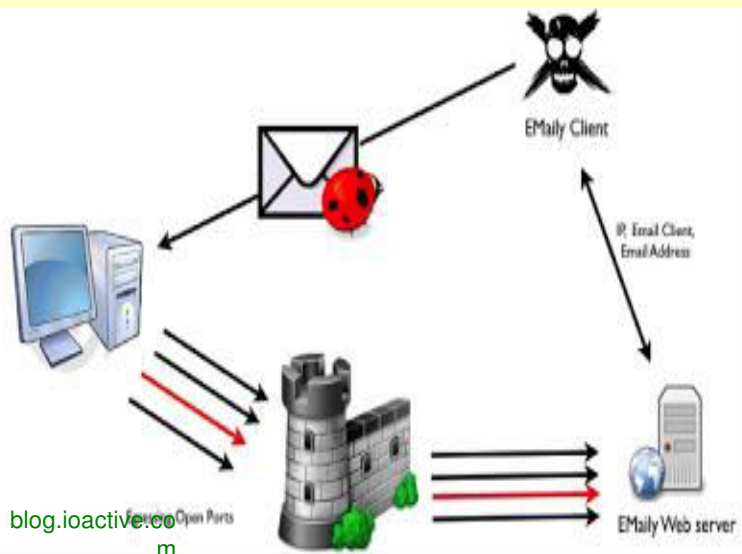


Social Engineering

Social engineering refers to the methods attackers use to deceive victims into performing an action. Typically, these actions are opening a malicious webpage or running an unwanted file attachment.

Many social engineering efforts are focused on tricking users into disclosing usernames or passwords, allowing attackers to send messages as an internal user to further their data stealing attempts.



In August 2013, for example, malicious hackers distributed emails that simulated the messages Facebook sends when a user is tagged in a post. The links in the messages led to sites that recommended installing a plugin to view the videos supposedly posted on Facebook. The plugin was, in fact, malware designed to steal saved passwords and hack into users' Facebook accounts.

Before releasing any information to anyone it is essential to establish:



- ▣ The sensitivity of the information
- ▣ Your authority to exchange/release the information
- ▣ The real identity of the third party
- ▣ The purpose and method of the exchange.

SOCIAL ENGINEERING
The clever manipulation of the natural human tendency to trust.

thewindowsclub.com