Bài: 9. Tấn công phi kỹ thuật - Khái niệm, giai đoạn, phương pháp tấn công phi kỹ thuật và mạo danh trên mạng xã hội

Xem bài học trên website để ủng hộ Kteam: 9. Tấn công phi kỹ thuật - Khái niệm, giai đoạn, phương pháp tấn công phi kỹ thuật và mạo danh trên mạng xã hội

Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage How Kteam nhé!

Tóm tắt

Ở chương này, chúng ta sẽ tìm hiểu khái niệm cơ bản và cách thức hoạt động của **tấn công phi kĩ thuật**.

Kĩ thuật này khá khác biệt với các kĩ thuật đánh cắp thông tin trước đây. Tất cả các công cụ và kĩ thuật để hack một hệ thống đều thuộc chuyên môn và đòi hỏi kiến thức về mạng, hệ điều hành và các lĩnh vực khác. Tấn công phi kĩ thuật là một phần của việc đánh cắp thông tin phi kĩ thuật. Đây là kĩ thuật phổ biến nhất do dễ thực hiện bởi **vì tính cách bất cẩn thường thấy ở con người**.

Mô hình an ninh bao gồm an ninh mạng, bảo mật tài nguyên hệ thống, trong đó **con người là nhân tố quan trọng nhất**. Nếu người dùng bất cẩn để lộ chứng thư đăng nhập, tất cả các lớp bảo mật còn lại sẽ thất bại. Tuyên truyền về phi kĩ thuật, tấn công phi kĩ thuật và hậu quả của sự bất cẩn sẽ tăng cường an ninh mạng cho người dùng.

Chương này bao gồm tổng quan khái niệm phi kĩ thuật, các kiểu tấn công phi kĩ thuật; bạn sẽ tìm hiểu về cách thức hoạt động của các tấn công phi kĩ thuật khác nhau, mối nguy hiểm, cách kẻ tấn công mạo danh người dùng, lấy cắp nhân dạng và giảm thiểu nguy cơ tấn công phi kĩ thuật. Chúng ta sẽ bắt đầu với khái niệm tấn công phi kĩ thuật.

Khái niệm phi kĩ thuật

Giới thiệu phi kĩ thuật

Phi kĩ thuật là hành động lấy cắp thông tin từ người dùng. Bởi vì nó không bao gồm tương tác với hệ thống mục tiêu hay mạng, nó được coi là một tấn công phi kĩ thuật.

Phi kĩ thuật được xem là **nghệ thuật thuyết phục mục tiêu tiết lộ thông tin**. Có thể là tương tác một một với mục tiêu hoặc thuyết phục mục tiêu trên nền tảng bất kì. Ví dụ, mạng xã hội là một nền tảng phổ biến của phi kĩ thuật. Sự xuất hiện của tấn công phi kĩ thuật chứng minh sự bất cẩn hay kém nhận thức của người dùng về các thông tin họ sở hữu.

Nguy cơ tấn công phi kĩ thuật

Một nhân tố quan trọng dẫn đến tấn công phi kĩ thuật là "**niềm tin**". Người dùng A tin tưởng một người B và không bảo vệ các chứng thư đăng nhập trước người đó. Người B có thể để lộ thông tin với người C, từ đó người C thực hiện tấn công với người dùng A.

Những tổ chức không nhận thức hay nhân viên không được luyện tập đầy đủ về tấn công phi kĩ thuật và cách phòng tránh có nguy cơ trở thành nạn nhân của tấn công này. Mỗi tổ chức cần huấn luyện nghiệp vụ nhân viên về tấn công phi kĩ thuật.

Các tổ chức cũng cần bảo vệ cơ sở hạ tầng của mình. Nhân viên ở các cấp độ khác nhau nên bị giới hạn ở những đặc quyền khác nhau. Ví dụ nhân viên ở các văn phòng ban khác không được truy cập vào tài nguyên của ban Tài chính. Trong trường hợp một nhân viên có quyền tự do truy cập thì tấn công phi kĩ thuật như **Dumpster Diving** hay **Shoulder surfing** dễ xảy ra.

Thiếu chính sách an ninh và bảo mật cũng là một nguy cơ khác. Chính sách an ninh cần phải chặt chẽ để ngăn người dùng mạo danh người dùng khác. Bảo mật giữa người dùng không thẩm quyền hay client và nhân viên tổ chức cần phải được duy trì để phòng tránh truy cập không thẩm quyền hay đánh cắp.

Các giai đoạn tấn công phi kĩ thuật

Tấn công phi kĩ thuật không phải là một tấn công phức tạp đòi hỏi kiến thức chuyên môn sâu sắc. Tấn công phi kĩ thuật bao gồm các bước sau đây:

Nghiên cứu

Giai đoạn nghiên cứu là thu thập thông tin về tổ chức mục tiêu. Những thông tin này có thể thu thập thông qua **dumpster diving**, quét website của tổ chức, tìm hiểu thông tin trên mạng, thu thập thông tin từ nhân viên tổ chức, ...

Chọn mục tiêu

Trong giai đoạn này, kẻ tấn công chọn mục tiêu trong số các nhân viên của tổ chức. Một nhân viên chán nản và mệt mỏi sẽ dễ được lựa chọn bởi vì anh ta dễ để lộ thông tin hơn.

Tạo mối quan hệ

Giai đoạn này bao gồm việc tạo ra một mối quan hệ với mục tiêu sao cho anh ta không nhận ra được ý định của kẻ tấn công. Mục tiêu sẽ có niềm tin với kẻ tấn công. Niềm tin càng lớn thì mục tiêu càng dễ tiết lộ thông tin.

Khai thác

Khai thác mối quan hệ để lấy được các thông tin nhạy cảm như tên người dùng, mật khẩu, thông tin mạng, ...

Phương pháp tấn công phi kĩ thuật

Các loại tấn công phi kĩ thuật

Tấn công phi kĩ thuật có thể thực hiện bằng những phương pháp khác nhau. Những phương pháp ấy được chia thành những loại sau đây:

Tấn công phi kĩ thuật dựa trên con người

Kĩ thuật này bao gồm **tương tác một một** giữa kẻ tấn công với nạn nhân. Tấn công phi kĩ thuật thu thập thông tin nhạy cảm bằng những chiêu trò như tạo niềm tin, lợi dụng thói quen, hành vi và bổn phận đạo đức.

1. Mạo danh

Mạo danh là một phương pháp tấn công dựa trên con người. Về cơ bản, mạo danh là giả mạo thành một người hay một vật nào đó. Mạo danh trong tấn công phi kĩ thuật là kẻ tấn công giả mạo thành một người dùng chính thống hay người có thẩm quyền. Phương pháp này thực hiện trong thực tế hoặc qua một kênh giao tiếp như email, điện thoại, ...

Mạo danh nhân dạng được thực hiện bởi đánh cắp nhân dạng, khi kẻ tấn công có đủ thông tin cá nhân về một người có thẩm quyền, kẻ tấn công sẽ mạo danh thành người dùng chính thống đang cung cấp thông tin cá nhân của người dùng chính thống. Một cách khác là mạo danh thành cố vấn chuyên môn để yêu cầu chứng thư đăng nhập.

2. Nghe trộm và nhìn qua vai (Eavesdropping and Shoulder Surfing)

Nghe trộm là kĩ thuật trong đó kẻ tấn công lấy thông tin bằng các nghe đoạn hội thoại. Nó không gồm nghe đoạn hội thoại mà bao gồm đọc hoặc truy cập vào thông tin nào đó mà người dùng không được thông báo về hoạt động đó.

Kĩ năng nhìn qua vai (Shoulder Surfing) đã được định nghĩa trong chương DẤU VẾT. Như tên gọi của nó, kĩ thuật này là lấy thông tin bằng cách đứng sau mục tiêu khi anh ta đang tương tác với thông tin nhạy cảm.

3. Dò tìm bãi phế thải (Dumpster Diving)

Nói đơn giản, thuật ngữ này nghĩa là tìm "kho báu" từ bãi rác. Đây là một kĩ thuật tuy cũ nhưng vẫn hiệu quả. Nó bao gồm tiếp cận với thùng rác của người dùng như rác máy in, bàn làm việc hay rác công ti để tìm hóa đơn điện thoại, thông tin liên lạc, thông tin tài chính, mã tài nguyên và các tài liệu hữu ích khác.

4. Tấn công phi kĩ thuật đảo ngược

Đây là quá trình yêu cầu tương tác giữa kẻ tấn công và nạn nhân, khi mà kẻ tấn công làm nạn nhân tin rằng anh ta đang có vấn đề hoặc sẽ có vấn đề trong tương lai. Nếu nạn nhân bị thuyết phục, anh ta sẽ cung cấp thông tin mà kẻ tấn công yêu cầu. Tấn công phi kĩ thuật đảo ngược được thực hiện qua những bước sau:

- Kẻ tấn công phá hoại hệ thống mục tiêu hay nhận diện lỗ hổng bảo mật.
- Kẻ tấn công giới thiệu bản thân như một người có thẩm quyền có thể giải quyết mục tiêu.
- Kẻ tấn công tạo niềm tin với nạn nhân và lấy quyền truy cập đến các thông tin nhạy cảm.
- Sau khi tấn công phi kĩ thuật đảo ngược thành công, người dùng thường liên lạc kẻ tấn công để giúp đỡ.

5. Piggybacking và Tailgating

Piggybacking và **Tailgating** là hai kĩ thuật giống nhau. **Piggyback** là phương pháp mà trong đó người không có thẩm quyền chờ một người có thẩm quyền để lấy quyền truy cập vào khu vực giới hạn. Còn **tailgating** là kĩ thuật trong đó người không có thẩm quyền lấy quyền truy cập vào khu vực giới hạn bằng cách theo người có thẩm quyền. Bằng cách sử dụng ID giả và theo sát người dùng khi đi qua điểm kiểm tra, tailgating trở nên đơn giản.

Phi kĩ thuật dựa trên máy tính

Có nhiều cách khác nhau để thực hiện phi kĩ thuật dựa trên máy tính bao gồm cửa sổ yêu cầu chứng thư đăng nhập, tin nhắn internet và email ví dụ như chữ cái Hoax, chữ cái Chain và Spam.

Phishing

Quá trình phishing là kĩ thuật gửi một email giả trông như email chính thống đến host mục tiêu. Khi người nhận mở link, anh ta bị dụ dỗ đưa ra thông tin. Người nhận thường được đưa đến một webpage giả giống như webpage thật. Do điểm tương đồng nên người dùng sẽ cung cấp các thông tin nhạy cảm cho webpage giả này.

Spear Phishing

Đây là loại phishing tập trung vào một cá nhân. Loại phishing này tạo ra tỉ lệ phản hồi cao hơn so với một tấn công phishing ngẫu nhiên.

Phi kĩ thuật dựa trên điện thoại

1. Phát hành ứng dụng ác ý

Tấn công phi kĩ thuật dựa trên điện thoại bao gồm phát hành ứng dụng ác ý trên cửa hàng cho người dùng tải về trên diện rộng. Những ứng dụng ác ý này thường là bản sao của một ứng dụng phổ biến. Ví dụ, kẻ tấn công phát triển ứng dụng ác ý cho Facebook. Người dùng thay vì tải về ứng dụng chính thức sẽ vô tình tải về ứng dụng ác ý của bên thứ ba này. Khi người dùng đăng nhập, ứng dụng này sẽ gửi chứng thư đăng nhập đến server ở xa mà kẻ tấn công kiểm soát.

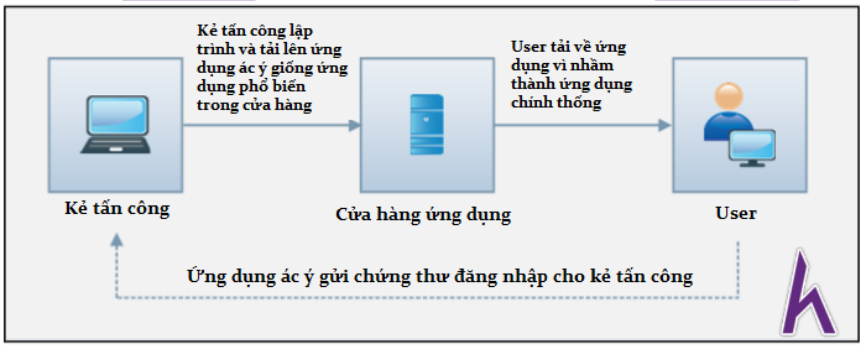

Figure 9-01 Publishing Malicious Application

2. Đóng gói ứng dụng chính thống

Trong tấn công phi kĩ thuật dựa trên điện thoại, một kĩ thuật có thể sử dụng là **đóng gói ứng dụng chính thống với malware**. Kẻ tấn công ban đầu tải về một ứng dụng phổ biến từ cửa hàng, thường là trò chơi hay phần mềm anti-virus. Kẻ tấn công đóng gói ứng dụng với malware và tải nó lên một cửa hàng bên thứ ba. Người dùng không nhận thức được sự hiện diện của ứng dụng ác ý trên cửa hàng hoặc lấy link download miễn phí một ứng dụng trả phí nên người dùng tải về ứng dụng ác ý. Khi người dùng đăng nhập, ứng dụng ác ý sẽ gửi chứng thư đăng nhập đến server ở xa mà kẻ tấn công kiểm soát.

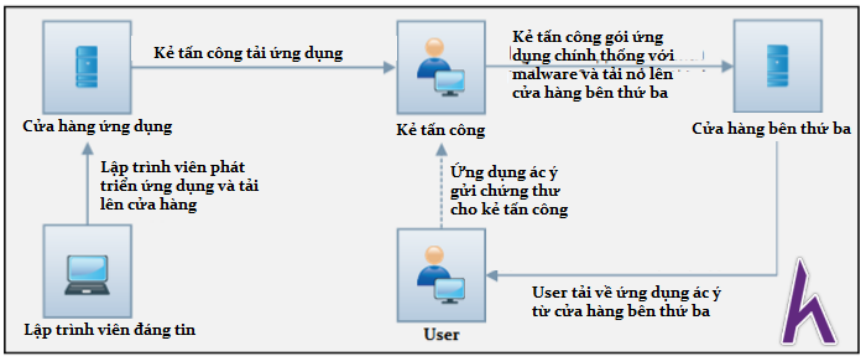

Figure 9-02 Repackaging Legitimate Application

3. Ứng dụng bảo mật giả

Giống với kĩ thuật trên, kẻ tấn công sẽ phát triển một ứng dụng bảo mật giả. Ứng dụng bảo mật được tải về từ cửa số mở lên khi người dùng mở website trên internet.

Tấn công nội sinh

Không phải tất cả tấn công phi kĩ thuật đều do người bên ba thu thập thông tin về tổ chức của bạn. Đó có thể là một nhân viên của tổ chức có đặc quyền hay không, thăm dò tổ chức với mục đích ác ý. Tấn công nội sinh được thực hiện bởi những người ở trong tổ chức đó. Đối thủ của tổ chức có thể đứng sau những kẻ tấn công này để lấy cắp thông tin và bí mật.

Bên cạnh thăm dò, người trong tổ chức có thể vì mục đích trả thù công ti. Một nhân tố bất mãn trong công ti có thể lấy cắp thông tin tuyệt mật để trả thù. Nguyên nhân bất mãn có thể do không hài lòng với sự quản lí, vấn đề từ tổ chức, giáng chức hoặc sa thải.

Mạo danh trên mạng xã hội

Tấn công phi kĩ thuật nhờ mạo danh trên mạng xã hội

Mạo danh trên mạng xã hội rất phổ biến và dễ dàng thực hiện. Người dùng ác ý thu thập thông tin nạn nhân từ nhiều nguồn khác nhau, chủ yếu từ các mạng xã hội. Các thông tin thu thập được như ảnh đại diện gần đây, ngày sinh, địa chỉ gia đình, địa chỉ email, chi tiết liên lac, chi tiết chuyên môn hay thông tin về giáo dục.

Sau khi thu thập thông tin về mục tiêu, kẻ tấn công sẽ tạo một tài khoản giống hệt với tài khoản mục tiêu. Tài khoản giả này được giới thiệu đến bạn bè và nhóm mà mục tiêu tham gia. Thông thường, mọi người không thăm dò quá nhiều khi họ nhận được một lời mời kết bạn, và khi họ thấy thông tin chính xác thì họ chắc chắn sẽ chấp nhận lời mời.

Figure 9-03 Social Networking Sites

Khi kẻ tấn công tham gia vào nhóm mà người dùng chia sẻ thông tin cá nhân và thông tin công ti, kẻ đó sẽ nhận được cập nhật từ nhóm. Kẻ tấn công cũng có thể giao tiếp với bạn bè của nạn nhân để thuyết phục họ tiết lộ thông tin.

Các nguy cơ của mạng xã hội trong hệ thống mạng

Một mạng xã hội không được bảo mật chi tiết như hệ thống mạng, do hệ thống mạng bảo mật xác thực, nhận dạng và cấp phép của một nhân viên truy cập vào tài nguyên. Nguy cơ lớn nhất của mạng xã hội là lỗ hổng xác thực. Một kẻ tấn công có thể dễ dàng thao tác trên bước thẩm định quyền và tạo ra một tài khoản giả mạo để truy cập thông tin.

Một nhân viên khi giao tiếp trên mạng xã hội có thể lơ là các thông tin nhạy cảm, do đó để lộ thông tin với người cùng giao tiếp, hoặc người thứ ba quan sát cuộc trò chuyện. Điều này đòi hỏi chính sách chặt chẽ chống lại rò rỉ dữ liệu.

Đánh cắp nhân dạng

Tổng quan

Đánh cắp nhân dạng là hành vi lấy cắp thông tin nhận dạng của một người nào đó, thường sử dụng để lừa đảo. Một người có mục đích ác ý có thể đánh cắp danh tính của bạn bằng cách thu thập tài liệu như hóa đơn tiện ích, thông tin cá nhân và các thông tin liên quan khác, và tạo một thẻ ID để mạo danh. Không chỉ là thẻ ID, hắn có thể sử dụng thông tin này để chứng minh nhân dạng và lợi dụng nó.

Quy trình đánh cắp nhân dạng

Ban đầu, kẻ tấn công tập trung tìm những thông tin hữu ích như thông tin cá nhân và nghề nghiệp. **Dumpster Diving** hoặc tiếp cận bàn làm việc của một nhân viên là những kĩ thuật hiệu quả trong giai đoạn này. Bên cạnh đó, phi kĩ thuật như tìm kiếm hóa đơn tiện ích, thẻ ID, hay tài liệu cũng giúp tạo thẻ ID giả từ một nguồn có thẩm quyền như cơ quan cấp bằng lái xe.

Khi bạn đã có ID từ cơ quan thẩm quyền, bạn có thể lợi dụng nó. Tuy nhiên, bạn cần có hóa đơn tiện ích hay các giấy tờ cần thiết khác để chứng minh ID của bạn. Một khi bạn vượt qua được hàng rào kiểm tra này, bạn có thể truy cập với ID bằng cách giả mạo nhân viên chính thống.

Biện pháp chống lại phi kĩ thuật

Tấn công phi kĩ thuật có thể được giảm thiểu bằng nhiều cách khác nhau. Môi trường làm việc nên đảm bảo sự riêng tư cá nhân để tránh **shoulder surfing** và **dumpster diving**. Thiết lập mật khẩu mạnh, an toàn, giữ chúng bí mật cũng là một cách phòng vệ tốt. Mạng xã hội là nơi cần cảnh giác vì chứa nhiều nguy cơ để lộ thông tin. Hiện nay, tấn công phi kĩ thuật đã trở thành nền tảng quan trọng của nhiều tổ chức. Tiếp tục quan sát mạng xã hội, ghi nhật kí, đào tạo, kiểm kê, nâng cao nhận thức giúp giảm thiểu nguy cơ tấn công phi kĩ thuật một cách hiệu quả.

Mindmap

Lab 09-1: Tấn công phi kĩ thuật bằng Kali Linux

Case Study

Chúng ta dùng bộ công cụ Kali Linux để tạo một website giả mạo và gửi link cho nạn nhân. Khi nạn nhân đăng nhập vào website qua link, chứng thư của anh ta sẽ bị thiết bị cuối Linux trích rút.

Quy trình

1. Mở Kali Linux.

2. Đến ứng dụng.

3. Nhấn vào **Social Engineering Tools** (Công cụ phi kĩ thuật).
4. Nhấn vào **Social Engineering Toolkit** (Bộ công cụ phi kĩ thuật).

5. Nhập "**Y**" để tiếp tục

6. Nhập "**1**" đến tấn công phi kĩ thuật.

7. Nhập "**2**" đến vectơ tấn công website.

8. Nhập "**3**" đến phương pháp tấn công thu thập chứng thư.

9. Nhập "**2**" để đến **Site Cloner**.

10. Nhập địa chỉ IP của máy **Kali Linux** (ở đây là **10.10.50.200**).

11. Nhập URL mục tiêu.

12. Bây giờ, http://10.10.50.200 sẽ được sử dụng. Chúng ta có thể dùng địa chỉ này trực tiếp, nhưng đó không phải là một cách hiệu quả trong thực tế.

    Địa chỉ này được giấu trong một URL giả và chuyển tiếp đến nạn nhân. Do việc giả mạo, user không thể nhận dạng được website giả trừ khi quan sát URL. Nếu anh ta vô tình click vào website và đăng nhập, chứng thư sẽ được gửi đến thiết bị cuối Linux. Trong ảnh dưới, chúng tôi đang dùng http://10.10.50.200 để tiếp tục.

13. Đăng nhập bằng tên người dùng và mật khẩu

- Tên người dùng: admin
- Mật khẩu: Admin@123

14. Quay lại thiết bị cuối Linux và quan sát.

Tên người dùng admin và mật khẩu đã được trích rút. Nếu user nhập chính xác thì tài khoản có thể được dùng. Nếu không, bạn cũng đã lấy được một vài gợi ý và có thể đoán ID và mật khẩu. Nạn nhân sau đó sẽ được chuyển hướng đến page chính thống.