



Security In Computing (CC5004NI)

Course Work 1

TOPIC CHOSEN: CRYPTOGRAPHIC VULNERABILITIES

Submitted By: Manish Giri
Student ID Number: 16034959

Submitted To: Lecturer: Akchyat Bikram Joshi
Submission Date: 14/8/2018

ACKNOWLEDGEMENT

The success and final outcome of this project required a lot of guidance and assistance from many people and I am extremely privileged to have got this all along the completion of my project. All that I have done is only due to such supervision and assistance and I would not forget to thank them.

I respect and thank to **Mr. Akchyat Bikram Joshi** , for providing me an opportunity to do the project work in and giving us all support and guidance which made me complete the project duly. I am extremely thankful to him for providing such a nice support and guidance, although he had busy schedule managing the college affairs.

ABSTRACT

The fundamental subject of this coursework is to show about the man-in-the-middle attack in detail. It depicts the issue, its motivation, dangers, Vulnerabilities and effects. The attack scenario and Problem situation has been investigated alongside its points and destinations. A basic man-in-the-middle attack situation has been performed and the result has been screenshot and clarified

This project won't have been completed without the help of various research papers, journals, websites and EBooks. Therefore they are taken as the references.

TABLE OF CONTENTS

Acknowledgement	2
Abstract	2
List of figures	4
Introduction	5
Attack Scenario	6
MITM attack progression	6
Interception	6
Decryption	6
Problem Scenario	7
Background	8
Pre-requirements and Tools	8
Requirements	8
Tools used on Kali LINUX	8
STEPS INVOLVED	8
Demonstration	9
1)USING ETTERCAP	9
2)USING Driftnet	12
3)USING URLSNARF	14
4)USING Wireshark	15
5)USING SSISTRip	17
Prevention and Recommendations:	19
Analysis of the Prevenntion methodology	19
Enhanced ARP: preventing ARP poisoning-based man-in-the-middle attacks	19
Summary:.....	Error! Bookmark not defined.
Analysis	19

Recommendation	20
Conclusion	20
References	21
Appendices	22

LIST OF FIGURES

Figure 1 MITM INTRO	5
Figure 2 Revelations	7
Figure 3 IP TABLE	9
Figure 4 USING ETTERCAP	9
Figure 5 Using ETTERCAP	10
Figure 6 ARP Poisoning	10
Figure 7 ARP poisoning	10
Figure 8 ARP poisoning	11
Figure 9 Victims of ARP poisoning	11
Figure 10 Start sniffing.....	11
Figure 11 Using Driftnet.....	12
Figure 12 Driftnet Victim PC	12
Figure 13 Driftnet Window	13
Figure 14 Saving Images captured by Driftnet.....	13
Figure 15 Using URL Snarf.....	14
Figure 16 URL Snarfing.....	14
Figure 17 Wireshark.....	15
Figure 18 SSLSTRIP terminal	17
Figure 19 SSLSTRIP in action	18
Figure 20 SSLSTRIPPED Website	18
Figure 21 Prevention Table.....	19

MAN IN THE MIDDLE ATTACK

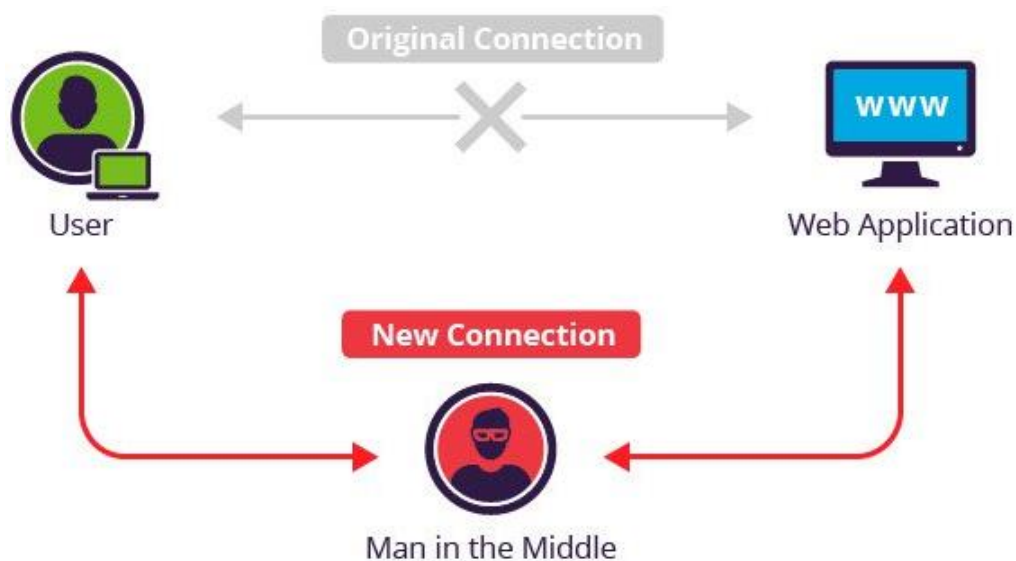


Figure 1 MITM INTRO

INTRODUCTION

A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.

The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications, SaaS businesses, e-commerce sites and other websites where logging in is required.

Information obtained during an attack could be used for many purposes, including identity theft, unapproved fund transfers or an illicit password change.

Additionally, it can be used to gain a foothold inside a secured perimeter during the infiltration stage of an advanced persistent threat (APT) assault.. (INCAPSULA, n.d.)

ATTACK SCENARIO

MITM ATTACK PROGRESSION

Effective MITM execution has two particular stages: Interception and Decryption.

INTERCEPTION

The first step intercepts user traffic through the attacker's network before it reaches its intended destination.

Attackers wishing to take a more active approach to interception may launch one of the following attacks:

- IP spoofing involves an attacker disguising himself as an application by altering packet headers in an IP address. As a result, users attempting to access a URL connected to the application are sent to the attacker's website.
- DNS spoofing, also known as DNS cache poisoning, involves infiltrating a DNS server and altering a website's address record. As a result, users attempting to access the site are sent by the altered DNS record to the attacker's site. (INCAPSULA, n.d.)

DECRYPTION

After interception, any two-way SSL traffic needs to be decrypted without alerting the user or application. A number of methods exist to achieve this:

- HTTPS spoofing sends a phony certificate to the victim's browser once the initial connection request to a secure site is made. It holds a digital thumbprint associated with the compromised application, which the browser verifies according to an existing list of trusted sites. The attacker is then able to access any data entered by the victim before it's passed to the application.
- SSL stripping downgrades a HTTPS connection to HTTP by intercepting the TLS authentication sent from the application to the user. The attacker sends an unencrypted version of the application's site to the user while maintaining the secured session with the application. Meanwhile, the user's entire session is visible to the attacker. (INCAPSULA, n.d.)

PROBLEM SCENARIO

Today's security systems in particular, in order to save pre-computing there is a trend for sensor networks to design a sensor-group-leader rather than every sensor node communicates to the end database, which indicated the needs to prevent from the man-in-the middle attacking. (Huang, 2010)

Attempting to establish a secure session , your browser makes up a random private key , generates its corresponding public key and attempts to send that public key to the server. The man-in-the-middle stops that communication from arriving, and stashes that public key for later use. The MITM makes up its own random private key , generates its corresponding public key , and sends that public key to the server, making it appear that it came from your browser.

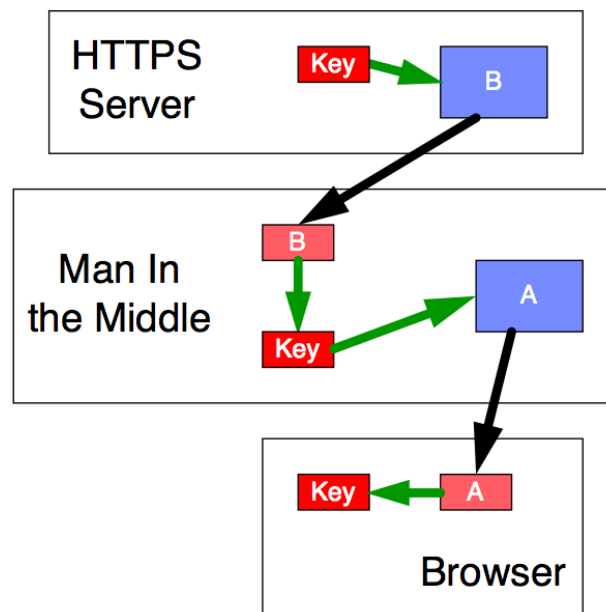


Figure 2 Revelations

Then the server creates a random session key , encrypts it with the public key it thinks it got from your browser. It attempts to send that to your browser, but the MITM intercepts. The MITM decrypts with its private key , revealing the session key. It then re-encrypts that session key with the public key that it held onto from earlier, and sends it to your browser as if it came from the server. Your browser decrypts it with its private key , and thinks all is well.

But the MITM has the same session key , and can now decrypt all communications throughout the entire “secure” session. (Finley, 2011)

BACKGROUND

PRE-REQUIREMENTS AND TOOLS

REQUIREMENTS

This attack requires us to know to how to work with basic Kali Linux and the command line.

- **Kali Linux:** Its a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.

TOOLS USED ON KALI LINUX

Kali Linux is an operating system developed by linux which includes all the penetration testing application in one single package

Applications required that are included in Kali Linux

- **ETTERCAP**
- **DRIFTNET**
- **SSLSTRIP**
- **URLSNARF**
- **WIRESHARK**

STEPS INVOLVED

Step 1: First we are going to use ETTERCAP which basically sniffs the live connection and traffic while filtering the content. It basically works like an ARP spoof.

Step 2: Now since the victim host is being sniffed we use DRIFTNET which basically captures pictures which are being seen in the PC's

Step 3: Using SSLSTRIP makes any secured website that the victim uses unsecure as it basically strips of the S in HTTP(S) by providing identical but fake certificates

Step 4: Using URLSNARF we can keep track of all the URL's that are being visited by the victim host

Step 5: Using WIRESHARK we can sniff login credentials and other interesting information that passes through unencrypted. (Fernandez, 2016)

DEMONSTRATION

The current scenario is as follows PC1 PC2 and PC 3 are all connected via a wireless network.

PC 1 has IP address **10.106.130.152**. **PC 2** has IP address **10.106.130.50** and **PC 3** has IP address **10.106.130.148** and we will be conducting various Man-in-the-middle-Attacks from PC 2 on victim PC 3 using the network provided by the **router** which has IP address **10.106.130.1**

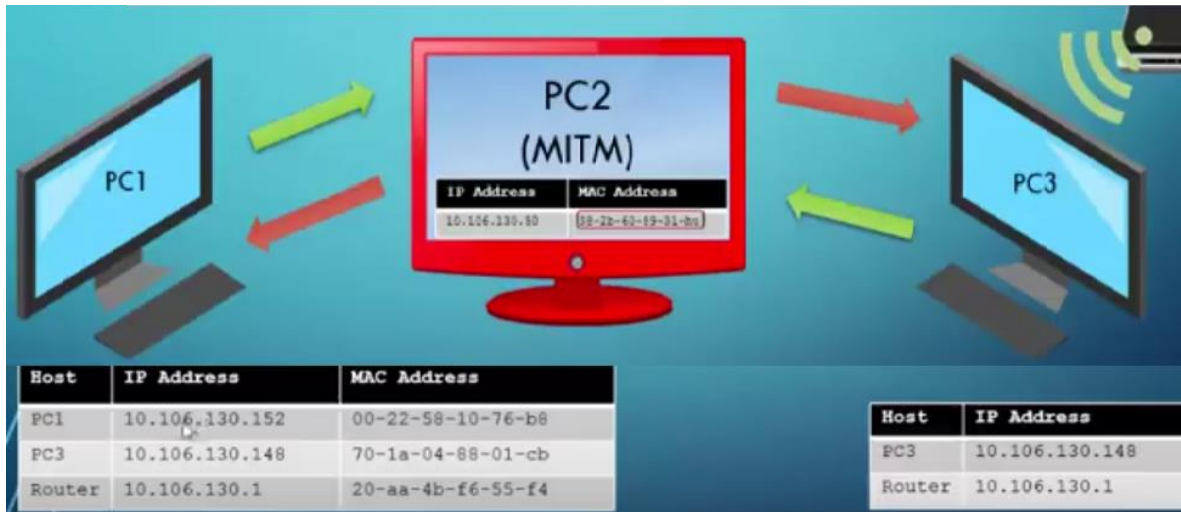


Figure 3 IP TABLE

1) USING ETTERCAP

We first have to launch the **ETTERCAP** and we will be using **Unified Sniffing** from the **Sniff** menu



Figure 4 USING ETTERCAP

Then we are gonna scan for the victim host so we will be clicking the **HOSTS** menu and then **SCAN FOR HOSTS**



Figure 5 Using ETTERCAP

Then we will get the host list from which we are going to select the victim host and in this scenario **10.106.130.5** is the IP that we are going to use as our router which we will add as our target 1 by clicking the button **Add to Target 1**. The victims host IP address in the scenario is **10.106.130.148** which we will add as target by clicking the button **Add to Target 2**

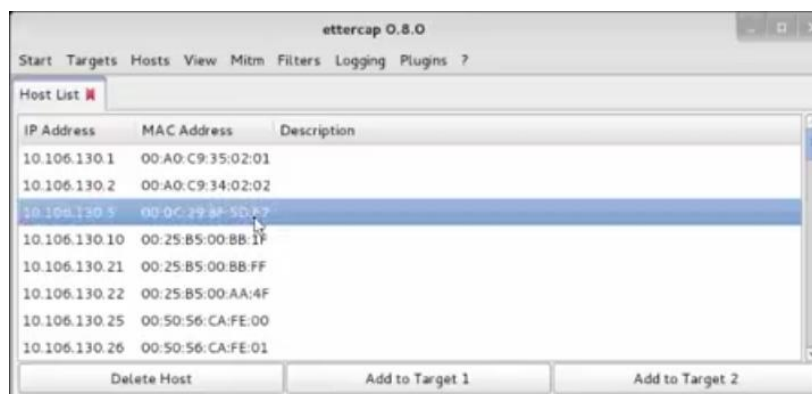


Figure 6 ARP Poisoning

Then we are going to click on **MITM** menu and the click on **ARP Poisoning**

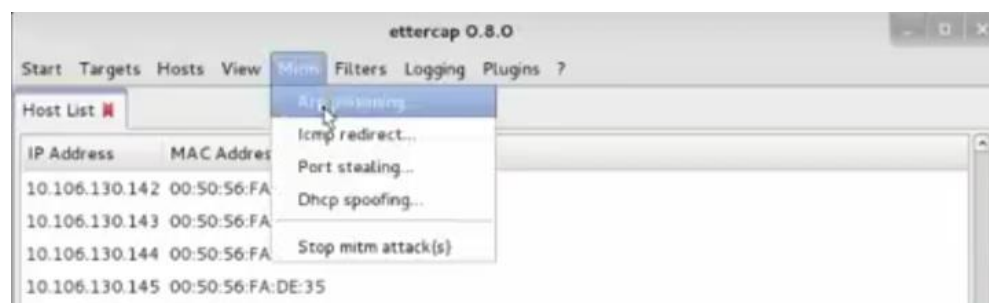


Figure 7 ARP poisoning

Then we are going to click on **Sniff Remote Connections** and then click **OK**

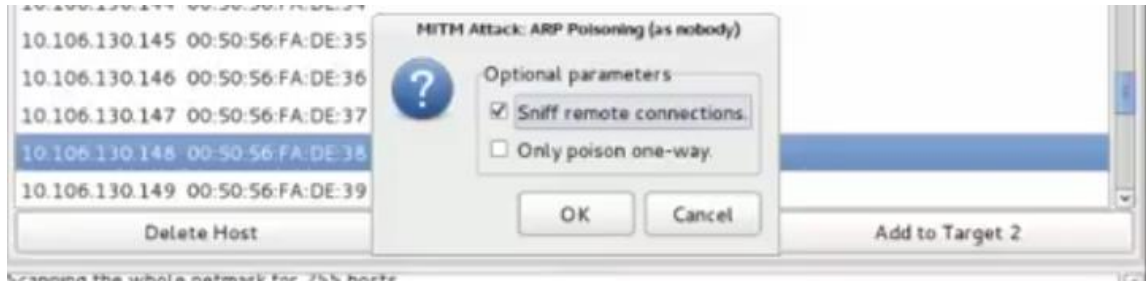


Figure 8 ARP poisoning

It will then show the victims of our Sniffing process which are our required **IPS**



Figure 9 Victims of ARP poisoning

Then we click on **START** and then on **START SNIFFING**

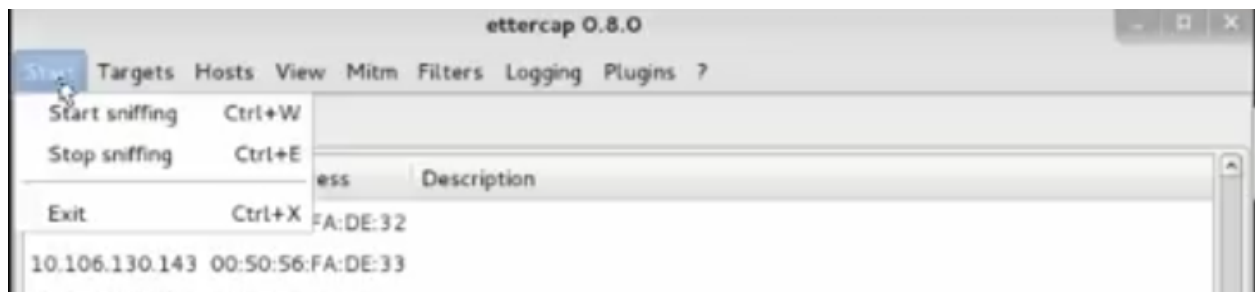


Figure 10 Start sniffing

2) USING DRIFTNET

By using driftnet we can sniff out all the pictures and the data that our sniffing victim host is currently viewing. First we open driftnet from the Kali terminal.

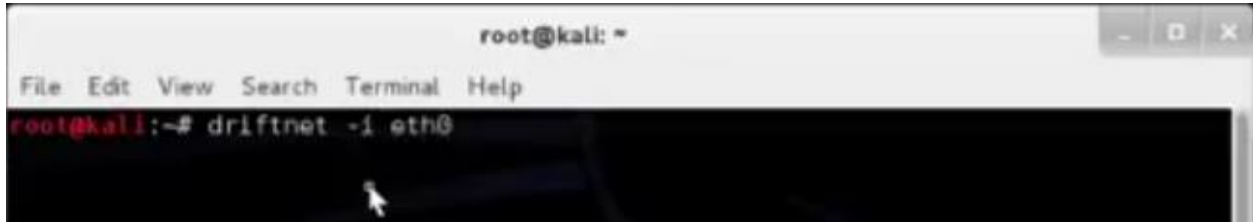


Figure 11 Using Driftnet

A small black window will pop up in the Linux.

Now if the victim host is viewing an example URL such as below



Figure 12 Driftnet Victim PC

Now if we go back and watch our small drift net window we can see all the images that the victim viewed on his machine



Figure 13 Driftnet Window

Now the MITM attacker can save not only view but save all the images by using driftnet by typing a simple command shown below. So now the images viewed by the victim is saved to the attacker's PC.



Figure 14 Saving Images captured by Driftnet

3) USING URLSNARF

We will open the application URLSNARF from the Kali Linux terminal by typing the code shown as below.

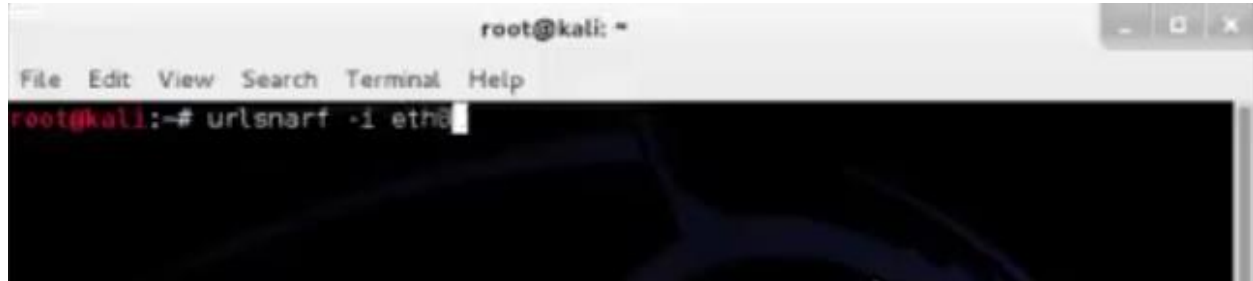


Figure 15 Using URL Snarf

The application will automatically start to listen on the IPs that were being sniffed by the ETTERCAP and the if the victim surfs the internet and browse different sites then a successful URLSNARF listening will show all the different URLs that the victim visited.



Figure 16 URL Snarfing

4) USING WIRESHARK

Using another tool which is known as wire shark.

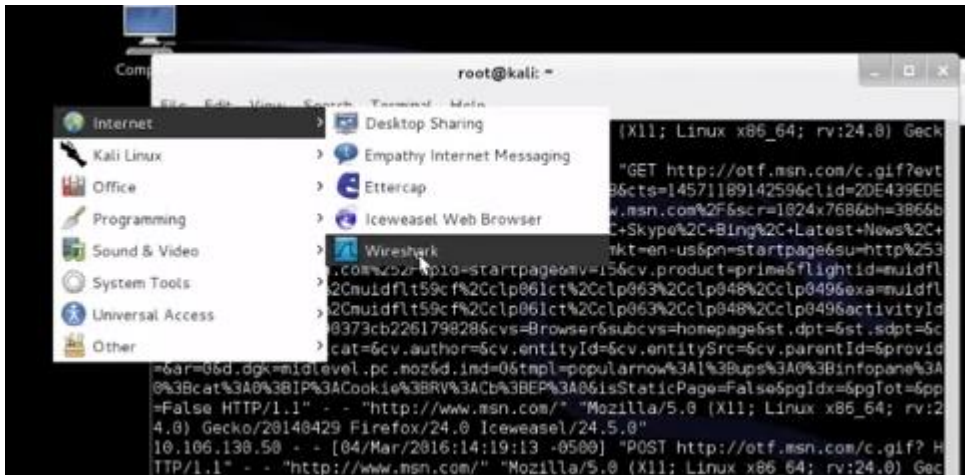
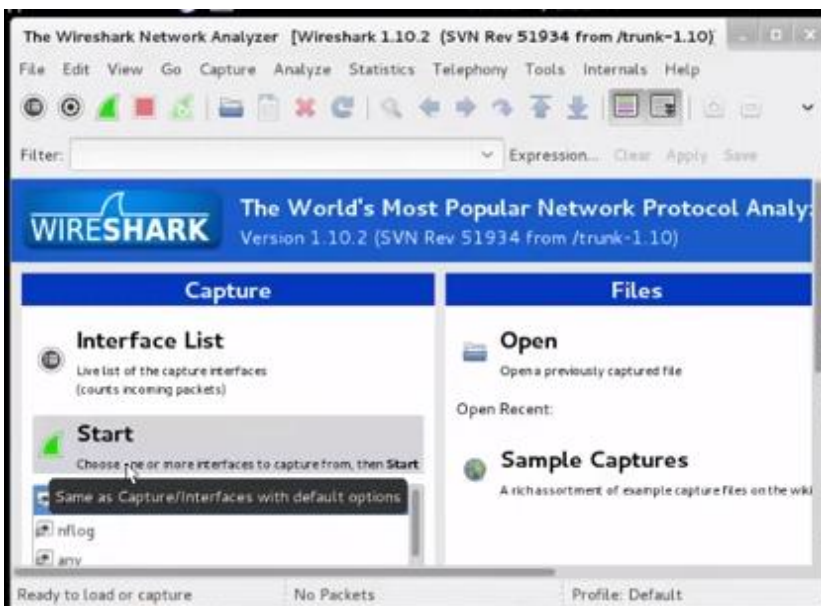




Figure 17 Wireshark



By doing this we have to select it in the interface. Basically what this does is that it will capture every packets going to that interface.

After that go to testfire.net which is a test site and log in there but as we are not already log in there it won't give access to log in there.

 ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
PERSONAL <ul style="list-style-type: none"> • Deposit Product • Checking • Loan Products • Cards • Investments & Insurance • Other Services SMALL BUSINESS <ul style="list-style-type: none"> • Deposit Products • Lending Services • Cards • Insurance • Retirement • Other Services INSIDE ALTORO MUTUAL <ul style="list-style-type: none"> • About Us • Contact Us 	<h2>Online Banking Login</h2> <p>Username: <input type="text" value="carlos"/></p> <p>Password: <input type="password" value="*****"/></p> <p><input type="button" value="Login"/></p>		

 ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
PERSONAL <ul style="list-style-type: none"> • Deposit Product • Checking • Loan Products • Cards • Investments & Insurance • Other Services SMALL BUSINESS <ul style="list-style-type: none"> • Deposit Products • Lending Services • Cards • Insurance • Retirement • Other Services INSIDE ALTORO MUTUAL <ul style="list-style-type: none"> • About Us • Contact Us 	<h2>Online Banking Login</h2> <p>Login Failed: We're sorry, but this username was not found in our system. Please try again.</p> <p>Username: <input type="text" value="carlos"/></p> <p>Password: <input type="password"/></p> <p><input type="button" value="Login"/></p>		

But if we go back to our kali machine and type http in the filter section it will show the user id and password that previously entered.

User = carlos

Password = hackingisthebest



Hence, with the help of wireshark tools all the packets within the interface is captured. Within the second we can get the username and password of the victim machine as shown in the figure above.

5) USING SSLSTRIP

Before starting the SSLSTRIP following command line is to be entered in the terminal which will redirect the destination port of the victim to the SSLSTRIP port which is 6666. This will strip the secured HTTPS and make the website vulnerable.

```
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 6666
root@kali:~# iptables --list -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination
REDIRECT   tcp  --  anywhere               anywhere            tcp dpt:http redirect
ports 6666
REDIRECT   tcp  --  anywhere               anywhere            tcp dpt:http redirect
ports 6666
REDIRECT   tcp  --  anywhere               anywhere            tcp dpt:http redirect
ports 6666
REDIRECT   tcp  --  anywhere               anywhere            tcp dpt:http redirect
ports 6666
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
```

Figure 18 SSLSTRIP terminal

Now by typing `sslstrip -l 6666` in the terminal we start our SSLSTRIP process which will be as follows.:

```
root@kali:~# sslstrip -l 6666
Traceback (most recent call last):
  File "/usr/bin/sslstrip", line 108, in <module>
    main(sys.argv[1:])
  File "/usr/bin/sslstrip", line 101, in main
    reactor.listenTCP(int(listenPort), strippingFactory)
  File "/usr/lib/python2.7/dist-packages/twisted/internet/posixbase.py", line 43
6, in listenTCP
    p.startListening()
  File "/usr/lib/python2.7/dist-packages/twisted/internet/tcp.py", line 641, in
startListening
    raise CannotListenError, (self.interface, self.port, la)
```

Figure 19 SSLSTRIP in action

Now if the victim goes to a website for example such as facebook.com then a warning box will popup which says that the certificate of the websites might be fake but will run as normal website.

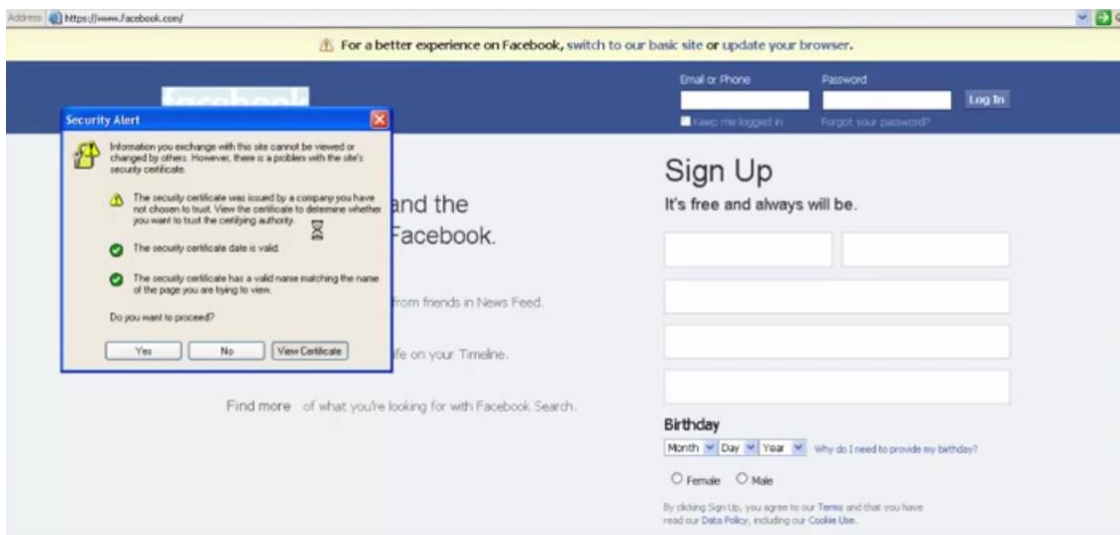


Figure 20 SSLSTRIPPED Website

PREVENTION AND RECOMMENDATIONS:

Most of the effective defenses against MITM can be found only on router or server-side. We can use a strong encryption between the client and the server.

There are some cases where Man In the Middle attacks are prevented which were published on research papers that I found in IEEE.

ANALYSIS OF THE PREVENTION METHODOLOGY

ENHANCED ARP: PREVENTING ARP POISONING-BASED MAN-IN-THE-MIDDLE ATTACKS ANALYSIS

According to the research paper In order to prevent MITM attacks even for a new IP address, a voting-based resolution mechanism is proposed. The proposed scheme is backward compatible with existing ARP and incrementally deployable. (Seung Yeob Nam, 2010). Several DoS attack patterns were used, and the lowest response probability was obtained from smurf attack because more machines have been involved in the attack than for other DoS attack types. In this case, if the victim sends a voting request for its own IP address under the assumption that there are a sufficient number of MR-ARP-enabled nodes, then the victim can easily know whether its own IP address is used by another machine based on the voting results and avoid MITM attack by stopping the use of the intercepted IP address. (Seung Yeob Nam, 2010)

# of ARP requests	1	5	10	15	20	25
response prob. (%)	24.7	68.4	92.2	97.6	99.6	100

Figure 21 Prevention Table

They next evaluated the voting-based resolution mechanism in a test-bed where six MR-ARP-enabled machines, are interconnected by a Gigabit Ethernet switch. They implemented the proposed MR-ARP mechanism by modifying the ARP module code. False decision is made when the aggregate number of votes from the adversaries exceeds. They found that the votes from different nodes are arriving in an approximately round-robin manner. Because of a rather deterministic pattern of voting outcomes, the false decision ratios are measured to be nearly zero when the MR-ARP-enabled nodes outnumber the adversary nodes. (Seung Yeob Nam, 2010)

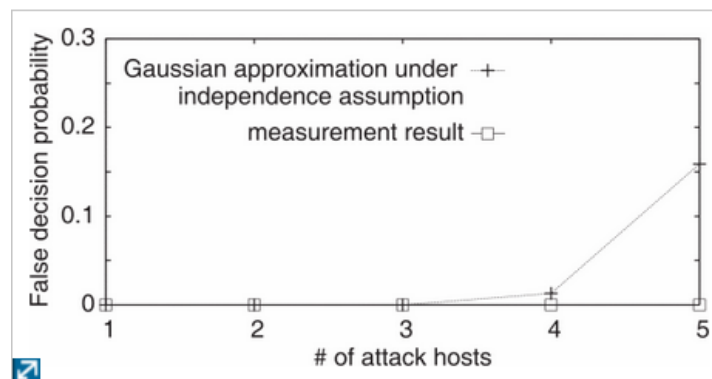


Figure 22 Voting based resolution Mechanism

RECOMMENDATION

As for recommendation, the Man-In-the-Middle attack is one of the dangerous threats which have many less countermeasures so what should we do to prevent our networks is by encrypting. Most of the effective defenses against MITM can be found only on router or server-side. You won't be having any dedicated control over the security of your transaction. Instead, you can use a strong encryption between the client and the server. In this case server authenticates client's request by presenting a digital certificate, and then only connection could be established. Another method to prevent such MITM attacks is, to never connect to open Wi-Fi routers directly.

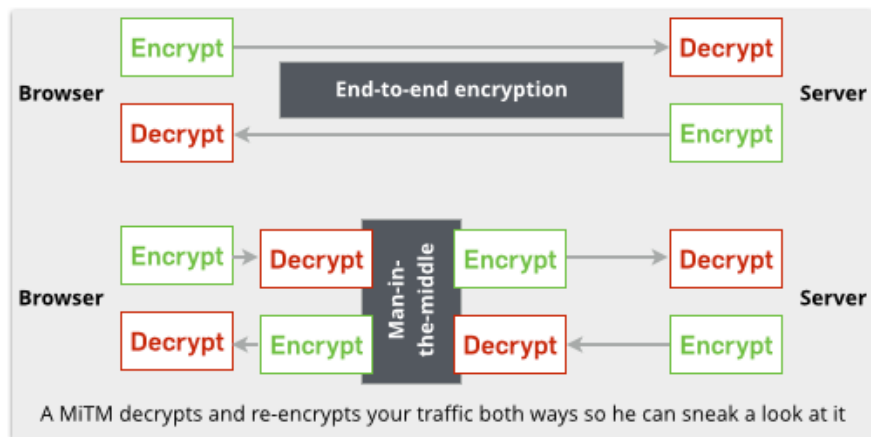
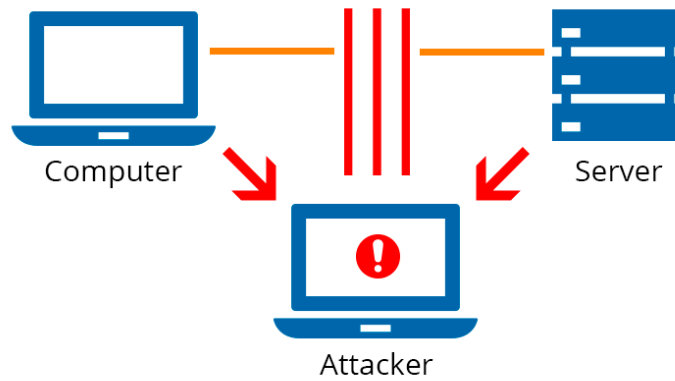
CONCLUSION

According the report the Man-in-the-Middle attack is a huge threat with much vulnerability which is difficult to deal. It can access the network and victims within the network by running some of the command and sniff the data that is transferring in network through victims and default gateway.

Since we cannot eliminate the MIM attack completely we can try to minimize the possibilities of this attack onto the network. Some of these security measures include host hardening i.e. operating systems onto the network should be upgraded, network designing from security point of view, network devices and the computers onto the network should be updated periodically and the patches should be installed regularly.

REFERENCES

- Anon., 2017. *cisco*. [Online] Available at: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11_603839.html.
- Anon., 2017. *keycdn*. [Online] Available at: <https://www.keycdn.com/support/dns-spoofing/>.
- Anon., 2017. *Networks*. [Online] Available at: <http://www.valencynetworks.com/articles/cyber-attacks-explained-man-in-the-middle-attack.html>.
- Cisco, 2017. *ARP Poisoning Attack and Mitigation Techniques - Cisco*. [Online] Available at: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11_603839.html.
- club, 2017. *club*. [Online] Available at: <http://www.thewindowsclub.com/man-in-the-middle-attack>.
- Fernandez, C., 2016. *Youtube channel*. [Online] Available at: <https://www.youtube.com/watch?v=bEMwES6TQUw>.
- Finley, D.R., 2011. *http://alienryderflex.com*. [Online] Available at: http://alienryderflex.com/man_in_the_middle/.
- Huang, X., 2010. *IEEE*. [Online] Available at: <http://0-ieeeexplore.ieee.org.emu.londonmet.ac.uk/xpls/icp.jsp?arnumber=5635945>.
- INCAPSULA, n.d. *www.incapsula.com*. [Online] Available at: <https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html>.
- Khanse, A., 2016. *TheWindowsClub*. [Online] Available at: <http://www.thewindowsclub.com/man-in-the-middle-attack>.
- MICE, M.&., 2017. *DNS Spoofing | Men & Mice*. [Online] Available at: <https://www.menandmice.com/resources/dns-spoofing/>.
- Networks, V., 2017. *Article : Cyber Attacks Explained: Man In The Middle : Ethical Hacking, Pen Test Pune, India - Valency Networks*. [Online] Available at: <http://www.valencynetworks.com/articles/cyber-attacks-explained-man-in-the-middle-attack.html>.
- Seung Yeob Nam, D.K.J.K., 2010. *IEEE Communications Letters*. [Online] Available at: <http://0-ieeeexplore.ieee.org.emu.londonmet.ac.uk/document/5403629/>.
- Technologies, C., 2017. *Ca Technologies*. [Online] Available at: <https://www.veracode.com/security/man-middle-attack>.



Man in the Middle attacks

Covering

- 1 DHCP based attacks
- 2 ARP cache poisoning
- 3 DNS based attacks
- 4 DNS based attacks
- 5 Man in the browser against internet banking
- 6 The man on the side attacks (the NSA and others)
- 7 Human-assisted phishing attacks

