TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Hacking Enterprises - 2021 Edition

Date of the online training: **October 18-20, 2021**

Overview

This is an immersive hands-on course aimed at a technical audience. Over the 3 days we will fully compromise a simulated enterprise covering a multitude of TTP's. The training is based around modern operating systems, using modern techniques and emphasising the exploitation of configuration weaknesses rather than throwing traditional exploits. This means logical thinking and creativity will definitely be put to the test.

This is an immersive hands-on course aimed at a technical audience. Over the 3 days we will fully compromise a simulated enterprise covering a multitude of TTP's. The training is based around modern operating systems, using modern techniques and emphasizing the exploitation of configuration weaknesses rather than throwing traditional exploits. This means logical thinking and creativity will definitely be put to the test.

Students will access a cloud-based LAB configured with multiple networks, some easily accessible, others not so. Course material and exercise content has been designed to reflect real-world challenges and students will perform numerous hands-on exercises including executing exploitative phishing campaigns against our simulated users to gain access to new networks, in turn bringing new challenges including IPv6 exploitation, subverting AMSI and AWL, passphrase cracking, pivoting, lateral movement, OOB persistence mechanisms and much more!

We also like to do things with a difference. You'll be provided access to an in LAB Elastic instance, where logs from all targets get pushed and processed. This allows you, whether an attacker or defender, to understand the types of artefacts your attacks leave and how you might catch or be caught in the real world.

Also included:

We realize that training courses are limited for time and therefore students are also provided with the following:

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

- Completion certificate
- 14-day extended LAB access after the course finishes
- 14-day access to a CTF platform with subnets/hosts not seen during training!
- Discord support channel access where our security consultants are available

Agenda:

Day 1

- MITRE ATT&CK framework
- Overview on using the in-LAB ELK stack
- Offensive OSINT
- Enumerating and exploiting IPv6 targets
- Pivoting, routing, tunnelling and SOCKS proxies
- Application enumeration and exploitation via pivots
- Linux living off the land and post exploitation
- Kubernetes and container security

Day 2

- Exploitative phishing against our simulated enterprise users
- Living off the land tricks and techniques in Windows
- P@ssw0rd and p@ssphras3 cracking
- Windows exploitation and privilege escalation techniques
- Windows Defender/AMSI and UAC bypasses
- Situational awareness and domain reconnaissance
- RDP hijacking

Day 3

- Bypassing AWL (AppLocker, PowerShell CLM and Group Policy)
- Extracting LAPS secrets
- Lateral movement for domain trust exploitation

- WMI Event Subscriptions for persistence
- Out of Band (OOB) data exfiltration
- Domain Fronting and C2

Who should attend this training?

This training is suited to a variety of students, including:

- Penetration testers / Red Team operators
- SOC analysts
- Security professionals
- IT Support, administrative and network personnel

Prerequisites

- A firm familiarity of Windows and Linux command line syntax
- Understanding of networking concepts
- Previous pentesting and/or SOC experience is advantageous, but not required
- Students will need to bring a laptop to which they have administrative/root access, running either Windows, Linux or Mac operating systems
- Students will need to have access to VNC, SSH and OpenVPN clients on their laptop (these can be installed at the start of the training)

About the Trainers

Will Hunt co-founded In.security in 2018. Will's been in infosec for over a decade and has helped secure many organisations through technical security services and training. Will's delivered hacking courses globally at several conferences including Black Hat and has spoken at various conferences and events. Will also assists the UK government in various technical, educational and advisory capacities. Before Will was a security consultant he was an experienced digital forensics consultant and trainer.

Owen Shearing (@rebootuser) is a co-founder of In.security, a specialist cyber security consultancy offering technical and training services based in the UK. He has a strong

background in networking and IT infrastructure, with well over a decade of experience in technical security roles. Owen has provided technical training to a variety of audiences at bespoke events as well as Black Hat, Wild West Hackin' Fest, NolaCon, 44CON and BruCON. He keeps projects at https://github.com/rebootuser.

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@hm-ts.de

+49 6022 5089999 / https://www.hm-ts.de