PowerShell for Penetration Testers

Nikhil Mittal (@nikhil_mitt)

http://www.labofapenetrationtester.com/

Certifications: http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

About Me

- Speaker/Trainer
  - Defcon, Blackhat Europe/US/AbuDhabi, Troopers, DeepSec, PHDays, EuSecWest, HackFest, RSA China and more.
- Creator of Kautilya and Nishang
  https://github.com/samratashok/
  - Nishang helps in using PowerShell for Penetration Testing .
  - Kautilya is a toolkit for using Human Interface Devices in Penetration Tests
- Freelancer/Hacker/Pen-tester
- Interested in and research on new attack vectors and methodologies to pwn systems.

Course Contents

- Introduction to PowerShell
- Basics of PowerShell
- Scripting
- Advanced Scripting Concepts
- Modules
- Jobs

Course Contents

- PowerShell with .Net
- Using Windows API with PowerShell
- PowerShell and WMI
- Working with COM objects
- Interacting with the Registry

Course Contents

- Recon and Scanning
- Exploitation
  - Brute Forcing
  - Client Side Attacks
  - Using existing exploitation techniques
  - Porting exploits to PowerShell – When and how
  - Human Interface Device

Course Contents

- PowerShell and Metasploit
  - Running PowerShell scripts
  - Using PowerShell in Metasploit exploits
- Post Exploitation
  - Information Gathering and Exfiltration
  - Backdoors
  - Privilege Escalation
  - Getting system secrets

Course Contents

- Post Exploitation
  - Passing the hashes/credentials
  - PowerShell Remoting
  - WMI and WSMAN for remote command execution
  - Web Shells
  - Achieving Persistence
- Using PowerShell with other security tools

- Defense against PowerShell attacks