

Laborator 4

Securitatea Sistemelor Informatice

1.

A -> 4

B -> 2

C -> 1

D -> 3

E -> 6


F -> 5

2.

- Titlul este “mesaj important”.
- Email-ul a fost catalogat drept “junk” de catre serviciul de mail folosit.
- Sender-ul este “Home bank.ro”, neavand legatura cu ing.ro.
- Email-ul este primit de la mbm@externalys.net, nu de la o adresa cu numele de domeniu ing.ro.
- Aspect neingrijit al textului. (ex: litera mica la inceputul unui paragraph, “Telefon” scris pe un rand, iar numarul scris pe urmatorul etc.)
- Email-ul nu este semnat de o persoana concreta, ci de “ING Bank Romania”.
- In email apare link-ul “zozweb.com/RRO”, care nu are legatura cu ing.ro.

3.

Am folosit urmatorul email (catre un angajat al firmei Endava):

From Name: Endava IT 

From E-mail: it@endava.ro

To: qwewrrrsdfd@gmail.com

Subject: Schimbarea parolei contului dumneavoastra

Attachment: No file chosen
[Attach another file](#)

Content-Type: ☒ text/plain ☐ text/html ☐ Editor

Text: Bună ziua!

A fost sesizată o încercare de a schimba parola contului
dumneavoastră de institutional.
Pentru a ne asigura că dumneavoastră ati încercat să faceti
această schimbare, completati următorul formular cu numele
si parola contului dumneavoastră: formular.com
Odata completat acest formular, veti primi un email de
schimbare a parolei.

O zi frumoasă,
Echipa IT Endava.

Solve reCAPTCHA v2 instead of v3

Rezultat dupa introducerea header-ului pe <https://mha.azurewebsites.net/> :

Summary

Subject

Message Id

Creation time

From

Reply to

To

Schimbarea parolei contului dumneavoastra

<20211109220049.BD5E62872E@emkei.cz>

Tue, 9 Nov 2021 23:00:49 +0100 (CET) (Delivered after 1 second)

Endava IT <it@endava.ro>

it@endava.ro

qwewrrsdfd@gmail.com

Received headers

Hop↓	Submitting host	Receiving host	Time	Delay	Type ⇒
1		emkei.cz (Postfix, from user: id 33)	11/10/2021 12:00:49 AM		
2	emkei.cz (emkei.cz [101.99.94.116])	mx.google.com	11/10/2021 12:00:50 AM	1 second	ESMTPS
3		2002:a05:600c:21c7:0:0:0:0	11/10/2021 12:00:50 AM	0 seconds	SMTP

Other headers

#↓	Header	Value
1	Delivered-To	qwewrrsdfd@gmail.com
2	X-Google-Smtp-Source	ABdhPly8HcMRurTLf7Z6wiWgrynVxuHnCe88TpNfj9qtNqG2SLodmVTP4ml4XqQ8Ejd186rkS
3	X-Received	by 2002:a17:907:1693:: with SMTP id hc19mr14113829ejc.396.1636495250327; Tue, 09 Nov 2021 14:00:50 -0800 (PST)
4	ARC-Seal	i=1; a=rsa-sha256; t=1636495250; cv=none; d=google.com; s=arc-20160816; b=JNZNxyLZumvRxUtpOyh9ANjiNDIW4+aHd89ZmsEc3WuR1RACBwoX+R8GW/UbTEcaJS 9Gl6w5IZ+QDDHXI5zJyhLOUFADhbm66luoKagIghmmDKITPcC+zqQztC8C420L1Vp4UezulUxmJ2mkcgSxODLeWU4iLaDd+LEyVTS yfNw==
5	ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816; h=date:message-id:reply-to:errors-to:importance:from:subject;to; bh=Ki5A+KIQTq1zGyhHfDcNo64M9Hf9CCtwAY/SoA=: b=ChDX7SrypVDYEXS7IGs0veSH7NN W7HqYqms2V2 d5vEXStk6ao8WyQonyNkCT0y6aT896NcDJa/lakqcpZFkh/Pxm6coo 1aCCOpSxcmqkbS YqKmWtVvceKYDCHC+1WOMg5pbU6SK7w8BVPHDGc3UuQd7DK3cRNX3i13RbC0xpr14g8 0aQQ==
6	ARC-Authentication-Results	i=1; mx.google.com: spf=neutral (google.com: 101.99.94.116 is neither permitted nor denied by best guess record for domain of it@endava.ro) smtp.mailfrom=it@endava.ro
7	Return-Path	<it@endava.ro>
8	Received-SPF	neutral (google.com: 101.99.94.116 is neither permitted nor denied by best guess record for domain of it@endava.ro) client-ip=101.99.94.116;
9	Authentication-Results	mx.google.com: spf=neutral (google.com: 101.99.94.116 is neither permitted nor denied by best guess record for domain of it@endava.ro) smtp.mailfrom=it@endava.ro
10	X-Priority	3 (Normal)
11	Importance	Normal
12	Errors-To	it@endava.ro
13	Content-Type	text/plain; charset=utf-8

Rezultat dupa introducerea header-ului pe <https://toolbox.googleapps.com/apps/messageheader/> :

Message Id

20211109220049.BD5E62872E@emkei.cz

Created at:

11/10/2021, 12:00:49 AM GMT+2 (Delivered after 1 sec)

From:

Endava IT <it@endava.ro>

To:

qwewrrsdfd@gmail.com

Subject:

Schimbarea parolei contului dumneavoastra

SPF:

neutral with IP Unknown!
[Learn more](#)

#	Delay	From *	To *	Protocol	Time received
0	1 sec	emkei.cz	→ [Google] mx.google.com	ESMTPS	11/10/2021, 12:00:50 AM GMT+2
1			→ [Google] 2002:a17:907:1693::	SMTP	11/10/2021, 12:00:50 AM GMT+2
2			→ [Google] 2002:a05:600c:21c7:0:0:0:0	SMTP	11/10/2021, 12:00:50 AM GMT+2

Rezultat dupa introducerea IP-ului pe <https://dawhois.com/> :

Site Info new

Who Is

Trace Route

RBL Check

What's My IP?

Enter Domain Name or IP Address:

101.99.94.116

Whois

101.99.94.116 - Geo Information

Map Location new☒ [World Map](#) ☐ [Google Maps](#) ☐ [Yahoo Maps](#) ☐ [Microsoft Live Maps](#)

101.99.94.116 - Whois Information

Raspunsuri pentru intrebari:

- Daca atacul ar fi cu success, as obtine datele unei persoane din firma Endava si as putea obtine informatii confidentiale din interiorul firmei.
- SPF pentru email-ul trimis: *NEUTRAL* cu adresa IP 101.99.94.116
SPF pentru un email legitim: *PASS* cu adresa IP 172.82.230.59
DKIM pentru email-ul trimis: -
DKIM pentru un email legitim: '*PASS*' cu domeniul *m1.email.samsung.com*
DMARC pentru email-ul trimis: -
DMARC pentru un email legitim: '*PASS*'