

PBQ:

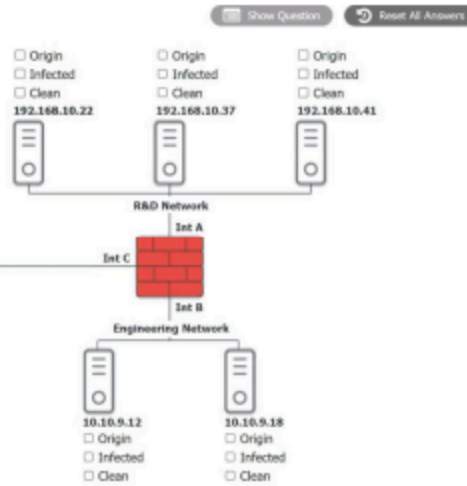
This is simulation

TEST QUESTION

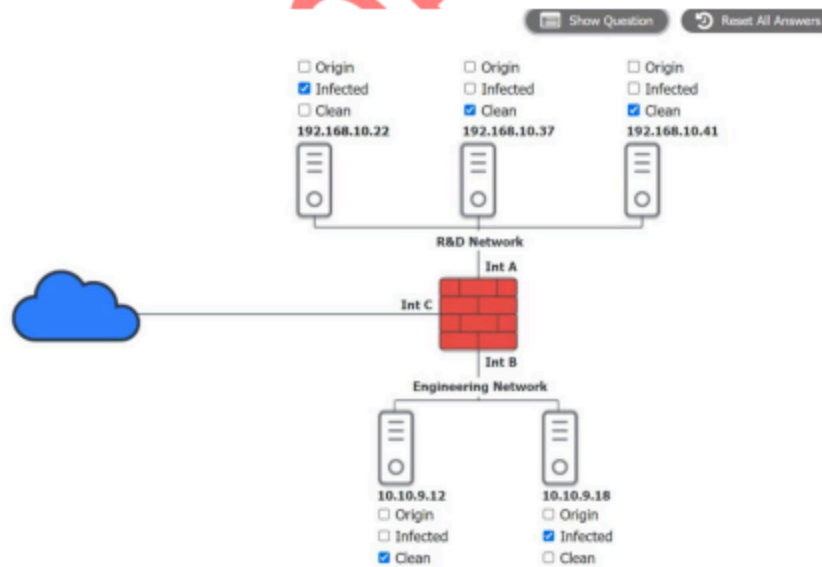
You are a security administrator investigating a potential infection on a network.

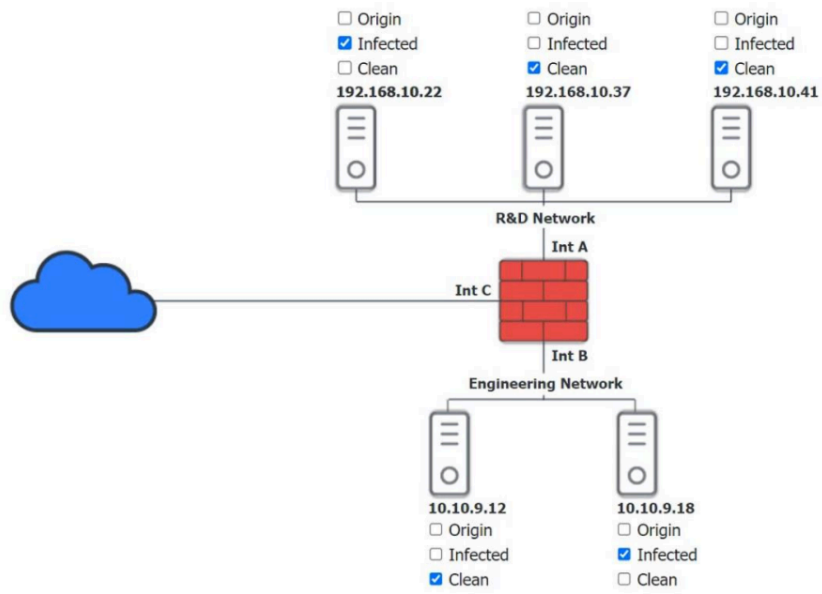
INSTRUCTIONS

Click on each host and firewall. Review all logs to determine which host originated the infection and then identify if each remaining host is clean or infected.
If at any time you would like to bring back the initial state of the simulation, please click the *Reset All* button.



Below is solved





PBQ:

This is simulation

TEST QUESTION

To view the entire simulation, click the X in the upper right corner of this window.

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

| Target | Attack identified | Best preventative or remediation action |
|-----------------|-------------------|---|
| Web server | | |
| User | | |
| Database server | | |
| Executive | | |
| Application | | |

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.

Below is solved

Show Question

Reset All Answers

| 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 |

Below is solved

Show Question

Reset All Answers

| 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 |