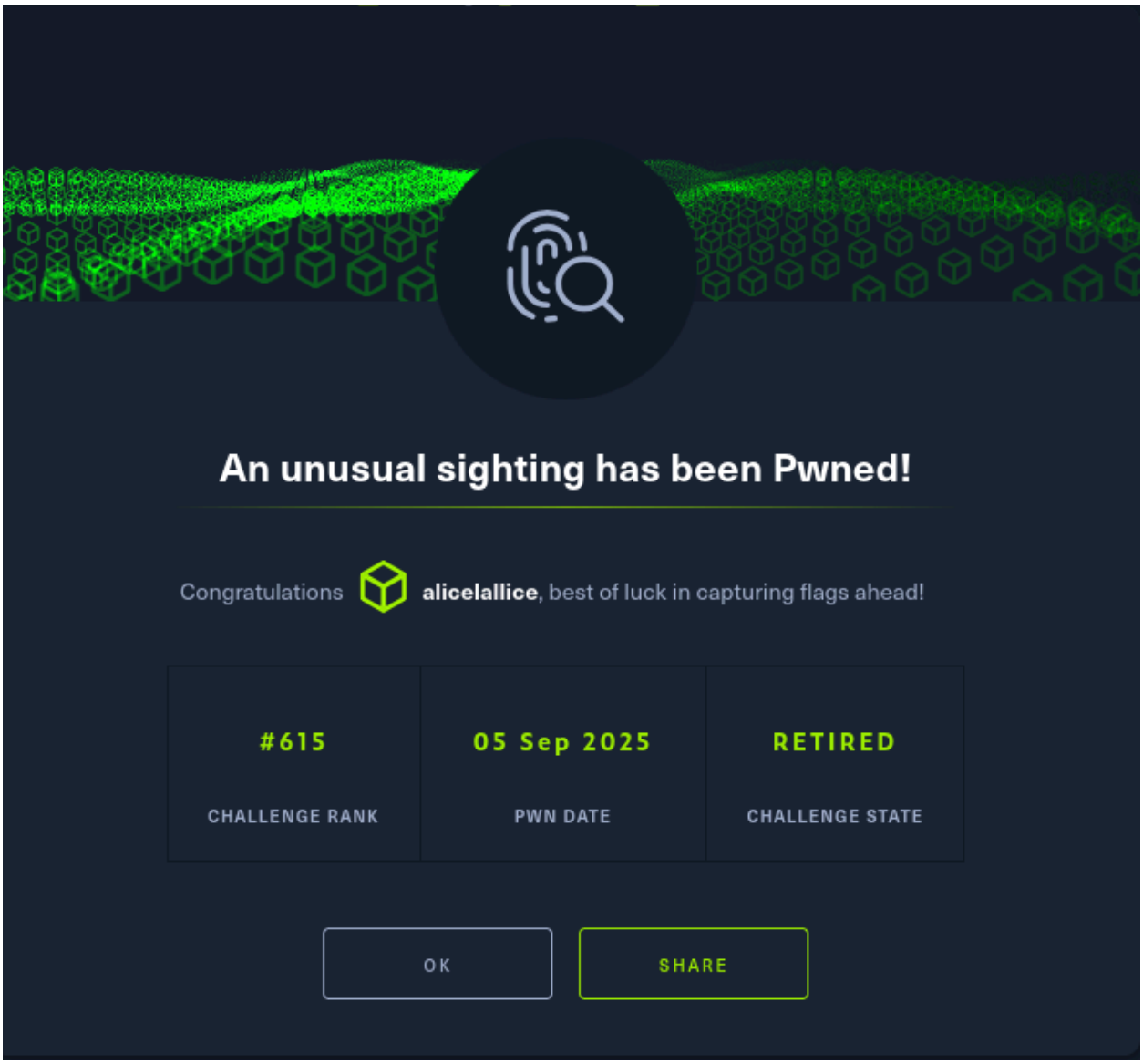
An unusual sighting

Types	forensic
CTF	HTB



```
What is the IP Address and Port of the SSH Server (IP:PORT)
> 100.107.36.130:2221
[+] Correct!
```

```
[2024-02-13 11:29:50] Connection from 100.81.51.199 port 63172 on 100.107.36.130 port 2221 rdomain "
"
```

```
What time is the first successful Login

> 2024-02-13 11:29:50
[+] Correct!
```

```
What is the Fingerprint of the attacker's public key

> OPkBSs6okUKraq8pYo4XwwBg55QSo210F09FCe1-yj4
[+] Correct!
```

```
[2024-02-19 04:00:14] Failed publickey for root from 2.67.182.119 port 60071 ssh2: ECDSA SHA256:OPkB
Ss6okUKraq8pYo4XwwBg55QSo210F09FCe1-yj4
```

all this we can see on sshd.log

```
What is the first command the attacker executed after logging in
> whoami
[+] Correct!
```

```
[2024-02-19 04:00:18] whoami
```

from bash_history.txt

```
What is the final command the attacker executed before logging out

> ./setup
[+] Correct!

[+] Here is the flag: HTB{4n_unusual_s1ght1ng_1n_SSH_l0gs!}
```

```
[2024-02-19 04:14:02] ./setup
```

```
HTB{4n_unusual_s1ght1ng_1n_SSH_l0gs!}
```

Step-by-Step Guide: How to Read SSH Logs

🔷 1. Understand the Log Format

SSH logs typically follow this structure:

Code

`[YYYY-MM-DD HH:MM:SS] <log message>`

Each line includes:

- **Timestamp**: When the event occurred
- **Message**: What happened (connection, authentication, command, etc.)

Example:

Code

`[2024-02-19 04:00:14] Accepted password for root from 2.67.182.119 port 60071 ssh2`

🔷 2. Identify Key Event Types

Here are the most common log messages and what they mean:

🔍 Log Message Type	🧩 Meaning
`Server listening on ...`	SSH service started and is ready
`Connection from <IP>`	Someone tried to connect
`Failed publickey/password for ...`	Authentication attempt failed
`Accepted password for ...`	Successful login
`Starting session: shell ...`	Shell session began
`Disconnected from user ...`	User logged out or session ended

🔷 3. Track a Full Session

To analyze a full login session, follow this sequence:

1. **Connection initiated**

   Code

   `Connection from 2.67.182.119 port 60071`

2. **Authentication attempts**

   Code

   `Failed publickey for root ...`
   `Accepted password for root ...`

3. **Session start**

   Code

   `Starting session: shell on pts/2 ...`

4. **Commands executed** (from `bash_history.txt`)

   Code

   `whoami`
   `uname -a`
   `./setup`

5. **Session end**

   Code

   `Disconnected from user root ...`

🔷 4. Spot Suspicious Behavior

Look for patterns that stand out:

- **Unusual login times** (e.g. 04:00 AM)
- **Rare IP addresses** (only appear once)
- **Use of `root` account**
- **Failed logins followed by success**
- **Commands like `wget`, `shred`, `setup`**—often used in attacks

🔷 5. Correlate with Bash History

If you have access to `bash_history.txt`, match timestamps with logins to see what the user did after logging in.

Example:

Code

```
[2024-02-19 04:00:14] Accepted password for root ...
[2024-02-19 04:00:18] whoami
[2024-02-19 04:14:02] ./setup
```

This shows the attacker logged in, checked privileges, downloaded a file, and ran a setup script.