VNCERT

**MỤC LỤC**

[DANH MỤC HÌNH VẼ 2](#_Toc133325071)

[PHẦN I. MÔ TẢ TÌNH HUỐNG 3](#_Toc133325072)

[PHẦN II. KỊCH BẢN TỔNG THỂ 4](#_Toc133325073)

[PHẦN III. THỰC HIỆN KỊCH BẢN 6](#_Toc133325074)

[Phase 1: Thu Thập Thông Tin Mục Tiêu 6](#_Toc133325075)

[Phase 2: Gửi Mail Cho Nạn Nhân 6](#_Toc133325076)

[A) Cấu hình Sending Profile 7](#_Toc133325077)

[B) Cấu hình Landing Pages 10](#_Toc133325078)

[C) Cấu hình Email Template 12](#_Toc133325079)

[D) Cấu hình Campaigns 15](#_Toc133325080)

[Phase 3: Nạn Nhân Mở Mail Của Hacker 17](#_Toc133325081)

[Phase 4: Thu Thập Thông Tin Của Nạn Nhân 18](#_Toc133325082)

# DANH MỤC HÌNH VẼ

[Hình 3. 1 Lệnh quét thông tin website với uniscan 6](#_Toc133325044)

[Hình 3. 2 Giao diện chính của gophish 6](#_Toc133325045)

[Hình 3. 3 Thông tin tài khoản 7](#_Toc133325046)

[Hình 3. 4 Truy cập Security 7](#_Toc133325047)

[Hình 3. 5 3 Bật tính năng xác thực hai bước 8](#_Toc133325048)

[Hình 3. 6 Tìm “App Password” 8](#_Toc133325049)

[Hình 3. 7 Tạo mật khẩu mới 8](#_Toc133325050)

[Hình 3. 8 Mật khẩu mới được cấp 9](#_Toc133325051)

[Hình 3. 9 Tạo Profile để gửi mail phishing 9](#_Toc133325052)

[Hình 3. 10 Đường dẫn của website cần clone 10](#_Toc133325053)

[Hình 3. 11 Kết quả của clone bằng gophish 11](#_Toc133325054)

[Hình 3. 12 Giao diện tramg web chính thống 11](#_Toc133325055)

[Hình 3. 13 Lựa chọn lưu lại thông tin của nạn nhân 12](#_Toc133325056)

[Hình 3. 14 Các biến trong gophish 12](#_Toc133325057)

[Hình 3. 15 URL được thay thế bằng link mà gophish thiết lập 13](#_Toc133325058)

[Hình 3. 16 Các biến được sử dụng để đặt tên 13](#_Toc133325059)

[Hình 3. 17 Thiết lập cuối cùng để tạo email template 13](#_Toc133325060)

[Hình 3. 18 Nội dung của file foo.txt 14](#_Toc133325061)

[Hình 3. 19 Thêm file phishing 14](#_Toc133325062)

[Hình 3. 20 File phishing đã được thêm vào email template 15](#_Toc133325063)

[Hình 3. 21 Thêm một cuộc phishing 15](#_Toc133325064)

[Hình 3. 22 Thay thế các nội dung cần thiết 16](#_Toc133325065)

[Hình 3. 23 Cuộc phishing đã bắt đầu 16](#_Toc133325066)

[Hình 3. 24 Giao diện khi nạn nhân mở email phishing 17](#_Toc133325067)

[Hình 3. 25 Giao diện web phishing 17](#_Toc133325068)

[Hình 3. 26 Theo dõi tình trạng phishing 18](#_Toc133325069)

[Hình 3. 27 Thông tin chi tiết của nạn nhân 18](#_Toc133325070)

# PHẦN I. MÔ TẢ TÌNH HUỐNG

Vào ngày 24/04/2023 website của một tổ chức trong quá trình phát triễn vì không kiểm tra đầy đủ về phần lập trình cũng như không đề cao tính bảo mật thông tin nên đã để lộ thông tin email của toàn bộ các thành viên của mình. Và vì vậy hacker đã dễ dàng lấy toàn bộ thông tin đó.

Bây giờ hãy vào vai là hacker với mục đích là dựa vào những thông tin bị lộ đó hãy sử dụng những mánh khóe cũng như công cụ thuận tiện nhất để lừa nạn nhân cung cấp những thông tin của họ.

# PHẦN II. KỊCH BẢN TỔNG THỂ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TT | Thời gian | Nhiệm vụ | Nội dung | Thực hiện |
| 1. Phase1: Thu thập thông tin mục tiêu | | | | |
| 1 | Xác định tổ chức muốn phishing | Thu thập thông tin | Hacker sẽ thực hiện các thao tác nhằm thu thập được những thông tin của tổ chức | Dựa vào các thông tin đã được công khai trên mạng xã hội, internet như là facebook, kênh tiktok để có thể đoán biết được website lưu trữ thông tin. |
| 2 | Sau khi đã có những thông tin của tổ chức | Quét thông tin | Hacker sẽ sử dụng những công cụ để lấy thông tin thông qua website | Khi đã đoán biết được website lưu trữ thông tin của tổ chức thì hacker tiến hành sử dụng những công cụ đặc biệt, hoặc các công cụ có thể chạy online trên website để quét thông tin của website và từ đó có thể thu thập được email của các thành viên trong tổ chức đó. |
| 1. Phase2: Gửi mail cho nạn nhân | | | | |
| 1 | Khi đã có các thông tin cần để phishing trước tiên hacker sẽ tạo ra một website trông giống hệt của tổ chức. | | | |
| 2 | Hacker sẽ tạo thêm một file đính kèm với những mô tả dễ bị đánh lừa như: “ảnh mèo con, file lưu trữ mật khẩu, …” nhằm để nạn nhân mở ra và truy cập vào những đường dẫn đã được đính kèm | | | |
| 3 | Hacker sẽ gửi mail phishing cho nạn nhân với tiêu đề dễ bị lừa như là: “Khôi phục lại mật khẩu, Vui lòng đăng nhập để tiến hành điểm danh, …” | | | |
| 1. Phase3: Nạn nhân mở mail của hacker | | | | |
| 1 | Khi nạn nhân nhận được email của hacker vì tiêu đề dễ khiến cho nạn nhân nhầm lẫn vì tưởng đó là email thật của tổ chức nên đã nhấn vào link mà hacker đã cấu hình từ trước trong mail, dẫn đến được thông tin được gửi tới cho hacker | | | |
| 1. Phase4: 4: thu thập thông tin của nạn nhân | | | | |
| 1 | Ngay khi nạn nhân mở email ra và truy cập vào đường dẫn thì thông tin đã được gửi về cho hacker. | | | |
| 2 | Khi nạn nhân gửi thông tin đăng nhập lên hệ thống thì dữ liệu được gửi về phía hacker khiến cho thành viên đó bị lộ thông tin đăng nhập từ đó hacker có thể truy cập vào hệ thống của tổ chức và tùy theo cấp độ phân quyền của tài khoản mà hacker có thể làm được nhiều thứ hơn. | | | |

# PHẦN III. THỰC HIỆN KỊCH BẢN

## Phase 1: Thu Thập Thông Tin Mục Tiêu

Hacker quét thông tin của một website bằng uniscan với tùy chọn *“-d”,* từ đó có thể thu thập được những thông tin nhạy cảm của tổ chức trong đó có email của các thành viên.

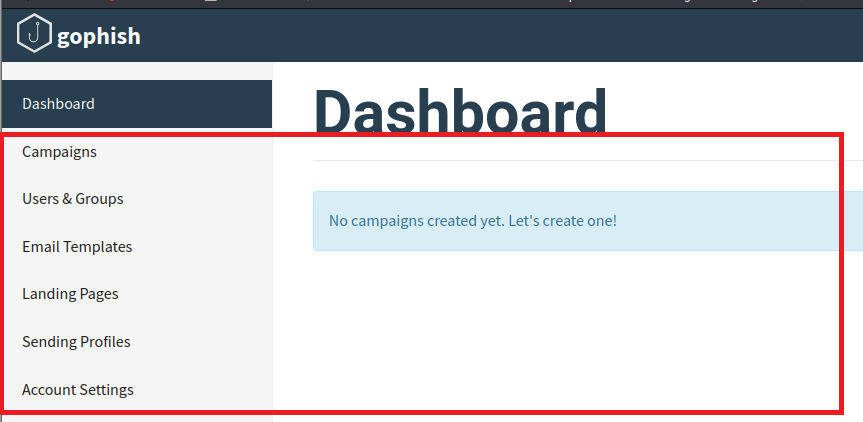
Text

Description automatically generated

Hình 3. Lệnh quét thông tin website với uniscan

## Phase 2: Gửi Mail Cho Nạn Nhân

Trong lần tấn công phishing lần này hacker quyết định sử dụng công cụ gophish để tạo email, website, tệp đính kèm cũng như là để tạo ra server nhằm phục vụ cho nhiệm vụ lấy thông tin mà nạn nhân gửi lên hệ thống, sau đây chúng ta sẽ cấu hình từng phần của gophish.



Hình 3. Giao diện chính của gophish

### Cấu hình Sending Profile

Trước khi cấu hình “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 quản lý tài khoản.

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

Description automatically generated

Hình 3. 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 3. 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 3. 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 3. 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 3. 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 3. 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 3. 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 3. Đường dẫn của website cần clone

Dưới đây là kết quả của việc clone website.

Graphical user interface, text, application

Description automatically generated

Hình 3. 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 3. 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 3. 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 3. 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 3. 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 3. 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 3. Thiết lập cuối cùng để tạo email template

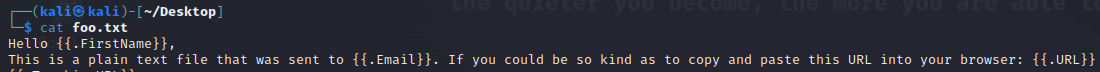
Ngoài ra gophish không chỉ gửi mail mà còn giúp chúng ta gửi các tệp đính kèm nhằm có thể tăng cao tỷ lệ thành công phishing, dưới đây là các file được hỗ trợ cho việc thay thế các biến được định nghĩa ở trên.

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 3. Nội dung của file foo.txt

Và thêm file đó vào mẫu của email.

Graphical user interface, text, application

Description automatically generated

Hình 3. 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 3. File phishing đã được thêm vào email template

### Cấu hình Campaigns

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

Graphical user interface, text, application

Description automatically generated

Hình 3. 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 3. 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 3. Cuộc phishing đã bắt đầu

## Phase 3: Nạn Nhân Mở Mail Của Hacker

Nạn nhân nhận được email phishing của hacker nhưng do tiêu đề và tên đại diện cho mail đó khi cho nạn nhân trở nên mất cảnh giác nên đã truy cập vào link mà hacker đã cấu hình ở trong email.

Graphical user interface, text, application

Description automatically generated

Hình 3. Giao diện khi nạn nhân mở email phishing

Khi truy cập vào đường link nhằm khôi phục lại mật khẩu vì do giao diện quá giống làm cho nạn nhân bị nhầm lẫn từ đó nhập thông tin đăng nhập vào hệ thống và gửi cho hacker.

Graphical user interface, application

Description automatically generated

Hình 3. Giao diện web phishing

## Phase 4: Thu Thập Thông Tin Của Nạn Nhân

Hacker theo dõi quá trình thao tác gửi mail của mình và nhận thấy rằng đã có một nạn nhân đã mở mail, truy cập vào đường dẫn và cũng như đã gửi thông tin gì đó lên server của mình.

Graphical user interface, application

Description automatically generated

Hình 3. Theo dõi tình trạng phishing

Tiến hành xem chi tiết thông tin của nạn nhân thì hacker đã thu được thông tin đăng nhập cũng như là có được phiên bản của trình duyệt, phiên bản windows, …

Graphical user interface, application

Description automatically generated

Hình 3. Thông tin chi tiết của nạn nhân