ProLUG Security Engineering

Unit 7 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 7 Discussion Post 1: Read about telemetry, logs, and traces. Ther are many good sources, even from Microsoft: https://microsoft.github.io/code-with-engineering-playbook/observability/log-vs-metric-vs-trace/

a. How does the usage guidance of that blog (at bottom) align with your understanding of these three items?
b. What other useful blogs or AI write-ups were you able to find?
c. What is the usefulness of this in securing your system?

Unit 7 Discussion Post 2: When we think of our systems, sometimes an airgapped system is simple to think about because everything is closed in. The idea of alerting or reporting is the opposite. We are trying to get the correct, timely, and important information out of the system when and where it is needed.

Read the summary at the top of: https://docs.google.com/document/d/199PqyG3UsyXlwieHaqbGiWVa8eMWi8zzAn0YfcApr8Q/edit?tab=t.0

a. What is the litmus test for a page? (Sending something out of the system?)
b. What is over-monitoring v. under-monitoring. Do you agree with the assessment of the paper? Why or why not, in your experience?
c. What is cause-based v. symptom-based and where do they belong? Do you agree?

Definitions/Terminology

- Telemetry

- Tracing
    - Span
    - Label
- Time Series Database (TSDB)
- Queue
- Upper control limit / Lower control limit (UCL/LCL)
- Aggregation
- SLO, SLA, SLI
- Push v. Pull of data
- Alerting rules
- Alertmanager
    - Alert template
    - Routing
    - Throttling
- Monitoring for defensive operations
    - SIEM
    - Intrusion Detection Systems - IDS
    - Intrusion Prevention Systems - IPS

Notes During Lecture/Class:

Links:

- https://promlabs.com/promql-cheat-sheet/
- 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
- SCC Tool (version varies by type of scan)
- OpenScap

Lab and Assignment

Unit7_Monitoring_and_Alerting - To be completed outside of lecture time.

Digging Deeper

1. Look into Wazuh: Security Information and Event Management (SIEM). Real Time Monitoring | Wazuh
    a. What are their major capabilities and features? (what they advertise)
    b. What are they doing with logs that increases visibility and usefulness in the security space? Log data analysis - Use cases · Wazuh documentation

Reflection Questions

1. What do I mean when I say that security is an art and not an engineering practice?

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?