**Phishing (tấn công lừa đảo)**

1. **Intro To Phishing Attacks (giới thiệu về tấn công lừa đảo)**

Social engineering là sự thao túng tâm lý con người để thực hiện hoặc tiết lộ thông tin bằng cách khai thác các điểm yếu trong bản chất con người. Điểm yếu này có thể là tính tò mò, sự đố kỵ, tham lam và thậm chí là lòng tốt và sự sẵn lòng giúp đỡ. Phising là một trong những kỹ thuật lừa đảo xã hội, cái mà sẽ phân phát email để lừa ai đó tiết lộ các thông tin cá nhân (personal information), thông tin xác thực (credential) hoặc thậm chí là thực hiện mã độc trong chính máy tính của họ. **Phising:** khi các email được gửi tới mục tiêu có chủ đích từ những người đáng tin cậy để thu hút các các nhân cung cấp các thông tin nhạy cảm

Những email thường xuất hiện từ những nguồn đáng tin cậy, có thể là những cá nhân hoặc doanh nghiệp. Chúng sẽ bao gồm nội dung cái mà cố gắng cám dỗ hoặc lừa đảo người khác tải các phần mềm, mở tệp đính kèm, và truy cập đường dẫn tới một trang web không có thật.

**Spear-phishing** là một hình thức phishing mà kẻ tấn công nhắm vào một cá nhân hoặc tổ chức cụ thể chứ không phải phising thông thường (phishing thông thường: gửi đến hàng loạt người nhận). Đây là một hình thức lừa đảo hiệu quả cho sự tham gia của red-team vì chúng được đặt riêng ra cho mục tiêu, điều đó khiến họ khó phát hiện bằng công nghệ như bộ lọc thư rác, chống vi -rút và tường lửa.

Một số phương pháp lừa đảo khác thông qua các phương tiện khác là smishing tức là lừa đảo qua tin nhắn SMS và vishing được thực hiện thông qua các cuộc gọi điện thoại.

1. Writing Convincing Phishing Emails (viết một email lừa đảo thuyết phục)

3 điều cần quan tâm: địa chỉ mail của người gửi, tiêu đề và nội dụng

1. Địa chỉ mail của người gửi

Lý tưởng nhất là từ:

* Thương hiệu quan trọng
* Một liên hệ đã biết
* Một đồng nghiệp

Triển khai các chiến thuật OSINT (Open Source Intelligence):

* Quan sát tài khoản MXH để tìm thương hiệu/bạn bè mà nạn nhân nói chuyện cùng
* Search google để biết tên nạn nhân và vị trí gần đúng của bất kỳ đánh giá nào mà nạn nhân để lại về các doanh nghiệp hoặc thương hiệu địa phương
* Nhìn vào website kinh doanh của nạn nhân để tìm nhà cung cấp.
* Looking at LinkedIn to find coworkers of the victim

1. Tiêu đề

Đặt về những điều cấp bách, bận tâm hoặc tính tò mò của nạn nhân 🡪 để nạn nhân không thể bỏ qua nó và hành động ngay lập tức.

Ví dụ:

* Tài khoản của bạn đã bị xâm phạm.
* Gói hàng của bạn đã được gửi đi/vận chuyển.
* Thông tin bảng lương nhân viên (không chuyển tiếp!)
* Ảnh của bạn đã được xuất bản.

1. Nội dung

* Nếu mạo danh một thương hiệu hoặc nhà cung cấp, sẽ cần nghiên cứu về mẫu email của họ: phong cách, logo, ký kết,..
* Nếu mạo danh một liên hệ hoặc đồng nghiệp, có thể có lợi khi liên hệ với họ; Đầu tiên, họ có thể có một số thương hiệu trong mẫu của họ, có một chữ ký email cụ thể hoặc thậm chí chí một cái gì đó nhỏ như cách họ đề cập đến chính họ, ví dụ, ai đó có thể có tên Dorothy và email của họ là dorothy@company.thm. Tuy nhiên, trong chữ ký của họ, không có thể nói "Trân trọng, chấm". Học những điều nhỏ bé này đôi khi có thể có tác dụng tâm lý khá ấn tượng đối với nạn nhân và thuyết phục họ nhiều hơn để mở và hành động trên email.

Chú ý: Giả mạo liên kết

**<a href="http://spoofsite.thm">Click Here</a>**

**<a href="http://spoofsite.thm">https://onlinebank.thm</a>**

1. **Phishing Infrastructure (Cở sở hạ tầng phishing)**

Sẽ cần phải có một lượng cơ sở hạ tầng nhất định để khởi động một chiến dịch lừa đảo thành công.

* Domain Name
* SSL/TLS Certificates
* Email Server/Account
* DNS Records
* Web Server
* Analytics
* Automation And Useful Software
* GoPhish - (Open-Source Phishing Framework) - getgophish.com
* SET - (Social Engineering Toolkit) - trustedsec.com

1. **Using GoPhish**

Nhiệm vụ này sẽ hướng dẫn bạn thiết lập GoPhish, gửi chiến dịch lừa đảo và lấy thông tin xác thực của người dùng từ một trang web giả mạo.

1. **Sending profiles:**

Đây chỉ đơn giản là một máy chủ SMTP mà bạn có quyền truy cập.

A screenshot of a computer

Description automatically generated

1. **Landing Pages:**

Đây là nơi chứa mã nguồn của website giả mạo, nơi này sẽ hiển thị giao diện với nạn nhận

Click the Landing Pages link on the left-hand menu and then click the "New Page" Give the Landing Page the name **ACME Login**, next in the HTML box; you'll need to press the **Source** button to allow us to enter the HTML code as shown below:

<!DOCTYPE html>  
<html lang="en">  
<head>  
 <meta charset="UTF-8">  
 <title>ACME IT SUPPORT - Admin Panel</title>  
 <style>  
 body { font-family: "Ubuntu", monospace; text-align: center }  
 div.login-form { margin:auto; width:300px; border:1px solid #ececec; padding:10px;text-align: left;font-size:13px;}  
 div.login-form div input { margin-bottom:7px;}  
 div.login-form input { width:280px;}  
 div.login-form div:last-child { text-align: center; }  
 div.login-form div:last-child input { width:100px;}  
 </style>  
</head>  
<body>  
 <h2>ACME IT SUPPORT</h2>  
 <h3>Admin Panel</h3>  
 <form method="post">  
 <div class="login-form">  
 <div>Username:</div>  
 <div><input name="username"></div>  
 <div>Password:</div>  
 <div><input type="password" name="password"></div>  
 <div><input type="submit" value="Login"></div>  
 </div>  
 </form>  
</body>  
</html>

Click the **Source** button again, and you should see a login box with username and password fields as per the image below, also click the **Capture Submitted Data** box and then also the **Capture Passwords** box and then click the Save Page button.

A screenshot of a computer

Description automatically generated

1. **Email Templates**

Đây là thiết kế và nội dung của email bạn sắp gửi cho nạn nhân; nó cần phải thuyết phục và chứa liên kết đến trang đích của bạn để cho phép chúng tôi lấy được tên người dùng và mật khẩu của nạn nhân.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Hiển thị là: <https://admin.acmeitsupport.thm>, nhưng liên kết thực là {{.URL }}

A screenshot of a computer

Description automatically generated

1. **Users and groups**

Nơi lưu trữ thông tin về các mục tiêu

A screenshot of a group

Description automatically generated

1. **Campaigns:**

Bây giờ là lúc gửi email đầu tiên của bạn

A screenshot of a computer

Description automatically generated

1. **Result**

Trang kết quả giúp chúng ta biết được chiến dịch lừa đảo đang diễn ra như thế nào bằng cách cho chúng ta biết có bao nhiêu email đã được gửi, đã mở, đã nhấp và có bao nhiêu người dùng đã gửi dữ liệu đến trang web giả mạo của chúng tôi.

Bạn sẽ thấy thông tin chi tiết về từng địa chỉ email ở cuối màn hình; bạn sẽ nhận thấy rằng cả email của Martin và Brian đều đã được gửi thành công, nhưng email của tài khoản lại bị lỗi.

A screenshot of a computer

Description automatically generated

Chúng ta có thể tìm hiểu sâu hơn về lỗi bằng cách nhấp vào mũi tên thả xuống bên cạnh hàng tài khoản và khi xem chi tiết hoặc lỗi, chúng ta có thể thấy thông báo lỗi cho biết người dùng không xác định.

A screenshot of a computer

Description automatically generated

Sau một phút nếu bạn làm theo đúng hướng dẫn, bạn sẽ thấy trạng thái của brian thay đổi thành **Dữ liệu đã gửi.**

A screenshot of a computer

Description automatically generated

Mở rộng thông tin chi tiết của Brian và sau đó xem thông tin chi tiết về dữ liệu đã gửi, bạn sẽ có thể thấy tên người dùng và mật khẩu của Brian, điều này sẽ giúp bạn trả lời câu hỏi bên dưới.

A screenshot of a computer

Description automatically generated

1. **Droppers**

Droppers là những phần mềm lừa nạn nhân tải xuống và chạy trên máy của họ. Dropper có thể quảng cáo chúng như là một thứ hữu dụng,…

Droppers thì thường không chứa mã độc, do đó nó có thể vượt qua được antivirus checks. Tuy nhiên sau khi được cài đặt, phần mềm độc hại dự định sẽ được giải nén hoặc tải xuống từ máy chủ và cài đặt vào máy tính của nạn nhân. Phần mềm độc hại thường kết nối trở lại cơ sở hạ tầng của kẻ tấn công. Kẻ tấn công có thể chiếm quyền kiểm soát máy tính của nạn nhân, máy tính này có thể khám phá và khai thác mạng cục bộ hơn nữa.

1. **Choosing A Phishing Domain (cách chọn miền phishing)**

* Expired Domains (tên miền hết hạn)
* Typosquatting (tên miền kiểu lỗi đánh máy)
* Lỗi chính tả: goggle.com Vs google.com
* Kỳ bổ sung: go.ogle.com so với google.com
* Đổi số thành chữ cái: g00gle.com Vs google.com
* Cụm từ: googles.com Vs google.com
* Từ bổ sung: googleresults.com so với google.com
* Top Alternatives:

TLD (Top Level Domain) là phần .com .net .co.uk .org .gov v.v. của tên miền, hiện nay có hàng trăm biến thể của TLD. Một mẹo phổ biến để chọn tên miền là sử dụng cùng một tên nhưng với TLD khác. Ví dụ, đăng ký tryhackme.co.uk để mạo danh tryhackme.com.

* IDN Homograph Attack/Script Spoofing:

Ban đầu, tên miền được tạo thành từ các ký tự Latin az và 0-9, nhưng vào năm 1998, IDN (tên miền quốc tế hóa) đã được triển khai để hỗ trợ chữ viết hoặc bảng chữ cái cụ thể của ngôn ngữ từ các ngôn ngữ khác như tiếng Ả Rập, tiếng Trung, tiếng Kirin, tiếng Hebrew, v.v. Một vấn đề phát sinh từ việc triển khai IDN là các chữ cái khác nhau từ các ngôn ngữ khác nhau thực sự có thể xuất hiện giống hệt nhau. Ví dụ, ký tự Unicode U+0430 (chữ cái thường a của chữ Kirin) trông giống hệt với ký tự Unicode U+0061 (chữ cái thường a của chữ Latin) được sử dụng trong tiếng Anh, cho phép kẻ tấn công đăng ký một tên miền trông gần như giống hệt với một tên miền khác.

A screenshot of a computer screen

Description automatically generated

1. **Using MS Office In Phishing**

Thông thường trong các chiến dịch lừa đảo, tài liệu Microsoft Office (thường là Word, Excel hoặc PowerPoint) sẽ được đính kèm dưới dạng tệp đính kèm. Tài liệu văn phòng có thể chứa **macro**; macro có mục đích sử dụng hợp pháp nhưng cũng có thể được sử dụng để chạy các lệnh máy tính có thể khiến phần mềm độc hại được cài đặt vào máy tính của nạn nhân hoặc kết nối lại với mạng của kẻ tấn công và cho phép kẻ tấn công chiếm quyền kiểm soát máy tính của nạn nhân.

Một nhân viên làm việc cho bộ phận Hỗ trợ CNTT của Acme nhận được email từ bộ phận nhân sự kèm theo bảng tính excel có tên "Staff\_Salaries.xlsx" định gửi đến gặp sếp nhưng bằng cách nào đó lại chuyển vào hộp thư đến của nhân viên.

Điều thực sự đã xảy ra là kẻ tấn công đã giả mạo địa chỉ email của bộ phận nhân sự và tạo ra một email lôi cuốn về mặt tâm lý một cách hoàn hảo nhằm dụ nhân viên mở tệp đính kèm.

Sau khi nhân viên mở tệp đính kèm và bật **macro**, máy tính của họ sẽ bị xâm phạm.

1. **Using Browser Exploits**

Một phương pháp khác để giành quyền kiểm soát máy tính của nạn nhân có thể là thông qua việc khai thác trình duyệt; đây là khi có lỗ hổng trên chính trình duyệt (Internet Explorer/Edge, Firefox, Chrome, Safari, v.v.), cho phép kẻ tấn công chạy các lệnh từ xa trên máy tính của nạn nhân.

Việc khai thác trình duyệt thường không phải là con đường phổ biến để thực hiện khi tham gia vào nhóm đỏ trừ khi bạn có kiến ​​thức trước về công nghệ cũ đang được sử dụng tại chỗ. Nhiều trình duyệt được cập nhật, khó khai thác do cách trình duyệt được phát triển và việc khai thác thường có giá trị rất lớn nếu được báo cáo lại cho nhà phát triển.

Nói như vậy, điều đó có thể xảy ra và như đã đề cập trước đó, nó có thể được sử dụng để nhắm mục tiêu vào các công nghệ cũ tại chỗ vì có thể phần mềm trình duyệt không thể cập nhật do không tương thích với phần mềm/phần cứng thương mại, điều này có thể xảy ra khá thường xuyên ở các tổ chức lớn như như giáo dục, chính phủ và đặc biệt là chăm sóc sức khỏe.

Thông thường, nạn nhân sẽ nhận được email thuyết phục họ truy cập một trang web cụ thể do kẻ tấn công thiết lập. Sau khi nạn nhân truy cập vào trang web, việc khai thác sẽ hoạt động dựa trên trình duyệt và giờ đây kẻ tấn công có thể thực hiện bất kỳ lệnh nào chúng muốn trên máy tính của nạn nhân.

Một ví dụ về điều này là CVE-2021-40444 từ tháng 9 năm 2021, đây là một lỗ hổng được tìm thấy trong các hệ thống của Microsoft cho phép thực thi mã chỉ bằng cách truy cập một trang web.

1. **Phishing Practical**

Phân biệt email phishing hay email safe