**Sarcina nr.1:**

Obtinerea de informatii utile in desfasurarea atacurilor:

* Adresele IP externe ale companiei tinta (+ ISP-ul)
* Subdomenii alocate
* Numere de telefon si adrese de email ale angajatilor
* Profile ale angajatilor (site-uri de socializare)
* Metadate in documentele publice
* Statii si servicii active in retea (pentest intern)
* Statii pornite in retea (live hosts)
* Porturi deschise
* Versiuni ale serviciilor care ruleaza
* Sistemul de operare
* Network shares
* Local users

**Activitate pasiva – nu se interactioneaza cu tinta**

 Subdomenii alocate

 Numere de telefon si adrese de email ale angajatilor

 Profile ale angajatilor (site-uri de socializare)

 Metadate in documentele publice

 Statii si servicii active in retea (pentest intern)

**Exemple:**

 Google hacking (Google Dorks - <https://www.exploit-db.com/google-hacking-database>)

Exercitii

1. Cautati toate fisierele de tip *xls* ce pot fi accesate de pe site-ul *xyz*

2. Verificati daca pe site-ul *xyz* se poate face directory browsing

3. Gasiti adrese de email ale angajatilor din firma *xyz*

4. Cautati toate posturile pe site-ul *softpedia.com* ale unei persoane gasite

la cautarea anterioara

5. Gasiti subdomenii ale domeniului *xyz*

6. Faceti o cautare dupa expresia: *mysql dump filetype:sql* . Ce obtineti?

7. Cautati camere live pe web: *inurl:/view/index.shtml*

*inurl:viewerFrame?Mode=*

 Interogari Whois - Se pot obtine informatii despre compania tinta precum:

1. Servere de nume

2. Intervalul de adrese IP alocat

3. Locatia si adresa firmei

4. Persoane de contact (nume, telefon, email)

**Exemplu:**

whois cisco.com

whois 128.107.241.185

**Exercitiu:**

Identificati spatiile de adrese IP alocate firmei *xyz*

 Interogari DNS

Utilitare: *dig, host, nslookup*

Tipuri de inregistrari DNS: *A, NS, MX, PTR, AXFR*, etc

**Exercitii:**

1. Care sunt serverele de nume ale domeniului *xyz*?

2. Pentru fiecare server de nume descoperit anterior, faceti cerere de

transfer de zona (type=axfr)

 Baze de date publice: Netcraft.com , zone-h.com

 Inspectare site web

 Network Sniffing

**Sarcina nr.2:**

Descoperirea vulnerabilitatilor (cite 1 de pe fiecare portal) si descrierea lor succinta cum ar putea fi folosita pentru a realiza o amenintare si cum poate fi prevenita:

În bazele de vulnerabilități, in functie de serviciul descoperit - <http://www.securityfocus.com/bid>, <http://www.kb.cert.org/vuls/>, <http://nvd.nist.gov/>, <http://osvdb.org/> sau utilizând unul din scannere de vulnerabilitati - Nessus, OpenVAS, QualisGuard, GFI LANGuard, Retina Nikto, w3af, Paros, BurpSuite, WebScarab, DirBuster

**Sarcina nr.3:**

Teste PHISHING /SI :

* Sarcina 1. **PHISHING QUIZ** disponibil pe <https://www.security.org/resources/something-smells-phishy/> (la sf. articolului)
* Sarcina 2. Testul propus de Google <https://phishingquiz.withgoogle.com/?fbclid=IwAR3NHUzNsz5NsCMYTEWVabltbFZt0DM1HHsa6IVTWd1Q49ng6rhLWIKr2v8>
* Sarcina 3. <https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/quiz/phishing>

**Sarcina nr.4:**

1. Textul clar NUMAR este criptat ˆın ”Orice vant nu bate seara”. Sa se descrie sistemul

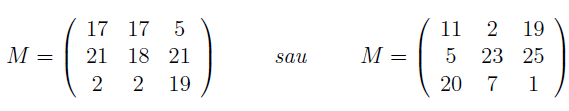
de criptare.

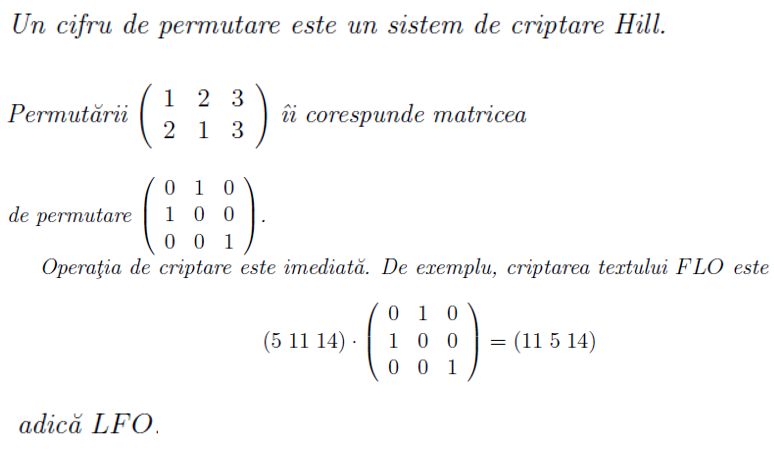
2 Folosind atacul prin forta bruta, decriptati mesajul WYPTBSJBYZ criptat cu un

sistem Cezar.

3. Sa se cripteze textul clar INAINTE SI LA DREAPTA folosind sistemul de criptare

Hill cu matricea





4. Consider˘am urm˘atorul cifru de permutare: Se fixeaz˘a numerele naturale p, q. Textul

clar se ˆımparte ˆın blocuri de cˆate p· q caractere. Fiecare astfel de bloc se scrie pe liniile

unei matrici de p linii ¸si q coloane. Criptarea blocului se realizeaz˘a scriind aceste matrici

pe coloane.

De exemplu, pentru p = 3, q = 4, textul clar MAINI CURATE se scrie

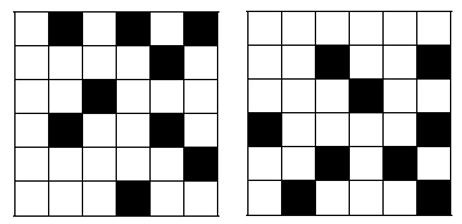
M A I N

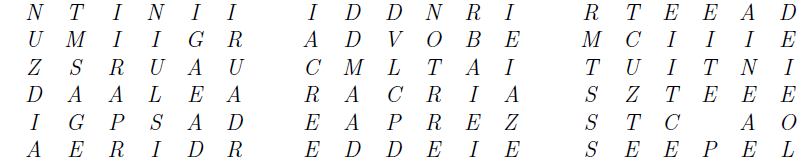
I C U R

A T E X

(textul s-a completat cu litera X). Textul criptat va fi MIAACTIUENRX.

Decriptat¸i urm˘atorul text DJNOUDNAINPAPANONZ criptat ˆıntr-un mod similar

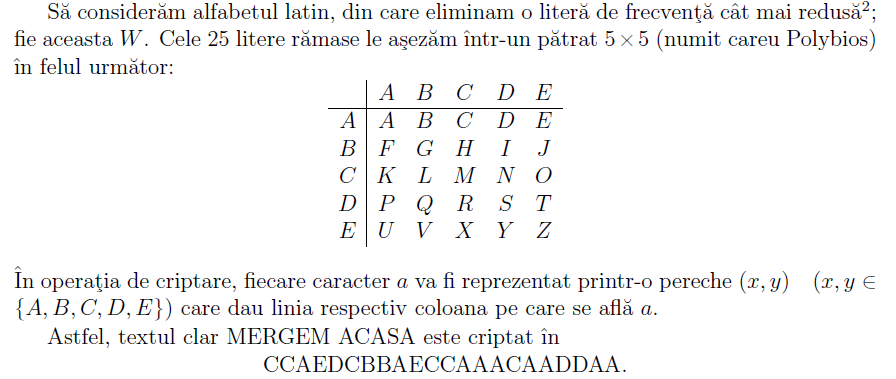
5. Sa se decripteze mesajul¸ stiind ca a fost criptat cu matricea Richelieu



6. S-a receptionat mesajul ARAU RIRU ITAA URIR EESU URAP IUTE IRI

Despre el, criptanalistul are urm˘atoarele informat¸ii: s-a folosit un careu de criptare

tip Polybios, precum ¸si cuvantul cheie STROP. Sa se decripteze mesajul.



**Sarcina nr.5:**

**Sistemul de management al securitarii informatiei conform ISO 27001**

<https://advisera.com/insight/chatbot-tool-iso-27001-scope/>

<https://advisera.com/27001academy/free-tools/free-return-security-investment-calculator/>

<https://advisera.com/insight/quiz-iso-27001-requires-passwords-to-be-changed/>

<https://advisera.com/insight/quiz-iso-27001-requires-each-security-control-to-be-documented/>

<https://advisera.com/insight/iso-27001-2013-to-iso-27001-2022-conversion-tool/>