Hacking Etikoaren Prozedura (Pentesting)

1. Helburua

Zabala Gailetak-eko sistemen segurtasuna ebaluatzea, ahultasunak kontrolatutako modu batean ustiatuz, konpondu ahal izateko.

2. Irismena

- **Barne:** Sarea (Wi-Fi eta Kableatua), Webgunea, App Mugikorra.
- **Mugak: EZ** eraso OT sareko makineria martxan dagoen bitartean (arrisku fisikoa). **EZ** egin DoS erasorik produkzio sistemetan.

3. Metodologia (PTES / OSSTMM)

Fase 1: Informazio Bilketa (Reconnaissance)

- **Pasiboa:** Google Dorks, Shodan, Whois, TheHarvester (domeinuak, emailak bilatu).
- **Aktiboa:** Portu eskanerra (Nmap), Zerbitzuen identifikazioa.

Fase 2: Ahultasunen Analisia

- Eskaneatze automatizatua: Nessus, OpenVAS.
- Web azterketa: OWASP ZAP, Burp Suite (XSS, SQLi, CSRF bilatzeko).

Fase 3: Ustiapena (Exploitation)

- Metasploit erabili detektatutako CVE-ak ustiatzeko.
- Helburua: “Flag”-a lortzea edo administratzaile baimenak eskuratzea (Shell).

Fase 4: Ustiapen Ostekoa (Post-Exploitation)

- Pribilegioen igoera (Privilege Escalation).
- Pibotajea (Sare batetik bestera jauzi egitea).
- Datu sentikorrak bilatu (frogak lortzeko).

Fase 5: Txostena

- Aurkitutako ahultasunak zerrendatu (CVSS puntuazioarekin).

- Ustiapenaren froga (PoC).
- Konponbide teknikoak proposatu.

4. Baimenak

- Jarduera hauek **baimen idatziarekin soilik** egin daitezke.