ProLUG Security Engineering

Unit 8 Worksheet

Instructions

Fill out this sheet as you progress through the lab and discussions. Hold your worksheets until the end to turn them in as a final submission packet.

Discussion Questions:

Unit 8 Discussion Post 1: Read about configuration management here: https://en.wikipedia.org/wiki/Configuration_management

a. What overlap of terms and concepts do you see from this week's meeting?
b. What are some of the standards and guidelines organizations involved with configuration management?
    i. Do you recognize them from other IT activities?

Unit 8 Discussion Post 2: Review the SRE guide to treating configurations as code. Read as much as you like, but focus down on the "Practical Advice" section: https://google.github.io/building-secure-and-reliable-systems/raw/ch14.html#treat_configuration_as_code

a. What are the best practices that you can use in your configuration management adherence?
b. What are the security threats and how can you mitigate them?
    a. Why might it be good to know this as you design a CMDB or CI/CD pipeline?

Definitions/Terminology

- System Lifecycle
- Configuration Drift
- Change management activities
    - CMDB
    - CI
    - Baseline

- Build book
- Run book
- Hashing
    - md5sum
    - sha<x>sum
- IaC
- Orchestration
- Automation
- AIDE

Notes During Lecture/Class:

Links:

- https://google.github.io/building-secure-and-reliable-systems/raw/ch14.html#treat_configuration_as_code
- https://en.wikipedia.org/wiki/Configuration_management
- https://www.sans.org/information-security-policy/
- https://www.sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/

Terms:

Useful tools:

- STIG Viewer 2.18
- Ansible
- Killercoda

Lab and Assignment

Unit8-Configuration-drift-remediation - To be completed outside of lecture time.

Digging Deeper

1. Review more of the SRE books from Google: https://sre.google/books/ to try to find more useful change management practices and policies.

Reflection Questions

1. How does the idea of control play into configuration management? Why is it so important?

2. What questions do you still have about this week?

3. How are you going to use what you've learned in your current role?