storm.malditainternet.com

Buscando formas de elevar privilegios en Windows – parte 1 (PowerSploit)

storm

4 minutos

Inicio > Miscs > Buscando formas de elevar privilegios en Windows – parte 1 (PowerSploit)

sábado, 14 de marzo de 2020

PowerSploit es una colección de módulos de Microsoft PowerShell que te facilita la vida al momento de hacer un pentest, y aca me voy a enfocar principalmente en buscar formas de ganar privilegios de administrador en un Windows (en el cuál ya tenemos un usuario no-administrador).

Lo primero, es bajar/subir el PowerSploit en la maquina victima.
Se puede descargar de aca: https://github.com/PowerShellMafia

/PowerSploit/

Creamos un directorio en la maquina victima, por ejemplo «C:\Temp\» y ahí copiamos el zip de PowerSploit y el unzip.exe (el unzip.exe lo tenés en Kali, o podes bajarlo de internet sin muchas vueltas).

Una vez copiaste ambos archivos, ejecuta lo siguiente:

```
1 powershell.exe -nop -exec bypass
```

De la documentacion de powershell:

> –Exec Bypass: to bypass/ignore the execution policy like Restricted which restricts the PowerShell scripts from running.
> –Nop / -Noprofile : to ignore the commands in the Profile file

Ya en la nueva session de powershell, hacemos:

```
1 C:\temp\unzip.exe C:\temp\PowerSploit-
  master.zip
```

```
2 CD C:\temp\PowerSploit-master\
```

Una vez ahí, importas el módulo de powersploit:

```
1 Import-Module C:\temp\PowerSploit-master
```

```
\PowerSploit
```

Con eso, ya tenés PowerSploit cargado.

Si queres ver todos los comandos que te habilita este módulo, podes ejecutar:

```
1 Get-Command -Module PowerSploit
```

El comando en particular que nos interesa, es ‘Invoke-AllChecks’, que básicamente ejecuta todos los chequeos que tiene el PowerSploit y genera un reporte.
La mejor forma de verlo, es ejecutar algo como:

```
1 PS C:\temp\PowerSploit-master\> Invoke-
  AllChecks
```

La salida va a ser algo similar a esto:

```
1 PS C:\temp\PowerSploit-master\> Invoke-
  AllChecks
```

```
3 [*] Running Invoke-AllChecks
```

```
5 [*] Checking if user is in a local group with
  administrative privileges...
```

```
7  [*] Checking for unquoted service paths...
```

```
8  [*] Use 'Write-UserAddServiceBinary' or
   'Write-CMDServiceBinary' to abuse
```

```
10 [+] Unquoted service path:
   ProcessExplorerService - C:\Program
   Files\procexp.exe
```

```
11 [+] Unquoted service path:
   ProcessMonitorService - C:\Program
   Files\Sysinternals\Process
   Monitor\Procmon.exe
```

```
13 [*] Checking service executable
   permissions...
```

```
14 [*] Use 'Write-ServiceEXE -ServiceName SVC'
   or 'Write-ServiceEXECMD' to abuse
```

```
16 [+] Vulnerable service executable:
   ProcessExplorerService - C:\Program
   Files\procexp.exe
```

```
18 [+] Vulnerable service executable:
   ProcessMonitorService - C:\Program
   Files\Sysinternals\Process
   Monitor\Procmon.exe

20 [*] Checking service permissions...

22 [*] Checking for unattended install files...

24 [*] Checking %PATH% for potentially
   hijackable .dll locations...

26 [*] Checking for AlwaysInstallElevated
   registry key...

28 [*] Checking for Autologon credentials in
   registry...

30 [*] Checking for encrypted web.config
   strings...

32 [*] Checking for encrypted application pool
   and virtual directory passwords...
```

En el reporte vas a poder ver un detalle de cada vector de ataque que PowerSploit encontró. Ejemplo:

> [+] Vulnerable service executable: ProcessExplorerService – C:\Program Files\procexp.exe

Ya en base a lo que encontres, vas a tener que proceder de diferentes formas, pero por ejemplo aca hay una guia de como elevar privilegios, usando un servicio mal configurado: https://www.harmj0y.net/blog/powershell/powerup-a-usage-guide/

Cheatsheet de PowerSploit: https://h4ck.co/wp-content/uploads/2017/11/PowerUp.pdf