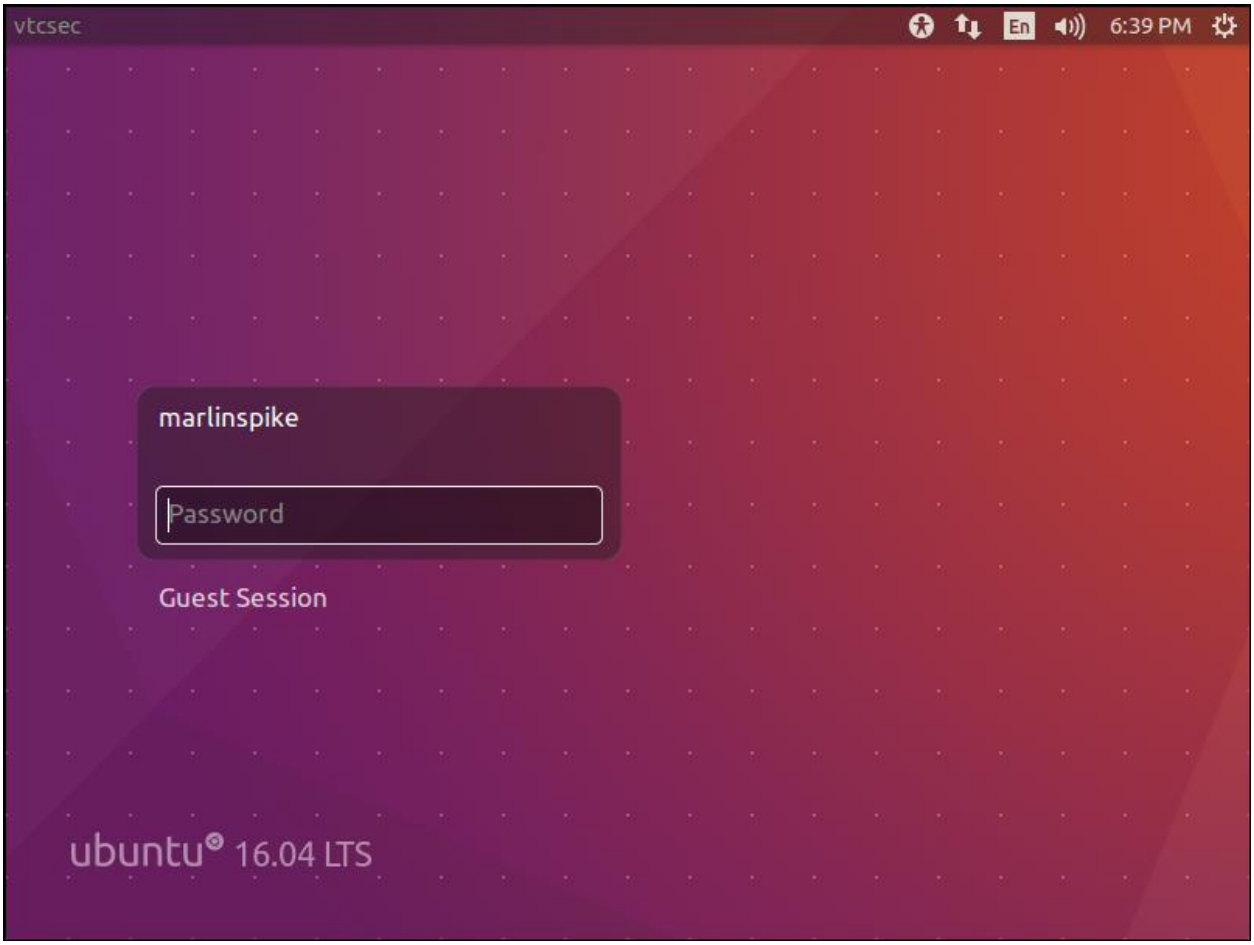
CTF-BASIC PENTESTING 1
(https://www.vulnhub.com/entry/basic-pentesting-1,216/)

Objective:-
Remotely attack the VM and gain root privileges.

Setting up the environment:
I used VMware for this task. I booted up the target machine as well as my Kali Linux. Both the machines were on the same network.

Footprinting and Scanning:-
Initially, at the log-in page of the target machine, I entered the password as 'marlinspike'; same as the username and was able to gain access. It was possible to gain root privileges from there, but the task was to do so remotely.



[Screenshot 1: Target Machine]

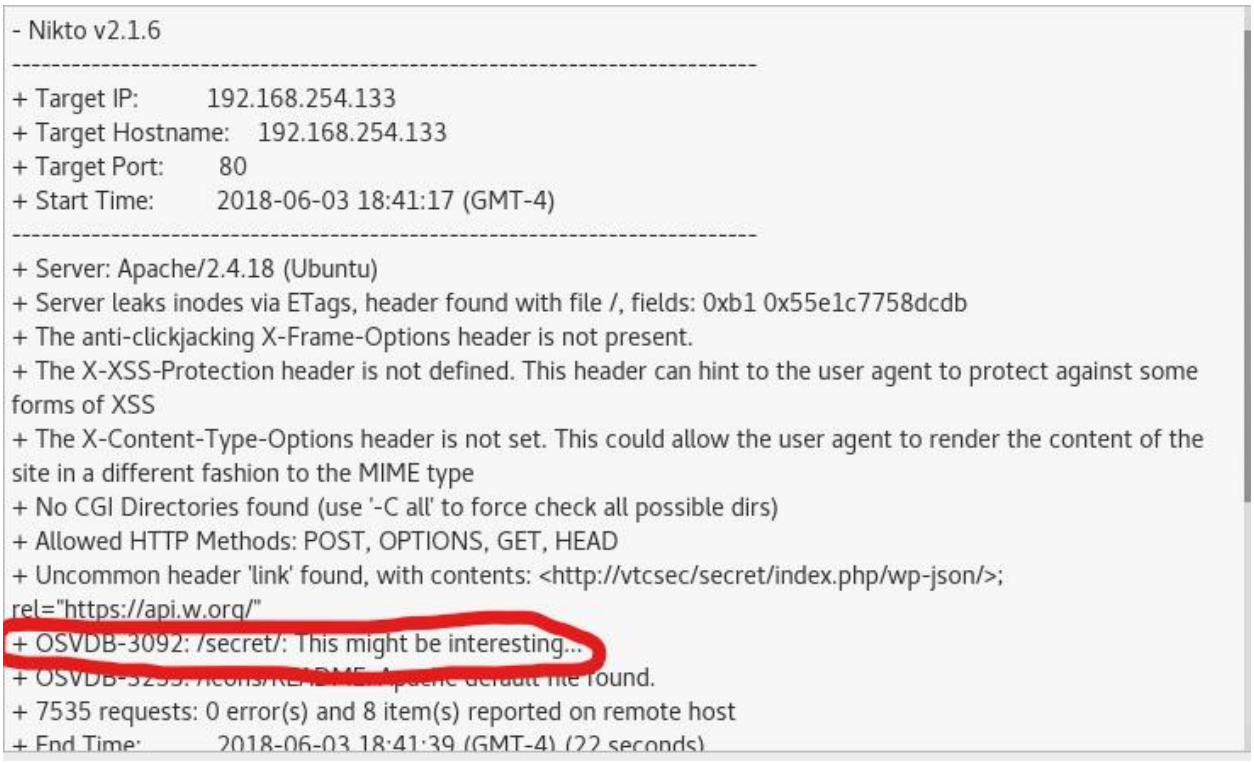
```
root@Dagger:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.254.132  netmask 255.255.255.0  broadcast 192.168.254.255
        inet6 fe80::20c:29ff:fe51:a8c0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:51:a8:c0  txqueuelen 1000  (Ethernet)
        RX packets 85604  bytes 20991290 (20.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 80162  bytes 6577858 (6.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 332  bytes 111123 (108.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 332  bytes 111123 (108.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@Dagger:~# nmap -sP 192.168.254.1/24
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-03 18:40 EDT
Nmap scan report for 192.168.254.1
Host is up (0.00081s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.254.2
Host is up (0.00015s latency).
MAC Address: 00:50:56:ED:6F:0F (VMware)
Nmap scan report for 192.168.254.133
Host is up (0.0011s latency).
MAC Address: 00:0C:29:B9:3A:2B (VMware)
Nmap scan report for 192.168.254.254
Host is up (0.00043s latency).
MAC Address: 00:50:56:F2:5C:9D (VMware)
Nmap scan report for 192.168.254.132
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.81 seconds
root@Dagger:~#
```

[Screenshot 2: Kali Linux and Nmap Ping Sweep results]

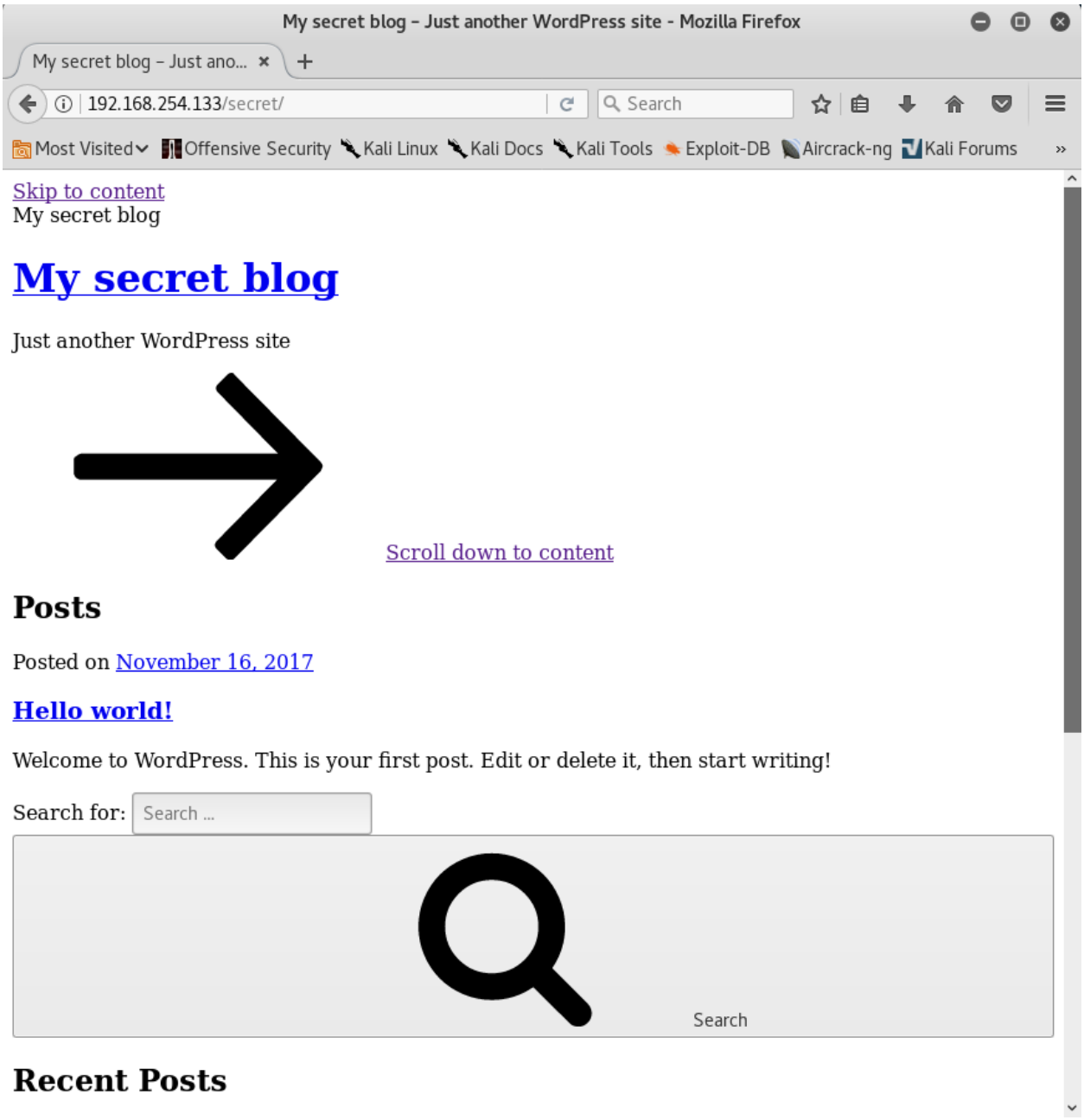
In my Kali machine, I did a ping sweep of the network and identified the IP address of the target machine (which was 192.168.254.133). I did vulnerability assessment of the target using 'Sparta'. I found 3 open ports: 21, 22 and 80. Also, Nikto found a 'secret' directory.

Port	Protocol	State	Name	Version
21	tcp	open	ftp	ProFTPD 1.3.3c
22	tcp	open	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux...
80	tcp	open	http	Apache httpd 2.4.18 ((Ubuntu))

[Screenshot 3: Sparta scan results]

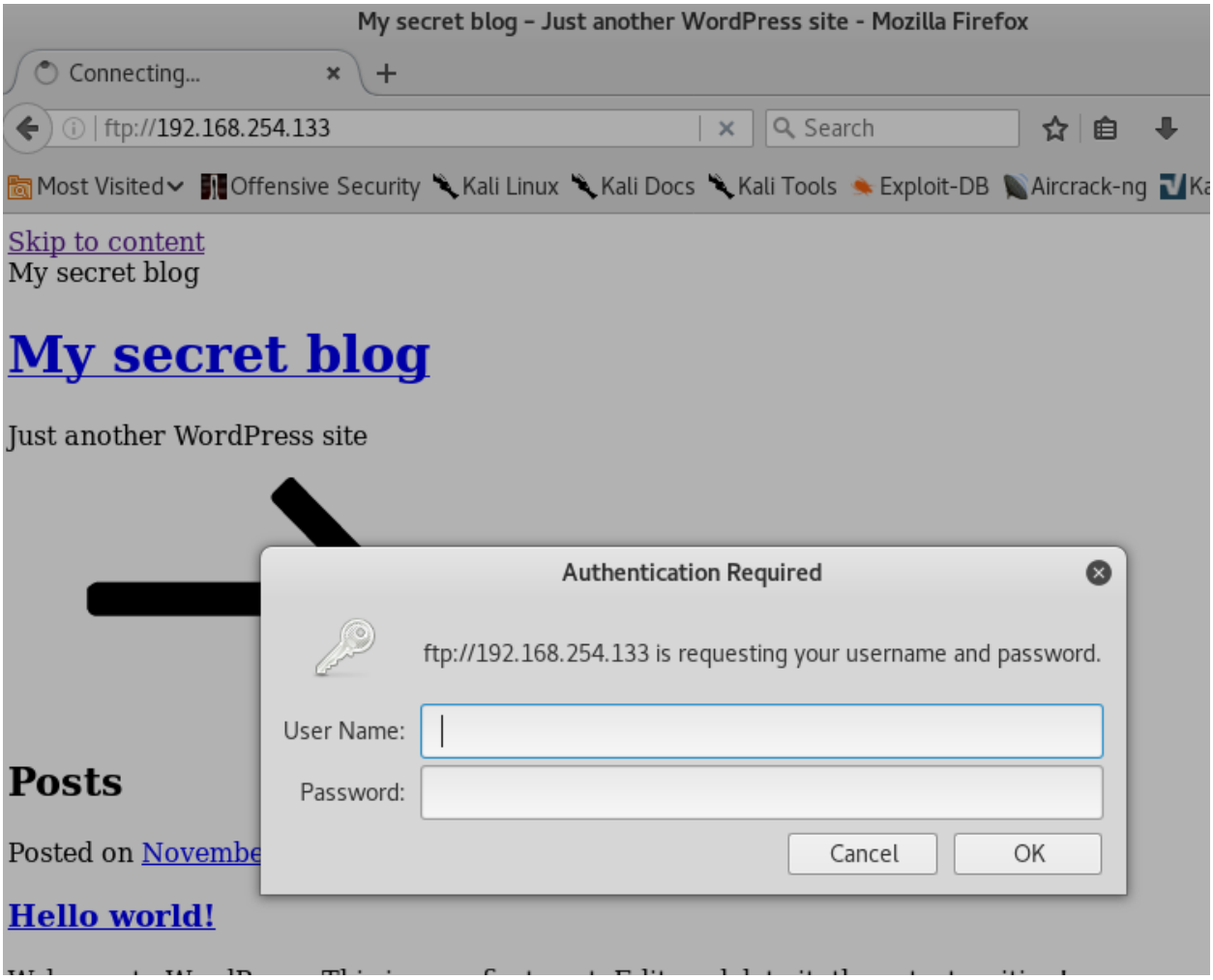


[Screenshot 4: Nikto revealed a 'secret' directory]

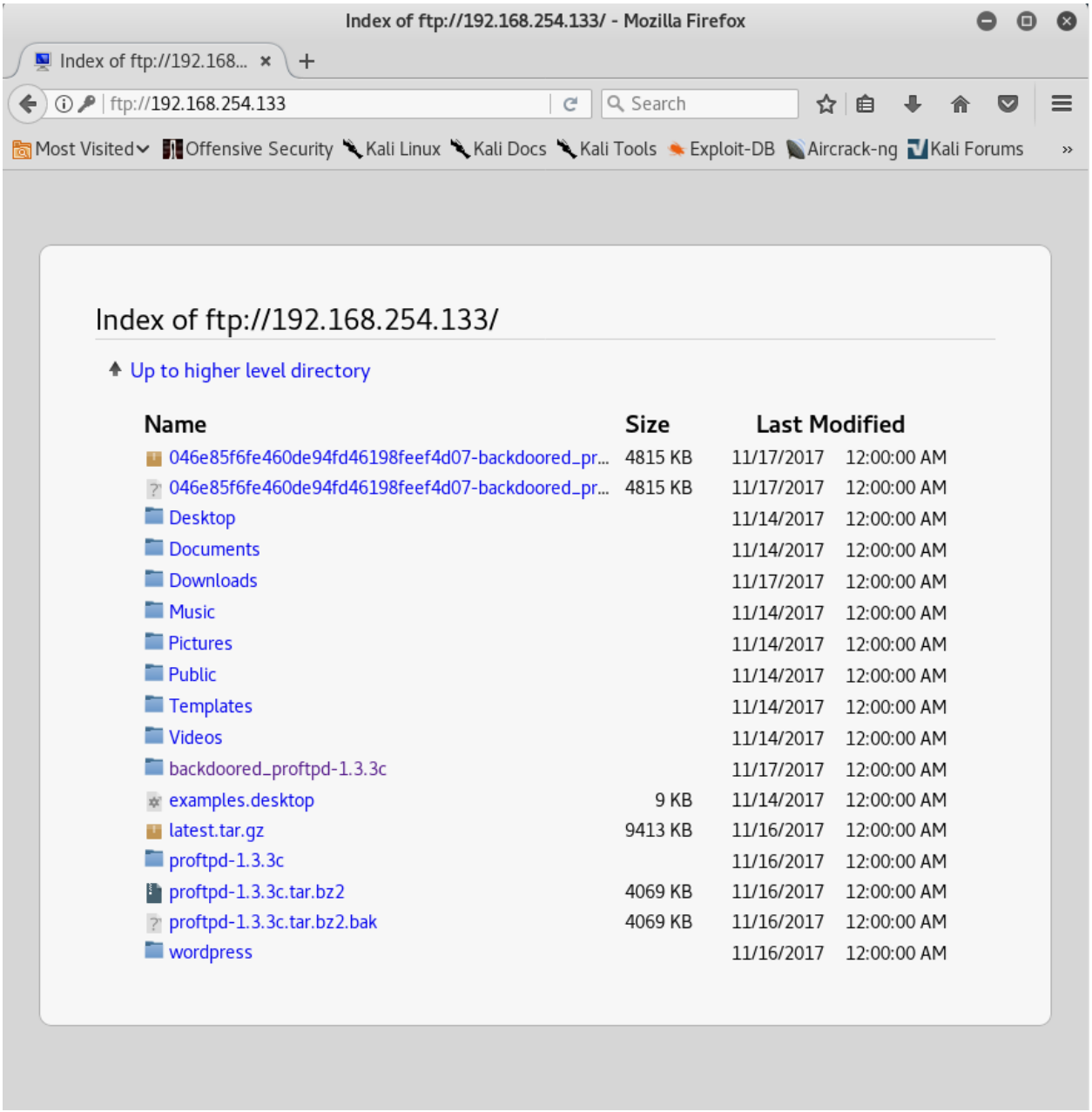


[Screenshot 5: Contents of the secret directory]

I tried to connect to the target using ftp protocol and used ‘marlinspike’ as both login credentials and I was able to get through.



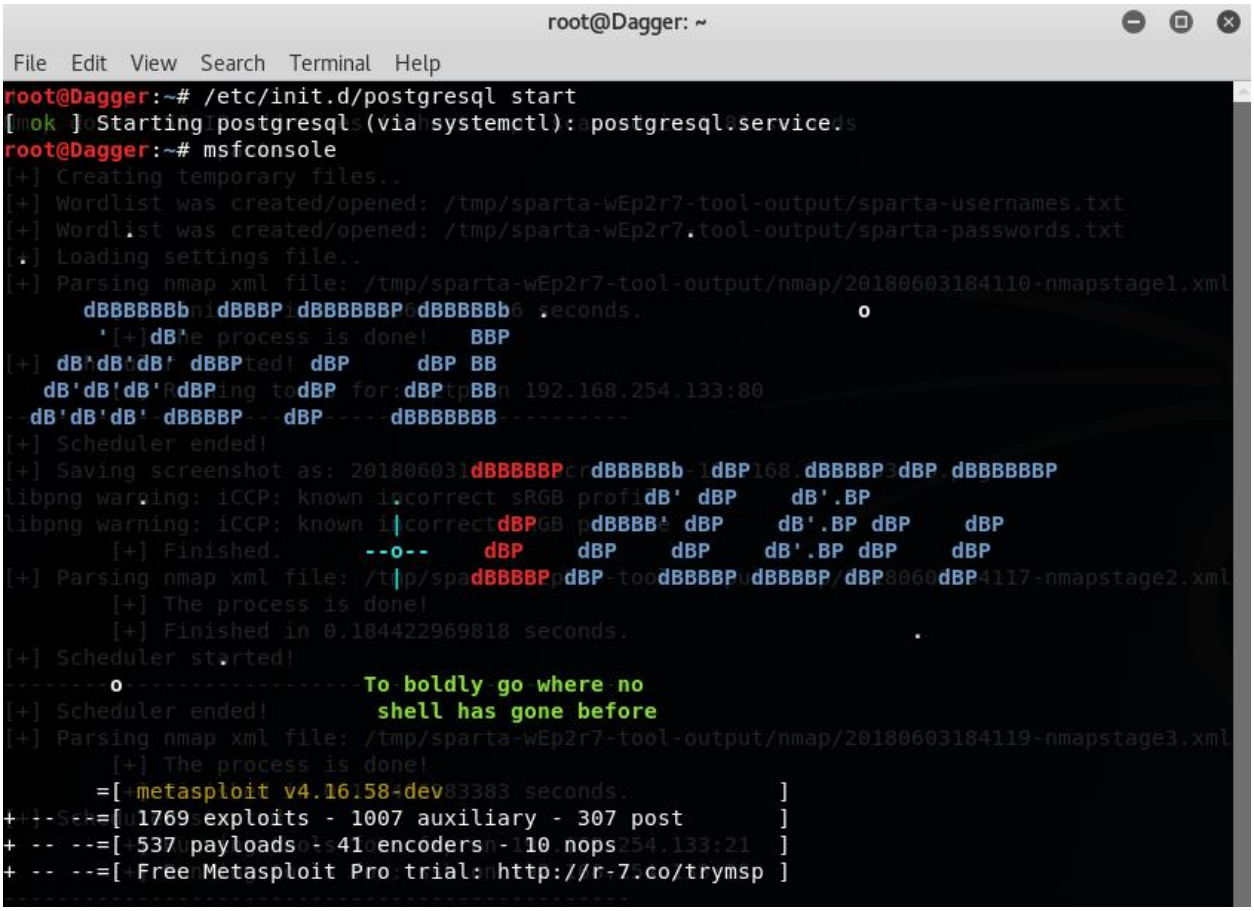
[Screenshot 6: Connecting to target with ftp]



[Screenshot 7: Gained access using the specified credentials]

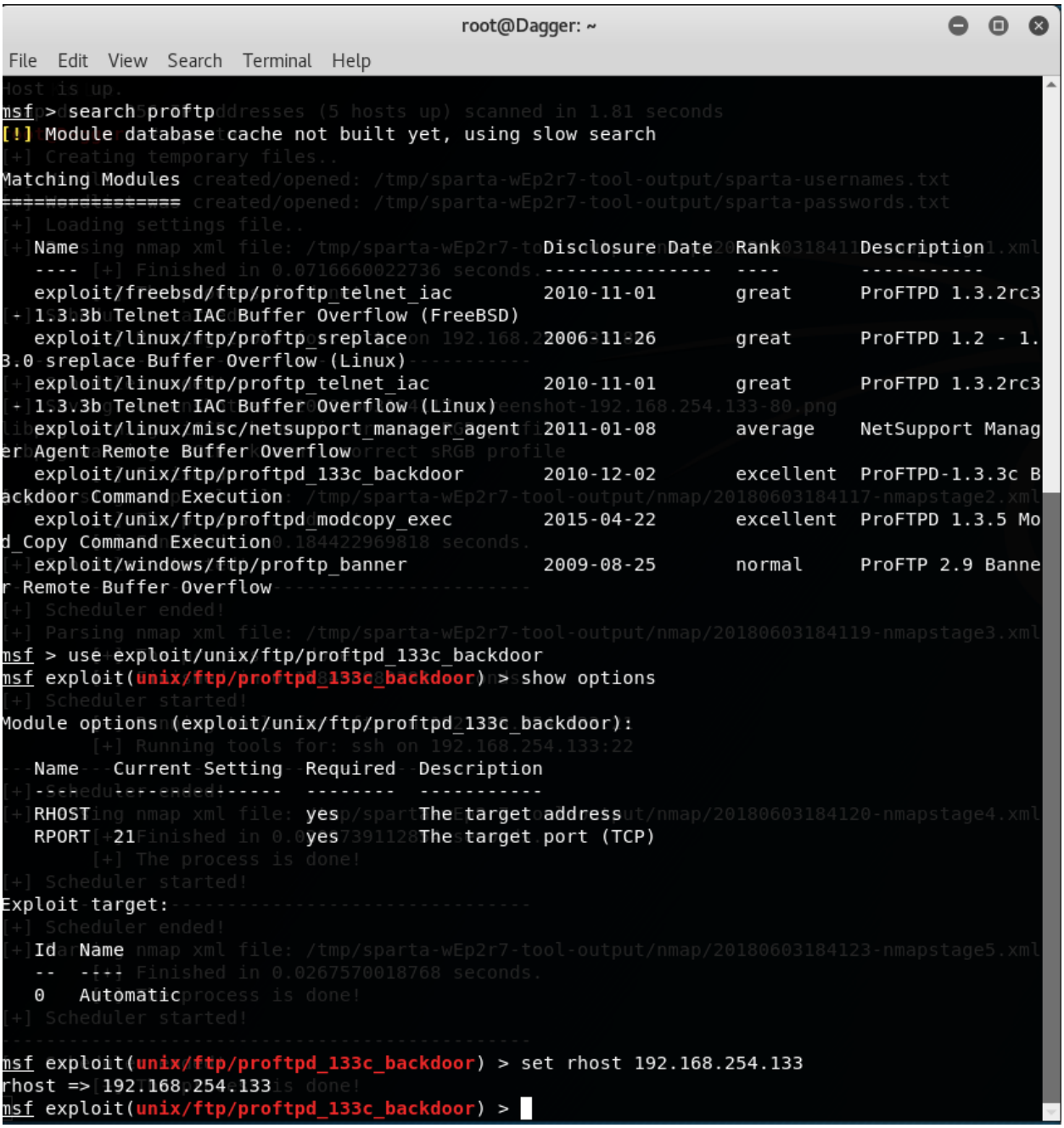
Exploitation:-

The Sparta scan showed that the target was running ProFTPD service on port 21. I initialized the database and started Metasploit.

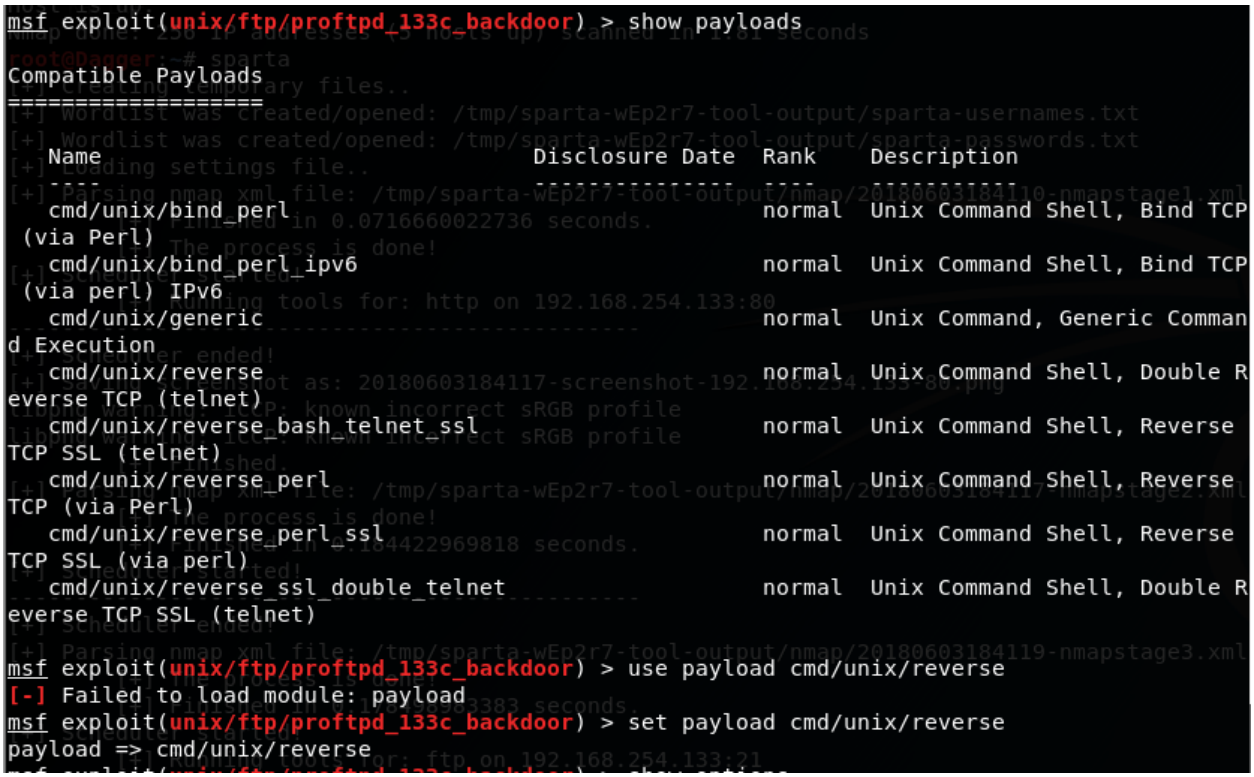


[Screenshot 8: Initialized database and started Metasploit]

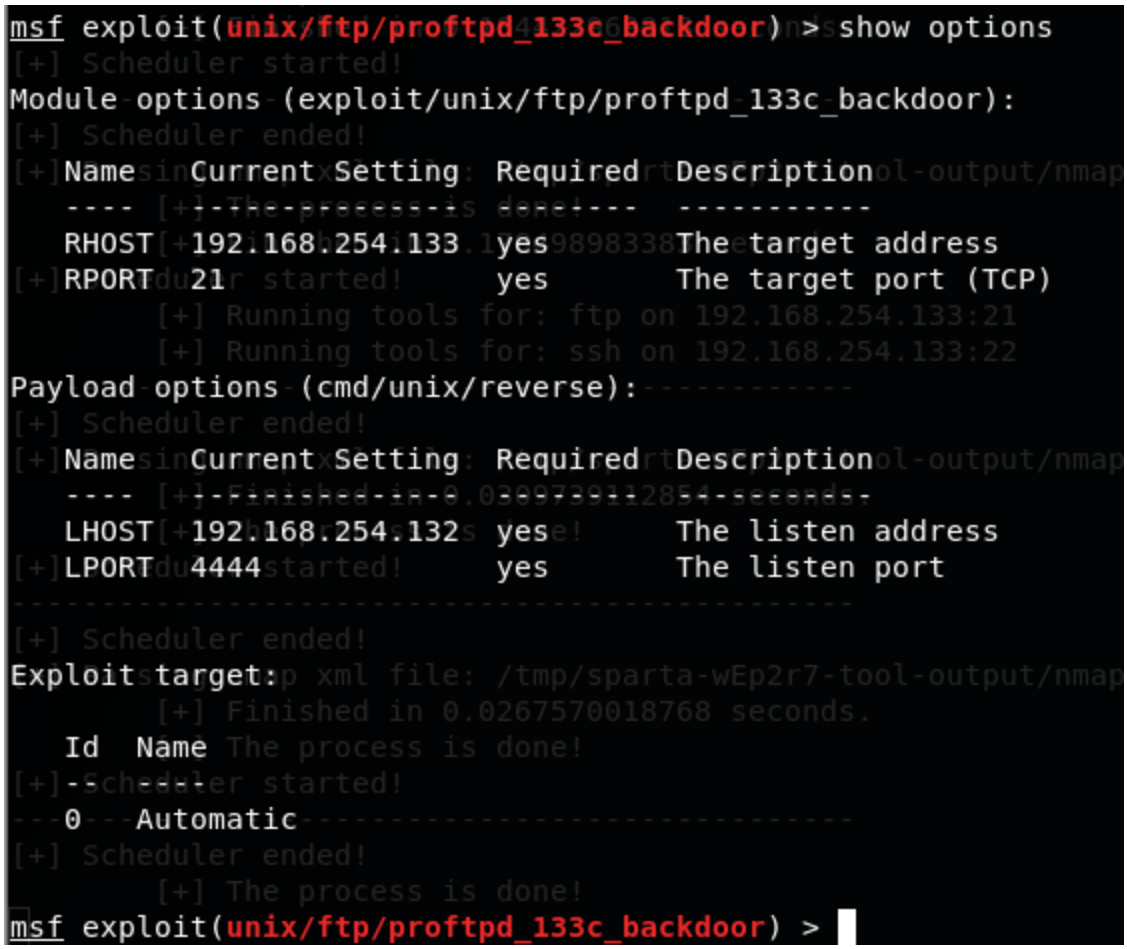
I searched for any 'ProFTPD' exploits and decided to use proftpd_133c_backdoor exploit. After searching for compatible payloads, I decided to use cmd/unix/reverse payload.



[Screenshot 9: Set up the exploit]

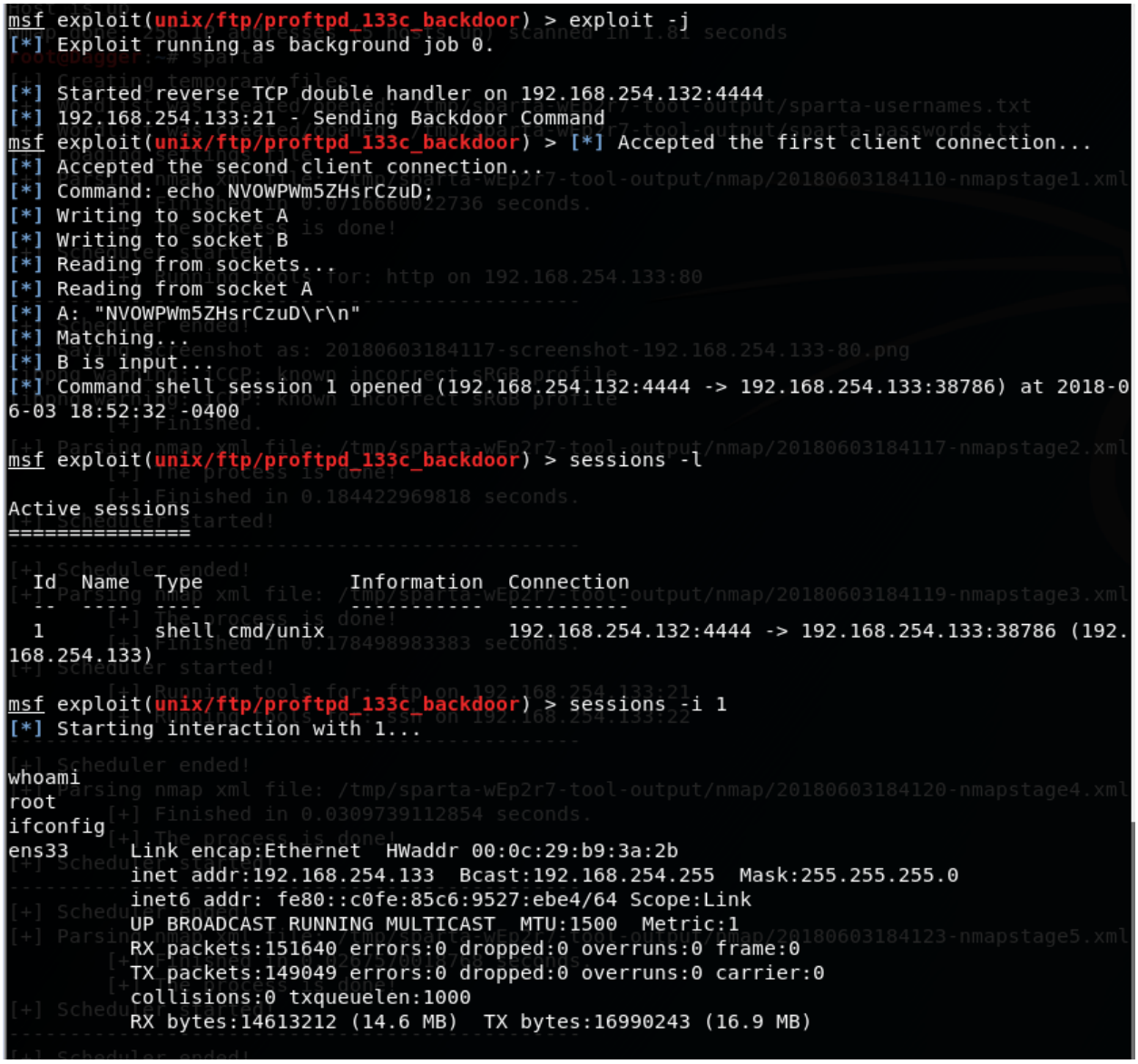


[Screenshot 10: Set the payload]



[Screenshot 11: Raincheck on the exploit and payload]

I ran the exploit in background and started interaction with the target machine as root.



[Screenshot 12: Execution of exploit and interaction with the target machine]

Thus, the objectives were met and this concludes this CTF task.

Additional Resources: This same task was done by JackkTutorials in a different way.
Link: https://www.youtube.com/watch?v=82S8wFSypB4