

# A.

**Smurf Attack**

# B.

Man in the middle

# C.

Backdoor

# D.

Replay

# E.

Spear Phishing

# F.

Xmas Attack

# G.

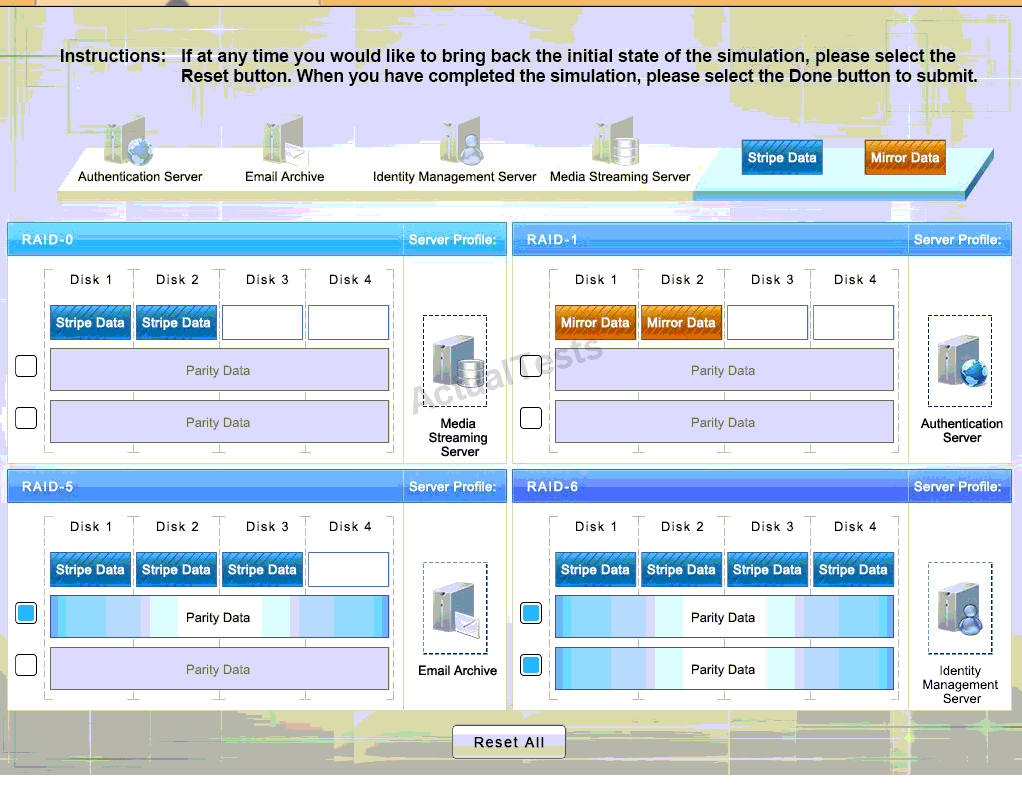
Blue Jacking

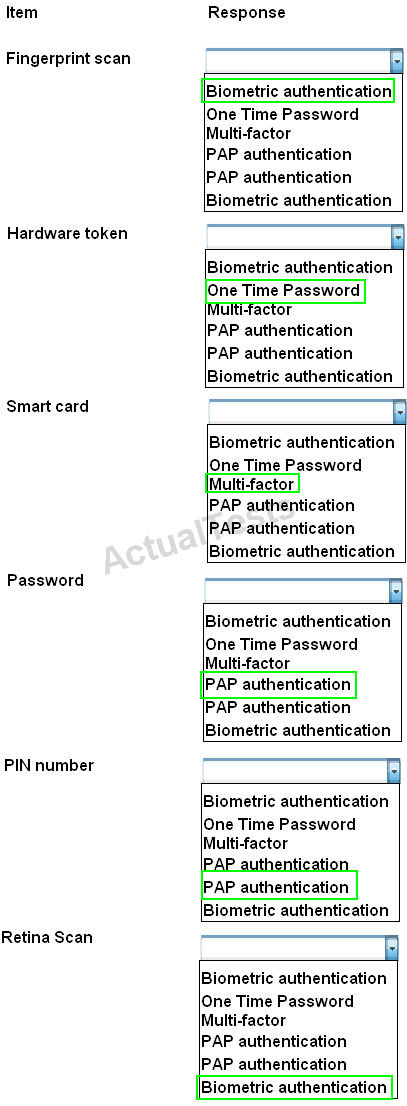
# H. Ping of Death

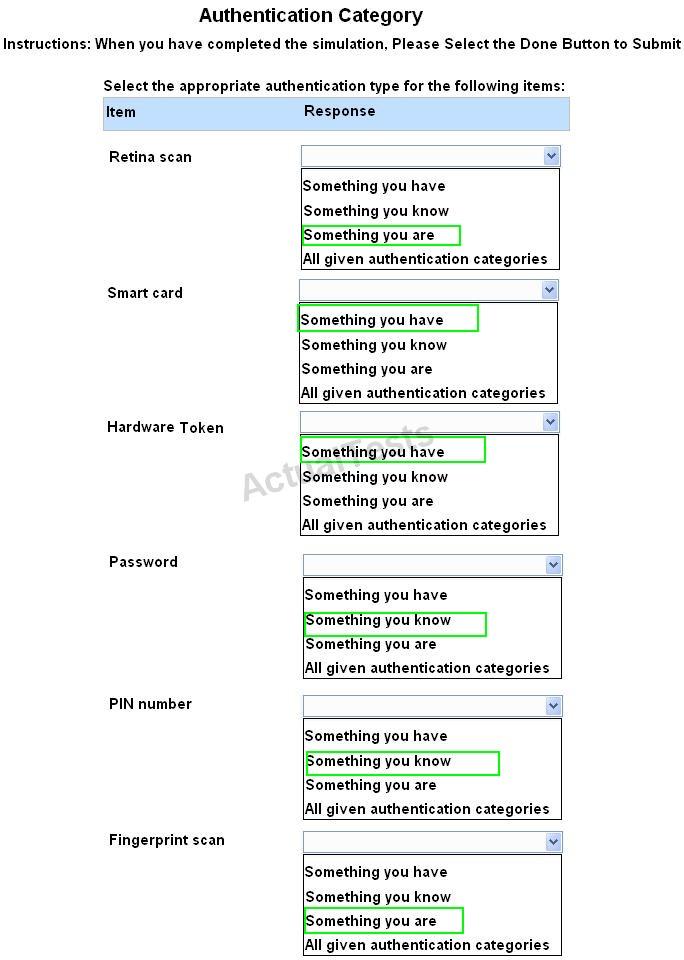
The exhibit shows that all the computers on the network are being ‘pinged’. This indicates that the ping request was sent to the network broadcast address. We can also see that all the replies were received by one (probably with a spoofed address) host on the network. This is typical of a smurf attack.

A smurf attack is a type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to its knees.

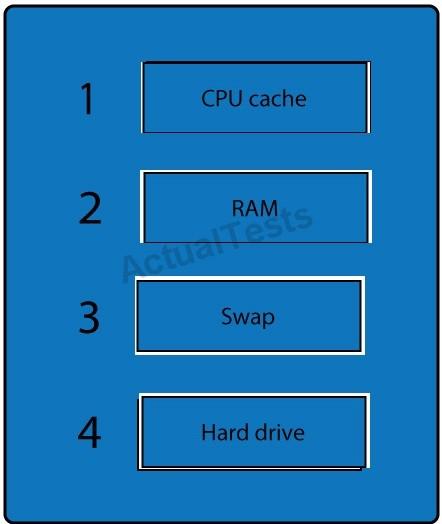
Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network.

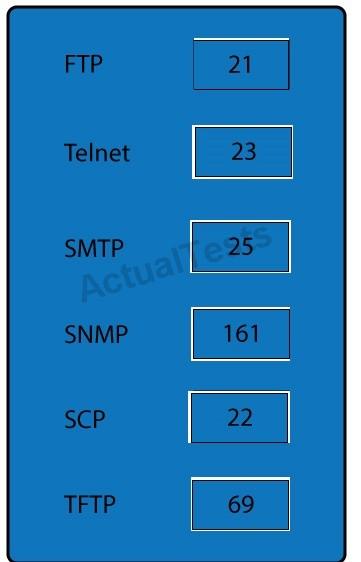


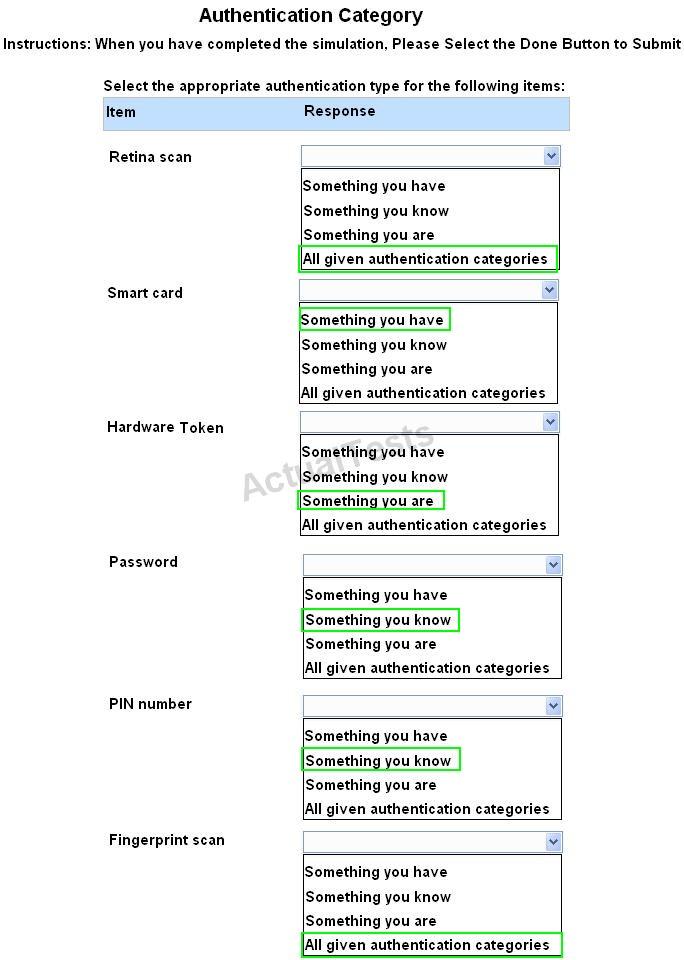


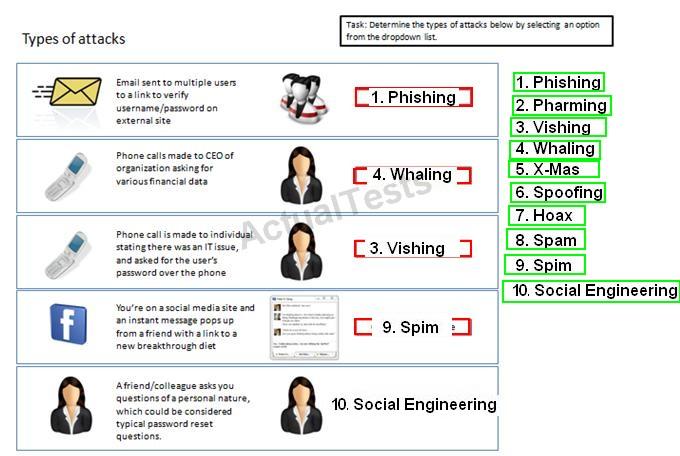


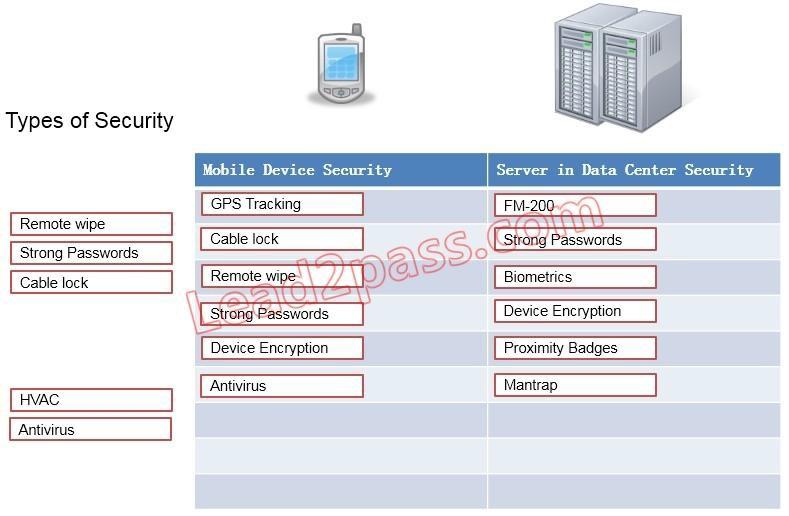


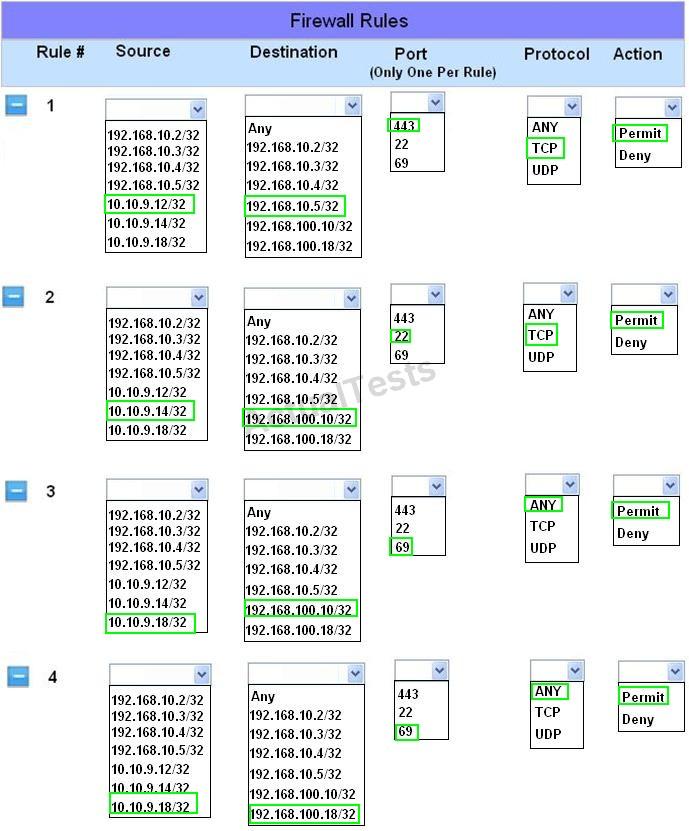


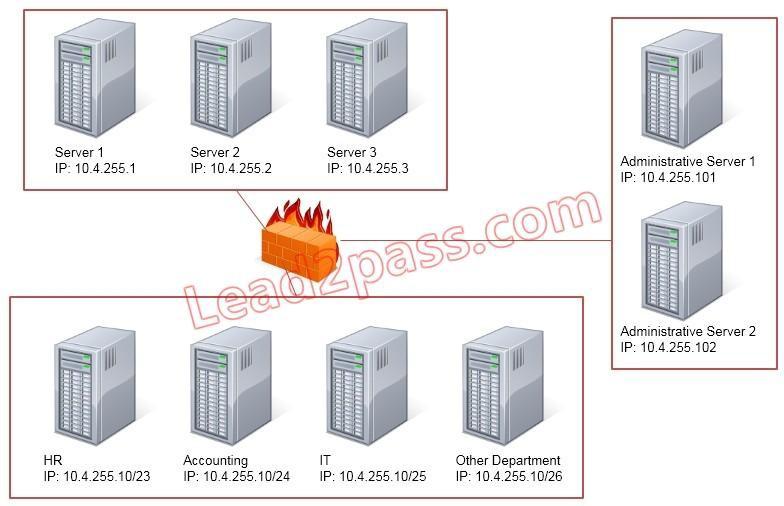


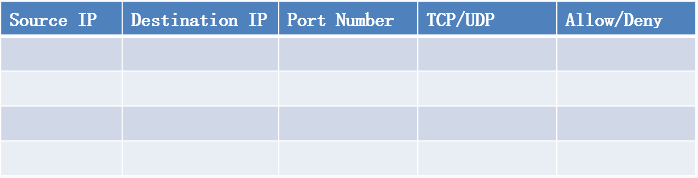






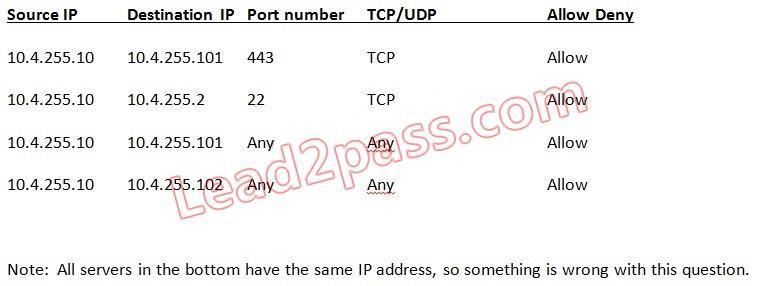


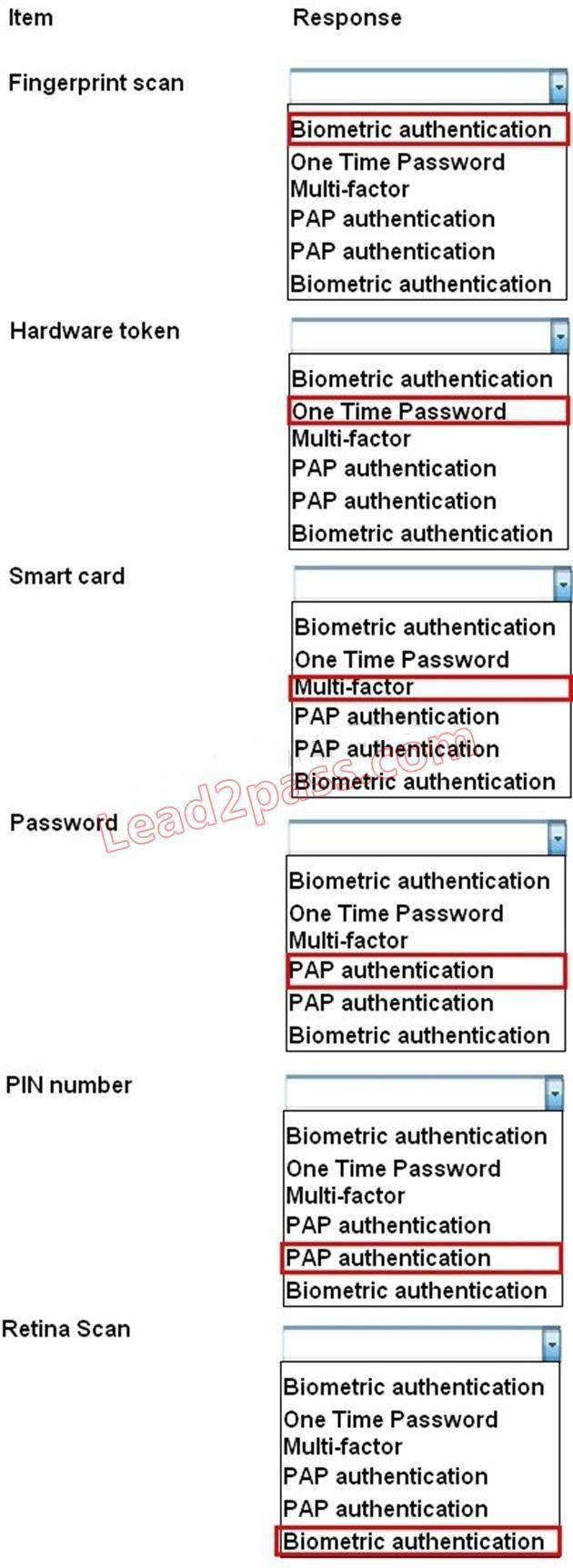




### Answer:

Use the following answer for this simulation task. Below table has all the answers required for this question.





Hotspot Question

The security administrator has installed a new firewall which implements an implicit DENY policy by default Click on the firewall and configure it to allow ONLY the following communication.

* 1. The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.
  2. The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port
  3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.

Instructions: The firewall will process the rules in a top-down manner in order as a first match The port number must be typed in and only one port number can be entered per rule Type ANY for all ports. The original firewall configuration can be reset at any time by pressing the reset button.

Once you have met the simulation requirements, click save and then Done to submit

