Telly

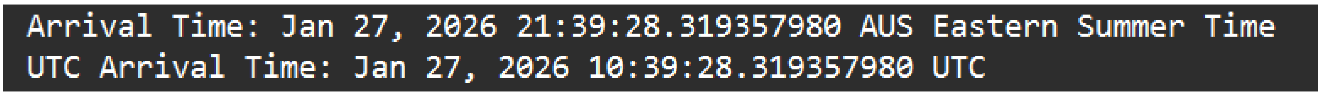
Task 1

CVE-2026-24061 - https://www.safebreach.com/blog/safebreach-labs-root-cause-analysis-and-poc-exploit-for-cve-2026-24061/

- Attackers can establish telnet connection without providing valid credentials
- Environment variable USER can be controlled by the user through telnet protocol

Task 2

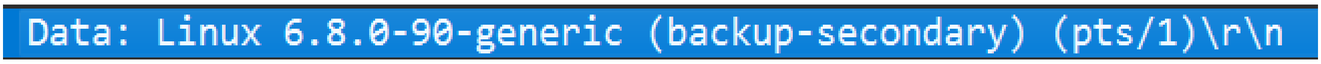
Answer in packet 52 under frame header



```
Arrival Time: Jan 27, 2026 21:39:28.319357980 AUS Eastern Summer Time
UTC Arrival Time: Jan 27, 2026 10:39:28.319357980 UTC
```

Task 3

From my knowledge hostname can be identified in login banner from telnet server which is usually sent before the welcome page/message. Hostname can be found in packet 57 of file.



```
Data: Linux 6.8.0-90-generic (backup-secondary) (pts/1)\r\n
```

Task 4

Upon scrolling though next telnet packets you can see following commands in packet 2452.

```
sudo useradd -m -s /bin/bash cleanupsvc; echo "cleanupsvc:YouKnowWhoiam69" |
sudo chpasswd
```

I can see the username and password being printed and added:

- useradd - creates new user account
- echo - prints username and password
- chpasswd - sets the password

Task 5

Packet 3968 tells you the link to the script and the packets before will provide letters to the command which spells out wget. Wget is often used in Linux for downloading file from the web.

Task 6

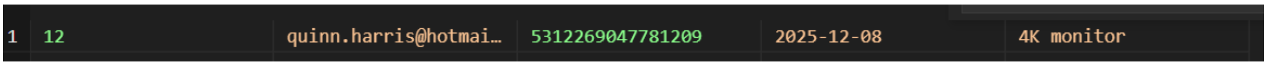
IP address can be found on packet 6416

Task 7

Scrolling through telnet packets will lead to a get command on credit card database in this format:

```
GET /credit-cards-25-blackfriday.db HTTP/1.1" 200
```

Task 8

1. On Wireshark go file> export objects> http...
2. Select database file and save it
3. Open the file using visual studio code with sqlite editor extension
   
   ```
   1  12                  quinn.harris@hotmai…  5312269047781209  2025-12-08  4K monitor
   ```
   Use find function to locate Quinn Harris.

https://labs.hackthebox.com/achievement/sherlock/2343373/1144

Attack Summary

The attacker obtained initial access by exploiting the Telnet vulnerability **CVE-2026-24061**, allowing unauthenticated root access to the server without valid credentials. To establish persistence, the attacker created a new user account on the system. Following this, the attacker exfiltrated a credit card database containing purchase details, customer email addresses, transaction dates, and stored credit card numbers.