Co-op work term report

Denial of Service and Man in the Middle Attack

Vaibhav Sharma 200365101
Co op Coordinator : Robert Hilderman
Due: Aug 21th 2019

Table of Contents

Denial of Service

Once we discover an attack, it's usually repaired, prevented or mitigated very quickly but that is an exception for Denial of service attack. A denial of Service attack is designed to do one thing and that is to Deny Service. Imagine we have a server, it can be web, email, DNS or anything other type of server. The whole idea behind Denial of service attack is that there are so many people coming in to talk to that server that it cannot take care of anybody else. In a typical Denial of service attack, the focus is to create any sort of congestion on the server so that it cannot invoke any services/tasks it's supposed to do.

Types of Denial of Service:

There are lots of different types of denial of service attack but in this paper we will categorize them in three major types that are volumetric, protocol and application attack.

Volumetric Attack :

In volumetric attack, attacker is not doing anything evil in terms of how they are talking to the server but instead they are just doing a lot of talking so the server cannot help anybody else.

Example of Volumetric attack would be ping flood. In ping flood attack, the client sends a huge number of ping requests and never wait for the response from the server. This leads server to be always busy by replying to the ping request and not being able to do anything else.

Another example could be UDP flood. In UDP flood, the client send huged number of UDP request to all the ports in the server which keep the server and the ports busy for anyone else to connect. The attacking machine overwhelms the server by keeping an active session on all the ports available on the server.

Majority of the Volumetric attacks are easily negated today. The routers and servers these days are built to counter these types of attacks. However, later we will discuss Distributed

denial of service attack which is still very powerful these days and a major issue for big companies to battle.

Protocol Attack :

The protocol attack does something with the underlying protocol. It can be web, Http, DNS or any other protocol. It does something that is not normally accepted by the protocol which leads to server getting busy and not responding on time.

A protocol attack take advantage of the protocol to create confusion, an example would be syn-flood or syn attack. In syn flood attack, a client will send a syn in a particular tcp/ip conversation and the server will send a syn-ack back which initiates the conversation between tcp/ip. Attacker use the tcp/ip conversation architecture to its benefit and keep sending syn to the server and disregard all the syn-ack back. Everytime attacker sends a syn, it leads to a new connection between client and server which keeps the server busy from replying to genuine clients. This clogs the system and server denies service.

The protocol attack is still a huge problem to combat these days as most of the networks still use the well published protocols and networks and attackers exploit the vulnerabilities in these protocols.

Application Attack:

An Application attack works within the application conversation itself which exploit the application services to keep the application running and stopping the server from responding in a timely fashion.

An example of Application attack will be slow loris attack. To explain slow loris attack, we will assume we are working with apache web server so we can take advantage of something within the application and exploit it. The slow loris attack is named because loris is a slow animal and it just does things really slow. To perform a slow loris on apache web server, attacker will initiate a conversation with the Apache web server and it'll get the conversation going. Once the attacker establish a conversation between client and server then it will just stop talking or communicating which will leave apache

web server waiting for the client to get back but client will never get back. The client keeps track of the active session and initiates a new session as soon as the last one ends. In the meantime, the attacker is sending out more conversations and just not talking back And as a result of that the poor Apache server simply gets overwhelmed. Now this is fairly easy to fix and later versions of Apache simply lowered their timeout value. Slow loris is not nearly as big of a problem as it used to be.

Application attacks are still possible these days but they are easily negated by better design and development practices of routers, servers and applications.

Amplification(Smurf) Attack :

Apart from the big three types of denial of service attacks, Amplification attack is very powerful as well. To show an example of Amplification attack, we will look at Smurf attack.

To explain smurf attack, we will again take the example of apache web server and this time we will send in an ICMP packet into the network. Once the ICMP packet is in the network, attacker spoofs the Web site's IP address, so it sends out a broadcast into the network and then everybody in the network starts replying/responding back except they are responding back to the target. Smurf attack is very powerful because only one packet sent into the network can produce so many more packets that it can lead to denial of service inside the network.

Distributed Denial of Service

Among all the examples of denial of service attack so far, we are looking at one attacking client on one target server. Now, if we add multiple attackers to synchronize and attack one server together then it takes the shape of Distributed Denial of Service attack and it's one of the biggest challenges for companies today.

How DDos works?

To explain distributed Denial of server, we will again take the example of apache web server but this time instead of one machine attacking the server, the attacker will use multiple machines. We can approach attacking from multiple computers in two major ways. Either we can form a team which will attack a given server at the same time or the attacker can create a form of malware on it's system known as botnet.

Using botnet, Attacker can control multiple machines. The parent computer is referred as botnet and the child computer which are being controlled are referred as zombies. Architecture where attackers use a single computer to use multiple computers to attack is called botnet.

Distributed Denial of service attacks are nightmares of security companies all around the globe. To show an example of how bad these attacks are, security companies use live forecasting and maps to represent live DDOS attacks where user can see who is being attacked, kind of attack and who is attacking. Distributed denial of service attack is the biggest challenge today when it comes to denial of service.

Man in the Middle Attack

On the internet, on any tcp/ip connection, we have some sort of communication going on between two clients. It could be a web browser accessing a web page or a computer access a shared folder on a network or any other time of connection, we always have session going on between two computers in almost every situation. A man in the middle attack is simply a third party that is sneaking between this active session and getting in the middle of two machines talking to each other.

How to approach Man in the Middle ?

When approaching man in the middle attack, there are two big parts to it:

- Attacker have to get in the middle of the conversation
- Once the attacker is in the middle of the stream then what are we going to do with it ?

The first job as an attacker is to figure out how to get in the middle, somehow attackers have to get in the middle of the active stream. Getting in the middle of the conversation always depends on the type of connection. There are basically two ways to connection, It's either wireless or wired.

Wireless :

Wireless is a fantastic way to get in the middle of the stream. if the conversation is unencrypted then the attacker can just plug in 801.11 wireless network card and start sniffing all the packets from everywhere. Wireless connection is further split into many forms but we will discuss the major three :

Wireless 802.11:

Wireless 802.11 is wifi technology which allows clients to connect with routers and modems over wifi. 802.11 wireless have some protections. For example WPA/WPA2. If a user is using

WPA2 end-to-end encryption then it makes it very difficult for the attacker to get in the middle but the encryption type WEP is not secure and attacker can get in the middle and sniff the packets as it's unencrypted. WPA/WPA2 use isolation technology which makes it difficult for one endpoint to see any other end point.

Bluetooth and NFC

Bluetooth and NFC are also susceptible to man in the middle attack. Bluetooth have encryption built into it but bluetooth counts on short distances and short session duration to make it very difficult for attacker to get in the middle. NFC communication include device to very extremely close to the other end point and it communicates using a chip built into the device. The attackers use hardware spoofing where they install their own equipment over the nfc reader which can look like the original equipment and can go unnoticeable by a non-technical person. Once attacker equipment read input from the device i.e NFC card then it takes the input and pass it to the reader. This way, the reader gets the correct input and user never finds out and the attacker gets all the data.

Wired :

If a user is on wireless network, it's very easy for the attacker to use 802.11 to get in the middle but things change drastically when user is connected on a wired connection. In a wired network, the packets are sent between different systems based on mac addresses, IP addresses,etc. To perform a man in the middle attack on a wired connection, the attacker takes advantage of Spoofing.

In spoofing on wired connection, the attacker makes their address look like the victims address which includes spoofing ip address, mac address, dhcp spoofing etc.

There are many ways to approach spoofing. One of them is using penetration tools like ettercap, wireshark, arpSpoofing etc. There are a lot of tools available in the market for attackers to use when spoofing but in this report we will discuss ettercap.

Ettercap is one of the best tools when it comes to wired man in the middle attack. Ettercap is old program and it's free. It allows attacker to not just apply different type of network poisoning but also gathered important information within the packets.

Mac Spoofing :

In a given network, router is passing data traffic according to the mac address. Attacker can use mac spoofing to make his mac address look like the victim's mac address and show the router that attacking machine is in the middle of the router and the victim's machine. This way router starts sending all the data to attackers machine.

Next thing is to figure out what to do with the traffic received from the router. One of the functions of man in the middle attack is garner data/ data scraping. One of the things we can use is arp gathering tools. Arp Gathering tools collect packets from the stream but create a lot of unnecessary noise which is easily detectable by the routers these days. Attacker can however use ettercap. Ettercap also have the capability to search the data and grab the important information for us/

Ip Spoofing :

When it comes to IP spoofing, the attacker doesnt lie to switch as it does in mac spoofing. Ip spoofing is also known as ARP posing in which attacker lies to the other systems so all the other systems will think a particular Ip address have a specific mac address which will route all the traffic to the attackers machine .

Ettercap helps when performing IP spoofing as well because every system on the network have an arp cache which maintains the record of ip address to mac address. Ettercap helps attacker to choose the targets and it changes their ip address to mac address cache to send all the traffic to attackers machine. If a user tries to log into any website during arp poisoning, ettercap will automatically grab the username and password for attacker.

Arp poisoning creates a lot of noise as it sends out packets to different targets and lie to them about their arp cache. A Lot of noise within a network can be easily detected by the routers these days.

DHCP Spoofing :

In DHCP spoofing, the attacker does not touch the machines connected or the router but instead it changes the dns information. After DNS spoofing, all the devices on the network which are using DHCP will start reaching the new fake DNS server without changing their subnet mask, default gateway or mac address. Once attacker set up a fake dns server then it can route all the traffic in the network to the ip address of it's choice.

Effectiveness :

Man in the middle attack is very powerful if attacker can get in the stream undetected. Network and security companies use different types of detection mechanism to stop and eliminate these types of attacks but man in the middle attack is still very damaging in small networks.

Planning a breach/ Exploiting vulnerabilities :

When planning an attack, attackers need to identify the Objective, purpose and Action. In objective, attacker focus on what is the outcome/expectations from this attack. It looks into what are we trying to steal/break. In purpose, Attacker looks at why are they attacking. It can pen testing, team testing. There are no boundaries/rules to follow for attacker. so the security teams have to be ready for every possible way an attacker can attack. In action, attacker figures out how they are going to attack. It can include exploiting a vulnerability or getting in their network. Attacker further have a choice if he wants to silently steal information or bring the system down.

One example of planned attack will be attacker getting in victim's network and performing a distributed denial of service attack. In this scenario, the security will be busy attending the volume of packets form denial of service and the noise created inside the network by the attacker will be ignored. Attackers can use multiple attacks at the same time as there is no limit to what attackers can for a successful breach.

Reference

- Bishop,M., Sullivan, E, & Ruppel, M (2019). Computer security: Art and science.Boston Addison-Wesley.
- Conklin, W. A., White, G. B., Cothren, C., Davis, R., & Williams, D. (2018). *Principles of computer security: CompTIA security and beyond, (exam SY0-501)*. New York: McGraw-Hill Education.
- *NIST*. (1990). Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology.
- Bravo, S., & Mauricio, D. (2018). DDoS attack detection mechanism in the application layer using user features. *2018 International Conference on Information and Computer Technologies (ICICT)*. doi:10.1109/infoct.2018.8356848
- Alomari, E., Manickam, S., Gupta, B. B., Karuppayah, S., & Alfaris, R. (2012). Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art. *International Journal of Computer Applications, 49*(7), 24-32. doi:10.5120/7640-0724
- Rahim, R. (2017). Man-In-The-Middle-Attack Prevention Using Interlock Protocol Method. doi:10.31227/osf.io/8txn7
- Guha, R. K., Furqan, Z., & Muhammad, S. (2007). Discovering Man-in-the-Middle Attacks in Authentication Protocols. *MILCOM 2007 - IEEE Military Communications Conference*. doi:10.1109/milcom.2007.4455039