Introduction

To the course

What is this course?

- **Understand** the concept, components and architecture of **modern day Active Directory** environment.

- Understand, **practice** and **leverage** modern day **AD** attacks and threats **offensively**

- Learn to **exploit** a **complete AD** attack **chain** from initial low privilege access to **becoming** a domain **administrator**

- Learn to **create your own** Active Directory Lab Environment and practice with variety of **industry standard** tools

- **Ace** the **OSCP** exam and much more!

Why is this course?

- **95%** of **fortune 500** companies use Active Directory

- There is a **large knowledge gap** between security professionals and SysAdmins for AD security

- Windows environment for pentesting is **quite new and complex** with **incomplete** and **scattered** resources

- AD concepts are **quite overwhelming** and require **different** set of **tools**

- A **lack of documentation** due to non open sourceness

Who is this course for?

- Security Enthusiasts **familiar** with pentesting
- Security Professionals who work in **network** and **infrastructure** security
- Students wanting to get jobs in **Red Teaming**
- Windows **administrators** who want to learn AD Security

Prerequisites

- **Basic Knowledge of Windows Pentesting**

- **Strong CS background**

- **Strong Networking knowledge**

- **Basic Red Teaming experience**

Content

- **Active Directory Basics**
- **Active Directory Lab Setup**
- **Active Directory Enumeration**
- **Active Directory Authentication**
- **Active Directory Lateral Movement and Pivoting**
- **Active Directory Persistence**
- **Assembling the Pieces**

What else you get?

- **Presentation Slides as PDFs**
- **Additional Study Content**
- **External references to learn more**
- **LIVE classes every month**
- **Lifetime access to course material**
- **Community Support (1000+)**