Training: Mile2
C)PSH - Certified PowerShell Hacker

TRAINING GOALS:

This **C)PSH - Certified PowerShell Hacker** course is an intense few days covering the keys to hacking with PowerShell. We know that 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, which only makes sense. Did youknow that a large percentage of hacks over the last year included PowerShell based attacks? Well they did, which is why we spend 4days 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! Here are just a few things you will take away from this course:

- Detailed Lab Manual
- VMs for performing labs on your own
- New ideas on testing your own AD infrastructure
- Attacks you can use immediately
- How to secure against PowerShell attacks

Upon Completion:

Upon completion, the Certified PowerShell Hacker candidate will be able to competently take the CPSH exam.

Who Should Attend:

- Penetration Testers
- Microsoft Administrators
- Security Administrators
- Active Directory Administrators
- Anyone looking to learn more about security

Mile2® is:

- ACCREDITED by the NSA CNSS 4011-4016

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- MAPPED to NIST / Homeland Security NICCS's Cyber Security Workforce Framework
- APPROVED on the FBI Cyber Security Certification Requirement list (Tier 1-3)

CONSPECT:

- 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
- 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
- Pen Testing Methodology Revisited
  - Introduction to the methodology
  - The Plan!!
  - Vulnerability Identification
  - Client-side attacks with and without PowerShell
- Information Gathering and Enumeration
  - What can a domain user see?
  - Domain Enumeration
  - Trust and Privileges Mapping
  - After the client exploit
- Privilege Escalation
  - Local Privilege Escalation
  - Credential Replay Attacks
  - Domain Privilege Escalation
  - Dumping System and Domain Secrets

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- PowerShell with Human Interface Devices
- 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
- Persistence and Bypassing Defenses
  - Abusing Active Directory ACLs
  - Maintaining Persistence
  - Bypassing Defenses
  - Attacking Azure Active Directory
- Defending Against PowerShell Attacks
  - Defending an Active Directory Infrastructure
  - Detecting Attacks
  - Logging
  - Transcripts
  - Using Certificates
  - Using Bastion Hosts
  - Using AppLocker

REQUIREMENTS:

- General Understanding of Pen Testing
- General Understanding of Active Directory
- General Understanding of scripting and programming

Difficulty level

CERTIFICATE:

The participants will obtain certificates signed by Mile2 (course completion).

This course will help prepare you for the Certified PowerShell Hacker exam, which is available through the on-line Mile2's Assessment and Certification System ("MACS"), and is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple choice questions.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

Each participant in an authorized training C)PSH - Certified PowerShell Hacker will receive a free CPSH exam voucher.

TRAINER:

Certified Mile2 Instructor.

ADDITIONAL INFORMATION:

We also recommend further training and certification:

- C)PTC - Penetration Testing Consultant
- C)IHE - Incident Handling Engineer

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007