ProLUG Security Engineering

Unit 6 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 5 Discussion Post 1: Review chapter 15 of the SRE book: https://google.github.io/building-secure-and-reliable-systems/raw/ch15.html#collect_appropriate_and_useful_logs. There are 14 references at the end of the chapter. Follow them for more information. One of them: https://jvns.ca/blog/2019/06/23/a-few-debugging-resources/ should be reviewed for question "c".

a. What are some concepts that are new to you?
b. There are 5 conclusions drawn, do you agree with them? Would you add or remove anything from the list?
c. In Julia Evan's debugging blog, which shows that debugging is just another form of troubleshooting, what useful things do you learn about the relationship between these topics? Are there any techniques you already do that this helps solidify for you?

Unit 5 Discussion Post 2: Read https://sre.google/sre-book/monitoring-distributed-systems/

a. What interesting or new things do you learn in this reading? What may you want to know more about?
b. What are the "4 golden signals"?
c. After reading these, why is immutability so important to logging? What do you think the other required items are for logging to be effective?

Definitions/Terminology

- Types of logs

    - Host
    - Application
    - Network
    - DB
- Immutable
- Structure of Logs
    - RFC 3164 BSD Syslog
    - RFC 5424 IETF Syslog
    - Systemd Journal
- Log rotation
- Rsyslog
- Log aggregation
    - ELK
    - Splunk
    - Graylog
    - Loki
- SIEM

Notes During Lecture/Class:

Links:

- https://grafana.com/docs/loki/latest/query/analyzer/
- https://www.sans.org/information-security-policy/
- https://www.sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/
- https://public.cyber.mil/stigs/downloads/

Terms:

Useful tools:

- STIG Viewer 2.18
- SCC Tool (version varies by type of scan)
- OpenScap

Lab and Assignment

Unit6_Logs_and_Parsing - To be completed outside of lecture time.

Digging Deeper

1. Find a cloud service and see what their logging best practices are for security incident response. Here is AWS: https://aws.amazon.com/blogs/security/logging-strategies-for-security-incident-response/
    a. What are the high level concepts mentioned?
    b. What are the tools available and what actions do they take?
    c. What are the manual and automated query capabilities provided, and how do they help you rapidly get to a correct assessment of the logged events?
2. Open up that STIG Viewer and filter by “logging” for any of the previous STIGs we’ve worked on. (Mariadb has some really good ones.)
    a. What seems to be a common theme?
    b. What types of activities MUST be logged in various applications and operating systems?
        i. Does it make sense why all logins are tracked?
        ii. Does it make sense why all admin actions, even just attempted admin actions, are logged?

Reflection Questions

1. What architectures have you used in your career?
    a. If you haven’t yet worked with any of these, what do you think you would architect in the ProLUG lab (~60 virtual machines, 4 physical machines, 1 NFS share, and 2 Windows laptops?)

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?