Mosse Security: Threat Hunting Master Course

Course Overview

Mossé Security teaches students a unique approach to threat hunting based on data science, active deception and the development of custom intrusion detection tools.

In this five-day master course, students will learn how to hunt for threat actors on large scale computer networks. No prior knowledge in incident response, threat hunting, reverse engineering or malware analysis is required prior to attending this course. Detailed step-by-step instructions will be given, and students will leave this course with practical skills to hunt for attackers on their networks, or their clients' networks.

Our approach to teaching Threat Hunting is to teach the fundamental concepts and strategies that can be used to detect threat actors on any operating systems and types of networks. In this way, we ensure that our students can immediately apply the techniques they have learnt, and rapidly build upon their skills to hunt for more complex attack techniques. Theoretical knowledge makes up 40% of the course content, and 60% is devoted to practical exercises. At the end of the course, a Threat Hunting exercise is conducted that can be reproduced at your workplace.

Duration

3 Days

Course Outline

Students will complete the following modules

Module 1: Introduction

- What is Threat Hunting and how to do it?
- The Threat Hunting process
- The Threat Hunting toolset
- Building a Threat Hunting division
- Preparing a Threat Hunting playbook

Module 2: Windows Internals

- User-land vs. kernel-land
- Processes, thread, services and drivers
- The registry
- The file system
- Event logs
- Users and groups
- Access tokens
- Schedules tasks
- Active Directory
- Windows Management Instrumentation
- Networking
- Command execution and scripting

Module 3: Data Science Toolset

- Mastering Numpy and Pandas
- Mastering Google BigQuery
- Mastering Graph Databases
- Using the Jupyter Notebook
- Rapid environment deployment with Ansible

Our credentials

- Rapid web services with Google App Engine
- Messaging services with Google Pub/Sub

Module 4: Compromise Assessments

- Rapid capture of security data using WMI and PowerShell
- Building a lightweight incident response data collection tool
- Rapid incident detection using Pandas, statistics and data visualisation
- Rapid file acquisition techniques

Module 5: Real-Time Endpoint Monitoring

- Building your own real-time endpoint detection and response tool
- Monitoring processes, services and drivers
- Monitoring sensitive user accounts
- Monitoring event logs
- Building a threat graph
- Detecting compromise phases:
- Initial compromise
- Privilege escalation
- Host reconnaissance
- Network reconnaissance
- Password dumping
- Persistence
- Lateral movement
- Building IOCs based on endpoint behavior

Module 6: Rapid Malware Analysis

- Building a malware research lab in the cloud
- Using virtual machines to analyse malware
- Using a virtual network to extract IOCs
- Static code analysis
- Reverse engineering common attacker toolkits
- Building countermeasures against attacker toolkits

Module 7: Network Security Monitoring

- Analysing Netflow data
- Analysing PCAP files
- Analysing web server logs
- Detecting covert communication channels
- Extract IOCs from NSM data

Module 8: Rapid Incident Response

- Pre-incident preparation
- Security logs to enable
- Checklists, report templates, processes, policies
- Network design and architecture for incident response
- The RIR Process
- Initial response

- Investigation
- Remediation
- Reporting
- Extracting lessons learnt
- Building the timeline of a security intrusion
- Communicating effectively during incident response

Module 9: Threat Hunting Workshop
The last day of the training is a large-scale threat hunting workshop across hundreds of machines, multiple organisations and going against many adversary groups.

Audience

Students who attend this training should already have the following technical knowledge:

- Experience with AD DS concepts and technologies in Windows Server 2012 or Windows Server 2016.
- Experience configuring Windows Server 2012 or Windows Server 2016.
- Basic experience with Windows PowerShell.
- Basic experience with cloud services such as Microsoft Office 365.
- Basic experience with the Azure platform.
- Basic experience with identities on premises or in cloud.

Pre-Requisites

Recommended Study
We recommend that you read about the Windows components listed under Module 2 “Windows Internals”. Even if those components will be covered in detailed during the course, studying them prior to the course will make it a lot easier for you to understand every other module in the class.

Software Requirement
Bring a laptop running the Windows or UNIX operating system with the OpenVPN or Tunnelblick client to connect into our training lab in the cloud.

Learning Outcomes

You will learn strategies and tactics to deliver threat hunting campaigns on large scale computer networks:

- The threat hunting process and how to build a threat hunting team
- Key Windows internals knowledge for threat hunting
- How to use data science to hunt for adversaries on large networks
- Search for indicators of compromise (IOCs) across the entire kill chain
- Build your own compromise assessment tools
- Build your own real-time endpoint detection and response tool
- Rapidly reverse-engineer malware
- Extract indicators of compromise on the network and the endpoints
- Rapidly respond and contain intrusions