

Exploitation of vulnerabilities

Santiago Hernández Ramos
@santiagohramos

EXPLOITATION OF VULNERABILITIES

- This phase involves using techniques that allow the analyst to **exploit an identified vulnerability to gain some advantage** from the perspective of an Ethical Hacking exercise.
- It corresponds to one of the most important and intrusive phases of the Ethical Hacking process.
- The organization's protection and detection tools must be carefully considered, including: Anti-Virus, EDR, IPS, IDS, HIDS, WAF, and others.

EXPLOITATION OF VULNERABILITIES

- Depending on the technological component where the vulnerability is located, we will divide the exploitation phase into:
 - Exploitation of Vulnerabilities in Hosts
 - Exploitation of Vulnerabilities in Web Applications
 - Exploitation of Vulnerabilities in Networks