Friday 13. November. 2020, Oslo

Bachelor thesis, Project Outline.

Bachelorproject in Software Engineering and informatics, spring 2021.

Oslo Metropolitan University.

Members, Group 23.

- Martin Bang, s315602.
- Frithjof Brate, s336406.
- Kristian Marison Haugerud, s331048.
- Mohammad Tayyab Khalid, s319229.
- Jørgen Sandnes, s331423.

Employer

- CYBR, Pilestredet 52, 0167 Oslo, website: https://cybr.no/
- Joe Jones, Director of Operations.

Description of CYBR.

CYBR is a startup that focuses on providing a learning platform and security testing to businesses. By implementing various techniques they are able to create a testing tool for checking overall security issues a business might face. Making these testing tools, CYBR have also been able to provide a learning platform that can help people in these businesses take steps necessary to secure themselves from potential attacks or close those vulnerabilities altogether.

Research and prototyping of an email phishing emulation system.

Project Overview: Research and prototyping of an email phishing emulation system that can be utilized to detect weaknesses in an organization (human links) and estimate the cost of breach. The focus should be on research and prototyping of an overall system instead of developing a tool or a software. It's recommended to use available tools in the open-source community to build different parts of the system of the PoC.

Requirements for research: There are several aspects of this project that require more research and investigation before diving into the prototyping phase. This will be discussed in more detail at a later point, but some of the outstanding items for research are:Understand and evaluate modus operandi for phishing attacks. Checkout some case studies available on the internet.

- From the above list, prepare a subset that could be applied in a corporate setting.

- Identify an attack mechanism that can be generalized as a pipeline. For example few email templates can be used only once, while others could be a long term engagement. One time emails should be part of a prototype while long engagements should be part of the research topic.
- Identifying the targets and relevant email templates for the targets. This would need research on how to source email addresses and add some meta-data on these to identify the targets correctly based on department, industry and position of the target user.
- Research on preparing attack pipelines. For example if a CEO/CTO/CFO clicks on the first email, what should the next email be? Again longer engagements should be prioritized only when one off prototype works.
- What metric to collect?
    - emails opened, targets, clicks on the links in email.
    - scope of the attack (e.g. information gathering, email with payloads,)
- Estimation on losses based on attack success.

High level requirements for prototype: More details will be provided during further discussions but the core idea is to:

- Implement a prototype (PoC) that helps to simulate targeted phishing attacks to uncover security holes in an organization.
- A system to prepare email templates based on research above. Ability to tag emails with metadata so to suggest email templates for attack.
- The focus should be on creating a system and not building a tool. Use readily available tools like gophish and managed services like mailchimp etc to send emails. Tool research should be part of the project.
- Analysing and observing response.