11.6.2 Analyzing Network Attacks Facts

For a network security operations team to effectively defend its network, it should understand common attacks and how those attacks work.

This lesson covers the following topics:

- Man-in-the-middle (MTM) attacks
- Layer 2 attacks
- DNS attacks
- Distributed denial of service (DDoS) attacks

Man-in-the-Middle Attacks

A very common attack is the man-in-the-middle attack. In this attack, the attacker is positioned between two devices and intercepts a transmission between them. For example, if a device sends its login information to a website, the hacker intercepts the transmission and steals the credentials. There are a variety of methods that can be used to perform a man-in-the-middle attack. The follow table describes some of them.

MTM Attack	Description
IP address spoofing	The hacker modifies an IP address in a communication. The recipient intends to send information to the originally specified IP address, but the packets go to the hacker instead.
DNS spoofing	The hacker modifies a website's address in the DNS server. The user attempts to go to that website, but instead is redirected to the hacker's malicious site.
HTTPS spoofing	The hacker uses a website name that looks similar to a real site. For example, www.testout.com could be replaced with www.test0ut.com.
SSL hijacking	The hacker passes forged authentication keys to both the user and application/server. The user and application/server are talking directly to each other, but all communication is going through the hacker.
Email hijacking	The hacker compromises the target's email account and is able to monitor and gather information.
Wi-Fi eavesdropping	This is also known as a evil-twin attack. The hacker tricks users into connecting to a malicious wireless network in order to monitor and manipulate the data packets flowing across the wireless network.
Browser cookie theft	This is also known as session hijacking. When a user logs into a website, a session cookie is generated. The hacker intercepts the session cookie and can access the user's website account.

A variation on the man-in-the-middle attack is the man-in-the-browser attack. This attack works on the application layer and inserts a Trojan horse on the victim’s computer. The Trojan horse exploits the browser to manipulate the data and send it to the attacker.

Layer 2 Attacks

When an attacker gains access to the network, attacks can be levied against layer 2 devices and protocols. The following table describes some of these attacks:

Layer 2 Attack	Description
The Address Resolution Protocol (ARP) poisoning	ARP is used to translate IP addresses into MAC addresses. ARP was designed for speed, not security. It can be exploited by an attacker using ARP poisoning, also referred to as an ARP spoofing attack. To perform an ARP poisoning attack, the attacker does the following: 1. Scans the network to get a list of all connected devices. 2. Selects two devices to intercept communication between. This is usually a computer and the router. 3. Sends a malicious ARP request to both devices to update their ARP caches, remapping the IP address of each to the attacker's MAC address. The devices then send all communication between the two to the attacker's computer. A successful ARP poisoning attack will allow the hacker to: ▪ Perform packet sniffing ▪ Carry out session hijacking attacks ▪ Alter the communications between the two devices ▪ Perform a distributed denial of service attack To protect against ARP poisoning attacks, use HTTPS whenever possible. Because HTTPS is encrypted, the attacker is unable to read or modify the data. This makes the ARP poisoning attack worthless for the hacker.
MAC spoofing	A MAC spoofing attack starts with the attacker scanning the network for valid MAC addresses. The attacker spoofs the MAC address to match the gateway's and overwrites the switch's CAM table with this new mapping. All data that would normally go to the gateway is sent to the attacker's computer.
MAC flooding	MAC flooding is an attack against the network switch. Network switches maintain a MAC table. The MAC table is a list of the MAC addresses for each connected device and the port each device is connected to. The MAC table allows the switch to send data packets to only the intended recipient. In a MAC flooding attack, the attacker sends a large number of Ethernet frames with different MAC addresses. The switch begins adding these new MAC addresses to the MAC table. Eventually, the MAC table gets overloaded causing the switch to dump the MAC table. During this time, the switch begins sending packets to all ports, just like a hub. An attacker can use a MAC Flooding attack to: ▪ Carry out a DDoS attack ▪ Intercept and analyze packets ▪ Perform advanced attacks such as ARP poisoning while the switch is down

Domain Name System (DNS) Attacks

DNS is the system that translates IP addresses into names, such as a website's URL. Attackers can use DNS to steal data or perform other attacks. The following table explains some common DNS attacks:

DNS Attack	Description
DNS hijacking	To carry out a DNS hijacking attack, the attacker needs to gain access to the DNS records of a website. A variety of techniques can be used to gain access. These include: ▪ Using phishing attacks ▪ Using social engineering ▪ Exploiting a vulnerability in the domain name registrar With access to the DNS records, the attacker can change the record to redirect the URL. This means that when attempting to go the legitimate site, the user is redirected to the attacker's malicious site. The attacker can also transfer the DNS or perform other malicious activities.
DNS poisoning	DNS poisoning is a man-in-the-middle type of attack. The attacker intercepts DNS requests from a browser and sends back a malicious response. The response usually redirects the user to the attacker's malicious site. The DNS response also gets stored in the browser's DNS cache. This means that every time the user enters the website URL, the browser's cache redirects to the malicious site.
URL redirection attack	A URL redirection attack is very similar to the DNS poisoning attack in that the attacker's goal is to get the user to go to a different site than the user intends to. In this attack, the attacker uses social engineering and phishing emails to get the victim to click what looks like a legitimate link, but the link sends the victim to the attacker's malicious site. The goal is usually to get the victim to input login credentials into the fake site allowing the attacker to steal them. >
Domain/IP reputation attack	Security firms keep track of a domain's activities to determine if it is being used for malicious activity. The activity would include sending spam emails or if the domain is being used as part of a zombie network to perform denial of service (DOS) attacks. Either activity would result in the domain's reputation being degraded. A negative domain reputation can cause the domain to be put on a list that many security programs use to identify sites to block and prohibit users from visiting. Domain reputation attacks can be extremely devastating to an organization.

Distributed Denial of Service

A distributed denial of service attack is designed to bombard the target with more data than it can handle causing it to shut down. A DDoS attack will usually target a network; specific applications or services; and even the systems used to monitor and control industrial operations (Operational Technology).

There are many different methods to pull off a DDoS attack. The following table explains the three main methods.

DDoS Attack Method	Description

Application layer DDoS	An application layer attack's goal is to exhaust the target's resources by overloading a specific program or service. For example, an attacker sends a large number of HTTP requests to a web server causing it to repeatedly load a web page. This method takes little effort by the attacker, but will quickly overwhelm the web server as it repeatedly loads the media files including images, audio, and video.
Protocol DDoS	The attacker can also target different protocols such as TCP flags to overload network devices such as a firewall. A SYN flood attack is a common example of this method: ▪ The attacker sends a large number of SYN packets with a spoofed IP address. ▪ The victim responds with the SYN-ACK packet, but it goes to the wrong IP address. The victim never receives a response. ▪ The victim leaves the connection open waiting for a response to complete the 3-way handshake. ▪ Eventually the victim gets overwhelmed waiting for the response packets to come back.
Amplification DDoS	An amplification attack consumes the bandwidth between the victim and the internet, effectively cutting the victim off. DNS amplification attacks are a common example of this. ▪ The attacker sends a large number of DNS queries to multiple open DNS servers with the victim's IP address spoofed as the sender. ▪ The DNS servers send the DNS responses back to the victim. ▪ The victim quickly get overloaded with the amount of data and is unable to function.