C)PSH: Certified PowerShell Hacker

Course ID #: 7000-790-ZZ-Z
Hours: 28

Course Content

Course Description:

In this course you will cover the keys to being a Powershell hacker. Most companies have an Active Directory infrastructure that manages authentication and authorization to most devices and objects within the organization. Many use PowerShell to speed up and simplify management.

Did you know that a large percentage of hacks over the last year included PowerShell based attacks? Well, they did. A Powershell Hacker can be a security risk, or an asset to prevent breaches. Which is why we spend 4 days learning how to hack like the pros using nothing but what is already available to us in Windows or now in open-source code on Mac and Linux! The course is based on real world implementations of a windows infrastructure along with real world penetration testing techniques. You will leave with a real strong skill set to help test your windows environment like never before. An attendee will also walk away with a strong skill set on how to help prevent these attacks from happening in the first place!

Course Objectives:

Upon successful completion of this course students will be able to:

- Competently take the C)PSH exam
- Protect a powershell system from attack

Prerequisites:

- C)PEH and C)PTE or equivalent knowledge
- Understanding of pen testing
- General understanding of active directory
- General understanding of scripting and programming

Target Audience:

- Microsoft Administrators
- Cybersecurity Managers/Administrators
- Penetration Testers
- Active Directory Administrators

Topics:

Lesson 1: Introduction to PowerShell

- Different Tool Options
- Installing everything needed
- Language Basics
- Using the Windows API and WMI
- Interacting with the Registry
- Managing Objects and COM Objects

C)PSH: Certified PowerShell Hacker

Course ID #: 7000-790-ZZ-Z

Hours: 28

Lesson 2: Introduction to Active Directory and Kerberos

- Overview of Kerberos
- The three-headed monster
- Key Distribution Center
- Kerberos in Detail
- Why we care about Kerberos as a Hacker
- Overview of Active Directory
- Understanding AD concepts
- AD Objects and Attributes

Lesson 3: Pen Testing Methodology Revisited

- Introduction to the methodology
- The Plan!!
- Vulnerability Identification
- Client-side attacks with and without PowerShell

Lesson 4: Information Gathering and Enumeration

- What can a domain user see?
- Domain Enumeration
- Trust and Privileges Mapping
- After the client exploit

Lesson 5: Privilege Escalation

- Local Privilege Escalation
- Credential Replay Attacks
- Domain Privilege Escalation
- Dumping System and Domain Secrets
- PowerShell with Human Interface Devices

Lesson 6: Lateral Movements and Abusing Trust

- Kerberos attacks (Golden, Silver Tickets and more)
- Delegation Issues
- Attacks across Domain Trusts
- Abusing Forest Trusts
- Abusing SQL Server Trusts
- Pivoting to other machines

Lesson 7: Persistence and Bypassing Defenses

- Abusing Active Directory ACLs
- Maintaining Persistence
- Bypassing Defenses
- Attacking Azure Active Directory

C)PSH: Certified PowerShell Hacker

Course ID #: 7000-790-ZZ-Z
Hours: 28

Lesson 8: Defending Against PowerShell Attacks

- Defending an Active Directory Infrastructure
- Detecting Attacks
- Logging
- Transcripts
- Using Certificates
- Using Bastion Hosts
- Using AppLocker

Labs:

Lab 1 – PowerShell Basics
Lab 2 – Active directory Navigation
Lab 3 – Metasploit Attack
Lab 4 – PowerShell Enumeration
Lab 5 – Guessing Passwords
Lab 6 – AD Golden Ticket
Lab 7 – Using PowerShell Empire for Everything

Accreditations:

Register for this class by visiting us at:
www.tcworkshop.com or calling us at 800-639-3535