Denial of Service and Man in the Middle Attack

Vaibhav Sharma sharma3v@uregina.ca
200365101

1. 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.

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.

1.1 Volumetric Attack

In a volumetric attack, the 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 a ping flood. In a ping flood attack, the client sends a huge number of ping requests and never waits for the response from the server. This leads the server to be always busy by replying to the ping request and not being able to do anything else. Another example could be the UDP flood. In UDP flood, the client send huged number of UDP requests 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 attacks which are still very powerful these days and a major issue for big companies to battle.

1.2 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 the server getting busy and not responding on time. A protocol attack takes 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. Attackers 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 the 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.

1.3 Application Attack

An Application attack works within the application conversation itself which exploits 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 the slow loris attack, we will assume we are working with an 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, the attacker will initiate a conversation with the Apache web server and it'll get the conversation going. Once the attacker establishes a conversation between client and server then it will just stop talking or communicating which will leave the 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.

1.4 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 the 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, the 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.

1.5 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.

1.5.1 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 a botnet, Attacker can control multiple machines. The parent computer is referred to as a botnet and the child computer which is being controlled are referred to 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 users 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.

2. 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 accessing a shared folder on a network or any other time of connection, we always have sessions 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.

2.1 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 connect, It's either wireless or wired.

2.2 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 :

2.2.1 Wireless 802.11

Wireless 802.11 is wifi technology which allows clients to connect with routers and modems over wifi. 802.11 wireless has 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 the 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.

2.2.2 Bluetooth and NFC

Bluetooth and NFC are also susceptible to man in the middle attack. Bluetooth has encryption built into it but bluetooth counts on short distances and short session duration to make it very difficult for attackers to get in the middle. NFC communication includes devices 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 reads input from the device i.e NFC card then it takes the input and passes it to the reader. This way, the reader gets the correct input and the user never finds out and the attacker gets all the data.

2.3 Wired

If a user is on a wireless network, it's very easy for the attacker to use 802.11 to get in the middle but things change drastically when the 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 victim's 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 an old program and it's free. It allows attackers to not just apply different types of network poisoning but also gather important information within the packets.

2.3.1 Mac Spoofing

In a given network, the 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 the attacking machine is in the middle of the router and the victim's machine. This way the router starts sending all the data to the attacker's 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. Attackers can however use ettercap. Ettercap also have the capability to search the data and grab the important information for us

2.3.2 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 the attacker lies to the other systems so

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

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

2.3.3 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 an attacker sets up a fake dns server then it can route all the traffic in the network to the ip address of it's choice.

2.4 Effectiveness

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

3. Planning a breach/ Exploiting vulnerabilities

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

References

Esraa Alomari, Selvakumar Manickam, BB Gupta, Shankar Karuppayah, and Rafeef Alfaris. Botnet-based distributed denial of service (ddos) attacks on web servers: classification and art. *arXiv preprint arXiv:1208.0403*, 2012.

Matthew A Bishop. The art and science of computer security. 2002.

Silvia Bravo and David Mauricio. Ddos attack detection mechanism in the application layer using user features. In *2018 International Conference on Information and Computer Technologies (ICICT)*, pages 97–100. IEEE, 2018.

WM Arthur Conklin. Principles of computer security: Comptia security+ and beyond. *Netw Secur*, 3:18, 2009.

Ratan K Guha, Zeeshan Furqan, and Shahabuddin Muhammad. Discovering man-in-the-middle attacks in authentication protocols. In *MILCOM 2007-IEEE Military Communications Conference*, pages 1–7. Ieee, 2007.

Barbara Guttman and Edward A Roback. *An introduction to computer security: the NIST handbook*. Diane Publishing, 1995.

Robbi Rahim. Man-in-the-middle-attack prevention using interlock protocol method. *ARPN J. Eng. Appl. Sci*, 12(22):6483–6487, 2017.