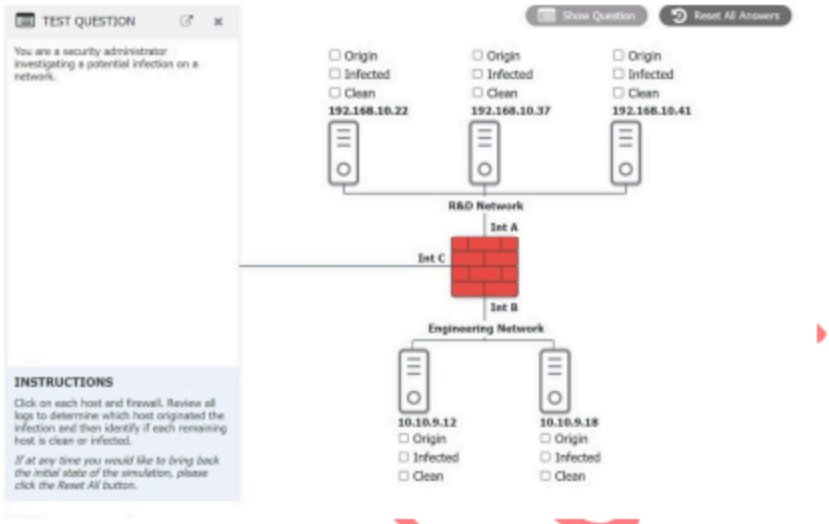
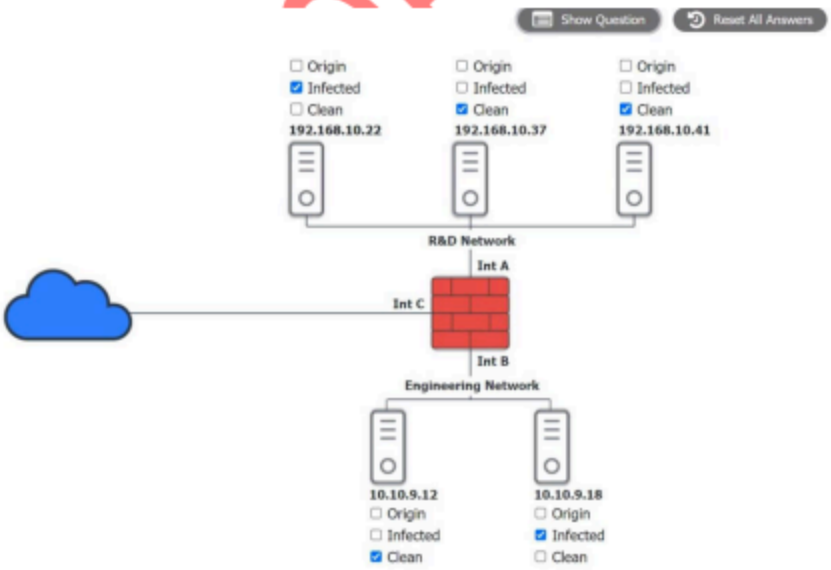
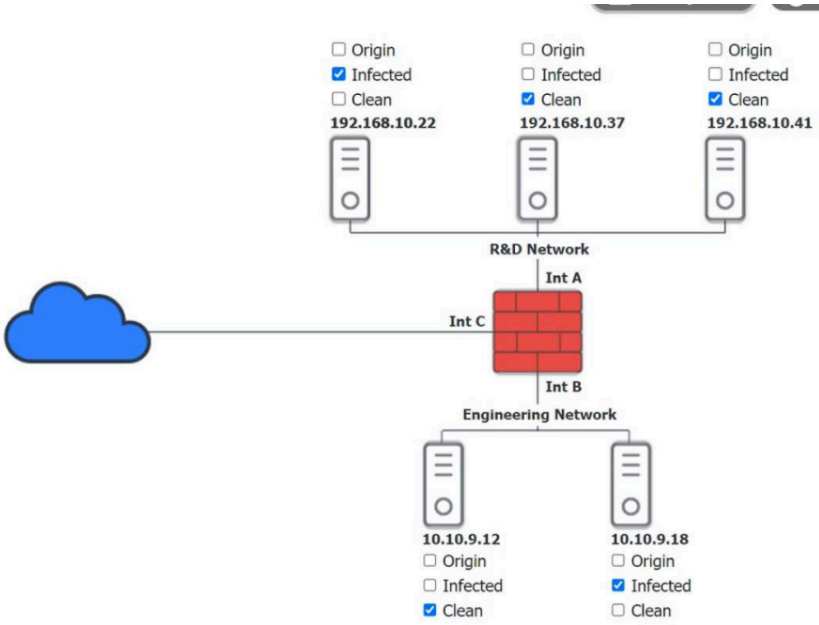
PBQ:

This is simulation



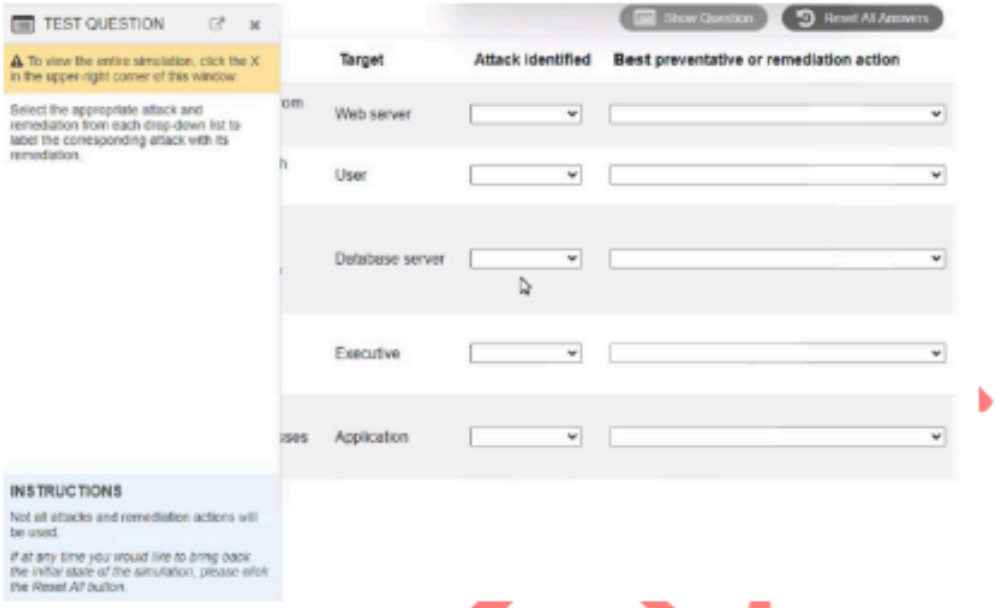
Below is solved



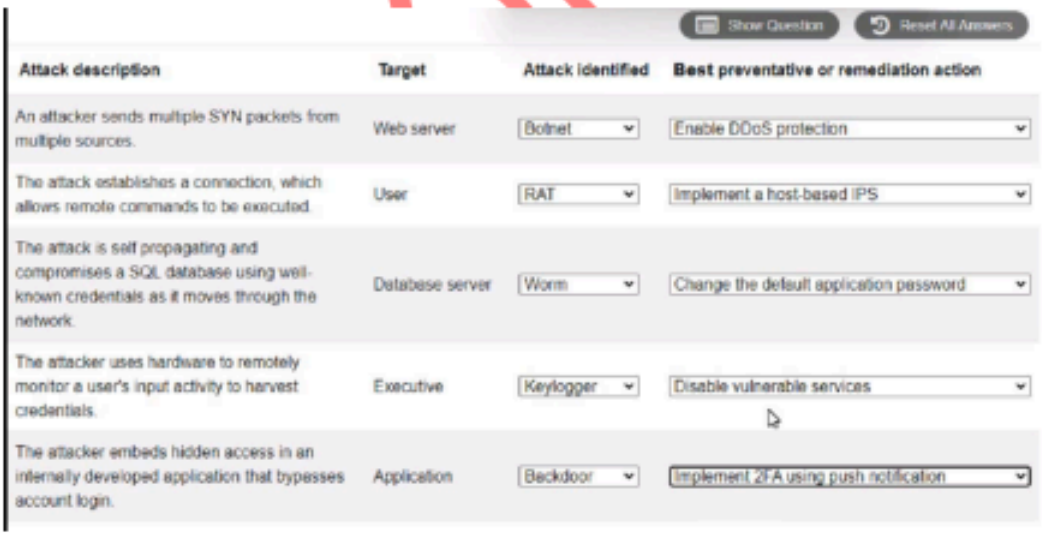

Origin
Infected
Clean
192.168.10.22
Origin
Infected
Clean
192.168.10.37
Origin
Infected
Clean
192.168.10.41
R&D Network
Int A
Int C
Int B
Engineering Network
10.10.9.12
Origin
Infected
Clean
10.10.9.18
Origin
Infected
Clean

PBQ:

This is simulation



Below is solved



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