

WHAT IS SOCIAL ENGINEERING

Social Engineering with AI

Cybersecurity & Ethical Hacking

Matteo Mattia

INDICE GENERALE

INTRODUZIONE

PARTE I: [OFFICIAL] Attacchi di Phishing

1. Gophish
2. SET - Social Engineering Toolkit

PARTE II: [FACOLTATIVO] ChatGPT - Analisi Email di Phishing

CONCLUSIONE

INTRODUZIONE

In questo laboratorio ho esplorato le tecniche di ingegneria sociale utilizzate dagli attaccanti per compromettere la sicurezza informatica.

Ho utilizzato strumenti professionali come **Gophish** e **SET (Social Engineering Toolkit)** per comprendere come vengono condotte le campagne di phishing e quanto sia facile ingannare gli utenti con i giusti strumenti.

PARTE I: [OFFICIAL] Attacchi di Phishing

Il phishing è una delle tecniche di attacco più diffuse e pericolose.

Consiste nell'ingannare la vittima facendole credere di interagire con un servizio legittimo, quando in realtà sta fornendo le proprie credenziali a un attaccante.

Gli elementi chiave di un attacco di phishing includono:

- Email convincenti che imitano comunicazioni ufficiali
- Landing page false che replicano siti web autentici
- Tecniche di social engineering per creare urgenza o fiducia

1. Gophish

Gophish è un framework open-source per la simulazione di campagne di phishing.

L'ho installato su Windows 10 e configurato per creare una campagna di test.

Installazione e Configurazione

Durante l'installazione ho riscontrato un errore sulla porta 80, che ho risolto modificando il file di configurazione:

```
Directory di C:\Users\user\Desktop\gophish-v0.12.1-windows-64bit
14/12/2025 12:29 <DIR> .
14/12/2025 12:29 <DIR> ..
14/12/2025 12:29 460 config.json
14/12/2025 12:29 <DIR> db
14/12/2025 12:29 122.889 gophish.db
14/12/2025 12:29 34.590.314 gophish.exe
14/12/2025 12:29 1.115 LICENSE
14/12/2025 12:29 3.285 README.md
14/12/2025 12:29 <DIR> static
14/12/2025 12:29 <DIR> templates
14/12/2025 12:29 7 VERSION
6 File 34.718.061 byte
5 Directory 18.541.088.768 byte disponibili

C:\Users\user\Desktop\gophish-v0.12.1-windows-64bit>cd %USERPROFILE%\Desktop\gophish-v0.12.1-windows-64bit
C:\Users\user\Desktop\gophish-v0.12.1-windows-64bit>notepad config.json

C:\Users\user\Desktop\gophish-v0.12.1-windows-64bit>gophish.exe
time="2025-12-14T12:32:02+01:00" level=warning msg="No contact address has been configured."
time="2025-12-14T12:32:02+01:00" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: no migrations to run, current version: 20220321133237
time="2025-12-14T12:32:02+01:00" level=info msg="Please login with the username admin and the password cbdfc2beb436f6df"
time="2025-12-14T12:32:02+01:00" level=info msg="Starting admin server at http://127.0.0.1:3333"
time="2025-12-14T12:32:02+01:00" level=info msg="Starting IMAP monitor manager"
time="2025-12-14T12:32:02+01:00" level=info msg="Starting new IMAP monitor for user admin"
time="2025-12-14T12:32:02+01:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2025-12-14T12:32:02+01:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2025-12-14T12:32:02+01:00" level=fatal msg="listen tcp 0.0.0.0:80: bind: Tentativo di accesso al socket con modalità non consentite dalle rispettive autorizzazioni di accesso."
C:\Users\user\Desktop\gophish-v0.12.1-windows-64bit>
```

Ho modificato il file **config.json** per utilizzare la porta 8080 invece della 80:

```
config.json - Blocco note
File Modifica Formato Visualizza ?
{
    "admin_server": {
        "listen_url": "127.0.0.1:3333",
        "use_tls": false,
        "cert_path": "gophish_admin.crt",
        "key_path": "gophish_admin.key",
        "trusted_origins": []
    },
    "phish_server": {
        "listen_url": "0.0.0.0:8080",
        "use_tls": false,
        "cert_path": "example.crt",
        "key_path": "example.key"
    },
    "db_name": "sqlite3",
    "db_path": "gophish.db",
    "migrations_prefix": "db/db_",
    "contact_address": "",
    "logging": {
        "filename": "",
        "level": ""
    }
}
```

Dashboard e Creazione Campagna

Una volta avviato correttamente, ho acceduto alla dashboard di Gophish per configurare la campagna:

The screenshot shows the Gophish application interface. On the left is a sidebar with navigation links: Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages, Sending Profiles, Account Settings, User Management, and Webhooks. The main area is titled 'Dashboard' and contains a log of network traffic captured by Fiddler. The log shows several requests from various user agents (e.g., Chrome, Safari, Firefox) over different ports (e.g., 127.0.0.1:3333, 127.0.0.1:8080). The log includes details like timestamp, method, URL, and response status code.

Email di Phishing Creato

Ho creato un template email che simula una notifica di spedizione DHL:

The screenshot shows an email message from 'DHL Express <noreply@dhl.com>' to 'Sakura konoa <sakura.konoa@huckla.it>'. The subject is 'Il tuo pacco è in arrivo!'. The email body contains a tracking link: 'Il tuo pacco è in consegna! Traccia la spedizione: Tracking: DHL-BWUWeRw'. Below the tracking link is a red button labeled 'TRACCIA PACCO'. At the bottom of the email, there is a copyright notice: '© 2025 DHL Express'.

L'email è stata inviata con successo tramite Mailtrap e ricevuta nella inbox.

2. SET - Social Engineering Toolkit

SET è uno degli strumenti più potenti per condurre attacchi di ingegneria sociale.

L'ho utilizzato su Kali Linux per clonare un sito web e catturare le credenziali.

Avvio di SET Ho avviato SET dal terminale di Kali Linux con il comando: **sudo setoolkit**



Passaggi di Configurazione

Ho seguito questi passaggi per configurare l'attacco:

1. **Menu principale** - Ho selezionato **1) Social-Engineering Attacks**
2. **Tipo di attacco** - Ho selezionato **2) Website Attack Vectors**
3. **Metodo di attacco** - Ho selezionato **3) Credential Harvester Attack Method**
4. **Modalità** - Ho selezionato **2) Site Cloner**
5. **Indirizzo IP** - Ho inserito il mio IP locale: **192.168.50.100**
6. **URL da clonare** - Ho inserito: **<http://testphp.vulnweb.com/login.php>**

```
set> 1
set> 2
set:webattack> 3
set:webattack> 2
set:webattack> IP address for the POST back in Harvester/Tabnabbing:
192.168.50.100
set:webattack> Enter the url to clone: http://testphp.vulnweb.com/
login.php

[*] Cloning the website: http://testphp.vulnweb.com/login.php
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Una volta completata la configurazione, SET ha clonato il sito di test:

The screenshot shows a web browser window with the URL `http://192.168.50.100`. The page is titled "acunetix acuart" and describes itself as a "TEST and Demonstration site for Acunetix Web Vulnerability Scanner". It features a navigation menu on the left with links like "Home", "categories", "artists", "disclaimer", "your cart", "guestbook", and "AJAX Demo". The main content area contains a login form with fields for "Username" and "Password", and a "login" button. Below the form, there is a note about signing up and a warning message in a box stating: "Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: The best way to use this attack is if `username` and `password` form fields are available. Regardless, this captures all POSTs on a website. You can use it to test other tools and your manual hacking skills as well. Tip: The Social-Engineer Toolkit Credential Harvester Attack, Test Forgery (CSRF), and more." A blue arrow points to the bottom of the warning message.

Quando la "vittima" ha inserito le credenziali nel sito clonato, SET le ha catturate immediatamente:

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.3.15]: 192.168.50.100
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://testphp.vulnweb.com/login.php
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

[*] Cloning the website: http://testphp.vulnweb.com/login.php
[*] This could take a little bit ...

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks.
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website. You can use it to test other tools and your manual hacking skills as well. Tip:
[*] The Social-Engineer Toolkit Credential Harvester Attack, Test Forgery (CSRF), and more.
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.50.100 - - [14/Dec/2025 12:01:28] "GET / HTTP/1.1" 200 -
192.168.50.100 - - [14/Dec/2025 12:01:30] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE PASSWORD FIELD FOUND: uname=epicode
POSSIBLE PASSWORD FIELD FOUND: pass=epicode
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Come si può vedere, le credenziali inserite (username: `epicode`, password: `epicode`) sono state intercettate con successo.

PARTE II: [FACOLTATIVO]

ChatGPT - Analisi Email di Phishing

Come richiesto dalla traccia, ho analizzato l'email di phishing utilizzando ChatGPT.

Codice Sorgente dell'Email

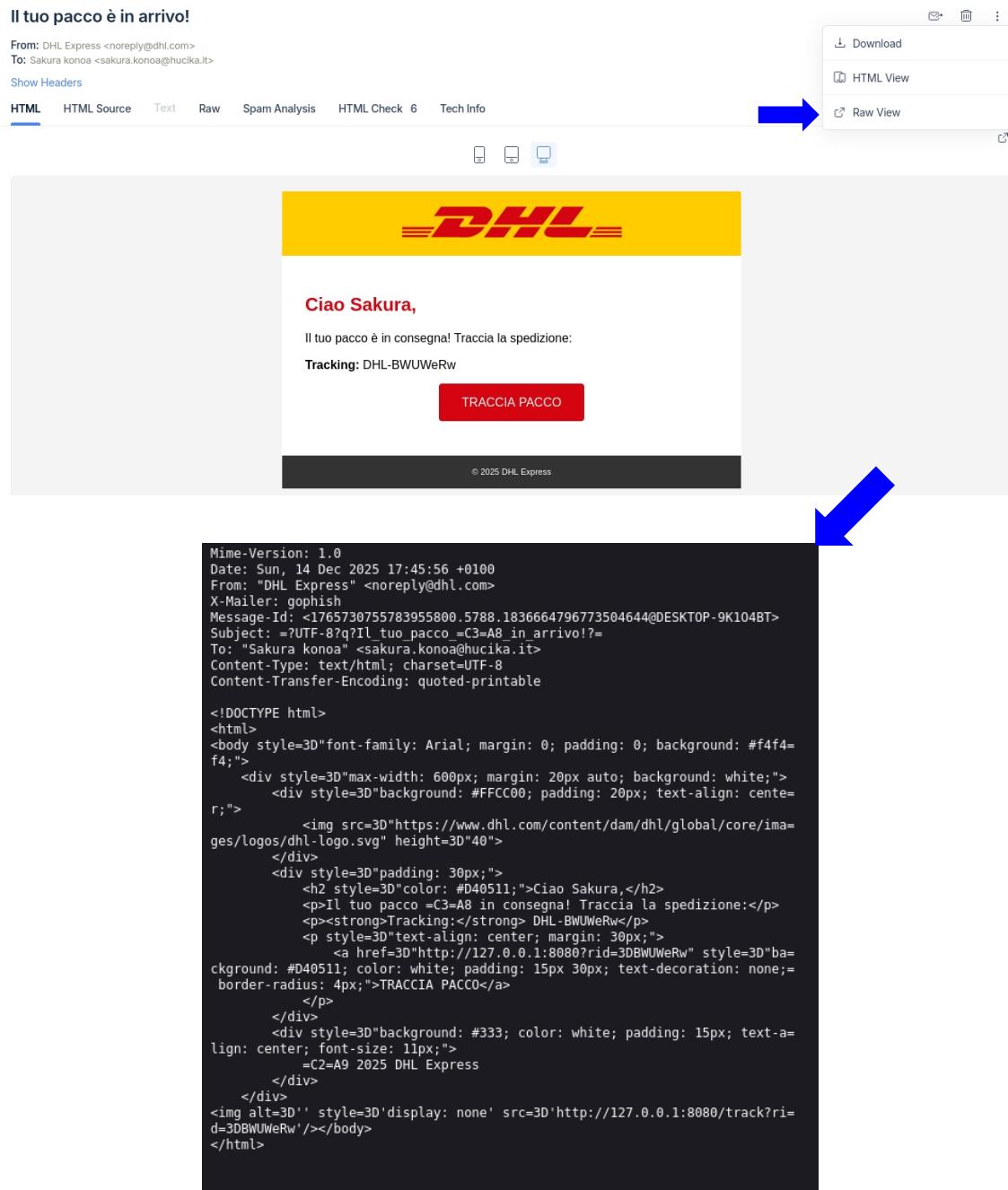
Ho estratto il codice sorgente raw dell'email da Mailtrap:

Il tuo pacco è in arrivo!

From: DHL Express <noreply@dhl.com>
To: Sakura konoa <sakura.konoa@hucika.it>

Show Headers

HTML HTML Source Text Raw Spam Analysis HTML Check 6 Tech Info



Analisi di ChatGPT

Ho fornito a ChatGPT l'email di phishing e questa è stata la sua risposta:

Certo! L'email che hai ricevuto sembra essere un tentativo di phishing. Ecco alcuni segnali di allarme:

- Link sospetto:** Il link di tracciamento (`http://127.0.0.1:8080?rid=3DBWUWeRw`) è un indirizzo locale, che funziona solo sul tuo computer e non è un sito legittimo di DHL.
- Indirizzo email generico:** Anche se proviene da `noreply@dhl.com`, l'email è inviata tramite un sistema chiamato `gophish`, che viene spesso utilizzato per creare campagne di phishing.
- Lingua e formattazione:** L'email è principalmente in italiano, ma la codifica nel soggetto (`=?UTF-8? q?...?=`) e la formattazione sembrano un po' strani. Le email legittime di DHL di solito sono più curate e professionali.
- Richiesta di azione immediata:** Gli attacchi di phishing spesso cercano di creare un senso di urgenza, invitandoti a cliccare su un link per tracciare un pacco o aggiornare le informazioni sulla spedizione.

Per essere sicuro, **non cliccare su nessun link** e non fornire alcuna informazione personale. Ti consiglio di visitare direttamente il sito ufficiale di DHL o di contattare il loro servizio clienti per verificare se ci sono consegne in arrivo. Se pensi che l'email sia una truffa, puoi anche segnalarla a DHL come tentativo di phishing.

Posso aiutarti a segnalare questa email o a fare qualche altra verifica?



Ask anything

Attach

Search

Study

Create image

Voice

ChatGPT can make mistakes. Check important info. See [Cookie Preferences](#).

ChatGPT ha identificato correttamente i seguenti segnali di allarme:

- Link sospetto** - L'URL `http://127.0.0.1:8080` è un indirizzo locale, non un sito DHL
- Indirizzo email generico** - L'uso di `gophish` come sistema di invio
- Lingua e formattazione** - Codifica UTF-8 sospetta nell'oggetto
- Richiesta di azione immediata** - Tipica tecnica di phishing per creare urgenza

La Mia Analisi

Analizzando gli header dell'email, ho identificato i seguenti indicatori di phishing:

Elemento	Valore	Indicatore di Rischio
X-Mailer	gophish	Tool noto per campagne phishing
From	noreply@dhl.com	Mitente falsificato (spoofing)
Message-ID	DESKTOP-9K1O4BT	Inviato da PC personale, non server aziendale
URL nel Body	Http://127.0.0.1:8080	Indirizzo locale, non sito DHL reale
Tracking pixel	Presente	Usato per tracciare apertura email

Conclusione dell'analisi

Questa email presenta tutti gli indicatori tipici di un attacco di phishing.

L'utilizzo di Gophish come X-Mailer, il Message-ID anomalo e i link che puntano a localhost sono prove evidenti della natura malevola del messaggio.

CONCLUSIONE

Questo laboratorio mi ha permesso di comprendere quanto sia semplice per un attaccante creare campagne di phishing convincenti.

Con strumenti come Gophish e SET, è possibile clonare siti web, creare email ingannevoli e catturare credenziali in pochi minuti.

La lezione più importante è che la formazione degli utenti rimane la prima linea di difesa contro questi attacchi.

Tecnologie come SPF, DKIM e DMARC possono aiutare, ma come dimostrato, possono essere aggirate.

La consapevolezza e l'attenzione critica verso email sospette sono fondamentali per proteggersi.