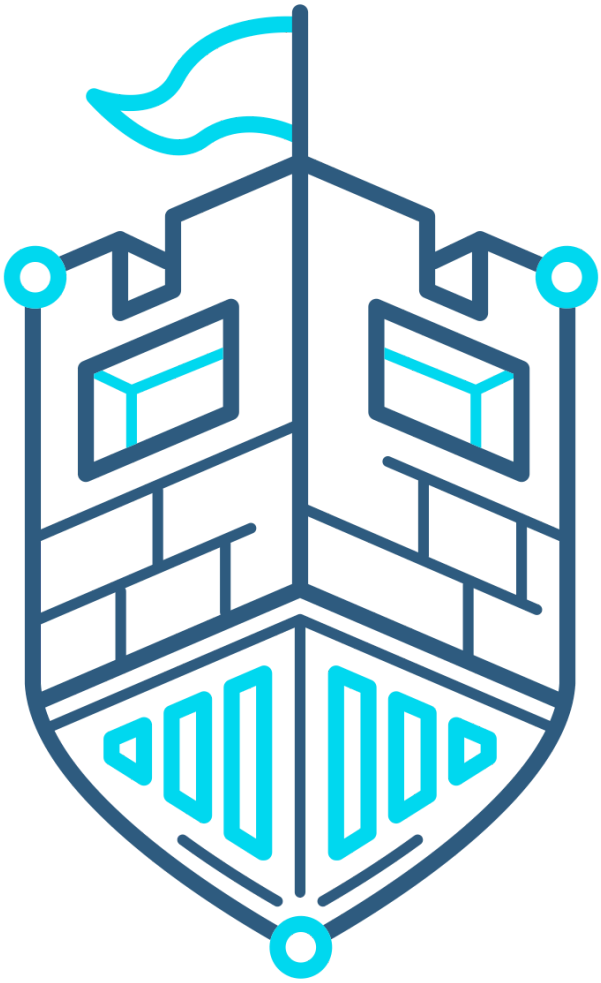
Security Operations and Defensive Analysis

Syllabus



PowerShell

d. Programming on Windows
   - Component Object Model
   - .NET and .NET Core
e. Windows Event Log
   - Introduction to Windows Events
   - PowerShell and Event Logs
f. Empowering the Logs
   - System Monitor (Sysmon)
   - Sysmon and Event Viewer
   - Sysmon and PowerShell
   - Remote Access with PowerShell Core
g. Wrapping Up

5. Windows Server Side Attacks
   a. Credential Abuse
      - The Security Account Manager (SAM) and Windows Authentication
      - Suspicious Logins
      - Brute Force Logins
   b. Web Application Attacks
      - Internet Information Services (IIS)
      - Local File Inclusion
      - Command Injection
      - File Upload
   c. Binary Exploitation
      - Binary Attacks
      - Windows Defender Exploit Guard (WDEG)
   d. Wrapping Up
6. Windows Client-Side Attacks
   a. Attacking Microsoft Office
      - Social Engineering and Spearphishing
      - Installing Microsoft Office
      - Using Macros
   b. Monitoring Windows PowerShell
      - Introduction to PowerShell Logging

- PowerShell Module Logging
- PowerShell Script Block Logging
- PowerShell Transcription
- Case Study: PowerShell Logging for Phishing Attacks
- Obfuscating/Deobfuscating Commands

c. Wrapping Up

7. Windows Privilege Escalation
   a. Privilege Escalation Introduction
      - Privilege Escalation Enumeration
      - User Account Control
      - Bypassing UAC
   b. Escalating to SYSTEM
      - Service Creation
      - Attacking Service Permissions
      - Leveraging Unquoted Service Paths
   c. Wrapping Up
8. Windows Persistence
   a. Persistence on Disk
      - Persisting via Windows Service
      - Persisting via Scheduled Tasks
      - Persisting by DLL-Sideloading/ Hijacking
   b. Persistence in Registry
      - Using Run Keys
      - Using Winlogon Helper
   c. Wrapping Up
9. Linux Endpoint Introduction
   a. Linux Applications and Daemons
      - Daemons
      - Logging on Linux and the Syslog Framework
      - Rsyslog Meets Journal
      - Web Daemon Logging
   b. Automating the Defensive Analysis
      - Python for Log Analysis
      - DevOps Tools

- Hunting for Login Attempts
- c. Wrapping Up

10. Linux Server Side Attacks
    - a. Credential Abuse
        - Suspicious Logins
        - Password Brute Forcing
    - b. Web Application Attacks
        - Command Injection
        - SQL Injection
    - c. Wrapping Up
11. Linux Privilege Escalation
    - a. Attacking the Users
        - Becoming a User
        - Backdooring a User
    - b. Attacking the System
        - Abusing System Programs
        - Weak Permissions
    - c. Wrapping Up
12. Network Detections
    - a. Intrusion Detection Systems
        - Theory and Methodology
        - Foundations of IDS and Rule Crafting
    - b. Detecting Attacks
        - Known Vulnerabilities
        - Extra Mile I
        - Unknown Vulnerabilities
    - c. Detecting C2 Infrastructure
        - C2 Infrastructure
        - Extra Mile II
        - Network Communications
    - d. Wrapping Up
13. Antivirus Alerts and Evasion
    - a. Antivirus Basics
        - Antivirus Overview

- Signature-Based Detection
- Real-time Heuristic and Behavioral-Based Detection

b. Antimalware Scan Interface (AMSI)
- Understanding AMSI
- Bypassing AMSI

c. Wrapping Up

14. Network Evasion and Tunneling

a. Network Segmentation
- Network Segmentation Concepts and Benefits
- Segmentation Theory

b. Egress Busting
- Detecting Egress Busting

c. Port Forwarding and Tunneling
- Port Forwarding and Tunneling Theory
- Port Forwarding and Tunneling in Practice

d. Wrapping Up

15. Active Directory Enumeration

a. Abusing Lightweight Directory Access Protocol
- Understanding LDAP
- Interacting with LDAP
- Enumerating Active Directory with PowerView

b. Detecting Active Directory
- Auditing Object Access
- Baseline Monitoring
- Using Honey Tokens

c. Wrapping Up

16. Windows Lateral Movement

a. Windows Authentication
- Pass the Hash
- Brute Force Domain Credentials
- Terminal Services

b. Abuse the Kerberos Ticket
- Pass the Ticket
- Kerberoasting

c. Wrapping Up

17. Active Directory Persistence
    a. Keeping Domain Access
        Domain Group Memberships
        Domain User Modifications
        Golden Tickets
    b. Wrapping Up
18. SIEM Part One: Intro to ELK
    a. Log Management Introduction
        SIEM Concepts
        Elastic Stack (ELK)
        ELK Integrations with OSQuery
    b. ELK Security
        Rules and Alerts
        Timelines and Cases
    c. Wrapping Up
19. SIEM Part Two: Combining the Logs
    a. Phase One: Web Server Initial Access
        Enumeration and Command Injection of web01
        Phase One Detection Rules
    b. Phase Two: Lateral Movement to Application Server
        Brute Force and Authentication to appsrv01
        Phase Two Detection Rules
    c. Phase Three: Persistence and Privilege Escalation on Application Server
        Persistence and Privilege Escalation on appsrv01
        Phase Three Detection Rules
    d. Phase Four: Perform Actions on Domain Controller
        Dump AD Database
        Phase Four Detection Rules
    e. Wrapping Up
20. Trying Harder: The Labs
    a. Challenges
        Completing the SOC-200 Challenges
    b. Wrapping Up