Phishing as a Service

Degree programme: BSc in Computer Science | Specialisation: IT Security
Thesis advisor: Prof. Dr. Bruce Nikkel

Phishing emails are a growing concern and one of the most successful attack vectors. Phishing campaigns can be a great tool for education and risk assessment. Conducting a phishing campaign is very costly due to the large amount of manual labour that is involved. In my thesis, I show how the deployment of a phishing campaign can be automated in order to reduce the manual labour involved.

Phishing emails are among the most common cyber-attacks any company suffers. Due to the human error that is preyed upon, they are one of the most successful attack vectors relative to the technical complexity.

Conducting phishing campaigns against your employees can be a great tool for:

- Risk assessment
- Educating employees
- Demonstrating the need for a larger budget to spend on cybersecurity

Unfortunately conducting a phishing campaign can be very expensive because there is a lot of manual labour involved.

- Domains need to be registered and configured
- Mailing needs to be set up and tested
- A website needs to be created for the user to interact with
- The results need to be analyzed and summarized in a report

This binds a lot of resources and time causing the conduction of a phishing campaign to be expensive. This limits accessibility and availability, especially for smaller companies. To solve this problem, my thesis will outline a way to automate the deployment of a phishing campaign allowing for the configuration and evaluation through a Web UI.

The following steps were automated:
Setup and execution:

- Registration of a DNS name
- Setting of the DNS records
- Provisioning a webserver hosting the landing page
- Configuring the mail server to send emails from a specific domain
- Sending phishing emails
- Collecting user interactions with the landing page

Clean-up:

- Removing the domain from the mail server
- Removing the DNS records from the domain
- Cleaning up log files
- Stopping and removing the webserver

To automate these steps, I have deployed all services as docker containers. Docker allows for the versioning of configuration files as well as the rapid deployment of services. To deploy multiple webservers on one host I have used Traefik as a proxy server for routing the traffic. Landing pages are deployed using a modified NGINX docker container. Mails are sent and received through a Dovecot and Postfix server, using a MYSQL 8 database to store the data. The Web UI is a Ruby on Rails webserver using a Postgres database.

The steps mentioned above were automated to the point where they can easily be triggered through the Web UI with minimal user interactions. Through this, it is possible to quickly deploy landing pages, register DNS names, send phishing emails and collect and analyze user interactions with the landing page.

This setup allows for the easy configuration and the rapid deployment of a phishing campaign.
As a consequence, fewer resources are bound making this tool more readily available on a smaller budget.

Rolf Michael Zurbrügg
rolf.zurbrugg@gmail.com