Overview of interception tactics

In the previous course items, you learned how packet sniffing and IP spoofing are used in network attacks. Because these attacks intercept data packets as they travel across the network, they are called interception attacks.

This reading will introduce you to some specific attacks that use packet sniffing and IP spoofing. You will learn how hackers use these tactics and how security analysts can counter the threat of interception attacks.

A closer review of packet sniffing

As you learned in a previous video, **packet sniffing** is the practice of capturing and inspecting data packets across a network. On a private network, data packets are directed to the matching destination device on the network.

The device's Network Interface Card (NIC) is a piece of hardware that connects the device to a network. The NIC reads the data transmission, and if it contains the device's MAC address, it accepts the packet and sends it to the device to process the information based on the protocol. This occurs in all standard network operations. However, a NIC can be set to promiscuous mode, which means that it accepts all traffic on the network, even the packets that aren't addressed to the NIC's device. You'll learn more about NIC's later in the program. Malicious actors might use software like Wireshark to capture the data on a private network and store it for later use. They can then use the personal information to their own advantage. Alternatively, they might use the IP and MAC addresses of authorized users of the private network to perform IP spoofing.

A closer review of IP spoofing

After a malicious actor has sniffed packets on the network, they can impersonate the IP and MAC addresses of authorized devices to perform an IP spoofing attack. Firewalls can prevent IP spoofing attacks by configuring it to refuse unauthorized IP packets and suspicious traffic. Next, you'll examine a few common IP spoofing attacks that are important to be familiar with as a security analyst.

On-path attack

An **on-path attack** happens when a hacker intercepts the communication between two devices or servers that have a trusted relationship. The transmission between these two trusted network devices could contain valuable information like usernames and passwords that the malicious actor can collect. An on-path attack is sometimes referred to as a **meddler-in-the middle attack** because the hacker is hiding in the middle of communications between two trusted parties.

Or, it could be that the intercepted transmission contains a DNS system look-up. You'll recall from an earlier video that a DNS server translates website domain names into IP addresses. If a malicious actor intercepts a transmission containing a DNS lookup, they could spoof the DNS response from the server and redirect a domain name to a different IP address, perhaps one that contains malicious code or other

threats. The most important way to protect against an on-path attack is to encrypt your data in transit, e.g. using TLS.

Smurf attack

A **smurf attack** is a network attack that is performed when an attacker sniffs an authorized user's IP address and floods it with packets. Once the spoofed packet reaches the broadcast address, it is sent to all of the devices and servers on the network.

In a smurf attack, IP spoofing is combined with another denial of service (DoS) technique to flood the network with unwanted traffic. For example, the spoofed packet could include an Internet Control Message Protocol (ICMP) ping. As you learned earlier, ICMP is used to troubleshoot a network. But if too many ICMP messages are transmitted, the ICMP echo responses overwhelm the servers on the network and they shut down. This creates a denial of service and can bring an organization's operations to a halt.

An important way to protect against a smurf attack is to use an advanced firewall that can monitor any unusual traffic on the network. Most next generation firewalls (NGFW) include features that detect network anomalies to ensure that oversized broadcasts are detected before they have a chance to bring down the network.

DoS attack

As you've learned, once the malicious actor has sniffed the network traffic, they can impersonate an authorized user. A **Denial of Service attack** is a class of attacks where the attacker prevents the compromised system from performing legitimate activity or responding to legitimate traffic. Unlike IP spoofing, however, the attacker will not receive a response from the targeted host. Everything about the data packet is authorized including the IP address in the header of the packet. In IP spoofing attacks, the malicious actor uses IP packets containing fake IP addresses. The attackers keep sending IP packets containing fake IP addresses until the network server crashes.

Pro Tip: Remember the principle of defense-in-depth. There isn't one perfect strategy for stopping each kind of attack. You can layer your defense by using multiple strategies. In this case, using industry standard encryption will strengthen your security and help you defend from DoS attacks on more than one level.

Key takeaways

This reading covered several types of common IP spoofing attacks. You learned about how packet sniffing is performed and how gathering information from intercepting data transmissions can give malicious actors opportunities for IP spoofing. Whether it is an on-path attack, IP spoofing attack, or a smurf attack, analysts need to ensure that mitigation strategies are in place to limit the threat and prevent security breaches.