PennState
College of Information Sciences and Technology

Lab Assignment Report

COURSE:	**IST 894**
ASSIGNMENT:	**LAB ASSIGNMENT REPORT 3**
SUBMITTED BY:	**BRANTLEY PRICE**
DUE DATE:	**JUNE 22TH, 2025**
INSTRUCTOR:	**DR. BARTOLACCI**

Contents

General Context

Supervisory Control and Data Acquisition (SCADA) systems play an important role in operational technology (OT) by managing infrastructure like power grids and water treatment facilities. Often times, however, they prove to be difficult to properly protect. Vargas (2023) says that just 13% of OT professionals have achieved centralized visibility into all their OT activities and that just 15% of OT security professionals say that their CISO is responsible for OT security. The two exercises in this report, Firewall Rules for SCADA and SCADA - Attacking the Infrastructure, show the student both offensive and defensive ways to approach their SCADA systems.

In the first lab, the student was shown how to develop firewire rules in Linux via terminal and using the iptables firewall utility. Typically, SCADA systems require more specificity in firewall management because of their unique, and often proprietary system structure (Amos, n.d.). In this exercise, the student gained hands-on experience by configuring logging chains and drop rules, which allowed the student to control network traffic at the network and payload level. This type of specificity is necessary in SCADA systems, especially those that are older and whose developers never considered cybersecurity.

The second lab was more about the offensive side of the coin. In the Attacking the Infrastructure lab, the student walked through a simulation of how threat actors can compromise a SCADA system through phishing and privilege escalation. In this exercise, a .deb package delivers a trojan via an email phishing attack. After the attack is executed, the student is walked through accessing the /etc/shadow file, with a user originally created with general privileges. This gives the student access to hashed passwords for users on the system.

Technical Context

Firewall Rules for SCADA systems begins with the student executing commands to set up a Modbus TCP simulator. With Iptables, the student added rules to log traffic which targeted port 502 as 502 is Modbus's standard port. Going deeper, a custom rule was applied to allow packet-level filtering to inspect specific byte sequences. Modbus has been around since 1979 and was developed during a time when the cybersecurity terms confidentiality and integrity were not even concepts (Parian et al., 2020). Being able to use rules to this level of granularity allows for deep packet inspection of legacy protocols to be integrated into more modern cybersecurity tools. This exercise is particularly useful because of the protocol-specific nature of the rules being written.

Attacking the Infrastructure transitioned the student from defensive-minded operations to the offensive-minded side of things. Using Kali Linux, the student embedded a reverse shell into the DigiTemp utility using MSFVenom and served it over HTTP via Apache. Using mutt, the student sent a phishing email with a malicious package hidden inside, which when installed, triggered a reverse shell payload. This provided the student with a backdoor threat vector.

What the exercise doesn't really mention, however, is the demonstration of the entire cyber kill chain, as explained by Lockheed Martin. Reconnaissance of emails to target, weaponization of an exploit with a backdoor, delivery of the exploit, exploitation after delivery, installation of the trojan, remote control of system, and finally, actions against the objective (Lockheed Martin, n.d.). If the student understands the concept of the cyber kill chain, they are able to identify it and see an example of it unfolding within the lab.

Screenshots

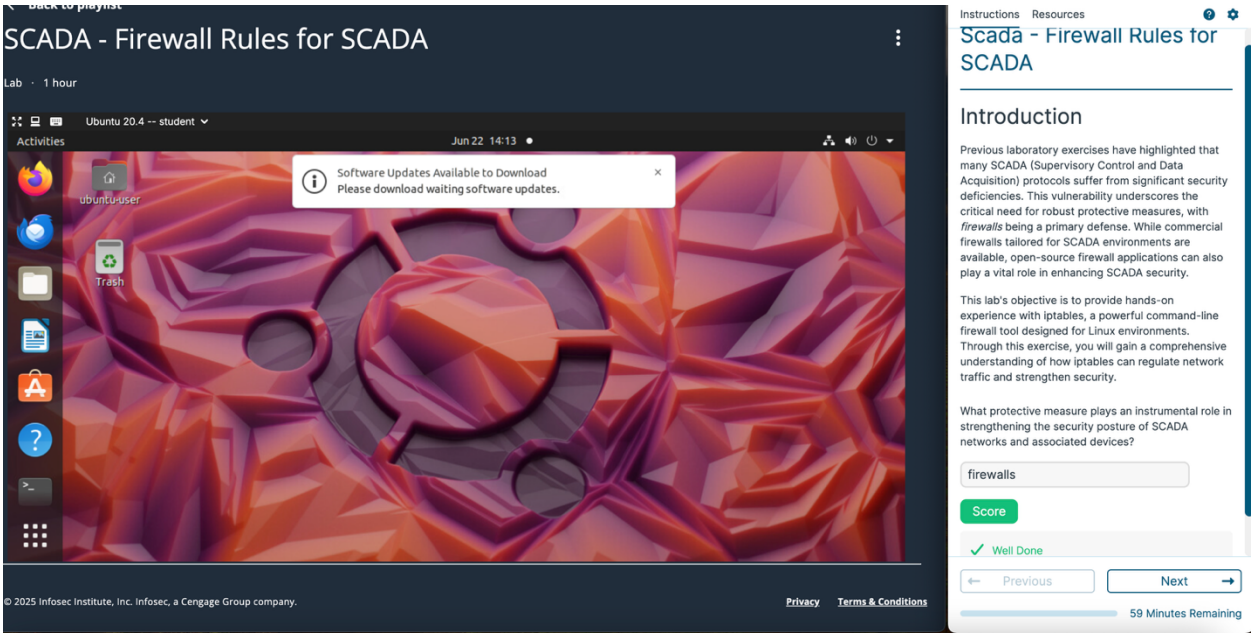

Figure 1: Firewall Rules for SCADA Intro

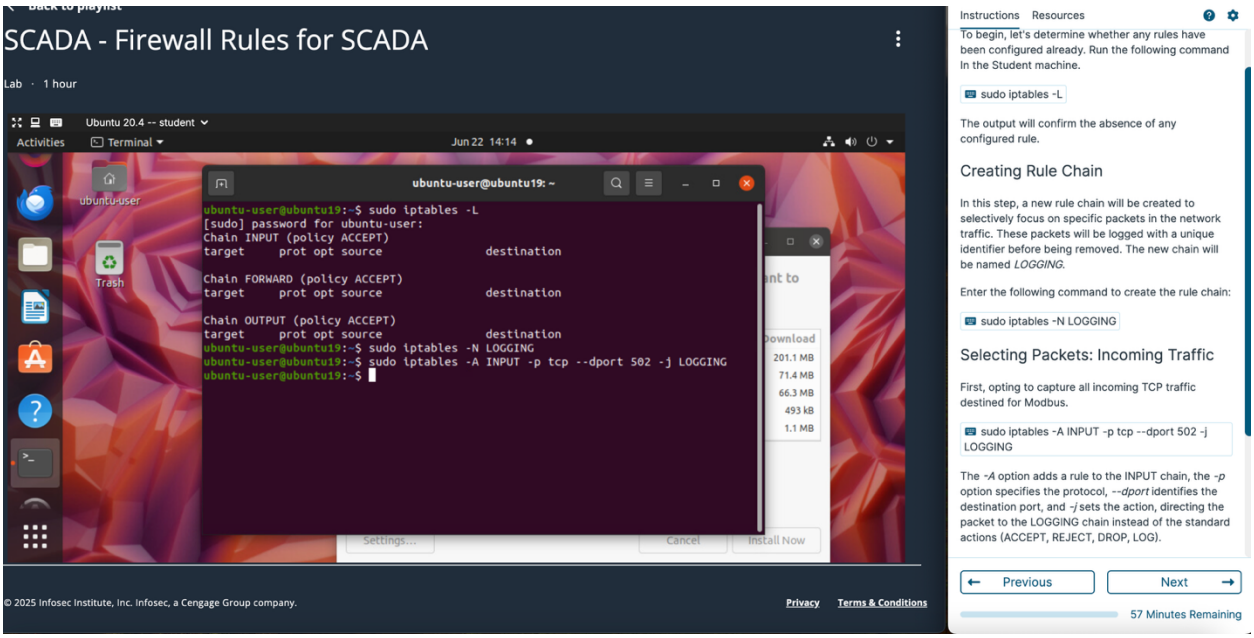

Figure 2: Rule Creation

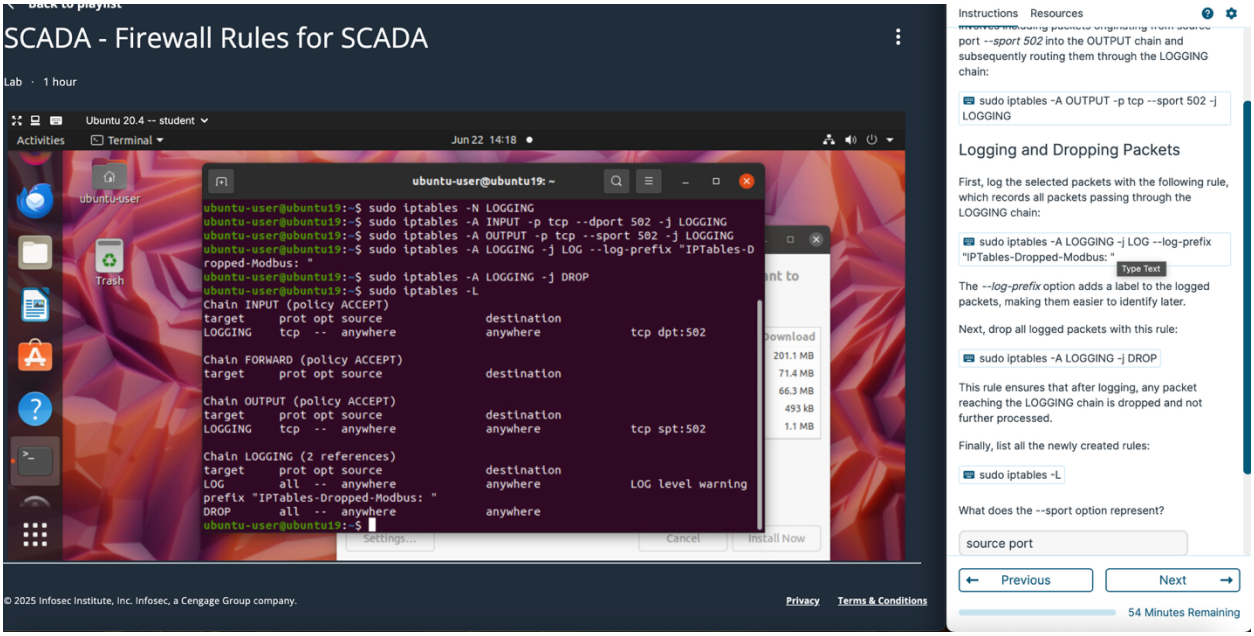

Figure 3: Packet Logging

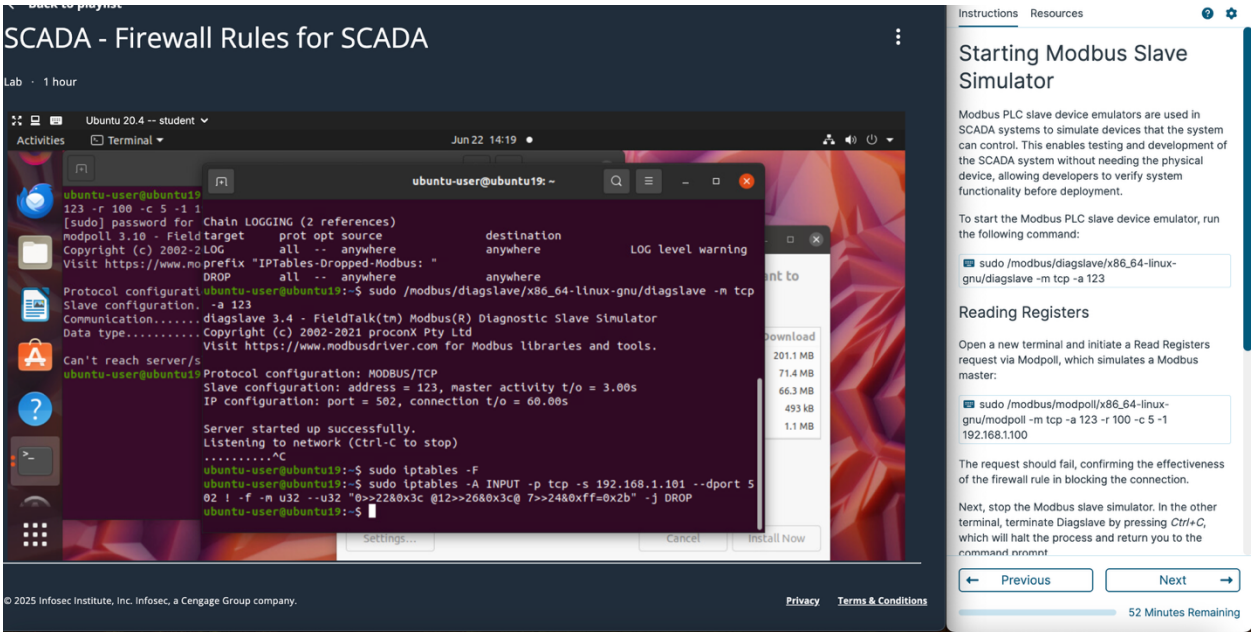

Figure 4: Modbus Simulator

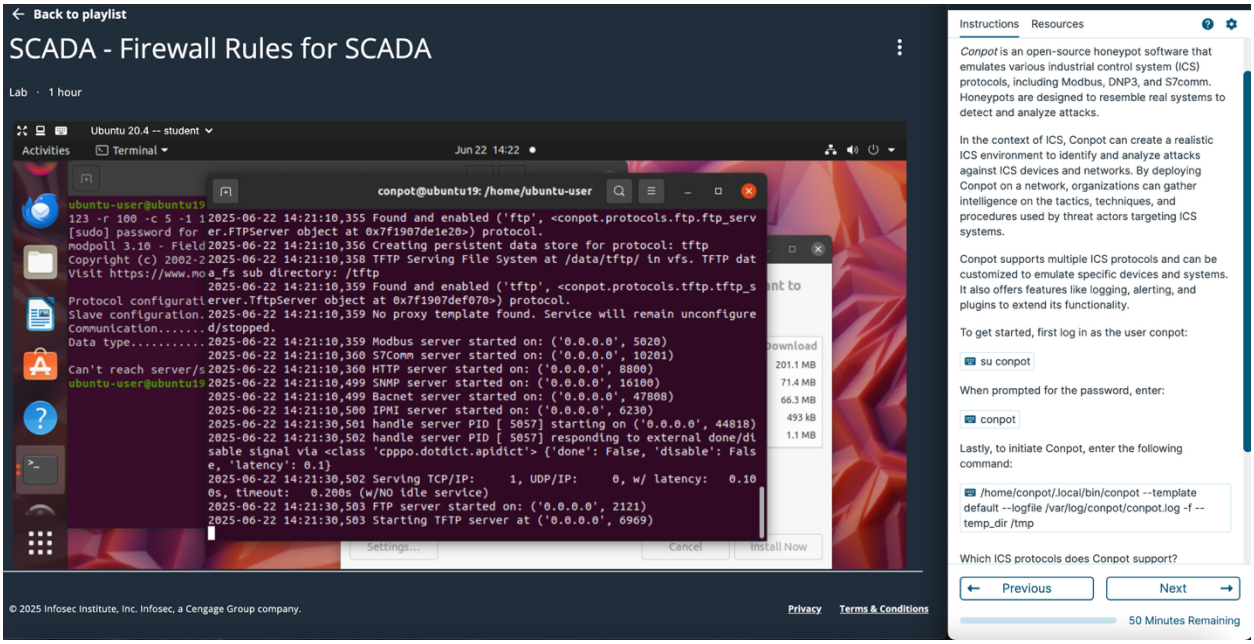

Figure 5: Firewall Final Screenshot

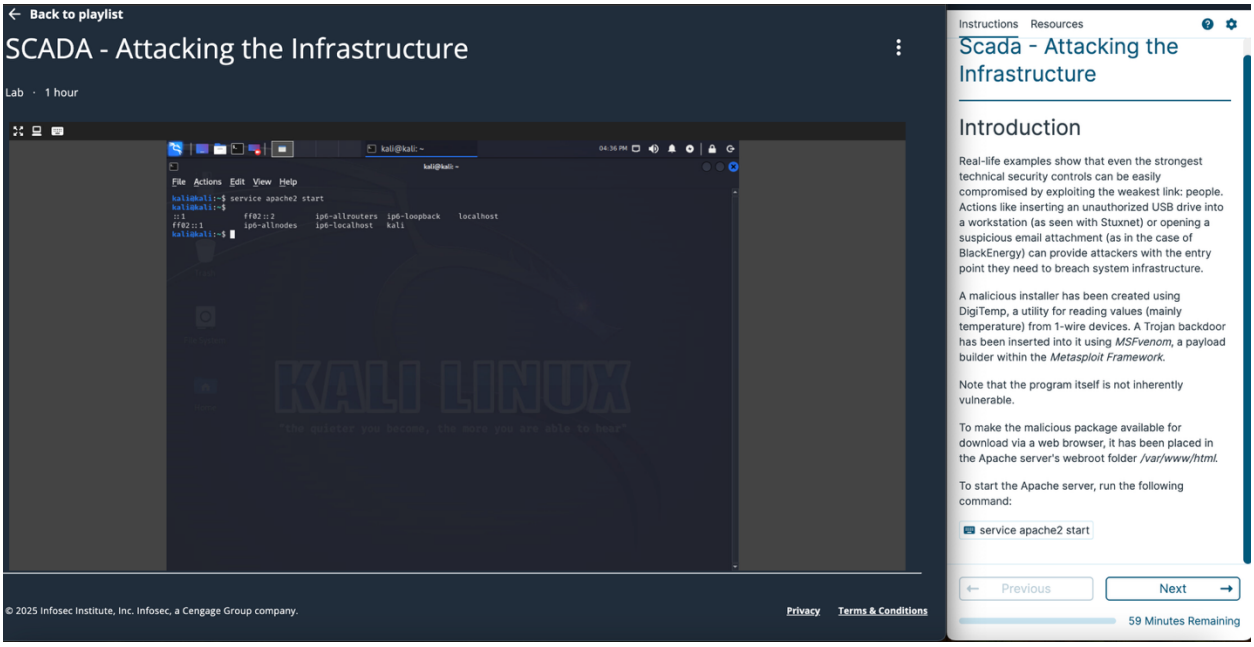

Figure 6: Attacking the Infrastructure Intro

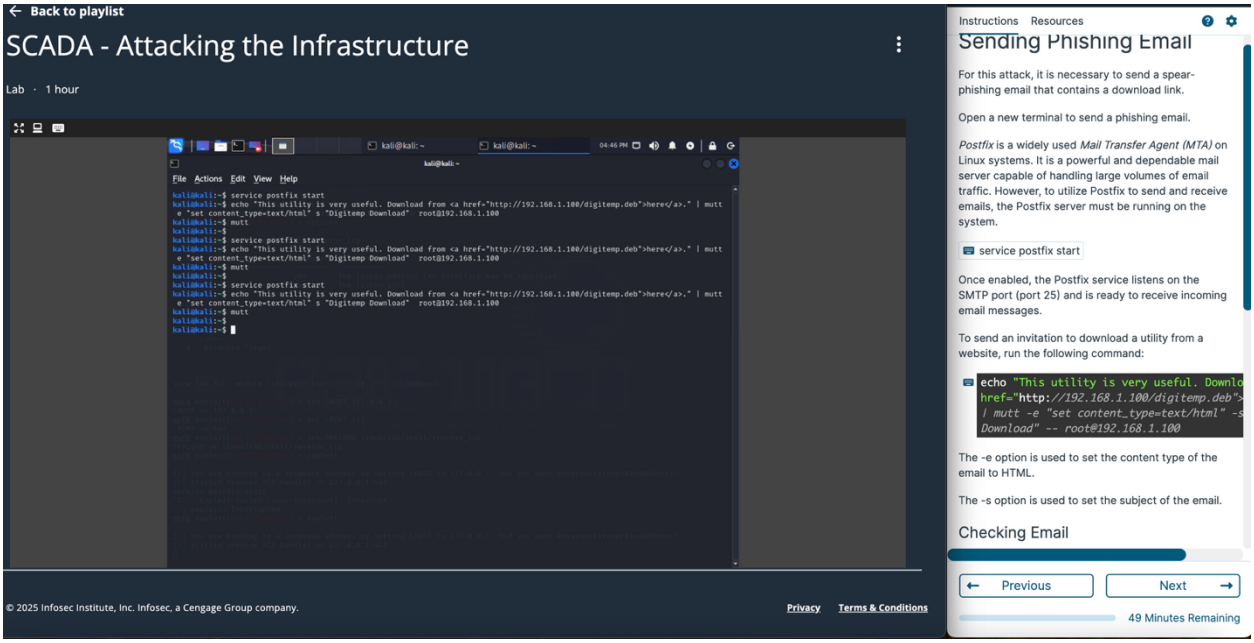

Figure 7: Sending the Phishing Email

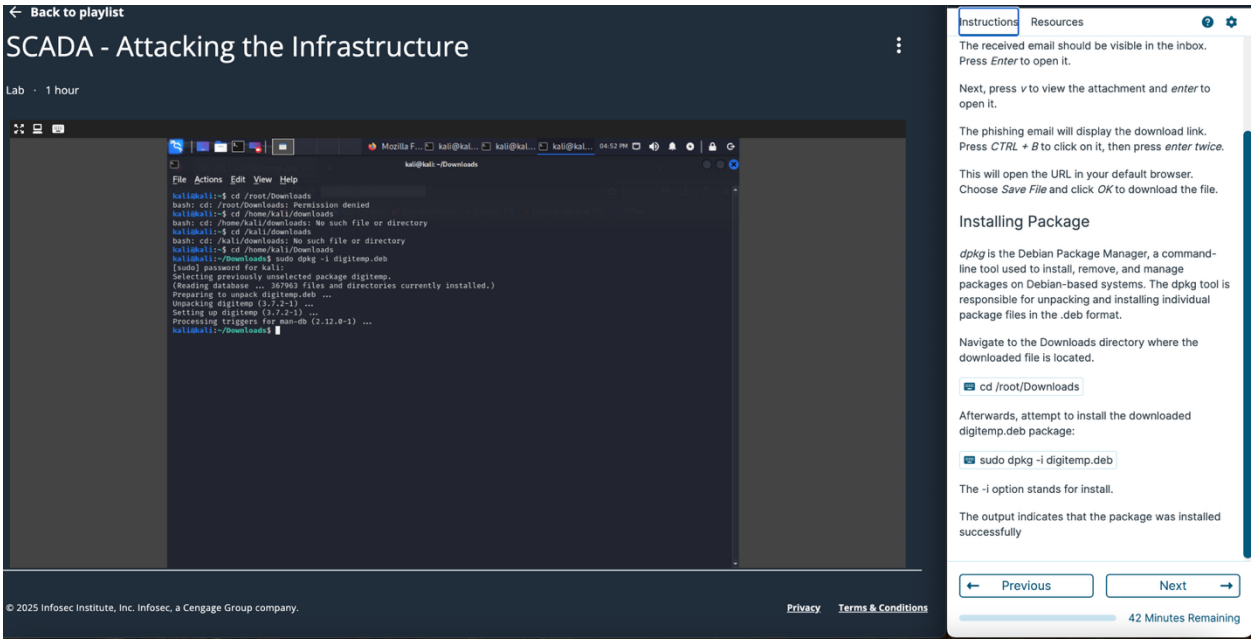

Figure 8: Exploiting and Installing the Trojan

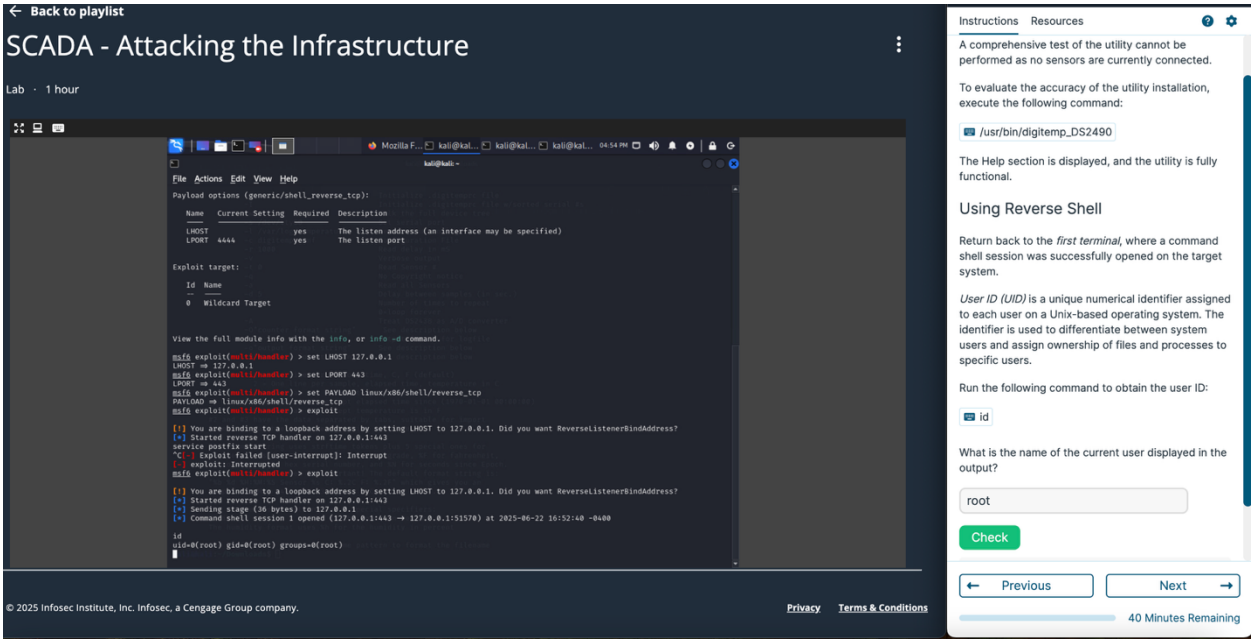

Figure 9: Executing the Reverse Shell

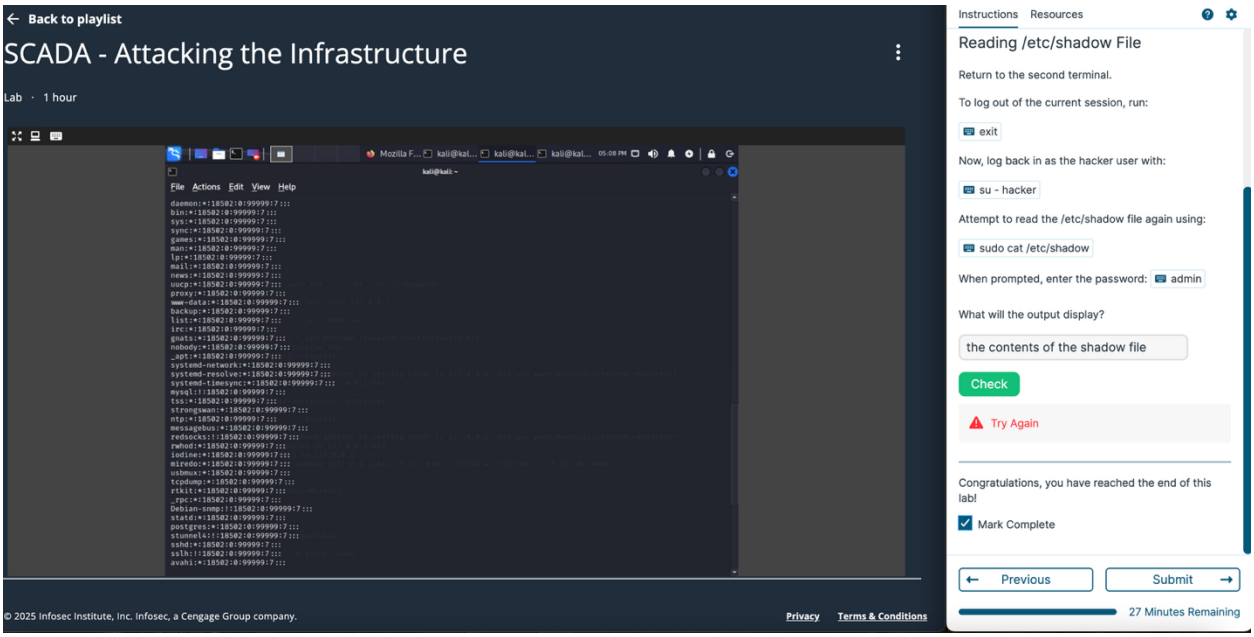

Figure 10: Attacking the Infrastructure Final

References

Amos, Z. (n.d.). *9 SCADA system vulnerabilities and how to secure them*. https://gca.isa.org/blog/9-scada-system-vulnerabilities-and-how-to-secure-them

Cyber Kill chain. (n.d.). Lockheed Martin. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Parian, C., Guldimann, T., & Bhatia, S. (2020). Fooling the Master: Exploiting weaknesses in the Modbus protocol. *Procedia Computer Science*, *171*, 2453–2458. https://doi.org/10.1016/j.procs.2020.04.265

Vargas, J. (2023, July 25). *Protecting SCADA networks in an evolving threat landscape*. CDW.com. https://www.cdw.com/content/cdw/en/articles/networking/protecting-scada-networks-in-an-evolving-threat-landscape.html#:~:text=OT%20Security:%20By%20the%20Numbers,13%25