CYBRARY

Application of the MITRE Attack Framework

Instructor Name: Robert Smith

Instructor Contact: Robertjsmith88@gmail.com

Instructor Website:
https://www.cybrary.it/instructor/robert-smith

Course Creation Date: 01/30/2020

Course Description and Goals

Course Description: The MITRE Attack Framework is a globally accessible knowledge base of tactics and techniques provided from real-world observations. Using the attack framework, a security consultant or blue team member can formulate a strategy for reducing risk in both the Public and Private Sectors.

During this course we will move through the 12 areas of the MITRE Attack Framework and discuss how security professionals should use the matrix to assist them in overlaying solutions or controls to address current threats.

Since the methods of attack change regularly this course is going to focus on examples for several of the attack types in each section and applicable mitigation tactics. These principles can then be applied across the entire framework whether you are looking at adding a security solution to your current stack or are doing research on known attack vectors for academic purposes.

Prerequisites:

- Basic technical terminology understanding
- Basic terminology in association with controls
- Basic terminology in association with risk reduction

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

Understand Initial Access Attack Vectors Such As:

- Drive-by Compromise
- Spear phishing Link
- Supply Chain Compromise
- Trusted Relationship

Course Resources

The Site for the Framework is here: https://attack.mitre.org/

Course Outline

Module 1 | Introduction

Lesson 1.1: What is the MITRE Attack Framework?
Lesson 1.2: Where is the MITER Attack Framework Being Used?
Lesson 1.3: Site Navigation and Review

Module 2 | Initial Access

Lesson 2.1: What is Initial Access
Lesson 2.2: External Remote Services
Lesson 2.3: Spear Phishing Link
Lesson 2.4: Supply Chain Compromise
Lesson 2.5: Trusted Relationship
Lesson 2.6: Valid Accounts
Lesson 2.7: Case Study: Initial Access
Lesson 2.8: Summary

Module 3 | Execution

Lesson 3.1: What is Execution
Lesson 3.2: Command Line Interface
Lesson 3.3: Execution through API
Lesson 3.4: Control Panel Items
Lesson 3.5: PowerShell
Lesson 3.6: Scripting
Lesson 3.7: User Execution
Lesson 3.8: Case Study: Execution
Lesson 3.9: Summary

Module 4 | Persistence

Lesson 4.1: What is Persistence
Lesson 4.2: Accessibility Features
Lesson 4.3: Bootkit
Lesson 4.4: Browser Extension
Lesson 4.5: Component Firmware
Lesson 4.6: Create Account
Lesson 4.7: Hooking
Lesson 4.8: New Service
Lesson 4.9: Case Study: Persistence
Lesson 4.10: Summary

Module 5 | Privilege Escalation

5.1 What is Privilege Escalation
5.2 Access Token Manipulation
5.3 Elevated Execution with Prompt
5.4 Exploitation for Privilege Escalation
5.5 File System Permission Weakness
5.6 Scheduled Task
5.7 Sudo
5.8 Web Shell
5.9 Case Study: Privilege Escalation
5.10 Summary

Module 6 | Defense Evasion

Lesson 6.1: What is Defense Evasion
Lesson 6.2: Clear Command History
Lesson 6.3: Compile After Delivery
Lesson 6.4: Disabling Security Tools
Lesson 6.5: Hidden Files and Directories
Lesson 6.6: Hidden Users

Lesson 6.7: Hidden Window
Lesson 6.8: Process Hollowing
Lesson 6.9: Software Packing
Lesson 6.10: Case Study: Defense Evasion
Lesson 6.11: Summary

Module 7 | Credential Access

Lesson 7.1: What is Credential Access
Lesson 7.2: Bash History
Lesson 7.3: Brute Force
Lesson 7.4: Credential Dumping
Lesson 7.5: Credentials in Files
Lesson 7.6: Keychain
Lesson 7.7: Network Sniffing
Lesson 7.8: Steal Web Session Cookie
Lesson 7.9: Case Study: Credential Access
Lesson 7.10: Summary

Module 8 | Discovery

Lesson 8.1: What is Discovery
Lesson 8.2: Account Discovery
Lesson 8.3: Browser Bookmark Discovery
Lesson 8.4: Network Service Scanning
Lesson 8.5: Password Policy Discovery
Lesson 8.6: Query Registry
Lesson 8.7: Software Discovery
Lesson 8.8: System Owner/User Discovery
Lesson 8.9: Case Study: Discovery
Lesson 8.10: Summary

Module 9 | Lateral Movement

Lesson 9.1: What is Lateral Movement
Lesson 9.2: Application Deployment Software
Lesson 9.3: Exploitation of Remote Services
Lesson 9.4: Internal Spear Phishing
Lesson 9.5: Logon Scripts
Lesson 9.6: Pass the Hash
Lesson 9.7: SSH Hijacking
Lesson 9.8: Case Study: Lateral Movement
Lesson 9.9: Summary

Module 10 | Collection

Lesson 10.1: What is Collection
Lesson 10.2: Audio Capture
Lesson 10.3: Clipboard Data
Lesson 10.4: Data from Local System
Lesson 10.5: Data from Removable Media
Lesson 10.6: Email Collection
Lesson 10.7: Man in the Browser
Lesson 10.8: Case Study: Collection
Lesson 10.9: Summary

Module 11 | Command and Control

Lesson 11.1: What is Command and Control
Lesson 11.2: Commonly Used Port
Lesson 11.3: Custom Command and Control Protocol
Lesson 11.4: Data Encoding
Lesson 11.5: Fallback Channels
Lesson 11.6: Multi-hop Proxy
Lesson 11.7: Remote Access Tools
Lesson 11.8: Uncommonly Used Port

Lesson 11.9: Case Study: Command and Control
Lesson 11.10: Summary

Module 12 | Exfiltration

Lesson 12.1: What is Exfiltration
Lesson 12.2: Automated Exfiltration
Lesson 12.3: Data Compressed
Lesson 12.4: Data Transfer Size Limits
Lesson 12.5: Exfiltration Over Alternative Protocol
Lesson 12.6: Scheduled Transfer
Lesson 12.7: Case Study: Exfiltration
Lesson 12.8: Summary

Module 13 | Impact

Lesson 13.1: What is Impact
Lesson 13.2: Account Access Removal
Lesson 13.3: Defacement
Lesson 13.4: Disk Content Wipe
Lesson 13.5: Firmware Corruption
Lesson 13.6: Service Stop
Lesson 13.7: System Shutdown/Reboot
Lesson 13.8: Case Study: Impact
Lesson 13.9: Summary

Module 14 | Conclusion

Lesson 14.1: Course Summary