Real-world Man-in-the-middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use

Bhargav Pingle, Aakif Mairaj, Ahmad Y. Javaid

Electrical Engineering and Computer Science Department
University of Toledo, Toledo, OH 43606, USA
Bhargav.Pingle@rockets.utoledo.edu, Aakif.Mairaj@rockets.utoledo.edu, Ahmad.Javaid@utoledo.edu

***Abstract*— Cybersecurity is becoming more significant with the increased reliance on the internet; and wireless networks like Bluetooth and Wi-Fi. There are many vulnerabilities in the cyber world which the attackers are exploiting. One such attack is Man-In-The-Middle (MITM) attack. Man-In-The-Middle (MITM) is one of the primary attacks employed in computer-based hacking. In this paper, we will discuss how the attacker performs the Man-in-the-middle (MITM) attack using the open source Ettercap tool in Kali Linux environment. Ettercap tool is a sniffing tool available in the Kali Linux operating system. It is used to perform sniffing, using Man-in-the-middle attack and other attacks like DDOS attack, packet filtering, DNS spoofing, etc. This paper attempts to implement this attack for instructional use in an academic setup for teaching a foundational cybersecurity course.**

***Keywords* —Sniffing, Kali Linux, man-in-the-middle attack, Ettercap tool. ARP poisoning, SSL strip, MAC address, IP address.**

I. Introduction

Today, networks play a vital role in everyone's life to perform a wide array of tasks including communication, finance, banking, and shopping. The massive usefulness of networks makes them continuous targets of attacks. Therefore, it is essential to understand their implementation along with the associated threats and their countermeasures. Although every institute offers courses on networks and security, the courses need to be equipped with hands-on training to enhance students' learning. To this end, we aim to develop a foundational cybersecurity course with in-built hands-on activities. This paper presents one such successful implementation of a popular network attack.

Kali Linux is Debian derived Linux distribution designed digital forensics and penetration testing. It is one of the best security packages of an ethical hacker. Offensive Security Limited maintains and funds Kali Linux. It was developed by Mati Aharoni and Devon Kearns. Kali Linux has more than 300 penetration testing tools. Multiple languages are also supported by Kali Linux.

A. Ettercap

Alberto Ornaghi and Marco Valleri (a.k.a ALoR and NaGa) developed Ettercap tool. It is a free and open source tool. It runs on various UNIX like operating systems including Linux, Mac OS X, and Solaris. Ettercap is a "multipurpose sniffer/interceptor/logger for switched LANs [1]". It has evolved into a versatile network manipulation tool as it can perform character injection, packet filtering, kill any connection, etc.., apart from the man-in-the-middle attack. Once Ettercap places itself in the middle of a switched connection, it can acquire and analyze all the communication happening between the two victim hosts, and then if the attacker can take advantage of the situation.

Ettercap also has other features that the attacker can take advantage of [2]. They include:

- *Character Injection*: The attacker can insert any arbitrary characters into a live connection in both the directions. He can emulate either commands sent from the client or the replies sent from the server.
- *Packet filtering*: Attacker can sift the TCP or UDP payload of packets in a live connection by looking for an arbitrary ASCII or hexadecimal string, and substituting it with his string, or by simply removing the filtered packet.
- *Automatic password collection* (for most of the common network protocols): The *active dissector* block automatically picks and extracts relevant information from many protocols including TELNET, FTP, POP3, RLOGIN, SSH1, ICQ, SMB, MySQL, HTTP, NNTP, X11, NAPSTER, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, and SNMP.
- *Secure Shell (SSH) support*: Attacker can sniff the username, password and the data of an SSH1 connection.
- *Hyper Text Transfer Protocol Secure (HTTPS) support*: Attacker can hijack HTTP SSL session, as long as the user accepts the false certificate.
- *Point-to-Point Tunneling Protocol (PPTP) suite*: Attacker can perform MITM attack against PPTP tunnels.

978-1-5386-5398-2/18/$31.00 ©2018 IEEE

- *Kill connection*: Attacker can kill any connection using this tool between two hosts or a client and a host with their IPs known.

B. SSL-strip

An independent computer security researcher called Moxie Marlinspike developed SSL-strip. He revealed this tool in the Black Hat Convention in 2009 held at Washington D.C. He also discovered many vulnerabilities in SSL implementations. By the use of man in the middle attack with SSL strip, the tool makes sure that the browser does not warn the user about the false certificate or an expired certificate. The user will not notice any warning signs, nor will he be able to notice the lock icon missing from https:// in the address bar. Majority of the users of the internet do not ever type https or HTTP in the address bar; they automatically get secure websites through HTTP redirects. The SSL strip redirects all the traffic to itself by acting as a proxy [3].

For example, if a user opens Gmail, and as we know that Gmail normally redirects to SSL enabled webpage login, but if the SSL strip is working, it will receive that redirect, and it will strip the SSL enabled webpage login and instead give the user a non-SSL enabled version of the same site Gmail. The attacker will be able to listen with a packet sniffer like Ettercap or NMAP, and he can see all traffic that is being transmitted over the user's HTTP connection that is unsecured. An article states that: "SSL strip does not demonstrate a weakness in SSL encryption, but rather takes advantage of users who fail to look for trusted SSL encryption when sending sensitive information over the internet." (DigiCert EV SSL Certificated Protect Users from SSL strip and Man-in-the-Middle Attacks) [4].

C. Man-In-the-Middle (MITM) Attack

Man-In-The-Middle (MITM, also referred to as MIM, MiM, MitM, or MITMA in the literature) is a type of attack in which a third party in stealth takes control of the communication channel between two or more parties. In MITM attack, the attacker can intercept, modify, change, or replace target victim's communication traffic. The victims are not aware of the man in the middle, so, they believe that the communication channel is protected [4] Man-in-the-middle attacks allow the attacker to intercept, send and receive the data which is never meant to be for them without the outside party knowing about it.

Man-in-the-middle can be used to invoke attacks such as Distributed denial of service (DDOS) attack, DNS spoofing, port stealing and session hijacking. MITM has many consequences such as stealing someone's online user ID and password, stealing telnet session, stealing local FTP ID, etc. Man-in-the-middle attacks can be active or passive. In a passive attack, the attacker's presence is not detected, but he only captures the data that is being transmitted and sends it to the original person who is supposed to receive it. Whereas in an active attack, the contents are intercepted and manipulated before being sent to the expected destination. The Only difference between an active MITM attack and passive MITM attack is the attacker modifies the information to be sent in an active attack, while, in a passive attack he just records it without modification.

MITM attacks are rare on the wired internet due to lack of the spots where the attacker can insert himself between two communicating terminals and remain undetected [4]. But for wireless connection, there is a difference in the situation. It can be effortless for the attacker to insert his information depending on the nature of the wireless link layer protocol.

Figure 1 shows the difference between the flow of information or data in the regular communication and the flow of data in the man-in-the-middle kind of flow. In normal flow, the communication is taking place in between the two parties communicating with each other i.e.., the client and server and there is no intrusion or mediation of any man in the middle. Whereas, in the Man-in-the-middle flow we can see that the communication is happening between through the attacker or the man in the middle. Therefore, the attacker can spoof the victim as the server. He can affect the confidentiality, integrity, availability of the data. The storage of cryptocurrencies is also prone to a Man-In-The-Middle (MITM) attack. The most recent MITM attack exposed the vulnerability of ledger hardware wallets that were once considered safer methods to store cryptocurrencies. This attack would allow a cybercriminal to show the customer, a fake address of the cryptocurrency and use the original address to transfer to his wallet [6]. A Man-In-The-Middle (MITM) attack will transfer the cryptocurrency to a fraudulent address instead of the user's wallet. This attack is accomplished by infecting the victim's computer with malware that will accommodate the MITM attack.

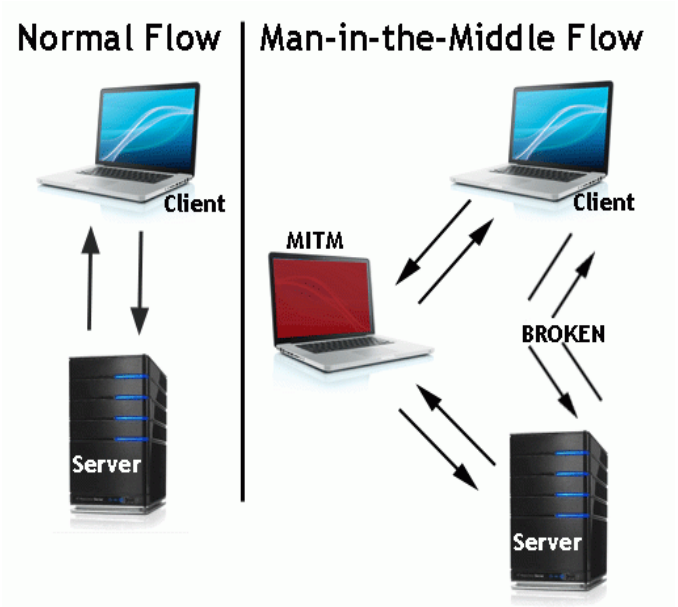

Fig. 1. Difference between the flow data in normal flow VS the flow in the Man-in-the-middle flow [5].

D. Methods in Man-In-The-Middle Attack

A variety of methods can achieve man-in-the-middle attacks. Anybody who gets access to network packets as they travel between two hosts can perform these attacks [7]:

- *Address Recall Protocol (ARP) poisoning*: Using Ettercap, we can perform ARP poisoning. An attacker can monitor and then hijack a TCP session. This is subject to the condition that the attacker must be on the same network as either the victim or the host with which it is communicating.
- *Internet Control Message Protocol (ICMP) redirects*: The attacker can make a router to forward packets intended for the victim through the attacker's machine. There is a chance that the attacker can also change the packets even before they have reached the destination.
- *Domain Name System (DNS) poisoning*: An attacker can redirect victim's traffic by poisoning the victim's DNS cache with the incorrect hostname to IP address mapping.

E. ARP Poisoning

1) *Address Recall Protocol (ARP):* Address recall protocol (ARP) maps Internet Protocol address (IP Address) to a physical machine address (MAC address) that is recognized in the local network. There is a table called ARP cache, which is used for mapping the MAC address to its corresponding IP address.

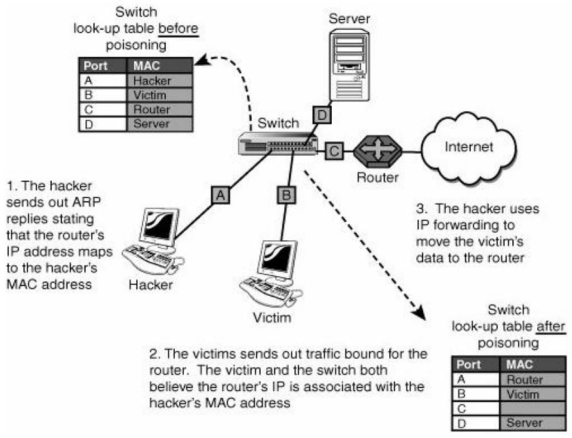

Fig. 2. Example of how the ARP poisoning is happening [7].

2) Working:

When a packet, which is supposed to be received, by a host machine on a particular LAN (Local Area Network) arrives at a gateway, the gateway will ask for the ARP program to search and find a MAC address which matches the IP address. The ARP program searches in the ARP cache, and it provides it so that packets can be converted to the right packet length format if it finds the address. The ARP program makes updates to the ARP cache for future reference, and then packets are sent to the MAC address associated with it [8].

3) ARP poisoning:

In ARP poisoning the host's ARP table or ARP cache is corrupted, allowing the hacker to redirect all the traffic to his machine. When an attacker sends forged ARP replies, the ARP poisoning happens.

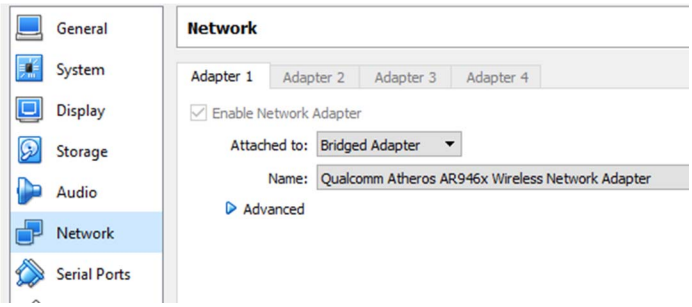

Fig. 3. Virtual machine setting changed to "bridged adapter" from "NAT" which was a default.

II. Literature Survey

In the existing literature, several works explain, demonstrate and propose the protection mechanisms against the Man-in-the-middle (MITM) attack. In [9], the author discusses different types of MITM attacks, its consequences and proposes some solutions against MITM attack, for example the use of ARP request packet to the gateway, monitoring ARP –a database, using static entry in layer-3 switch or in the gateway and restricting ICMP packet. Yogesh Joshi in [10], proposes another MITM prevention technique: It explains the use of the public key of the server's digital certificate, required for hashing the user password to prevent the MITM attack over secure socket layer. In [11], Sumit kumar proposes the use of centralized system as a solution to the ARP cache poisoning. The prevention of ARP poisoning with the use of an advanced version of ARP is discussed in [12] by Seung Yeob. Another Technique JPCAP, which is a Java library for capturing and sending network packets to prevent the MITM attack in a LAN environment, is explained in [13].

III. Man-In-The-Middle Attack Implementation

A. Virtual box setup

The Man-in-the-middle (MITM) attack was implemented on Oracle VM VirtualBox. An open source computer software supports the creation and management of virtual machines. The students can download the VirtualBox software from oracle's virtualbox website [14]. We create a virtual environment with two virtual machines: 1. the attacker machine that runs kali Linux operating system, and 2. the victim machine which runs windows operating system.

The network settings of the virtual machine i.e.., the victim and the attacker will have to be changed to "bridged network." This will make the communication to happen through the IP address of the virtual machine rather than the main machine. Now

the Ettercap tool can scan for the victim's IP address. The victim that was used for the demonstration of attack was Windows 7 operating system, and the attacker was Kali Linux operating system.

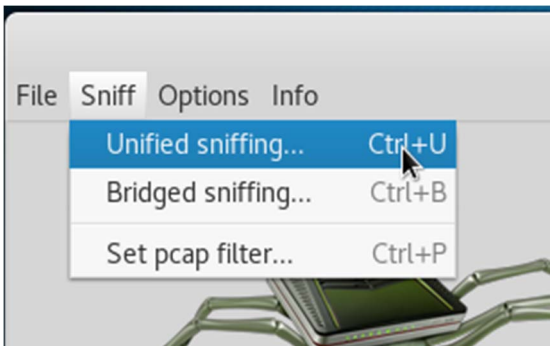

Fig. 4. Unified sniffing being selected in Ettercap

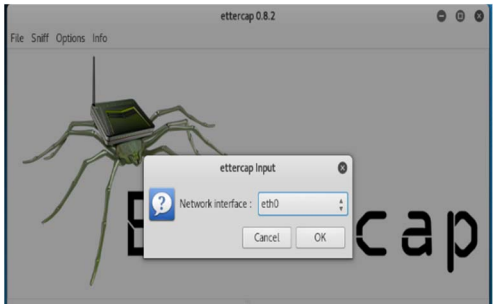

Fig. 5. "Eth0" being selected in unified sniffing.

B. Procedure:

Here we discuss the procedure of carrying out the attack.

- The Ettercap graphical is opened for applications in Kali Linux. Unified sniffing is started in the Ettercap graphical application.
- Select network interface as "Eth0" in the unified sniff. This is nothing but ethernet connection.
- Ettercap will start the unified sniff now; then, we have to scan for hosts so that we can select the targets. Therefore, we go to hosts and select scan for the hosts. Once the scan for hosts is selected, the software is going to start scanning for the hosts in the network which will be shown as "scanning the whole netmask for 65535 hosts…" This will take approximately 10 minutes to scan as there are 65535 hosts in our network.
- The target machine which is "Windows 7" has to be selected as Target 1, and the Target 2 will be all hosts as we do not know at which host the request will be received. So, the virtual machine's IP was found to be "172.31.231.123". We should select this IP address as the target.

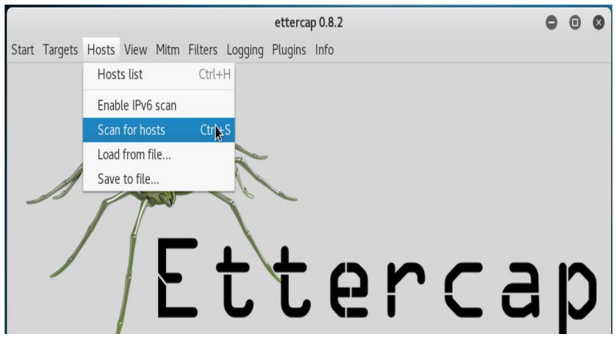

Fig. 6. "Scan for hosts" being selected in the hosts section.

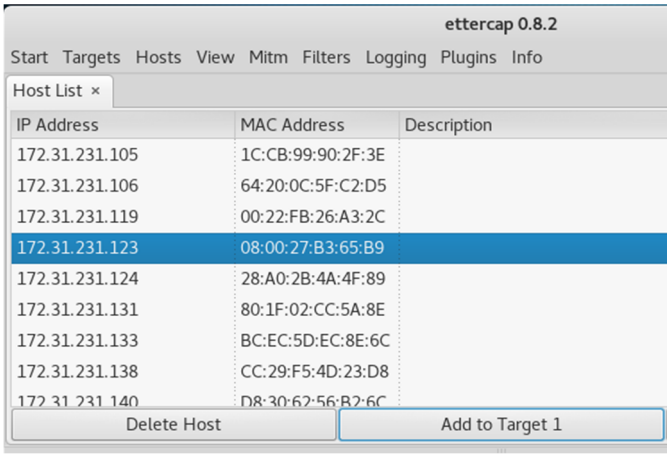

Fig. 7. Target's IP being selected in the Ettercap

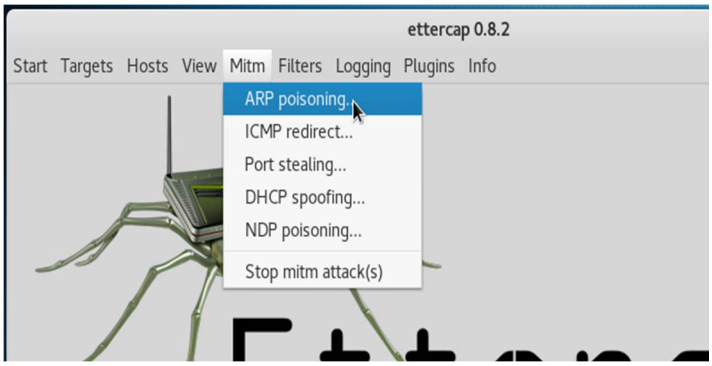

Fig. 8. ARP poisoning being selected in MITM (attack) section.

- Then start Man-in-the-middle (MITM) attack with Address Recall Protocol (ARP) poisoning by selecting "ARP poisoning."
- The MITM attack has started now all the user credentials entered in victim's browser will be displayed in the ettercap software. But this works only on sites that use HTTP protocol if we have to make it work on the sites that use HTTPS

protocol we have to use the tool SSL strip which is used to prevent the web browser from updating to an SSL connection.

The following commands are to be entered in the terminal of the attacker machine:

1) iptables -t nat -A PREROUTING -p TCP –destination -port 80 -j REDIRECT –to-port 8080 (This will redirect all the victim's requests to port 80 which is unsecured from the port 8080 which is secure.)

2) SSL strip -l 8080 (This will open sslstrip.)

- The MITM attack using Ettercap is now successful. The user credentials will all be displayed in the Ettercap software for the sites using HTTPS protocol too. The sslstrip will strip the SSL certificate to the user, but for the server, the requests will be HTTPS. So, the man in the middle attack sniffed the user credentials using Ettercap.

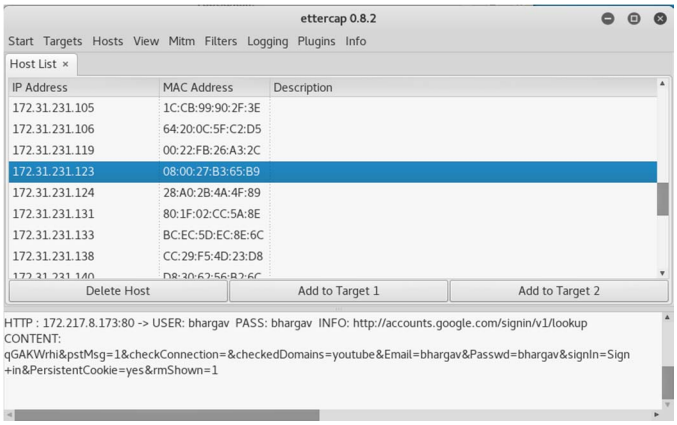

Fig. 9. Ettercap displaying the user credentials which it has sniffed.

IV. Defence against Man-In-The-Middle Attacks

A. Monitoring ARP table database

Before sending the data, the system always checks its ARP cache to deliver the data to specific MAC address. If ARP cache has wrong MAC address for a given IP address, then the data will be delivered to the mismatched MAC address [9]. In the MITM attack the attacker poisons the ARP cache with his own MAC address so that all the data is sent to his system. So if the ARP table is monitored at regular intervals of time to check for any mismatch in MAC address, the user can detect if there is any sniffing. An ARP monitoring software can be used for this purpose.

B. Static ARP entries

When the attacker performs MITM attack, his computer performs ARP poisoning which fool the victim's computer to believe that his MAC address is the address of the router. However, if we use a static ARP entry, the computer has the information that MAC address of the router is constant and does not vary and hence the computer ignores any false ARP packets that are sent by the attacker [9].

V. Conclusion

Cybersecurity is growing in its importance. It is a requirement for every individual to be knowledgeable of attacks and follow certain safety measures when on the internet. Privacy and data protection have become the needs of the hour. The sensitive data like the username and password can easily be sniffed if the user does not follow the security principle when on the internet. We have seen that the user credentials are easily sniffed using the Ettercap tool. The user can observe some safety precautions which might prevent his data from getting stolen. To train the next generation of workers in this area, it is necessary for students to learn cybersecurity and related attacks/concepts using actual real-world attack and protection implementation. Additionally, the user needs to be aware of best practices in safeguarding themself against popular cyber-attacks.

Firstly, the user should never be connected to insecure or untrusted networks. If he/she is unsure of the credible source on the internet, he should never get connected to it. Only the secure and trusted source should be relied on. In most of the cases, the password enabled connections can be trusted. Secondly, the user should never enter his credentials on a public network. He should only trust his network and never enter sensitive data over public networks or open networks. The data on the insecure networks can easily be traced by MITM attack.

Thirdly, even if the user has to enter the sensitive information he must always check for the https certificate. It can easily be removed using SSL strip by the attacker. So, anytime the user had to enter any sensitive information over the internet, he has to check whether there is SSL present or not. Users have to be wary of fake SSL certificates. We have seen that how easily an attacker can perform Man-In-The-Middle (MITM) attack using simple and open source tools like Ettercap and SSL Strip. Even the script kiddies can perform this kind of attacks. These attacks can be prevented if the user is alert while browsing over the internet. Especially when giving sensitive data over the internet, the user had to check twice for an encryption or an SSL certificate. Data can easily be compromised if the user is not alert over the internet.

VI. References

[1] A. Ornaghi, "Ettercap project," [Online]. Available: http://ettercap.sourceforge.net/. [Accessed 10 Feb 2018].

[2] D. Norton, "sans.org," sans institute, [Online]. Available: https://www.sans.org/reading-room/whitepapers/tools/ettercap-primer-1406. [Accessed 10 Feb 2018].

[3] J. Elks, "grin.com," [Online]. Available: https://www.grin.com/document/170676. [Accessed 10 Feb 2018].

[4] M. Conti, D. Nicola, and V. Lesyk. "A survey of man in the middle attacks." IEEE Communications Surveys & Tutorials 18, no. 3 (2016): 2027-2051.

[5] N. Du Paul, "veracode.com," CA technologies, [Online]. Available: https://www.veracode.com/security/man-middle-attack. [Accessed 08 Feb 2018].

[6] P. Smith, "bitcoinist.com," 09 Feb 2018. [Online]. Available: https://bitcoinist.com/ledger-hardware-wallets-vulnerable-man-middle-attacks/. [Accessed 10 Feb 2018].

[7] “iugaza.edu.ps,” [Online].Available:http://site.iugaza.edu.ps/nour/files/lab4-MITM1.pdf. [Accessed 05 Feb 2018].

[8] xinlwang,“mtu.edu,”[Online].Available:http://pages.mtu.edu/~xinlwang/itseed/labs/Spoof_MiTM.pdf. [Accessed 09 Feb 2018].

[9] G. N. Nayak, “Different Flavours of Man-In-The-Middle attack, Condequences and Feasible solutions,” *IEEE,* pp. 491-495, 2010.

[10] D. D. Yogesh Joshi, “Mitigating Man in the middle attack over Secure socket layer,” in *IEEE*, Bangalore, 2009.

[11] S. T. Sumit kumar, “A Centralized Detection and prevention Technique against ARP poisoning,” pp. 259-264.

[12] S. Y. Nam, “Enhanced ARP: Preventing ARP poisoning-Based Man-in-the-Middle Attacks,” *IEEE COMMUNICATIONS LETTERS,,* vol. 14, pp. 187-189, 2010.

[13] h. R. Faheen Fayyaz, “Using JPCAP to prevent man-in-the-middle attacks in a local area network environment,” 2012.

[14] “virtualbox,” or, [Online]. Available: https://www.virtualbox.org/. [Accessed 14 04 2018].