PennState
College of Information
Sciences and Technology

Lab Assignment Report

COURSE:	**IST 894**
ASSIGNMENT:	**LAB ASSIGNMENT REPORT 10**
SUBMITTED BY:	**BRANTLEY PRICE**
DUE DATE:	**AUGUST 8TH, 2025**
INSTRUCTOR:	**DR. BARTOLACCI**

Contents

General Context

This cyber range exercise was within the InfoSec CySA+ cyber range course and was entitled, “Indicators of Compromise.” In this exercise, the student learned about server investigation and cleanup. The student began by attempting to determine whether or not the system was compromised via log review. From a general IT professional’s perspective, this is a common task when things feel off or flags are being thrown up. Fortinet (2024) identifies several different IOCs, one of them being port-application traffic, which happens to be the key IOC from this exercise.

While the student investigated the logs, it was determined that an attacker had successfully accessed the system with persistence. This was accomplished using a script file aptly named “backdoor.sh.” For what it's worth, such scripts will rarely be so obviously named. Through further investigation, the student identified the script was set to run every minute from within the system’s task scheduler on port 7777. This is not a commonly used port, so checking network traffic and seeing inbound and outbound traffic on this port would also be a red flag had this not been found during log review. In fact, the SANS Technology Institute (2025) shows some of the most recent data for port 7777 to be Trojan attacks.

After identifying that port 7777 was compromised, the student moved to addressing the persistent attack. This involved killing the scheduled task, removing the scheduled event, stopping the process, and removing the file from the machine. In a real-world scenario, further research would need to be done to identify how the attacker actually gained access to the system in the first place, but this was a good exercise to walk the student through the steps necessary to identify, contain, and remove the threat from the machine.

Technical Context

The opening stages of this exercise walked the student through a live analysis of the system. This started with a root-level file inspection. A shell script, */backdoor.sh*, was detected and it was revealed that this was not an authorized script. Using *ncat* to analyze the file, it was determined that the script was running on port 7777 which gave the attacker a persistent method for remote access to the system. The student further verified this fact by running *netstat -lntp* and confirmed the process was indeed running on port 7777.

The next question to answer for the student was regarding the threat actor's persistence mechanism. Just how persistent was the attack? Through a review of the *crontab*, which is a utility used for task scheduling and task automation (GeeksforGeeeks, 2025), it was determined that the attack was executing every minute via a scheduled job (***** sh /backdoor.sh 2>&1*). Executing this job every minute would ensure persistence even through system reboots. Using *iftop*, which is typically used for monitoring data traffic to and from a system (Boelen, 2025), the student was able to verify the open connection to the attacker's system.

Finally, the student stepped through the eradication of the attack and began the recovery. Using *crontab -r*, the student removed the persistent threat by deleting the cron job. Then the active shell process running on port 7777 was killed using *pkill ncat*, and the student deleted the */backdoor.sh* script from the system. Finally, upon reviewing the */etc/ssh/sshd_config* file, it was found that a directory different from the default directory used to verify public keys had been used, which the student addressed by removing from the config file.

Screenshots

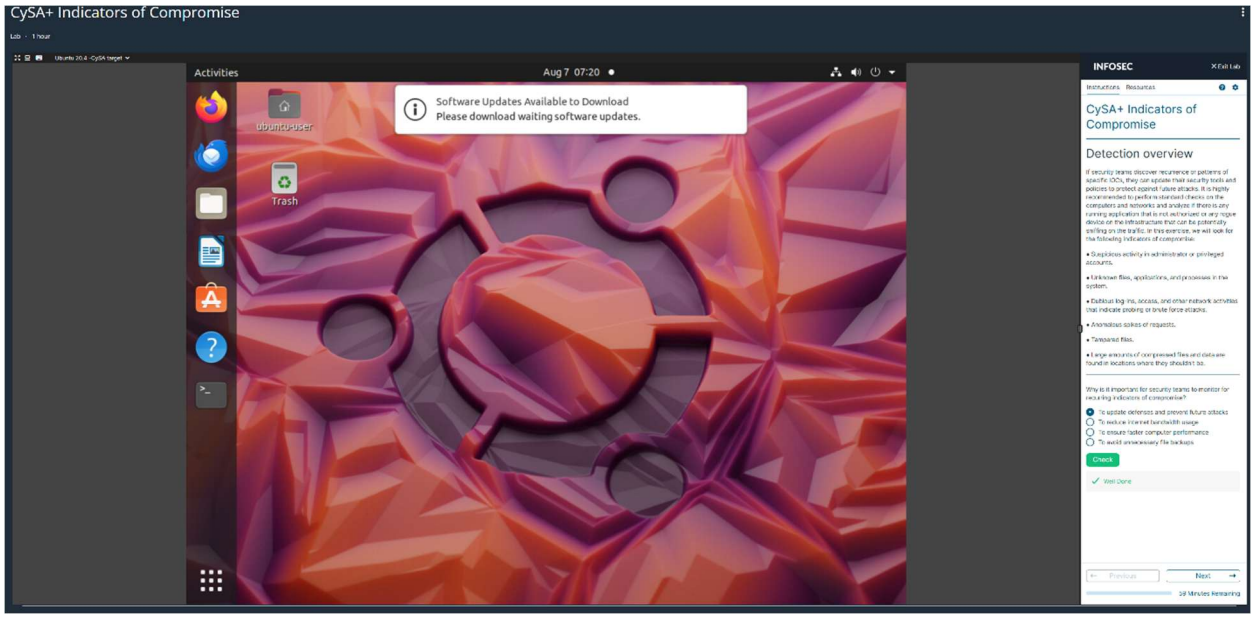

Figure 1: IOC Introduction and Overview

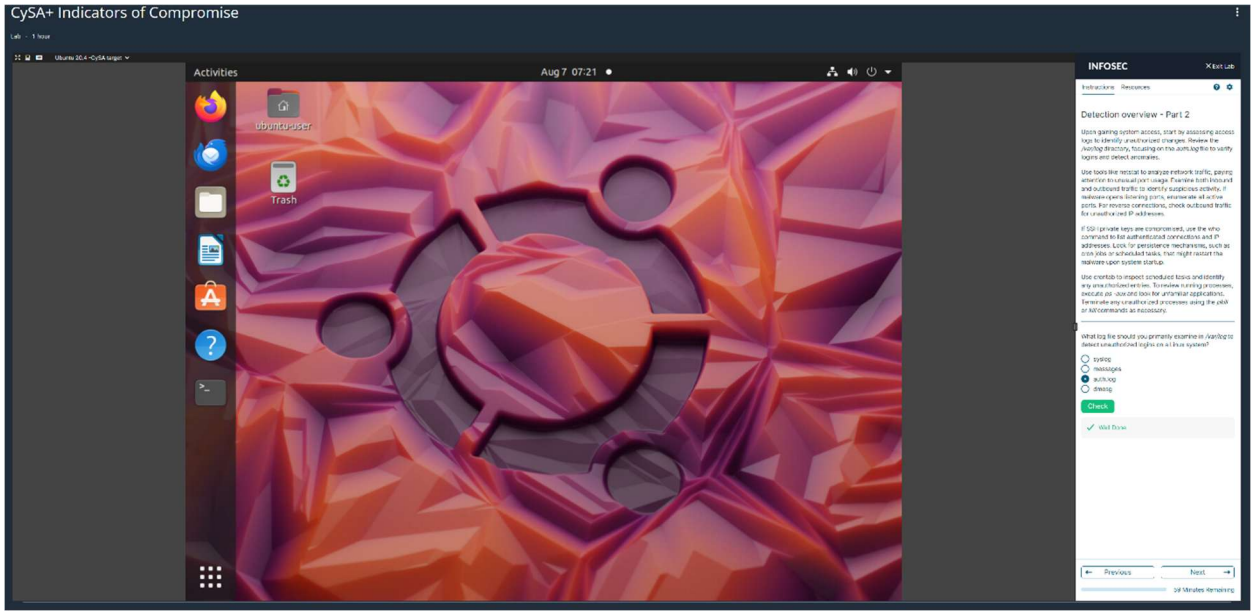

Figure 2: IOC Introduction and Overview Part II

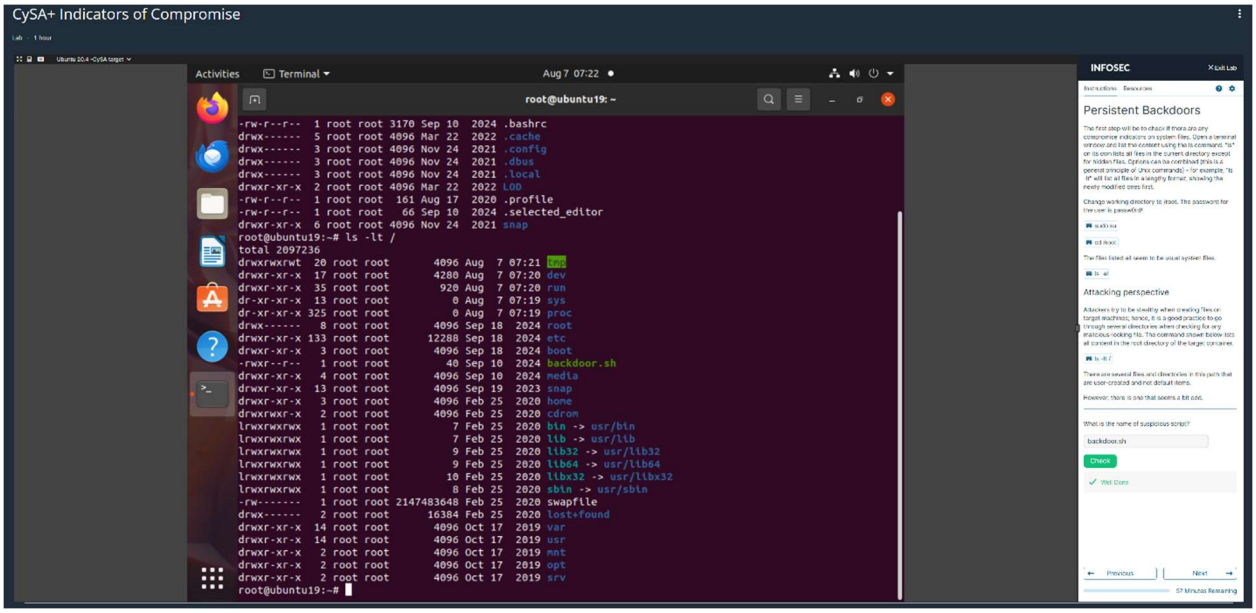

Figure 3: Identification of the Backdoor

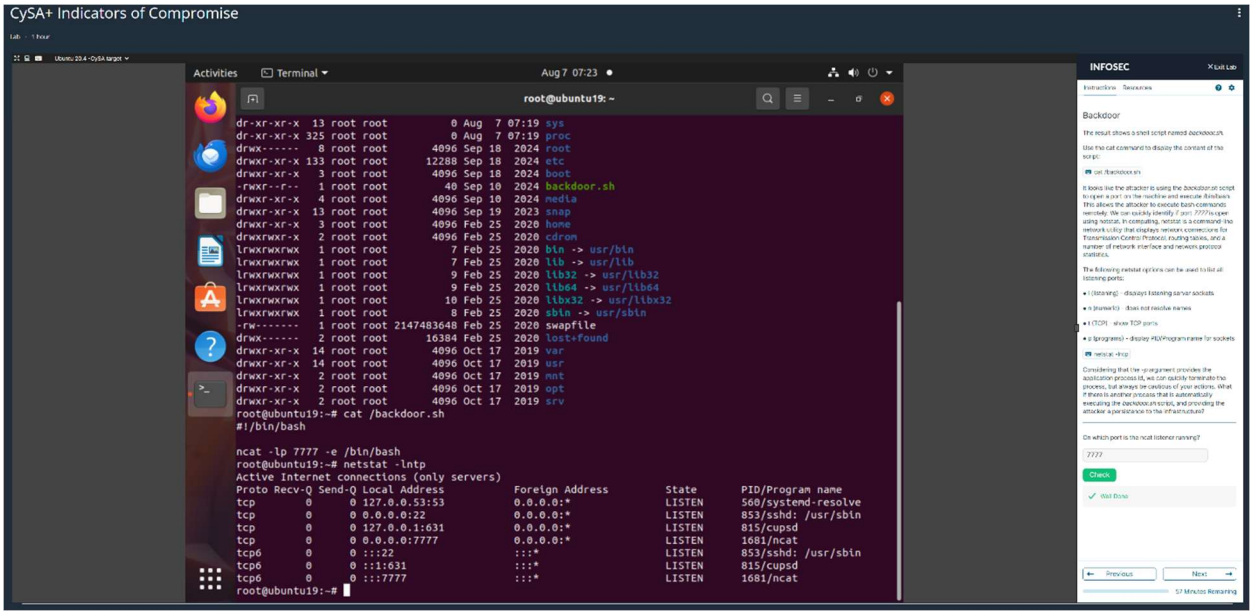

Figure 4: Port Identification

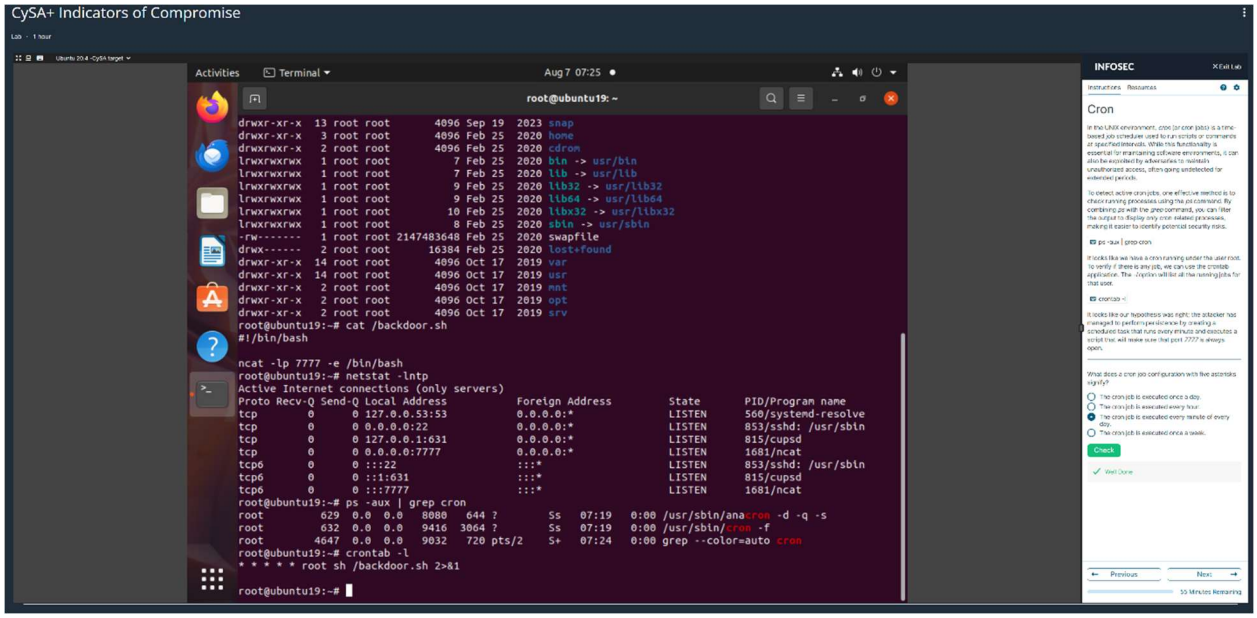

Figure 5: Cron

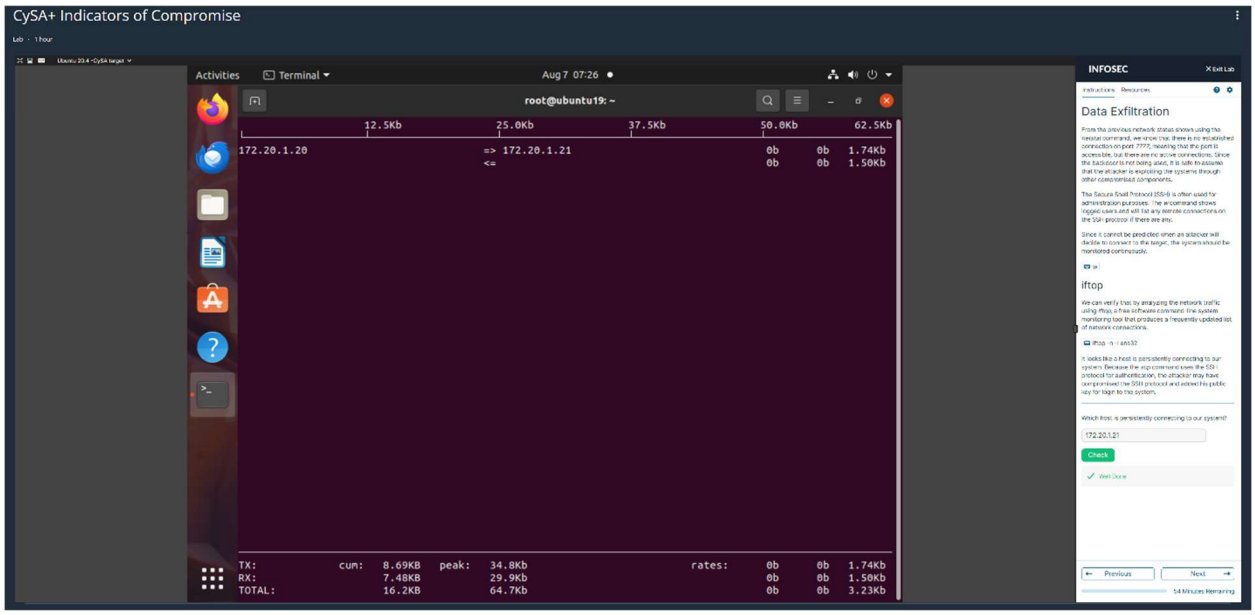

Figure 6: Validation of Data Exfiltration

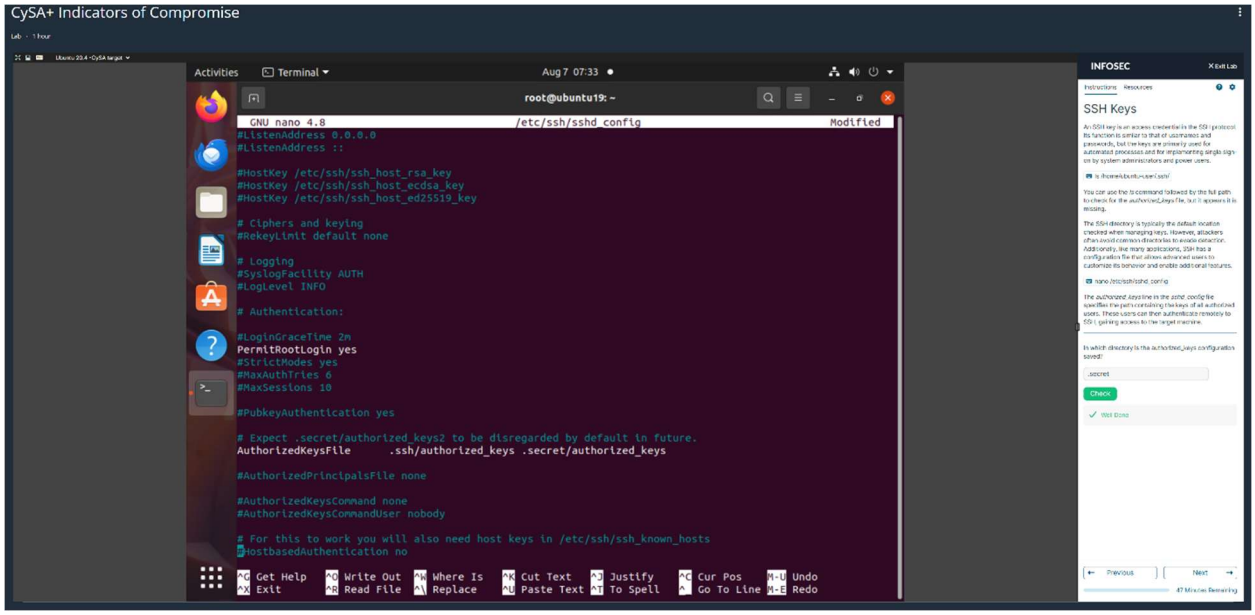

Figure 7: Suspect SSH Key Stores

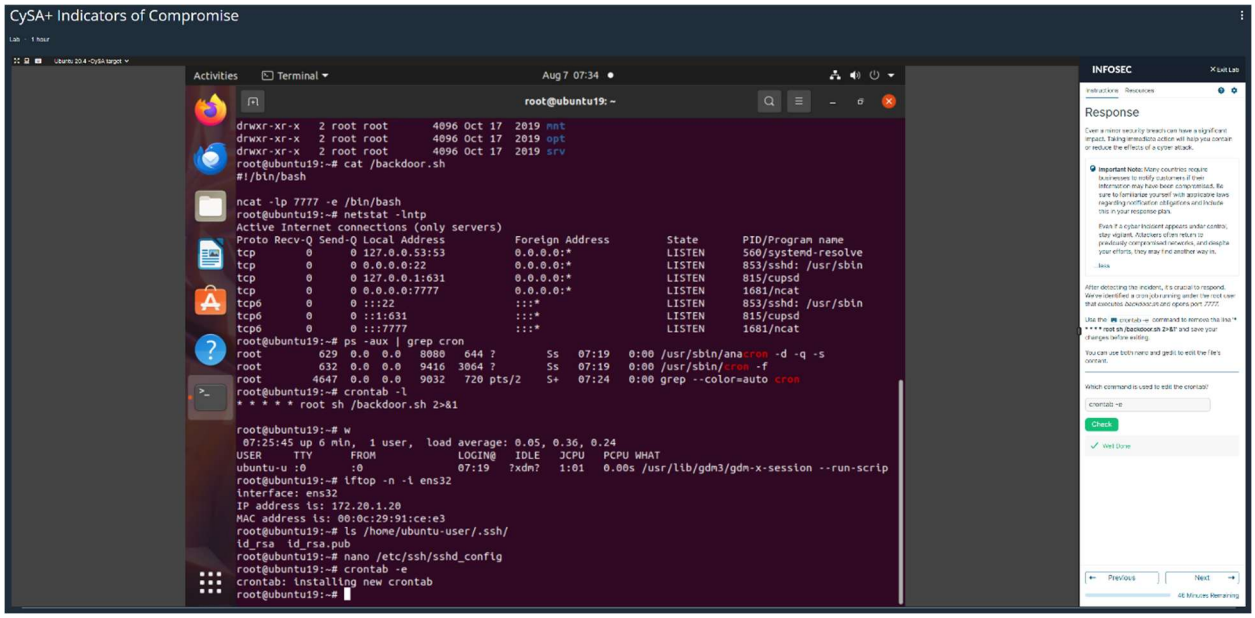

Figure 8: Response to the Attack

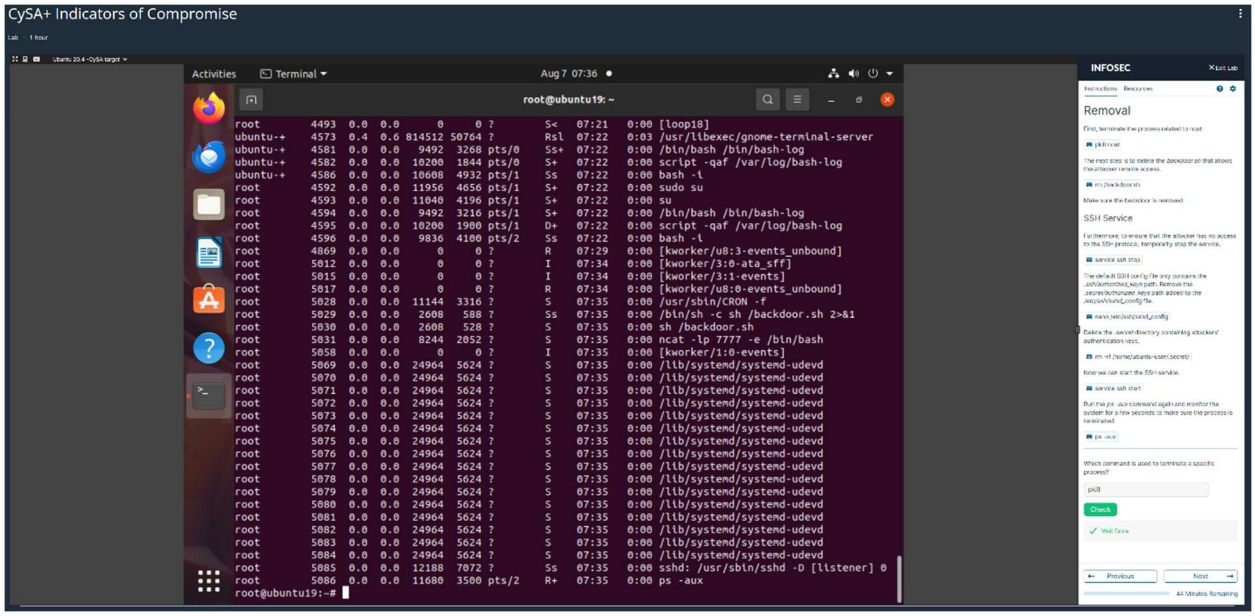

Figure 9: Removing the Threat

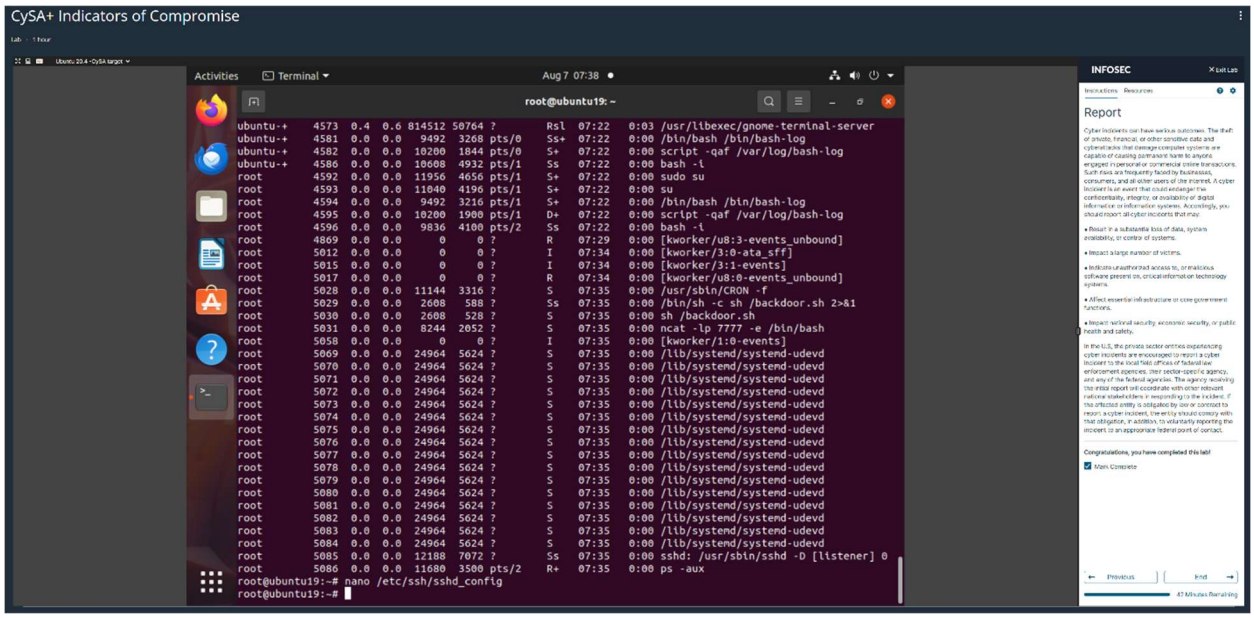

Figure 10: Report and Recovery

References

Boelen, M. (2025, March 12). *iftop*. Linux Audit. https://linux-audit.com/system-administration/commands/iftop/

Fortinet. (2024). *Indicators of Compromise (IOCs)*. Retrieved August 7, 2025, from https://www.fortinet.com/resources/cyberglossary/indicators-of-compromise

GeeksforGeeks. (2025, July 28). *"crontab" in Linux with Examples*. GeeksforGeeks. https://www.geeksforgeeks.org/linux-unix/crontab-in-linux-with-examples/

SANS Technology Institute. (2025). *Internet Storm Center*. Data for Port 7777. Retrieved August 7, 2025, from https://www.dshield.org/data/port/7777