Naloga 2 – Footprinting & Reconnaissance

Za izbrano podjetje opravite osnovni pregled informacijske infrastrukture podjetja. Pri tem sledite smernicam iz dokumenta PDF (Footprinting&Reconnaissance.pdf). Vaš cilj je pridobiti čim več informacij o določenem podjetju, in sicer:

1. Informacije o organizaciji
    a. Informacije o zaposlenih
    b. Ozadje organizacije
    c. Telefonske številke
    d. Lokacije
2. Informacije o sistemih
    a. Operacijski sistemi spletnih strežnikov
    b. Lokacije strežnikov
    c. Uporabniki
    d. Gesla
3. Informacije o omrežju
    a. Domene
    b. Poddomene
    c. Naslovi IP
    d. Zapisi Whois in DNS

Pri opravljanju izvidništva uporabite naslednja orodja:

1. *OSINT framework - zbiranje informacij iz brezplačnih orodij ali virov
2. *Google dorks – osnovni (težje dostopni) podatki
    a. https://securitytrails.com/blog/google-hacking-techniques
3. *Shodan – IoT naprave, OS
    a. https://medium.com/@ciph3r/how-to-use-shodan-like-a-pro-50c15e085563
4. *Netcraft – OS, domene, poddomene
5. Censys – OS
6. *DomainTools in nslookup – Whois in DNS
7. EmailTrackerPro ali Infoga
8. *theHarvester – brskanje po družbenih omrežjih, email seznami
9. Web Data Extractor – kontaktni podatki, URLji , meta tags
10. *ARIN Whois database

- orodja označena z * so **obvezna.**

Oddaja

Oddajte podrobno poročilo, ki vsebuje prikaz pridobljenih podatkov (po točkah) za podano podjetje. Poročilo naj bo sistematično, naj vsebuje kazalo ter posamezna poglavja kjer bodo prikazani rezultati. Pri poročanju rezultatov najprej opišite postopek (uporaba) orodja (katere ukaze ali ključne besede ste uporabili pri iskanju) in nato pridobljene rezultate pokomentirajte. Kot dodatno pojasnitev k razlagi lahko vključite še print screen.

Poimenovanje oddane naloge naj bo sledeče: **Ime_Priimek_Naloga2.pdf** ali **Ime_Priimek_Naloga2.docx**