IT-Exams.com®
Easiest way to pass any IT exams

-The original certification question!

https://www.it-exams.com

Exam Number: SY0-601

Exam Name: CompTIA Security+ Exam 2021

Version: Demo

Q1
SIMULATION

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

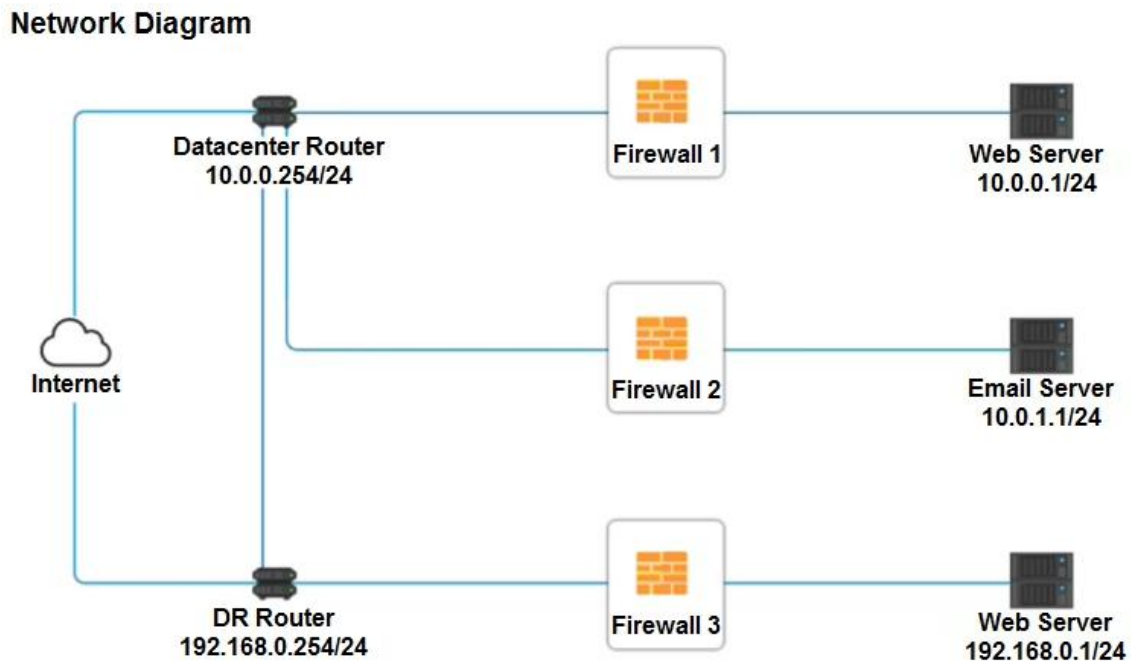
INSTRUCTIONS

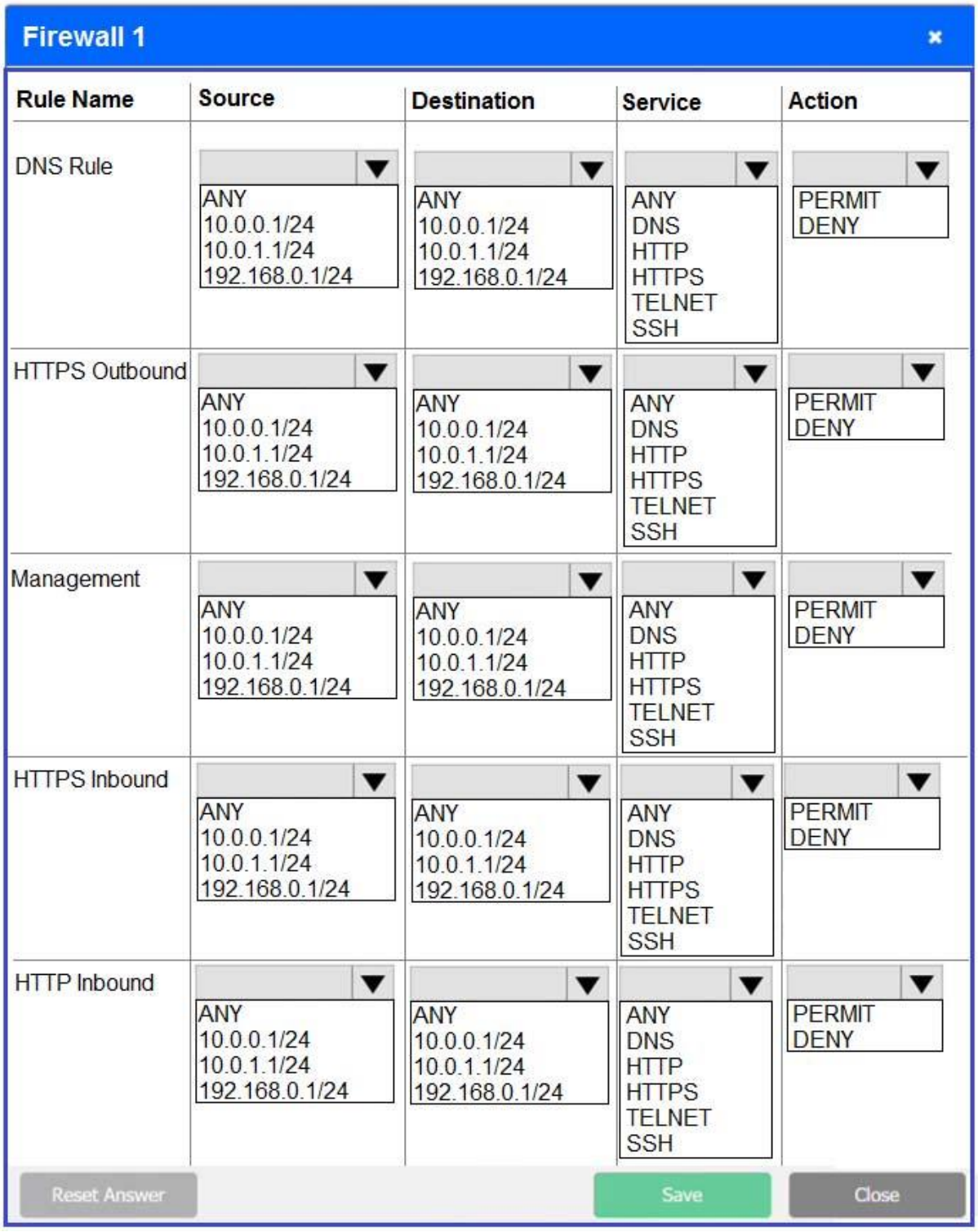
Click on each firewall to do the following:

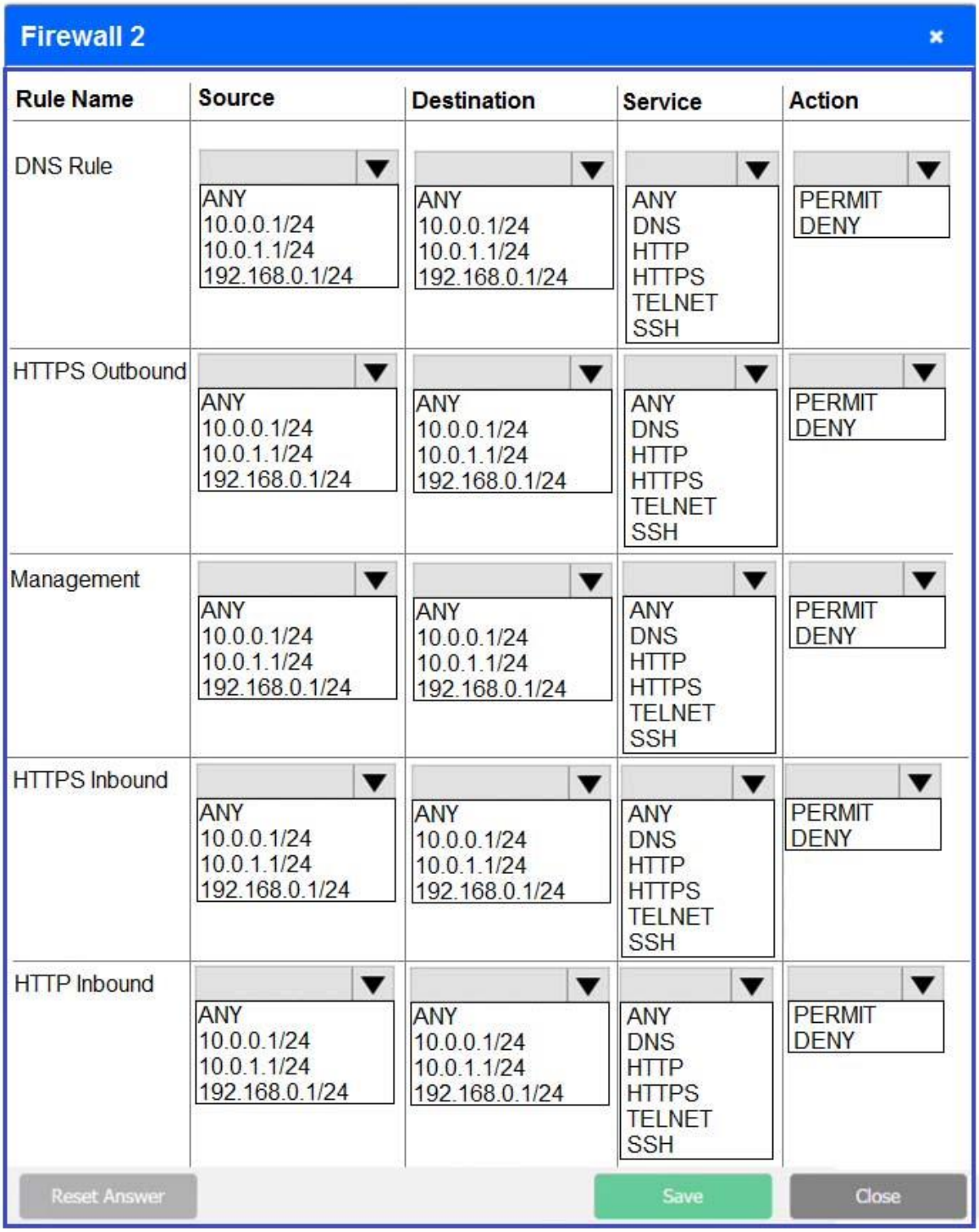
1. Deny cleartext web traffic.
2. Ensure secure management protocols are used.
3. Resolve issues at the DR site.

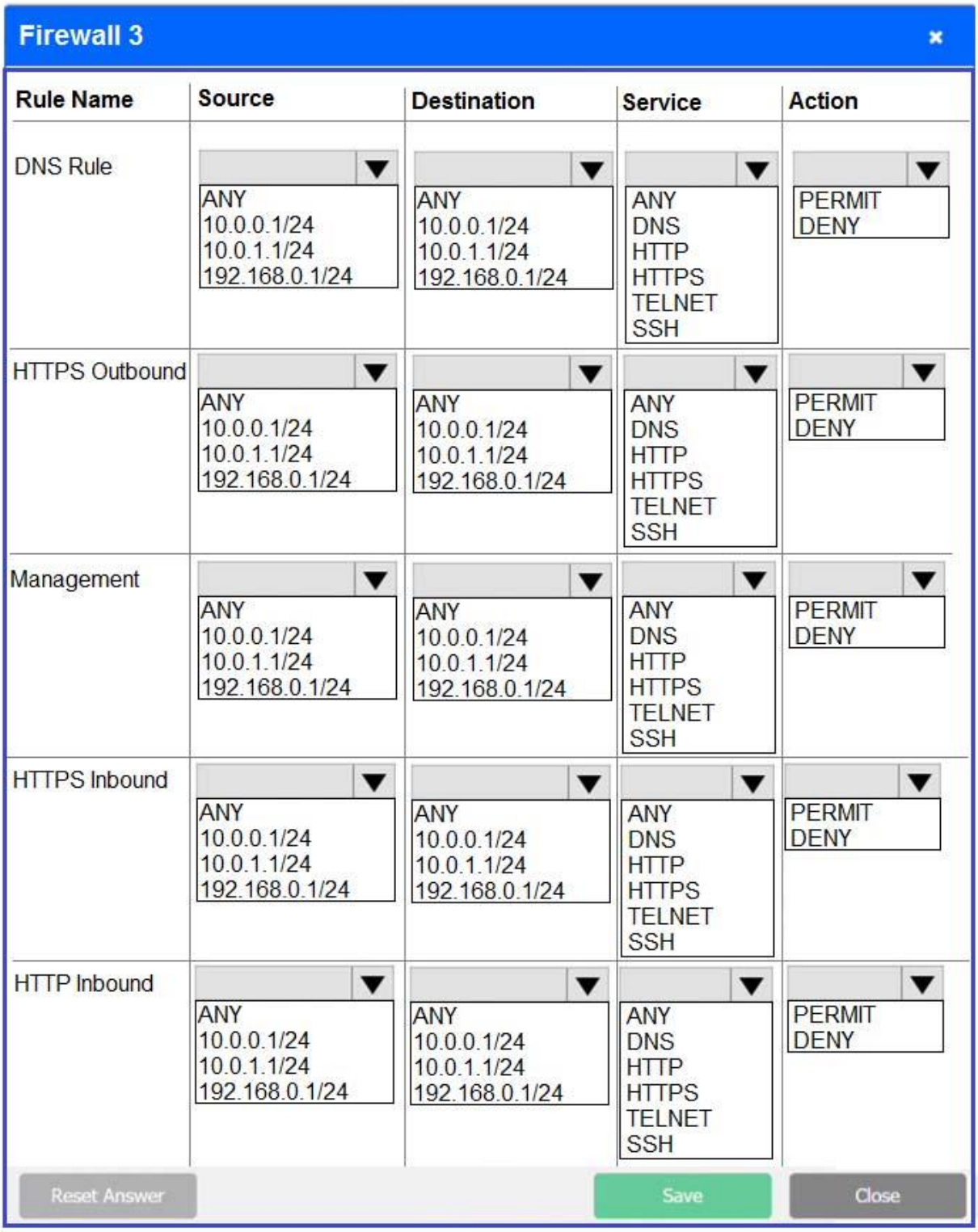
The ruleset order cannot be modified due to outside constraints.

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




Firewall 1
Rule Name
Source
Destination
Service
Action
DNS Rule
HTTPS Outbound
Management
HTTPS Inbound
HTTP Inbound
ANY
10.0.0.1/24
10.0.1.1/24
192.168.0.1/24
ANY
DNS
HTTP
HTTPS
TELNET
SSH
PERMIT
DENY
Reset Answer
Save
Close


Firewall 2
Rule Name
Source
Destination
Service
Action
DNS Rule
HTTPS Outbound
Management
HTTPS Inbound
HTTP Inbound
ANY
10.0.0.1/24
10.0.1.1/24
192.168.0.1/24
ANY
DNS
HTTP
HTTPS
TELNET
SSH
PERMIT
DENY
Reset Answer
Save
Close



A.See explanation below.

Explanation:

Firewall 1:

DNS Rule ?ANY ->; ANY ->; DNS ->; PERMIT

www.it-exams.com original question and answer

HTTPS Outbound ?10.0.0.1/24 ->; ANY ->; HTTPS ->; PERMIT
Management ?ANY ->; ANY ->; SSH ->; PERMIT
HTTPS Inbound ?ANY ->; ANY ->; HTTPS ->; PERMIT
HTTP Inbound ?ANY ->; ANY ->; HTTP ->; DENY

Firewall 2: No changes should be made to this firewall

Firewall 3:

DNS Rule ?ANY ->; ANY ->; DNS ->; PERMIT
HTTPS Outbound ?192.168.0.1/24 ->; ANY ->; HTTPS ->; PERMIT Management ?ANY ->; ANY ->; SSH ->; PERMIT
HTTPS Inbound ?ANY ->; ANY ->; HTTPS ->; PERMIT
HTTP Inbound ?ANY ->; ANY ->; HTTP ->; DENY

Answer:A

Q2
DRAG DROP

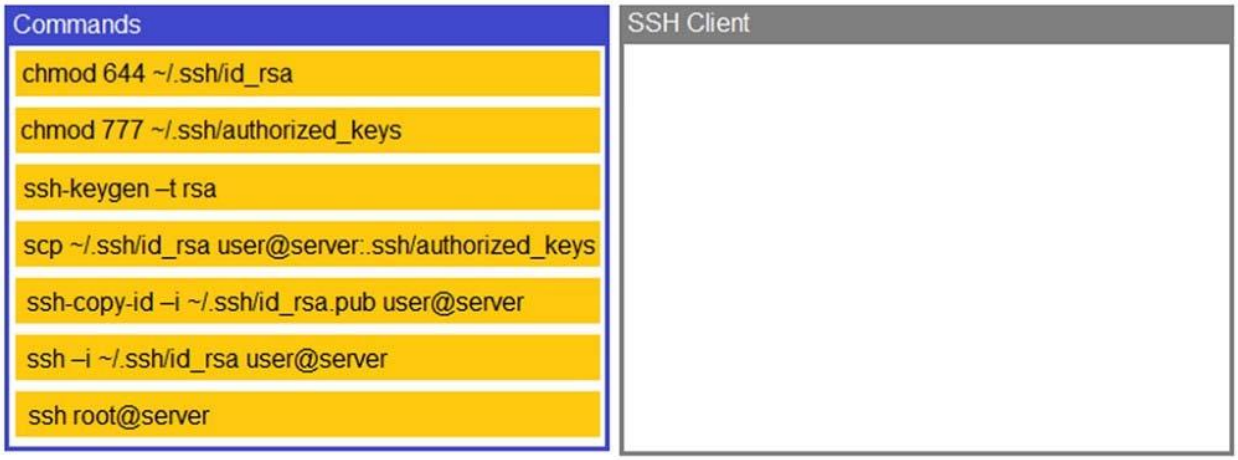
A security engineer is setting up passwordless authentication for the first time.

INSTRUCTIONS

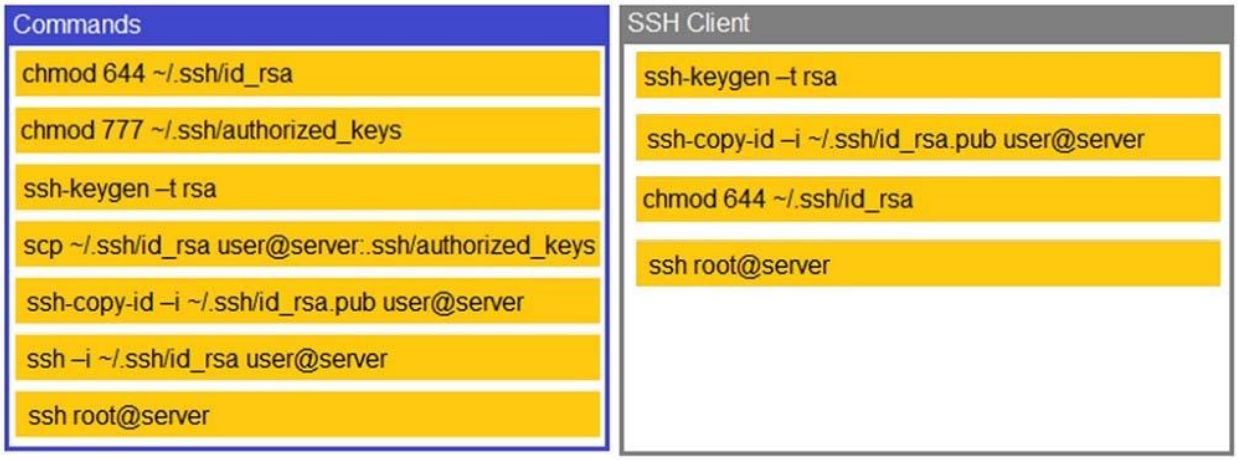
Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.

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

Select and Place:



Answer:



Q3
HOTSPOT

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

INSTRUCTIONS

Not all attacks and remediation actions will be used.

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

Hot Area:

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:

www.it-exams.com original question and answer

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

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

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

Q4
Which of the following will MOST likely adversely impact the operations of unpatched traditional programmable-logic controllers, running a back-end LAMP server and OT systems with human-management interfaces that are accessible over the Internet via a web interface? (Choose two.)

A. Cross-site scripting
B. Data exfiltration
C. Poor system logging
D. Weak encryption
E. SQL injection
F. Server-side request forgery

Answer:DF

Q5
A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices. Which of the following technologies would be BEST to balance the BYOD culture while also protecting the company's data?

A. Containerization
B. Geofencing
C. Full-disk encryption
D. Remote wipe

Answer:C

Q6
A Chief Security Office's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?

A. Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.
B. Purchase cyber insurance from a reputable provider to reduce expenses during an incident.
C. Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.
D. Implement application whitelisting and centralized event-log management, and perform regular testing and validation of full backups.

Answer:D

Q7
A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Choose two.)

A. Perform a site survey
B. Deploy an FTK Imager
C. Create a heat map
D. Scan for rogue access points
E. Upgrade the security protocols
F. Install a captive portal

Answer:AC

Q8
A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk. Which of the following should the administrator use?

A. dd
B. chmod
C. dnsenum
D. logger

Answer:A

Q9
Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

A. SSAE SOC 2
B. PCI DSS
C. GDPR
D. ISO 31000

Answer:C

Q10
Phishing and spear-phishing attacks have been occurring more frequently against a company's staff. Which of the following would MOST likely help mitigate this issue?

A. DNSSEC and DMARC
B. DNS query logging
C. Exact mail exchanger records in the DNS
D. The addition of DNS conditional forwarders

Answer:C

Q11
On which of the following is the live acquisition of data for forensic analysis MOST dependent? (Choose two.)

A. Data accessibility
B. Legal hold
C. Cryptographic or hash algorithm
D. Data retention legislation
E. Value and volatility of data
F. Right-to-audit clauses

Answer:EF

Q12
Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?

A. Investigation
B. Containment
C. Recovery
D. Lessons learned

Answer:B

Q13
A security auditor is reviewing vulnerability scan data provided by an internal security team. Which of the following BEST indicates that valid credentials were used?

A. The scan results show open ports, protocols, and services exposed on the target host
B. The scan enumerated software versions of installed programs
C. The scan produced a list of vulnerabilities on the target host
D. The scan identified expired SSL certificates

Answer:B

Q14
Which of the following BEST explains the difference between a data owner and a data custodian?

A. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data
B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protection to the data
C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data
D. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data

Answer:B

Q15
A network engineer needs to build a solution that will allow guests at the company's headquarters to access the Internet via WiFi. This solution should not allow access to the internal corporate network, but it should require guests to sign off on the acceptable use policy before accessing the Internet. Which of the following should the engineer employ to meet these requirements?

A. Implement open PSK on the APs
B. Deploy a WAF
C. Configure WIPS on the APs
D. Install a captive portal

Answer:D

Q16
A security analyst has been asked to investigate a situation after the SOC started to receive alerts from the SIEM. The analyst first looks at the domain controller and finds the following events:

Keywords	Date and time	Source	Event ID
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:22 PM	Microsoft Windows security auditing	4771

To better understand what is going on, the analyst runs a command and receives the following output:

name	lastbadpasswordattempt	badpwdcount
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst's findings, which of the following attacks is being executed?

A. Credential harvesting
B. Keylogger
C. Brute-force
D. Spraying

Answer:D

Q17
Which of the following cloud models provides clients with servers, storage, and networks but nothing else?

A. SaaS
B. PaaS
C. IaaS
D. DaaS

Answer:C

Q18
A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Choose two.)

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

Answer:AB

Q19
A researcher has been analyzing large data sets for the last ten months. The researcher works with colleagues from other institutions and typically connects via SSH to retrieve additional data. Historically, this setup has worked without issue, but the researcher recently started getting the following message:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@   WARNING:  REMOTE HOST IDENTIFICATION HAS CHANGED!   @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
The fingerprint for the RSA key sent by the remote host is
SHA256:cBqYjal6ToV3jEIJHUSKtjjVziqnVd4Cz+1fhTM6+k4.
Please contact your system administrator.
RSA host key for 18.231.33.78 has changed and you have requested strict checking.
Host key verification failed.
```

Which of the following network attacks is the researcher MOST likely experiencing?

A. MAC cloning
B. Evil twin
C. Man-in-the-middle
D. ARP poisoning

Answer:C

Q20
An organization is developing an authentication service for use at the entry and exit ports of country borders. The service will use data feeds obtained from passport systems, passenger manifests, and high-definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them. Which of the following biometrics will MOST likely be used, without the need for enrollment? (Choose two.)

A. Voice
B. Gait
C. Vein
D. Facial
E. Retina
F. Fingerprint

Answer:BD

Q21
An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:
Check-in/checkout of credentials

The ability to use but not know the password

Automated password changes

Logging of access to credentials

Which of the following solutions would meet the requirements?

A. OAuth 2.0

B. Secure Enclave
C. A privileged access management system
D. An OpenID Connect authentication system

Answer:D

Q22
Several employees return to work the day after attending an industry trade show. That same day, the security manager notices several malware alerts coming from each of the employee's workstations. The security manager investigates but finds no signs of an attack on the perimeter firewall or the NIDS. Which of the following is MOST likely causing the malware alerts?

A. A worm that has propagated itself across the intranet, which was initiated by presentation media
B. A fileless virus that is contained on a vCard that is attempting to execute an attack
C. A Trojan that has passed through and executed malicious code on the hosts
D. A USB flash drive that is trying to run malicious code but is being blocked by the host firewall

Answer:A

Q23
After reading a security bulletin, a network security manager is concerned that a malicious actor may have breached the network using the same software flaw. The exploit code is publicly available and has been reported as being used against other industries in the same vertical. Which of the following should the network security manager consult FIRST to determine a priority list for forensic review?

A. The vulnerability scan output
B. The IDS logs
C. The full packet capture data
D. The SIEM alerts

Answer:A

Q24

A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems. Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization's security posture?

A. Configure the DLP policies to allow all PII
B. Configure the firewall to allow all ports that are used by this application
C. Configure the antivirus software to allow the application
D. Configure the DLP policies to whitelist this application with the specific PII
E. Configure the application to encrypt the PII

Answer:D

Q25
An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state?

A. The system was configured with weak default security settings.
B. The device uses weak encryption ciphers.
C. The vendor has not supplied a patch for the appliance.
D. The appliance requires administrative credentials for the assessment.

Answer:C

Q26
A company's bank has reported that multiple corporate credit cards have been stolen over the past several weeks. The bank has provided the names of the affected cardholders to the company's forensics team to assist in the cyber-incident investigation.

An incident responder learns the following information:
The timeline of stolen card numbers corresponds closely with affected users making Internet-based purchases from diverse websites via enterprise desktop PCs. All purchase connections were encrypted, and the company uses an SSL inspection proxy for the inspection of encrypted traffic of the hardwired network.
Purchases made with corporate cards over the corporate guest WiFi network, where no SSL inspection occurs, were unaffected.

Which of the following is the MOST likely root cause?

A. HTTPS sessions are being downgraded to insecure cipher suites
B. The SSL inspection proxy is feeding events to a compromised SIEM
C. The payment providers are insecurely processing credit card charges
D. The adversary has not yet established a presence on the guest WiFi network

Answer:C

Q27
A pharmaceutical sales representative logs on to a laptop and connects to the public WiFi to check emails and update reports. Which of the following would be BEST to prevent other devices on the network from directly accessing the laptop? (Choose two.)

A. Trusted Platform Module
B. A host-based firewall
C. A DLP solution
D. Full disk encryption
E. A VPN
F. Antivirus software

Answer:AB

Q28
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

Answer:C

Q29
The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

A. Install a NIDS device at the boundary.
B. Segment the network with firewalls.
C. Update all antivirus signatures daily.
D. Implement application blacklisting.

Answer:B

Q30
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

Answer:A

Q31
A development team employs a practice of bringing all the code changes from multiple team members into the same development project through automation. A tool is utilized to validate the code and track source code through version control. Which of the following BEST describes this process?

A. Continuous delivery
B. Continuous integration
C. Continuous validation
D. Continuous monitoring

Answer:B

Q32
A cybersecurity administrator needs to add disk redundancy for a critical server. The solution must have a two- drive failure for better fault tolerance. Which of the following RAID levels should the administrator select?

A. 0
B. 1
C. 5
D. 6

Answer:B