Case Study:Comparative Analysis of Man-In-The-Middle-Attacks and Preventive Measures.

[1]Miss.Nikita Nitin Bhagat
[1]2nd Yr-M.Tech(Computer Engineering)
[1]K.J.Somaiya College Of Engineering Mumbai-400077

Abstract - **The Man-In-The-Middle (MITM) attack is one of the most well-known attacks in computer security, representing one of the biggest concerns for security professionals. MITM targets the actual data that flows between endpoints, and the confidentiality and integrity of the data itself. In this paper gives exhaustive study on MITM attack and analysis their types. We survey existing countermeasures and discuss the types among them. Finally, based on our analysis, we categorized the MITM attack and their prevention mechanisms, and we identify some possible defense techniques for people. One of them is Penetration testing and cryptography technique. It helps to secure networks, and highlights the security issues. Penetration testing can be investigate different aspects of penetration testing including tools, attack methodologies, and defense strategies. More specifically, we analyzed different penetration tests using a private networks, devices, and virtualized systems and tools.**

keywords - **Man-In-The-Middle (MITM) attack, MITM defense techniques, types of MITM, and security.**

I. INTRODUCTION

Today, almost every one of our life could be the usage of cellular networks and websites. As an example, we use on-line banking, online entertainment and shopping, social networks, and so on. These entire on-line services store or transfer user's sensitive data that represents a key target for hackers. Hackers target enterprises and organizations, resulting in massive economical loss. During this new world of "people and things invariably connected" by means that of the net, it's quite common to daily examine successful attacks to connected things and on-line services. One of the most successful attacks is known as Man-In-The-Middle, which ends up in seizure over end-users' transferred knowledge. The name MITM Attack is derived from the basketball situation where 2 players can pass a ball to each different, whereas one player between them tries to seize it [1]. MITM attacks are many times referred to as bucket brigade attacks or fire brigade attacks [1]. Those all names are derived from the fire brigade operation of dousing off the fire by passing buckets from one person to another, between the water source and the fire. MITM attack is also known as:

-Monkey-in-the-middle attack.
-Session hijacking.
-TCP hijacking and
-TCP session hijacking.

Researchers showed that MITM attack is one of the most common types of security attacks. Such publications, articles, and previously specified awareness's clearly show that MITM attack has become more important and widespread attack. They able to affect every online interaction.

1.1 What is MITM attack?

In the MITM attack, the common scenario involves:
-Victims (two endpoints).
-Attacker (third party).
The attacker has access on communication channel between two victims, and can manipulate their messages. The MITM attack can be visualized as shown on Fig 1.
-Victims try to initialize secure communication by sending each other public keys (messages M1 and M2).
-Attackers intercept M1 and M2, and as a return sends its public key to the victims (messages M3 and M4).

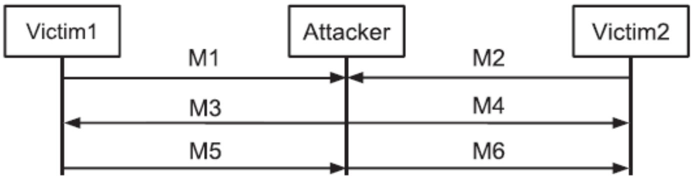


Figure 1: Exchanged messages in a typical MITM attack.

-After that, victim1 encrypts its message by attacker's public key, and Sends it to victim2 (message M5).
-Attacker intercepts M5, and decrypts it using known private key. Then, Attacker encrypts plaintext by victim2's public key, and sends it to victim2 (message M6).

-As a result, the attacker has convinced both victims that they use secure channel, but in reality it has access to all encrypted messages.

II. LITERATURE SURVEY

In this paper, we've analyzed MITM attack and given a comprehensive classification of such attack supported impersonation techniques. Also, we tend to provided varied MITM defense mechanisms beside their descriptions. We gather all MITM prevention mechanisms, according to used approaches and defense mechanism. We will collect the foremost effective strategies within the MITM attack like cryptologic technique and penetration testing [2]. These strategies are mentioned throughout the paper. To the best of our information, the term Man-In-The-Middle attack was first mentioned by Bellovin et al. in [10] with relevance [11]. After that paper, the term MITM has become a reference attack within the security community, counting an increasing range of citations once a year. Researchers showed that MITM attack is one among the foremost common sort of security attacks. Frankel et al. [14] represented MITM attack as one of the most important threats against network security. Such publications aboard with previously specified awareness's clearly show that MITM attack has become more and more necessary and widespread, in theory having the ability to have an effect on each on-line interaction.

Penetration testing is a vital subject that IT administrators should remember of. With the net growing each day, the computer security field has become a really difficult topic not just for the companies but also for normal users. It's time to understand that we are not secure simply having an antivirus any longer. Penetration tools are obtaining tons of attention, since there are not any limitations in their production. Open supply tools may be changed according individual desires. Imagine a penetration tool to hack satellites and change predictions for weather patterns, or even modification the time, or maybe worst to active nuclear weapons. Nowadays, using these tools, we will hack medical devices, or maybe cars. This paper [2] careful crucial penetration testing attacks. In paper [3] describe a vulnerability within the mobile networks' knowledge usage billing system was demonstrated by using a mobile knowledge consumption attack. The attack works by delivering a malicious captive portal to the victim, forcing them to attach to their mobile data plan, and causing them to use data by the captive portal. Our attack would work once the victim connects to a free open Wi-Fi network that's offered in most low outlets, fast food restaurants, and airport.

III. HOW DOES A MITM ATTACK WORK?

Over the years, hackers found varied ways that to execute MITM attacks and believe it or not, it's become comparatively low-cost to buy a hacking tool online, simply proving however simple hacking someone can be if you have enough cash. Here are some common examples of MITM attacks your business can possibly encounter:

Example: Similar from the case above, hackers who use this tactic target email accounts of large organizations, especially financial institutions and banks. Once they gain access to special email accounts, they're going to monitor the transactions to create their ultimate attack a lot more convincing. for example, they can wait for a situation wherever the client are sending cash and respond, spoofing the company's email address, with their own bank details rather than the company's. This way, the client thinks they're sending their payment to the corporate; however they're really sending it right to the hacker.

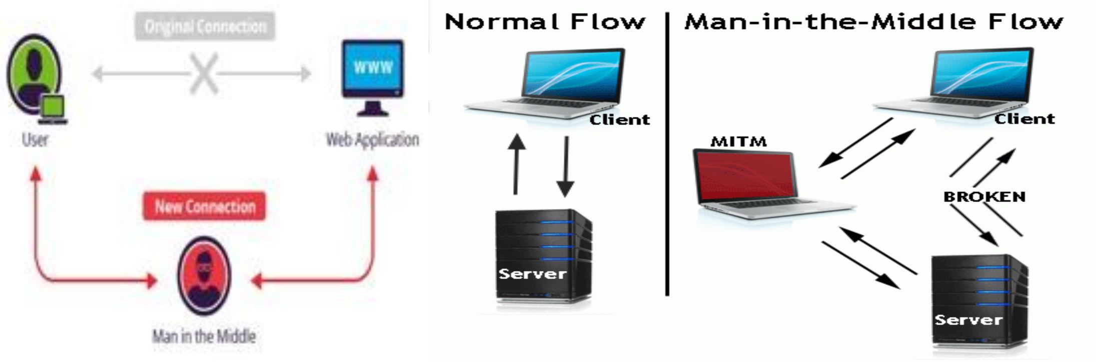


Figure 2: How does a MITM Attack Work.

In the Most MITM attacks thrive on Wi-Fi connections. All the hacker has to do is wait for you to connect and he'll instantly have access to your device. Alternatively, the hacker can create a fake Wi-Fi node disguised as a legitimate Wi-Fi access point to steal the personal information of everyone who connects [8]. In the Session Hijacking Once you log into a website, a connection between your computer and the website is established. Hackers can hijack your session with the website. One popular possibility they use is stealing your browser cookies. Cookies means store small pieces of information that makes web browsing convenient for you. It can be your online activity and login credentials. If they got hold of your login cookies, they can easily log into your accounts and assume your identity [8].

Examples: In the image above, you'll notice that the attacker inserted him/herself in-between the flow of traffic between client and server. Now that the attacker has intruded into the communication between the 2 endpoints, he/she can inject false data and intercept the information transferred between them.Below is another example of what might happen once the person in the middle has inserted him/herself [5].

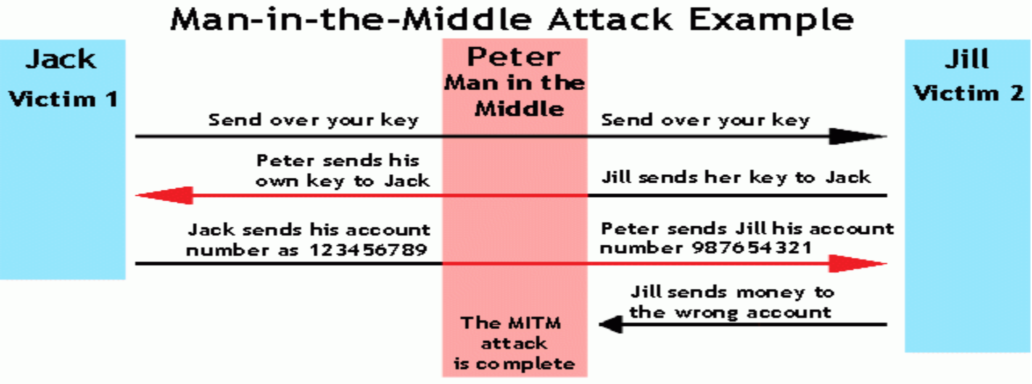

Man-in-the-Middle Attack Example
Jack
Victim 1
Peter
Man in the Middle
Jill
Victim 2
Send over your key
Send over your key
Peter sends his own key to Jack
Jill sends her key to Jack
Jack sends his account number as 123456789
Peter sends Jill his account number 987654321
Jill sends money to the wrong account
The MITM attack is complete

Figure 3: Example of MITM Attack.

The hacker is impersonating either side of the conversation to gain access to funds. This example holds true for a conversation with a client and server also as person-to-person conversations. Within the example higher than, the wrongdoer intercepts a public key and therewith will transpose his own credentials to trick the people on either end into believing they're talking to each other securely.

IV. COMPARISON BETWEEN MITM ATTACKS.

Cybercriminals can use MITM attacks to gain control of devices in a different ways.

SR.NO	TYPES	ATTACK ON	PURPOSES
1	**Wi-Fi Eavesdropping (Public Wi-Fi)**	System	1. Hacker to snoop on user activity. **2.** Hacker can access users system.
2	**DNS Spoofing**	create a phony website at the new IP address that looks just like a genuine website	Access user's sensitive information and personal data.
3	**Email Hijacking**	social engineering **(Email)**	1. They may also use spear-phishing to manipulate a user to install malicious software. 2. use information from a hacked email account to impersonate an online friend
4	**SSL Stripping**	Creates a duplicate website for the user like- http://.	Steal the personal data
5	**Man-in-the-Browser**	Website	1. Hacker used to capture financial information. 2. When the user logs in to their bank account, malware captures their credentials and then modify the transaction receipt to hide the transaction
6	**Session Hijacking**	social media accounts	1. Attacker steals a session cookie This can happen if the user's machine is infected with malware or browser hijackers. 2. Steal the data

Table 1: Comparison between MITM Attacks.

V. GOAL AND TARGETS

The goal of an attacker is to steal personal information and important data such as-

- Login credentials.
- Account details.
- Credit card numbers.

Targets of an attackers is to–

- Financial applications.
- SaaS businesses.
- E-commerce sites.
- Other websites where logging in is required and social media.
- Information obtained during an attack could be used for many purposes such as-
- Identity theft.
- Unapproved fund transfers or an illicit password change.

VI. DEFENSE MECHANISM

Man-in-the-Middle Attacks are generally prevented using cryptographic techniques.

6.1. Cryptography:

Cryptography is a method of protecting data and communications through the use of codes so that only those for whom the data is intended can read and process it.

The pre-fix "crypt" means "hidden" and the suffix "graphy" stands for "writing [15]"

Advantages-

- It hides a message and your privacy is safe.
- No one would be able to know what it says unless there's a key to the code. We can write whatever we want & however we want to keep your code a secret [15].

6.2 Penetration testing:

Penetration testing is a simulation of an attack to verify the security of a system to be analyzed. This test can be performed through physical means utilizing hardware, or through social engineering. The objective of this test is: to examine, under extreme circumstances, the behavior of systems, networks, or personnel devices, in order to identify their weaknesses and vulnerabilities. In terms of tools, there exist penetration testing tools which simply analyze a system, as well as ones which actually attack the system to find vulnerabilities.

The main objective of penetration testing is to determine the security weaknesses. A penetration test can also be used to:

- Test an organization's security policy compliance.
- Test employee security awareness
- Test an organization's ability to respond to security incidents.

- There are four typical types of penetration testing:

i. **External testing**: An external test targets a company's externally visible servers or devices, such as domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective in this case is to find out if an outside attacker can gain illegitimate access and what level of access can he get.

ii. **Internal testing:** An internal test simulates an inside attack behind the firewall by an authorized user with standard access privileges.

iii. **Blind testing**: A blind test simulates the actions and procedures of a real attacker by strictly limiting the information given to the person or team that is performing the test beforehand.

iv. **Double blind testing:** In double blind testing, it takes the blind test even further, in that only a few individuals within the organization would be aware that a test is being conducted. There are many different tools that can be used for penetration testing. Several are available on the market that one can download and use for free. Many of them are even able to be customized; known as Open Source tools there are also several penetration testing software that one can purchase. Some of them cost as little of 10 dollars for their license, and others may cost thousands of dollars.

- Examples of these tools include:

- Kali Linux – An Linux based OS containing a suite of penetration tools.
- Meta sploit – An advanced Framework used for pen testing that contains command-line and GUI interfaces.
- Wire shark – A protocol analyzer with a GUI.
- w3af – A web application attack and audit framework.
- John The Ripper – A password cracker.
- Nessus – A very robust vulnerability identifier.
- Nmap – A network mapper, as the name suggest, that aids in understanding the characteristics of any target network.
- Dradis – An open source framework that helps with maintaining the information that can be shared among the participants of a pen-test.

6.3 Penetration Test Attack Using Wireshark

Performing MITM attack as a penetration test using Ettercap and Wireshark. MITM is an attack where the attacker secretly relays and is an assault where the aggressor furtively transfers and potentially modifies the correspondence between two gatherings who trust they are specifically speaking with the point is to relate the assailant's MAC address with the IP address of another host, for Example, the default entryway, causing any traffic implied for that IP address to be sent to the assailant. Along these lines assailant will catch the parcels utilizing Wire shark and block the information that is being conveyed between the client and the site while Ettercap is being utilized for ARP harming. Wireshark is utilized to go into indiscriminate mode. Indiscriminate mode is the system interface mode in which NIC reports each packet that it observes

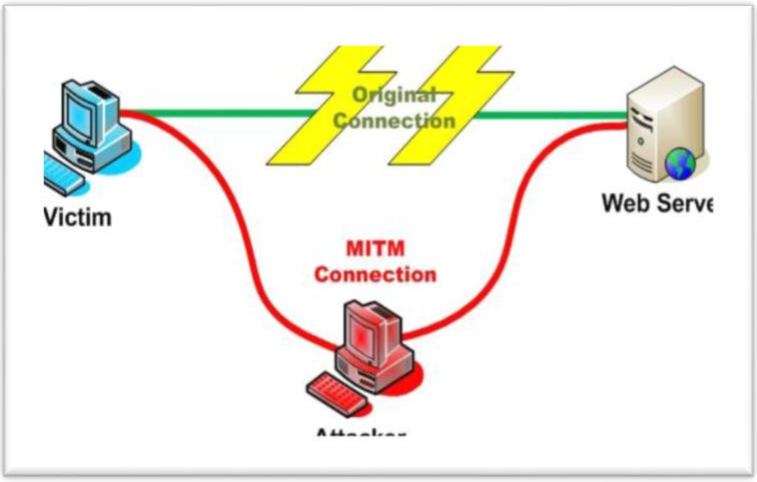


Figure 4: MITM attack model view.

- **Steps Involved In Attack**

1. First, we are using Ettercap for sniffing the packets and after opening the Ettercap we started unified sniffing.

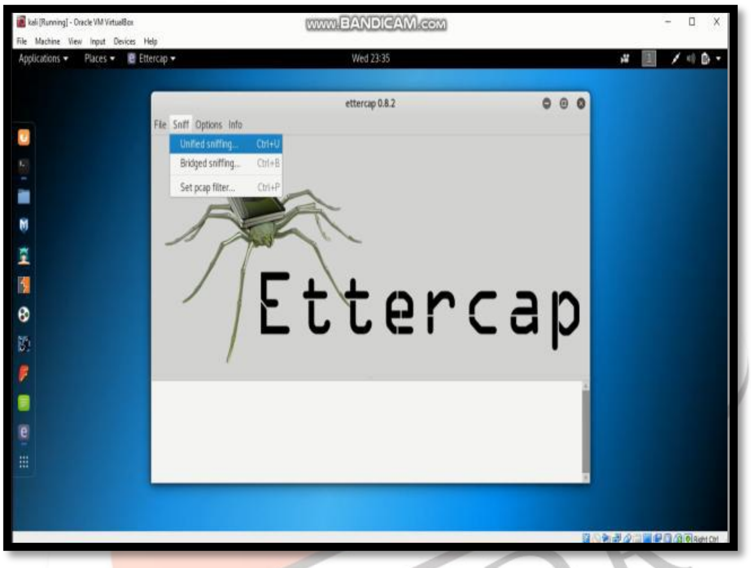
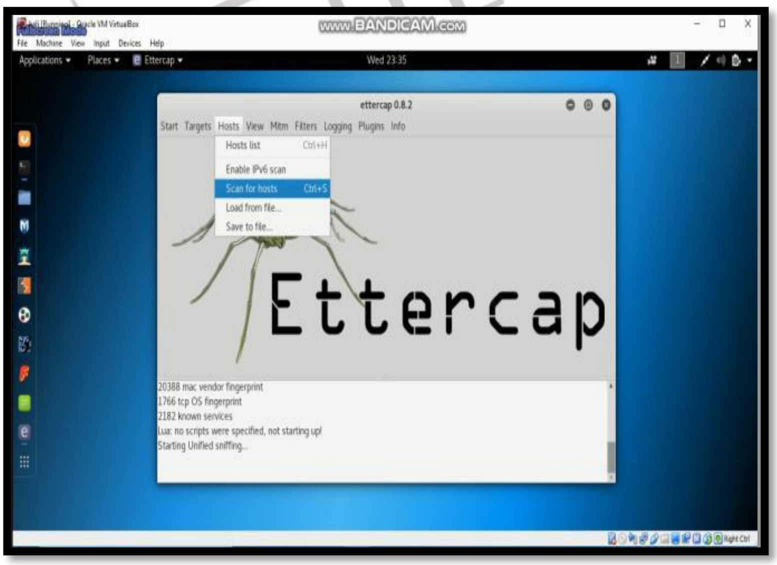

kali [Running] - Oracle VM VirtualBox
www.BANDICAM.com
File Machine View Input Devices Help
Applications ▾ Places ▾ Ettercap ▾
Wed 23:35
ettercap 0.8.2
File Sniff Options Info
Unified sniffing... Ctrl+U
Bridged sniffing... Ctrl+B
Set pcap filter... Ctrl+P
Ettercap

Figure 5: Starting unified sniffing.

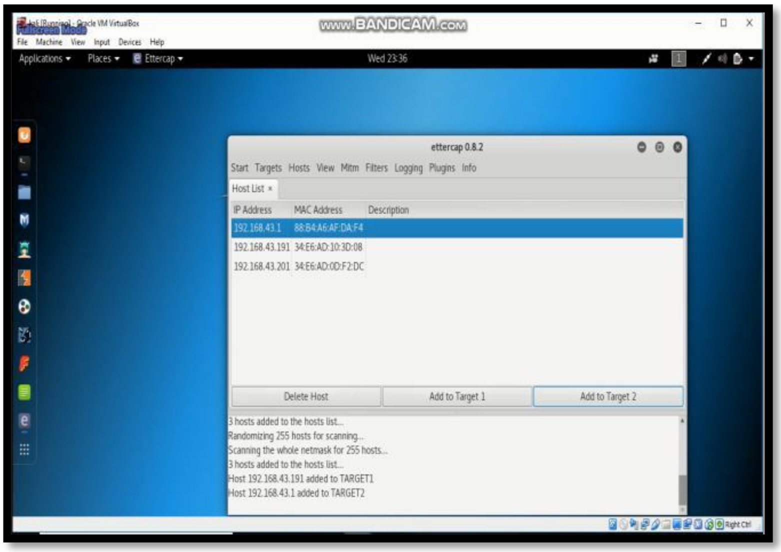
2. Next, we are scanning for hosts that are in our network in which one will be the victim and other will be the router or gateway


kali [Running] - Oracle VM VirtualBox
www.BANDICAM.com
File Machine View Input Devices Help
Applications ▾ Places ▾ Ettercap ▾
Wed 23:35
ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Hosts list Ctrl+H
Enable IPv6 scan
Scan for hosts Ctrl+S
Load from file...
Save to file...
Ettercap

```
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

Figure 6: Scanning for hosts.

3. After scanning we are adding the router’s IP to target 2 and victim’s IP to target 1.

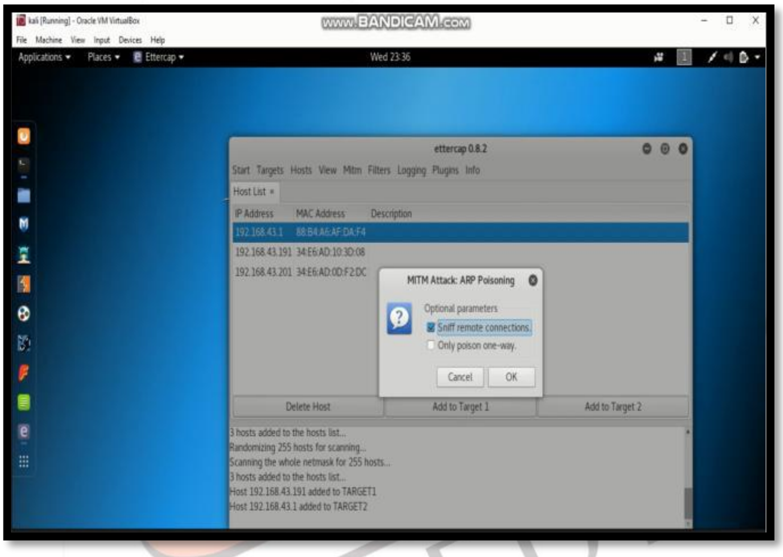


IP Address	MAC Address	Description
192.168.43.1	88:B4:A6:AF:DA:F4	
192.168.43.191	34:E6:AD:10:3D:08	
192.168.43.201	34:E6:AD:0D:F2:DC	

```
3 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Host 192.168.43.191 added to TARGET1
Host 192.168.43.1 added to TARGET2
```

Figure 7: Adding target's IP address.

4. Then we started ARP poisoning of remote connections.



IP Address	MAC Address	Description
192.168.43.1	88:B4:A6:AF:DA:F4	
192.168.43.191	34:E6:AD:10:3D:08	
192.168.43.201	34:E6:AD:0D:F2:DC	

Optional parameters

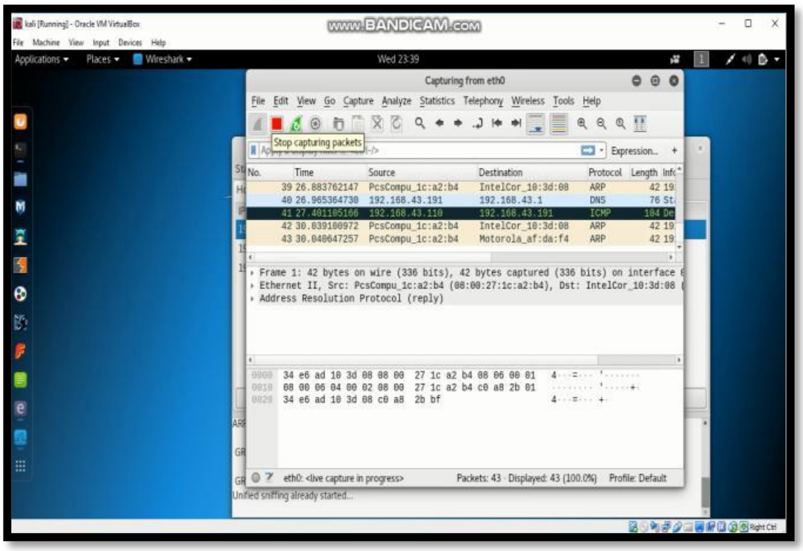
☑ Sniff remote connections.

☐ Only poison one-way.

```
3 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Host 192.168.43.191 added to TARGET1
Host 192.168.43.1 added to TARGET2
```

Figure 8: Starting ARP poisoning.

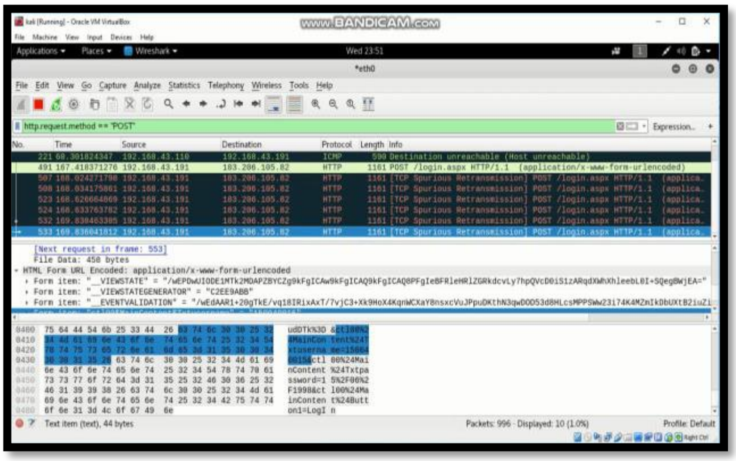
5. Now Wireshark is used for capturing packets that are being transferred between router and victim. And we can filter packets using IP address of victim



```
No.  Time             Source              Destination          Protocol  Length  Info
  39 26.883762147   PcsCompu_1c:a2:b4   IntelCor_10:3d:08    ARP          42  19
  40 26.965364738   192.168.43.191      192.168.43.1         DNS          76  St
  41 27.401105166   192.168.43.110      192.168.43.191       ICMP        104  De
  42 30.039100972   PcsCompu_1c:a2:b4   IntelCor_10:3d:08    ARP          42  19
  43 30.040647257   PcsCompu_1c:a2:b4   Motorola_af:da:f4    ARP          42  19

› Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
› Ethernet II, Src: PcsCompu_1c:a2:b4 (08:00:27:1c:a2:b4), Dst: IntelCor_10:3d:08 (
› Address Resolution Protocol (reply)

0000  34 e6 ad 10 3d 08 08 00  27 1c a2 b4 08 06 00 01   4···=··· '·······
0010  08 00 06 04 00 02 08 00  27 1c a2 b4 c0 a8 2b 01   ········ '·····+·
0020  34 e6 ad 10 3d 08 c0 a8  2b bf                     4···=··· +·

eth0: <live capture in progress>    Packets: 43 · Displayed: 43 (100.0%)    Profile: Default
Unified sniffing already started...
```

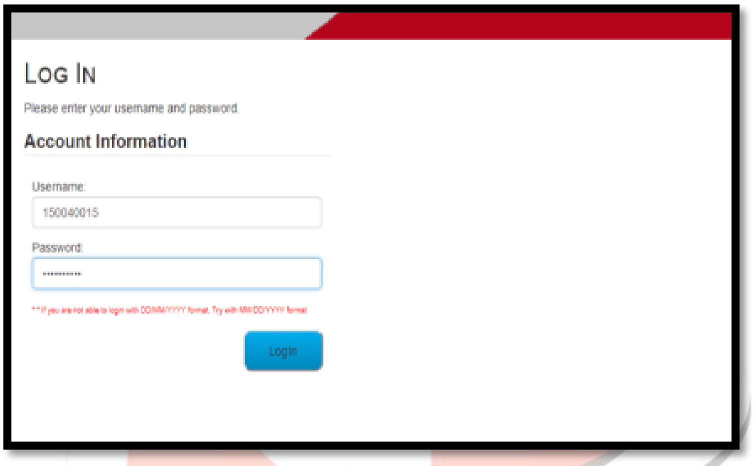
Figure 9: Capturing live packets using Wireshark.

6. And whenever victim goes to a website and login into that website those packets are captured using POST request which is used to filter and capture those packets which are sent by the user to the server by request message.


kali [Running] - Oracle VM VirtualBox
www.BANDICAM.com
File Machine View Input Devices Help
Applications ▾ Places ▾ Wireshark ▾
Wed 23:51
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…

```
http.request.method == "POST"
No.  Time             Source          Destination     Protocol Length Info
 221 68.301824347     192.168.43.110  192.168.43.191  ICMP      590 Destination unreachable (Host unreachable)
 491 167.418371276    192.168.43.191  183.206.105.82  HTTP     1161 POST /login.aspx HTTP/1.1  (application/x-www-form-urlencoded)
 507 168.024271798    192.168.43.191  183.206.105.82  HTTP     1161 [TCP Spurious Retransmission] POST /login.aspx HTTP/1.1  (applica…
 508 168.034175861    192.168.43.191  183.206.105.82  HTTP     1161 [TCP Spurious Retransmission] POST /login.aspx HTTP/1.1  (applica…
 523 168.626664869    192.168.43.191  183.206.105.82  HTTP     1161 [TCP Spurious Retransmission] POST /login.aspx HTTP/1.1  (applica…
 524 168.633763782    192.168.43.191  183.206.105.82  HTTP     1161 [TCP Spurious Retransmission] POST /login.aspx HTTP/1.1  (applica…
 532 169.830463385    192.168.43.191  183.206.105.82  HTTP     1161 [TCP Spurious Retransmission] POST /login.aspx HTTP/1.1  (applica…
 533 169.836041812    192.168.43.191  183.206.105.82  HTTP     1161 [TCP Spurious Retransmission] POST /login.aspx HTTP/1.1  (applica…

    [Next request in frame: 553]
    File Data: 458 bytes
  ▾ HTML Form URL Encoded: application/x-www-form-urlencoded
    ▸ Form item: "__VIEWSTATE" = "/wEPDwUIODE1MTk2MDAPZBYCZg9kFgICAw9kFgICAQ9kFgICAQ8PFgIeBFRleHRlZGRkdcvLy7hpQVcD0iS1zARqdXWhXhleebL0I+SQegBWjEA="
    ▸ Form item: "__VIEWSTATEGENERATOR" = "C2EE9ABB"
    ▸ Form item: "__EVENTVALIDATION" = "/wEdAAR1+20gTkE/vq18IRixAxT/7vjC3+Xk9HoX4KqnWCXaY8nsxcVuJPpuDKthN3qwDOD53d8HLcsMPPSWw23174K4MZmIkDbUXtB2iuZi

0400  75 64 44 54 6b 25 33 44  26 63 74 6c 30 30 25 32   udDTk%3D &ctl00%2
0410  34 4d 61 69 6e 43 6f 6e  74 65 6e 74 25 32 34 54   4MainCon tent%24T
0420  78 74 75 73 65 72 6e 61  6d 65 3d 31 35 30 30 34   xtuserna me=15004
0430  30 30 31 35 26 63 74 6c  30 30 25 32 34 4d 61 69   0015&ctl 00%24Mai
0440  6e 43 6f 6e 74 65 6e 74  25 32 34 54 78 74 70 61   nContent %24Txtpa
0450  73 73 77 6f 72 64 3d 31  35 25 32 46 30 36 25 32   ssword=1 5%2F06%2
0460  46 31 39 39 38 26 63 74  6c 30 30 25 32 34 4d 61   F1998&ct l00%24Ma
0470  69 6e 43 6f 6e 74 65 6e  74 25 32 34 42 75 74 74   inConten t%24Butt
0480  6f 6e 31 3d 4c 6f 67 49  6e                        on1=LogI n

Text item (text), 44 bytes                    Packets: 996 · Displayed: 10 (1.0%)        Profile: Default
```

Figure 10: Searching login packets using POST request.



Log In

Please enter your username and password.

Account Information

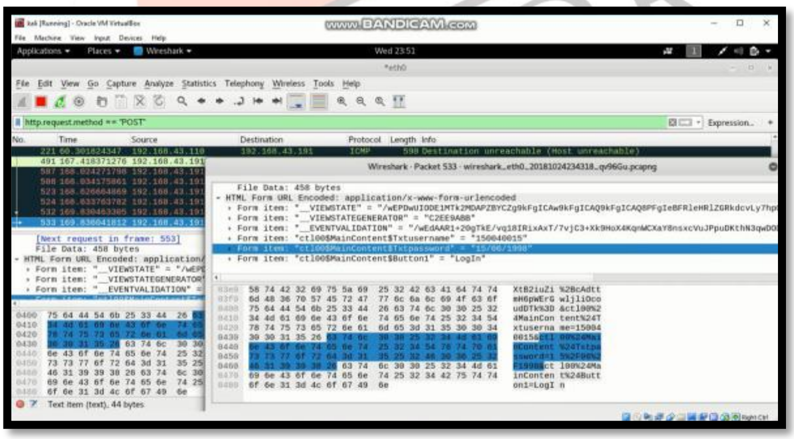
Username: 150040015

Password: ••••••••••

* * If you are not able to login with DD/MM/YYYY format. Try with MM/DD/YYYY format

Figure 11: Logging into vulnerable website.

7. After the POST request, we can see the login credentials in hexadecimal by that packet and that can be converted to plain text.


kali [Running] - Oracle VM VirtualBox
www.BANDICAM.com
File Machine View Input Devices Help
Applications ▾ Places ▾ Wireshark ▾
Wed 23:51
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
Right Ctrl

```
Wireshark · Packet 533 · wireshark_eth0_20181024234318_qv96Gu.pcapng

    File Data: 458 bytes
  ▾ HTML Form URL Encoded: application/x-www-form-urlencoded
    ▸ Form item: "__VIEWSTATE" = "/wEPDwUIODE1MTk2MDAPZBYCZg9kFgICAw9kFgICAQ9kFgICAQ8PFgIeBFRleHRlZGRkdcvLy7hp
    ▸ Form item: "__VIEWSTATEGENERATOR" = "C2EE9ABB"
    ▸ Form item: "__EVENTVALIDATION" = "/wEdAAR1+20gTkE/vq18IRixAxT/7vjC3+Xk9HoX4KqnWCXaY8nsxcVuJPpuDKthN3qwDO
    ▸ Form item: "ctl00$MainContent$Txtusername" = "150040015"
    ▸ Form item: "ctl00$MainContent$Txtpassword" = "15/06/1998"
    ▸ Form item: "ctl00$MainContent$Button1" = "LogIn"

03e0  58 74 42 32 69 75 5a 69  25 32 42 63 41 64 74 74   XtB2iuZi %2BcAdtt
03f0  6d 48 36 70 57 45 72 47  77 6c 6a 6c 69 4f 63 6f   mH6pWErG wljliOco
0400  75 64 44 54 6b 25 33 44  26 63 74 6c 30 30 25 32   udDTk%3D &ctl00%2
0410  34 4d 61 69 6e 43 6f 6e  74 65 6e 74 25 32 34 54   4MainCon tent%24T
0420  78 74 75 73 65 72 6e 61  6d 65 3d 31 35 30 30 34   xtuserna me=15004
0430  30 30 31 35 26 63 74 6c  30 30 25 32 34 4d 61 69   0015&ctl 00%24Mai
0440  6e 43 6f 6e 74 65 6e 74  25 32 34 54 78 74 70 61   nContent %24Txtpa
0450  73 73 77 6f 72 64 3d 31  35 25 32 46 30 36 25 32   ssword=1 5%2F06%2
0460  46 31 39 39 38 26 63 74  6c 30 30 25 32 34 4d 61   F1998&ct l00%24Ma
0470  69 6e 43 6f 6e 74 65 6e  74 25 32 34 42 75 74 74   inConten t%24Butt
0480  6f 6e 31 3d 4c 6f 67 49  6e                        on1=LogI n
```

Figure 12: Captured Login credentials.

- **Results and Defensive Mechanisms**

By performing this attack, we can steal the user login credentials using Wireshark tool. From this we can conclude that the website has vulnerabilities in it [16].

- **Defensive mechanisms:**

- In order to protect from the attack that we did, there are the steps that need to be followed;
- ARP Detection Software is used to verify the IP/MAC address resolution and grant them if they are authenticated and ignores unsolicited ARP reply packets.

- In this way it is useful in protecting the system from this attack. Website should be upgraded from HTTP to HTTPS because HTTP does not require any certificates.
- But HTTPS requires SSL certificates which provides security and cryptographic (encryption protocols) are present in HTTPS 3.Static ARP entries which are used to manually create the link between the MAC address and IP address. So, it should be used so device cannot be fooled by fake ARP requests [16].

VII. MAN-IN-THE-MIDDLE ATTACK PREVENTION

- Don't use Public or Free Wi-Fi connections directly a VPN encrypts your internet connection on public hotspots to protect the private data you send and receive while using public Wi-Fi (e.g., coffee shops, hotels) when conducting sensitive transactions.
- Attacker mostly uses a Wi-Fi router to intercept user's communication. This technique is compute by exploiting a router with some malicious programs to intercept user's sessions on the router. Here, the attacker initial configures his laptop computer as a Wi-Fi hotspot, choosing a name commonly used in a public area, such as an airport or coffee shop. Once a user connects to that malicious router to succeed in websites like on-line banking sites or commerce sites, the attacker then logs a user's credentials for later use [7].
- Some website are unsecured so pay the attention to the browser notifications.
- When application is not in use immediately logging out.
- To use SSL/TLS to secure every page of their site and not just the pages that require users to log in [6].
- Make sure "HTTPS" — with the S — is always in the URL bar of the websites you visit.
- Be wary of potential phishing emails from attackers asking you to update your password or any other login credentials [7]. Instead of clicking on the link provided within the email, manually kind the web site address into your browser.
- Always Install internet security solution on your computer such as Norton Security and keep the security software up to date.
- Be sure that your home Wi-Fi network is secure and use the (strong) unique passwords and usernames on your home router.
- Connected with world, it's important to understand the types of threats that could compromise the online security of your personal information. Stay informed and make sure your devices are proper secure.

VIII. CONCLUSION

The man-in-the-middle attack is very dangerous. People can easily fall to such malicious attacks it breaks the user's confidence because the user feels he / she communicates with the intended recipient over a secured network. The attacker may steal and misuse private information for personal gain. The purpose of this paper is to create a sense of awareness among the general public who are not well educated about security attacks and how they can easily fall prey unknowingly to such malicious attacks.

IX. ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to my guide and HOD of Computer Department "Dr. Deepak Sharma" sir for their able guidance and support in completing my project and for providing me with all the facility that was required. I would also like to extend my gratitude to the Principal Mam "Dr. Shubha Pandit".

REFERENCES

[1] Conti, Mauro, Nicola Dragoni, and Viktor Lesyk. "A survey of man in the middle attacks." IEEE Communications Surveys & Tutorials 18.3 (2016): 2027-2051.

[2] Denis, Matthew, Carlos Zena, and Thaier Hayajneh. "Penetration testing: Concepts, attack methods, and defense strategies." 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). IEEE, 2016.

[3] Wasil, Dean, et al. "Exposing vulnerabilities in mobile networks: A mobile data consumption attack." 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS). IEEE, 2017.

[4] Daş, Resul, Abubakar Karabade, and Gurkan Tuna. "Common network attack types and defense mechanisms." 2015 23nd Signal Processing and Communications Applications Conference (SIU). IEEE, 2015.

[5] https://www.veracode.com/security/man-middle-attack.

[6] https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/.

[7] https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html.

[8] https://www.globalsign.com/en-in/blog/what-is-a-man-in-the-middle-attack/

[9] https://www.thewindowsclub.com/man-in-the-middle-attack.

[10] S. M. Bellovin and M. Merritt, "Encrypted key exchange: Password based protocols secure against dictionary attacks," in Proc. IEEE Computer. Soc. Symp. Res. Secur. Privacy, 1992, pp. 72–84.

[11] R. Demillo and M. Merritt, "Protocols for data security," Computer, vol. 2, no. 16, pp. 39–51, 1983.

[12] W. Baker et al., "Data breach investigations report," Methodology, vol. 36, pp. 1–63, 2011.

[13] CAPEC. (2014). Capec-94: Man in the Middle Attack [Online].Available: http://capec.mitre.org/data/definitions/94.html.

[14] S. Frankel, B. Eydt, L. Owens, and K. Scarfone, "Establishing wireless robust security networks: A guide to IEEE 802.11i," National Institute of Standards and Technology, Gaithersburg, Maryland, USA, Report no.1 NIST SP 800-97, 2007.

[15] 27th January 2020,https://searchsecurity.techtarget.com/definition/cryptography.

[16] Sahiti, Prasanth. Tilakchand, Balu. Kowshik, Pokala. Avinash, Simhadri Leela Kavya "Penetration Testing Using Wireshark and Defensive Mechanisms against MITM" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277 3878, Volume-7, Issue-6, March 2019.

[17] https://www.slideshare.net/CROCOCHOCOBARROSHAN/overview-of-cryptography-41884171.

[18] https://www.streetdirectory.com/travel_guide/156642/security/benefits_of_norton_security_software_for_your_computer.html.