VishwaCTF

CHALLENGE NAME : DATESLIP LOGS

DEV : ANANYA BISHT

CATEGORY : DIGITAL FORENSICS

LEVEL : EASY

2025

Question Description:

While reviewing the logs, one login stands out—strangely familiar yet misplaced. The date seems off. Dig deeper into the records from the start of the year, and you'll uncover what doesn't belong.

Given-->

auth.log file will be given

Solution:

Step 1:

After reading the question title and description well, you will realize the few given hints-

1. **Anomaly in the dates**
2. **Start of the year come centric towards January, February and March or at max April.**

Step 2:

Review the Log File

Now that we have some direction, we need to examine the log file closely. You can do this manually or with terminal commands. Here, using terminal commands will be much faster and more efficient.

Do so for the required months, here's Feb, a step closer to our answer.

Terminal Command (Linux/macOS):

bash Copy Edit

```
grep "Feb" /path/to/auth.log
```

This will filter out all log entries that mention "Feb," making it easier to spot anything unusual.

Terminal Command (Windows PowerShell):

powershell Copy Edit

```
Select-String "Feb" "C:\path\to\auth.log"
```

Step 3:

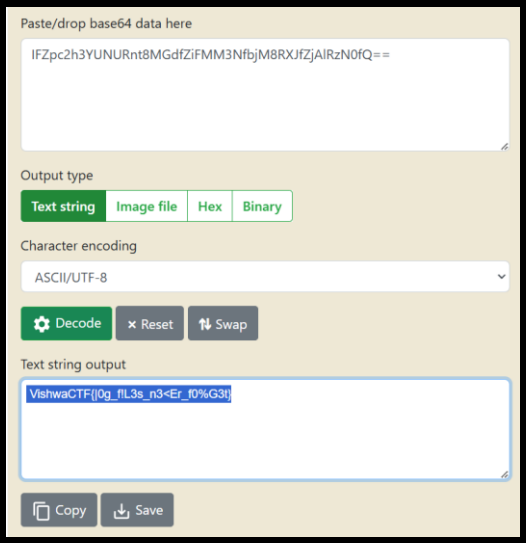
Look for any irregularities in the dates. Anomalies like "Feb 64" will stand out as strange, since February can never have 64 days.

```
PS C:\Users\ANANYA_BISHT> Select-String "Feb" "D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log"

D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:16:Feb 15 00:00:00 2024 server sshd[9574]: Connection
closed by testuser from 203.0.113.8 port 7476 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:31:Feb 28 00:00:00 2024 server sshd[6056]: Failed
password for guest from 172.16.3.12 port 7555 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:38:Feb 07 00:00:00 2024 server sshd[3728]: Invalid user
backup from 172.16.44.2 port 7608 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:50:Feb 29 00:00:00 2024 server sshd[4361]: Connection
closed by backup from 192.168.5.6 port 4704 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:53:Feb 04 00:00:00 2024 server sshd[6076]: Accepted
password for testuser from 172.16.3.12 port 7490 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:69:Feb 11 00:00:00 2024 server sshd[4291]: Connection
closed by webadmin from 192.168.1.50 port 9697 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:75:Feb 07 00:00:00 2024 server sshd[2105]: Failed
password for admin from 172.16.44.2 port 6892 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:80:Feb 21 00:00:00 2024 server sshd[5740]: Accepted
password for researcher from 172.16.44.2 port 4904 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:96:Feb 08 00:00:00 2024 server sshd[8602]: Failed
password for admin from 10.10.1.1 port 1623 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:103:Feb 27 00:00:00 2024 server sshd[8405]: Failed
password for backup from 198.51.100.9 port 8285 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:107:Feb 01 00:00:00 2024 server sshd[1448]: Accepted
password for guest from 203.0.113.8 port 4276 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:115:Feb 03 00:00:00 2024 server sshd[5105]: Accepted
password for admin from 203.0.113.8 port 9863 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:170:Feb 27 00:00:00 2024 server sshd[1829]: Accepted
password for testuser from 198.51.100.9 port 1123 ssh2
.                                                                .
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:181:Feb 22 00:00:00 2024 server sshd[3816]: Connection
closed by root from 10.10.1.1 port 8962 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:187:Feb 29 00:00:00 2024 server sshd[1974]: Invalid
user researcher from 10.10.1.1 port 7525 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:201:Feb 02 00:00:00 2024 server sshd[8293]: Accepted
password for admin from 192.168.5.6 port 1770 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:213:Feb 19 00:00:00 2024 server sshd[3023]: Connection
closed by guest from 172.16.44.2 port 6928 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:215:Feb 14 00:00:00 2024 server sshd[7185]: Accepted
password for root from 172.16.44.2 port 5642 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:216:Feb 25 00:00:00 2024 server sshd[2844]: Failed
password for admin from 172.16.44.2 port 5529 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:232:Feb 08 00:00:00 2024 server sshd[7996]: Failed
password for webadmin from 172.16.44.2 port 9402 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:237:Feb 64 13:00:50 2025 server sshd[14102]:Invalid
user IFZpc2h3YUNURnt8MGdfZiFMM3NfbjM8RXJfZjAlRzN0fQ==
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:244:Feb 23 00:00:00 2024 server sshd[8548]: Connection
closed by testuser from 198.51.100.9 port 5636 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:252:Feb 01 00:00:00 2024 server sshd[1283]: Invalid
user webadmin from 198.51.100.9 port 3997 ssh2
D:\COLLEGE\SEM4\cybercell\forensics\log file analysis\auth.log:284:Feb 13 00:00:00 2024 server sshd[4179]: Failed
password for developer from 10.10.1.1 port 4787 ssh2
```

Step 4:

Now we have Identified the only anomaly of **"Feb 64"** along with an encoded string.



So, on instinct we know the popular base64 encoders-decoders from the record and we try it out.

https://www.rapidtables.com/web/tools/base64-decode.html?base64=IFZpc2h3YUNURnt8MGdfZiFMM3NfbjM8RXJfZjAlRzN0fQ==

Input = IFZpc2h3YUNURnt8MGdfZiFMM3NfbjM8RXJfZjAlRzN0fQ==

Output = VishwaCTF{|0g_f!L3s_n3<Er_f0%G3t}

Enter this flag on the platform and get your points!