International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.102.24

A Prototype For Generating Man In The Middle Attack

Shashank Malik[1], Yojna Arora[2]
[1,2] *Department of Computer Science & Engineering, Amity University Haryana, India*

Abstract- MITM has been defined as a type of attack where a user gets between the sender and receiver of information and sniffs any information being sent. Another author has defined MITM as attacks in which the attacker infiltrates unnoticed the communication channel between two partners and is thereby able to spy on or even modify their data exchanges. Man-in-the-Middle attack is the type of attack where attackers intrude into an existing connection to intercept the exchanged data and inject false information. It involves eavesdropping on a connection, intruding into a connection, intercepting messages, and selectively modifying data. MITM attacks are often referred to as "session hijacking attacks", suggesting that the intruder aims to gain access to a legitimate user's session to tamper it. The attacker usually starts with sniffing and eavesdropping on a network stream, and ends with trying to alter, forge or reroute the intercepted data. One of the objectives for MITM attacks is to gain access to the client's messages and modify them before finally transmitting them to the server end. Other objectives of MITM can be to mislead the communicators at the client or server end, to intercept pertinent information (e.g., identity, address, password, or any other confidential information for malicious purposes) and also, at times, manipulate transactions

I. INTRODUCTION

Man-in-the-middle attack (often abbreviated as MITM), is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker. A man-in-
the-middle attack can only be successful when the attacker can impersonate each endpoint to the satisfaction of the other. MITM is also known a s:

- Bucket-brigade attack
- Fire brigade attack
- Monkey-in-the-middle attack
- Session hijacking
- TCP hijacking

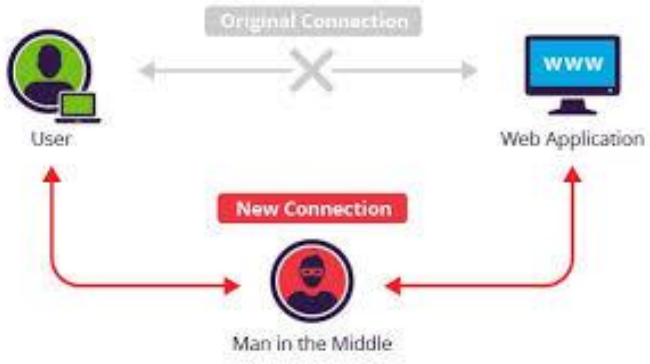


Fig 1 MITM Attack

In the real world game of keep-away, two people toss a ball back and forth while a third person –the man in the middle – tries to intercept the ball while it is enroute. In the cyber world, the game of keep-away gets a new twist; the two players have no idea the man in the middle (MITM) exists. It works like this:

- Computer A initiates conversation with computer B
- Computer C intercepts the attempt and then relays the request to computer B
- Computer B responds, computer C intercepts it, and returns that response to computer A.

While computer C has the intercepted communication, it can modify the communication or even redirect it to an entirely new destination (i.e. Computer D). Meanwhile, computer A continues to believe that it is communicating only with computer B. Computer C has been able to interject itself between A and B. DNS poisoning is another form of MITM attack. The DNS, or Domain Name System, resolves IP addresses to domain names. Vulnerabilities on the DNS server can allow attackers to insert malicious DNS information, for example directing all attempts to access a particular banking site to a lookalike site under the attacker's control. Hosts file manipulation is another method used to redirect traffic. Every Windows-based computer has a local Hosts file which, like DNS, resolves IP address to domain names. However, entries in the local Hosts file typically override DNS and the Hosts file is generally more accessible to attackers – thus malicious Hosts file manipulation is common.

1.1 The Hacker

The term hacker is somewhat fluid: it is often used by the press to refer to someone who seeks to penetrate a computer system to steal or corrupt data, whereas people who call themselves hackers would reject that definition and use the term to describe someone who is enthusiastic and knowledgeable about computer systems .To avoid this confusion we use the term 'white hat' and 'black hat' (from the days of black and white cowboy films). Thus a 'white hat' hacker might be employed to test a system for flaws, whilst a 'black hat' hacker is synonymous with a cracker. A script kiddie is someone who uses already established and part of automated techniques in attacking a system. Their expertise is less than a hacker, but still considerably more than a normal computer use. A hacker is a person who is able to access other people's computers and modify programs or information. Hacking wireless networks has provided a wider spectrum of victims throughout modern cities.

1.2 The Victim

The victims are the sessions that get hijacked. For TCP and UDP, the sessions are the periods of time where the clients are connected and actively passing information to the server. At the beginning of the session, the user/client is authenticated and then it is assumed that as long as the ACK numbers on the packets are correct, the server is talking to the same user. For HTTP, the sessions are the periods of time where the user is accessing a web application, from user logon to user logoff. The HTTP sessions are related to and distinguished from TCP sessions in that "requests" from a single user can come over different TCP/IP streams, directly or through proxies, or even from different IP address. The sessions are all the interaction the user has with the application, regardless of the TCP/IP streams its data travels on. HTTP is a stateless protocol. The result is that web application sessions have to be kept track of separately from the protocol. How this is implemented is dependent on the web application. In general, "when a user logs into an application, a session is created on the server to maintain the state for other requests originating from the same user." The sessions store all necessary parameters and identity information for the particular user it's associated with. It is kept in memory and cached until the user logs out of the application of the application or is inactive for a predefined period of time.

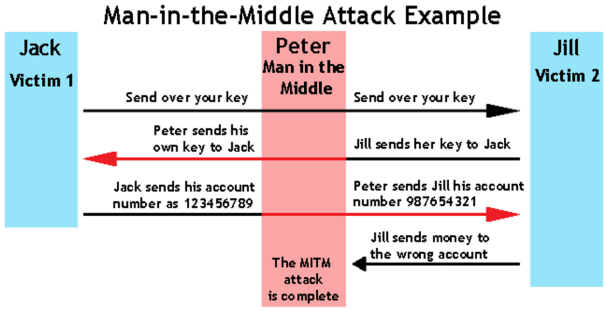


Fig 1. Example of MITM Attack

II. METHODOLOGY

The main objective of the research is to design an application for MITM attack in wireless networks. This has been done by studying and understanding the state of the art of executing MITM attack in order to come out with an effective protocol.

The application contains various tools:

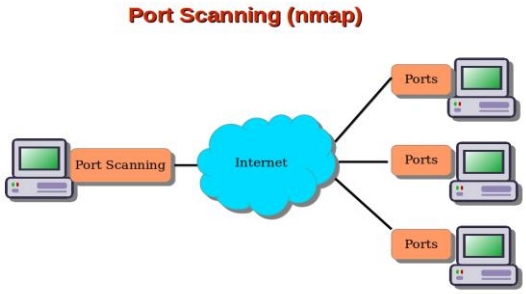
2.1 Scanning the Network

The first step is network scanning. The whole network is scanned using nmap scanning and we get IP address and MAC address of all the available devices. The desired target is then selected to attack various modules on it.

2.2 PORT scan

A port scanner is an application designed to probe a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify network services running on a host and exploit vulnerabilities.

A port scan or portscan is a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port; this is not a nefarious process in and of itself. The majority of uses of a port scan are not attacks, but rather simple probes to determine services available on a remote machine



.

Fig 3 Port Scanning

2.3 Denial-of-Service (DOS Attack)

In computing, a **denial-of-service attack** (**DoS attack**) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

In a **distributed denial-of-service attack** (**DDoS attack**), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

A DoS or DDoS attack is analogous to a group of people crowding the entry door of a shop, making it hard for legitimate customers to enter, disrupting trade.

Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web server such as banks or credit card payment gateways, Revenge, blackmail and activism can motivate these attacks.

2.4 Sniffing Attack

Sniffing attack or a Sniffer attack, in context of network security, corresponds to theft or interception of data by capturing the network traffic using a sniffer (an application aimed at capturing network packets). When data is transmitted across networks, if the data packets are not encrypted, the data within the network packet can be read using a sniffer. Using a sniffer application, an attacker can analyze the network and gain information to eventually cause the network to crash or to become corrupted, or read the communications happening across the network. Sniffing attacks can be compared to tapping of phone wires and get to know about the conversation, and for this reason, it is also referred as wiretapping applied to the computer networks. Using the Sniffing tools, attackers can sniff sensitive information from a network, including Email traffic (SMTP, POP, IMAP traffic), Web traffics (POP, IMAP, HTTP Basic), FTP traffic (Telnet authentication, FTP Passwords, SMB, NFS) and many more. The Packet Sniffer utility usually sniffs the network data without making any modifications in the network's packets. Packet sniffers can just watch, display, and log the traffic and this information can be accessed by the attacker.

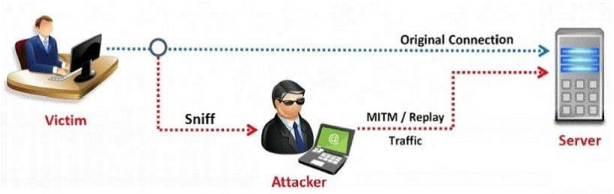


Fig 4. Sniffing Attack

2.5 Spoofing Attack

A spoofing attack is when an attacker or malicious program successfully acts on another person's (or program's) behalf by impersonating data.takes place when the attacker pretends to be someone else (or another computer, device, etc.) on a network in order to trick other computers, devices or people into performing legitimate actions or giving up sensitive data. Some common types of spoofing attacks include ARP spoofing, DNS spoofing and IP address spoofing. These types of spoofing attacks are typically used to attack networks, spread malware and to access confidential information and data.

2.6.Types of Spoofing Attacks :

2.61. ARP Spoofing Attack

The Address Resolution Protocol (ARP) is a protocol used to translate IP addresses into Media Access Control (MAC) addresses in order to be properly transmitted. In short, the protocol maps an IP address to a physical machine address. This type of spoofing attack occurs when a malicious attacker links the hacker's MAC address with the IP address of a company's network. This allows the attacker to intercept data intended for the company computer. ARP spoofing attacks can lead to data theft and deletion, compromised accounts and other malicious consequences. ARP can also be used for DoS, hijacking and other types of attacks.

2.6.2. DNS Spoofing Attack

The Domain Name System (DNS) is responsible for associating domain names to the correct IP addresses. When a user types in a domain name, the DNS system corresponds that name to an IP address, allowing the visitor to connect to the correct server. For a DNS spoofing attack to be successful, a malicious attacker reroutes the DNS translation so that it points to a different server which is typically infected with malware and can be used to help spread viruses and worms. The DNS server spoofing attack is also sometimes referred to as DNS cache poisoning, due to the lasting effect when a server caches the malicious DNS responses and serving them up each time the same request is sent to that server.

2.6.3. IP Spoofing Attack

The most commonly-used spoofing attack is the IP spoofing attack. This type of spoofing attack is successful when a malicious attacker copies a legitimate IP address in order to send out IP packets using a trusted IP address. Replicating the IP address forces systems to believe the source is trustworthy, opening any victims up to different types of attacks using the 'trusted' IP packets.The most popular type of IP spoofing attack is a Denial of Service attack, or DoS, which overwhelm and shut down the targeted servers. One outcome attackers can achieve using IP spoofing attacks is the ability to perform DoS attacks, using multiple compromised computers to send out spoofed IP packets of data to a specific server. If too many data packets reach the server, the server will be unable to handle all of the requests, causing the server to overload. If trust relationships are being used on a server, IP spoofing can be used to bypass authentication methods that depend on IP address verification.

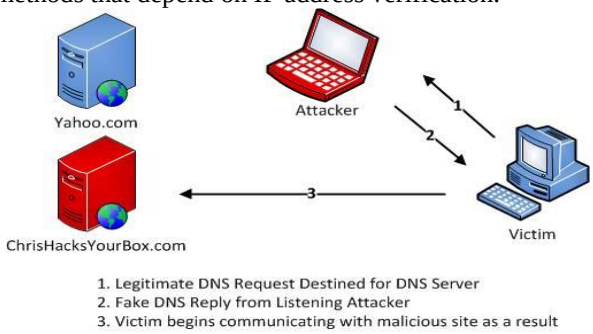


Fig 5. Spoofing Attack

III. IMPLEMENTATION AND SECURITY MEASURES

3.1 Creating a Network

A network is to be created to implement or test MITM attack. We can also connect to a LAN network to test and attack MITM on several IP's. Another option we have is to create a network using a mobile hotspot or USB tethering. As ubuntu (OS) is running on virtual machine, we can test and implement MITM on our original OS that is Windows 8.1 or we can connect several PC in our network to implement MITM. We can also connect to a WIFI router to test MITM.

3.2 Steps for Testing MITM

As soon as the MITM starts, our first job is to scan the network we are connected to. The nmap scanning gives us IP address and MAC address of all the devices connected with us. Using social engineering toolkit we then find out the IP of our target. We can also attack on all the users in our network using "all" command at terminal.

After choosing the desired IP address we need to choose the attack we want to exploit on victim. If we choose Pscan, we get a list of all the open ports on the victims PC. If we choose DOS attack, we can flood fill the server of the victim which will make the server crash. If we choose Ping, it gives us the information whether we are still connected to the victim's IP or not. If we choose Sniffing, a new window opens where we get details of all the data transmission in the network. If we choose Spoofing attack, we enter an IP address where we want to redirect the target browser. For example if we enter the IP address as 103.221.244.65 (Amizone IP address) in the terminal, the web browser on victim pc will just open www.amizone.net, whatever the victim will try to search he/she will end up on Amizone.net. A drawback here is, that it doesn't works on HTTPS weebsites as they are much secured. So I tried the attack on www.yahoo.com,www.w3schoo.com and www.way2sms.com. And if we choose, Yplay module, we need to enter the ID of desired youtube video in the terminal and the victim will listen the audio of the selected video while surfing on his browser.

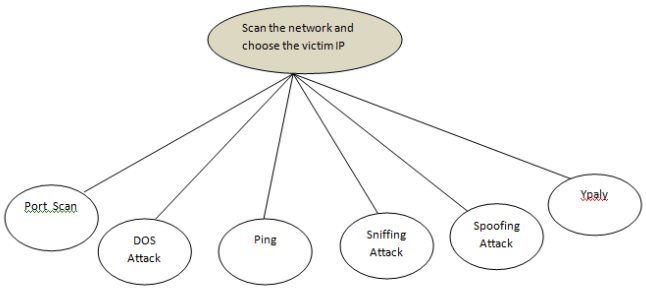


Fig 6 Data Flow Diagram

Fortunately, there are several ways to protect your computer from the hackers on internet:

Software Updates: Software companies are always updating their products, trying to eliminate any security breach that could be exploited by hackers. For this reason, their software makes a periodic check on the latest version available in the internet. It doesn't matter if they are operating systems, office suites, drivers, games or any other kind of specialized software, you always need to assure yourself that every software package is up to date.

Firewall: Firewalls became main stream with the Internet. Now-a-days it's impossible to be connected to the net without being checked by hackers, looking for possible breaches in your 39 connection. Although they can be hardware or software, the most common one among users are the software firewalls, which are installed in your operating system and continually check the transmission of information from your PC to the external world and vice versa. Antivirus: from all the security packages that a user needs to have installed in his PC, antivirus software is the first. It has been with us for a long time, even before the internet and the now common news on internet hacking. In the old days, virus spread through corporate networks to employee home computers who innocently took work home via diskettes. Finally, it spread to their friends' computers. Today, the Internet has provided viruses a better way to spread themselves through the world. A real time antivirus software package is a must for any user who wishes to navigate safely through the net and not find himself being a victim of a hacker attack.

Data Encryption: All digital mobile systems provide security through some kind of encryption. Data can be encrypted in many ways, but algorithms used for secure data transfer fall into two categories: symmetric and asymmetric. Both rely on performing mathematical operations using a secret number known as a key. The difficulty with symmetric algorithms is that both parties need to have a copy of the key. On the other hand, asymmetric techniques use two separate keys for encryption and decryption. Usually, the encryption key can be publicly distributed, whereas the decryption key is held securely by the recipient. The most widely used symmetric algorithm in DES (data encryption standard), developed by IBM in 1977. It uses a 56-bit key, which seemed unbreakable at that time. In 1997, a group of Internet users managed to read a DES-coded message. Most organization now use triple-DES, which uses 112 bits. The basic idea is that larger keys mean more possible permutations, and so better encryption

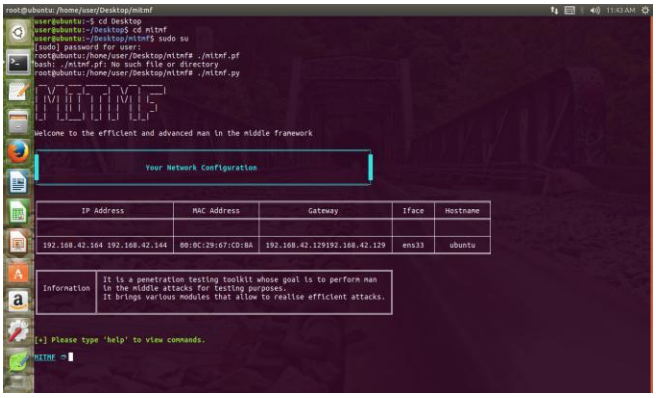


Fig 7 Starting MITM

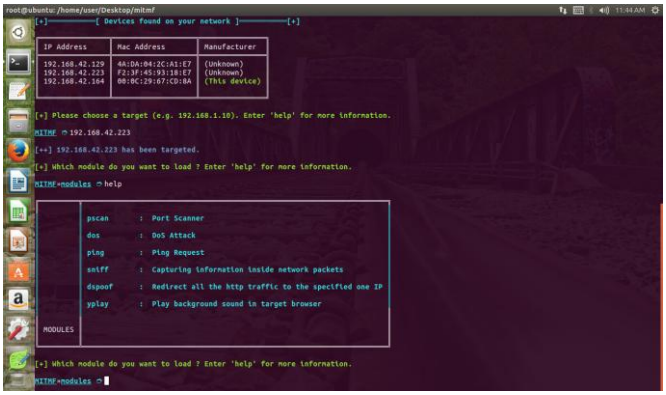


Fig 8. Choosing the Victim's IP Address

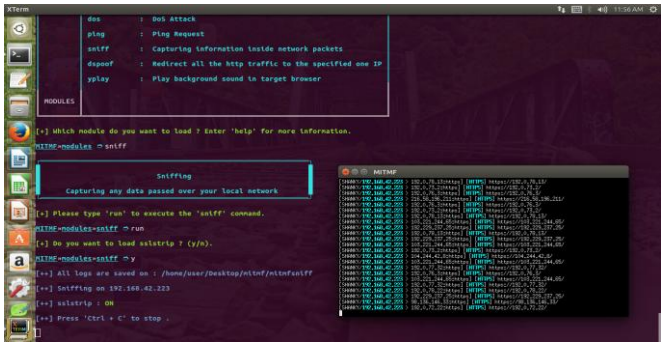


Fig 9. Sniffing Attack

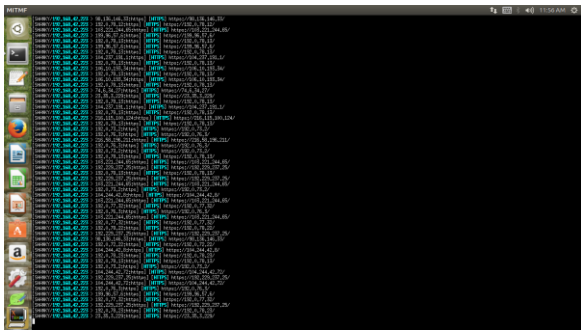


Figure 10. Results after Sniffing Attack

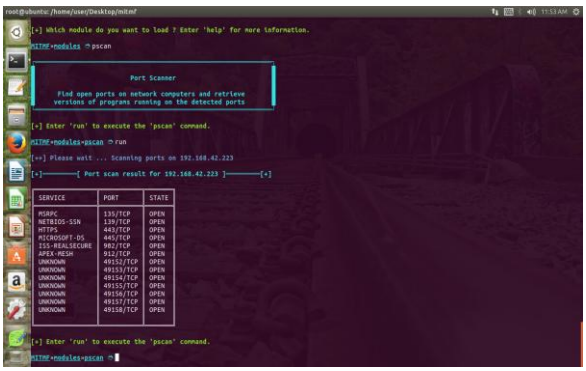


Fig 11. Port Scaning

Fig 12. PIng Request

IV. CONCLUSION

Based on the testing done in the project, which was conducted in varying network sizes, the detection mechanism was able to identify all the IP address and MAC address in the network.

The tools used for this project were much effective to penetrate through the network. It was quiet easy to spoof and sniff through the network. Sniffing through payment gateways and capturing the crucial information is quiet easy. Redirecting the victim IP to the desired IP address was just an attack away.

V. REFERENCE

[1] www.hackingarticles.com
[2] www.github.com
[3] Web Hacking 101 is written by Peter Yaworski
[4] Hacking: The Art of Exploitation (2nd Edition)