

Фишинг с gophish

Клонирование репозитория

```
ildar@debian:~/ZIS/Phishing$ git clone https://github.com/Ivanhahanov/InformationSecurityMethodsAndTools.git
Cloning into 'InformationSecurityMethodsAndTools'...
remote: Enumerating objects: 916, done.
remote: Counting objects: 100% (916/916), done.
remote: Compressing objects: 100% (723/723), done.
remote: Total 916 (delta 169), reused 876 (delta 136), pack-reused 0
Receiving objects: 100% (916/916), 40.39 MiB | 5.85 MiB/s, done.
Resolving deltas: 100% (169/169), done.
ildar@debian:~/ZIS/Phishing$
```

Запуск контейнера

```
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing$ ls
docker-compose.yml  Gophish  MailServer  README.md
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing$ docker-compose up -d
Creating network "phishing_default" with the default driver
Creating volume "phishing_maildata" with default driver
Creating volume "phishing_mailstate" with default driver
Creating volume "phishing_maillogs" with default driver
Pulling mailserver (tvial/docker-mailserver:latest)...
latest: Pulling from tvial/docker-mailserver
a076a628af6f: Pull complete
b5afddf182ca: Pull complete
5ebe891e3bb9: Pull complete
6884ed77b465: Pull complete
a7f3ed9aa5e0: Pull complete
67f2c647b931: Pull complete
957fffd1ae7c: Pull complete
1c4b0df1cd9e: Pull complete
```

Создание сертификатов

```
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing$ docker run -it --rm -v "$(pwd)"/config/ssl:/tmp/docker-mailserver-ssl-certificate
CA certificate filename (or enter to create)

Making CA certificate ...
=====
openssl req -new -keyout ./demoCA/private/cakey.pem -out ./demoCA/careq.pem
Generating a RSA private key
.....+++++
.....+++++
writing new private key to './demoCA/private/cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:Moscow
Locality Name (eg, city) []:Moscow
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MIREA
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:domain.com
Email Address []:admin@domain.com
```

Создание пользователей с пересборкой контейнера

```
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing/MailServer$ ls
config mailserver.env setup.sh
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing/MailServer$ chmod +x setup.sh
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing/MailServer$ ./setup.sh -i tvial/docker-mailserver:latest email add
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing/MailServer$ ./setup.sh -i tvial/docker-mailserver:latest email add
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing/MailServer$ ./setup.sh -i tvial/docker-mailserver:latest email list
admin@domain.com
user@domain.com
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing/MailServer$ docker-compose up --build -d
Starting mail ... done
Starting gophish ... done
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing/MailServer$
```

Тестирование SMTP с помощью swaks

```
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing/MailServer$ swaks --from admin@domain.com --to user@domain.com
23 --header "Subject: test from admin" --body "testing 123"
=== Trying 127.0.0.1:587...
=== Connected to 127.0.0.1.
<- 220 mail.domain.com ESMTP
-> EHLO debian
<- 250-mail.domain.com
<- 250-PIPELINING
<- 250-SIZE 10240000
<- 250-ETRN
<- 250-STARTTLS
<- 250-ENHANCEDSTATUSCODES
<- 250-8BITMIME
```

Sending profile

Edit Sending Profile ×

Name:

Interface Type:

SMTP

SMTP From: ?

Host:

Username:

Password:

☒ Ignore Certificate Errors ?

Email Headers:

Тестовое сообщение

Send Test Email

Send Test Email to:

Kevin

Mitnick

user@domain.com

SEO

Cancel

Send

Send Test Email

✓ Email Sent!

Send Test Email to:

Kevin

Mitnick

user@domain.com

SEO

Cancel

Send

Email Headers:

X-Custom-Header

{{.URL}}-gophish

+ Add Custom Header

Show 10 entries

Search:

Header	Value
No data available in table	

Showing 0 to 0 of 0 entries

Send Test Email

Cancel

Save Profile

Search:

3, 4:08:42 am

Previous

1

Next

Thunderbird

user@domain.com received 1 new message

Default Email from Gophish from admin@domain.com

It works! This is an email letting you k

Настройка почтового клиента ThunderBird

Manual configuration

INCOMING SERVER

Protocol:

IMAP

Hostname:

127.0.0.1

Port:

143

Connection security:

STARTTLS

Authentication method:

Normal password

Username:

user@domain.com

OUTGOING SERVER

Hostname:

127.0.0.1

Port:

143

Connection security:

STARTTLS

Authentication method:

Normal password

Username:

user@domain.com

Advanced config

Re-test

Cancel

Done

Настройка фишинговой страницы

Landing Pages

+ New Page

Show

10

entries

Name

Last Modified Date

tryhackme

November 28th 2023, 4:18:14 am

Showing 1 to 1 of 1 entries

Настройка шаблона фишингового письма

Edit Template

Name:

Admin support

✉ Import Email

Envelope Sender: ⓘ

admin@tryhackme.com

Subject:

Admin Support

Text HTML

Hello, {{.FirstName}} {{.LastName}}.
For security reasons you need to update password in {{.URL}}.

Best regards,
Tryhackme Support

☐ Add Tracking Image

Настройка получателей рассылки

New Group

Name:

test

+ Bulk Import Users

📄 Download CSV Template

First Nam

Last Nam

Email

Position

+ Add

Show 10 entries

Search:

First Name	Last Name	Email	Position	
Admin	Admin	admin@domain...	admin	🗑
Ildar	Iskyandyarov	user@domain.c...	user	🗑

Showing 1 to 2 of 2 entries

Previous 1 Next

Close

Save changes

Запуск фишинговой кампании

New Campaign

Name:

MyCompany

Email Template:

Admin support

Landing Page:

tryhackme

URL: ?

http://192.168.244.131

Launch Date

November 28th 2023, 4:24 am

Send Emails By (Optional) ?

Sending Profile:

admin

Send Test Email

Groups:

× test

Полученное сообщение

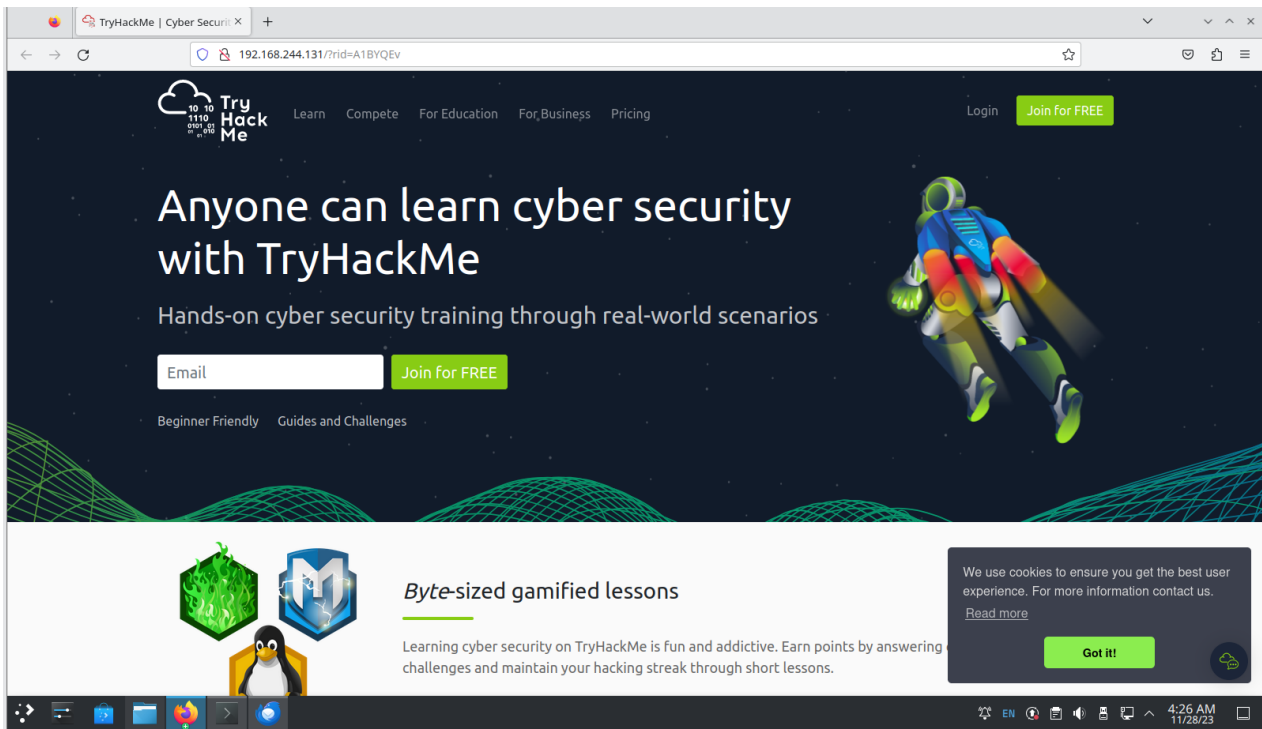
The screenshot shows an email client interface. On the left is a sidebar with folders: 'user@domain.com' (Inbox, Drafts, Sent, Junk, Trash) and 'Local Folders' (Trash, Outbox). The main pane shows an inbox list with the following entries:

From	Time	Subject
admin@domain.com	04:01	test from admin
admin@domain.com	04:15	Default Email from Gophish
admin@tryhackme.com	04:25	Admin Support

The selected email is from 'admin@tryhackme.com' with the subject 'Admin Support'. The email body contains the following text:

Hello, Ildar Iskyandyarov.
For security reasons you need to update password in <http://192.168.244.131?rid=A1BYQEv>.
Best regards,
Tryhackme Support

Переход по ссылке из письма



Статистика запущенной кампании

