

- 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.

[Download Full Version JK0-022 Exam Dumps\(Updated in Feb/2023\)](#)

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

Correct Answer:

[Download Full Version JK0-022 Exam Dumps\(Updated in Feb/2023\)](#)

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

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

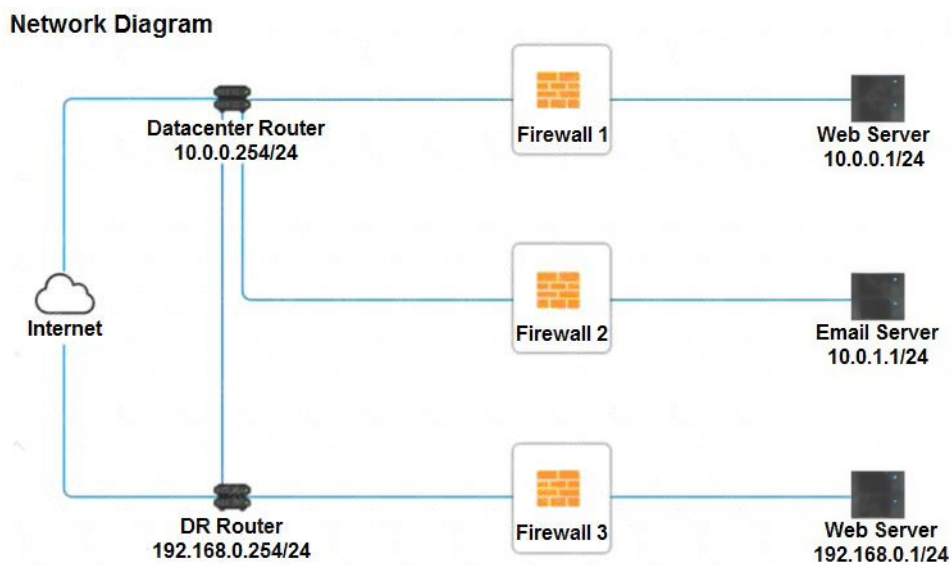
Click on each firewall to do the following:

- 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	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> PERMIT DENY </div> </div>
HTTPS Outbound	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> PERMIT DENY </div> </div>
Management	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> PERMIT DENY </div> </div>
HTTPS Inbound	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> PERMIT DENY </div> </div>
HTTP Inbound	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24 </div> </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> ANY DNS HTTP HTTPS TELNET SSH </div> </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼</div> <div style="padding: 2px;"> PERMIT DENY </div> </div>

Reset Answer

Save

Close