Question #1 *Topic 1*

SIMULATION -

A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.

INSTRUCTIONS -

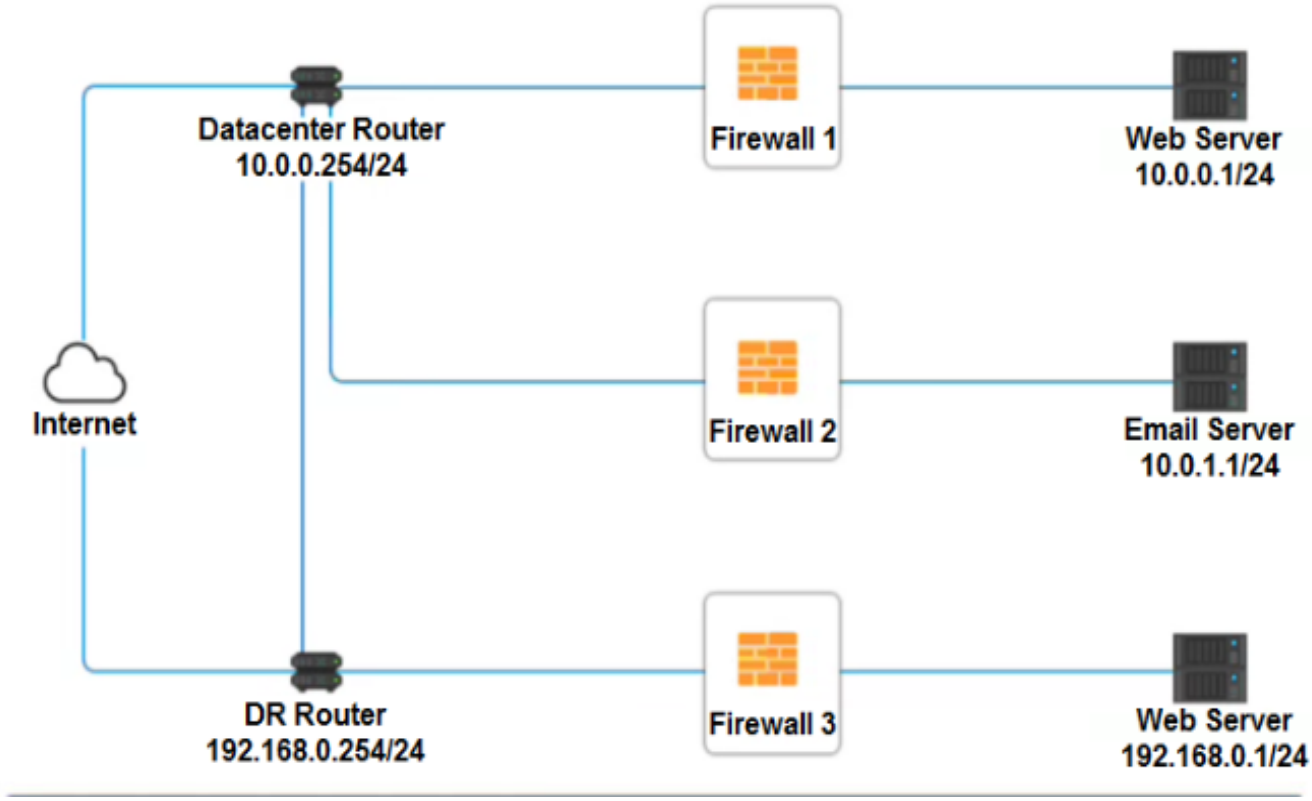
Click on each firewall to do the following:

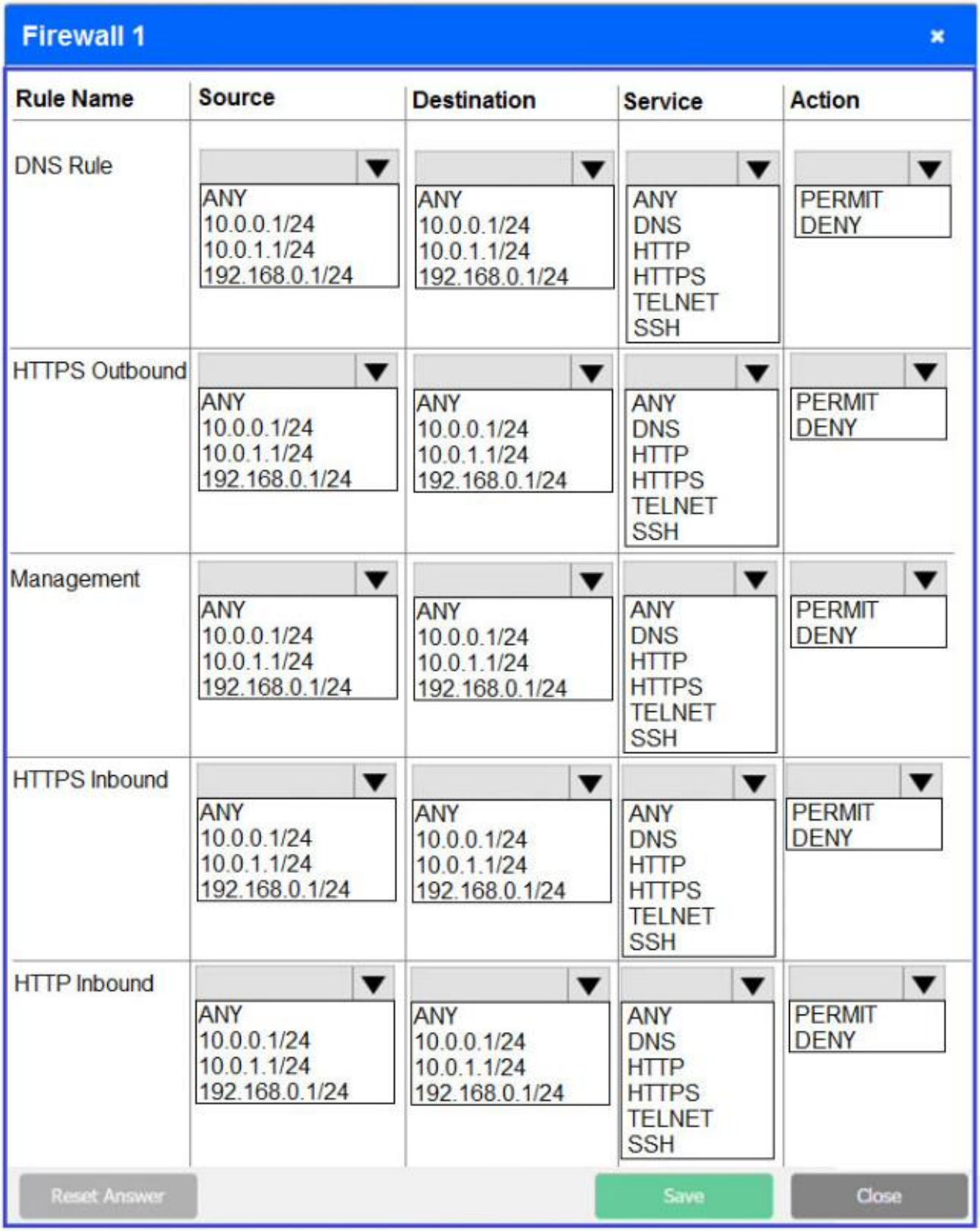
1. Deny cleartext web traffic.
2. Ensure secure management protocols are used.
3. Resolve issues at the DR site.

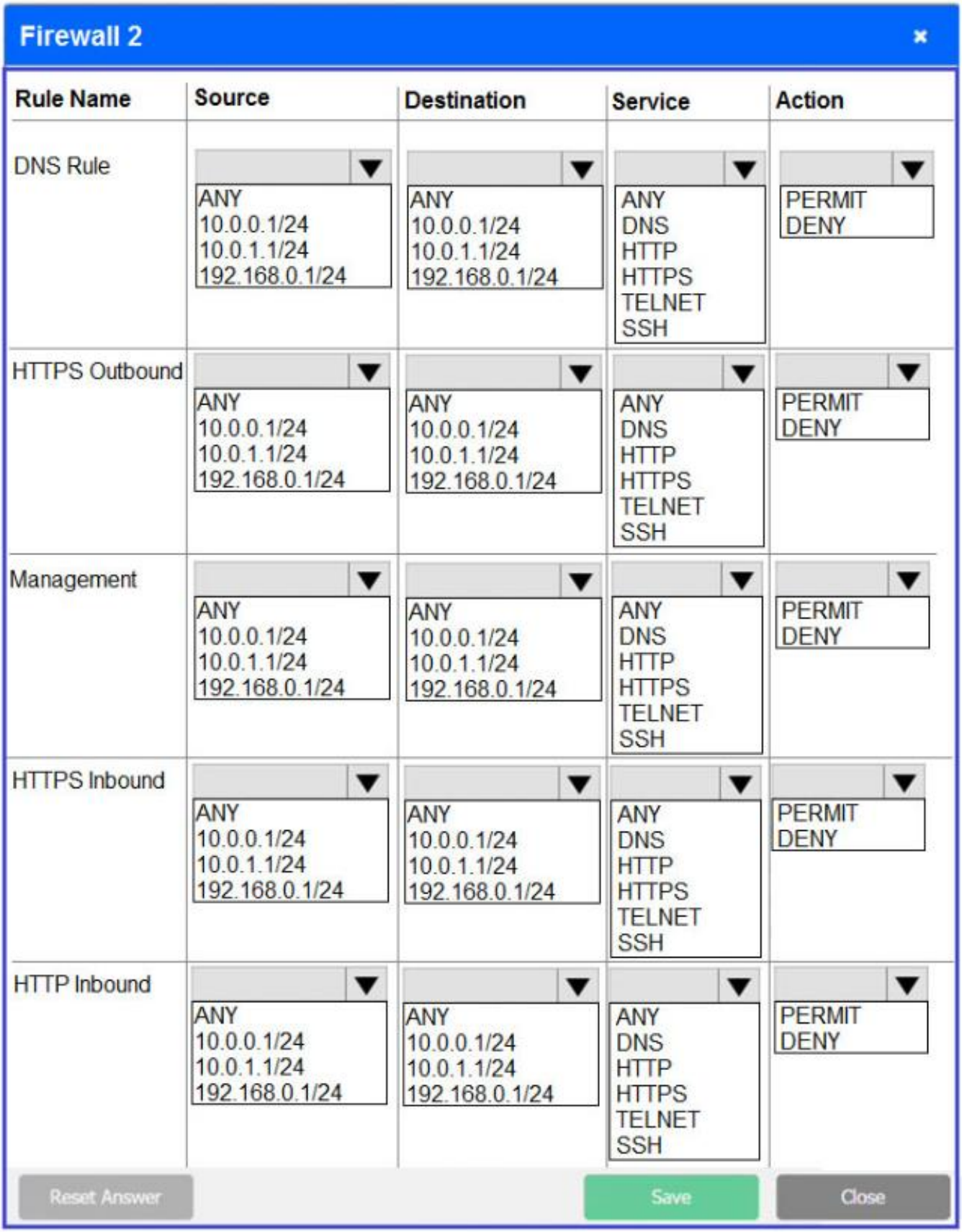
The ruleset order cannot be modified due to outside constraints.

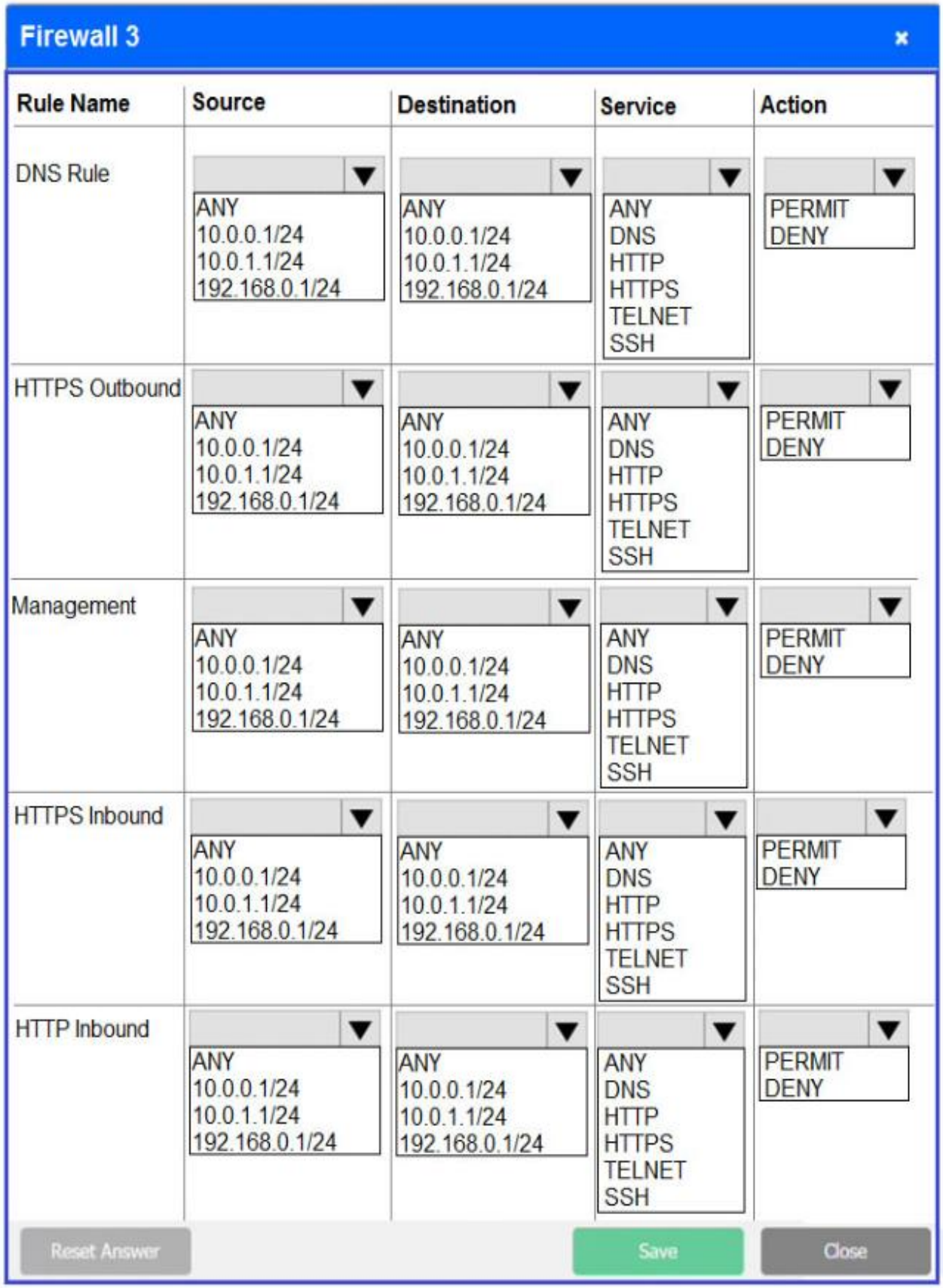
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Network Diagram









Firewall 1:

DNS Rule – ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound – 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT

Management – ANY --> ANY --> SSH --> PERMIT

HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT

HTTP Inbound – ANY --> ANY --> HTTP --> DENY

Firewall 2: No changes should be made to this firewall

Firewall 3:

DNS Rule – ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound – 192.168.0.1/24 --> ANY --> HTTPS --> PERMIT

Management – ANY --> ANY --> SSH --> PERMIT

HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT

HTTP Inbound – ANY --> ANY --> HTTP --> DENY

Question #2 *Topic 1*

DRAG DROP -

A security engineer is setting up passwordless authentication for the first time.

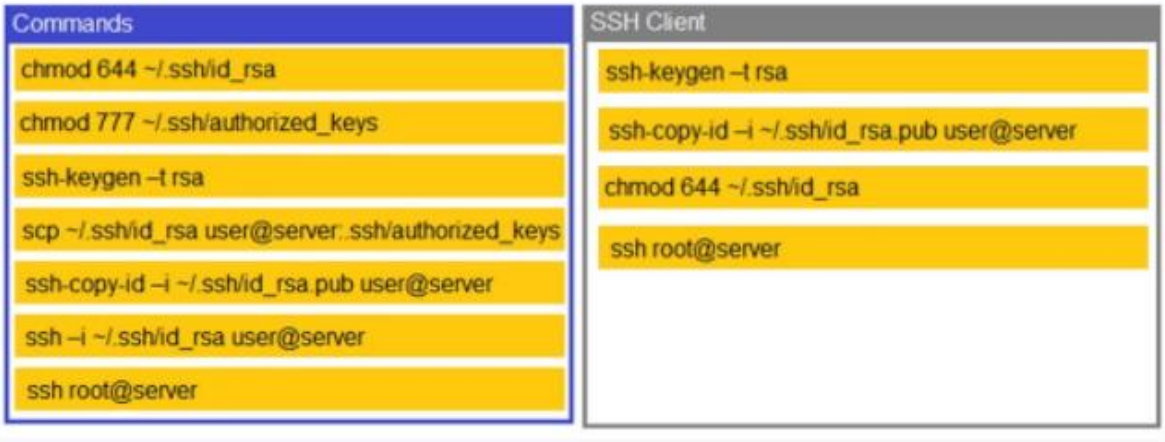
INSTRUCTIONS -

Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.

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

Select and Place:

Correct Answer:



Question #3 *Topic 1*

HOTSPOT -

Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

INSTRUCTIONS -

Not all attacks and remediation actions will be used.

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

Hot Area:

Correct Answer:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Implement a host-based IPS
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm	Change the default application password
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Disable vulnerable services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Implement 2FA using push notification

Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing

Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services

Question #4 *Topic 1*

Which of the following will MOST likely adversely impact the operations of unpatched traditional programmable-logic controllers, running a back-end LAMP server and OT 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

Question #5 *Topic 1*

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 companyâ€™s data?

A. Containerization Most Voted

B. Geofencing

C. Full-disk encryption

D. Remote wipe

Question #6 *Topic 1*

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.

Question #7 *Topic 1*

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

Question #8 *Topic 1*

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 employeeâ€™s hard disk. Which of the following should the administrator use?

- A. dd **Most Voted**
- B. chmod
- C. dnsenum
- D. logger

Question #9 *Topic 1*

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

Question #10 *Topic 1*

Phishing and spear-phishing attacks have been occurring more frequently against a companyâ€™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

Question #11 *Topic 1*

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

Question #12 *Topic 1*

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

Question #13 *Topic 1*

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

Question #14 *Topic 1*

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

Question #15 *Topic 1*

A network engineer needs to build a solution that will allow guests at the companyâ€™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

Question #16 — Topic 1

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 analystâ€™s findings, which of the following attacks is being executed?

A. Credential harvesting

B. Keylogger

C. Brute-force

D. Spraying

Question #17 — Topic 1

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

A. SaaS

B. PaaS

C. IaaS

D. DaaS

Question #18 *Topic 1*

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 **Most Voted**

B. Off-site backups

C. Automatic OS upgrades

D. NIC teaming **Most Voted**

E. Scheduled penetration testing

F. Network-attached storage

Question #19 *Topic 1*

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 requested strict checking.
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

Question #20 *Topic 1*

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. Fingerprint

Question #21 *Topic 1*

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 **Most Voted**

D. An OpenID Connect authentication system

Question #22 — Topic 1

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 employeeâ€™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

Question #23 — Topic 1

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

Question #24 — Topic 1

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 organizationâ€™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

Question #25 *Topic 1*

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 applianceâ€™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.

Question #26 *Topic 1*

A companyâ€™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 companyâ€™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 **Most Voted**

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

Question #27 *Topic 1*

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

Question #28 *Topic 1*

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

Question #29 *Topic 1*

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.

Question #30 *Topic 1*

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

Question #31 *Topic 1*

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

Question #32 *Topic 1*

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

Question #33 *Topic 1*

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.

Question #34 *Topic 1*

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

Question #35 *Topic 1*

An organizationâ€™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 **Most Voted**

B. Domain hijacking

C. Distributed denial-of-service

D. DNS tunneling

Question #36 *Topic 1*

A cybersecurity manager has scheduled biannual meetings with the IT team and department leaders to discuss how they would respond to hypothetical cyberattacks. During these meetings, the 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

Question #37 *Topic 1*

A RAT that was used to compromise an organizationג€™s banking credentials was found on a userג€™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.

Question #38 *Topic 1*

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
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
Which of the following application attacks is being tested?

A. Pass-the-hash

B. Session replay

C. Object deference

D. Cross-site request forgery **Most Voted**

Question #39 *Topic 1*

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

Question #40 *Topic 1*

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

Question #41 *Topic 1*

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

Question #42 *Topic 1*

A root cause analysis reveals that a web application outage was caused by one of the companyâ€™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

Question #43 *Topic 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

Question #44 *Topic 1*

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

Question #45 *Topic 1*

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:

```
CPU 0 percent busy, from 300 sec ago
1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
```

Which of the following is the router experiencing?

A. DDoS attack

B. Memory leak

C. Buffer overflow

D. Resource exhaustion

Question #46 *Topic 1*

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.

Question #47 *Topic 1*

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

Question #48 *Topic 1*

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 'o'='o' And Password/text='bar']
[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.

Question #49 *Topic 1*

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.

Question #50 *Topic 1*

The IT departmentâ€™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.

Question #51 *Topic 1*

A cybersecurity analyst needs to implement secure authentication to third-party websites without usersа€™ passwords. Which of the following would be the BEST way to achieve this objective?

A. OAuth

B. SSO

C. SAML

D. PAP

Question #52 *Topic 1*

An analyst needs to identify the applications a user was running and the files that were open before the userа€™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

Question #53 *Topic 1*

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 userа€™s inability to connect the laptop to the VPN?

A. Due to foreign travel, the userа€™s laptop was isolated from the network.

B. The userа€™s laptop was quarantined because it missed the latest path update.

C. The VPN client was blacklisted.

D. The userа€™s account was put on a legal hold.

Question #54 *Topic 1*

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

A. Obfuscation

B. Integrity

C. Non-repudiation

D. Blockchain

Question #55 *Topic 1*

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

A. A password reuse policy **Most Voted**

B. Account lockout after three failed attempts

C. Encrypted credentials in transit

D. A geofencing policy based on login history

Question #56 *Topic 1*

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

A. Transference

B. Avoidance

C. Acceptance

D. Mitigation

Question #57 *Topic 1*

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

Question #58 *Topic 1*

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

Question #59 *Topic 1*

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

Question #60 *Topic 1*

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

Question #61 *Topic 1*

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

Question #62 *Topic 1*

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.

Question #63 *Topic 1*

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 fireless virus is spreading in the local network environment.

Question #64 *Topic 1*

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

Question #65 *Topic 1*

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

Question #66 *Topic 1*

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

Question #67 *Topic 1*

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

Question #68 *Topic 1*

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

Question #69 *Topic 1*

The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the companyа€™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

Question #70 *Topic 1*

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 organizationа€™s needs for a third factor?

A. Date of birth

B. Fingerprints

C. PIN

D. TPM

Question #71 *Topic 1*

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

Question #72 *Topic 1*

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

Question #73 *Topic 1*

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

A. Deploy an MDM solution. **Most Voted**

B. Implement managed FDE.

C. Replace all hard drives with SEDs.

D. Install DLP agents on each laptop.

Question #74 *Topic 1*

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 **Most Voted**

C. DNS poisoning

D. ARP poisoning

Question #75 *Topic 1*

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

Question #76 *Topic 1*

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.

Question #77 *Topic 1*

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 Joeא€™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 #78 *Topic 1*

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

Question #79 *Topic 1*

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

Question #80 *Topic 1*

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

Question #81 *Topic 1*

Which of the following policies would help an organization identify and mitigate potential single points of failure in the companyâ€™s IT/security operations?

A. Least privilege

B. Awareness training

C. Separation of duties

D. Mandatory vacation

Question #82 *Topic 1*

Which of the following would be the BEST method for creating a detailed diagram of wireless access points and hotspots?

A. Footprinting

B. White-box testing

C. A drone/UAV

D. Pivoting

Question #83 *Topic 1*

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? (Choose two.)

A. Something you know

B. Something you have

C. Somewhere you are

D. Someone you know

E. Something you are

F. Something you can do

Question #84 *Topic 1*

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

A. Transference

B. Avoidance

C. Acceptance

D. Mitigation

Question #85 *Topic 1*

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

Question #86 *Topic 1*

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

Question #87 — Topic 1

An analyst visits an Internet forum looking for information about a tool. The analyst finds a thread 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://website.com/user.js>
Onload=sqlexec();
</script>

Thank you,

Joe
```

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

A. SQLi attack

B. DLL attack

C. XSS attack

D. API attack

Question #88 — Topic 1

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

Question #89 *Topic 1*

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?
(Choose two.)

A. COPE

B. VDI

C. GPS

D. TOTP

E. RFID

F. BYOD

Question #90 *Topic 1*

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

A. SSO would simplify username and password management, making it easier for hackers to 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 systems if the identity provider goes offline.

Question #91 *Topic 1*

A smart switch has the ability to monitor electrical levels and shut off power to a building in the event of power surge 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 patching 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.

Question #92 *Topic 1*

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

Question #93 *Topic 1*

A security assessment determines DES and 3DES are 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

Question #94 *Topic 1*

Which of the following types of controls is a turnstile?

A. Physical

B. Detective

C. Corrective

D. Technical

Question #95 *Topic 1*

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.

Question #96 *Topic 1*

A security analyst is investigating 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 address
10.0.0.1	00-18-21-ad-24-bc
10.0.0.114	01-31-a3-cd-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

Question #97 *Topic 1*

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

A. Multifactor authentication

B. Something you can do

C. Biometrics

D. Two-factor authentication

Question #98 *Topic 1*

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

Question #99 *Topic 1*

Joe, a user at a company, clicked an email links that 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 a security 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.

Question #100 *Topic 1*

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 λ€"S comptia.org λ€"p 80

B. nc λ€"l λ€"v comptia.org λ€"p 80

C. nmap comptia.org λ€"p 80 λ€"sV

D. nslookup λ€"port=80 comptia.org

Question #101 *Topic 1*

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 executiveλ€™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

Question #102 *Topic 1*

A security analyst is performing a forensic investigation involving compromised account credentials. Using the Event Viewer, the analyst was able to detect the following message: λ€Special privileges assigned to new logon.λ€ 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

Question #103 *Topic 1*

A systems administrator needs to implement an access control scheme that will allow an objectλ€™s access policy to 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

Question #104 *Topic 1*

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

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

B. http://sample.url.com/someotherpageonsite/../../../etc/shadow

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

D. http://redirect.sameple.url.sampleurl.com/malicious-dns-redirect

Question #105 *Topic 1*

A company has limited storage space available and an online presence that cannot be down for more than four hours. Which of the following backup methodologies should the company implement to allow for the FASTEST database restore time in the event of a failure, while being mindful of the limited available storage space?

A. Implement full tape backups every Sunday at 8:00 p.m. and perform nightly tape rotations.

B. Implement differential backups every Sunday at 8:00 p.m. 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.

Question #106 *Topic 1*

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 organizationλ€™s security and customer privacy. Which of the following would be BEST to address the CIOλ€™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. **Most Voted**

D. Deploy mobile devices using the COPE methodology.

Question #107 *Topic 1*

A malicious actor recently penetrated a companyâ€™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

Question #108 *Topic 1*

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 companyâ€™s reputation.

C. social engineering.

D. credential exposure.

Question #109 *Topic 1*

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.

Question #110 *Topic 1*

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.

Question #111 *Topic 1*

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

A. RAID 0

B. RAID 1

C. RAID 5

D. RAID 10

Question #112 *Topic 1*

A companyа€™s Chief Information Officer (CIO) is meeting with the Chief Information Security Officer (CISO) to plan some activities to enhance the skill levels of the companyа€™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

Question #113 *Topic 1*

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.

Question #114 *Topic 1*

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

Question #115 *Topic 1*

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 all systems and applications.

C. Rebuild all workstations and install new antivirus software.

D. Implement application whitelisting and perform user application hardening.

Question #116 *Topic 1*

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 organizationâ€™s executives determine their next course of action?

A. An incident response plan

B. A communications plan

C. A disaster recovery plan

D. A business continuity plan

Question #117 *Topic 1*

Which of the following describes the ability of code to target a hypervisor from inside a guest OS?

A. Fog computing

B. VM escape

C. Software-defined networking

D. Image forgery

E. Container breakout

Question #118 *Topic 1*

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 Most Voted

B. The NetFlow data

C. A checksum

D. The event log

Question #119 *Topic 1*

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

```
GET http://www.companysite.com/product_info.php?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

Question #120 *Topic 1*

Which of the following ISO standards is certified for privacy?

A. ISO 9001

B. ISO 27002

C. ISO 27701

D. ISO 31000

Question #121 *Topic 1*

A document that appears to be malicious has been discovered in an email that was sent to a companyא€™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 documentא€™s metadata for origin clues.

C. Search for matching file hashes on malware websites.

D. Detonate the document in an analysis sandbox.

Question #122 — Topic 1

A security analyst is running a vulnerability scan to check for missing patches during a suspected security incident. 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 #123 — Topic 1

Which of the following is a team of people dedicated to 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

Question #124 — Topic 1

A security analyst discovers that a companyâ€™s username and password database was posted on an Internet forum. The usernames 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. Most Voted

C. Configure the web content filter to block access to the forum.

D. Increase password complexity requirements.

Question #125 *Topic 1*

Which of the following are requirements that must be configured for PCI DSS compliance? (Choose two.)

A. Testing security systems and processes regularly **Most Voted**

B. Installing and maintaining a web proxy to protect cardholder data

C. Assigning a unique ID to each person with computer access **Most Voted**

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

Question #126 *Topic 1*

A security analyst needs to be proactive in understanding the types of attacks that could potentially target the companyâ€™s executives. Which of the following intelligence sources should the 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

Question #127 *Topic 1*

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 sinkholing

B. DLP rules on the terminal

C. An IP blacklist

D. Application whitelisting

Question #128 *Topic 1*

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 identifies the following:

- The legitimate websiteâ€™s IP address is 10.1.1.20 and eRecruit.local resolves to this IP.
- The forged websiteâ€™s IP address appears to be 10.2.12.99, based on NetFlow records.
- All three of the organizationâ€™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 poisoned a name server.

D. An ARP poisoning attack was successfully executed.

Question #129 *Topic 1*

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 transfers 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

Question #130 *Topic 1*

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. A BPDU guard

B. WPA-EAP

C. IP filtering

D. A WIDS

Question #131 *Topic 1*

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 organizationâ€™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.

Question #132 *Topic 1*

A security engineer is reviewing log files after a third party discovered usernames and passwords for the organizationâ€™s accounts. The engineer sees there was a change in the IP address for a vendor website one week 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

Question #133 — Topic 1

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. Order of volatility

D. A log analysis

E. A right-to-audit clause

Question #134 — Topic 1

A large industrial systemλ€™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 companyλ€™s security manager notices the generatorλ€™s IP is sending packets to an internal file serverλ€™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

Question #135 — Topic 1

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

A. Data encryption

B. Data masking

C. Data deduplication

D. Data minimization

Question #136 *Topic 1*

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 throughout the global network. Which of the following would be BEST to help mitigate this concern?

A. Create different 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.

Question #137 *Topic 1*

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 **Most Voted**

C. Normalization

D. Staging

Question #138 *Topic 1*

A security analyst is configuring a large number of new company-issued laptops. The analyst received the following requirements:

- The devices will be used internationally by staff who travel extensively.
- Occasional personal use is acceptable due to the travel requirements.
- Users must be able to install and configure sanctioned programs and productivity suites.
- The devices must be encrypted.
- The devices must be capable of operating in low-bandwidth environments.

Which of the following would provide the GREATEST benefit to the security posture of the devices?

A. Configuring an always-on VPN

B. Implementing application whitelisting

C. Requiring web traffic to pass through the on-premises content filter

D. Setting the antivirus DAT update schedule to weekly

Question #139 *Topic 1*

An organization has decided to host its web application and database in the cloud. Which of the following BEST describes the security concerns for this decision?

A. Access to the organizationλ€™s servers could be exposed to other cloud-provider clients.

B. The cloud vendor is a new attack vector within the supply chain.

C. Outsourcing the code development adds risk to the cloud provider.

D. Vendor support will cease when the hosting platforms reach EOL.

Question #140 *Topic 1*

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

A. business continuity plan.

B. communications plan.

C. disaster recovery plan.

D. continuity of operations plan.

Question #141 *Topic 1*

A user received an SMS on a mobile phone that asked for bank details. Which of the following social-engineering techniques was used in this case?

A. SPIM

B. Vishing

C. Spear phishing

D. Smishing

Question #142 *Topic 1*

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

Question #143 *Topic 1*

Which of the following will provide the BEST physical security countermeasures to stop intruders? (Choose two.)

A. Alarms

B. Signage

C. Lighting

D. Mantraps **Most Voted**

E. Fencing **Most Voted**

F. Sensors

Question #144 *Topic 1*

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

A. CVE

B. SIEM

C. SOAR

D. CVSS

Question #145 *Topic 1*

A security incident may have occurred on the desktop PC of an organizationλ€™s Chief Executive Officer (CEO). A duplicate copy of the CEOλ€™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 CEOλ€™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 in a live Linux environment to create a duplicate copy.

C. Remove the CEOλ€™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 analysis of the CEOλ€™s hard drive until after the incident is confirmed; duplicating the hard drive at this stage could destroy evidence.

Question #146 *Topic 1*

The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, including during a pandemic or crisis. However, the CEO is concerned that some staff members may take advantage of the flexibility and work from high-risk countries while on holiday or outsource work to 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 the CEOλ€™s concerns? (Choose two.)

A. Geolocation

B. Time-of-day restrictions

C. Certificates

D. Tokens

E. Geotagging

F. Role-based access controls

Question #147 *Topic 1*

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

A. Identification

B. Preparation

C. Lessons learned

D. Eradication

E. Recovery

F. Containment

Question #148 *Topic 1*

The SOC is reviewing processes 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. This 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

Question #149 — Topic 1

A security analyst is reviewing the following attack log output:

```
user comptia\john.smith attempted login with the password password123
user comptia\jane.doe attempted login with the password password123
user comptia\user.one attempted login with the password password123
user comptia\user.two attempted login with the password password123
user comptia\user.three attempted login with the password password123

user comptia\john.smith attempted login with the password password234
user comptia\jane.doe attempted login with the password password234
user comptia\user.one attempted login with the password password234
user comptia\user.two attempted login with the password password234
user comptia\user.three attempted login with the password password234
```

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

A. Rainbow table

B. Brute-force

C. Password-spraying

D. Dictionary

Question #150 — Topic 1

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

A. A captive portal

B. PSK

C. 802.1X

D. WPS

Question #151 — Topic 1

Which of the following are the MOST likely vectors for the unauthorized or unintentional inclusion of vulnerable code in a software companyâ€™s final software releases? (Choose 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 #152 *Topic 1*

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

Question #153 *Topic 1*

An organization just experienced a major cyberattack incident. 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

Question #154 *Topic 1*

A security analyst has received an alert about PII being sent via email. The analystâ€™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

Question #155 *Topic 1*

An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has been given all the developerâ€™s documentation about the internal architecture. Which of the following BEST represents the type of testing that will occur?

A. Bug bounty

B. White-box

C. Black-box

D. Gray-box

Question #156 *Topic 1*

A security engineer has enabled two-factor authentication on all workstations. Which of the following approaches are the MOST secure? (Choose two.)

A. Password and security question

B. Password and CAPTCHA

C. Password and smart card

D. Password and fingerprint

E. Password and one-time token

F. Password and voice

Question #157 — Topic 1

A security analyst needs to determine how an attacker was able to use User3 to gain a foothold within a companyâ€™s network. The companyâ€™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 Success: CompanyNetwork\User3 Successful logon.
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: CompanyNetworkd\User4 Successful logon.
```

Which of the following attacks MOST likely occurred?

A. Dictionary

B. Credential-stuffing

C. Password-spraying

D. Brute-force

Question #158 — Topic 1

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

Question #159 *Topic 1*

A Chief Information Security Officer (CISO) is concerned about the organizationâ€™s ability to continue business operations 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.

Question #160 *Topic 1*

A local coffee shop runs a small WiFi hotspot for its customers that utilizes WPA2-PSK. The coffee shop would like to stay current with security trends and wants to implement
WPA3 to make its WiFi even more secure. Which of the following technologies will the coffee shop MOST likely use in place of PSK?

A. WEP

B. MSCHAP

C. WPS

D. SAE

Question #161 *Topic 1*

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? (Choose two.)

A. An air gap

B. A cold aisle

C. Removable doors

D. A hot aisle

E. An IoT thermostat

F. A humidity monitor

Question #162 *Topic 1*

Which of the following will MOST likely cause machine-learning and AI-enabled systems to operate with unintended consequences?

A. Stored procedures

B. Buffer overflows

C. Data bias

D. Code reuse

Question #163 *Topic 1*

The process of passively gathering information prior to launching a cyberattack is called:

A. tailgating.

B. reconnaissance.

C. pharming.

D. prepending.

Question #164 *Topic 1*

During a routine scan of a wireless segment at a retail company, a security administrator discovers several devices are connected to the network that do not match the companyâ€™s naming convention and are not in the asset inventory. WiFi access is protected with 256-bit encryption via WPA2. Physical access to the companyâ€™s facility requires two-factor authentication using a badge and a passcode. Which of the following should the administrator implement to find and remediate the issue? (Choose two.)

A. Check the SIEM for failed logins to the LDAP directory.

B. Enable MAC filtering on the switches that support the wireless network.

C. Run a vulnerability scan on all the devices in the wireless network.

D. Deploy multifactor authentication for access to the wireless network.

E. Scan the wireless network for rogue access points.

F. Deploy a honeypot on the network.

Question #165 *Topic 1*

An organization has various applications that contain sensitive data hosted in the cloud. The companyزâ€™s leaders are concerned about lateral movement across applications of different trust levels. Which of the following solutions should the organization implement to address the concern?

A. ISFW

B. UTM

C. SWG

D. CASB

Question #166 *Topic 1*

A security engineer at an offline government facility is concerned about the validity of an SSL certificate. The engineer wants to perform the fastest check with the least delay to determine if the certificate has been revoked. Which of the following would BEST meet these requirements?

A. RA

B. OCSP

C. CRL

D. CSR

Question #167 *Topic 1*

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 backups for the computer equipment. Which of the following would BEST fulfill the ownerزâ€™s second need?

A. Lease a point-to-point circuit to provide dedicated access.

B. Connect the business router to its own dedicated UPS.

C. Purchase services from a cloud provider for high availability. **Most Voted**

D. Replace the businessزâ€™s wired network with a wireless network.

Question #168 *Topic 1*

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 gets a five-minute pcap to analyze. The analyst observes the following output:

No	Time	Source	Destination	Protocol	Length	Info
1234	9.1195665	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=655, FN=0
1235	9.1265649	Sagemcom_87:9f:a3	Broadcast	802.11	39	Deauthentication, SN=655, FN=0
1236	9.2223212	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=657, FN=0

Which of the following attacks does the analyst MOST likely see in this packet capture?

A. Session replay

B. Evil twin

C. Bluejacking

D. ARP poisoning

Question #169 *Topic 1*

Which of the following would be BEST to establish between organizations to define the responsibilities of each party, 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

Question #170 *Topic 1*

Users at an organization have been installing programs from the Internet on their workstations without first receiving 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 properly.
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

Question #171 *Topic 1*

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? (Choose two.)

A. Containerization

B. Storage segmentation

C. Posturing

D. Remote wipe

E. Full-device encryption

F. Geofencing

Question #172 *Topic 1*

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 following 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.

Question #173 *Topic 1*

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

Question #174 *Topic 1*

A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent the exfiltration of data? (Choose two.)

A. VPN

B. Drive encryption

C. Network firewall

D. File-level encryption

E. USB blocker

F. MFA

Question #175 *Topic 1*

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 applianceâ€™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

Question #176 — Topic 1

After consulting with the Chief Risk Officer (CRO), a manager decides to acquire cybersecurity insurance for the company. Which of the following risk management strategies is the manager adopting?

A. Risk acceptance

B. Risk avoidance

C. Risk transference

D. Risk mitigation

Question #177 — Topic 1

A companyâ€™s Chief Information Security Officer (CISO) recently warned the security manager that the companyâ€™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 Most Voted

B. White-hat hackers

C. Script kiddies

D. Insider threats Most Voted

Question #178 — Topic 1

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 storing.
Which of the following techniques BEST explains this action?

A. Predictability

B. Key stretching

C. Salting Most Voted

D. Hashing

Question #179 *Topic 1*

The website http://companywebsite.com requires users to provide personal information, including security question responses, for registration. Which of the following would MOST likely cause a data breach?

A. Lack of input validation

B. Open permissions

C. Unsecure protocol **Most Voted**

D. Missing patches

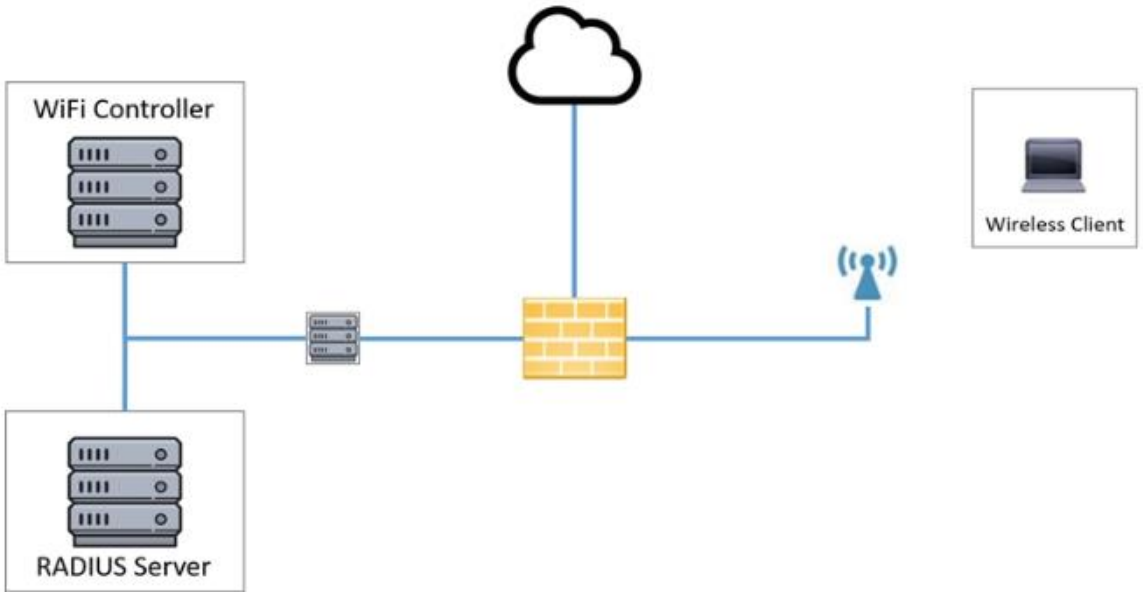
Question #180 *Topic 1*

SIMULATION -
A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802.1X using the most secure encryption and protocol available.

INSTRUCTIONS -
Perform the following steps:
1. Configure the RADIUS server.
2. Configure the WiFi controller.
3. Preconfigure the client for an incoming guest. The guest AD credentials are:

User: guest01 -

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



Question #181 *Topic 1*

HOTSPOT -

The security administrator has installed a new firewall which implements an implicit DENY policy by default.

INSTRUCTIONS -

Click on the firewall and configure it to allow ONLY the following communication:

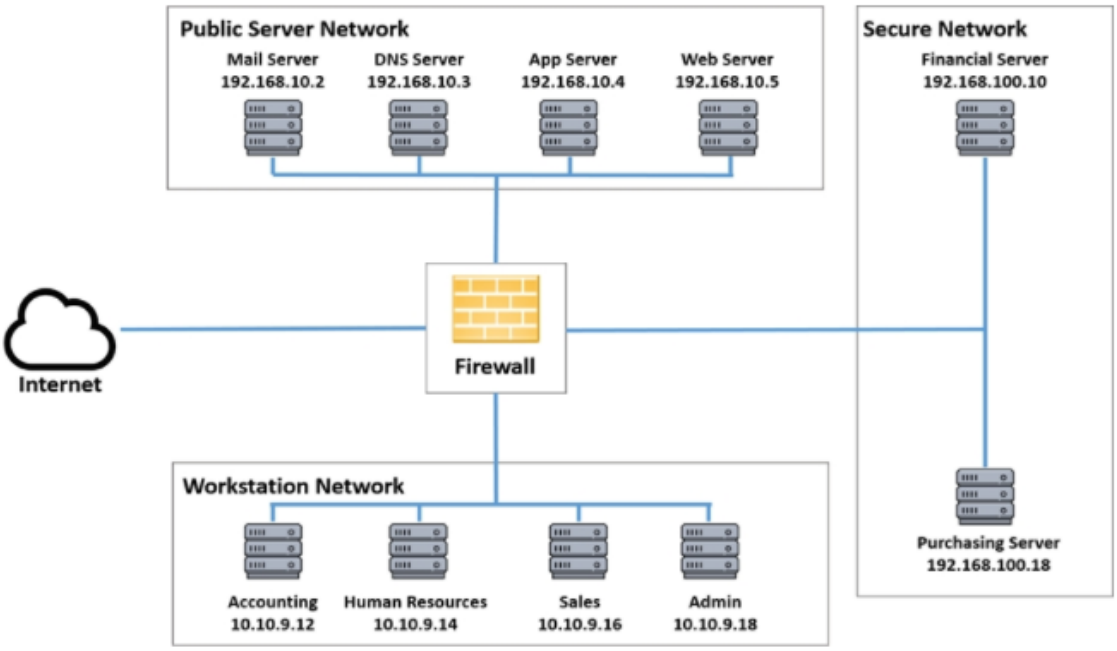
☞ The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.

☞ The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port.

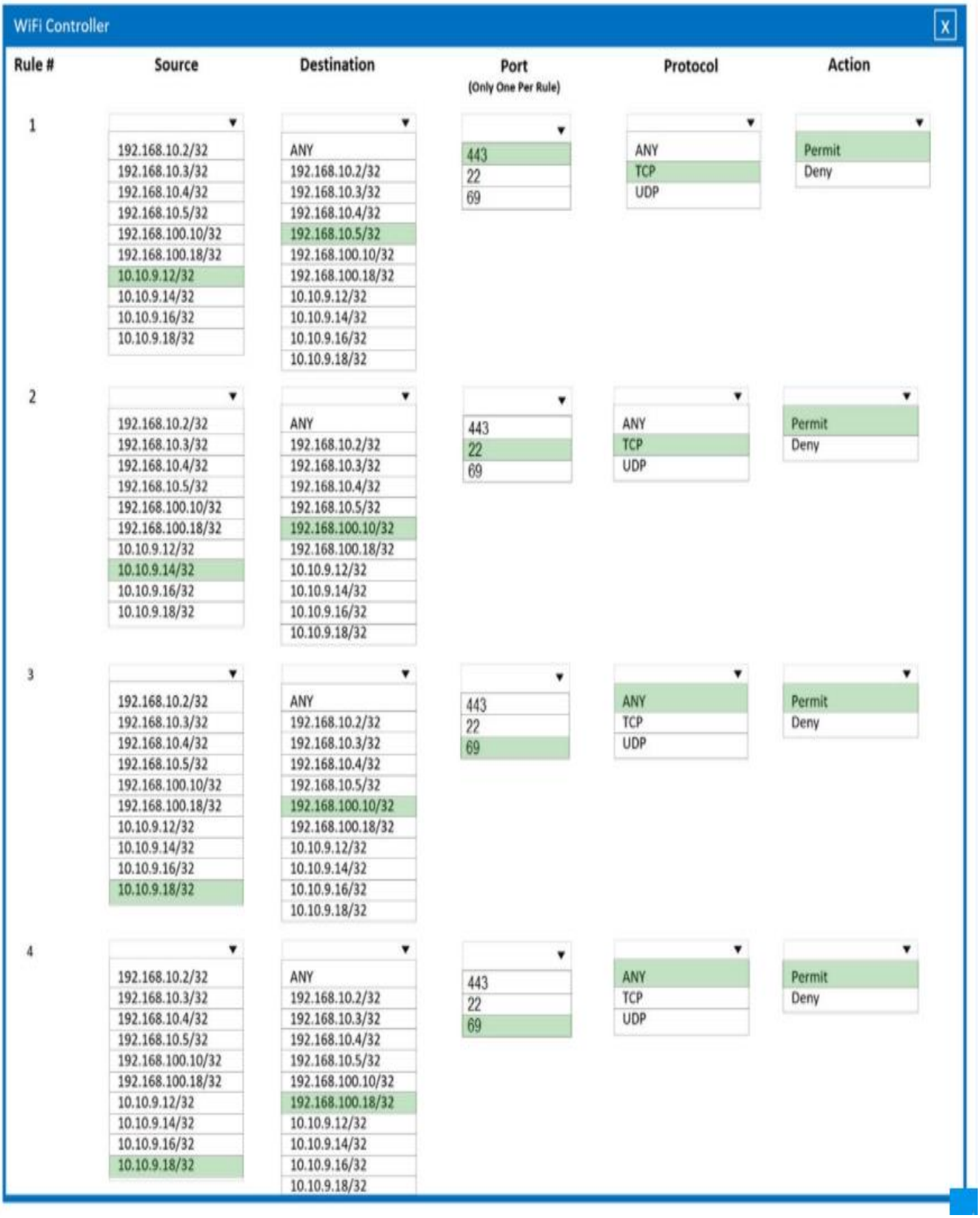
☞ The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.

The firewall will process rules in a top-down manner in order as a first match. The port number must be typed in and only one port number can be entered per rule. Type ANY for all ports.

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



Correct Answer:



Question #182 *Topic 1*

An organization relies on third-party video conferencing to conduct daily business. Recent security changes now require all remote workers to utilize a VPN to corporate resources. Which of the following would BEST maintain high-quality video conferencing while minimizing latency when connected to the VPN?

A. Using geographic diversity to have VPN terminations closer to end users

B. Utilizing split tunneling so only traffic for corporate resources is encrypted

C. Purchasing higher-bandwidth connections to meet the increased demand

D. Configuring QoS properly on the VPN accelerators

Question #183 *Topic 1*

An analyst is trying to identify insecure services that are running on the internal network. After performing a port scan, the analyst identifies that a server has some insecure services enabled on default ports. Which of the following BEST describes the services that are currently running and the secure alternatives for replacing them? (Choose three.)

A. SFTP, FTPS

B. SNMPv2, SNMPv3

C. HTTP, HTTPS

D. TFTP, FTP

E. SNMPv1, SNMPv2

F. Telnet, SSH

G. TLS, SSL

H. POP, IMAP

I. Login, rlogin

Question #184 *Topic 1*

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

```
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=5000000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=1000000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500 HTTP/1.1
```

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

A. SQLi

B. CSRF

C. Session replay

D. API

Question #185 *Topic 1*

A privileged user at a company stole several proprietary documents from a server. The user also went into the log files and deleted all records of the incident. The systems administrator has just informed investigators that other log files are available for review. Which of the following did the administrator MOST likely configure that will assist the investigators?

A. Memory dumps

B. The syslog server

C. The application log

D. The log retention policy

Question #186 — 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] 09:00:01UTC 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 "FTPL0gin!"
[ATTEMPT] 09:00:01UTC 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 #187 — Topic 1

A security administrator currently spends a large amount of time on common security tasks, such as 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 attempt?

A. DAC

B. ABAC

C. SCAP

D. SOAR

Question #188 *Topic 1*

A company just developed a new web application for a government agency. The application must be assessed and authorized prior to being deployed. Which of the following is required to assess the vulnerabilities resident in the application?

A. Repository transaction logs

B. Common Vulnerabilities and Exposures

C. Static code analysis

D. Non-credentialed scans

Question #189 *Topic 1*

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 this task? (Choose two.)

A. head

B. tcpdump

C. grep

D. tail

E. curl

F. openssl

G. dd

Question #190 *Topic 1*

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?
(Choose two.)

A. DNSSEC

B. Reverse proxy

C. VPN concentrator

D. PKI

E. Active Directory

F. RADIUS

Question #191 *Topic 1*

A university is opening a facility in a location where there is an elevated risk of theft. The university wants to protect the desktops in its classrooms and labs. Which of the following should the university use to BEST protect these assets deployed in the facility?

A. Visitor logs

B. Cable locks

C. Guards

D. Disk encryption

E. Motion detection

Question #192 *Topic 1*

Which of the following BEST describes the MFA attribute that requires a callback on a predefined landline?

A. Something you exhibit

B. Something you can do

C. Something you know

D. Something you are

Question #193 *Topic 1*

A security analyst needs to perform periodic vulnerability scans on production systems. Which of the following scan types would produce the BEST vulnerability scan report?

A. Port

B. Intrusive

C. Host discovery

D. Credentialed

Question #194 *Topic 1*

A worldwide manufacturing company has been experiencing email account compromises. 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

Question #195 *Topic 1*

A network administrator has been asked to design a solution to improve a companyа€™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

Question #196 — Topic 1

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	c6a9:6b16:758e	Dynamic	GE0/5
1	a3aa:b6a3:1212	Dynamic	GE0/5
1	8025:2ad8:bfac	Dynamic	GE0/5
1	b839:f995:a00a	Dynamic	GE0/5

Which of the following is happening to this switch?

A. MAC flooding

B. DNS poisoning

C. MAC cloning

D. ARP poisoning

Question #197 — Topic 1

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 meet this requirement?

A. RAID 0+1

B. RAID 2

C. RAID 5

D. RAID 6

Question #198 *Topic 1*

A security engineer needs to implement the following requirements:

- All Layer 2 switches should leverage Active Directory for authentication.
- All Layer 2 switches should use local fallback authentication of 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? (Choose two.)

A. Implement RADIUS. **Most Voted**

B. Configure AAA on the switch with local login as secondary. **Most Voted**

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.

Question #199 *Topic 1*

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

A. A tabletop exercise

B. NIST CSF

C. MITRE ATT&CK

D. OWASP

Question #200 *Topic 1*

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

Question #201 *Topic 1*

Which of the following types of controls is a CCTV camera that is not being monitored?

A. Detective Most Voted

B. Deterrent Most Voted

C. Physical

D. Preventive

Question #202 *Topic 1*

A company is setting up a web server on the Internet that will utilize both encrypted and unencrypted web-browsing protocols. A security engineer runs a port scan against the server from the Internet and sees the following output:

Port	Protocol	State	Service
22	tcp	open	ssh
25	tcp	filtered	smtp
53	tcp	filtered	domain
80	tcp	open	http
443	tcp	open	https

Which of the following steps would be best for the security engineer to take NEXT?

A. Allow DNS access from the Internet.

B. Block SMTP access from the Internet.

C. Block HTTPS access from the Internet.

D. Block SSH access from the Internet.

Question #203 *Topic 1*

A security analyst reviews the datacenter access logs for a fingerprint scanner and notices an abundance of errors that correlate with usersâ€™ reports of issues accessing the facility. Which of the following MOST likely indicates the cause of the access issues?

A. False rejection

B. Cross-over error rate

C. Efficacy rate

D. Attestation

Question #204 *Topic 1*

A forensics examiner is attempting to dump password 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.

Question #205 *Topic 1*

Which of the following is the BEST reason to maintain a functional and effective asset management policy that aids in ensuring the security of an organization?

A. To provide data to quantify risk based on the organizationâ€™s systems

B. To keep all software and hardware fully patched for known vulnerabilities

C. To only allow approved, organization-owned devices onto the business network

D. To standardize by selecting one laptop model for all users in the organization

Question #206 *Topic 1*

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

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.

Question #207 *Topic 1*

Which of the following would cause a Chief Information Security Officer (CISO) the MOST concern regarding newly installed Internet-accessible 4K surveillance cameras?

A. An inability to monitor 100% of every facility could expose the company to unnecessary risk.

B. The cameras could be compromised if not patched in a timely manner.

C. Physical security at the facility may not protect the cameras from theft.

D. Exported videos may take up excessive space on the file servers.

Question #208 *Topic 1*

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. EDR

Question #209 *Topic 1*

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

Question #210 *Topic 1*

During an incident, a companyâ€™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 microsegmentation rules.

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

D. Apply network blacklisting rules for the adversary domain.

Question #211 *Topic 1*

An organizationâ€™s Chief Security Officer (CSO) wants to validate the businessâ€™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

Question #212 — Topic 1

Which of the following scenarios would make 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. Routing tables have been compromised, and an attacker is rerouting traffic to malicious websites.

Question #213 — Topic 1

Which of the following provides the BEST protection for sensitive information and data stored in cloud-based services but still allows for full functionality and searchability of data within the cloud-based services?

A. Data encryption

B. Data masking

C. Anonymization

D. Tokenization

Question #214 — Topic 1

An attacker is trying to gain access by installing malware on a website that is known to be visited by the target victims. Which of the following is the attacker MOST likely attempting?

A. A spear-phishing attack

B. A watering-hole attack Most Voted

C. Typo squatting

D. A phishing attack

Question #215 *Topic 1*

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

Question #216 *Topic 1*

A company has three technicians who share the same credentials for troubleshooting system. Every time credentials are changed, the new ones are sent by email to all three technicians. The security administrator has become aware of this situation and wants to implement a solution to mitigate the risk. Which of the following is the BEST solution for company to implement?

A. SSO authentication

B. SSH keys

C. OAuth authentication

D. Password vaults

Question #217 *Topic 1*

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

```
[02/Feb2019:03:39:21 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=%2f..%2f..%2f..%2fetc%2fpassword HTTP/1.0" 80 200 200
[02/Feb2019:03:39:85 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=/../../../etc/password 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

Question #218 *Topic 1*

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

A. Tokenization

B. Data masking

C. Normalization

D. Obfuscation

Question #219 *Topic 1*

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

A. MTBF

B. RPO

C. RTO

D. MTTR **Most Voted**

Question #220 *Topic 1*

[1]
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

Question #221 *Topic 1*

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 **Most Voted**

C. Application whitelisting

D. An NG-SWG

Question #222 *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 #223 *Topic 1*

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 serverâ€™s listening ports.
Which of the following tools can BEST accomplish this task?

A. Netcat

B. Netstat

C. Nmap

D. Nessus

Question #224 *Topic 1*

Which of the following environments minimizes end-user disruption and 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

Question #225 *Topic 1*

An attacker is attempting to exploit users by creating a fake website with the URL www.validwebsite.com. The attackerâ€™s intent is to imitate the look and feel of a legitimate website to obtain personal information from unsuspecting users. Which of the following social-engineering attacks does this describe?

A. Information elicitation

B. Typo squatting

C. Impersonation

D. Watering-hole attack

Question #226 *Topic 1*

A security operations analyst is using the companyâ€™s SIEM solution to correlate alerts. Which of the following stages of the incident response process is this an example of?

A. Eradiction

B. Recovery

C. Identification

D. Preparation

Question #227 *Topic 1*

To reduce and overhead, an organization wants to move from an on-premises email solution to a cloud-based email solution. At this time, no other services will be moving.
Which of the following cloud models would BEST meet the needs of the organization?

A. MaaS

B. IaaS

C. SaaS

D. PaaS

Question #228 — Topic 1

A security analyst is reviewing the following command-line output:

```
Internet address      Physical address      Type
192.168.1.1           aa-bb-cc-00-11-22     dynamic
192.168.1.2           aa-bb-cc-00-11-22     dynamic
192.168.1.3           aa-bb-cc-00-11-22     dynamic
192.168.1.4           aa-bb-cc-00-11-22     dynamic
192.168.1.5           aa-bb-cc-00-11-22     dynamic
---output omitted-
--
192.168.1.251         aa-bb-cc-00-11-22     dynamic
192.168.1.252         aa-bb-cc-00-11-22     dynamic
192.168.1.253         aa-bb-cc-00-11-22     dynamic
192.168.1.254         aa-bb-cc-00-11-22     dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

Which of the following is the analyst observing?

- A. ICMP spoofing
- B. URL redirection
- C. MAC address cloning
- D. DNS poisoning

Question #229 — Topic 1

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

Question #230 *Topic 1*

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.

Question #231 *Topic 1*

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

Question #232 *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-team

C. Bug bounty

D. Gray-box

E. Black-box

Question #233 — Topic 1

An organization blocks user access to command-line interpreters, but hackers still managed to invoke the interpreters using native administrative tools. Which of the following should the security team do to prevent this from happening in the future?

A. Implement HIPS to block inbound and outbound SMB ports 139 and 445.

B. Trigger a SIEM alert whenever the native OS tools are executed by the user.

C. Disable the built-in OS utilities as long as they are not needed for functionality. Most Voted

D. Configure the AV to quarantine the native OS tools whenever they are executed.

Question #234 — Topic 1

A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The OSs are still supported by the vendor, but the industrial software is no longer supported. The Chief Information Security Officer (CISO) has created a resiliency plan for these systems that will allow OS patches to be installed in a non-production environment, while also creating backups of the systems for recovery. Which of the following resiliency techniques will provide these capabilities?

A. Redundancy

B. RAID 1+5

C. Virtual machines

D. Full backups

Question #235 — Topic 1

A security administrator is analyzing the corporate wireless network. The network only has two access points running on channels 1 and 11. While using airodump-ng. the administrator notices other access points are running with the same corporate ESSID on all available channels and with the same BSSID of one of the legitimate access points.
Which of the following attacks is happening on the corporate network?

A. Man in the middle

B. Evil twin

C. Jamming

D. Rogue access point

E. Disassociation

Question #236 *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 **Most Voted**

Question #237 *Topic 1*

A major political party experienced a server breach. The hacker then publicly posted stolen internal communications concerning campaign strategies to give the opposition party an advantage. Which of the following BEST describes these threat actors?

A. Semi-authorized hackers

B. State actors

C. Script kiddies

D. Advanced persistent threats

Question #238 *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 #239 *Topic 1*

Which of the following would satisfy three-factor authentication?

A. Password, retina scanner, and NFC card

B. Password, fingerprint scanner, and retina scanner

C. Password, hard token, and NFC card

D. Fingerprint scanner, hard token, and retina scanner

Question #240 *Topic 1*

The human resources department of a large online retailer has received multiple customer complaints about the rudeness of the automated chatbots it uses to interface and assist online shoppers. The system, which continuously learns and adapts, was working fine when it was installed a few months ago. Which of the following BEST describes the method being used to exploit the system?

A. Baseline modification

B. A fileless virus

C. Tainted training data

D. Cryptographic manipulation

Question #241 *Topic 1*

While reviewing the wireless router, a systems administrator of a small business determines someone is spoofing the MAC address of an authorized device. Given the table below:

Hostname	IP address	MAC	MAC filter
PC1	192.168.1.20	00:1E:1B:43:21:B2	On
PC2	192.168.1.23	31:1C:3C:13:25:C4	Off
PC3	192.168.1.25	20:A2:22:45:11:D2	On
UNKNOWN	192.168.1.21	12:44:B2:FF:A1:22	Off

Which of the following should be the administratorâ€™s NEXT step to detect if there is a rogue system without impacting availability?

A. Conduct a ping sweep.

B. Physically check each system. **Most Voted**

C. Deny Internet access to the â€UNKNOWNâ€ hostname.

D. Apply MAC filtering.

Question #242 *Topic 1*

An organization that has a large number of mobile devices is exploring enhanced security controls to manage unauthorized access if a device is lost or stolen. Specifically, if mobile devices are more than 3mi (4.8km) from the building, the management team would like to have the security team alerted and server resources restricted on those devices. Which of the following controls should the organization implement?

A. Geofencing

B. Lockout

C. Near-field communication

D. GPS tagging

Question #243 *Topic 1*

A security engineer is installing a WAF to protect the companyâ€™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 split-tunnel VPN

D. Load-balanced servers

Question #244 *Topic 1*

When implementing automation with IoT devices, which of the following should be considered FIRST to keep the network secure?

A. Z-Wave compatibility

B. Network range

C. Zigbee configuration

D. Communication protocols

Question #245 *Topic 1*

A security researcher is attempting to gather data on the widespread use of a zero-day exploit. Which of the following will the researcher MOST likely use to capture this data?

A. A DNS sinkhole

B. A honeypot

C. A vulnerability scan

D. CVSS

Question #246 *Topic 1*

A systems administrator needs to install the same X.509 certificate on multiple servers. Which of the following should the administrator use?

A. Key escrow

B. A self-signed certificate

C. Certificate chaining

D. An extended validation certificate **Most Voted**

Question #247 *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 #248 *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 #249 *Topic 1*

A security analyst has been reading about a newly discovered cyberattack from a known threat actor. Which of the following would BEST support the analystâ€™s review of the tactics, techniques, and protocols the threat actor was observed using in previous campaigns?

A. Security research publications

B. The MITRE ATT&CK framework

C. The Diamond Model of Intrusion Analysis

D. The Cyber Kill Chain

Question #250 *Topic 1*

An incident, which is affecting dozens of systems, involves malware that reaches out to an Internet service for rules and updates. The IP addresses for the Internet host appear to be different in each case. The organization would like to determine a common IoC to support response and recovery actions. Which of the following sources of information would BEST support this solution?

A. Web log files

B. Browser cache

C. DNS query logs

D. Antivirus

Question #251 *Topic 1*

DRAG DROP -

Leveraging the information supplied below, complete the CSR for the server to set up TLS (HTTPS).

- Hostname: ws01
- Domain: comptia.org
- IPv4: 10.1.9.50
- IPv4: 10.2.10.50
- Root: home.aspx
- DNS CNAME: homesite

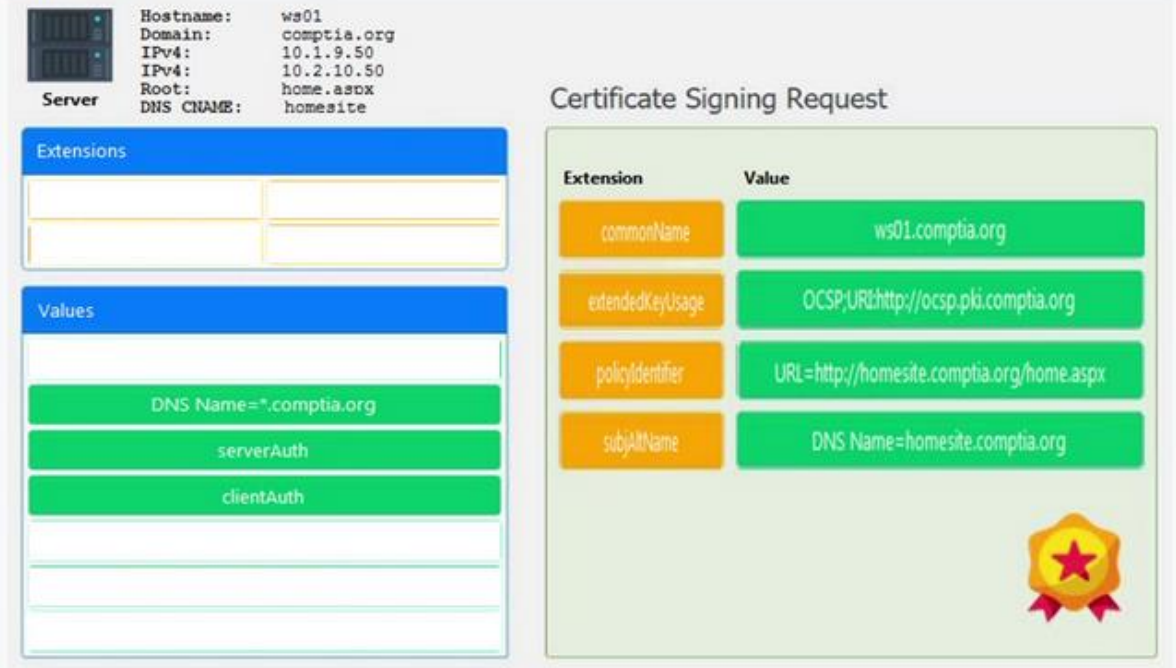
INSTRUCTIONS -

Drag the various data points to the correct locations within the CSR. Extension criteria belong in the left-hand column and values belong in the corresponding row in the right- hand column.

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

Select and Place:

Correct Answer:



Question #252 — Topic 1

Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Choose two.)

A. Block cipher

B. Hashing

C. Private key

D. Perfect forward secrecy

E. Salting

F. Symmetric keys

Question #253 — Topic 1

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

A. Code signing

B. Fuzzing Most Voted

C. Manual code review

D. Dynamic code analysis

Question #254 — Topic 1

A security analyst is reviewing a penetration-testing report from a third-party contractor. The penetration testers used the organizationλ€™s new API to bypass a driver to perform privilege escalation on the organizationλ€™s web servers. Upon looking at the API, the security analyst realizes the particular API call was to a legacy system running an outdated
OS. Which of the following is the MOST likely attack type?

A. Request forgery

B. Session replay

C. DLL injection

D. Shimming Most Voted

Question #255 *Topic 1*

Entering a secure area requires passing through two doors, both of which require someone who is already inside to initiate access. Which of the following types of physical security controls does this describe?

A. Cameras

B. Faraday cage

C. Access control vestibule

D. Sensors

E. Guards

Question #256 *Topic 1*

The concept of connecting a user account across the systems of multiple enterprises is BEST known as:

A. federation.

B. a remote access policy.

C. multifactor authentication.

D. single sign-on.

Question #257 *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 algorithmâ€™s longevity Most Voted

C. A method of introducing entropy into key calculations

D. The computational overhead of calculating the encryption key

Question #258 — Topic 1

Which of the following types of attacks is specific to the individual it targets?

A. Whaling **Most Voted**

B. Pharming

C. Smishing

D. Credential harvesting

Question #259 — Topic 1

Several large orders of merchandise were recently purchased on an e-commerce companyâ€™s website. The totals for each of the transactions were negative values, resulting in credits on the customersâ€™ accounts. Which of the following should be implemented to prevent similar situations in the future?

A. Ensure input validation is in place to prevent the use of invalid characters and values.

B. Calculate all possible values to be added together and ensure the use of the proper integer in the code.

C. Configure the web application firewall to look for and block session replay attacks.

D. Make sure transactions that are submitted within very short time periods are prevented from being processed.

Question #260 — Topic 1

A security engineer obtained the following output from a threat intelligence source that recently performed an attack on the companyâ€™s server:

```
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2..2fetc2fpasswd
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
```

Which of the following BEST describes this kind of attack?

A. Directory traversal

B. SQL injection

C. API

D. Request forgery

Question #261 *Topic 1*

After installing a Windows server, a cybersecurity administrator needs to harden it, following security best practices. Which of the following will achieve the administratorâ€™s goal?
(Choose two.)

- A. Disabling guest accounts
- B. Disabling service accounts
- C. Enabling network sharing
- D. Disabling NetBIOS over TCP/IP
- E. Storing LAN manager hash values
- F. Enabling NTLM

Question #262 *Topic 1*

A web server administrator has redundant servers and needs to ensure failover to the secondary server when the primary server goes down. Which of the following should the administrator implement to avoid disruption?

- A. NIC teaming **Most Voted**
- B. High availability **Most Voted**
- C. Dual power supply
- D. IaaS

Question #263 *Topic 1*

After a phishing scam for a userâ€™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 #264 *Topic 1*

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

A. Perfect forward secrecy **Most Voted**

B. Elliptic-curve cryptography

C. Key stretching

D. Homomorphic encryption

Question #265 *Topic 1*

Following a prolonged datacenter outage that affected web-based sales, a company has decided to move its operations to a private cloud solution. The security team has received the following requirements:

☞ There must be visibility into how teams are using cloud-based services.

☞ The company must be able to identify when data related to payment cards is being sent to the cloud.

☞ Data must be available regardless of the end userа€™s geographic location.

Administrators need a single pane-of-glass view into traffic and trends.

▪

Which of the following should the security analyst recommend?

A. Create firewall rules to restrict traffic to other cloud service providers.

B. Install a DLP solution to monitor data in transit.

C. Implement a CASB solution. **Most Voted**

D. Configure a web-based content filter.

Question #266 *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 #267 *Topic 1*

Which of the following should a data owner require all personnel to sign to legally protect intellectual property?

A. An NDA

B. An AUP

C. An ISA

D. An MOU

Question #268 *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 that 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? (Choose two.)

A. 135

B. 139

C. 143

D. 161

E. 443

F. 445

Question #269 *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 #270 *Topic 1*

A Chief Executive Officer (CEO) is dissatisfied with the level of service from the companyâ€™s new service provider. The service provider is preventing the CEO from sending email from a work account to a personal account. Which of the following types of service providers is being used?

A. Telecommunications service provider

B. Cloud service provider

C. Master managed service provider

D. Managed security service provider **Most Voted**

Question #271 *Topic 1*

During an incident, an EDR system detects an increase in the number of encrypted outbound connections from multiple hosts. A firewall is also reporting an increase in outbound connections that use random high ports. An analyst plans to review the correlated logs to find the source of the incident. Which of the following tools will BEST assist the analyst?

A. A vulnerability scanner

B. A NGFW

C. The Windows Event Viewer

D. A SIEM

Question #272 — Topic 1

Which of the following distributes data among nodes, making it more difficult to manipulate the data while also minimizing downtime?

A. MSSP

B. Public cloud

C. Hybrid cloud

D. Fog computing **Most Voted**

Question #273 — Topic 1

Ann, a forensic analyst, needs to prove that the data she originally acquired has remained unchanged while in her custody. Which of the following should Ann use?

A. Chain of custody **Most Voted**

B. Checksums

C. Non-repudiation

D. Legal hold

Question #274 — Topic 1

An organizationâ€™s RPO for a critical system is two hours. The system is used Monday through Friday, from 9:00 a.m. to 5:00 p.m. 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 MOST efficient 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 **Most Voted**

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

Question #275 *Topic 1*

Which of the following threat actors is MOST likely to be motivated by ideology?

A. Business competitor

B. Hacktivist

C. Criminal syndicate

D. Script kiddie

E. Disgruntled employee

Question #276 *Topic 1*

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

Question #277 *Topic 1*

A network administrator is concerned about users being exposed to malicious content when accessing company cloud applications. The administrator wants to be able to block access to sites based on the AUP. The users must also be protected because many of them work from home or at remote locations, providing on-site customer support. Which of the following should the administrator employ to meet these criteria?

A. Implement NAC.

B. Implement an SWG.

C. Implement a URL filter.

D. Implement an MDM.

Question #278 *Topic 1*

A security administrator needs to inspect in-transit files on the enterprise network to search for PII, credit card data, and classification words. Which of the following would be the BEST to use?

A. IDS solution

B. EDR solution

C. HIPS software solution

D. Network DLP solution

Question #279 *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 #280 *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 #281 *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 **Most Voted**

D. Weak encryption

Question #282 *Topic 1*

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 performs regular audits to determine if violations have occurred.

D. A security control objective cannot be met through a technical change, so the Chief Information Officer decides to sign off on the risk.

Question #283 *Topic 1*

A company just implemented a new telework policy that allows employees to use personal devices for official email and file sharing while working from home. Some of the requirements are:
☞ Employees must provide an alternate work location (i.e., a home address).
☞ Employees must install software on the device that will prevent the loss of proprietary data but will not restrict any other software from being installed.
Which of the following BEST describes the MDM options the company is using?

A. Geofencing, content management, remote wipe, containerization, and storage segmentation

B. Content management, remote wipe, geolocation, context-aware authentication, and containerization

C. Application management, remote wipe, geofencing, context-aware authentication, and containerization **Most Voted**

D. Remote wipe, geolocation, screen locks, storage segmentation, and full-device encryption

Question #284 *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 #285 *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 #286 *Topic 1*

A user must introduce a password and a USB key to authenticate against a secure computer, and authentication is limited to the state in which the company resides. Which of the following authentication concepts are in use?

A. Something you know, something you have, and somewhere you are

B. Something you know, something you can do, and somewhere you are

C. Something you are, something you know, and something you can exhibit

D. Something you have, somewhere you are, and someone you know

Question #287 *Topic 1*

A global company is experiencing unauthorized logins 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 #288 *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 #289 *Topic 1*

The lessons-learned analysis from a recent incident reveals that an administrative office worker received a call from someone claiming to be from technical support. The caller convinced the office worker to visit a website, and then download and install a program masquerading as an antivirus package. The program was actually a backdoor that an attacker could later use to remote control the workerא€™s PC. Which of the following would be BEST to help prevent this type of attack in the future?

A. Data loss prevention

B. Segmentation

C. Application whitelisting

D. Quarantine

Question #290 *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 **Most Voted**

B. Staging **Most Voted**

C. Development

D. Production

Question #291 *Topic 1*

An organization regularly scans its infrastructure for missing security patches but is concerned about hackers gaining access to the scannerא€™s account. Which of the following would be BEST to minimize this risk while ensuring the scans are useful?

A. Require a complex, eight-character password that is updated every 90 days.

B. Perform only non-intrusive scans of workstations.

C. Use non-credentialed scans against high-risk servers.

D. Log and alert on unusual scanner account logon times.

Question #292 *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 #293 *Topic 1*

A multinational organization that offers web-based services has datacenters that are located only in the United States; however, a large number of its customers are in Australia, Europe, and China. Payments for services are managed by a third party in the United Kingdom that specializes in payment gateways. The management team is concerned the organization is not compliant with privacy laws that cover some of its customers. Which of the following frameworks should the management team follow?

A. Payment Card Industry Data Security Standard

B. Cloud Security Alliance Best Practices

C. ISO/IEC 27032 Cybersecurity Guidelines

D. General Data Protection Regulation **Most Voted**

Question #294 *Topic 1*

Which of the following is the correct order of volatility from MOST to LEAST volatile?

A. Memory, temporary filesystems, routing tables, disk, network storage

B. Cache, memory, temporary filesystems, disk, archival media

C. Memory, disk, temporary filesystems, cache, archival media

D. Cache, disk, temporary filesystems, network storage, archival media

Question #295 *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

C. A VLAN

D. An ACL **Most Voted**

Question #296 — 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 ג€cloud-firstג€ adoption strategy?

A. Risk matrix

B. Risk tolerance

C. Risk register

D. Risk appetite Most Voted

Question #297 — Topic 1

A bank detects fraudulent activity on userג€™s account. The user confirms transactions completed yesterday on the bankג€™s website at https:/www.company.com. A security analyst then examines the userג€™s Internet usage logs and observes the following output:

```
date;username;url;destinationport;responsecode
2020-03-01;userann;http://www.company.org/;80;302
2020-03-01;userann:http://www.company.org/secure_login/;80;200
2020-03-01;userann:http://www.company.org/dashboard/;80;200
```

Which of the following has MOST likely occurred?

A. Replay attack

B. SQL injection

C. SSL stripping

D. Race conditions

Question #298 — Topic 1

An organization plans to transition the intrusion detection and prevention techniques on a critical subnet to an anomaly-based system. Which of the following does the organization need to determine for this to be successful?

A. The baseline

B. The endpoint configurations

C. The adversary behavior profiles

D. The IPS signatures

Question #299 *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? (Choose two.)

A. Identity processor

B. Service requestor

C. Identity provider

D. Service provider

E. Tokenized resource

F. Notarized referral

Question #300 *Topic 1*

A Chief Security Officer (CSO) is concerned about the volume and integrity of sensitive information that is exchanged between the organization and a third party through email.
The CSO is particularly concerned about an unauthorized party who is intercepting information that is in transit between the two organizations. Which of the following would address the CSOâ€™s concerns?

A. SPF

B. DMARC

C. SSL

D. DKIM

E. TLS **Most Voted**

Question #301 *Topic 1*

SIMULATION -

A newly purchased corporate WAP needs to be configured in the MOST secure manner possible.

INSTRUCTIONS -

Please click on the below items on the network diagram and configure them accordingly:

a€¢ WAP

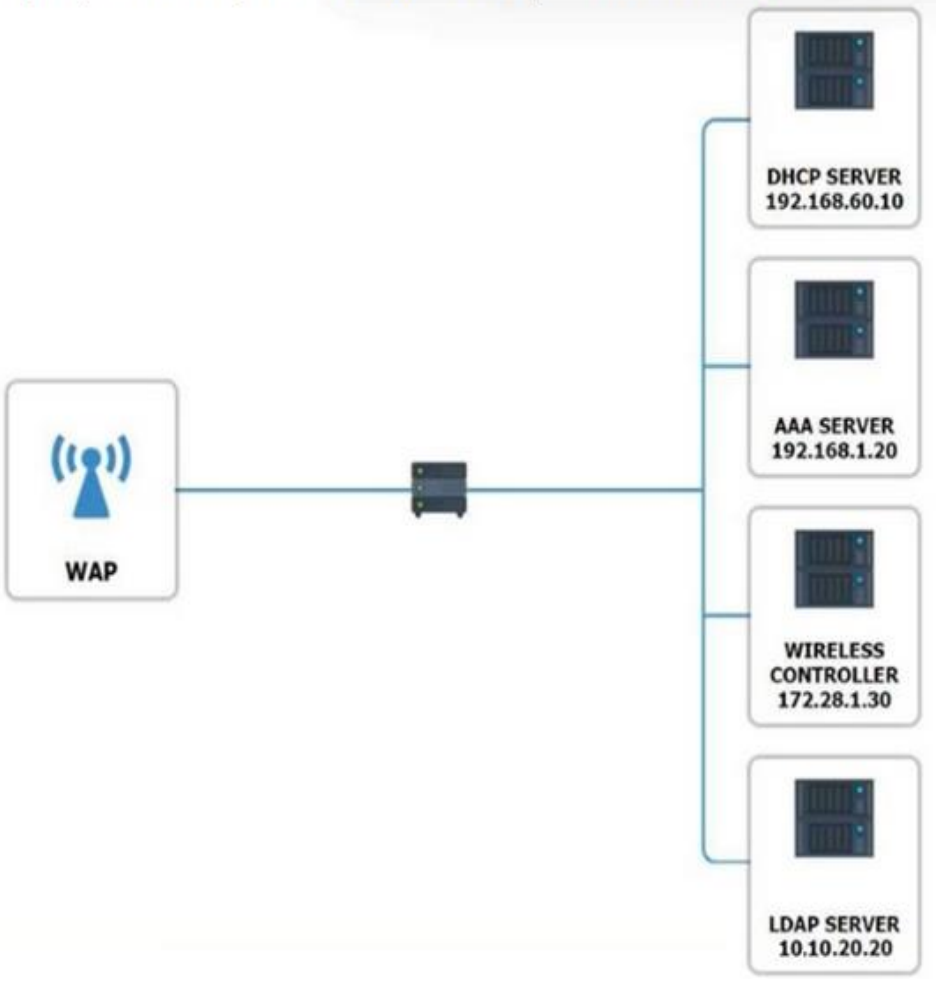
a€¢ DHCP Server

a€¢ AAA Server

a€¢ Wireless Controller

a€¢ LDAP Server

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



Correct Answer: *See explanation below.*