Exam Topic Breakdown

Exam Topic	**Number of Questions**
Topic 1 : Exam Set 1	180
Topic 2 : Exam Set 2	182
Topic 3 : Exam Set 3	111
Topic 4 : Exam Set 4	75
TOTAL	548

Topic 1, Exam Set 1

Question #:1 - (Exam Topic 1)

During a Chief Information Security Officer (CISO) convention to discuss security awareness, the attendees are provided with a network connection to use as a resource. As the convention progresses, one of the attendees starts to notice delays in the connection, and the HTTPS site requests are reverting to HTTP. Which of the following BEST describes what is happening?

A. Birthday collision on the certificate key

B. DNS hacking to reroute traffic

C. Brute force to the access point

D. A SSL/TLS downgrade

Question #:2 - (Exam Topic 1)

A security administrator wants to implement a program that tests a user's ability to recognize attacks over the organization's email system. Which of the following would be BEST suited for this task?

A. Social media analysis

B. Annual information security training

C. Gamification

D. Phishing campaign

Question #:3 - (Exam Topic 1)

A financial institution would like to store its customer data in a cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would BEST meet the requirement?

A. Asymmetric

B. Symmetric

C. Homomorphic

D. Ephemeral

Question #:4 - (Exam Topic 1)

The Chief Technology Officer of a local college would like visitors to utilize the school's WiFi but must be able to associate potential malicious activity to a specific person. Which of the following would BEST allow this objective to be met?

A. Requiring all new, on-site visitors to configure their devices to use WPS

B. Implementing a new SSID for every event hosted by the college that has visitors

C. Creating a unique PSK for every visitor when they arrive at the reception area

D. Deploying a captive portal to capture visitors' MAC addresses and names

Question #:5 - (Exam Topic 1)

A company would like to provide flexibility for employees on device preference. However, the company is concerned about supporting too many different types of hardware. Which of the following deployment models will provide the needed flexibility with the GREATEST amount of control and security over company data and infrastructure?

A. BYOD

B. VDI

C. COPE

D. CYOD

Question #:6 - (Exam Topic 1)

An organization wants to enable built-in FDE on all laptops Which of the following should the organization ensure is Installed on all laptops?

A. TPM

B. CA

C. SAML

D. CRL

Question #:7 - (Exam Topic 1)

The compliance team requires an annual recertification of privileged and non-privileged user access. However, multiple users who left the company six months ago still have access. Which of the following would have prevented this compliance violation?

A. Account audits

B. AUP

C. Password reuse

D. SSO

Question #:8 - (Exam Topic 1)

A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

A. A reverse proxy

B. A decryption certificate

C. A spill-tunnel VPN

D. Load-balanced servers

Question #:9 - (Exam Topic 1)

During a security assessment, a security finds a file with overly permissive permissions. Which of the following tools will allow the analyst to reduce the permission for the existing users and groups and remove the set-user-ID from the file?

A. 1s

B. chflags

C. chmod

D. lsof

E. setuid

Question #:10 - (Exam Topic 1)

Which of the following must be in place before implementing a BCP?

A. SLA

B. AUP

C. NDA

D. BIA

Question #:11 - (Exam Topic 1)

Which of the following provides a catalog of security and privacy controls related to the United States federal information systems?

A. GDPR

B. PCI DSS

C. ISO 27000

D. NIST 800-53

Question #:12 - (Exam Topic 1)

A retail company that is launching a new website to showcase the company’s product line and other information for online shoppers registered the following URLs:

* www companysite com
* shop companysite com
* about-us companysite com
* contact-us. companysite com
* secure-logon company site com

Which of the following should the company use to secure its website if the company is concerned with convenience and cost?

A. A self-signed certificate

B. A root certificate

C. A code-signing certificate

D. A wildcard certificate

E. An extended validation certificate

Question #:13 - (Exam Topic 1)

An employee's company account was used in a data breach Interviews with the employee revealed:

- The employee was able to avoid changing passwords by using a previous password again.
- The account was accessed from a hostile, foreign nation, but the employee has never traveled to any other countries.

Which of the following can be implemented to prevent these issues from reoccurring? (Select TWO)

A. Geographic dispersal

B. Password complexity

C. Password history

D. Geotagging

E. Password lockout

F. Geofencing

Question #:14 - (Exam Topic 1)

A security architect is implementing a new email architecture for a company. Due to security concerns, the Chief Information Security Officer would like the new architecture to support email encryption, as well as provide for digital signatures. Which of the following should the architect implement?

A. TOP

B. IMAP

C. HTTPS

D. S/MIME

Question #:15 - (Exam Topic 1)

A user attempts to load a web-based application, but the expected login screen does not appear A help desk analyst troubleshoots the issue by running the following command and reviewing the output on the user's PC

```
user> nslookup software-solution.com
Server: rogue.comptia.com
Address: 172.16.1.250
Non-authoritative answer:
Name: software-solution.com
Address: 10.20.10.10
```

The help desk analyst then runs the same command on the local PC:

```
helpdesk> nslookup software-solution.com
Server: dns.comptia.com Address: 172.16.1.1
Non-authoritative answer:
Name: software-solution.com Address: 172.16.1.10
```

Which of the following BEST describes the attack that is being detected?

A. Domain hijacking

B. DNS poisoning

C. MAC flooding

D. Evil twin

Question #:16 - (Exam Topic 1)

The Chief Information Security Officer (CISO) has decided to reorganize security staff to concentrate on incident response and to outsource outbound Internet URL categorization and filtering to an outside company. Additionally, the CISO would like this solution to provide the same protections even when a company laptop or mobile device is away from a home office. Which of the following should the CISO choose?

A. CASB

B. Next-generation SWG

C. NGFW

D. Web-application firewall

Question #:17 - (Exam Topic 1)

A security engineer is hardening existing solutions to reduce application vulnerabilities. Which of the following solutions should the engineer implement FIRST? (Select TWO)

A. Auto-update

B. HTTP headers

C. Secure cookies

D. Third-party updates

E. Full disk encryption

F. Sandboxing

G. Hardware encryption

Question #:18 - (Exam Topic 1)

Per company security policy, IT staff members are required to have separate credentials to perform administrative functions using just-in-time permissions. Which of the following solutions is the company Implementing?

A. Privileged access management

B. SSO

C. RADIUS

D. Attribute-based access control

Question #:19 - (Exam Topic 1)

A security analyst is running a vulnerability scan to check for missing patches during a suspected security rodent During which of the following phases of the response process is this activity MOST likely occurring?

A. Containment

B. Identification

C. Recovery

D. Preparation

Question #:20 - (Exam Topic 1)

A third party asked a user to share a public key for secure communication. Which of the following file formats should the user choose to share the key?

A. .pfx

B. .csr

C. .pvk

D. .cer

Question #:21 - (Exam Topic 1)

A user reports trouble using a corporate laptop. The laptop freezes and responds slowly when writing documents and the mouse pointer occasionally disappears.

The task list shows the following results

Name	CPU%	Memory	Network %
Calculator	0%	4.1MB	0Mbps
Chrome	0.2%	207.1MB	0.1Mbs
Explorer	99.7%	2.15GB	0.1Mbs
Notepad	0%	3.9MB	0Mbs

Which of the following is MOST likely the issue?

A. RAT

B. PUP

C. Spyware

D. Keylogger

Question #:22 - (Exam Topic 1)

A company reduced the area utilized in its datacenter by creating virtual networking through automation and by creating provisioning routes and rules through scripting. Which of the following does this example describe?

A. laC

B. MSSP

C. Containers

D. SaaS

Question #:23 - (Exam Topic 1)

An organization is moving away from the use of client-side and server-side certificates for EAR The company would like for the new EAP solution to have the ability to detect rogue access points. Which of the following would accomplish these requirements?

A. PEAP

B. EAP-FAST

C. EAP-TLS

D. EAP-TTLS

Question #:24 - (Exam Topic 1)

A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

A. An incident response plan

B. A communications plan

C. A business continuity plan

D. A disaster recovery plan

Question #:25 - (Exam Topic 1)

An employee received multiple messages on a mobile device. The messages instructing the employee to pair the device to an unknown device. Which of the following BEST describes What a malicious person might be doing to cause this issue to occur?

A. Jamming

B. Bluesnarfing

C. Evil twin

D. Rogue access point

Question #:26 - (Exam Topic 1)

A company is required to continue using legacy software to support a critical service. Which of the following BEST explains a risk of this practice?

A. Default system configuration

B. Unsecure protocols

C. Lack of vendor support

D. Weak encryption

Question #:27 - (Exam Topic 1)

A security manager needs to assess the security posture of one of the organization's vendors. The contract with the vendor does not allow for auditing of the vendor's security controls. Which of (he following should the manager request to complete the assessment?

A. A service-level agreement

B. A business partnership agreement

C. A SOC 2 Type 2 report

D. A memorandum of understanding

Question #:28 - (Exam Topic 1)

A company recently experienced a major breach. An investigation concludes that customer credit card data was stolen and exfiltrated through a dedicated business partner connection to a vendor, who is not held to the same security control standards. Which of the following is the MOST likely source of the breach?

A. Side channel

B. Supply chain

C. Cryptographic downgrade

D. Malware

Question #:29 - (Exam Topic 1)

A help desk technician receives an email from the Chief Information Officer (C/O) asking for documents. The technician knows the CIO is on vacation for a few weeks. Which of the following should the technician do to validate the authenticity of the email?

A. Check the metadata in the email header of the received path in reverse order to follow the email’s path.

B. Hover the mouse over the CIO's email address to verify the email address.

C. Look at the metadata in the email header and verify the "From." line matches the CIO's email address.

D. Forward the email to the CIO and ask if the CIO sent the email requesting the documents.

Question #:30 - (Exam Topic 1)

Which of the following describes a maintenance metric that measures the average time required to troubleshoot and restore failed equipment?

A. RTO

B. MTBF

C. MTTR

D. RPO

Question #:31 - (Exam Topic 1)

A network analyst is setting up a wireless access point for a home office in a remote, rural location. The requirement is that users need to connect to the access point securely but do not want to have to remember passwords. Which of the following should the network analyst enable to meet the requirement?

A. MAC address filtering

B. 802.1X

C. Captive portal

D. WPS

Question #:32 - (Exam Topic 1)

After segmenting the network, the network manager wants to control the traffic between the segments. Which of the following should the manager use to control the network traffic?

A. A DMZ

B. A VPN a

C. A VLAN

D. An ACL

Question #:33 - (Exam Topic 1)

A large enterprise has moved all its data to the cloud behind strong authentication and encryption. A sales director recently had a laptop stolen, and later, enterprise data was found to have been compromised from a local database. Which of the following was the MOST likely cause?

A. Shadow IT

B. Credential stuffing

C. SQL injection

D. Man in the browser

E. Bluejacking

Question #:34 - (Exam Topic 1)

A company is concerned about individuals driving a car into the building to gain access. Which of the following security controls would work BEST to prevent this from happening?

A. Bollard

B. Camera

C. Alarms

D. Signage

E. Access control vestibule

Question #:35 - (Exam Topic 1)

Employees at a company are receiving unsolicited text messages on their corporate cell phones. The unsolicited text messages contain a password reset Link. Which of the attacks is being used to target the company?

A. Phishing

B. Vishing

C. Smishing

D. Spam

Question #:36 - (Exam Topic 1)

A company Is planning to install a guest wireless network so visitors will be able to access the Internet. The stakeholders want the network to be easy to connect to so time is not wasted during meetings. The WAPs are configured so that power levels and antennas cover only the conference rooms where visitors will attend meetings. Which of the following would BEST protect the company's Internal wireless network against visitors accessing company resources?

A. Configure the guest wireless network to be on a separate VLAN from the company's internal wireless network

B. Change the password for the guest wireless network every month.

C. Decrease the power levels of the access points for the guest wireless network.

D. Enable WPA2 using 802.1X for logging on to the guest wireless network.

Question #:37 - (Exam Topic 1)

Which of the following environments can be stood up in a short period of time, utilizes either dummy data or actual data, and is used to demonstrate and model system capabilities and functionality for a fixed, agreed-upon duration of time?

A. PoC

B. Production

C. Test

D. Development

Question #:38 - (Exam Topic 1)

A security assessment found that several embedded systems are running insecure protocols. These Systems were purchased two years ago and the company that developed them is no longer in business Which of the following constraints BEST describes the reason the findings cannot be remediated?

A. inability to authenticate

B. Implied trust

C. Lack of computing power

D. Unavailable patch

Question #:39 - (Exam Topic 1)

A systems analyst determines the source of a high number of connections to a web server that were initiated by ten different IP addresses that belong to a network block in a specific country. Which of the following techniques will the systems analyst MOST likely implement to address this issue?

A. Content filter

B. SIEM

C. Firewall rules

D. DLP

Question #:40 - (Exam Topic 1)

A software company is analyzing a process that detects software vulnerabilities at the earliest stage possible. The goal is to scan the source looking for unsecure practices and weaknesses before the application is deployed in a runtime environment. Which of the following would BEST assist the company with this objective?

A. Use fuzzing testing

B. Use a web vulnerability scanner

C. Use static code analysis

D. Use a penetration-testing OS

Question #:41 - (Exam Topic 1)

A company recently decided to allow its employees to use their personally owned devices for tasks like checking email and messaging via mobile applications. The company would like to use MDM, but employees are concerned about the loss of personal data. Which of the following should the IT department implement to BEST protect the company against company data loss while still addressing the employees' concerns?

A. Enable the remote-wiping option in the MDM software in case the phone is stolen.

B. Configure the MDM software to enforce the use of PINs to access the phone.

C. Configure MDM for FDE without enabling the lock screen.

D. Perform a factory reset on the phone before installing the company's applications.

Question #:42 - (Exam Topic 1)

An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?

A. It allows for the sharing of digital forensics data across organizations

B. It provides insurance in case of a data breach

C. It provides complimentary training and certification resources to IT security staff.

D. It certifies the organization can work with foreign entities that require a security clearance

E. It assures customers that the organization meets security standards

Question #:43 - (Exam Topic 1)

A security engineer needs to create a network segment that can be used for servers that require connections from untrusted networks. Which of the following should the engineer implement?

A. An air gap

B. A hot site

C. A VUAN

D. A screened subnet

Question #:44 - (Exam Topic 1)

A Chief information Officer is concerned about employees using company-issued laptops to steal data when accessing network shares. Which of the following should the company implement?

A. DLP

B. CASB

C. HIDS

D. EDR

E. UEFI

Question #:45 - (Exam Topic 1)

An organization wants to integrate its incident response processes into a workflow with automated decision points and actions based on predefined playbooks. Which of the following should the organization implement?

A. SIEM

B. SOAR

C. EDR

D. CASB

Question #:46 - (Exam Topic 1)

A security analyst needs an overview of vulnerabilities for a host on the network. Which of the following is the BEST type of scan for the analyst to run to discover which vulnerable services are running?

A. Non-credentialed

B. Web application

C. Privileged

D. Internal

Question #:47 - (Exam Topic 1)

Which of the following identifies the point in time when an organization will recover data in the event of an outage?

A. SLA

B. RPO

C. MTBF

D. ARO

Question #:48 - (Exam Topic 1)

A company recently experienced an attack during which its main website was directed to the attacker's web server, allowing the attacker to harvest credentials from unsuspecting customers. Which of the following should the company implement to prevent this type of attack from occurring in the future?

A. IPsec

B. SSL/TLS

C. DNSSEC

D. S/MIME

Question #:49 - (Exam Topic 1)

A security analyst must enforce policies to harden an MDM infrastructure. The requirements are as follows:

* Ensure mobile devices can be tracked and wiped.

* Confirm mobile devices are encrypted.

Which of the following should the analyst enable on all the devices to meet these requirements?

A. A Geofencing

B. Biometric authentication

C. Geolocation

D. Geotagging

Question #:50 - (Exam Topic 1)

Which of the following function as preventive, detective, and deterrent controls to reduce the risk of physical theft? (Select TWO).

A. Mantraps

B. Security guards

C. Video surveillance

D. Fences

E. Bollards

F. Antivirus

Question #:51 - (Exam Topic 1)

A security incident has been resolved Which of the following BEST describes the importance of the final phase of the incident response plan?

A. It examines and documents how well the team responded discovers what caused the incident, and determines how the incident can be avoided in the future

B. It returns the affected systems back into production once systems have been fully patched, data restored and vulnerabilities addressed

C. It identifies the incident and the scope of the breach how it affects the production environment, and the ingress point

D. It contains the affected systems and disconnects them from the network, preventing further spread of the attack or breach

Question #:52 - (Exam Topic 1)

The technology department at a large global company is expanding its Wi-Fi network infrastructure at the headquarters building. Which of the following should be closely coordinated between the technology, cybersecurity, and physical security departments?

A. Authentication protocol

B. Encryption type

C. WAP placement

D. VPN configuration

Question #:53 - (Exam Topic 1)

The security team received a report of copyright infringement from the IP space of the corporate network. The report provided a precise time stamp for the incident as well as the name of the copyrighted files. The analyst has been tasked with determining the infringing source machine and instructed to implement measures to prevent such incidents from occurring again. Which of the following is MOST capable of accomplishing both tasks?

A. HIDS

B. Allow list

C. TPM

D. NGFW

Question #:54 - (Exam Topic 1)

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

Question #:55 - (Exam Topic 1)

Which of the following is required in order for an IDS and a WAF to be effective on HTTPS traffic?

A. Hashing

B. DNS sinkhole

C. TLS inspection

D. Data masking

Question #:56 - (Exam Topic 1)

Which of the following in a forensic investigation should be priorities based on the order of volatility? (Select TWO).

A. Page files

B. Event logs

C. RAM

D. Cache

E. Stored files

F. HDD

Question #:57 - (Exam Topic 1)

A security engineer needs to build a solution to satisfy regulatory requirements that stale certain critical servers must be accessed using MFA However, the critical servers are older and are unable to support the addition of MFA, Which of the following will the engineer MOST likely use to achieve this objective?

A. A forward proxy

B. A stateful firewall

C. A jump server

D. A port tap

Question #:58 - (Exam Topic 1)

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 the employee'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

Question #:59 - (Exam Topic 1)

A backdoor was detected in the containerized application environment. The investigation detected that a zero-day vulnerability was introduced when the latest container image version was downloaded from a public registry. Which of the following is the BEST solution to prevent this type of incident from occurring again?

A. Enforce the use of a controlled trusted source of container images

B. Deploy an IPS solution capable of detecting signatures of attacks targeting containers

C. Define a vulnerability scan to assess container images before being introduced on the environment

D. Create a dedicated VPC for the containerized environment

Question #:60 - (Exam Topic 1)

A company acquired several other small companies The company that acquired the others is transitioning network services to the cloud. The company wants to make sure that performance and security remain intact. Which of the following BEST meets both requirements?

A. High availability

B. Application security

C. Segmentation

D. Integration and auditing

Question #:61 - (Exam Topic 1)

A store receives reports that shoppers’ credit card information is being stolen. Upon further analysis, those same shoppers also withdrew money from an ATM in that store.

The attackers are using the targeted shoppers’ credit card information to make online purchases. Which of the following attacks is the MOST probable cause?

A. Identity theft

B. RFID cloning

C. Shoulder surfing

D. Card skimming

Question #:62 - (Exam Topic 1)

A desktop support technician recently installed a new document-scanning software program on a computer. However, when the end user tried to launch the program, it did not respond. Which of the following is MOST likely the cause?

A. A new firewall rule is needed to access the application.

B. The system was quarantined for missing software updates.

C. The software was not added to the application whitelist.

D. The system was isolated from the network due to infected software

Question #:63 - (Exam Topic 1)

Which of the following environments utilizes dummy data and is MOST likely to be installed locally on a system that allows code to be assessed directly and modified easily with each build?

A. Production

B. Test

C. Staging

D. Development

Question #:64 - (Exam Topic 1)

A bad actor tries to persuade someone to provide financial information over the phone in order to gain access to funds. Which of the following types of attacks does this scenario describe?

A. Vishing

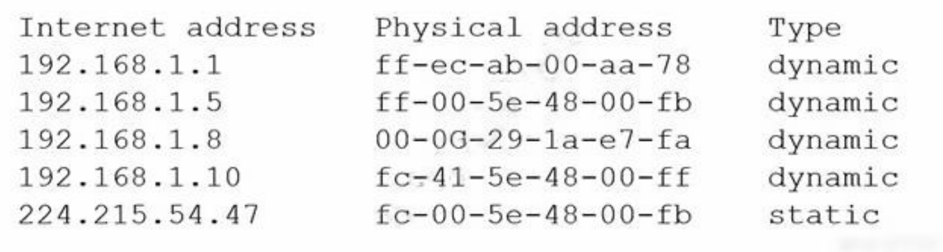
B. Phishing

C. Spear phishing

D. Whaling

Question #:65 - (Exam Topic 1)

A security analyst has received several reports of an issue on an internal web application. Users state they are having to provide their credentials twice to log in. The analyst checks with the application team and notes this is not an expected behavior. After looking at several logs, the analyst decides to run some commands on the gateway and obtains the following output:



```
Internet address     Physical address     Type
192.168.1.1          ff-ec-ab-00-aa-78    dynamic
192.168.1.5          ff-00-5e-48-00-fb    dynamic
192.168.1.8          00-0G-29-1a-e7-fa    dynamic
192.168.1.10         fc-41-5e-48-00-ff    dynamic
224.215.54.47        fc-00-5e-48-00-fb    static
```

Which of the following BEST describes the attack the company is experiencing?

A. MAC flooding

B. URL redirection

C. ARP poisoning

D. DNS hijacking

Question #:66 - (Exam Topic 1)

A company wants to modify its current backup strategy to modify its current backup strategy to minimize the number of backups that would need to be restored in case of data loss. Which of the following would be the BEST backup strategy

A. Incremental backups followed by differential backups

B. Full backups followed by incremental backups

C. Delta backups followed by differential backups

D. Incremental backups followed by delta backups

E. Full backup followed by different backups

Question #:67 - (Exam Topic 1)

Which of the following is a risk that is specifically associated with hosting applications in the public cloud?

A. Unsecured root accounts

B. Zero day

C. Shared tenancy

D. Insider threat

Question #:68 - (Exam Topic 1)

A company was compromised, and a security analyst discovered the attacker was able to get access to a service account. The following logs were discovered during the investigation:

```
User account 'JHDoe' does not exist…
User account 'VMAdmin' does not exist…
User account 'tomcat' wrong password…
User account 'Admin' does not exist…
```

Which of the following MOST likely would have prevented the attacker from learning the service account name?

A. Race condition testing

B. Proper error handling

C. Forward web server logs to a SIEM

D. Input sanitization

Question #:69 - (Exam Topic 1)

As part of the building process for a web application, the compliance team requires that all PKI certificates are rotated annually and can only contain wildcards at the secondary subdomain level. Which of the following certificate properties will meet these requirements?

A. HTTPS://*.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022

B. HTTPS://app1.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022

C. HTTPS://*.app1.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022

D. HTTPS://".comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2023

Question #:70 - (Exam Topic 1)

Remote workers in an organization use company-provided laptops with locally installed applications and locally stored data. Users can store data on a remote server using an encrypted connection. The organization discovered data stored on a laptop had been made available to the public Which of the following security solutions would mitigate the risk of future data disclosures?

A. FDE

B. TPM

C. HIDS

D. VPN

Question #:71 - (Exam Topic 1)

Which of the following is the MOST secure but LEAST expensive data destruction method for data that is stored on hard drives?

A. Pulverizing

B. Shredding

C. Incinerating

D. Degaussing

Question #:72 - (Exam Topic 1)

An organization discovered a disgruntled employee exfiltrated a large amount of PII data by uploading files. Which of the following controls should the organization consider to mitigate this risk?

A. EDR

B. Firewall

C. HIPS

D. DLP

Question #:73 - (Exam Topic 1)

As part of a company's ongoing SOC maturation process, the company wants to implement a method to share cyber threat intelligence data with outside security partners. Which of the following will the company MOST likely implement?

A. TAXII

B. TLP

C. TTP

D. STIX

Question #:74 - (Exam Topic 1)

Which of the following incident response steps occurs before containment?

A. Eradication

B. Recovery

C. Lessons learned

D. Identification

Question #:75 - (Exam Topic 1)

Which of the following environments would MOST likely be used to assess the execution of component parts of a system at both the hardware and software levels and to measure performance characteristics?

A. Test

B. Staging

C. Development

D. Production

Question #:76 - (Exam Topic 1)

A customer has reported that an organization's website displayed an image of a smiley face rather than the expected web page for a short time two days earlier. A security analyst reviews log tries and sees the following around the lime of the incident:

Website	Time	Name server	A record
CompTIA.org	8:10	names.comptia.org	192.168.1.10
CompTIA.org	9:00	names.comptia.org	192.168.1.10
CompTIA.org	9:30	ns.attacker.org	10.10.50.5
CompTIA.org	10:00	names.comptia.org	192.168.1.10

Which of the following is MOST likely occurring?

A. Invalid trust chain

B. Domain hijacking

C. DNS poisoning

D. URL redirection

Question #:77 - (Exam Topic 1)

A company recently experienced an attack during which its main website was directed to the attacker's web server, allowing the attacker to harvest credentials from unsuspecting customers. Which of the following should the company Implement to prevent this type of attack from occurring in the future?

A. IPSec

B. SSL/TLS

C. DNSSEC

D. S/MIME

Question #:78 - (Exam Topic 1)

A company has discovered unauthorized devices are using its WiFi network, and it wants to harden the access point to improve security. Which of the following configurations should an analysis enable To improve security? (Select TWO.)

A. RADIUS

B. PEAP

C. WPS

D. WEP-EKIP

E. SSL

F. WPA2-PSK

Question #:79 - (Exam Topic 1)

A systems engineer is building a new system for production. Which of the following is the FINAL step to be performed prior to promotion to production?

A. Disable unneeded services.

B. Install the latest security patches.

C. Run a vulnerability scan.

D. Encrypt all disks.

Question #:80 - (Exam Topic 1)

An application owner reports suspicious activity on an internal financial application from various internal users within the past 14 days. A security analyst notices the following:

•Financial transactions were occurring during irregular time frames and outside of business hours by unauthorized users.

•Internal users in question were changing their passwords frequently during that time period.

•A jump box that several domain administrator users use to connect to remote devices was recently compromised.

•The authentication method used in the environment is NTLM.

Which of the following types of attacks is MOST likely being used to gain unauthorized access?

A. Pass-the-hash

B. Brute-force

C. Directory traversal

D. Replay

Question #:81 - (Exam Topic 1)

A dynamic application vulnerability scan identified code injection could be performed using a web form.

Which of the following will be BEST remediation to prevent this vulnerability?

A. Implement input validations

B. Deploy MFA

C. Utilize a WAF

D. Configure HIPS

Question #:82 - (Exam Topic 1)

A company installed several crosscut shredders as part of increased information security practices targeting data leakage risks. Which of the following will this practice reduce?

A. Dumpster diving

B. Shoulder surfing

C. Information elicitation

D. Credential harvesting

Question #:83 - (Exam Topic 1)

While reviewing pcap data, a network security analyst is able to locate plaintext usernames and passwords being sent from workstations to network witches. Which of the following is the security analyst MOST likely observing?

A. SNMP traps

B. A Telnet session

C. An SSH connection

D. SFTP traffic

Question #:84 - (Exam Topic 1)

Which of the following authentication methods sends out a unique password to be used within a specific number of seconds?

A. TOTP

B. Biometrics

C. Kerberos

D. LDAP

Question #:85 - (Exam Topic 1)

A network engineer and a security engineer are discussing ways to monitor network operations. Which of the following is the BEST method?

A. Disable Telnet and force SSH.

B. Establish a continuous ping.

C. Utilize an agentless monitor

D. Enable SNMPv3 With passwords.

Question #:86 - (Exam Topic 1)

A global company is experiencing unauthorized logging due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks. Which of the following would be the BEST control for the company to require from prospective vendors?

A. IP restrictions

B. Multifactor authentication

C. A banned password list

D. A complex password policy

Question #:87 - (Exam Topic 1)

A Chief Information Officer receives an email stating a database will be encrypted within 24 hours unless a payment of $20,000 is credited to the account mentioned In the email. This BEST describes a scenario related to:

A. whaling.

B. smishing.

C. spear phishing

D. vishing

Question #:88 - (Exam Topic 1)

A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager claimed the reports were previously sent via email, but then quickly generated and backdated the reports before submitting them as plain text within the body of a new email message thread. Which of the following actions MOST likely supports an investigation for fraudulent submission?

A. Establish chain of custody.

B. Inspect the file metadata.

C. Reference the data retention policy.

D. Review the email event logs

Question #:89 - (Exam Topic 1)

A major clothing company recently lost a large amount of proprietary information. The security officer must find a solution to ensure this never happens again.

Which of the following is the BEST technical implementation to prevent this from happening again?

A. Configure DLP solutions

B. Disable peer-to-peer sharing

C. Enable role-based

D. Mandate job rotation

E. Implement content filters

Question #:90 - (Exam Topic 1)

Which of the following involves the inclusion of code in the main codebase as soon as it is written?

A. Continuous monitoring

B. Continuous deployment

C. Continuous Validation

D. Continuous integration

Question #:91 - (Exam Topic 1)

During an investigation, the incident response team discovers that multiple administrator accounts were suspected of being compromised. The host audit logs indicate a repeated brute-force attack on a single administrator account followed by suspicious logins from unfamiliar geographic locations. Which of the following data sources would be BEST to use to assess the accounts impacted by this attack?

A. User behavior analytics

B. Dump files

C. Bandwidth monitors

D. Protocol analyzer output

Question #:92 - (Exam Topic 1)

The Chief Information Security Officer wants to pilot a new adaptive, user-based authentication method. The concept Includes granting logical access based on physical location and proximity. Which of the following Is the BEST solution for the pilot?

A. Geofencing

B. Self-sovereign identification

C. PKl certificates

D. SSO

Question #:93 - (Exam Topic 1)

Which of the following authentication methods is considered to be the LEAST secure?

A. TOTP

B. SMS

C. HOTP

D. Token key

Question #:94 - (Exam Topic 1)

Which of the following controls would provide the BEST protection against tailgating?

A. Access control vestibule

B. Closed-circuit television

C. Proximity card reader

D. Faraday cage

Question #:95 - (Exam Topic 1)

The SIEM at an organization has detected suspicious traffic coming to a workstation in its internal network. An analyst in the SOC investigates the workstation and discovers malware that is associated with a botnet is installed on the device. A review of the logs on the workstation reveals that the privileges of the local account were escalated to a local administrator. To which of the following groups should the analyst report this real-world event?

A. The NOC team

B. The vulnerability management team

C. The CIRT

D. The read team

Question #:96 - (Exam Topic 1)

Which of the following should a technician consider when selecting an encryption method for data that needs to remain confidential for a specific length of time?

A. The key length of the encryption algorithm

B. The encryption algorithm's longevity

C. A method of introducing entropy into key calculations

D. The computational overhead of calculating the encryption key

Question #:97 - (Exam Topic 1)

After a phishing scam for a user's credentials, the red team was able to craft a payload to deploy on a server. The attack allowed the installation of malicious software that initiates a new remote session.

Which of the following types of attacks has occurred?

A. Privilege escalation

B. Session replay

C. Application programming interface

D. Directory traversal

Question #:98 - (Exam Topic 1)

An organization would like to remediate the risk associated with its cloud service provider not meeting its advertised 99.999% availability metrics. Which of the following should the organization consult for the exact requirements for the cloud provider?

A. SLA

B. BPA

C. NDA

D. MOU

Question #:99 - (Exam Topic 1)

Which of the following BEST describes the team that acts as a referee during a penetration-testing exercise?

A. White team

B. Purple team

C. Green team

D. Blue team

E. Red team

Question #:100 - (Exam Topic 1)

During a forensic investigation, a security analyst discovered that the following command was run on a compromised host:

```
crackmapexec smb 192.168.10.232 -u localadmin -H 0A3CE8D07A46E5C51070F03593E0A5E6
```

Which of the following attacks occurred?

A. Buffer overflow

B. Pass the hash

C. SQL injection

D. Replay attack

Question #:101 - (Exam Topic 1)

The Chief Information Security Officer directed a risk reduction in shadow IT and created a policy requiring all unsanctioned high-risk SaaS applications to be blocked from user access. Which of the following is the BEST security solution to reduce this risk?

A. CASB

B. VPN concentrator

C. MFA

D. VPC endpoint

Question #:102 - (Exam Topic 1)

A grocery store is expressing security and reliability concerns regarding the on-site backup strategy currently being performed by locally attached disks. The main concerns are the physical security of the backup media and the durability of the data stored on these devices. Which of the following is a cost-effective approach to address these concerns?

A. Enhance resiliency by adding a hardware RAID.

B. Move data to a tape library and store the tapes off-site

C. Install a local network-attached storage.

D. Migrate to a cloud backup solution

Question #:103 - (Exam Topic 1)

Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?

A. Risk matrix

B. Risk tolerance

C. Risk register

D. Risk appetite

Question #:104 - (Exam Topic 1)

Developers are writing code and merging it into shared repositories several times a day, where it is tested automatically. Which of the following concepts does this BEST represent?

A. Functional testing

B. Stored procedures

C. Elasticity

D. Continuous integration

Question #:105 - (Exam Topic 1)

As part of annual audit requirements, the security team performed a review of exceptions to the company policy that allows specific users the ability to use USB storage devices on their laptops The review yielded the following results.

- The exception process and policy have been correctly followed by the majority of users

- A small number of users did not create tickets for the requests but were granted access

- All access had been approved by supervisors.

- Valid requests for the access sporadically occurred across multiple departments.

- Access, in most cases, had not been removed when it was no longer needed

Which of the following should the company do to ensure that appropriate access is not disrupted but unneeded access is removed in a reasonable time frame?

A. Create an automated, monthly attestation process that removes access if an employee's supervisor denies the approval

B. Remove access for all employees and only allow new access to be granted if the employee's supervisor approves the request

C. Perform a quarterly audit of all user accounts that have been granted access and verify the exceptions with the management team

D. Implement a ticketing system that tracks each request and generates reports listing which employees actively use USB storage devices

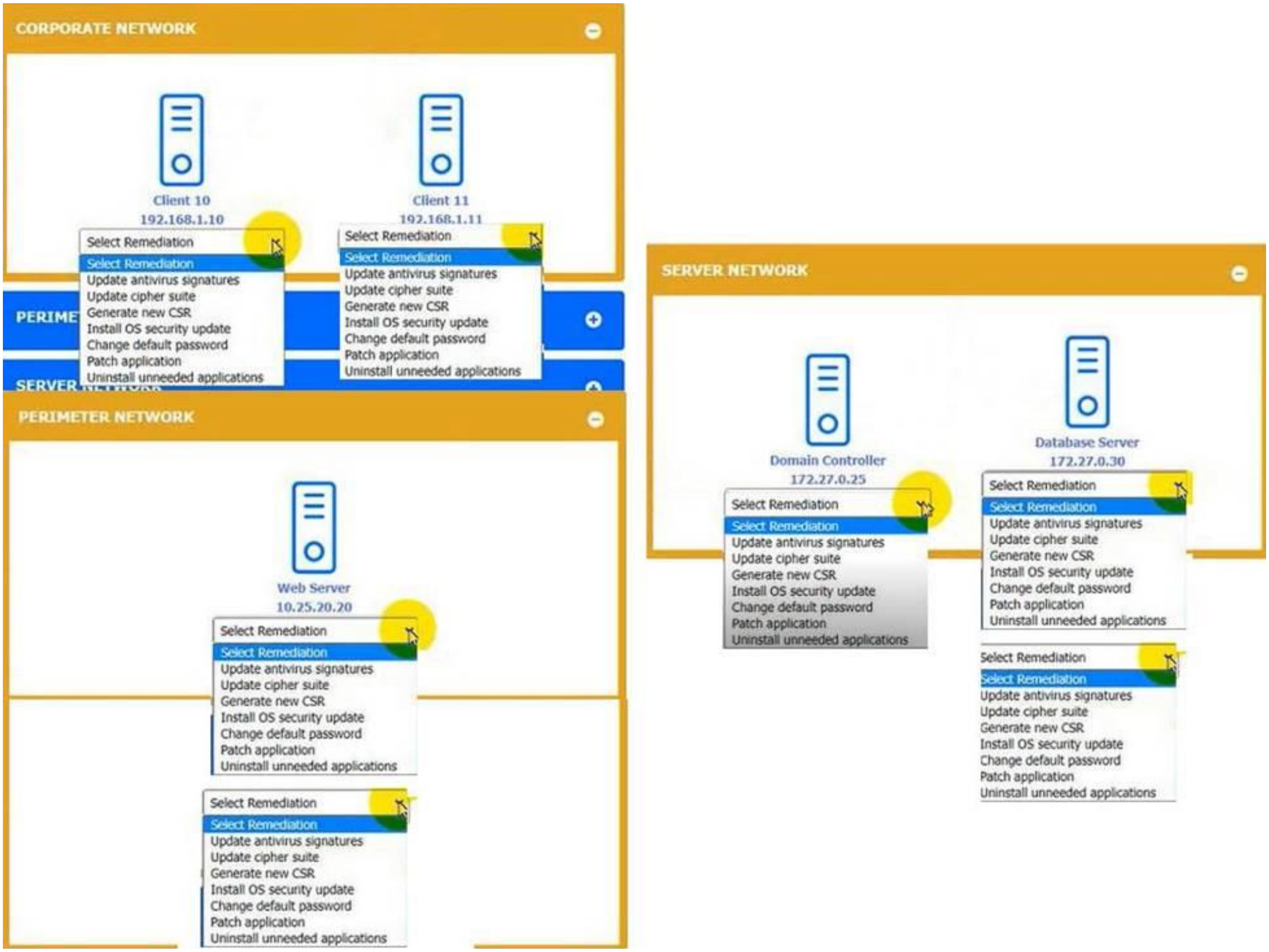
Question #:106 - (Exam Topic 1)

You received the output of a recent vulnerability assessment.

Review the assessment and scan output and determine the appropriate remediation(s) for each device.

Remediation options may be selected multiple times, and some devices may require more than one remediation.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Question #:107 - (Exam Topic 1)

Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Select TWO)

A. Block cipher

B. Hashing

C. Private key

D. Perfect forward secrecy

E. Salting

F. Symmetric keys

Question #:108 - (Exam Topic 1)

A security analyst notices several attacks are being blocked by the NIPS but does not see anything on the boundary firewall logs. The attack seems to have been thwarted. Which of the following resiliency techniques was applied to the network to prevent this attack?

A. NIC Teaming

B. Port mirroring

C. Defense in depth

D. High availability

E. Geographic dispersal

Question #:109 - (Exam Topic 1)

A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned tf servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN. Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).

A. 135

B. 139

C. 143

D. 161

E. 443

F. 445

Question #:110 - (Exam Topic 1)

After a hardware incident, an unplanned emergency maintenance activity was conducted to rectify the issue. Multiple alerts were generated on the SIEM during this period of time. Which of the following BEST explains what happened?

A. The unexpected traffic correlated against multiple rules, generating multiple alerts.

B. Multiple alerts were generated due to an attack occurring at the same time.

C. An error in the correlation rules triggered multiple alerts.

D. The SIEM was unable to correlate the rules, triggering the alerts.

Question #:111 - (Exam Topic 1)

Hackers recently attacked a company's network and obtained several unfavorable pictures from the Chief Executive Officer's workstation. The hackers are threatening to send the images to the press if a ransom is not paid. Which of the following is impacted the MOST?

A. Identify theft

B. Data loss

C. Data exfiltration

D. Reputation

Question #:112 - (Exam Topic 1)

An analyst is working on an email security incident in which the target opened an attachment containing a worm. The analyst wants to implement mitigation techniques to prevent further spread. Which of the following is the BEST course of action for the analyst to take?

A. Apply a DLP solution.

B. Implement network segmentation

C. Utilize email content filtering,

D. isolate the infected attachment.

Question #:113 - (Exam Topic 1)

Which of the following biometric authentication methods is the MOST accurate?

A. Gait

B. Retina

C. Signature

D. Voice

Question #:114 - (Exam Topic 1)

Certain users are reporting their accounts are being used to send unauthorized emails and conduct suspicious activities. After further investigation, a security analyst notices the following:

• All users share workstations throughout the day.

• Endpoint protection was disabled on several workstations throughout the network.

• Travel times on logins from the affected users are impossible.

• Sensitive data is being uploaded to external sites.

• All user account passwords were forced to be reset and the issue continued.

Which of the following attacks is being used to compromise the user accounts?

A. Brute-force

B. Keylogger

C. Dictionary

D. Rainbow

Question #:115 - (Exam Topic 1)

Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested?

A. Whaling

B. Spam

C. Invoice scam

D. Pharming

Question #:116 - (Exam Topic 1)

A security analyst reviews a company’s authentication logs and notices multiple authentication failures. The authentication failures are from different usernames that share the same source IP address. Which of the password attacks is MOST likely happening?

A. Dictionary

B. Rainbow table

C. Spraying

D. Brute-force

Question #:117 - (Exam Topic 1)

An information security manager for an organization is completing a PCI DSS self-assessment for the first time. Which of the following is the MOST likely reason for this type of assessment?

A. An international expansion project is currently underway.

B. Outside consultants utilize this tool to measure security maturity.

C. The organization is expecting to process credit card information.

D. A government regulator has requested this audit to be completed

Question #:118 - (Exam Topic 1)

A network analyst is investigating compromised corporate information. The analyst leads to a theory that network traffic was intercepted before being transmitted to the internet. The following output was captured on an internal host:

```
IPv4 Address ............ 10.0.0.87
Subnet Mask ............. 255.255.255.0
Default Gateway ......... 10.0.0.1
Internet Address        Physical Address
10.10.255.255           ff-ff-ff-ff-ff-ff
10.0.0.1                aa-aa-aa-aa-aa-aa
10.0.0.254              aa-aa-aa-aa-aa-aa
244.0.0.2               01-00-5e-00-00-02
```

Based on the IoCS, which of the following was the MOST likely attack used to compromise the network communication?

A. Denial of service

B. ARP poisoning

C. Command injection

D. MAC flooding

Question #:119 - (Exam Topic 1)

Ann, a customer, received a notification from her mortgage company stating her PII may be shared with partners, affiliates, and associates to maintain day-to-day business operations.

Which of the following documents did Ann receive?

A. An annual privacy notice

B. A non-disclosure agreement

C. A privileged-user agreement

D. A memorandum of understanding

Question #:120 - (Exam Topic 1)

When planning to build a virtual environment, an administrator need to achieve the following;

• Establish policies to limit who can create new VMs.

• Allocate resources according to actual utilization.

• Require justification for requests outside of the standard requirements.

• Create standardized categories based on size and resource requirements.

Which of the following is the administrator MOST likely trying to do?

A. Implement IaaS replication

B. Product against VM escape

C. Deploy a PaaS

D. Avoid VM sprawl

Question #:121 - (Exam Topic 1)

The help desk has received calls from users in multiple locations who are unable to access core network services The network team has identified and turned off the network switches using remote commands. Which of the following actions should the network team take NEXT?

A. Disconnect all external network connections from the firewall

B. Send response teams to the network switch locations to perform updates

C. Turn on all the network switches by using the centralized management software

D. Initiate the organization's incident response plan.

Question #:122 - (Exam Topic 1)

A security analyst is investigating a phishing email that contains a malicious document directed to the company's Chief Executive Officer (CEO). Which of the following should the analyst perform to understand the threat and retrieve possible IoCs?

A. Run a vulnerability scan against the CEOs computer to find possible vulnerabilities

B. Install a sandbox to run the malicious payload in a safe environment

C. Perform a traceroute to identify the communication path

D. Use netstat to check whether communication has been made with a remote host

Question #:123 - (Exam Topic 1)

An organization wants seamless authentication to its applications. Which of the following should the organization employ to meet this requirement?

A. SOAP

B. SAML

C. SSO

D. Kerberos

Question #:124 - (Exam Topic 1)

A cybersecurity administrator needs to implement a Layer 7 security control on a network and block potential attacks. Which of the following can block an attack at Layer 7? (Select TWO).

A. HIDS

B. NIPS

C. HSM

D. WAF

E. NAC

F. NIDS

G. Stateless firewall

Question #:125 - (Exam Topic 1)

The Chief Executive Officer announced a new partnership with a strategic vendor and asked the Chief Information Security Officer to federate user digital identities using SAML-based protocols. Which of the following will this enable?

A. SSO

B. MFA

C. PKI

D. OLP

Question #:126 - (Exam Topic 1)

A junior security analyst is reviewing web server logs and identifies the following pattern in the log file:

```
http://comptia.org/../../../etc/passwd
```

Which ol the following types of attacks is being attempted and how can it be mitigated?

A. XSS, implement a SIEM

B. CSRF, implement an IPS

C. Directory traversal, implement a WAF

D. SQL infection, implement an IDS

Question #:127 - (Exam Topic 1)

A company would like to set up a secure way to transfer data between users via their mobile phones. The company's top priority is utilizing technology that requires users to be in as close proximity as possible to each other. Which of the following connection methods would BEST fulfill this need?

A. Cellular

B. NFC

C. Wi-Fi

D. Bluetooth

Question #:128 - (Exam Topic 1)

Which of the technologies is used to actively monitor for specific file types being transmitted on the network?

A. File integrity monitoring

B. Honeynets

C. Tcpreplay

D. Data loss prevention

Question #:129 - (Exam Topic 1)

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

Question #:130 - (Exam Topic 1)

A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even though the data is still viewable from the user’s PCs. Which of the following is the most likely cause of this issue?

A. TFTP was disabled on the local hosts

B. SSH was turned off instead of modifying the configuration file

C. Remote login was disabled in the networkd.config instead of using the sshd.conf

D. Network services are no longer running on the NAS

Question #:131 - (Exam Topic 1)

A security analyst was deploying a new website and found a connection attempting to authenticate on the site's portal. While Investigating The incident, the analyst identified the following Input in the username field:

```
admin’ or 1=1--
```

Which of the following BEST explains this type of attack?

A. DLL injection to hijack administrator services

B. SQLi on the field to bypass authentication

C. Execution of a stored XSS on the website

D. Code to execute a race condition on the server

Question #:132 - (Exam Topic 1)

Which of the following uses six initial steps that provide basic control over system security by including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments?

A. ISO 27701

B. The Center for Internet Security

C. SSAE SOC 2

D. NIST Risk Management Framework

Question #:133 - (Exam Topic 1)

A security analyst has been tasked with creating a new WiFi network for the company. The requirements received by the analyst are as follows:

•Must be able to differentiate between users connected to WiFi
•The encryption keys need to change routinely without interrupting the users or forcing reauthentication
•Must be able to integrate with RADIUS
•Must not have any open SSIDs

Which of the following options BEST accommodates these requirements?

A. WPA2-Enterprise

B. WPA3-PSK

C. 802.11n

D. WPS

Question #:134 - (Exam Topic 1)

A systems administrator is considering different backup solutions for the IT infrastructure. The company is looking for a solution that offers the fastest recovery time while also saving the most amount of storage used to maintain the backups. Which of the following recovery solutions would be the BEST option to meet these requirements?

A. Snapshot

B. Differential

C. Full

D. Tape

Question #:135 - (Exam Topic 1)

A security researcher is tracking an adversary by noting its attacks and techniques based on its capabilities, infrastructure, and victims. Which of the following is the researcher MOST likely using?

A. The Diamond Model of Intrusion Analysis

B. The Cyber Kill Chain

C. The MITRE CVE database

D. The incident response process

Question #:136 - (Exam Topic 1)

As part of the lessons-learned phase, the SOC is tasked with building methods to detect if a previous incident is happening again. Which of the following would allow the security analyst to alert the SOC if an event is reoccurring?

A. Creating a playbook within the SOAR

B. Implementing rules in the NGFW

C. Updating the DLP hash database

D. Publishing a new CRL with revoked certificates

Question #:137 - (Exam Topic 1)

The Chief Information Security Officer has directed the security and networking team to retire the use of shared passwords on routers and switches. Which of the following choices BEST meets the requirements?

A. SAML

B. TACACS+

C. Password vaults

D. OAuth

Question #:138 - (Exam Topic 1)

Which of the following would produce the closest experience of responding to an actual incident response scenario?

A. Lessons learned

B. Simulation

C. Walk-through

D. Tabletop

Question #:139 - (Exam Topic 1)

Which of the following roles would MOST likely have direct access to the senior management team?

A. Data custodian

B. Data owner

C. Data protection officer

D. Data controller

Question #:140 - (Exam Topic 1)

A company is implementing a new SIEM to log and send alerts whenever malicious activity is blocked by its antivirus and web content filters. Which of the following is the primary use case for this scenario?

A. Implementation of preventive controls

B. Implementation of detective controls

C. Implementation of deterrent controls

D. Implementation of corrective controls

Question #:141 - (Exam Topic 1)

A developer is building a new portal to deliver single-pane-of-glass management capabilities to customers with multiple firewalls. To Improve the user experience, the developer wants to implement an authentication and authorization standard that uses security tokens that contain assertions to pass user Information between nodes. Which of the following roles should the developer configure to meet these requirements? (Select TWO).

A. Identity processor

B. Service requestor

C. Identity provider

D. Service provider

E. Tokenized resource

F. Notarized referral

Question #:142 - (Exam Topic 1)

Which of the following BEST describes a technique that compensates researchers for finding vulnerabilities?

A. Penetration testing

B. Code review

C. Wardriving

D. Bug bounty

Question #:143 - (Exam Topic 1)

Which of the following controls would be the MOST cost-effective and time-efficient to deter intrusions at the perimeter of a restricted, remote military training area? (Select TWO).

A. Barricades

B. Thermal sensors

C. Drones

D. Signage

E. Motion sensors

F. Guards

G. Bollards

Question #:144 - (Exam Topic 1)

An enterprise has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that is discovered. Which of the following BEST represents the type of testing that is being used?

A. White-box

B. Red-leam

C. Bug bounty

D. Gray-box

E. Black-box

Question #:145 - (Exam Topic 1)

A security analyst wants to verify that a client-server (non-web) application is sending encrypted traffic.

Which of the following should the analyst use?

A. openssl

B. hping

C. netcat

D. tcpdump

Question #:146 - (Exam Topic 1)

An attacker replaces a digitally signed document with another version that goes unnoticed Upon reviewing the document's contents the author notices some additional verbiage that was not originally in the document but cannot validate an integrity issue. Which of the following attacks was used?

A. Cryptomalware

B. Hash substitution

C. Collision

D. Phishing

Question #:147 - (Exam Topic 1)

A new plug-and-play storage device was installed on a PC in the corporate environment. Which of the following safeguards will BEST help to protect the PC from malicious files on the storage device?

A. Change the default settings on the PC.

B. Define the PC firewall rules to limit access.

C. Encrypt the disk on the storage device.

D. Plug the storage device in to the UPS

Question #:148 - (Exam Topic 1)

An analyst is generating a security report for the management team. Security guidelines recommend disabling all listening unencrypted services. Given this output from Nmap:

```
PORT        STATE
21/tcp      filtered
22/tcp      open
23/tcp      open
443/tcp     open
```

Which of the following should the analyst recommend to disable?

A. 21/tcp

B. 22/tcp

C. 23/tcp

D. 443/tcp

Question #:149 - (Exam Topic 1)

Which of the following conditions impacts data sovereignty?

A. Rights management

B. Criminal investigations

C. Healthcare data

D. International operations

Question #:150 - (Exam Topic 1)

A security administrator is setting up a SIEM to help monitor for notable events across the enterprise. Which of the following control types does this BEST represent?

A. Preventive

B. Compensating

C. Corrective

D. Detective

Question #:151 - (Exam Topic 1)

Which of the following is a cryptographic concept that operates on a fixed length of bits?

A. Block cipher

B. Hashing

C. Key stretching

D. Salting

Question #:152 - (Exam Topic 1)

During an incident, a company’S CIRT determines it is necessary to observe the continued network-based transactions between a callback domain and the malware running on an enterprise PC. Which of the following techniques would be BEST to enable this activity while reducing the risk of lateral spread and the risk that the adversary would notice any changes?

A. Physically move the PC to a separate internet point of presence

B. Create and apply micro segmentation rules.

C. Emulate the malware in a heavily monitored DMZ segment.

D. Apply network blacklisting rules for the adversary domain

Question #:153 - (Exam Topic 1)

Which of the following BEST describes data streams that are compiled through artificial intelligence that provides insight on current cyberintrusions, phishing, and other malicious cyberactivity?

A. Intelligence fusion

B. Review reports

C. Log reviews

D. Threat feeds

Question #:154 - (Exam Topic 1)

If a current private key is compromised, which of the following would ensure it cannot be used to decrypt ail historical data?

A. Perfect forward secrecy

B. Elliptic-curve cryptography

C. Key stretching

D. Homomorphic encryption

Question #:155 - (Exam Topic 1)

After a WiFi scan of a local office was conducted, an unknown wireless signal was identified Upon investigation, an unknown Raspberry Pi device was found connected to an Ethernet port using a single connection. Which of the following BEST describes the purpose of this device?

A. loT sensor

B. Evil twin

C. Rogue access point

D. On-path attack

Question #:156 - (Exam Topic 1)

A security analyst is responding to an alert from the SIEM. The alert states that malware was discovered on a host and was not automatically deleted. Which of the following would be BEST for the analyst to perform?

A. Add a deny-all rule to that host in the network ACL

B. Implement a network-wide scan for other instances of the malware.

C. Quarantine the host from other parts of the network

D. Revoke the client's network access certificates

Question #:157 - (Exam Topic 1)

A cybersecurity administrator needs to allow mobile BYOD devices to access network resources. As the devices are not enrolled to the domain and do not have policies applied to them, which of the following are best practices for authentication and infrastructure security? (Select TWO).

A. Create a new network for the mobile devices and block the communication to the internal network and servers

B. Use a captive portal for user authentication.

C. Authenticate users using OAuth for more resiliency

D. Implement SSO and allow communication to the internal network

E. Use the existing network and allow communication to the internal network and servers.

F. Use a new and updated RADIUS server to maintain the best solution

Question #:158 - (Exam Topic 1)

Which of the following environments typically hosts the current version configurations and code, compares user-story responses and workflow, and uses a modified version of actual data for testing?

A. Development

B. Staging

C. Production

D. Test

Question #:159 - (Exam Topic 1)

An organization's Chief Information Security Officer is creating a position that will be responsible for implementing technical controls to protect data, including ensuring backups are properly maintained. Which of the following roles would MOST likely include these responsibilities?

A. Data protection officer

B. Data owner

C. Backup administrator

D. Data custodian

E. Internal auditor

Question #:160 - (Exam Topic 1)

A business is looking for a cloud service provider that offers a la carte services, including cloud backups, VM elasticity, and secure networking. Which of the following cloud service provider types should business engage?

A. A laaS

B. PaaS

C. XaaS

D. SaaS

Question #:161 - (Exam Topic 1)

A security researcher is using an adversary's infrastructure and TTPs and creating a named group to track those targeted. Which of the following is the researcher MOST likely using?

A. The Cyber Kill Chain

B. The incident response process

C. The Diamond Model of Intrusion Analysis

D. MITRE ATT&CK

Question #:162 - (Exam Topic 1)

Which of the following would MOST likely be identified by a credentialed scan but would be missed by an uncredentialed scan?

A. Vulnerabilities with a CVSS score greater than 6.9.

B. Critical infrastructure vulnerabilities on non-IP protocols.

C. CVEs related to non-Microsoft systems such as printers and switches.

D. Missing patches for third-party software on Windows workstations and servers.

Question #:163 - (Exam Topic 1)

Which of the following is a physical security control that ensures only the authorized user is present when gaining access to a secured area?

A. A biometric scanner

B. A smart card reader

C. API Token

D. A PIN pad

Question #:164 - (Exam Topic 1)

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

Question #:165 - (Exam Topic 1)

A security administrator is working on a solution to protect passwords stored in a database against rainbow table attacks Which of the following should the administrator consider?

A. Hashing

B. Salting

C. Lightweight cryptography

D. Steganography

Question #:166 - (Exam Topic 1)

After gaining access to a dual-homed (i.e. wired and wireless) multifunction device by exploiting a vulnerability in the device's firmware, a penetration tester then gains shell access to another networked asset. This technique is an example of:

A. privilege escalation

B. footprinting

C. persistence

D. pivoting

Question #:167 - (Exam Topic 1)

An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box. Which of the following should be the first lines of defense against such an attack? (Select TWO)

A. MAC filtering

B. Zero trust segmentation

C. Network access control

D. Access control vestibules

E. Guards

F. Bollards

Question #:168 - (Exam Topic 1)

A security analyst is reviewing the vulnerability scan report for a web server following an incident. The vulnerability that was used to exploit the server is present in historical vulnerability scan reports, and a patch is available for the vulnerability. Which of the following is the MOST likely cause?

A. Security patches were uninstalled due to user impact.

B. An adversary altered the vulnerability scan reports.

C. A zero-day vulnerability was used to exploit the web server.

D. The scan reported a false negative for the vulnerability.

Question #:169 - (Exam Topic 1)

A security engineer is reviewing the logs from a SAML application that is configured to use MFA, during this review the engineer notices a high volume of successful logins that did not require MFA from users who were traveling internationally. The application, which can be accessed without a VPN, has a policy that allows time-based tokens to be generated. Users who changed locations should be required to reauthenticate. Which of the following statements BEST explains the issue?

A. OpenID is mandatory to make the MFA requirements work

B. An incorrect browser has been detected by the SAML application

C. The access device has a trusted certificate installed that is overwriting the session token

D. The user's IP address is changing between logins, but the application is not invalidating the token

Question #:170 - (Exam Topic 1)

A company's public-facing website, https://www.organization.com, has an IP address of 166.18.75.6. However, over the past hour, the SOC has received reports of the site's homepage displaying incorrect information. A quick nslookup search shows https://www.organization.com is pointing to 151.191.122.115. Which of the following is occurring?

A. DoS attack

B. ARP poisoning

C. DNS spoofing

D. NXDOMAIN attack

Question #:171 - (Exam Topic 1)

A security analyst reports a company policy violation in a case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investigation, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized downloads are occurring. The analyst also discovers a couple of WAPs are using the same SSID, but they have non-standard DHCP configurations and an overlapping channel.

Which of the following attacks is being conducted?

A. Evil twin

B. Jamming

C. DNS poisoning

D. Bluesnarfing

E. DDoS

Question #:172 - (Exam Topic 1)

A security administrator has discovered that workstations on the LAN are becoming infected with malware. The cause of the infections appears to be users receiving phishing emails that are bypassing the current email-filtering technology. As a result, users are being tricked into clicking on malicious URLs, as no internal controls currently exist in the environment to evaluate their safety. Which of the following would be BEST to implement to address the issue?

A. Forward proxy

B. HIDS

C. Awareness training

D. A jump server

E. IPS

Question #:173 - (Exam Topic 1)

The following are the logs of a successful attack.

```
[DATA] attacking service ftp on port 21-
[ATTEMPT] 09:00:01UTC target 192.168.50.1 login "admin" -pass "p@55w0rd"
[ATTEMPT] 09:00:01 UTC target 192.168.50.1 login "admin" -pass "AcCe55"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 login "admin" -pass "A110w!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 login "admin" -pass "PL34s3#"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 login "admin" -pass "FTPL0gin!"
[ATTEMPT] 09:00:01 UTC target 192.168.50.1 login "admin" -pass "L3tM31N!"
[21] [ftp] host: 192.168.50.1 login: admin password: L3tM31N!
1 of 1 target successfully completed, 1 valid password found in <1 second
```

Which of the following controls would be BEST to use to prevent such a breach in the future?

A. Password history

B. Account expiration

C. Password complexity

D. Account lockout

Question #:174 - (Exam Topic 1)

The spread of misinformation surrounding the outbreak of a novel virus on election day led to eligible voters choosing not to take the risk of going to the polls. This is an example of:

A. prepending.

B. an influence campaign.

C. a watering-hole attack.

D. intimidation.

E. information elicitation.

Question #:175 - (Exam Topic 1)

An enterprise needs to keep cryptographic keys in a safe manner. Which of the following network appliances can achieve this goal?

A. HSM

B. CASB

C. TPM

D. DLP

Question #:176 - (Exam Topic 1)

Which of the following BEST describes the method a security analyst would use to confirm a file that is downloaded from a trusted security website is not altered in transit or corrupted using a verified checksum?

A. Hashing

B. Salting

C. Integrity

D. Digital signature

Question #:177 - (Exam Topic 1)

A Chief Information Security Officer (CISO) is evaluating the dangers involved in deploying a new ERP system for the company. The CISO categorizes the system, selects the controls that apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system. Which of the following is the CISO using to evaluate the environment for this new ERP system?

A. The Diamond Model of Intrusion Analysis

B. CIS Critical Security Controls

C. NIST Risk Management Framework

D. ISO 27002

Question #:178 - (Exam Topic 1)

A security team suspects that the cause of recent power consumption overloads is the unauthorized use of empty power outlets in the network rack. Which of the following options will mitigate this issue without compromising the number of outlets available?

A. Adding a new UPS dedicated to the rack

B. Installing a managed PDU

C. Using only a dual power supplies unit

D. Increasing power generator capacity

Question #:179 - (Exam Topic 1)

A company uses a drone for precise perimeter and boundary monitoring. Which of the following should be MOST concerning to the company?

A. Privacy

B. Cloud storage of telemetry data

C. GPS spoofing

D. Weather events

Question #:180 - (Exam Topic 1)

A security analyst is investigating multiple hosts that are communicating to external IP addresses during the hours of 2:00 a.m – 4:00 am. The malware has evaded detection by traditional antivirus software. Which of the following types of malware is MOST likely infecting the hosts?

A. A RAT

B. Ransomware

C. Polymorphic

D. A worm