Exam Topic Breakdown

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

Topic 3, Exam Set 3

Question #:1 - (Exam Topic 3)

A web server has been compromised due to a ransomware attack. Further Investigation reveals the ransomware has been in the server for the past 72 hours. The systems administrator needs to get the services back up as soon as possible. Which of the following should the administrator use to restore services to a secure state?

A. The last incremental backup that was conducted 72 hours ago

B. The last known-good configuration stored by the operating system

C. The last full backup that was conducted seven days ago

D. The baseline OS configuration

Question #:2 - (Exam Topic 3)

A company recently experienced a significant data loss when proprietary information was leaked to a competitor. The company took special precautions by using proper labels; however, email filter logs do not have any record of the incident. An investigation confirmed the corporate network was not breached, but documents were downloaded from an employee's COPE tablet and passed to the competitor via cloud storage. Which of the following is the best mitigation strategy to prevent this from happening in the future?

A. User training

B. CAsB

C. MDM

D. EDR

Question #:3 - (Exam Topic 3)

An organization experiences a cybersecurity incident involving a command-and-control server. Which of the following logs should be analyzed to identify the impacted host? (Select two).

A. Application

B. Authentication

C. Error

D. Network

E. Firewall

F. System

Question #:4 - (Exam Topic 3)

Which of the following is most likely to contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented?

A. An RTO report

B. A risk register

C. A business impact analysis

D. An asset value register

E. A disaster recovery plan

Question #:5 - (Exam Topic 3)

During an assessment, a systems administrator found several hosts running FTP and decided to immediately block FTP communications at the firewall. Which of the following describes the greatest risk associated with using FTP?

A. Private data can be leaked

B. FTP is prohibited by internal policy.

C. Users can upload personal files

D. Credentials are sent in cleartext.

Question #:6 - (Exam Topic 3)

Which of the following security concepts should an e-commerce organization apply for protection against erroneous purchases?

A. Privacy

B. Availability

C. Integrity

D. Confidentiality

Question #:7 - (Exam Topic 3)

A security professional wants to enhance the protection of a critical environment that is used to store and manage a company's encryption keys. The selected technology should be tamper resistant. Which of the following should the security professional implement to achieve the goal?

A. DLP

B. HSM

C. CA

D. FIM

Question #:8 - (Exam Topic 3)

A security analyst discovers that one of the web APIs is being abused by an unknown third party. Logs indicate that the third party is attempting to manipulate the parameters being passed to the API endpoint. Which of the following solutions would best help to protect against the attack?

A. DLP

B. SIEM

C. NIDS

D. WAF

Question #:9 - (Exam Topic 3)

Which of the following automation use cases would best enhance the security posture Of an organi-zation by rapidly updating permissions when employees leave a company or change job roles internally?

A. Provisioning resources

B. Disabling access

C. APIs

D. Escalating permission requests

Question #:10 - (Exam Topic 3)

A company's help desk has received calls about the wireless network being down and users being unable to connect to it. The network administrator says all access points are up and running One of the help desk technicians notices the affected users are working in a building near the parking lot. Which of the following is the most likely reason for the outage?

A. Someone near the building is jamming the signal

B. A user has set up a rogue access point near the building

C. Someone set up an evil twin access point in the affected area.

D. The APs in the affected area have been unplugged from the network

Question #:11 - (Exam Topic 3)

Which of the following types of controls is a turnstile?

A. Physical

B. Detective

C. Corrective

D. Technical

Question #:12 - (Exam Topic 3)

A company wants to deploy decoy systems alongside production systems in order to entice threat actors and to learn more about attackers. Which of the following best describes these systems?

A. DNS sinkholes

B. Honey pots

C. Virtual machines

D. Neural networks

Question #:13 - (Exam Topic 3)

A security analyst is hardening a network infrastructure The analyst is given the following requirements

• Preserve the use of public IP addresses assigned to equipment on the core router

• Enable "in transport" encryption protection to the web server with the strongest ciphers.

Which of the following should the analyst implement to meet these requirements? (Select two).

A. Configure VLANs on the core router

B. Configure NAT on the core router.

C. Configure BGP on the core router

D. Enable AES encryption on the web server

E. Enable 3DES encryption on the web server

F. Enable TLSv2 encryption on the web server

Question #:14 - (Exam Topic 3)

An organization is repairing damage after an incident. Which of the following controls is being implemented?

A. Detective

B. Preventive

C. Corrective

D. Compensating

Question #:15 - (Exam Topic 3)

Which of the following best ensures minimal downtime for organizations with critical computing equipment located in earthquake-prone areas?

A. Generators and UPS

B. Off-site replication

C. Additional warm site

D. Local

Question #:16 - (Exam Topic 3)

An organization is building a new headquarters and has placed fake cameras around the building in an attempt to discourage potential intruders. Which of the following kinds of controls describes this security method?

A. Detective

B. Deterrent

C. Directive

D. Corrective

Question #:17 - (Exam Topic 3)

Which of the following roles is responsible for defining the protection type and Classification type for a given set of files?

A. General counsel

B. Data owner

C. Risk manager

D. Chief Information Officer

Question #:18 - (Exam Topic 3)

A technician is setting up a new firewall on a network segment to allow web traffic to the internet while hardening the network. After the firewall is configured, users receive errors stating the website could not be located. Which of the following would best correct the issue?

A. Setting an explicit deny to all traffic using port 80 instead of 443

B. Moving the implicit deny from the bottom of the rule set to the top

C. Configuring the first line in the rule set to allow all traffic

D. Ensuring that port 53 has been explicitly allowed in the rule set

Question #:19 - (Exam Topic 3)

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

A. OWASP

B. Vulnerability scan results

C. NIST CSF

D. Third-party libraries

Question #:20 - (Exam Topic 3)

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

A. Nmap

B. CURL

C. Neat

D. Wireshark

Question #:21 - (Exam Topic 3)

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

A. Redundancy

B. RAID 1+5

C. Virtual machines

D. Full backups

Question #:22 - (Exam Topic 3)

Which of the following is a primary security concern for a company setting up a BYOD program?

A. End of life

B. Buffer overflow

C. VM escape

D. Jailbreaking

Question #:23 - (Exam Topic 3)

An organization's corporate offices were destroyed due to a natural disaster, so the organization is now setting up offices in a temporary work space. Which of the following will the organization most likely consult?

A. The business continuity plan

B. The risk management plan

C. The communication plan

D. The incident response plan

Question #:24 - (Exam Topic 3)

A company has installed badge readers for building access but is finding unauthorized individuals roaming the hallways. Which of the following is the most likely cause?

A. Shoulder surfing

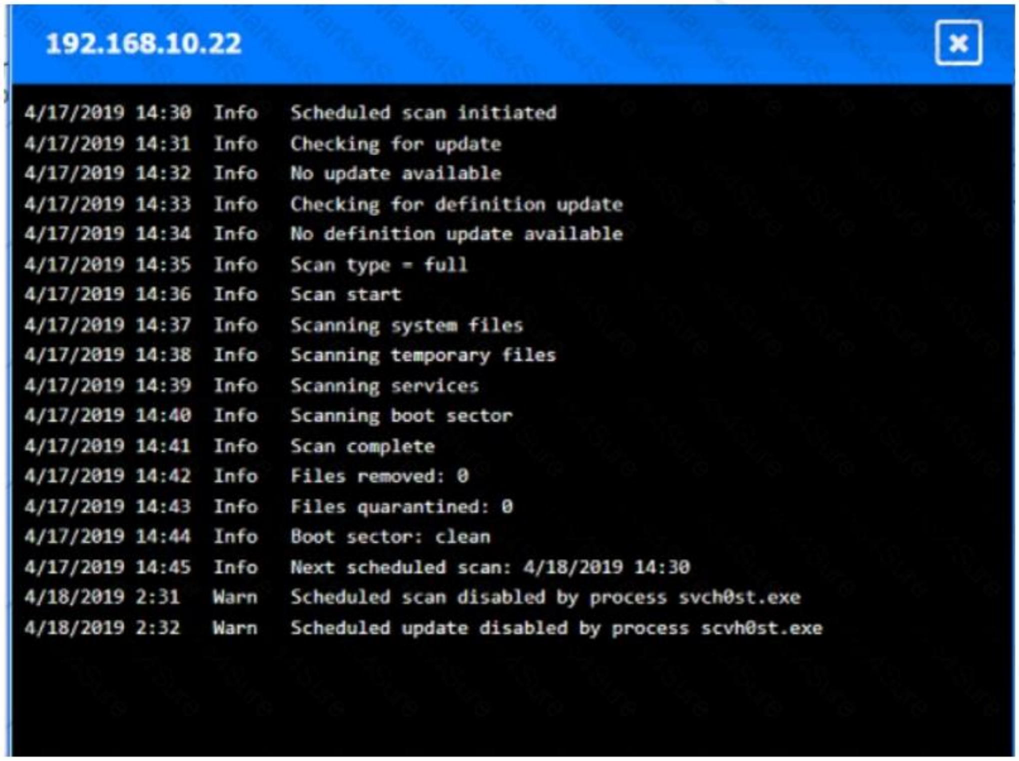
B. Phishing

C. Tailgating

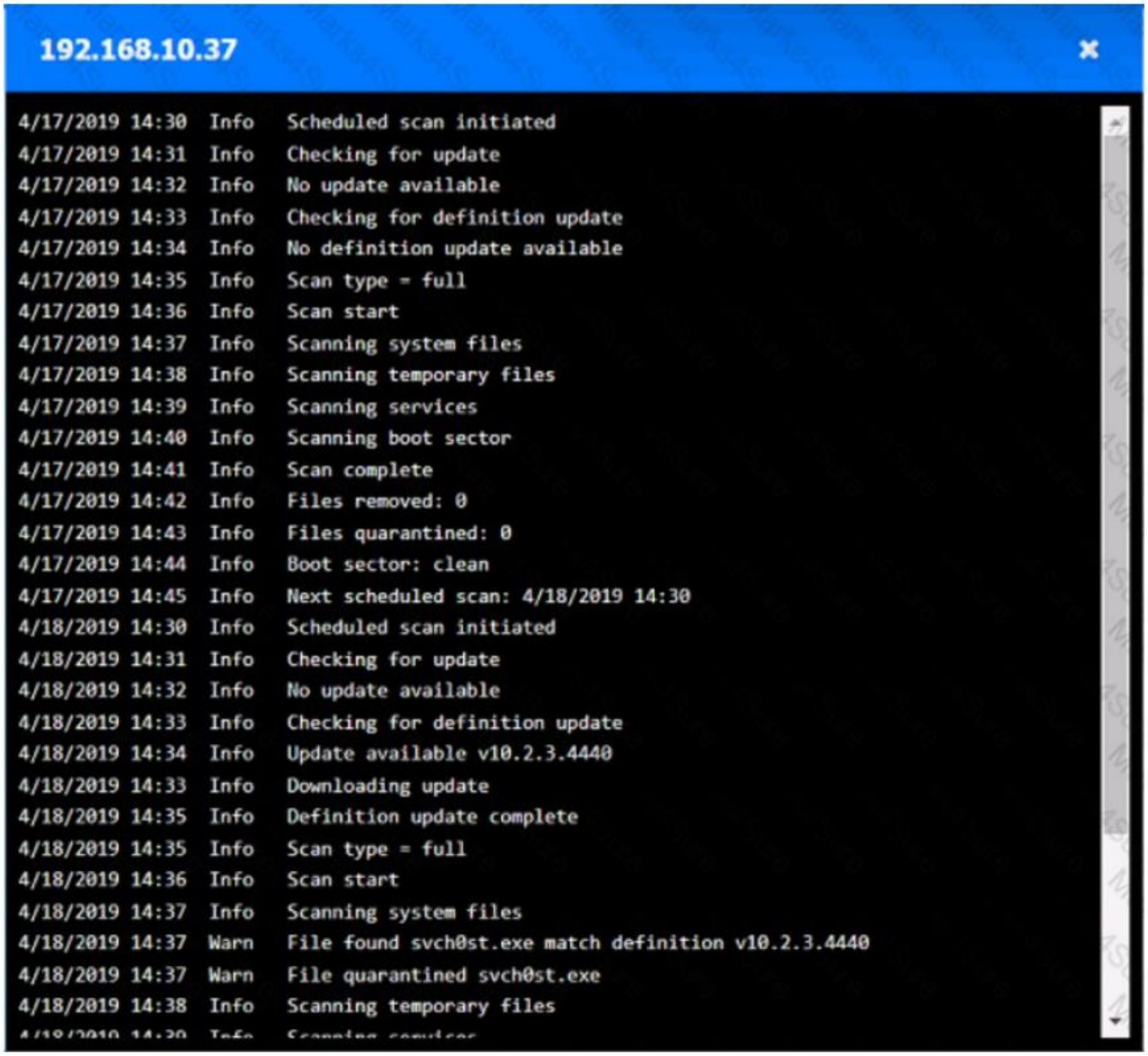
D. Identity fraud

Question #:25 - (Exam Topic 3)

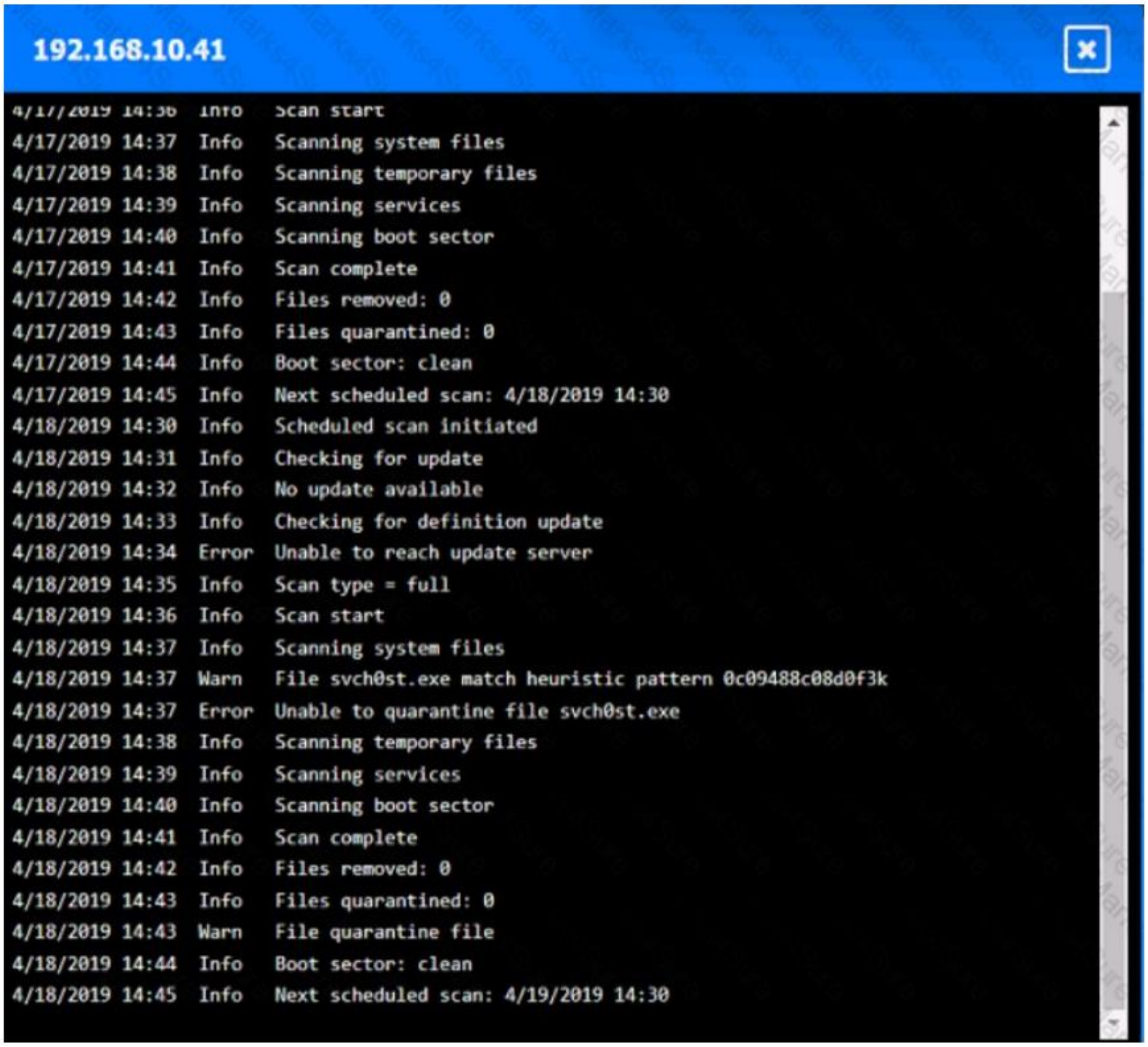
You are security administrator investigating a potential infection on a network.
Click on each host and firewall. Review all logs to determine which host originated the infection and then deny each remaining hosts clean or infected.



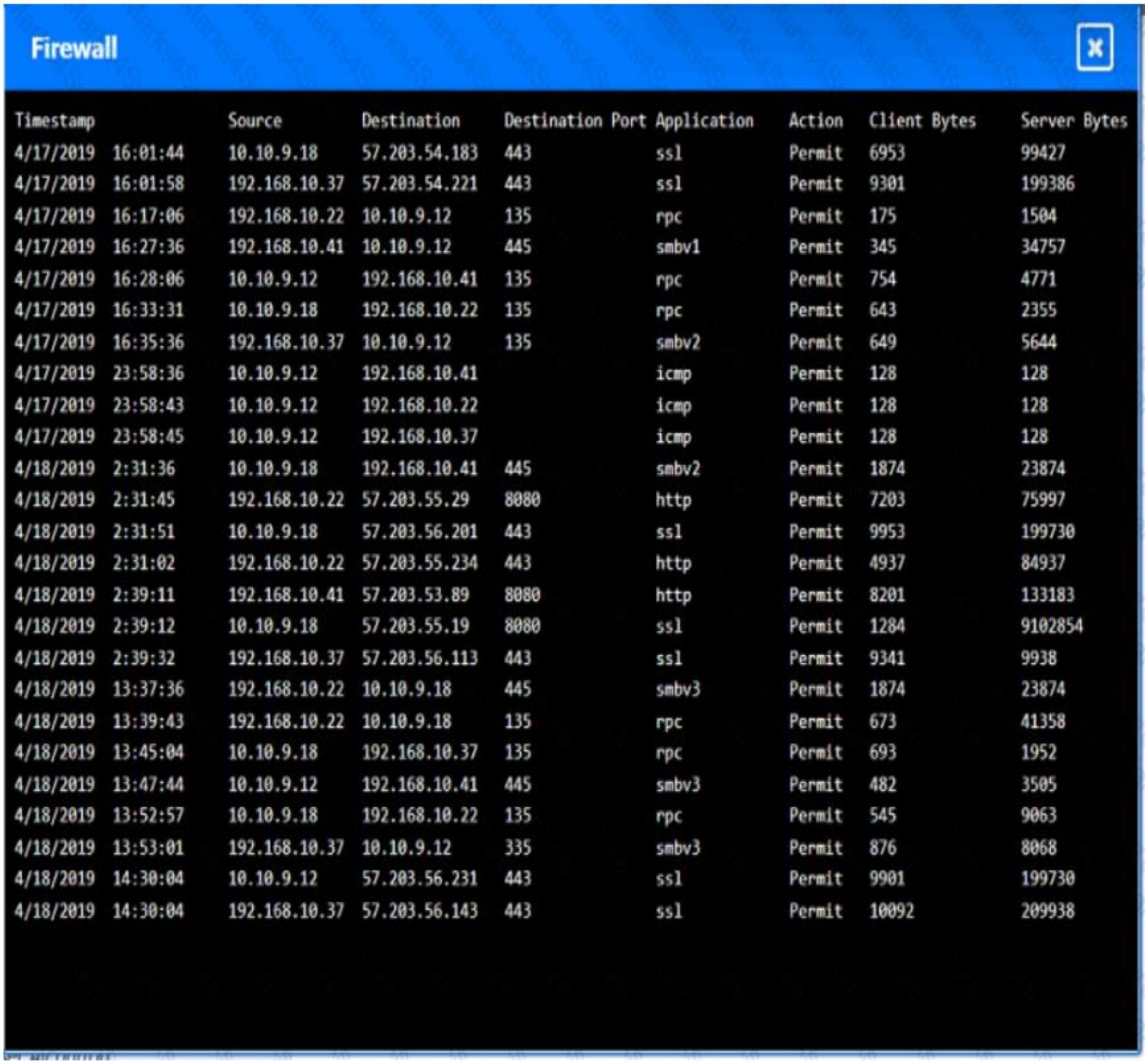
```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 2:31   Warn   Scheduled scan disabled by process svch0st.exe
4/18/2019 2:32   Warn   Scheduled update disabled by process scvh0st.exe
```



```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Info   Update available v10.2.3.4440
4/18/2019 14:33  Info   Downloading update
4/18/2019 14:35  Info   Definition update complete
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37  Warn   File quarantined svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
4/18/2019 14:39  Info   Scanning services
```

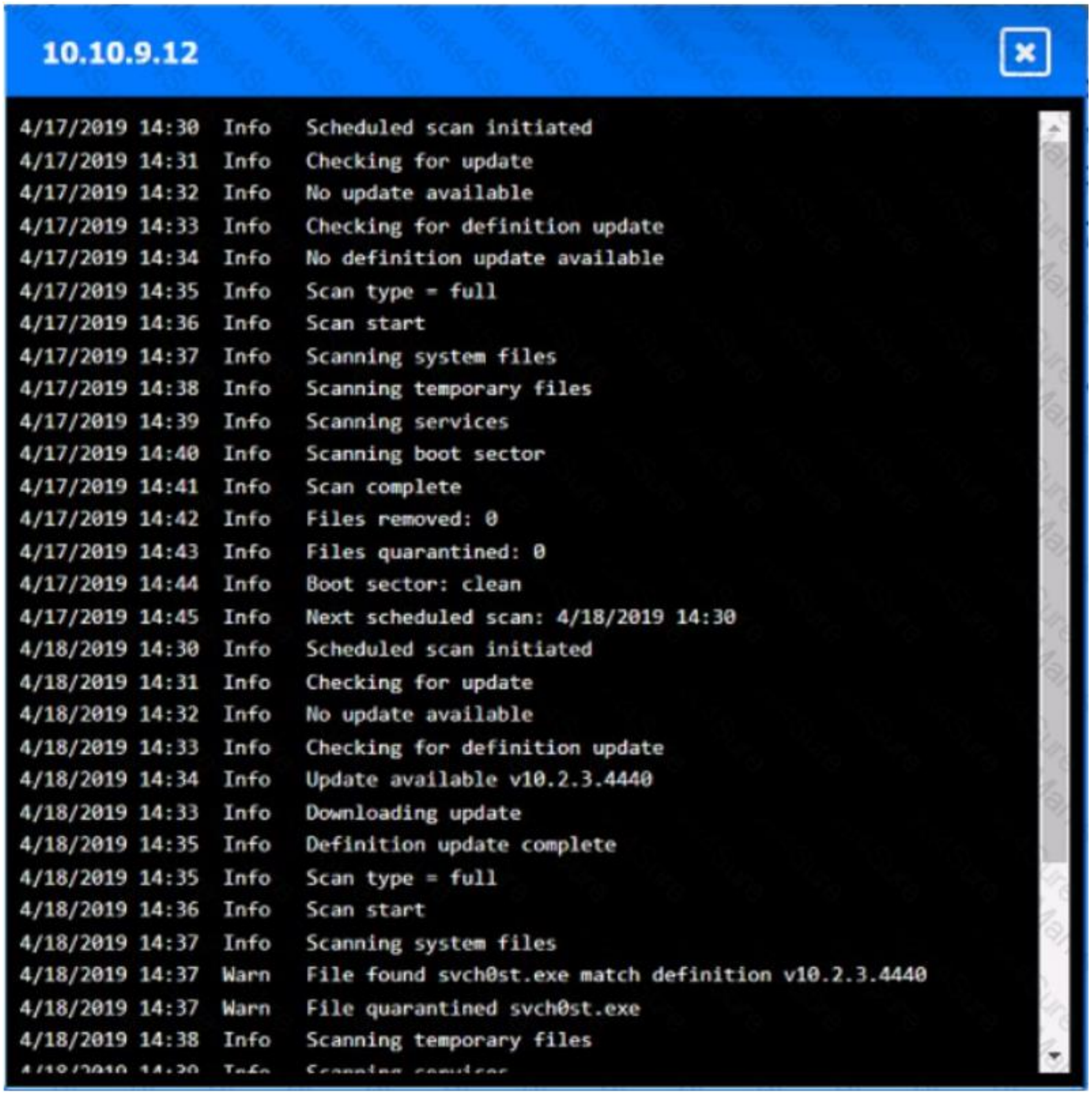


```
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Error  Unable to reach update server
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37  Error  Unable to quarantine file svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
4/18/2019 14:39  Info   Scanning services
4/18/2019 14:40  Info   Scanning boot sector
4/18/2019 14:41  Info   Scan complete
4/18/2019 14:42  Info   Files removed: 0
4/18/2019 14:43  Info   Files quarantined: 0
4/18/2019 14:43  Warn   File quarantine file
4/18/2019 14:44  Info   Boot sector: clean
4/18/2019 14:45  Info   Next scheduled scan: 4/19/2019 14:30
```

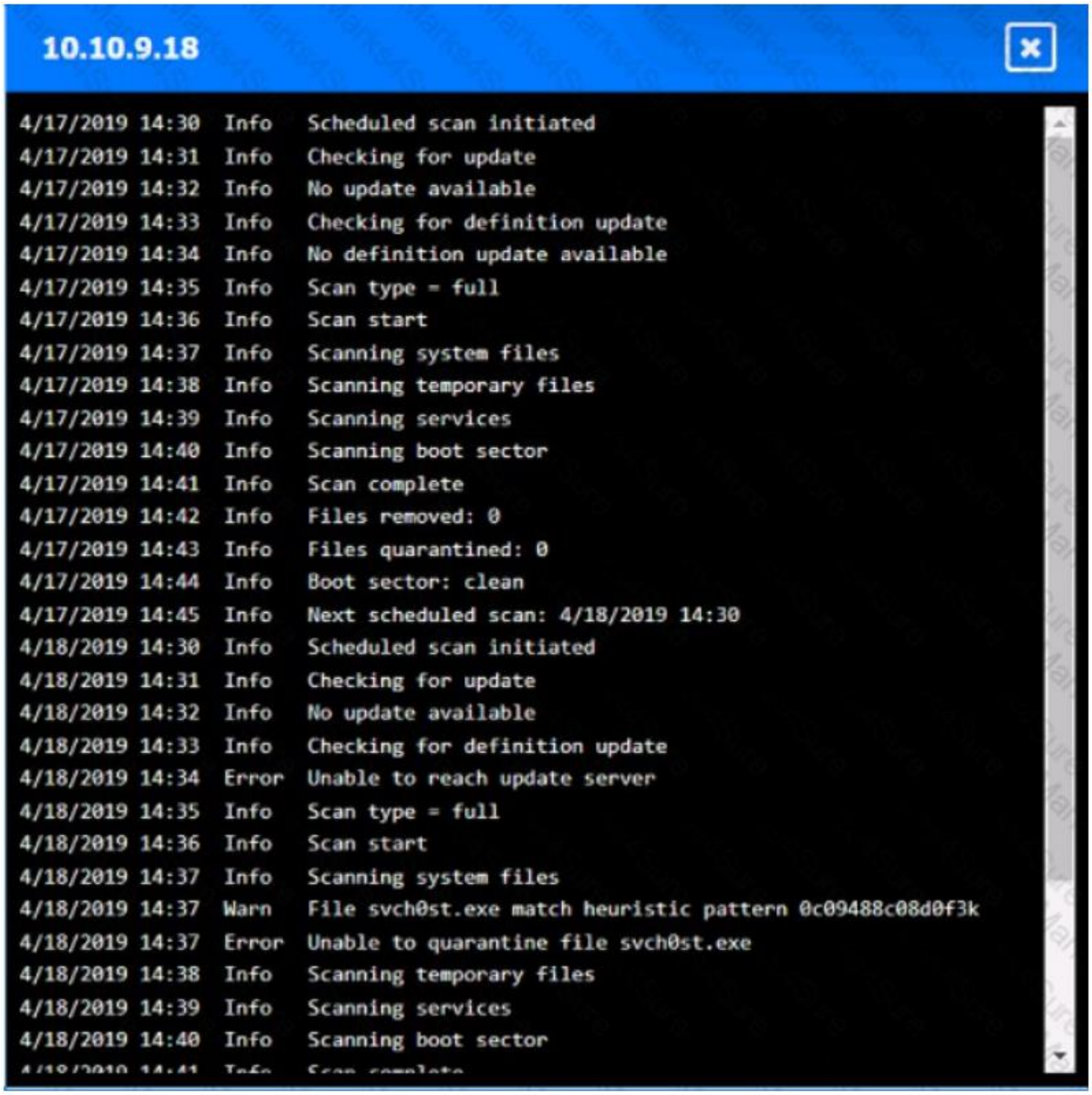


Firewall

```
Timestamp            Source          Destination     Destination Port Application  Action  Client Bytes     Server Bytes
4/17/2019  16:01:44  10.10.9.18      57.203.54.183   443              ssl          Permit  6953             99427
4/17/2019  16:01:58  192.168.10.37   57.203.54.221   443              ssl          Permit  9301             199386
4/17/2019  16:17:06  192.168.10.22   10.10.9.12      135              rpc          Permit  175              1504
4/17/2019  16:27:36  192.168.10.41   10.10.9.12      445              smbv1        Permit  345              34757
4/17/2019  16:28:06  10.10.9.12      192.168.10.41   135              rpc          Permit  754              4771
4/17/2019  16:33:31  10.10.9.18      192.168.10.22   135              rpc          Permit  643              2355
4/17/2019  16:35:36  192.168.10.37   10.10.9.12      135              smbv2        Permit  649              5644
4/17/2019  23:58:36  10.10.9.12      192.168.10.41                    icmp         Permit  128              128
4/17/2019  23:58:43  10.10.9.12      192.168.10.22                    icmp         Permit  128              128
4/17/2019  23:58:45  10.10.9.12      192.168.10.37                    icmp         Permit  128              128
4/18/2019  2:31:36   10.10.9.18      192.168.10.41   445              smbv2        Permit  1874             23874
4/18/2019  2:31:45   192.168.10.22   57.203.55.29    8080             http         Permit  7203             75997
4/18/2019  2:31:51   10.10.9.18      57.203.56.201   443              ssl          Permit  9953             199730
4/18/2019  2:31:02   192.168.10.22   57.203.55.234   443              http         Permit  4937             84937
4/18/2019  2:39:11   192.168.10.41   57.203.53.89    8080             http         Permit  8201             133183
4/18/2019  2:39:12   10.10.9.18      57.203.55.19    8080             ssl          Permit  1284             9102854
4/18/2019  2:39:32   192.168.10.37   57.203.56.113   443              ssl          Permit  9341             9938
4/18/2019  13:37:36  192.168.10.22   10.10.9.18      445              smbv3        Permit  1874             23874
4/18/2019  13:39:43  192.168.10.22   10.10.9.18      135              rpc          Permit  673              41358
4/18/2019  13:45:04  10.10.9.18      192.168.10.37   135              rpc          Permit  693              1952
4/18/2019  13:47:44  10.10.9.12      192.168.10.41   445              smbv3        Permit  482              3505
4/18/2019  13:52:57  10.10.9.18      192.168.10.22   135              rpc          Permit  545              9063
4/18/2019  13:53:01  192.168.10.37   10.10.9.12      335              smbv3        Permit  876              8068
4/18/2019  14:30:04  10.10.9.12      57.203.56.231   443              ssl          Permit  9901             199730
4/18/2019  14:30:04  192.168.10.37   57.203.56.143   443              ssl          Permit  10092            209938
```

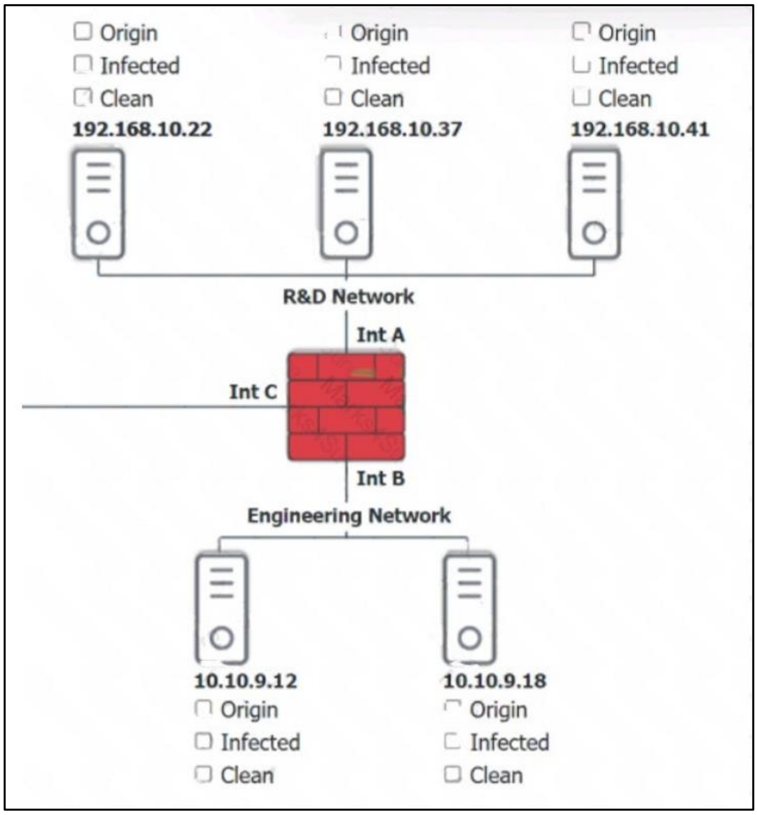


```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Info   Update available v10.2.3.4440
4/18/2019 14:33  Info   Downloading update
4/18/2019 14:35  Info   Definition update complete
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37  Warn   File quarantined svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
4/18/2019 14:39  Info   Scanning services
```



10.10.9.18

```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Error  Unable to reach update server
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37  Error  Unable to quarantine file svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
4/18/2019 14:39  Info   Scanning services
4/18/2019 14:40  Info   Scanning boot sector
4/18/2019 14:41  Info   Scan complete
```



Question #:26 - (Exam Topic 3)

A systems administrator is required to enforce MFA for corporate email account access, relying on the possession factor. Which of the following authentication methods should the systems administrator choose? (Select two).

A. passphrase

B. Time-based one-time password

C. Facial recognition

D. Retina scan

E. Hardware token

F. Fingerprints

Question #:27 - (Exam Topic 3)

An annual information security has revealed that several OS-level configurations are not in compliance due to Outdated hardening standards the company is using. Which of the following would be best to use to update and reconfigure the OS.level security configurations?

A. CIS benchmarks

B. GDPR guidance

C. Regional regulations

D. ISO 27001 standards

Question #:28 - (Exam Topic 3)

Which of the following supplies non-repudiation during a forensics investigation?

A. Dumping volatile memory contents first

B. Duplicating a drive with dd

C. Using a SHA-2 signature of a drive image

D. Logging everyone in contact with evidence

E. Encrypting sensitive data

Question #:29 - (Exam Topic 3)

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

Question #:30 - (Exam Topic 3)

A company recently suffered a breach in which an attacker was able to access the internal mail servers and directly access several user inboxes. A large number of email messages were later posted online. Which of the following would best prevent email contents from being released should another breach occur?

A. Implement S/MIME to encrypt the emails at rest.

B. Enable full disk encryption on the mail servers.

C. Use digital certificates when accessing email via the web.

D. Configure web traffic to only use TLS-enabled channels.

Question #:31 - (Exam Topic 3)

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

Question #:32 - (Exam Topic 3)

An attack has occurred against a company.

INSTRUCTIONS

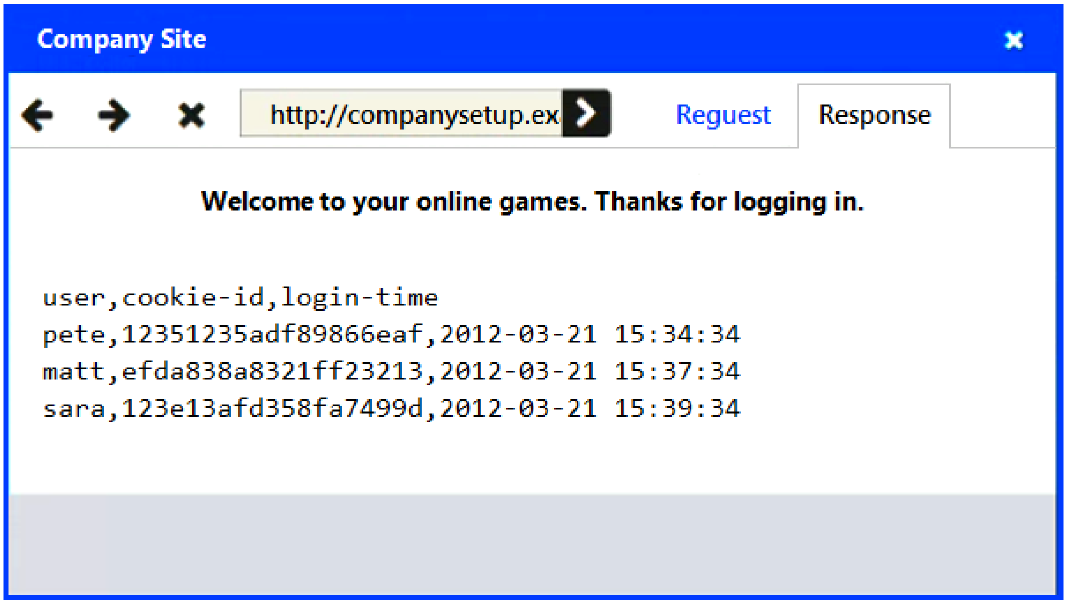
You have been tasked to do the following:

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.

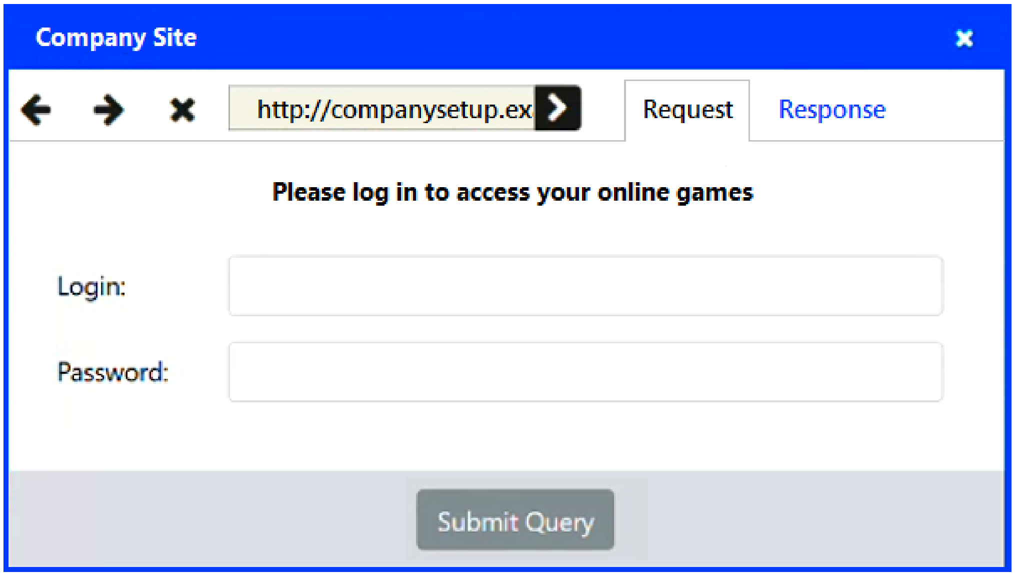
(Answer area 2) All objects will be used, but not all placeholders may be filled. Objects may only be used once.

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



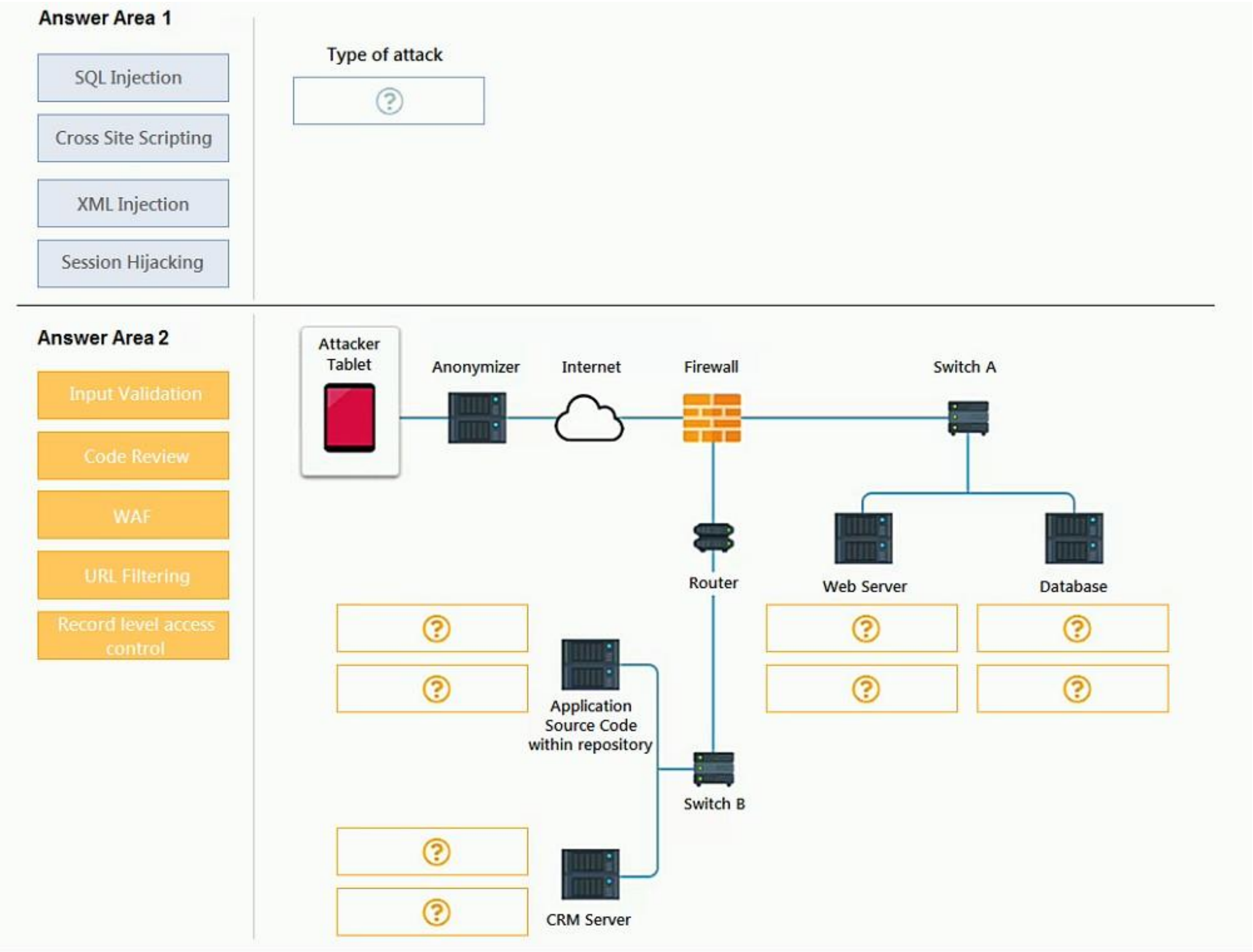
Welcome to your online games. Thanks for logging in.

```
user,cookie-id,login-time
pete,12351235adf89866eaf,2012-03-21 15:34:34
matt,efda838a8321ff23213,2012-03-21 15:37:34
sara,123e13afd358fa7499d,2012-03-21 15:39:34
```



Please log in to access your online games

Select and Place:



Answer Area 1

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

Type of attack

Answer Area 2

- Input Validation
- Code Review
- WAF
- URL Filtering
- Record level access control

Question #:33 - (Exam Topic 3)

Which of the following would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed?

A. A full inventory of all hardware and software

B. Documentation of system classifications

C. A list of system owners and their departments

D. Third-party risk assessment documentation

Question #:34 - (Exam Topic 3)

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

A. SaaS

B. PaaS

C. laaS

D. DaaS

Question #:35 - (Exam Topic 3)

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

A. CVE

B. SIEM

C. SOAR

D. CVSS

Question #:36 - (Exam Topic 3) NEW

A software development manager wants to ensure the authenticity of the code created by the company. Which of the following options is the most appropriate?

A. Testing input validation on the user input fields

B. Performing code signing on company-developed software

C. Performing static code analysis on the software

D. Ensuring secure cookies are used

Question #:37 - (Exam Topic 3)

During a recent security assessment, a vulnerability was found in a common OS. The OS vendor was unaware of the issue and promised to release a patch within the next quarter. Which of the following best describes this type of vulnerability?

A. Legacy operating system

B. Weak configuration

C. Zero day

D. Supply chain

Question #:38 - (Exam Topic 3)

A security analyst needs to implement security features across smartphones, laptops, and tablets. Which of the following would be the most effective across heterogeneous platforms?

A. Enforcing encryption

B. Deploying GPOs

C. Removing administrative permissions

D. Applying MDM software

Question #:39 - (Exam Topic 3)

An administrator is configuring a firewall rule set for a subnet to only access DHCP, web pages, and SFTP, and to specifically block FTP. Which of the following would BEST accomplish this goal?

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

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

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

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

Question #:40 - (Exam Topic 3)

Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?

A. Compensating control

B. Network segmentation

C. Transfer of risk

D. SNMP traps

Question #:41 - (Exam Topic 3)

A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption.

Which of the following best describes this step?

A. Capacity planning

B. Redundancy

C. Geographic dispersion

D. Tabletop exercise

Question #:42 - (Exam Topic 3)

A network manager is concerned that business may be negatively impacted if the firewall in its data center goes offline. The manager would like to implement a high availability pair to:

A. decrease the mean time between failures.

B. remove the single point of failure.

C. cut down the mean time to repair

D. reduce the recovery time objective

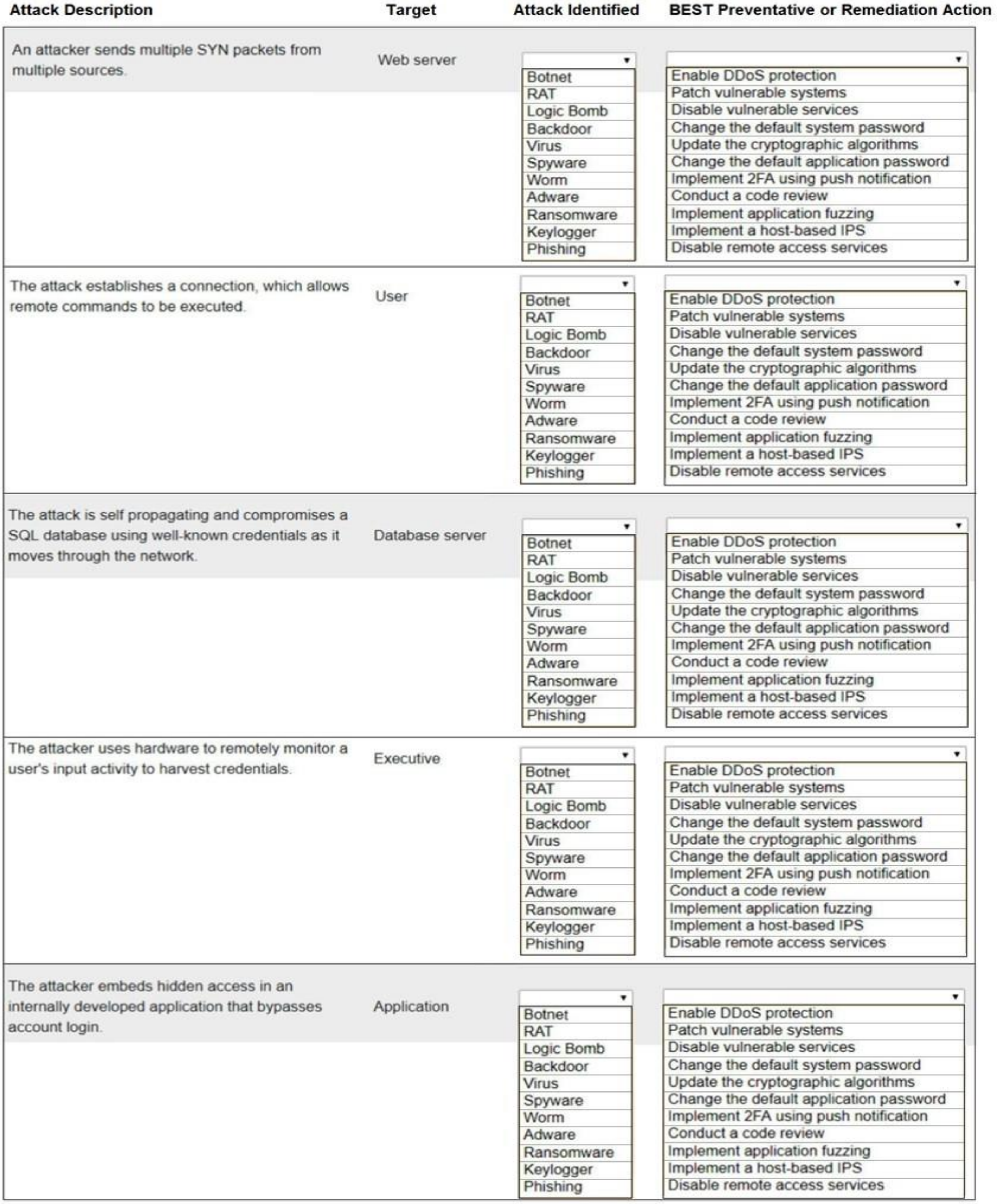
Question #:43 - (Exam Topic 3)

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

Question #:44 - (Exam Topic 3)

Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's PII?

A. SCAP

B. NetFlow

C. Antivirus

D. DLP

Question #:45 - (Exam Topic 3)

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

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

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

A. Session replay

B. Evil twin

C. Bluejacking

D. ARP poisoning

Question #:46 - (Exam Topic 3)

During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the company will grant the employee access to other company-owned websites based on the intranet profile.

Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Select two).

A. Federation

B. Identity proofing

C. Password complexity

D. Default password changes

E. Password manager

F. Open authentication

Question #:47 - (Exam Topic 3)

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

A. IDS solution

B. EDR solution

C. HIPS software solution

D. Network DLP solution

Question #:48 - (Exam Topic 3)

A network penetration tester has successfully gained access to a target machine. Which of the following should the penetration tester do next?

A. Clear the log files of all evidence

B. Move laterally to another machine.

C. Establish persistence for future use.

D. Exploit a zero-day vulnerability.

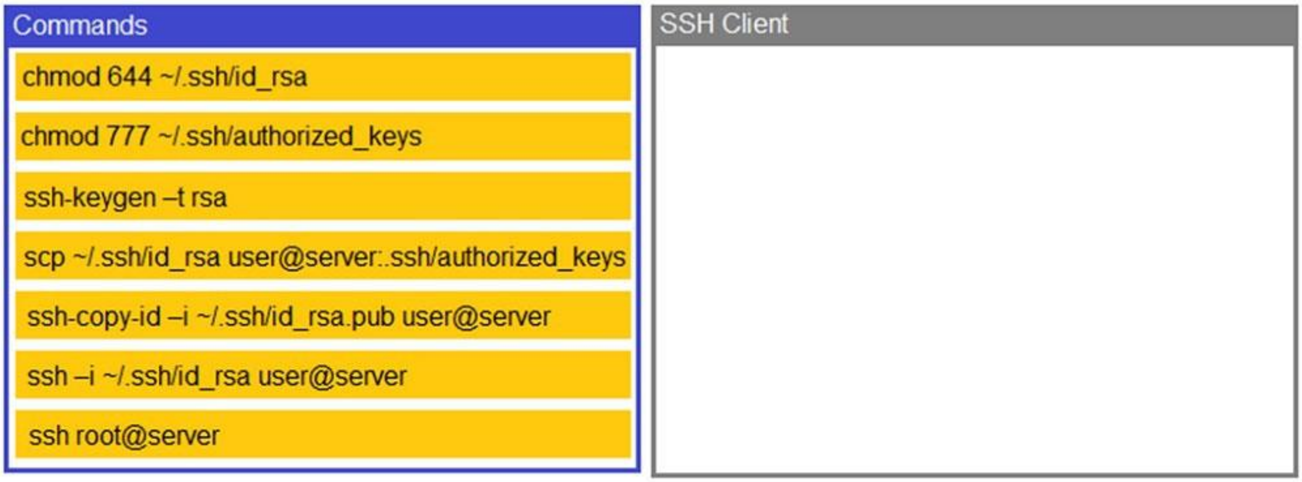
Question #:49 - (Exam Topic 3)

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

INSTRUCTIONS

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

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



```
chmod 644 ~/.ssh/id_rsa
chmod 777 ~/.ssh/authorized_keys
ssh-keygen –t rsa
scp ~/.ssh/id_rsa user@server:.ssh/authorized_keys
ssh-copy-id –i ~/.ssh/id_rsa.pub user@server
ssh –i ~/.ssh/id_rsa user@server
ssh root@server
```

Question #:50 - (Exam Topic 3)

A large retail store's network was breached recently. and this news was made public. The Store did not lose any intellectual property, and no customer information was stolen. Although no fines were incurred as a result, the Store lost revenue after the breach. Which of the following is the most likely reason for this issue?

A. Employee training

B. Leadership changes

C. Reputation

D. Identity theft

Question #:51 - (Exam Topic 3)

A customer called a company's security team to report that all invoices the customer has received over the last five days from the company appear to have fraudulent banking details. An investigation into the matter reveals the following

- The manager of the accounts payable department is using the same password across multiple external websites and the corporate account

- One of the websites the manager used recently experienced a data breach.

- The manager's corporate email account was successfully accessed in the last five days by an IP address located in a foreign country.

Which of the following attacks has most likely been used to compromise the manager's corporate account?

A. Remote access Trojan

B. Brute-force

C. Dictionary

D. Credential stuffing

E. Password spraying

Question #:52 - (Exam Topic 3)

An audit identified Pll being utilized in the development environment of a crit-ical 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 CPOs and the development team's requirements?

A. Data purge

B. Data encryption

C. Data masking

D. Data tokenization

Question #:53 - (Exam Topic 3)

A company wants to deploy PKI on its internet-facing website The applications that are currently deployed are

• www company.com (mam website)

• contact us company com (for locating a nearby location)

• quotes company.com (for requesting a price quote)

The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store company com Which of the following certificate types would best meet the requirements?

A. SAN

B. Wildcard

C. Extended validation

D. Self-signed

Question #:54 - (Exam Topic 3)

An annual information security assessment has revealed that several OS-level configurations are not in compliance due to outdated hardening standards the company is using. Which of the following would be best to use to update and reconfigure the OS-level security configurations?

A. CIS benchmarks

B. GDPR guidance

C. Regional regulations

D. ISO 27001 standards

Question #:55 - (Exam Topic 3)

Which of the following can best protect against an employee inadvertently installing malware on a company system?

A. Host-based firewall

B. System isolation

C. Least privilege

D. Application allow list

Question #:56 - (Exam Topic 3)

A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfiltrated. The report also indicates that users tend to choose the same credentials on different systems and applications. Which of the following policies should the CISO use to prevent someone from using the exfiltrated credentials?

A. MFA

B. Lockout

C. Time-based logins

D. Password history

Question #:57 - (Exam Topic 3)

An organization has expanded its operations by opening a remote office. The new office is fully furnished with office resources to support up to 50 employees working on any given day. Which of the following VPN solutions would best support the new office?

A. Always-on

B. Remote access

C. Site-to-site

D. Full tunnel

Question #:58 - (Exam Topic 3)

A security analyst receives an alert from the company's S1EM 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 property. The IP address the employee provides is 192 168.34 26. Which of the following describes this type of alert?

A. True positive

B. True negative

C. False positive

D. False negative

Question #:59 - (Exam Topic 3)

Which Of the following will provide the best physical security countermeasures to Stop intruders? (Select two).

A. Alarm

B. Signage

C. Lighting

D. Access control vestibules

E. Fencing

F. Sensors

Question #:60 - (Exam Topic 3)

Two organizations are discussing a possible merger Both Organizations Chief Financial Officers would like to safely share payroll data with each Other to determine if the pay scales for different roles are similar at both organizations. Which Of the following techniques would be best to protect employee data while allowing the companies to successfully share this information?

A. Pseudo-anonymization

B. Tokenization

C. Data masking

D. Encryption

Question #:61 - (Exam Topic 3)

A security analyst is taking part in an evaluation process that analyzes and categorizes threat actors Of real-world events in order to improve the incident response team's process. Which Of the following is the analyst most likely participating in?

A. MITRE ATT&CK

B. Walk-through

C. Red team

D. Purple team-I

E. TAXI

Question #:62 - (Exam Topic 3)

A local server recently crashed, and the team is attempting to restore the server from a backup. During the restore process, the team notices the file size of each daily backup is large and will run out of space at the current rate.

The current solution appears to do a full backup every night. Which of the following would use the least amount of storage space for backups?

A. A weekly, incremental backup with daily differential backups

B. A weekly, full backup with daily snapshot backups

C. A weekly, full backup with daily differential backups

D. A weekly, full backup with daily incremental backups

Question #:63 - (Exam Topic 3)

Which Of the following is the best method for ensuring non-repudiation?

A. SSO

B. Digital certificate

C. Token

D. SSH key

Question #:64 - (Exam Topic 3)

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

A. Mobile device management

B. Full device encryption

C. Remote wipe

D. Biometrics

Question #:65 - (Exam Topic 3)

A security analyst is concerned about traffic initiated to the dark web from the corporate LAN. Which of the following networks should the analyst monitor?

A. SFTP

B. AIS

C. Tor

D. loC

Question #:66 - (Exam Topic 3)

An audit report indicates multiple suspicious attempts to access company resources were made. These attempts were not detected by the company. Which of the following would be the best solution to implement on the company's network?

A. Intrusion prevention system

B. Proxy server

C. Jump server

D. Security zones

Question #:67 - (Exam Topic 3)

A security architect is designing a remote access solution for a business partner. The business partner needs to access one Linux server at the company. The business partner wants to avoid managing a password for authentication and additional software installation. Which of the following should the architect recommend?

A. Soft token

B. Smart card

C. CSR

D. SSH key

Question #:68 - (Exam Topic 3)

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

A. Business competitor

B. Hacktivist

C. Criminal syndicate

D. Script kiddie

E. Disgruntled employee

Question #:69 - (Exam Topic 3)

A building manager is concerned about people going in and out of the office during non-working hours.

Which of the following physical security controls would provide the best solution?

A. Cameras

B. Badges

C. Locks

D. Bollards

Question #:70 - (Exam Topic 3)

A cyber-security administrator is using iptables as an enterprise firewall. The administrator created some rules, but the network now seems to be unresponsive. All connections are being dropped by the firewall. Which of the following would be the best option to remove the rules?

A. # iptables -t mangle -X

B. # iptables -F

C. # iptables -2

D. # iptables -P INPUT -j DROP

Question #:71 - (Exam Topic 3)

A web architect would like to move a company's website presence to the cloud. One of the management team's key concerns is resiliency in case a cloud provider's data center or network connection goes down. Which of the following should the web architect consider to address this concern?

A. Containers

B. Virtual private cloud

C. Segmentation

D. Availability zones

Question #:72 - (Exam Topic 3)

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

A. Security information and event management

B. A web application firewall

C. A vulnerability scanner

D. A next-generation firewall

Question #:73 - (Exam Topic 3)

A security analyst is currently addressing an active cyber incident. The analyst has been able to identify affected devices that are running a malicious application with a unique hash. Which of the following is the next step according to the incident response process?

A. Recovery

B. Lessons learned

C. Containment

D. Preparation

Question #:74 - (Exam Topic 3)

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

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

Which of the following is The router experiencing?

A. DDoS attack

B. Memory leak

C. Buffer overflow

D. Resource exhaustion

Question #:75 - (Exam Topic 3)

Which of the following is constantly scanned by internet bots and has the highest risk of attack in the case of the default configurations?

A. Wearable sensors

B. Raspberry Pi

C. Surveillance systems

D. Real-time operating systems

Question #:76 - (Exam Topic 3)

A security architect is required to deploy to conference rooms some workstations that will allow sensitive data to be displayed on large screens. Due to the nature of the data, it cannot be stored in the conference rooms. The file share is located in a local data center. Which of the following should the security architect recommend to best meet the requirement?

A. Fog computing and KVMs

B. VDI and thin clients

C. Private cloud and DLP

D. Full drive encryption and thick clients

Question #:77 - (Exam Topic 3)

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

A. SED

B. HSM

C. DLP

D. TPM

Question #:78 - (Exam Topic 3)

Which of the following vulnerabilities is exploited by an attacker to overwrite a register with a malicious address that changes the execution path?

A. VM escape

B. SQL injection

C. Buffer overflow

D. Race condition

Question #:79 - (Exam Topic 3)

A government organization is developing an advanced AI defense system. Developers are using information collected from third-party providers. Analysts are noticing inconsistencies in the expected performance of the system and attribute the outcome to a recent attack on one of the suppliers. Which of the following IS the most likely reason for the inaccuracy of the system?

A. Improper algorithms security

B. Tainted training data

C. Virus

D. Crypto Malware

Question #:80 - (Exam Topic 3)

Which of the following describes the exploitation of an interactive process to gain access to restricted areas?

A. Persistence

B. Port scanning

C. Privilege escalation

D. Pharming

Question #:81 - (Exam Topic 3)

After multiple on-premises security solutions were migrated to the cloud, the incident response time increased. The analysts are spending a long time trying 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

Question #:82 - (Exam Topic 3)

Cloud security engineers are planning to allow and deny access to specific features in order to increase data security. Which of the following cloud features is the most appropriate to ensure access is granted properly?

A. API integrations

B. Auditing

C. Resource policies

D. Virtual networks

Question #:83 - (Exam Topic 3)

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

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

Which of the following best describes this kind of attack?

A. Directory traversal

B. SQL injection

C. API

D. Request forgery

Question #:84 - (Exam Topic 3)

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

Question #:85 - (Exam Topic 3)

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

A. Something you know

B. Something you have

C. Somewhere you are

D. Someone you know

E. Something you are

F. Something you can do

Question #:86 - (Exam Topic 3)

During a security incident, the security operations team identified a sustained network traffic from a malicious IP address: 10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?

A. access-list inbound deny ip source 0.0.0.0/0 destination 10.1.4.9/32

B. access-list inbound deny ip source 10.1.4.9/32 destination 0.0.0.0/0

C. access-list inbound permit ip source 10.1.4.9/32 destination 0.0.0.0/0

D. access-list inbound permit ip source 0.0.0.0/0 destination 10.1.4.9/32

Question #:87 - (Exam Topic 3)

A security analyst discovers that a company's username and password database were posted on an internet forum. The usernames and passwords are stored in plaintext. Which of the following would mitigate the damage done by this type of data exfiltration in the future?

A. Create DLP controls that prevent documents from leaving the network.

B. Implement salting and hashing.

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

D. Increase password complexity requirements.

Question #:88 - (Exam Topic 3)

A company's help desk received several AV alerts indicating Mimikatz attempted to run on the remote systems. Several users also reported that the new company flash drives they picked up in the break room only have 512KB of storage. Which of the following is most likely the cause?

A. The GPO prevents the use of flash drives, which triggers a false positive AV indication and restricts the drives to only 512KB of storage

B. The new flash drives need a driver that is being blocked by the AV software because the flash drives are not on the application's allow list, temporarily restricting the drives to 512KB of storage.

C. The new flash drives are incorrectly partitioned, and the systems are automatically trying to use an unapproved application to repartition the drives.

D. The GPO blocking the flash drives is being bypassed by a malicious flash drive that is attempting to harvest plaintext credentials from memory.

Question #:89 - (Exam Topic 3)

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

A. SPIM

B. Vishing

C. Spear phishing

D. Smishing

Question #:90 - (Exam Topic 3)

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

A. The DLP appliance should be integrated into a NGFW.

B. Split-tunnel connections can negatively impact the DLP appliance's performance.

C. Encrypted VPN traffic will not be inspected when entering or leaving the network.

D. Adding two hops in the VPN tunnel may slow down remote connections

Question #:91 - (Exam Topic 3)

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. laaS

B. PaaS

C. DaaS

D. SaaS

Question #:92 - (Exam Topic 3)

Which of the following would be used to find the most common web-application vulnerabilities?

A. OWASP

B. MITRE ATT&CK

C. Cyber Kill Chain

D. SDLC

Question #:93 - (Exam Topic 3)

A research company discovered that an unauthorized piece of software has been detected on a small number of machines in its lab. The researchers collaborate with other machines using port 445 and on the internet using port 443. The unauthorized software is starting to be seen on additional machines outside of the lab and is making outbound communications using HTTPS and SMS. The security team has been instructed to resolve the issue as quickly as possible while causing minimal disruption to the researchers. Which of the following is the best course of action in this scenario?

A. Update the host firewalls to block outbound Stv1B.

B. Place the machines with the unapproved software in containment,

C. Place the unauthorized application in a Bocklist.

D. Implement a content filter to block unauthorized software communication.

Question #:94 - (Exam Topic 3)

Which of the following are common VoIP-associated vulnerabilities? (Select two).

A. SPIM

B. Vishing

C. VLAN hopping

D. Phishing

E. DHCP snooping

F. Tailgating

Question #:95 - (Exam Topic 3)

Which of the following terms should be included in a contract to help a company monitor the ongoing security maturity of a new vendor?

A. A right-to-audit clause allowing for annual security audits

B. Requirements for event logs to be kept for minimum of 30 days

C. Integration of threat intelligence in the company's AV

D. A data-breach clause requiring disclosure of significant data loss

Question #:96 - (Exam Topic 3)

An organization has hired a red team to simulate attacks on its security pos-ture, which Of 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

Question #:97 - (Exam Topic 3)

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 the file 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. SMIME

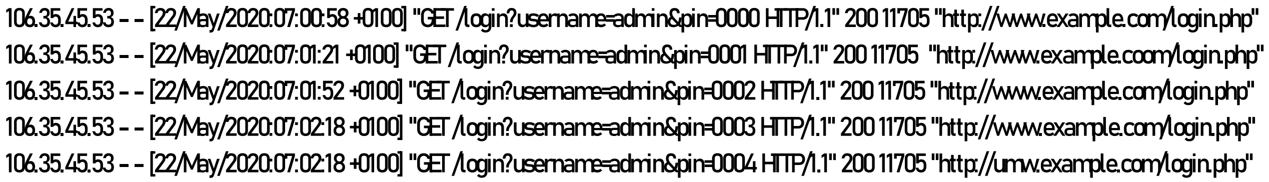
B. LDAPS

C. SSH

D. SRTP

Question #:98 - (Exam Topic 3)

A security analyst is investigating what appears to be unauthorized access to a corporate web application. The security analyst reviews the web server logs and finds the following entries:



```
106.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /login?username=admin&pin=0000 HTTP/1.1" 200 11705 "http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:01:21 +0100] "GET /login?username=admin&pin=0001 HTTP/1.1" 200 11705  "http://www.example.coom/login.php"
106.35.45.53 - - [22/May/2020:07:01:52 +0100] "GET /login?username=admin&pin=0002 HTTP/1.1" 200 11705 "http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:02:18 +0100] "GET /login?username=admin&pin=0003 HTTP/1.1" 200 11705 "http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:02:18 +0100] "GET /login?username=admin&pin=0004 HTTP/1.1" 200 11705 "http://umw.example.com/login.php"
```

Which of the following password attacks is taking place?

A. Dictionary

B. Brute-force

C. Rainbow table

D. Spraying

Question #:99 - (Exam Topic 3)

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

INSTRUCTIONS

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

WAP

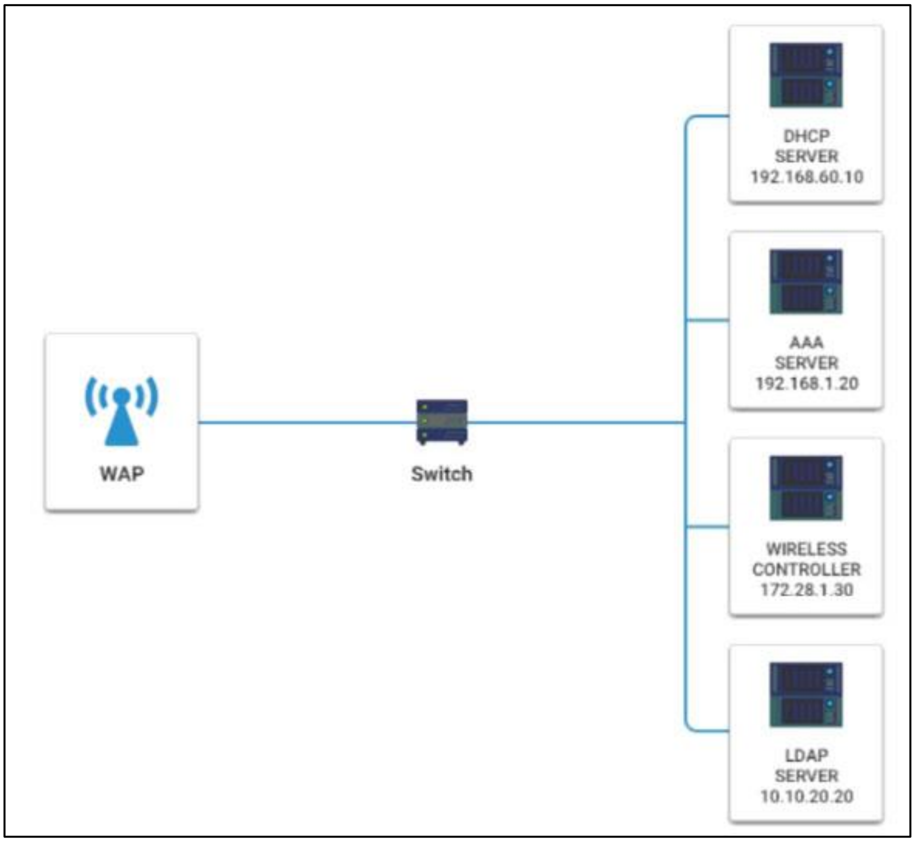
DHCP Server

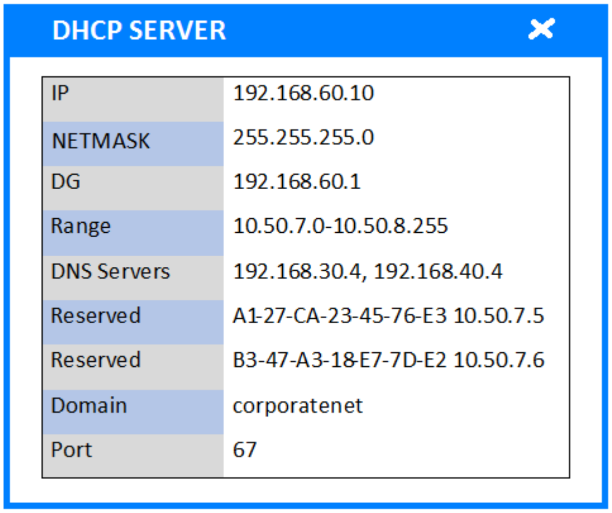
AAA Server

Wireless Controller

LDAP Server

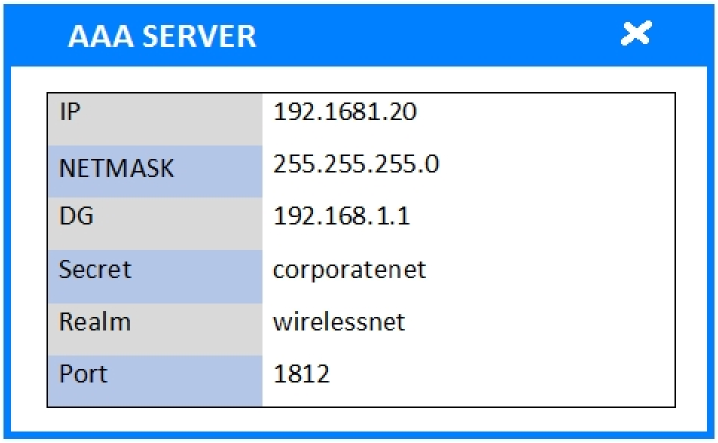
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





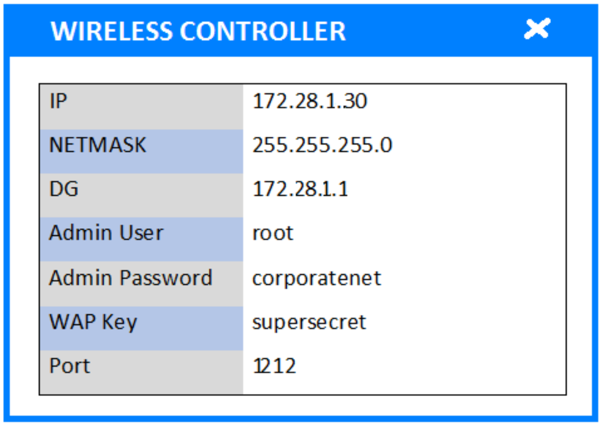
DHCP SERVER

IP	192.168.60.10
NETMASK	255.255.255.0
DG	192.168.60.1
Range	10.50.7.0-10.50.8.255
DNS Servers	192.168.30.4, 192.168.40.4
Reserved	A1-27-CA-23-45-76-E3 10.50.7.5
Reserved	B3-47-A3-18-E7-7D-E2 10.50.7.6
Domain	corporatenet
Port	67



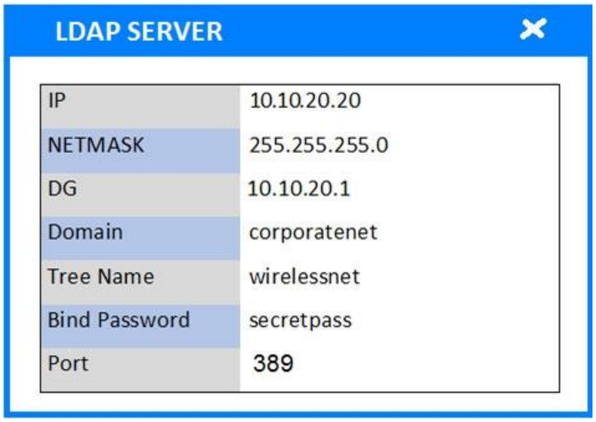
AAA SERVER

IP	192.1681.20
NETMASK	255.255.255.0
DG	192.168.1.1
Secret	corporatenet
Realm	wirelessnet
Port	1812



WIRELESS CONTROLLER

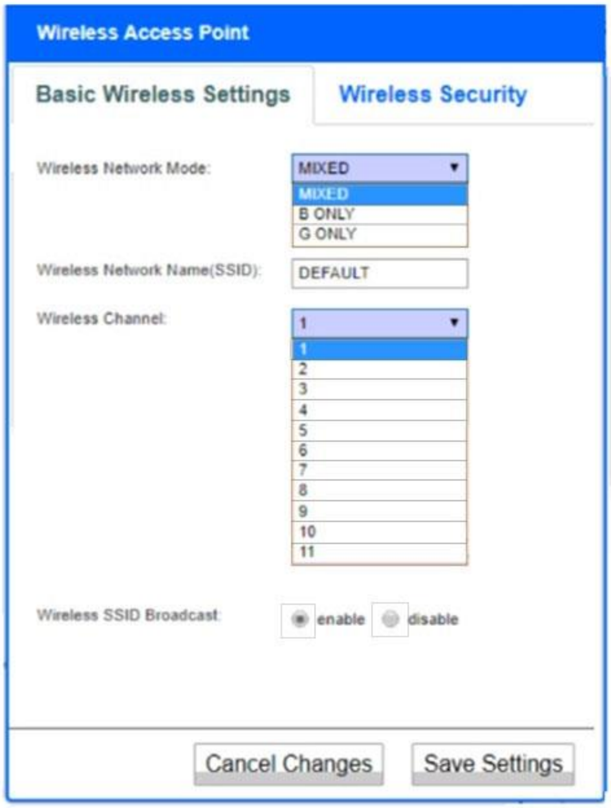
IP	172.28.1.30
NETMASK	255.255.255.0
DG	172.28.1.1
Admin User	root
Admin Password	corporatenet
WAP Key	supersecret
Port	1212



LDAP SERVER

IP	10.10.20.20
NETMASK	255.255.255.0
DG	10.10.20.1
Domain	corporatenet
Tree Name	wirelessnet
Bind Password	secretpass
Port	389

Hot Area:

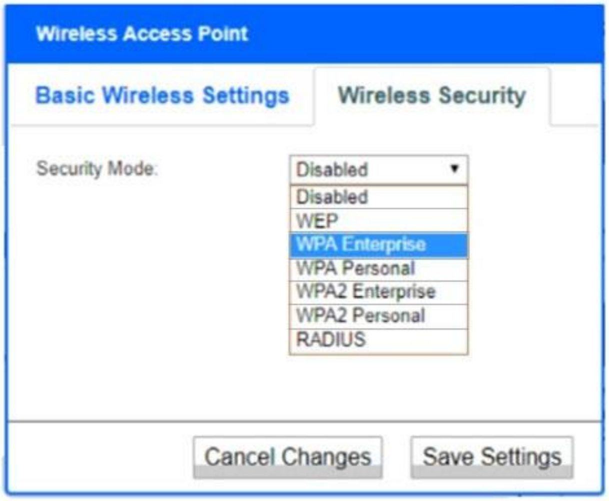


Wireless Network Mode: MIXED

Wireless Network Name(SSID): DEFAULT

Wireless Channel: 1

Wireless SSID Broadcast: ● enable ○ disable



Security Mode: Disabled

Question #:100 - (Exam Topic 3)

While troubleshooting a firewall configuration, a technician determines that a "deny any" policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable. Which of the following actions would prevent this issue?

A. Documenting the new policy in a change request and submitting the request to change management

B. Testing the policy in a non-production environment before enabling the policy in the production network

C. Disabling any intrusion prevention signatures on the "deny any" policy prior to enabling the new policy

D. Including an "allow any" policy above the "deny any" policy

Question #:101 - (Exam Topic 3)

A security analyst notices an unusual amount of traffic hitting the edge of the network. Upon examining the logs, the analyst identifies a source IP address and blocks that address from communicating with the network. Even though the analyst is blocking this address, the attack is still ongoing and coming from a large number of different source IP addresses. Which of the following describes this type of attack?

A. DDoS

B. Privilege escalation

C. DNS poisoning

D. Buffer overflow

Question #:102 - (Exam Topic 3)

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.

Question #:103 - (Exam Topic 3

A company wants to build a new website to sell products online. The website will host a storefront application that allows visitors to add products to a shopping cart and pay for products using a credit card. Which of the following protocols would be most secure to implement?

A. SSL

B. SFTP

C. SNMP

D. TLS

Question #:104 - (Exam Topic 3)

A user downloaded an extension for a browser, and the user's device later became infected. The analyst who is investigating the incident saw various logs where the attacker was hiding activity by deleting data. The following was observed running:

```
New-Partition -DiskNumber 2 -UseMaximumSize -AssignDriveLetter C| Format-Volume
-Driveletter C - FileSystemLabel "New"-FileSystem NTFS - Full -Force -
Confirm:$false
```

Which of the following is the malware using to execute the attack?

A. PowerShell

B. Python

C. Bash

D. Macros

Question #:105 - (Exam Topic 3)

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

A. An external access point is engaging in an evil-Twin attack

B. The signal on the WAP needs to be increased in that section of the building

C. The certificates have expired on the devices and need to be reinstalled

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

Question #:106 - (Exam Topic 3)

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

A. One-time passwords

B. Email tokens

C. Push notifications

D. Hardware authentication

Question #:107 - (Exam Topic 3)

Law enforcement officials sent a company a notification that states electronically stored information and paper documents cannot be destroyed. Which of the following explains this process?

A. Data breach notification

B. Accountability

C. Legal hold

D. Chain of custody

Question #:108 - (Exam Topic 3)

Which of the following best describes configuring devices to log to a centralized, off-site location for possible future reference?

A. Log aggregation

B. DLP

C. Archiving

D. SCAP

Question #:109 - (Exam Topic 3)

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

A. Security

B. Application

C. Dump

D. Syslog

Question #:110 - (Exam Topic 3)

An information security officer at a credit card transaction company is conducting a framework-mapping exercise with the internal controls. The company recently established a new office in Europe. To which of the following frameworks should the security officer map the existing controls? (Select two).

A. ISO

B. PCI DSS

C. SOC

D. GDPR

E. CSA

F. NIST

Question #:111 - (Exam Topic 3)

Security analysts notice a server login from a user who has been on vacation for two weeks, The analysts confirm that the user did not log in to the system while on vacation After reviewing packet capture the analysts notice the following:

Which of the following occurred?

A. A buffer overflow was exploited to gain unauthorized access.

B. The user's account was con-promised, and an attacker changed the login credentials.

C. An attacker used a pass-the-hash attack to gain access.

D. An insider threat with username logged in to the account.