PennState
College of Information
Sciences and Technology

Lab Assignment Report

COURSE:	**IST 894**
ASSIGNMENT:	**LAB ASSIGNMENT REPORT 8**
SUBMITTED BY:	**BRANTLEY PRICE**
DUE DATE:	**JULY 27TH, 2025**
INSTRUCTOR:	**DR. BARTOLACCI**

Contents

General Context

Regardless of an organization's size, reliance on network infrastructure is ubiquitous, and properly securing that infrastructure is an absolute imperative. The two cyber range exercises from this week's lab provided the student with the chance to interact with network protocols and cryptographic algorithms, both of which are used on every network in operation today. Two fundamental tenets of cybersecurity were covered: confidentiality and integrity, defined as protecting information from unauthorized access and ensuring data has not been accidentally altered or modified by an unauthorized user (Washington University, 2025).

The first exercise, "Network and Security Diagnostics," covered portions of network security. In a sense, network security can be thought of as the frontline of network defense. During the exercise, the student stepped through identifying issues with network traffic flows, the identification of potential bottlenecks and/or misconfigurations, and the implementation of rules that determine the information that can enter or exit a system. This information is important to understand for any I.T. professional, but even more so in the context of cybersecurity, as safeguarding information traversing the network is top of mind for many companies. In fact, 76% of security leaders worry about cyber threats (Reed, 2024).

As a complement to the first exercise, the second, "Cryptography," allowed the student to interact with different types of encryption algorithms used to protect data from prying eyes. Understanding how to encrypt and decrypt data to maintain confidentiality and ensure secure exchange is a non-negotiable. This exercise covered methods for scrambling data, steganography, a cryptographic technique used to embed hidden information into images, and digital signatures, which are used for non-repudiation. The proper implementation of cryptographic solutions can help keep information secure, ensuring that even if it is compromised, the data will be unusable for the attacker.

Technical Context

Within the two cyber range exercises, the student is provided a practical lesson on two core cybersecurity domains. The first exercise allowed the student to use Linux-based command-line tools to inspect network configurations, diagnose issues, and provided an overview of the *Iptables* software firewall for implementing network access control. The student used *ping* to test node reachability, *nmap* for port scanning and host enumeration, and *curl* to test HTTP interactions. *Iptables* is a Linux kernel firewall that can provide robust protection against attacks when configured appropriately (Barman, 2023). The student established stateful packet filtering and managed network traffic based on IP address, port numbers, and connection/port states.

The second exercise provided the student with hands-on experience with fundamental cryptographic algorithms and gave examples of how they can be practically implemented within the *openssl* utility. First, the student explored symmetric key algorithms like DES, 3DES, and a few different variations of AES. Symmetric key algorithms are highly effective at securing data efficiently, particularly for local use. However, because there is only one key in use, to decrypt the information, both the sender and the receiver must possess the key. That makes secure communication with a symmetric key a problem. For that, the student was introduced to an asymmetric key. Asymmetric keys' primary use cases are secure email, digital signatures, and key exchanges (Poggi, 2025). The student created RSA and ECC key pairs and walked through the process of encrypting data with a public key, decrypting it with a private key, and developed digital signatures to ensure non-repudiation. Additionally, *steghide* was used to demonstrate steganography and hashing algorithms, specifically SHA256, were on display.

These exercises gave the student a quick but deep look at network security. The networking portion reinforced the need for well-defined rules to manage inbound and outbound network traffic via a network policy. The cryptographic portion demonstrated the often enigmatic but foundational role

cryptography plays in the CIA triad. For a company's cybersecurity program to be successful, proficiency in both of these disciplines is necessary to design, implement, and maintain a secure infrastructure, while also recognizing that this is only a small part of the entire puzzle.

Screenshots

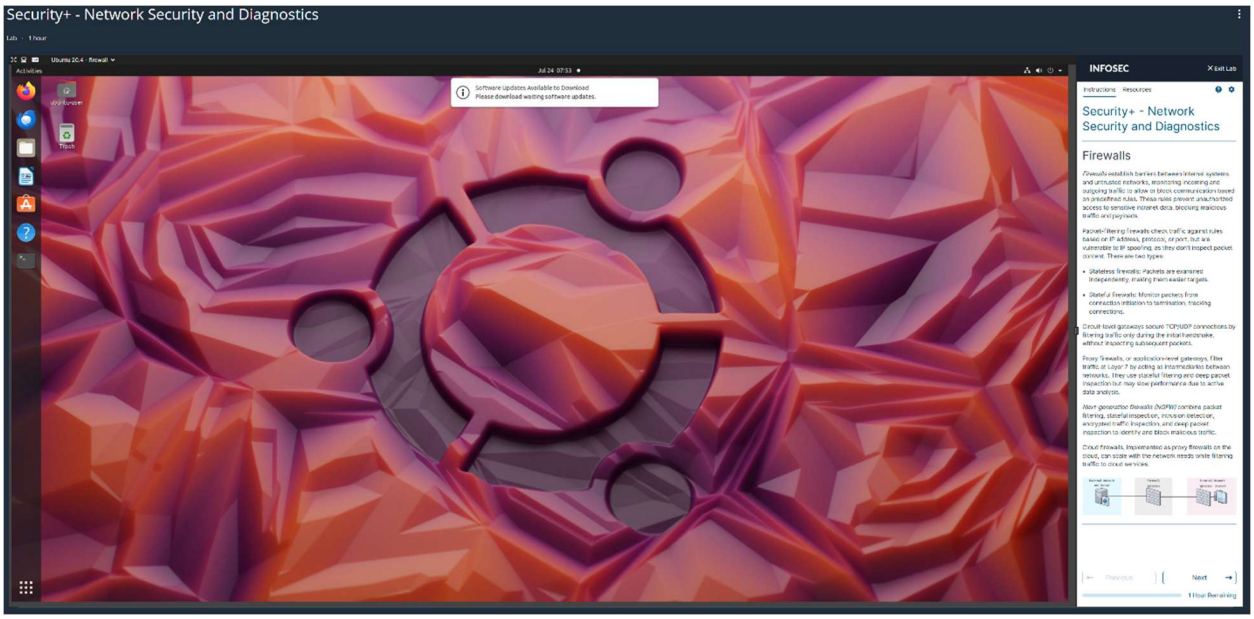

Figure 1: Network Security and Diagnostics Intro

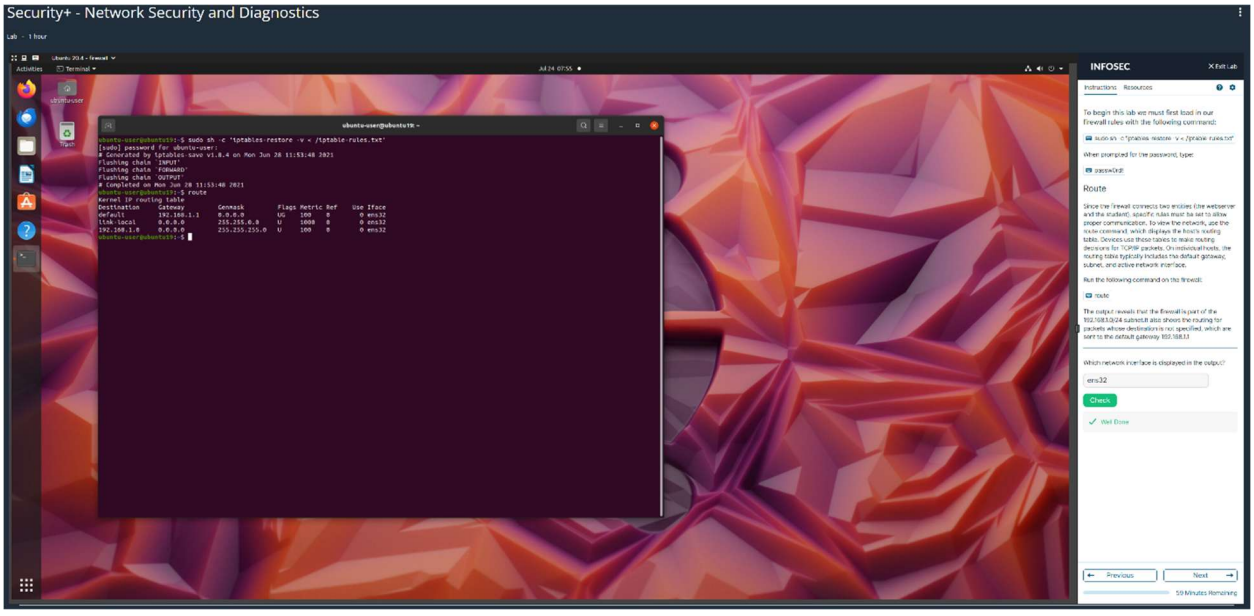

Figure 2: Starting Iptables

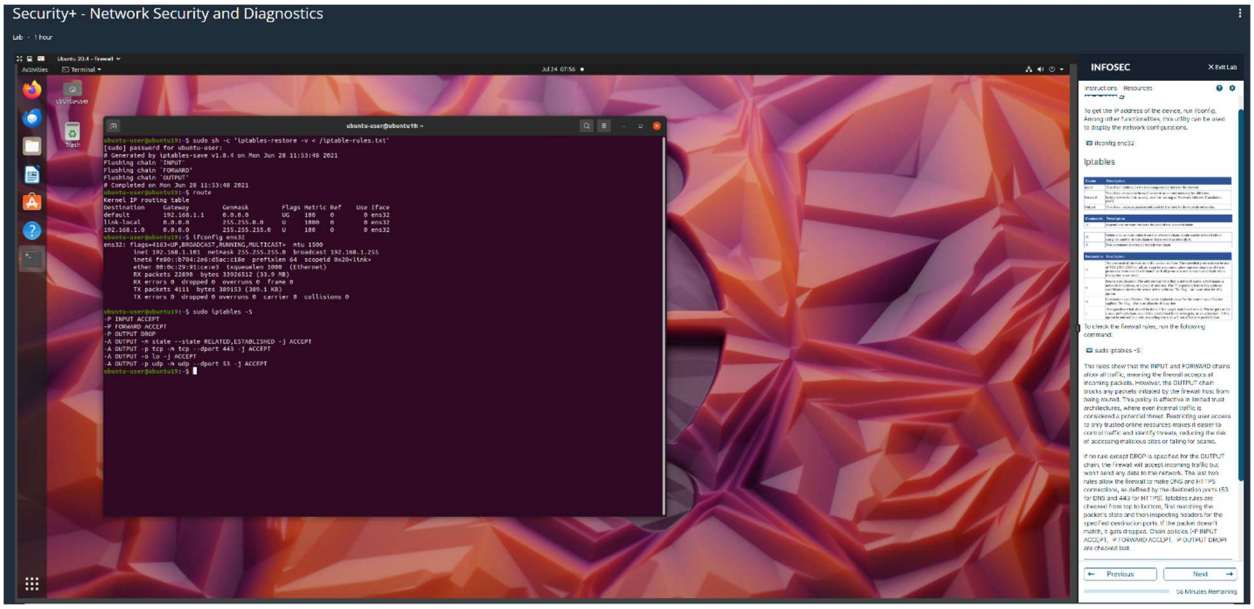

Figure 3: Iptables Intro

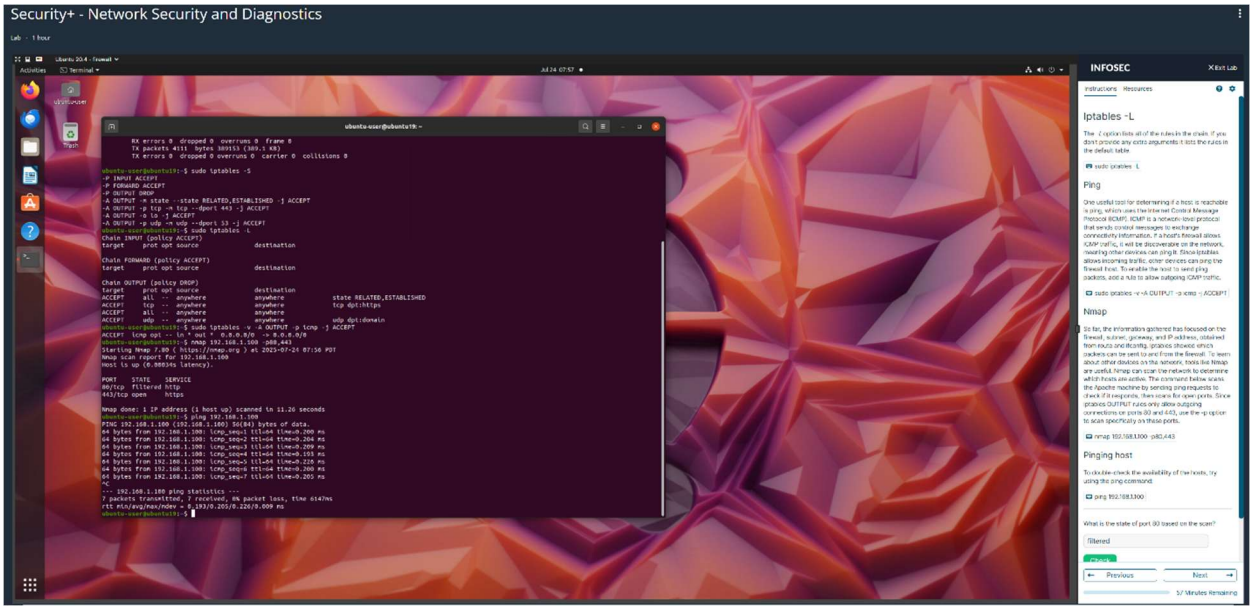

Figure 4: Viewing Iptables rules, pinging, and host enumeration

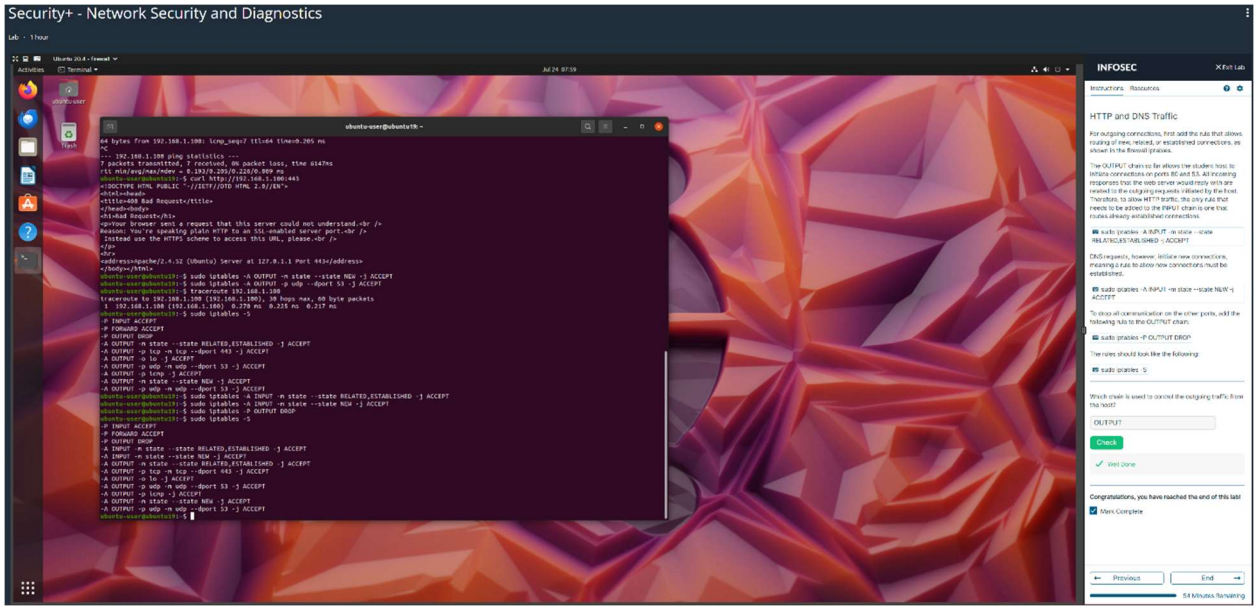

Figure 5: Checking HTTP and DNS Traffic/Final Step

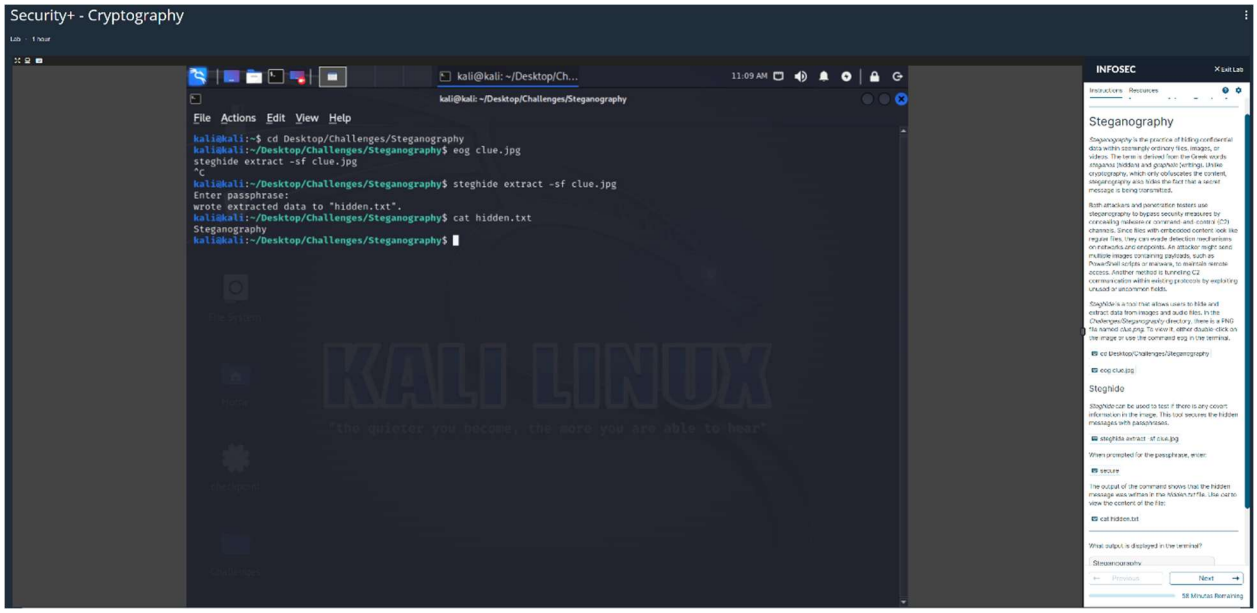

Figure 6: Cryptography Intro/Steganography

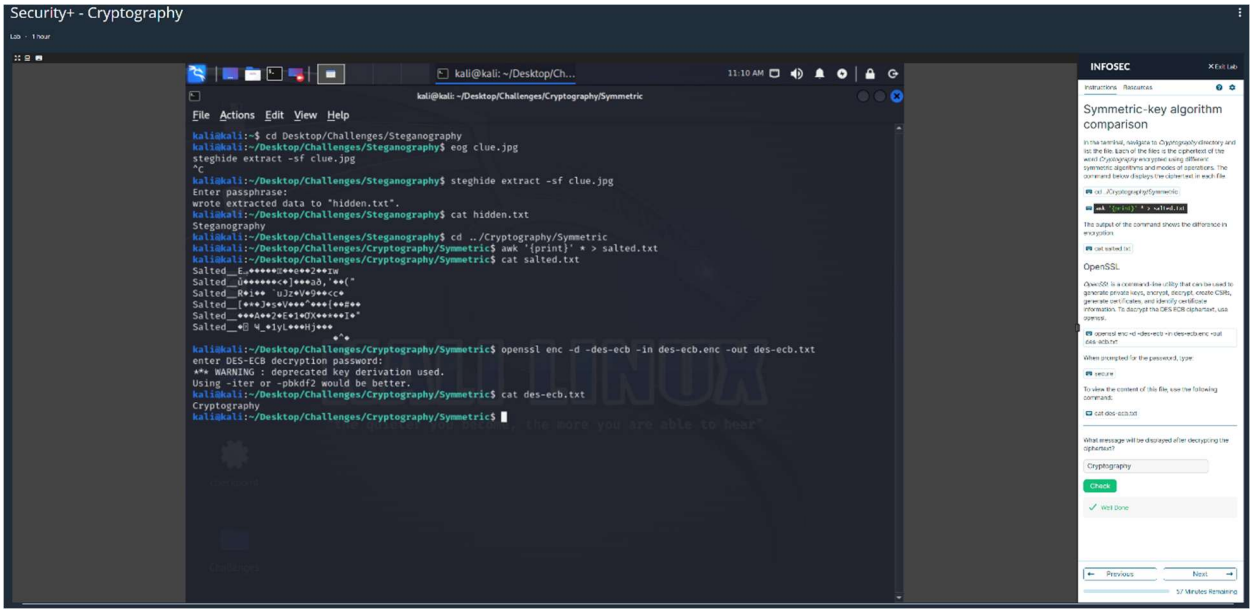

Figure 7: Asymmetric keys

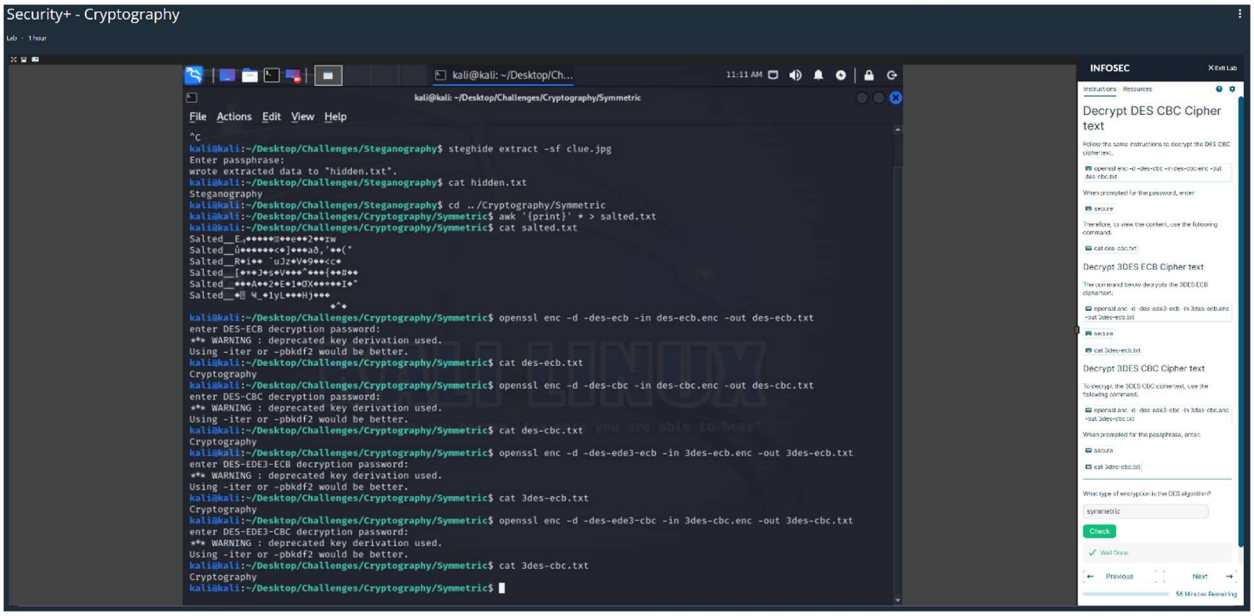

Figure 8: DES and 3DES

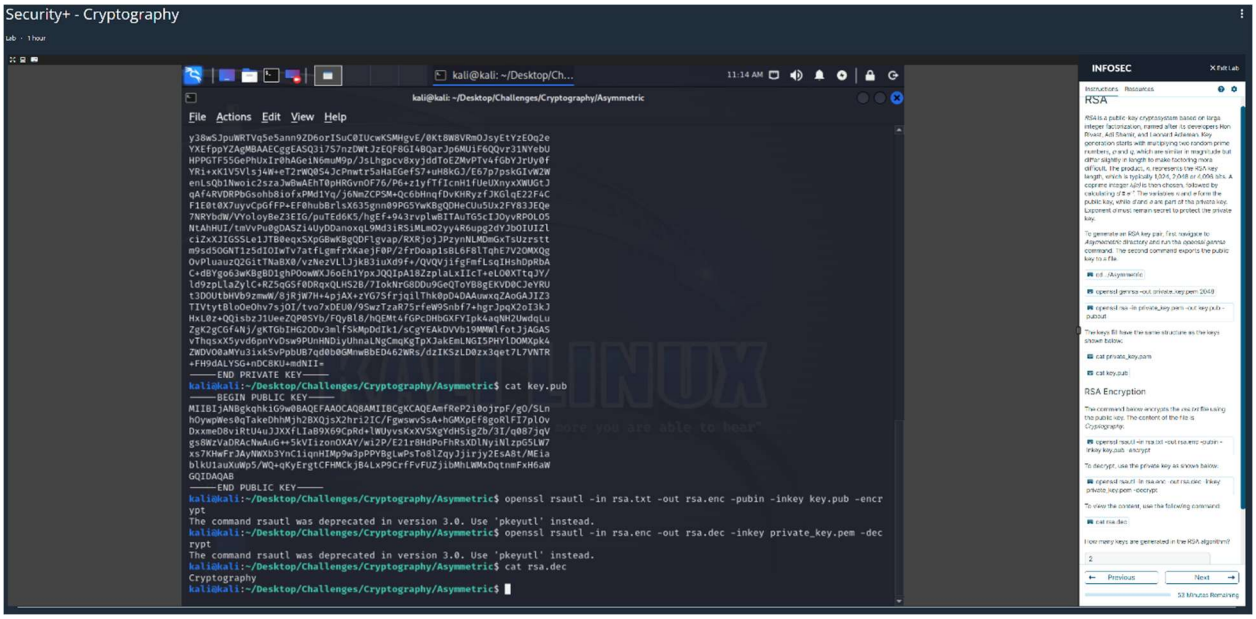

Figure 9: Symmetric Key Generation Using RSA

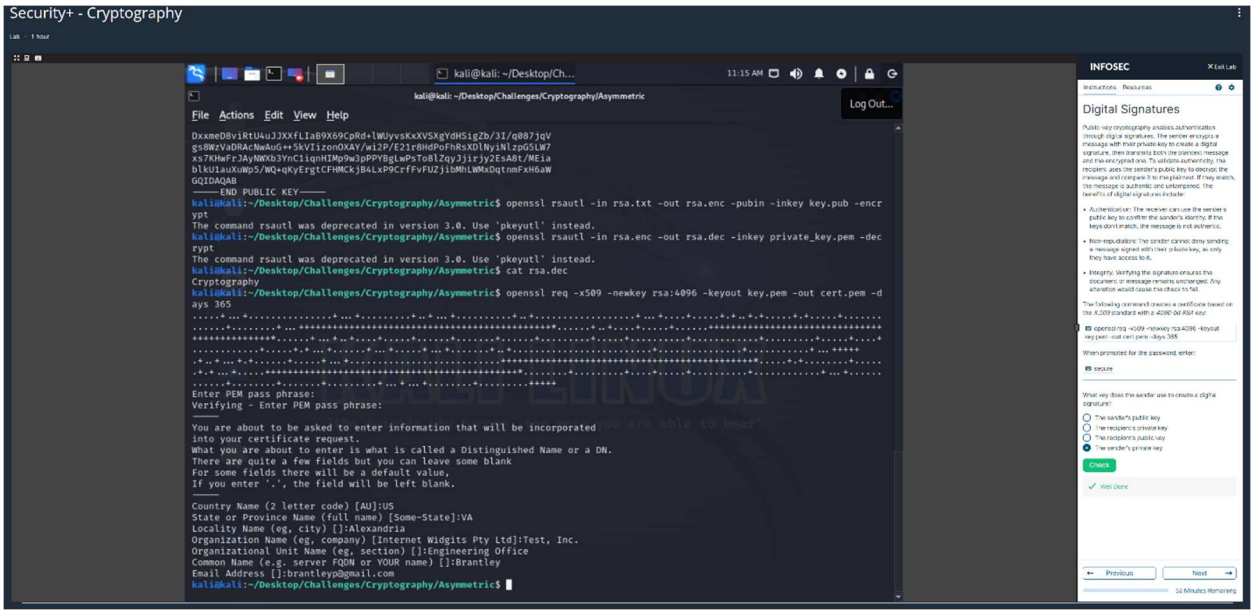

Figure 10: Digital Signature Creation

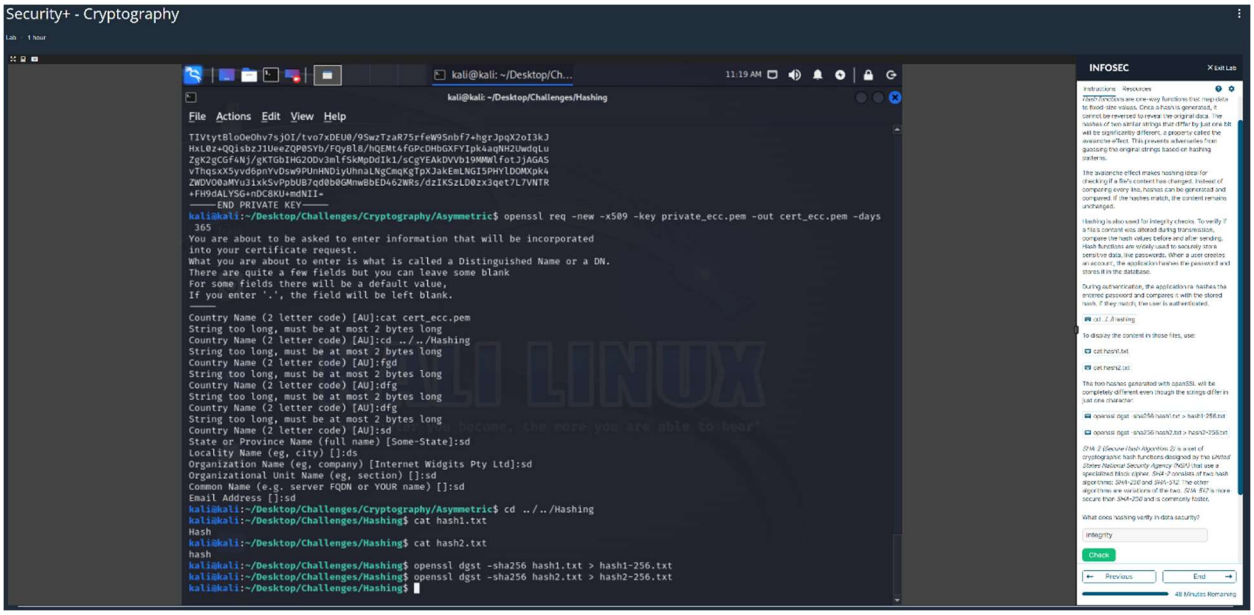

Figure 11: SHA256 Hashing Functions/Final Cryptography Slide

References

Barman, A. (2023, March 29). Secure Network with Iptables Firewall Demo. *Kubesimplify*. https://blog.kubesimplify.com/iptables-demo

Poggi, N. (2025, June 2). *Symmetric and asymmetric encryption explained: RSA vs. AES*. Retrieved July 26, 2025, from https://preyproject.com/blog/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes

Reed, J. (2024, November 15). Cybersecurity dominates concerns in the C-suite, small businesses, and the nation. *IBM Thnk*. Retrieved July 26, 2025, from https://www.ibm.com/think/insights/cybersecurity-dominates-concerns-c-suite-small-businesses-nation

Washington University. (2025). *Confidentiality, Integrity, and availability: The CIA triad*. Office of Information Security. Retrieved July 26, 2025, from https://informationsecurity.wustl.edu/guidance/confidentiality-integrity-and-availability-the-cia-triad/