honeypot_plan

Honeypot Inplementazio Plana - Zabala Gailetak

1. Helburua

Irudizko sistema zaurgarri bat (Honeypot) ezartzea Interneten, erasotzaileen teknikak, jatorria eta helburuak aztertzeko gure ekoizpen sistemak arriskuan jarri gabe.

2. Honeypot Mota

- **Mota:** Interakzio ertaina/altua.
- **Simulazioa:**
    - SSH Zerbitzua (erasotzaileak komandoak exekutatzen saiatzeko).
    - Web Zerbitzua (Login faltsu batekin).
    - Modbus/PLC simulazioa (OT ingurunea denez, interesgarria izan daiteke erasotzaile industrialak erakartzeko).

3. Aukeratutako Tresna

- **T-Pot:** Honeypot plataforma integrala, hainbat honeypot containerretan (Cowrie, Dionaea, Honeytrap…).
- **Cowrie:** SSH eta Telnet honeypot espezifikoa.
- **Conpot:** Sistema Industrialak (ICS/SCADA) simulatzeko.

4. Kokapena

- Sare isolatu batean (DMZ berezi bat edo guztiz kanpoko IP batean), barne saretik guztiz bereizita.
- **EZ** da inoiz produkzio sare berdinean jarriko.

5. Konfigurazioa

- Portuak ireki: 22 (SSH), 80/443 (Web), 502 (Modbus).
- Logak zentralizatu eta aztertu (ELK Stack T-Pot barruan dator).

6. Segurtasun Neurriak

- Honeypot-a bera “gotortu” behar da erasotzaileak ez dezan erabili beste eraso batzuk egiteko (sandbox).
- Irteerako trafikoa mugatu.

7. Analisia

- Erasoen jatorria (GeoIP).
- Erabilitako erabiltzaile/pasahitzak (Hiztegiak eguneratzeko).
- Deskargatutako malware-a aztertu (Forentse taldearentzat).