EXYS1400-POSEIDON

Ethical Phishing and Awareness Made Easy

EXYS1400-POSEIDON:

POSEIDON is an ethical phishing tool to assess a company's resilience to social engineering and phishing in particular. It is an essential tool to help organizations improve the security awareness of their employees, thus reducing the risk of falling victim to real-world phishing attacks. Whether used independently, or combined with training in the form of workshops or specific courses, the tool is intended as a security awareness exercise that, through ethical phishing, is able to evaluate user's preparedness and continuously improve any found weak spots. All in accordance to existing privacy regulations. Send emails using a variety of pre-built templates or custom ones. An exhaustive dashboard displays statistics about:

- who received the email
- who opened the email
- who clicked on a fraudulent link
- who provided own credentials (on phishing campaigns that include this feature)

Immediate feedback can be given to users who fall into the trap, explaining all red flags that they should have noticed.

ECLEXYS

Where Passion Meets Technology

INCREASE RESILIENCE AGAINST SOCIAL ENGINEERING
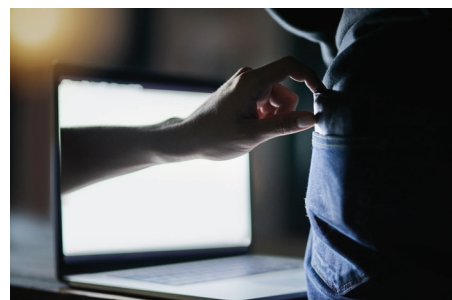
POSEIDON is an ethical phishing tool designed to simulate phishing attacks in a controlled and secure environment. Its main goal is to educate and inform final users (e.g. company employees) on how to recognize and react to real phishing attacks.

Here are some of the main characteristics of POSEIDON:

Phishing attacks

- Phishing emails: sending of fraudulent emails that lead recipients to the disclosure of sensitive information.
- Spear Phishing: more specific attacks that target individuals or groups using more personalized information, usually leading to more successful results.
- Phishing via SMS (Smishing): sending of SMS messages containing links or asking for personal information.
- Phishing via Social Media: simulation of attacks through social media platforms.
- Qshing: sending of fraudulent emails which contain a malicious link hidden behind a QR code.

Customization of attacks

- Set of custom email templates: POSEIDON includes a variety of email templates that can be customized to fit specific scenarios.
- Diversification of attacks: attacks with varying degrees of complexity and techniques can be created, such as malicious attachments, link to fake web pages, etc..

Monitoring and Analysis

- Tracking responses and actions of users under attack:
  - receiving the email,
  - opening the email,
  - click on the fraudulent link,
  - who entered own credentials (if requested by the phishing attack),
  - in generals the insertion of data into fake pages used for the attack.
- Timeline of the custom attack for each user, including a list of actions performed since reception of the attack.
- Detailed reporting: generation of reports that show the success rates of simulated attacks and the areas of user vulnerability.
- Privacy: all reports are strictly anonymized and in full compliance with current privacy regulations.

Compliance and Security

- Regulatory compliance: from the inception of the POSEIDON service, ECLEXYS paid attention to make sure that the tool complies with regulations and laws on privacy and data security.
- Secure environment: the system architecture was designed to provide assurance that all simulations are conducted in a safe environment, without real exposure of sensitive user data.
- Data confidentiality: the system and all data handled by the system are encrypted in order to guarantee a high level of safety.

DISCLAIMER:
Like any IT and technological tool, it is possible to make the best (and ethical) use of it, but also the worst use (exploiting the tool for real attacks). ECLEXYS states herewith that it is EXPRESSLY PROHIBITED to use POSEIDON for malicious purposes.

EXPERIENCE   SUPPORT   NETWORK   DLT   TSP   CYBER SECURITY   IOT   MOBILE COM.   CLOUD