Team Jupiter

VGU SIEM-Project

Instructor: Prof. Martin Kappes and Manuel Grob

Team leader: Vo Le Tung contact email: 13105@student.vgu.edu.vn

Dang Chi Cong

Bui Xuan Phuoc

Pham Nguyen Thanh An

Communication

Daily scrum will be hosted **every weekday** and **Saturday** at 1PM ICT.

Sprint duration: 1 week.

Sprint review and **sprint retrospective** at the **end of every week**.

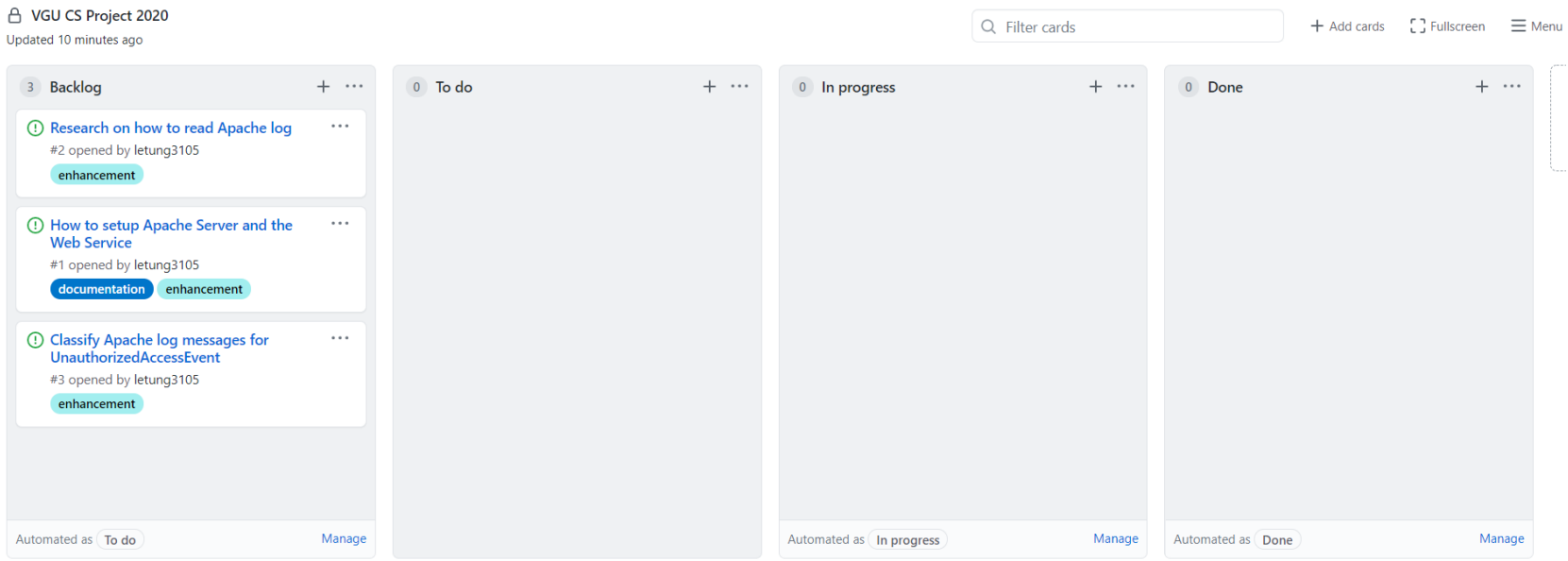
Zoom channel as the communication channel for daily scrums, sprint review and sprint retrospective.

Additional meetings can be hosted via **Zoom** or these can be **face to face meetings**.

Meetings duration may vary, depends on the purpose of the meeting and problems being brought up.

Document and code sharing

- Version control system and code sharing: **Github**.
- Project planning schedule and description: **Github's project service**



Sprint backlog

Subtasks	Time allocated	Personnel
How to setup Apache Server	4 hours	Dang Cong
Research how to read Apache log (raw event)	6 hours	Xuan Phuoc
Research on how to use Pcap4J (raw event)	7 hours	Thanh An
Classify Apache log messages for ConsecutiveFailedPasswordEvent	10.5 hours	
Classify Apache log messages for UnauthorizedAccessEvent	10.5 hours	
Detect HorizontalPortScanEvent	10.5 hours	
Detect BlockPortScanEvent	10.5 hours	
Detect VerticalPortScanEvent	10.5 hours	Le Tung

This week plan

- Each team member is assigned to one task.
- Continue taking items from the sprint backlog after finishing a task.

This week plan – Setting up Apache server

Description

Details the steps needed to setup an Apache Server.
The setup should be reproducible on different machines and OSes.

Expected time to completed: 4 hours

Dependencies: None

Checklist

[] Which software will be used to run the Apache Server?
[] Which web service will run on the server? (Ask Manuel and Prof. Kappes)
[] Documentation: details of how to setup?
[] References

This week plan – Research on how to read Apache log

Description

The SIEM system should be able to read log coming from Apache server.
The SIEM system should be able to extract Apache server's log messages and store them in the corresponding Java classes.

Expected time to complete: 6 hours

Dependencies: #1

Checklist

[] Where the log messages can be read?
[] Log format -> Corresponding Java classes?
[] Extract log message information. -> Which information will be used? Describe the java class?
[] Documentation

This week plan – Research on how to use Pcap4J

Description

The SIEM system should use Pcap4J to capture network packets from multiple host.
The SIEM system should be able to extract packet information.
The SIEM system should represent network packet with appropriate data structure.

Expected time to complete: 7 hours

Dependencies: None

Checkout

[] How to setup dependencies for Pcap4J?
[] Which elements of Pcap4J can be used to read network packet?
[] How to represent network packet in Java? -> What are the corresponding classes? -> Raw event type?
[] Documentation.

This week plan – Detect VerticalPortScanEvent

Description

The SIEM system should be able to alerts user about vertical port scans that are happening.

- The technique use for port scan is assumed to be simple TCP-connect, i.e, to check for open port, the malicious actor performs a full 3-way handshake with the host.
  The SIEM system should be able to prioritize vertical port scan events among themselves.

Expected time to complete: 10.5 hours

Dependencies: #5

Checklist

[] Which information of the packet can be used?
[] What is the event hierarchy? -> EPL? -> Java classes?
[] Events pattern?
[] How to different events of the same type can be prioritized? (e.g: more failures => higher priority)
[] Documentation