Course Syllabus

Sniffing

Instructor Name: Ken Underhill, CEH,CHFI

Instructor Contact: https://www.linkedin.com/in/ken-underhill-ceh-chfi-7b640a140/

Course Creation Date: 03/25/2019

Course Description and Goals

Course Description: In this course, we focus our attention on two common tools for sniffing for penetration testing: Wireshark and TCPDump. The course is intended to be primarily hands-on, so you will need access to either the Cybrary lab environment or you will need to build out your own virtual systems for testing. We do not cover the build out of your own virtual systems in this course. All hands-on labs for the course will have an associated step by step guide and we have also provided additional study resources with this course.

The course is focused on hands-on learning and students will need access to the Cybrary lab environment to complete the step by step labs as well as the final assessments. However, students can also choose to set up their own labs but setup and configuration of those labs will not be covered in this course.

Prerequisites: Basic knowledge of Cyber security, Linux (Ubuntu) and networking.

Study Resources:

TCPDump Cheat Sheet
Wireshark Cheat Sheet
Wireshark & TCPDump Study Guide
Wireshark Filters
Wireshark & TCPDump Sources

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

- □ Use Wireshark and TCPDump to analyze captured network traffic.
- □ Use Wireshark and TCPDump filters to perform packet analysis.

Labs Used:
Lab 1 Wireshark
Lab 2 Packet Sniffing
Lab 3 Applying Filters to TCPDump and Wireshark
Lab 4 TCPDump

Course Outline

Module 1 | Introduction

Lesson 1.1 Introduction (05:54)

Module 2 | Wireshark and TCPDUMP

Lesson 2.1 Wireshark Lab Part 1 (07:44)
Lesson 2.2 Wireshark Lab Part 2 (07:10)
Lesson 2.3 Wireshark Lab Part 3 (04:59)
Lesson 2.4 Packet Sniffing Lab Part 1 (09:04)
Lesson 2.5 Packet Sniffing Lab Part 2 (04:25)
Lesson 2.6 Applying Filters to TCPDUMP and Wireshark Lab Part 1 (10:03)
Lesson 2.7 Applying Filters to TCPDUMP and Wireshark Lab Part 2 (09:32)
Lesson 2.8 TCPDUMP Lab (08:56)

Module 3 | Conclusion

Lesson 3.1 Capstone Lab Navigation (01:56)
Lesson 3.2 Conclusion (02:48)