- C. An IP blacklist
- D. Application whitelisting

### Correct Answer: D

## **QUESTION 96**

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

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

### Correct Answer: D

### **QUESTION 97**

A company recently experienced a data breach and the source was determined to be an executive who was charging a phone in a public area. Which of the following would MOST likely have prevented this breach?

- A. A firewall
- B. A device pin
- C. A USB data blocker
- D. Biometrics

Correct Answer: C

## **QUESTION 98**

#### 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.

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Ac
An attacker sends multiple SYN packets from	Web server		· · · · · · · · · · · · · · · · · · ·
multiple sources.	web server	Botnet RAT	Enable DDoS protection Patch vulnerable systems
		Logic Bomb Backdoor	Disable vulnerable services Change the default system password
		Virus	Update the cryptographic algorithms
		Spyware	Change the default application password
		Worm Adware	Implement 2FA using push notification Conduct a code review
		Ransomware	Implement application fuzzing
		Keylogger	Implement a host-based IPS
		Phishing	Disable remote access services
The attack establishes a connection, which allows	User	•	
remote commands to be executed.	User	Botnet	Enable DDoS protection
		RAT Logic Bomb	Patch vulnerable systems Disable vulnerable services
		Backdoor	Change the default system password
		Virus	Update the cryptographic algorithms
		Spyware	Change the default application password
		Worm	Implement 2FA using push notification
		Adware Ransomware	Conduct a code review Implement application fuzzing
		Keylogger	Implement a host-based IPS
		Phishing	Disable remote access services
The attack is self propagating and compromises a			
SQL database using well-known credentials as it	Database server	• Retrot	Enable DDoS protection
moves through the network.		Botnet RAT	Patch vulnerable systems
		Logic Bomb	Disable vulnerable services
		Backdoor	Change the default system password
		Virus	Update the cryptographic algorithms
		Spyware	Change the default application password
		Worm	Implement 2FA using push notification
		Adware	Conduct a code review Implement application fuzzing
		Ransomware Keylogger	Implement a host-based IPS
		Phishing	Disable remote access services
The attacker uses hardware to remotely monitor a	Executive	•	
user's input activity to harvest credentials.	Executive	Botnet	Enable DDoS protection
		RAT	Patch vulnerable systems
		Logic Bomb	Disable vulnerable services Change the default system password
		Backdoor Virus	Update the cryptographic algorithms
		Spyware	Change the default application password
		Worm	Implement 2FA using push notification
		Adware	Conduct a code review
		Ransomware	Implement application fuzzing
		Keylogger Phishing	Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses	Application	V Datast	Fashia DDaS protection
account login.		Botnet RAT	Enable DDoS protection Patch vulnerable systems
		Logic Bomb	Disable vulnerable services
		Backdoor	Change the default system password
		Virus	Update the cryptographic algorithms
		Spyware	Change the default application password
		Worm	Implement 2FA using push notification
		Adware	Conduct a code review
		Ransomware	Implement application fuzzing Implement a host-based IPS
		Keylogger Phishing	Disable remote access services
		r manning	Provide 1011010 000033 30141003

**Correct Answer:** 

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Act
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet I RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection I 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 TPS 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 I Phishing	Enable DDoS protection     Patch vulnerable systems     Disable vulnerable services     I     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 <sup>1</sup> 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 1     Conduct a code review     Implement application fuzzing     Implement a host-based IPS     Disable remote access services

# **QUESTION 99**

HOTSPOT

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

#### INSTRUCTIONS

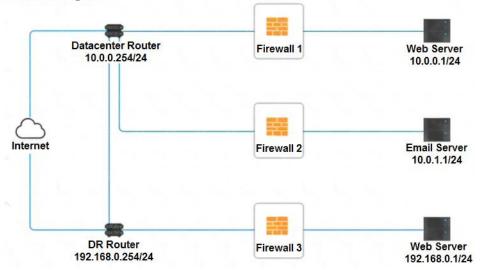
Click on each firewall to do the following:

- Deny cleartext web traffic.
- Ensure secure management protocols are used. Please Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.

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

#### Network Diagram



Firewall 1 ×								
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				
Reset Answer			Save	Close				