TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

PowerShell - Keeping the SOCs on their Toes - Taking the Best of PowerShell Blue & Red for Your Enterprise

Date of the online training: **October 25-26, 2021**

Overview

PowerShell is a Windows administration tool and an open-source cross-platform scripting environment included out of the box in Windows operating system. Very powerful and easy to learn, it can interact with almost anything from a raspberry-pi to a data center, and its remoting capabilities make it ideal to manage windows environments at scale. With great powers come great dangers, and since its early day's attackers have known how to use PowerShell to their advantage... But time has passed, and it is nowadays one of the most securable scripting languages there is. In this 2-day workshop, we will review the basics of PowerShell scripting and tool building, to then explore it's various offensive and defensive capabilities with a hands-on approach to facilitate and strengthen the theoretical knowledge. Lab access will be provided for practice and exercises associated with each module.

And don't forget to bring a laptop with administrative privileges, this is a hands-on training and you have to install tools, if you would like to participate in the exercises.

Day 1

PowerShell Basics

- Get-Help

ERNW Enno Rey Netzwerke GmbH
Carl-Bosch-Str. 4
69115 Heidelberg
info@ernw.de

Tel. +49 – 6221 – 48 03 90
Fax +49 – 6221 – 41 90 08
BIC: GENODE61HD3
IBAN: DE43 6729 0100 0059 7891 04

Managing Directors
Florian Grunow
Michael Schaefer
VAT-ID: DE 813 376 919

- PowerShell Survival Kit
- PowerShell Scripting 101

PowerShell for Active Directory

- Active Directory Module
- PowerShell & ADSI
- PowerShell & LDAP

PowerShell Remoting

- Invoke-Command & PSSessions
- PowerShell & WMI

PowerShell Tool Making

- Scripts vs Functions
- Basic/Advanced/Compiled Cmdlets

PowerShell without PowerShell

- the "System.Management.Automation" dll

Day 2

Offensive PowerShell

- Download Craddles & obfuscation
- Reflection
- Win32Api calls
- AMSI Bypass
- Overview Red Team Tools

Defensive PowerShell

- Built-in Security features
- Working with Logs
- JEA
- Hunting Empire
- Overview Blue Team Tools

Detection of PowerShell Activities

About the Trainer

Jean-Damien Douillard is a Windows Security consultant at ERNW with interest in scripting and automation. Fan of PowerShell and Bloodhound. Creator of CypherDog.

Booking

Recommended online booking of trainings through:

https://tickets.ernw.de/troopers/tr21training/

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German. +49 6221 480390 or info@troopers.de

Booking is also possible offline through your trusted partner:

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany

+49 6022 508200 / info@hmtrainingsolutions.com

+49 6022 5089999 / www.hmtrainingsolutions.com