Lab 2 Report

Jason Tolbert

The Pennsylvania State University

IST 894-001: Capstone Experience

Dr. Michael Bartolacci, Instructor

February 9th, 2025

Table of Contents

General Overview

This lab introduces participants to network reconnaissance, vulnerability assessment, and security auditing — all taught primarily through the application of Nmap, a widely-used network scanning program. Participants use Nmap to identify open ports, outdated services, and vulnerable network configurations on a remote machine.

The lab explores the use of automation in cybersecurity through the Nmap Scripting Engine (NSE). NSE allows users to write scripts that automate various Nmap tasks. Studies show that automated scanners can significantly reduce the time vulnerability assessments take without compromising accuracy (Ifeyinwa et al., 2019).

Research highlights that effective security assessments combine both manual and automated approaches (Railkar, 2022). The lab reinforces this by teaching participants how to inspect and analyze Nmap's scans for themselves and identify key information that could help inform them of potential security risks.

Though most of the lab covers high-level network reconnaissance with Nmap, a small part of it is dedicated to lower-level network testing via hping — an open-source tool that can create custom TCP, UDP, and ICMP packets. Participants use hping to simulate network traffic and examine the specifics of how the lab's virtual machine responds to it.

Technical Overview

This lab provides detailed introductions to network reconnaissance, service enumeration, and vulnerability analysis. Nmap's TCP connect and SYN scanning modes are used to show participants how ports and services on remote machines can reveal information that might indicate vulnerabilities. These scans rely on packet-based probes and responses to determine whether ports are open, filtered, or closed and to reveal specific network services and machine characteristics (Liao et al., 2020).

Participants additionally learn how to conduct service OS fingerprinting with Nmap. Studies have shown that such fingerprinting is key to narrowing down potential security issues; different versions of a software program or operating system may widely vary in the vulnerabilities they are susceptible to (Nikiforakis & Kondracki, 2024). Inaccurate fingerprinting may raise false alarms about vulnerabilities that are not actually relevant — or worse, create ignorance of vulnerabilities that are.

The lab also teaches participants how to conduct low-level network security testing using hping and tcpdump. Participants use hoping to create and send their own TCP packets and use tcpdump to record and analyze the contents of those packets on the receiving end.

References

Ifeyinwa, A., Sunday, A., & C, E. P. (2019). Network Vulnerability Analysis. *International Journal of Computer (IJC)*, *34*(1), 129–139.

Liao, S., Zhou, C., Zhao, Y., Zhang, Z., Zhang, C., Gao, Y., & Zhong, G. (2020). *A Comprehensive Detection Approach of Nmap: Principles, Rules and Experiments*. 64–71. https://doi.org/10.1109/CyberC49757.2020.00020

Nikiforakis, N., & Kondracki, B. (2024, June 27). *Understanding and Improving Web Application Fingerprinting with WASABO*. USENIX. https://www.usenix.org/publications/loginonline/understanding-and-improving-web-application-fingerprinting-wasabo

Railkar, D. (2022). A Study on Vulnerability Scanning Tools for Network Security. *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, *8*, 340. https://doi.org/10.32628/CSEITCN228641

Screenshots

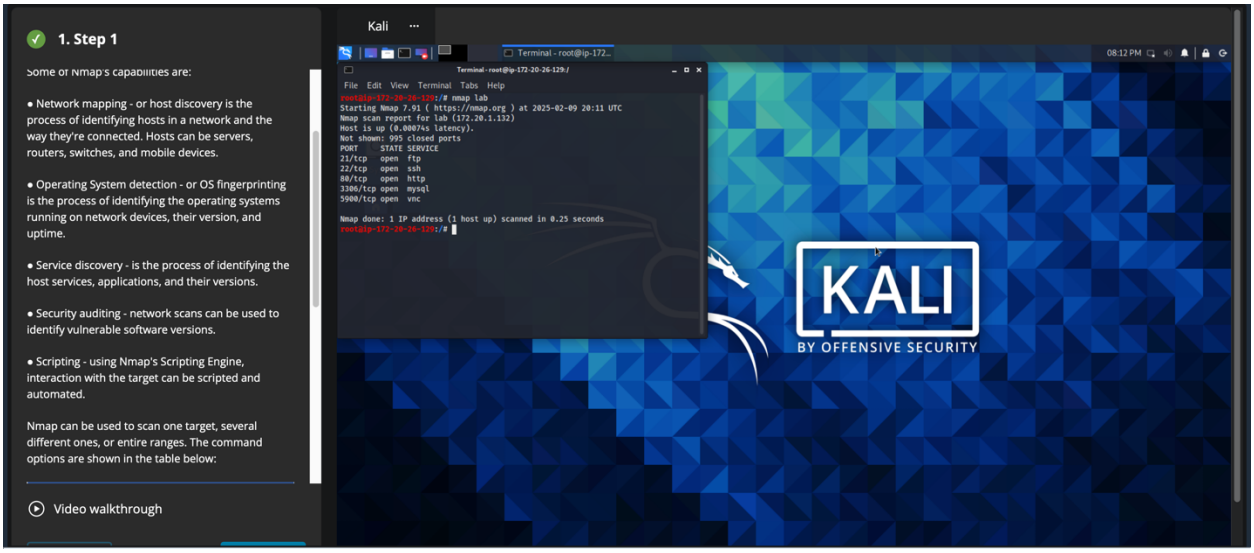

Figure 1. Scanning host "lab" with nmap.

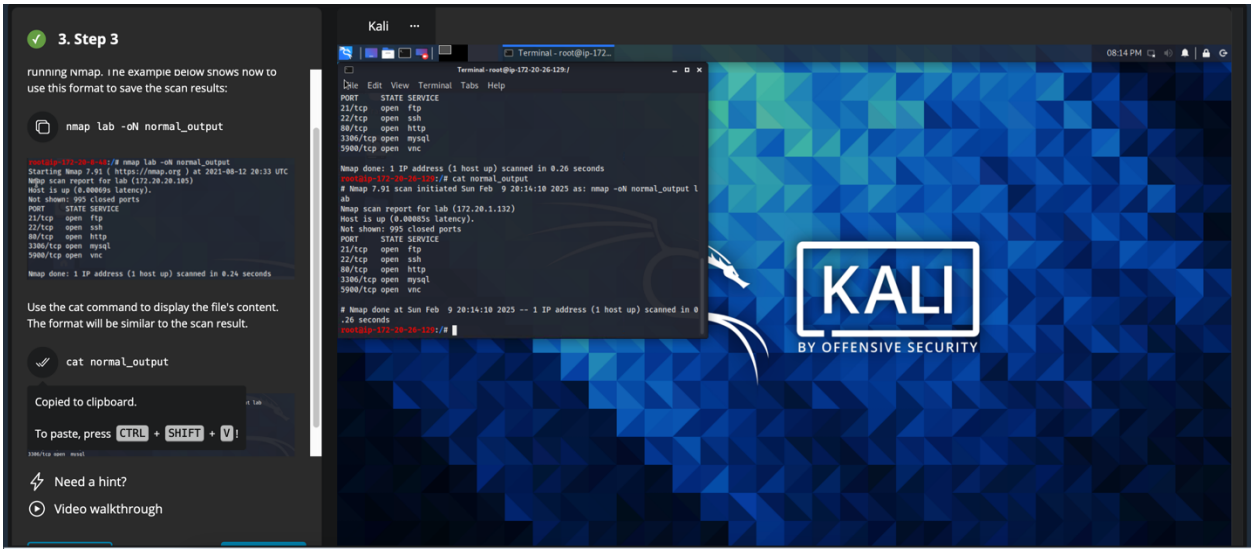

Figure 2. Reading saved nmap output as text.

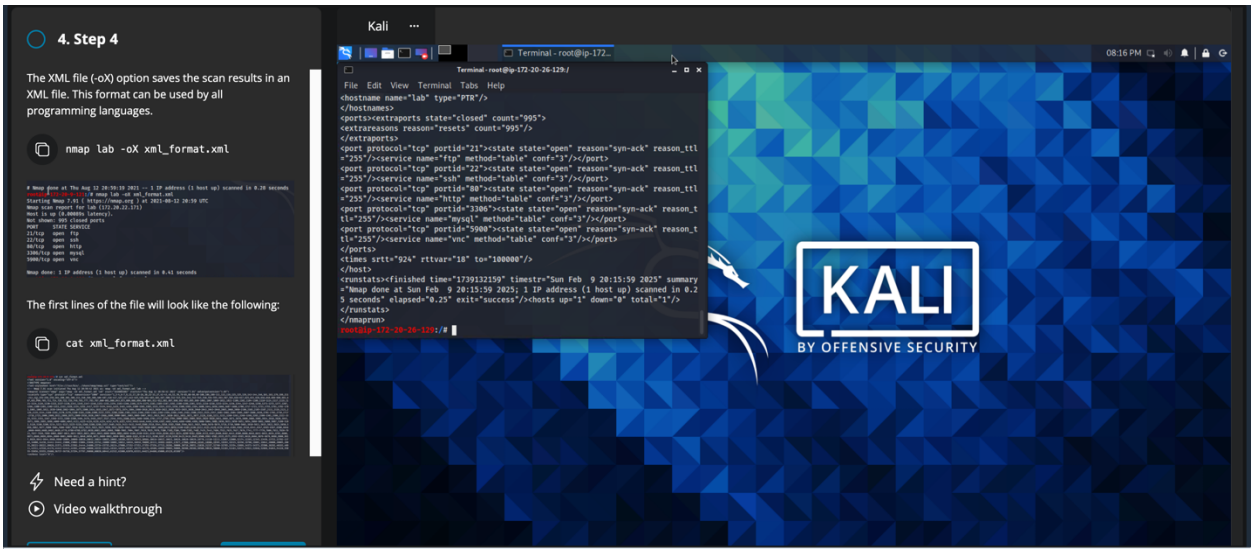

Figure 3. Reading saved nmap output as XML.

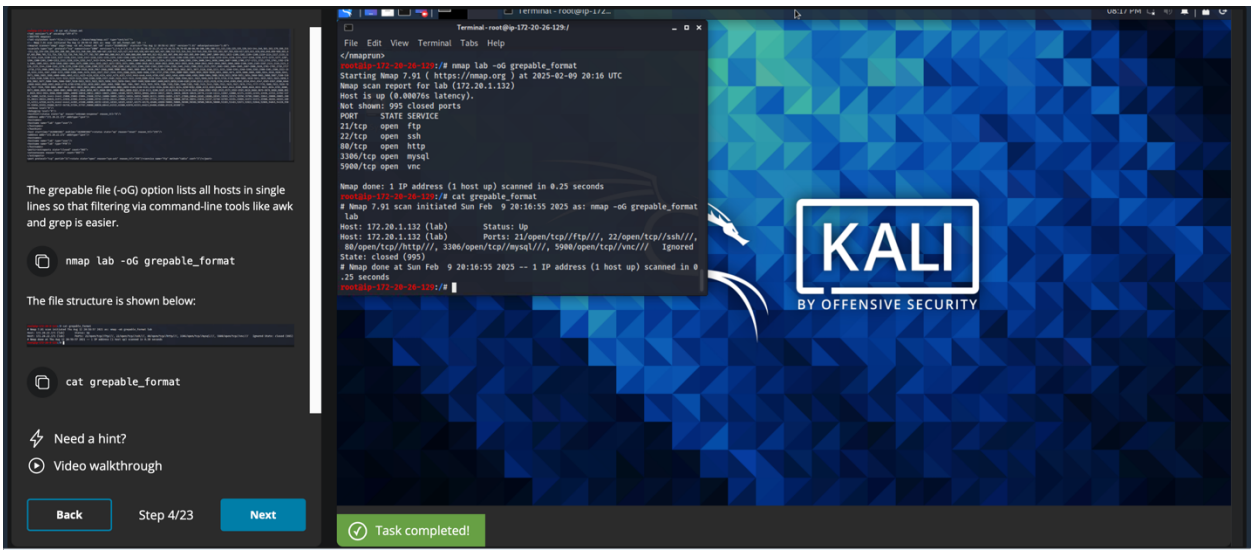

Figure 4. Reading saved nmap output in a grep-optimized format.

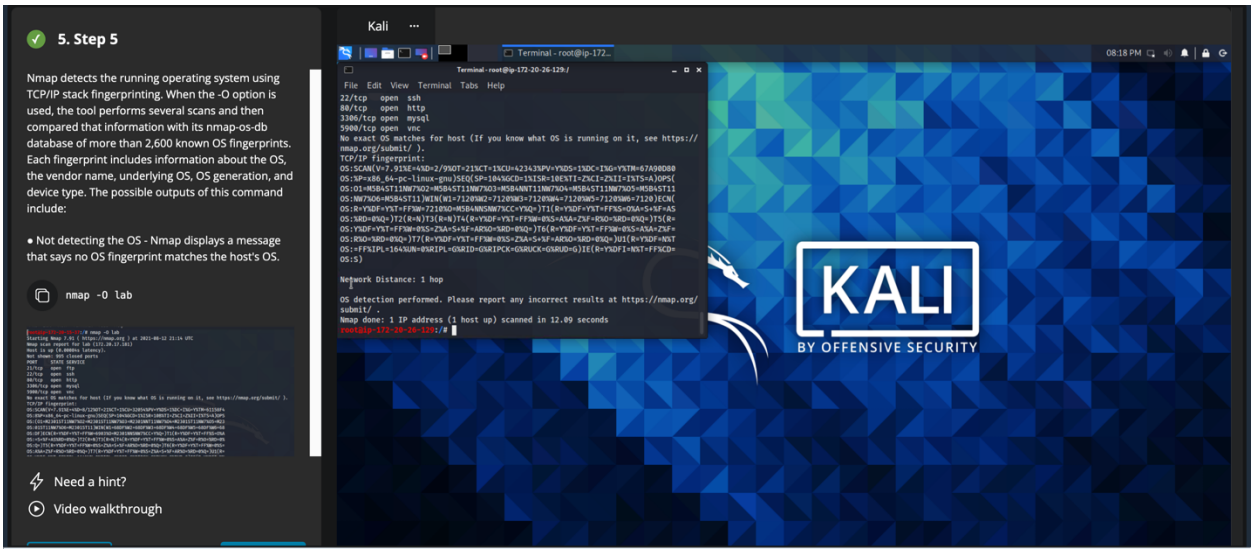

Figure 5. Running nmap's OS detection on "lab".

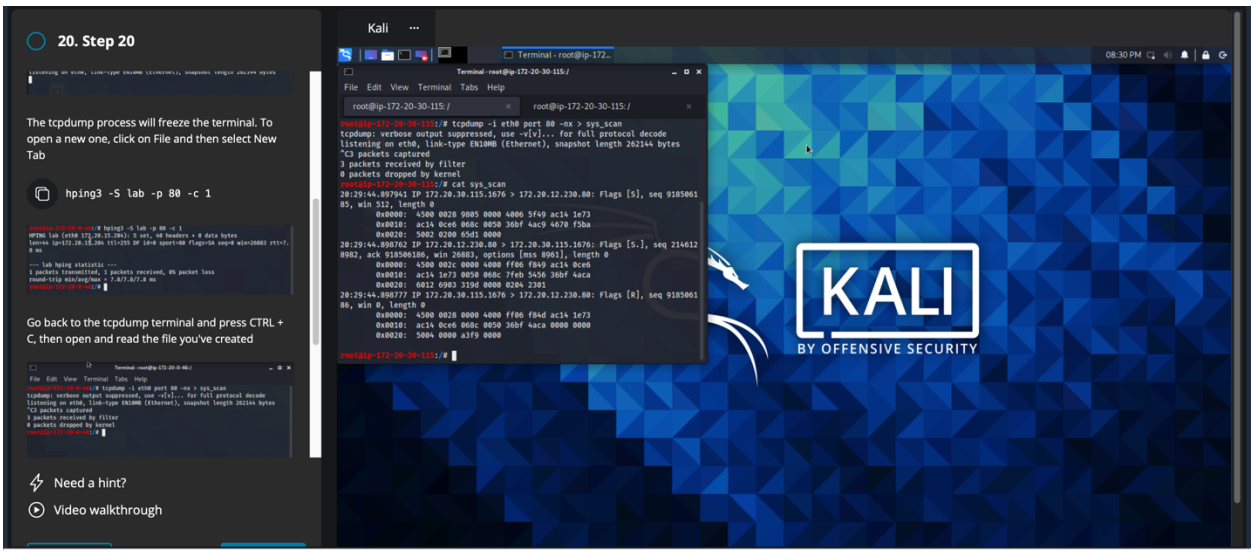

Figure 6. Viewing hping-created packets captured by tcpdump.

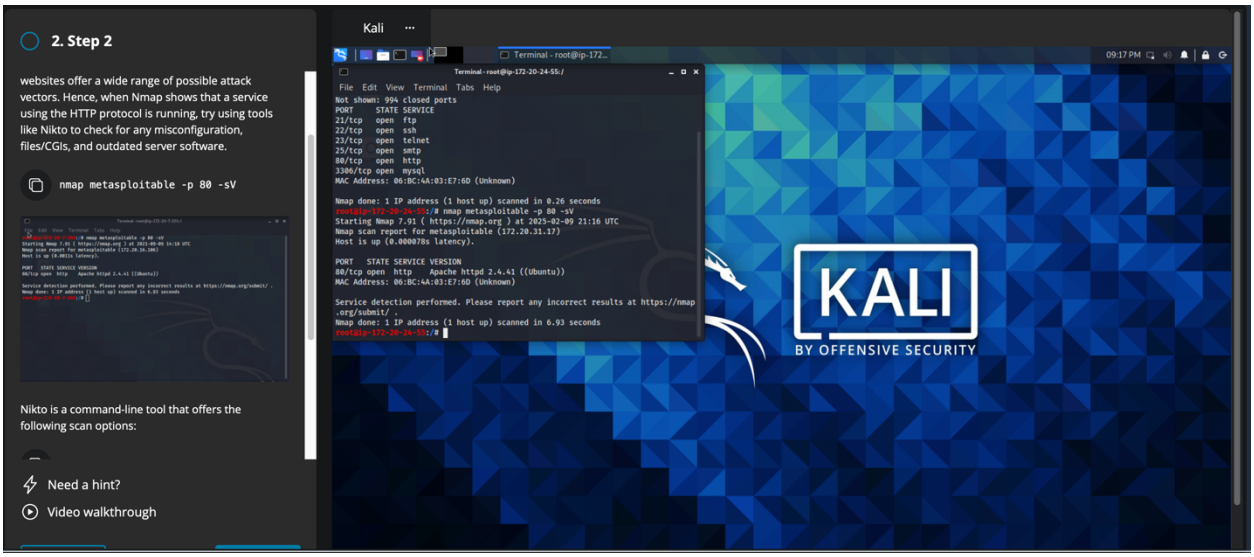

Figure 7. Checking for outdated software on "metasploitable".

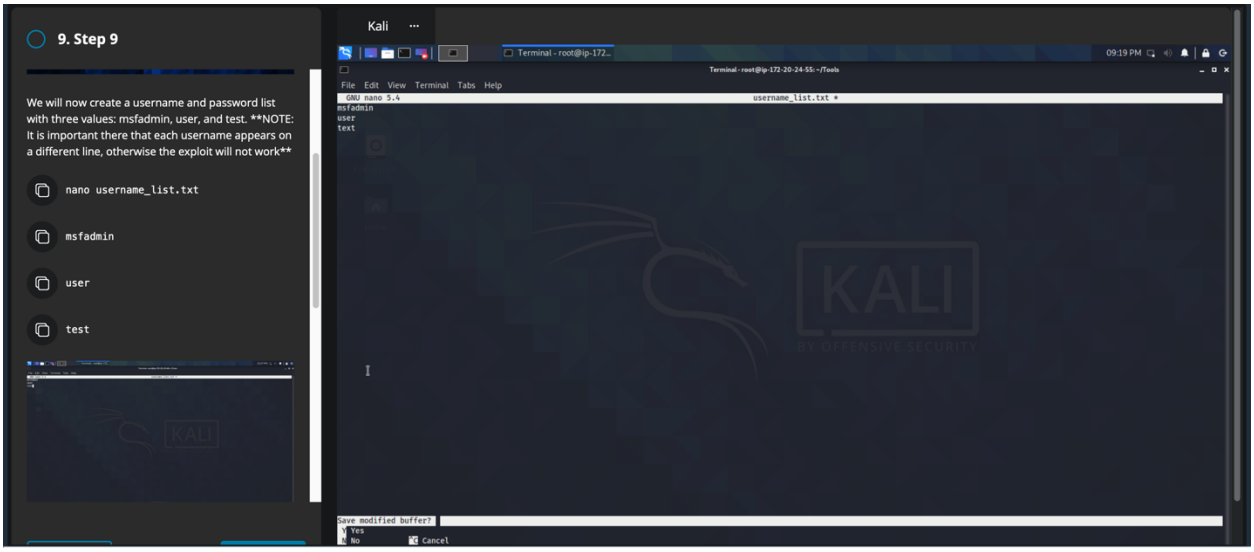

Figure 8. Editing username_list.txt.

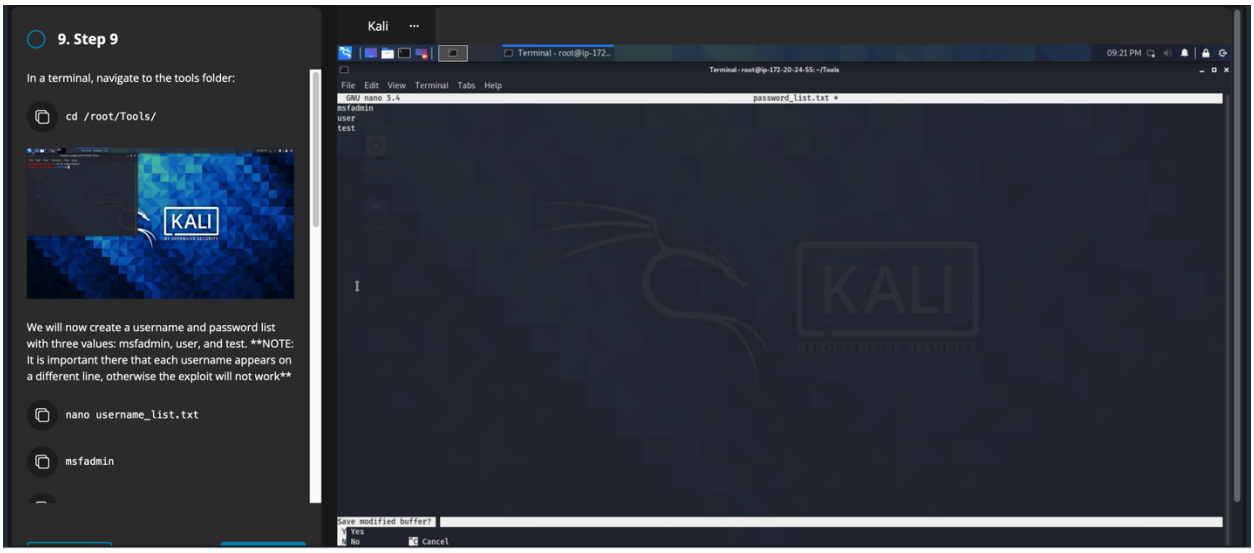

Figure 9. Editing password_list.txt.

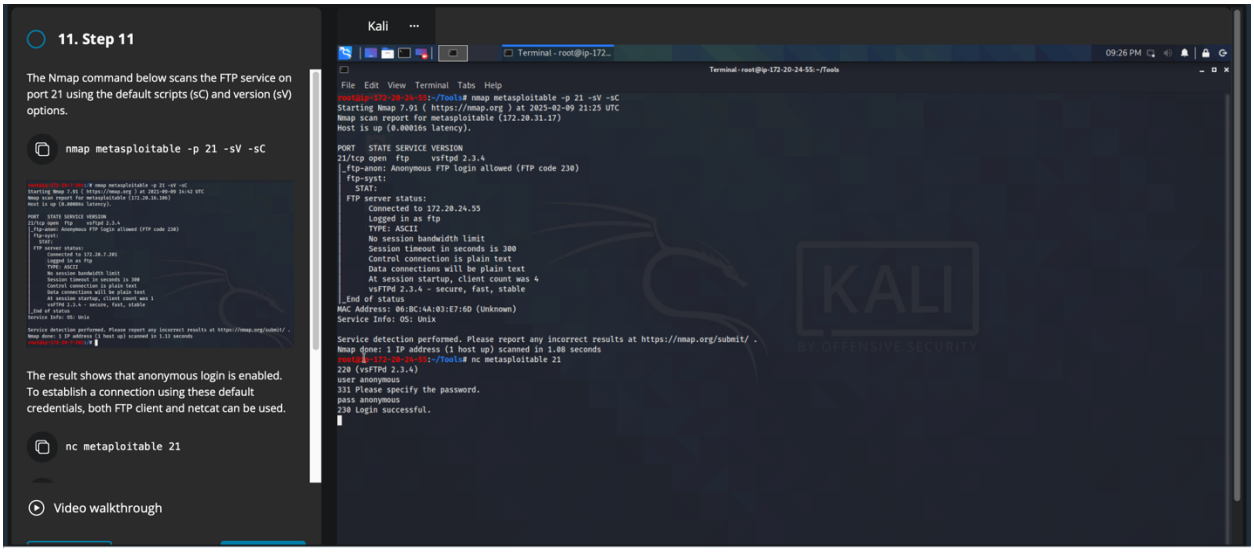

Figure 10. Establishing a connection to the FTP service on "metasploitable" via netcat.