Lab 10 Report

Jason Tolbert

The Pennsylvania State University

IST 894-001: Capstone Experience

Dr. Michael Bartolacci, Instructor

April 6th, 2025

Table of Contents

General Overview

This lab introduces participants to essential skills in both digital forensics and the identification of indicators of compromise.

Digital Forensics

The first part of the lab teaches participants basic digital forensics skills. Digital forensics is the practice of collecting and investigating media stored on computers or sent over networks, typically with the intent of using it as evidence of a crime. Key to investigating any crime is the preservation of evidence. The lab introduces participants to one of the primary ways digital evidence is preserved — hashing.

Hashing is a process that takes the contents of a file and outputs a string of characters called a hash. A given hash can only be produced by the file it was created from; if that file changes, even a little bit, the hash it produces will also change. Thus, if you have the hash of a file, and want to determine whether that file has been altered in the time since you hashed it, you can rehash the file in its current state and compare the new hash to the one you originally took; if they differ, the file has been altered. This makes hashing a highly effective tool for determining whether digital evidence has been tampered with (Premanand Narasimhan & Dr.N.Kala, 2024).

Once participants are familiarized with preserving evidence, the focus of the lab turns to capturing it. Participants are shown how to use command-line tools to capture traffic being sent over a network for later review. In the real world, these kinds of tools provide investigators with a perpetual snapshot of all activity on a network within a given window of time, and are commonly-used to reconstruct the events of computer crimes (Sikos, 2020).

Indicators of Compromise

The second part of the lab focuses on detecting indicators of compromise – signs that a security breach may have happened or be happening. Participants are taught how to spot these signs, respond to them, and clean up any damage.

Threat hunting, broadly, is about identifying and investigating behavior that looks like it shouldn't be happening (Mahboubi et al., 2024). To that end, participants begin their search for indicators of compromise by looking for new or unauthorized behavior on their system. Participants eventually uncover the presence of a malicious script that forcibly opens their machine to network traffic and a scheduled task that runs said script at regular intervals. Once they discover the backdoor, they move to shut it down, deleting the script and the task that executes it. This approach is a point-for-point mirror of the standard real-world cyber incident response playbook – identify the threat, contain it, eradicate it, and then return the system to a safe state (Cybersecurity and Infrastructure Security Agency, n.d.).

Technical Overview

This lab introduces participants to essential skills and digital forensics and the identification of indicators of compromise.

Digital Forensics

The first part of the lab gives participants a practical introduction the forensic analysis of digital information. Participants use tcpdump capture live network traffic, learning how to tailor the interface and duration of the capture session and save the captured data to a pcap file. They then review the pcap file in Wireshark, using its filtering capabilities to isolate unencrypted Telnet traffic and inspect it to find plaintext credentials that were used to execute a successful login to a remote machine.

Once participants acquire their first piece of digital evidence – the pcap file – they learn how to preserve it using hashing. Using both md5sum and shasum, participants how to apply hashes to verify that the packet capture has not been altered between acquisition and examination.

Indicators of Compromise

The second part of the lab focuses on identifying indicators of compromise on a system that has already been breached. Participants meticulously scour the system for evidence

of unusual behavior. They begin with relatively obvious checks, like examining authentication logs for suspicious login activity, and looking through shell history for possibly malicious commands. They continue to search for compromise in places that are not as easily visible, using ps, netstat, and iftop to analyze active processes and network connections. Through iftop, they discover that they attacker has gained persistent access to their machine via SSH.

During their investigation, participants find a malicious script that forcibly opens port 7777 and a cron job that runs said script every minute. After deleting the script and removing the cron job, they move to fully return their machine to a secure state by deleting the attacker's SSH key.

References

Cybersecurity and Infrastructure Security Agency. (n.d.). *Cybersecurity incident & vulnerability response playbooks*.

Mahboubi, A., Luong, K., Aboutorab, H., Bui, H. T., Jarrad, G., Bahutair, M., Camtepe, S., Pogrebna, G., Ahmed, E., Barry, B., & Gately, H. (2024). Evolving techniques in cyber threat hunting: A systematic review. *Journal of Network and Computer Applications*, *232*, 104004. https://doi.org/10.1016/j.jnca.2024.104004

Premanand Narasimhan & Dr.N.Kala. (2024). Ensuring the integrity of digital evidence: The role of the chain of custody in digital forensics. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *10*(6), 2438–2450. https://doi.org/10.32628/CSEIT2410612443

Sikos, L. F. (2020). Packet analysis for network forensics: A comprehensive survey. *Forensic Science International: Digital Investigation*, *32*, 200892. https://doi.org/10.1016/j.fsidi.2019.200892

Screenshots

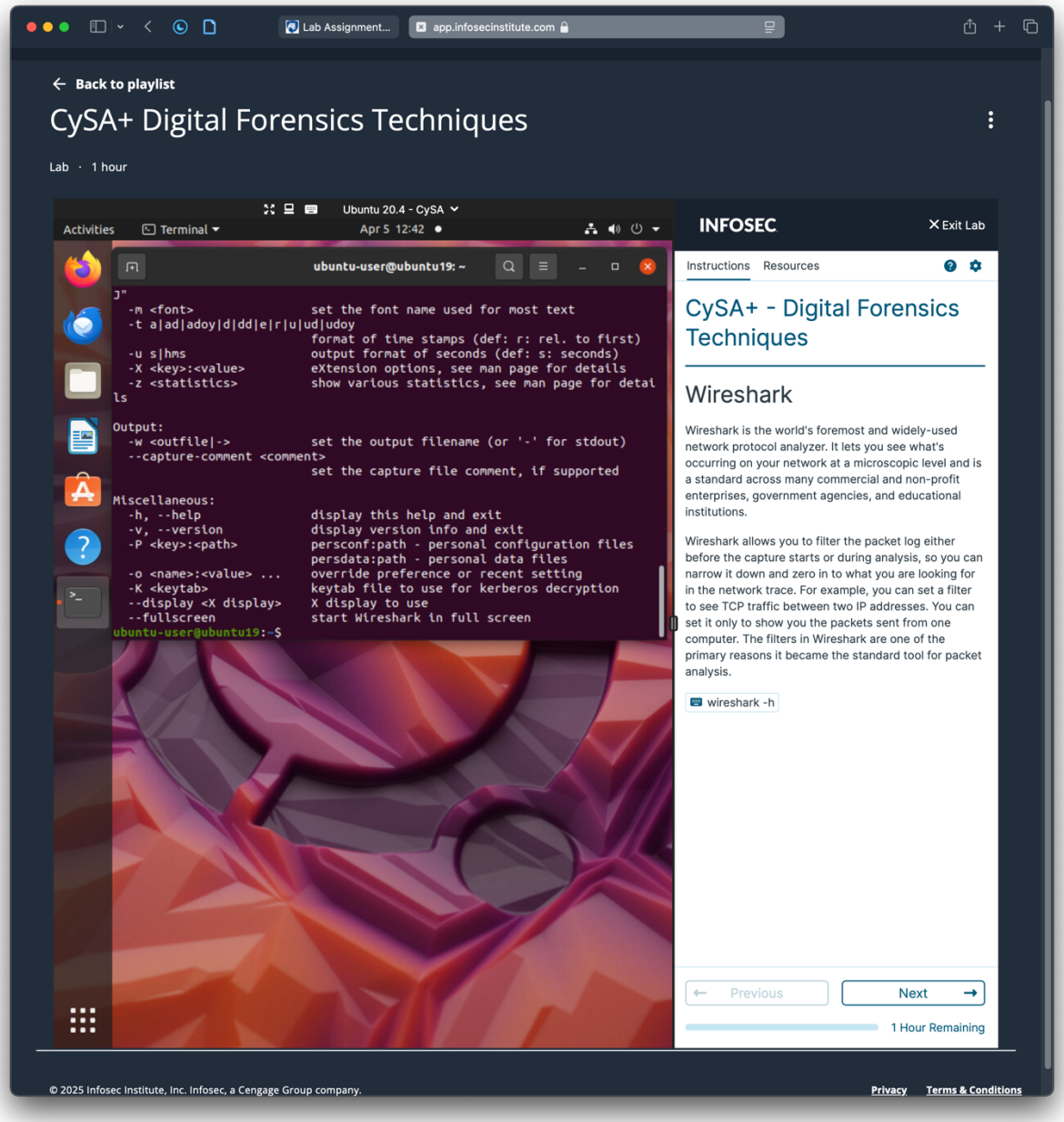

Figure 1. The Wireshark help text.

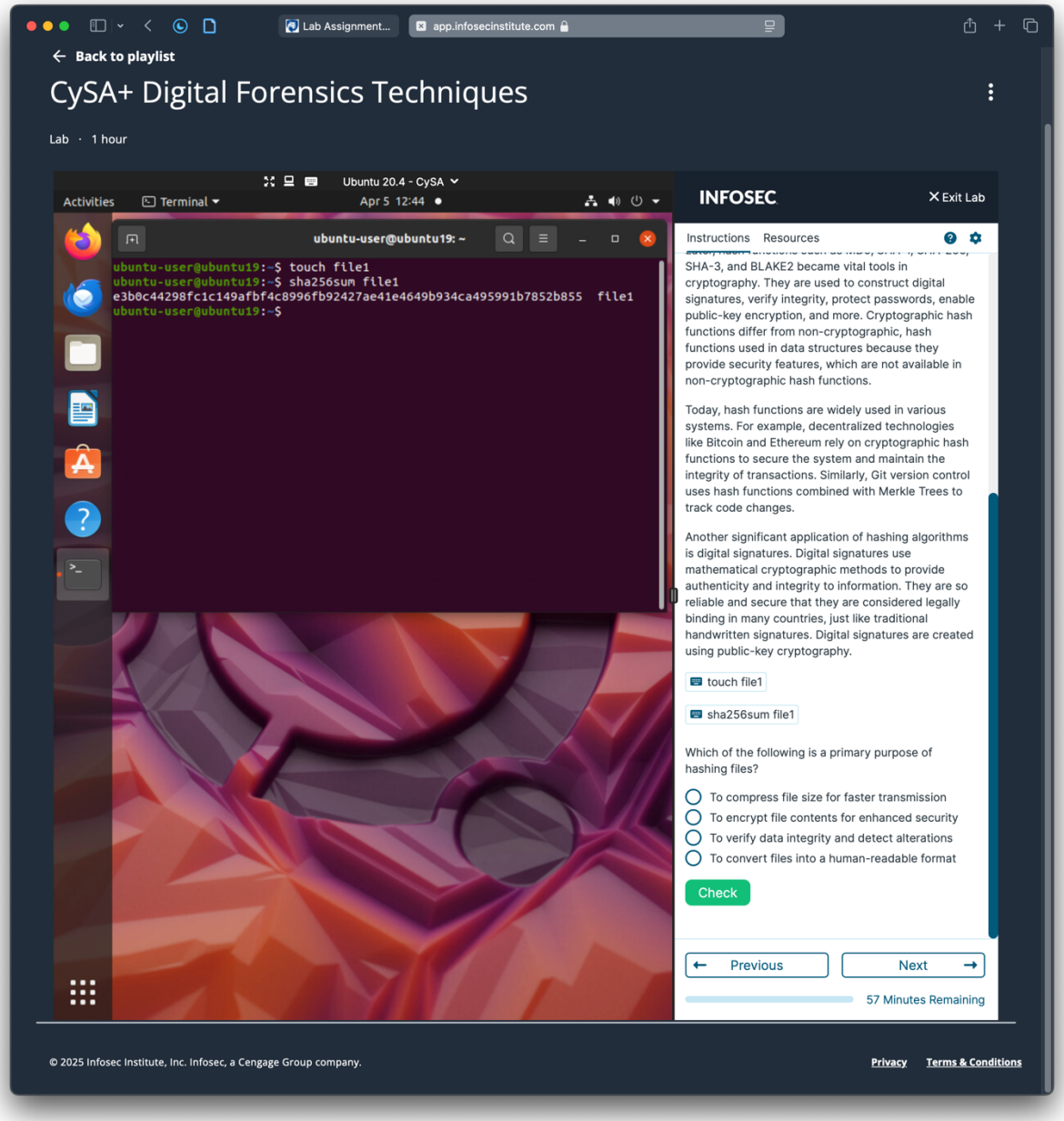

Figure 2. Creating file1 and reading its SHA-256 hash.

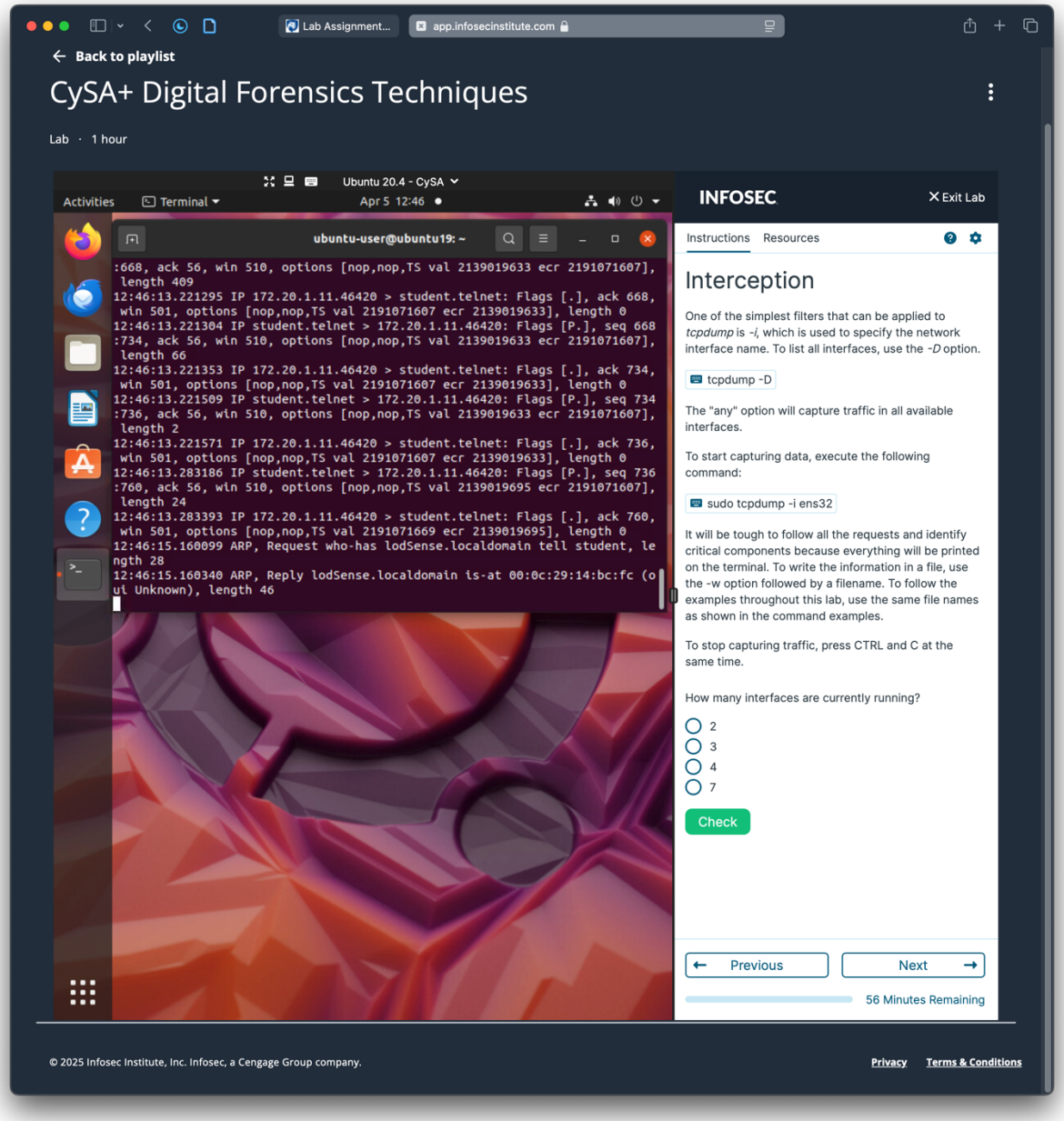

Figure 3. Capturing traffic with tcpdump.

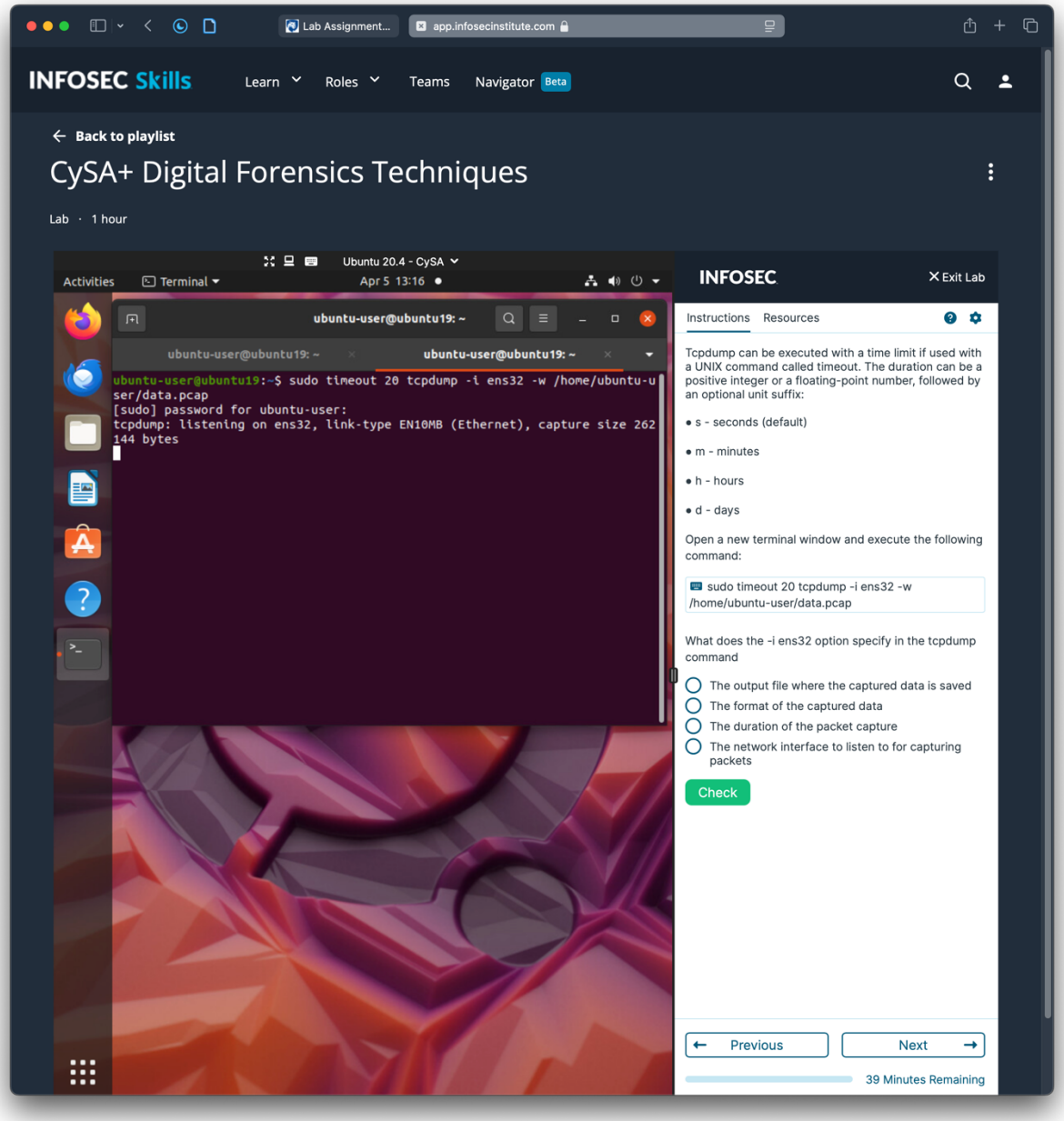

Figure 4. Running tcpdump with a 20-second time limit.

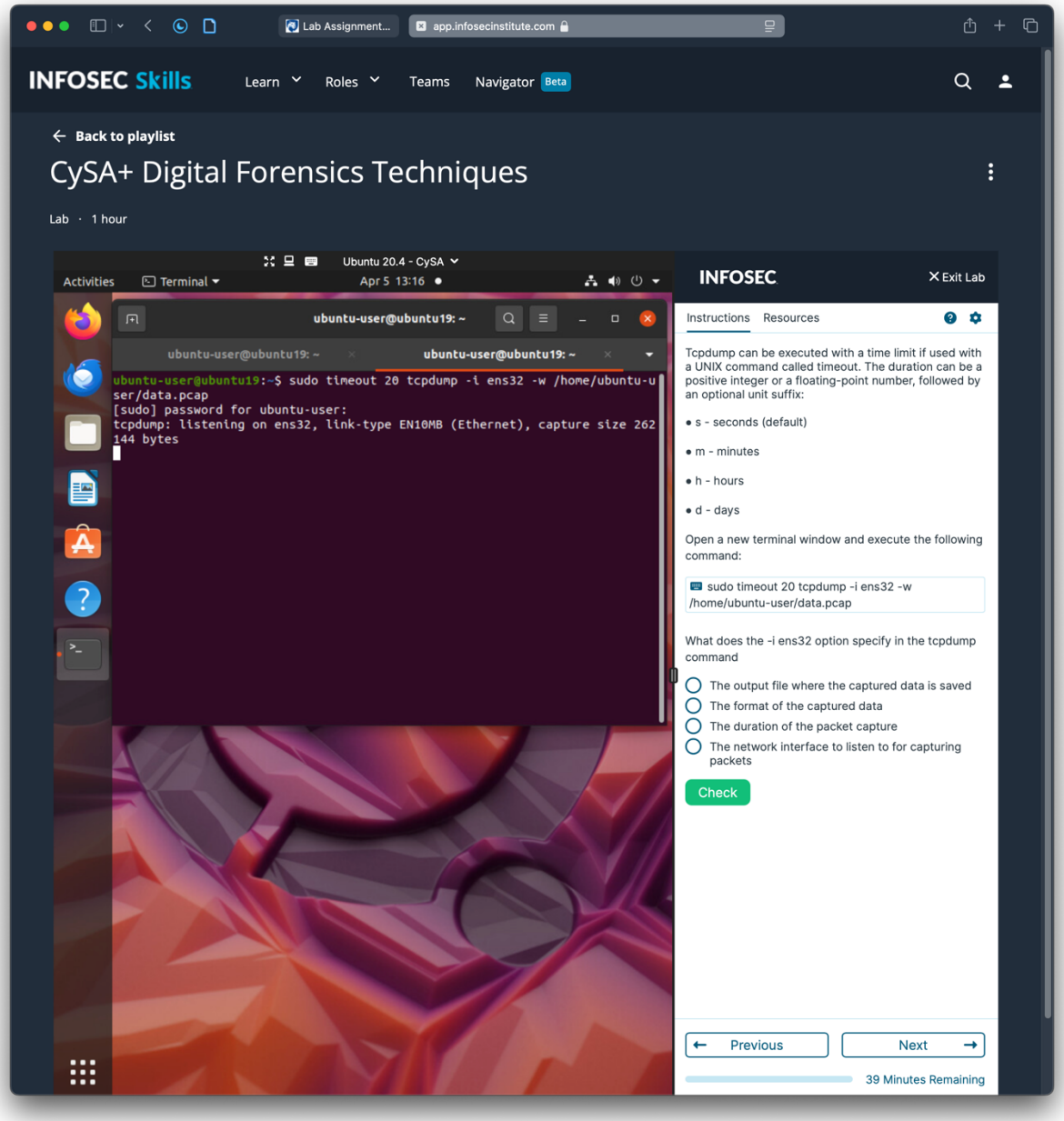

Figure 5. Observing the contents of the data.pcap file in Wireshark.

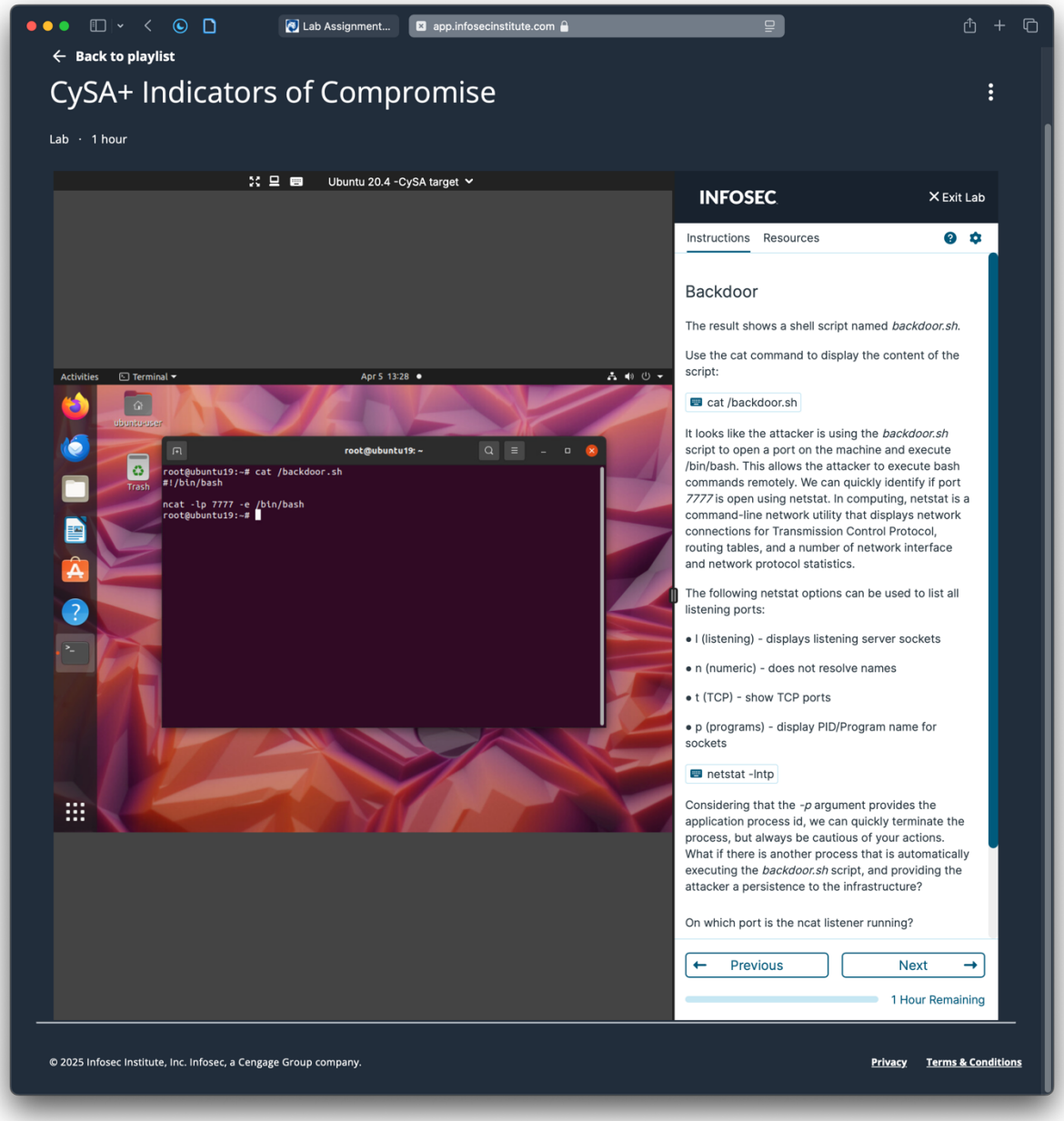

Figure 6. Reading the contents of backdoor.sh.

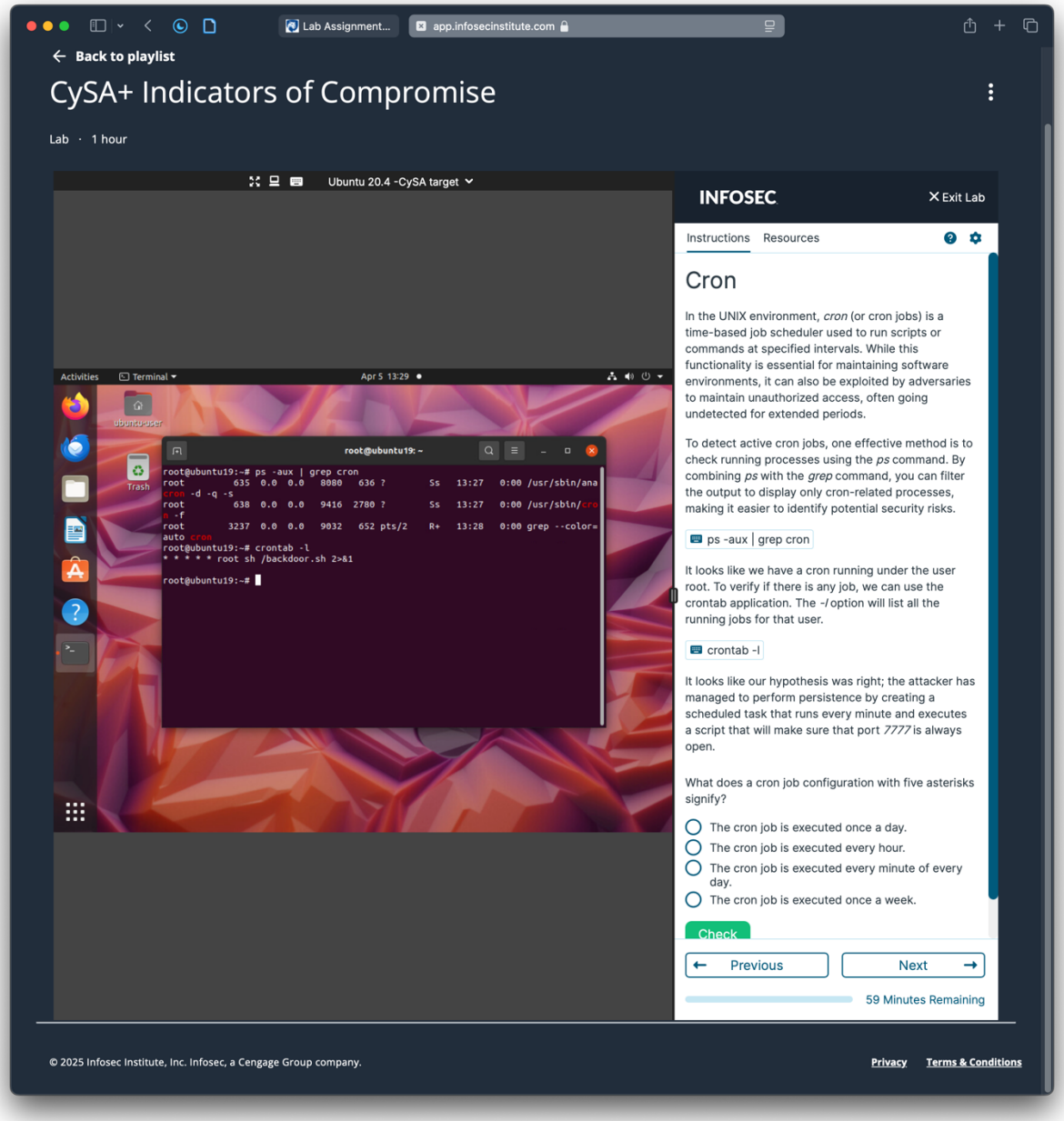

Figure 7. Examining a malicious cron job that keeps port 7777 open.

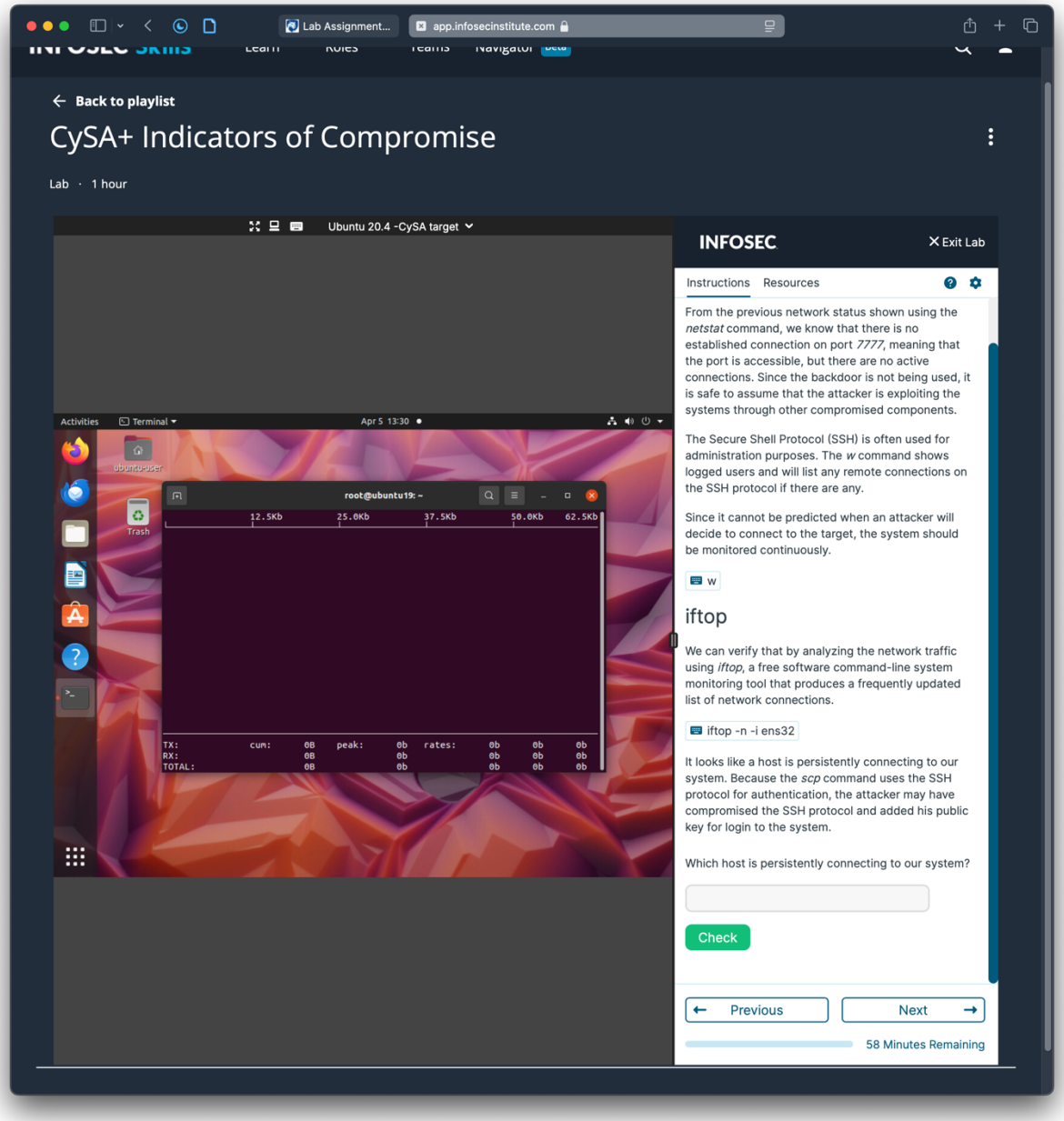

Figure 8. Monitoring network traffic with iftop.

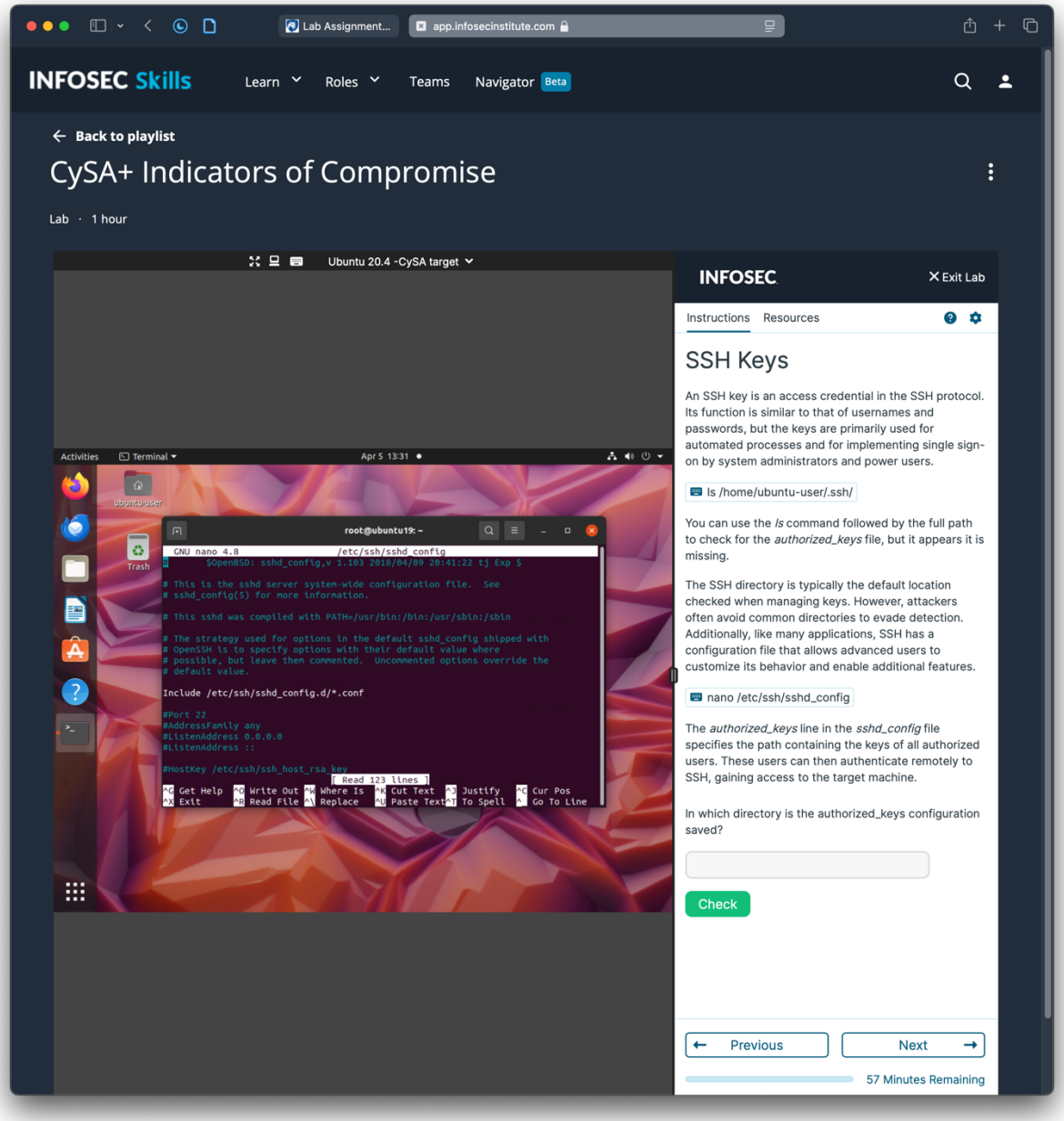

Figure 9. Examining the SSH server configuration file.

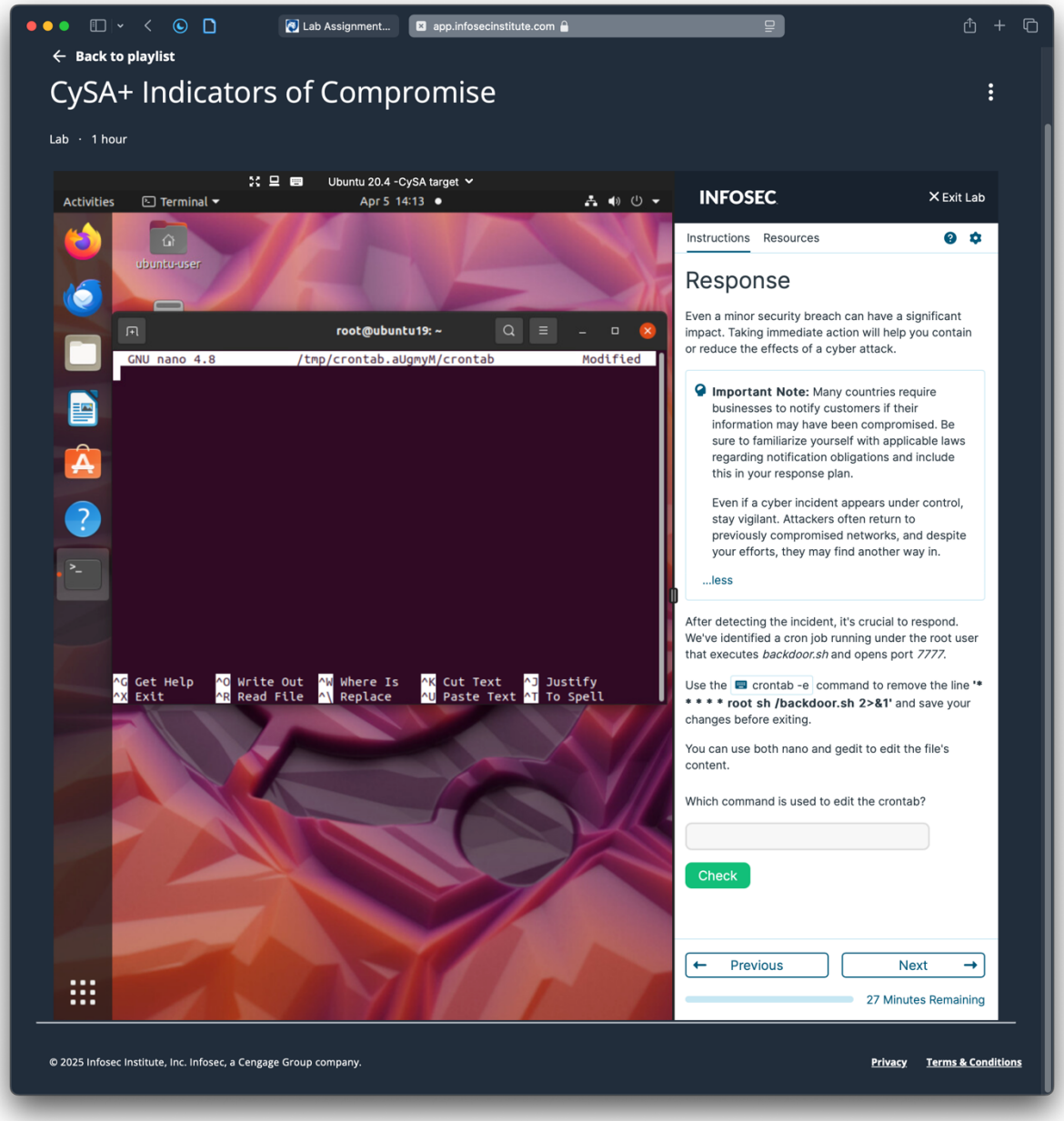

Figure 10. The crontab file, newly empty now that the malicious cron job depicted in Figure 7 has been removed.