Internship EY

Plan Of Action

Bachelor in Electronics-ICT
Cloud & Cyber Security

Mickey De Baets

Academic year 2020-2021

Campus Geel, Kleinhoefstraat 4, 2440 Geel

TABLE OF CONTENTS

About EY

For my internship I wanted a big company with a high quality specialty in cybersecurity. EY offers me exactly that. EY is an international company that offers Assurance, Tax, Consulting and Strategy services to their clients. Their headquarters is located in London. They have over 300.000 employees in over 150 countries. I was lucky to score a place in their office in Diegem.

During my internship I am part of the cybersecurity consulting team. Cybersecurity at EY is further divided in FSO (Financial Services Office) and Industries. The FSO team's clients exist out of banks and financial institutions while the Industries team, the team I'm working with, deals with all the other industries.

The cybersecurity consulting at EY is even further divided into four kinds of services:

- Cybersecurity Strategy, Risk, Compliance and Resilience
- Data Protection & Privacy
- Identity & Access Management
- Next Generation Security Operations & Response

Of these four services my project and the people in my team lean more towards the last service. This is also the service that deals with the very technical assessments like pentesting.

1 PROJECT

The title of my project is “Design and deploy a cloud-based hacker toolbox”. When we think about this the following technologies come to mind: Infrastructure as Code, cloud, automated deployment and cybersecurity. Together with my mentor, I translated this into the following research question: “What are the benefits of deploying a cloudnative cybersecurity training platform compared to a traditional on-prem setup?”

This means that during my time at EY, I will be working on a cloud based platform where people can train their cybersecurity skills and learn about trending attacks. The platform will consist out of multiple modules that really give an in-depth explanation of upcoming trends in cybersecurity. For every module, the necessary infrastructure will be spawned using IaC and Azure cloud.

1.1 Motivation and background

Cloud really is the future of computing, so combining the knowledge of how infrastructure is built in the cloud with cybersecurity is the reason I chose this project. The further elaboration of the assignment was done together with my mentor at EY, Andreas Van Den Broucke. We came to the conclusion that a lot of platform focus on teaching old techniques and attacks and also don’t really give an in-depth explanation.

This is why we thought of working out a platform that focuses on trending attacks such as the SolarWinds supply chain attack. This kind of project is something that has a lot of business value and at the same time challenges me to get out of my comfortzone and really get into these attacks and do my best to understand them.

Another reason why this was such a great project, is that it takes on some shortages of the big platforms like HackTheBox and TryHackMe. They don’t offer the flexibility and depth that I do. Active HackTheBox machines do not get a writeup and on TryHackMe only some rooms get a full or partial explanation. So this in depth exercise combined with the latest exploits and not something from years ago is a big advantage on the other solutions.

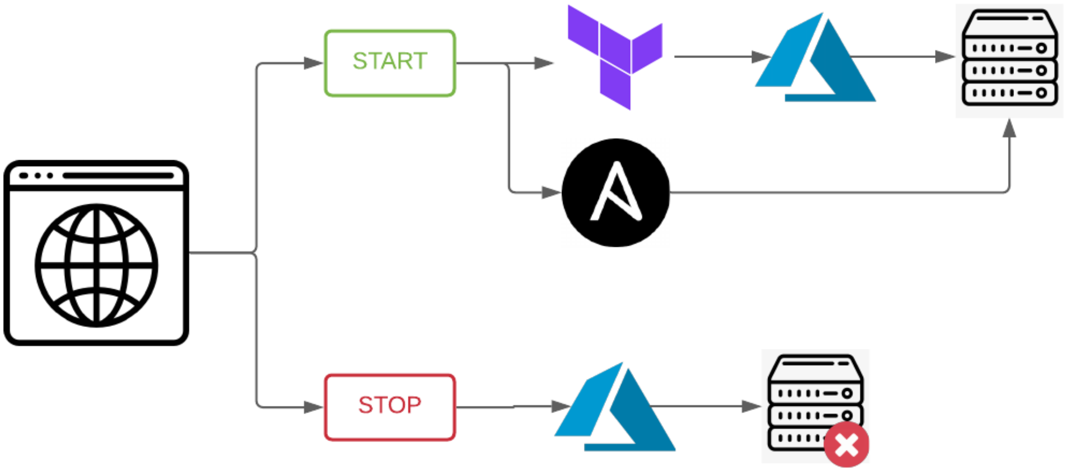
	SecuriEY	HackTheBox	TryHackMe
Deployable on demand	✓	✓	✓
Easily create custom exercises	✓	✗	✗
Always fully explained	✓	✗	✗
Full Walkthrough available	✓	✗	✗
Most trending attacks available	✓	✗	✗

1.2 Project goals

The main goals of this project are to have a working platform with a few modules that give an in-depth explanation of the chosen attacks and automated deployment of cloud native infrastructure needed to practice these attacks. The project is also divided into a few milestones:

- Working infrastructure as code for the first module
- Working webinterface
- First complete module
- Working website with at least three modules

Besides these main goals about the product, EY also emphasizes that I should get out of my comfortzone and learn as much as possible from this project. This comes down to technical skills as well as soft skills such as professional communication and project management. In conclusion, working out my project is a goal, but so is my own personal development.



In the diagram above you can see how the different Infrastructure as Code technologies will interact.

When you go on the platform to a module, you''ll be able to start or stop the infrastructure. When you start it, Terraform will connect with azure and build the infrastructure. When this has happened, Ansible will apply all of the necessary configurations.

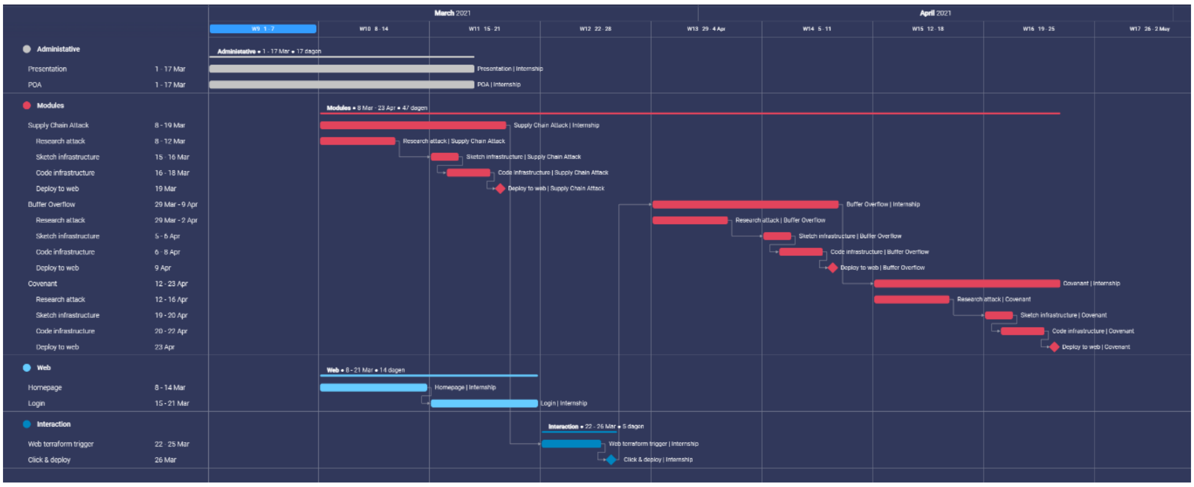
When you stop the infrastructure, Azure will delete all of the resources

1.3 Business case

The business value of this project really comes down to the current popularity of these attacks. Most platforms either test skills and don't really explain much or they bother you with outdated exploits such as EternalBlue, a cyberattack created by the NSA that exploits a common Windows service. A company that can educate its employees on upcoming and trending attacks will only benefit from this in the future.

Besides educating the current cyber security staff, it will also be available to use for demonstrations. You could give a demo to the Supply Chain team to create awareness. Or you could use it to give a demo to students to demonstrate the capabilities of EY and maybe spark their interest in cyber security.

2 Planning



Administative	
Presentation	1 - 17 Mar
POA	1 - 17 Mar
Modules	
Supply Chain Attack	8 - 19 Mar
Research attack	8 - 12 Mar
Sketch infrastructure	15 - 16 Mar
Code infrastructure	16 - 18 Mar
Deploy to web	19 Mar
Buffer Overflow	29 Mar - 9 Apr
Research attack	29 Mar - 2 Apr
Sketch infrastructure	5 - 6 Apr
Code infrastructure	6 - 8 Apr
Deploy to web	9 Apr
Covenant	12 - 23 Apr
Research attack	12 - 16 Apr
Sketch infrastructure	19 - 20 Apr
Code infrastructure	20 - 22 Apr
Deploy to web	23 Apr
Web	
Homepage	8 - 14 Mar
Login	15 - 21 Mar
Interaction	
Web terraform trigger	22 - 25 Mar
Click & deploy	26 Mar

March 2021
April 2021
W9 1 - 7
W10 8 - 14
W11 15 - 21
W12 22 - 28
W13 29 - 4 Apr
W14 5 - 11
W15 12 - 18
W16 19 - 25
W17 26 - 2 May
Administative • 1 - 17 Mar • 17 dagen
Presentation | Internship
POA | Internship
Modules • 8 Mar - 23 Apr • 47 dagen
Supply Chain Attack | Internship
Research attack | Supply Chain Attack
Sketch infrastructure | Supply Chain Attack
Code infrastructure | Supply Chain Attack
Deploy to web | Supply Chain Attack
Buffer Overflow | Internship
Research attack | Buffer Overflow
Sketch infrastructure | Buffer Overflow
Code infrastructure | Buffer Overflow
Deploy to web | Buffer Overflow
Covenant | Internship
Research attack | Covenant
Sketch infrastructure | Covenant
Code infrastructure | Covenant
Deploy to web | Covenant
Web • 8 - 21 Mar • 14 dagen
Homepage | Internship
Login | Internship
Interaction • 22 - 26 Mar • 5 dagen
Web terraform trigger | Internship
Click & deploy | Internship

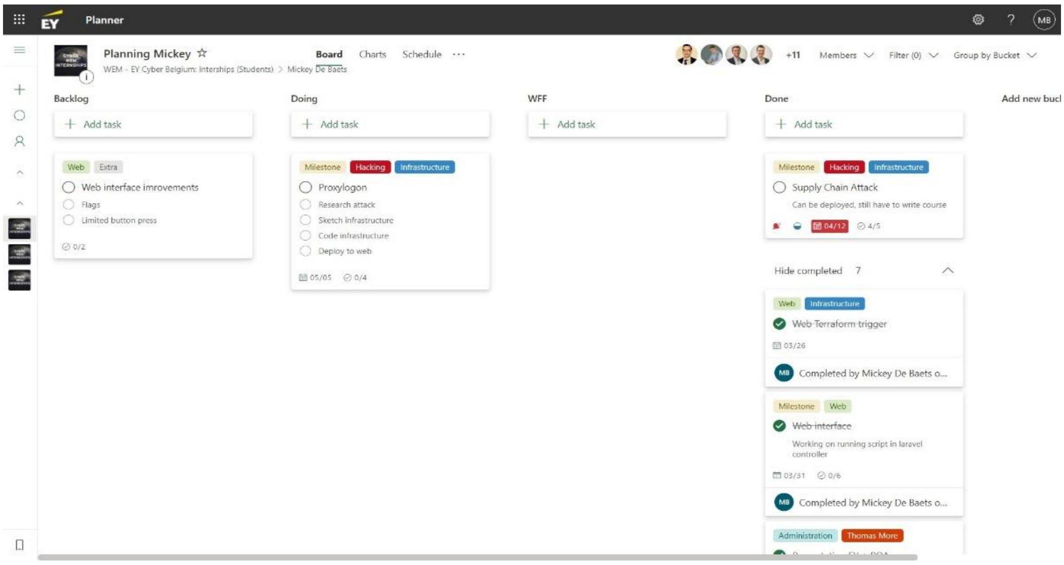
In the image above you can get an overview of planning up until the start of may. I will be working out module after module. During the first module I'll also be working on the interface, since this will only be basic. In the end, this is still a cybersecurity internship.

I decided to not plan anymore work since these are three very interesting modules which will require a lot of research. This current planning also leaves room for any unforeseen events while at the same time giving me enough time to dive into the subjects.

For an interactive view of my planning visit this link.

3 Information gathering and reporting

In order for the team to keep track of what I'm doing, they've set up a Teams structure for all the interns. In my own Teams channel there's a link to my Microsoft planner, my files and also my notes. This way they can always see what I'm doing and what I'm working on. I also regularly post updates about what I worked on in this Teams channel.



Planning Mickey ☆

WEM - EY Cyber Belgium: Interships (Students) > Mickey De Baets

Backlog

+ Add task

Web | Extra

○ Web interface imrovements

○ Flags

○ Limited button press

0/2

Doing

+ Add task

Milestone | Hacking | Infrastructure

○ Proxylogon

○ Research attack

○ Sketch infrastructure

○ Code infrastructure

○ Deploy to web

05/05 0/4

WFF

+ Add task

Done

+ Add task

Milestone | Hacking | Infrastructure

○ Supply Chain Attack

Can be deployed, still have to write course

04/12 4/5

Hide completed 7

Web | Infrastructure

✓ ~~Web Terraform trigger~~

03/26

Completed by Mickey De Baets o...

Milestone | Web

✓ ~~Web interface~~

Working on running script in laravel controller

03/31 0/6

Completed by Mickey De Baets o...

Administration | Thomas More

Besides the Teams channel, we also do a weekly update with the whole team to track project progress. I also meet multiple times a week with my mentor.