Definition of Bachelor Thesis Project

Phishing As A Service

ID	NKB1-2-19
Students	Rolf Michael Zurbrügg
Advisor	Dr. Bruce Nikkel
Experts	Dr. Federico Flueckiger

Assignment There are many companies who wish to test the IT-security awareness of their employees in order to raise their security awareness and in turn make the company as a whole more resilient against cyber-attacks that involve social engineering.

From the perspective from an IT-security company conducting phishing attacks demands a high amount of resources and a comparably low level of knowhow and technical expertise. Therefore, conducting Phishing attacks is not very lucrative and binds a lot of resources.

So why conduct phishing attacks at all? Phishing attacks are very simple in their concept. Attacker sends mail containing a malicious payload for example a link pointing to a website controlled by the attacker looking like a login page. The user clicks on the link and enters his password. The attacker now has the password of the user. Therefore, the People in charge of the IT infrastructure can use the results from a phishing attack to convince the management (non- technical users) to invest more in hardening and testing their infrastructure and in educational staff-programs.

Conducting phishing attacks is not very efficient, but it has a high strategic importance, as it is a good door opener and way to unlock more resources for follow up tests. Which are financially and technically more interesting.

As we have seen there is a good reason to conduct phishing's, but we don't want it to bind unnecessary time from our tester which can be better used elsewhere. Moreover we want to stay competitive with our pricing for phishing attacks against other providers. Which may be operating from a country where salaries and infrastructure is cheaper.

The solution is automation. If it is possible to largely automate the phishing process this would increase the cost efficiency immensely and also free up resources.

This bachelor thesis will be aimed at creating a platform, that can be used to automate phishing campaigns through minimal user interaction. The idea is that a person can then set up a phishing campaign through a web UI. In the background mail servers and landing pages will be set up automatically.