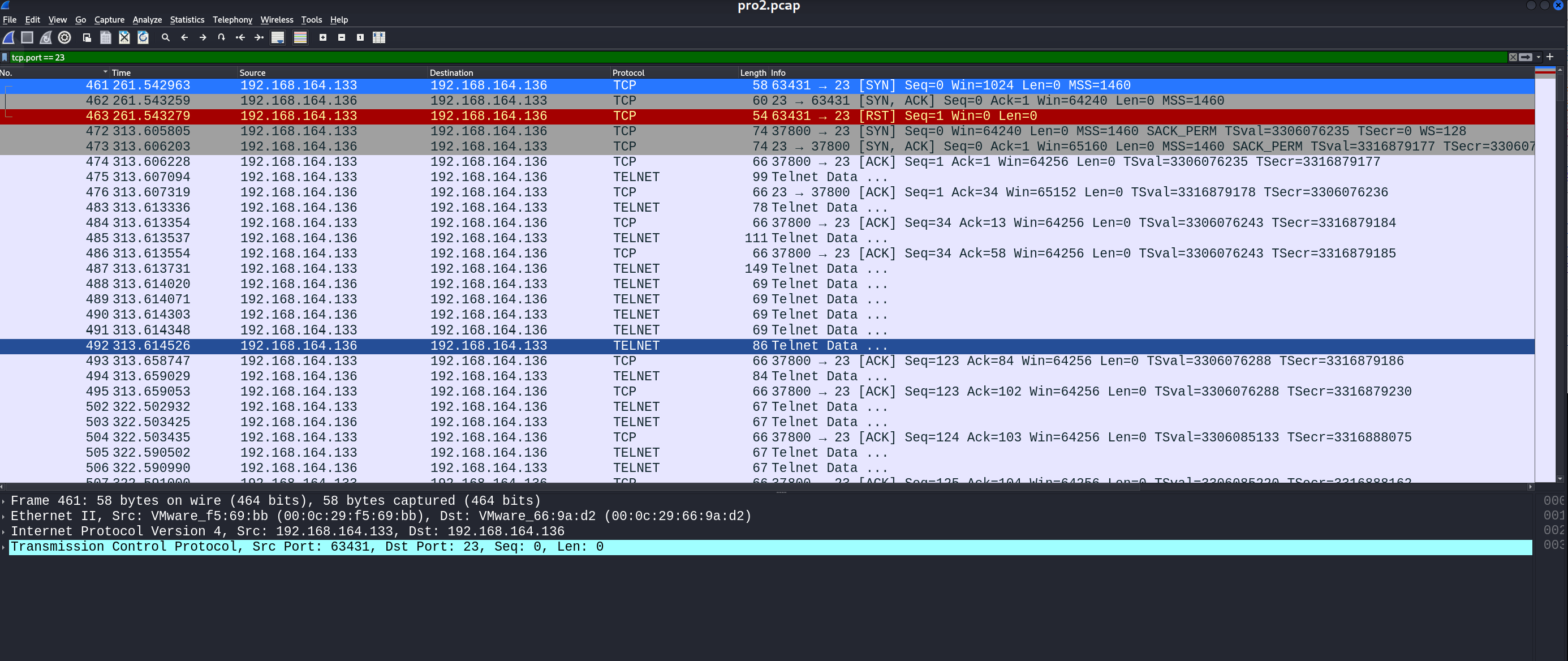
### **Stage 3 Report: Analysis of Captured Traffic and Logs in Telnet Attack**

#### **1. Analyzing the Captured Traffic with Wireshark**

##### **Step 1.1: Capturing the Traffic**

* **Tool Used**: Wireshark
* Start Wireshark on the Kali Linux (attacker) machine and select the appropriate network interface (e.g., eth0 or wlan0) to capture traffic.
* Apply a filter to capture only Telnet traffic by using the following Wireshark filter:



* I used the command “tcp.port == 23” to filter any traffic that didn’t include port 23 open
* Begin capturing traffic and save the capture file as pro2.pcap for analysis.

##### **Step 1.2: Inspecting the Captured Telnet Traffic**

* Open the pro2.pcap file in Wireshark.
* Look for the following:
  + **Initial Connection**: Identify the TCP handshake (SYN, ACK packets) between the attacker (Kali Linux) and the victim (Ubuntu) on port 23.
  + **Telnet Authentication**: Locate the Telnet login sequence, which will contain the username and password sent in plaintext.
  + **Command Execution**: Observe the commands executed by the attacker once the login is successful.

##### **Step 1.3: Reconstructing the TCP Stream**

* Right-click on a Telnet packet and select “**Follow** > **TCP Stream**” to see the entire raw data exchanged between the attacker and victim.



* This will show the entire Telnet session, including the login credentials and commands executed.
* Document any **malicious commands** or suspicious activity identified in the session.

##### **Step 1.4: Using Hex Tools for Data Analysis**

* If the captured data contains suspicious software or malicious payloads, open the raw data in a **Hex editor** such as **HxD** (Windows) or **Hex Fiend** (macOS).
* Look for **hexadecimal patterns** that could indicate an executable file or payload (such as a virus or script).
* Note down any unusual code or data that could have been transferred during the Telnet session.

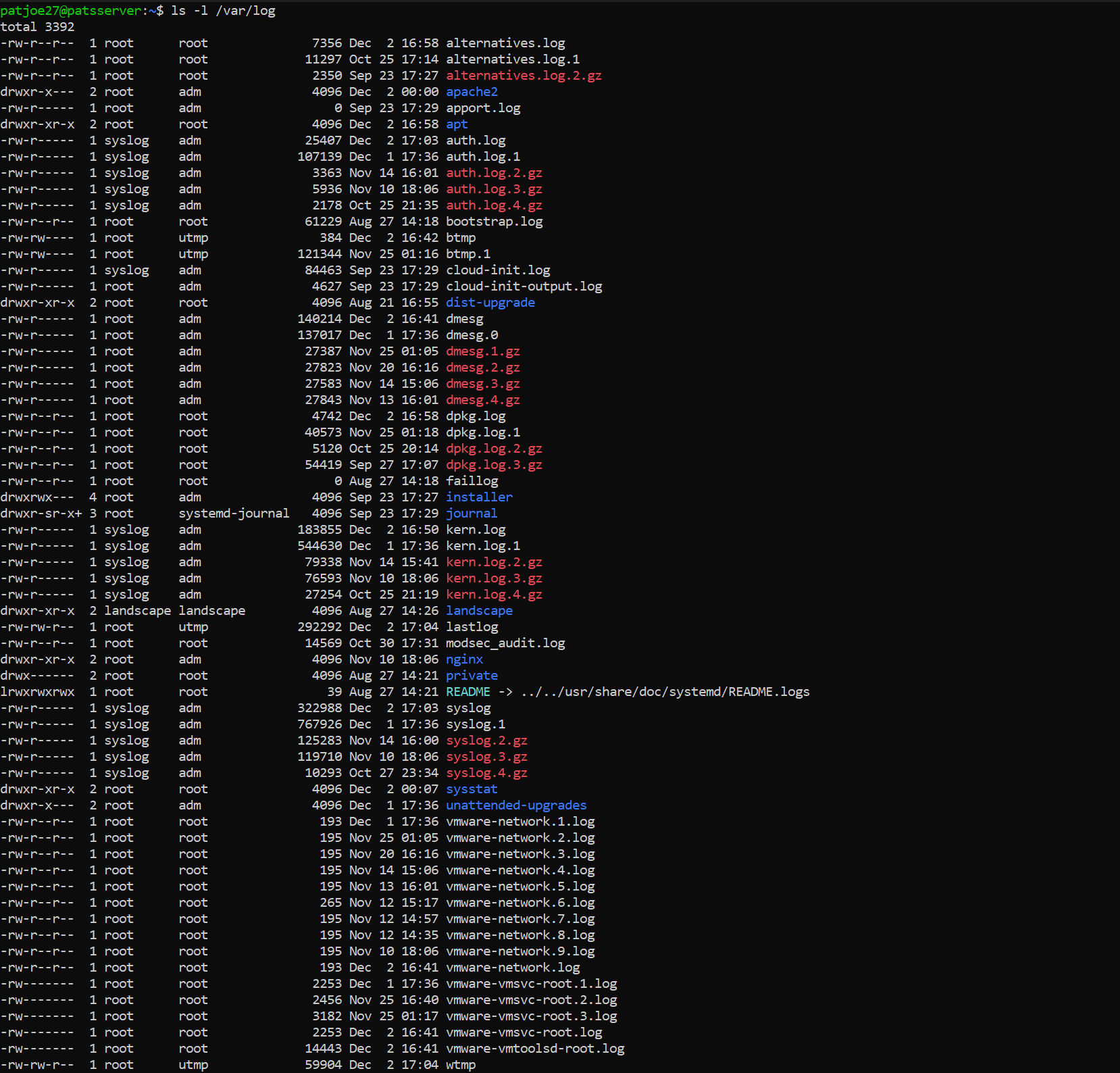
##### **Step 1.5: Decoding Data with Notepad++**

* If the data captured appears to be encoded (e.g., base64 encoded), use **Notepad++** with the appropriate plugin (e.g., Base64 Decode).
* Decode any suspicious encoded payload or script and analyze it for malicious intent.

#### **2. Analyzing the Log Files on the Victim Machine (Ubuntu)**

##### **Step 2.1: Locating the Log Files**

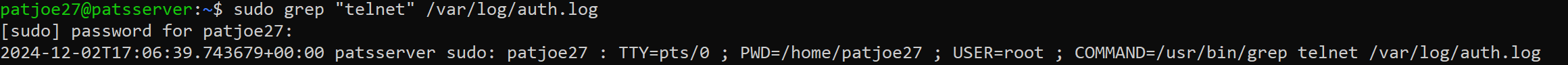
* On the victim machine (Ubuntu), use the following command to list the logs:

ls -l /var/log  


* Identify key log files such as:
  + **auth.log**: Contains authentication details, including Telnet login attempts.
  + **syslog**: General system logs, including Telnet service and system activity.

##### **Step 2.2: Analyzing Authentication Logs**

* Use the grep command to search for Telnet-related entries in the authentication logs:



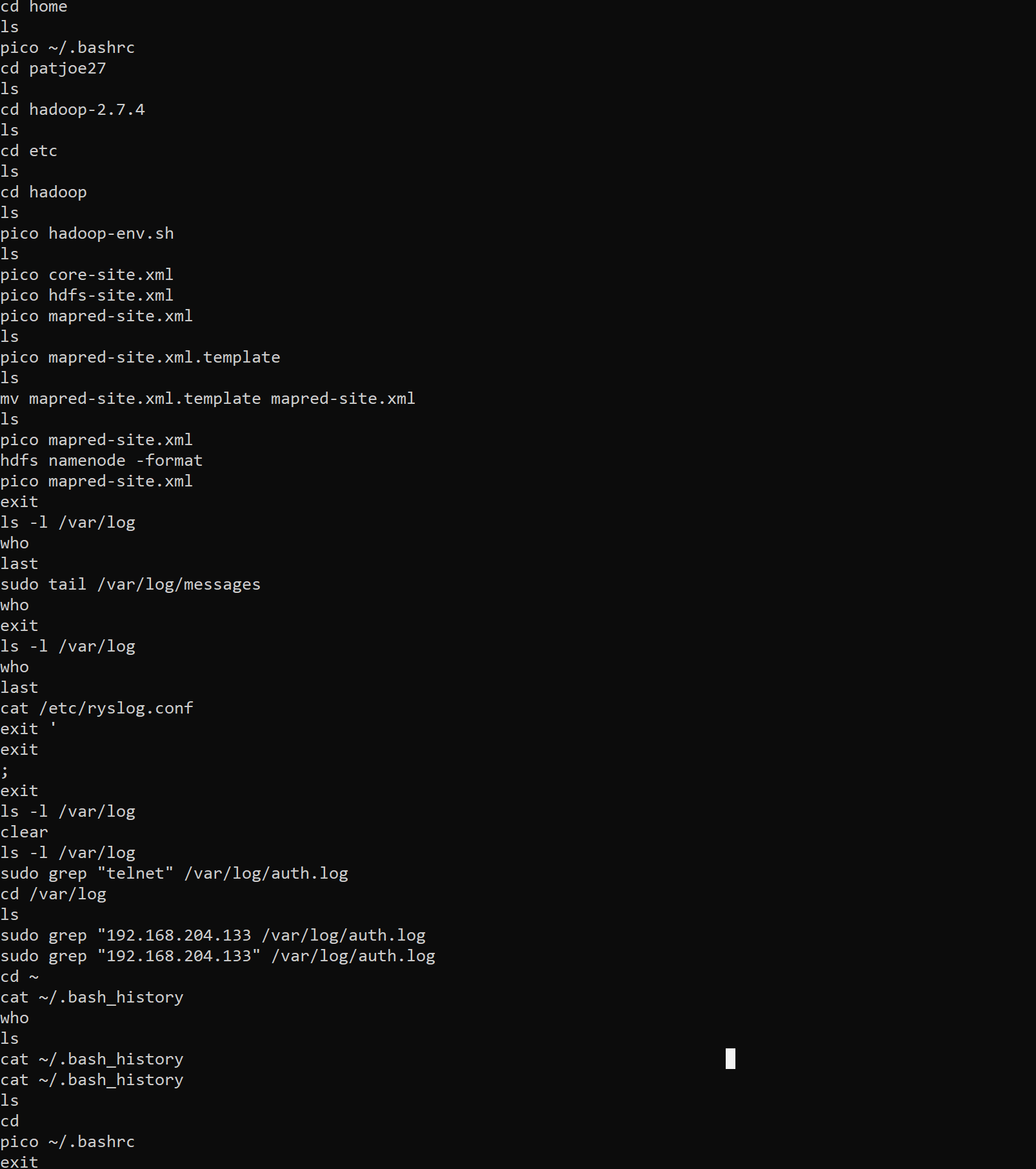
sudo grep "telnet" /var/log/auth.log

* Look for log entries that show the attacker’s IP address (Kali Linux: 192.168.164.133) and any login attempts or successful logins. Example of log entries:

Jan 1 10:01:01 victim-machine telnetd[1234]: Connection from 192.168.164.133  
Jan 1 10:02:00 victim-machine telnetd[1234]: Login from 192.168.164.133 with user "attacker"

##### **Step 2.3: Checking for Executed Commands**

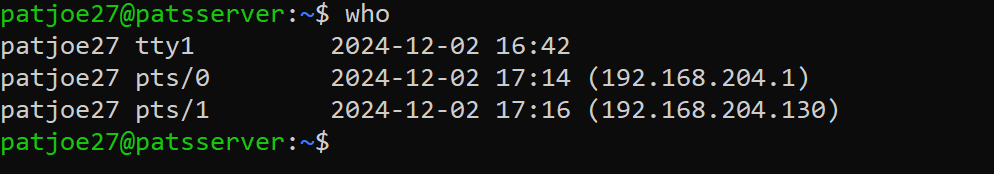
* Check the .bash\_history file for any commands executed by the attacker:



* List any suspicious commands or unauthorized actions performed by the attacker.

##### **Step 2.4: Identifying Logged-in Users**

* Use the who command to identify logged-in users:



* Verify that the attacker’s IP address appears in the logged-in user list, indicating they are still connected to the victim machine.

#### **3. Advanced Log Analysis with Splunk (Optional)**

##### **Step 3.1: Importing Logs into Splunk**

* Import the log files (such as auth.log and syslog) into **Splunk** for more advanced analysis.
* Create an index in Splunk for easier searching.

##### **Step 3.2: Searching for Telnet Connections**

* Use the following Splunk search query to filter Telnet-related logs:

index=ubuntu\_logs sourcetype=syslog "telnet"  
index=ubuntu\_logs sourcetype=auth "192.168.164.133"

* These queries will help you pinpoint Telnet connection attempts and filter logs related to the attacker's IP address.