Hacking and Securing Microsoft Environments Using PowerShell

Course 4118 – 24 Hours

Overview

In this 3 days training you will learn how Windows PowerShell can be used both to hack common Windows componenets (including passwords, Windows applications, Active Directory etc.), as well as to secure and protect your environment. You will take PowerShell to the next level, with tips, best practices & using some advanced & hardly documented techniques to get the most of your IT environment.

On Completion, Delegates will be able to

- Understand advanced concepts behind Windows PowerShell & how it works
- Understand and be able to Pen test your core windows enviroment
- Use PowerShell & .NET in the best way to secure your organization
- Leverage tips & best practices for deploying PowerShell properly and Securely across your organization

Who Should Attend

This course is intended for IT Professionals and Security professionals who are somewhat experienced with Windows PowerShell, or completed the PowerShell courses (10961 / 50414 etc.), or have equivalent scripting skills (Python, Bash etc.).

This course is not intended to be a scripting or programming course, and includes only a quick coverage of core PowerShell topics. It focuses on using PowerShell for hacking and securing. Students are expected to have some scripting or programming experience, and are expected to have some prior Windows PowerShell experience.

Prerequisites

Before attending this course, students must have:

- Previous Windows Server and Windows Client management knowledge and hands on experience.
- Experience Installing and Configuring Windows Server into existing enterprise environments, or as standalone installations.
- Knowledge and experience of Windows PowerShell.

Course Contents

Module 1: Windows PowerShell - Architecture & Considerations

- Understand & demonstarte the concepts behind Windows PowerShell
- Understand how Powershell works exactly behind the scenes
- The connection between CMD, Powershell cmdlets, WMI, COM and .NET.
- Review core alternatives to get things done in PowerShell, and their Pros and Cons
- PowerShell Security events

Module 2: Running Scripts – Black and White hat approach

- Understand Execution policies and enabling/disabling script execution
- PKI concepts relevant to Code signing with PowerShell
- Sign & seal Powershell scripts
- How to deploy signed scripts in the enterprise – full life cycle
- How to bypass script execution -> black hat
- Mitigating attempts to bypass execution policies

Module 3: Secure Remoting

- Remoting - all the considerations - Performance and Architecture factors
- Controlling who can do what - custom security with session configurations
- Just Enough Administration (JEA) vs. PSSession configurations
- Remoting Kerberos Double hop – the options and the solutions
- Auditing PowerShell sessions – full logging of PowerShell consoles locally and remote

Module 4: Working with Win APIs

- How to run win APIs and system functions directly from PowerShell
- The use of Win APIs and system components in exploits through PowerShell

Module 5: Working with Base64-encoded strings

- How to use encoded strings to execute code
- Leveraging exploits using base64 encoded strings

Module 6: Active Directory Security

- Understand Active Directory security concepts & architecture
- Hacking your AD environment
- Securing your AD environment with PowerShell commands

Module 7: Secure strings

- Understand how secure strings work in Powershell
- Exploiting secure-string and hashes
- Using Secure-String for Passwords, Connection strings etc

Module 8: Full attack cycle – from Remote Shell into Your Apps & data

- Demonstrating the cycle of hacking into an organization using PowerShell
  - Scanning
  - Penetration
  - Elevated privilege attempts
  - Accessing remote Shell
  - File download and execution
- How to inject PowerShell code into applications
- How to mitigate the different steps of the attack
- Demonstrate tools: Empire, Powersploit, Powerpreter, bloodhound, p0wnedShell etc.