

INTERNSHIP

Attack and Defend: Cyber Attacks

Description of the assignment

This internship assignment aims to investigate a number of specific cyberattacks and to analyse how organizations can protect themselves against them. To do so, a test environment will be set up in which the selected attacks are first carried out and then countered with appropriate security measures. Afterwards, the impact of these security measures on the course and effectiveness of the attacks will be evaluated.

Within the scope of this assignment, two cyberattacks will be studied: Pass-the-Hash and Cryptolockers.

Pass-the-Hash is an attack technique in which an attacker abuses stolen password hashes to gain unauthorised access to systems without knowing the original password. The aim of this study is to examine how effective a Privileged Access Management (PAM) solution is at preventing or limiting such attacks. The study will also evaluate how different configurations of the PAM solution affect the level of protection.

Cryptolockers, also known as ransomware, aim to encrypt the files on a system. Once the files have been made inaccessible, cybercriminals demand a ransom in exchange for restoring access to the data. In this internship assignment, the behaviour and impact of Cryptolockers will be compared between an unprotected and a protected environment. An Endpoint Security Solution will be used to protect the environment.

Both security scenarios will use the cloud-based Palo Alto Idera solution. It will be used to secure the test environment and to evaluate how effective the different defence mechanisms are against the cyberattacks under study.

Objectives

The following deliverables will be required:

- Setting up a test environment to be attacked and defended.
- Successfully executing a cyberattack using a cryptolocker within a test environment.
- Successfully executing a Pass-the-Hash cyberattack within a test environment.
- Securing the test environment using CyberArk's Endpoint Security Solution.
- Demonstrating that the cryptolocker and Pass-the-Hash attacks are no longer possible, without any day-to-day impact on users.

Possible extensions:

- Securing the environment against credential theft and being able to demonstrate that the protection works.
- Configuring JIT (Just-in-Time) elevation of applications for users.
- Evaluating how implementing CyberArk's Endpoint Security Solution affects system performance. Measuring and comparing the delays and system load across both environments.

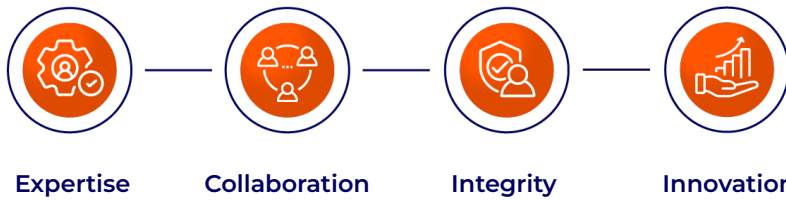
Technologies & concepts involved

✓ Palo Alto Idira	✓ Cloud
✓ Privileged Access Management	✓ Hyper-V
✓ Endpoint Management	✓ Pash-The-Hash Attack
✓ Windows	✓ Cryptolocker Attack

Project Methodology

For its projects, Acen uses agile project methodologies such as XP and SCRUM. The project described above follows the same approach. These methodologies focus on safeguarding the quality of software solutions. This is achieved by breaking the project down into shorter iterations and through intensive communication both within and outside the project team. The emphasis on intensive communication is an intrinsic characteristic of agile, resulting in thorough supervision throughout the internship period.

Profile



The ideal intern is first and foremost motivated to improve their skills and learn about a new field of technology.

The ideal intern has a basic understanding of information security principles in networked environments, works well in teams and demonstrates great communication skills.

Contact details

Contact person	Cindy Van den Hoecke	cindy.vandenhoecke@acen.eu
----------------	----------------------	----------------------------