Powershell Security Best Practices

Modality: Self-Paced Learning

Duration: 12 Hours

About this course:

This course will show understudies how to safely achieve authoritative undertakings utilizing Windows PowerShell 5.x. Understudies will learn PowerShell operational security, review the fundamentals of PowerShell, and configuration management.

Understudies will also figure out how to utilize administration devices, for example, Just Enough Administration (JEA) and Desired State Configuration (DSC) to secure and configure servers. Also, this course takes a gander at new exploits, new threats, the ever-changing attack surface, and the way to remediate them.

Course Objective:

- Comprehend the PowerShell architecture.
- Windows PowerShell Architecture
- Deploy the operational security of PowerShell
- PowerShell versions and editions
- Running Windows PowerShell
- Handling the execution of Local Script with the Policy of Windows PowerShell Execution.
- Running the capabilities of Remote Execution Windows PowerShell
- Constrained Endpoints
- Analyze Logging and Auditing of PowerShell
- Anti-Malware Scan Interface (AMSI)
- PowerShell-based attacks for Windows
- PowerShell-based security tools for Windows
- Summary of the technologies of Windows PowerShell-based security
- Increase the management of servers with Just Enough Administration and Desired State Configuration.
- Debug and Analyze scripts
- PowerShell based exploits Comprehension and their remediation.

Audience:

Programmers

Windows Server administrator

Prerequisite:

- Windows networking Experience
- Windows Server administration Experience

- Windows PowerShell usage Experience

Course Outline:

Windows PowerShell Fundamentals

- Windows PowerShell Architecture
- Powershell editions and versions
- Running Windows PowerShell

PowerShell Operational Security

- Managing Local Script Execution with Windows PowerShell Execution Policy
- Managing Remote Execution Capabilities of Windows PowerShell
- Constrained Endpoints
- Language Mode
- Anti-Malware Scan Interface (AMSI)

Implementing PowerShell-based Security

- Windows PowerShell DSC
- Just Enough Administration (JEA)
- Windows PowerShell Auditing and Logging

Windows PowerShell-based Exploits and their Mitigation

- Windows PowerShell-based attacks
- Windows PowerShell-based security tools
- Summary of Windows PowerShell-based security-related technologies

Launch Lab

- Download the student manual
- Lab Launch

Final Exam

- Final Exam**?**