**Buy tickets**: https://romhack.io/buy-tickets/

ROMHACK TRAINING

# ADVANCED ACTIVE DIRECTORY EXPLOITATION

## by John Iatridis (SensePost)


### TRAINING DESCRIPTION

Mere vulnerability scanning has been rendered obsolete, in particular for more conscious and mature organizations. Penetration testing, red team and purple team engagements against Active Directory environments deployed on the premises require, among others, robust knowledge of the relationships between domain objects and of the Kerberos protocol, in order to meet their goals.

Although many tools have been made available which aid in the enumeration of domain environments and the discovery and abuse of misconfigurations thereof, they are rarely used efficiently. Rather than the tools themselves, this most often stems from the fundamental misconception and misinterpretation of those relationships and protocols in place. In consequence, contributing to further confusion and to the failure to attack and defend a domain environment appropriately. Standing on the shoulders of giants in the industry, the Advanced Active Directory Exploitation (AADE) course provides a meticulous and thorough examination of domain object relationships and of the quite complicated Kerberos protocol, the latter being scrutinized on a request and response level.

The end goal being to enable attackers and defenders into engaging with domain environments deployed on the premises with efficiency and precision. This is achieved by comprehensive theory in conjunction with a series of practical exercises within a unique to each student domain environment.

### TRAINING TOPICS

- > Windows authentication and access tokens
- > Relayed and coerced authentication
- > Domain object relationships abuse
- > Group Policy Objects abuse
- > Kerberos Protocol
- > Domain Compromise

Training page: https://romhack.io/advanced-active-directory-exploitation/
RomHack Training 2024: https://romhack.io/training/

- > Attacking Domain Trust Relationships
- > Active Directory Certificate services and abuse thereof
- > 20+ practicals, including bonus ones.

## TRAINING OUTCOMES

- > Domain objects and the relationships between them
- > The misunderstood Kerberos protocol and its delegation flavors
- > How to attack or defend a domain environment

## ABOUT THE TRAINER

SensePost, an elite ethical hacking team of Orange Cyberdefense have been training internationally since 2002. We pride ourselves on ensuring our content, our training environment and trainers are all epic in every way possible. The trainers you will meet are working penetration testers, responsible for numerous tools, talks and 0-day releases. This provides you with real experiences from the field along with actual practitioners who will be able to support you in a wide range of real-world security discussions. We have years of experience building environments and labs tailored for learning, after all education is at the core of SensePost and Orange Cyberdefense.

John Iatridis is an intensely pedantic security analyst as SensePost, with academic background in computer engineering and informatics, and various information security certificates, although he would not list those right next to his LinkedIn profile name. He has trained internationally at conferences like Black Hat and DefCon.

## WHAT TO BRING

- > A Laptop with a modern browser (Chrome, Firefox) - all labs will be accessed via a virtual environment via the browser

## WHAT WILL BE PROVIDED

- > Access to a training portal which includes all course materials.
  - o This will be accessible after the training as well.
- > Access to online lab environment for the duration of the training

## PARTICIPANT SKILL SET

Extensive hacking experience is not required for this course, albeit a solid technical grounding is an absolute must. We recommend familiarity with the Windows operating system and its command line at a minimum.

## CLASS SYLLABUS

### MODULE 1: **Windows authentication and access tokens**

- > How does Windows authentication work in a domain environment?
- > What are the differences between local and domain authentication?
- > Access tokens; what are they and how can they be compromised?

### MODULE 2: **Relayed and coerced authentication**

- > What are network spoofing and relay attacks?

- > What is coerced authentication and cross-protocol relaying?

**MODULE 3: Domain object relationships**

- > What constitutes a domain object?
- > What are the relationships between them?
- > What are the access controls imposed on them?
- > What is inheritance and how does it work?

**MODULE 4: Group Policy Objects**

- > What are Group Policy Objects?
- > How can they be abused?
- > Can they facilitate lateral movement?

**MODULE 5: Kerberos Protocol**

- > How does Kerberos work on a request and response level?
- > What are the roasting attacks against the Kerberos protocol?
- > What is the double-hop problem and how does delegation solve it?
- > What is domain user impersonation and how does it aid in delegation?
- > How does delegation work on a request and response level?
- > How can each delegation flavor be configured or misconfigured?
- > How can each delegation flavor be abused?

**MODULE 6: Domain Compromise**

- > What are some significant persistence avenues?
- > What are Kerberos Silver and Golden Tickets?
- > What is credential dumping?

**MODULE 7: Domain Trust Relationships**

- > What are trust relationships between domains?
- > How can they be abused?

**MODULE 8: Bonus Content**

- > Active Directory Certificate Services
  - What is the Active Directory Certificate Service?
  - How do domain objects enroll certificates?
  - How can they be misconfigured and abused?