Certified PowerShell Hacker

Description:

The Certified Powershell Hacker, C)PSH, course is an intense few days covering 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.

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!

Annual Salary Potential $110,000 AVG/year

Key Course Information

Live Class Duration: 4 Days
CEUs: 32
Language: English
Class Formats Available:

Instructor Led

Self-Study

Live Virtual Training

Suggested Prerequisites:

- Mile2 C)PEH and C)PTE or equivalent knowledge

- Understanding of pen testing

- General Understanding of active directory

- General understanding of scripting and programing

Modules/Lessons

Module 1 - Introduction to PowerShell

Module 2 - Indroduction to Active Directory and Kerberos

Module 3 - Pen Testing Revisited for the Powershell Hacker

Module 4 - Information Gathering and Enumeration

Module 5 - Privilege Escalation

Module 6 - Lateral Movements and Abusing Trust

Module 7 - Persistence and Bypassing Defenses

Module 8 - Defending Against PowerShell Attacks

Hands-On 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

Upon Completion

Upon completion, the Certified PowerShell Hacker, C)PSH candidate will be able to competently take the C)PSH exam and protect a powershell system from attack.

Who Should Attend

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

Accreditations

Exam Information

The Certified Powershell Hacker exam is taken online through Mile2's Learning Management System and is accessible on you Mile2.com account. The exam will take approximately 2 hours and consist of 100 multiple choice questions.

A minimum grade of 70% is required for certification.

Re-Certification Requirements

All Mile2 certifications will be awarded a 3-year expiration date.

There are two requirements to maintain Mile2 certification:

1) Pass the most current version of the exam for your respective existing certification
2) Earn and submit 20 CEUs per year in your Mile2 account.

Course FAQ's

Question: Do I have to purchase a course to buy a certification exam?

Answer: No

Question: Do all Mile2 courses map to a role-based career path?

Answer: Yes. You can find the career path and other courses associated with it at www.mile2.com.

Question: Are all courses available as self-study courses?

Answer: Yes. There is however 1 exception. The Red Team vs Blue Team course is only available as a live class.

Question: Are Mile2 courses transferable/shareable?

Answer: No. The course materials, videos, and exams are not meant to be shared or transferred.

Course and Certification Learning Options

Detailed Outline:

Course Introduction

Module 1 Introduction to PowerShell

a. Different Tool Options
b. Installing everything needed
c. Language Basics
d. Using the Windows API and WMI
e. Interacting with the Registry
f. Managing Objects and COM Objects

Module 2 – Introduction to Active Directory and Kerberos

a. Overview of Kerberos
b. The three-headed monster
c. Key Distribution Center
d. Kerberos in Detail
e. Why we care about Kerberos as a Hacker
f. Overview of Active Directory
g. Understanding AD concepts
h. AD Objects and Attributes

Module 3 – Pen Testing Methodology Revisited

a. Introduction to the methodology
b. The Plan!!
c. Vulnerability Identification
d. Client-side attacks with and without PowerShell

Module 4 – Information Gathering and Enumeration

a. What can a domain user see?
b. Domain Enumeration
c. Trust and Privileges Mapping
d. After the client exploit

Module 5 – Privilege Escalation

a. Local Privilege Escalation
b. Credential Replay Attacks
c. Domain Privilege Escalation
d. Dumping System and Domain Secrets
e. PowerShell with Human Interface Devices

Module 6 – Lateral Movements and Abusing Trust

1. Kerberos attacks (Golden, Silver Tickets and more)
2. Delegation Issues
3. Attacks across Domain Trusts
4. Abusing Forest Trusts
5. Abusing SQL Server Trusts
6. Pivoting to other machines

Module 7 – Persistence and Bypassing Defenses

a. Abusing Active Directory ACLs
b. Maintaining Persistence
c. Bypassing Defenses
d. Attacking Azure Active Directory

Module 8 – Defending Against PowerShell Attacks

a. Defending an Active Directory Infrastructure
b. Detecting Attacks
c. Logging
d. Transcripts
e. Using Certificates
f. Using Bastion Hosts
g. Using AppLocker

Detailed Labs Outline:

Lab 1 – PowerShell Basics

a. Understanding the Lab Setup
b. PowerShell or Powershell ISE
c. Leveraging Microsoft's Management Components
d.

Lab 2 – Active directory Navigation

Lab 3 – Metasploit Attack

Lab 4 – PowerShell Enumeration

a. Basic Enumeration from a Windows System
b. Basic Enumeration from Kali