# Lab 5: Kĩ thuật xã hội

## Mục tiêu

Trong bài này, bạn sẽ nghiên cứu các ví dụ về kỹ thuật xã hội và xác định các cách để nhận biết và ngăn chặn nó.

## Bối cảnh

Con người là mắc xích yếu nhất nếu bị phá vỡ sẽ khiến cho toàn bộ hệ thống bảo mật bị thất bại. Bài này sẽ nêu ra một số trường hợp như vậy.

## Tài nguyên yêu cầu

Máy tính có truy cập Internet.

## Phần 1: Nghiên cứu các Ví dụ về Kỹ thuật Xã hội

Kỹ thuật xã hội, vì nó liên quan đến an toàn thông tin, được sử dụng để mô tả các kỹ thuật được dùng bởi một (hoặc nhiều) người thao túng người khác để truy cập hoặc xâm phạm thông tin về tổ chức hoặc hệ thống máy tính của họ. Một người thực hiện kỹ thuật xã hội thường khó xác định và có thể tự xưng là nhân viên mới, người sửa chữa hoặc nhà nghiên cứu. Những người thực hiện kỹ thuật xã hội thậm chí có thể cung cấp thông tin xác thực để hỗ trợ danh tính đó. Bằng cách đạt được sự tin tưởng và đặt câu hỏi, kẻ ấy có thể chấp nối đủ thông tin để xâm nhập vào mạng của một tổ chức.

Sử dụng trình duyệt Internet bất kỳ để nghiên cứu các sự cố về kỹ thuật xã hội. Tóm tắt ba ví dụ được tìm thấy trong nghiên cứu của bạn.

**Vụ tấn công bằng cuộc gọi điện thoại của ngân hàng (The Bank Phone Call Attack):**

**Trong một trường hợp, một kẻ xấu đã gọi vào một ngân hàng giả vờ là một nhà cung cấp dịch vụ IT hàng đầu. Họ tạo ra một văn phòng tưởng tượng với tên và số điện thoại có liên quan. Kẻ xấu này đã gặt hái thông tin từ trang web công ty ngân hàng và sử dụng nó trong cuộc gọi để xác thực danh tính giả mạo của họ. Họ cố gắng thuyết phục một nhân viên ngân hàng rằng họ cần thông tin xác thực để cải thiện bảo mật và hệ thống. Nhân viên, ngây thơ và tin tưởng, đã cung cấp thông tin xác thực và mã PIN, cho phép kẻ xấu truy cập vào mạng nội bộ của ngân hàng.**

**Cuộc tấn công "Nhà sửa ống nước" (The Plumbing Repairman Attack):**

**Một kẻ xấu đã mặc đồ hội thảo như một nhân viên sửa chữa ống nước và tới một doanh nghiệp lớn. Họ cho rằng họ được gọi đến để kiểm tra hệ thống cấp nước. Kẻ xấu này thực sự cắm một thiết bị USB nhỏ vào một máy tính trong văn phòng nhằm thu thập thông tin nhạy cảm và truy cập vào hệ thống mạng nội bộ.**

**Kỹ thuật xã hội qua email (Phishing Attack):**

**Một tổ chức lớn đã trải qua một cuộc tấn công qua email kỹ thuật xã hội. Kẻ xấu đã gửi một email giả mạo đến các nhân viên, giả vờ là một thông báo quan trọng từ bộ phận IT. Email yêu cầu người nhận cập nhật thông tin tài khoản của họ bằng cách nhấp vào một liên kết giả mạo và điền thông tin đăng nhập. Khi nhân viên cung cấp thông tin, kẻ xấu đã có thể sử dụng nó để truy cập vào hệ thống của tổ chức và gây hậu quả nghiêm trọng.**

## Phần 2: Nhận biết các dấu hiệu của kỹ thuật xã hội

Người thực hiện kỹ thuật xã hội chẳng là gì ngoài kẻ trộm và gián điệp. Thay vì xâm nhập vào mạng của bạn thông qua Internet, họ cố gắng giành quyền truy cập bằng cách dựa vào lòng hảo tâm của người khác. Mặc dù không cụ thể đối với an ninh mạng, kịch bản dưới đây minh họa cách một người có thể vô tình cung cấp thông tin bí mật một cách không nghi ngờ.

*"Quán cà-phê tương đối yên tĩnh lúc tôi, mặc bộ com-lê, ngồi ở một chiếc bàn trống. Tôi đặt chiếc cặp của mình lên bàn và đợi một nạn nhân thích hợp. Chẳng mấy chốc, một nạn nhân như vậy đến với một người bạn và ngồi ở bàn bên cạnh tôi. Cô đặt túi mình lên ghế bên cạnh, kéo chiếc ghế lại gần và luôn đặt tay lên túi.*

*Sau vài phút, bạn của cô ấy đi vệ sinh. Đối tượng ở một mình, vì vậy tôi ra hiệu cho Alex và Jess. Đóng vai một cặp vợ chồng, Alex và Jess nhờ đối tượng chụp hình cho mình. Cô ấy sẵn lòng. Cô nhấc tay khỏi chiếc túi để cầm cái máy chụp hình và chụp một bức ảnh cho “cặp đôi hạnh phúc”, và rồi trong khi bị xao lãng, tôi với tay ra, cầm lấy túi và khóa nó vào trong cặp của mình. Nạn nhân của tôi vẫn chưa nhận thấy túi của mình đã bị mất khi Alex và Jess rời quán cà-phê. Alex sau đó đi đến một nhà để xe gần đó.*

*Không mất nhiều thời gian để cô nhận ra chiếc túi của mình đã biến mất. Cô bắt đầu hoảng loạn, nhìn quanh điên cuồng. Đây chính xác là những gì chúng tôi hy vọng, tôi hỏi cô ấy có cần giúp đỡ không.*

*Cô ấy hỏi tôi có thấy điều gì không. Tôi nói rằng mình không thấy và thuyết phục cô ấy ngồi xuống rồi nghĩ về những gì có trong túi. Một cái điện thoại. Đồ trang điểm. Một ít tiền mặt. Và thẻ tín dụng của cô ấy. Bingo!*

*Tôi hỏi cô ấy dùng ngân hàng nào rồi nói với cô ấy rằng tôi đã làm việc ở ngân hàng đó. Thật là may mắn! Tôi cam đoan với cô ấy rằng mọi thứ sẽ ổn, nhưng cô ấy cần phải hủy thẻ tín dụng ngay lập tức. Tôi gọi là số “help-desk”, thực ra là Alex, và đưa điện thoại của tôi cho cô.*

*Alex đang ở trong một chiếc xe tải trong nhà để xe. Trên bảng điều khiển, một máy nghe nhạc CD đang mở tiếng ồn của văn phòng. Anh đảm bảo rằng thẻ của cô có thể dễ dàng được hủy nhưng, để xác minh danh tính của cô, cô cần nhập mã PIN của cô trên bàn phím của điện thoại cô đang sử dụng. Điện thoại của tôi và bàn phím của tôi.*

*Khi có mã PIN, tôi đã rời đi. Nếu chúng tôi là kẻ trộm thực sự, chúng tôi sẽ có quyền truy cập vào tài khoản của cô ấy bằng cách rút tiền ATM và mua hàng bằng mã PIN. May cho cô ấy, đây chỉ là một chương trình truyền hình."*

"Hacking VS Social Engineering -by [Christopher Hadnagy](http://www.amazon.com/Christopher-Hadnagy/e/B004D1T9F4/ref=dp_byline_cont_book_1) http://www.hackersgarage.com/hacking-vs-social-engineering.html

*Ghi nhớ: “Người xây tường nghĩ khác với người tìm cách đi qua, đi dưới, đi vòng hoặc đi xuyên chúng.” Paul Wilson - The Real Hustle*

Nghiên cứu các cách để nhận ra kỹ thuật xã hội. Mô tả ba ví dụ được tìm thấy trong nghiên cứu của bạn.

**Trong các ví dụ về kỹ thuật xã hội mà bạn đã cung cấp, mô tả một số tình huống mà kẻ xấu tận dụng lòng tin và sự không nghi ngờ của người khác để chiếm đoạt thông tin quan trọng. Dưới đây là ba ví dụ khác về các kỹ thuật xã hội và cách chúng có thể ảnh hưởng đến an ninh thông tin:**

**Vụ trộm thông tin qua cửa phía sau:**

**Kẻ xấu đóng vai trò nhân viên giao hàng và mang một hộp giả mạo đến cửa phía sau của một doanh nghiệp. Họ thuyết phục người bảo vệ hoặc nhân viên tiếp tân rằng họ có giao hàng quan trọng từ công ty vận chuyển và cần được cho phép vào bên trong để giao hàng. Khi họ được phép vào, họ có thể di chuyển trong tòa nhà mà không gặp sự kiểm soát và truy cập vào hệ thống máy tính hoặc các khu vực nhạy cảm khác để lấy thông tin quan trọng.**

**Cuộc gọi lừa đảo từ người quen:**

**Kẻ xấu có thể giả mạo cuộc gọi từ người quen, ví dụ như đồng nghiệp hoặc bạn bè của một nhân viên trong một tổ chức. Trong cuộc gọi, họ có thể thuyết phục người nhận cung cấp thông tin nhạy cảm hoặc mật khẩu bằng cách giả vờ cần giúp đỡ trong công việc hoặc vấn đề khẩn cấp. Kỹ thuật này dựa vào lòng tin và quen thuộc giữa các cá nhân để truy cập vào thông tin nhạy cảm.**

**Kỹ thuật xã hội qua email và tấn công "CEO":**

**Trong một tình huống này, kẻ xấu giả danh là CEO hoặc người quyền lực cao trong tổ chức và gửi email giả mạo đến một nhân viên quan trọng, chẳng hạn như kế toán viên. Trong email, họ yêu cầu người nhận chuyển tiền vào một tài khoản ngân hàng mới hoặc cung cấp thông tin tài khoản ngân hàng nhằm lừa đảo. Vì vậy, thông qua sự tin tưởng vào địa vị của người gửi, nhân viên có thể bị đánh lừa và cung cấp thông tin tài chính quan trọng.**

## Phần 3: Nghiên cứu các các ngăn chặn kĩ thuật xã hội

Trường của bạn có các quy trình để giúp ngăn chặn kĩ thuật xã hội không?

**Em không biết trường TDTU có ngăn chặn kĩ thuật xã hội không nữa.**

Dùng Internet để nghiên cứu các quy trình mà các tổ chức khác dùng để ngăn chặn những người dùng kĩ thuật xã hội được truy cập vào thông tin bí mật. Hãy liệt kê những gì mình tìm được.

**Các tổ chức thường triển khai nhiều biện pháp để ngăn chặn và bảo vệ chống lại kỹ thuật xã hội. Dưới đây là một số biện pháp thông thường mà các tổ chức sử dụng để giảm thiểu nguy cơ truy cập không đúng vào thông tin bí mật:**

**Đào tạo và tăng cường ý thức: Tổ chức thường cung cấp đào tạo cho nhân viên về các mối nguy hiểm liên quan đến kỹ thuật xã hội và cách nhận biết và phản ứng với các cuộc tấn công như phishing và cuộc gọi lừa đảo. Đào tạo này giúp nhân viên nhận ra các mẹo và kỹ thuật mà kẻ xấu sử dụng để lừa đảo họ.**

**Xác minh danh tính: Các tổ chức sử dụng các biện pháp xác minh danh tính chặt chẽ để đảm bảo rằng chỉ những người có quyền truy cập mới được phép vào các thông tin nhạy cảm hoặc hệ thống nội bộ. Điều này bao gồm việc sử dụng xác thực hai yếu tố, mật khẩu mạnh và các phương pháp xác minh danh tính tiên tiến khác.**

**Phân quyền và quản lý quyền truy cập: Tổ chức thường thiết lập các quy tắc phân quyền và giới hạn quyền truy cập vào thông tin chỉ dành cho những người cần thiết. Nhân viên chỉ có thể truy cập vào các dữ liệu và hệ thống cần thiết để thực hiện công việc của họ, giúp giảm thiểu nguy cơ truy cập không đúng.**

**Kiểm tra bảo mật định kỳ: Các tổ chức thường thực hiện kiểm tra bảo mật thường xuyên để xác định các lỗ hổng và điểm yếu trong hệ thống của họ. Điều này giúp họ cải thiện các biện pháp bảo mật và đảm bảo rằng hệ thống của họ luôn được bảo vệ tốt nhất.**

## Tham khảo

CISCO, CCNA Security 2.0, 1.2.4.12 Lab - Social Engineering