POWERSHELL FOR RED TEAMING COURSE

The PowerShell for Red Teaming Course (PoRT) is based on the methodologies and processes used by professional government and corporate penetration testers, but with a strong emphasis on utilizing Windows PowerShell to leverage the .NET framework and Windows Management Instrumentation. PoRT focuses on scanning, host enumeration, remote and local exploitation, as well as tool building and scripting, with an emphasis on avoiding detection by users or security products. Students will be exposed to and learn penetration testing using advanced persistent threat techniques. PoRT covers a wide range of tactics, including client-side exploitation, process analysis, redirection and tunneling, as well as maintaining persistent presence on a target. 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 THREAT EMULATION PROFESSIONAL™ (CTEP)™

DURATION
5 DAYS

RECOMMENDED PRE-REQUISITES

- Familiarity with Windows Administration and basic exploitation techniques
- 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 RED TEAMING 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 custom PowerShell functions, modules, and scripts

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 RED TEAMING 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 target, and check for potential malware infections.
- Knowledge of PowerShell payload types and the inherent functionality of each type.
- Demonstrate the ability to scan and enumerate a network using only PowerShell.
- Understanding of PowerShell techniques to bypass Microsoft security protections, increasing the effectiveness of client-side exploits.
- Understanding of PowerShell remote and local exploitation techniques.
- Demonstrate the ability to successfully exploit a target using social engineering and masquerade PowerShell techniques and elevate privileges.

OUTLINE

- PS Payloads
  - Veil-PS payloads
  - Building PS payloads
- PS Client-side Exploitation
  - Embedding PS payloads in documents
  - PS Exchange phishing attacks
  - Using the Nishang framework
- PS Surveys
  - Full host enumeration surveys
  - Remote host enumeration surveys
  - PS Security product enumeration
- PS Privilege Escalation
  - Power-Up
  - Getting SYSTEM with PS
- PS Scanning
  - Building network enumeration scanning tools
  - PS port scanning
  - Host SMB enumeration using PS & WMI
- PS Masquerade Techniques
  - Utilizing PS drives and scheduled jobs to exploit remote hosts
  - Exploiting RDP sessions utilizing memory resident techniques

DAY 4:

LEARNING OBJECTIVES

- Understanding of how to enumerate Active Directory using both the PowerShell AD modules and the Active Directory Services Interface (ADSI)
- Understanding of how the Powertools framework can be leveraged to enumerate a network.
- Understanding of PowerShell persistence techniques and which would be optimal for a given situation.
- Understanding of PowerShell collection tools and techniques.

OUTLINE

- Active Directory
  - PS Active Directory Modules
  - Leveraging ADSI
- PowerTools
  - Overview of the PowerTools framework
- Persistence
  - PS service persistence techniques
  - PS persistence using scheduled jobs
  - PS backdoors with WMI triggers
- PS Collection
  - Packet sniffers
  - Data exfiltration
  - Automating collection

DAY 5:

LEARNING OBJECTIVES

- Understanding of how the PowerSploit framework can be leveraged to enumerate a network.
- Understanding of how the PS Empire framework can be used for operations on multiple targets simultaneously.
- 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

- PowerSploit
  - Overview of the Powersploit Framework
- PowerShell Empire
  - PS Empire Basics
  - Advanced Empire tactics
- Culmination Exercise (CULEX)