Man in the Middle Attack: Demonstration using Kali Linux and Defense Mechanism

Kamran Adil, Lalit Manohar Challa, Mysura Reddy Kuchuru, Sai Milind Bedarakota

Department of Computer Science,
New York Institute of Technology, New York

***Abstract* - In a time when the whole world is impacted by the COVID-19 virus, and the greatest intellectual minds of our civilization have to confine behind a computer screen, the usage of the internet has jumped exponentially, not to mention the unwavering need for everyone to use social networking and video conferencing to stay connected with their co-workers and family. This increased dependence on the internet and wireless network has also given rise to the risks it comes with. The risk of the data breach, when data packets are transmitted over the wireless network, it is susceptible to spoofing and cyber attacks like Man in the Middle Attack (MITM). This paper attempts to demonstrate this cyber attack and simulate it using open source Ettercap tool in the Kali Linux environment, for instruction use in the academic setup.**

Keyword- Man-in-the-Middle (MITM), ARP- Address Resolution Protocol

Ⅰ. *Introduction*

A man-in-the-middle attack is a cyberattack that is carried out on two targets connected to the same network either on LAN or wireless. The attacker can sniff the data that has been transmitted by the user including personal details or confidential business information. MITM attacks can be done in different ways but we have chosen the ARP spoofing method over Kali Linux. It is a web penetration testing OS that has tools like ARP(Address Resolution Protocol) spoofing, and DNS spoofing. We are performing a MITM attack using ARP spoofing with the help of the Ettercap tool that was present in the kali Linux software. Since a MITM attack is the most common way of sniffing data from the target system a defense mechanism has to be carried out to prevent MITM attacks and have a secure link with the router.[1]

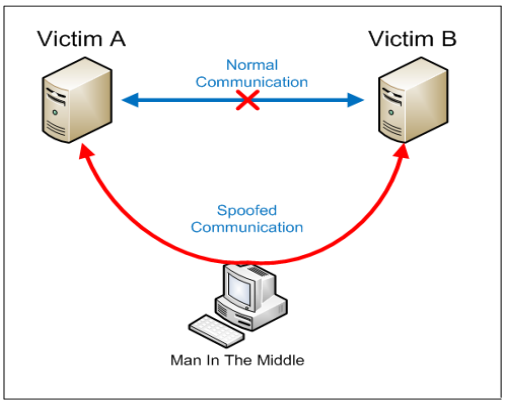


Fig.1 Man in the Middle Attack [2]

Ⅱ. *History*

The first MITM attack was figured out in the early 1900s when Professor Fleming was demonstrating the ability to transmit a message from one location to another wirelessly. During this process, the man-in-the-middle, Mr.Maskelyne set up his own receiver and captured the message that Prof. Fleming wanted to send from Cornwall to the Royal Institute. Instead of receiving the original message, the royal institute received a new/revised message. Several years later, during world war II. The Nazi Forces were targeted by British Intelligence in which operators used to transmit to German listeners with false information with the intent to make them lose confidence.[3]

Ⅲ. *Types of MITM Attacks*

When the attacker manages to get in between the sender and the receiver by making them believe that they are communicating and vice versa. The communication we are talking about here may be between two end users or between the client and server. The types of MITM attacks are given below:[4]

- HTTPS Spoofing
- SSL Stripping
- Wi-Fi Eavesdropping
- DHCP Spoofing
- DNS Spoofing
- ARP Poisoning

HTTPS Spoofing- Creating a duplicate website with the same figures and data, an attacker can capture the personal, professional, and financial data of a potential user of that website and make a copy of it and use them on a legitimate server is called HTTPS Spoofing.

SSL(Secure Socket Layer) Stripping- Here the attacker removes the SSL encryption between the source and destination by creating a bridge between them. By creating this bridge the attacker can form a connection between the server and the source.

Wi-Fi Eavesdropping- Creating a fake Address Protocol and making the users connect to it. When the Address Protocol doesn't consist of a password, the attacker can sniff all the network traffic and successfully implements HTTPS Spoofing and SSL Stripping.

DHCP Spoofing- DHCP Spoofing is executed in LAN Networks. Here the attacker uses DNS Spoofing to create a Rogue DHCP Server. When a client requests a message to communicate with DHCP Server, the request is received by the two servers, one is the main one and the other is fake. The server which is close to the client responds first, but in this case, the DHCP server which was created by the attacker responds as the original server has been already DOS-ed.

DNS Spoofing- DNS is a protocol that translates domains to Ip addresses. But, it has a flaw the user cannot verify the DNS response it gets from the client that flaw is used by the attackers to create DNS spoofing. When a user wants to access a website he sends a DNS request to get the IP address of the website and the DNS server sends back the IP to the user. If the attacker can identify the unique identification number sent by the DNR server he can create a fake DNS server and connect to the user system.

ARP Poisoning- The most commonly used MITM technique is ARP Poisoning because of the poor security of the ARP Protocol. It is one of the simplest ways to perform the MITM attack. It focuses on creating a bridge between the MAC address and the IP address. The methodology used in this method is a request-response protocol. The problem with the non-state protocol is the host accepts the ARP reply even if it didn't send any request. This is the case where they upgrade their ARP caches at every interval for an ARP reply. This is where the attacker sends a response using the modified/copied MAC Address and attacks the communication.

Ⅳ. *Implementation*

A. Installing Kali Linux

1. Download VirtualBox for Windows machines and UTM for MAC machines.
2. Download the Kali Linux ARM image from the following link https://www.kali.org/get-kali/#kali-bare-metal
3. Setup the UTM and/or VirtualBox with the needed configurations.
4. Install Kali Linux using the Graphical Installation method.

B. Using Ettercap

1. Open the Ettercap configuration file using the below command on the root terminal and change ec_gid & ec_uid to 0.

leafpad /etc/ettercap/etter.conf

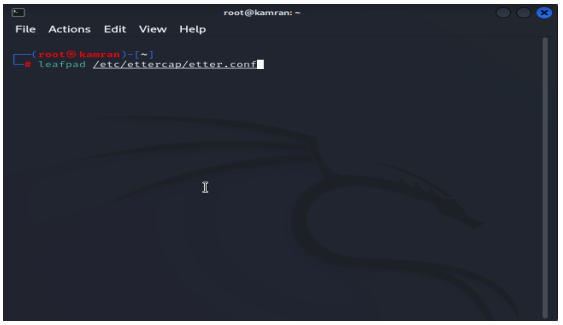


Fig.2 Changing Ettercap Configuration

2. Open Ettercap Graphical from the applications given and set your network interface (Example: Eth0)

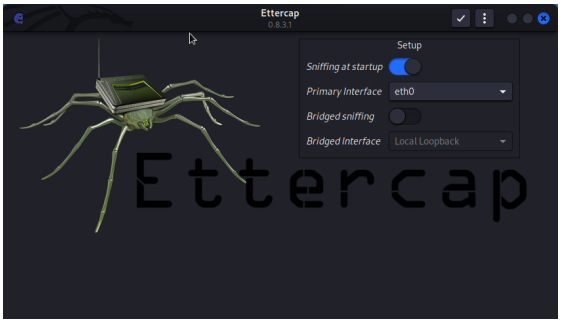


Fig.3 Starting Unified Sniffing

3. Start the unified sniffing and go to Host to scan the available hosts in the same network.

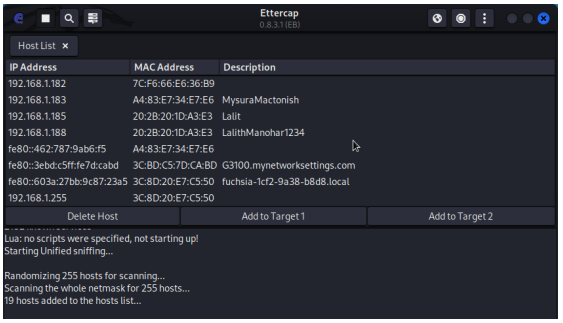


Fig.4 Scanning for Hosts

4. Add the router IP or the gateway IP to target 1 and the victim IP to target 2.

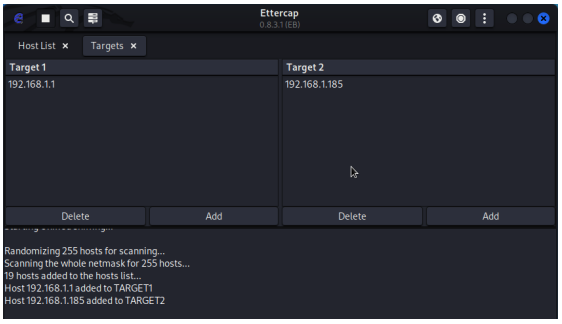


Fig.5 Selecting Hosts for Attack

5. Start MITM attack through ARP Poisoning.

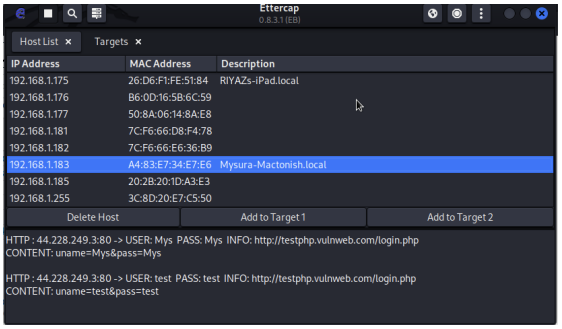


Fig.6 User info being displayed

This method only works for HTTP websites, if we want to sniff an HTTPS website, we have to do a process called SSL strip.

Write the following command on the root terminal of the attacker's machine. [2]

1. *iptables -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT*
2. *iptables -A INPUT -i eth0 -p tcp --dport 8080 -j ACCEPT*
3. *iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080*
4. SSL strip -l 8080

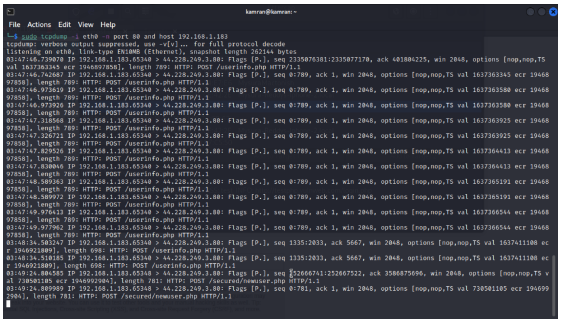
V. *Applications*

1. The users can safeguard their PC against man-in-the-middle attacks with LAN Connection from Network.
2. The testers can check the strength of the man-in-the-middle attack tool or software and whether it is vulnerable to the attack.[1]
3. Ethical hackers can challenge their attacking powers and the quality of code by attempting different attacks.
4. The business firms can prevent their data which is confidential being leaked and inappropriately shared.
5. Educators or Researchers can work on different mechanisms or methodologies to learn about defense mechanisms in a virtual environment.

VI. *Defense Mechanism against MITM attack*

1. The attacker initiates the MITM attack using ARP Poisoning which makes the user's computer believe that the attacker's MAC address is the same as the router's address. So, by using a Static ARP Entry, the user will have the information that the router MAC Address is standard and it ignores any false data sent by the attacker.

2. Monitoring the ARP tables in regular intervals for checking for any mismatch in MAC Address. If there is any sniffing happening, the user can detect it by using ARP Monitoring Software.



VII. *Conclusion*

The post-Covid world in which we are living today revolves around the internet and data. As much as we like working from the comforts of our homes, the risk of cyber-attacks has increased, considering all of our transactions are digital. Following security protocols is essential in these crucial times, this paper shows how easily an intruder can sniff our personal and sensitive data. We users have to take precautions to make our data safe from sniffing, never use public networks to share or login to our personal information, the attackers can easily sniff the data like the login credentials and bank transactions in an open network. MITM is just one type of attack, the conclusion is to stay informed about these attacks, and learn more about digital systems before using them. Awareness is important, it helps prevent falling prey to these cyber-attacks.

VIII. *References*

[1] H. Shah, H. Dudhat, H. Gogri, and K. Dani, "Man in the Middle Attack: Implementation using Kali Linux and Defense Mechanism." Accessed: Nov. 01, 2022. [Online]. Available: https://web.archive.org/web/20180409220955id_/http://www.ijritt.org/paper/IJRITTV1IS010002.pdf

[2] B. Pingle, A. Mairaj and A. Y. Javaid, "Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use," 2018 IEEE International Conference on Electro/Information Technology (EIT), 2018, pp. 0192-0197, doi: 10.1109/EIT.2018.8500082.

[3]"Cybersecurity History: The 1st Man-in-the-Middle Attack," *blog.havocshield.com*. https://blog.havocshield.com/en-us/cybersecurity-history-the

-very-first-man-in-the-middle-attack

[4]D. Javeed and U. MohammedBadamasi, “Man in the Middle Attacks: Analysis, Motivation and Prevention,” *International Journal of Computer Networks and Communications Security*, vol. 8, no. 7, pp. 52–58, Jul. 2020, doi: 10.47277/ijcncs/8(7)1.