority list for forensic review?

A. The vulnerability scan output
B. The IDS logs
C. The full packet capture data
D. The SIEM alerts

Correct Answer: D
Explanation

Explanation/Reference:
Section:
Explanation:
In the field of computer security, security information and event management (SIEM) software products and services combine
security information management (SIM) and
security event management (SEM).
They provide real-time analysis of security alerts generated by applications and network hardware.



QUESTION 149
A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device approach?

A. The most common set of MDM configurations will become the effective set of enterprise mobile security controls.
B. All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.
C. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.
D. MDMs typically will not support heterogeneous deployment environments, so multiple MDMs will need to be installed and configured.

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 150
Which of the following should be put in place when negotiating with a new vendor about the timeliness of the response to a significant outage or incident?

A. MOU
B. MTTR
C. SLA
D. NDA

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 151
Which of the following types of controls is a turnstile?

A. Physical
B. Detective
C. Corrective
D. Technical

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 152
To secure an application after a large data breach, an e-commerce site will be resetting all users' credentials. Which of the following will BEST ensure the site's users are not compromised after the reset?

A. A password reuse policy
B. Account lockout after three failed attempts
C. Encrypted credentials in transit
D. A geofencing policy based on login history

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 153
Which of the following would be the BEST method for creating a detailed diagram of wireless access points and hot-spots?

A. Footprinting
B. White-box testing
C. A drone/UAV
D. Pivoting

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 154
A RAT that was used to compromise an organization's banking credentials was found on a user's computer. The RAT evaded antivirus detection. It was installed by a user who has local administrator rights to the system as part of a remote management tool set. Which of the following recommendations would BEST prevent this from reoccurring?

A. Create a new acceptable use policy.
B. Segment the network into trusted and untrusted zones.
C. Enforce application whitelisting.
D. Implement DLP at the network boundary.

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 155
A security analyst is performing a forensic investigation of compromised account credentials. Using the Event Viewer, the analyst able to detect the following message, "Special privileges assigned to new login." Several of these messages did not have a valid logon associated with the user before these privileges were assigned. Which of the following attacks is MOST likely being detected?

A. Pass-the-hash
B. Buffer overflow
C. Cross-site scripting
D. Session replay

Correct Answer: A
Explanation

Explanation/Reference:
Section:

Explanation:
Pass-the-hash (PtH) is a credential theft and lateral movement technique in which an attacker can abuse the challenge-and-response nature of the NTLM authentication protocol to authenticate as a user with only the NTLM hash of the user’s password.
All Windows were susceptible because they store hash values of user's passwords in LSA. LSA security was exploited by PtH

QUESTION 156
Phishing and spear-phishing attacks have been occurring more frequently against a company's staff. Which of the following would MOST likely help mitigate this issue?

A. DNSSEC and DMARC
B. DNS query logging
C. Exact mail exchanger records in the DNS
D. The addition of DNS conditional forwarders

Correct Answer: A
Explanation

Explanation/Reference:
Section:
Explanation:
DNSSEC is a security extension to DNS.
DMARC (Domain-based Message Authentication, Reporting and Conformance) is a add on to DNSSEC that authenticates email senders.

QUESTION 157
A security engineer needs to enhance MFA access to sensitive areas in a building. A key card and fingerprint scan are already in use. Which of the following would add another factor of authentication?

A. Hard token
B. Retina scan
C. SMS text
D. Keypad PIN

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 158
An organization has implemented a policy requiring the use of conductive metal lockboxes for personal electronic devices outside of a secure research lab. Which of the following did the organization determine to be the GREATEST risk to intellectual property when creating this policy?

A. The theft of portable electronic devices
B. Geotagging in the metadata of images
C. Bluesnarfing of mobile devices
D. Data exfiltration over a mobile hotspot

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 159
A document that appears to be malicious has been discovered in an email that was sent to a company's Chief Financial Officer (CFO). Which of the following would be BEST to allow a security analyst to gather information and confirm it is a malicious document without executing any code it may contain?

A. Open the document on an air-gapped network
B. View the document's metadata for origin clues
C. Search for matching file hashes on malware websites
D. Detonate the document in an analysis sandbox

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 160

A malicious actor recently penetration tested a company's network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know what was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

A. Security
B. Application
C. Dump
D. Syslog

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 161
The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the company's Chief Executive Officer (CEO), requesting a transfer of $10,000 to an account. The email states Ann is on vacation and has lost her purse, containing cash and credit cards. Which of the following social-engineering techniques is the attacker using?

A. Phishing
B. Whaling
C. Typo squatting
D. Pharming

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 162
A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

A. SIEM
B. DLP
C. CASB
D. SWG

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 163
A security assessment determines DES and 3DES at still being used on recently deployed production servers. Which of the following did the assessment identify?

A. Unsecure protocols
B. Default settings
C. Open permissions

D. Weak encryption

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 164
A cybersecurity manager has scheduled biannual meetings with the IT team and department manager presents a scenario and injects additional information throughout the session to replicate what might occur in a dynamic cybersecurity event involving the company, its facilities, its data, and its staff. Which of the following describes what the manager is doing?

A. Developing an incident response plan
B. Building a disaster recovery plan
C. Conducting a tabletop exercise
D. Running a simulation exercise

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 165
An organization is developing a plan in the event of a complete loss of critical systems and data. Which of the following plans is the organization MOST likely developing?

A. Incident response
B. Communications
C. Disaster recovery
D. Data retention

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 166
Which of the following allows for functional test data to be used in new systems for testing and training purposes to protect the data against reading?

A. Data encryption
B. Data masking
C. Data deduplication
D. Data minimization

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 167

Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?

A. Investigation
B. Containment
C. Recovery
D. Lessons learned

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 168
Given the following logs:

[DATA] attacking service ftp on port 21
[ATTEMPT] target 192.168.50.1 - login "admin" pass "password"
[ATTEMPT] target 192.168.50.1 - login "admin" pass "access" [
ATTEMPT] target 192.168.50.1 - login "admin" pass "allow"
[ATTEMPT] target 192.168.50.1 - login "admin" pass "please"
[ATTEMPT] target 192.168.50.1 - login "admin" pass "ftp"
[ATTEMPT] target 192.168.50.1 - login "admin" pass "letmein"
[21] [ftp] host: 192.168.50.1 loginLadmin password:letmein
1 of 1 target successfully completed, 1 valid password found
Which of the following BEST describes the type of attack that is occurring?

A. Rainbow table
B. Dictionary
C. Password spraying
D. Pass-the-hash

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 169
A company needs to centralize its logs to create a baseline and have visibility on its security events. Which of the following technologies will accomplish this objective?

A. Security information and event management
B. A web application firewall
C. A vulnerability scanner
D. A net generation firewall

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 170
Some laptops recently went missing from a locked storage area that is protected by keyless, RFID-enabled

locks. There is no obvious damage to the physical space. The security manager identifies who unlocked the door, however, human resources confirms this employee was on vacation at the time of the incident. Which of the following describes what MOST likely occurred?

A. The employee's physical access card was cloned.
B. The employee is colluding with human resources.
C. The employee's biometrics were harvested.
D. A criminal used lock-picking tools to open the door.

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 171
An analyst has determined that a server was not patched and an external actor exfiltrated data on port 139. Which of the following sources should the analyst review to BEST ascertain how the incident could

A. The vulnerability scan output
B. The security logs
C. The baseline report
D. The correlation of events

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 172
A forensics examiner is attempting to dump passwords cached in the physical memory of a live system but keeps receiving an error message. Which of the following BEST describes the cause of the error?

A. The examiner does not have administrative privileges to the system.
B. The system must be taken offline before a snapshot can be created.
C. Checksum mismatches are invalidating the disk image.
D. The swap file needs to be unlocked before it can be accessed.

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 173
The following is an administrative control that would be MOST effective to reduce the occurrence of malware execution?

A. Security awareness training
B. Frequency of NIDS updates
C. Change control procedures
D. EDR reporting cycle

Correct Answer: D

Explanation

Explanation/Reference:
Section:
Explanation:
EDR solutions are tools which help you in detection and investigation of suspicious activities across all the endpoints of your digital perimeter. It is becoming the preferred technology for enterprises to provide better security for their networks when compared with the traditional antivirus.

QUESTION 174
A security analyst needs to produce a document that details how a security incident occurred, the steps that were taken for recovery, and how future incidents can be avoided. During which of the following stages of the response process will this activity take place?

A. Recovery
B. Identification
C. Lesson learned
D. Preparation

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 175
A security analyst needs to implement an MDM solution for BYOD users that will allow the company to retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen. Which of the following would BEST meet these requirements? (Select TWO).

A. Full-device encryption
B. Network usage rules
C. Geofencing
D. Containerization
E. Application whitelisting
F. Remote control

Correct Answer: AD
Explanation

Explanation/Reference:
Section:
Explanation:
MDM containerization refers to the process of segregating personal and corporate data & apps on personal devices by creating a logical container to separate and enhance corporate data security.

QUESTION 176
A nuclear plant was the victim of a recent attack, and all the networks were air gapped. A subsequent investigation revealed a worm as the source of the issue. Which of the following BEST explains what happened?

A. A malicious USB was introduced by an unsuspecting employee.
B. The ICS firmware was outdated
C. A local machine has a RAT installed.
D. The HVAC was connected to the maintenance vendor

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 177
A well-known organization has been experiencing attacks from APTs. The organization is concerned that custom malware is being created and emailed into the company or installed on USB sticks that are dropped in parking lots. Which of the following is the BEST defense against this scenario?

A. Configuring signature-based antivirus io update every 30 minutes
B. Enforcing S/MIME for email and automatically encrypting USB drives upon insertion.
C. Implementing application execution in a sandbox for unknown software.
D. Fuzzing new files for vulnerabilities if they are not digitally signed

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 178
Local guidelines require that all information systems meet a minimum-security baseline to be compliant. Which of the following can security administrators use to assess their system configurations against the baseline?

A. SOAR playbook
B. Security control matrix
C. Risk management framework
D. Benchmarks

Correct Answer: A
Explanation

Explanation/Reference:
Section:
Explantion:
From notifications to remediations of threats, vulnerability management processes can be orchestrated by integrating SOAR playbooks into a company's existing solutions.
The playbooks automate actions to scan, discover patches, validate remediation, and more, addressing critical issues.

QUESTION 179
An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sale systems The IT administrator has been asked to improve both server data fault tolerance and site availability under high consumer load. Which of the following are the BEST options to accomplish this objective'? (Select TWO)

A. Load balancing
B. Incremental backups
C. UPS
D. RAID
E. Dual power supply
F. NIC teaming

Correct Answer: ADF

Explanation

Explanation/Reference:
Section:
Explanation:
NIC teaming is adding extra NIC's to take up the load.

QUESTION 180
A security analyst needs to complete an assessment. The analyst is logged into a server and must use native tools to map services running on it to the server's listening ports. Which of the following tools can BEST accomplish this talk?

A. Netcat
B. Netstat
C. Nmap
D. Nessus

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 181
An organization's Chief Security Officer (CSO) wants to validate the business's involvement in the incident response plan to ensure its validity and thoroughness. Which of the following will the CSO MOST likely use?

A. An external security assessment
B. A bug bounty program
C. A tabletop exercise
D. A red-team engagement

Correct Answer: C
Explanation

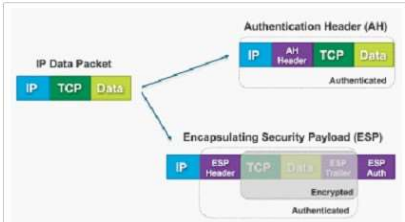
Explanation/Reference:
Section:

QUESTION 182
A security analyst receives the configuration of a current VPN profile and notices the authentication is only applied to the IP datagram portion of the packet. Which of the following should the analyst implement to authenticate the entire packet?

A. AH
B. ESP
C. SRTP
D. LDAP

Correct Answer: A
Explanation

Explanation/Reference:
Section:
Explanation:



When ESP provides authentication functions, it uses the same algorithms as AH, but the coverage is different.

- AH-style authentication authenticates the entire IP packet, including the outer IP header.
- ESP authentication mechanism authenticates only the IP datagram portion of the IP packet.

QUESTION 183
A network engineer needs to create a plan for upgrading the wireless infrastructure in a large office. Priority must be given to areas that are currently experiencing latency and connection issues. Which of the following would be the BEST resource for determining the order of priority?

A. Nmap
B. Heat maps
C. Network diagrams
D. Wireshark

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 184
Employees are having issues accessing the company's website. Some employees report very slow performance, while others cannot get to the website at all. The web and security administrators search the logs and find millions of half-open connections to port 443 on the web server. Further analysis reveals thousands of different source IPs initiating this traffic.
Which of the following attacks is MOST likely occurring?

A. DDoS
B. Man-in-the-middle
C. MAC flooding
D. Domain hijacking

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 185
A network engineer is troubleshooting wireless network connectivity issues that were reported by users. The issues are occurring only in the section of the building that is closest to the parking lot. Users are intermittently experiencing slow speeds when accessing websites and are unable to connect to network drives. The issues appear to increase when laptop users return to their desks after using their devices in other areas of the building. There have also been reports of users being required to enter their credentials on web pages in order to gain access to them. Which of the following is the MOST likely cause of this issue?

A. An external access point is engaging in an evil-twin attack.
B. The signal on the WAP needs to be increased in that section of the building
C. The certificates have expired on the devices and need to be reinstalled

D. The users in that section of the building are on a VLAN that is being blocked by the firewall.

Correct Answer: B
Explanation

Explanation/Reference:
Section:
Explanation:
Problems only happen in one side of the building. Poor connections does cause TCP timeouts and authentiation failures.

QUESTION 186
A user recently attended an exposition and received some digital promotional materials The user later noticed blue boxes popping up and disappearing on the computer, and reported receiving several spam emails, which the user did not open Which of the following is MOST likely the cause of the reported issue?

A. There was a drive-by download of malware
B. The user installed a cryptominer
C. The OS was corrupted
D. There was malicious code on the USB drive

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 187
A Chief Information Security Officer (CISO) is concerned about the organization's ability to continue business operation in the event of a prolonged DDoS attack on its local datacenter that consumes database resources. Which of the following will the CISO MOST likely recommend to mitigate this risk?

A. Upgrade the bandwidth available into the datacenter
B. Implement a hot-site failover location
C. Switch to a complete SaaS offering to customers
D. Implement a challenge response test on all end-user queries

Correct Answer: C
Explanation

Explanation/Reference:
Section:
Explanation:
Even if you failover to a Hot Site the traffic coming from the internet is supposed to follow you to the failover site. Attackers are piggy backing on the same bandwidth that is open to legitimate users.
Only viable solution for this is to have cloud offering. Cloud provides elasticity. Only cloud offering possible here is SaaS.

QUESTION 188
An engineer wants to access sensitive data from a corporate-owned mobile device. Personal data is not allowed on the device. Which of the following MDM configurations must be considered when the engineer travels for business?

A. Screen locks
B. Application management
C. Geofencing

D. Containerization

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 189
A symmetric encryption algorithm Is BEST suited for:

A. key-exchange scalability.
B. protecting large amounts of data.
C. providing hashing capabilities,
D. implementing non-repudiation.

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 190
An organization routes all of its traffic through a VPN Most users are remote and connect into a corporate datacenter that houses confidential information There is a firewall at the Internet border followed by a DLP appliance, the VPN server and the datacenter itself.
Which of the following is the WEAKEST design element?

A. The DLP appliance should be integrated into a NGFW.
B. Split-tunnel connections can negatively impact the DLP appliance's performance
C. Encrypted VPN traffic will not be inspected when entering or leaving the network
D. Adding two hops in the VPN tunnel may slow down remote connections

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 191
An end user reports a computer has been acting slower than normal for a few weeks. During an investigation, an analyst determines the system is sending the user's email address and a ten-digit number to an IP address once a day. The only recent log entry regarding the user's computer is the following:

Time: 06:32:29 UTC
Event Description: The file meets the ML algorithm's medium-confidence threshold.
Process Blocked: False
Operating System: Windows 10
File Name: \Device\HarddiskVolume4\Users\jdoe\AppData\Local\Microsoft\Windows \NetCache\IE \pdftodocx.msi
Connection Details: 35.242.219.202:80

Which of the following is the MOST likely cause of the issue?

A. The end user purchased and installed a PUP from a web browser
B. A bot on the computer is brute forcing passwords against a website

C. A hacker is attempting to exfiltrate sensitive data
D. Ransomware is communicating with a command-and-control server.

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 192
A security analyst needs to determine how an attacker was able to use User3 to gain a foothold within a company's network. The company's lockout policy requires that an account be locked out for a minimum of 15 minutes after three unsuccessful attempts. While reviewing the log files, the analyst discovers the following:

3/16/20 3:31:10 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:11 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:12 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:13 AM Audit Failure: CompanyNetwork\User1 Account locked out.. 3/16/20 3:31:14 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:15 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:16 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:18 AM Audit Failure: CompanyNetwork\User2 Account locked out... 3/16/20 3:31:19 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:20 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:22 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:22 AM Audit Success: CompanyNetwork\User3 Successful login. 3/16/20 3:31:10 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:31:22 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:32:40 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:33:25 AM Audit Success: CompanyNetwork\User4 Successful login.

Which of the following attacks MOST likely occurred?

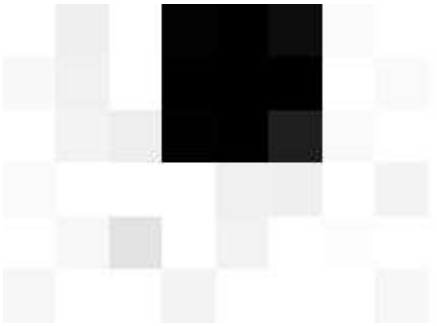
A. Dictionary
B. Credential-stuffing
C. Password-spraying
D. Brute-force

Correct Answer: C
Explanation

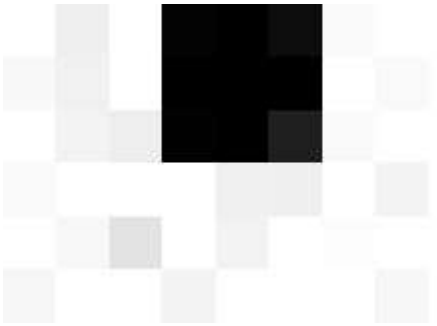
Explanation/Reference:
Section:

QUESTION 193
A security engineer needs to Implement the following requirements:

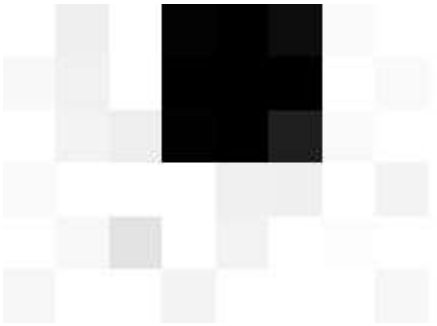
All Layer 2 switches should leverage Active Directory tor authentication.



All Layer 2 switches should use local fallback authentication If Active Directory Is offline.



All Layer 2 switches are not the same and are manufactured by several vendors.



Which of the following actions should the engineer take to meet these requirements? (Select TWO).

A. Implement RADIUS.
B. Configure AAA on the switch with local login as secondary.
C. Configure port security on the switch with the secondary login method.
D. Implement TACACS+
E. Enable the local firewall on the Active Directory server.
F. Implement a DHCP server.

Correct Answer: AB
Explanation

Explanation/Reference:
Section:

QUESTION 194
A company has determined that if its computer-based manufacturing is not functioning for 12 consecutive hours, it will lose more money that it costs to maintain the equipment. Which of the following must be less than 12 hours to maintain a positive total cost of ownership?

A. MTBF
B. RPO
C. RTO
D. MTTR

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 195
Which of the following would BEST identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms?

A. SIEM
B. CASB
C. UTM
D. DLP

Correct Answer: D
Explanation

Explanation/Reference:
Section:
Explanation:
Answer is not as clear-cut straight forward to be DLP.
https://dlpexperts.com/2016/05/casb-and-dlp-its-all-the-same-or-is-it/
It is the best guess for now. With more data inserted into the question it could be CASB.

QUESTION 196
The manager who is responsible for a data set has asked a security engineer to apply encryption to the data on a hard disk. The security engineer is an example of a:

A. data controller.
B. data owner
C. data custodian.
D. data processor

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 197
A security analyst is reviewing logs on a server and observes the following output:

01/01/2020 03:33:23 admin attempted login with password sneak
01/01/2020 03:33:32 admin attempted login with password sneaked
01/01/2020 03:33:41 admin attempted login with password sneaker
01/01/2020 03:33:50 admin attempted login with password sneer
01/01/2020 03:33:59 admin attempted login with password sneeze
01/01/2020 03:34:08 admin attempted login with password sneezy

Which of the following is the security analyst observing?

A. A rainbow table attack
B. A password-spraying attack
C. A dictionary attack
D. A keylogger attack

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 198
A security analyst is reviewing information regarding recent vulnerabilities. Which of the following will the analyst MOST likely consult to validate which platforms have been affected?

A. OSINT
B. SIEM
C. CVSS
D. CVE

Correct Answer: D
Explanation

Explanation/Reference:
Section:
Explanation:
OSINT,or open source intelligence, is the practice of collecting information from published or otherwise publicly available sources.
Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities.
Common Vulnerabilities and Exposures (CVE) is a catalog of known security threats.

QUESTION 199
A small retail business has a local store and a newly established and growing online storefront. A recent storm caused a power outage to the business and the local ISP, resulting in several hours of lost sales and delayed order processing. The business owner now needs to ensure two things:
Protection from power outages
Always-available connectivity in case of an outage.
The owner has decided to implement battery backup for the computer equipment.

Which of the following would BEST fulfill the owner's second need?

A. Lease a telecommunications line to provide POTS for dial-up access
B. Connect the business router to its own dedicated UPS
C. Purchase services from a cloud provider for high availability
D. Replace the business's wired network with a wireless network

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 200

Which of the following scenarios would make a DNS sinkhole effective in thwarting an attack?

A. An attacker is sniffing traffic to port 53, and the server is managed using unencrypted usernames and passwords.
B. An organization is experiencing excessive traffic on port 53 and suspects an attacker is trying to DoS the domain name server.
C. Malware is trying to resolve an unregistered domain name to determine if it is running in an isolated sandbox.
D. DNS routing tables have been compromised, and an attacker is rerouting traffic to malicious websites.

Correct Answer: D
Explanation

Explanation/Reference:
Section:
Explantion
Question and answer here don't precisely fit together. But it is the best possible answer from the given set of answers.
DNS sinkhole or black hole DNS is used to spoof DNS servers to prevent resolving host names of specified URLs.
This can be achieved by configuring the DNS forwarder to return a false IP address to a specific URL. DNS sinkholing can be used to prevent access of malicious URLs in an enterprise level.

QUESTION 201
Which of the following would be BEST to establish between organizations that have agreed cooperate and are engaged in early discussion to define the esponsibilities of each party, but do not want to establish a contractually binding agreement?

A. SLA
B. NDA
C. BPA
D. MOU

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 202
A user is concerned that a web application will not be able to handle unexpected or random input without crashing. Which of the following BEST describes the type of testing the user should perform?

A. Code signing
B. Fuzzing
C. Manual code review
D. Dynamic code analysis

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 203
A security analyst reviews the datacenter access logs for a fingerprint scanner and notices an abundance of

errors that correlate with users' reports of issues accessing the facility.
Which of the following MOST likely the cause of the cause of the access issues?

A. False rejection
B. Cross-over error rate
C. Efficacy rate
D. Attestation

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 204
A well-known organization has been experiencing attacks from APIs. The organization is concerned that custom malware is being created and emailed into the company or installed on USB sticks that are dropped in parking lots. Which of the following is the BEST defense against this scenario?

A. Configuring signature-based antivirus to update every 30 minutes
B. Enforcing S/MIME for email and automatically encrypting USB drives upon insertion.
C. Implementing application execution in a sandbox for unknown software.
D. Fuzzing new files for vulnerabilities if they are not digitally signed

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 205
Which of the following algorithms has the SMALLEST key size?

A. DES
B. Twofish
C. RSA
D. AES

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 206
When used at the design stage, which of the following improves the efficiency, accuracy, and speed of a database?

A. Tokenization
B. Data masking
C. Normalization
D. Obfuscation

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 207
Which of the following disaster recovery tests is The LEAST time-consuming for the disaster recovery team?

A. Tabletop
B. Parallel
C. Full interruption
D. Simulation

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 208
A security analyst needs to make a recommendation for restricting access to certain segments of the network using only data-link layer security. Which of the following controls will the analyst MOST likely recommend?

A. MAC
B. ACL
C. BPDU
D. ARP

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 209
An analyst needs to set up a method for securely transferring files between systems. One of the requirements is to authenticate the IP header and the payload. Which of the following services would BEST meet the criteria?

A. TLS
B. PFS
C. ESP
D. AH

Correct Answer: D
Explanation

Explanation/Reference:
Section:

QUESTION 210
An incident response technician collected a mobile device during an investigation. Which of the following should the technician do to maintain chain of custody?

A. Document the collection and require a sign-off when possession changes.
B. Lock the device in a safe or other secure location to prevent theft or alteration.
C. Place the device in a Faraday cage to prevent corruption of the data.

D. Record the collection in a blockchain-protected public ledger.

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 211
Which of the following organizational policies are MOST likely to detect fraud that is being conducted by existing employees? (Select TWO).

A. Offboarding
B. Mandatory vacation
C. Job rotation
D. Background checks
E. Separation of duties
F. Acceptable use

Correct Answer: BC
Explanation

Explanation/Reference:
Section:

QUESTION 212
A security manager for a retailer needs to reduce the scope of a project to comply with PCI DSS. The PCI data is located in different offices than where credit cards are accepted. All the offices are connected via MPLS back to the primary datacenter. Which of the following should the security manager implement to achieve the objective?

A. Segmentation
B. Containment
C. Geofencing
D. Isolation

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 213
The facilities supervisor for a government agency is concerned about unauthorized access to environmental systems in the event the staff WiFi network is breached. Which of the blowing would BEST address this security concern?

A. install a smart meter on the staff WiFi.
B. Place the environmental systems in the same DHCP scope as the staff WiFi.
C. Implement Zigbee on the staff WiFi access points.
D. Segment the staff WiFi network from the environmental systems network.

Correct Answer: D
Explanation

Explanation/Reference:
Section:
Explanation:
Zigbee is a Wifi technology utilized by iOT devices that is for low bandwidth data and consumes lower power.

QUESTION 214
Which of the following control sets should a well-written BCP include? (Select THREE)

A. Preventive
B. Detective
C. Deterrent
D. Corrective
E. Compensating
F. Physical
G. Recovery

Correct Answer: DEG
Explanation

Explanation/Reference:
Section:
Explanation:
Business Continuity Plans are about avoiding harm due to unusual events effecting business.

QUESTION 215
An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has only been given the documentation available to the customers of the applications. Which of the following BEST represents the type of testing that will occur?

A. Bug bounty
B. Black-box
C. Gray-box
D. White-box

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 216
A Chief Executive Officer's (CEO) personal information was stolen in a social engineering attack. Which of the following sources would reveal if the CEO's personal information is for sale?

A. Automated information sharing
B. Open-source intelligence
C. The dark web
D. Vulnerability databases

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 217
A security engineer needs to implement an MDM solution that complies with the corporate mobile device policy.
The policy states that in order for mobile users to access corporate resources on their devices the following requirements must be met:
* Mobile device OSs must be patched up to the latest release
* A screen lock must be enabled (passcode or biometric)
* Corporate data must be removed if the device is reported lost or stolen
Which of the following controls should the security engineer configure? (Select TWO)

A. Containerization
B. Storage segmentation
C. Posturing
D. Remote wipe
E. Full-device encryption
F. Geofencing

Correct Answer: BD
Explanation

Explanation/Reference:
Section:

QUESTION 218
A company is launching a new internet platform for its clients. The company does not want to implement its own authorization solution but instead wants to rely on the authorization provided by another platform. Which of the following is the BEST approach to implement the desired solution?

A. OAuth
B. TACACS+
C. SAML
D. RADIUS

Correct Answer: A
Explanation

Explanation/Reference:
Section:
Explanation:
OAuth is used for authorization using 3rd party authenticated tokens.

QUESTION 219
Which of the following scenarios BEST describes a risk reduction technique?

A. A security control objective cannot be met through a technical change, so the company purchases insurance and is no longer concerned about losses from data breaches.
B. A security control objective cannot be met through a technical change, so the company implements a policy to train users on a more secure method of operation.
C. A security control objective cannot be met through a technical change, so the company changes as method of operation
D. A security control objective cannot be met through a technical change, so the Chief Information Officer (CIO) decides to sign off on the risk.

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 220
A cybersecurity department purchased o new PAM solution. The team is planning to randomize the service account credentials of the Windows server first. Which of the following would be the BEST method to increase the security on the Linux server?

A. Randomize the shared credentials
B. Use only guest accounts to connect.
C. Use SSH keys and remove generic passwords
D. Remove all user accounts.

Correct Answer: C
Explanation

Explanation/Reference:
Section:
Explanation:
Privileged access management (PAM) consists of the cybersecurity strategies and technologies for exerting control over the elevated ("privileged") access and permissions for users, accounts, processes, and systems across an IT environment. By dialing in the appropriate level of privileged access controls, PAM helps organizations condense their organization's attack surface, and prevent, or at least mitigate, the damage arising from external attacks as well as from insider malfeasance or negligence.

QUESTION 221
A security administrator currently spends a large amount of time on common security tasks, such aa report generation, phishing investigations, and user provisioning and deprovisioning This prevents the administrator from spending time on other security projects. The business does not have the budget to add more staff members. Which of the following should the administrator implement?

A. DAC
B. ABAC
C. SCAP
D. SOAR

Correct Answer: D
Explanation

Explanation/Reference:
Section:
Explanation:

SOAR technologies enable organisations to collect and aggregate vast amounts of security data and alerts from a wide range of sources. This helps to build automated processes to respond to low-level security events and standardise threat detection and remediation procedures.

QUESTION 222
Which of the following would be the BEST resource lor a software developer who is looking to improve secure coding practices for web applications?

A. OWASP
B. Vulnerability scan results
C. NIST CSF
D. Third-party libraries

Correct Answer: A
Explanation

Explanation/Reference:
Section:
Explanation:

OWASP, which stands for the Open Web Application Security Project, is a credible non-profit foundation that focuses on improving security for businesses, customers, and developers alike.

It does this through dozens of open source projects, collaboration and training opportunities.
OWASP Security Knowledge Framework, or SFK for short, is an open-source resource knowledgebase for app developers that provides those types of information.

QUESTION 223
A network technician is installing a guest wireless network at a coffee shop. When a customer purchases an Item, the password for the wireless network is printed on the receipt so the customer can log in. Which of the following will the technician MOST likely configure to provide the highest level of security with the least amount of overhead?

A. WPA-EAP
B. WEP-TKIP
C. WPA-PSK
D. WPS-PIN

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 224
A company's Chief Information Security Officer (CISO) recently warned the security manager that the company's Chief Executive Officer (CEO) is planning to publish a controversial opinion article in a national newspaper, which may result in new cyberattacks Which of the following would be BEST for the security manager to use in a threat model?

A. Hacktivists
B. White-hat hackers
C. Script kiddies
D. Insider threats

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 225
Which of the following are requirements that must be configured for PCI DSS compliance? (Select TWO).

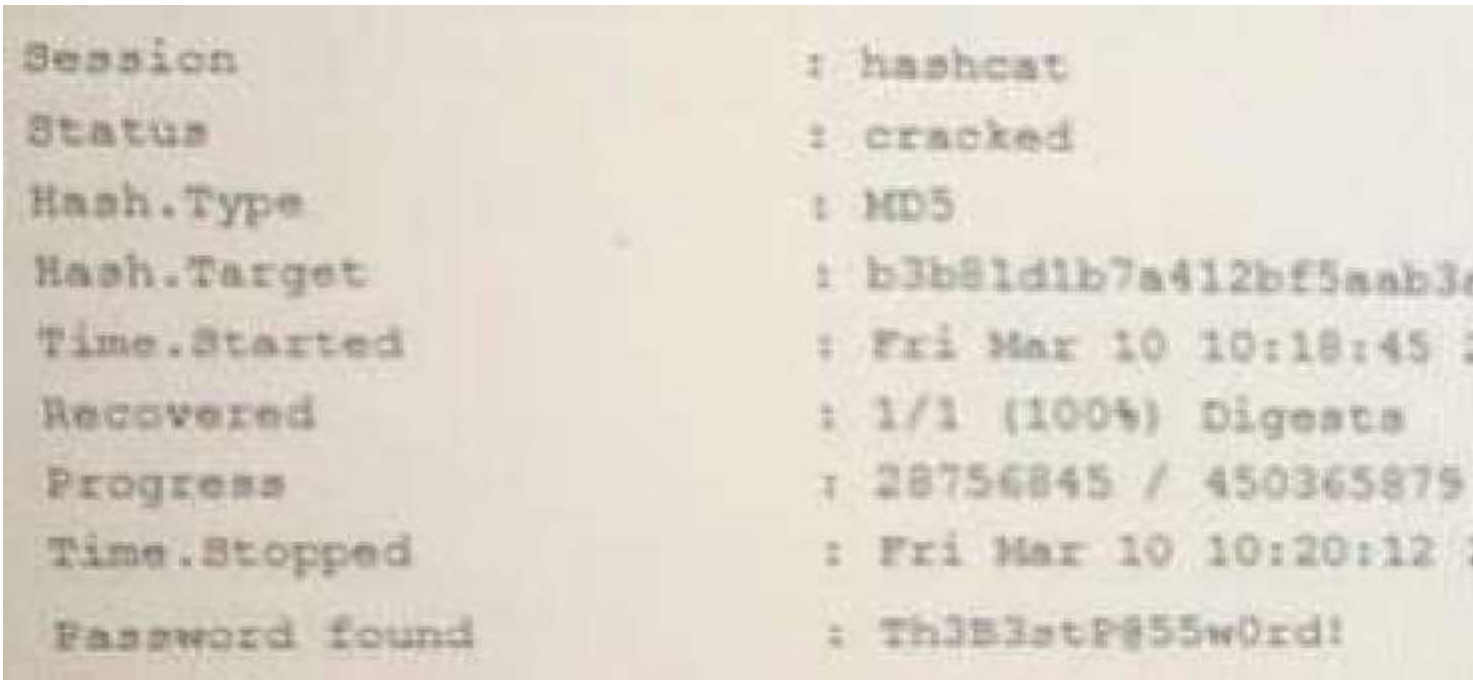
A. Testing security systems and processes regularly
B. Installing and maintaining a web proxy to protect cardholder data
C. Assigning a unique ID to each person with computer access
D. Encrypting transmission of cardholder data across private networks
E. Benchmarking security awareness training for contractors

F. Using vendor-supplied default passwords for system passwords

Correct Answer: AC
Explanation

Explanation/Reference:
Section:
Explanation:
The PCI DSS (Payment Card Industry Data Security Standard) is a security standard developed and maintained by the PCI Council. Its purpose is to help secure and protect the entire payment card ecosystem.

QUESTION 226
An attacker has successfully exfiltrated several non-salted password hashes from an online system. Given the logs below:



Which of the following BEST describes the type of password attack the attacker is performing?

A. Dictionary
B. Pass-the-hash
C. Brute-force
D. Password-spaying

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 227
A security analyst needs to produce a document that details how a security incident occurred, the steps that were taken for recovery, and how future incidents can be avoided. During which of the following stages of the response process will this activity take place?

A. Recovery

B. Identification
C. Lessons learned
D. Preparation

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 228
A company is upgrading its wireless infrastructure to WPA2-Enterprise using EAP-TLS. Which of the following must be part of the security architecture to achieve AAA? (Select TWO)

A. DNSSEC
B. Reverse proxy
C. VPN concentrator
D. PKI
E. Active Directory
F. RADIUS

Correct Answer: DF
Explanation

Explanation/Reference:
Section:

QUESTION 229
Some laptops recently went missing from a locked storage area that is protected by keyless RFID-enabled locks. There is no obvious damage to the physical space. The security manager identifies who unlocked the door, however, human resources confirms the employee was on vacation at the time of the incident. Which of the following describes what MOST likely occurred?

A. The employee's physical access card was cloned.
B. The employee is colluding with human resources
C. The employee's biometrics were harvested
D. A criminal used lock picking tools to open the door.

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 230
A company is designing the layout of a new datacenter so it will have an optimal environmental temperature Which of the following must be included? (Select TWO)

A. An air gap
B. A cold aisle
C. Removable doors
D. A hot aisle
E. An IoT thermostat
F. A humidity monitor

Correct Answer: EF
Explanation

Explanation/Reference:
Section:

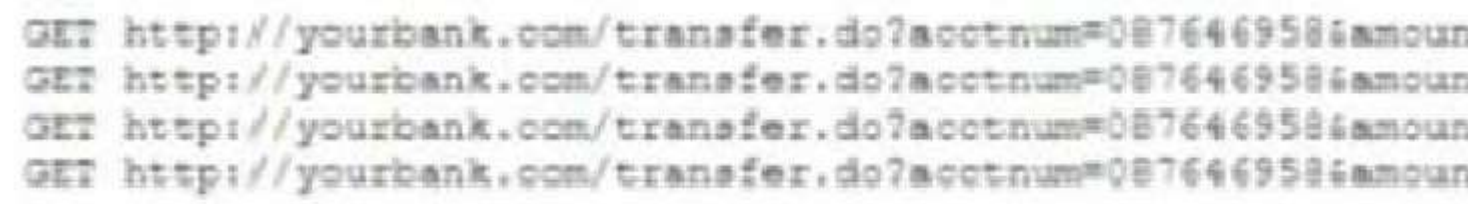
QUESTION 231
A security analyst is logged into a Windows file server and needs to see who is accessing files and from which computers Which of the following tools should the analyst use?

A. netstat
B. net share
C. netcat
D. nbtstat
E. net session

Correct Answer: E
Explanation

Explanation/Reference:
Section:

QUESTION 232
A security analyst is reviewing the output of a web server log and notices a particular account is attempting to transfer large amounts of money:



Which of the following types of attack is MOST likely being conducted?

A. SQLi
B. CSRF
C. Session replay
D. API

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 233
Which of the following environments minimizes end-user disruption and is MOST likely to be used to assess the impacts of any database migrations or major system changes by using the final version of the code?

A. Staging
B. Test
C. Production

D. Development

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 234
A security analyst is investigating an incident to determine what an attacker was able to do on a compromised laptop. The analyst reviews the following SIEM log:

Host	Event ID	Event source	Description
PC1	865	Microsoft-Windows-SoftwareRestrictionPolicies	C:\asdf234\asdf234.exe was blocked by Group Policy
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:powershell.exe Creator Process Name:outlook.exe
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:lat.ps1 Creator Process Name:powershell.exe
PC2	4625	Microsoft-Windows-Security-Auditing	An account failed to log on. LogonType:3 SecurityID:Null SID Workstation Name:PC1 Authentication Package Name:NTLM

Which of the following describes the method that was used to compromise the laptop?

A. An attacker was able to move laterally from PC1 to PC2 using a pass-the-hash attack
B. An attacker was able to bypass application whitelisting by emailing a spreadsheet attachment with an embedded PowerShell in the file
C. An attacker was able to install malware to the CAasdf234 folder and use it to gain administrator nights and launch Outlook
D. An attacker was able to phish user credentials successfully from an Outlook user profile

Correct Answer: B
Explanation

Explanation/Reference:
Section:
Explanation
This is the best possible guess after eliminating the other 3 answers.

QUESTION 235
An information security incident recently occurred at an organization, and the organization was required to report the incident to authorities and notify the affected parties. When the organization's customers became of aware of the incident, some reduced their orders or stopped placing orders entirely. Which of the following is the organization experiencing?

A. Reputation damage
B. Identity theft
C. Anonymization
D. Interrupted supply chain

Correct Answer: A
Explanation

Explanation/Reference:
Section:

QUESTION 236
An attacker is attempting to exploit users by creating a fake website with a similar URL to what users are familiar with. Which of the following social-engineering attacks does this describe?

A. Information elicitation
B. Typo squatting
C. Impersonation
D. Watering-hole attack

Correct Answer: C
Explanation

Explanation/Reference:
Section:

QUESTION 237
Users at organization have been installing programs from the internet on their workstations without first proper authorization. The organization maintains a portal from which users can install standardized programs. However, some users have administrative access on their workstations to enable legacy programs to function property. Which of the following should the security administrator consider implementing to address this issue?

A. Application code signing
B. Application whitelisting
C. Data loss prevention
D. Web application firewalls

Correct Answer: B
Explanation

Explanation/Reference:
Section:

QUESTION 238
A company has decided to move its operations to the cloud. It wants to utilize technology that will prevent users

from downloading company applications for personal use, restrict data that is uploaded, and have visibility into which applications are being used across the company. Which of the following solutions will BEST meet these requirements?

A. An NGFW
B. A CASB
C. Application whitelisting
D. An NG-SWG

Correct Answer: B
Explanation

Explanation/Reference:
Section: