🛡️ Cybersecurity Portfolio Lab

Welcome to my personal cybersecurity lab! This repository showcases a collection of hands-on projects that demonstrate my skills in vulnerability simulation, system diagnostics, SIEM analysis, Linux/Windows security, and privilege escalation. Each project folder contains documentation and technical summaries to showcase my practical capabilities.

📁 Project Overview

🔧 Smart Thermostat Firmware Vulnerability Lab

Simulates an unsigned firmware update vulnerability in a smart thermostat environment. Demonstrates how attackers could exploit weak update mechanisms and how these flaws can be safely tested in a lab.

📊 Real-World Attack Monitoring with Splunk

Monitored simulated attacks using Splunk SIEM. Collected and analyzed log data to detect anomalies, generate alerts, and understand attacker behavior through dashboards and queries.

🕵️ Simulated Penetration Test Report

Developed a structured pentest report following a simulated system assessment. Includes defined scope, methodology, discovered vulnerabilities, and actionable remediation recommendations.

🛠️ Linux Hardening with Technical Brief

Performed a hardening process on a Linux system, disabling unnecessary services and enforcing security configurations. Includes a concise technical brief explaining the steps and their impact.

👤 Linux User Manager CLI Tool

Built a command-line interface (CLI) tool to manage users and groups on a Linux system. Demonstrates scripting, user/group management, and secure system administration skills.

🌐 Linux Network Diagnostics Project

Conducted a network diagnostics session on Ubuntu using command-line tools such as `ip`, `ss`, `netstat`, `ping`, and `traceroute`. Includes log captures, analysis, and documentation — highlighting proficiency in system networking fundamentals and troubleshooting.

🪟 Windows Privilege Escalation: AlwaysInstallElevated

Exploited the AlwaysInstallElevated setting on Windows 10 to gain elevated privileges. Demonstrates a well-known local escalation method and includes walkthrough steps and mitigation advice.

🧰 Tools & Skills Demonstrated

- 🔹 Vulnerability Simulation & Exploitation
- 🔹 Splunk SIEM & Log Analysis
- 🔹 Linux User and Group Management
- 🔹 Network Troubleshooting (Ubuntu)
- 🔹 Penetration Testing Methodology
- 🔹 Windows Privilege Escalation
- 🔹 Secure Configuration & Hardening
- 🔹 Technical Documentation & Reporting

📌 Purpose

This repository serves as a learning and demonstration platform. Each project is designed to reflect real-world scenarios or certification-level skills, with a focus on clarity, reproducibility, and security best practices.

📫 Contact

Want to connect, collaborate, or ask questions?

- GitHub: Chontele-C
- Email: chontelec@gmail.com