Course Syllabus

Identifying Web Attacks through Logs

Instructor Name: Igor Max Fernandes Vieira

Instructor Website: N/A

Instructor Contact: igormax@gmail.com

Course Creation Date: 01/06/2020

Course Description and Goals

Course Description:
This free course will review web application infrastructure, web servers, and the logs associated with them. We will also simulate 10 attack scenarios and identify the attack through logs that are generated by the web server.

An Akamai Report from 2018 described SQLi (SQL Injection), LFI (Local File Injection) and XSS (Cross-Site Scripting) as the most common web attacks.
(Summer SOTI - Web Attacks)

There are multiple types of web attacks. This course will review these attacks and teach you how to use the web application logs to identify them. To do this, the student will need to learn how to read a log and how to extract some of the key information from the log.

Subsequently, this first analysis of real world web server log examples will be used to get a better understanding of the attack. We will also use some scripts to find the information faster.

Following the log analysis of the web attacks, students will learn about some of the network that can affect the web application like DDOS (Distributed Denial of Service) and other types of flooding. Later with the completion of the course, the student should be able to read a web application log originated from the web server and identify some of the most common web attacks.

Prerequisites:

- Basic Computer Network knowledge
    - OSI and TCP/IP Model.
- Basic knowledge in common application and technology
    - Firewalls, DNS, IPS/IDS
    - HTTP/HTTPS

Study Resources:

- Quiz
- Supplementary Material

Course Goals: By the end of this course, students should be able to:

- ❑ Identify Key information on web server logs
- ❑ Identify malicious actions analyzing logs
- ❑ Identify web attacks after analyzing logs

Labs Used: In this course I will use a customized lab environment and I will teach how to set it up.

Course Outline

Module 1 | Introduction and Review

Lesson 1.1: Course Introduction.mp4 (04:05)
Lesson 1.2: Web Applications Architecture Review - Part 1.mp4 (09:43)
Lesson 1.3: Web Applications Architecture Review - Part 2.mp4 (09:13)
Lesson 1.4: Web Server Logs Review - Part 1.mp4 (07:11)
Lesson 1.5: Web Server Logs Review - Part 2.mp4 (07:46)
Lesson 1.6: Tips and Common Issues - Part 1.mp4 (08:25)
Lesson 1.7: Tips and Common Issues - Part 2.mp4 (09:35)

Module 2 | Identifying Web Attacks with Logs

Lesson 2.1: Web Application Attacks Review.mp4 (10:18)
Lesson 2.2: Vulnerability Scans.mp4 (09:38)
Lesson 2.3: Brute Force Attacks.mp4 (07:42)
Lesson 2.4: SQL Injection Attacks.mp4 (10:!5)
Lesson 2.5: File Inclusion Attacks.mp4 (08:09)
Lesson 2.6: XSS Attacks.mp4 (09:57)
Lesson 2.7: CSRF Attacks.mp4 (04:24)
Lesson 2.8: Other log Sources - Part 1.mp4 (10:17)
Lesson 2.8: Other log Sources.mp4 (08:21)
Lesson 2.9: Other log Sources - Part 2.mp4 (04:15)
Lesson 2.10: Course Summary.mp4