You are concerned that an attacker might use a null session to connect to your IPC$ share on your Windows domain controller. You know you need to leave the NetBIOS and SMB ports open on the domain controller itself to allow file sharing within the network, but have decided to block those ports at the network’s perimeter firewall to prevent anyone outside from attempting a connection. Which ports should you block?

389 and 3389

139 and 445

110 and 443

135 and 636

Answer: B

Explanation: NetBIOS requires ports 137, 138, and 139 to be left open to operate. SMB utilizes port 445 for its communications. Therefore, if we block ports 139 and 445 at the firewall, but leave them open within the network, the attackers will not be able to access the IPC$ share and create a null session over these ports from outside of the network.

Tammy is currently working as a Tier 2 service desk analyst. She has received a call from a user stating that when they attempt to go to MyBank.com, they are redirected to a website that isn’t MyBank.com. Tammy is concerned that a DNS attack may have occurred, so she checks the local DNS server’s cache, but it appears to be normal and functioning properly. What might be causing this issue for the user?

DNS poisoning

Domain name kiting

Modified hosts file

ARP poisoning

Answer: C

Explanation: If the user’s workstation has had its hosts file modified by an attacker, it would bypass the local DNS server when conducting the domain lookups and direct the user to a malicious website instead. DNS poisoning would only be occurring if the local DNS server’s cache had been modified. Domain name kiting only prevents a domain name from being purchased. ARP poisoning affects IP addresses to MAC addresses, not IP addresses to domain names.

Your company’s web server has just gone offline and rebooted itself. Once the reboot is complete, you log into the server to analyze the logs and determine why it rebooted. After some analysis of the logs, you found a log entry in the HTTP logs showing that a user had conducted a search using a very long string of random data. This was the last entry before the reboot occurred, so you suspect this caused the issue. What type of attack may have been conducted?

Denial of Service

Distributed Denial of Service

Fraggle

Smurf

Answer: A

Explanation: A denial of service occurs when a single user or system attacks a server and causes it to go offline or reboot. In the scenario provided, there was a single user entering a long random string of data, and shortly afterwards the server rebooted. This is most likely a denial of service attack. We don’t know what exactly caused this string to make the reboot occurred, but it does describe a very generic type of denial of service condition based on the scenario given.