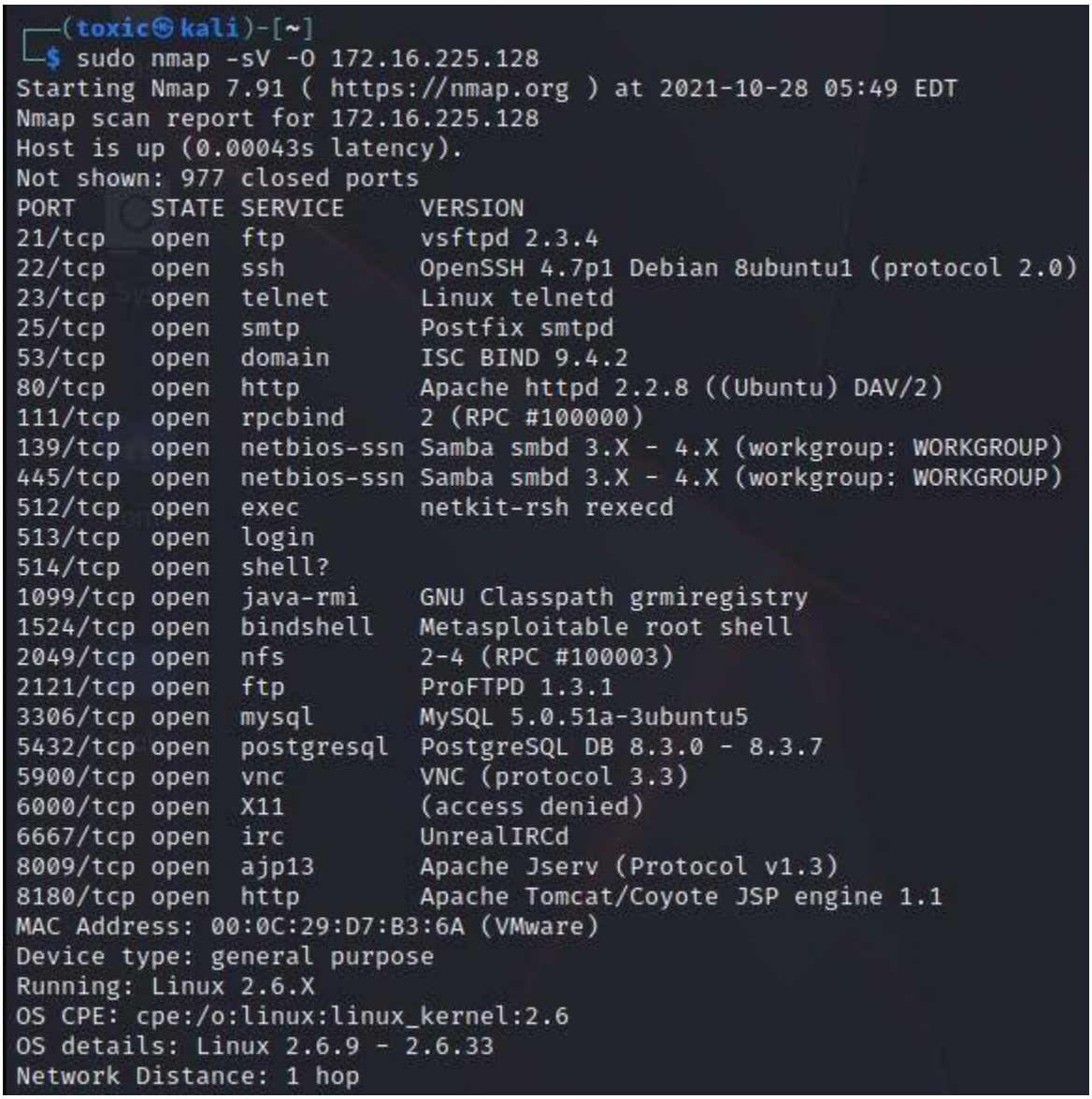
Scanning target system for vulnerabilities

Having the IP address we now move to our Kali Linux for the purpose of auditing our target system using NMAP for the purpose of identifying vulnerabilities within our target system.We now scan the target system using NMAP command

```
nmap -sV -O 172.16.225.128
```

In the screen below, we see the vulnerabilities within our target system. The **-O** NMAP command is to determine the operating system within which target system is operating on. the **-sV** option will help us determine the version of the services running on these ports. The system has many open ports as it can be seen in the screenshot below. Each port has a technique or else a way of exploiting its vulnerabilities.



We now have the information we require to exploit the vulnerable system.We will be exploiting some of the vulnerabilities we have just discovered above.

FTP port 21 exploit

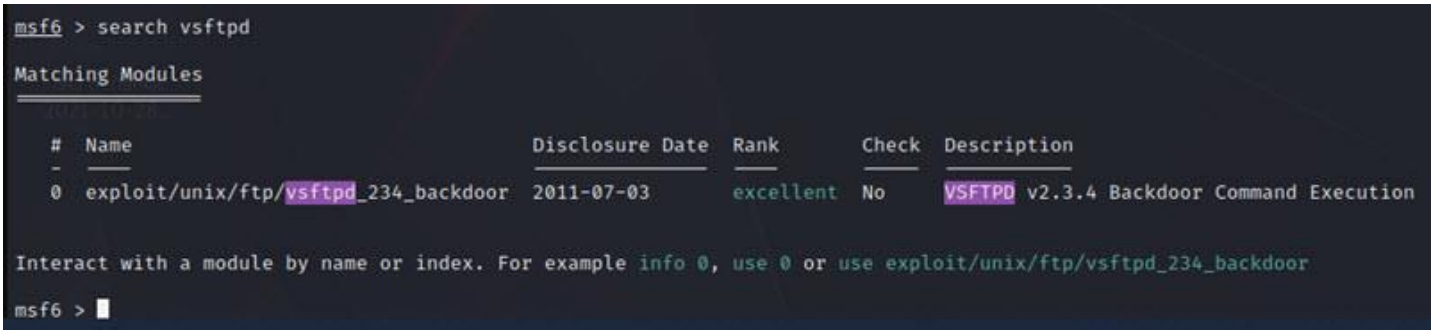
Our first vulnerability to exploit will be FTP which runs on port 21.

Step-1: Launching Metasploit and searching for exploit

We fire up our Metasploit using:

```
msfconsole
```

command and search for vulnerability relating to vsftpd. (Metasploit has the known vulnerabilities exploit database hence makes it easier for a pen-tester to load and use the exploit). On searching for exploits related to FTP services, we find an exploit "`exploit/unix/ftp/vsftpd_234_backdoor`" as shown below.



Step-2: Using the found exploit to attack target system

We now have to use the exploit to attack out target system. We enter command to use the backdoor.

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

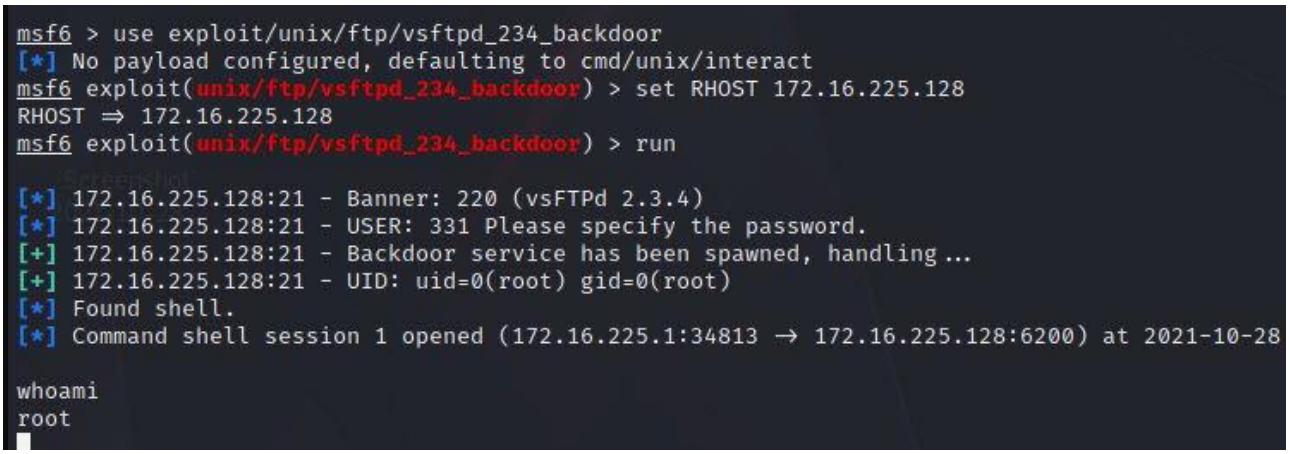
set the remote host

```
set RHOST 172.16.225.128
```

to our target system IP address and run the exploit.

Step-3: Checking privileges from the shell

We get a shell from the target system and we can test by checking which account the shell is on. The shell is running on the system with root privileges as Shown below. From the shell you can access and make changes to our target system.



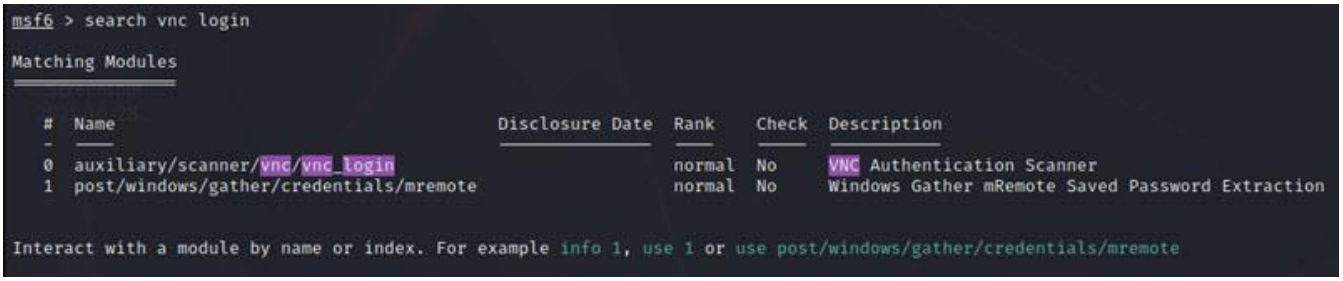
Exploit VNC port 5900 remote view vulnerability

VNC (Virtual Network Computing) enables a users to control another computer over a network connection. In this attack we will be attacking our target system on port 5900 in order to control it over remotely.

Step-1: Launching Metasploit and searching for exploits

We fire up our Metasploit framework and search for a vulnerability which will enable us to crack the VNC remote login credentials as shown below. using key words "vnc login"

```
search vnc login
```



Step-2: Using the found exploit to get VNC password

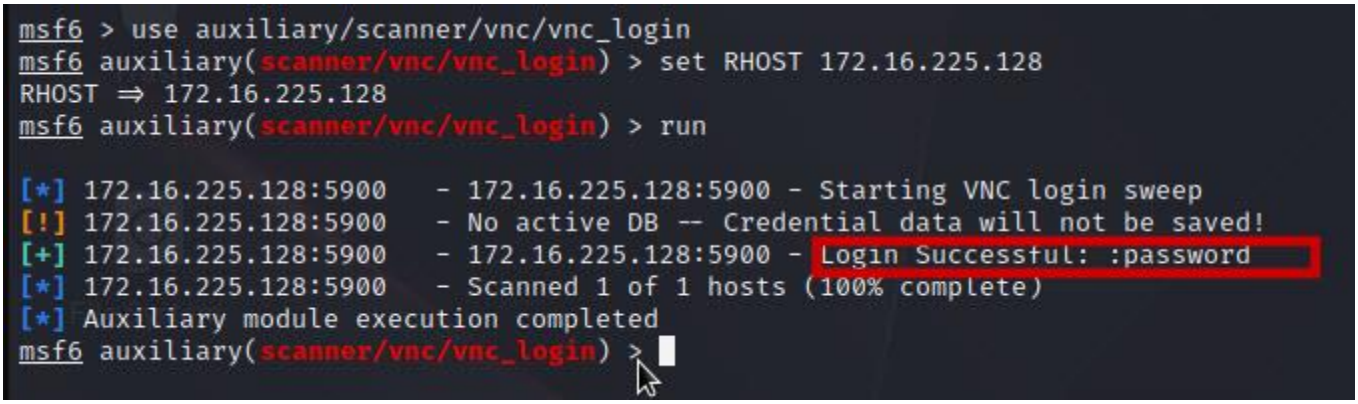
We have to use "auxiliary/scanner/vnc/vnc_login"

```
use auxiliary/scanner/vnc/vnc_login
```

vulnerability and set our remote host or else our target system IP address and run.

```
set RHOST 172.16.225.128
```

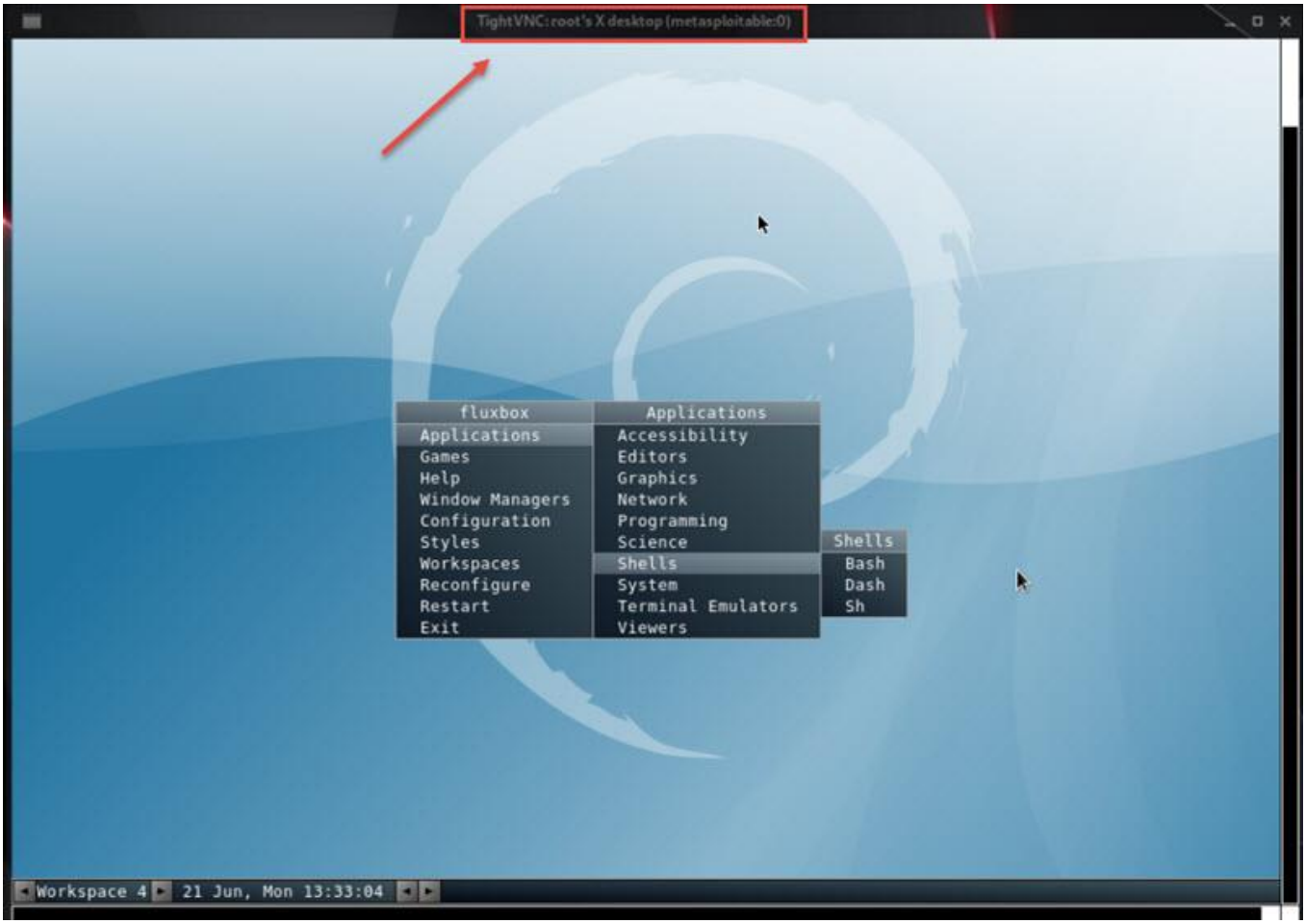
On the screen below you can see metasploit was able to crack the VNC login password and it is shown below.



Step-3: Gaining remote control of target system via VNC

Having the IP address and VNC login password, we will open another terminal from where we will try to connect remotely to our target system. The password login credentials are "password: **password**"

And we have a remote connection to the target system as shown on the screen below. We are able to view what is happening on our target's screen. We can also be able to control the system and launch different terminals. In short, it is as if you have the system in front of you and can do anything you want to do with it.



Exploit Samba server vulnerability

Our last vulnerability is the samba server vulnerability. We will be exploiting this vulnerability on our target machine to gain a TCP shell from which a hacker can be able to perform malicious activity on a vulnerable server since our target system has Samba "`username map script`" Command Execution.

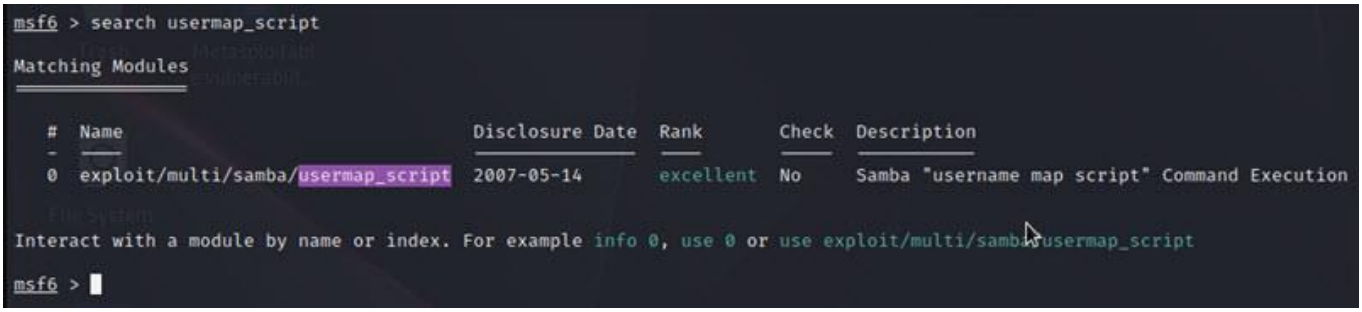
Step-1: Launching Metasploit and searching for exploits

We will first launch `msfconsole` and search for an exploit which matches the vulnerability found on metasploit from which we will launch our attack.

```
msfconsole
```

As you can see we have our "`exploit/multi/samba/usermap_script`" vulnerability which we need to launch our attack.

```
search usermap script
```



Step-2: Using the found exploit to gain remote shell

We set to use the script vulnerability, set the target IP address and run the exploit.

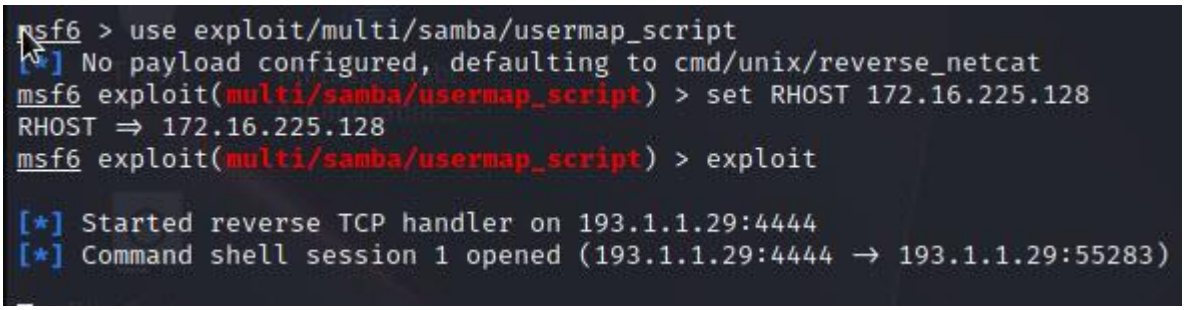
```
exploit/multi/samba/usermap_script



set RHOST 172.16.225.128



exploit
```

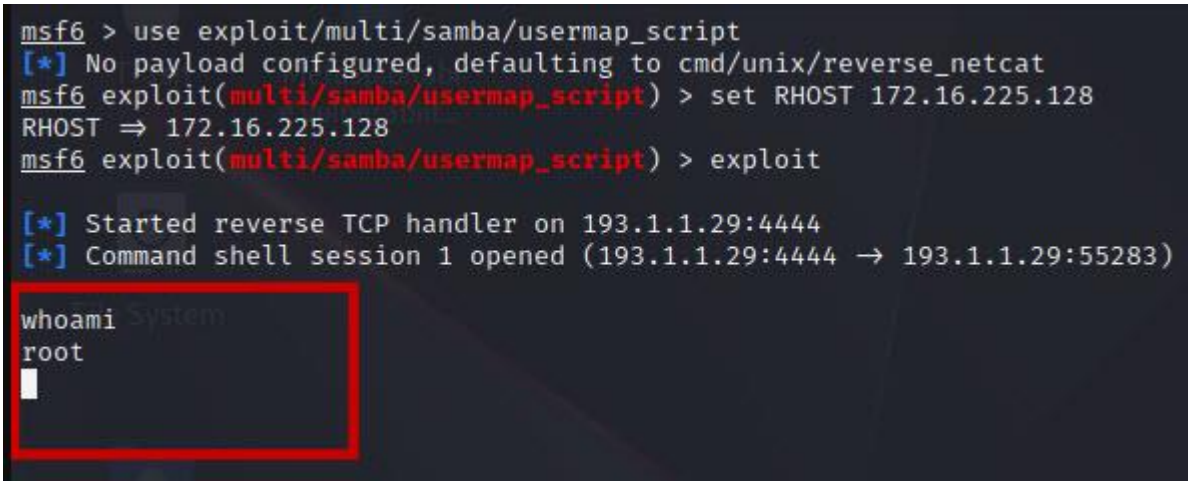


Step-3: Checking privileges of the shell acquired

We now have a remote shell. We can check our privileges on on the shell established using the command "**whoami**"

```
whoami
```

We are in the target system as the "**root**"



Conclusion

In the above tutorial we learnt on different vulnerabilities which are available on Metasploitable 2. With the help of Metasploit we are able to exploit the vulnerability with more ease as it helps us in searching for the right vulnerability by just a single command. On a live system, we do not expect these many vulnerabilities but be sure to find one or two. You can use our other guides to try and exploit the other vulnerabilities which are on Metasploitable 2.