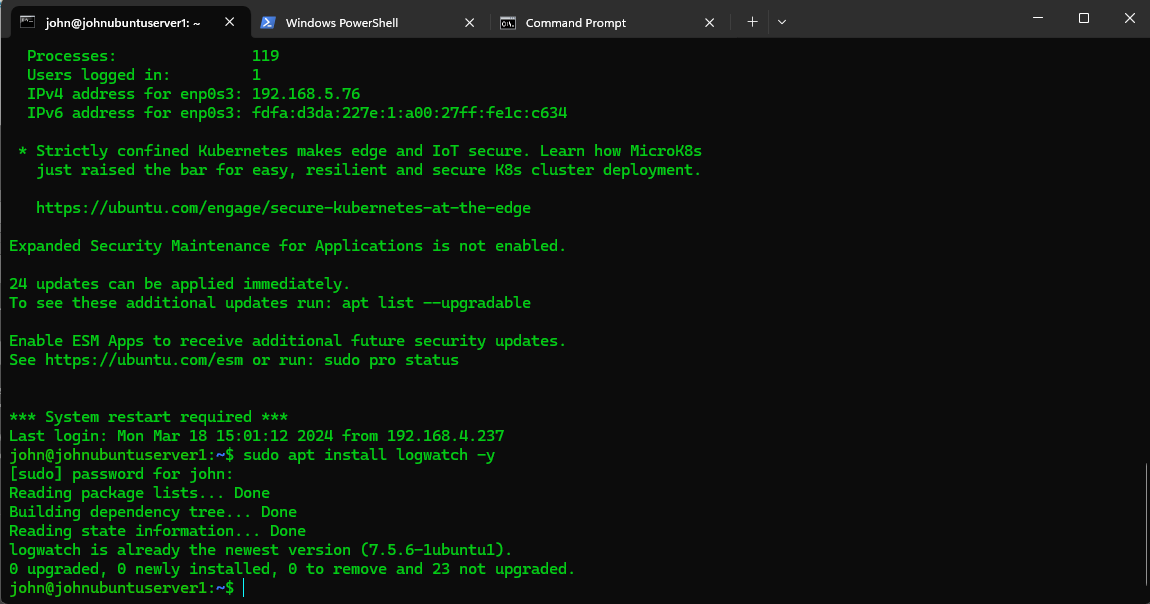
**Log Watch Lab**

EXERCISE 4 – Installing Logwatch

sudo apt install logwatch -y

Using the Advanced Package Tool install the Logwatch application.

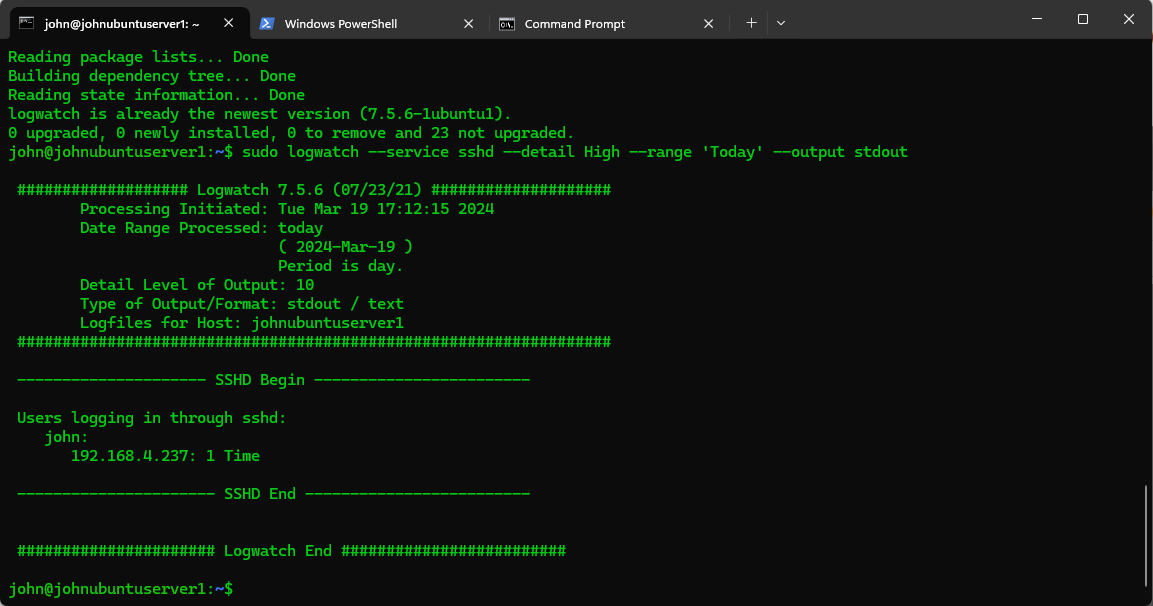


EXERCISE 5 – Basic service usage

Create a Detailed Report for a Specific Service

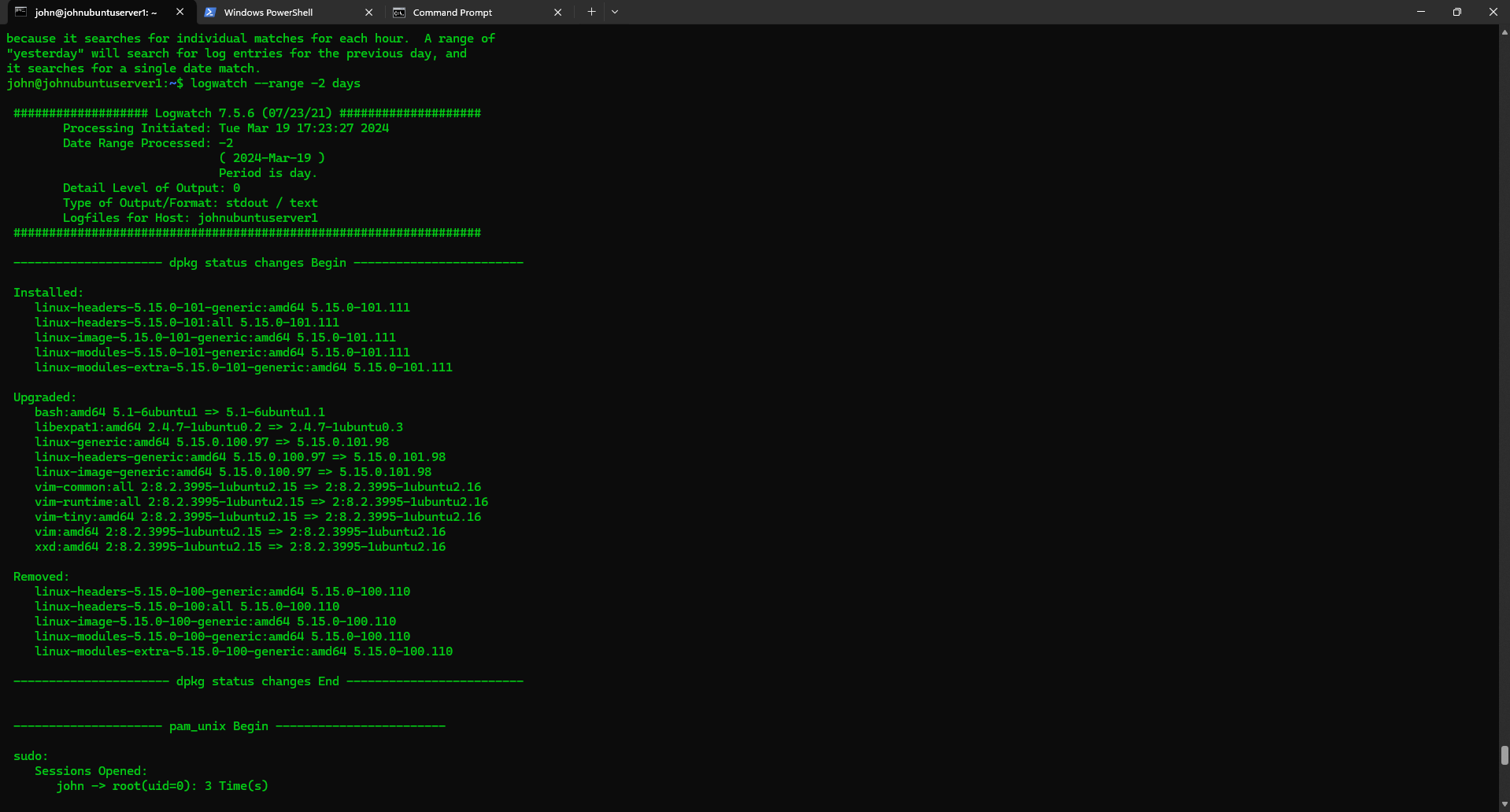
To focus on a particular service, such as SSH, and get more detailed information, you can adjust the detail level and specify the service of interest.

sudo logwatch --service sshd --detail High --range 'Today' --output stdout

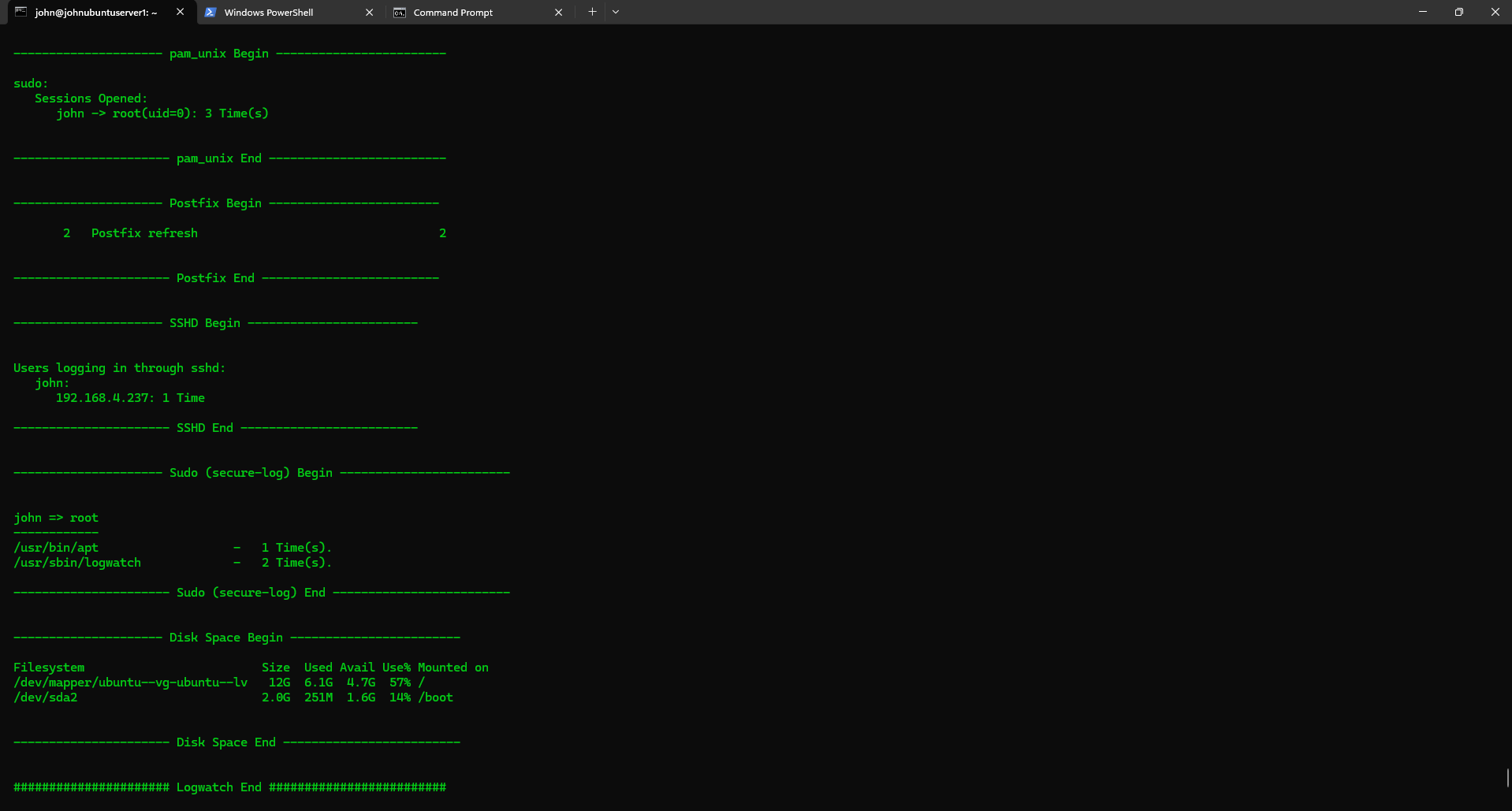


EXERCISE 6 – Examining logs over certain date ranges

Purpose: Examining logs over certain date ranges is crucial for pinpointing issues or detecting security threats in a system. Adjusting the detail level lets you tailor the report's verbosity, enabling focused and efficient log review.

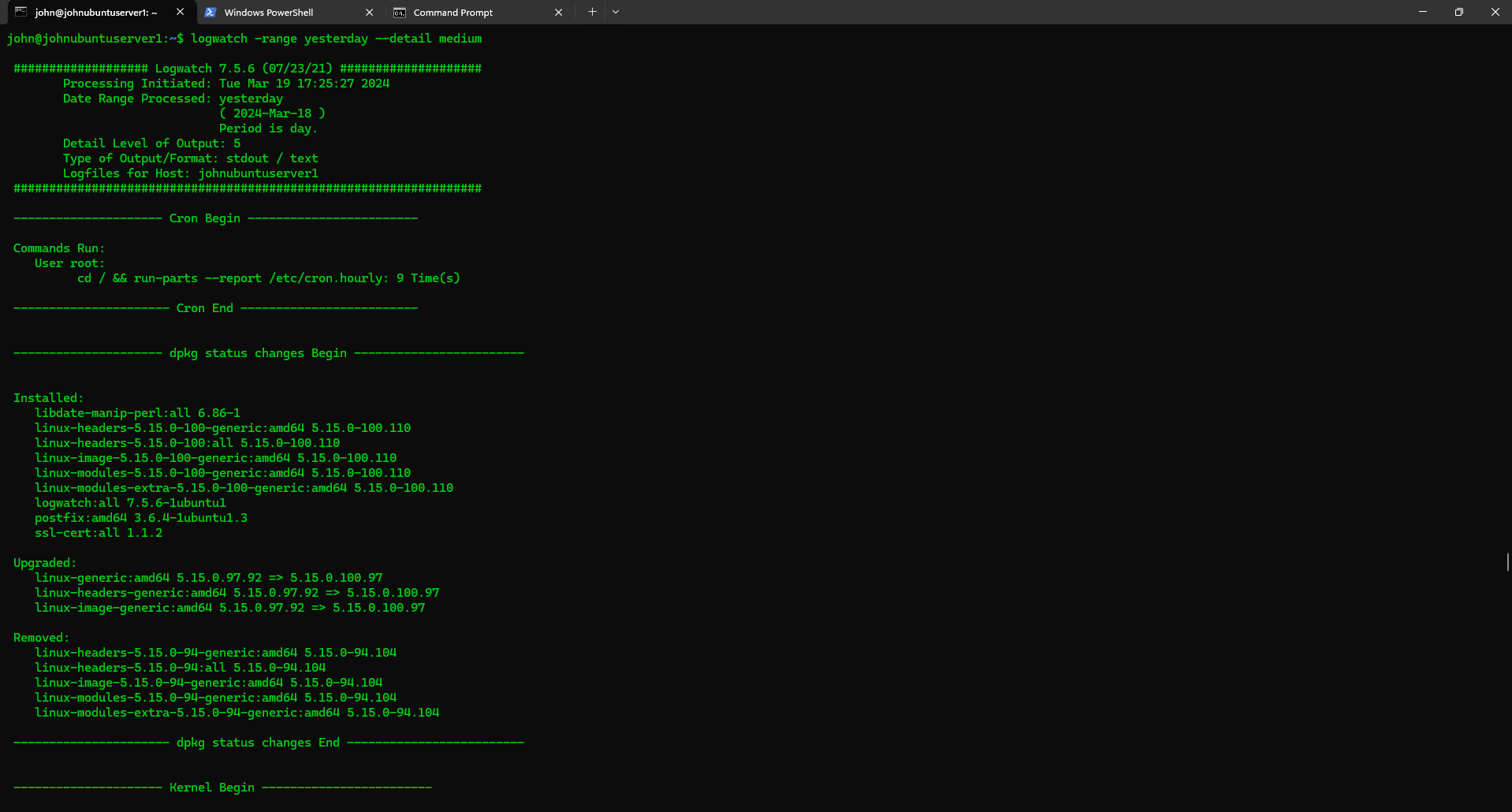


The following command was run in order to retrieve linux log data from two days ago: logwatch \_--range 2 days

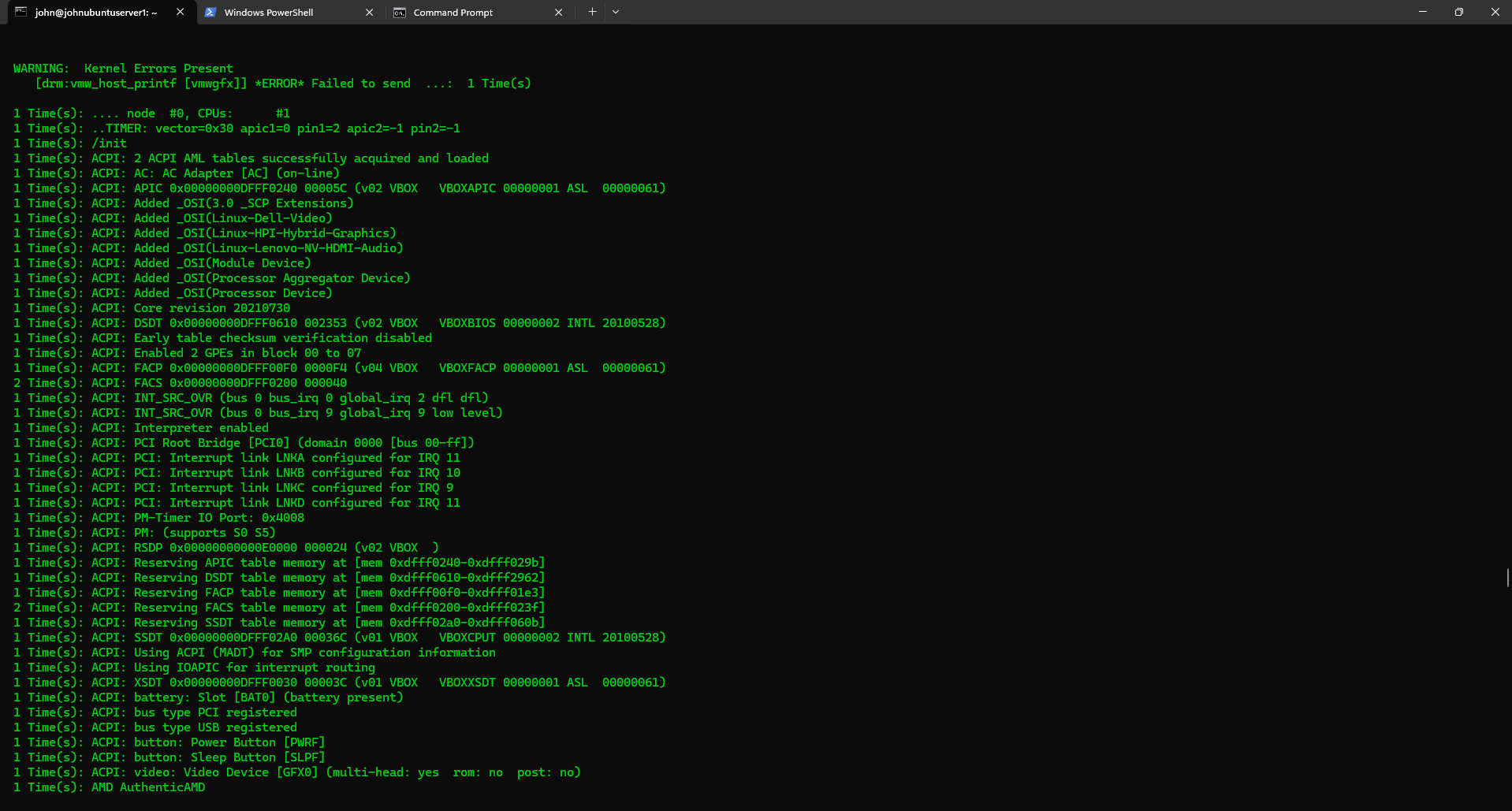


Basic information from this log data are the following:

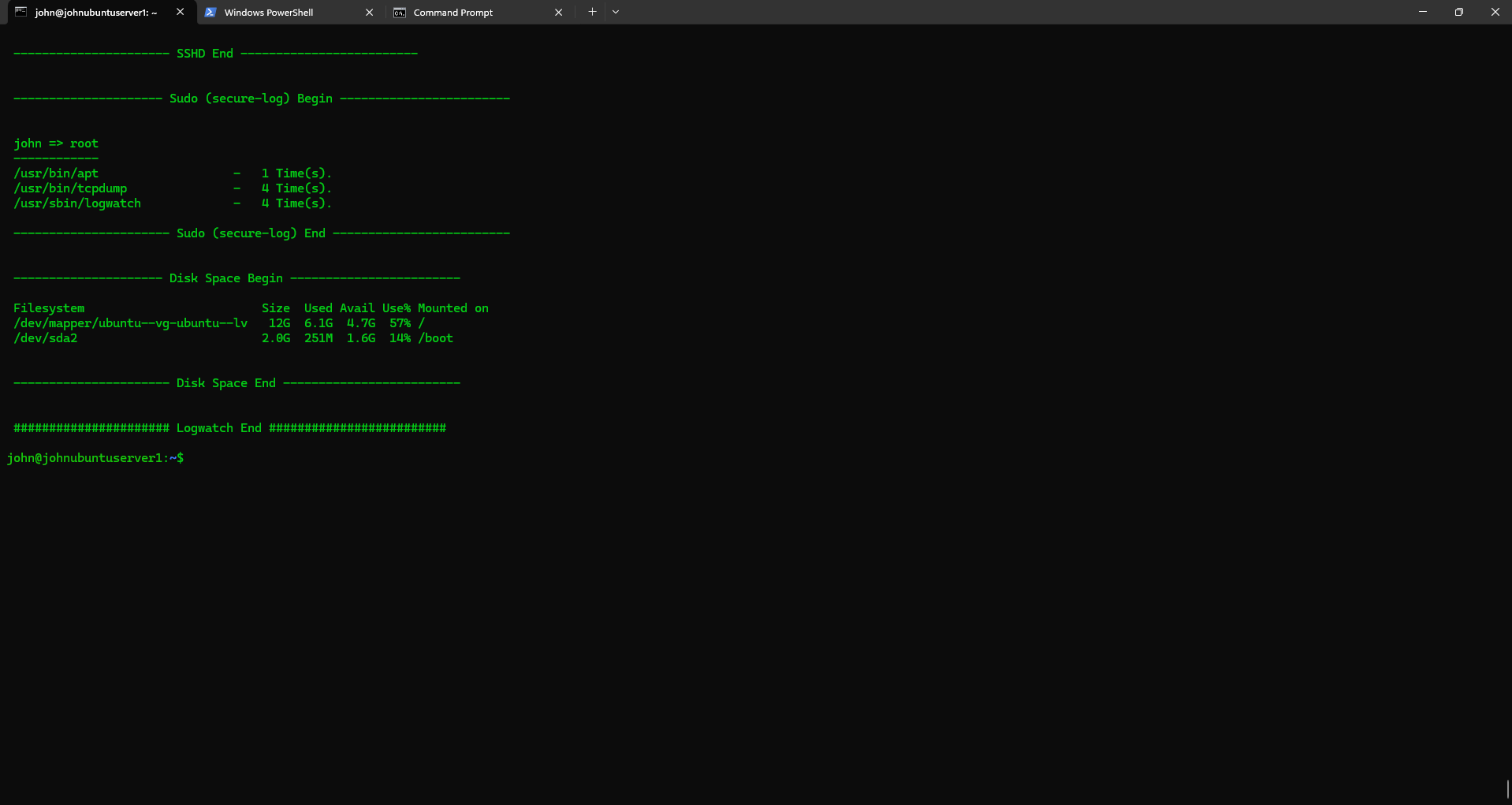
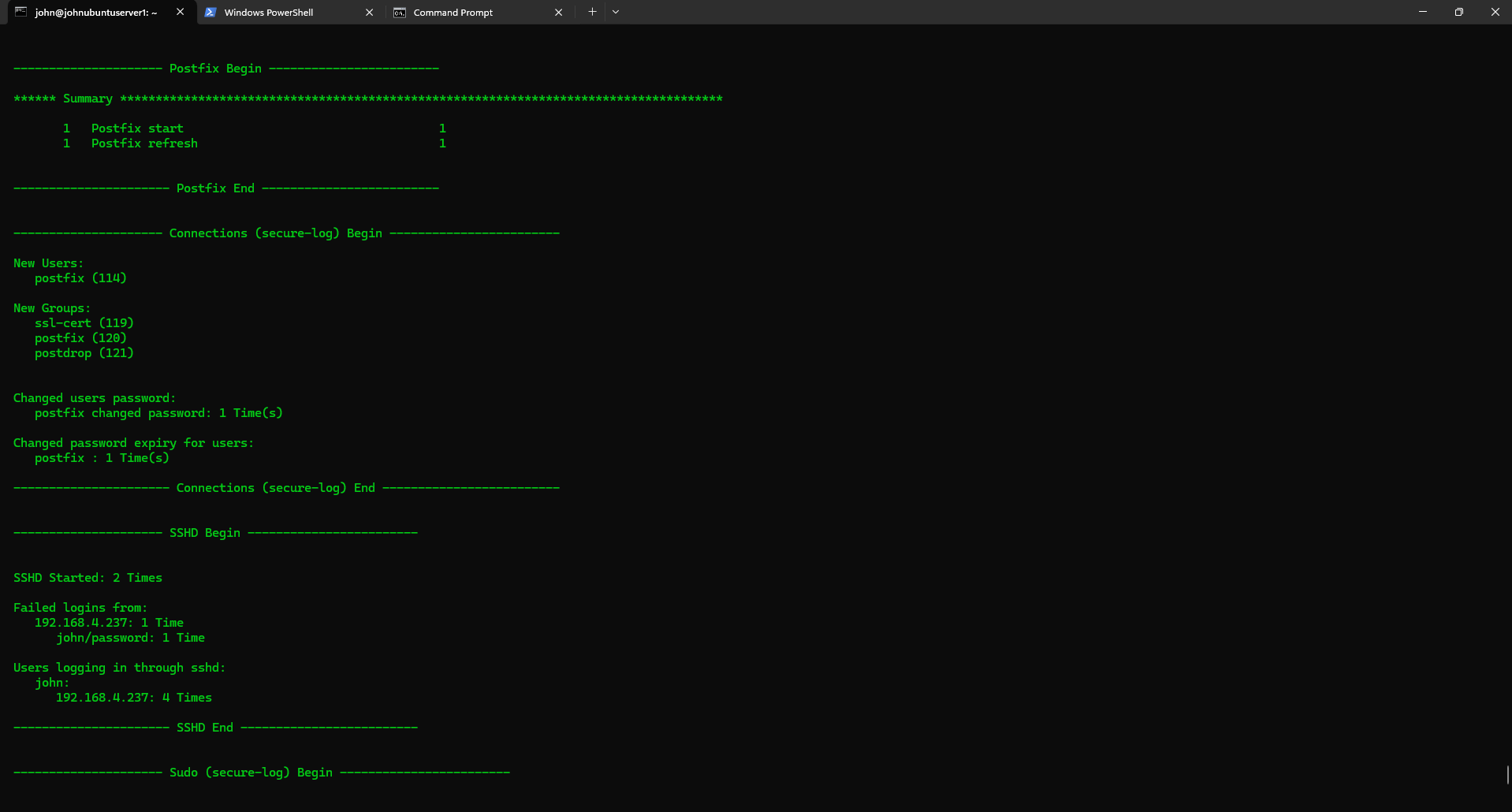
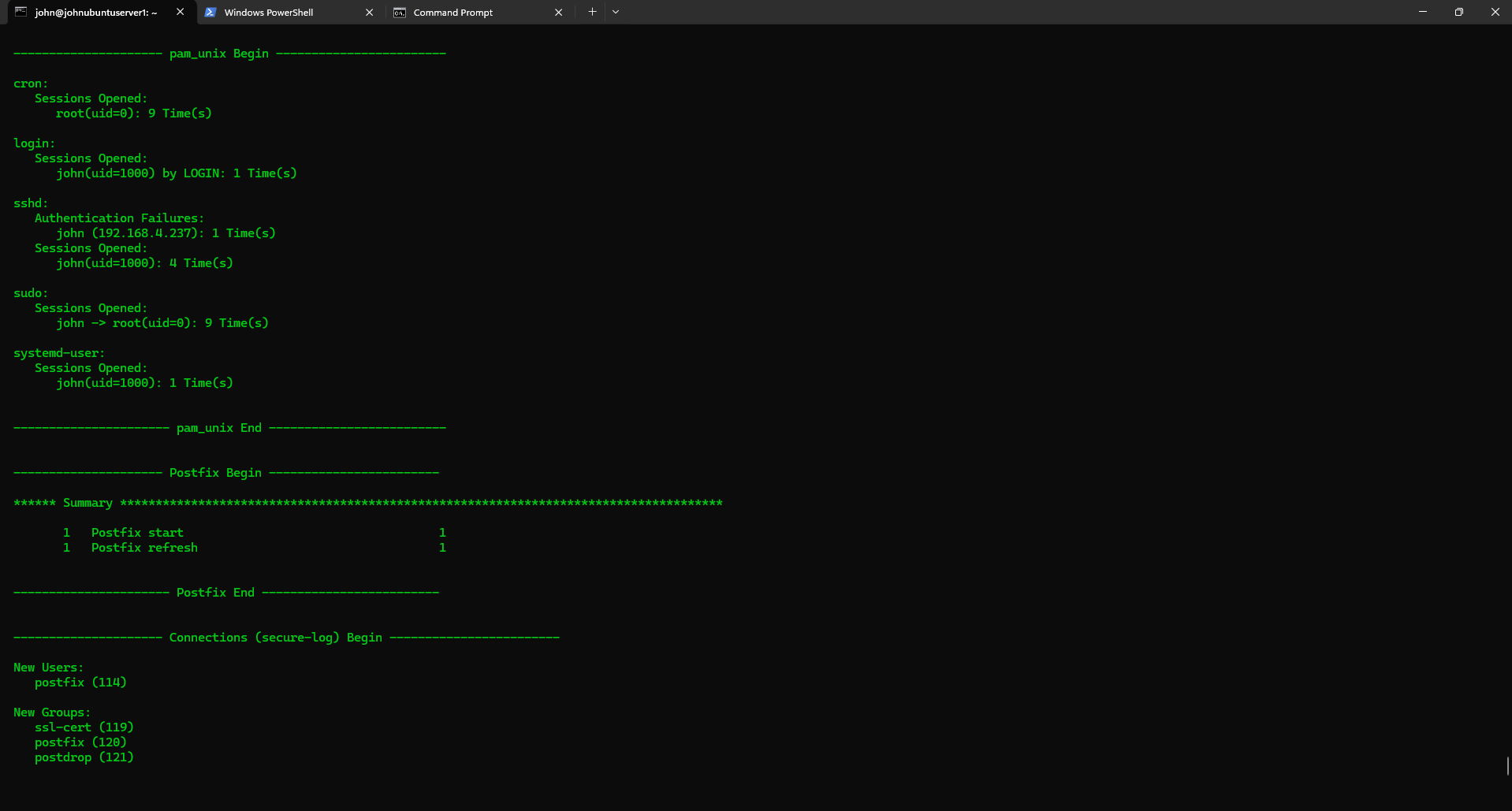
* **Sessions Opened:** This section shows that the user john logged in three times in a root session (uid=0)
* **Postfix:** This section shows that the computer runs Postfix, an email server software. It shows that Postfix was refreshed twice.
* **SSHD:** This section shows that the user john logged in to the computer through SSH from the IP address 192.168.4.237.
* **Sudo (secure log):** This section shows that the user john used sudo to run two commands: /usr/bin/apt and /usr/sbin/logwatch.
* **Disk Space:** This section shows the available disk space on two partitions of the hard drive.
* **Logwatch:** This section shows that the command /usr/sbin/logwatch was executed successfully.



The following linux command was ran to retrieve medium detailed log data: logwatch –range yesterday –detail medium



The log data generated by this command provides details of kernel start up applications and the number of times started, pam\_unix execution, postfix, connections, sshd operations, and sudo secure log data.

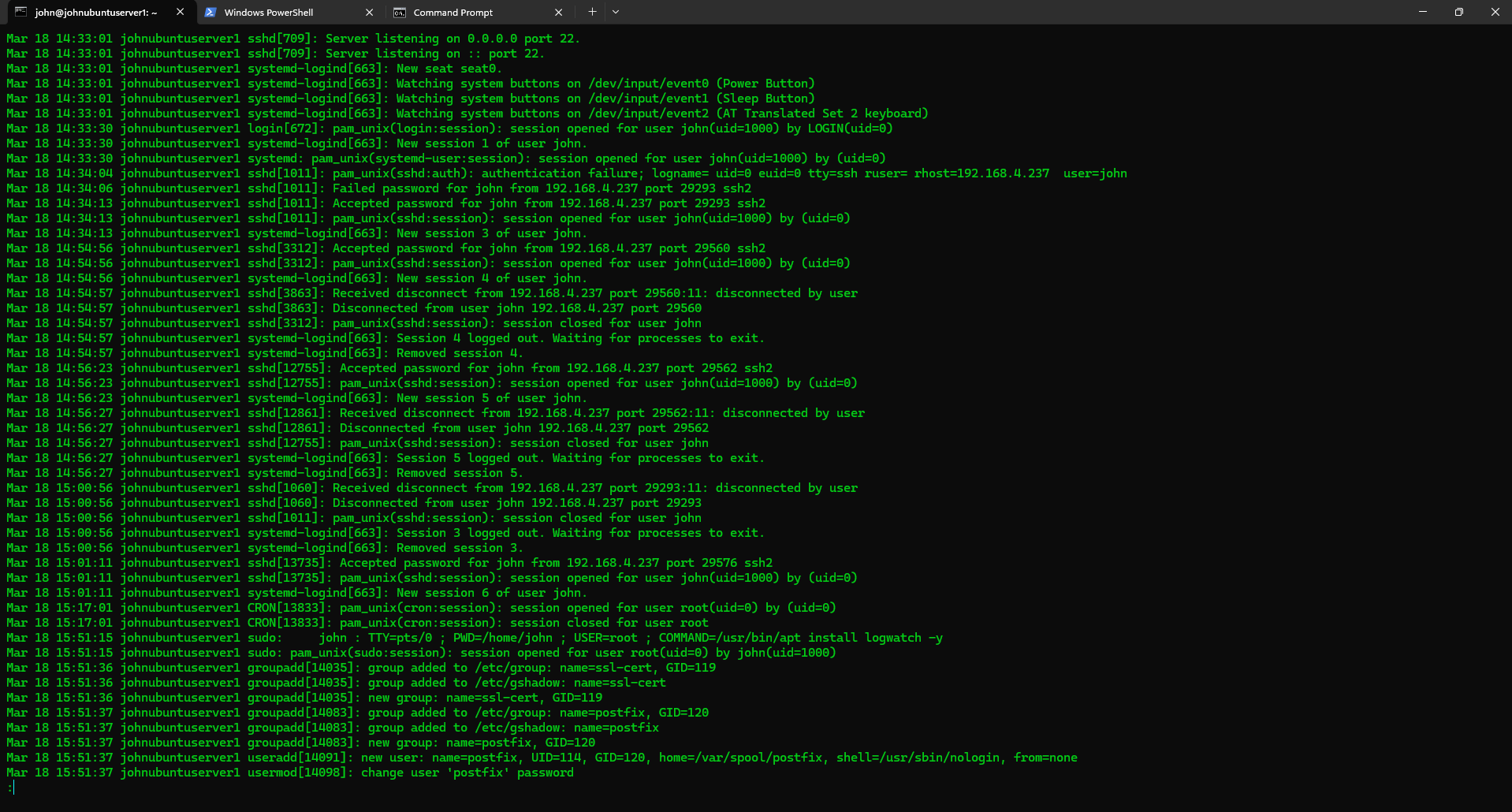


EXERCISE 7 – View the local Auth Log and compare it to the output of Logwatch

Task 1. Review Raw Log Entries

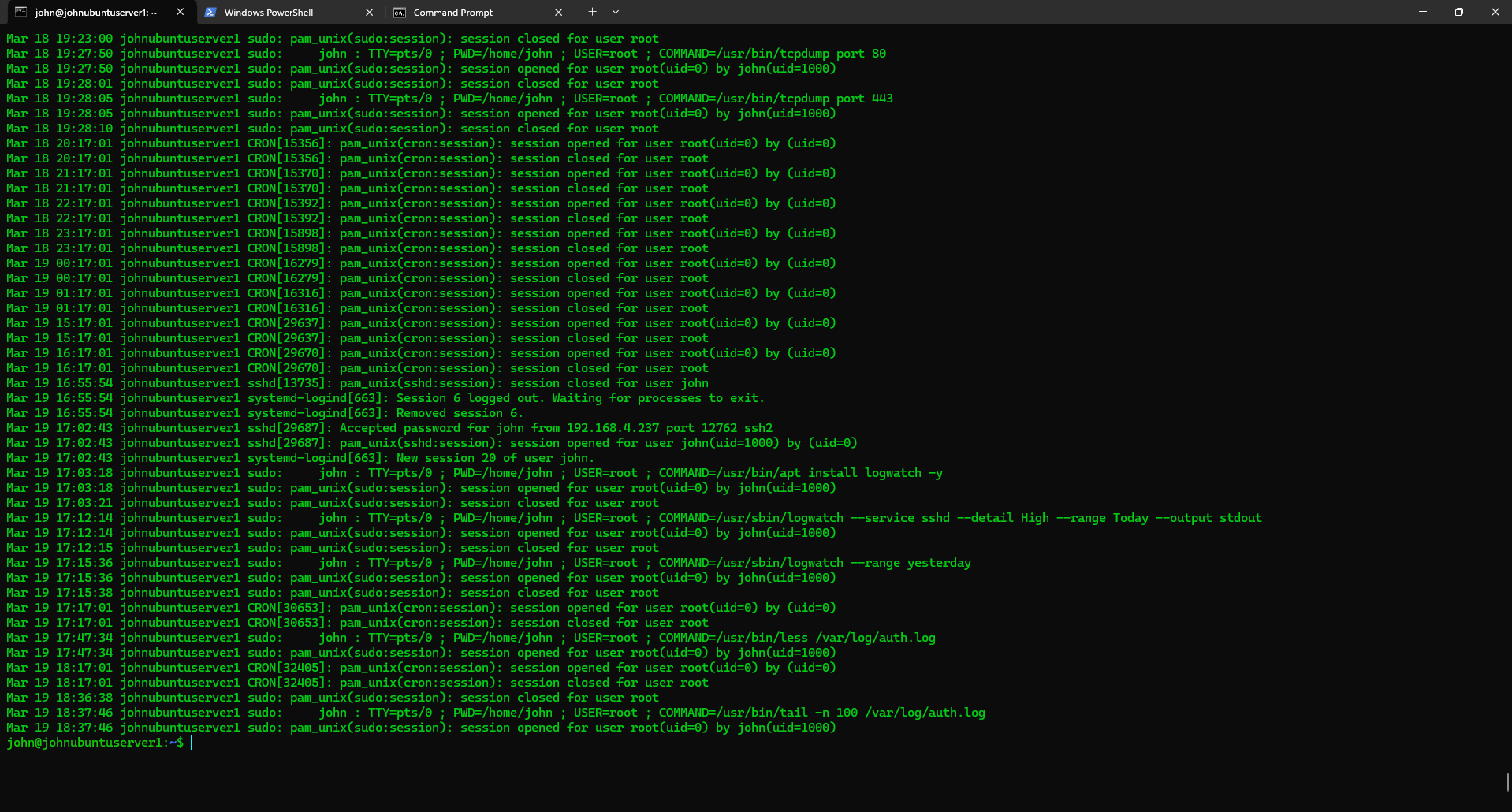
First, inspect the raw log entries in /var/log/auth.log. You can view the contents of this file using a command like less or tail, depending on whether you want to read from the beginning or just see the most recent entries.

sudo less /var/log/auth.log



# or to see the most recent entries

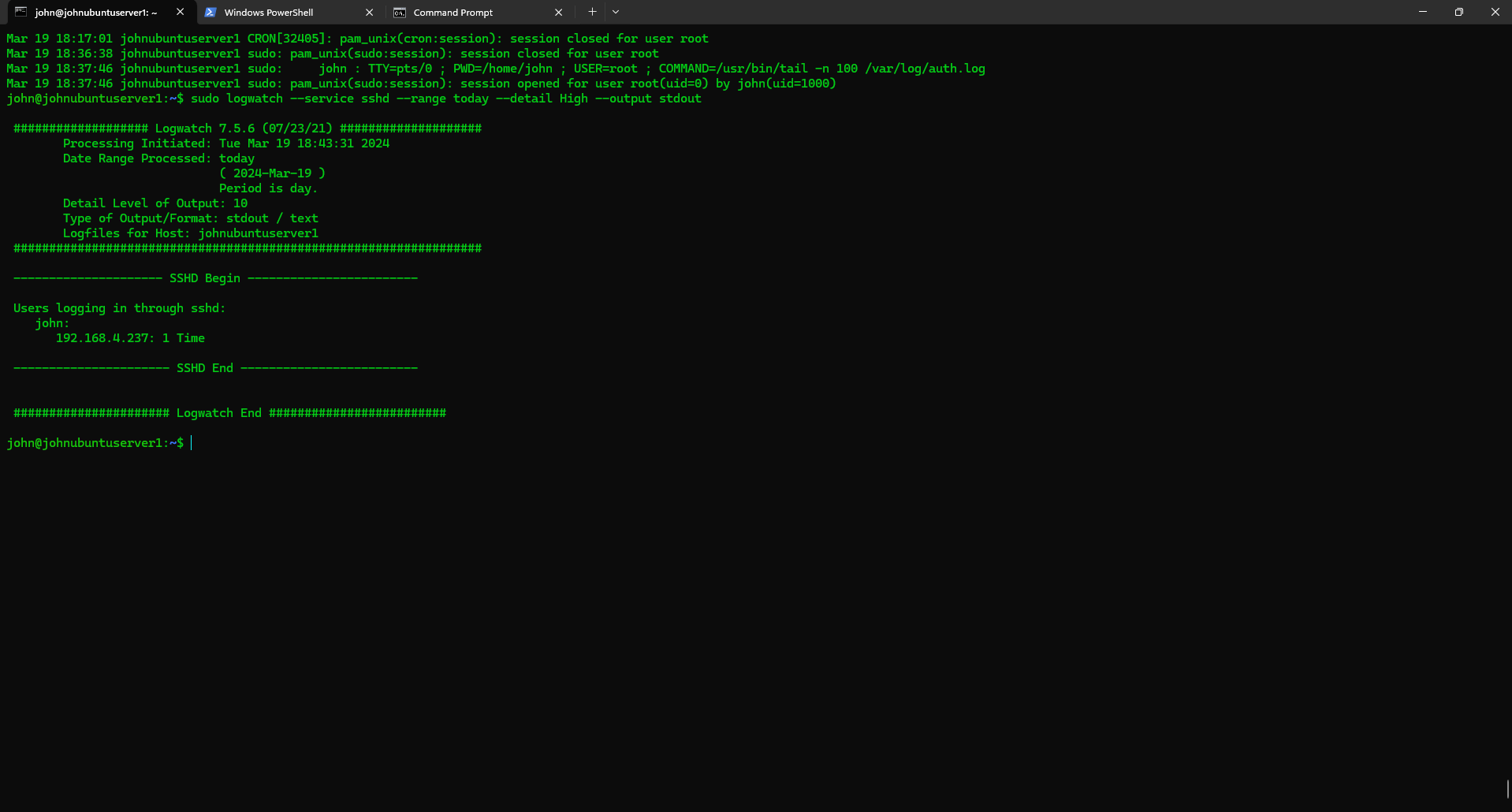
sudo tail -n 100 /var/log/auth.log



2. Generate a Logwatch Report

Next, generate a Logwatch report that includes the authentication logs. You might need to specify the service (--service sshd for SSH logs, for example) and ensure the report covers the same date range as the entries you're examining in auth.log.

sudo logwatch --service sshd --range today --detail High --output stdout



Task 1. Configure Syslog

Configure Syslog to send to Host OS

Task 1. tcpdump

Task 2. Using tcpdump, detect syslog traffic by running the following command:

sudo tcpdump -i any udp port 514 -w syslog\_traffic.pcap

