Syllabus

Threat Hunting

CYBERIUM ARENA
-SIMULATOR-

Description

In today's cybersecurity landscape, it isn't possible to prevent every attack. Threat hunting is the proactive technique that focuses on pursuing attacks and the evidence that attackers leave behind when they patrol an attack using malware or expose sensitive data. The process is important and is based on thinking that the attacker has already managed to infiltrate and test everything possible to detect intrusion earlier to stop them before intruders can carry out their attacks and exploit them illegally.

Target Audience

This course targets people with networking knowledge who want to acquire the threat hunting capabilities to protect their organization better.

Pre-requisites

Linux
Networking

Objectives

- Identify and create intelligence requirements through practices
- Generate threat intelligence to detect and respond
- Learn the different sources to collect adversary data
- Create Indicators of Compromise (IOCs)

Module 1: Introduction to Threat Intelligence

In this module, students will learn about techniques and procedures necessary to effectively hunt, detect, and contain various adversaries and minimize incidents.

Intrusion Analysis

- Phases of Threat Intelligence
- Phases of the Intrusion Kill Chain
- Understanding MITRE ATT&CK
- Identifying Intrusions in Logs
- Creating Automation for Notification of Malicious
- Activity Analyzing Network-Based Tools Logs
- Analyzing Host-Based Tools Logs
- Linking Intrusions

Memory Forensics

- Process Injection
- Thread Injection
- Malware Analysis
- Malicious Document Analysis

Module 2: Data Collection

Students will use practical tools to collect data throughout this module. Students will deepen their understanding of various information sources.

Hunting

- Parsing Relevant Data Techniques
- Virus Total
- OSINT
- Dynamic Indicators
- Tracking Network Traffic
- Passive DNS
- Ransomware Traffic

Sources

- Malware Analysis Data Bases
- Intrusion Key Indicators
- Domain Data Collection
- Open-Source Intelligence Tools
- C2 Samples

Module 3: Threat Intelligence Automation

During this module, students will be creating tool automation to take threat intelligence to a higher level. Students will understand how to use their knowledge and maximize the use of different filtering and customization options for searching.

Automation

- YARA Examples
- Working with YARA
- Automating Malware Analysis
- Configuring Honeypots
- Extracting and Analysing Honeypots Logs

Domain Automation

- Running Campaigns
- Checking Key Indicators Inside Domains
- Creating Your Indicators
- Tactical Intelligence Tools
- Operational Intelligence Tools

Darknet

- Relevant Leaks
- Hacking Forums