PennState
College of Information
Sciences and Technology

Lab Assignment Report

COURSE:	**IST 894**
ASSIGNMENT:	**LAB ASSIGNMENT REPORT 6**
SUBMITTED BY:	**BRANTLEY PRICE**
DUE DATE:	**JULY 13TH, 2025**
INSTRUCTOR:	**DR. BARTOLACCI**

Contents

General Context

This lab report covers two cyber range exercises from the Infosec Advanced Adversary Tactics cyber range: Privilege Escalation, XSS, and Defense Evasion. The goal of the two exercises was for the student to simulate real-world attacker behavior on a vulnerable web application and a Linux host, respectively. Both exercises demonstrated how an adversary may be able to bypass typical safeguards to gain unauthorized access, be it through cross-site scripting or planting a persistent backdoor. The XSS portion of this lab is particularly relevant, as OWASP (n.d.) notes that the variety of attacks based on XSS is almost limitless.

The Privilege Escalation XSS exercise allowed the student to explore the concepts of client-side input validation, content sanitization, and session hijacking through cookie exploitation. Starting out as a "student" user, the student attempted to inject JavaScript payloads into a blog-posting feature that was vulnerable to XSS exploitation. The student crafted a payload to trigger an alert in the browser, which proved the exploitation capability. They then exploited the XSS vulnerability by hijacking a site administrator's session cookie via the payload and accessed their private post.

The Defense Evasion exercise moved from the web app to a Linux host and allowed the student to establish a persistent backdoor. Using Metasploit, the student shut down ClamAV, an open-source antivirus software, designed primarily for scanning emails for phishing attacks (Cisco Talos Intelligence Group, n.d.). After shutting ClamAV down, the student ran an Nmap port scan to ensure the port ClamAV was previously running on was indeed closed. Once this was confirmed, the student used a modified Pluggable Authentication Module (PAM) to create a backdoor by using a malicious PAM module to escalate to root privileges. Although shutting down detection services may not always be as simple as it seemed in this exercise, the exercise is still effective in driving home the point that continuous monitoring of systems is necessary.

Technical Context

The Privilege Escalation XSS lab showcased the importance of understanding how web apps can process and sanitize user input. Like with so many vulnerabilities, input validation and sanitization are key. In fact, Banach (2025) calls input validation errors “the root of all evil in web security.” To escalate privileges using XSS, the student embedded a script tag that referenced a JavaScript file they created and hosted on their Kali Linux machine. The filter being used appeared to focus only on inline code patterns, allowing the execution of a remote script to be successful. Once this script was executed, the student received session cookie information from all users who logged into the web app. As it turns out, using this cookie information, the student was able to inspect the page and input the hijacked cookie information to hijack the administrator’s session. This ultimately gave the student access to the administrator’s private page as they were effectively logged in as the administrator.

The Defense Evasion exercise used Metasploit to attack a Linux host. After using msfconsole to launch Metasploit, the student loaded the clamav_control auxiliary module, configured the target IP using RHOST, and discovered the ClamAV version running on the target machine. The student then used the ACTION SHUTDOWN command to shutdown ClamAV. To determine that port 3310 was closed, Nmap was used on the target. Port 3310 was indeed in a closed state, meaning ClamAV was no longer monitoring the system.

PAM is a robust authentication framework that can be used across many different applications. Research shows that proper PAM implementation can help organizations develop zero-trust architectures on Linux (Pietropaolo, 2023). That said, PAM is a double-edged sword and is vulnerable to exploitation, as evidenced by the student’s subsequent actions. Using the linux-pam-backdoor toolkit, the student was able to exploit the PAM framework by replacing the legitimate PAM with a malicious PAM. Using a

password the student provided to the module, they gained persistent root access to the machine, all while the monitoring mechanisms were disabled.

Screenshots

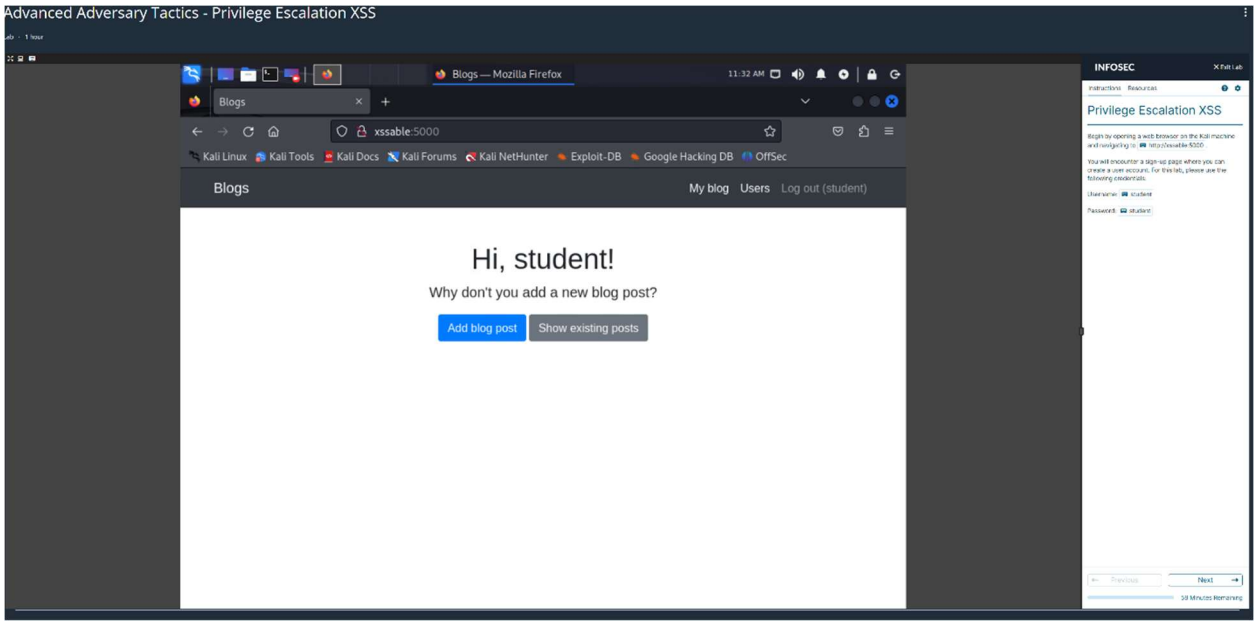

Figure 1: Logged into the Blog as "student"

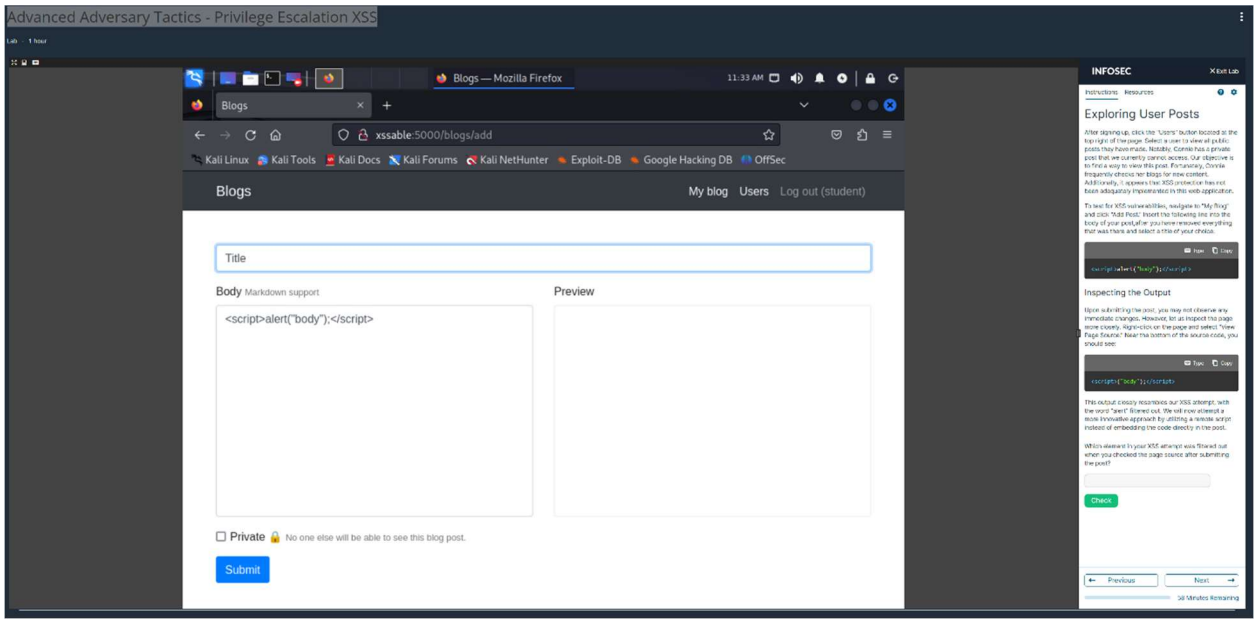

Figure 2: Testing the XSS Vulnerability

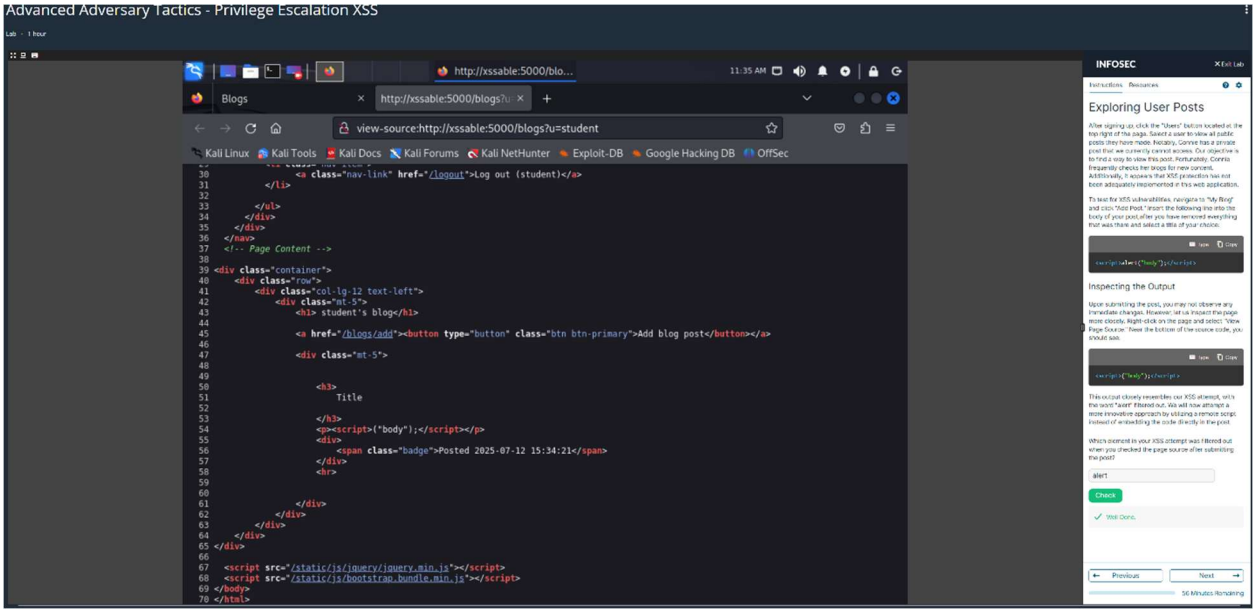

Figure 3: XSS Vulnerability Test Success

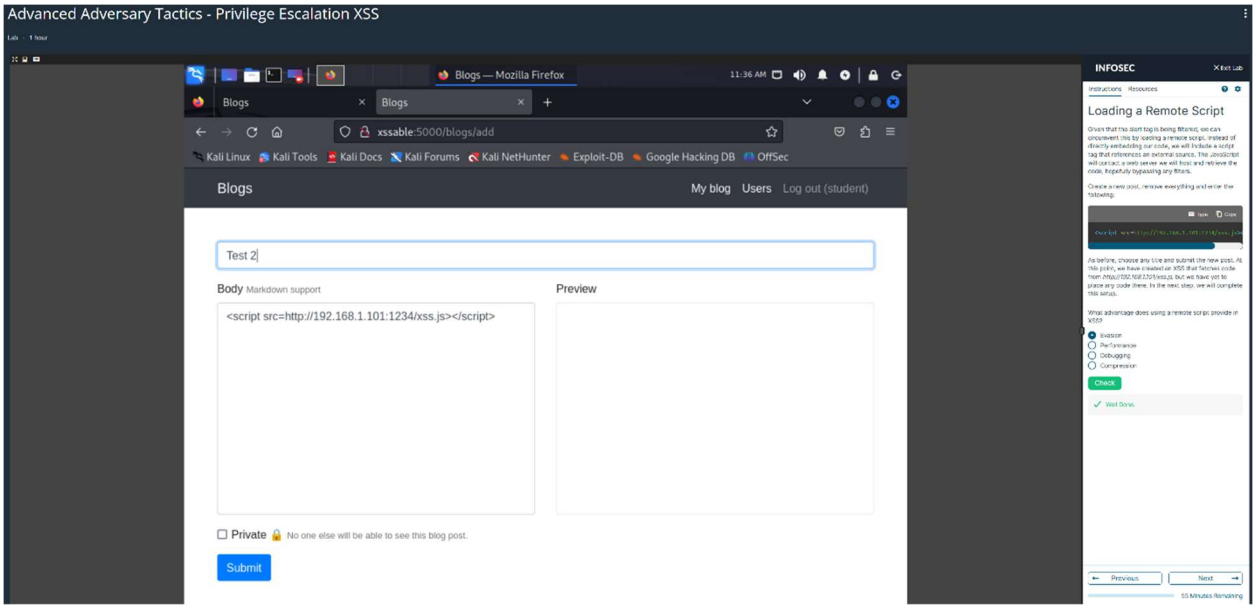

Figure 4: Preparing for Loading the Remote Script

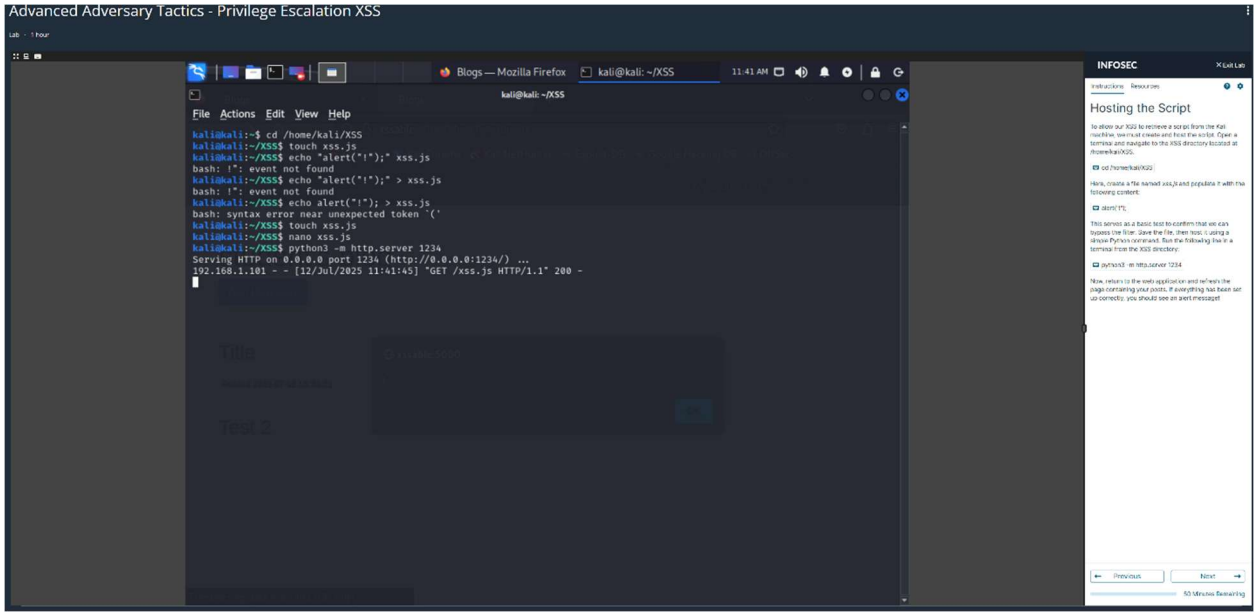

Figure 5: Creating the Script

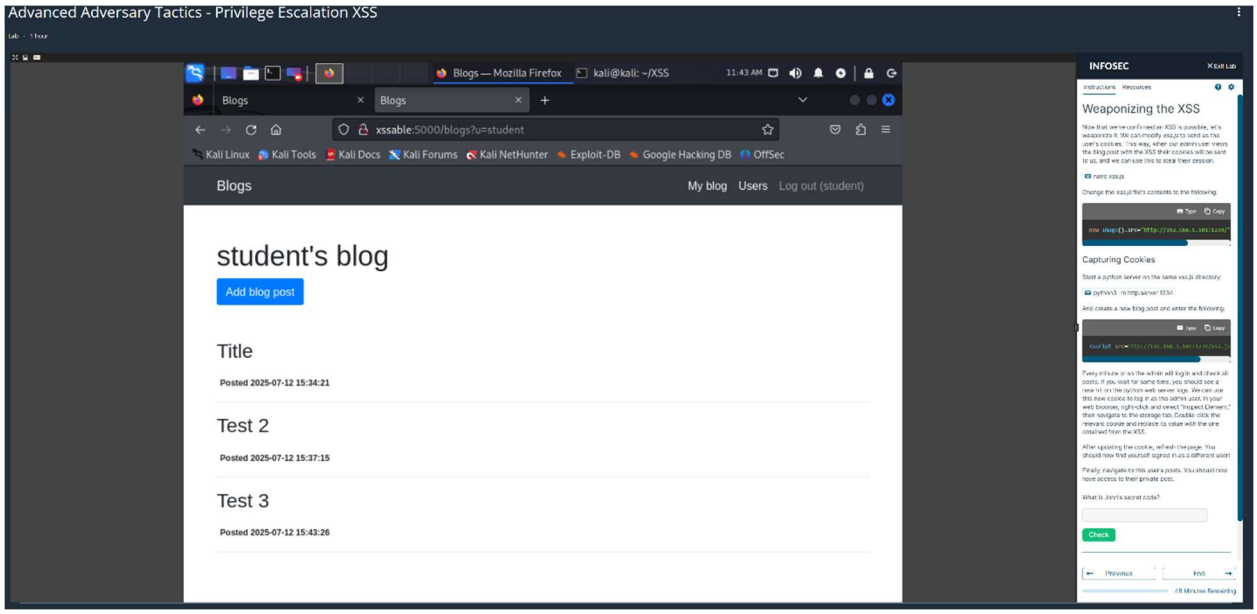

Figure 6: Weaponizing the Script

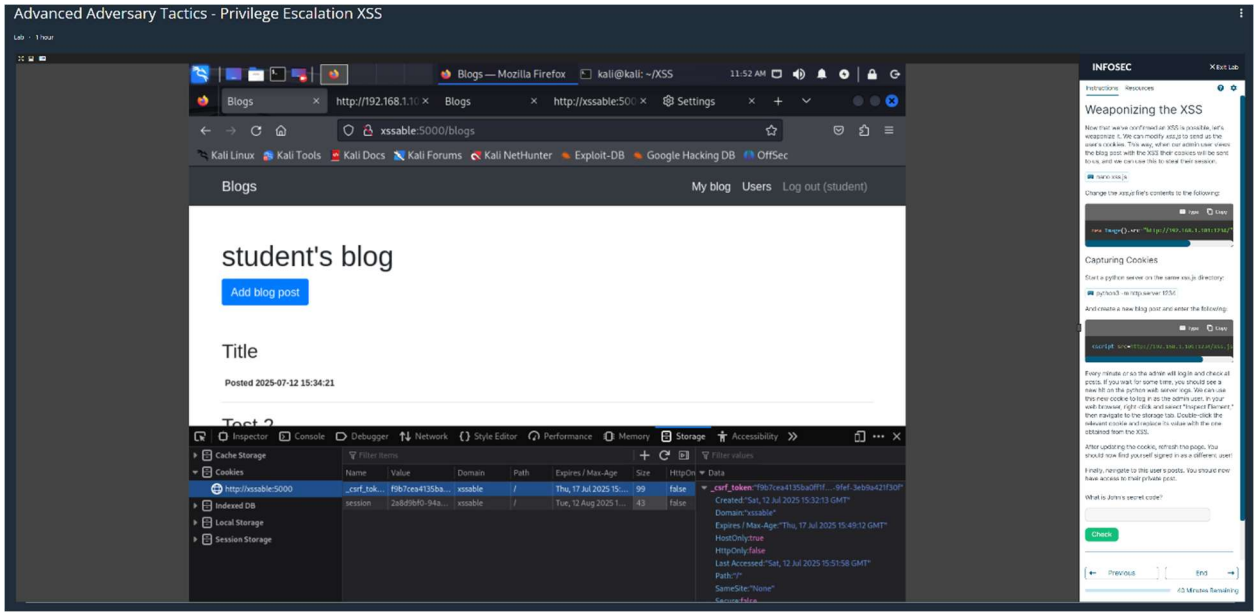

Figure 7: Inputting Hijacked Cookie Information (as student)

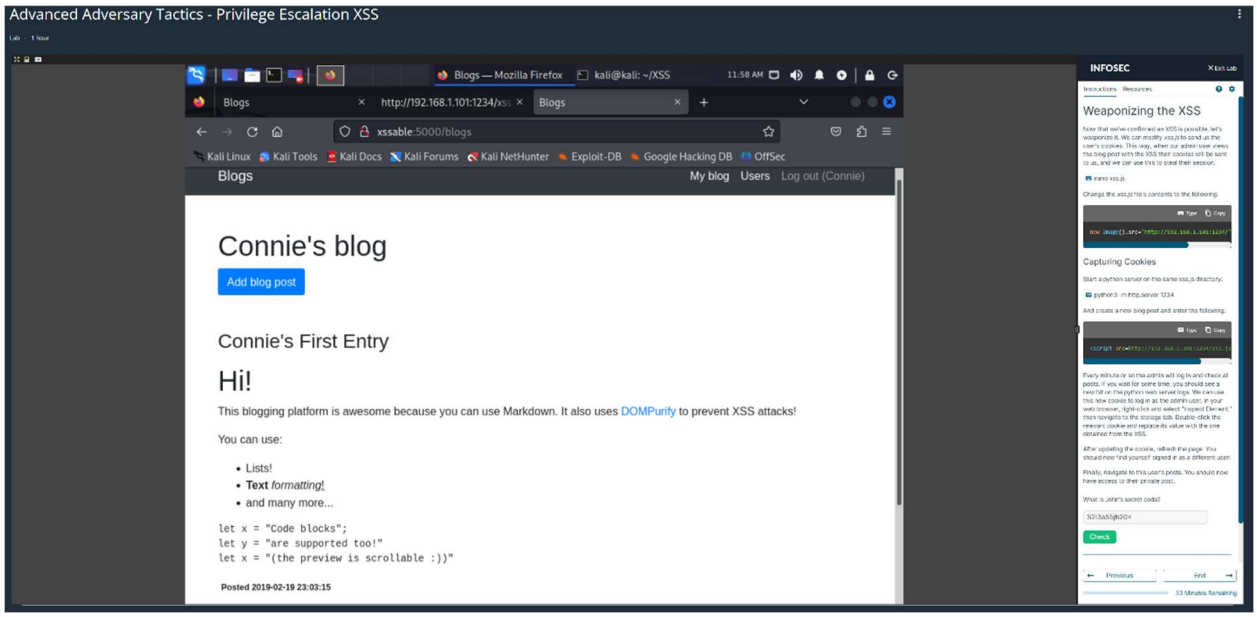

Figure 8: Successful Hijacking of Administrator (Connie) Account

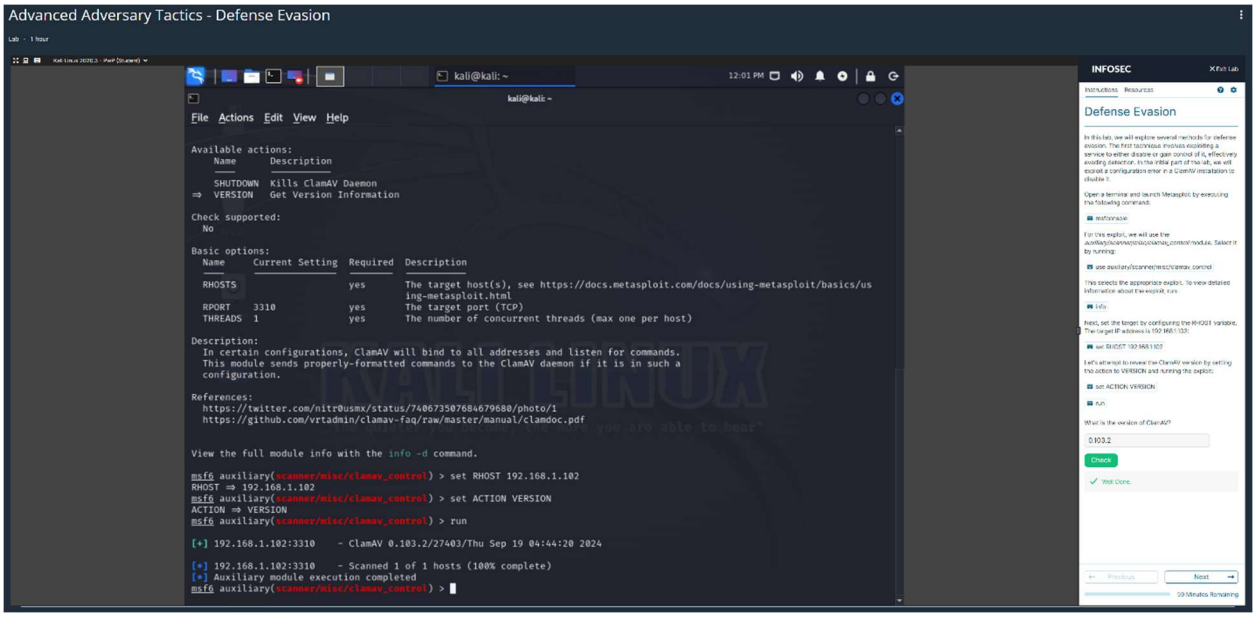

Figure 9: Using msfconsole and clamav_control Module to Prepare the Attack

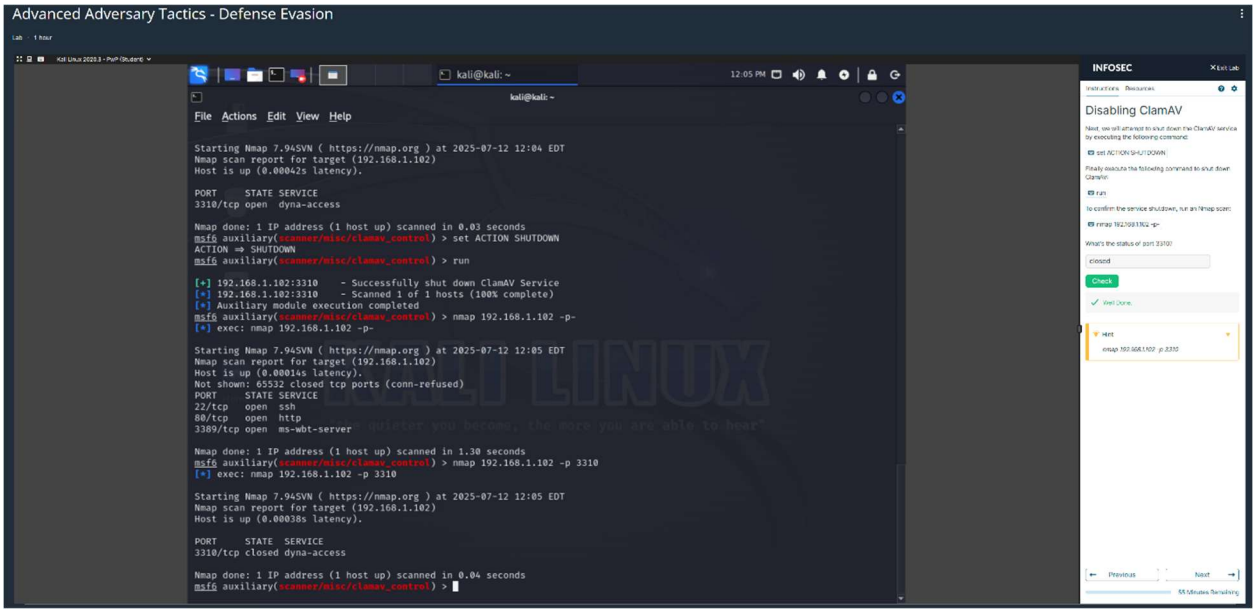

Figure 10: Nmap Probe to Verify 3310 is Closed

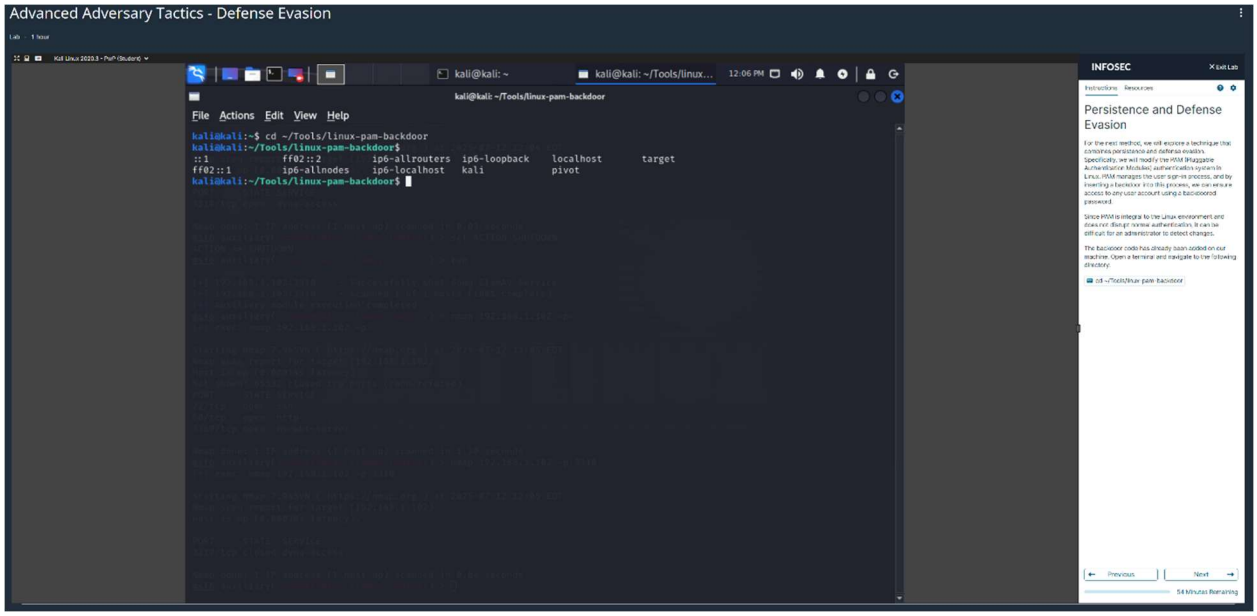

Figure 11: Accessing linux-pam-backdoor

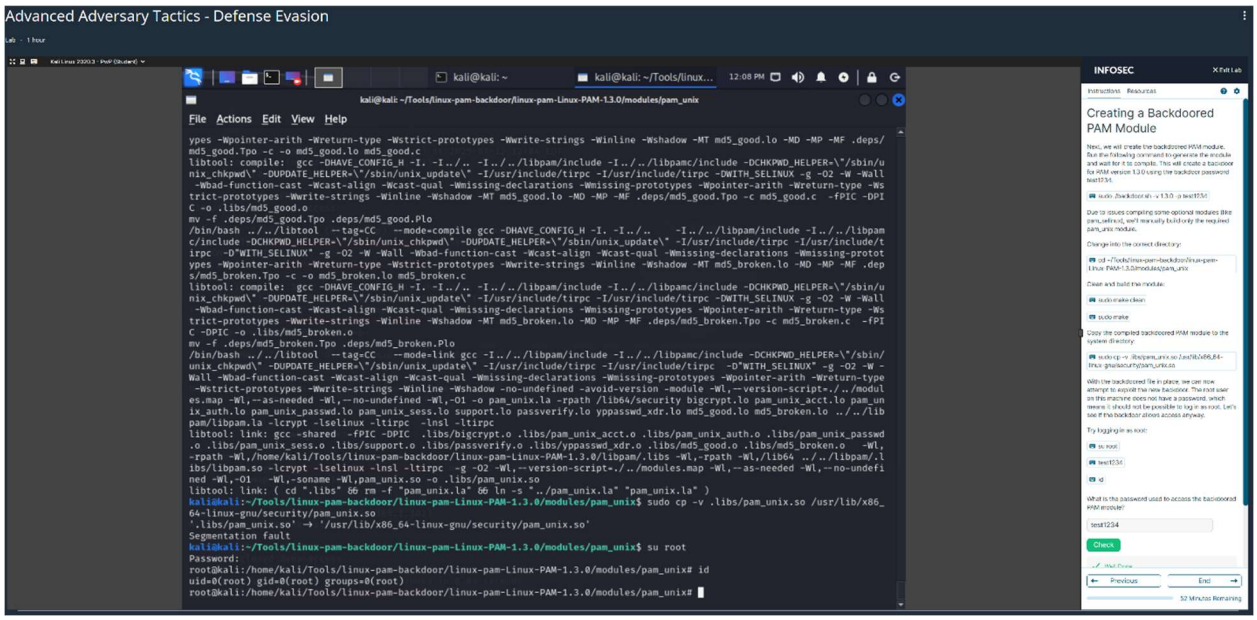

Figure 12: Successfully Replacing Authentic PAM with Backdoor PAM

References

Banach, Z. (2025, January 29). *Input Validation Errors: Vulnerability, Examples, Fixes, Missing Input, and more*. Invicti. https://www.invicti.com/blog/web-security/input-validation-errors-root-of-all-evil/

Cisco Talos Intelligence Group. (n.d.). *CLAMAV - Open-Source Antivirus Software Toolkit for UNIX*. Cisco Talos. Retrieved July 12, 2025, from https://www.talosintelligence.com/clamav

OWASP. (n.d.). *Cross Site Scripting (XSS)*. Retrieved July 12, 2025, from https://owasp.org/www-community/attacks/xss/

Pietropaolo, A. (2023, August 3). *SGNL brings Zero-Trust access to Linux*. Retrieved July 12, 2025, from https://sgnl.ai/2023/08/sgnl-brings-zero-trust-access-to-linux/