Lab 1 Report

Jason Tolbert

The Pennsylvania State University

IST 894-001: Capstone Experience

Dr. Michael Bartolacci, Instructor

February 2nd, 2025

Table of Contents

Non-Technical Overview

The two cyber ranges that comprise this lab – one on vulnerability scanning and one on the Metasploit framework – together instruct participants on how to identify, assess, and exploit vulnerabilities in computer systems. The first range focuses on the identification and assessment of vulnerabilities related to network services, misconfigurations, and outdated software on a remote machine. Participants view reports detailing the vulnerabilities that were found and learn to triage them by severity.

The first half of the second range deals with penetration testing, a practice in which authorized individuals attempt to identify and exploit vulnerabilities in a system so that they can be patched before bad actors do the same. Participants learn how to conduct reconnaissance by scanning target machines for open ports and services and how to exploit vulnerabilities found in reconnaissance using the popular Metasploit framework. Participants also see firsthand how common attack vectors, such as weak credentials, can expose a system to serious threats.

The second half of the second range is about post-exploitation activities — the things bad actors can do to damage a system after having gained access to it. The focus is primarily on privilege escalation. In privilege escalation attacks, the attacker exploits vulnerabilities to gain a high level of access to the system and the ability to execute administrative commands or control sensitive resources. This part of the lab intends to reinforce the importance of

proper configuration and robust user access control in mitigating the damage threat actors can do.

Technical Overview

This lab covers several key technical concepts in skills in the areas of vulnerability assessment and exploitation. It is split into three parts — vulnerability scanning, penetration testing, and post-exploitation activities.

The first part centers on vulnerability scanning, specifically using the OpenVAS vulnerability scanning software. Participants learn how to use OpenVAS to identify and triage weakness in remote machines. By setting preconfigured credentials in OpenVAS, participants gain deeper visibility into the system than they would with an unauthenticated scan. (Aksu et al., 2019)

The second part of the lab deals with penetration testing. It first teaches participants how to perform reconnaissance with Nmap, identifying network services and software versions that have known vulnerabilities (Rahalkar, 2019). Once these services are identified, participants use Metasploit to apply attacks targeted at those specific services (Rani & Nagpal, 2019). Participants experience gaining unauthorized control over vulnerable systems via shell access and remote code execution. (The MITRE Corporation, n.d.).

The final part of the lab guides participants through conducting post-exploitation attacks. LinPEAS is used to automate the process of detecting potential paths to privilege escalation, including SUID-enabled binaries and outdated versions of sudo. Participants take advantage of the vulnerabilities LinPEAS detects to elevate themselves to root access. As root, they enumerate open ports, interfaces, and permissions, and learn how that information can be used to carry out further attacks.

References

Aksu, M. U., Altuncu, E., & Bicakci, K. (2019). A first look at the usability of OpenVAS vulnerability scanner. Proceedings 2019 Workshop on Usable Security, San Diego, CA. https://doi.org/10.14722/usec.2019.23026

Rahalkar, S. (2019). Introduction to Nmap. In S. Rahalkar, Quick Start Guide to Penetration Testing (pp. 1–45). Apress. https://doi.org/10.1007/978-1-4842-4270-4_1

The MITRE Corporation. (n.d.). Exploitation for privilege escalation, technique T1068—Enterprise MITRE ATT&CK®. MITRE. https://attack.mitre.org/techniques/T1068/

Rani, S., & Nagpal, R. (2019). Penetration testing using Metasploit framework: An ethical approach. International Research Journal of Engineering and Technology, 06(08).

Screenshots

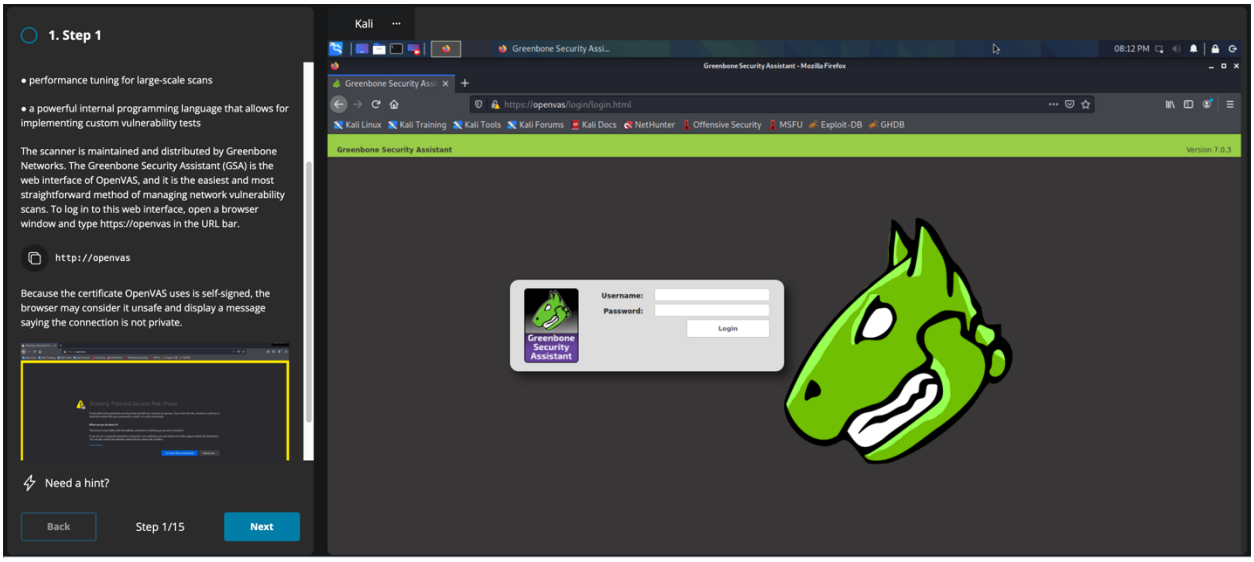

Figure 1. Launching the OpenVAS web UI.

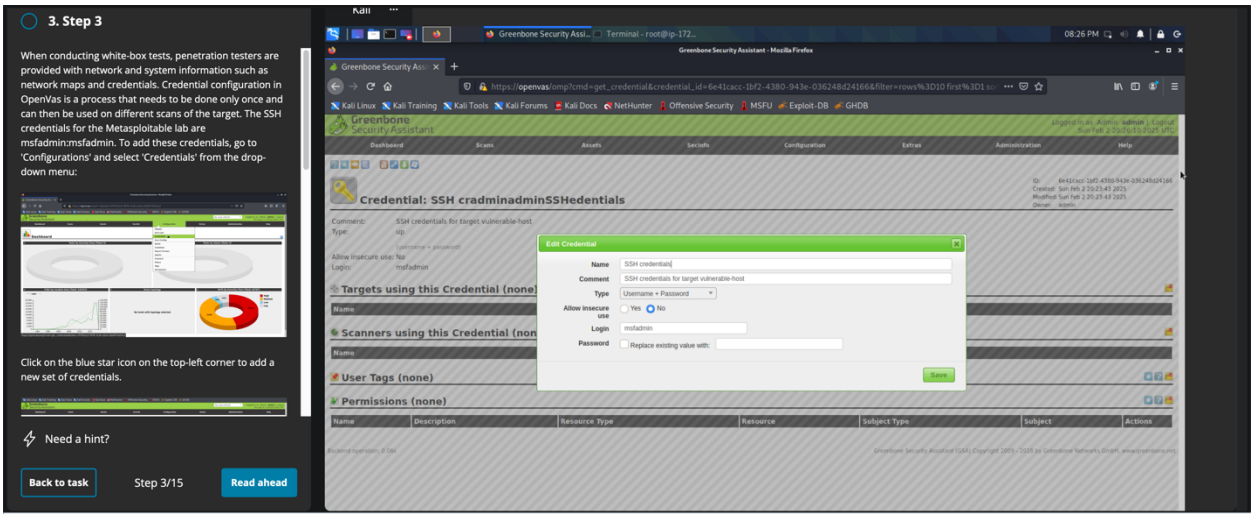

Figure 2. Creating SSH credentials.

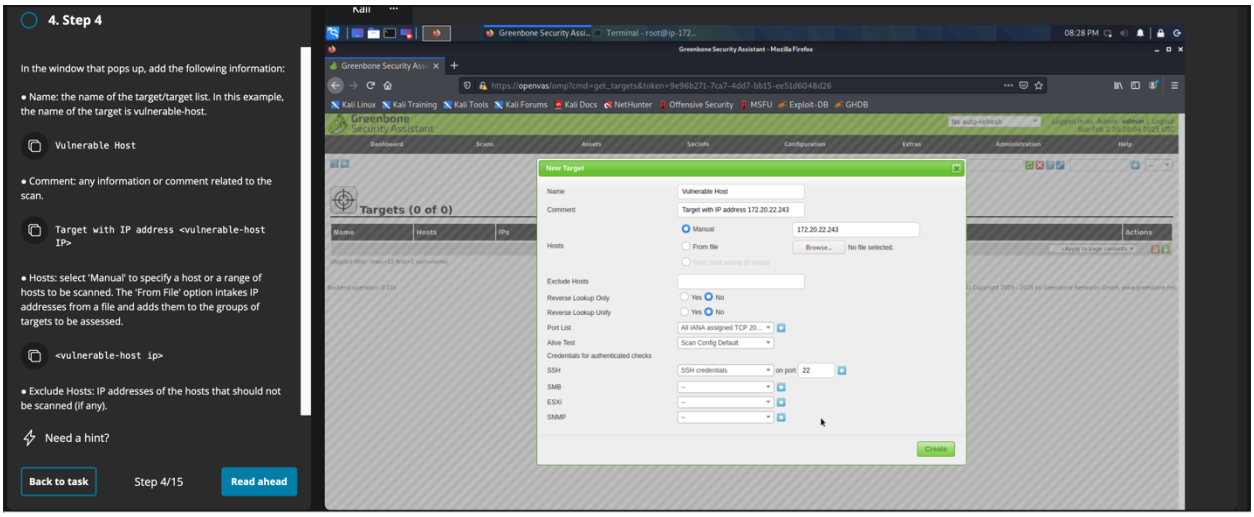

Figure 3. Creating a target configuration.

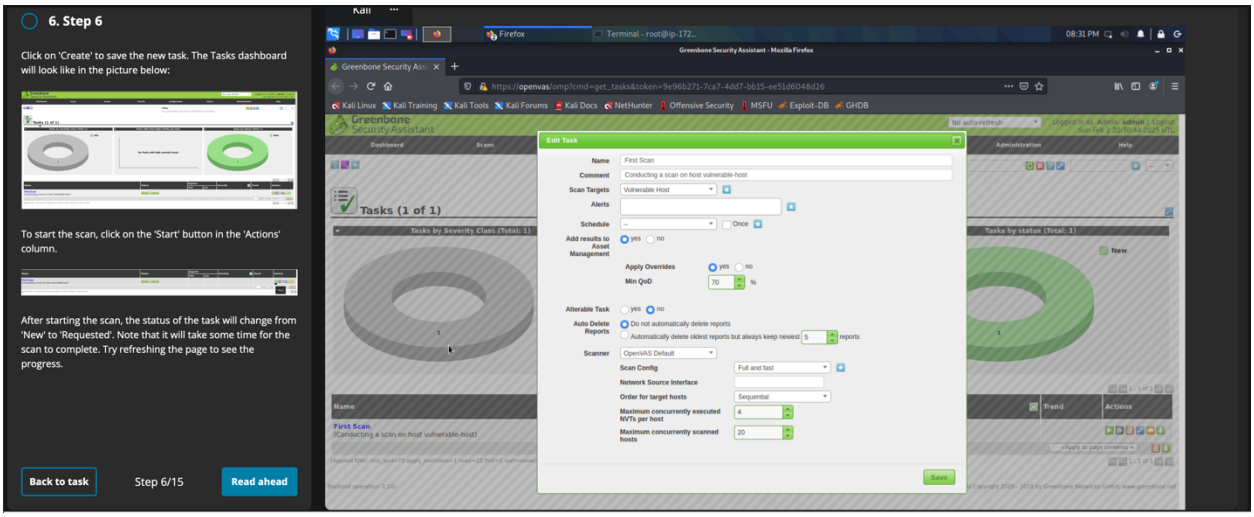

Figure 4. Creating a task.

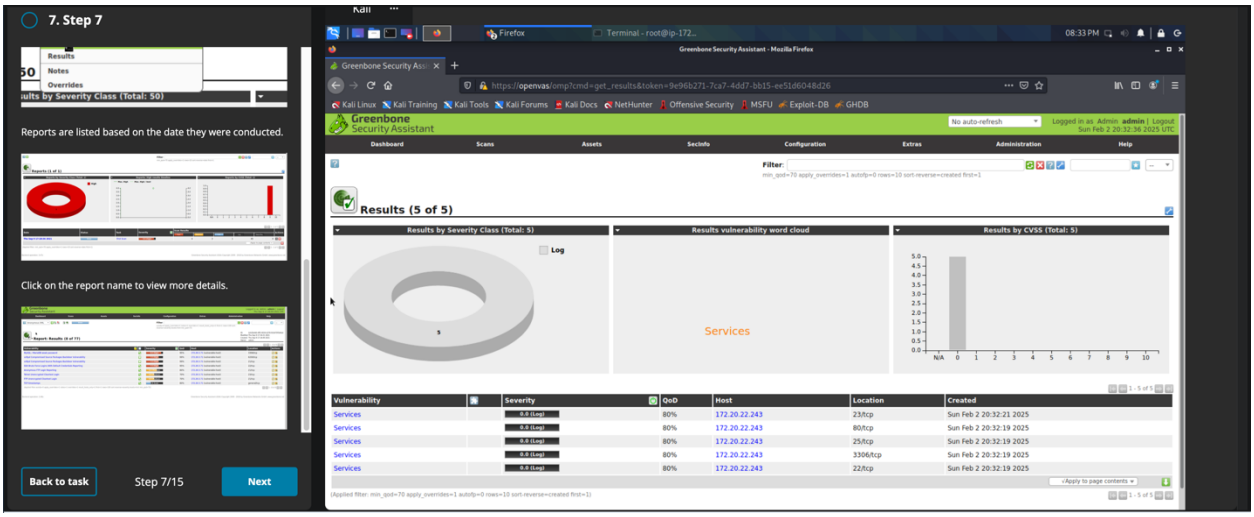

Figure 5. vulnerable-host scan results.

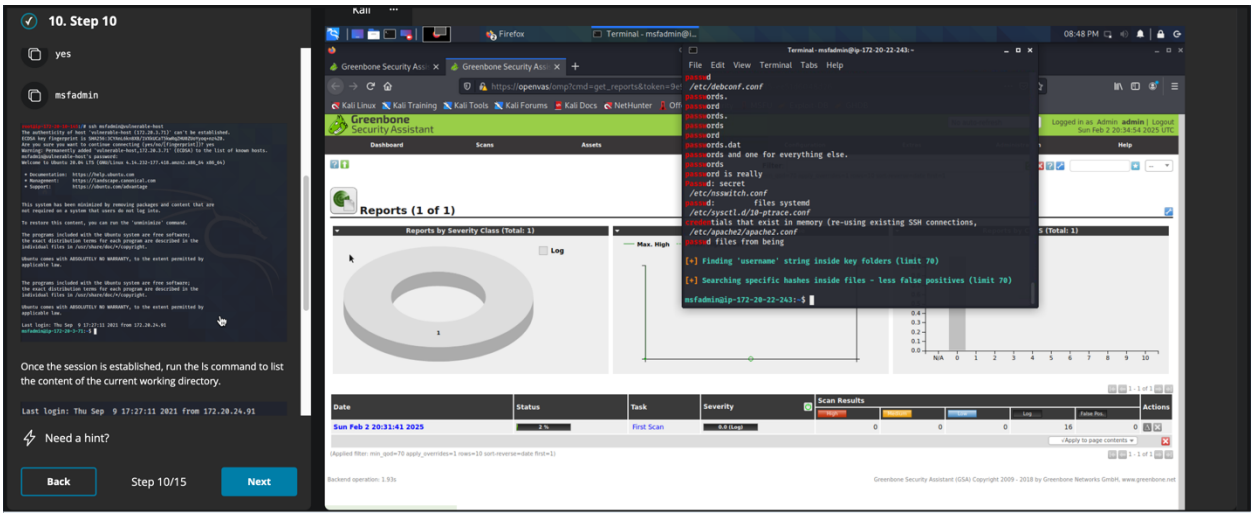

Figure 6. Running linpeas.sh.

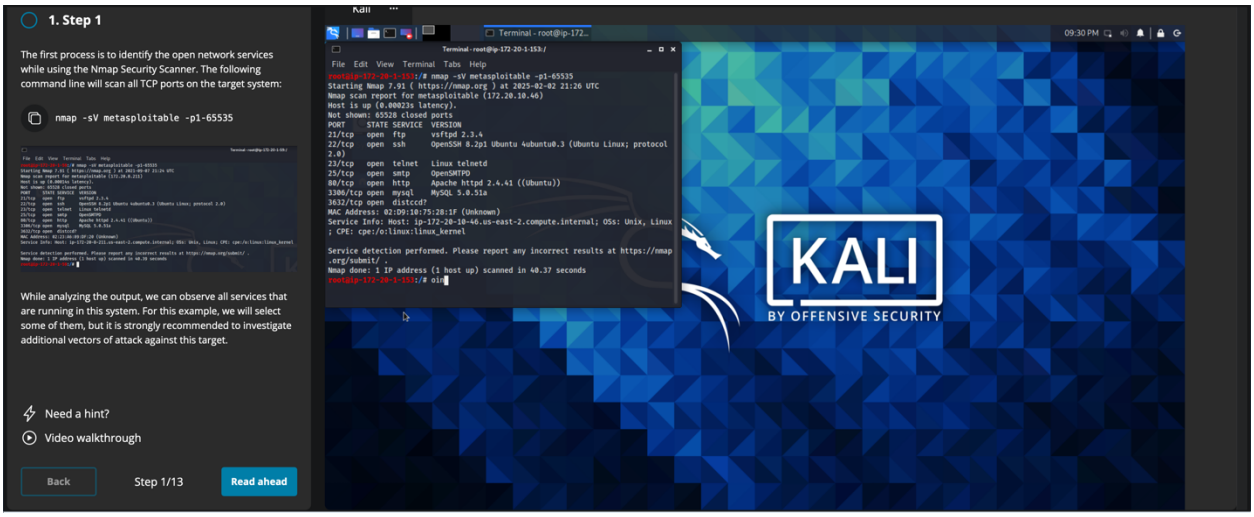

Figure 7. Scanning all TCP ports on metasploitable.

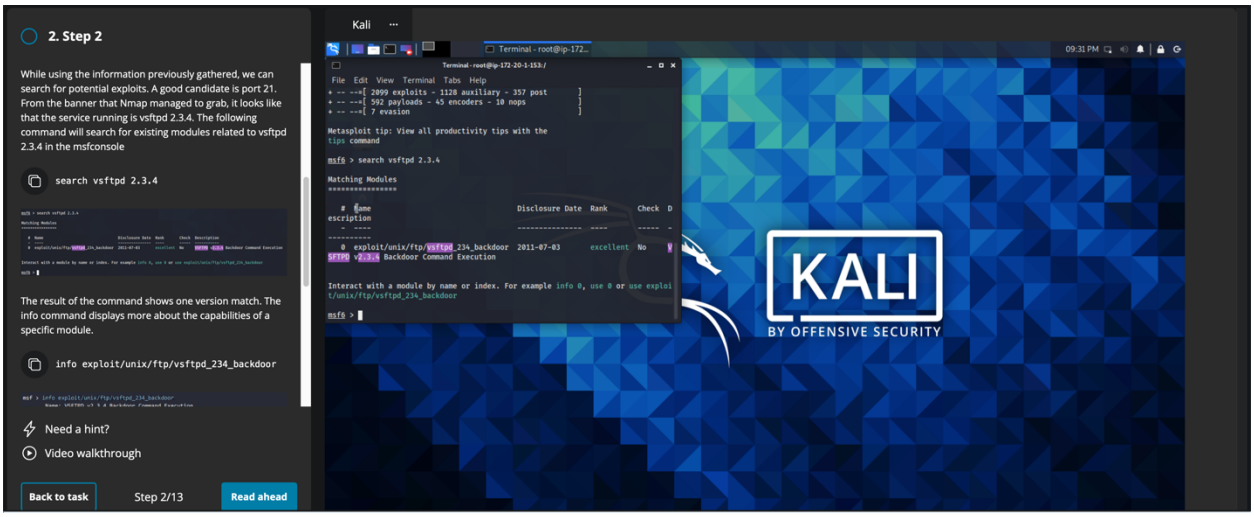

Figure 8. Searching for exploits with msfconsole.

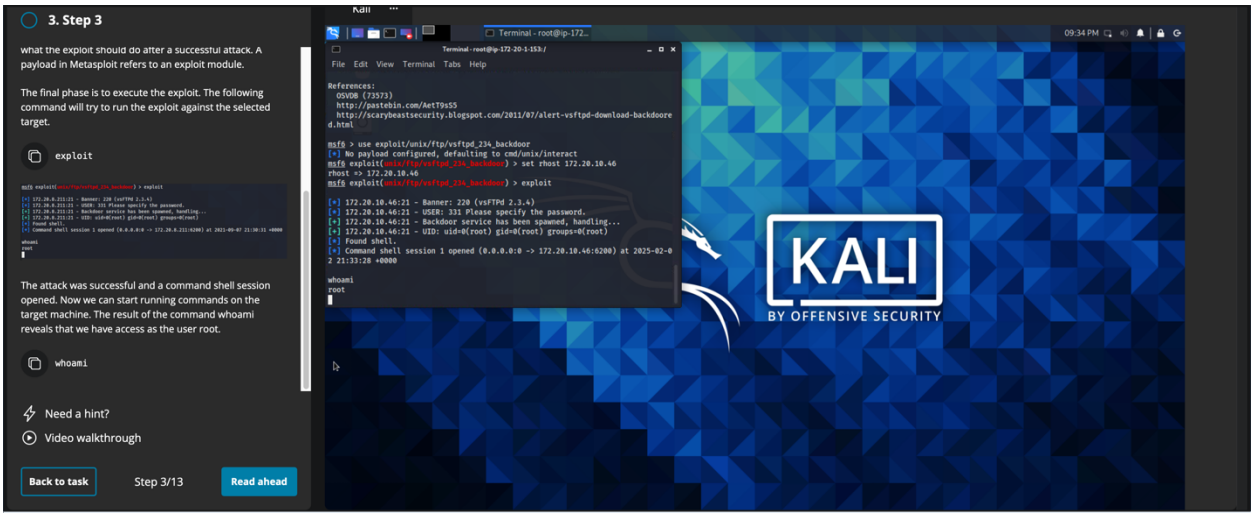

Figure 9. Gaining root access on metasploitable.

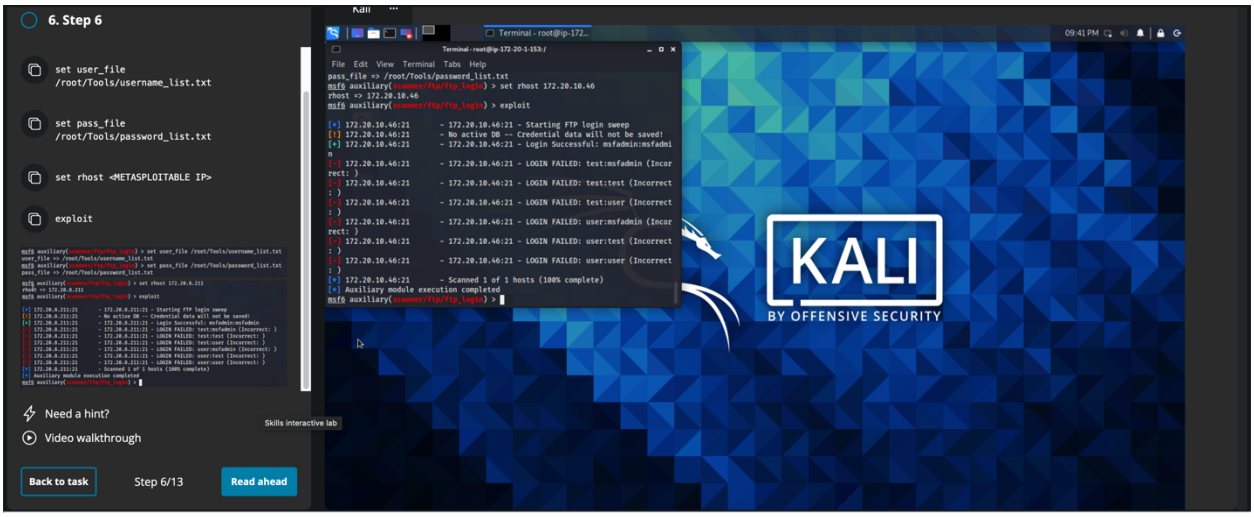

Figure 10. Attempting FTP login.

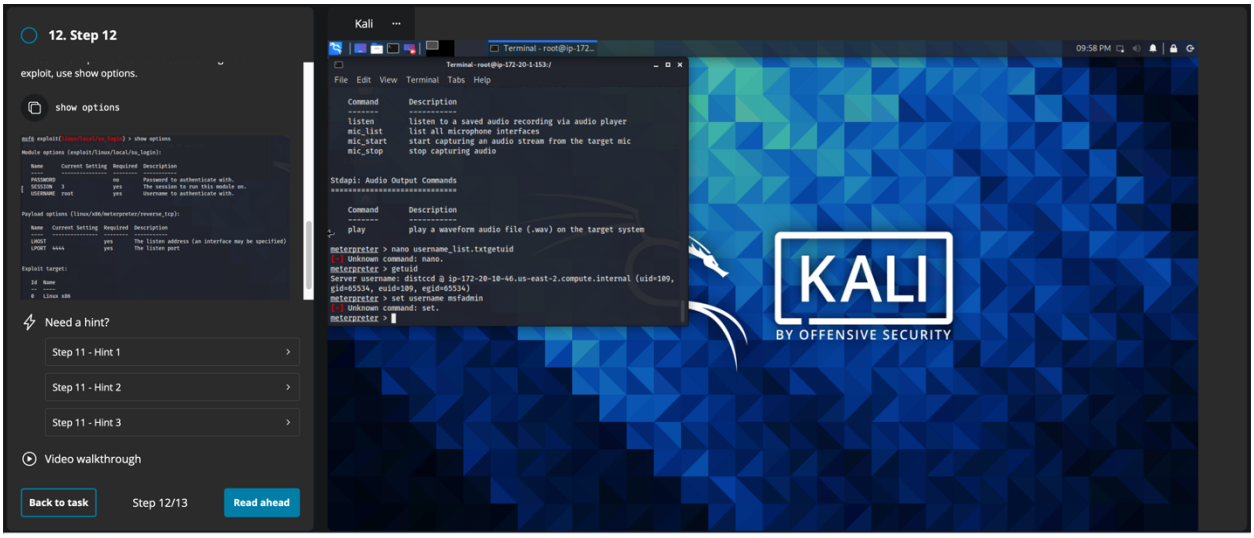

Figure 11. Interacting with meterpreter.

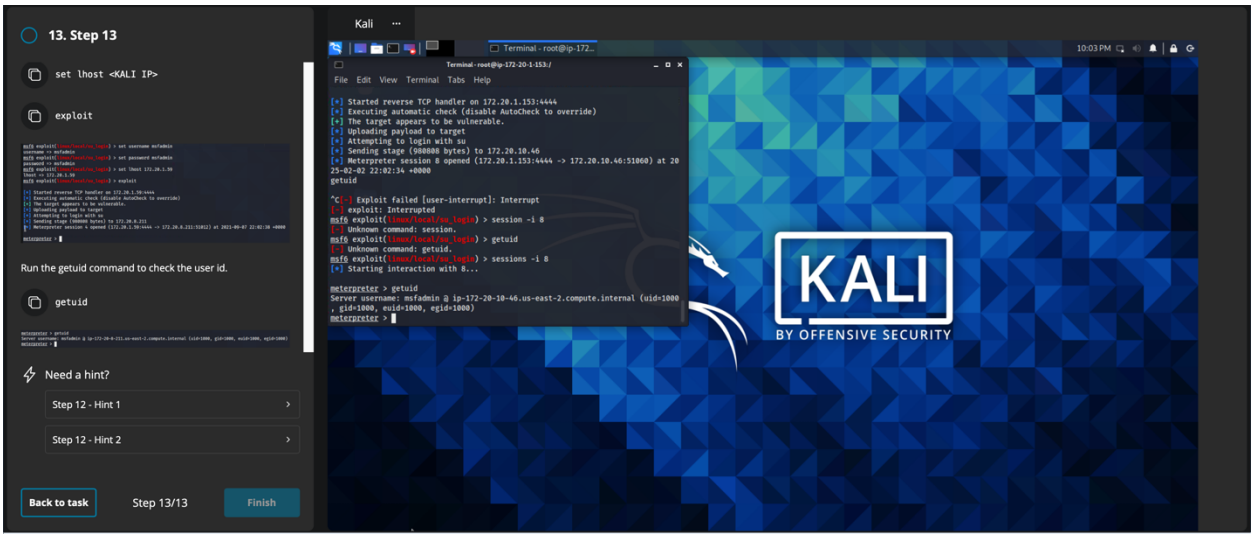

Figure 12. Getting the user ID of msfadmin.