Securitate ofensiva. Tema 2. Algortim pentru test de penetrare fizica

1. Se va crea o cercetare preliminara utilizand surse disponibile online (OSINT) pentru a afla detalii despre companie cum ar fi retele sociale precum LinkedIn, utilizare Google Maps etc.

2. Planificarea patrunderii:

a. Timpul optim va fi dimineata devreme sau seara tarziu cand activitatea angajatilor este redusa.

b. Obiecte comune care nu ridica suspiciuni

c. Echipamentul necesar va fi o legitimatie falsa, laptop, dispozitiv de proximitate RFID

d. Haine comune sau uniforma

3. Legenda in caz de interceptare, vom folosi inginerie sociala si ne vom prezenta ca fiind un tehnician IT extern, angajat pentru verificarea echipamentelor de retea, avand o poveste plauzibila.

4. Executie:

a. Patrundere in birou – vom indentifica biroul contabilului sef fie individual fie prin interactiune cu angajatii, vom nota caile de acces iar pentru incuietoarea magnetica avem cateva variante pentru a o debloca: folosire RFID-ului, exploatarea unei surse de alimentare a incuietorii precum cutia de control sau cabluri electrice, folosirea unui magnet puternic, iar in ultim caz folosirea ingineriei sociale pentru a solicita acces unui angajat.

b. Accesare informatii, cautare parole scrise pe post-it-uri, agende sau documente lasate pe birou sau, in cazul de fata utilizarea unui Phising email care ar putea arata astfel:

Subiect: Actualizare urgenta pentru contul dumneavoasta de contabilitate

Buna ziua [nume contabil sef],

In urma unor actualizari recente ale sistemului financiar utilizat de compania Simir SRL, va rugam sa verificati contul dumneavoastra si sa confirmati datele de acces.

Pentru aceasta, va rugam sa accesati linkul de mai jos si sa introduceti datele de autentificare:

(vom folosi un link ce va la un site ce va simula unul legitim)

Aceasta actiune este necesara pentru a evita blocarea temporara a contului dumneavoastra incepand cu data de 10.01.2025.

Va multumim pentru colaborare!

Echipa IT

5. Finalizare actiune: Dupa obtinerea informatiilor vom iesi din cladire, eventual pe o usa secundara si ne vom asigura ca nu au ramas urme evidente in urma.