CS436 HW 1

Network Attacks

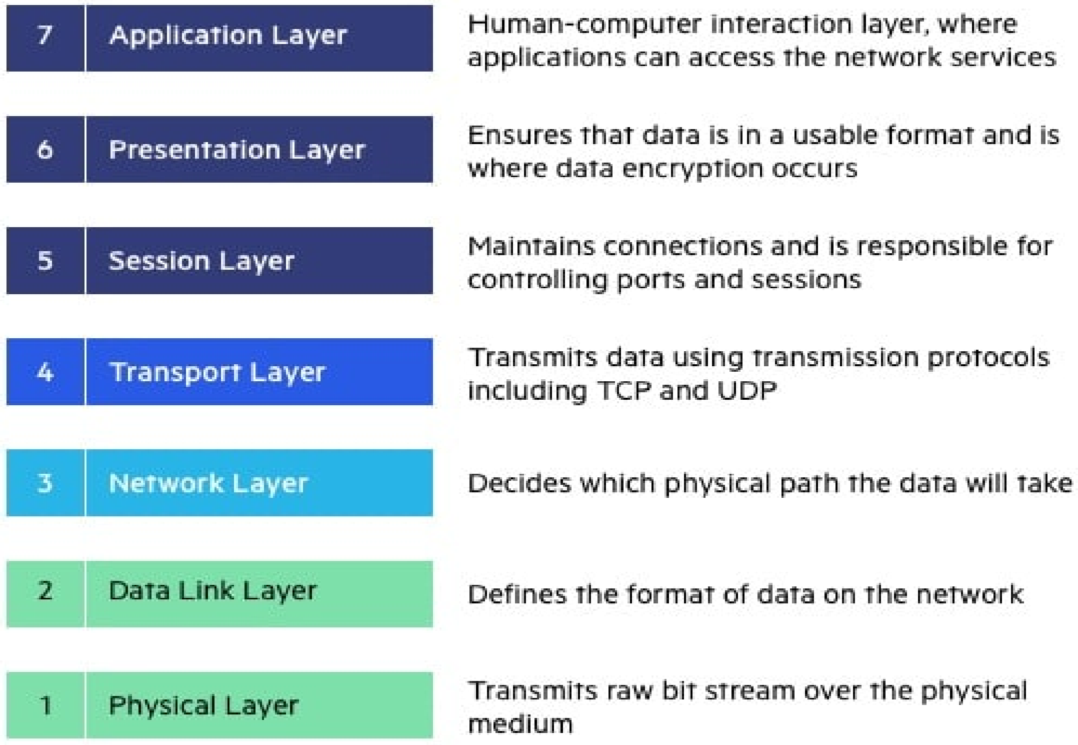
Simon Hausmaninger

There are a significant number of ways to attack a network. Some of these attacks have been figured out and exploited, while others are still yet to be found. Networks can be large and have a number of connected endpoints, which provides numerous ways for the security of the network to be compromised. If your network security is compromised, this can leave you exposed to data breaches.

There are two general types of attacks on networks. They are passive attacks and active attacks. A passive attack takes place when the attacker seeks to gain access to information, without altering any of the data. An active attack happens when an attacker not only gains access but also modifies data. The three most popular network attacks are distributed denial of service (DDoS) attacks, man in the middle attacks, and cross-site scripting attacks.

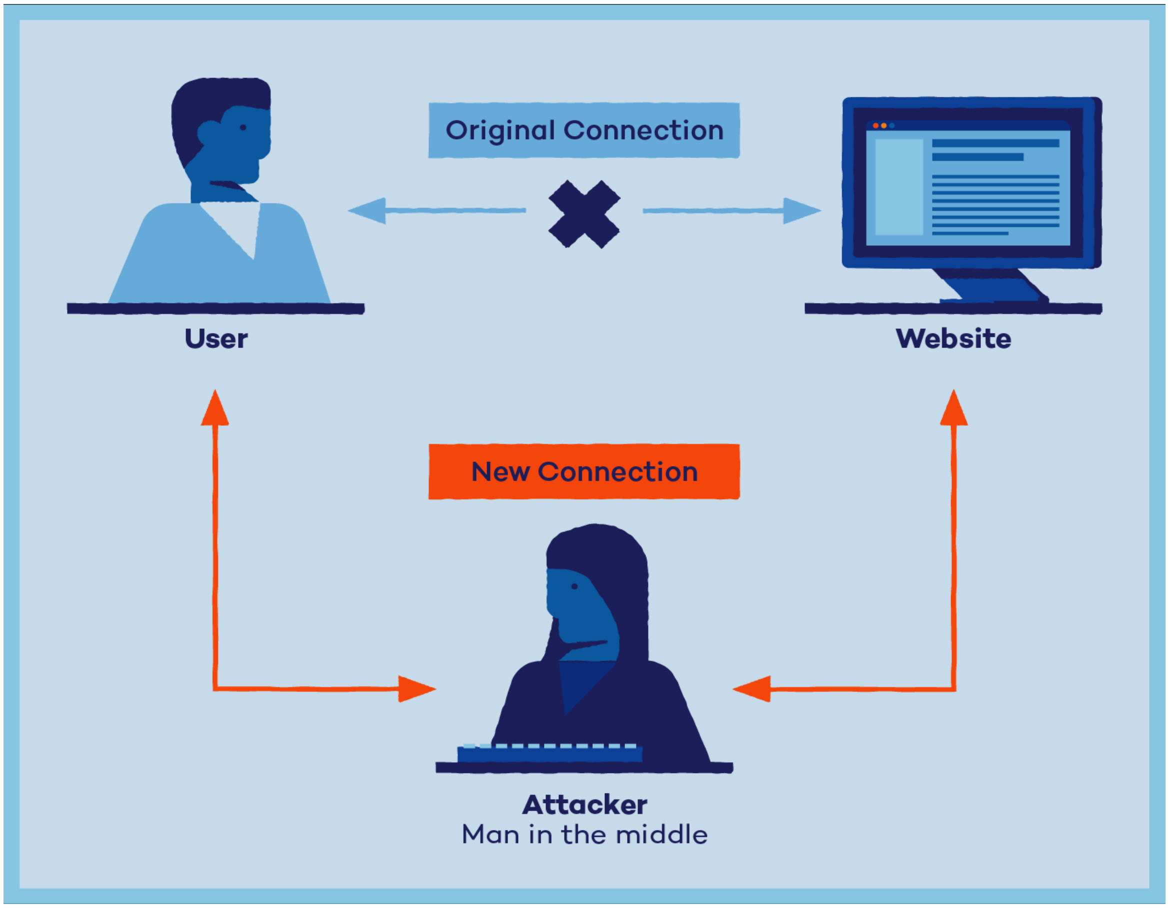
A distributed denial of service attack is probably the one that you have heard most about if you are fluent in networking. A DDoS attack is an example of an active attack. This happens when an attacker makes an attempt to alter the flow of traffic of a server, service, or network by overflowing the normal flow of network traffic, which can result in a denial of service for other users operating under the server.

The three most common types of DDoS attacks are application layer attacks (commonly referred to as layer 7 attacks), protocol attacks, and volumetric attacks. During an application layer attack, an attacker overwhelms the server with requests like HTTP GET or HTTP POST [3]. This is a popular attack due to not only the server resources it requests, but also the network resources. Unlike application layer attacks and volumetric attacks, protocol attacks exploit weakness in internet connection protocols. An example of this would be a SYN flood attack. Basically, when you connect to something on the internet, you and the computer you are connecting to must initiate a TCP handshake. This is a connection between the two computers. The first step of a TCP handshake is usually a SYN packet. The attack works by sending a flux of SYN packets to the target, resulting in the target receiving new requests before it can finish the final step of the TCP handshake [2]. The last kind of DDoS attack, and usually what most people visualize when they hear DDoS is a volumetric attack. A volumetric attack is when the attacker tries to overwhelm the server by utilizing all of the bandwidth the server has to offer.



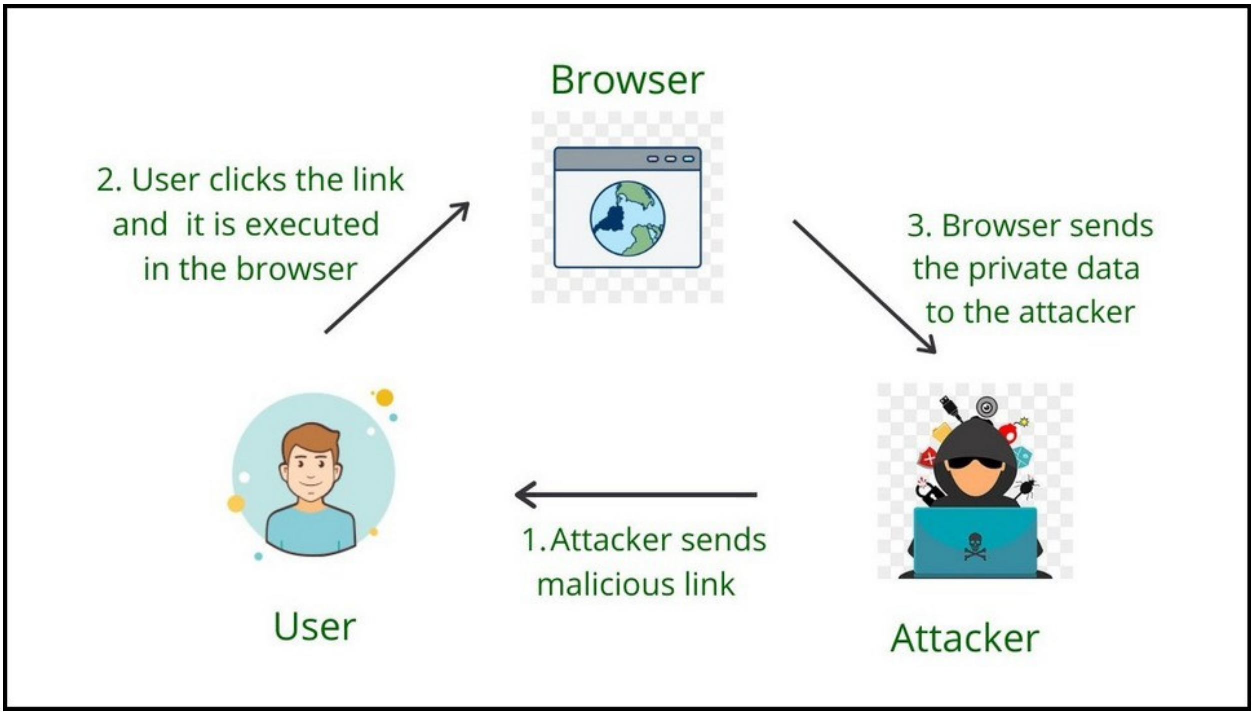
7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

A man-in-the-middle attack is a form of eavesdropping where the attacker will seek to gain access to the data between two parties who are communicating directly with one another. According to Kinza Yasar, a Technical Writer for techtarget.com, these attacks happen through a two-step process called data interception and decryption. Data interception happens when the attacker fools the user and server into believing they are connected to each other, when they are really connected to the attacker who is acting as a proxy between them [4]. They are then able to read and insert false information between the two. There is a three step process that is commonly involved in the data interception technique. The first step is installing a packet sniffer to test network traffic that could not be secure, such as an HTTP website. Once a user is logged in to an unsecured website, the attacker is able to get the user's information and redirect them into a fake website. The website appears legitimate and the user enters real data into a fake website which the attacker then saves.



There are a few concepts that one should keep in mind while surfing the web to ensure that they are not vulnerable to man-in-the-middle attacks. The first, is making sure that the URL of the website that you are on begins with ‘HTTPS’ instead of ‘HTTP’. The difference is that a URL that begins with HTTPS will use the SSL/TLS protocol to encrypt data making it invulnerable to attackers. Another way to stay safe online is to avoid phishing emails. Phishing is the idea of tricking someone into giving up their sensitive data by usually acting as if you were a large company. These attacks can take place not only on personal emails, but corporate emails as well. You can also utilize a Virtual Private Network (VPN) in order to encrypt your end-to-end data so that if compromised, you have an additional layer of protection.

A cross-site scripting attack is an attack where scripts are run on websites that are commonly visited. XSS attacks happen when the attacker uses a website to send malware to users. They trick the user's computer into thinking the script that they are sending is coming from a secure website. While the possibilities for these kinds of attacks are virtually endless, there are a few common forms that one should look out for. One is a stored XSS Attack. Stored attacks happen when the attacker’s inserted script is saved on the target servers [1]. After this happens, it is sent to the user’s machine when accessing the targeted website. Another form of stored XSS attacks is called Blind Cross-site Scripting. This can happen when you submit some sort of data into a website loaded with script. Upon opening, the attacker's script will execute. The last common type of XSS attack is called a reflected attack. This is the type of script that is reflected off of a web server in some form of response from the website. When the target is tricked into clicking the malicious link, their browser begins being used.


Browser
2. User clicks the link and it is executed in the browser
3. Browser sends the private data to the attacker
User
1.Attacker sends malicious link
Attacker

For example, in the photo above, the attacker sends a malicious link. The user then clicks and the browser is initiated. The browser then sends the private data back to the attacker.

In order for the average person to stay safe while browsing the world wide web, they don’t need to use more than a little bit of critical thinking and common sense. But to be secure and to have a foot forward, it helps to know what kind of attacks one can be vulnerable to. Distributed denial of service (DDoS) attacks, man in the middle attacks, and cross-site scripting attacks are all things you should at least be aware of if you want to be extra secure. Knowing that DDoS attacks work by flooding requests to a server, knowing you can be vulnerable to man-in-the-middle attacks on public unprotected networks, and knowing how to identify and protect yourself from phishing and cross site scripting which can happen any time.

References

[1] “Cross Site Scripting (XSS).” *Cross Site Scripting (XSS) | OWASP Foundation*, https://owasp.org/www-community/attacks/xss/.

[2] “What Is a DDOS Attack: Types, Prevention & Remediation.” *OneLogin*, https://www.onelogin.com/learn/ddos-attack.

[3] What Is a Distributed Denial-of-Service (Ddos) Attack? - Cloudflare. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

[4] Yasar, Kinza, and Michael Cobb. “What Is a Man-in-the-Middle Attack (MITM)? - Definition from Iotagenda.” *IoT Agenda*, TechTarget, 28 Apr. 2022, https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM.