INVADING SSH,TELNET,VNC SERVICES WITH METASPLOIT AND THC-HYDRA

Ms.Shruti
Computer Science and Engineering
Lovely Professional University
Jalandhar, India
shruti.24906@lpu.co.in

Ganeshbabu Aleti
Computer Science and Engineering
Lovely Professional University
Jalandhar, India
aletigo1234@gmail.com

AnkushKumar
Computer Science and Engineering
Lovely Professional University
Jalandhar, India
ankush8233346877@gmail.com

Abstract*—The services like SSH, Telnet, VNC etc which enables internet users or administrators to remotely connect and control a computer operating system with the aid of software or command line tools. To connect those services one must complete the authentication process. Attackers or Cyber criminals can crack those remote connection services using different methodologies. With help of Penetration testing tools like Hydra, Metasploit, Brutus etc weak passwords can easily compromised. In the following paper those services passwords are compromised and gain unauthorized access to user account of a computer.

Keywords--Metasploit, Hydra, Raspberry pi, SHH, Telnet,VNC

1.Introduction

The need of accessing computer remotely is frequent nowadays. Computer users who are unable to physically access the computer uses bidirectional interactive communication services like SSH, Telnet, VNC etc. A computer can be accessible remotely when those internet services are available and running on certain port. Using the IP address and port number one can access those services. For authentication, Login process can be implemented to those services in order to prevent unwanted logins, although it is a common feature of servers. A username and password is provided for authentication process to validate the legitimate users for telnet and SSH.

Attackers can find the computer devices running those remote control services using the following search engine shodan,zoomeye, censys etc. Attacks has tactics and methodologies to compromise the computer devices remotely. They use password cracking tools including hydra,

metasploit, etc to crack the user authentication passwords using dictionary attacks. After successful password cracking of computer device, they gain unauthorized access to computer device. Further they can perform secondary level or post attacks on computer. Intruder can harm computer in the following ways deploy a backdoor, install any virus or worm, deploy any malware including spyware, ransomware, rootkit, Privilege escalation etc.

Raspberry Pi with SSH telnet and VNC services enabled device is taken into consideration for demonstrating the password attacks. It is a single board computer, raspbian OS is installed on it.

Basic information gathering is mandatory to identify the ports and services of the target. Using reconnaissance and scanning technique attackers find information like IP, ports, services etc. With the obtained information attacker start cracking passwords with help of Pentest tools. Many Password cracking tools are available on the market. Metasploit and Hydra are open source tools. Metasploit has several modules, each has its function. Hydra is a best tool cracking login passwords. Both tools are used to crack or compromise the remote login services.

2.Literature Review

Remote Login Protocols

A client/server model enable a user to establish a session on the remote machine and then run its applications. This application is called as remote login. A user may want to use such applications at a remote site, that results to be transferred back to its local site. For instance, an individual working at home can log in to his/her work server to access applications programs for doing a task. This can be done by a client/server application program for the desired service. Both telnet and SSH are login protocols.

Telnet
Telnet is a TCP/IP standard for establishing a command line remote connection to a remote system. It enables a user to log in to a remote device across the Internet. By default it runs on 21 port. This application can be interpreted as if the text being transferred had been typed on a keyboard attached to the remote machine. A client uses application telnet CLI tool to log in and access remote device.

SSH
SSH stands for Secure Shell another remote login protocol, by default runs on 22 port [1]. It uses TCP for communications but it is powerful and flexible than telnet and allows the user to more easily execute a single command on a remote client. It provides a secure communication by encryption and authentication messages.

VNC
The VNC is a simple TCP/IP protocol for remote access to graphical user interfaces over a network connection. It is based on the notion of a remote framebuffer aka RFB. A VNC viewer or client is installed on the local computer and connects to the server component, which must be installed on the remote computer. The server transmit a duplicate of the remote computer's display screen to the viewer. It also interprets commands coming from the viewer and carries them out on the remote computer.

Password Cracking
Password Cracking is refer to recovering passwords or attempting to gain unauthorized access to restricted systems. It is done by repeatedly guessing the password, usually through a computer algorithm in which computer tries numerous combinations until the password is successfully discovered.

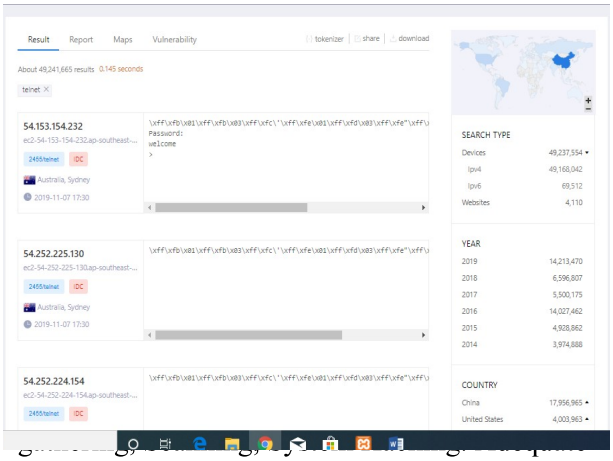
Dictionary Attack
Dictionary attack is a command password attack which uses a pre-arranged list of passwords by trying all the strings presented in the list [2]. It attempts to login with all passwords in the password list , when the password is matched with actual password the attack is terminated.

Raspberry Pi
In this We use The Raspberry Pi is a low cost, small sized computer that use a computer monitor or TV as a monitor of raspberry pi, and uses a standard keyboard and mouse. It is a capable little device that enables people of all ages to explore computing, and to learn how to program in languages like Scratch and Python. It's capable of doing everything you'd expect a desktop computer to do, from browsing the internet and playing high-definition video, to making spreadsheets, word-processing, and playing games.

Nmap
Nmap aka network mapper is an open source port scanner tools typically use by network admins and penetration testers [3]. It is capable of following scanning target open ports, operating systems, vulnerabilities and many more.

Metasploit
Metasploit is a Ruby-based penetrating testing tool uses by security professionals that enables to write, test and execute exploit code [4]. It consists of several tools that one can use to test security vulnerabilities, enumerate networks, execute attacks and evade detection. It is a collection of tools so it provides complete environment for penetration testing and exploit development. It is a cross platform framework which means available for all Windows, Linux and Mac OS.

Hydra
Hydra is open source login cracker penetration testing tool which supports numeros protocols to attack. This tool enables security professionals



time is given for information gathering and scanning phases to understand the target. Attackers find the devices running any of the services using search engine shodan or zoomeye. Those search engine can fetch desired results with the help of operators or normal search bar. In the following SSH and telnet services are search, in result shodan and zoomeye provided finite number of devices that running SSH or telnet.

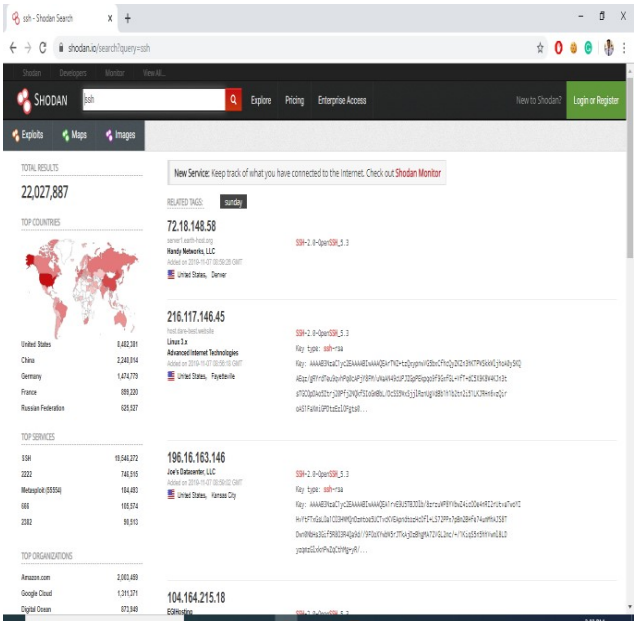
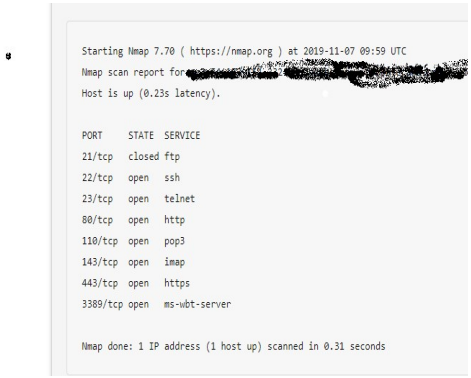


Fig 1 : Resulting SSH enables devices using shodan

Fig 2: zoomeye fetched results in which devices running telnet service

After collecting basic information about the target. Attacker perform the second phase called scanning. Scanning technique reveals the services, Operating systems, Vulnerabilities etc of a target. A port scanner tool is used to perform scanning phase. Nmap is an open source port scanner that enables one to run commands against server or computer devices which are connected to the internet. Nmap provides many features to fetch juicy information about target. A basic Nmap scan against target can give the list of open ports of the target. Nmap command "nmap IPaddress".



```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-07 09:59 UTC
Nmap scan report for [redacted]
Host is up (0.23s latency).

PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   open   telnet
80/tcp   open   http
110/tcp  open   pop3
143/tcp  open   imap
443/tcp  open   https
3389/tcp open   ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

Fig 3: Nmap results showing open ports on the target system.

In phase three system hacking, password crack is take place. Hydra and metasploit tools are used to perform password cracking wordlist attack.

Dictionary attack on Telnet service using Command line Hydra

Using command line hydra tool dictionary attack can be performed. "hydra" is command to access CLI hydra tool. The following command to start telnet password cracking against target "hydra -l admin -P passlist.txt 192.168.1.6 telnet". Where

- l : login name
- P : password list
- 192.168.1.6 : IP address of the target
- Telnet : Service that we cracking.

If the user is not determined, hydra accepts a wordlist for users too. Command : "hydra -L

loginlist.txt –P passlist.txt 192.168.1.6 telnet".

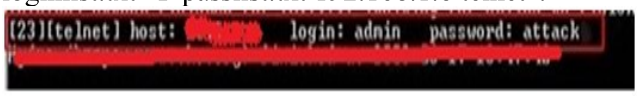


Fig 4: Login name and password displaying after successful attack.

Brute forcing VNC service password using Hydra:

VNC service can be compromised using password wordlists by trying one password each time taken from wordlist.
The target device has VNC service enabled on port 5091 hosting on 192.168.1.3 IP address. Fig[5]

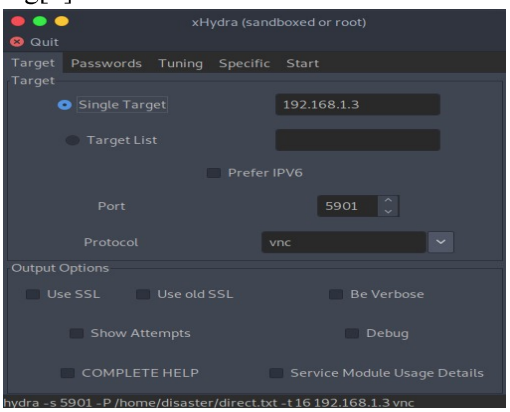


Fig 5: Setting the target, port and service

Next, click passwords tab for setting up wordlist against our target to bruteforce. Bruteforcing VNC service doesn't need user, so enable "Protocol does not require usernames".Fig[6]
Select password list field to provide wordlist located in your filesystem. To find wordlists in your machine use "loca
Te wordlist" command. Fig[7]

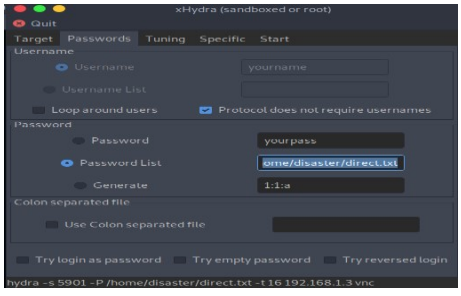


Fig 6: Select the wordlists in which contains passwords

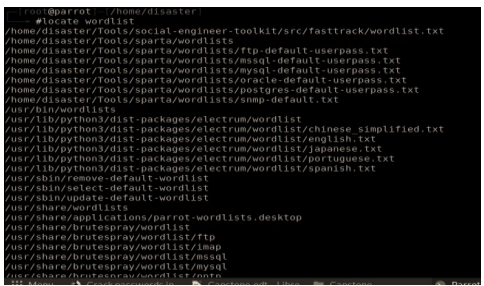


Fig 7: locating wordlists in your local system

Next, click the tuning tab for setting no of tasks to 3 to 5.Note it may lead to denial of service .

Next, click the start tab for initiating the brute force attack. Click on the start button below for starting the attack. When the password is cracked it stops it displays the password.Fig[8]

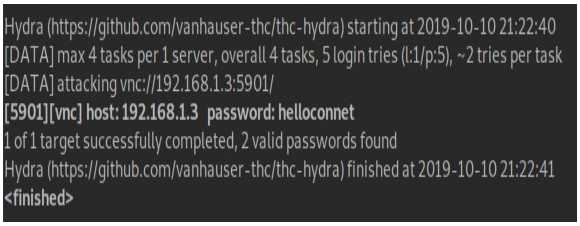


Fig 8: Password is displayed after the brute force attack.

Cracking SSH Password using Metasploit FrameWork

Scanning the target using Nmap shows SSH service is open that indicates SSH is enabled. Using metasploit SSH_LOGIN module brute force can be carried out.

Start Metasploit

Before opening msfconsole it is worth to run this command "service postgresql start". To open Metasploit framework in terminal use the following command "msfcosole".Fig[9]

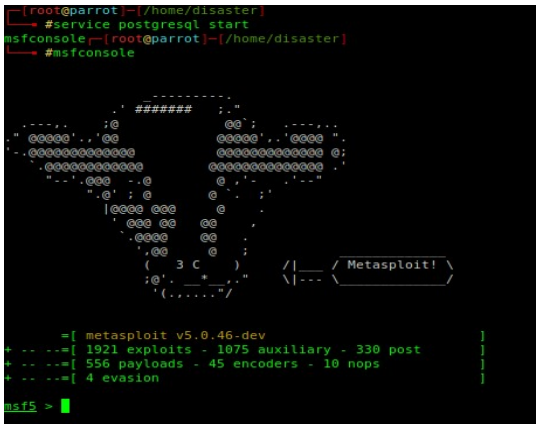


Fig 9:

Msf banner

After running msfconsole command it opens the metasploit , “ssh_login” auxiliary module is used to brute force SSH user and password. To find the module type “search ssh_login”
To use the ssh_login module , type this command in terminal “use auxiliary/scanner/ssh/ssh_login”. Fig[10]

Fig 10: Selecting module ssh_login to brute force ssh credentials

It loads the module and currently ready to use it. Options of the module need to be set which target , target port (22), wordlists etc. To see options type “show options”.Fig[11]

Fig 11: Options available with ssh_login module

Options need to be setting according to our target, so our target is Raspberry Pi . It has default user
pi ,thus we directly set username option as pi. In your case you can set wordlists for both user and password.

Set the options as following:

msf5 auxiliary(scanner/ssh/ssh_login)> set RHOSTS 192.168.1.102

msf5 auxiliary(scanner/ssh/ssh_login)> set USERNAME pi

msf5 auxiliary(scanner/ssh/ssh_login)> set pass_file /home/disaster/hello.txt

msf5 auxiliary(scanner/ssh/ssh_login)> exploit

After setting required options run “exploit” command to start brute force. When the password in your wordlist get match it stop the attack and displays the password and user.Fig[12]

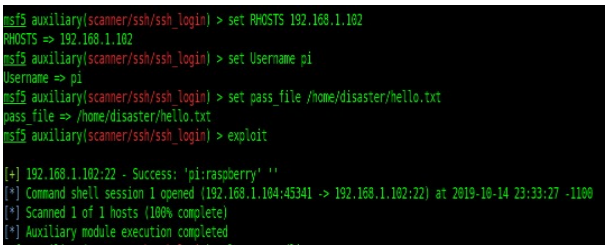


Fig 12 : Options required to set and exploit to start brute force.

Session gets create after successful brute force attack. “sessions -i” command can be used to see the sessions list. To access the session write “sessions x” (x is the serial number of the session). Home directory of the user will be the current working directory of the SSH service. Privilege escalation is possible to take root access.

4. Conclusion :

Services like SSH, Telnet and VNC are so helpful for internet users or administrators to control remote systems. Using weak passwords make the authentication easy to break. An attacker can use password cracking tools like Hydra, Metasploit, etc. It takes less time to crack those weak passwords with the help of wordlists using dictionary attack methodology. To avoid the password attacks use strong password for authentication process. Disable the services if you don’t need them.

5. References

[1] N. KANDHIL and D. A. KUMAR, "A STUDY ON SECURE SHELL (SSH) PROTOCOL," *International Journal of Computer Science & Management Studies,* pp. 300-305, Aug 2011.

[2] S. K. Kulkarni, "A Survey of Password Attacks, Countermeasures and Comparative Analysis of Secure Authentication Methods," *International Journal of Advanced Research in Computer Science ,* pp. 319-331, Nov 2015.

[3] M. G. Kaur and N. Kaur, "Penetration Testing – Reconnaissance with NMAP Tool," *International Journal of Advanced Research in Computer Science,* p. 3, April 2017.

[4] P. K. S. S. Pandey, V. Dixit and L. K. Tiwari, "A study on Penetration Testing Using Metasploit Framework," *International Research Journal of Engineering and Technology(IRJET) ,* pp. 193-200, Dec 2018.