Common Security Threats

by Sophia

WHAT'S COVERED

In this lesson, you will learn about attacks against network security.

Specifically, this lesson will cover the following types of attacks:

1. Attacks Against Network Security

Attackers (also known as hackers) who create threats to a network generally have one of two purposes in mind: destruction or reconnaissance. They are seeking to destroy data or deny access, and maybe even steal valuable information. In this tutorial, we will look at several common attacks that hackers use to breach the security of networks.

BIG IDEA

All attacks against networks seek to interrupt the confidentiality, integrity, or availability of networked resources.

1a. Denial of Service (DoS)

Denial of service (DoS) is an attack on availability and prevents users from accessing the network and/or its resources. A DoS attack generates a high volume of useless traffic to a target server, bogging down the system so the server's legitimate users experience delays or even outages if the attack crashes the server.

HINT

Today, DoS attacks are commonly launched against enterprise networks and especially websites. DoS attacks come in a variety of flavors as explained below.

TERM TO KNOW

Denial of Service (DoS)

An attack on the availability of network resources.

1b. Distributed DoS (DDoS)

A **distributed denial of service** (DDoS) is a DoS attack that originates from many different sources, typically on the internet. DDoS attacks are highly effective because they are amplified by bots in the attack process.

HINT

A **bot** is a piece of software designed to perform a minor but repetitive task automatically or on command.

TERMS TO KNOW

Distributed DoS (DDoS)

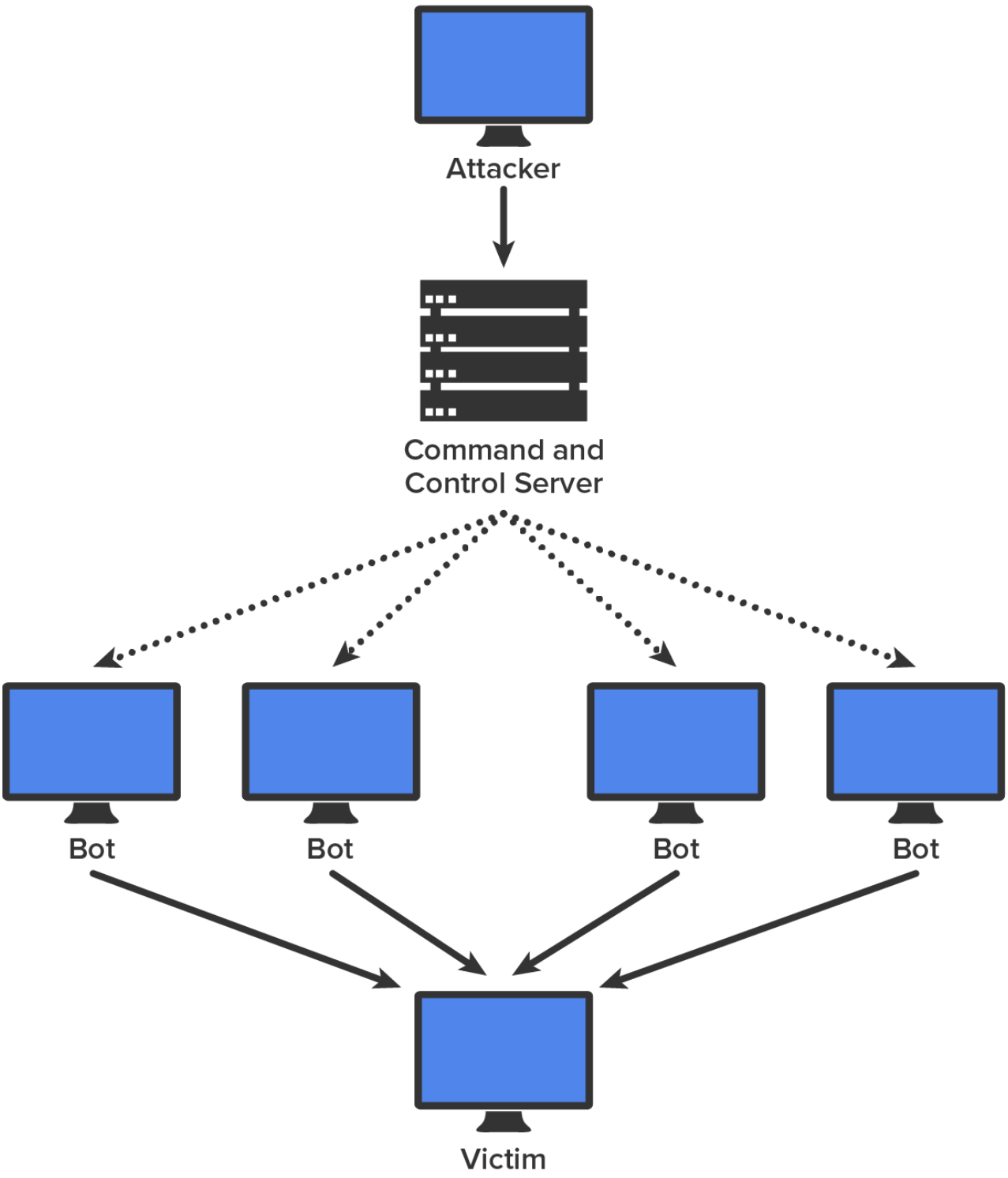
A distributed denial-of-service attack, one that originates from many different (geographically and network topographically) sources, on a network of networks such as the internet.

Bot

A piece of software designed to perform a minor but repetitive task automatically or on command, especially when operating with the appearance of a (human) user profile or account.

1c. Botnets

A **botnet** is a collection of compromised computers that is gradually built up and then unleashed as a DDoS attack, usually from the internet. Some botnets are legal, such as those created to maintain control of internet relay chat (IRC) channels, while others are illegally created to launch a DDoS attack. An attacker can recruit and build a botnet to help amplify a DoS attack, as illustrated in the diagram below.



STEP BY STEP

The steps in the process of building a botnet are as follows:

1. A botnet operator sends out viruses or worms whose payloads are malicious applications, the bots, infecting ordinary users' computers.
2. The bots on the infected PCs log into a server called a command-and-control (C&C) server under the control of the attacker.

3. At the appropriate time, the attacker, through the C&C server, sends a command to all bots to attack the victim at the same time, thereby significantly amplifying the effect of the attack.

One of the hallmarks of a DDoS attack is a major spike in traffic in the network as bots that have been recruited mount the attack. For this reason, any major spike in traffic should be regarded with suspicion. A network intrusion detection system (IDS) can recognize these traffic spikes and may be able to prevent them from growing larger or, in some cases, prevent the traffic in the first place.

Another unmistakable feature of a DDoS attack is the presence of a coordinated attack. To properly amplify the attack, the bots must attack the victim at the same time. The coordination of the bots is orchestrated by the C&C server depicted in the previous diagram. If all the bots can be instructed to attack at precisely the same second, the attack becomes much more dangerous to the victim.

TERM TO KNOW

Botnet

A collection of compromised computers that is gradually built up and then unleashed as a DDoS attack or used to send very large quantities of spam.

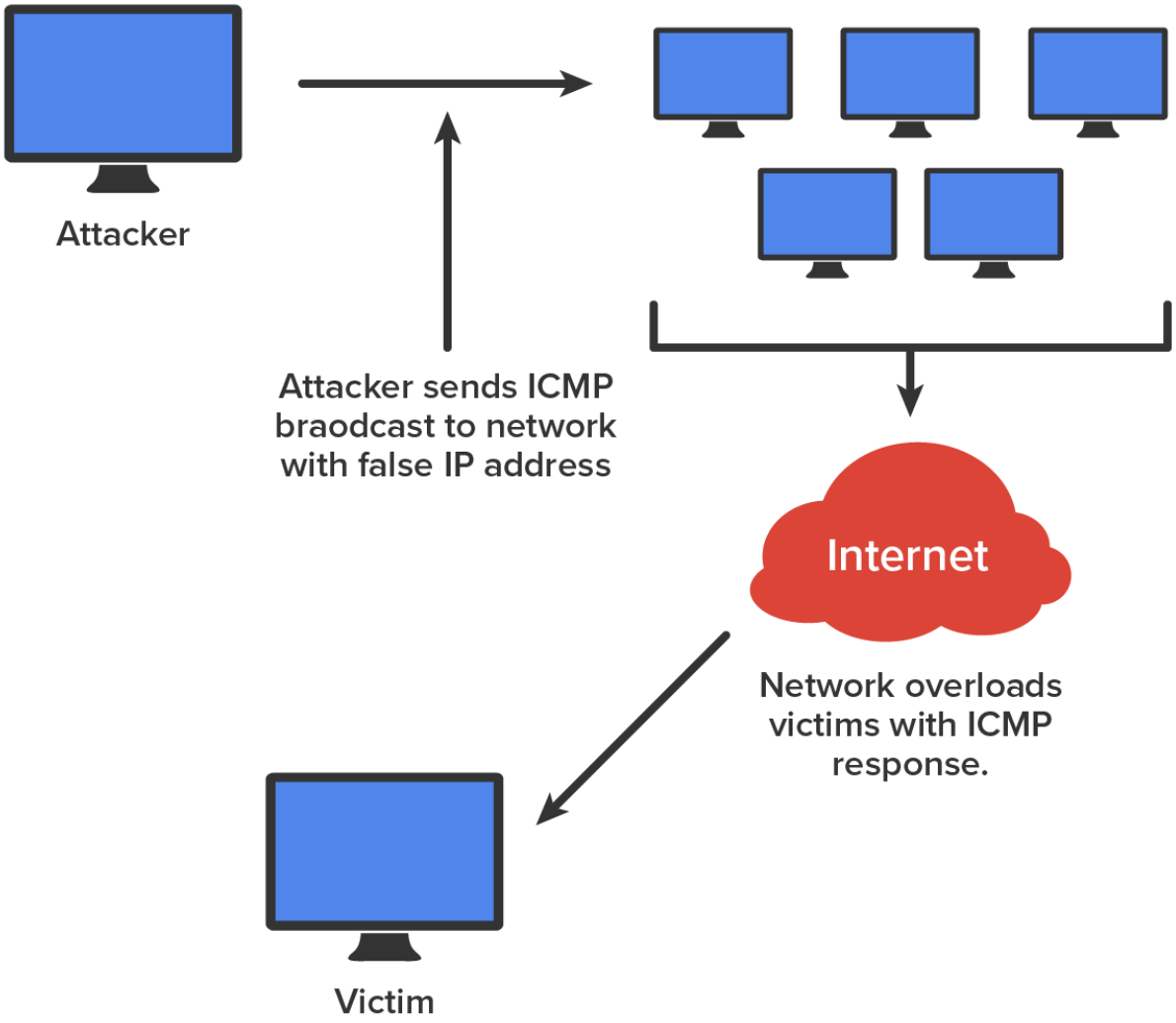
1d. Smurf Attack

A **Smurf attack** is a version of a DoS attack that floods its victim with spoofed broadcast ping messages. Here is how it works: the attacker spoofs the intended victim's IP address and then sends a large number of pings (IP echo requests) to IP broadcast addresses. The receiving router responds by delivering the broadcast to all hosts in the subnet, and all the hosts respond with an IP echo reply at the same time.

KEY CONCEPT

On a network with hundreds of hosts, this results in major network gridlock because all the machines are kept busy responding to each echo request. The situation is even worse if the routers have not been configured to keep these types of broadcasts confined to the local subnet.

EXAMPLE The diagram below shows a Smurf attack in progress.



Smurf attacks are not very common anymore because most routers are configured in a way that prevents them from forwarding broadcast packets to other networks.

TERM TO KNOW

Smurf Attack

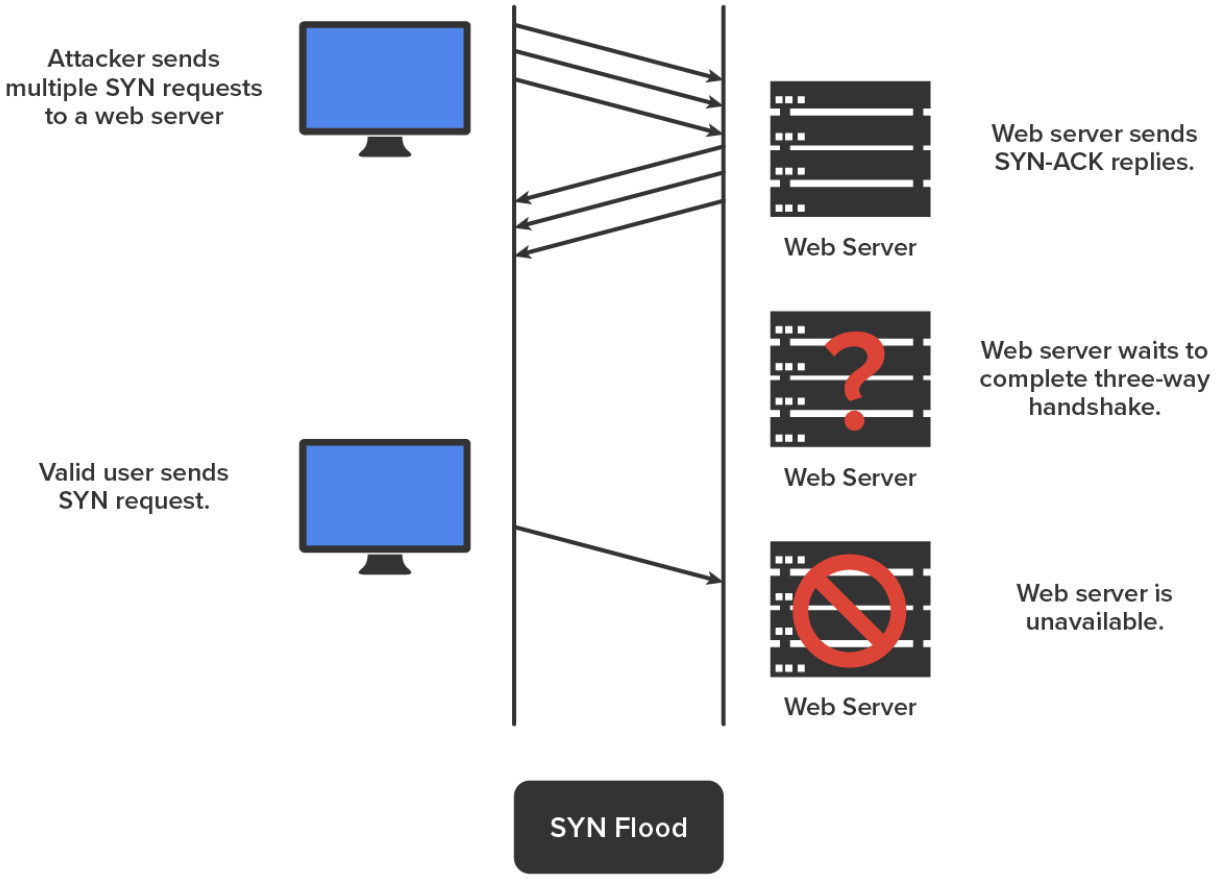
A form of denial-of-service attack involving broadcasting ICMP packets with the intended victim's IP address to a large computer network, causing the victim's computer to be overwhelmed by the response packets from the network.

1e. SYN Flood Attack

A **SYN flood** is also a DoS attack that inundates the receiving machine with lots of packets that cause the victim to waste resources by holding connections open. In normal communications, a workstation that wants to open a Transmission Control Protocol/Internet Protocol (TCP/IP) communication with a server sends a TCP/IP packet with the SYN flag set to 1. The server automatically responds to the request, indicating that it is ready to start communicating with a SYN-ACK. In the SYN flood, the attacker sends a SYN, the victim sends back a SYN-ACK,

and the attacker leaves the victim waiting for the final ACK. While the server is waiting for the response, a small part of memory is reserved for it. As the SYNs continue to arrive, memory is gradually consumed.

EXAMPLE The diagram shows a simple DoS/SYN flood attack:



TERM TO KNOW

SYN Flood Attack

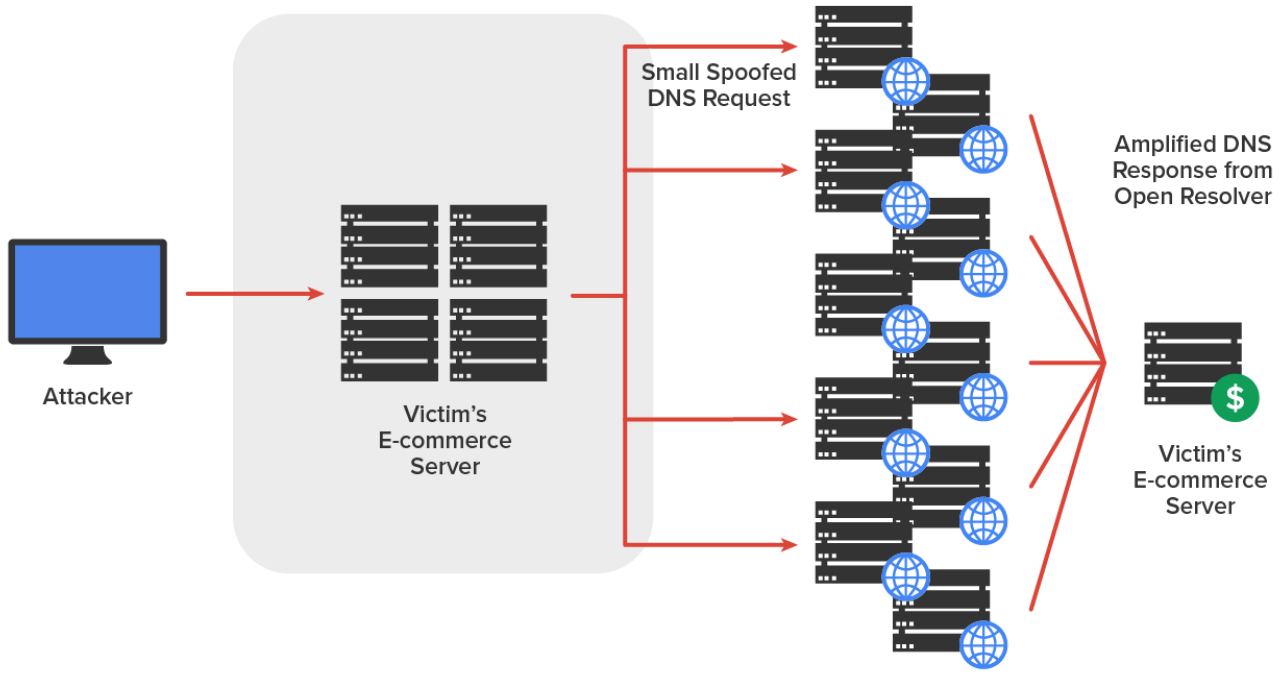
A denial-of-service attack in which the attacker sends a succession of SYN (synchronization) requests to the target system in an attempt to consume its resources and make the system unresponsive to legitimate traffic.

1f. DNS Amplification Attack

A **DNS amplification attack** is an attack on availability that delivers traffic to the victim by reflecting it off a third-party network. Reflection conceals the source of the attack. It relies on the exploitation of publicly accessible open DNS servers to deluge victims with DNS response traffic.

EXAMPLE The attacker sends a small DNS message using the victim's IP address as the source to an open resolver. The type of request used returns all known information about the DNS zone, which allows for the maximum level of response amplification directed to the victim's server. The attack is magnified by recruiting a botnet to send the small messages to a large list of open resolvers (DNS servers).

The response from the DNS server overwhelms the victim, as shown in the diagram below:



TERM TO KNOW

DNS Amplification Attack

An attack that delivers traffic to the victim by reflecting it off a third-party network.

1g. DNS Cache Poisoning Attack

DNS clients send requests for name-to-IP address resolution (called queries) to a DNS server. The search for the IP address that goes with a computer or domain name usually starts with a local DNS server that is not authoritative for the DNS domain in which the requested computer or website resides. When this occurs, the local DNS server makes a request to the DNS server that does hold the record in question. After the local DNS server receives the answer, it returns it to the local DNS client. After this, the local DNS server maintains that record in its DNS cache for a period called the time to live (TTL), which is usually an hour.

A **DNS cache poisoning attack** is an attack on data confidentiality in which the attacker attempts to refresh or update that record when it expires with a different address than the correct address. If the attacker can convince the DNS server to accept this refresh, the local DNS server will then be responding to client requests for that computer with the address inserted by the attacker. Typically, the address they now receive is for a fake website that appears to look in every way like the site the client is requesting. The hacker can then harvest all the name and password combinations entered on their fake site.

HINT

To prevent this type of attack, the DNS servers should be limited in the updates they accept. In most DNS software, you can restrict the DNS servers from which a server will accept updates. This can help prevent the server from accepting these false updates.

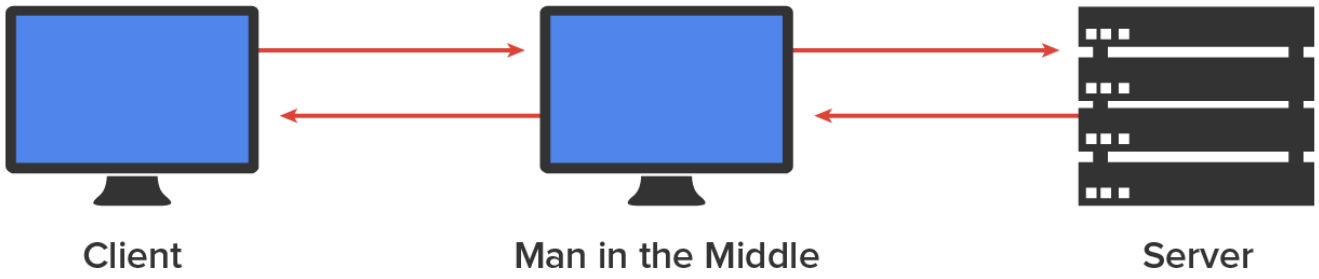
TERM TO KNOW

DNS Poisoning Attack

A form of computer security hacking in which corrupt Domain Name System (DNS) data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g., an IP address.

1h. On-Path Attacks

An **on-path attack (OPA)** happens when someone intercepts packets intended for one computer and reads the data. A common guilty party could be someone working for your very own ISP using a packet sniffer and augmenting it with routing and transport protocols. Rogue ATM machines and even credit-card swipers are tools that are increasingly used for this type of attack. OPA is an attack on data confidentiality. The diagram below shows a man-in-the-middle attack.



TERM TO KNOW

On-Path Attack

Computer network crime where the criminal passes on messages between two communicating parties without them knowing it.

1i. ARP Poisoning Attack

ARP cache poisoning is a type of man-in-the-middle attack and is an attack on data confidentiality. The ARP cache contains mappings from IP address to MAC address that a device has learned through the ARP process. One of the ways this cache can be poisoned is by pinging a device with a spoofed IP address. In this way, an attacker can force the victim to insert an incorrect mapping from IP address to MAC address into its ARP cache. If the attacker can accomplish this with two computers having a conversation, they can effectively be placed in the middle of the transmission. After the ARP cache is poisoned on both machines, they will be sending data packets to the attacker, all the while thinking they are sending them to the other member of the conversation.

TERM TO KNOW

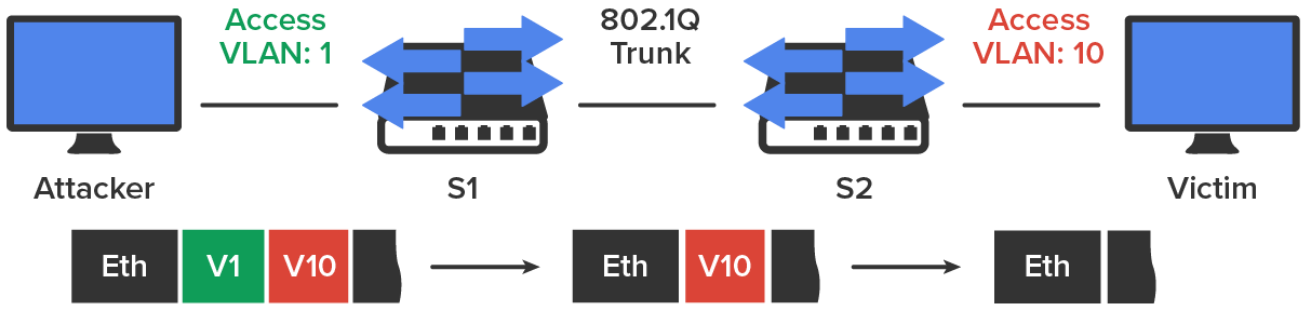
ARP Poisoning Attack

An attack by a hacker that sends spoofed Address Resolution Protocol (ARP) messages onto a local area network to redirect traffic to the attacker.

1j. VLAN Hopping Attack

VLANs, or virtual LANs, are Layer 2 subdivisions of the ports in a single switch. A **VLAN hopping attack** results in traffic from one VLAN being sent to the wrong VLAN. Normally, this is prevented by the trunking protocol placing a VLAN tag in the packet to identify the VLAN to which the traffic belongs. The attacker can circumvent

this through a process called double tagging, which is placing a fake VLAN tag into the packet along with the real tag. When the frame goes through multiple switches, the real tag is taken off by the first switch, leaving the fake tag. When the frame reaches the second switch, the fake tag is read, and the frame is sent to the VLAN to which the hacker intended the frame to go. VLAN hopping is an attack on network integrity. This process is shown in the diagram below.



TERM TO KNOW

VLAN Hopping Attack

A computer security exploit, a method of attacking networked resources on a virtual LAN (VLAN).

1k. Physical Attack

Physical attacks are those that cause hardware damage to, or the theft of, a network device. These attacks can be mitigated, but not eliminated, by preventing physical access to the device. Routers, switches, firewalls, servers, and other infrastructure devices should be locked away and protected by strong physical access controls. Physical intrusions can result in loss of data confidentiality, data integrity, and data availability.

BIG IDEA

If an attacker can touch your hardware, then they can “own” your hardware. They can do this either by stealing the actual device or configuring administrative access to it.

TERM TO KNOW

Physical Attack

A physical intrusion to gain unauthorized access to network hardware.

SUMMARY

In this lesson, you learned about **attacks against the network**, including the confidentiality, integrity, and availability of networked resources. We introduced different type of attacks against network security, including denial of service, distributed denial of service, botnets, Smurf attack, SYN flood attack, DNS amplification attack, DNS cache poisoning attack, man-in-the-middle attack, ARP poisoning attack, VLAN hopping attack, and physical attack.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

ARP Poisoning Attack
An attack by a hacker that sends spoofed Address Resolution Protocol (ARP) messages onto a local area network to redirect traffic to the attacker.

Bot
A piece of software designed to perform a minor but repetitive task automatically or on command, especially when operating with the appearance of a (human) user profile or account.

Botnet
A collection of compromised computers that is gradually built up and then unleashed as a DDoS attack or used to send very large quantities of spam.

DNS Amplification Attack
An attack that delivers traffic to the victim by reflecting it off a third-party network.

DNS Poisoning Attack
A form of computer security hacking in which corrupt Domain Name System (DNS) data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g., an IP address.

Denial of Service (DoS)
An attack on the availability of network resources.

Distributed DoS (DDoS)
A distributed denial-of-service attack, one that originates from many different (geographically and network topographically) sources, on a network of networks such as the internet.

On-Path Attack
Computer network crime where the criminal passes on messages between two communicating parties without them knowing it.

Physical Attack
A physical intrusion to gain unauthorized access to network hardware.

SYN Flood Attack
A denial-of-service attack in which the attacker sends a succession of SYN (synchronization) requests to the target system in an attempt to consume its resources and make the system unresponsive to legitimate traffic.

Smurf Attack
A form of denial-of-service attack involving broadcasting ICMP packets with the intended victim's IP address to a large computer network, causing the victim's computer to be overwhelmed by the response packets from the network.

VLAN Hopping Attack

A computer security exploit, a method of attacking networked resources on a virtual LAN (VLAN).