PennState
College of Information
Sciences and Technology

Lab Assignment Report

COURSE:	**IST 894**
ASSIGNMENT:	**LAB ASSIGNMENT REPORT 5**
SUBMITTED BY:	**BRANTLEY PRICE**
DUE DATE:	**JULY 5TH, 2025**
INSTRUCTOR:	**DR. BARTOLACCI**

Contents

General Context

This lab assignment covered two exercises within the Advanced Adversarial Tactics cyber range: Reconnaissance and Resource Development and Pivoting with ProxyChains. Both labs were malfunctioning and required a significant amount of troubleshooting to identify the issue. To be clear, this troubleshooting was not intended to be part of the lab; they simply were not operating correctly. The student needed to add information to the /etc/host file as well as restart the web server on the Target machine for both labs (screenshots below). That said, these two exercises, when functioning, show the early stages of a cyber-attack. While both are different, together they show the practical steps an attacker may take to compromise vulnerable networks. If the student ties the two together in chronological order, they are shown how an attacker can credential harvest and then use those credentials to access segmented systems.

The Recon and Resource Development exercise allowed the student to see a portion of development and intelligence gathering. Web scraping, employee enumeration, and word list generation were all key to the beginning steps of this exercise, which ultimately amounted to a form of phishing. To put a bow on things, the student utilized the Social Engineering Toolkit (SET), a popular collection of open-source utilities primarily used for red teaming purposes (Moyle, 2024), to clone a target site and initiate credential harvesting.

The Pivoting with ProxyChains exercise transitioned from phishing to targeting segmented networks. In this exercise, the student configured multiple layers of tunneling using proxies to pivot through hosts to reach what would usually be unreachable systems. Network segmentation, when executed correctly, makes it very difficult for attackers to move across a network by isolating segments, thereby reducing the attack surface (Vaideeswaran, 2025). This exercise demonstrated that by chaining traffic through SOCKS proxies via SSH tunnels, attackers can access otherwise inaccessible systems, provided they have obtained the necessary credentials to do so.

Technical Context

The Reconnaissance and Resource Development exercise showed the student fairly advanced phishing techniques. To begin, the student needed to navigate to the target system and add "192.168.1.102 target" to the /etc/hosts file. Once done, the student needed to run "sudo systemctl restart nginx" to restart the web server. This needed to be done at the beginning of both labs; otherwise, they would not run properly. This information was not provided in the instructions; however, if it was not completed, the student was unable to move forward. Once this was completed, the student began working with the cewl tool to crawl the target website for email addresses to phish for credentials. Gobuster was used to enumerate the /downloads and /news directories on the target site. These directories were hidden initially, and within the /new directory, the student found an employee contact list.

Once the reconnaissance portion of the exercise was complete, the student moved on to the social engineering aspect and began using the SET to clone the login page of the target website, which is meant to be served to the target organization without their knowledge. As users attempt to log in, their credentials will be provided to the attacker in plaintext. This attack could have been stopped with multi-factor authentication, as according to OWASP (n.d.), "MFA is by far the best defense against the majority of password-related attacks…with Microsoft suggesting it would stop 99.9% of account compromises."

Moving to the Pivoting with ProxyChains exercise, the student was given the opportunity to see technical methods that can be used to move through a segmented, but compromised infrastructure using SSH and ProxyChains. For context, ProxyChains is a tool that forces any TCP connection to connect through a proxy (Haad, 2023). For this exercise, SOCKS4, an older proxy protocol that lacks features like authentication (Tamuliunait, 2025), serves the purpose of hiding the attacker's IP address to obfuscate the fact that the traffic is flowing to them. An SSH tunnel was established, and then ProxyChains was used

to route all outbound traffic on this port through the SSH tunnel. This was done by forwarding traffic from the pivot machine, with a SOCKS4 proxy listening on port 9050 for any traffic passing through. Effectively, any data passing over port 9050 from the target machine to the trusted pivot machine is also shared with the attacker's IP, via the SOCKS4 proxy through the SSH tunnel. These two exercises provide clear evidence of how credential harvesting can evolve into a deep infiltration of a network, even when a layered defense concept is in place.

Screenshots

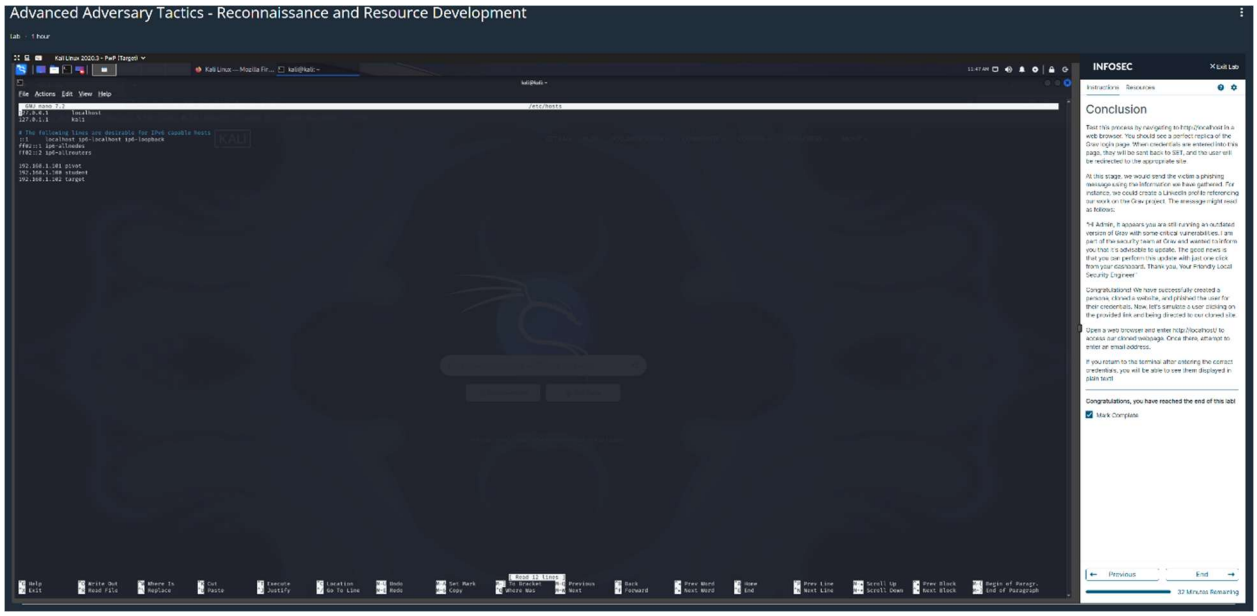

Figure 1: Troubleshooting – Adding information to /etc/hosts

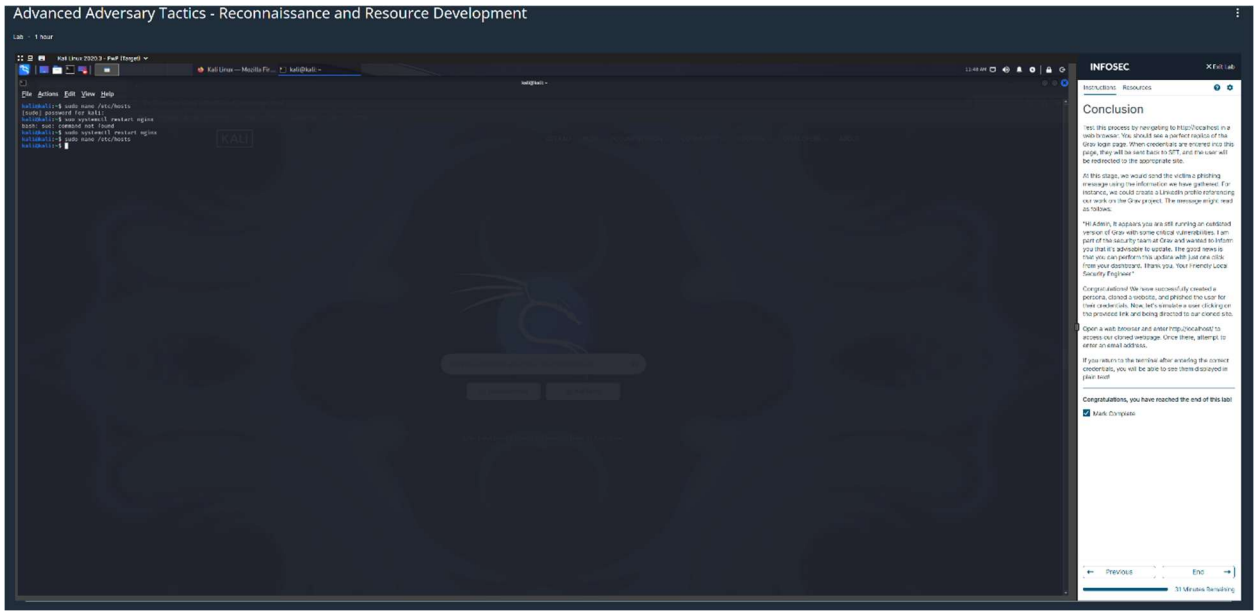

Figure 2: Troubleshooting – Restarting the Web Server

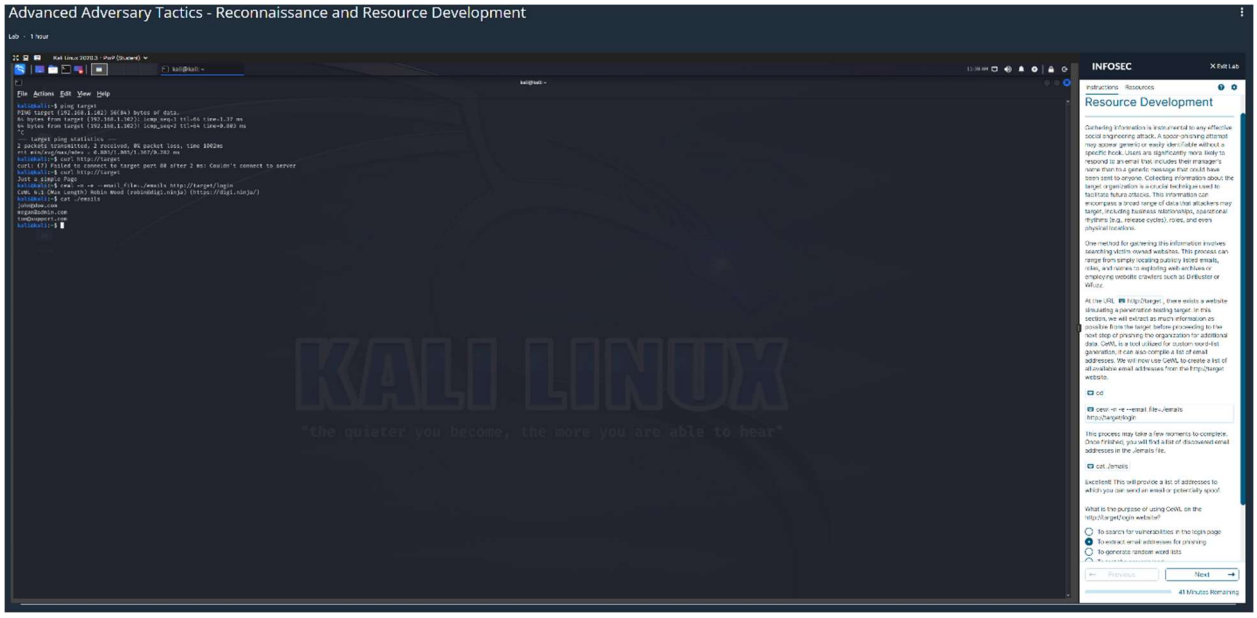

Figure 3: Using Cewl to Scrape Email Addresses

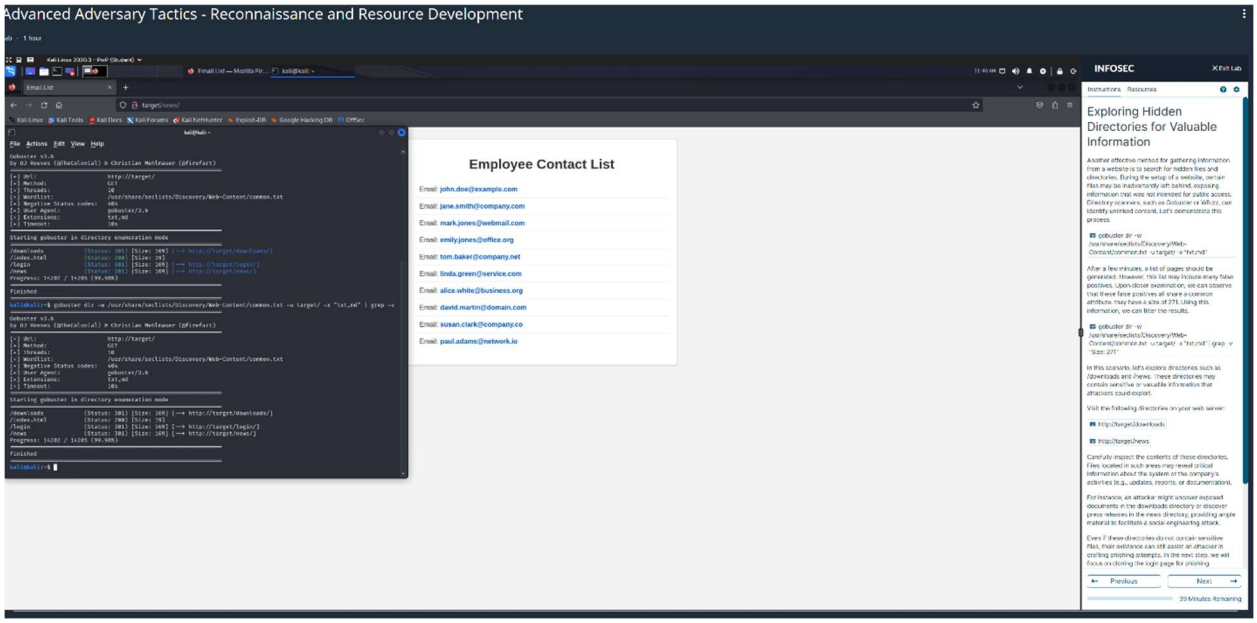

Figure 4: Gobuster Enumeration

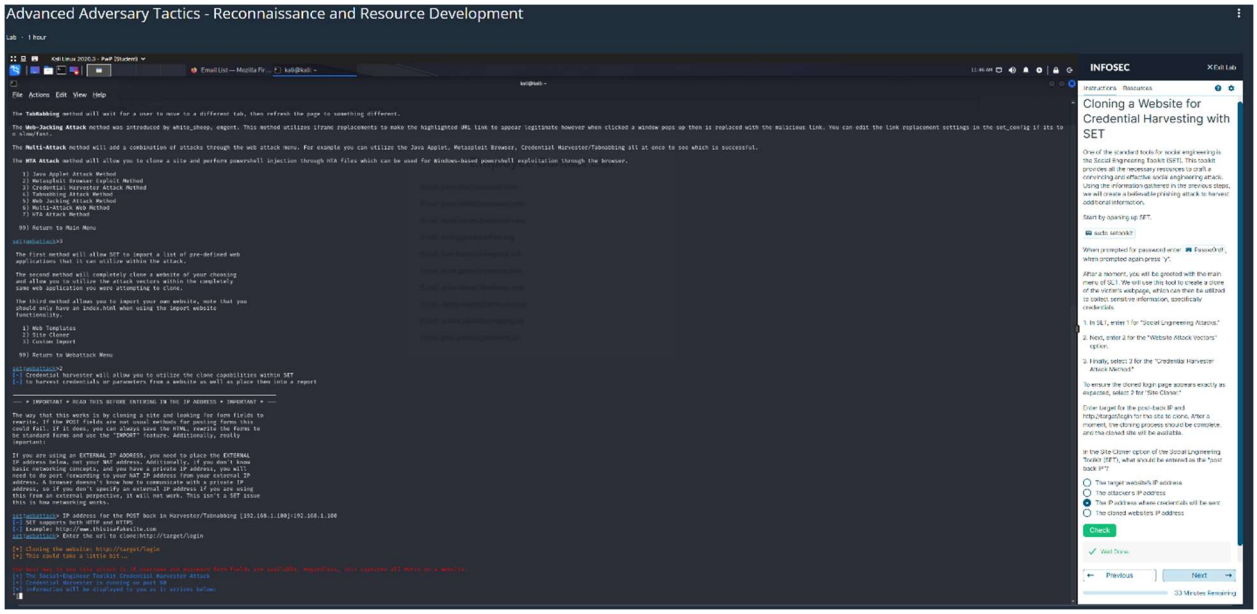

Figure 5: SET Website Cloning

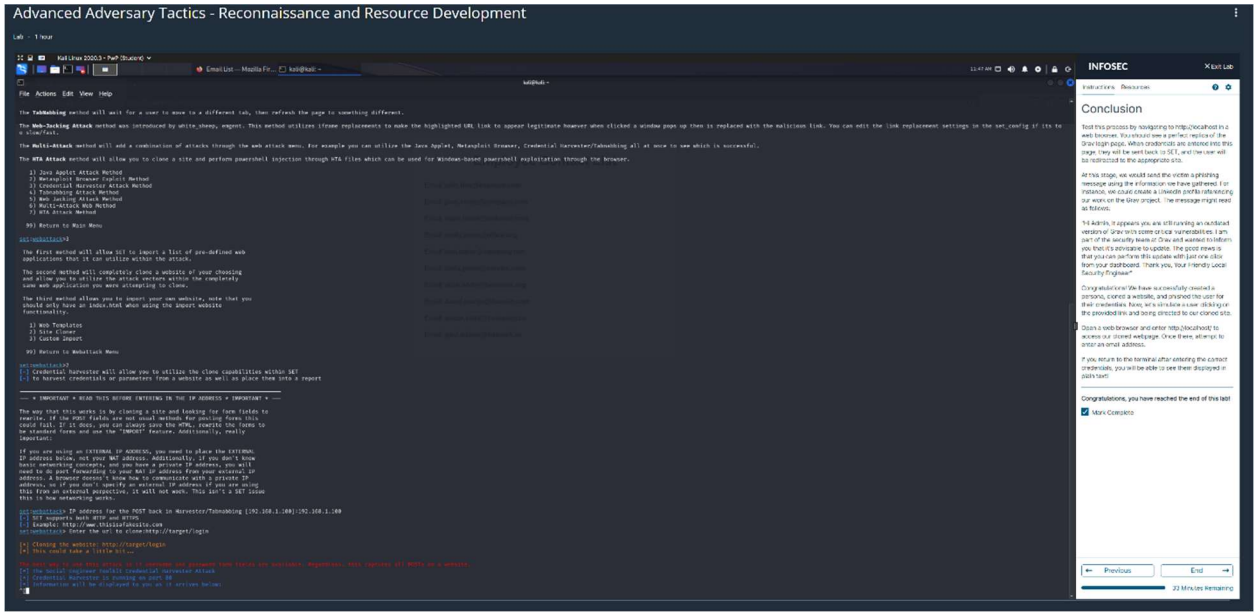

Figure 6: Recon and Resource Development Conclusion

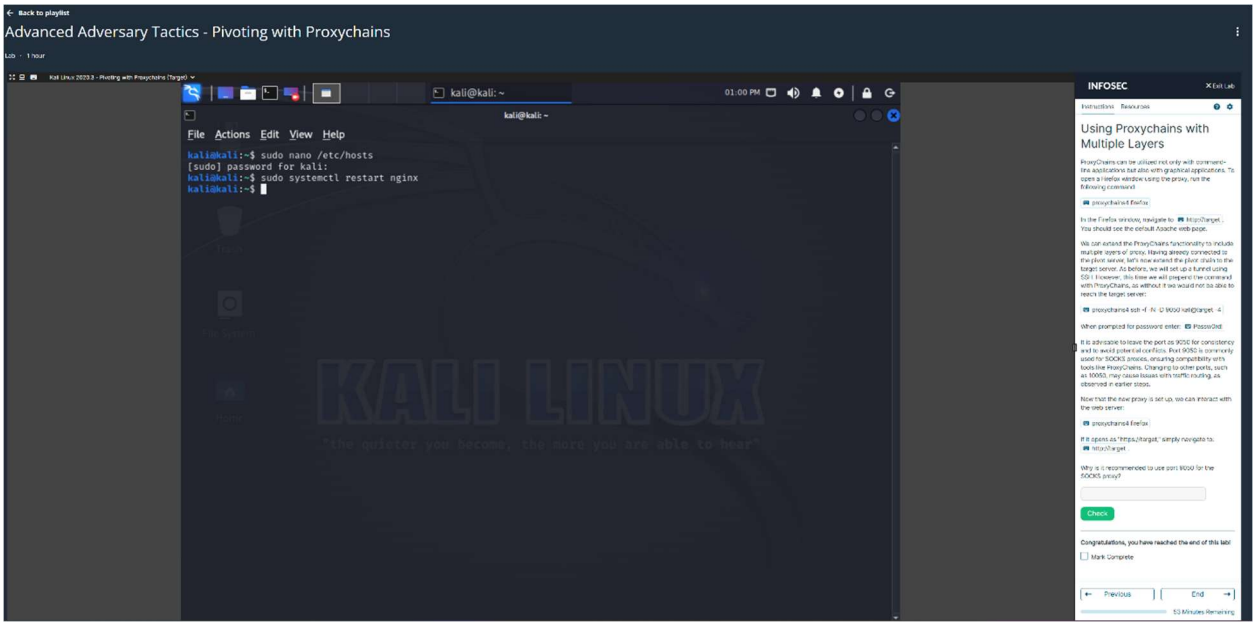

Figure 7: Pivoting with ProxyChains Troubleshooting – Same as Exercise 1

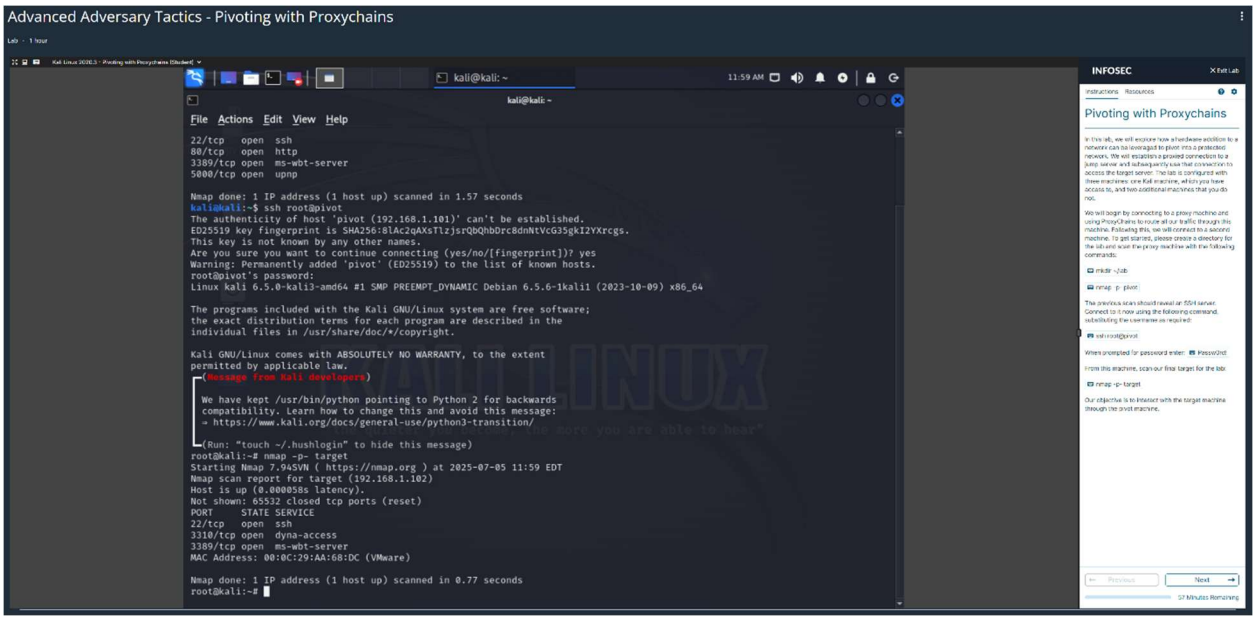

Figure 8: Nmaping in Preparation for ProxyChains Setup

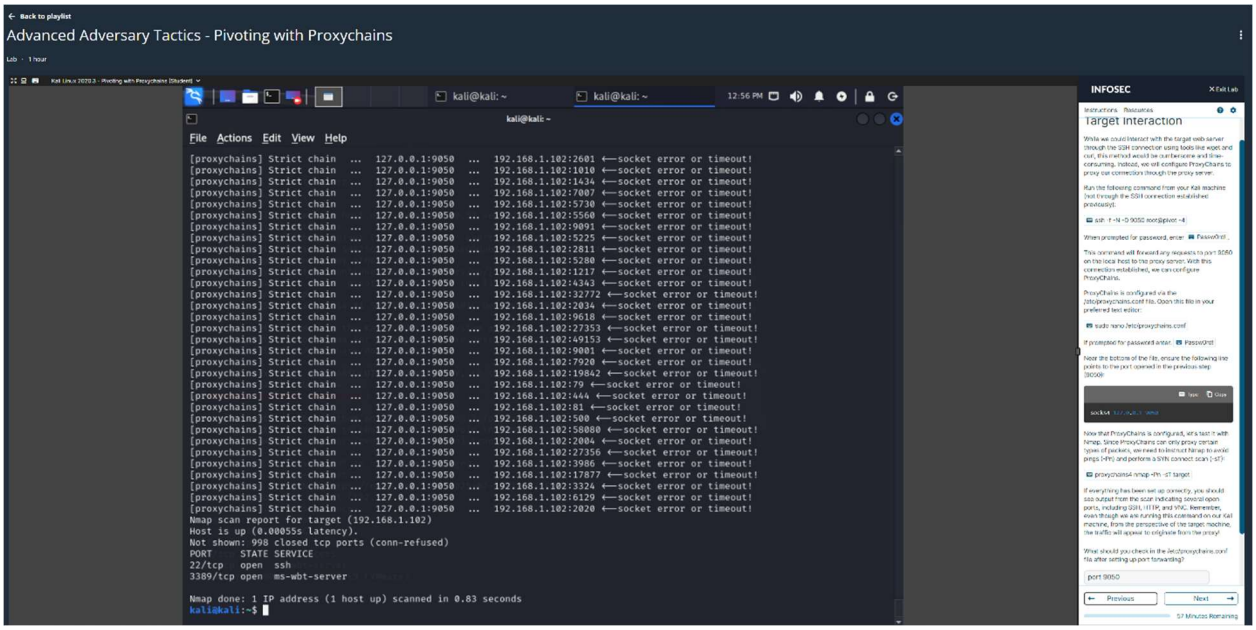

Figure 9: ProxyChains Setup / SOCKS4 Proxy Setup

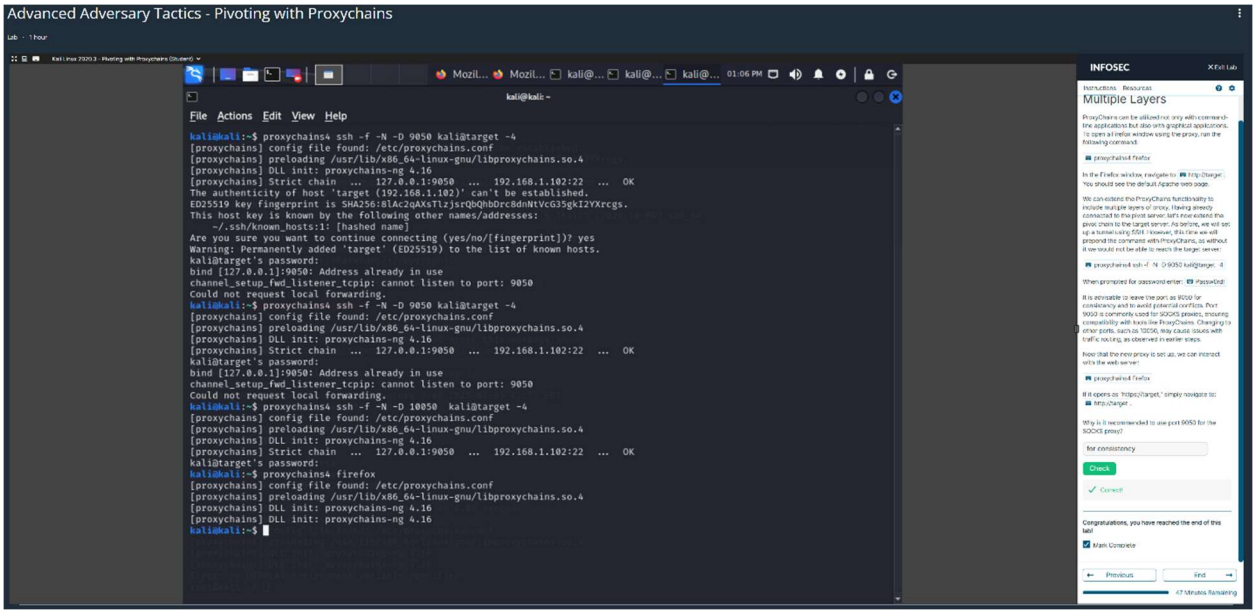

Figure 10: Layering the Attack

References

Haad. (2023). *GitHub - haad/proxychains*. GitHub. https://github.com/haad/proxychains

Moyle, E. (2024, June 28). *How to use Social-Engineer Toolkit*. Search Security. https://www.techtarget.com/searchsecurity/tutorial/How-to-use-Social-Engineer-Toolkit

OWASP. (n.d.). *Credential Stuffing Prevention*. OWASP Cheat Sheet. Retrieved July 5, 2025, from https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html

Tamuliunait, V. (2025, May 30). *SOCKS vs HTTP Proxy: What Is the Difference?* Retrieved July 5, 2025, from https://oxylabs.io/blog/socks-vs-http-proxy

Vaideeswaran, N. (2025, January 8). *What is Network Segmentation?* Crowdstrike.com. Retrieved July 5, 2025, from https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/network-segmentation/