VNCERT

**MỤC LỤC**

[DANH MỤC HÌNH VẼ 2](#_Toc132916999)

[I. QUÉT VÀ XỬ LÝ DỮ LIỆU VỚI PYTHON: 4](#_Toc132917000)

[II. GOPHISH 7](#_Toc132917001)

[2.1. Cấu hình Sending Profile 7](#_Toc132917002)

[2.2. Cấu hình Landing Pages 11](#_Toc132917003)

[2.3. Cấu hình Email Template 14](#_Toc132917004)

[2.4. Cấu hình Users & Groups 17](#_Toc132917005)

[2.5. Cấu hình Campaigns 19](#_Toc132917006)

# DANH MỤC HÌNH VẼ

[Hình 1. 1 Lệnh quét thông tin website với uniscan 4](#_Toc132916958)

[Hình 1. 2 Thông tin được quét ra 4](#_Toc132916959)

[Hình 1. 3 Dữ liệu khi chưa được lọc 5](#_Toc132916960)

[Hình 1. 4 Code python lọc dữ liệu 5](#_Toc132916961)

[Hình 1. 5 Sau khi lọc dữ liệu 5](#_Toc132916962)

[Hình 1. 6 Tạo file csv bằng python 5](#_Toc132916963)

[Hình 1. 7 File csv được tạo ra 6](#_Toc132916964)

[Hình 2. 1 Thông tin tài khoản 7](#_Toc132916965)

[Hình 2. 2 Truy cập Security 8](#_Toc132916966)

[Hình 2. 3 Bật tính năng xác thực hai bước 9](#_Toc132916967)

[Hình 2. 4 Tìm “App Password” 9](#_Toc132916968)

[Hình 2. 5 Tạo mật khẩu mới 9](#_Toc132916969)

[Hình 2. 6 Mật khẩu mới được cấp 10](#_Toc132916970)

[Hình 2. 7 Tạo Profile để gửi mail phishing 10](#_Toc132916971)

[Hình 2. 8 Tạo trang đích bằng cách clone website 11](#_Toc132916972)

[Hình 2. 9 Đường dẫn của website cần clone 11](#_Toc132916973)

[Hình 2. 10 Kết quả của clone bằng gophish 12](#_Toc132916974)

[Hình 2. 11 Giao diện tramg web chính thống 12](#_Toc132916975)

[Hình 2. 12 Lựa chọn lưu lại thông tin của nạn nhân 13](#_Toc132916976)

[Hình 2. 13 Các biến trong gophish 14](#_Toc132916977)

[Hình 2. 14 URL được thay thế bằng link mà gophish thiết lập 14](#_Toc132916978)

[Hình 2. 15 Các biến được sử dụng để đặt tên 14](#_Toc132916979)

[Hình 2. 16 Thiết lập cuối cùng để tạo email template 15](#_Toc132916980)

[Hình 2. 17 Các dạng file được hỗ trợ trong gophish 16](#_Toc132916981)

[Hình 2. 18 Nội dung của file foo.txt 16](#_Toc132916982)

[Hình 2. 19 Thêm file phishing 16](#_Toc132916983)

[Hình 2. 20 File phishing đã được thêm vào email template 17](#_Toc132916984)

[Hình 2. 21 Thêm user thủ công 17](#_Toc132916985)

[Hình 2. 22 Kết quả 18](#_Toc132916986)

[Hình 2. 23 Thêm user bằng file csv 18](#_Toc132916987)

[Hình 2. 24 Kết quả sau khi thêm user 19](#_Toc132916988)

[Hình 2. 25 Thêm một cuộc phishing 19](#_Toc132916989)

[Hình 2. 26 Thay thế các nội dung cần thiết 20](#_Toc132916990)

[Hình 2. 27 Cuộc phishing đã bắt đầu 21](#_Toc132916991)

[Hình 2. 28 Email phishing đã được gửi 21](#_Toc132916992)

[Hình 2. 29 Tệp đính kèm được gửi 22](#_Toc132916993)

[Hình 2. 30 Các biến được thay thế chính xác 22](#_Toc132916994)

[Hình 2. 31 Giao diện của website phishing 22](#_Toc132916995)

[Hình 2. 32 Login trong website phishing 23](#_Toc132916996)

[Hình 2. 33 Bảng theo dõi tình trạng phishing 23](#_Toc132916997)

[Hình 2. 34 Dữ liệu của nạn nhân 24](#_Toc132916998)

# QUÉT VÀ XỬ LÝ DỮ LIỆU VỚI PYTHON:

Quét thông tin của một website bằng uniscan với tùy chọn *“-d”.*

Text

Description automatically generated

Hình 1. 1 Lệnh quét thông tin website với uniscan

Thông tin email được quét ra:

Graphical user interface, text

Description automatically generated

Hình 1. 2 Thông tin được quét ra

Tuy nhiên email lấy ra có dính các chuỗi “E-Mail …” nên chúng ta sẽ sử dụng python để lọc lại dữ liệu

Text

Description automatically generated with medium confidence

Hình 1. 3 Dữ liệu khi chưa được lọc

Đoạn code lọc chuỗi “E-mail Found” bằng python

A screenshot of a computer

Description automatically generated with medium confidence

Hình 1. 4 Code python lọc dữ liệu

Kết quả sau khi lọc:

Text

Description automatically generated

Hình 1. 5 Sau khi lọc dữ liệu

Vì có trên 5000 account nên không thể import từng account được và dưới đây là đoạn code python nhằm tạo ra file csv để import vào gophish

A screenshot of a computer

Description automatically generated with medium confidence

Hình 1. 6 Tạo file csv bằng python

Data của file csv:

Text

Description automatically generated

Hình 1. 7 File csv được tạo ra

# GOPHISH

## Cấu hình Sending Profile

Trước khi cấu hình tài sending Profile chúng ta phải lựa chọn loại tài khoản sử dụng và sever smtp, trong ví dụ lần này chúng tôi sẽ sử dụng tài khoản và smtp của google với lý do là miễn phí và dễ dàng cấu hình cho việc gửi mail, dưới đây là tài khoản mà chúng ta sẽ sử dụng để gửi mail, tiến hành chọn vào vùng “Manage Your Google Account” để tiến hành quản lý tài khoản.

Graphical user interface, text, application, chat or text message

Description automatically generated

Hình 2. 1 Thông tin tài khoản

Tiếp theo ta chọn vào mục security nhằm bật chức năng xác thực hai bước.

Graphical user interface, text, application

Description automatically generated

Hình 2. 2 Truy cập Security

Chúng ta thấy rằng xác thực hai bước đã được bật, có thể click thẳng vào để có thể cấu hình “App Password”.

Graphical user interface, text, application

Description automatically generated

Hình 2. 3 Bật tính năng xác thực hai bước

Tuy nhiên giao diện của google sẽ thay đổi theo thời gian nên chúng ta sẽ sử dụng chức năng tìm kiếm “app password” nhằm đơn giản hóa việc truy cập và cấu hình.

Graphical user interface, text, application, email

Description automatically generated

Hình 2. 4 Tìm “App Password”

Trong “App Passwords” đây là chức năng nhằm giúp chúng ta có thể đăng nhập mà không phải xác thực hai bước trong khi lập trình, test mail trên hệ thống, … Tiếp theo lựa chọn như hình dưới để tạo mật khẩu tương ứng.

Graphical user interface, application

Description automatically generated

Hình 2. 5 Tạo mật khẩu mới

Sau khi cấu hình như hình trên thì dưới đây là mật khẩu được sử dụng cho công việc của chúng ta khi tiến hành đăng nhập mail.

Graphical user interface, application

Description automatically generated

Hình 2. 6 Mật khẩu mới được cấp

Khi đã hoàn tất việc cấu hình tài khoản chúng ta sẽ cấu hình cho “Sending Profile” với mật khẩu đã được tạo ra từ thao tác vừa rồi của chúng ta như sau:

Graphical user interface, text, application, email

Description automatically generated

Hình 2. 7 Tạo Profile để gửi mail phishing

## Cấu hình Landing Pages

Như đã nói ở trên “Landing Pages” được sử dụng để cấu hình trang đích và gophish có chức năng mạnh mẽ đó là có thể bắt chước giao diện của một website khác, chúng ta sẽ đặt tên cho trang phishing, và import giao diện website mà ta muốn phishing, trong ví dụ lần này chúng ta sẽ sử dụng “elearning2.vku.udn.vn” làm trang ví dụ.

Graphical user interface, application

Description automatically generated with medium confidence

Hình 2. 8 Tạo trang đích bằng cách clone website

Tiến hành nhập trang địa chỉ của website.

Graphical user interface, application

Description automatically generated

Hình 2. 9 Đường dẫn của website cần clone

Dưới đây là kết quả của việc clone website.

Graphical user interface, text, application

Description automatically generated

Hình 2. 10 Kết quả của clone bằng gophish

Và dưới đây là trang web khi chúng ta truy cập bằng link chính thống ta thấy rằng gophishing đã thành công trong việc clone website.

Graphical user interface, text, application

Description automatically generated

Hình 2. 11 Giao diện tramg web chính thống

Để lưu lại thông tin được gửi lên hệ thống phishing chúng ta sẽ tích vào hai ô tương ứng “Capture Submitted Data” và “Capture Passwords” và chuyển hướng tới trang web chính thống khi nạn nhân bấm nút login trên giao diện nhằm đánh lừa người dùng là đã đăng nhập thành công.

Graphical user interface, application

Description automatically generated

Hình 2. 12 Lựa chọn lưu lại thông tin của nạn nhân

## Cấu hình Email Template

Dưới đây là các biến mà khi chúng ta nhúng vào trong html của email:

A screenshot of a computer

Description automatically generated with medium confidence

Hình 2. Các biến trong gophish

“https://github.com/lelong1210/phishing/blob/main/email\_template.html” source code này được chúng tôi sử dụng để tạo email template và trong đó chúng tôi sẽ thay thế nút reset thành một thẻ a với href là “{{.URL}}” nhằm khi nạn nhân click vào sẽ tới địa chỉ mà hacker đã cấu hình để thực thi web phishing.

Text

Description automatically generated

Hình 2. 14 URL được thay thế bằng link mà gophish thiết lập

Để tăng tính thuyết phục chúng ta sẽ cấu hình tên cho email bằng hai biến là {{.FirstName}} {{.LastName}} ngoài ra còn có thể thêm biến {{.Email}} nhưng trong ví dụ lần này chúng tôi không sử dụng đến.

Text

Description automatically generated

Hình 2. 15 Các biến được sử dụng để đặt tên

Tuy rằng gophish cung cấp cho chúng ta chức năng “Import Email” nhưng trong ví dụ lần này chúng tôi không sử dụng đến, Khi đã có source code cần thiết chúng ta sẽ cấu hình như hình bên dưới và dán đoạn mã đó vào ô html, chúng ta sẽ thấy các biến vẫn được giữ nguyên nhưng khi được gophish gửi thì sẽ tự động thay các biến đó với các nội dung tương ứng.

Graphical user interface, text, application, email

Description automatically generated

Hình 2. 16 Thiết lập cuối cùng để tạo email template

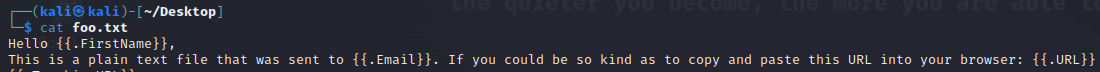
Ngoài ra gophish không chỉ gửi mail mà còn giúp chúng ta gửi các tệp đính kèm nhằm có thể tăng cao tỷ lệ thành công phishing, dưới đây là các file được hỗ trợ cho việc thay thế các biến được định nghĩa ở trên.

Table

Description automatically generated

Hình 2. 17 Các dạng file được hỗ trợ trong gophish

Chúng ta sẽ tạo một file foo.txt với nội dung như sau:



Hình 2. 18 Nội dung của file foo.txt

Và thêm file đó vào mẫu của email.

Graphical user interface, text, application

Description automatically generated

Hình 2. 19 Thêm file phishing

sau khi thêm vào sẽ có tên file mà chúng ta chọn và nhấn nút “save template” để lưu trữ file.

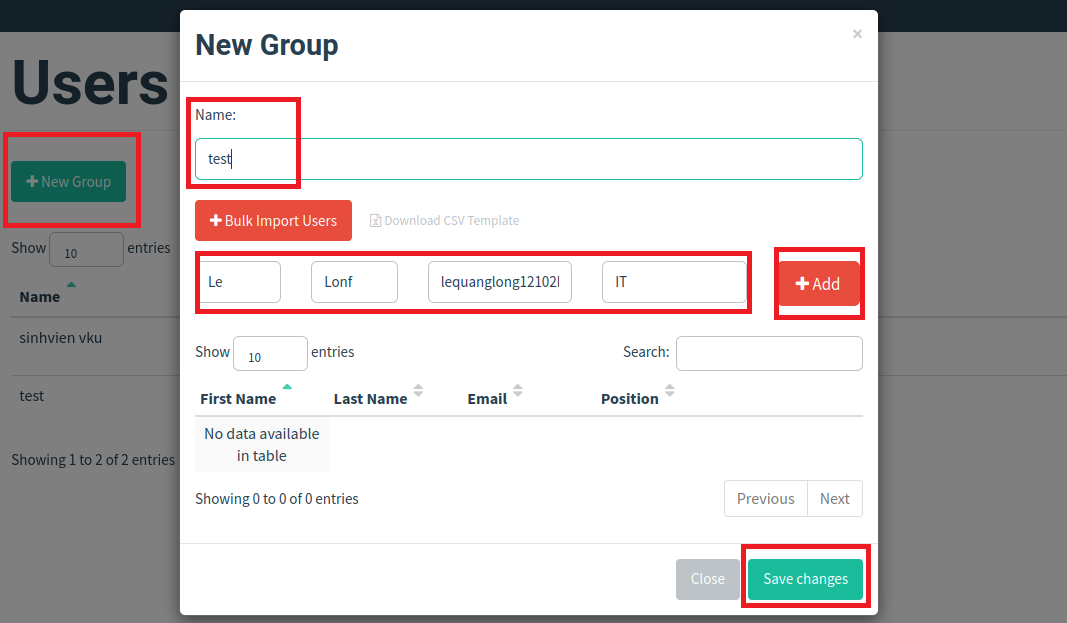
Graphical user interface, application

Description automatically generated

Hình 2. 20 File phishing đã được thêm vào email template

## Cấu hình Users & Groups

Chúng ta sẽ thêm thủ công các tài khoản để tiến hành có thể gửi mail phishing như bên dưới:



Hình 2. 21 Thêm user thủ công

Kết quả khi thêm tài khoản:

Graphical user interface, application

Description automatically generated

Hình 2. 22 Kết quả

Nhưng khi tài khoản quá nhiều chúng ta không thể thêm thủ công từng account mà phải sử dụng đến mẫu csv mà chúng tôi đã tiến hành lọc từ đầu, chúng tôi lưu trữ hơn 5000 tài khoản của sinh viên vku ở được lưu trữ bằng github với đường dẫn như sau: “https://github.com/lelong1210/phishing/blob/main/output.csv”.

Graphical user interface, text, application, email, website

Description automatically generated

Hình 2. 23 Thêm user bằng file csv

Kết quả sau khi thêm account bằng file csv:

Table

Description automatically generated

Hình 2. 24 Kết quả sau khi thêm user

## Cấu hình Campaigns

Sau khi đã hoàn tất các thiết lập ở trên chúng ta tiến hành phishing bằng tính năng mạnh mã “Campaigns” của gophish.

Graphical user interface, text, application

Description automatically generated

Hình 2. 25 Thêm một cuộc phishing

Chúng ta sẽ nhập địa chỉ của server phishing và chọn group cần gửi (lưu ý email template, landing page đã được chúng ta thiết lập từ trước) và tiến hành gửi mail phishing và chờ đợi kết quả.

Graphical user interface, text, application

Description automatically generated

Hình 2. 26 Thay thế các nội dung cần thiết

Giao diện thành công khi đã lên lịch gửi mail cho các nạn nhân.

Graphical user interface, text, application, chat or text message

Description automatically generated

Hình 2. 27 Cuộc phishing đã bắt đầu

Email đã được gửi tới nạn nhân



Các biến trong email được hoạt động tốt và đã thay thế thành tên của các user.

Graphical user interface, text, application

Description automatically generated

Hình 2. 28 Email phishing đã được gửi

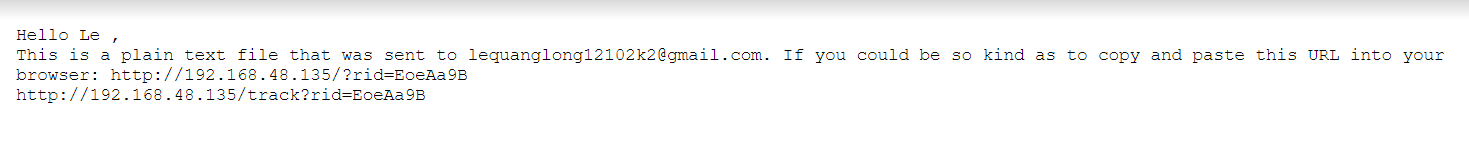
Tệp đính kèm mà chúng ta đã thêm vào email template.

Graphical user interface

Description automatically generated

Hình 2. 29 Tệp đính kèm được gửi

Thông tin được gophish gửi đi đã thay thế chính xác.



Hình 2. 30 Các biến được thay thế chính xác

Đường dẫn khi chúng ta click vào giao diện được gophish clone khiến người dùng có thể bị nhầm lẫn.

Graphical user interface, application

Description automatically generated

Hình 2. 31 Giao diện của website phishing

Khi người dùng nhập thông tin và tiến hành đăng nhập sẽ chuyển hướng quay trở lại trang chính thống.

Graphical user interface, application

Description automatically generated

Hình 2. 32 Login trong website phishing

Trên thanh thông báo cho thấy rằng gophish đã lấy được thông tin đăng nhập mà nạn nhân gửi về.

Graphical user interface, application

Description automatically generated

Hình 2. 33 Bảng theo dõi tình trạng phishing

Ngoài thông tin đăng nhập ra còn có thông tin của hệ điều hành và bên cạnh đó là phiên bản của trình duyệt.

Graphical user interface, application

Description automatically generated

Hình 2. 34 Dữ liệu của nạn nhân