Details of Training

‘Windows and Active Directory security in-depth’

OUTFLANK

clear advice with a hacker mindset

Overview

This two-day knowledge-packed training is a deep-dive into the inner workings and security of Windows and Active Directory. This training will help you to understand and implement security controls that aid in stopping or detecting modern attacks attack techniques used by red teams and targeted attackers.

Combining a large and private hands-on lab and having instructors with over 12+ year's experience in breaking into Windows networks, you will leave this training excited and prepared for the next steps in Windows and AD security.

Who should attend

The training is optimally suited for:

- **Defenders, Windows and Active Directory administrators** who want to strengthen their knowledge of Windows and Active Directory internals, security concepts and defensive measures.
- **Penetration testers and ethical hackers** wanting to provide better recommendations to their clients on defensive measures.
- **Security professionals** interested in expanding their knowledge of Windows and Active Directory related modern attack techniques, Red Teaming and defend against it.
- **Forensic professionals** who want to better understand the entire flow of an attacker and offensive tactics.
- **Technical auditors** wanting to increase their hands-on experience and technical skills.
- **Attendees of other Outflank trainings** who are looking for more in-depth knowledge on Windows and Active Directory security concepts as well as defensive measures.

Key learning objectives

The training is focussed on several key elements:

- Key theoretical concepts e.g. kill chain, course of action matrix, pyramid of pain, tiering security model, etc.
- Windows inner workings and key concepts that are often abused by attackers, or can help you in stopping or detecting attackers. Amongst others: How do processes work in detail? ACL and security descriptors, AMSI, Local Security Authority Subsystem Service, DCOM/WMI, relaying attacks.
- Active Directory inner workings and key concepts that are often abused by attackers, or can help you in stopping or detecting attackers. Amongst others: the inner workings of Kerberos and LDAP, attacks abusing the Kerberos protocol (i.e. golden ticket, silver ticket), domain trusts and attacks such as unconstrained delegation, resource-based delegation or Microsoft Exchange and common misconfigurations.
- Windows logging in detail, with amongst others topics such as WEF, Sysmon, centralised logging, ATT&CK and EDR features.
- Security of networking protocols, and the power of the built-in Windows firewall.
- Recent developments related to Azure Active Directory that could introduce new risks or help you addressing them.
- Relevant security models to enhance the security of Windows and Active Directory environments. Amongst others: privilege access workstations, the clean source principal and the Microsoft tiering model.

Approach

This training uses the same approach as other trainings by Outflank. This means:

- Interactive setting with multiple trainers, each bringing their dedicated area of expertise.
- A combination of theory and learning by doing.
- Large lab environments per student that represent real office networks.
- Students will learn about and perform both offensive and defensive steps in the lab; working with Cobalt Strike and with modern ways of log centralisation and security monitoring.
- Detailed labmanual that guides the students through each lab assignment, including extra assignments for more experienced students.
- Full set of training material to take home and restudy at a later moment.

Personal lab environment

During the training, participants have access to a personal lab environment that acts as a playground area. Having a personal lab is a key differentiator compared to many other labs. This environment is comparable to common enterprise networks as it contains Windows servers and desktops, an Active Directory domain, multiple services, user accounts and service accounts. Furthermore, commonly found insecurities are configured on purpose, as well as detective measures are in place, e.g. central monitoring environments using open source and commercial tools (e.g. IDS, Splunk/ELK stack). We have spent significant time making this lab as real as possible.

Hardware requirements for attendees

A laptop that has the ability to run a Remote Desktop Connection.

Pre-required knowledge for attendees

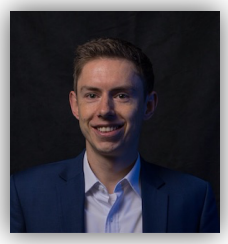
It helps if you already have detailed experience with Windows and Active Directory, commonly found in a systems engineering role. Yet, the training is setup in such a way that any participant with a technical IT background and a basic level of security knowledge can follow the topics; it welcomes both novices and veterans. There are extra lab assignments for students that want to go the extra mile.

About the trainers

The training is hosted by a selection of three of the trainers enlisted below. Working at the Dutch company Outflank, they focus on Red Teaming operations and advanced penetration tests. The training is created based on their 10+ years of experience with offensive operations and advising their clients on defending against targeted attackers. They each bring their own unique expertise to this training, ranging from SOC operations, custom malware and infrastructure security.

Stan Hegt

Jarno van de Moosdijk



Marc Smeets

Testimonials from past students

Below you can find a selection of quotes from previous attendees.

"The trainers really know what they are talking about, and also are very good in transferring their knowledge. Trainings by Outflank are one of the best trainings I've ever had"
Stefan Cox, systems engineer at Hogeschool Rotterdam.

As a consultant implementing security measures for clients, it was really valuable to hear what the experienced red-teamers believe is important in order to protect an AD environment. I can definitely use what I have learned from the course to improve my hardening deliveries.
Jonas Bülow Knudsen, Improsec A/S

Training with a full overview and content that matters to be able to prevent and react on ransomware and malware attacks like notPetaya. As an Identity Access Management consultant working mainly on the 'business' side to get "In Control" the focus was now on the 'technical' side with the security risks related to Windows and Active Directory/Azure AD. Highly recommend!
Jaap Hoekstra, IAM Consultant at Cloud Control Consultancy.

Excellent course and exceptional knowledgeable trainers. Having the opportunity to discuss different approaches to AD Security and Tiering with experts like the Outflank guys is greatly appreciated, and definitely something you don't get to experience daily.
Casper Schjøtt, Security Advisor at Improsec A/S

Marc, Stan and Jarno are professionals that know what they are talking about and this is reflected in the training. I left the training with lots of ideas and knowledge!
M. Buijs Technical Security Specialist at GR IJsselgemeenten.

Great training delivered in an understandable way. Especially the three-teacher setup is a great way to learn. Because of the specialisms in different areas, the trainers can provide extensive information. Roy Aerts, DevOps engineer