
LIGHTHOUSE LABS

Week 2 Day 4
Cyber Security Bootcamp

Attack Patterns Logs

We are making time to answer questions! Please don't worry!

LIGHTHOUSE LABS

Today . . .

Discussion: Logs and Indicators of Compromise and Best Practices

Demo: Demonstration Logs and Network Monitoring

Demo: Setting Thresholds and Alerts

Exercise: Setting Thresholds and Alerts

Lab Overview: Logging & Monitoring Scenario

Questions ?

Remarks on Yesterday. . .

Pushing Left: Cybersecurity requirements must be determined early in a project

Confidentiality, Integrity, and Availability

People Processes and Technology

Symmetric vs Asymmetric Encryption

Hashing vs Encryption

Threats to Encryption?

Questions ?

Logs, IoCs and Best Practices (1)

Logs are a record of an event at a time and a source, perhaps with some context

- Apps, Databases, Firewalls, Endpoints, IoT devices, Networks, Servers and Web Services

Logs are used to

- Uncover clues around the ‘who, when, where’ of an attack
- Identify suspicious activity
- See spikes in blocked/allowed traffic

https://www.crowdstrike.com/cybersecurity-101/observability/log-file/

Questions ?

Logs, IoCs and Best Practices (2)

Indicators of Compromise (IoC) are pieces of digital evidence that suggests an asset has been breached

Log events, Files, Processes, Network Connections

IoCs are monitored for by cyberdefense systems

Can be used to prevent further attacks on other systems

https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/

Questions ?

Logs, IoCs and Best Practices (3)

Best Practices

- Automation
- Centralized logging
- Customization of logging

https://www.crowdstrike.com/cybersecurity-101/observability/log-management/

Questions ?

Log discussion

Group 1: https://www.techtarget.com/searchsecurity/tip/Security-log-management-and-logging-best-practices

Group 2: https://crashtest-security.com/insufficient-logging-monitoring-guide/

Group 3: https://www.exabeam.com/explainers/event-logging/event-log/

Group 4: https://www.exabeam.com/explainers/event-logging/events-and-logs/

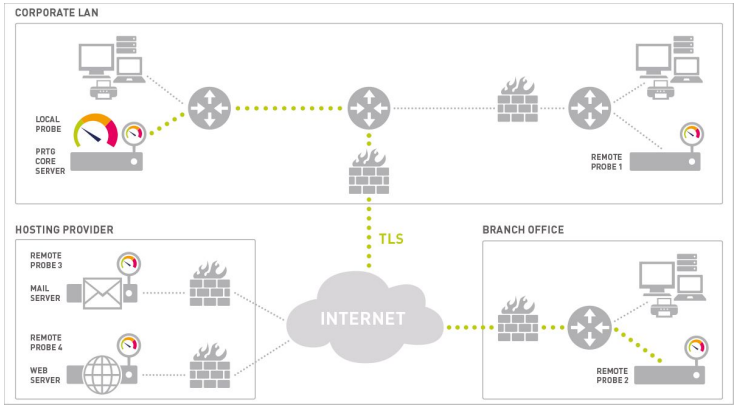
Group 5: https://www.exabeam.com/explainers/event-logging/log-aggregation/

Questions ?

Demo: PRTG

Unified monitoring tool that can monitor almost any object with an IP address

- Core server
  - Config, data management, etc.
- Probes
  - Collect data and monitor processes
  - Collection via sensors



Questions ?

Part 3 Demo: Setting Thresholds and Alerts

This section is to explain how you set Minimum and Maximum thresholds for monitoring a sensor.

Context

- Understand how the selection of monitored data and setting of thresholds can help protect an organization.
- Understand how changes in the environment or system use can change those thresholds.

Questions ?

Part 4 Exercise: Setting Thresholds and Alerts

Have groups explain which Sensor (data or event) they were researching, and the type of threshold, Minimum, Maximum or both that they would monitor, and why. Ask how changes in the system or use might change their thresholds.

Context

- Prove understanding of how the selection of monitored data and setting of thresholds can help protect an organization.
- Prove understanding of how changes in the environment or system use can change those thresholds.

Questions ?

Part 5 Lab Overview: Logging & Monitoring Scenario

Take what you have learned to do in Windows Based Systems, that is understand the purpose of the Event Log and logging and apply it to the Linux OS.

Activity

- Prepare for Monitoring exercise in Linux. Add a new system (Linux) to PRTG and monitor it.
- Prepare for Case Study and understand the scenario given and the expectations of the study.

Questions ?