International Journal of Research in Advent Technology, Vol.3, No.12, December 2015
E-ISSN: 2321-9637
Available online at www.ijrat.org

Hacking Target Machine Using Social Engineering and SSH

Nirav Shah[1] ,Vinit Patel[2]
B.E Computer Engineering[1,2]
Rajiv Gandhi Institute of Technology[1,2]
nrvshah10@gmail.com[1],patelvinit128@gmail.com[2]
Mumbai, India.

Abstract - Hacking is the word that shakes everyone whenever it is said or heard by someone at any time anywhere. Everyone born in this world with attitude wants to be a Hacker at some point of time. A Hacker needs a brilliant mind to hack anything. His skills should be so powerful that he can't get caught and at same time his need get satisfied, need can be anything like money, getting valuable information, etc of organization. Nowadays Hacking has been one of the common practices made by the computer expert in order to try and find vulnerabilities in a network infrastructure. In this paper we have shown how to hack into server or target machine with simple steps using SSH protocol.

Keywords: Hacking, Vulnerabilities, SSH Protocol, nmap, hydra tool

1. INTRODUCTION

What comes to mind when you hear the word 'hacker'? For most it means stealing information through the Internet, gaining illegal access to another person's PC, or simply - disruptive behaviour using a computer.

The state of security on the Internet is bad and becoming worse. The subject of hacking is no secret to the general public. Many people have been exposed to it by a bad experience or through the news and media. The idea of hacking that is stuck in the minds of people is that of which they have seen in the movies. The movies portray hackers as young and devious criminals. However, in reality these individuals are talented people who use their abilities to find new and challenging ways to change how computers work. The meaning of Hacker is one who accesses a computer which is he is not supposed to access and maybe he belongs non-authorised people of the community. Different Ethical Views on Computer Hacking by different people can help us to understand computer hacking process [1].

Now let's define hacking in simple language, hacking a process which allows you to enter into system which he/she not allowed and not getting caught. There are three different types of Hacking i.e. White Hat Hacking, Grey Hat Hacking and Black Hat hacking [2]. White Hat Hacking is the practice made by the hackers to dominant the world by their criminal skills. It is used in the profit making purpose. Similarly other type of hacking is Grey Hat Hacking in which he or she is submerged in the world of hacking for non-profitable purpose and also want to prove themselves that they can dominant the world by their criminal skills. For example if he or she is intended to enter into other computers and able to extract important data without causing harm to the victim can be term as he or she is Grey Hat Hackers. Grey Hat Hackers can also be known as ethical hackers that they can be both helpful and harmful as it is the combination of both White & Black Hat Hacking. In addition to that if the Grey Hat Hackers crosses their boundaries then there is no chance to become Black Hat Hackers. Similarly last and most high demanding types of hacking known as Black Hat Hacking is describe in this paper. It is also known as cracker or dark side hacker. In this types of hacking he or she is fully involve in profit making activities by destroying organization network, stealing others valuable data ,documents, hacking bank account and transferring money to their own and so on.

Don't take the advice of the people who give simple steps as if you are not careful enough you can get caught and for doing it in the perfect way you need to master the art, know the risks and learn to avoid it.

If the hacker is experienced and smart, the hacker will use telnet to access a shell on another machine so that the risk of getting caught is lower than doing it using their own system. We have also used SSH for hacking purpose. SSH [3] is a protocol for authenticating and encrypting remote shell sessions. But, using SSH for just remote shell sessions ignores 90% of what it can do. It is one of protocol like ftp which can be used to connect two machines. It is a long process, but there is a shortcut you can use and that's termed as social engineering which can help u to hack system very early.

Social engineering is a non-technical procedure of intrusion hacker's use that is based on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter. Example a employer can break security for personal reason Social engineering [4] can also be thought as art of manipulating people so they give up confidential information also it is an art guessing things which can so common but its confidential .Example People keep their name as username and password 123456.So this details are confidential but by observing and guessing the details we can damage or do bad things.

2. WORKING

OK, now I am going to give you the exact steps. Hacking is not easy, but it can be done with sufficient knowledge and understanding.

We will provide snapshots so you can understand steps in easy way.

Before you start you need to have patience and time to learn the art and properly do it.

This steps which we will tell you is only applicable to CentOs (Linux) which is running on target or victim's machine. The operating system we are using is Kali Linux. It is basically a penetration tool used for Hacking purpose only.

Steps :

1. The victim i.e. target computer should be in the same network or a LAN.
2. Identify the victim's ip address.
3. In order to do that, scan the ip address of the victim pc using Nmap tool. Nmap is short for Network Mapper. It is an open source security tool for network exploration, security scanning and auditing. However, nmap command comes with lots of options that can make the utility more robust and difficult to follow for new users [5].
4. Command to do that is nmap –A victim's_ip_address
5. This will return the services, open ports, protocol running on victim's pc as you can see in snapshot example of it with Ip as

.Now you can see what all servies are running in target machine, there can be many like vsftpd, httpd, ssh but we are going to use ssh. So see the details of ssh service properly when you use nmap command.

Fig: 2.1 nmap command result

Now as we have earlier specified we will use ssh to enter into the target system (hack the system).

6. Now will use Hydra tool for cracking password in order to get access the target system. Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add. This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely**.**

So now this step takes use of social engineering and your smartness to guess the common user name and passwords. It's kind of easy as it is guess user name of particular system. Example mostly system have account with user name who owns that system and if we are in any organization, organization name can be user of system in most case. Similarly people keep simple passwords like 123456 in most of organization, so you have to be smart to guess the passwords and user names which can exists. Rest all will be done by hydra tool itself .You can find more important information about hydra here [6, 7].

7. In Hydra tool we need to have two files.
   i. Users.txt = this will contain the list of all possible users that can be the users of that target system.
   ii. Pass.txt = this will contain all the passwords you think that can be the password with any user which is present in users.txt file.

8. We note that we actually don't know the correct user with respected password. Hydra tool will do the brute force approach on the users.txt file and pass.txt file and gives the output as highlighting the match username and its respective password.

9. Now you will enter into the victim's pc by using the following command as now you already know the username and password. Snapshot is given to show example.

ssh username@victim's ip .

In my example gautam is username. You can use various commands like ls, cd to explore victim pc. Note. You don't have root access you can only read and not execute files which requires root privilege.also.#gautam indicates that we moved from rocketmail user to victim' machine and we are asking for permission to connect.

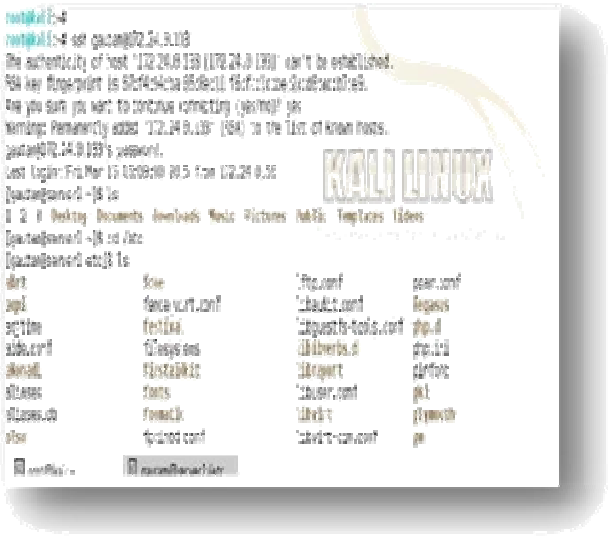

Fig 2.2 Command SSH and Files and Directories of victim's machine.

10. Now it will ask to enter the password. Now enter the password which you got already by the Hydra tool.

11. Now you are in the victim's machine with normal user privileges. The $ mode indicates you that you are not a root user. You need to have # mode with log in to have root privileges.

12. So somehow by end of the procedure you should get # mode with your selected user name.

13. To have a root access, go to password file [8] which you can only read but cannot modify as you are not root user.

14. To go to password file use following command.

vi /etc/passwd .

15. Now you can read the list of all users with various fields like UID, GID, and Shell.

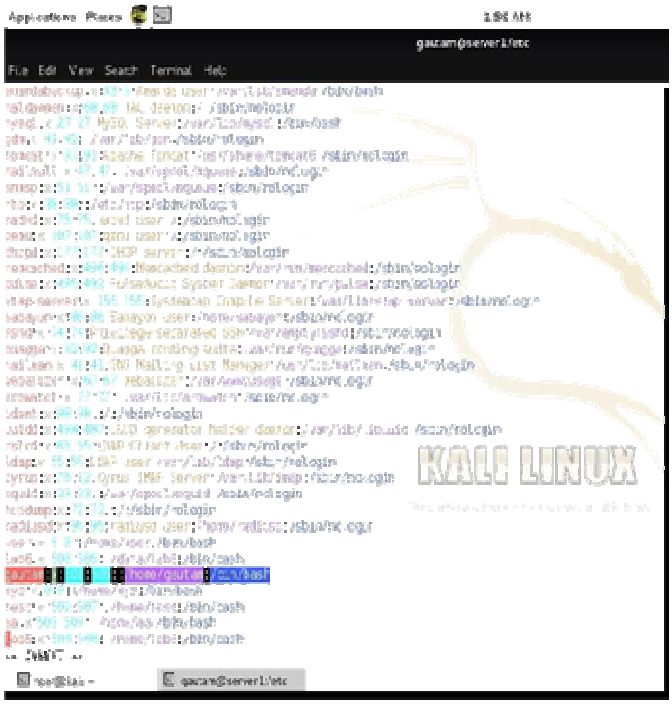

Fig 2.3 Users List (passwd file)

16. Now we need to make UID, GID of the user to which we have logged in to 0(zero). So that system will give this normal user a root privileges. We are making user gautam a root user as an example.

17. In order to do this use following steps

i. Press i or insert to edit the passwd file.

ii. Insert 0 at UID and also GID at row of the user you want to give root privileges. As you are normal user you cannot modify the passwd file as it will throw error saying "read only file".

iii. Now in order to save the changes to modified passwd file use following steps

iv. Press ESC Then press shift colon (:).this is used to come into command mode.now type "w !sudo tee passwd".

Snapshot is shown for better understanding of command given in earlier sub step. As we can see in highlighted part UID and GID is made 0 and command is written to save changes and get the root privilege now and do anything we want.

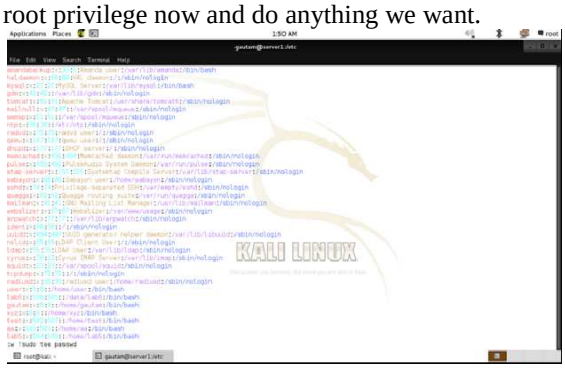

Fig 2.4 Command for Root Access

18..Now you have given the current user a ROOT privileges so that you can do any modification in the target system including deleting, changing of file, etc.
Enjoy…!!

3. ADVANTAGES

1. To gain Information about the Victim.
2. Modify the resources of victim's machine.
3. Confidential data can be leaked and used by attacker to do damage.
4. Attacker can also make system unavailable for victim which in turn is harm for victim as he/she cannot access their own machine.
5. Attacker can launch a virus or any attack once it het root access.

4. CONCLUSION

Linux systems face a unique threat of compromise from brute force attacks against SSH servers that may be running without the knowledge of system owners/operators. Many Linux distributions install the SSH service by default, some without the benefit of an effective firewall. Thus, otherwise conscientious system administrators who keep their systems fully patched may fall prey to a system compromise caused by a carelessly chosen password. As our study results show, not all vulnerable passwords can be considered weak, based on commonly-held beliefs of password strength. Attackers are using and sharing attack dictionaries of username/password pairs that incorporate a significant percentage of apparently strong passwords. Using a password checking tool, especially one that restricts systematic approaches to password selection, can provide an extra measure of protection against malicious login traffic, especially when combined with other protective measures designed to reduce the visibility of Internet facing servers.

REFERENCES

[1]http://www.directessays.com/viewpaper/94312.html
[2] http://drmzz.blogspot.in/2013/07/abstract-of-typesof-hacking-that-may.html
[3] http://matt.might.net/articles/ssh-hacks/
[4]http://www.webroot.com/in/en/home/resources/t ips/online-shopping-banking/secure-what-is-social-engineering
[5] http://www.cyberciti.biz/networking/nmap-command-examples-tutorials/
[6] http://www.concise-courses.com/security/what-is-hydra/
[7] http://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-online-passwords-with-tamper-data-thc-hydra-0155374/ /
[8]http://www.cyberciti.biz/faq/understanding-etcpasswd-file-format