

Real-World Scenario 7-3: Identifying Network Attacks

Scenario: You are interviewing for a job with a marketing company. The company's servers have been victims of various DoS attacks and other malicious network attacks over the past year. The company wants to employ a resourceful server technician who can quickly identify the different types of network attacks common today.

Your task is to research the four types of DoS attacks listed below and give a few examples of how they can be prevented.

- DNS amplification attack

- Smurf attack

- SYN flood

- Teardrop attack

Real-World Scenario 7-3 Solution

DoS (and DDoS) attacks can harm routers and other various hosts but are most commonly used to flood servers, causing them to send only intermittent data to clients or fail altogether.

The DNS amplification attack generates a high volume of packets ultimately intended to flood a target website. In a DNS amplification attack, the attacker initiates DNS requests with a spoofed source IP address. The attacker relies on reflection; responses are not sent back to the attacker but are instead sent "back" to the victim server. Because the DNS response is larger than the DNS request (usually), it amplifies the amount of data being passed to the victim. An attacker can use a small number of systems with little bandwidth to create a sizable attack. The primary way of preventing this attack is to block spoofed source packets. It can also be prevented by blocking specific DNS servers, blocking open recursive relay servers, rate limiting, and updating one's own DNS server(s). Finally, make use of the Domain Name System Security Extensions (DNSSEC), which are specifications that provide for origin authentication and data integrity.

The Smurf attack sends large amounts of ICMP packets to multiple targets on a network in an attempt to flood their network interfaces, and the network in general. The most obvious defense is to filter ICMP traffic at the router or firewall. However, you could also use a NIDS solution, filter for spoofed IP addresses, or utilize subnetting.

In a SYN flood, large amounts of SYN packets are sent to a server, rendering it inoperable. One way to prevent this is to implement flood control at the firewall (which can also help with Smurf and other DoS attacks). Another is to use an IDS.

The teardrop attack sends broken IP packets (fragments) in an attempt to crash the computer. To prevent this, utilize filtering and update and harden the OS.

Try to memorize the various network attacks covered in this chapter. This will undoubtedly help you on the job interview, as well as on the job itself. To help you remember them, run the following simulation.

Simulation: Complete the simulation "7-3: Identifying Network Attacks" Parts A, B, C, and D.