TẤN CÔNG VÀ PHÒNG THỦ HỆ THỐNG

Chương 8. Các tấn công khác (phần 1)

Phân công công việc	Slide
Nguyễn Bá Tiến	1-13
Bùi Thị Thư Thư	14-25
Bùi Thị Thúy	26-34
Dương Thị Thu Thìn	35-hết

Kỹ Nghệ Xã Hội

Mục Tiêu Mô - Đun

Mục Tiêu

- *Hiểu các khái niệm kỹ thuật xã hội*
- *Hiểu biết các kỹ thuật xây dựng xã hội khác nhau*
- *Hiểu các mối đe dọa từ người trong cuộc*
- *Tìm hiểu về mạo danh trên các trang wed mạng xã hội*
- *Hiểu trộm danh tính*
- *Hiểu các biện pháp đối phó với kỹ thuật xã hội khác nhau*
- *Tổng quan về thử nghiệm thâm nhập kỹ thuật*

1. Khái niệm kỹ thuật xã hội
2. Kỹ thuật xã hội
3. Mối đe dọa nội gián
4. Mạo danh trên các trang mạng xã hội
5. Hành vi trộm cắp danh tính
6. Biện pháp đối phó
7. Kiểm thử các kỹ thuật xã hội

Thế nào là kỹ nghệ xã hội ?

- Kỹ thuật xã hội là một nghệ thuật thao túng mọi người tiết lộ thông tin nhạy cảm
- Mục tiêu chung của kỹ nghệ xã hội là các nhân viên , hệ thống quản trị viên,...
- Các kỹ sư kỹ nghệ phụ thuộc vào thực tế rằng mọi người không biết thông tin có giá trị của họ và bất cẩn trong việc bảo vệ nó

Tác động của tấn công vào tổ chức

- Thiệt hại kinh tế
- Thiệt hại lợi ích thương mại
- Sự mất riêng tư
- Nguy cơ khủng hoảng
- Kiện tụng
- Đóng cửa tạm thời hoặc vĩnh viễn

Các hành vi dễ bị tấn công

- Bản chất của sự tin tưởng
- Sự thiếu hiểu biết về kỹ nghệ xã hội
- Lòng tham
- Tuân theo nghĩa vụ đạo đức

Thế nào là kỹ nghệ xã hội ?

Các yếu tố khiến công ty dễ bị tấn công

- Đào tạo bảo mật không đầy đủ
- Truy cập thông tin không được kiểm soát
- Một số đơn vị tổ chức
- Thiếu chính sách bảo mật

Tại sao kỹ nghệ xã hội lại hiệu quả

- Các chính sách bảo mật mạnh như mắt xích yếu nhất của chúng và con người là yếu tố dễ bị ảnh hưởng nhất
- Rất khó để phát hiện
- Không có biện pháp nào đảm bảo an ninh hoàn toàn khỏi kỹ nghệ xã hội
- Không có phần mềm hoặc phần cứng cụ thể nào bảo vệ lại một cuộc tấn công kỹ nghệ xã hội

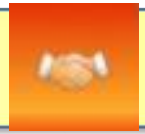
Các giai đoạn của cuộc tấn công kỹ nghệ xã hội

Nghiên cứu về công ty mục tiêu

Dumpster lặn , trang wed , nhân viên , công ty du lịch ,...

Chọn nạn nhân

Xác định những nhân viên có sơ hở của công ty



Phát Triển mối quan hệ

Phát triển mối quan hệ với nhân viên đã chọn

Khai thác mối quan hệ

Thu thập thông tin tài khoản

1. Khái niệm kỹ thuật xã hội
2. Kỹ thuật xã hội
3. Mối đe dọa nội gián
4. Mạo danh trên các trang mạng xã hội
5. Hành vi trộm cắp danh tính
6. Biện pháp đối phó
7. Kiểm thử các kỹ thuật xã hội

Kỹ thuật xã hội dựa trên con người

- Thu thập thông tin bằng cách giảm tương tác
- Kỹ thuật
  - Mạo danh
  - Kỹ thuật đảo ngược xã hội
  - Tailgating
  - Vishing
  - Dò tìm bãi phế thải
  - Nghe lén
  - Lướt qua vai
  - Piggybacking

Kỹ thuật xã hội dựa trên máy tính

- Kỹ nghệ xã hội thực hiên với sự giúp đỡ của máy tính
- Kỹ thuật
  - Lừa đảo
  - Tấn công cửa sổ bật lên
  - . Trò chuyện tức thời
  - . Thư rác

Kỹ nghệ xã hội dựa trên thiết bị di động

- Thực hiện với sự giúp đỡ của các thiết bị di động
- Kỹ thuật
  - Xuất bản ứng dụng độc hại
  - Sử dụng ứng dụng bảo mật giả
  - . Đóng gói lại các ứng dung hợp pháp
  - . Lừa đảo qua SMS

Kỹ thuật xã hội dựa trên con người

- Đây là kỹ thuật xã hội dựa trên con người phổ biến nhất mà kẻ tấn công giả làm ai đó hợp pháp hoặc một người ủy quyền
- Những kẻ tấn công có thể mạo danh một người hợp pháp hoặc cá nhân hoặc sử dụng phương thức liên lạc điện thoại , email ,....
- Mạo danh giúp kẻ tấn công lừa mục tiêu để tiết lộ thông tin nhạy cảm

Ví dụ về Mạo danh

Tạo dáng như một người dùng hợp pháp

Cung cấp danh tính và thông tin nhạy cảm

Ví dụ : tôi là A từ bộ phận tài chính có thể lấy ID của mình được không?

Tạo dáng như một người dùng quan trọng

Đóng vai trò Vip của một công ty , khách hang cao cấp ,....

Ví dụ : đây là Thư ký giám đốc , bạn có thể giúp tôi lấy lại mật khâu được không

Tạo dáng như một hỗ trỡ kỹ thuật

Gọi với tư cách nhân viên kỹ thuật và yêu cầu ID và mật khẩu

Ví dụ đây là công ty X , hỗ trợ kỹ thuật , hôm qua tôi gặp sự cố ở đây , bạn có thể cung cấp mật khẩu cho tôi được không

Kỹ thuật lừa đảo dựa trên con người (Vishing)

- Vishing(lừa đảo bằng giọng nói hoặc VoIP) là một kỹ thuật mạo danh (lừa đảo điện tử) trong đó kẻ tấn công đánh lừa các cá nhân để tiết lộ thông tin cá nhân và tài chính bằng cách sử dụng công nghệ thoại như hệ thống điện thoại , VoIP,...

Ví dụ

Sự hữu ích của bộ phận trợ giúp

- Tại đây kẻ tấn công gọi đến bàn trợ giúp của công ty , giả vờ là một người nào đó có chức có quyền hạn hoặc có liên quan và cố gắng trích xuất thông tin từ bàn trợ giúp

Ủy quyền bên thứ 3

- Ở đây kẻ tấn công có được tên nhân viên được ủy quyền của tổ chức được nhắm mục tiêu , người có quyền được truy cập vào thông tin mà anh ta/ cô ta muốn
- Tiếp kẻ tấn công thực hiện cuộc gọi đến tổ chức để tuyên bố rằng một nhân viên đã cung cấp thông tin đó

Hỗ trợ kỹ thuật

- Tại đây kẻ tấn công giả làm nhân viên kỹ thuật của các nhà cung cấp phầm mềm của tổ chức mục tiêu
- Anh ấy/ cô ấy có thể yêu cầu thông tin và mật khẩu để khắc phục sự cố tổ chức

Kỹ thuật xã hội dựa trên con người

Nghe lén (Eavesdropping)

- Nghe trộm, nghe trái phép cuộc trò chuyện hoặc đọc tin nhắn
- Chặn âm thanh, video hoặc thông tin liên lạc.
- Nó có thể được thực hiện bằng các kênh liên lạc như đường dây điện thoại, email, tin nhắn tức thời, v.v.

Lướt sóng vai (Shoulder Surfing)

- Sử dụng các kỹ thuật quan sát trực tiếp như nhìn qua vai ai đó để lấy thông tin: mật khẩu, mã PIN, số tài khoản, v.v.
- Nó cũng có thể được thực hiện từ khoảng cách xa hơn với sự hỗ trợ của các thiết bị tăng cường thị lực như ống nhòm, v.v.

Dò tìm bãi phế thải (Dumpster Diving)

- Là tìm kiếm kho báu trong thùng rác của người khác
- Việc thu thập hóa đơn điện thoại, thông tin liên lạc, thông tin tài chính, liên quan đến hoạt động của công ty, thùng rác máy in, ghi chú, v.v.

Kỹ thuật xã hội dựa trên con người

Kỹ thuật đảo ngược xã hội

Đây là tình huống mà kẻ tấn công tự thể hiện mình là một người có thẩm quyền và mục tiêu tìm kiếm lời khuyên của họ sau hoặc trước khi cung cấp thông tin mà anh ta cần

Piggybacking

-"Tôi quên thẻ căn cước ở nhà. Xin hãy giúp tôi."

- Người được ủy quyền cho phép (cố ý hoặc vô ý) người không được ủy quyền đi qua cửa an toàn

Tailgating

Tại đây, một người không được phép, đeo thẻ ID giả, đi vào khu vực an toàn bằng cách theo sát người được ủy quyền qua một cánh cửa yêu cầu chìa khóa truy cập.

Kỹ thuật xã hội dựa trên máy tính

Cửa sổ bật lên Có những cửa sổ đột nhiên bật lên khi đang lướt Internet và yêu cầu thông tin của người dùng để đăng nhập hoặc đăng nhập

Hoax Letters Thư Hoax là các email đưa ra cảnh báo cho người dùng về vi-rút, Trojan hoặc sâu có thể gây hại cho hệ thống

Chuỗi thư Chuỗi thư là các email cung cấp quà tặng miễn phí như tiền và phần mềm với điều kiện người dùng phải chuyển tiếp thư tới số id của một người.

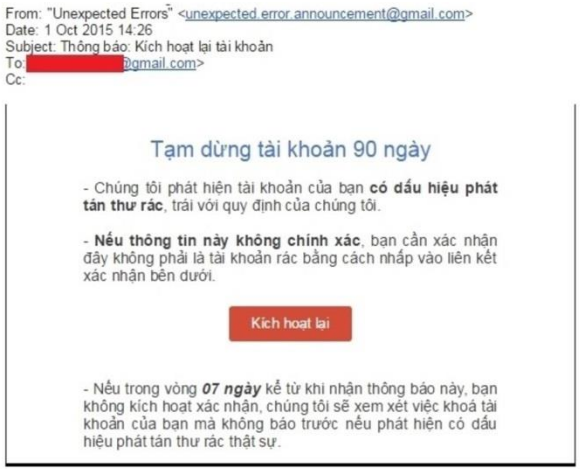
Tin nhắn trò chuyện tức thì Thu thập thông tin cá nhân bằng cách trò chuyện với một người dùng trực tuyến được chọn để nhận thông tin như ngày tháng năm sinh và tên thời con gái

Thư rác Email không liên quan, không mong muốn và không được yêu cầu để thu thập thông tin tài chính, số an sinh xã hội và thông tin mạng

Kỹ thuật xã hội dựa trên máy tính

Phishing

- Là hành vi gửi một email bất hợp pháp giả mạo là từ một trang web hợp pháp nhằm cố gắng lấy thông tin cá nhân hoặc tài khoản của người dùng
- Email lừa đảo hoặc cửa sổ bật lên chuyển hướng người dùng đến các trang web giả mạo bắt chước trang web đáng tin cậy yêu cầu user gửi thông tin cá nhân


From: "Unexpected Errors" <unexpected.error.announcement@gmail.com>
Date: 1 Oct 2015 14:26
Subject: Thông báo: Kích hoạt lại tài khoản
To: [redacted]@gmail.com>
Cc:

Tạm dừng tài khoản 90 ngày

- Chúng tôi phát hiện tài khoản của bạn **có dấu hiệu phát tán thư rác**, trái với quy định của chúng tôi.

- **Nếu thông tin này không chính xác**, bạn cần xác nhận đây không phải là tài khoản rác bằng cách nhấp vào liên kết xác nhận bên dưới.

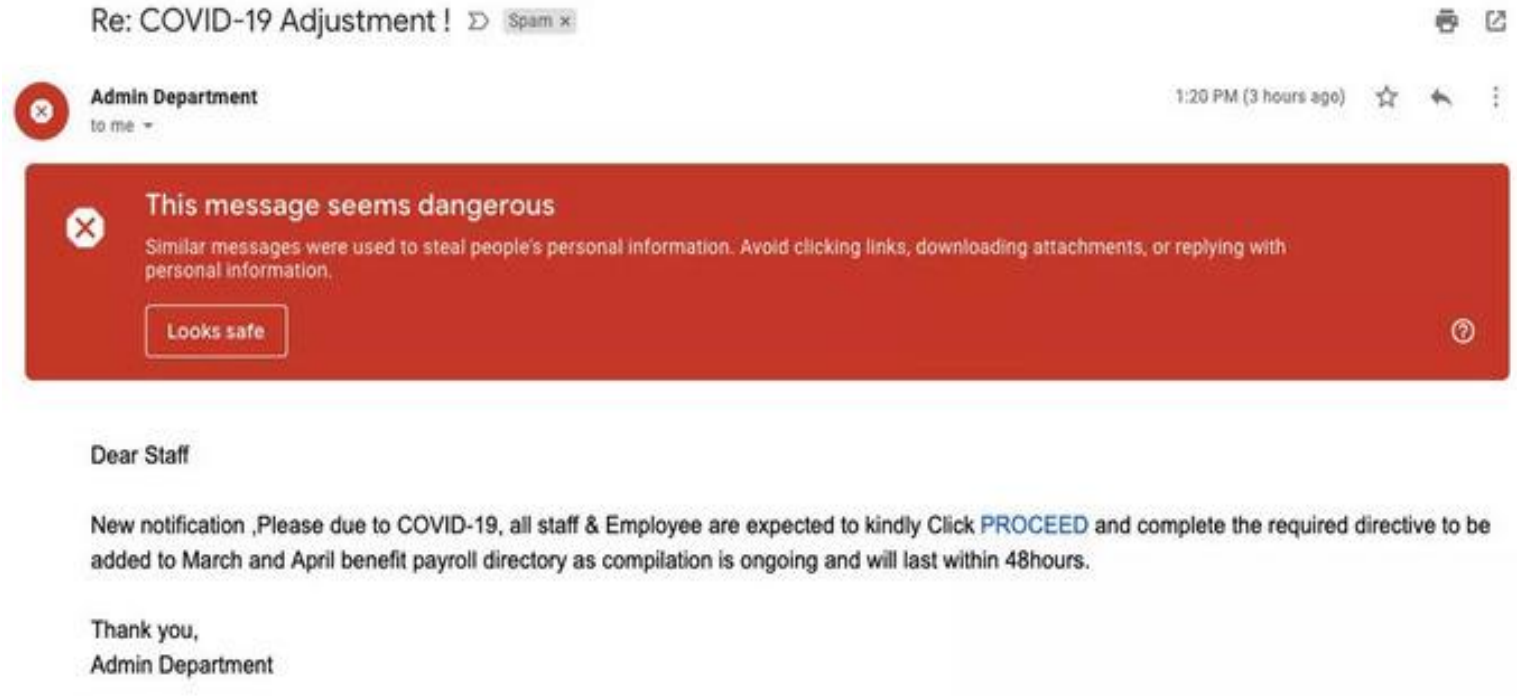
Kích hoạt lại

- Nếu trong vòng ***07 ngày*** kể từ khi nhận thông báo này, bạn không kích hoạt xác nhận, chúng tôi sẽ xem xét việc khoá tài khoản của bạn mà không báo trước nếu phát hiện có dấu hiệu phát tán thư rác thật sự.

Kỹ thuật xã hội dựa trên máy tính

Phishing(tt)

- *Ví dụ về thư lừa đảo:*



Kỹ thuật xã hội dựa trên máy tính

Lừa đảo lấy thông tin mật

- Một cuộc tấn công lừa đảo nhắm vào các cá nhân cụ thể trong một tổ chức
- Kẻ tấn công sử dụng trò lừa đảo trực tuyến để gửi tin nhắn có nội dung chuyên biệt, nhắm vào một người cụ thể hoặc một nhóm nhỏ

Whaling

- Nhắm mục tiêu vào Giám đốc điều hành, Giám đốc tài chính, chính trị gia, người nổi tiếng, người có quyền truy cập, thông tin giá trị cao
- Lừa nạn nhân tiết lộ thông tin cá nhân và công ty qua email hoặc giả mạo trang web

Pharming

- Kẻ tấn công chuyển hướng lưu lượng truy cập đến web lừa đảo qua cách cài đặt chương trình độc hại trên máy tính cá nhân, máy chủ
- Pharming cũng giống như "Lừa đảo không có Lure" được thực hiện bằng cách dùng DNS Cache Poisoning hoặc Host File Modification

Spimming

- Là một biến thể của spam khai thác các nền tảng Nhắn tin tức thời để tràn ngập spam trên các mạng
- Người dùng tấn công bot để thu thập ID tin nhắn tức thì và phát tán thư rác

Kỹ thuật xã hội dựa trên thiết bị di động

Xuất bản các ứng dụng độc hại

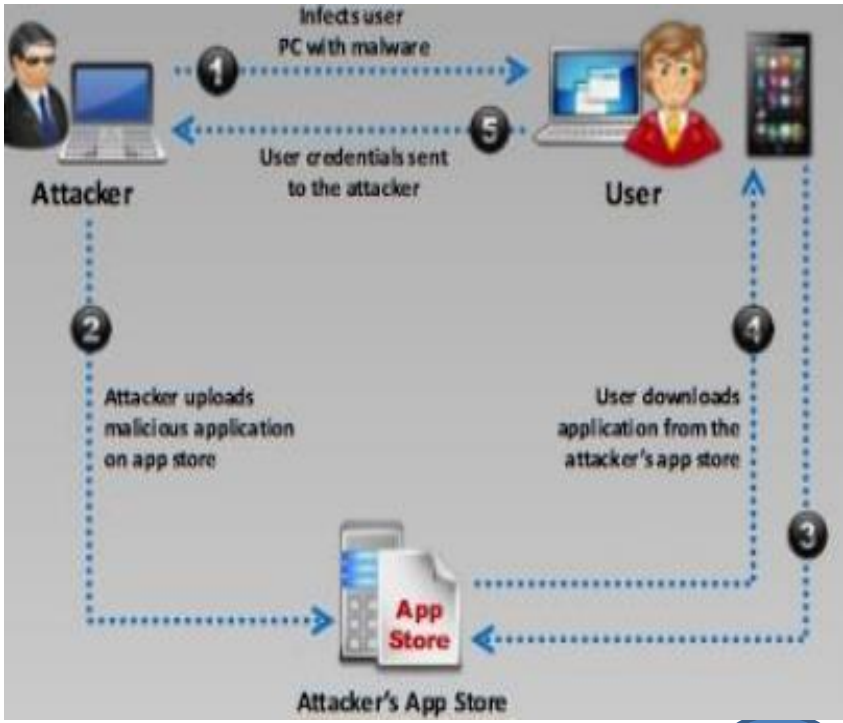
- Kẻ tấn công tạo ra app độc hại với tính năng hấp dẫn và tên tương tự với tên các app phổ biến, upload chúng trên App store
- Người dùng tải xuống các app này và bị nhiễm phần mềm độc hại gửi thông tin đăng nhập cho những kẻ tấn công

Đóng gói lại các ứng dụng hợp pháp

Kỹ thuật xã hội dựa trên thiết bị di động

Ứng dụng bảo mật giả mạo

1. Kẻ tấn công lây nhiễm vào máy tính của nạn nhân
2. Kẻ tấn công tải ứng dụng độc hại lên cửa hàng ứng dụng
3. Nạn nhân login vào tài khoản ngân hàng của mình. Phần mềm độc hại trong hệ thống hiển thị lên thông báo yêu cầu tải xuống đth để nhận tin nhắn bảo mật
4. Nạn nhân tải xuống ứng dụng độc hại vào điện thoại của mình
5. Lúc này, kẻ tấn công có thể truy cập yếu tố xác thực thứ hai được gửi đến từ ngân hàng qua SMS



Kỹ thuật xã hội dựa trên thiết bị di động

SMiShing(SMS PhiShing)

- SMiShing (SMS Phishing) là hành vi sử dụng hệ thống nhắn tin văn bản SMS của điện thoại di động hoặc các thiết bị di động khác để dụ nạn nhân thực hiện hành động tức thì như tải xuống phần mềm độc hại, truy cập trang web độc hại hoặc gọi đến một số điện thoại lừa đảo
- Thông báo SMiShing thường được tạo ra để kích động nạn nhân hành động tức thì, yêu cầu họ tiết lộ thông tin cá nhân và chi tiết tài khoản của họ

Ví dụ:

Kỹ thuật xã hội dựa trên thiết bị di động

SMiShing(SMS PhiShing)

1 Tracy đã nhận được một tin nhắn SMS (tin nhắn văn bản), có vẻ như là từ bộ phận an ninh của Ngân hàng XIM

2 Nó được cho là khẩn cấp và Tracy nên gọi số điện thoại trong tin nhắn SMS ngay lập tức. Lo lắng, cô ấy đã gọi điện để kiểm tra tài khoản của mình

3 Cô ấy gọi vì nghĩ rằng đó là số dịch vụ khách hàng của Ngân hàng XIM và đó là một đoạn ghi âm yêu cầu cung cấp số thẻ tín dụng hoặc thẻ ghi nợ của cô ấy

4 Có thể dự đoán, Tracy đã tiết lộ thông tin nhạy cảm do các văn bản lừa đảo

1. Khái niệm kỹ thuật xã hội
2. Kỹ thuật xã hội
3. Mối đe dọa nội gián
4. Mạo danh trên các trang mạng xã hội
5. Hành vi trộm cắp danh tính
6. Biện pháp đối phó
7. Kiểm thử các kỹ thuật xã hội

Mối đe dọa nội gián/ Tấn công nội gián

- Là bất kỳ nhân viên nào có quyền truy cập vào các tài sản quan trọng của tổ chức
- Một cuộc tấn công nội gián sử dụng quyền truy cập đặc quyền cố tình vi phạm các quy tắc hoặc gây ra mối đe dọa đối với thông tin, hệ thống thông tin của tổ chức dưới mọi hình thức
- Tấn công nội gián thường thực hiện bởi người dùng có đặc quyền, nhân viên bất mãn, nhân viên bị chấm dứt hợp đồng, nhân viên do tai nạn, bên thứ ba, v.v.

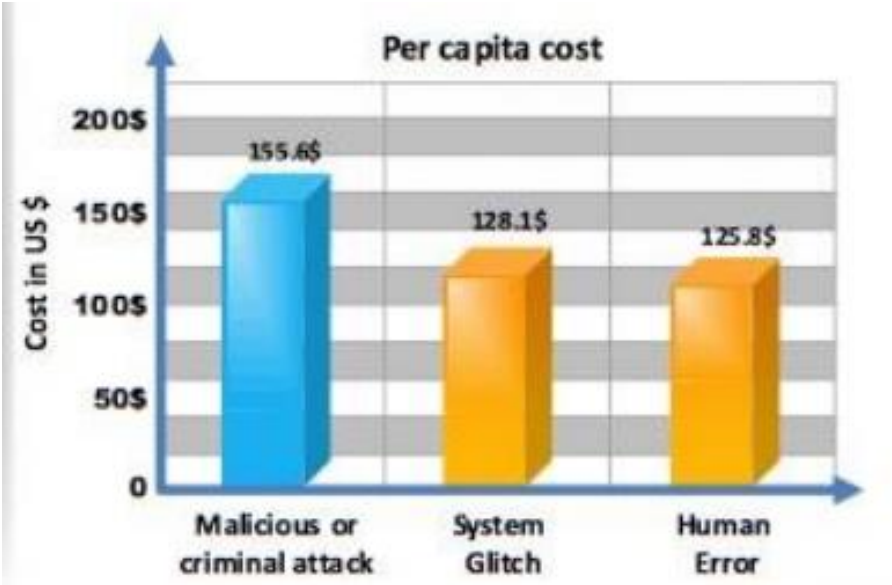
Lý do cho các cuộc tấn công Nội gián:

- Lợi nhuận tài chính
- Đánh cắp dữ liệu bí mật
- Trả thù
- Trở thành đối thủ cạnh tranh trong tương lai
- Thực hiện đặt giá thầu đối thủ cạnh tranh
- Thông báo công khai

Mối đe dọa nội gián/ Tấn công nội gián

Thống kê mối đe dọa nội bộ

Theo một Nghiên cứu về vi phạm dữ liệu có chi phí kỳ lạ năm 2017, một cuộc tấn công bởi một kẻ nội gián độc hại hoặc tội phạm sẽ gây giá trị thiệt hại hơn sự cố hệ thống và sơ suất (yếu tố con người)



Các loại mối đe dọa nối gián

Nội gián độc hại

- Nhân viên bất mãn/bị chấm dứt hợp đồng ăn cắp dữ liệu /phá hủy mạng của công ty trên toàn thế giới bằng cách đưa phần mềm độc hại vào mạng công ty

Người trong cuộc không cẩn thận

- Những người trong cuộc không được đào tạo về các mối đe dọa an ninh tiềm ẩn hoặc chỉ đơn giản là bỏ qua các quy trình an ninh chung đáp ứng hiệu quả tại nơi làm việc

Người trong cuộc chuyên nghiệp

- Người trong cuộc có hại, người sử dụng kiến thức kỹ thuật của họ để xác định các điểm yếu và lỗ hổng của mạng công ty và bán thông tin bí mật cho các đối thủ cạnh tranh hoặc các nhà thầu chợ đen

Người trong cuộc được thỏa hiệp

Đây là người trong cuộc có quyền truy cập vào các tài sản quan trọng của một tổ chức bị xâm phạm bởi một tác nhân đe dọa bên ngoài

Tại sao tấn công nội gián lại hiệu quả?

- Rất dễ dàng khởi chạy
- Phòng ngừa khó
- Có thể dễ thành công
- Người được tuyển dụng dễ dàng che đậy hành động của họ
- Rất khó để phân biệt các hành động có hại với công việc thường xuyên của nhân viên
- Nó không thể phát hiện trong nhiều năm và việc khắc phục rất tốn kém

1. Khái niệm kỹ thuật xã hội
2. Kỹ thuật xã hội
3. Mối đe dọa nội gián
4. Mạo danh trên các trang mạng xã hội
5. Hành vi trộm cắp danh tính
6. Biện pháp đối phó
7. Kiểm thử các kỹ thuật xã hội

Kỹ nghệ xã hội thông qua công nghệ trên các trang Web mạng xã hội

01	Người dùng độc hại tập hợp thông tin bí mật trên các trang mạng xã hội và tạo những tài khoản với tên người dung khác nhau
02	Kẻ tấn công sử dụng thông tin cá nhân của người khác để tạo một mạng lưới những người bạn bè với thông tin chính xác sử dụng kỹ thuật kỹ nghệ xã hội
03	Kẻ tấn công cố gắng tham gia vào nhóm nhân viên của tổ chức nơi mà có chia sẻ thông tin cá nhân và thông tin về công ty
04	Kẻ tấn công cũng có thể sử dụng thông tin thu thập được để thực hiện các hình thức tấn công kỹ nghệ xã hội khác

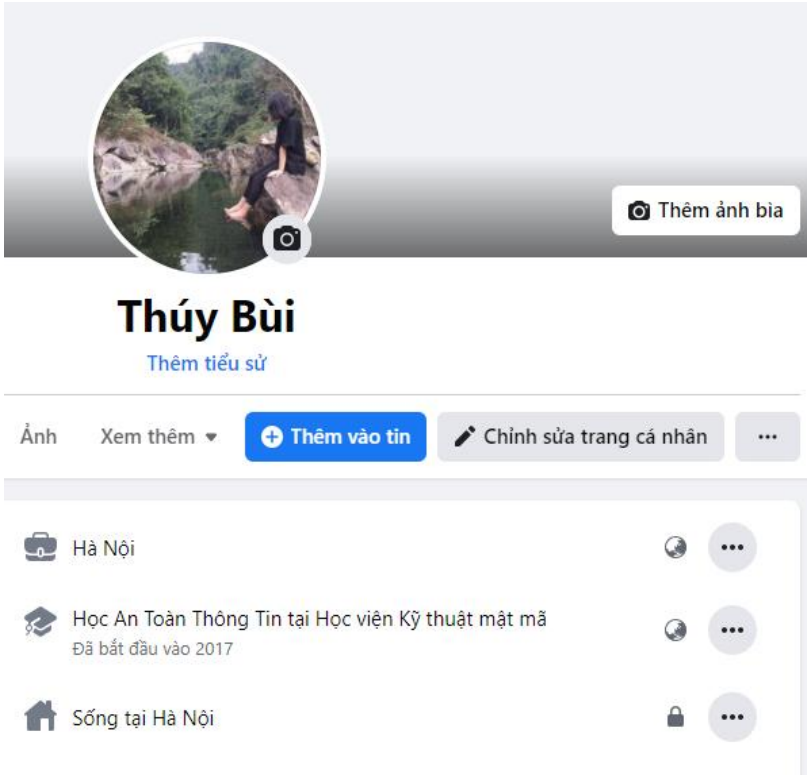
Mạo danh Facebook

Những kẻ tấn công tạo một nhóm người dùng giả mạo trên Facebook được xác định là "Nhân viên" của công ty mục tiêu

Sử dụng danh tính giả, kẻ tấn công sau đó tiến tới " bạn bè", hoặc mời nhân viên vào nhóm giả mạo "nhân viên của công ty"

Người dùng gia nhập nhóm và cung cấp những chứng thực của họ như ngày sinh, trường học,....

Bằng cách sử dụng bất kì thông tin chi tiết của nhân viên nào, kẻ tấn công có thể xâm phạm cơ sở bảo mật để truy cập vào tòa nhà



Mối đe dọa từ mạng xã hội đối với mạng công ty

1	Trộm dữ liệu
2	Rò rỉ dữ liệu không tự nguyện
3	Các cuộc tấn công có mục tiêu
4	Lỗ hổng mạng
5	Spam và Phising
6	Sửa đổi nội dung
7	Lan truyền phầm mềm độc hại
8	Độ phổ biến doanh nghiệp
9	Chi phí cơ sở hạ tầng và bảo trì
10	Mất năng suất

1. Khái niệm kỹ thuật xã hội
2. Kỹ thuật xã hội
3. Mối đe dọa nội gián
4. Mạo danh trên các trang mạng xã hội
5. Hành vi trộm cắp danh tính
6. Biện pháp đối phó
7. Kiểm thử các kỹ thuật xã hội

Trộm cắp danh tính

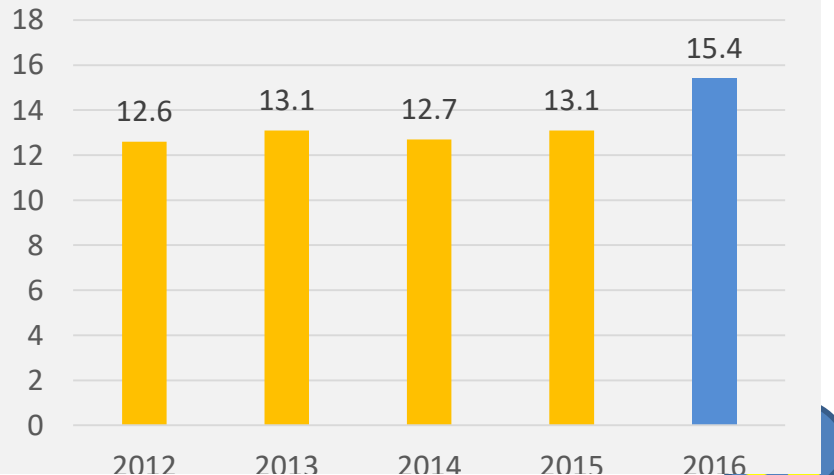
- Hành vi trộm cắp danh tính xảy ra khi ai đó đánh cắp thông tin nhận dạng cá nhân của bạn cho mục đích lừa đảo
- Đó là một tội ác trong đó kẻ mạo danh có được thông tin nhận dạng như Tên, số giấy phép lái xe, số tài khoản ngân hang….để thực hiện hành vi gian lận hay mục đích khác
- Kẻ tấn công có thể sử dụng những định danh trộm được với mục tiêu mạo danh nhân viên của tổ chức và truy cập vào cơ sở

Loại trộm cắp danh tính

- Trộm cắp danh tính trẻ em
- Trộm cắp danh tính tội phạm
- Trộm cắp nhận dạng tài chính
- Trộm cắp định danh giấy phép lái xe
- Trộm cắp nhận dạng bảo hiểm
- Trộm cắp nhận dạng y tế
- Đánh cắp nhận dạng thuế
- Nhân bản và che dấu danh tính
- Đánh cắp danh tính tổng hợp
- Đánh cắp danh tính xã hội

Số Lượng Truy Cập Gian Lận ID Cao Kỷ Lục

Gian lận danh tính đạt mức cao kỷ lục với 15.4 triệu nạn nhân Hoa Kỳ vào năm 2016, tăng 16%



Trộm cắp danh tính

Trộm ví, máy tính,laptop…	Pretexting	Những thay đổi bất thường về thẻ tín dụng mà bạn không nhận ra
Tìm kiếm trên Internet	Pharming	Không nhận được bảng sao kê thẻ tín dụng, ngân hang…
Kỹ nghệ xã hội	Hacking	Nhận được cuộc gọi từ bộ phận kiểm soát gian lận thẻ tín dụng hoặc thẻ ghi nợ
Dumpster diving và đọc lướt ván	Phần mềm độc hại	Các khoản phí điều trị y tế hoặc các dịch vụ bạn chưa bao giờ nhận được
Phising	Wardriving	Không nhận được hóa đơn dịch vụ gas, nước, hóa đơn…..
Skimming	Đánh cắp nội gián	

1. Khái niệm kỹ thuật xã hội
2. Kỹ thuật xã hội
3. Mối đe dọa nội gián
4. Mạo danh trên các trang mạng xã hội
5. Hành vi trộm cắp danh tính
6. Biện pháp đối phó
7. Kiểm thử các kỹ thuật xã hội

Các biện pháp đối phó với kỹ nghệ xã hội

- Các chính sánh và thủ tục tốt sẽ không hiệu quả nếu không được dạy và củng cố cho nhân viên
- Sau những buổi đào tại, nhân viên nên ký 1 tuyên bố xác nhận là họ đã hiểu các chính sách
- Mục tiêu chính của các chiến lược phòng ngừa kỹ nghệ xã hội là tạo ra nhận thức người dùng, kiểm soát mạng nội bộ mạnh mẽ và các chính sách, kế hoạch và quy trình an toàn

Chính sách mật khẩu

- Thay đổi mật khẩu định kỳ
- Tránh sử dụng mật khẩu dễ đoán
- Khóa tài khoản sau những lần đăng nhập không thành công
- Độ dài và độ phức tạp của mật khẩu
- Bí mật của mật khẩu

Chính sách an ninh vật lý

- Nhận dạng nhân viên bằng cách cấp thẻ căn cước, đồng phục…
- Hộ tống du khách
- Hạn chế khu vực tiếp cận
- Cắt nhỏ tài liệu không dùng tới đúng cách
- Sử dụng nhân viên an ninh

Chiến lược phòng thủ

- Chiến dịch kỹ nghệ xã hội
- Phân tích khoảng cách
- Chiến lược khắc phục hậu quả

Các biện pháp đối phó với kỹ nghệ xã hội

1. Đào tạo cá nhân về chính sách bảo mật
2. Thực hiện các đặc quyền truy nhập thích hợp
3. Có thời gian ứng phó sự cố thích hợp
4. Chỉ người dùng ủy quyền có sẵn tài nguyên
5. Xem xét kỹ lưỡng thông tin
6. Kiểm tra lý lịch và quá trình xác định phù hợp
7. Phòng chống virus, thư rác...
8. Triển khai xác thực 2 yếu tố
9. Áp dụng quản lý thay đổi bằng văn bản
10. Đảm bảo cập nhật thường xuyên phần mềm

Các biện pháp đối phó với các mối đe dọa nội gián

1 Tách biệt và luân chuyển nhiệm vụ

2 Đặc quyền nhất

3 Truy cập có kiểm soát

4 Logging và kiểm toán

5 Giám sát nhân viên

6 Chính sách pháp lý

7 Lưu lượng dữ liệu quan trọng

8 Đào tạo nhân viên về an ninh mạng

9 Xác minh lý lịch của nhân viên

10 Đánh giá rủi ro định kỳ

11 Giám sát người dùng đặc quyền

12 Hủy kích hoạt thông tin đăng nhập với người không còn là nhân viên

Biện pháp đối phó chống trộm cắp danh tính

- Bảo mật hoặc chia nhỏ tất cả các tài liệu có chứa thông tin cá nhân
- Đảm bảo tên của bạn không có trong danh sách truy cập của các nhà tiếp cận
- Xem lại báo cáo thẻ tín dụng của bạn thường xuyên
- Không bao giờ cung cấp bất kỳ thông tin cá nhân nào vào điện thoại
- Để giữ thư của bạn an toàn, hãy làm trống hộp thư nhanh chóng
- Nghi ngờ và xác minh tất cả các yêu cầu về dữ liệu cá nhân
- Bảo vệ thông tin cá nhân của bạn khỏi bị công khai
- Không hiển thị số tài khoản/ số liên lạc trừ khi bắt buộc
- Giám sát hoạt động ngân hàng trực tuyến thường xuyên
- Không bao giờ liệt kê bất kỳ định danh cá nhân nào trên các trang web truyền thông xã hội như tên của bố mẹ, địa chỉ, thành phố sinh, v.v

Biện pháp đối phó chống trộm cắp danh tính

Ngoài ra còn một số biện pháp khác như:

- Để giữ thư của bạn an toàn, hãy làm trống hộp thư của bạn một cách nhanh chóng và không trả lời các yêu cầu email không mong muốn yêu cầu thông tin cá nhân

- Không lưu trữ bất kỳ thông tin tài chính nào trên hệ thống và sử dụng mật khẩu mạnh cho tất cả các tài khoản tài chính.

- Kiểm tra hóa đơn điện thoại và điện thoại di động cho các cuộc gọi bạn không thực hiện.

- Giữ thẻ CMT, hộ chiếu, giấy phép và thông tin cá nhân có giá trị khác được ẩn và khóa

- Đọc chính sách bảo mật trang web.

- Hãy thận trọng trước khi nhấp vào liên kết được cung cấp trong hộp email hoặc tin nhắn tức thời.

Thanh công cụ chống lừa đảo

Netcraft

- Cung cấp cập nhập thông tin về trang web mà người dùng truy cập thường xuyên và cảnh báo các trang web nguy hiểm.
- Cung cấp thông tin về trang web mà người dùng truy cập.

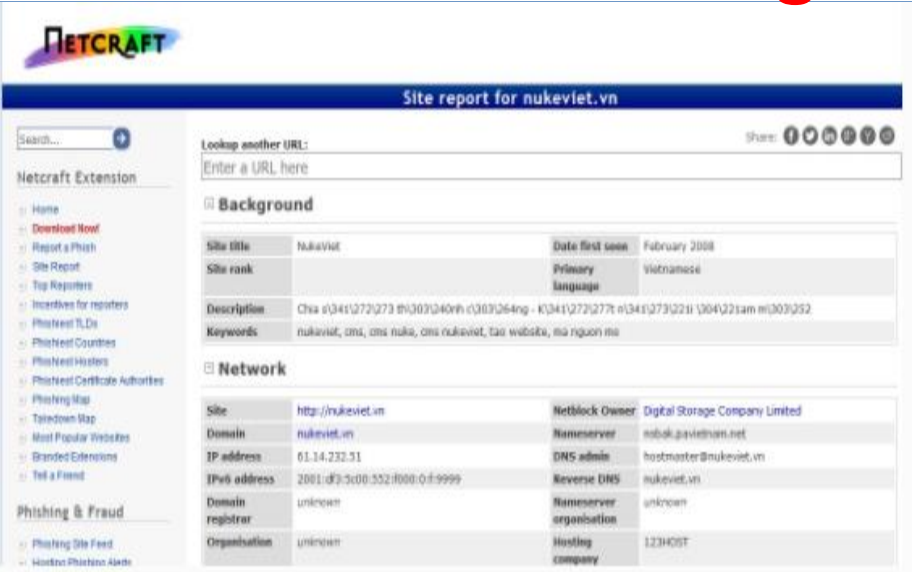
Features

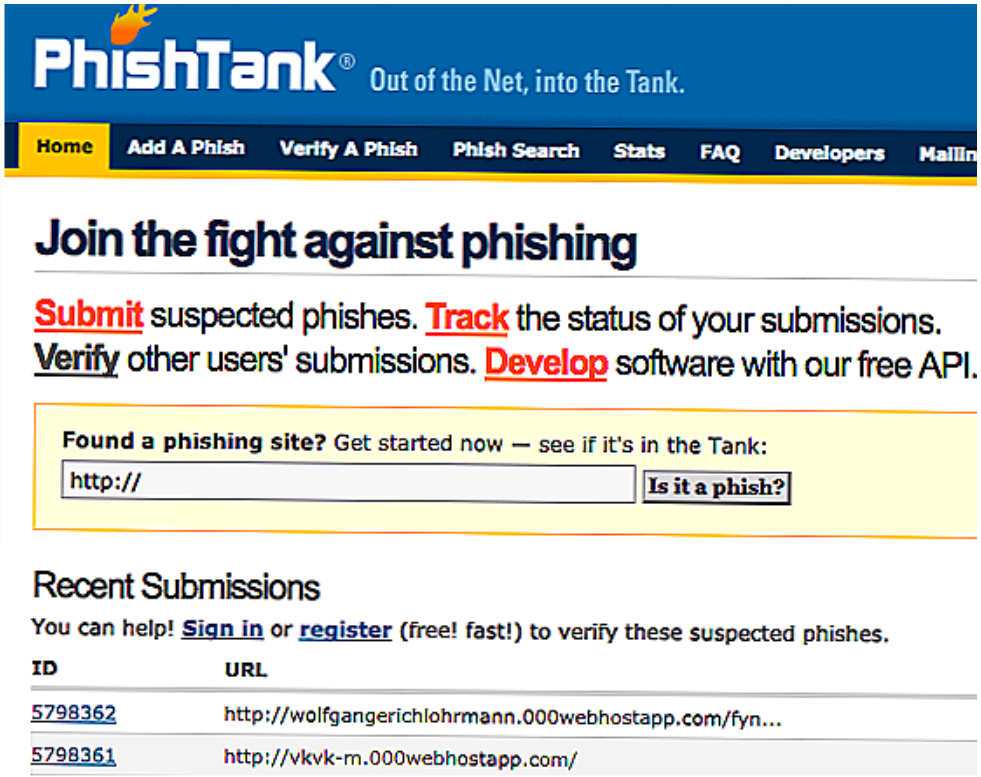
- Quan sát vị trí lưu trữ và xếp hạng rủi ro của mọi lần truy cập
- Kiểm tra trang web có hỗ trợ Perfect Forward (PFS)
- Quan sát xem trang web có bị ảnh hưởng của lỗ hổng Heartbleed không

Phis Tank

- Cung cấp một API mở cho các nhà phát triển mà các nhà nghiên cứu để tích hợp dữ liệu chống lừa đảo vào các ứng dụng của họ.

Thanh công cụ chống lừa đảo





Đối tượng dễ bị tấn công bởi Social Engineering

- Những kẻ tấn công thực hiện các kỹ thuật xã hội khác nhau để lừa mọi người cung cấp thông tin nhạy cảm về tổ chức của họ, giúp những kẻ tấn công tung ra các hoạt động độc hại, các kỹ thuật được sử dụng cho các cá nhân đặc quyền, hoặc những người có thông tin quan trọng.
- Các đối tượng thường bị khai thác thường là:

  + Lễ tân, bảo vệ

  + Nhân viên tạp vụ

  + Nhân viên văn phòng

  + Quản lý/ giám đốc cấp cao

  + Người dùng

Đối tượng dễ bị tấn công bởi Social Engineering

- Đào tạo nhân viên , lễ tân, bảo vệ, tạp vụ không được phép tiết lộ mật khẩu hoặc thông tin khác qua điện thoại.
- Đào tạo giám đốc điều hành hỗ trợ kỹ thuật và quản trị viên hệ thống không bao giờ tiết lộ mật khẩu thông tin khác qua điện thoại hoặc email
- Giữ tất cả rác trong các khu vực được bảo mật, giám sát, cắt nhỏ dữ liệu quan trọng, xóa phương tiện từ tính

Kỹ thuật kiểm tra xâm nhập

ĐN: Kiểm tra xâm nhập là quá trình xác định các lỗ hổng trong cơ sở hạ tầng công nghệ thông tin của tổ chức, theo cách giống như một kẻ tấn công thực sự nhằm phát hiện những nguy cơ đối với ATTT của hệ thống.

Các bước kiểm tra xâm nhập :

Bước 1: Xác định mục tiêu. Thiết lập các mục tiêu của việc đánh giá an ninh.
Bước 2: Thăm dò mục tiêu. Tìm hiểu càng nhiều càng tốt về tổ chức và các hệ thống trên cả phương diện trực tuyến (online) và ngoại tuyến (offline).
Bước 3: Khám phá mục tiêu. Quét cổng và tìm điểm yếu trong một dải IP để tìm hiểu thêm về thành phần khác.
Bước 4: Khai thác điểm yếu. Sử dụng thông tin về các lỗ hổng để khai thác mục tiêu ở mức hệ điều hành hoặc ứng dụng

Kỹ thuật kiểm tra xâm nhập

- Bước 5: Tấn công vét cạn (bruteforce). Kiểm tra tất cả các mật khẩu yếu để chiếm quyền truy cập.
- Bước 6: Sử dụng kỹ nghệ xã hội (Social engineering). Khai thác điểm yếu về con người như thư điện tử lừa đảo, mã độc USB,....
- Bước 7: Chiếm quyền điều khiển: Truy xuất dữ liệu của mục tiêu, chẳng hạn như mật khẩu, ảnh chụp màn hình, các tập tin, cài đặt keylogger,.... Lợi dụng để tiếp tục tấn công nhiều hơn nữa như vét cạn và lừa đảo.
- Bước 8: Chuyển hướng. Tiếp tục khai thác các dải mạng khác nếu có.
- Bước 9: Thu thập chứng cứ: Thu thập ảnh chụp màn hình, mật khẩu, các tập tin như là bằng chứng mà tổ chức đã thu được.
- Bước 10: Báo cáo. Tạo báo cáo về cách thử nghiệm xâm nhập và các thông tin có thể mất mát.
- Bước 11: Sửa lỗi. Chỉ ra các điểm yếu có thể bị lợi dụng xâm nhập vào hệ thống mạng.

Thực hiện một số kỹ năng giao tiếp xã hội

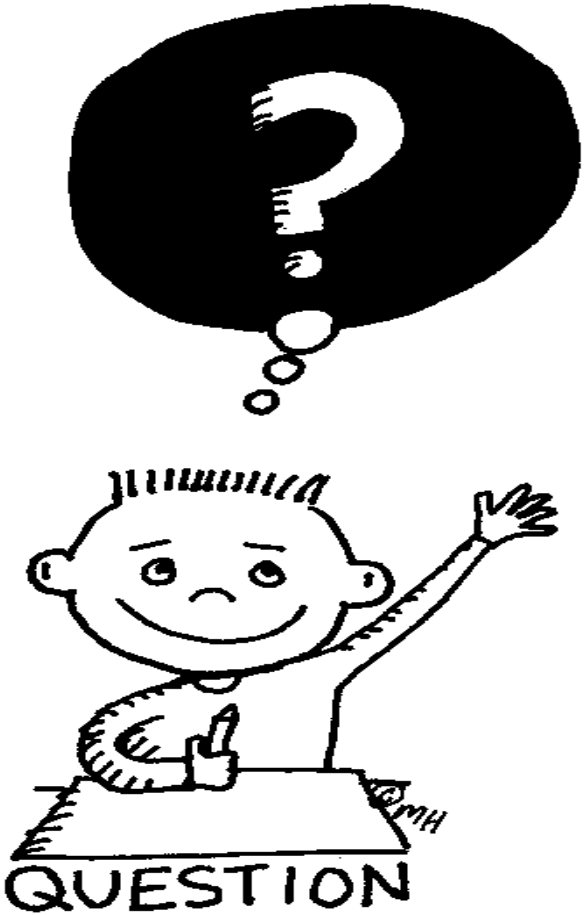
- Kết bạn, làm quen để tiếp cận nhân viên >> thu thập thêm thông tin
- Có thể đóng giả làm kĩ thuật viên sửa chữa từ bên ngoài,…
- Cố gắng nghe lén trên hệ thống và từ người dùng.
- Thao tác một số ID giả,..

Bộ công cụ SET

Bộ công cụ (SET) là một công cụ dựa trên Python mã nguồn mở nhằm kiểm tra thâm nhập thông qua kỹ thuật xã hội. Đây là một khai thác chung được thiết kế để thực hiện các cuộc tấn công tiên tiến chống lại các yếu tố của con người để thỏa hiệp một mục tiêu để cung cấp thông tin nhạy cảm. SET phân loại các cuộc tấn công như email, web và USB theo vectơ tấn công được sử dụng để lừa con người. Bộ công cụ tấn công điểm yếu của con người, khai thác niềm tin, nỗi sợ hãi và bản chất hay giúp đỡ của con người.

Một số công cụ kiểm tra Kiểm tra xâm nhập kỹ thuật xã hội được liệt kê dưới đây:

- SpeedPhish Framework (SPF) *(https://github.come*
- Gophish *(https://getgophish.come*
- King Phisher *(https://github.com]*
- LUCY *[https://www.lucysecurity.com]*
- MSI Simple Phish *(http://microsolved.com]*
- Ghost Phisher *(https://github.com]*
- Metasploit *(https://www.rapid7.com]*
- Umbrella *(https://github.come*
- Domain Hunter *(https://github.com)*
- Phishing Frenzy *[https.'//www.phishingfrenzy.com]*


QUESTION