Day 3 Activity File: Reporting

Congratulations, you've made it! You've worn two hats this week, playing the roles of both attacker and defender. Don't underestimate the magnitude of this achievement: Learning enough to infiltrate a machine and analyze data collected during the attack is a milestone that takes many professionals a long time to achieve.

Today, you'll take a break from flexing your technical skills and focus on communicating what you've learned in the past two days. In a real engagement, your client pays you not to break into their network, but to teach them how to protect it. This is why communication skills are vital in the cybersecurity field.

To that end, you will summarize your work in a presentation containing the following sections:

- **Network Topology**
  - What are the addresses and relationships of the machines involved?
  - All of the VMs in the attack should be described. Optionally, you can also include the hypervisor machine itself.
- **Red Team**
  - What were the three most critical vulnerabilities you discovered?
  - Choose the three vulnerabilities that *you* consider to be most critical.
- **Blue Team**
  - What evidence did you find in the logs of the attack?
  - What data should you be monitoring to detect these attacks next time?
- **Mitigation**
  - What alarms should you set to detect this behavior next time?
  - What controls should you put in place on the target to prevent the attack from happening?

Instructions

Open the template on Google Slides: Project 2 Report Template

- Make a copy by clicking **File** > **Make a Copy**.
- Fill out the prompts on the slides as indicated. Make sure to remove all instructional text and prompts.
- Some examples of vulnerabilities to look for are:
  - Sensitive Data Exposure
  - Unauthorized File Upload
  - Remote Code Execution
  - Brute Force Vulnerability
  - Local File Inclusion
  - Cross Site Scripting
  - Code Injection
  - SQL Injection
  - Security Misconfiguration

This presentation is due as homework. You must complete and submit it on BCS for credit. And remember, this document can be used to display your knowledge to interviewers and the larger cybersecurity network, so make it professional and presentable!