Review of Attacking and Defending Active Directory

medium.com/@riccardo.ancarani94/review-of-attacking-and-defending-active-directory-9ebcc26ae4d3

Riccardo Ancarani 4 марта 2019 г.

Riccardo Ancarani

Original blog post:

Intro Today we're going to make a quick review of the course I recently purchased: Attacking and Defending Active…

blog.riccardoancarani.it

Today we’re going to make a quick review of the course I recently purchased: Attacking and Defending Active Directory offered by PentesterAcademy. You can find the course here: https://www.pentesteracademy.com/activedirectorylab

The course’s aim is to give the student a basic working knowledge of Active Directory and to present the main security issues related to AD deployments in modern environments such as:

- Enumeration or how much information you can extract from an AD with regular user privileges (you'll be surprised!)
- Privilege escalation or how to get from zero to hero (Domain Admin and beyond)
- The main concepts for persistence, which is particularly tricky within Active Directory because of its enormous amount of features (seems a little bit vague, it will make sense).
- How to actually implement defenses and in general how to detect the attacks that you previously carried on

My Opinion

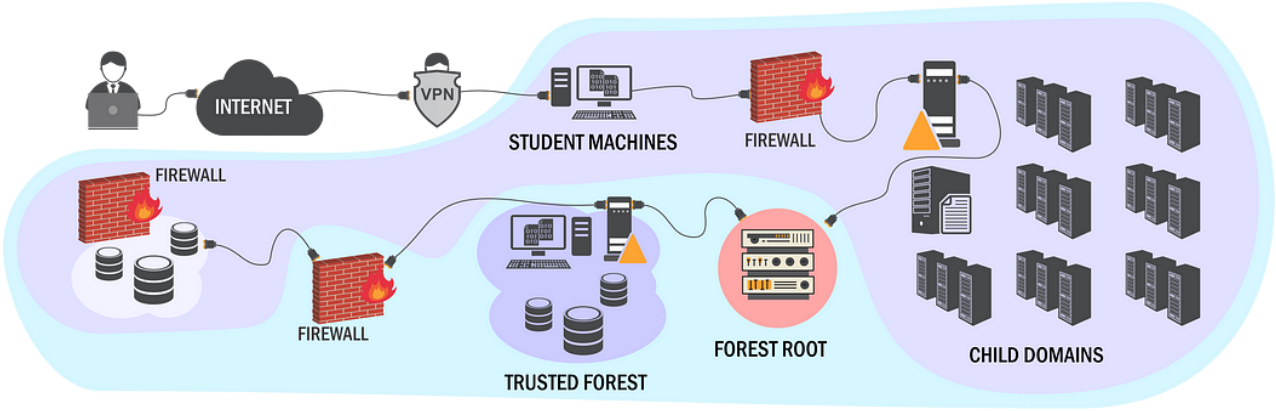
To be honest, I bought this course with very low expectations considering other reviews and opinions I got from other people about PentesterAcademy in general, but I still wanted to give it a shot (and it was discounted when I bought it :P)

After a few hours I was really impressed by the quality of the course, the explanations were clear and the examples consistent. Having already some knowledge on Active Directory exploitation (see my other review on PTX) gave me the opportunity to actually judge the completeness of the course.

One of the best things about this course was his white-box approach, in fact you'll see the instructor (and you can repeat it yourself) actually showing you how a misconfiguration looks like from a sysadmin perspective.

Let's make an example, a common topic while explaining AD oriented exploitation is Access Control List (ACL) abuses for both persistence and escalation. If you quickly google "how to abuse ACL active directory" or something like that you'll find plenty of powershell scripts to do the most exotic techniques, but did you ever had the chance of legitimately edit an ACL within AD? Don't take this for granted, a lot of other courses will treat vulnerabilities and misconfiguration as "black boxes" without digging deeper on how and why the issues are present. Having the knowledge on how things works is the first, and most of the time forgotten, step to know how to break them.

Alongside the slides and the video lessons you'll receive the access for a virtual lab which contains a good number of machines, servers, users and so on. The objective of the labs are to give the student the ability to safely and effortlessly practice the techniques explained in the lessons without having to manually deploy an AD environment (which btw is a good learning experience, totally recommend it).



The labs are not CTF-like, at the end of teach topic you'll have to complete a series of tasks (called Learning Objectives) which most of the time will consist in mimicking what the instructor just did (with some brain work, obviously)
It's not intended to be an hard-core challenge, we're here to learn at our own peace with enough "space" to try variations, different tools and technique and in general follow your curiosity.

I find this approach very beneficial when learning a new subject, that why I'm particularly enjoying this course. I think that it fits perfectly the needs of someone who's just starting (and for some more advanced folks too, don't get me wrong, especially if AD assessments are not your bread and butter)

For me personally, I don't know if the lab by its own has a lot of value, I could easily reproduce it on my laptop or cloud provider. But sometimes it's just easier to start an RDP connection and try your stuff without having the hassle of setting everything up.

To sum up, it's a very good course with an incredible amount of material and details. The only problem is that now I have to integrate my new notes in my personal wiki!

Considering the price at the moment of writing (149$ for the first 50 people and 30 days lab) I'd really consider this as a good option and a valid complement to every other course or training you're already doing.

PentesterAcademy is quickly gaining popularity and notoriety in the world of training providers, I think that one of their biggest strengths is the good amount of new technologies they're covering in their courses. But since this is the only course I own from them, I don't want to be off balance and say that 100% of their content is gold (because I don't know ¯_(ツ)_/¯) .

Originally published at on March 4, 2019.