Projecte de Ciberseguretat: Simulació d'un Atac i Defensa d'un Sistema Vulnerable

Guillem Arnau Saladié Martín

---

1. Introducció

Aquest projecte té com a objectiu realitzar una simulació d'un atac ètic complet contra una màquina vulnerable, utilitzant tècniques d'OSINT, enginyeria social i cracking de contrasenyes. Posteriorment, s'analitzaran els riscos, es proposaran mesures de seguretat i es simularà la resposta de la víctima davant de l'atac.

---

2. Objectius

- Simular un cicle d'atac ètic real (reconeixement, enginyeria social, accés, accions i defensa).
- Practicar l'ús d'eines com Kali Linux, theHarvester, SET, Hydra, Wireshark, etc.
- Analitzar els riscos associats a sistemes mal configurats o usuaris poc formats.
- Aplicar mesures de resposta i defensa per part de la víctima.

---

3. Entorn de simulació

3.1. Xarxa

- Tipus: Xarxa interna (VirtualBox)
- Sense accés a Internet
- IPs:
    - Kali Linux: 192.168.1.3
    - ubuntu: 192.168.1.2

3.2. Màquines virtuals

- **PC1 - Màquina víctima**
    - Sistema operatiu: linux ubuntu

    - Usuari: alumne
    - Contrasenya: alumne
    - Navegador i correu electrònic instal·lats
- **PC2 - Màquina atacant**
    - Sistema operatiu: Kali Linux
    - Eines: Nmap, SET, theHarvester, Wireshark, John the Ripper, Hydra

---

4. Fases del projecte

4.1. Reconeixement i OSINT

- Cerca d'informació sobre l'usuari fictici
- Detecció de correus, noms d'usuari i patrons de contrasenya

4.2. Enginyeria social i phishing

- Creació d'una pàgina falsa de login (SET o Evilginx)
- Enviament d'un correu simulat amb enllaç maliciós
- Captura de credencials

4.3. Cracking i accés al sistema

- Atac de força bruta amb Hydra
- Anàlisi del hash amb John the Ripper
- Accés remot a la màquina amb credencials capturades

4.4. Accions de la víctima (resposta defensiva)

- Canvi de contrasenyes

- Desconnexió de la xarxa
- Revisar logs i detectar accessos
- Instal·lació d'un antivirus o firewall

---

5. Anàlisi i gestió de riscos

Actiu	Vulnerabilitat	Amenaça	Risc
Usuari de Windows	Contrasenya senzilla	Cracking de credencials	Accés total al sistema
Navegador del Windows	Clica en enllaços sense verificar	Phishing	Robatori d'identitat
Xarxa interna	Sense xifrat / filtre	Captura de trànsit	Robatori de credencials
Sistema sense antivirus	No hi ha detecció d'atacs	Persistència de malware	Compromís total del sistema

---

6. Conclusions

Aquest projecte ha permès comprovar com una combinació d'informació exposada (OSINT), contrasenyes febles i manca de coneixement pot derivar en una intrusió completa. Alhora, s'ha pogut valorar la importància d'una bona formació en seguretat, l'actualització de sistemes i l'educació de l'usuari final.

---

7. Annexos

- Captures de pantalla de les eines
- Exemple del correu de phishing
- Exemple de pàgina falsa
- Logs de la màquina víctima