DoS Attacks Quiz

Directions: Chose the best answer to each question.

1. What does DoS stand for?
   1. Digital obstruction Services
   2. Denial of Service
   3. Decryption of Service
   4. Denial of Software
2. What is the difference between DDoS and DoS attacks?
   1. DoS originates from multiple sources while DDoS comes from one source
   2. DDoS targets Computers while DoS targets networks
   3. DDoS originates from multiple sources while DoS comes from one source
   4. DoS crashes networks while DDoS disrupts networks
3. What is a botnet and which attack uses them?
   1. A group of hijacked internet connected devices: DDoS
   2. A group of hijacked internet connected devices: DoS
   3. A small portable device that can attack a network nearby with the click of a button: DDoS
   4. A small portable device that can attack a network nearby with the click of a button: DoS
4. Victims of hijacked devices in a botnet normally know about their compromised system.
   1. True
   2. False
5. What is a smurf attack?
   1. When a hacker send a bunch of popups to your device with smurf images on them.
   2. Sending Messages Under Real Faculty, sending malicious emails posing as a faculty member.
   3. Attacker requests to connect to the target server but doesn’t complete the 3-way-handshake. By doing this multiple times all open ports get occupied.
   4. Sending Internet control message protocol broadcast packets to a number of hosts with spoofed IP’s of the target machine. Recipients respond, flooding the target.
6. How does a SYN flood work?
   1. Flooding the targets email with malicious emails.
   2. Attacker requests to connect to the target server but doesn’t complete the 3-way-handshake. By doing this multiple times all open ports get occupied.
   3. Sending a oversized packet to the target, “Flooding” the target machine.
   4. Sending multiple small packets to the target machine, which can’t respond to all of them efficiently, slowing the system down.
7. What’s a similarity between a ping flood and a smurf attack?
   1. Both need Botnets to work.
   2. Both leave the 3-way handshake incomplete.
   3. Neither of them are a common DDoS attack.
   4. Both overwhelm a target with ICMP packets.
8. What is the ping of death?
   1. A sent malformed oversized packet to the target machine that results in damaging behavior.
   2. Sending a ping with a fake IP address to a target machine.
   3. Hacking into the target machine breaking its ability to receive messages.
   4. Pinging a machine nonstop by using a Botnet.
9. How can you recognize a DoS attack?
   1. Unusually slow performance.
   2. Popup windows.
   3. Power outage.
   4. Laggy YouTube videos.
10. What should you do if you believe you are experiencing a DoS attack?
    1. Unplug your router.
    2. Sit and wait for it to eventually end.
    3. Contact your internet service provider to confirm its an attack and be advised for the next steps.
    4. Call 911 non-emergency number.