Lab 8 Report

Jason Tolbert

The Pennsylvania State University

IST 894-001: Capstone Experience

Dr. Michael Bartolacci, Instructor

March 23rd, 2024

Table of Contents

General Overview

This lab introduces participants to two foundational cybersecurity concepts: cryptography and access control.

Cryptography

The first half of the lab explores basic cryptographic techniques. Participants begin by exploring Steganography. Steganography is the practice of concealing secret information within nonsecret media. The nonsecret media can be text, images, videos, or just about anything else. Images are the most common choice, due to their ubiquity on the internet and the diverse array of methods that can be used to hide information within them (Johnson & Jajodia, 1998; Morkel et al., n.d.). Lab participants use command-line tools to extract hidden message from image files and understand how data can be covertly embedded and later recovered.

The lab then switches topics to encryption algorithms. Participants are introduced to both symmetric algorithms (in which the same key is used for both encryption and decryption) and asymmetric algorithms (in which the encryption key is different from the decryption key) (Yassein et al., 2017). The lab demonstrates these algorithms through the use of OpenSSL, a popular open-source SSL/TLS implementation that also includes a robust suite of cryptography tools.

Access Control

The second half of the lab focuses on access control — or Authentication, Authorization, and Accounting (AAA) to be specific. Much of this half lab focuses on securing remote access via SSH. Participants compare key pair-based SSH authentication with password-based SSH authentication and learn how key pairs provide significantly stronger security. Participants also explore best practices for securing SSH passwords (e.g., using a password manager and never reusing the same password for multiple machines) that they can apply in situations where key pair authentication is not an option.

This part of the lab also touches on Unix file permissions. On Linux and other Unix-like systems, each file has three categories of permissions: 1) permissions that apply only to a given user, 2) permissions that apply to a group of users, and 3) permissions that apply to users who don't fall in either of the other categories. Within each category, there are three permissions that can be set: permission to read the file, permission to write to the file, and permission to execute the file. (Grampp & Morris, 1984) Lab participants are taught how these permissions work, how to modify them, and how the ways different users are able to interact with files can change based on the permissions that have been set.

Technical Overview

This lab introduces participants to two foundational cybersecurity concepts: cryptography and AAA.

Cryptography

Participants being the cryptography portion of the lab with an introduction to steganography. Steghide is used to extract a secret message from a JPEG file, illustrating to participants how information steganographic techniques can be covertly hide and later retrieved without obviously altering the cover medium. Following that, participants use the OpenSSL cryptographic suite to practice encrypting and decrypting files. They're shown both symmetric algorithms, like DES, 3DES, and AES, and asymmetric algorithms, like RSA and ECC.

AAA

The AAA portion of these lab teaches participant several ways of controlling and securing access to Linux systems. Naturally, this means a substantial part of it is focused on the Unix permission system. Participants get hands-on experience using chmod, chown, and ls to configure and inspect permissions for files and directories. Once they've been introduced the basic r-w-x syntax, they learn how to convert it to octal notation. They also

switch user accounts throughout the lab to see firsthand how the permissions they've set have changed the way different users can interacting with the filesystem.

The lab then pivots to the subject of SSH — specifically, best practices when it comes to SSH credentials. They learn how key-pair authentication trades usability for stronger security, and how password-based authentication prioritizes usability at the expense of security. They also spend time working with the KeePass password manager and learn how to use it to securely store SSH passwords in the event that they must be used over key pairs.

References

Grampp, F. T., & Morris, R. H. (1984). The UNIX system UNIX operating system security. *AT&T Bell Laboratories Technical Journal*, *63*(8), 1649–1672. AT&T Bell Laboratories Technical Journal. https://doi.org/10.1002/j.1538-7305.1984.tb00058.x

Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer*, *31*(2), 26–34. Computer. https://doi.org/10.1109/MC.1998.4655281

Morkel, T., Eloff, J. H. P., & Olivier, M. S. (n.d.). *An overview of image steganography*.

Yassein, M. B., Aljawarneh, S., Qawasmeh, E., Mardini, W., & Khamayseh, Y. (2017). Comprehensive study of symmetric key and asymmetric key encryption algorithms. *2017 International Conference on Engineering and Technology (ICET)*, 1–7. https://doi.org/10.1109/ICEngTechnol.2017.8308215

Screenshots

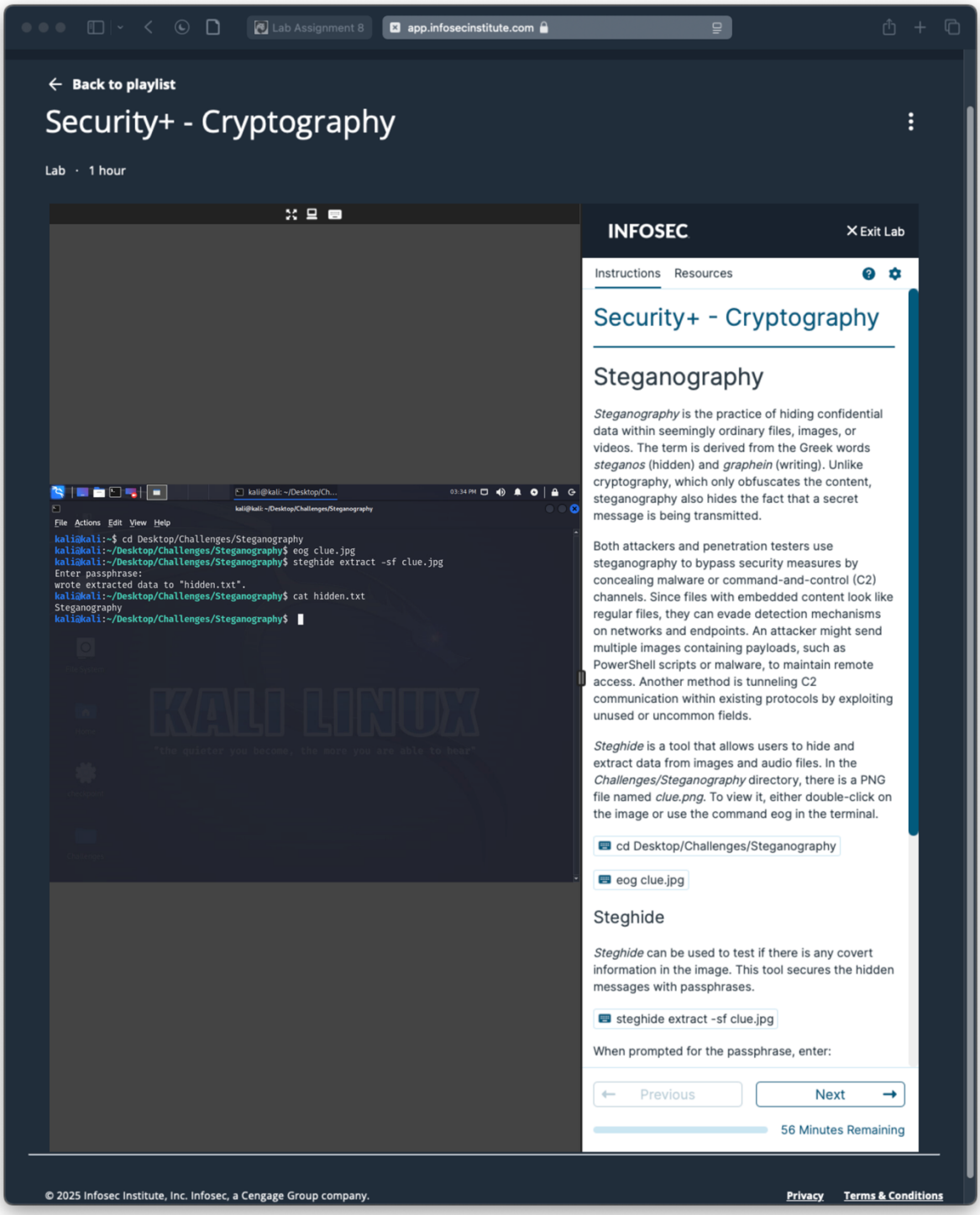

Figure 1. Viewing information hidden in the clue.jpg file.

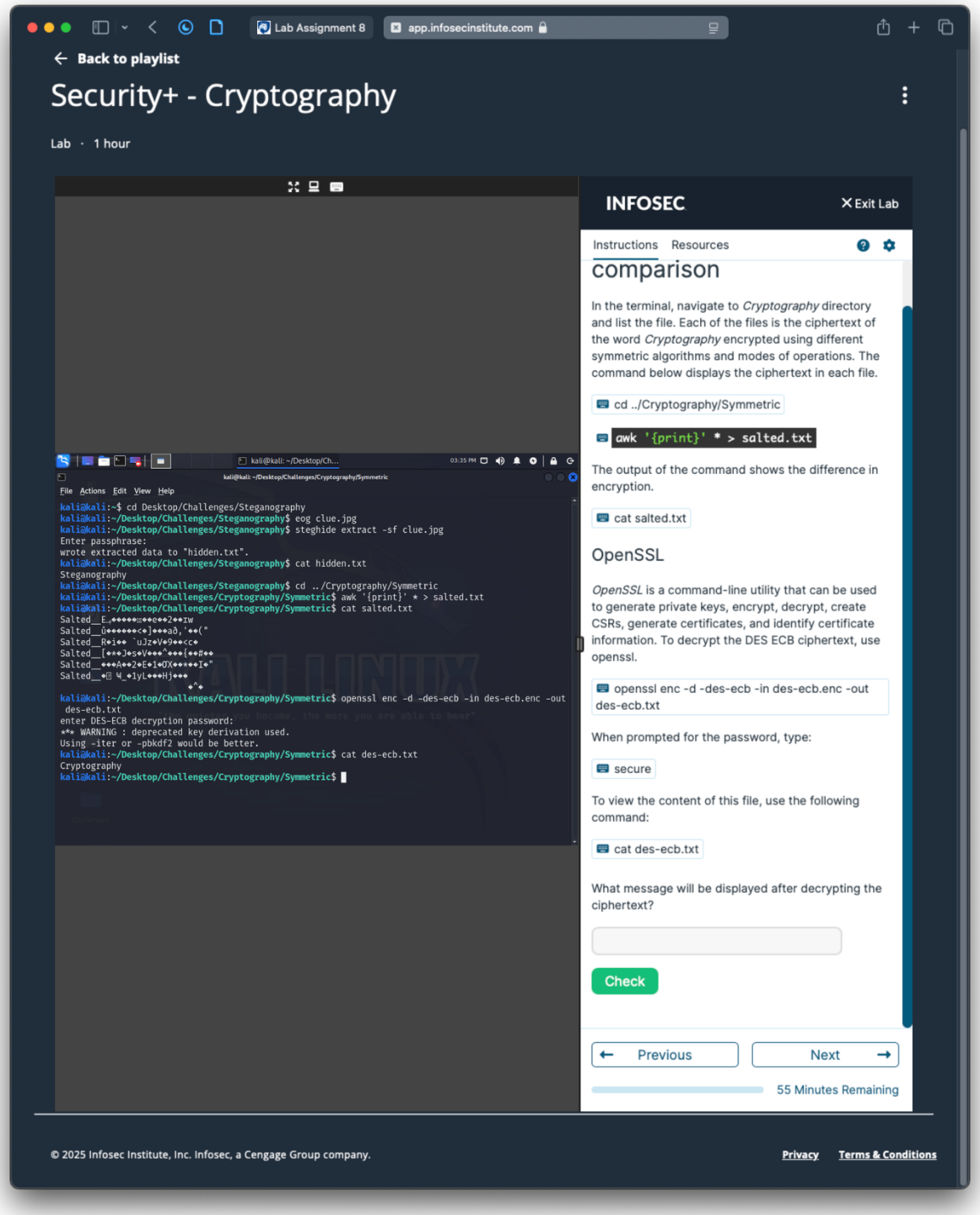

Figure 2. Decrypting DES-ECB ciphertext with OpenSSL.

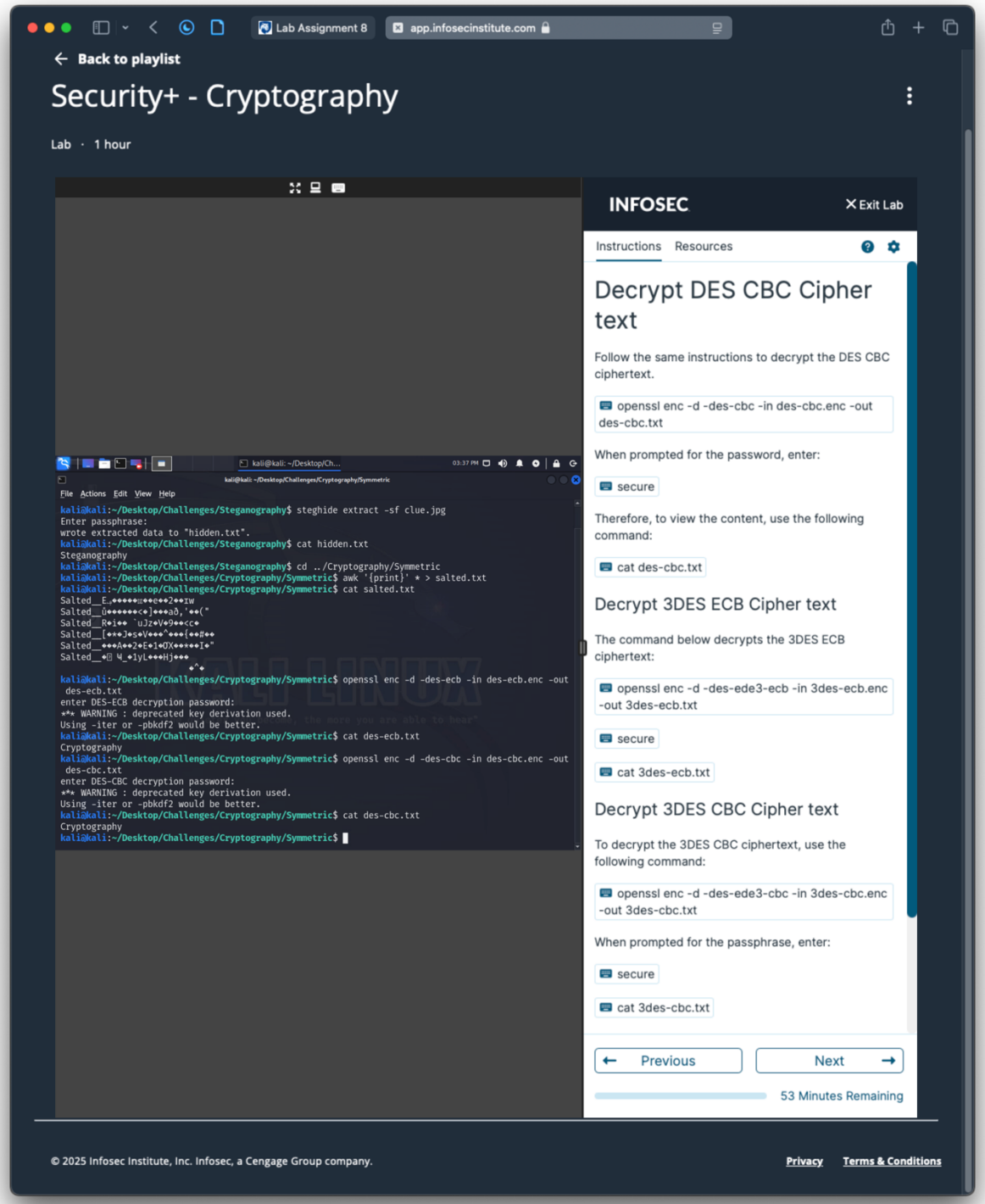

Figure 3. Decrypting DES-CBC ciphertext with OpenSSL.

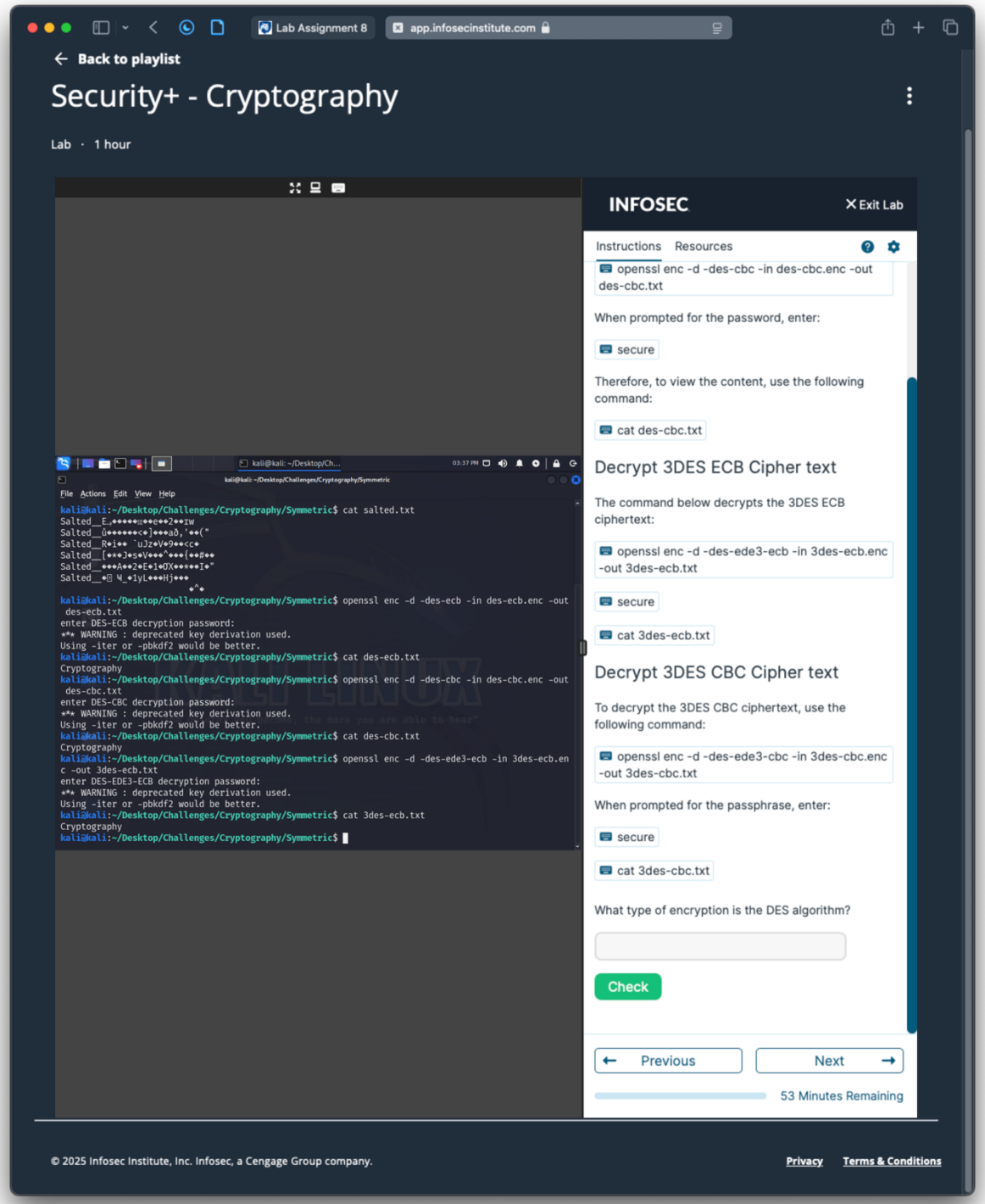

Figure 4. Decrypting 3DES-ECB ciphertext with OpenSSL.

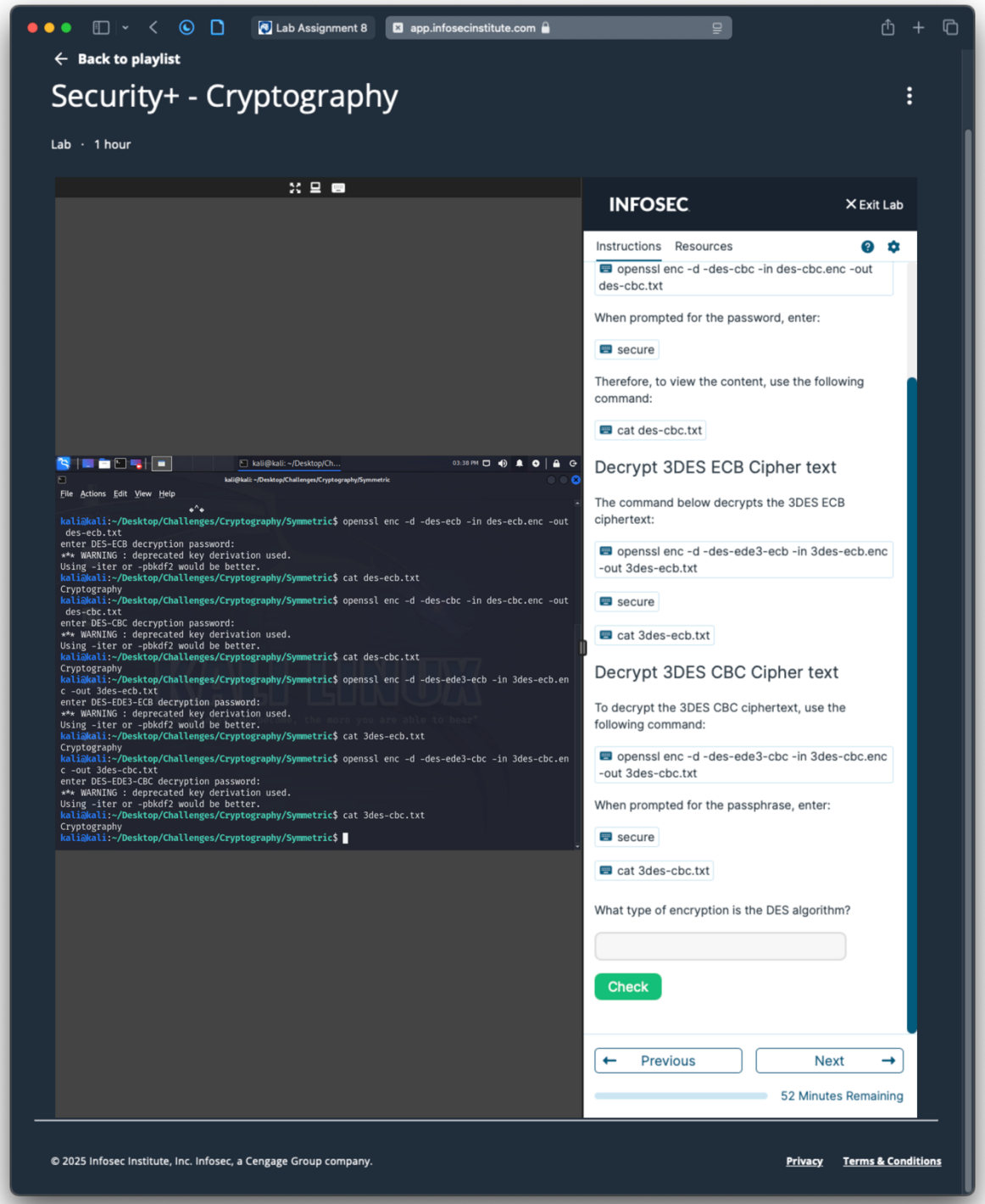

Figure 5. Decrypting 3DES-CBC ciphertext with OpenSSL.

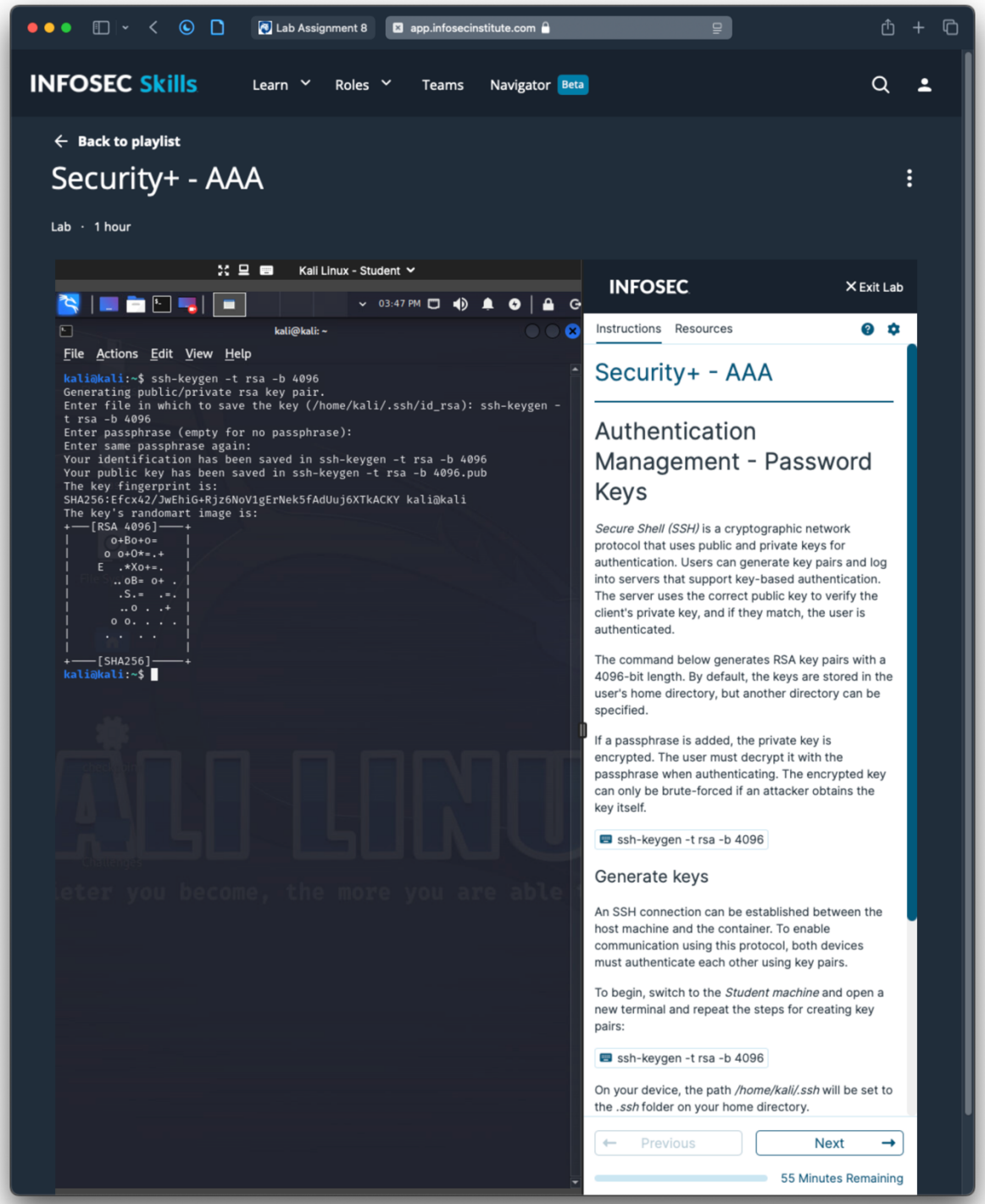

Figure 6. Creating an SSH keypair.

Figure 7. Connecting to 192.168.1.100 with the SSH key generated in Figure 6.

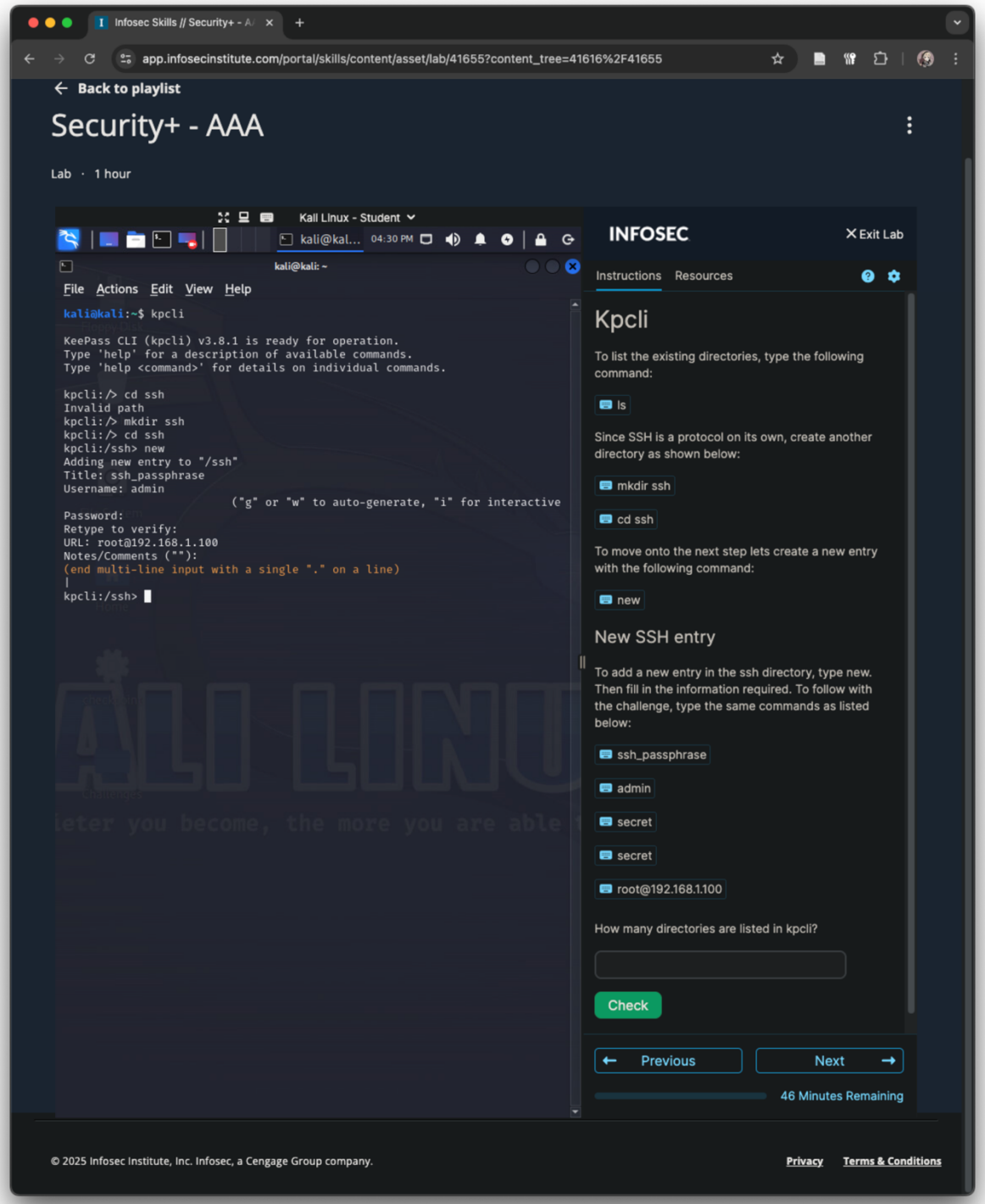

Figure 8. Adding SSH credentials to KeePass.

Figure 9. Saving and viewing the changes made to the KeePass database in Figure 8.

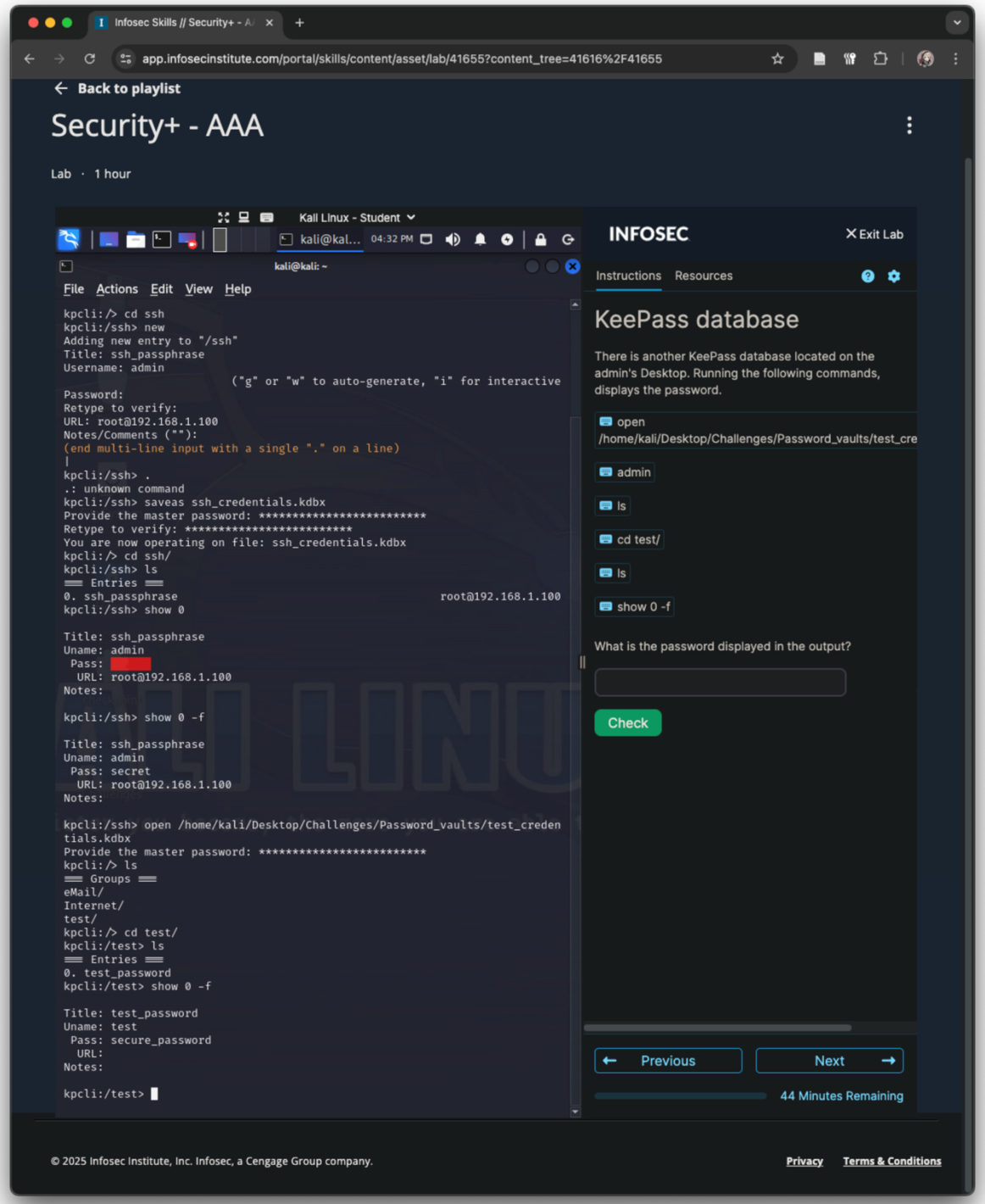

Figure 10. Viewing the test_password entry in the test_credentials KeePass database.