EY Internship

Design and deploy a cloud based hacker toolbox

Mickey De Baets

Contents

About EY

Ernst & Young, today better known as EY, is a professional services network with almost 300.000 employees in more than 700 offices in over 150 countries. The Belgian offices are in Diegem, Antwerp, Ghent and Bruges. EY is part of the big four. These are the four largest professional service networks in the world. In this group EY is joined by Deloitte, KPMG and PWC.

The office in Diegem, where the internship took place, is part of the EMEIA area. This means the area of operation consists of Europe, Middle East, India and Africa. Within this area multiple services are offered to the clients:

- **Tax**: provide information about (global) tax infrastructure.
- **Transaction advisory services**: provides information regarding raising, investing, preserving and optimizing the organizations capital.
- **Assurance**: provides general financial information.
- **Advisory**: provide clients with information regarding risk management and performance improvement.

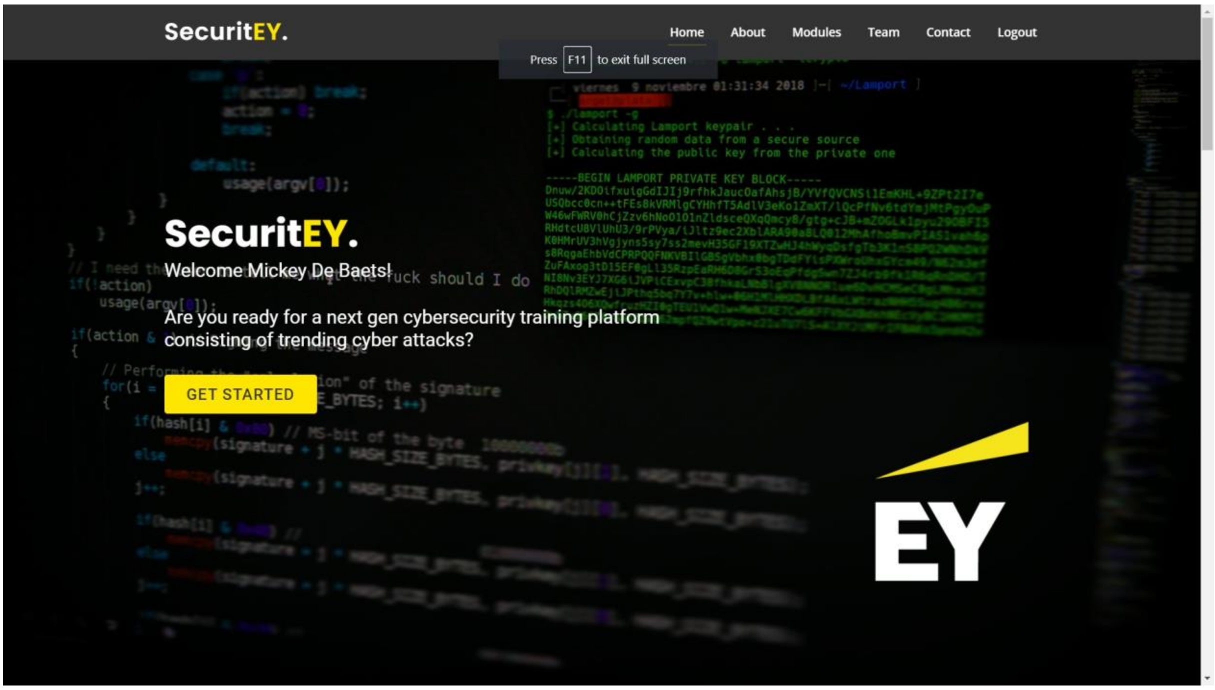
The field in which this internship took place, cybersecurity, is part of the advisory branch. Advisory consists again out of a number of other services:

- IT Transformation
- Data Analytics
- Finance
- Supply Chain
- Customer & Strategy
- People Advisory Services
- Risk Management
- Internal Audit & Controls
- Risk Transformation
- Cybersecurity
    - Cyber Program Management
    - Cyber Threat Management
    - Identity & Access Management
    - Data Protection & Privacy
    - Business Resilience
    - Business Continuity
    - Incident Response (IR)
- IT Assurance

EY has clients from a variety of sectors, but the most part is covered by the financial sector. The previous mentioned structure can again be split up in financial sector operations (FSO) and non-financial sector operations (non-FSO). This internship fell under guidance of the non-FSO team.

About the project

As the topic ‘Design and deploy a cloud based hacker toolbox’ is still pretty broad, further outlines had to be defined. The project had to be related to cloud, infrastructure as code and cybersecurity. A lot of ideas came along and the project took a lot of different shapes in the first two weeks, but with business value as a goal, SecuritEY was the most promising.



SecuritEY.

Welcome Mickey De Baets!

Are you ready for a next gen cybersecurity training platform consisting of trending cyber attacks?

SecuritEY is a platform built for cybersecurity training and awareness. The platform focusses on teaching the latest attacks. This way, EY cybersecurity professionals will have a playground to test out tools and techniques for topical scenarios. In its current state SecuritEY consists out of two modules: the Supply Chain Attack and ProxyLogon. Everything is of course shielded by a login page where you can only register using an EY email address.

SecuritEY provides a platform where the EY cybersecurity professionals can take on the role of instructor and provide explanation of how an attack works as well as a walkthrough of the hack using the provided infrastructure. This means the user will be presented with the technical information and background as well as a lab environment. The flow of the platform is as follows:

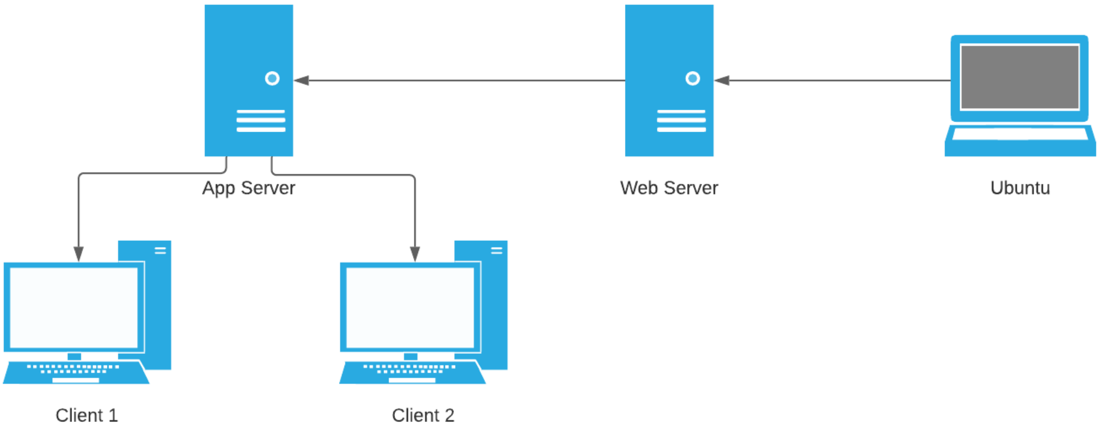
1. The user can go through all of the provided information and also has the option to spawn the infrastructure using the start button.
2. After clicking the start button, a Terraform script will connect with Azure and first create the necessary virtual machines.
3. After the machines are built, an Ansible script will run to apply all of the needed configurations and to put everything in place.
4. After clicking the stop button, all created resources will cease to exist. This way the user can experiment as much as they want and will always have a fresh and clean environment ready to use.

1. Modules

As mentioned above the platform is flexible to all kinds of modules. These can be just an in-depth explanation, but they can also be combined with cloud-native lab environments. The restrictions to the lab environments are simple, if it can be built using infrastructure as code and cloud, it can be used on the platform. The current state of the platform offers two modules.

1.1 Supply Chain Attack

Supply chain attacks are becoming one of the latest trends in cybersecurity. They happen more often and can have a very severe impact. A well trained ethical hacker has to know how these work and understand the risks. That’s why it is also the first module of the SecuritEY platform.



When booted, five virtual machines will be created and configured. One for the user, an Ubuntu hacking environment, and four to form a supply chain. The user will only be provided with a website, the one of HelloJava, a fictive company that provides Java applications to its customers. On this dummy website the attacker can abuse the contact form since it uses PHP’s eval function without input sanitation. This results in remote code execution and access to the web server.

When the connection to the web server has been established, the user can use this connection to read sensitive files and scan the internal network. They will find a new server that will turn out to be the distribution server of HelloJava’s software. Combining sensitive information from the web server and password reuse on the app server, a connection to the app server can be established. On this server you can add malicious code to the software they provide. Then, after a while, the two clients in the lab will use the software and be compromised. During the lab the user will also make use of a command and control server to keep a connection with all the compromised targets.

At the end of the lab the user will have executed a full, basic software supply chain attack. This lab is the ideal demonstration of how a small vulnerability can have an immense impact and how you getting hacked does not have to be your own fault.

1.2 ProxyLogon

ProxyLogon is the name given to one of the latest vulnerabilities of Microsoft's Exchange Server. Combining two previous known exploits, together they result in remote code execution on all of the following Exchange servers:

- Exchange Server 2019 < 15.02.0792.010
- Exchange Server 2019 < 15.02.0721.013
- Exchange Server 2016 < 15.01.2106.013
- Exchange Server 2013 < 15.00.1497.012

A lot of companies may not have the knowledge, infrastructure or time to immediately patch their Exchange server and so they remain vulnerable. Back in March of 2021 this was a big issue in Belgium and all over the world.

The module provides an environment with a Microsoft Exchange Server that is vulnerable to ProxyLogon. After spawning the infrastructure the user can use one of the many exploits available on GitHub to find out how easy it is to hack these vulnerable servers.

About the business value

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 from 2017 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 just benefitting from understanding these new attacks, the modules provided can also give the users the chance to see how their tools will react with these new attacks and techniques. In the end, this sandbox-like environment can be used for whatever purpose serves best.

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. You could even show clients why certain things are necessary and which impact it can have may they choose to neglect their investment in cybersecurity.

	SecuritEY	**HackTheBox**	**TryHackMe**
Deployable on demand	✓	✓	✓
Easily deploy custom exercises	✓	✗	✗
Always fully explained	✓	✗	✗
Full Walkthrough available	✓	✗	✗
Most trending attacks available	✓	✗	✗

Conclusion

The biggest advantage the SecuritEY platform offers is its accessibility and the elasticity in its purpose. It can be easily modified to deploy new modules and will provide a flexibility that you can't have from external resources. The topicality of the modules that are offered on the platform is unmatched which makes it perfect for all kinds of scenarios, whether it is for training the workforces or showing a client how quick it can go wrong. In the end, the final uniqueness of it all shows a well succeeded internship project.