I am taking the example of an OSINT tool called zPhisher. It is a phishing tool that can be used to lure users into giving their credentials.
Although the basic idea is the same, zPhisher goes a step ahead and automatically certifies the phishing URL with an SSL certificate so that the link will look authentic.

**Pre-Engagement:** Phishing can be used in a variety of ways in an organization. Red Teamers can use it to send out phishing links to the employees of the organization, educate them on its use cases, and make them aware of the security malpractices that are currently being done.

**Intelligence Gathering**: The pen tester can use a use-case database of a selected group of employees or obtain their emails through social engineering and using OSINT methods such as linkedin, company pages, etc

**Threat modeling**: The pen testers will first make a list of all the users and their access control permissions. Then they can rank the individuals with the highest level of access to the ones with the lowest level of access.
Eg: the CFO will have more information than an analyst in the same company.

**Vulnerability Analysis:** With all the information established from previous steps, the pen tester can proceed to vulnerability analysis. During this step, the pen tester will poke around the web application within the scope of the penetration test.

**Exploitation:** Once a vulnerability is found, the pen tester will carefully use the vulnerability for an exploit. In web application penetration tests, it’s highly recommended to perform this step in the staging environment since there may be a vulnerability that could potentially cause significant damage.

**Reporting:** At this step, the penetration tester or team will provide a written document on their discoveries and provide a risk analysis of the discoveries.