ACPM
Audit Consulting Project Management

OSINT

Avagy az internet egy hacker szemszögéből

OSINT - Open Source Intelligence

- Nyílt Forrású Információszerzés
- Definíció: *minden egyén számára nyilvánosan, legális eszközökkel megszerezhető, vagy korlátozott körben terjesztett, de nem minősített adatok szakmai szempontok alapján történő felkutatását, gyűjtését, szelektálását, elemzését-értékelését és felhasználását jelenti*
- *1939 Brit Hírszerzés*
- *Pro: Alacsony költségek, gyorsaság*
- *Kontra: Ellenőrzés, egyre növekvő adat mennyiség*
- *Elektronikai hírszerzés*
  - *Elemző algoritmusok*
  - *Több 10.000 weblap, blog, applikáció*
  - *Kapcsolatok és összefüggések elemzése*
- *Ma mindenki számára elérhető applikációk és adatok*

„A kémkedés az egyik legősibb mesterség a világon.”

Merülés a végtelenbe

Surface web

Deep web

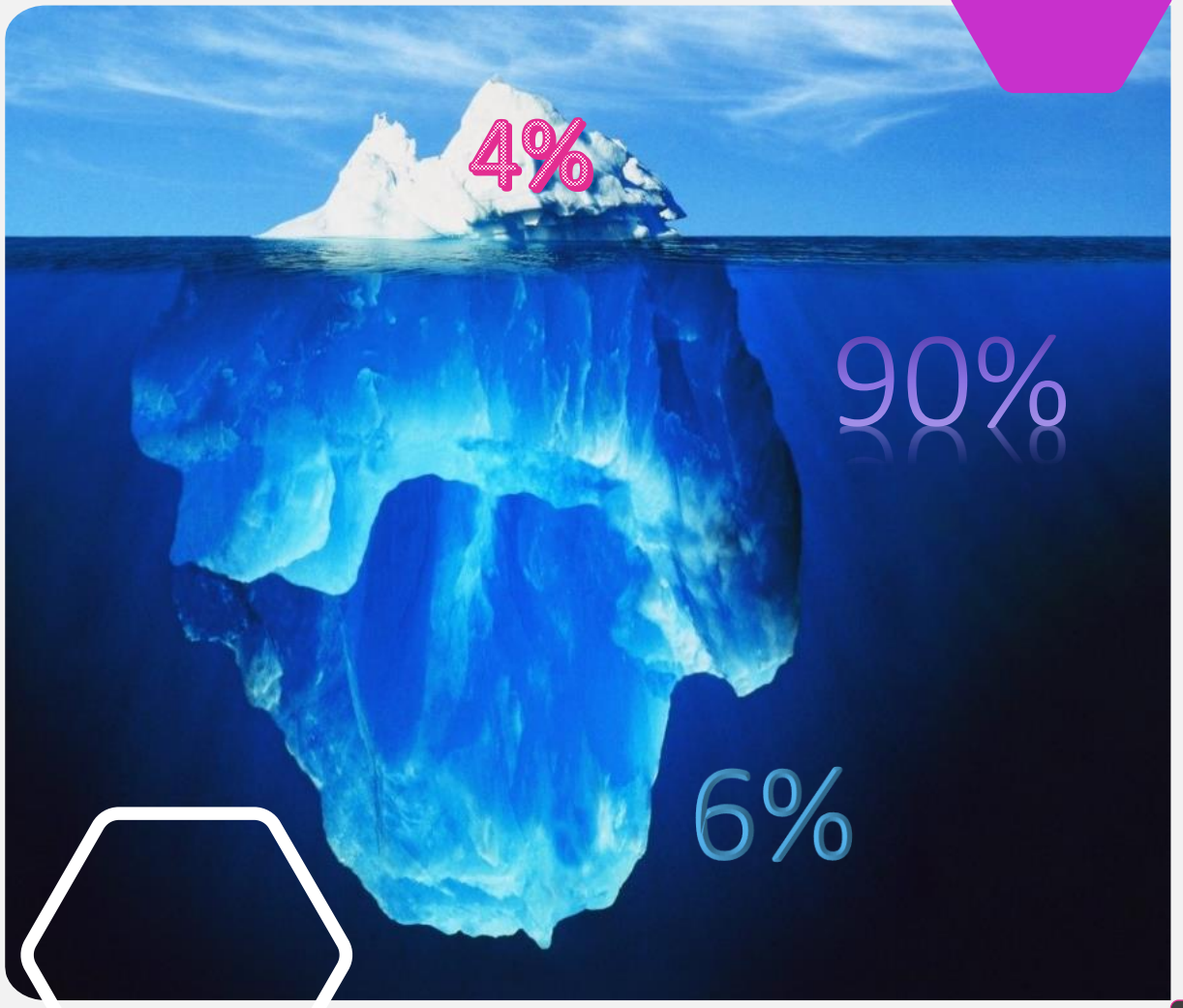
Dark web

Secret and Hidden web

Internet

- Surface Web
  - Közönséges kereső monitor
  - Google, Wikipedia, Yahoo, Twitter, Facebook stb.
- Deep Web
  - Proxy és deep web browser szükséges (Tor, Tails, I2P, Fresh Onions)
  - MySQL adatbankok, Reddit, Web Hosting, Dig, FTP Server, Honeypots, Streaming, speciális fórumok stb.
- Dark Web
  - Deep web browser, zárt rendszer, meghívás szükséges
  - Tiltott tartalmak, ember kereskedelem, drog- és fegyverkereskedelem, fogadások stb.

Mit látunk mi és mi látnak a hackerek?



Cyber Kill Chain – Hackerek lépései

Felderítés: A célpont beazonosítása.

A támadók tevékenységei: Ebben a fázisban a támadók a műveleteik megtervezését végzik, információt gyűjtenek, hogy megértsék a megtámadni tervezett rendszer működését, esetleges hibák után kutatnak, amiknek a kihasználásával elérhetik a céljaikat. Ehhez e-mail címeket gyűjtenek, a megtámadni tervezett szervezet munkatársait próbálják beazonosítani a közösségi oldalakon, átvizsgálják a sajtóban megjelent híreket, konferencia-résztvevők listáit és felmérik a szervezet Interneten elérhető szervereinek körét.

A védők tevékenységei: A támadók felderítéssel kapcsolatos tevékenységeit normális esetben nehéz lehet észlelni, de ha sikerül, az így szerzett információk nagy segítséget jelenthetnek a támadók céljainak azonosításában. Ilyen információkat lehet találni az Interneten elérhető szerverek logjaiban, a látogatásokról készült webes analitikákból (böngésző statisztikák, látogatási idők, stb.)*

Első lépés – Felderítés OSINT-tal

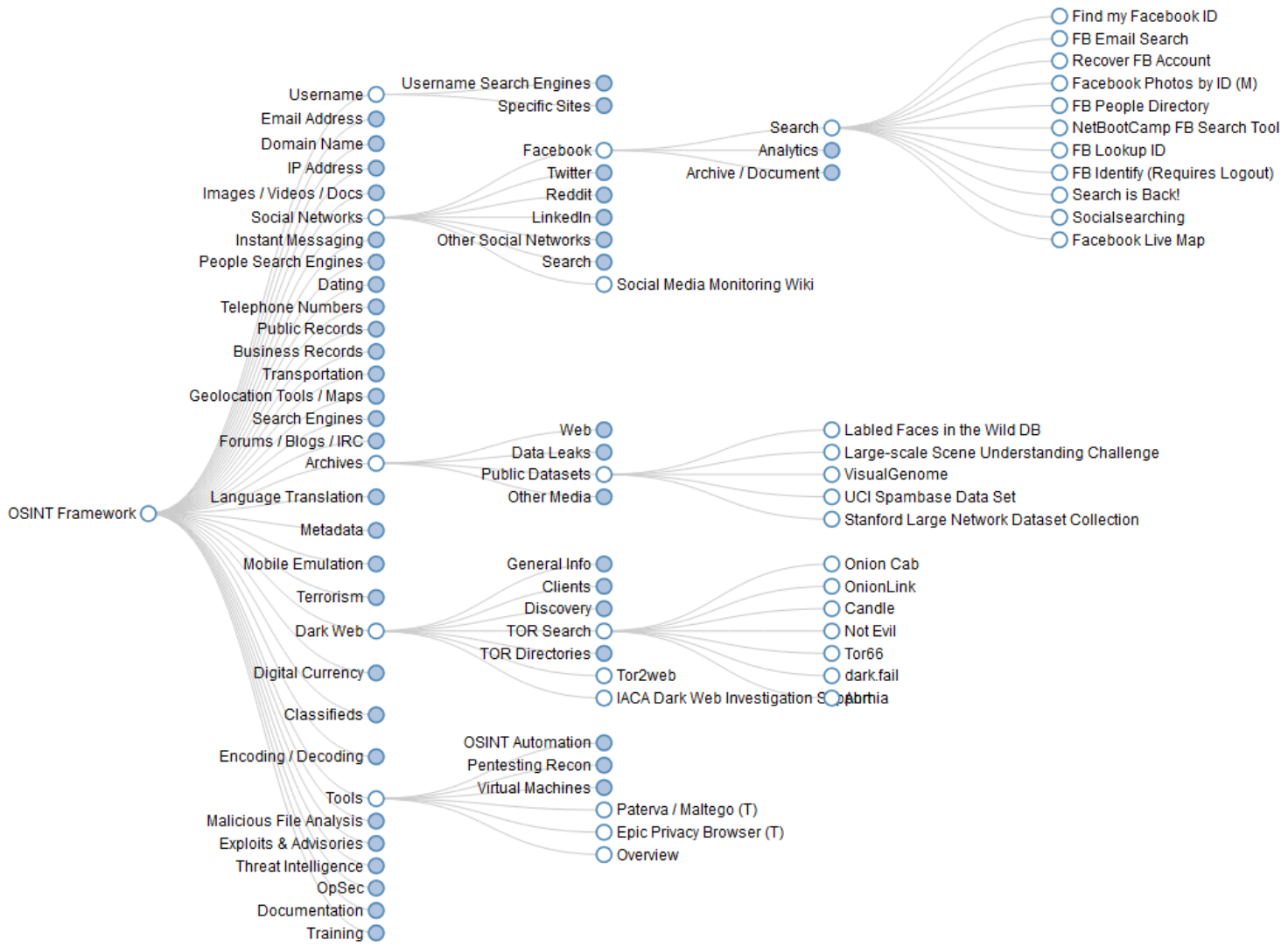
- Anonimitás:
  - Használj VPN-t
  - Változó IP címet
  - Különböző VM-t
  - Ne használj sose direkt kapcsolatot az internet szolgáltatóhoz (DMZ)
  - Töröld az adataidat (böngészési előzmények, cache, cookies)
  - TOR – The Onion Router:
    - Hidden Wiki:
      - http://ybp4oezfhk24hxmb.onion/ – Hitman Network
      - http://en35tuzqmn4lofbk.onion/ – US Fake ID Store
      - http://ll6lardicrvrljvq.onion/ – Brainmagic – Best psychedelics
      - http://zbnnr7qzaxlk5tms.onion/ – Wiki Leaks
      - http://jntlesnev5o7zysa.onion/ – The Pirate Bay – Torrent stb.
  - Hozz létre fake profilokat információszerzéshez
    - Rendszeres aktivitás, ismerősök, dokumentáció
    - Lehetnek más hamis profilok is!
  - Inkognitó mód aktiválása
  - Offline biztonság

Második lépés – Felderítés OSINT-tal

- Tervezés
  - Definiáld, hogy milyen típusú információkra van szükséged
  - Priorizáld az információk beszerzéséhez szükséges erőforrásokat
  - Konkrétan tűzd ki a céljaidat
- Információk: IP címek, telefonszámok, videók, fotók, dokumentumok, okos eszközök adatai, nyilvános kamerák, jelszavak, online aktivitás stb.
- Adatok osztályozása, kiértékelése
- Dokumentáció
- Felhasználás a következő lépésekben
- Eszközök: OSINT Framework, Namechk.com, Maltego, Shodan, Spokeo, Snapbird stb.
- Alakítsd ki a saját módszeredet, válaszd ki kedvenc OSINT eszközeidet
- Maradj láthatatlan
- Digitális nyomok: HW információ, képernyő beállítások, nyelv, browser verzió és pluginok stb.

OSINT Eszközök gyűjteménye

OSINT Framework



OSINT Eszközök gyűjteménye

OSINT Tools.

Social Media Resources

Facebook

- Search Facebook Basics
- Facebook Security

UserID:

- findmyfbid.com
- lookup-id.com

Search Tools:

- Who Posted What
- Graph Tips FB Search

People Search Engines

- Family Tree Now
- Spokeo
- PeekYou
- That'sThem
- Usersearch
- Qwant
- Searx
- Soolve

Twitter

- Twitter Advanced Search
- Twitter Search Tricks
- Twitter Directory
- Inteltechniques Twitter Search
- Tweet Deck

UserID:

- TweeterID
- GetTwitterID
- MyTwitterID
- TweetBeaver
- Twopcharts ID Check

_____

Analytics:

- Socialbearing
- Onemilliontweetmap
- Twitonomy
- Followerwonk
- Keyhole

YouTube

- Geo Search Tool
- Extract Metadata
- Yasiv
- Yout
- TubeChop
- Deturl
- Watchframebyframe
- Savefrom
- Y2mate
- Keepvid
- DreDown

Instagram

UserID:

- Code of ninja ID lookup
- Otzberg ID lookup

Third Party Platforms:

- Someture

Köszönjük a figyelmet!

Páhi Tímea, MA, BSc, CEH

+43 676 4835448

timea.pahi@acpmit.com

www.acpmit.com

ACPM

Audit Consulting Project Management