TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

BloodHound – Visualizing and Evaluating Critical Attack Paths in Active Directory Environments

Date of the online training: **March 22-23, 2021**

Overview

This workshop is designed to enable you to identify critical object relationships within your Active Directory enterprise environment. Active Directory is at the heart of practically all organizations and gaining control of Active Directory asset is often what an attacker is looking for after corporate post-exploitation scenarios. BloodHound is a visualization and evaluation tool designed to graph Active Directory attack paths and visualize Active Directory in the way an attacker would see it. Thinking in graphs allow defenders to better understand the complexity of object relationships, identify weak spots (vulnerabilities) to be mitigated, and improve their overall security posture of an Active Directory environment.

Think of the following questions:

- Are you responsible for administrating or securing a complex Active Directory environment?
- Do you want to know how many tier 2 users have a path to your tier 0 assets?
- Do you want to know if your Exchange ACLs open an attack path to your domain controllers and how these paths look like?

If the answer to these questions is “yes”, then this workshop has everything you need to use BloodHound efficiently in your environment. The workshop is designed to be hands-on with many practical lessons and covers everything from understanding / performing a basic installation of BloodHound, building basic queries, visualizing object relationships / potential attack paths to more advanced topics like using custom add-ons or automating the whole process of using BloodHound (data collection, ingestion, first analysis etc.).

BloodHound has been successfully used in many complex Active Directory environments to visualize critical attack paths that could lead to a full Active Directory compromise. Our trainer will share his experience, lessons learned, tips & tricks and pitfalls from using BloodHound in complex enterprise environments to efficiently identify critical relationships and derive appropriate mitigating controls.

Who should attend this training?

You should attend this training if you would like to:

- Understand Active Directory from an attacker POV
- Identify critical object relationships in your environment
- Think in Graphs
- Learn BloodHound UI functionalities
- Learn Cypher query language building blocks
- Learn how to extract metrics out of BloodHound data
- Build your own custom Cypher queries
- Extend tool capabilities via REST API

Prerequisites

- Basic Active Directory knowledge & understanding

Requirements

- A PC/laptop/tablet with a stable internet connection,
- An up-to-date browser is sufficient (current Microsoft Edge, Google Chrome or Firefox).

Access to the training lab will also take place via your browser. Exercises can be implemented without additional software. We provide the training material electronically before the start of the course.

About the Trainers

Walter Legowski is 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://troopers.de/tickets/

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