4. óra: Passzív információgyűjtés: Google hacking, archive.org, web scraping, email harvesting (harvester), netcraft, whois

Tartalom

1. Keresés a weben

https://duckduckgo.com/, http://www.bing.com/, https://search.yahoo.com/, https://yandex.com/, http://www.google.com/

1.1. Keresési operátorok

jel	jelentés	példák
site:	Megadott domén	site:cisco.com
related:	Kapcsolódó weboldalak	related:ripe.net
intitle:	A címben	intitle:"index of"
inurl:	Az urlben	inurl:scan_result_file
intext:	Csak a tartalomban	intext:"please login"
filetype:	Állománytípus	filetype:pdf
ext:	Állomány kiterjesztés.	ext:xls
AROUND(n)	Hány szó távolságra lehetnek.	tesla AROUND(3) edison
-	Kizárás a keresésből	• jaguar speed -car • site:cisco.com -site:www.cisco.com
""	Pontos egyezés	"unknown interface"
" * "	Pontos egyezés kihagyott szavakkal	"largest * in the world"
OR, AND, ()	Logikai műveletek	(emacs OR vi) scheme

1.2. Fontosabb keresések

- Webes jelenlét mértéke: Indexelt oldalak száma.

```
site:cisco.com
```

- Aldomén-enumeráció.

```
site:cisco.com -site:www.cisco.com
```

- Keresés kiterjesztés alapján

```
site:mol.hu ext:xls
```

1.3. Nem célzott támadás esetén

- Google Hacking Database: https://www.exploit-db.com/google-hacking-database/

2. Email harvesting

- Mire jó?
  - Kliens oldali és social engineeringtámadások lehetséges célpontjai,
  - az emailcímek konvencióinak megállapítása.
- theharvester (https://github.com/laramies/theHarvester)

```
theharvester -d cisco.com -b bing \
> bing.txt
```

```
theharvester -d cisco.com -b google \
> google.txt
```

3. whois

- A `whois`-nek 3 értelme van: 43-as (tcp, udp) porton elérhető szolgáltatás, egy parancssoros eszköz és két fajta adatbázis.

3.1. DNR (Domain Name Registries)

TLD (top-level domain) lista: http://www.iana.org/domains/root/db

3.1.1 Lekérdezhető adatok

- Domains,
- registrar,
- nameserver,
- Contacts,
  - Registrant,
  - admin contact,
  - tech contact,
  - billing contact.

3.1.2 DNR (Domain Name Registries) lekérdezése

- A cisco.com DNR lekérdezése a jogi szöveg (legal disclaimer) nélkül.

```
whois -H cisco.com
```

- .hu esetén: http://www.domain.hu/domain/domainsearch/

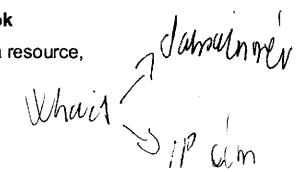
3.2. Regional Internet Registries (RIRs)

Olvasnivaló: https://www.arin.net/resources/services/whois_guide.html

Hely	Röv.	Név	URL
Észak-Amerika	ARIN	American Registry for Internet Numbers	https://whois.arin.net/ui/
Európa	RIPE	Réseaux IP Européens	http://www.ripe.net/whois
Ázsia, Óceánia	APNIC	Asia Pacific Network Information Centre	http://wq.apnic.net/apnic-bin/whois.pl
Afrika	AFRINIC	African Network Information Centre	http://www.afrinic.net/
Latin-Amerika és Karibi térség	LACNIC	Latin America and Caribbean Network Information Centre	http://www.lacnic.net/

3.2.1 Lekérdezhető adatok

- Organizations holding a resource,
- contacts
- IP addresses
- ASNs



3.2.2 RIR (Regional Internet Registries) lekérdezése

- A www.cisco.com RIR lekérdezése

```
whois 72.163.4.161
```

- Windowson ezt érdemes telepíteni: https://docs.microsoft.com/en-gb/sysinternals/downloads/whois

---

4. netcraft.com

- A https://www.netcraft.com/ oldalon a "What's that site running?" alatti szövegmezőbe:

```
cisco.com
```

Eredmények itt: https://searchdns.netcraft.com/?host=cisco.com&x=0&y=0

- A netcraft.com működése függ attól, hogy a bemenet tartalmaz-e aldomént is (pl. **www**.cisco.com).
  - Aldomén esetén ide továbbít: https://toolbar.netcraft.com/site_report?url=http://www.cisco.com ,
  - aldomén nélkül ide: https://searchdns.netcraft.com/?host=cisco.com&x=0&y=0

---

5. recon-ng

- Indítás:

```
recon-ng
```

- Whois_poc: nevek, emailcímek

```
use recon/domains-contacts/whois_pocs
```

```
show options
```

```
set SOURCE cisco.com
```

```
run
```

- Xssed: ismert cross-site scripting (XSS) sérülékenységek

```
use recon/domains-vulnerabilities/xssed
```

```
set SOURCE cisco.com
```

```
run
```

- google_site_web: aldomének keresése.

```
use recon/domains-hosts/google_site_web
```

```
set SOURCE cisco.com
```

```
run
```

---

6. Feladat

Válaszold meg az alábbi kérdéseket az órán kihúzott cégről.

1. Milyen doménnevei vannak?
2. Melyik hálózaton (IP cím tartományon) van a webszervere? Ha több van, válassz egyet.
3. Gyűjts ki 5, az adott szervezethez tartozó emailcímet.
