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