

Exam : **SY0-601**

Title : **CompTIA Security+ Exam**

Vendor : **CompTIA**

Version : **V36.35**

NO.1 Which of the following is a reason to publish files' hashes?

- (A). To validate the integrity of the files
- (B). To verify if the software was digitally signed
- (C). To use the hash as a software activation key
- (D). To use the hash as a decryption passphrase

Answer: B

NO.2 Which of the following are the BEST ways to implement remote home access to a company's intranet systems if establishing an always-on VPN is not an option? (Select Two)

- (A). Install VPN concentrations at home offices
- (B). Create NAT on the firewall for intranet systems
- (C). Establish SSH access to a jump server
- (D). Implement a SSO solution
- (E). Enable MFA for intranet systems
- (F). Configure SNMPv3 server and clients.

Answer: A,E

NO.3 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 projected network segment. Which of the following would be MOST effective to implement to further mitigate the reported vulnerability?

- (A). DNS sinkholding
- (B). DLP rules on the terminal
- (C). An IP blacklist
- (D). Application whitelisting

Answer: D

NO.4 A database administrator wants to grant access to an application that will be reading and writing data to a database. The database is shared by other applications also used by the finance department Which of the following account types is MOST appropriate for this purpose?

- (A). Service
- (B). Shared
- (C). eneric
- (D). Admin

Answer: A

NO.5 Which of the following BEST describes when an organization utilizes a ready-to-use application from a cloud provider?

- (A). IaaS
- (B). SaaS
- (C). Paas
- (D). XaaS

Answer: B

SaaS, or software as a service, is on-demand access to ready-to-use, cloud-hosted application software.

<https://www.ibm.com/cloud/learn/iaas-paas-saas>

NO.6 An administrator needs to protect user passwords and has been advised to hash the passwords. Which of the following BEST describes what the administrator is being advised to do?

- (A). Perform a mathematical operation on the passwords that will convert them into unique strings
- (B). Add extra data to the passwords so their length is increased, making them harder to brute force
- (C). Store all passwords in the system in a rainbow table that has a centralized location
- (D). Enforce the use of one-time passwords that are changed for every login session.

Answer: D

NO.7 After multiple on premises security solutions were migrated to the cloud, the incident response time increased. The analyst are spending a long time to trace information on different cloud consoles and correlating data in different formats. Which of the following can be used to optimize the incident response time?

- (A). CASB
- (B). VPC
- (C). SWG
- (D). CMS

Answer: A

NO.8 A security analyst has identified malware spreading through the corporate network and has activated the CSIRT. Which of the following should the analyst do NEXT? A

- (A). Review how the malware was introduced to the network
- (B). Attempt to quarantine all infected hosts to limit further spread
- (C). Create help desk tickets to get infected systems reimaged
- (D). Update all endpoint antivirus solutions with the latest updates

Answer: C

NO.9 A large bank with two geographically dispersed data centers is concerned about major power disruptions at both locations. Every day each location experiences very brief outages that last for a few seconds. However, during the summer, a high risk of intentional brownouts that last up to an hour exists, particularly at one of the locations near an industrial smelter. Which of the following is the BEST solution to reduce the risk of data loss?

- (A). Dual supply
- (B). Generator
- (C). UPS
- (D). PDU
- (E). Daily backups

Answer: E

NO.10 A security analyst is concerned about critical vulnerabilities that have been detected on some applications running inside containers. Which of the following is the BEST remediation strategy?

- (A). Update the base container image and redeploy the environment
- (B). Include the containers in the regular patching schedule for servers
- (C). Patch each running container individually and test the application
- (D). Update the host in which the containers are running

Answer: C

NO.11 After entering a username and password, and 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). Biometric
- (D). Two-factor authentication

Answer: D

NO.12 A security analyst is evaluating solutions to deploy an additional layer of protection for a web application. The goal is to allow only encrypted communications without relying on network devices. Which of the following can be implemented?

- (A). HTTP security header
- (B). DNSSEC implementation
- (C). SRTP
- (D). S/MIME

Answer: C

NO.13 A security analyst is tasked with classifying data to be stored on company servers. Which of the following should be classified as proprietary?

- (A). Customers' dates of birth
- (B). Customers' email addresses
- (C). Marketing strategies
- (D). Employee salaries

Answer: B

NO.14 Which of the following is the FIRST environment in which proper, secure coding should be practiced?

- (A). Stage
- (B). Development
- (C). Production
- (D). Test

Answer: D

NO.15 After a recent external audit, the compliance team provided a list of several non-compliant, in-scope hosts that were not encrypting cardholder data at rest. Which of the following compliance frameworks would address the compliance team's GREATEST concern?

- (A). PCI DSS
- (B). GDPR
- (C). ISO 27001
- (D). NIST CSF

Answer: A

NO.16 After a recent security incident, a security analyst discovered that unnecessary ports were open on a firewall policy for a web server. Which of the following firewall policies would be MOST secure for a web server?

A)

[Source	Destination	Port	Action]
Any	Any	TCP 55	Allow
Any	Any	TCP 80	Allow
Any	Any	TCP 443	Allow
Any	Any	Any	Any

B)

[Source	Destination	Port	Action]
Any	Any	TCP 55	Deny
Any	Any	TCP 80	Allow
Any	Any	TCP 445	Allow
Any	Any	Any	Allow

C)

[Source	Destination	Port	Action]
Any	Any	TCP 80	Deny
Any	Any	TCP 443	Allow
Any	Any	Any	Allow

D)

[Source	Destination	Port	Action]
Any	Any	TCP 80	Allow
Any	Any	TCP 443	Allow
Any	Any	Any	Deny

(A). Option A

(B). Option B

(C). Option C

(D). Option D

Answer: D

NO.17 Which of the following would be indicative of a hidden audio file found inside of a piece of source code?

(A). Steganography

(B). Homomorphlic encryption

(C). Cipher suite

(D). Blockchain

Answer: A

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. The word steganography is derived from the Greek words steganos (meaning hidden or covered) and the Greek root graph (meaning to write).

NO.18 An organization is concerned that its hosted web servers are not running the most updated

version of the software. Which of the following would work BEST to help identify potential vulnerabilities?

- (A). Hping3 -s comptia, org -p 80
- (B). Nc -1 -v comptia, org -p 80
- (C). nmp comptia, org -p 80 -aV
- (D). nslookup -port=80 comtia.org

Answer: C

Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

NO.19 An organization just experienced a major cyberattack modem. 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

Answer: D

<https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/>
https://csrc.nist.gov/glossary/term/advanced_persistent_threat

NO.20 A technician enables full disk encryption on a laptop that will be taken on a business trip. Which of the following does this process BEST protect?

- (A). Data in transit
- (B). Data in processing
- (C). Data at rest
- (D). Data tokenization

Answer: C

NO.21 An analyst is reviewing logs associated with an attack. The logs indicate an attacker downloaded a malicious file that was quarantined by the AV solution. The attacker utilized a local non-administrative account to restore the malicious file to a new location. The file was then used by another process to execute a payload. Which of the following attacks did the analyst observe?

- (A). Privilege escalation
- (B). Request forgeries
- (C). Injection
- (D). Replay attack

Answer: B

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf[1]) or XSRF, is a type of malicious exploit of a website where unauthorized commands are submitted from a user that the web application trusts.[2] There are many ways in which a malicious website can transmit such commands; specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests, for example, can all work without the user's interaction or even knowledge. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.[3] In a CSRF attack, an innocent end user is tricked by an attacker into submitting a web request that they did not intend.

This may cause actions to be performed on the website that can include inadvertent client or server data leakage, change of session state, or manipulation of an end user's account.

NO.22 The Chief Compliance Officer from a bank has approved a background check policy for all new hires Which of the following is the policy MOST likely protecting against?

- (A). Preventing any current employees' siblings from working at the bank to prevent nepotism
- (B). Hiring an employee who has been convicted of theft to adhere to industry compliance
- (C). Filternng applicants who have added false information to resumes so they appear better qualified
- (D). Ensuring no new hires have worked at other banks that may be trying to steal customer information

Answer: B

NO.23 A Chief Information Security Officer has defined resiliency requirements for a new data center architecture The requirements are as follows

- * Critical fileshares will remain accessible during and after a natural disaster
- * Frve percent of hard disks can fail at any given time without impacting the data.
- * Systems will be forced to shut down gracefully when battery levels are below 20% Which of the following are required to BEST meet these objectives? (Select THREE)

- (A). Fiber switching
- (B). IaC
- (C). NAS
- (D). RAID
- (E). UPS
- (F). Redundant power supplies
- (G). Geographic dispersal
- (H). Snapshots
- (I). Load balancing

Answer: A,C,G

NO.24 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

Answer: D

<https://www.techtarget.com/searchitchannel/definition/MSSP>

NO.25 The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, incident during a pandemic or crisis, However, the CEO is concerned that some staff members may take advantage of the of the flexibility and work from high-risk countries while on holidays work to a third-party organization in another country. The Chief information Officer (CIO) believes the company can implement some basic to mitigate the majority of the risk. Which of the following would be BEST to mitigate CEO's concern?

(Select TWO).

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

Answer: A,E

NO.26 An organization maintains several environments in which patches are developed and tested before deployed to an operation status. Which of the following is the environment in which patches will be deployed just prior to being put into an operational status?

- (A). Development
- (B). Test
- (C). Production
- (D). Staging

Answer: B

NO.27 A security analyst is investigating suspicious traffic on the web server located at IP address 10.10.1.1. A search of the WAF logs reveals the following output:

Source IP	Destination IP	Requested URL	Action Taken
172.16.1.3	10.10.1.1	/web/cgi-bin/contact?category=custname'--	permit and log
172.16.1.3	10.10.1.1	/web/cgi-bin/contact?category=custname+OR+1=1--	permit and log

Which of the following is MOST likely occurring?

- (A). XSS attack
- (B). SQLi attack
- (C). Replay attack
- (D). XSRF attack

Answer: B

NO.28 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

Answer: A

An attack in which an attacker targets specific groups or organizations, discovers which websites they frequent, and injects malicious code into those sites.

NO.29 Which of the following is a targeted attack aimed at compromising users within a specific industry or group?

- (A). Watering hole
- (B). Typosquatting
- (C). Hoax
- (D). Impersonation

Answer: A

A targeted attack refers to a type of threat in which threat actors actively pursue and compromise a target entity's infrastructure while maintaining anonymity. These attackers have a certain level of expertise and have sufficient resources to conduct their schemes over a long-term period. They can adapt, adjust, or improve their attacks to counter their victim's defenses. Background Targeted attacks often employ similar methods found in traditional online threats such as malicious emails, compromised or malicious sites, exploits, and malware. Targeted attacks differ from traditional online threats in many ways:

- * Targeted attacks are typically conducted as campaigns. APTs are often conducted in campaigns-a series of failed and successful attempts over time to get deeper and deeper into a target's network-and are thus not isolated incidents.
- * They usually target specific industries such as businesses, government agencies, or political groups. Attackers often have long-term goals in mind, with motives that include, but are not limited to, political gain, monetary profit, or business data theft. Attackers often customize, modify and improve their methods depending on the nature of their target sector and to circumvent any security measures implemented.

Phases of a Targeted Attack

- * Intelligence gathering. Threat actors identify and gather publicly available information about their target to customize their attacks. This initial phase aims to gain strategic information not only on the intended target's IT environment but also on its organizational structure. The information gathered can range from the business applications and software an enterprise utilizes to the roles and relationships that exist within it. This phase also utilizes social engineering techniques that leverage recent events, work-related issues or concerns, and other areas of interest for the intended target.
- * Point of entry. Threat actors may use varied methods to infiltrate a target's infrastructure. Common methods include customized spearphishing email, zero-day or software exploits, and watering hole techniques. Attackers also utilize instant-messaging and social networking platforms to entice targets to click a link or download malware. Eventually, establishing a connection with the target is acquired.
- * Command-and-control (C&C) communication. After security has been breached, threat actors constantly communicate to the malware to either execute malicious routines or gather information within the company network. Threat actors use techniques to hide this communication and keep their movements under the radar.
- * Lateral movement. Once inside the network, threat actors move laterally throughout the network to seek key information or infect other valuable systems.
- * Asset/Data Discovery. Notable assets or data are determined and isolated for future data exfiltration. Threat actors have access to "territories" that contain valuable information and noteworthy assets. These data are then identified and transferred through tools like remote access Trojans (RATs) and customized and legitimate tools. A possible technique used in this stage may be sending back file lists in different directories so attackers can identify what are valuable.
- * Data Exfiltration. This is the main goal of targeted attacks. An attack's objective is to gather key information and transfer this to a location that the attackers control. Transferring such data can be conducted quickly or gradually. Targeted attacks strive to remain undetected in the network in order to gain access to the company's crown jewels or valuable data. These valuable data include intellectual property, trade secrets, and customer information. In addition, threat actors may also seek other sensitive data such as top-secret documents from government or military institutions. Once a targeted attack is successful and has reached as far as the data exfiltration stage, it is not difficult for attackers to draw out the data. Although targeted attacks are not known to specifically

target consumers, their data are also at risk once target business sectors have been infiltrated. As a result, such attacks (if successful) may damage a company's reputation.

[https://www.trendmicro.com/vinfo/us/security/definition/targeted-](https://www.trendmicro.com/vinfo/us/security/definition/targeted-attacks#:~:text=A%20targeted%20attack%20refers%20to,over%20a%20long%2Dterm%20period.)

attacks#:~:text=A%20targeted%20attack%20refers%20to,over%20a%20long%2Dterm%20period.

NO.30 A user reports falling for a phishing email to an analyst. Which of the following system logs would the analyst check FIRST?

- (A). DNS
- (B). Message gateway
- (C). Network
- (D). Authentication

Answer: C

NO.31 A company labeled some documents with the public sensitivity classification This means the documents can be accessed by:

- (A). employees of other companies and the press
- (B). all members of the department that created the documents
- (C). only the company's employees and those listed in the document
- (D). only the individual listed in the documents

Answer: A

NO.32 Given the following logs:

```
[DATA] attacking service ftp on port 21
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "password"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "access"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "allow"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "please"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "ftp"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "letmein"
[21][ftp] host: 192.168.50.1 login:admin password:letmein
1 of 1 target successfully completed, 1 valid password found
```

Which of the following BEST describes the type of attack that is occurring?

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

Answer: C

NO.33 Which of the following is a benefit of including a risk management framework into an organization's security approach?

- (A). It defines expected service levels from participating supply chain partners to ensure system outages are remediated in a timely manner
- (B). It identifies specific vendor products that have been tested and approved for use in a secure environment.
- (C). It provides legal assurances and remedies in the event a data breach occurs
- (D). It incorporates control, development, policy, and management activities into IT operations.

Answer: C

NO.34 Business partners are working on a security mechanism to validate transactions securely. The requirement is for one company to be responsible for deploying a trusted solution that will register and issue artifacts used to sign, encrypt, and decrypt transaction files. Which of the following is the BEST solution to adopt?

- (A). PKI
- (B). Blockchain
- (C). SAML
- (D). OAuth

Answer: A

NO.35 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

Answer: C

NO.36 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 administration use?

- (A). RAID 0
- (B). RAID 1
- (C). RAID 5
- (D). RAID 10

Answer: C

<https://techgenix.com/raid-10-vs-raid-5/>

NO.37 Which of the following provides a calculated value for known vulnerabilities so organizations can prioritize mitigation steps?

- (A). CVSS
- (B). SIEM
- (C). SOAR
- (D). CVE

Answer: A

NO.38 A social media company based in North America is looking to expand into new global markets and needs to maintain compliance with international standards. With which of the following is the company's data protection officer MOST likely concerned?

- (A). NIST Framework
- (B). ISO 27001
- (C). GDPR
- (D). PCI-DSS

Answer: C

NO.39 A security analyst is looking for a solution to help communicate to the leadership team the seventy levels of the organization's vulnerabilities. Which of the following would BEST meet this need?

- (A). CVE
- (B). SIEM
- (C). SOAR
- (D). CVSS

Answer: D

The Common Vulnerability Scoring System (CVSS) is a system widely used in vulnerability management programs. CVSS indicates the severity of an information security vulnerability, and is an integral component of many vulnerability scanning tools.

NO.40 Which of the following describes a social engineering technique that seeks to exploit a person's sense of urgency?

- (A). A phishing email stating a cash settlement has been awarded but will expire soon
- (B). A smishing message stating a package is scheduled for pickup
- (C). A vishing call that requests a donation be made to a local charity
- (D). A SPIM notification claiming to be undercover law enforcement investigating a cybercrime

Answer: A

Phishing

As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.

<https://www.imperva.com/learn/application-security/social-engineering-attack/#:~:text=Phishing,curiosity%20or%20fear%20in%20victims>.

NO.41 Which of the following is an example of transference of risk?

- (A). Purchasing insurance
- (B). Patching vulnerable servers
- (C). Retiring outdated applications
- (D). Application owner risk sign-off

Answer: A

NO.42 Which of the following describes the continuous delivery software development methodology?

- (A). Waterfall
- (B). Spiral
- (C). V-shaped
- (D). Agile

Answer: D

NO.43 During a security incident investigation, an analyst consults the company's SIEM and sees an event concerning high traffic to a known, malicious command-and-control server. The analyst would like to determine the number of company workstations that may be impacted by this issue. Which of the following can provide the information?

- (A). WAF logs
- (B). DNS logs
- (C). System logs
- (D). Application logs

Answer: C

NO.44 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.

Answer: D

NO.45 Which of the following documents provides guidance regarding the recommended deployment of network security systems from the manufacturer?

- (A). Cloud control matrix
- (B). Reference architecture
- (C). NIST RMF
- (D). CIS Top 20

Answer: C

NO.46 Which of the following would be the BEST way to analyze diskless malware that has infected a VDI?

- (A). Shut down the VDI and copy off the event logs.
- (B). Take a memory snapshot of the running system.
- (C). Use NetFlow to identify command-and-control IPs.
- (D). Run a full on-demand scan of the root volume.

Answer: B

NO.47 Digital signatures use asymmetric encryption. This means the message is encrypted with:

- (A). the sender's private key and decrypted with the sender's public key
- (B). the sender's public key and decrypted with the sender's private key
- (C). the sender's private key and decrypted with the recipient's public key.
- (D). the sender's public key and decrypted with the recipient's private key

Answer: B

NO.48 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

Answer: C

NO.49 A company discovered that terabytes of data have been exfiltrated over the past year after an employee clicked on an email link. The threat continued to evolve and remain undetected until a security analyst noticed an abnormal amount of external connections when the employee was not working. Which of the following is the MOST likely threat actor?

- (A). Shadow IT
- (B). Script kiddies
- (C). APT
- (D). Insider threat

Answer: C

NO.50 During a recent security incident at a multinational corporation a security analyst found the following logs for an account called user:

Account	Login location	Time (UTC)	Message
user	New York	9:00 a.m.	Login: user, successful
user	Los Angeles	9:01 a.m.	Login: user, successful
user	Sao Paulo	9:05 a.m.	Login: user, successful
user	Munich	9:12 a.m.	Login: user, successful

Which Of the following account policies would BEST prevent attackers from logging in as user?

- (A). Impossible travel time
- (B). Geofencing
- (C). Time-based logins
- (D). Geolocation

Answer: A

NO.51 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 account to the account and pivot through the global network. Which of the following would be BEST to help mitigate this concern?

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

Answer: C

<https://www.crowdstrike.com/blog/service-accounts-performing-interactive-logins/>

NO.52 Which of the following employee roles is responsible for protecting an organization's collected personal information?

- (A). CTO
- (B). DPO
- (C). CEO
- (D). DBA

Answer: B

Many companies also have a data protection officer or DPO. This is a higher-level manager who is responsible for the organization's overall data privacy policies.

<https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-roles-and-responsibilities/#:~:text=Many%20companies%20also%20have%20a,organization's%20overall%20data%20privacy%20policies.>

NO.53 A user is attempting to navigate to a website from inside the company network using a desktop. When the user types in the URL. <https://www.site.com>, the user is presented with a certificate mismatch warning from the browser. The user does not receive a warning when visiting <http://www.anothersite.com>. Which of the following describes this attack?

- (A). On-path
- (B). Domain hijacking
- (C). DNS poisoning
- (D). Evil twin

Answer: C

NO.54 A Chief Information Security Officer wants to ensure the organization is validating and checking the Integrity of zone transfers. Which of the following solutions should be implemented?

- (A). DNSSEC
- (B). LOAPS
- (C). NGFW
- (D). DLP

Answer: D

NO.55 Which of the following is the MOST relevant security check to be performed before embedding third-party libraries in developed code?

- (A). Check to see if the third party has resources to create dedicated development and staging environments.
- (B). Verify the number of companies that downloaded the third-party code and the number of contributions on the code repository.
- (C). Assess existing vulnerabilities affecting the third-party code and the remediation efficiency of the libraries' developers.
- (D). Read multiple penetration-testing reports for environments running software that reused the library.

Answer: C

NO.56 A new company wants to avoid channel interference when building a WLAN. The company needs to know the radio frequency behavior, identify dead zones, and determine the best place for access points. Which of the following should be done FIRST?

- (A). Configure heat maps.
- (B). Utilize captive portals.
- (C). Conduct a site survey.
- (D). Install Wi-Fi analyzers.

Answer: A

NO.57 An administrator is experiencing issues when trying to upload a support file to a vendor. A pop-up message reveals that a payment card number was found in the file, and the file upload was Mocked. Which of the following controls is most likely causing this issue and should be checked FIRST?

- (A). DLP
- (B). Firewall rule
- (C). Content filter
- (D). MDM
- (E). Application allow list

Answer: A

NO.58 An attacker replaces a digitally signed document with another version that goes unnoticed. Upon reviewing the document's contents, the author notices some additional verbiage that was not originally in the document but can't validate an integrity issue. Which of the following attacks was used?

- (A). Cryptomalware
- (B). Prepending
- (C). Collision
- (D). Phishing

Answer: C

NO.59 A DBA reports that several production server hard drives were wiped over the weekend. The DBA also reports that several Linux servers were unavailable due to system files being deleted unexpectedly. A security analyst verified that software was configured to delete data deliberately from those servers. No backdoors to any servers were found. Which of the following attacks was MOST likely used to cause the data loss?

- (A). Logic bomb
- (B). Ransomware
- (C). Fileless virus
- (D). Remote access Trojans
- (E). Rootkit

Answer: A

NO.60 An engineer recently deployed a group of 100 web servers in a cloud environment. Per the security policy, all web-server ports except 443 should be disabled. Which of the following can be used to accomplish this task?

- (A). Application allow list
- (B). SWG
- (C). Host-based firewall
- (D). VPN

FAST2TEST.COM

Answer: B

NO.61 A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

- (A). Segmentation
- (B). Firewall whitelisting
- (C). Containment
- (D). isolation

Answer: A

NO.62 A security analyst is designing the appropriate controls to limit unauthorized access to a physical site. The analyst has a directive to utilize the lowest possible budget. Which of the following would BEST meet the requirements?

- (A). Preventive controls
- (B). Compensating controls
- (C). Deterrent controls
- (D). Detective controls

Answer: C

NO.63 A help desk technician receives a phone call from someone claiming to be a part of the organization's cybersecurity incident response team. The caller asks the technician to verify the network's internal firewall IP address. Which of the following is the technician's BEST course of action?

- (A). Direct the caller to stop by the help desk in person and hang up declining any further requests from the caller
- (B). Ask for the caller's name, verify the person's identity in the email directory and provide the requested information over the phone
- (C). Write down the phone number of the caller if possible, the name of the person requesting the information hang up, and notify the organization's cybersecurity officer
- (D). Request the caller send an email for identity verification and provide the requested information via email to the caller

Answer: D

NO.64 An amusement park is implementing a biometric system that validates customers' fingerprints to ensure they are not sharing tickets. The park's owner values customers above all and would prefer customers' convenience over security. For this reason, which of the following features should the security team prioritize FIRST?

- (A). Low FAR
- (B). Low efficacy

- (C). Low FRR
- (D). Low CER

Answer: C

NO.65 Which of the following is assured when a user signs an email using a private key?

- (A). Non-repudiation
- (B). Confidentiality
- (C). Availability
- (D). Authentication

Answer: A

NO.66 A security analyst is working on a project to implement a solution that monitors network communications and provides alerts when abnormal behavior is detected Which of the following is the security analyst MOST likely implementing?

- (A). Vulnerability scans
- (B). User behavior analysis
- (C). Security orchestration, automation, and response
- (D). Threat hunting

Answer: B

NO.67 A company suspects that some corporate accounts were compromised. The number of suspicious logins from locations not recognized by the users is increasing Employees who travel need their accounts protected without the risk of blocking legitimate login requests that may be made over new sign-in properties. Which of the following security controls can be implemented?

- (A). Enforce MFA when an account request reaches a risk threshold
- (B). Implement geofencing to only allow access from headquarters
- (C). Enforce time-based login requests that align with business hours
- (D). Shift the access control scheme to a discretionary access control

Answer: B

NO.68 An organization would like to give remote workers the ability to use applications hosted inside the corporate network Users will be allowed to use their personal computers or they will be provided organization assets Either way no data or applications will be installed locally on any user systems Which of the following mobile solutions would accomplish these goals?

- (A). VDI
- (B). MDM
- (C). COPE
- (D). UTM

Answer: A

NO.69 During a recent security assessment, a vulnerability was found in a common OS, The OS vendor was unaware of the issue and promised to release a patch within next quarter, Which of the following BEST describes this type of vulnerability?

- (A). Legacy operating system
- (B). Weak configuration
- (C). Zero day

(D). Supply chain

Answer: C

NO.70 Data exfiltration analysis indicates that an attacker managed to download system configuration notes from a web server. The web-server logs have been deleted, but analysts have determined that the system configuration notes were stored in the database administrator's folder on the web server Which of the following attacks explains what occurred? (Select TWO)

- (A). Pass-the- hash
- (B). Directory traversal
- (C). SQL injection
- (D). Privilege escalation
- (E). Cross-site scripting
- (F). Request forgery

Answer: A,D

NO.71 An incident has occurred in the production environment.

Analyze the command outputs and identify the type of compromise.

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

The screenshot shows a simulation interface with two tabs: 'Command output 1' and 'Command output 2'. The 'Command output 1' tab is active, displaying the following command sequence and output:

```
$ cat /var/log/www/file.sh
#!/bin/bash

user=$(grep john /etc/passwd)
if [ $user = "" ]; then
  mysql -u root -p mys3cr3tdbpw -e "drop database production"
fi

$ crontab -l
*/5 * * * * /var/log/www/file.sh
```

On the right side, there is a panel titled 'Compromise Type 1' with a list of options, each with a radio button:

- ☐ Logic bomb
- ☐ Backdoor
- ☐ RAT
- ☐ SQL injection
- ☐ Rootkit

```

Command output 1  Command output 2
$ cat /var/log/www/file.sh
#!/bin/bash

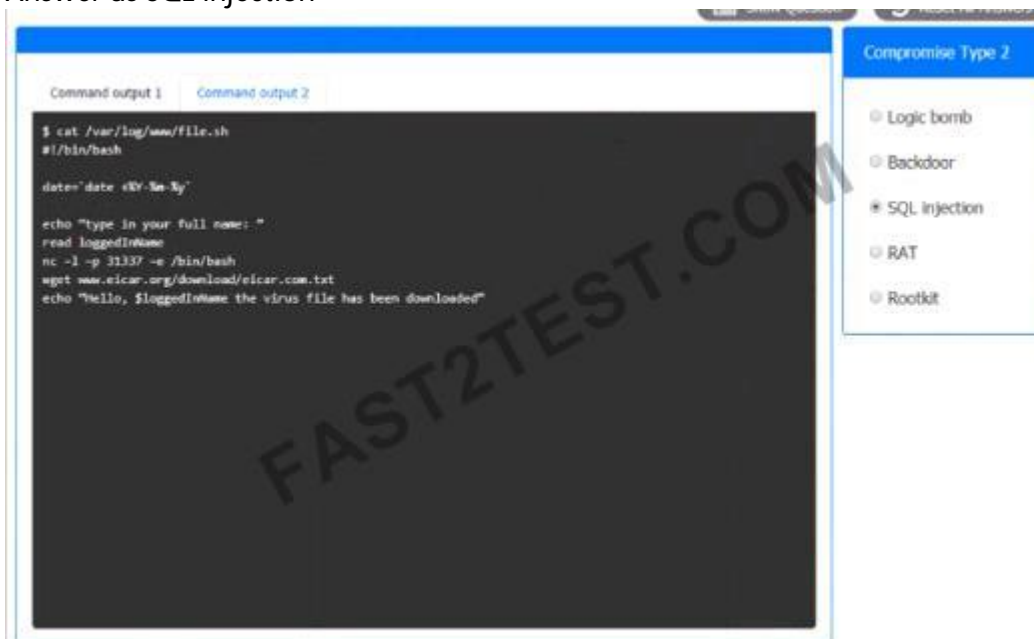
date=`date +%Y-%m-%y`

echo "type in your full name: "
read loggedInName
nc -l -p 31337 -e /bin/bash
wget www.eicar.org/download/eicar.com.txt
echo "Hello, $loggedInName the virus file has been downloaded"

```

Answer:

Answer as SQL injection



NO.72 A security analyst reviews the datacenter access logs for a fingerprint scanner and notices an abundance of errors that correlate with users' reports of issues accessing the facility. Which of the following MOST likely the cause of the cause of the access issues?

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

Answer: A

where a legitimate user is not recognized. This is also referred to as a Type I error or false non-match

rate (FNMR). FRR is measured as a percentage.

NO.73 A security analyst is reviewing application logs to determine the source of a breach and locates the following log:

```
https://www.comptia.com/login.php?id='%20or%20'1'1='1
```

Which Of the following has been observed?

- (A). DLL Injection
- (B). API attack
- (C). SQLI
- (D). XSS

Answer: C

NO.74 An analyst receives multiple alerts for beaconing activity for a host on the network, After analyzing the activity, the analyst observes the following activity:

- * A user enters comptia.org into a web browser.
- * The website that appears is not the comptia.org site.
- * The website is a malicious site from the attacker.
- * Users in a different office are not having this issue.

Which of the following types of attacks was observed?

- (A). On-path attack
- (B). DNS poisoning
- (C). Locator (URL) redirection
- (D). Domain hijacking

Answer: C

NO.75 A security forensics analyst is examining a virtual server. The analyst wants to preserve the present state of the virtual server, including memory contents Which of the following backup types should be used?

- (A). Snapshot
- (B). Differential
- (C). Cloud
- (D). Full
- (E). Incremental

Answer: A

NO.76 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

Answer: C

Password spraying is a type of brute-force attack in which a malicious actor uses a single password against targeted user accounts before moving on to attempt a second password, and so on. This technique allows the actor to remain undetected by avoiding rapid or frequent account lockouts. <https://us-cert.cisa.gov/ncas/current-activity/2019/08/08/acsc-releases-advisory-password-spraying-attacks#:~:text=Password%20spraying%20is%20a%20type,rapid%20or%20frequent%20account%20lockouts.>

NO.77 Which of the following control Types would be BEST to use in an accounting department to reduce losses from fraudulent transactions?

- (A). Recovery
- (B). Deterrent
- (C). Corrective
- (D). Detective

Answer: D

NO.78 A systems administrator is troubleshooting a server's connection to an internal web server. The administrator needs to determine the correct ports to use. Which of the following tools BEST shows which ports on the web server are in a listening state?

- (A). Ipconfig
- (B). ssh
- (C). Ping
- (D). Netstat

Answer: D

<https://www.sciencedirect.com/topics/computer-science/listening-port>

NO.79 An attacker has successfully exfiltrated several non-salted password hashes from an online system. Given the logs below:

```

Session           : hashcat
Status            : cracked
Hash.Type         : MD5
Hash.Target       : b3b81d1b7a412bf5aab3a507d0a586a0
Time.Started      : Fri Mar 10 10:18:45 2020
Recovered         : 1/1 (100%) Digests
Progress          : 28756845 / 450365879 (6.38%) hashes
Time.Stopped      : Fri Mar 10 10:20:12 2020
Password found    : Th3B3stP@55w0rd!

```

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

- (A). Dictionary
- (B). Pass-the-hash
- (C). Brute-force

(D). Password spraying

Answer: A

NO.80 DRAG DROP

An attack has occurred against a company.

INSTRUCTIONS

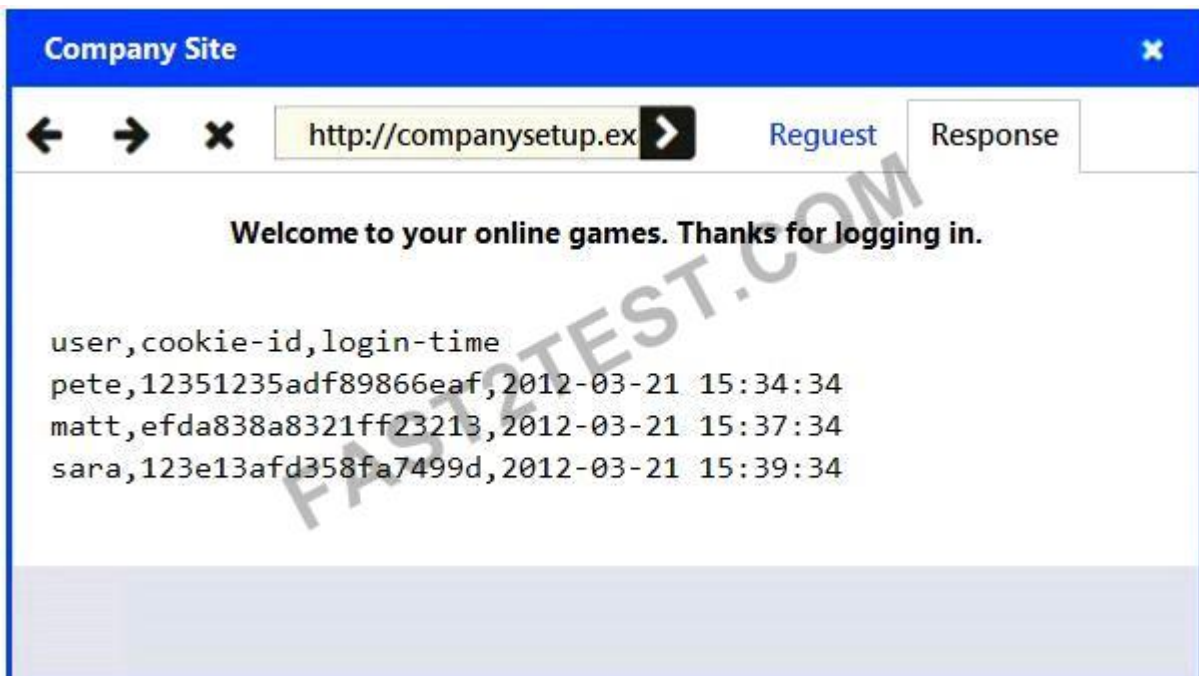
You have been tasked to do the following:

Identify the type of attack that is occurring on the network by clicking on the attacker's tablet and reviewing the output. (Answer Area 1).

Identify which compensating controls should be implemented on the assets, in order to reduce the effectiveness of future attacks by dragging them to the correct server.

(Answer area 2) All objects will be used, but not all placeholders may be filled. Objects may only be used once.

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



Answer Area 1

SQL Injection

Cross Site Scripting

XML Injection

Session Hijacking

Type of attack



Answer Area 2

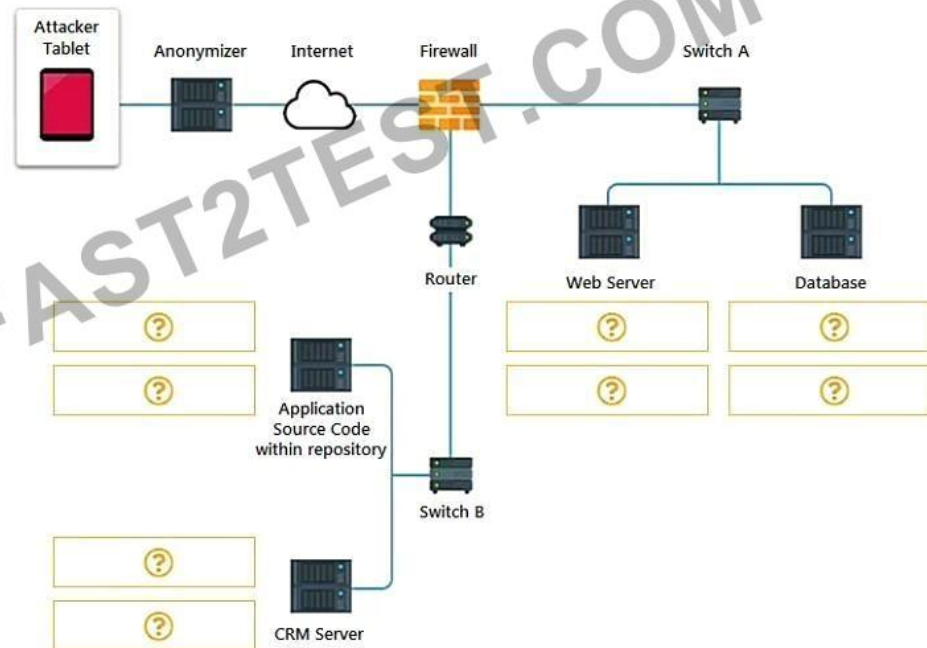
Input Validation

Code Review

WAF

URL Filtering

Record level access control

**Answer:**

Network Diagram

Show Question

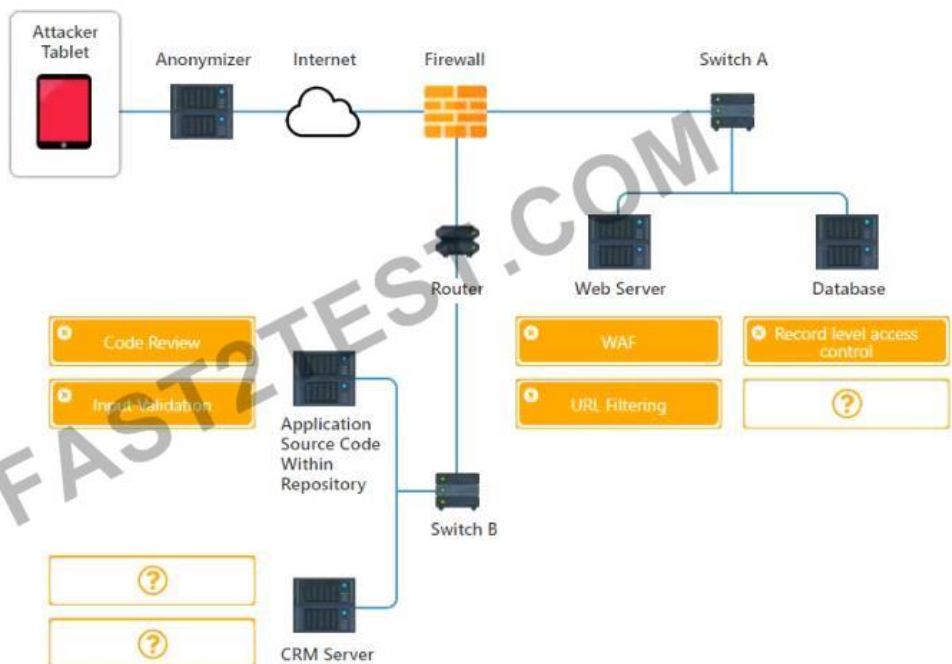
Reset All Answers

Drag & Drop

All attack mitigations have been used

Select type of attack

- ☒ SQL Injection
- ☐ Cross Site Scripting
- ☐ XML Injection
- ☐ Session Hijacking



NO.81 An organization that is located in a flood zone is MOST likely to document the concerns associated with the restoration of IT operation in a:

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

Answer: C

NO.82 DDoS attacks are causing an overload on the cluster of cloud servers. A security architect is researching alternatives to make the cloud environment respond to load fluctuation in a cost-effective way. Which of the following options BEST fulfils the architect's requirements?

- (A). An orchestration solution that can adjust scalability of cloud assets
- (B). Use of multipath by adding more connections to cloud storage
- (C). Cloud assets replicated on geographically distributed regions
- (D). An on-site backup that is deployed and only used when the load increases

Answer: A

NO.83 Which of the following would BEST provide detective and corrective controls for thermal regulation?

- (A). A smoke detector
- (B). A fire alarm
- (C). An HVAC system
- (D). A fire suppression system
- (E). Guards

Answer: C

NO.84 The board of directors at a company contracted with an insurance firm to limit the organization's liability. Which of the following risk management practices does the BEST describe?

- (A). Transference
- (B). Avoidance
- (C). Mitigation
- (D). Acknowledgement

Answer: A

NO.85 After a recent security breach a security analyst reports that several administrative usernames and passwords are being sent via cleartext across the network to access network devices over port 23. Which of the following should be implemented so all credentials sent over the network are encrypted when remotely accessing and configuring network devices?

- (A). SSH
- (B). SNMPv3
- (C). SFTP
- (D). Telnet
- (E). FTP

Answer: A

NO.86 An engineer wants to inspect traffic to a cluster of web servers in a cloud environment. Which

of the following solutions should the engineer implement?

- (A). Proxy server
- (B). WAF
- (C). Load balancer
- (D). VPN

Answer: B

NO.87 A business operations manager is concerned that a PC that is critical to business operations will have a costly hardware failure soon. The manager is looking for options to continue business operations without incurring large costs. Which of the following would mitigate the manager's concerns?

- (A). Implement a full system upgrade
- (B). Perform a physical-to-virtual migration
- (C). Install uninterruptible power supplies
- (D). Purchase cybersecurity insurance

Answer: B

NO.88 An organization has decided to purchase an insurance policy because a risk assessment determined that the cost to remediate the risk is greater than the five-year cost of the insurance policy. The organization is enabling risk

- (A). avoidance
- (B). acceptance
- (C). mitigation
- (D). transference

Answer: D

NO.89 Which of the following techniques eliminates the use of rainbow tables for password cracking?

- (A). Hashing
- (B). Tokenization
- (C). Asymmetric encryption
- (D). Salting

Answer: D

Rainbow table attacks can easily be prevented by using salt techniques, which is a random data that is passed into the hash function along with the plain text.

NO.90 Which of the following terms describes a broad range of information that is sensitive to a specific organization?

- (A). Public
- (B). Top secret
- (C). Proprietary
- (D). Open-source

Answer: C

NO.91 A company is implementing BYOD and wants to ensure all users have access to the same cloud-based services. Which of the following would BEST allow the company to meet this

requirement?

- (A). IaaS
- (B). PaaS
- (C). MaaS
- (D). SaaS

Answer: B

NO.92 A company is required to continue using legacy software to support a critical service. Which of the following BEST explains a risk of this practice?

- (A). Default system configuration
- (B). Unsecure protocols
- (C). Lack of vendor support
- (D). Weak encryption

Answer: B

NO.93 A company wants to restrict emailing of PHI documents. The company is implementing a DLP solution. In order to restrict PHI documents which of the following should be performed FIRST?

- (A). Retention
- (B). Governance
- (C). Classification
- (D). Change management

Answer: C

NO.94 Which of the following is the BEST action to foster a consistent and auditable incident response process?

- (A). Incent new hires to constantly update the document with external knowledge.
- (B). Publish the document in a central repository that is easily accessible to the organization.
- (C). Restrict eligibility to comment on the process to subject matter experts of each IT silo.
- (D). Rotate CIRT members to foster a shared responsibility model in the organization.

Answer: D

NO.95 A company recently experienced a significant data loss when proprietary information was leaked to a competitor. The company took special precautions by using proper labels; however, email filter logs do not have any record of the incident. An investigation confirmed the corporate network was not breached, but documents were downloaded from an employee's COPE tablet and passed to the competitor via cloud storage. Which of the following is the BEST remediation for this data leak?

- (A). User training
- (B). CASB
- (C). MDM
- (D). DLP

Answer: D

NO.96 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

Answer: D

<https://www.enterprisestorageforum.com/management/rpo-and-rto-understanding-the-differences/>

NO.97 A company wants to simplify the certificate management process. The company has a single domain with several dozen subdomains, all of which are publicly accessible on the internet. Which of the following BEST describes the type of certificate the company should implement?

- (A). Subject alternative name
- (B). Wildcard
- (C). Self-signed
- (D). Domain validation

Answer: B

Wildcard SSL certificates are for a single domain and all its subdomains. A subdomain is under the umbrella of the main domain. Usually subdomains will have an address that begins with something other than 'www.' For example, www.cloudflare.com has a number of subdomains, including blog.cloudflare.com, support.cloudflare.com, and developers.cloudflare.com. Each is a subdomain under the main cloudflare.com domain.

A single Wildcard SSL certificate can apply to all of these subdomains. Any subdomain will be listed in the SSL certificate. Users can see a list of subdomains covered by a particular certificate by clicking on the padlock in the URL bar of their browser, then clicking on "Certificate" (in Chrome) to view the certificate's details.

<https://www.cloudflare.com/learning/ssl/types-of-ssl-certificates/>

NO.98 Which of the following is the MOST effective way to detect security flaws present on third-party libraries embedded on software before it is released into production?

- (A). Employ different techniques for server- and client-side validations.
- (B). Use a different version control system for third-party libraries.
- (C). Implement a vulnerability scan to assess dependencies earlier on SDLC.
- (D). Increase the number of penetration tests before software release.

Answer: D

NO.99 Due to unexpected circumstances, an IT company must vacate its main office, forcing all operations to alternate, off-site locations. Which of the following will the company MOST likely reference for guidance during this change?

- (A). The business continuity plan
- (B). The retention policy
- (C). The disaster recovery plan
- (D). The incident response plan

Answer: A

NO.100 Which of the following control types fixes a previously identified issue and mitigates a risk?

- (A). Detective
- (B). Corrective
- (C). Preventative
- (D). Finalized

FAST2TEST.COM

Answer: B

NO.101 Which of the following is an example of risk avoidance?

- (A). Installing security updates directly in production to expedite vulnerability fixes
- (B). Buying insurance to prepare for financial loss associated with exploits
- (C). Not installing new software to prevent compatibility errors
- (D). Not taking preventive measures to stop the theft of equipment

Answer: C

NO.102 A security analyst was called to investigate a file received directly from a hardware manufacturer. The analyst is trying to determine whether modified in transit before installation on the user's computer. Which of the following can be used to safely assess the file?

- (A). Check the hash of the installation file
- (B). Match the file names
- (C). Verify the URL download location
- (D). Verify the code-signing certificate

Answer: A

NO.103 A security incident may have occurred on the desktop PC of an organization's Chief Executive Officer (CEO). A duplicate copy of the CEO's hard drive must be stored securely to ensure appropriate forensic processes and the chain of custody are followed. Which of the following should be performed to accomplish this task?

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

Answer: B

"To obtain a forensically sound image from nonvolatile storage, you need to ensure that nothing you do alters data or metadata (properties) on the source disk or file system. A write blocker assures this process by preventing any data on the disk or volume from being changed by filtering write commands at the driver and OS level. Data acquisition would normally proceed by attaching the target device to a forensics workstation or field capture device equipped with a write blocker." For purposes of knowing, <https://security.opentext.com/tableau/hardware/details/t8u> write blockers like this are the most popular hardware blockers

NO.104 During a recent penetration test, the tester discovers large amounts of data were exfiltrated over the course of 12 months via the internet. The penetration tester stops the test to inform the client of the findings. Which of the following should be the client's NEXT step to mitigate the issue?"

- (A). Conduct a full vulnerability scan to identify possible vulnerabilities
- (B). Perform containment on the critical servers and resources
- (C). Review the firewall and identify the source of the active connection
- (D). Disconnect the entire infrastructure from the internet

Answer: B

NO.105 A systems administrator reports degraded performance on a virtual server. The administrator increases the virtual memory allocation which improves conditions, but performance degrades again after a few days. The administrator runs an analysis tool and sees the following output:

```
==3214== timeAttend.exe analyzed
==3214== ERROR SUMMARY:
==3214== malloc/free: in use at exit: 4608 bytes in 18 blocks.
==3214== checked 3215 bytes
==3214== definitely lost: 4608 bytes in 18 blocks.
```

The administrator terminates the timeAttend.exe, observes system performance over the next few days, and notices that the system performance does not degrade. Which of the following issues is MOST likely occurring?

- (A). DLL injection
- (B). API attack
- (C). Buffer overflow
- (D). Memory leak

Answer: C

NO.106 Which of the following uses SAML for authentication?

- (A). TOTP
- (B). Federation
- (C). Kerberos
- (D). HOTP

Answer: B

NO.107 An attacker has determined the best way to impact operations is to infiltrate third-party software vendors. Which of the following vectors is being exploited?

- (A). Social media
- (B). Cloud
- (C). Supply chain
- (D). Social engineering

Answer: D

NO.108 Which of the following can work as an authentication method and as an alerting mechanism for unauthorized access attempts?

- (A). Smart card
- (B). push notifications
- (C). Attestation service
- (D). HMAC-based, one-time password

Answer: B

NO.109 Which of the following organizations sets frameworks and controls for optimal security configuration on systems?

- (A). ISO
- (B). GDPR
- (C). PCI DSS
- (D). NIST

Answer: D

NO.110 An organization is planning to open other data centers to sustain operations in the event of a natural disaster. Which of the following considerations would BEST support the organization's resiliency?

- (A). Geographic dispersal
- (B). Generator power
- (C). Fire suppression
- (D). Facility automation

Answer: A

NO.111 When selecting a technical solution for identity management, an architect chooses to go from an in-house to a third-party SaaS provider. Which of the following risk management strategies is this an example of?

- (A). Acceptance
- (B). Mitigation
- (C). Avoidance
- (D). Transference

Answer: D

Risk Transference refers to the shifting of the burden of loss for a risk to another party through legislation, contract, insurance or other means. https://www.bcmppedia.org/wiki/Risk_Transference

NO.112 Which of the following prevents an employee from seeing a colleague who is visiting an inappropriate website?

- (A). Job rotation policy
- (B). NDA
- (C). AUP
- (D). Separation Of duties policy

Answer: D

NO.113 In the middle of a cybersecurity, a security engineer removes the infected devices from the network and lock down all compromised accounts. In which of the following incident response phases is the security engineer currently operating?

- (A). Identification
- (B). Preparation
- (C). Eradication
- (D). Recovery
- (E). Containment

Answer: E

Isolation involves removing affected components from any environment the greater one. This can be

anything from removing the server from the network after become the target of DoS attacks, to the point of placing applications in a VM sandbox outside the environment where the host usually runs. Whatever the situation, you'll want to make sure you don't there is another Interface between the affected component and the production network or the Internet.

NO.114 A company is under investigation for possible fraud. As part of the investigation. the authorities need to review all emails and ensure data is not deleted.

Which of the following should the company implement to assist in the investigation?

- (A). Legal hold
- (B). Chain of custody
- (C). Data loss prevention
- (D). Content filter

Answer: C

NO.115 Which of the following typically uses a combination of human and artificial intelligence to analyze event data and take action without intervention?

- (A). TTP
- (B). OSINT
- (C). SOAR
- (D). SIEM

Answer: D

NO.116 A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?

- (A). A non-disclosure agreement
- (B). Least privilege
- (C). An acceptable use policy
- (D). Ofboarding

Answer: D

NO.117 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

Answer: D

NO.118 An untrusted SSL certificate was discovered during the most recent vulnerability scan. A security analyst determines the certificate is signed properly and is a valid wildcard. This same certificate is installed on other company servers without issue. Which of the following is the MOST likely reason for this finding?

- (A). The required intermediate certificate is not loaded as part of the certificate chain.

- (B). The certificate is on the CRL and is no longer valid.
- (C). The corporate CA has expired on every server, causing the certificate to fail verification.
- (D). The scanner is incorrectly configured to not trust this certificate when detected on the server.

Answer: A

NO.119 Several users have opened tickets with the help desk. The help desk has reassigned the tickets to a security analyst for further review. The security analyst reviews the following metrics:

Hostname	Normal CPU utilization %	Current CPU utilization %	Normal network connections	Current network connections
Accounting-PC	22%	48%	12	66
HR-PC	35%	55%	15	57
IT-PC	78%	98%	25	92
Sales-PC	28%	50%	20	56
Manager-PC	21%	44%	18	49

Which of the following is MOST likely the result of the security analyst's review?

- (A). The ISP is dropping outbound connections
- (B). The user of the Sales-PC fell for a phishing attack
- (C). Corporate PCs have been turned into a botnet
- (D). An on-path attack is taking place between PCs and the router

Answer: D

NO.120 A company is receiving emails with links to phishing sites that look very similar to the company's own website address and content. Which of the following is the BEST way for the company to mitigate this attack?

- (A). Create a honeynet to trap attackers who access the VPN with credentials obtained by phishing.
- (B). Generate a list of domains similar to the company's own and implement a DNS sinkhole for each.
- (C). Disable POP and IMAP on all Internet-facing email servers and implement SMTPS.
- (D). Use an automated tool to flood the phishing websites with fake usernames and passwords.

Answer: B

NO.121 A security manager has tasked the security operations center with locating all web servers that respond to an unsecure protocol. Which of the following commands could an analyst run to find requested servers?

- (A). nslookup 10.10.10.0
- (B). nmap -p 80 10.10.10.0/24
- (C). pathping 10.10.10.0 -p 80
- (D). no -1 -p 80

Answer: C

NO.122 Server administrators want to configure a cloud solution so that computing memory and processor usage is maximized most efficiently across a number of virtual servers. They also need to avoid potential denial-of-service situations caused by availability. Which of the following should administrators configure to maximize system availability while efficiently utilizing available computing power?

- (A). Dynamic resource allocation
- (B). High availability
- (C). Segmentation

(D). Container security

Answer: A

NO.123 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.

Answer: A

The reason the company had to pay the ransom is because they did not have valid backups, otherwise they would have just restored their data. If your company just had to pay ransom and your boss says, "Don't let this happen again", what is the first thing you are going to do. The only action after a ransomware attack is "restore from backup".

NO.124 A system administrator needs to implement an access control scheme that will allow an object's access policy be determined by its owner. Which of the following access control schemes BEST fits the requirements?

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

Answer: B

Discretionary access control (DAC) is a model of access control based on access being determined "by the owner" of the resource in question. The owner of the resource can decide who does and does not have access, and exactly what access they are allowed to have.

NO.125 Which of the following is the BEST example of a cost-effective physical control to enforce a USB removable media restriction policy?

- (A). Putting security/antitamper tape over USB ports logging the port numbers and regularly inspecting the ports
- (B). Implementing a GPO that will restrict access to authorized USB removable media and regularly verifying that it is enforced
- (C). Placing systems into locked key-controlled containers with no access to the USB ports
- (D). Installing an endpoint agent to detect connectivity of USB and removable media

Answer: B

NO.126 A security engineer is concerned about using an agent on devices that relies completely on defined known-bad signatures. The security engineer wants to implement a tool with multiple components including the ability to track, analyze, and monitor devices without reliance on definitions alone. Which of the following solutions BEST fits this use case?

- (A). EDR
- (B). DLP

- (C). NGFW
- (D). HIPS

Answer: A

The acronym EDR stands for Endpoint Detection and Response and is also known as EDTR. It is an endpoint security solution that is responsible for continuous monitoring of endpoints. This permanent monitoring enables the technology to detect and respond to cyber threats such as malware or ransomware at an early stage. The basis for this is always the analysis of context-related information, which can be used to make corrective proposals for recovery.

NO.127 Which of the following would detect intrusions at the perimeter of an airport?

- (A). Signage
- (B). Fencing
- (C). Motion sensors
- (D). Lighting
- (E). Bollards

Answer: C

NO.128 A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicates a directory-traversal attack has occurred. Which of the following is the analyst MOST likely seeing?

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)

- (A). Option A
- (B). Option B
- (C). Option C
- (D). Option D

Answer: B

NO.129 Which of the following is a security best practice that ensures the integrity of aggregated log files within a SIEM?

- (A). Set up hashing on the source log file servers that complies with local regulatory requirements,
- (B). Back up the aggregated log files at least two times a day or as stated by local regulatory requirements.
- (C). Write protect the aggregated log files and move them to an isolated server with limited access.
- (D). Back up the source log files and archive them for at least six years or in accordance with local regulatory requirements.

Answer: A

NO.130 A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better.

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

Answer: D

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

NO.131 A user recent an SMS on a mobile phone that asked for bank delays. Which of the following social-engineering techniques was used in this case?

- (A). SPIM
- (B). Vishing
- (C). Spear phishing
- (D). Smishing

Answer: D

NO.132 A global pandemic is forcing a private organization to close some business units and reduce staffing at others. Which of the following would be BEST to help the organization's executives determine the next course of action?

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

Answer: D

Business continuity may be defined as "the capability of an organization to continue the delivery of products or services at pre-defined acceptable levels following a disruptive incident", [1] and business continuity planning [2][3] (or business continuity and resiliency planning) is the process of creating systems of prevention and recovery to deal with potential threats to a company. [4] In addition to prevention, the goal is to enable ongoing operations before and during execution of disaster recovery. [5] Business continuity is the intended outcome of proper execution of both business continuity planning and disaster recovery.

NO.133 Which of the following is used to ensure that evidence is admissible in legal proceedings when it is collected and provided to the authorities?

- (A). Chain of custody
- (B). Legal hold
- (C). Event log
- (D). Artifacts

Answer: A

NO.134 While investigating a recent security incident, a security analyst decides to view all network connections on a particular server, Which of the following would provide the desired information?

- (A). arp
- (B). nslookup

- (C). netstat
- (D). nmap

Answer: C

NO.135 Which of the following in the incident response process is the BEST approach to improve the speed of the identification phase?

- (A). Activate verbose logging in all critical assets.
- (B). Tune monitoring in order to reduce false positive rates.
- (C). Redirect all events to multiple syslog servers.
- (D). Increase the number of sensors present on the environment.

Answer: A

NO.136 Which of the following risk management strategies would an organization use to maintain a legacy system with known risks for operational purposes?

- (A). Acceptance
- (B). Transference
- (C). Avoidance
- (D). Mitigation

Answer: A

NO.137 A security analyst is receiving several alerts per user and is trying to determine if various logins are malicious. The security analyst would like to create a baseline of normal operations and reduce noise. Which of the following actions should the security analyst perform?

- (A). Adjust the data flow from authentication sources to the SIEM.
- (B). Disable email alerting and review the SIEM directly.
- (C). Adjust the sensitivity levels of the SIEM correlation engine.
- (D). Utilize behavioral analysis to enable the SIEM's learning mode.

Answer: C

NO.138 Which of the following is a team of people dedicated testing the effectiveness of organizational security programs by emulating the techniques of potential attackers?

- (A). Red team
- (B). White team
- (C). Blue team
- (D). Purple team

Answer: A

Red team-performs the offensive role to try to infiltrate the target.

NO.139 A security analyst wants to fingerprint a web server. Which of the following tools will the security analyst MOST likely use to accomplish this task?

- (A). nmap -p1-65535 192.168.0.10
- (B). dig 192.168.0.10
- (C). curl --head http://192.168.0.10
- (D). ping 192.168.0.10

Answer: C

NO.140 A network engineer created two subnets that will be used for production and development servers. Per security policy, production and development servers must each have a dedicated network that cannot communicate with one another directly. Which of the following should be deployed so that server administrators can access these devices?

- (A). VLANs
- (B). Internet proxy servers
- (C). NIDS
- (D). Jump servers

FAST2TEST.COM

Answer: D

NO.141 A company has determined that if its computer-based manufacturing 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 to maintain a positive total cost of ownership?

- (A). MTBF
- (B). RPO
- (C). RTO
- (D). MTTR

Answer: C

NO.142 A security analyst generated a file named host1.pcap and shared it with a team member who is going to use it for further incident analysis. Which of the following tools will the other team member MOST likely use to open this file?

- (A). Autopsy
- (B). Memdump
- (C). FTK imager
- (D). Wireshark

Answer: D

Some common applications that can open .pcap files are Wireshark, WinDump, tcpdump, Packet Square - Capedit and Ethereal.

NO.143 The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve in the environment patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have been provided to frontline staff, and a risk analysis has not been performed. Which of the following is the MOST likely cause of the CRO's concerns?

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

Answer: D

NO.144 Several universities are participating in a collaborative research project and need to share compute and storage resources. Which of the following cloud deployment strategies would BEST meet this need?

- (A). Community

- (B). Private
- (C). Public
- (D). Hybrid

Answer: A

Community cloud storage is a variation of the private cloud storage model, which offers cloud solutions for specific businesses or communities. In this model, cloud storage providers offer their cloud architecture, software and other development tools to meet the requirements of the community. A community cloud in computing is a collaborative effort in which infrastructure is shared between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally.

NO.145 Which of the following will increase cryptographic security?

- (A). High data entropy
- (B). Algorithms that require less computing power
- (C). Longer key longevity
- (D). Hashing

Answer: C

NO.146 A company needs to validate its updated incident response plan using a real-world scenario that will test decision points and relevant incident response actions without interrupting daily operations. Which of the following would BEST meet the company's requirements?

- (A). Red-team exercise
- (B). Capture-the-flag exercise
- (C). Tabletop exercise
- (D). Phishing exercise

Answer: C

NO.147 An attacker browses a company's online job board attempting to find any relevant information regarding the technologies the company uses. Which of the following BEST describes this social engineering technique?

- (A). Hoax
- (B). Reconnaissance
- (C). Impersonation
- (D). pretexting

Answer: A

NO.148 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

Answer: B

<https://ktechproducts.com/Data-mask#:~:text=Data%20Masking%20is%20a%20method%20of%20creating%20a,partial%20data%20ba>

sed%20on%20the%20user%E2%80%99s%20security%20permissions.

The main reason for applying masking to a data field is to protect data that is classified as personally identifiable information, sensitive personal data, or commercially sensitive data. However, the data must remain usable for the purposes of undertaking valid test cycles. It must also look real and appear consistent. It is more common to have masking applied to data that is represented outside of a corporate production system. In other words, where data is needed for the purpose of application development, building program extensions and conducting various test cycles

https://en.wikipedia.org/wiki/Data_masking

NO.149 A routine audit of medical billing claims revealed that several claims were submitted without the subscriber's knowledge. A review of the audit logs for the medical billing company's system indicated a company employee downloaded customer records and adjusted the direct deposit information to a personal bank account. Which of the following does this action describe?

- (A). Insider threat
- (B). Social engineering
- (C). Third-party risk
- (D). Data breach

Answer: A

NO.150 Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases? (Select TWO.)

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

Answer: D,E

NO.151 A security analyst needs to be able to search and correlate logs from multiple sources in a single tool Which of the following would BEST allow a security analyst to have this ability?

- (A). SOAR
- (B). SIEM
- (C). Log collectors
- (D). Network-attached storage

Answer: B

NO.152 A tax organization is working on a solution to validate the online submission of documents The solution should be earned on a portable USB device that should be inserted on any computer that is transmitting a transaction securely. Which of the following is the BEST certificate for these requirements?

- (A). User certificate
- (B). Self-signed certificate
- (C). Computer certificate
- (D). Root certificate

Answer: D

NO.153 Which of the following processes will eliminate data using a method that will allow the storage device to be reused after the process is complete?

- (A). Pulverizing
- (B). Overwriting
- (C). Shredding
- (D). Degaussing

Answer: D

<https://dataspan.com/blog/what-are-the-different-types-of-data-destruction-and-which-one-should-you-use/>

NO.154 A company has limited storage available and online presence that cannot 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, which being mindful of the limited available storage space?

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

Answer: B

NO.155 A company recently experienced an inside attack using a corporate machine that resulted in data compromise. Analysis indicated an unauthorized change to the software circumvented technological protection measures, The analyst was tasked with determining the best method to ensure the integrity of the systems remains intact and local and remote boot attestation can take place. Which of the following would provide the BEST solution?

- (A). HIPS
- (B). Fly
- (C). TPM
- (D). DLP

Answer: C

<https://docs.microsoft.com/en-us/azure/security/fundamentals/measured-boot-host-attestation>

NO.156 A user wanted to catch up on some work over the weekend but had issues logging in to the corporate network using a VPN. On Monday, the user opened a ticket for this issue but was able to log in successfully. Which of the following BEST describes the policy that is being implemented?

- (A). Time-based logins
- (B). Geofencing
- (C). Network location
- (D). Password history

Answer: C

NO.157 While reviewing an alert that shows a malicious request on one web application, a cybersecurity analyst is alerted to a subsequent token reuse moments later on a different service using the same single sign-on method. Which of the following would BEST detect a malicious actor?

- (A). Utilizing SIEM correlation engines

- (B). Deploying Netflow at the network border
- (C). Disabling session tokens for all sites
- (D). Deploying a WAF for the web server

Answer: A

NO.158 A penetration tester is fuzzing an application to identify where the EIP of the stack is located on memory. Which of the following attacks is the penetration tester planning to execute?

- (A). Race-condition
- (B). Pass-the-hash
- (C). Buffer overflow
- (D). XSS

Answer: C

NO.159 A security analyst has identified malware spreading through the corporate network and has activated the CSIRT Which of the following should the analyst do NEXT?

- (A). Review how the malware was introduced to the network.
- (B). Attempt to quarantine all infected hosts to limit further spread.
- (C). Create help desk tickets to get infected systems reimaged.
- (D). Update all endpoint antivirus solutions with the latest updates.

Answer: B

NO.160 A malicious actor recently penetration a company's network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know what was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

- (A). Security
- (B). Application
- (C). Dump
- (D). Syslog

Answer: C

Dump files are a special type of files that store information about your computer, the software on it, and the data loaded in the memory when something bad happens. They are usually automatically generated by Windows or by the apps that crash, but you can also manually generate them

<https://www.digitalcitizen.life/view-contents-dump-file/>

NO.161 A security incident has been resolved Which of the following BEST describes the importance of the final phase of the incident response plan?

- (A). It examines and documents how well the team responded discovers what caused the incident, and determines how the incident can be avoided in the future
- (B). It returns the affected systems back into production once systems have been fully patched, data restored and vulnerabilities addressed
- (C). It identifies the incident and the scope of the breach how it affects the production environment, and the ingress point
- (D). It contains the affected systems and disconnects them from the network, preventing further spread of the attack or breach

Answer: A

NO.162 An attacker was eavesdropping on a user who was shopping online. The attacker was able to spoof the IP address associated with the shopping site. Later, the user received an email regarding the credit card statement with unusual purchases. Which of the following attacks took place?

- (A). On-path attack
- (B). Protocol poisoning
- (C). Domain hijacking
- (D). Bluejacking

Answer: A

NO.163 A security policy states that common words should not be used as passwords. A security auditor was able to perform a dictionary attack against corporate credentials. Which of the following controls was being violated?

- (A). Password complexity
- (B). Password history
- (C). Password reuse
- (D). Password length

Answer: B

NO.164 A Chief Security Officer is looking for a solution that can provide increased scalability and flexibility for back-end infrastructure, allowing it to be updated and modified without disruption to services. The security architect would like the solution selected to reduce the back-end server resources and has highlighted that session persistence is not important for the applications running on the back-end servers. Which of the following would BEST meet the requirements?

- (A). Reverse proxy
- (B). Automated patch management
- (C). Snapshots
- (D). NIC teaming

Answer: A

A reverse proxy would be the best solution for increased scalability and flexibility for back-end infrastructure.

NO.165 A company wants to build a new website to sell products online. The website will host a storefront application that will allow visitors to add products to a shopping cart and pay for the products using a credit card. Which of the following protocols would be the MOST secure to implement?

- (A). SSL
- (B). FTP
- (C). SNMP
- (D). TLS

Answer: A

NO.166 Which of the following concepts BEST describes tracking and documenting changes to software and managing access to files and systems?

- (A). Version control
- (B). Continuous monitoring
- (C). Stored procedures

(D). Automation

Answer: A

<https://www.perforce.com/blog/vcs/what-is-version-control>

NO.167 After gaining access to a dual-homed (i.e.. wired and wireless) multifunction device by exploiting a vulnerability in the device's firmware, a penetration tester then gains shell access on another networked asset. This technique is an example of:

- (A). privilege escalation
- (B). footprinting
- (C). persistence
- (D). pivoting.

Answer: A

NO.168 The Chief Information Security Officer (CISO) has requested that a third-party vendor provide supporting documents that show proper controls are in place to protect customer data. Which of the following would be BEST for the third-party vendor to provide to the CISO?

- (A). GDPR compliance attestation
- (B). Cloud Security Alliance materials
- (C). SOC 2 Type 2 report
- (D). NIST RMF workbooks

Answer: C

NO.169 Which of the following can be used by a monitoring tool to compare values and detect password leaks without providing the actual credentials?

- (A). Hashing
- (B). Tokenization
- (C). Masking
- (D). Encryption

Answer: A

<https://resources.infosecinstitute.com/topic/10-popular-password-cracking-tools/>

NO.170 A security architect is required to deploy to conference rooms some workstations that will allow sensitive data to be displayed on large screens. Due to the nature of the data, it cannot be stored in the conference rooms. The fileshare is located in a local data center. Which of the following should the security architect recommend to BEST meet the requirement?

- (A). Fog computing and KVMs
- (B). VDI and thin clients
- (C). Private cloud and DLP
- (D). Full drive encryption and thick clients

Answer: D

NO.171 A company is looking to migrate some servers to the cloud to minimize its technology footprint. The company has 100 databases that are on premises. Which of the following solutions will require the LEAST management and support from the company?

- (A). SaaS
- (B). IaaS

- (C). PaaS
- (D). SDN

Answer: A

NO.172 A customer service representative reported an unusual text message that was sent to the help desk. The message contained an unrecognized invoice number with a large balance due and a link to click for more details. Which of the following BEST describes this technique?

- (A). Vishing
- (B). Whaling
- (C). Phishing
- (D). Smishing

Answer: D

NO.173 During an incident response, an analyst applied rules to all inbound traffic on the border firewall and implemented ACLs on each critical server. Following an investigation, the company realizes it is still vulnerable because outbound traffic is not restricted and the adversary is able to maintain a presence in the network. In which of the following stages of the Cyber Kill Chain is the adversary currently operating?

- (A). Reconnaissance
- (B). Command and control
- (C). Actions on objective
- (D). Exploitation

Answer: B

NO.174 A user enters a username and a password at the login screen for a web portal. A few seconds later the following message appears on the screen: Please use a combination of numbers, special characters, and letters in the password field. Which of the following concepts does this message describe?

- (A). Password complexity
- (B). Password reuse
- (C). Password history
- (D). Password age

Answer: A

NO.175 An application developer accidentally uploaded a company's code-signing certificate private key to a public web server. The company is concerned about malicious use of its certificate. Which of the following should the company do FIRST?

- (A). Delete the private key from the repository.
- (B). Verify the public key is not exposed as well.
- (C). Update the DLP solution to check for private keys.
- (D). Revoke the code-signing certificate.

Answer: D

NO.176 Field workers in an organization are issued mobile phones on a daily basis. All the work is performed within one city and the mobile phones are not used for any purpose other than work. The organization does not want these phones used for personal purposes. The organization would like to

issue the phones to workers as permanent devices so the phones do not need to be reissued every day. Given the conditions described, which of the following technologies would BEST meet these requirements?

- (A). Geofencing
- (B). Mobile device management
- (C). Containerization
- (D). Remote wiping

Answer: B

NO.177 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.

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	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
The attack establishes a connection, which allows remote commands to be executed.	User	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
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	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
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	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
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	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

Answer:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	<div> <div>▼</div> <div> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing </div> </div>	<div> <div>▼</div> <div> 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 </div> </div>
The attack establishes a connection, which allows remote commands to be executed.	User	<div> <div>▼</div> <div> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing </div> </div>	<div> <div>▼</div> <div> 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 </div> </div>
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	<div> <div>▼</div> <div> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing </div> </div>	<div> <div>▼</div> <div> 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 </div> </div>
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	<div> <div>▼</div> <div> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing </div> </div>	<div> <div>▼</div> <div> 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 </div> </div>
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	<div> <div>▼</div> <div> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing </div> </div>	<div> <div>▼</div> <div> 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 </div> </div>

NO.178 A large financial services firm recently released information regarding a security breach

within its corporate network that began several years before. During the time frame in which the breach occurred, indicators show an attacker gained administrative access to the network through a file downloaded from a social media site and subsequently installed it without the user's knowledge. Since the compromise, the attacker was able to take command and control the computer systems anonymously while obtaining sensitive corporate and personal employee information. Which of the following methods did the attacker MOST likely use to gain access?

- (A). A bot
- (B). A fileless virus
- (C). A logic bomb
- (D). A RAT

Answer: D

Remote access trojans (RATs) are malware designed to allow an attacker to remotely control an infected computer. Once the RAT is running on a compromised system, the attacker can send commands to it and receive data back in response.

NO.179 Which of the following actions would be recommended to improve an incident response process?

- (A). Train the team to identify the difference between events and incidents
- (B). Modify access so the IT team has full access to the compromised assets
- (C). Contact the authorities if a cybercrime is suspected
- (D). Restrict communication surrounding the response to the IT team

Answer: A

NO.180 An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sale systems. The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load. Which of the following are the BEST options to accomplish this objective? (Select TWO)

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

Answer: A,D

NO.181 An organization has activated an incident response plan due to a malware outbreak on its network. The organization has brought in a forensics team that has identified an internet-facing Windows server as the likely point of initial compromise. The malware family that was detected is known to be distributed by manually logging on to servers and running the malicious code. Which of the following actions would be BEST to prevent reinfection from the initial infection vector?

- (A). Prevent connections over TFTP from the internal network
- (B). Create a firewall rule that blocks port 22 from the internet to the server
- (C). Disable file sharing over port 445 to the server
- (D). Block port 3389 inbound from untrusted networks

Answer: A

NO.182 A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfiltrated. The report also indicates that users tend to choose the same credentials on different systems and applications. Which of the following policies should the CISO use to prevent someone from using the exfiltrated credentials?

- (A). MFA
- (B). Lockout
- (C). Time-based logins
- (D). Password history

Answer: B

NO.183 A security analyst is investigating some users who are being redirected to a fake website that resembles www.comptia.org. The following output was found on the naming server of the organization:

Name	Type	Data
www	A	192.168.1.10
server1	A	10.10.10.10
server2	A	10.10.10.11
file	A	10.10.10.12

Which of the following attacks has taken place?

- (A). Domain reputation
- (B). Domain hijacking
- (C). Disassociation
- (D). DNS poisoning

Answer: D

NO.184 After returning from a conference, a user's laptop has been operating slower than normal and overheating and the fans have been running constantly. During the diagnosis process, an unknown piece of hardware is found connected to the laptop's motherboard. Which of the following attack vectors was exploited to install the hardware?

- (A). Removable media
- (B). Spear phishing
- (C). Supply chain
- (D). Direct access

Answer: C

NO.185 A user enters a password to log in to a workstation and is then prompted to enter an authentication code. Which of the following MFA factors or attributes are being utilized in the authentication process? (Select TWO).

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

Answer: A,B

NO.186 The new Chief Information Security Officer at a company has asked the security team to implement stronger user account policies. The new policies require:

- * Users to choose a password unique to their last ten passwords
- * Users to not log in from certain high-risk countries

Which of the following should the security team implement? (Select TWO).

- (A). Password complexity
- (B). Password history
- (C). Geolocation
- (D). Geofencing
- (E). Geotagging
- (F). Password reuse

Answer: A,B

NO.187 A user forwarded a suspicious email to the security team, Upon investigation, a malicious URL was discovered. Which of the following should be done FIRST to prevent other users from accessing the malicious URL?

- (A). Configure the web content filter for the web address.
- (B). Report the website to threat intelligence partners
- (C). Set me SIEM to alert for any activity to the web address.
- (D). Send out a corporate communication to warn all users Of the malicious email.

Answer: D

NO.188 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 ports Which of the following attacks in happening on the corporate network?

- (A). Man in the middle
- (B). Evil twin
- (C). Jamming
- (D). Rogue access point
- (E). Disassociation

Answer: B

NO.189 While preparing a software Inventory report, a security analyst discovers an unauthorized program installed on most of the company's servers. The program utilizes the same code signing certificate as an application deployed to only the accounting team. Which of the following mitigations would BEST secure the server environment?

- (A). Revoke the code signing certificate used by both programs.
- (B). Block all unapproved file hashes from installation.
- (C). Add the accounting application file hash to the allowed list.
- (D). Update the code signing certificate for the approved application.

Answer: C

NO.190 Which of the following controls is used to make an organization initially aware of a data compromise?

- (A). Protective
- (B). Preventative
- (C). Corrective
- (D). Detective

Answer: B

<https://purplesec.us/security-controls/>

NO.191 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

Answer: C

<https://www.hypr.com/encapsulating-security-payload-esp/>

Encapsulating Security Payload (ESP) is a member of the Internet Protocol Security (IPsec) set of protocols that encrypt and authenticate the packets of data between computers using a Virtual Private Network (VPN). The focus and layer on which ESP operates makes it possible for VPNs to function securely.

NO.192 A company wants to improve end users' experiences when they log in to a trusted partner website. The company does not want the users to be issued separate credentials for the partner website. Which of the following should be implemented to allow users to authenticate using their own credentials to log in to the trusted partner's website?

- (A). Directory service
- (B). AAA server
- (C). Federation
- (D). Multifactor authentication

Answer: C

NO.193 After a recent security breach, a security analyst reports that several administrative usernames and passwords are being sent via cleartext across the network to access network devices over port 23. Which of the following should be implemented so all credentials sent over the network are encrypted when remotely accessing and configuring network devices?

- (A). SSH
- (B). SNMPv3
- (C). SFTP
- (D). Telnet
- (E). FTP

Answer: A

NO.194 A recent phishing campaign resulted in several compromised user accounts. The security incident response team has been tasked with reducing the manual labor of filtering through all the phishing emails as they arrive and blocking the sender's email address, along with other time-

consuming mitigation actions. Which of the following can be configured to streamline those tasks?

- (A). SOAR playbook
- (B). MOM policy
- (C). Firewall rules
- (D). URL filter
- (E). SIEM data collection

Answer: A

NO.195 A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent the issue from reoccurring?

- (A). CASB
- (B). SWG
- (C). Containerization
- (D). Automated failover

Answer: C

Containerization is defined as a form of operating system virtualization, through which applications are run in isolated user spaces called containers, all using the same shared operating system (OS).

NO.196 A forensics investigator is examining a number of unauthorized payments the were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a link to attempt to unsubscribe. One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:

`Click here to unsubscribe` Which of the following will the forensics investigator MOST likely determine has occurred?

- (A). SQL injection
- (B). CSRF
- (C). XSS
- (D). XSRF

Answer: D

NO.197 A security analyst discovers that a company username and password database was posted on an internet forum. The username and passwords are stored in plan text. Which of the following would mitigate the damage done by this type of data exfiltration in the future?

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

Answer: A

NO.198 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 DIP appliance, the VPN server and the datacenter itself. Which of the following is the WEAKEST design element?

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

Answer: C

NO.199 Which of the following BEST reduces the security risks introduced when running systems that have expired vendor support and lack an immediate replacement?

- (A). Implement proper network access restrictions
- (B). Initiate a bug bounty program
- (C). Classify the system as shadow IT.
- (D). Increase the frequency of vulnerability scans

Answer: A

NO.200 A recent security breach exploited software vulnerabilities in the firewall and within the network management solution. Which of the following will MOST likely be used to identify when the breach occurred through each device?

- (A). SIEM correlation dashboards
- (B). Firewall syslog event logs
- (C). Network management solution login audit logs
- (D). Bandwidth monitors and interface sensors

Answer: A

NO.201 An organization is building backup server rooms in geographically diverse locations. The Chief Information Security Officer implemented a requirement on the project that states the new hardware cannot be susceptible to the same vulnerabilities in the existing server room. Which of the following should the systems engineer consider?

- (A). Purchasing hardware from different vendors
- (B). Migrating workloads to public cloud infrastructure
- (C). Implementing a robust patch management solution
- (D). Designing new detective security controls

Answer: A

NO.202 An organization wants to implement a biometric system with the highest likelihood that an unauthorized user will be denied access. Which of the following should the organization use to compare biometric solutions?

- (A). FRR
- (B). Difficulty of use
- (C). Cost
- (D). FAR
- (E). CER

Answer: A

NO.203 Which of the following describes the exploitation of an interactive process to gain access to restricted areas?

- (A). Persistence

- (B). Buffer overflow
(C). Privilege escalation
(D). Pharming

Answer: C

https://en.wikipedia.org/wiki/Privilege_escalation#:~:text=Privilege%20escalation%20is%20the%20act,from%20an%20application%20or%20user

NO.204 A cyber-security administrator is using an enterprise firewall. The administrator created some rules, but now Seems to be unresponsive. All connections being dropped by the firewall. Which of the following would be the BEST option to remove the rules?

- (A). # iptables -t mangle -x
(B). # iptables -f
(C). # iptables -z
(D). # iptables -p input -j drop

Answer: A

NO.205 Which of the following is the MOST likely reason for securing an air-gapped laboratory HVAC system?

- (A). To avoid data leakage
(B). To protect surveillance logs
(C). To ensure availability
(D). To facilitate third-party access

Answer: A

NO.206 Which of the following documents provides expectations at a technical level for quality, availability, and responsibilities?

- (A). EOL
(B). SLA
(C). MOU
(D). EOSL

Answer: B

NO.207 Which of the following should an organization consider implementing In the event executives need to speak to the media after a publicized data breach?

- (A). Incident response plan
(B). Business continuity plan
(C). Communication plan
(D). Disaster recovery plan

Answer: D

NO.208 A security analyst is reviewing web-application logs and finds the following log:

<https://www.comptia.org/contact-us/%3Ffile%3D.%2F.%2F.%2Fetc%2Fpasswd>

Which of the following attacks is being observed?

- (A). Directory traversal
(B). XSS

- (C). CSRF
- (D). On-path attack

Answer: A

NO.209 An organization has hired a red team to simulate attacks on its security posture. Which of the following will the blue team do after detecting an IoC?

- (A). Reimage the impacted workstations
- (B). Activate runbooks for incident response
- (C). Conduct forensics on the compromised system
- (D). Conduct passive reconnaissance to gather information

Answer: B

NO.210 A security engineer is building a file transfer solution to send files to a business partner. The users would like to drop off the files in a specific directory and have the server send them to the business partner. The connection to the business partner is over the internet and needs to be secure. Which of the following can be used?

- (A). S/MIME
- (B). LDAPS
- (C). SSH
- (D). SRTP

Answer: B

NO.211 After a ransomware attack a forensics company needs to review a cryptocurrency transaction between the victim and the attacker. Which of the following will the company MOST likely review to trace this transaction?

- (A). The public ledger
- (B). The NetFlow data
- (C). A checksum
- (D). The event log

Answer: A

<https://www.investopedia.com/tech/what-cryptocurrency-public-ledger/>

NO.212 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

Answer: A

Additionally, many organizations should abide by certain standards. For example, organizations handling credit card information need to comply with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS includes six control objectives and 12 specific requirements that help prevent fraud.

NO.213 Which of the following secure coding techniques makes compromised code more difficult for hackers to use?

- (A). Obfuscation
- (B). Normalization
- (C). Execution
- (D). Reuse

Answer: A

NO.214 A company is auditing the manner in which its European customers' personal information is handled Which of the following should the company consult?

- (A). GDPR
- (B). ISO
- (C). NIST
- (D). PCI DSS

Answer: A

NO.215 Which of the following ISO standards is certified for privacy?

- (A). ISO 9001
- (B). ISO 27002
- (C). ISO 27701
- (D). ISO 31000

Answer: C

ISO 27701 also abbreviated as PIMS (Privacy Information Management System) outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage data privacy. Privacy information management systems are sometimes referred to as personal information management systems.

<https://pecb.com/whitepaper/the-future-of-privacy-with-isoiec-27701>

NO.216 A company is considering transitioning to the cloud. The company employs individuals from various locations around the world The company does not want to increase its on-premises infrastructure blueprint and only wants to pay for additional compute power required. Which of the following solutions would BEST meet the needs of the company?

- (A). Private cloud
- (B). Hybrid environment
- (C). Managed security service provider
- (D). Hot backup site

Answer: B

NO.217 A company has a flat network in the cloud. The company needs to implement a solution to segment its production and non-production servers without migrating servers to a new network. Which of the following solutions should the company implement?

- (A). internet
- (B). Screened Subnet
- (C). VLAN segmentation
- (D). Zero Trust

Answer: C

NO.218 An organization is planning to roll out a new mobile device policy and issue each employee a new laptop. These laptops would access the users' corporate operating system remotely and allow them to use the laptops for purposes outside of their job roles. Which of the following deployment models is being utilized?

- (A). MDM and application management
- (B). BYOO and containers
- (C). COPE and VDI
- (D). CYOD and VMs

Answer: C

NO.219 A security analyst has received an alert about being sent via email. The analyst's Chief Information Security Officer (CISO) has made it clear that PII must be handled with extreme care. From which of the following did the alert MOST likely originate?

- (A). S/MIME
- (B). DLP
- (C). IMAP
- (D). HIDS

Answer: B

Network-based DLP monitors outgoing data looking for sensitive data. Network-based DLP systems monitor outgoing email to detect and block unauthorized data transfers and monitor data stored in the cloud.

NO.220 A security analyst receives an alert from the company's SIEM that anomalous activity is coming from a local source IP address of 192.168.34.26. The Chief Information Security Officer asks the analyst to block the originating source. Several days later, another employee opens an internal ticket stating that vulnerability scans are no longer being performed properly. The IP address the employee provides is 192.168.34.26. Which of the following describes this type of alert?

- (A). True positive
- (B). True negative
- (C). False positive
- (D). False negative

Answer: C

NO.221 Which of the following components can be used to consolidate and forward inbound Internet traffic to multiple cloud environments through a single firewall?

- (A). Transit gateway
- (B). Cloud hot site
- (C). Edge computing
- (D). DNS sinkhole

Answer: A

NO.222 A systems analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst include in this documentation? (Select TWO).

- (A). The order of volatility
- (B). A CRC32 checksum

- (C). The provenance of the artifacts
- (D). The vendor's name
- (E). The date time
- (F). A warning banner

Answer: A,E

NO.223 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

Answer: C

NO.224 An annual information security assessment has revealed that several OS-level configurations are not in compliance due to outdated hardening standards the company is using. Which of the following would be BEST to use to update and reconfigure the OS-level security configurations?

- (A). CIS benchmarks
- (B). GDPR guidance
- (C). Regional regulations
- (D). ISO 27001 standards

Answer: A

<https://www.beyondtrust.com/resources/glossary/systems-hardening>

NO.225 To reduce and limit software and infrastructure costs, the Chief Information Officer has requested to move email services to the cloud. The cloud provider and the organization must have security controls to protect sensitive data. Which of the following cloud services would BEST accommodate the request?

- (A). IaaS
- (B). PaaS
- (C). DaaS
- (D). SaaS

Answer: B

NO.226 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

Answer: E

<https://www.radware.com/security/ddos-knowledge-center/ddospedia/arp-poisoning>

NO.227 An IT security manager requests a report on company information that is publicly available. The manager's concern is that malicious actors will be able to access the data without engaging in active reconnaissance. Which of the following is the MOST efficient approach to perform the analysis?

- (A). Provide a domain parameter to tool.
- (B). Check public DNS entries using dnsenum.
- (C). Perform a vulnerability scan targeting a public company's IR
- (D). Execute nmap using the options: scan all ports and sneaky mode.

Answer: B

NO.228 A forensic analyst needs to prove that data has not been tampered with since it was collected. Which of the following methods will the analyst MOST likely use?

- (A). Look for tampering on the evidence collection bag
- (B). Encrypt the collected data using asymmetric encryption
- (C). Ensure proper procedures for chain of custody are being followed
- (D). Calculate the checksum using a hashing algorithm

Answer: D

NO.229 Which of the following is a policy that provides a greater depth of knowledge across an organization?

- (A). Asset management policy
- (B). Separation of duties policy
- (C). Acceptable use policy
- (D). Job Rotation policy

Answer: C

NO.230 The SOC is reviewing process and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected host was the best course of action. The allowed the malware to spread to additional hosts before it was contained. Which of the following would be BEST to improve the incident response process?

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

Answer: A

NO.231 An audit identified PII being utilized in the development environment of a critical application. The Chief Privacy Officer (CPO) is adamant that this data must be removed; however, the developers are concerned that without real data they cannot perform functionality tests and search

for specific data. Which of the following should a security professional implement to BEST satisfy both the CPO's and the development team's requirements?

- (A). Data anonymization
- (B). Data encryption
- (C). Data masking
- (D). Data tokenization

Answer: A

NO.232 A research company discovered that an unauthorized piece of software has been detected on a small number of machines in its lab. The researchers collaborate with other machines using port 445 and on the Internet using port 443. The unauthorized software is starting to be seen on additional machines outside of the lab and is making outbound communications using HTTPS and SMB. The security team has been instructed to resolve the problem as quickly as possible causing minimal disruption to the researchers. Which of the following contains the BEST course of action in this scenario?

- (A). Update the host firewalls to block outbound SMB.
- (B). Place the machines with the unapproved software in containment.
- (C). Place the unauthorized application in a blocklist.
- (D). Implement a content filter to block the unauthorized software communication.

Answer: B

NO.233 Which of the following statements BEST describes zero-day exploits'?

- (A). When a zero-day exploit is discovered, the system cannot be protected by any means
- (B). Zero-day exploits have their own scoring category in CVSS
- (C). A zero-day exploit is initially undetectable and no patch for it exists
- (D). Discovering zero-day exploits is always performed via bug bounty programs

Answer: C

NO.234 A Chief Security Officer (CSO) is concerned that cloud-based services are not adequately protected from advanced threats and malware. The CSO believes there is a high risk that a data breach could occur in the near future due to the lack of detective and preventive controls. Which of the following should be implemented to BEST address the CSO's concerns? (Select TWO)

- (A). A WAF
- (B). ACASB
- (C). An NG-SWG
- (D). Segmentation
- (E). Encryption
- (F). Containerization

Answer: B,F

NO.235 Which of the following tools is effective in preventing a user from accessing unauthorized removable media?

- (A). USB data blocker
- (B). Faraday cage
- (C). Proximity reader
- (D). Cable lock

Answer: A

NO.236 Which of the following is the MOST effective control against zero-day vulnerabilities?

- (A). Network segmentation
- (B). Patch management
- (C). Intrusion prevention system
- (D). Multiple vulnerability scanners

Answer: A

NO.237 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

Answer: B

NO.238 An organization just implemented a new security system. Local laws state that citizens must be notified prior to encountering the detection mechanism to deter malicious activities. Which of the following is being implemented?

- (A). Proximity cards with guards
- (B). Fence with electricity
- (C). Drones with alarms
- (D). Motion sensors with signage

Answer: D

NO.239 Which of the following is an effective tool to stop or prevent the exfiltration of data from a network?

- (A). DLP
- (B). NIDS
- (C). TPM
- (D). FDE

Answer: A

NO.240 An organization has a growing workforce that is mostly driven by additions to the sales department. Each newly hired salesperson relies on a mobile device to conduct business. The Chief Information Officer (CIO) is wondering if the organization may need to scale down just as quickly as it scaled up. The CIO is also concerned about the organization's security and customer privacy. Which of the following would be BEST to address the CIO's concerns?

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

Answer: C

NO.241 A penetration tester was able to compromise an internal server and is now trying to pivot the current session in a network lateral movement. Which of the following tools if available on the server, will provide the MOST useful information for the next assessment step?

- (A). Autopsy
- (B). Cuckoo
- (C). Memdump
- (D). Nmap

Answer: A

NO.242 Users are presented with a banner upon each login to a workstation. The banner mentions that users are not entitled to any reasonable expectation of privacy and access is for authorized personnel only.

In order to proceed past that banner, users must click the OK button. Which of the following is this an example of?

- (A). AUP
- (B). NDA
- (C). SLA
- (D). MOU

Answer: A

NO.243 A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security assessment. The analyst redirects the output to a file. After the capture is complete, the analyst needs to review the first transactions quickly and then search the entire series of requests for a particular string. Which of the following would be BEST to use to accomplish the task? (Select TWO).

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

Answer: A,C

A - "analyst needs to review the first transactions quickly"

C - "search the entire series of requests for a particular string"

NO.244 A security analyst in a SOC has been tasked with onboarding a new network into the SIEM. Which of the following BEST describes the information that should feed into a SIEM solution in order to adequately support an investigation?

- (A). Logs from each device type and security layer to provide correlation of events
- (B). Only firewall logs since that is where attackers will most likely try to breach the network
- (C). Email and web-browsing logs because user behavior is often the cause of security breaches
- (D). NetFlow because it is much more reliable to analyze than syslog and will be exportable from every device

Answer: B

NO.245 A public relations team will be taking a group of guest on a tour through the facility of a

large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboards are cleaned and all desks are cleared. The company is MOST likely trying to protect against.

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

Answer: A

In the context of information security, social engineering is the psychological manipulation of people into performing actions or divulging confidential information think phishing, spoofing. That is not being demonstrated in this question. The company is protecting themselves from loss of proprietary information by clearing it all out. so that if anyone in the tour is looking to take it they will be out of luck

NO.246 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

Answer: D

NO.247 Which of the following describes the ability of code to target a hypervisor from inside

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

Answer: B

Virtual machine escape is an exploit in which the attacker runs code on a VM that allows an operating system running within it to break out and interact directly with the hypervisor.

[https://whatis.techtarget.com/definition/virtual-machine-escape#:~:text=Virtual%20machine%20escape%20is%20an,VMs\)%20running%20on%20that%20host.](https://whatis.techtarget.com/definition/virtual-machine-escape#:~:text=Virtual%20machine%20escape%20is%20an,VMs)%20running%20on%20that%20host.)

NO.248 An organization implemented a process that compares the settings currently configured on systems against secure configuration guidelines in order to identify any gaps Which of the following control types has the organization implemented?

- (A). Compensating
- (B). Corrective
- (C). Preventive
- (D). Detective

Answer: C

NO.249 A software developer needs to perform code-execution testing, black-box testing, and non-

functional testing on a new product before its general release. Which of the following BEST describes the tasks the developer is conducting?

- (A). Verification
- (B). Validation
- (C). Normalization
- (D). Staging

Answer: A

NO.250 An organization has hired a security analyst to perform a penetration test. The analyst captures 1Gb worth of inbound network traffic to the server and transfer the pcap back to the machine for analysis. Which of the following tools should the analyst use to further review the pcap?

- (A). Nmap
- (B). cURL
- (C). Netcat
- (D). Wireshark

Answer: D

[https://www.comparitech.com/net-admin/pcap-guide/#:~:text=Packet%20Capture%20or%20PCAP%20\(also,packet%20data%20from%20a%20network.](https://www.comparitech.com/net-admin/pcap-guide/#:~:text=Packet%20Capture%20or%20PCAP%20(also,packet%20data%20from%20a%20network.)

NO.251 The president of a regional bank likes to frequently provide SOC tours to potential investors. Which of the following policies BEST reduces the risk of malicious activity occurring after a tour?

- (A). Password complexity
- (B). Acceptable use
- (C). Access control
- (D). Clean desk

Answer: C

NO.252 An organization discovered files with proprietary financial data have been deleted. The files have been recovered from backup but every time the Chief Financial Officer logs in to the file server, the same files are deleted again No other users are experiencing this issue. Which of the following types of malware is MOST likely causing this behavior?

- (A). Logic bomb
- (B). Crypto malware
- (C). Spyware
- (D). Remote access Trojan

Answer: A

NO.253 While preparing a software Inventory report, a security analyst discovers an unauthorized program installed on most of the company's servers. The program utilizes the same code signing certificate as an application deployed to only the accounting team. Which of the following mitigations would BEST secure the server environment?

- (A). Block all unapproved file hashes from installation.
- (B). Update the code signing certificate for the approved application.
- (C). Add the accounting application file hash to the allowed list.
- (D). Revoke the code signing certificate used by both programs.

Answer: C

NO.254 A security analyst was asked to evaluate a potential attack that occurred on a publicly accessible section of the company's website. The malicious actor posted an entry in an attempt to trick users into clicking the following:

`https://www.c0mpt1a.com/contact-us/?3Fname=3D%3Cscript%3Ealert(document.cookie)%3C%2Fscript%3E`

Which of the following was MOST likely observed?

- (A). DLL injection
- (B). Session replay
- (C). SOLI
- (D). XSS

Answer: B

NO.255 Which of the following would BEST provide a systems administrator with the ability to more efficiently identify systems and manage permissions and policies based on location, role, and service level?

- (A). Standard naming conventions
- (B). Domain services
- (C). Baseline configurations
- (D). Diagrams

Answer: C

NO.256 A security engineer is deploying a new wireless for a company. The company shares office space with multiple tenants. Which of the following should the engineer configure on the wireless network to ensure that confidential data is not exposed to unauthorized users?

- (A). EAP
- (B). TLS
- (C). HTTPS
- (D). AES

Answer: C

NO.257 A web server has been compromised due to a ransomware attack. Further investigation reveals the ransomware has been in the server for the past 72 hours. The systems administrator needs to get the services back up as soon as possible. Which of the following should the administrator use to restore services to a secure state?

- (A). The last incremental backup that was conducted 72 hours ago Most Voted
- (B). The last known-good configuration Most Voted
- (C). The last full backup that was conducted seven days ago
- (D). The baseline OS configuration

Answer: C

Ransomware will most likely render the web server unusable and must be isolated for forensic investigation. This will leave the only option to start a new web server from scratch and restore the last full backup, plus any differential or incremental backups which are sure to be clean from ransomware (if available).

NO.258 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:

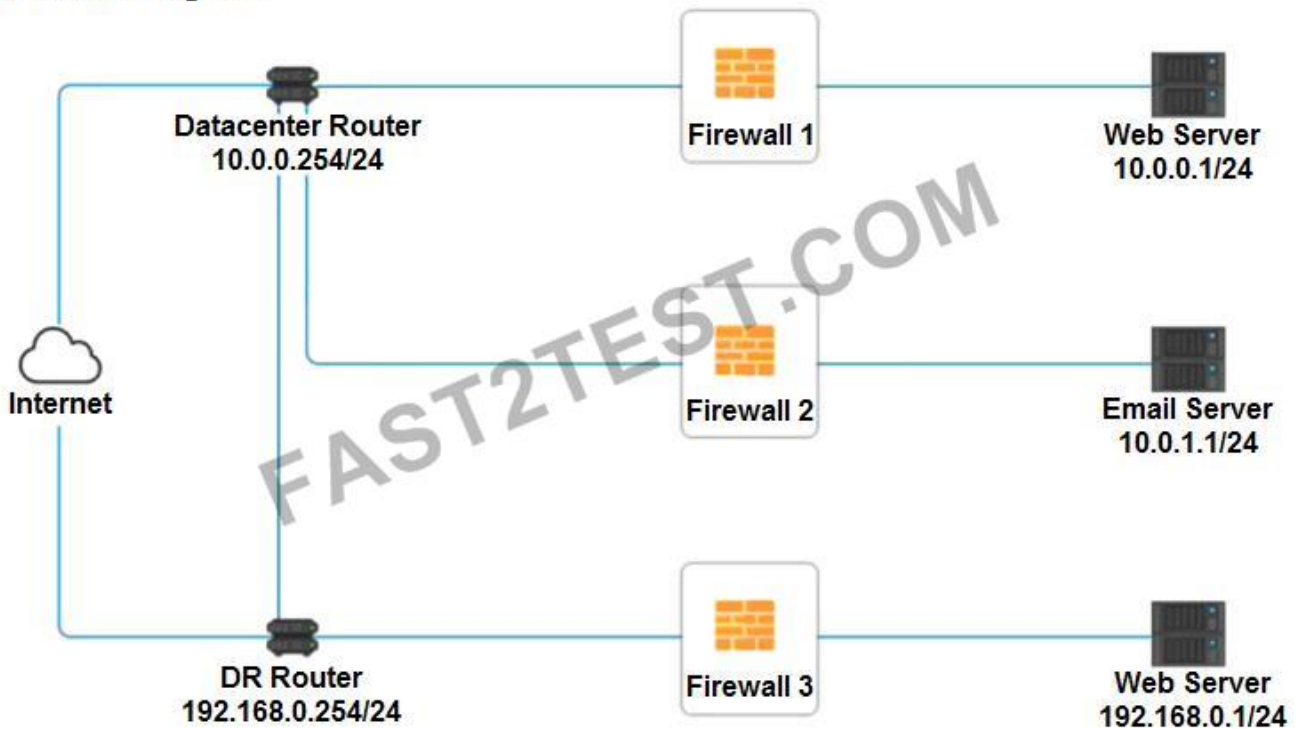
Deny cleartext web traffic.

Ensure secure management protocols are used. Please 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 2
✕

Rule Name	Source	Destination	Service	Action
DNS Rule	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> PERMIT DENY </div> </div>
HTTPS Outbound	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> PERMIT DENY </div> </div>
Management	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> PERMIT DENY </div> </div>
HTTPS Inbound	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> PERMIT DENY </div> </div>
HTTP Inbound	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> ▼ </div> <div style="padding: 2px;"> PERMIT DENY </div> </div>

Reset Answer
Save
Close

Firewall 3
✕

Rule Name	Source	Destination	Service	Action
DNS Rule	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> PERMIT DENY </div>
HTTPS Outbound	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> PERMIT DENY </div>
Management	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> PERMIT DENY </div>
HTTPS Inbound	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> PERMIT DENY </div>
HTTP Inbound	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div>	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div>	<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">▼</div> <div style="border: 1px solid black; padding: 2px;"> PERMIT DENY </div>

Reset Answer
Save
Close

Answer:

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



NO.259 The Chief Information Security Officer wants to prevent exfiltration of sensitive information from employee cell phones when using public USB power charging stations. Which of the following would be the BEST solution to Implement?

- (A). DLP
- (B). USB data blocker
- (C). USB OTG
- (D). Disabling USB ports

Answer: B

NO.260 During a trial, a judge determined evidence gathered from a hard drive was not admissible. Which of the following BEST explains this reasoning?

- (A). The forensic investigator forgot to run a checksum on the disk image after creation
- (B). The chain of custody form did not note time zone offsets between transportation regions
- (C). The computer was turned off, and a RAM image could not be taken at the same time
- (D). The hard drive was not properly kept in an antistatic bag when it was moved

Answer: A

NO.261 An organization is migrating several SaaS applications that support SSO. The security manager wants to ensure the migration is completed securely. Which of the following should the organization consider before implementation? (Select TWO).

- (A). The back-end directory source
- (B). The identity federation protocol
- (C). The hashing method
- (D). The encryption method
- (E). The registration authority
- (F). The certificate authority

Answer: C,F

NO.262 A document that appears to be malicious has been discovered in an email that was sent to a company's Chief Financial Officer (CFO). Which of the following would be BEST to allow a security analyst to gather information and confirm it is a malicious document without executing any code it may contain?

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

Answer: D

NO.263 Which of the following types of controls is a turnstile?

- (A). Physical
- (B). Detective
- (C). Corrective
- (D). Technical

Answer: A

[https://en.wikipedia.org/wiki/Turnstile#:~:text=A%20turnstile%20\(also%20called%20a,%2C%20a%20](https://en.wikipedia.org/wiki/Turnstile#:~:text=A%20turnstile%20(also%20called%20a,%2C%20a%20)

pass%2C%20or%20similar.

NO.264 Which of the following explains why RTO is included in a BIA?

- (A). It identifies the amount of allowable downtime for an application or system,
- (B). It prioritizes risks so the organization can allocate resources appropriately,
- (C). It monetizes the loss of an asset and determines a break-even point for risk mitigation.
- (D). It informs the backup approach so that the organization can recover data to a known time.

Answer: A

NO.265 Two hospitals merged into a single organization. The privacy officer requested a review of all records to ensure encryption was used during record storage, in compliance with regulations. During the review, the officer discovered thai medical diagnosis codes and patient names were left unsecured. Which of the following types of data does this combination BEST represent?

- (A). Personal health information
- (B). Personally Identifiable Information
- (C). ToKenized data
- (D). Proprietary data

Answer: A

NO.266 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/passwd HTTP/1.1
Host: www.companysite.com
```

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

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

Answer: D

NO.267 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 m 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

Answer: A

<https://oroinc.com/b2b-e-commerce/blog/testing-and-staging-environments-in-e-commerce-implementation/>

NO.268 A company's Chief Information Office (CIO) is meeting with the Chief Information Security Officer (CISO) to plan some activities to enhance the skill levels of the company's developers. Which of the following would be MOST suitable for training the developers'?

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

Answer: B

NO.269 A technician was dispatched to complete repairs on a server in a data center. While locating the server, the technician entered a restricted area without authorization. Which of the following security controls would BEST prevent this in the future?

- (A). Use appropriate signage to mark all areas.
- (B). Utilize cameras monitored by guards.
- (C). Implement access control vestibules.
- (D). Enforce escorts to monitor all visitors.

Answer: C

NO.270 A software company adopted the following processes before releasing software to production;

- * Peer review
- * Static code scanning
- * Signing

A considerable number of vulnerabilities are still being detected when code is executed on production Which of the following security tools can improve vulnerability detection on this environment?

- (A). File integrity monitonng for the source code
- (B). Dynamic code analysis tool
- (C). Encrypted code repository
- (D). Endpoint detection and response solution

Answer: A

NO.271 A user recently entered a username and password into a recruiting application website that had been forged to look like the legitimate site Upon investigation, a security analyst the identifies the following:

- * The legitimate websites IP address is 10.1.1.20 and eRecruit local resolves to the IP
- * The forged website's IP address appears to be 10.2.12.99. based on NetFlow records
- * AH three at the organization's DNS servers show the website correctly resolves to the legitimate IP
- * DNS query logs show one of the three DNS servers returned a result of 10.2.12.99 (cached) at the approximate time of the suspected compromise.

Which of the following MOST likely occurred?

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

Answer: B

NO.272 Server administrator want to configure a cloud solution so that computing memory and processor usage is maximized most efficiently across a number of virtual servers. They also need to

avoid potential denial-of-service situations caused by availability. Which of the following should administrator configure to maximize system availability while efficiently utilizing available computing power?

- (A). Dynamic resource allocation
- (B). High availability
- (C). Segmentation
- (D). Container security

Answer: C

NO.273 A user reports constant lag and performance issues with the wireless network when working at a local coffee shop. A security analyst walks the user through an installation of Wireshark and get a five-minute pcap to analyze. The analyst observes the following output:

No.	Time	Source	Destination	Protocol	Length	Info
1234	9.1195665	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

Answer: B

https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack

One of the main purposes of deauthentication used in the hacking community is to force clients to connect to an evil twin access point which then can be used to capture network packets transferred between the client and the access point.

NO.274 A security proposal was set up to track requests for remote access by creating a baseline of the users' common sign-in properties. When a baseline deviation is detected, an lv1FA challenge will be triggered. Which of the following should be configured in order to deploy the proposal?

- (A). Context-aware authentication
- (B). Simultaneous authentication of equals
- (C). Extensive authentication protocol
- (D). Agentless network access control

Answer: A

NO.275 Which biometric error would allow an unauthorized user to access a system?

- (A). False acceptance
- (B). False entrance
- (C). False rejection
- (D). False denial

Answer: C

NO.276 Which of the following should be monitored by threat intelligence researchers who search for leaked credentials?

- (A). Common Weakness Enumeration
- (B). OSINT
- (C). Dark web
- (D). Vulnerability databases

Answer: C

NO.277 An organization has developed an application that needs a patch to fix a critical vulnerability. In which of the following environments should the patch be deployed LAST?

- (A). Test
- (B). Staging
- (C). Development
- (D). Production

Answer: B

NO.278 Security analysts are conducting an investigation of an attack that occurred inside the organization's network. An attacker was able to connect network traffic between workstation throughout the network. The analysts review the following logs:

VLAN	Address
1	0007.1e5d.3213
1	002a.7d.44.8801
1	0011.1aab.4.344d

The layer 2 address table has hundred of entries similar to the ones above. Which of the following attacks has MOST likely occurred?

- (A). SQL injection
- (B). DNS spoofing
- (C). MAC flooding
- (D). ARP poisoning

Answer: D

NO.279 A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Choose two.)

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

Answer: A,B

<https://searchdatacenter.techtarget.com/definition/resiliency>

NO.280 The Chief information Security Officer wants to prevent exfiltration of sensitive information from employee cell phones when using public USB power charging stations. Which of the following would be the Best solution to implement?

- (A). DLP
- (B). USB data blocker
- (C). USB OTG
- (D). Disabling USB ports

Answer: C

NO.281 A news article states hackers have been selling access to IoT camera feeds. Which of the following is the Most likely reason for this issue?

- (A). Outdated software
- (B). Weak credentials
- (C). Lack of encryption
- (D). Backdoors

Answer: C

NO.282 In a phishing attack, the perpetrator is pretending to be someone in a position of power in an effort to influence the target to click or follow the desired response. Which of the following principles is being used?

- (A). Authority
- (B). Intimidation
- (C). Consensus
- (D). Scarcity

Answer: B

NO.283 A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate device using PKI. Which of the following should the administrator configure?

- (A). A captive portal
- (B). PSK
- (C). 802.1X
- (D). WPS

Answer: C

NO.284 A company is moving its retail website to a public cloud provider. The company wants to tokenize credit card data but not allow the cloud provider to see the stored credit card information. Which of the following would BEST meet these objectives?

- (A). WAF
- (B). CASB
- (C). VPN
- (D). TLS

Answer: B

NO.285 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 on to any thin client located throughout the building and see the same desktop each time. Which of the following

technologies are being utilized to provide these capabilities? (Select TWO)

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

Answer: B,E

NO.286 A junior security analyst is conducting an analysis after passwords were changed on multiple accounts without users' interaction. The SIEM has multiple logon entries with the following text:

```
suspicious event - user: scheduledtasks successfully authenticate on AD on abnormal time
suspicious event - user: scheduledtasks failed to execute c:\weekly_checkups\amazing-3rdparty-domain-assessment.py
suspicious event - user: scheduledtasks failed to execute c:\weekly_checkups\secureyourAD-3rdparty-compliance.sh
suspicious event - user: scheduledtasks successfully executed c:\weekly_checkups\amazing-3rdparty-domain-assessment.py
```

Which of the following is the MOST likely attack conducted on the environment?

- (A). Malicious script
- (B). Privilege escalation
- (C). Domain hijacking
- (D). DNS poisoning

Answer: A

NO.287 Which of the following is the GREATEST security concern when outsourcing code development to third-party contractors for an internet-facing application?

- (A). Intellectual property theft
- (B). Elevated privileges
- (C). Unknown backdoor
- (D). Quality assurance

Answer: C

NO.288 Which of the following control types is focused primarily on reducing risk before an incident occurs?

- (A). Preventive
- (B). Deterrent
- (C). Corrective
- (D). Detective

Answer: D

NO.289 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

Answer: C

<https://www.promorx.com/blogs/blog/how-does-a-usb-data-blocker-work> Connecting via the data port of your mobile device, the Data Blockers creates a barrier between your mobile device and the charging station. Your phone will draw power as usual, allowing you to use it normally and charge it at the same time, but this clever piece of equipment will prevent any data exchange.

"Malicious USB charging cables and plugs are also a widespread problem. As with card skimming, a device may be placed over a public charging port at airports and other transit locations. A USB data blocker can provide mitigation against these juice-jacking attacks by preventing any sort of data transfer when the smartphone or laptop is connected to a charge point "

NO.290 A company recently moved sensitive videos between on-premises. Company-owned websites. The company then learned the videos had been uploaded and shared to the internet. Which of the following would MOST likely allow the company to find the cause?

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

Answer: D

<https://www.sumologic.com/glossary/log-analysis/>

"While companies can operate private clouds, forensics in a public cloud are complicated by the right to audit permitted to you by your service level agreement (SLA) with the cloud provider."

NO.291 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.

Commands	SSH Client
<code>chmod 644 ~/.ssh/id_rsa</code>	
<code>chmod 777 ~/.ssh/authorized_keys</code>	
<code>ssh-keygen -t rsa</code>	
<code>scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys</code>	
<code>ssh-copy-id -i ~/.ssh/id_rsa.pub user@server</code>	
<code>ssh -i ~/.ssh/id_rsa user@server</code>	
<code>ssh root@server</code>	

Answer:

Commands	SSH Client
<code>chmod 644 ~/.ssh/id_rsa</code>	<code>ssh-keygen -t rsa</code>
<code>chmod 777 ~/.ssh/authorized_keys</code>	<code>ssh-copy-id -i ~/.ssh/id_rsa.pub user@server</code>
<code>ssh-keygen -t rsa</code>	<code>ssh -i ~/.ssh/id_rsa user@server</code>
<code>scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys</code>	
<code>ssh-copy-id -i ~/.ssh/id_rsa.pub user@server</code>	
<code>ssh -i ~/.ssh/id_rsa user@server</code>	
<code>ssh root@server</code>	

NO.292 Which of the following prevents an employee from seeing a colleague who is visiting an inappropriate website?

- (A). Job rotation policy
- (B). NDA
- (C). AUP
- (D). Separation of duties policy

Answer: C

NO.293 The Chief Information Security Officer (CISO) requested a report on potential areas of improvement following a security incident. Which of the following incident response processes is the CISO requesting?

- (A). Lessons learned
- (B). Preparation
- (C). Detection
- (D). Containment
- (E). Root cause analysis

Answer: A

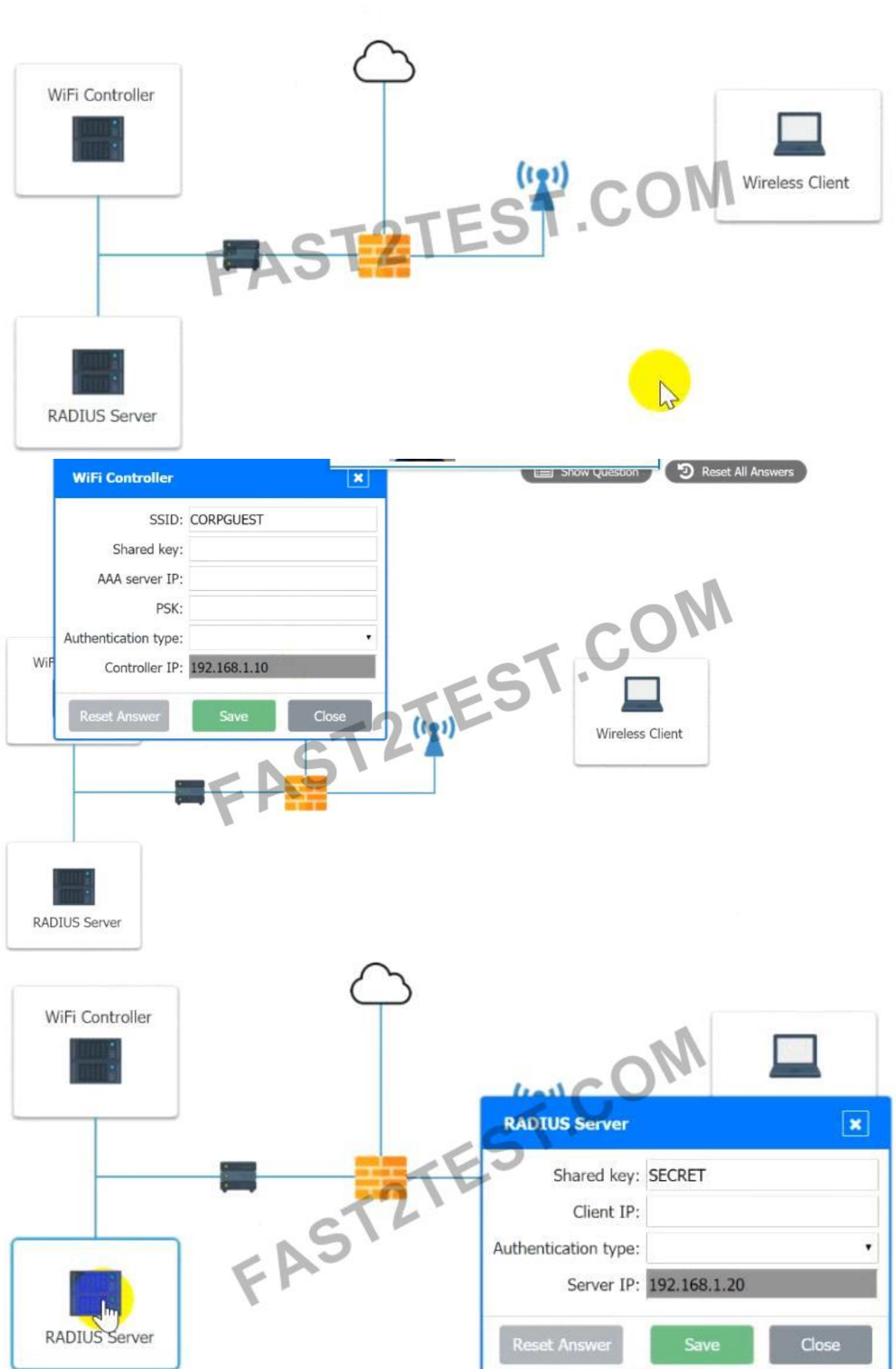
NO.294 A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802.1X using the most secure encryption and protocol available.

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:

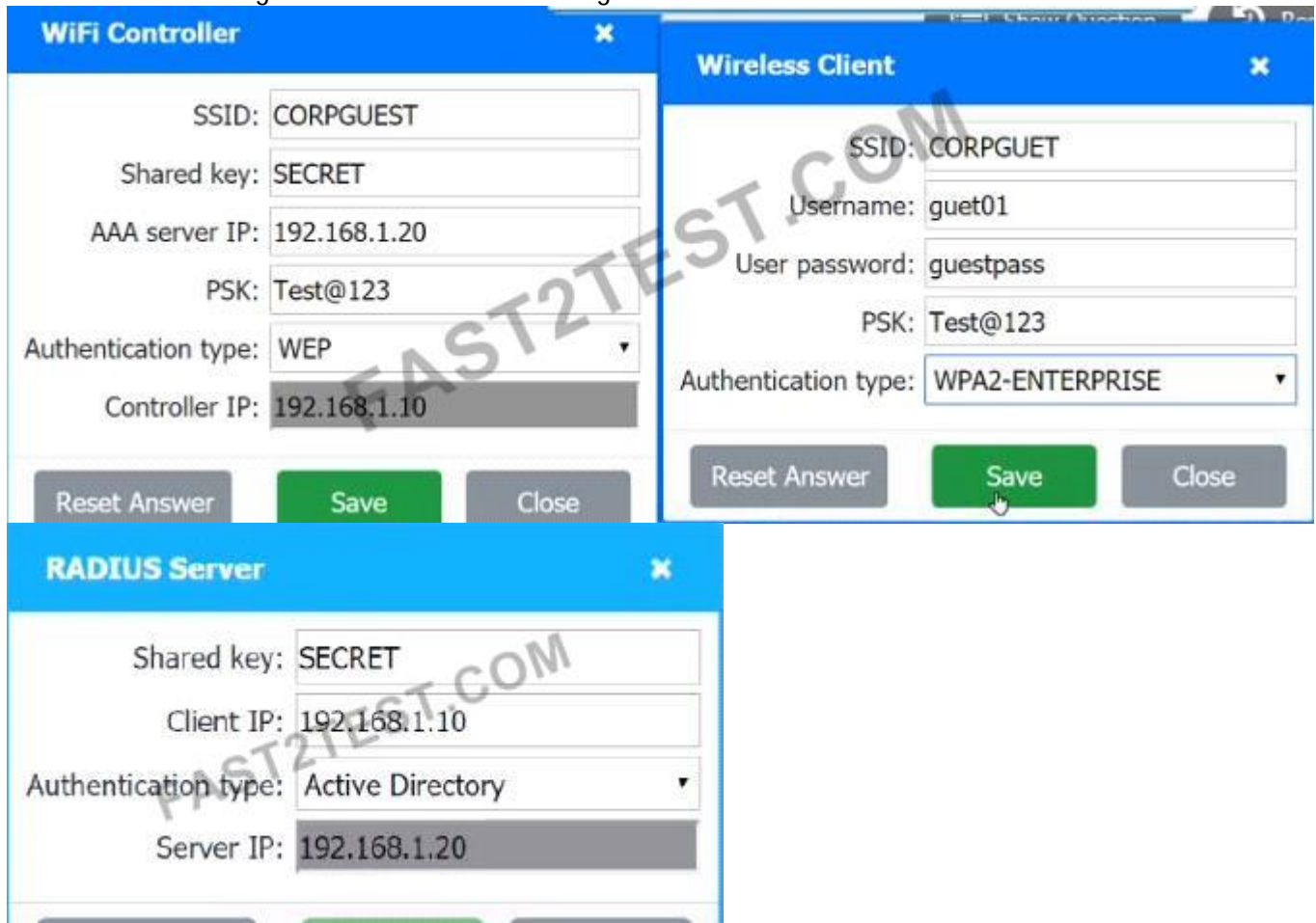
User: guest01

Password: guestpass



**Answer:**

Use the same settings as describe in below images.



NO.295 A SOC operator is receiving continuous alerts from multiple Linux systems indicating that unsuccessful SSH attempts to a functional user ID have been attempted on each one of them in a short period of time. Which of the following BEST explains this behavior?

- (A). Rainbow table attack
- (B). Password spraying

- (C). Logic bomb
- (D). Malware bot

Answer: B

Password Spraying is a variant of what is known as a brute force attack. In a traditional brute force attack, the perpetrator attempts to gain unauthorized access to a single account by guessing the password "repeatedly" in a very short period of time.

NO.296 Which of the following are common VoIP-associated vulnerabilities? (Select TWO).

- (A). SPIM
- (B). vishing
- (C). Hopping
- (D). Phishing
- (E). Credential harvesting
- (F). Tailgating

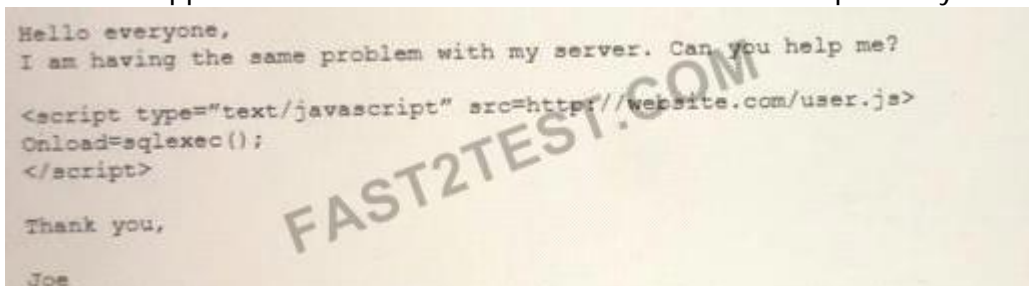
Answer: A,B

NO.297 A security analyst is receiving numerous alerts reporting that the response time of an internet-facing application has been degraded. However, the internal network performance was not degraded. Which of the following MOST likely explains this behavior?

- (A). DNS poisoning
- (B). MAC flooding
- (C). DDoS attack
- (D). ARP poisoning

Answer: C

NO.298 An analyst visits an internet forum looking for information about a tool. The analyst finds a threat that appears to contain relevant information. One of the posts says the following:



The image shows a screenshot of a forum post on a light yellow background. The text of the post is as follows:

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

 A large, diagonal watermark reading "FAST2TEST.COM" is overlaid across the middle of the post content.

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

- (A). SOU attack
- (B). DLL attack
- (C). XSS attack
- (D). API attack

Answer: C

Cross-site scripting attacks may occur anywhere that possibly malicious users are allowed to post unregulated material to a trusted website for the consumption of other valid users. The most common example can be found in bulletin-board websites which provide web based mailing list-style functionality. <https://owasp.org/www-community/attacks/xss/>
<https://www.acunetix.com/websitesecurity/cross-site-scripting/>

NO.299 A security analyst is tasked with defining the "something you are" factor of the company's MFA settings. Which of the following is BEST to use to complete the configuration?

- (A). Gait analysis
- (B). Vein
- (C). Soft token
- (D). HMAC-based, one-time password

Answer: C

NO.300 Which of the following will provide the BEST physical security countermeasures to stop intruders? (Select TWO.)

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

Answer: D,E

Alarms=deterrent, Signage=deterrent, Lighting=deterrent, Mantraps=physical countermeasure, Fencing=physical countermeasure and Sensors are either reactive or technical.

<https://www.professormesser.com/security-plus/sy0-501/physical-security-controls-2/>

NO.301 A SOC operator is analyzing a log file that contains the following entries:

```
[06-Apr-2021-18:00:06] GET /index.php/../../../../../../etc/passwd
[06-Apr-2021-18:01:07] GET /index.php/../../../../../../etc/shadow
[06-Apr-2021-18:01:26] GET /index.php/../../../../../../etc/passwd
[06-Apr-2021-18:02:16] GET /index.php?var1=;cat /etc/passwd;&var2=7865tgydk
[06-Apr-2021-18:02:56] GET /index.php?var1=;cat /etc/shadow;&var2=7865tgydk
```

- (A). SQL injection and improper input-handling attempts
- (B). Cross-site scripting and resource exhaustion attempts
- (C). Command injection and directory traversal attempts
- (D). Error handling and privilege escalation attempts

Answer: C

NO.302 Which of the following is a known security risk associated with data archives that contain financial information?

- (A). Data can become a liability if archived longer than required by regulatory guidance
- (B). Data must be archived off-site to avoid breaches and meet business requirements
- (C). Companies are prohibited from providing archived data to e-discovery requests
- (D). Unencrypted archives should be preserved as long as possible and encrypted

Answer: B

NO.303 Multiple business accounts were compromised a few days after a public website had its credentials database leaked on the internet. No business emails were identified in the breach, but the security team thinks that the list of passwords exposed was later used to compromise business accounts. Which of the following would mitigate the issue?

- (A). Complexity requirements
- (B). Password history

- (C). Acceptable use policy
- (D). Shared accounts

Answer: C

NO.304 A company's security team received notice of a critical vulnerability affecting a high-profile device within the web infrastructure. The vendor patch was just made available online but has not yet been regression tested in development environments. In the interim, firewall rules were implemented to reduce the access to the interface affected by the vulnerability. Which of the following controls does this scenario describe?

- (A). Deterrent
- (B). Compensating
- (C). Detective
- (D). Preventive

Answer: C

NO.305 An employee received a word processing file that was delivered as an email attachment. The subject line and email content enticed the employee to open the attachment. Which of the following attack vectors BEST matches this malware?

- (A). Embedded Python code
- (B). Macro-enabled file
- (C). Bash scripting
- (D). Credential-harvesting website

Answer: B

NO.306 The Chief Information Security Officer directed a risk reduction in shadow IT and created a policy requiring all unsanctioned high-risk SaaS applications to be blocked from user access. Which of the following is the BEST security solution to reduce this risk?

- (A). CASB
- (B). VPN concentrator
- (C). MFA
- (D). VPC endpoint

Answer: A

NO.307 An organization wants to participate in threat intelligence information sharing with peer groups. Which of the following would MOST likely meet the organization's requirement?

- (A). Perform OSINT investigations
- (B). Subscribe to threat intelligence feeds
- (C). Submit RFCs
- (D). Implement a TAXII server

Answer: B

NO.308 Security analysts notice a server login from a user who has been on vacation for two weeks. The analysts confirm that the user did not log in to the system while on vacation. After reviewing packet capture logs, the analysts notice the following:

username:smithJA
Password: 944d8697d8880ed401b5ba2c77811

Which of the following occurred?

- (A). A buffer overflow was exploited to gain unauthorized access
- (B). The user's account was compromised, and an attacker changed the login credentials
- (C). An attacker used a pass-the-hash attack to gain access
- (D). An insider threat with username smithJA logged in to the account

Answer: B

NO.309 Joe, a user at a company, clicked an email link led to a website that infected his workstation. Joe, was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and It has continues to evade detection. Which of the following should administrator implement to protect the environment from this malware?

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

Answer: C

Heuristic analysis is also one of the few methods capable of combating polymorphic viruses - the term for malicious code that constantly changes and adapts. Heuristic analysis is incorporated into advanced security solutions offered by companies like Kaspersky Labs to detect new threats before they cause harm, without the need for a specific signature. <https://usa.kaspersky.com/resource-center/definitions/heuristic-analysis>

NO.310 The database administration team is requesting guidance for a secure solution that will ensure confidentiality of cardholder data at rest only in certain fields in the database schem a. The requirement is to substitute a sensitive data field with a non-sensitive field that is rendered useless if a data breach occurs Which of the following is the BEST solution to meet the requirement?

- (A). Tokenization
- (B). Masking
- (C). Full disk encryption
- (D). Mirroring

Answer: B

NO.311 A vulnerability has been discovered and a known patch to address the vulnerability does not exist. Which of the following controls works BEST until a proper fix is released?

- (A). Detective
- (B). Compensating
- (C). Deterrent
- (D). Corrective

Answer: A

NO.312 During an incident response process involving a laptop, a host was identified as the entry point for malware. The management team would like to have the laptop restored and given back to the user. The cybersecurity analyst would like to continue investigating the intrusion on the host.

Which of the following would allow the analyst to continue the investigation and also return the laptop to the user as soon as possible?

- (A). dd
- (B). memdump
- (C). tcpdump
- (D). head

Answer: C

NO.313 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

Answer: D

NO.314 During a recent incident an external attacker was able to exploit an SMB vulnerability over the internet. Which of the following action items should a security analyst perform FIRST to prevent this from occurring again?

- (A). Check for any recent SMB CVEs
- (B). Install AV on the affected server
- (C). Block unneeded TCP 445 connections
- (D). Deploy a NIDS in the affected subnet

Answer: C

NO.315 A recent audit cited a risk involving numerous low-criticality vulnerabilities created by a web application using a third-party library. The development staff state there are still customers using the application even though it is end of life and it would be a substantial burden to update the application for compatibility with more secure libraries. Which of the following would be the MOST prudent course of action?

- (A). Accept the risk if there is a clear road map for timely decommission
- (B). Deny the risk due to the end-of-life status of the application.
- (C). Use containerization to segment the application from other applications to eliminate the risk
- (D). Outsource the application to a third-party developer group

Answer: C

NO.316 A startup company is using multiple SaaS and IaaS platform 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

Answer: C

A cloud access security broker is on-premises or cloud based software that sits between cloud service users and cloud applications, and monitors all activity and enforces security policies. A CASB has a separate, and more distinctive role. Differing from the use case for SWG, which focuses on the broader filtering and protection against inbound threats and filtering illegitimate web traffic, a CASB is more deeply integrated and has control over your cloud application usage. It can be tied into an applications API to scan data at rest or can be used with a proxy based deployment to enforce inline policies for more real time protection.

NO.317 A security engineer is reviewing log files after a third discovered usernames and passwords for the organization's accounts. The engineer sees there was a change in the IP address for a vendor website one 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

Answer: D

DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address. This results in traffic being diverted to the attacker's computer (or any other computer).

https://en.wikipedia.org/wiki/DNS_spoofing

NO.318 A security analyst is evaluating the risks of authorizing multiple security solutions to collect data from the company's cloud environment. Which of the following is an immediate consequence of these integrations?

- (A). Non-compliance with data sovereignty rules
- (B). Loss of the vendor's interoperability support
- (C). Mandatory deployment of a SIEM solution
- (D). Increase in the attack surface

Answer: C

NO.319 The SOC for a large MSSP is meeting to discuss the lessons learned from a recent incident that took much too long to resolve. This type of incident has become more common in recent weeks and is consuming large amounts of the analysts' time due to manual tasks being performed. Which of the following solutions should the SOC consider to BEST improve its response time?

- (A). Configure a NIDS appliance using a Switched Port Analyzer
- (B). Collect OSINT and catalog the artifacts in a central repository
- (C). Implement a SOAR with customizable playbooks
- (D). Install a SIEM with community-driven threat intelligence

Answer: C

NO.320 A company wants the ability to restrict web access and monitor the websites that employees visit. Which of the following would BEST meet these requirements?

- (A). Internet proxy
- (B). VPN
- (C). WAF
- (D). Firewall

Answer: C

NO.321 Certain users are reporting their accounts are being used to send unauthorized emails and conduct suspicious activities. After further investigation, a security analyst notices the following:

- * All users share workstations throughout the day
 - * Endpoint protection was disabled on several workstations throughout the network.
 - * Travel times on logins from the affected users are impossible
 - * Sensitive data is being uploaded to external sites
 - * All user account passwords were forced to be reset and the issue continued
- Which of the following attacks is being used to compromise the user accounts?

- (A). Brute-force
- (B). Keylogger
- (C). Dictionary
- (D). Rainbow

Answer: C

NO.322 Several attempts have been made to pick the door lock of a secure facility. As a result, the security engineer has been assigned to implement a stronger preventative access control. Which of the following would BEST complete the engineer's assignment?

- (A). Replacing the traditional key with an RFID key
- (B). Installing and monitoring a camera facing the door
- (C). Setting motion-sensing lights to illuminate the door on activity
- (D). Surrounding the property with fencing and gates

Answer: C

NO.323 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). Unsecured protocols
- (B). Default settings
- (C). Open permissions
- (D). Weak encryption

Answer: D

NO.324 The Chief Information Security Officer (CISO) of a bank recently updated the incident response policy. The CISO is concerned that members of the incident response team do not understand their roles. The bank wants to test the policy but with the least amount of resources or impact. Which of the following BEST meets the requirements?

- (A). Warm site failover
- (B). Tabletop walk-through
- (C). Parallel path testing

(D). Full outage simulation

Answer: B

NO.325 A cloud service provider has created an environment where customers can connect existing local networks to the cloud for additional computing resources and block internal HR applications from reaching the cloud. Which of the following cloud models is being used?

- (A). Public
- (B). Community
- (C). Hybrid
- (D). Private

Answer: C

NO.326 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.

Answer: A

NO.327 A company is providing security awareness training regarding the importance of not forwarding social media messages from unverified sources. Which of the following risks would this training help to prevent?

- (A). Hoaxes
- (B). SPIMs
- (C). Identity fraud
- (D). Credential harvesting

Answer: A

Hoax

A hoax is a falsehood deliberately fabricated to masquerade as the truth. It is distinguishable from errors in observation or judgment, rumors, urban legends, pseudo sciences, and April Fools' Day events that are passed along in good faith by believers or as jokes.

Identity theft

Identity theft occurs when someone uses another person's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes. The term identity theft was coined in 1964. Identity fraud (also known as identity theft or crime) involves someone using another individual's personal information without consent, often to obtain a benefit.

Credential Harvesting

Credential Harvesting (or Account Harvesting) is the use of MITM attacks, DNS poisoning, phishing, and other vectors to amass large numbers of credentials (username / password combinations) for reuse.

NO.328 A security analyst has been tasked with finding the maximum amount of data loss that can occur before ongoing business operations would be impacted. Which of the following terms BEST defines this metric?

- (A). MTTR
- (B). RTO
- (C). RPO
- (D). MTBF

Answer: A

NO.329 Which of the following supplies non-repudiation during a forensics investigation?

- (A). Dumping volatile memory contents first
- (B). Duplicating a drive with dd
- (C). Using a SHA-2 signature of a drive image
- (D). Logging everyone in contact with evidence
- (E). Encrypting sensitive data

Answer: C

NO.330 As part of a security compliance assessment, an auditor performs automated vulnerability scans. In addition, which of the following should the auditor do to complete the assessment?

- (A). User behavior analysis
- (B). Packet captures
- (C). Configuration reviews
- (D). Log analysis

FAST2TEST.COM

Answer: C

NO.331 A security engineer was assigned to implement a solution to prevent attackers from gaining access by pretending to be authorized users. Which of the following technologies meets the requirement?

- (A). SSO
- (B). IDS
- (C). MFA
- (D). TPM

Answer: C

NO.332 An administrator is configuring a firewall rule set for a subnet to only access DHCP, web pages, and SFTP, and to specifically block FTP. Which of the following would BEST accomplish this goal?

- A. [Permission Source Destination Port]
Allow: Any Any 80
Allow: Any Any 443
Allow: Any Any 67
Allow: Any Any 68
Allow: Any Any 22
Deny: Any Any 21
Deny: Any Any
- B. [Permission Source Destination Port]
Allow: Any Any 80
Allow: Any Any 443
Allow: Any Any 67
Allow: Any Any 68
Deny: Any Any 22
Allow: Any Any 21
Deny: Any Any
- C. [Permission Source Destination Port]
Allow: Any Any 80
Allow: Any Any 443
Allow: Any Any 22
Deny: Any Any 67
Deny: Any Any 68
Deny: Any Any 21
Allow: Any Any
- D. [Permission Source Destination Port]
Allow: Any Any 80
Allow: Any Any 443
Deny: Any Any 67
Allow: Any Any 68
Allow: Any Any 22
Allow: Any Any 21
Allow: Any Any

- (A). Option A
(B). Option B
(C). Option C
(D). Option D

Answer: A

NO.333 An IT manager is estimating the mobile device budget for the upcoming year Over the last five years, the number of devices that were replaced due to loss damage or theft steadily increased by 10%. Which of the following would BEST describe the estimated number of devices to be replaced next year?

- (A). ALE
(B). ARO
(C). RPO
(D). SLE

Answer: A

NO.334 A company is implementing a DLP solution on the file server. The file server has PII, financial information, and health information stored on it. Depending on what type of data that is hosted on the file server, the company wants different DLP rules assigned to the data. Which of the following should the company do to help accomplish this goal?

- (A). Classify the data
- (B). Mask the data
- (C). Assign an application owner
- (D). Perform a risk analysis

Answer: A

NO.335 Two organizations plan to collaborate on the evaluation of new SIEM solutions for their respective companies. A combined effort from both organizations' SOC teams would speed up the effort. Which of the following can be written to document this agreement?

- (A). MOU
- (B). ISA
- (C). SLA
- (D). NDA

Answer: A

NO.336 A Chief Security Officer is looking for a solution that can reduce the occurrence of customers receiving errors from back-end infrastructure when systems go offline unexpectedly. The security architect would like the solution to help maintain session persistence. Which of the following would BEST meet the requirements?

- (A). Reverse proxy
- (B). NIC teaming
- (C). Load balancer
- (D). Forward proxy

Answer: B

NO.337 A security analyst has been asked by the Chief Information Security Officer to

- * develop a secure method of providing centralized management of infrastructure
- * reduce the need to constantly replace aging end user machines
- * provide a consistent user desktop experience

Which of the following BEST meets these requirements?

- (A). BYOD
- (B). Mobile device management
- (C). VDI
- (D). Containers ation

Answer: C

NO.338 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

Answer: B

A certificate signing request (CSR) is one of the first steps towards getting your own SSL/TLS certificate. Generated on the same server you plan to install the certificate on, the CSR contains information (e.g. common name, organization, country) the Certificate Authority (CA) will use to create your certificate. It also contains the public key that will be included in your certificate and is signed with the corresponding private key. We'll go into more details on the roles of these keys below.

NO.339 A security analyst needs to be proactive in understand the types of attacks that could potentially target the company's execute. Which of the following intelligence sources should to security analyst review?

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

Answer: D

NO.340 A company uses wireless tor 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

Answer: B

"EAP is in wide use. For example, in IEEE 802.11 (WiFi) the WPA and WPA2 standards have adopted IEEE 802.1X (with various EAP types) as the canonical authentication mechanism."

https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol The Wi-Fi Alliance added EAP-FAST (along with EAP-TLS and EAP-TTLS) to its list of supported protocols for WPA/WPA2 in 2010.

Source: <https://jaimelightfoot.com/blog/comptia-security-wireless-security/> "EAP has been expanded into multiple versions." * "The Wi-Fi Alliance added PEAP to its list of supported protocols for WPA/WPA2/WPA3." * "The Wi-Fi Alliance added EAP-FAST to its list of supported protocols for WPA/WPA2/WPA3." * "The Wi-Fi Alliance added EAP-TTLS to its list of supported protocols for WPA/WPA2/WPA3." Excerpt From: Wm. Arthur Conklin. "CompTIA Security+ All-in-One Exam Guide (Exam SY0-601)."