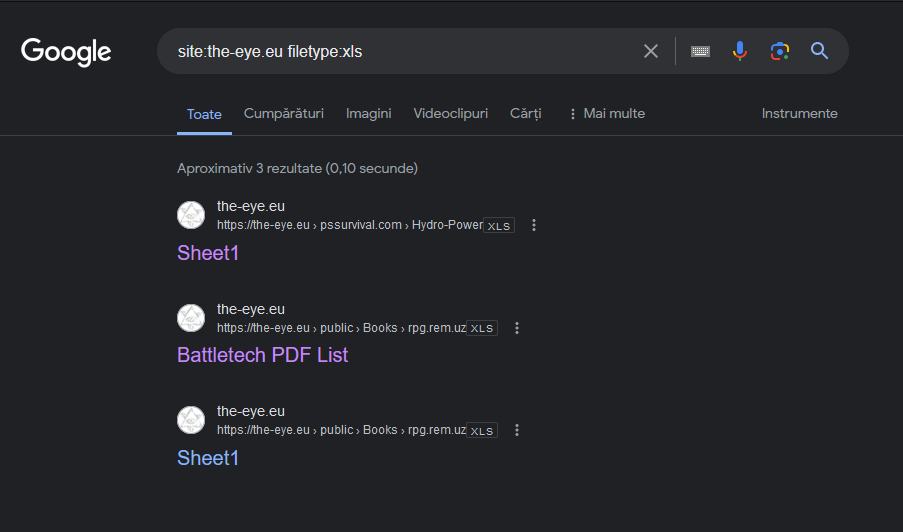
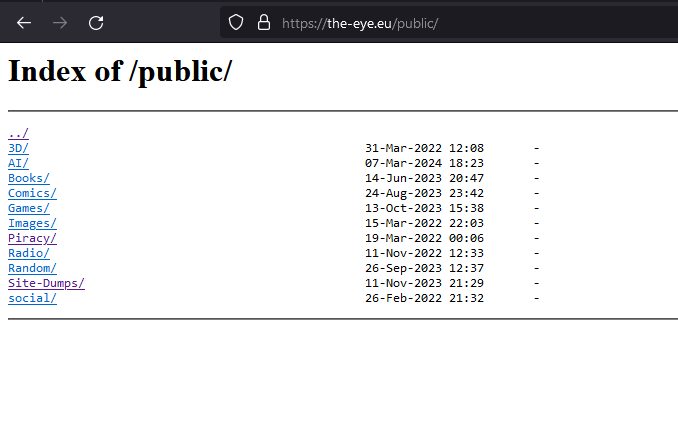
Sarcina nr 1

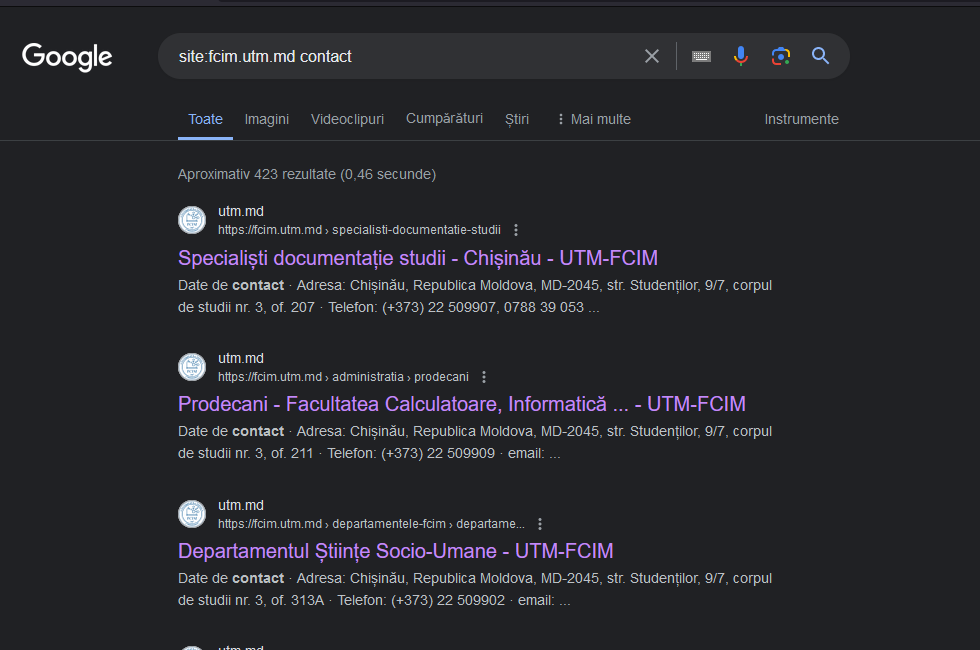
1. Cautati toate fisierele de tip *xls* ce pot fi accesate de pe site-ul *xyz*



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

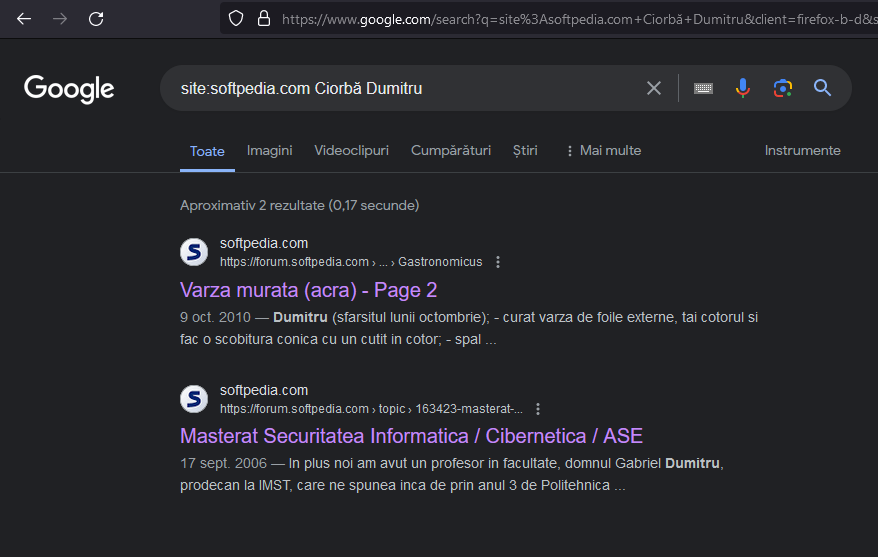


3. Gasiti adrese de email ale angajatilor din firma *xyz*



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

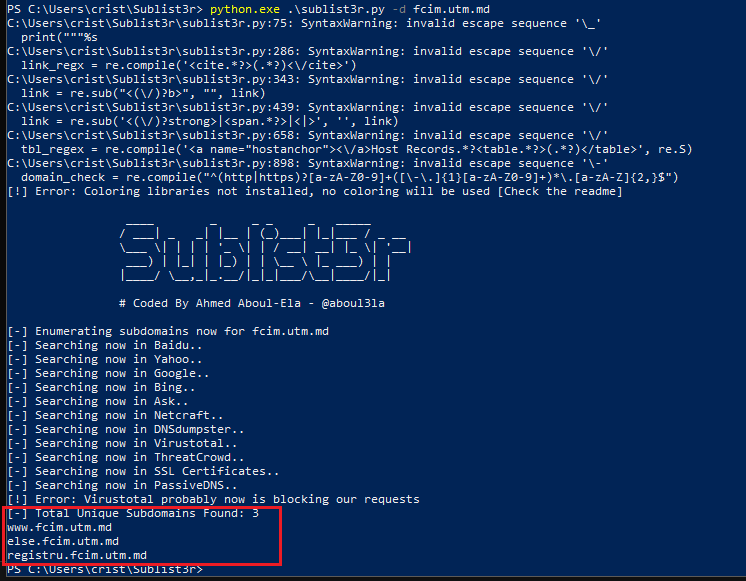
la cautarea anterioara



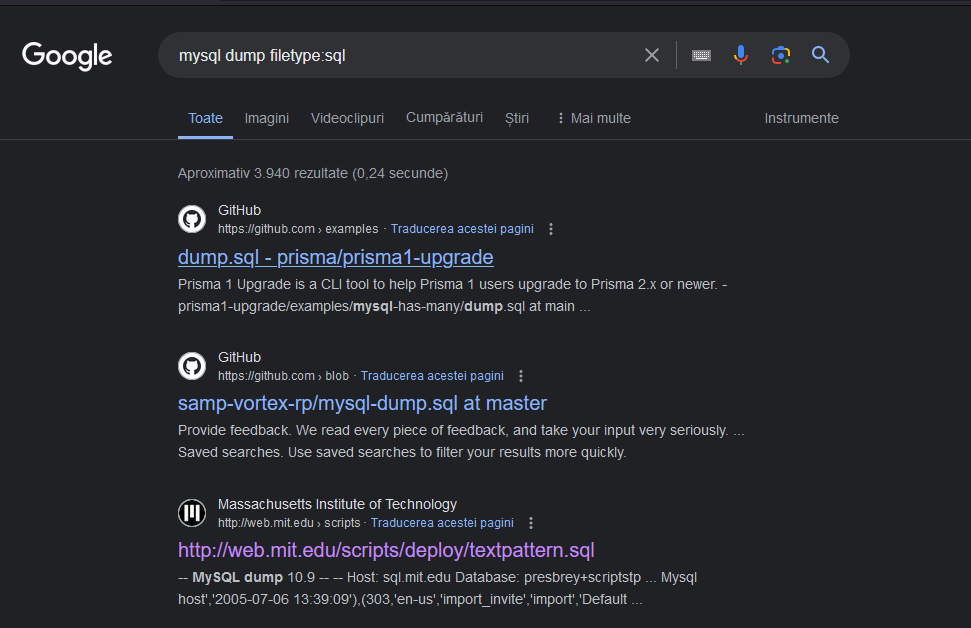
5. Gasiti subdomenii ale domeniului *xyz*

Pentru a gasi subdomenii ale fcim.utm.md, am folosit instrumentul open-source **Sublist3r** scris in Python   
Pentru aceasta, am folosit comanda

> python.exe .\sublist3r.py -d fcim.utm.md



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

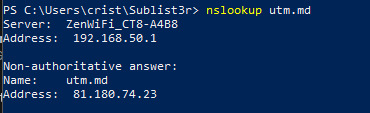


7. Cautati camere live pe web: *inurl:/view/index.shtml*

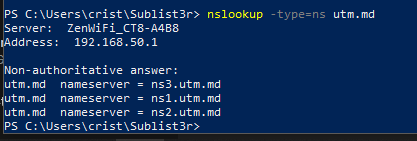
*inurl:viewerFrame?Mode=*

In urma cautarii am gasit site-ul web https://www.webcamplaza.net/  

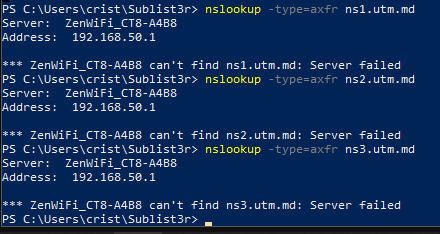

Identificati spatiile de adrese IP alocate firmei *xyz*



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)



Sarcina 2

Vulnerabilitate VU#488902 de pe <http://www.kb.cert.org/vuls/>

Descriere: CPU hardware care utilizează execuția speculativă poate fi vulnerabil la race condition (condiție de cursă).

Un atacator cu acces la resursele CPU poate citi date privilegiate arbitrare sau valori ale registrului de sistem utilizând condiția de cursă, denumită condiție de cursă speculativă. Hardware-ul CPU care utilizează execuția speculativă care este vulnerabil la Spectre v1 este probabil afectat. Un atacator neautentificat poate exploata această vulnerabilitate pentru a dezvălui date arbitrare de la CPU folosind condiții de cursă pentru a accesa căile de cod executabil speculativ. Cercetătorii de securitate au etichetat această variantă a vulnerabilității Spectre v1 „GhostRace”, pentru ușurința comunicării.

Soluție: Utilizatorii trebuie să-și actualizeze software-ul conform recomandărilor furnizorilor respectivi cu cele mai recente atenuări disponibile pentru a aborda această vulnerabilitate și variantele acesteia.

Vulnerabilitatea CVE-2024-2815 de pe <http://nvd.nist.gov/>

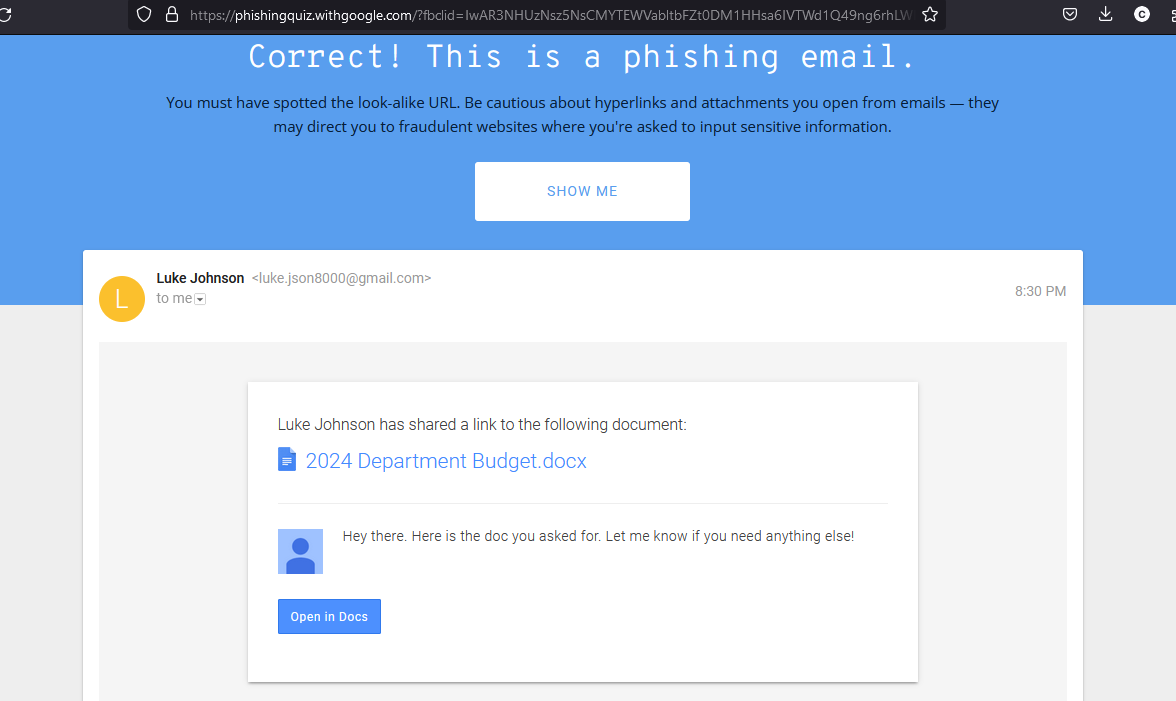
Descriere: O vulnerabilitate clasificată ca critică a fost găsită în Tenda AC15 15.03.20\_multi. Afectată este funcția R7WebsSecurityHandler a fișierului /goform/execCommand a componentei Cookie Handler. Manipularea parolei argument duce la depășirea tamponului bazat pe stivă. Este posibil să lansați atacul de la distanță.

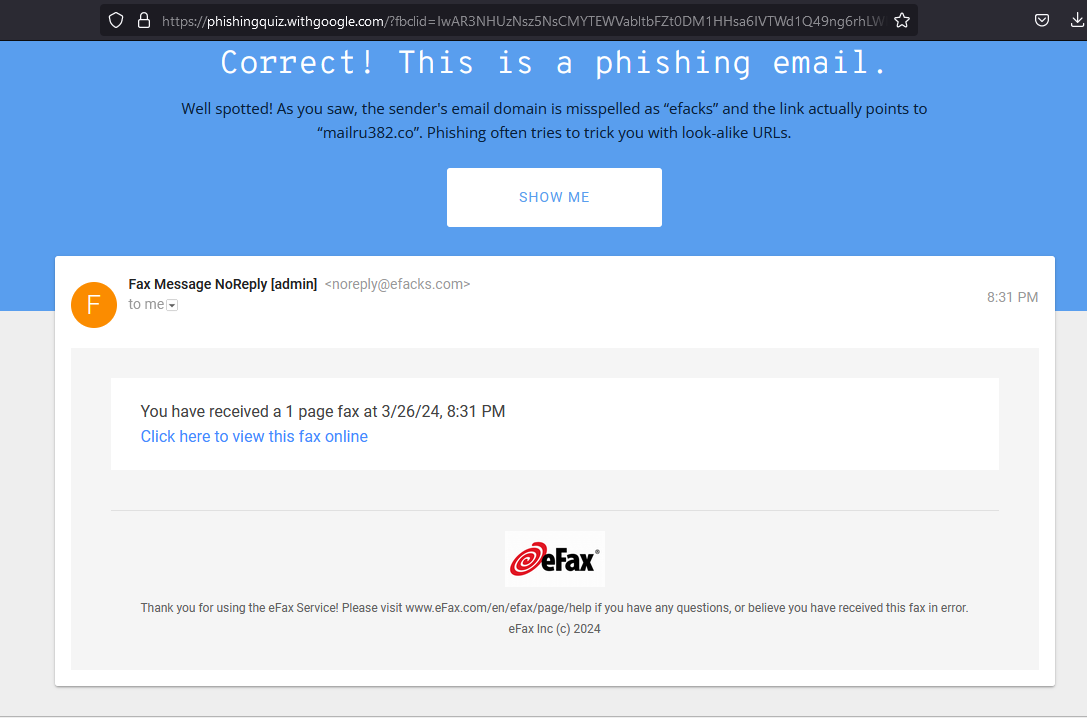
Firmware-ul Tenda AC15 V15.03.05.18 are o vulnerabilitate de depășire a stivei în funcția R7WebsSecurityHandler. Variabila src primește parametrul de parolă dintr-o solicitare POST și este atribuită ulterior variabilei v35, care este fixată la 128 de octeți. Cu toate acestea, deoarece utilizatorul poate controla introducerea parolei, instrucțiunea strcpy(v35, src); poate provoca o depășire a buffer-ului. Parola furnizată de utilizator poate depăși capacitatea matricei v35, declanșând această vulnerabilitate de securitate.

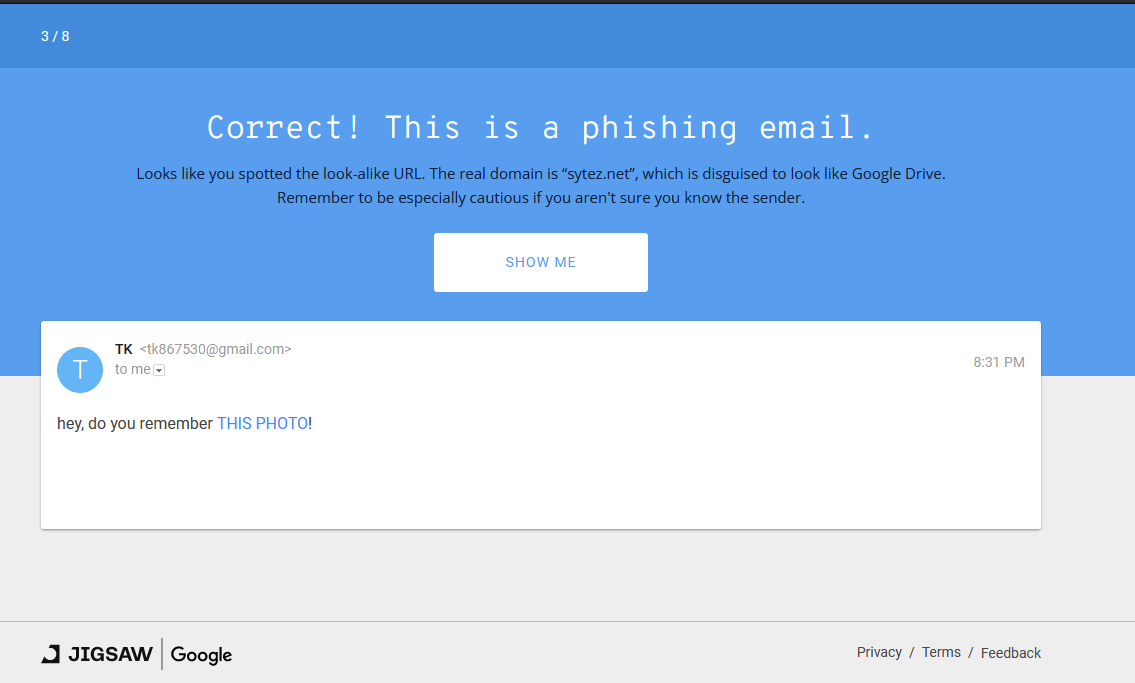
Soluție: Utilizatorii sunt îndemnați să pună versiunea actualizată a firmware-ului.

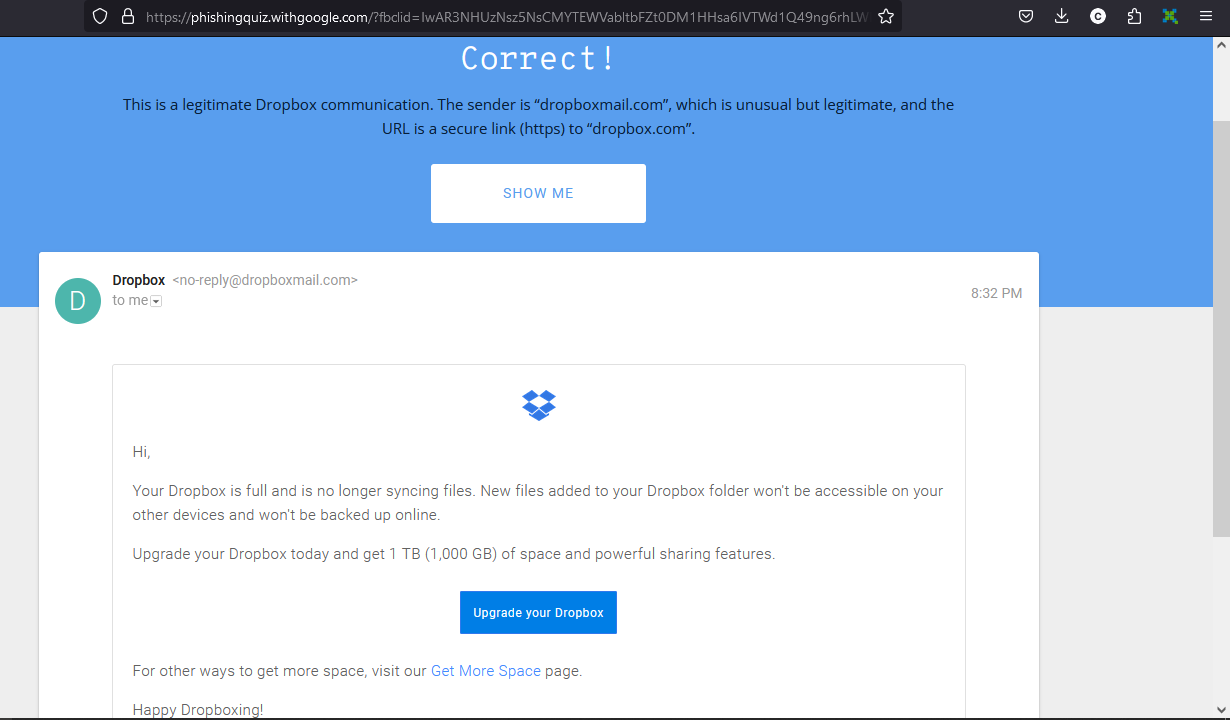
Sarcina nr 3

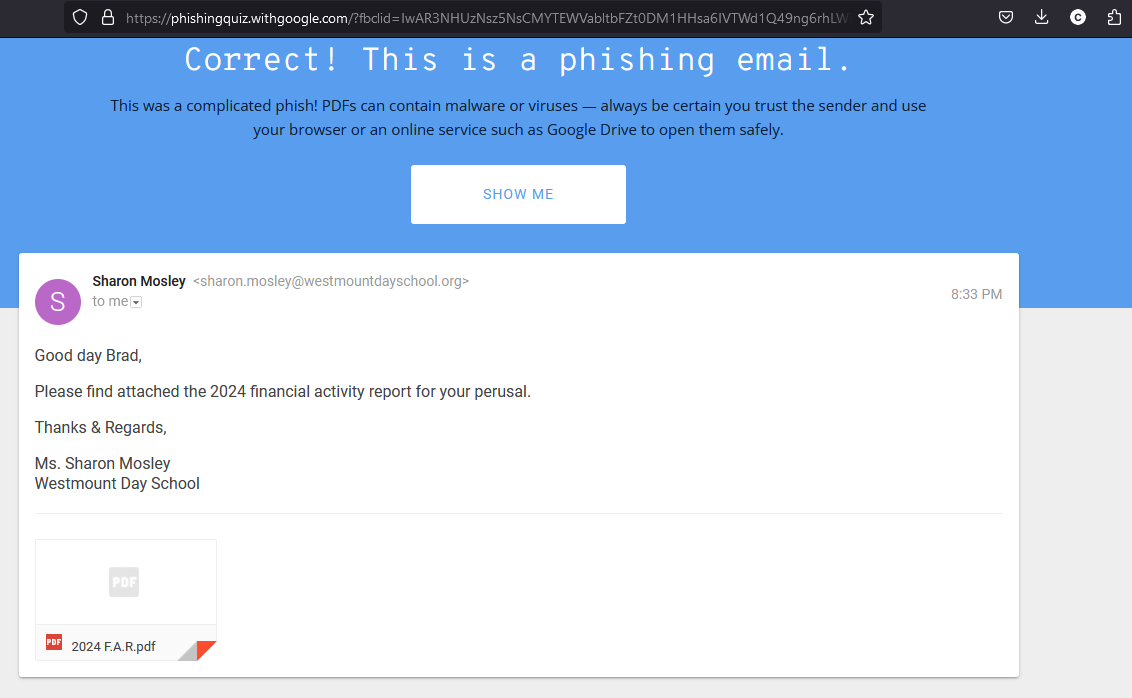
2. Testul propus de Google

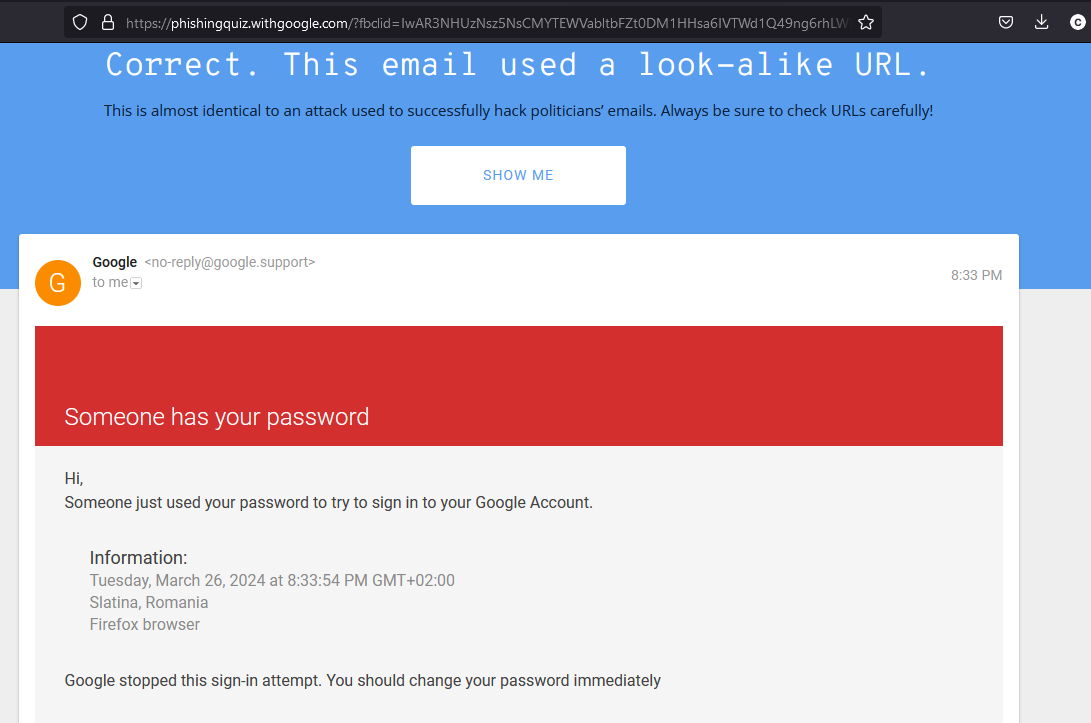


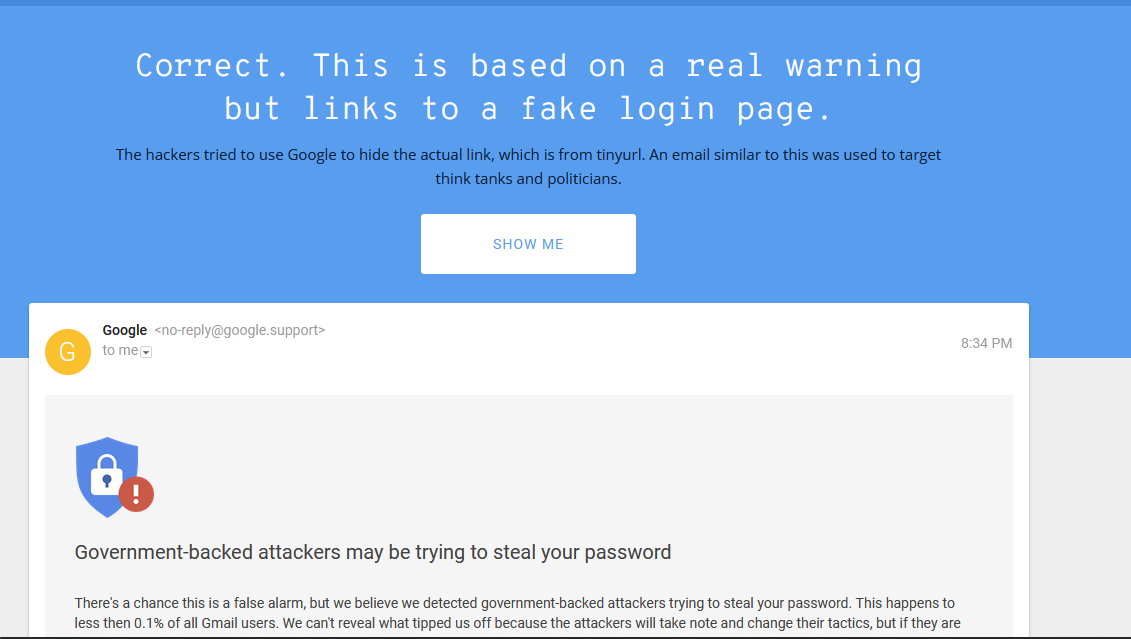


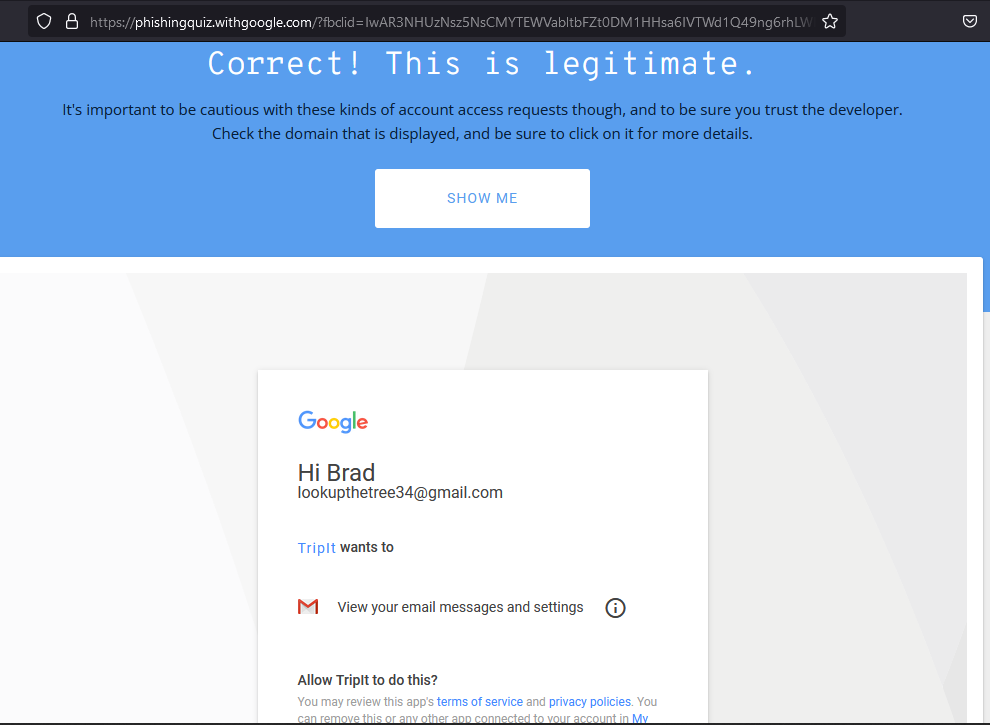




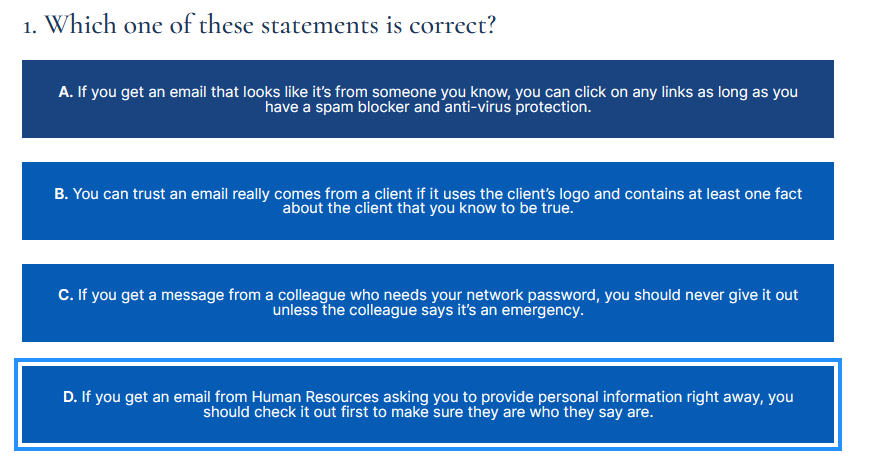


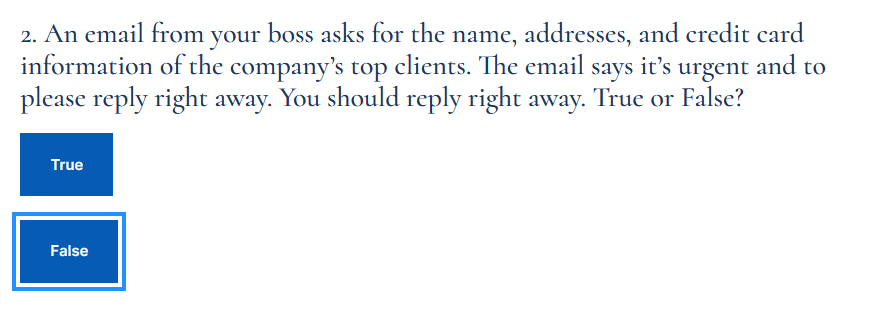


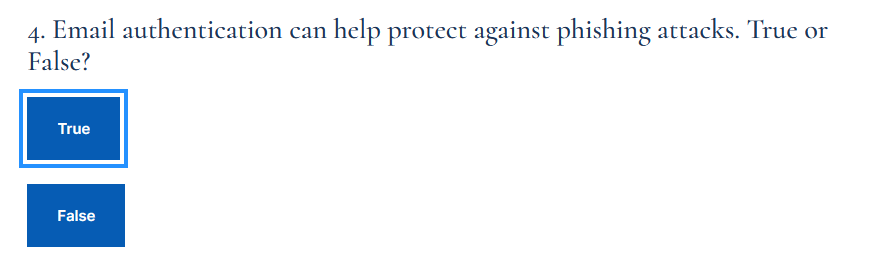
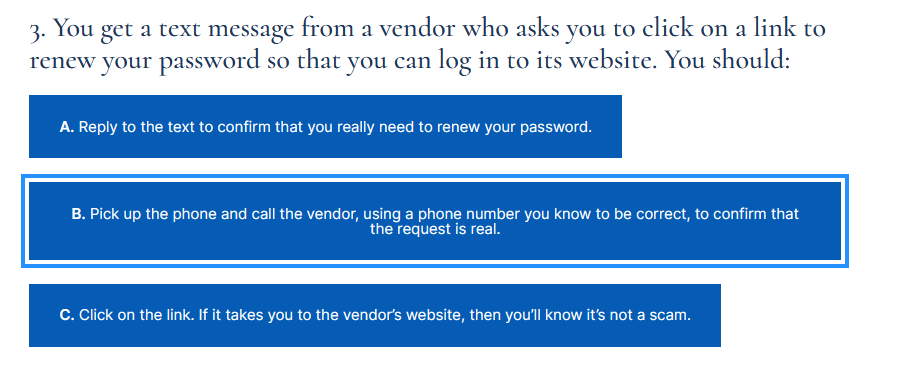


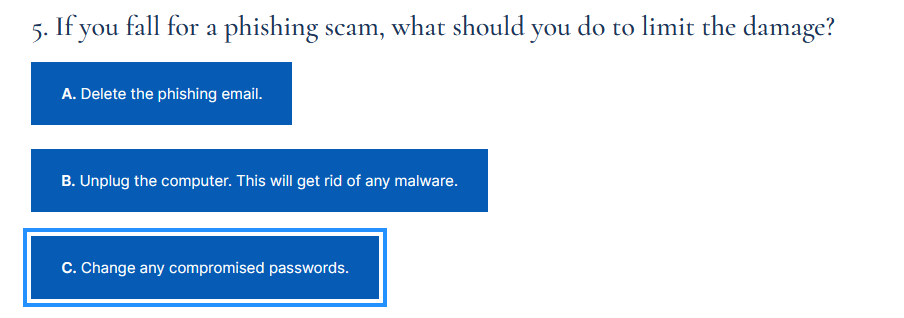


3









Sarcina nr4

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

Este folosit un tip de criptare de substituție în care fiecare literă din textul simplu este înlocuită cu un cuvânt corespunzător din textul cifrat. Astfel,

„N” corespunde cu „Orice”

„U” corespunde cu „vant”

„M” corespunde cu „nu”

„A” corespunde cu „bate”

„R” corespunde cu „seara”

1. Folosind atacul prin forta bruta, decriptati mesajul WYPTBSJBYZ criptat cu un sistem Cezar.

În cazul unui alfabet standard de 26 de litere, există 25 de posibile deplasări (de la 1 la 25).

Deplasare 1: VXOSARIAXY

Deplasare 2: UWNRZQHZWX

Deplasare 3: TVMQYPGYVW

Deplasare 4: SULPXOFXUV

Deplasare 5: RTKOWNEWTU

Deplasare 6: QSJNVMDVST

Deplasare 7: PRIMUMCURS

Deplasare 8: OQHLTLBTQR

Deplasare 9: NGGKSKASPQ

Deplasare 10: MFFJRJZROP

Deplasare 11: LEEIQIYQNO

Deplasare 12: KDDHPHXPNM

Deplasare 13: JCCGOGWOML

Deplasare 14: IBBFNFVNLK

Deplasare 15: HAAEMEUMKJ

Deplasare 16: GZZDLDTLJI

Deplasare 17: FYYCKCSKIH

Deplasare 18: EXXBJBRJHG

Deplasare 19: DWWAIQQIGF

Deplasare 20: CVVZHPPHFE

Deplasare 21: BUUGGOOGED

Deplasare 22: ATTFFNNFDC

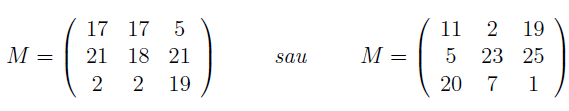
Deplasare 23: ZSSEEMMECB

Deplasare 24: YRRDDLLDBA

Deplasare 25: XQQCCKKCZA

Cel mai evident cuvânt existent este la încercarea 7: PRIMUMCURS

1. Sa se cripteze textul clar INAINTE SI LA DREAPTA folosind sistemul de criptare Hill cu matricea



1. Asociem fiecare literă din text cu numărul corespunzător de ordine din alfabet

I = 8, N = 13, A = 1, T = 20, E = 5, S = 19, L = 12, D = 4, R = 18, P = 16

1. Împărțim textul clar în grupuri de câte trei litere

"INA", "INT", "ESI", "LAD", "REA", "PTA"

1. Convertim fiecare grup cu vectorul de numere corespunzător

"INA" devine [8, 13, 0]

"INT" devine [8, 13, 19]

"ESI" devine [4, 18, 8]

"LAD" devine [11, 0, 3]

"REA" devine [17, 4, 0]

"PTA" devine [15, 19, 0]

1. Înmulțim fiecare vector de litere cu matricea de criptare M

"INA" devine [ 423, 385, 320 ]

"INT" devine [ 609, 599, 706 ]

"ESI" devine [ 592, 553, 423 ]

"LAD" devine [ 213, 213, 74 ]

"REA" devine [ 433, 427, 169 ]

"PTA" devine [ 475, 472, 380 ]

1. Împărțim fiecare element al vectorului rezultat la 26 și reținem restul

Exemplu: pentru "INA"

423 devine 423 mod 26 = 21,

385 devine 385 mod 26 = 15,

320 devine 320 mod 26 = 16

1. Asociem fiecărui număr rezultat o literă din alfabetul englezesc

21 = V

15 = P

16 = Q

Textul criptat:

"INA" devine "VPU"

"INT" devine "VSQ"

"ESI" devine "FSR"

"LAD" devine "SQN"

"REA" devine "PSM"

"PTA" devine "VPZ"

"INAINTE SI LA DREAPTA" criptat folosind matricea M este "VPUVSQFSRSQNPSMVPZ"

1. Consideram urmatorul cifru de permutare: Se fixeaza numerele naturale p, q. Textul clar se ımparte ın blocuri de cate p· q caractere. Fiecare astfel de bloc se scrie pe liniile unei matrici de p linii ¸si q coloane. Criptarea blocului se realizeaza 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.

Decriptati urmatorul text DJNOUDNAINPAPANONZ criptat ıntr-un mod similar

Impartim textul criptat in matrice 3x6

D O N N P O

J U A P A N

N D I A N Z

Textul decriptat este DONNPOJUAPANNDIANZ

Impartim textul criptat in matrice 2x9  
D N U N I P P N N

J O D A N A A O Z

Textul decriptat este DNUNIPPNNJODANAAOZ

Impartim textul criptat in matrice 6x3

D N P

J A A

N I N

O N O

U P N

D A Z

Textul decriptat este DNPJAANINONOUPNDAZ

Impartim textul criptat in matrice 9x2

D N

J P

N A

O P

U A

D N

N O

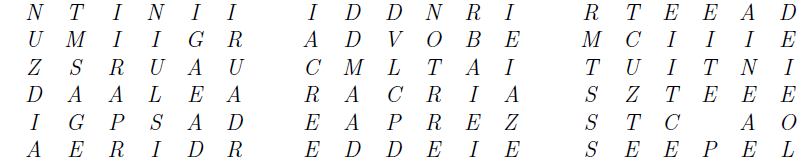
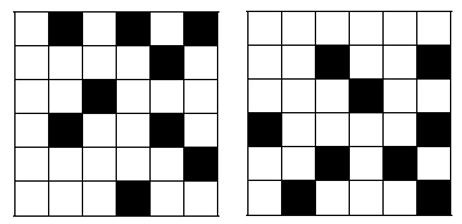
A N

I Z

Textul decriptat este DNJPNAOPUADNNOANIZ

Nicio varianta nu are sens

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

La prima aplicare a matricei, obtinem   
T N I G R A E D I

La a doua

I R U D A P A E R

La a treia

I U S A L G A R D

1. S-a receptionat mesajul ARAU RIRU ITAA URIR EESU URAP IUTE IRI Despre el, criptanalistul are urmatoarele informatii: s-a folosit un careu de criptare tip Polybios, precum si cuvantul cheie STROP. Sa se decripteze mesajul.
2. Se construieste careul de criptare Polybios

S T R O P

A B C D E

F G H I K

L M N Q U

V W X Y Z

1. Identificăm cifrele corespunzătoare literelor în careul de criptare Polybios:

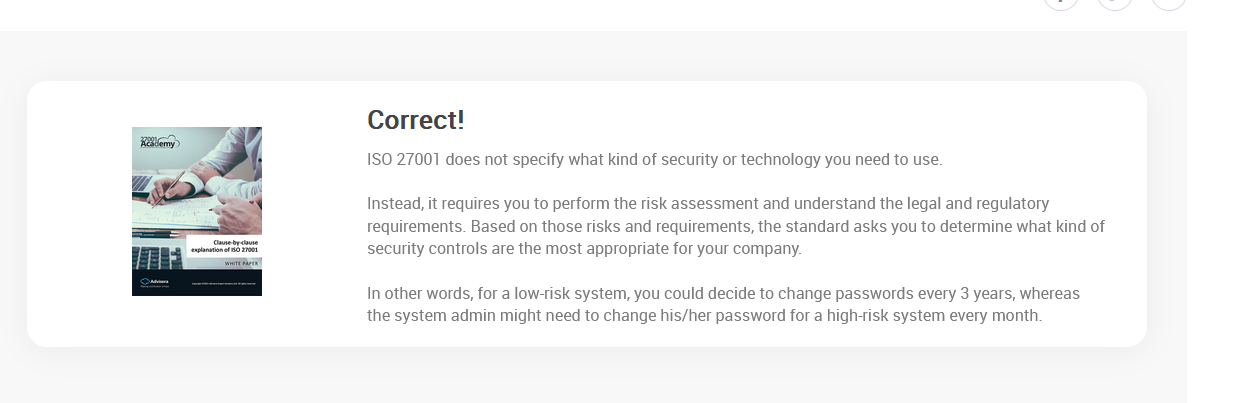
A = 11, R = 21, U = 35, I = 32, T = 31, E = 34, S = 11, P = 15, O = 12

1. Mesajul decriptat

SALUTAREPOTIFOSTCASTIGATJOCUL

Sarcina nr 5

ISO 27001 requires passwords to be changed



ISO 27001 requires each security control to be documented

