storm.malditainternet.com

Buscando formas de elevar privilegios en Windows – parte 2 (Sherlock)

storm

3-4 minutos

Inicio > Miscs > Buscando formas de elevar privilegios en Windows – parte 2 (Sherlock)

domingo, 15 de marzo de 2020

Sherlock es un script de PowerShell que nos permite buscar rápidamente todo el software instalado en el equipo que esté sin actualizar y tenga vulnerabilidades conocidas, permitiéndonos de esta forma explotarlos para ganar privilegios de administrador.

La ventaja de Sherlock es que es un único script, por lo tanto con copiar/descargar un archivo ya estás listo.

El script se puede descargar de aca: https://github.com/rastamouse/Sherlock

Una vez que lo copiaste a la maquina víctima, tenés que ejecutar:

```
C:\Temp> powershell.exe -nop -exec bypass
PS C:\Temp> Import-Module .\Sherlock.ps1
PS C:\Temp> Find-AllVulns
```

Y eso te va a dar un reporte similar a este:

```
Title      : User Mode to Ring (KiTrap0D)
MSBulletin : MS10-015
CVEID      : 2010-0232
Link       : https://www.exploit-db.com/exploits
/11199/
VulnStatus : Not supported on 64-bit systems

Title      : Task Scheduler .XML
MSBulletin : MS10-092
CVEID      : 2010-3338, 2010-3888
Link       : https://www.exploit-db.com/exploits
/19930/
VulnStatus : Appears Vulnerable
```

```
Title      : NTUserMessageCall Win32k Kernel Pool
Overflow
MSBulletin : MS13-053
CVEID      : 2013-1300
Link       : https://www.exploit-db.com/exploits
/33213/
VulnStatus : Not supported on 64-bit systems

Title      : TrackPopupMenuEx Win32k NULL Page
MSBulletin : MS13-081
CVEID      : 2013-3881
Link       : https://www.exploit-db.com/exploits
/31576/
VulnStatus : Not supported on 64-bit systems

Title      : TrackPopupMenu Win32k Null Pointer
Dereference
MSBulletin : MS14-058
CVEID      : 2014-4113
Link       : https://www.exploit-db.com/exploits
/35101/
```

```
VulnStatus : Not Vulnerable

Title      : ClientCopyImage Win32k
MSBulletin : MS15-051
CVEID      : 2015-1701, 2015-2433
Link       : https://www.exploit-db.com/exploits
/37367/
VulnStatus : Appears Vulnerable

Title      : Font Driver Buffer Overflow
MSBulletin : MS15-078
CVEID      : 2015-2426, 2015-2433
Link       : https://www.exploit-db.com/exploits
/38222/
VulnStatus : Not Vulnerable

Title      : 'mrxdav.sys' WebDAV
MSBulletin : MS16-016
CVEID      : 2016-0051
Link       : https://www.exploit-db.com/exploits
/40085/
```

```
VulnStatus : Not supported on 64-bit systems

Title      : Secondary Logon Handle
MSBulletin : MS16-032
CVEID      : 2016-0099
Link       : https://www.exploit-db.com/exploits
/39719/
VulnStatus : Not Supported on single-core systems

Title      : Windows Kernel-Mode Drivers EoP
MSBulletin : MS16-034
CVEID      : 2016-0093/94/95/96
Link       : https://github.com/SecWiki/windows-
kernel-exploits/tree/master/MS1
             6-034?
VulnStatus : Not Vulnerable

Title      : Win32k Elevation of Privilege
MSBulletin : MS16-135
CVEID      : 2016-7255
Link       : https://github.com/FuzzySecurity
```

```
/PSKernel-Primitives/tree/master/S
             ample-Exploits/MS16-135
VulnStatus : Not Vulnerable

Title      : Nessus Agent 6.6.2 - 6.10.3
MSBulletin : N/A
CVEID      : 2017-7199
Link       : https://aspe1337.blogspot.co.uk
/2017/04/writeup-of-cve-2017-7199.h
             tml
VulnStatus : Not Vulnerable
```