POWERSHELL FOR DEFENDERS COURSE

The PowerShell for Defenders Course (PoD) is based on the tools and practices used by professional government and corporate network defenders and incident responders, but with a strong emphasis on utilizing Windows PowerShell to leverage the .NET framework and Windows Management Instrumentation. PoD focuses on detection, counter-infiltration and prevention, as well as tool building and scripting, with an emphasis on leveraging the core capabilities for defense, rather than relying on security products. Students will be exposed to and learn network defense and incident response techniques. PoD covers a wide range of defensive tactics, including hashing and baselining, process analysis, Log analysis and correlation, as well as the basics of digital forensics and incident response (DFIR). The course is very hands on, with each section being reinforced with multiple labs, and concludes with a culmination exercise to test the skills the students have learned.

CHIRON METHODOLOGY DOMAIN

CYBER PROTECTION PROFESSIONAL™ (CPP)™

DURATION
5 DAYS

RECOMMENDED PRE-REQUISITES

- Familiarity with Windows Administration and basic defensive concepts
- Familiarity with VMware Workstation
- Exposure to Windows PowerShell
- Exposure to basic scripting concepts

PHONE: 410.672.1552 x 109 **FAX:** 410.672.3187 **ADDRESS** 7021 Columbia Gateway Dr. Suite 250 Columbia, MD 21046

POWERSHELL FOR DEFENDERS COURSE

COURSE SCHEDULE

DAY 1:

LEARNING OBJECTIVES

- Understanding how Windows PowerShell works and the fundamentals of how it leverages both Windows Management Instrumentation (WMI) and the .NET framework
- Knowledge of how to find the correct PowerShell command to complete the desired action, and how to determine the proper syntax for that command
- Demonstrate the ability to identify digital remnants of exploitation in both the Windows event logs and on the file system using PowerShell
- Knowledge of registry navigation and manipulation using PowerShell.
- Demonstrate the ability to fully prosecute a running process or service suspected of being malware using only PowerShell

OUTLINE

- Orientation
- Introductions
- Introduction to PowerShell
  - Overview of PowerShell & the .NET framework
- PowerShell Basics
  - Cmdlets
  - Finding commands and Using Help
  - Commands & the pipeline
  - PowerShell providers & drives
  - PowerShell and the Windows File System
  - Finding digital artifacts using PS
- Event Logs & Registry
  - Basic event log queries
  - Filtering event logs based on event, time, and message
  - Custom logging in PS
  - Querying the registry using PS
  - Adding, modifying, and deleting registry keys using PS
- Prosecuting Processes and Services
  - Process investigation leveraging .NET
  - Service investigation leveraging WMI

DAY 2:

LEARNING OBJECTIVES

- Deep understanding of WMI Objects and how they are leveraged by PowerShell
- Understanding of how to schedule both standard and background jobs in PowerShell
- Demonstrate the ability to successfully manipulate a remote target using PowerShell
- Understanding of PowerShell scripting fundamentals
- Demonstrate the ability to write a custom PowerShell function, load it, and then execute the function

OUTLINE

- PowerShell & WMI
  - Using PS to manipulate WMI objects
  - Creating PS script that trigger on WMI event registration
- PowerShell Scheduled Jobs
  - Basics of PS scheduled jobs
  - Scheduling background jobs in PS
- PowerShell Remoting
  - Executing PS commands on remote hosts
  - Manipulating PS script execution policy on a remote host
  - Running local scripts on remote targets
- PowerShell Scripting
  - Working with the PowerShell ISE
  - Variables, nomenclature & syntax
  - Writing & calling PS functions
  - Writing PS tools, functions, scripts, and modules

POWERSHELL FOR DEFENDERS COURSE

COURSE SCHEDULE

DAY 3:

LEARNING OBJECTIVES

- Demonstrate the ability to write a host enumeration survey to determine general host information, as well as the security posture of the host, and check for potential malware infections
- Knowledge of how to generate file hashes using PowerShell to baseline a system
- Knowledge of PowerShell methods of process investigation leveraging both .NET and WMI objects
- Demonstrate the ability to conduct deep process investigation using only PowerShell
- Understanding of PowerShell techniques to read, filter and correlate Windows Event Logs, as well as how to create custom entries to the event log
- Understanding of WMI permanent event registrations, including how to write WQL filters, consumers, and bindings
- Demonstrate the ability to successfully configure the Uproot host-based intrusion detection system (HIDS) to detect malicious activity on the host

OUTLINE

- PS Surveys
  - Persistence vector enumeration
  - Network activity enumeration
  - Security posture enumeration (auditing and AV settings)
- Hashes & Baselines
  - Generating file hashes using older versions of PowerShell
  - Creating System baselines
  - Automating file integrity checks
- Process & Service Analysis
  - Using PowerShell for deep process analysis
  - Using PowerShell for deep service analysis
  - Correlating network activity and persistence vectors to processes
  - Writing process investigation scripts
- Advanced event log monitoring
  - Event Log enumeration deep dive
  - Filtering based on specific users and computers for anomalies
  - Filtering for specific attack types
  - Lab – Log Analysis
- Uproot HIDS
  - WMI permanent event registration
  - Writing custom filters and consumers
  - Lab – Uproot IDS

DAY 4:

LEARNING OBJECTIVES

- Understanding of Locard's exchange principal and other incident response concepts
- Demonstrate the ability to detect malicious PowerShell code utilization on a host
- Understanding of how the Powertools and PowerSploit frameworks can be leveraged for defensive purposes
- Understanding of how PowerForensics collects file system information without corrupting evidence
- Demonstrate the ability to conduct timeline analysis of an incident using PowerForensics

OUTLINE

- Incident response and timeline analysis Overview
  - Fundamentals of IR
- Leveraging offensive tools for defense
  - PowerSploit for defense
  - PowerTools for defense
- Detecting Malicious Powershell
  - Powershell auditing techniques and capabilities
  - Developing signatures for offensive powershell frameworks
- PowerForensics
  - Intro to PowerForensics
  - PowerForensics for timeline analysis

POWERSHELL FOR DEFENDERS COURSE

COURSE SCHEDULE

DAY 5:

LEARNING OBJECTIVES

- Demonstrate the ability to analyze a compromised system to determine the intrusion and construct a timeline of events
- Demonstrate the ability to put new defensive measures in place to detect and prevent future intrusions
- Demonstrate the ability to detect a simulated attack in real time and counter act it as it occurs
- Demonstrate the ability to perform all actions and objectives taught during the course in a six-hour culmination exercise in a virtualized network environment

OUTLINE

- Culmination Exercise (CULEX)