HMTS
HM Training Solutions

INDEPENDENT • INNOVATIVE
INTERNATIONAL

ONLINE WORKSHOP

M 66

A two day course in English ONLINE

BloodHound – Visualizing and Evaluating Critical Attack Paths in Active Directory Environments (upon request in French – handout in English)

Your trainer is Jean-Damien Douillard
Requirements: Basic Active Directory knowledge & understanding

A workshop particpation is possible from any PC/lap top/tablet with a stable internet connection. You don´t need additional software. 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. The workshop will of course be transmitted live from the ERNW studio. The workshop material as well as possible demos and of course the trainer are always visible and will be shown depending on the requirements or will be emphasized. We will provide the training material electronically before the start of the course. The trainer will answer questions live. The microfone and/or camera are optional. You can also ask questions via chat.

Description

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.

24. – 25. März 2021

Various institutions will acknowledge this workshop as a re-certification measure.

HM Training Solutions, Falkenstraße 6 · D-63820 Elsenfeld
Telefon +49 (0) 6022 508 200,Fax +49 (0) 6022 508 9999
E-Mail: info@hm-ts.de – Internet: https://www.hm-ts.de

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

M 66

A two day course in English

Course Agenda

Introduction
- ❒ What is BloodHound?
- ❒ Graph DB: Concept & Terminology

BloodHound Basics
- ❒ Installation / Requirements
- ❒ Nodes & Edge Types
- ❒ Edge Abuse Information
  - o Default/ACL/Container/Special
- ❒ Data Collection & Ingestion
  - o Technical Information
  - o Practical Steps
- ❒ User Interface
  - o Components & Features
  - o Viewing Nodes, Paths and Relationships

Cypher Basics (UI)
- ❒ What is Cypher?
- ❒ Node Queries
- ❒ Path Queries

Advanced BloodHound Features
- ❒ Build-In Queries
- ❒ Attack Path Reduction Methodology
- ❒ Tips & Tricks

Advanced Cypher Features
- ❒ Adding/Updating/Deleting data
- ❒ Calculating Metrics
- ❒ Debugging Queries

Extending BloodHound
- ❒ REST API Basics
- ❒ CypherDog
- ❒ WatchDog
- ❒ Automating BloodHound
  - o Data Collection
  - o Ingestion
  - o First Analysis

Using BloodHound in Complex Active Directory Environments
- ❒ Lessons Learned
- ❒ Pitfalls
- ❒ Tips & Tricks

You should attend if you want 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

Target Groups
- ❒ Red/Blue Teams
- ❒ Active Directory Security Consultants
- ❒ Active Directory Security Administrators
- ❒ Active Directory Operations Team

HM TRAINING SOLUTIONS ON-SITE SERVICE

All HM Training Solutions Seminars are available as On-Site presentations, tailored to meet the specific requirements of your organisation. For details please telephone +49 (0) 6022 508 200 (international).

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

M 66

A two day course in English

Why you should attend

- 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

Target Groups

- Red/Blue Teams
- Active Directory Security Consultants
- Active Directory Security Administrators
- Active Directory Operations Team

Biography Jean-Damien Douillard

Jean-Damien Douillard began his journey into Windows / Active Directory security back in 2010 at a fortune 500 company. Since 2018 he is part of the Microsoft Security Team at ERNW GmbH where he focuses on attack path visualization via BloodHound and PowerShell scripting. He presented on various conferences (e.g. PSConf) all around the globe where he shares his insights and knowledge. He is one of the leading experts in the industry for BloodHound and the author of the well-known Dog Whisperer Handbook.

REGISTRATION DETAILS

Three Ways to Register

By Post: Please complete and return this form to HM Training Solutions.
By Fax: Please fax this registration form to: +49 6022 508 9999.
By e-Mail: **Info@hm-ts.de**
Per Webseite: https://www.hm-ts.de/

Registration Fees

€ 1,990 + VAT 19%

Joining Instructions

Your booking will be confirmed by e-mail containing full event details.

Change of Terms

It may be necessary for reasons beyond our control to alter the venue, timetable or content of this seminar or to appoint another speaker alternatively or to cancel the event. We accept no liability for any other cost.

Cancellations

Should you need to cancel your booking please confirm in writing either by email (info@hm-ts.de), fax (+49 6022 508 9999) or post. No refunds will be considered for cancellations occurring withing six weeks of the start of the event. However, we are happy to accept substitutions at any time; prior notice is appreciated

On-Site Presentations

All HM Training Solutions seminars are available as on-site presentations tailored to meet the specific requirements of your organisation. For more information please call +49 (60 22) 508200.

The number of delegates is limited. Therefore please immediately return this booking form

REGISTRATION FORM

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

❒ **24.-25. März 2021, ONLINE**

❒ Please reserve _____ places at a cost of **1,990 €** + VAT 19% per participant

Mr/Mrs/Miss/Other First Name Last Name

_____

Job Title _____

Company _____

Address _____

_____

_____

Postcode _____

Country _____

Telephone _____

Mobile number _____

E-Mail _____

Signature _____

BOOKING REFERENCE: M66

You will receive the course documentation as pdf before the beginning of the course.

Payment

❒ Cheque enclosed for € _____

❒ Please invoice my company _____

Invoice address (if different) _____

_____

_____

Purchase order no. _____

Additional Registrations

1. Mr/Mrs/Miss/Other First Name Last Name

_____

Job Title _____

2. Mr/Mrs/Miss/Other First Name Last Name

_____

Job Title _____

3. Mr/Mrs/Miss/Other First Name Last Name

_____

Job Title _____