HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

KIỂM THỬ XÂM NHẬP

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

KIỂM THỬ XÂM NHẬP

Giới thiệu về kiểm thử xâm nhập

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY

Biên soạn từ bài giảng: Nguyễn Ngọc Điệp, Bài giảng Kiểm thử xâm nhập, Học viện Công nghệ Bưu chính Viễn thông, 2021.

1.1 KHÁI NIỆM VÀ VAI TRÒ CỦA KIỂM THỬ XÂM NHẬP

1.1.1. Tổng quan về An toàn thông tin

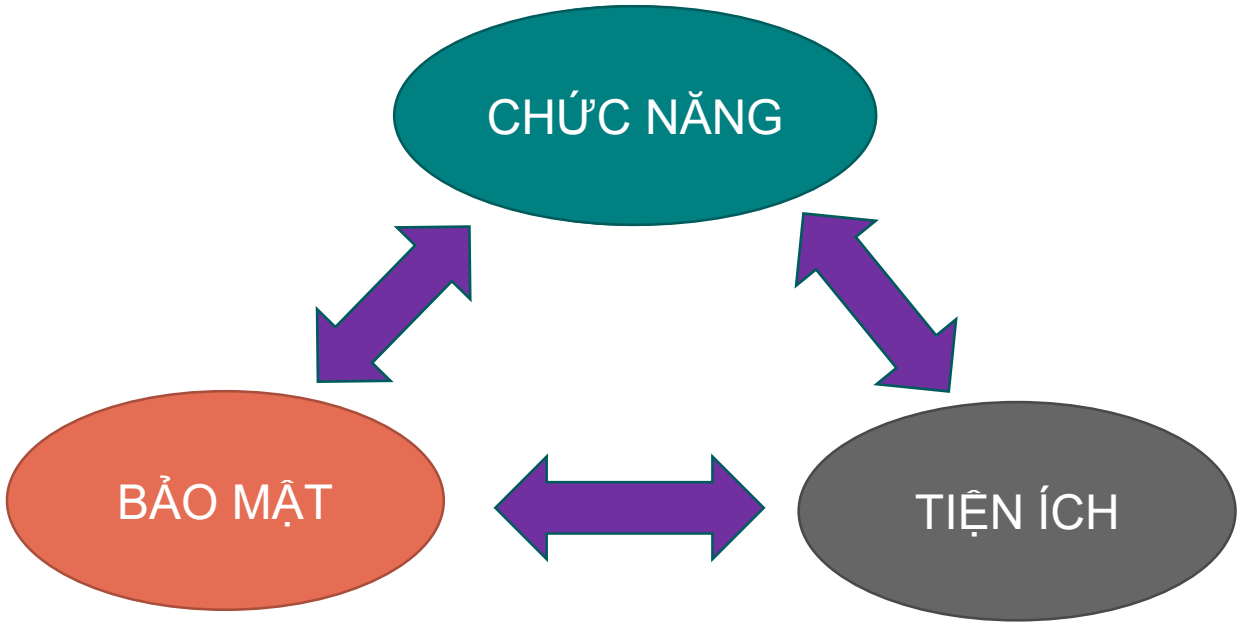
1.1.2. Một số kĩ thuật tấn công và giải pháp phòng chống

KHÁI NIỆM VÀ VAI TRÒ CỦA KIỂM THỬ XÂM NHẬP

- Tổng quan về an ninh mạng
- Khái niệm về tấn công mạng (hack)
- Các giai đoạn tấn công mạng
- Các loại tấn công mạng
- Kiểm thử xâm nhập
- Nghiên cứu lỗ hổng

Tổng quan về an ninh mạng

- Mức độ bảo mật của hệ thống có thể được xác định bởi khả năng của ba thành phần:



Mô hình tam giác

Tổng quan về an ninh mạng

- Các thách thức cần quan tâm:
  - Gia tăng tội phạm mạng tinh vi
  - Rò rỉ dữ liệu,thất thoát trong nội bộ và nhân viên làm việc xa
  - An ninh di động,xác thực và các phương tiện truyền thông xã hội
  - Nguồn nhân lực an ninh mạng
  - Khai thác các lỗ hổng ,vận hành hệ thống an ninh
  - Bảo vệ các cơ sở hạ tầng quan trọng
  - Cân bằng giữa việc công và tư
  - Tiếp cận với việc nhận dạng các chiến thuật và chu trình.

Tổng quan về an ninh mạng

- Danh sách các nguy cơ an ninh:

Trojans, đánh cắp thông tin, keylogger,…	Vishing
Mạng ma Flux Botnet	Chợ đen
Thất thoát giữ liệu,vi phạm an ninh	Tống tiền trên mạng
Các mối đe dọa an ninh trong nội bộ	Di chuyển dữ liệu (usb,máy tính xách tay,băng sao lưu..)
Tổ chức tội phạm mạng	Mạng ma
Lừa đảo	Lỗ hổng trong công nghệ mới
Các loại virus mới	Dự án gia công phần mềm
Gián điệp mạng	Mạng xã hội
Zero-Day	Gián đoạn kinh doanh
Mối đe dọa từ web 2.0	Công nghệ ảo hóa và điện toán đám mây

Khái niệm tấn công mạng (hack) (1)

- Ảnh hưởng của tấn công mạng
  - Theo thông tin nghiên cứu an ninh quốc gia Symantec, các cuộc tấn công của hacker gây thiệt hại cho các doanh nghiệp lớn khoản 2,2 triệu $ mỗi năm.
  - Hành vi trộm cắp tài khoản của khách hàng có thể làm giảm danh tiếng của doanh nghiệp.
  - Hacker có thể ăn cắp bí mật thông tin tài chính, hợp đồng quan trọng và bán chúng cho đối thủ cạnh tranh.
  - Botnet có thể được sử dụng để khởi động DOS và các cuộc tấn công dựa trên web khác, dẫn đến các doanh nghiệp bị giảm doanh thu.
  - Có thể làm các công ty phá sản.

Khái niệm tấn công mạng (hack) (2)

- Khái niệm hacker
  - Một người thông minh với kỹ năng máy tính xuất sắc, có thể tạo ra hay khám phá các phần mềm và phần cứng máy tính
  - Đối với một số hacker hack là một sở thích của họ có thể tấn công nhiều máy tính hoc mạng
  - Mục đích của họ là tìm hiểu kiến thức hoặc phá hoại bất hợp pháp
  - Một số mục đích xấu của hacker từ việc hack như: đánh cắp dữ liệu kinh doanh, thông tin thẻ tín dụng, sổ bảo hiểm xã hội, mật khẩu e-mail
- Các loại hacker
  - Mũ đen
  - Mũ trắng
  - Khủng bố (suicide hacker)
  - Mũ xám
  - Script Kiddie

Các giai đoạn tấn công (1)

1. Trinh sát
2. Quét
3. Truy cập
4. Duy trì truy cập
5. Xóa dấu vết

Các giai đoạn tấn công: Trinh sát

- Trinh sát đề cập đến giai đoạn chuẩn bị để một kẻ tấn công tìm kiếm để thu thập thông tin về 1 mục tiêu trước khi tung ra một cuộc tấn công.
- Mục đích chính là tìm hiểu một lượng lớn thông tin của mục tiêu để việc tấn công trong tương lai trở nên dễ dàng hơn.
- Phạm vi trinh sát mục tiêu có thể bao gồm các khách hàng, nhân viên, hoạt động, mạng, và hệ thống,..
- Các loại trinh sát
  - Trinh sát thụ động: Trinh sát mục tiêu mà không cần trực tiếp tương tác với mục tiêu. Vd : tìm kiếm hồ sơ công khai hoặc các bản tin đã phát hành.
  - Trinh sát chủ động: Trinh sát mục tiêu cần phải trực tiếp tương tác với mục tiêu qua nhiều phương tiện. Vd : các cuộc gọi để gọi để lấy thông tin kĩ thuật cá nhân

Các giai đoạn tấn công: Quét

- Trước khi tấn công, trên cơ sở các thông tin thu thập được qua quá trình trinh sát, kẻ tấn công quét mạng lưới thông tin của mục tiêu.
- Quét có thể bao gồm việc sử dụng các trình quay số, máy quét cổng, lập bản đồ mạng, quét bao quát, quét lỗ hổng,..
- Kẻ tấn công khai thác các thông tin như tên máy tinh, địa chỉ IP, và tài khoản người dùng để bắt đầu tấn công.

Các giai đoạn tấn công: Truy cập

- Truy cập dùng để chỉ việc kẻ tấn công có được quyền truy cập vào hệ thống điều hành hoặc ứng dụng mạng
- Kẻ tấn công có thể truy cập ở cấp hệ điều hành, cấp ứng dụng hoặc cấp mạng.
- Kẻ tấn công có thể nâng cấp quyền để có thể truy cập toàn bộ hệ thống. kẻ tấn công đoạt được quyền kiểm soát hệ thống rồi mới khai thác thông tin.
- Vd : bẻ mật khẩu, tràn bộ đệm, từ chối dịch vụ, đánh cắp tài khoản,..

Các giai đoạn tấn công: duy trì truy cập

- Duy trì truy cập nói đến việc kẻ tấn công cố gắng giữ lại quyền sở hữu hệ thống.
- Kẻ tấn công sử dụng các hệ thống đã chiếm được để bắt đầu các cuộc tấn công tiếp theo.
- Kẻ tấn công có thể giữ quyền sở hữu hệ thống của mình khỏi những kẻ tấn công khác bằng backdoors, rootkits, hoặc trojan.
- Kẻ tấn công có thể thực hiện tất cả các thao tác với dữ liệu của hệ thống đang sở hữu.

Các giai đoạn tấn công: xóa dấu vết

- Kẻ tấn công tiến hành xóa các bản ghi trên máy chủ, hệ thống và các ứng dụng để tránh bị nghi ngờ..
- Mục đích:
  - Là các hoạt động để che giấu hành vi tấn công của kẻ tấn công.
  - Tiếp tục truy cập vào hệ thống của nạn nhân vì không bị chú ý và phát hiện, xóa bằng chứng liên quan đến bản thân.

Các loại tấn công (1)

- Tấn công vào hệ điều hành
  - Kẻ tấn công tìm kiếm các lỗ hổng của hệ điều hành và khai thác chúng để truy cập vào hệ thống mạng. Các lỗ hổng như :
  - ❑ Lỗ hổng tràn bộ đệm
  - ❑ Lỗi trong hệ điều hành
  - ❑ Hệ điều hành chưa vá lỗi
- Tấn công cấp ứng dụng
  - Phần mềm ứng dụng đi kèm với nhiều chức năng nên dễ phát sinh lỗi
  - Phát hành gấp rút nên thiếu thời gian thử nghiệm

Các loại tấn công (2)

- Tấn công vào cấu hình sai
  - Khi một hệ thống bị lỗi cấu hình, như sự thay đổi trong quyền truy cập vào tập tin, thì nó đã trở nên không an toàn.
  - Các quản trị viên sẽ thiết lập các cấu hình thiết bị trước khi triển khai trong mạng. nếu không có những thiết lập mặc định này thiết bị sẽ dễ dàng bị tấn công.
- Tấn công gói tin nhỏ
  - Khi cài đặt các hệ điều hành hoặc phần mềm ứng dụng thì bản mẫu sẽ có các mặc định để việc quản lý trở nên dễ dàng hơn. Khi chúng ta thay đổi các mặc định đó thì sẽ lộ ra các lỗ hổng để cho nhưng kẻ tấn công có thể khai thác và tấn công vào các gói tin nhỏ.

Vấn đề về kiểm thử xâm nhập mạng

- Không có mạng nào là an toàn tuyệt đối.
- Giúp đưa ra các chiến lược theo chiều sâu. Tức là việc phân tích, xâm nhập vào mạng của chính mình và tiếp xúc cũng như tính toán về chúng.
- Kiểm thử xâm nhập mạng là cần thiết bởi vì nó cho phép phòng chống các cuộc tấn công từ hacker bằng cách dự đoán các cách tấn công mà họ có thể sử dụng để xâm nhập vào một hệ thống.
- Phòng thủ chiều sâu:
  - Phòng thủ chiều sâu là một chiến lược an ninh trong đó một số lớp bảo vệ được đặt trên toàn bộ hệ thống thông tin
  - Nó giúp ngăn chặn các cuộc tấn công vì khi kẻ tấn công qua một lớp thì sẽ gặp lớp phòng thủ tiếp theo

Kiểm thử xâm nhập mạng

- Ưu điểm
  - Là một phần quan trọng của đánh giá nguy cơ, kiểm toán, quản trị hệ thống,..
  - Được sử dụng để nhận diện rủi ro làm các hoạt động khắc phục hậu quả và làm giảm nguy cơ an toàn hệ thống thông qua việc giải quyết các lỗ hổng
- Hạn chế
  - Chỉ khi các doanh nghiệp biết hệ thống của họ có lỗi họ mới thuê kiểm tra hệ thống của mình và cũng chỉ có một lần duy nhất.
  - Chỉ có các tổ chức cần có bảo vệ mạng mới có nhu cầu

Nghiên cứu lỗ hổng (1)

- **Định nghĩa**
  - Quá trình phát hiện ra các lỗ hổng trong thiết kế để tấn công hoặc lợi dụng hệ điều hành và các ứng dụng của nó.
  - Các lỗ hổng thường được phân loại dựa trên mức độ nghiêm trọng (thấp, trung bình, cao) và phạm vi khai thác (cục bộ hoặc từ xa).
- **Mục đích**
  - Để xác định và sửa chữa các lỗ hổng mạng
  - Để bảo vệ mạng khỏi bị tấn công bởi những kẻ xâm nhập
  - Thu thập thông tin về các loại virus
  - Để có được thông tin giúp giải quyết các vấn đề an ninh
  - Để tìm ra các điểm yếu và cảnh báo người quản trị mạng trước khi bị tấn công
  - Để biết làm sao khôi phục được các thiết bị sau khi bị tấn công.

Nghiên cứu lỗ hổng (2)

- Kiểm thử xâm nhập là một phương pháp chủ động đánh giá sự an toàn của mạng hoặc hệ thống thông tin bằng cách mô phỏng các cuộc tấn công từ một nguồn độc hại.
- Tích cực phân tích những điểm yếu thiết kế sai sót kĩ thuật và các lỗ hổng.
- Trong một cuộc kiểm tra :
  - Hộp đen mô phỏng một cuộc tấn công từ một người không có kiến thức về hệ thống
  - Hộp trắng mô phỏng một cuộc tấn công từ một người có thông tin/ kiến thức về hệ thống.
- Kết quả được gửi toàn bộ trong một báo cáo để người sử dụng có thể kiểm tra về điều hành, quản lý và kĩ thuật

Nghiên cứu lỗ hổng (3)

- Tại sao phải tiến hành kiểm thử xâm nhập
  - Xác định các mối đe dọa đối với hệ thống thông tin của một tổ chức.

  → Xác định, giải quyết các lỗ hổng và điểm yếu trong đầu tư an ninh để cung cấp lại tốt hơn.
  - Cung cấp cho một tổ chức với một sự bảo đảm – một đánh kỹ lưỡng và toàn diện về an ninh bao gồm chính sách, thủ tục, thiết kế, và thực hiện.

  → Đạt được và duy trì chứng nhận theo quy định nghành công nghiệp.
  - Cung cấp các sản phẩm tốt nhất tuân theo các quy định của pháp luật và công nghiệp.

  → Tập trung vào các lỗ hổng có mức độ nghiêm trọng cao. Nhấn mạnh các vấn đề bảo mật ứng dụng cho các nhà phát triển và các nhà quản lý.
  - Cung cấp một phương pháp chuẩn bị toàn diện để có thể ngăn chặn các cuộc tấn công.

  → Đánh giá hiệu quả của các thiết bị an ninh mạng như firewall, route, và web server.

Phương pháp xâm nhập thử nghiệm

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

KIỂM THỬ XÂM NHẬP

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

KIỂM THỬ XÂM NHẬP

Kỹ thuật kiểm thử xâm nhập

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY

Biên soạn từ bài giảng: Nguyễn Ngọc Điệp, Bài giảng Kiểm thử xâm nhập, Học viện Công nghệ Bưu chính Viễn thông, 2021.

Module Objectives

- Kiểm thử xâm nhập
- Thẩm định bảo mật
- Quản lý rủi ro
- Tự động kiểm tra
- Hướng dẫn kiểm tra
- Liệt kê các thiết bị

- Tấn công từ chối dịch vụ
- Phòng chống hacker
- Pentest sử dụng các thiết bị khác nhau
- Webscarab
- Các công cụ khác

Module Flow

Khái niêm kiểm thử xâm nhập
Các hình thức kiểm thử xâm nhập
Kỹ thuật kiểm thử xâm nhập
Các giai đoạn kiểm thử xâm nhập
Lộ trình kiểm thử xâm nhập
Dịch vụ kiểm thử xâm nhập
Công cụ kiểm thử

Giới thiệu về kiểm thử xâm nhập

- Pen-test: Một mô phỏng các phương pháp mà những kẻ xâm nhập sử dụng để truy cập trái phép vào hệ thống mạng của một tổ chức và sau đó kiểm soát chúng
- Trong giai đoạn của kiểm thử thâm nhập, thử nghiệm được giới hạn bởi các tài nguyên cụ thể là thời gian, nguồn lực có tay nghề cao, và phạm vi truy cập như đã nêu trong thỏa thuận Pen-test
- Hầu hết các kẻ tấn công theo một cách tiếp cận chung để thâm nhập vào một hệ thống

Đánh giá bảo mật

- Mỗi tổ chức đều sử dụng các mức đánh giá an ninh khác nhau để xác nhận mức độ an toàn về tài nguyên mạng

Các mức đánh giá an ninh

- Kiểm tra an ninh
- Đánh giá tính dễ bị tấn công
- Kiểm thử xâm nhập

- Mỗi loại hình đánh giá an toàn đòi hỏi người thực hiện việc đánh giá phải có kỹ năng khác nhau

Đánh giá lỗ hổng

Network Scanning	• Đánh giá lỗ hổng: quét một mạng để tìm các lỗ hổng
Scanning Tools	• Công cụ quét lỗ hổng cho phép tìm kiếm các phân đoạn mạng của các thiết bị IP-enabled và liệt kê hệ thống, hệ điều hành và ứng dụng
Security Mistakes	• Ngoài ra, trình quét lỗ hổng có thể xác định sai sót phổ biến của việc cấu hình bảo mật
Test Systems/Network	• Trình quét lỗ hổng có thể kiểm tra hệ thống và mạng lưới các thiết bị ảnh hưởng trực tiếp bởi các cuộc tấn công thông thường

Hạn chế của đánh giá bảo mật

1. Phần mềm đánh giá bảo mật bị giới hạn trong khả năng phát hiện các lỗ hổng tại một điểm nhất định trong thời gian nhất định
2. Nó phải được cập nhật khi các lỗ hổng mới được phát hiện hoặc các sửa đổi được làm cho các phần mềm đang được sử dụng
3. Điều này có thể ảnh hưởng đến kết quả của đánh giá
4. Phương pháp được sử dụng cũng như các phần mềm Vulnerability scanning đa dạng đánh giá an ninh khác nhau

Kiểm thử xâm nhập

- Đánh giá các mô hình bảo mật của tổ chức một cách tổng thể
- Khác biệt ở chỗ là một tấn công có mục đính chính đáng và không ác ý
- Cho thấy hậu quả tiềm tàng của một tấn công thực sự vào mạng
- Nếu không được hoàn thành một cách chuyên nghiệp có thể dẫn đến sự mất mát của các dịch vụ và sự gián đoạn sự ổn định kinh doanh.

Tại sao phải kiểm thử xâm nhập (1)

- Xác định các mối đe dọa đối với tài sản thông tin của một tổ chức
- Giảm chi phí bảo mật của một tổ chức và đầu tư công nghệ bảo mật một cách tốt hơn bằng cách xác định và giải quyết các lỗ hổng và điểm yếu
- Cung cấp một tổ chức với sự đảm bảo - một đánh giá kỹ lưỡng và toàn diện của một tổ chức an ninh bao gồm chính sách, thủ tục, thiết kế và thực hiện
- Đạt được và duy trì chứng nhận quy định ngành (BS7799, HIPAA…)
- Thông qua thực hiện tốt bằng cách xác nhận quy định của pháp luật và ngành

Tại sao phải kiểm thử xâm nhập (2)

- Đối với thử nghiệm và xác nhận hiệu quả của việc bảo vệ an ninh và kiểm soát
- Tập trung vào các lỗ hổng có mức độ cao và nhấn mạnh các vấn đề bảo mật cấp độ ứng dụng cho các nhóm phát triển và quản lý
- Cung cấp phương pháp tiếp cận toàn diện của các bước chuẩn bị có thể được thực hiện để ngăn chặn khai thác trái phép sắp tới
- Đánh giá hiệu quả của các thiết bị an ninh mạng như firewalls, routers, and web servers
- Để thay đổi, nâng cấp cơ sở hạ tầng hiện có của phần mềm, phần cứng, hoặc thiết kế mạng

Đối với các tổ chức

- Tổ chức phải tiến hành một hoạt động đánh giá rủi ro trước khi thử nghiệm xâm nhập sẽ giúp xác định các mối đe dọa chính, chẳng hạn như:
  - Truyền tải thất bại, thất bại trong các giao dịch trên mạng, và mất thông tin bí mật
  - Hệ thống phải đối mặt với cộng đồng, các trang web, cổng email, và các nền tảng truy cập từ xa
  - Mail, DNS, firewall, password, FTP, IIS, web server.

Lưu ý

- Thiết lập các tham số cho các kiểm thử như mục tiêu, hạn chế và sự đúng đắn của quy trình
- Thuê chuyên gia lành nghề và giàu kinh nghiệm để thực hiện các kiểm tra
- Chọn một bộ các phần kiểm tra phù hợp để cân bằng chi phí và lợi ích
- Một phương pháp luận luôn đi với lập kế hoạch và tài liệu
- Ghi chép kết quả một cách cẩn thận và làm cho nó dễ hiểu cho khách hàng
- Nêu rõ rủi ro tiềm ẩn và việc tìm kiếm một cách rõ ràng trong báo cáo cuối cùng

ROI với kiểm thử xâm nhập

- Các công ty sẽ chi cho các kiểm tra pen-test chỉ khi họ hiểu một cách đúng đắn về lợi ích của các kiểm pen-test
- Kiểm thử giúp các công ty trong việc xác định, hiểu biết, và giải quyết các lỗ hổng, nhờ đó tiết kiệm rất nhiều tiền trong ROI (Return on Investment)
- Chứng tỏ tỷ lệ hoàn vốn cho việc kiểm thử với sự giúp đỡ của một kế hoạch kinh doanh, bao gồm các chi phí và lợi nhuận liên quan đến nó
- Thử nghiệm của ROI là một quá trình quan trọng cho sự thành công trong việc bán dịch vụ kiểm thử xâm nhập

Điểm khởi đầu kiểm thử

- Tổ chức phải đạt được một sự đồng thuận về mức độ thông tin có thể được tiết lộ cho các đội kiểm thử để xác định điểm khởi đầu của thử nghiệm
- Cung cấp cho nhóm kiểm thử xâm nhập các thông tin bổ sung này tạo cho họ một lợi thế thực tế
- Tương tự như vậy, mức độ mà các lỗ hổng cần được khai thác mà không làm gián đoạn các dịch vụ quan trọng, cần được xác định.

Địa điểm kiểm tra

- Nhóm nghiên cứu pen- test có thể có một sự lựa chọn làm các kiểm tra từ xa hoặc tại chỗ
- Một đánh giá từ xa có thể mô phỏng một cuộc tấn công của hacker từ bên ngoài. Tuy nhiên, nó có thể bỏ lỡ đánh giá bảo vệ nội bộ
- Đánh giá tại chỗ có thể rất tốn kém và không thể mô phỏng tác động bên bên ngoài một cách chính xác

Module Flow

Khái niêm kiểm thử xâm nhập
Các hình thức kiểm thử xâm nhập
Kỹ thuật kiểm thử xâm nhập
Các giai đoạn kiểm thử xâm nhập
Lộ trình kiểm thử xâm nhập
Dịch vụ kiểm thử xâm nhập
Công cụ kiểm thử

Các hình thức kiểm thử

- Có 2 hình thức kiểm thử là:
  - External testing: Kiểm thử bên ngoài bao gồm phân tích các thông tin công khai sẵn có, một giai đoạn liệt kê mạng lưới, và hoạt động của các thiết bị phân tích an ninh
  - Internal Testing: Kiểm thử nội bộ sẽ được thực hiện từ một số điểm truy cập mạng, đại diện cho mỗi phân đoạn logic và vật lý

Kiểm thử bên ngoài

- Là phương pháp truyền thống để kiểm thử xâm nhập
- Kiểm thử tập trung vào cơ sở hạ tầng máy chủ và phần mềm cơ bản gồm các mục tiêu
- Nó có thể được thực hiện mà không cần biết thông tin trước đó của trang web (hộp đen)
- Công bố cấu trúc liên kết và môi trường (hộp trắng)
- Pen-testing bên ngoài bao gồm phân tích một cách toàn diện về cách thức sử dụng thông tin, chẳng hạn như: Web server, mail server, firewall, router…

Black box Pen-test

- Sẽ không biết rõ nếu cơ sở hạ tầng chưa được kiểm tra
- Chỉ được gợi ý tên công ty
- Pen-test phải được tiến hành sau khi đã thu thập thông tin nhiều phía và nghiên cứu
- Kiểm thử này mô phỏng quá trình của một hacker thực sự
- Nó quyết định đáng kể đến việc phân bổ của quá trình, qua đó tìm ra bản chất của cơ sở hạ tầng và làm thế nào nó kết nối và liên hệ với nhau
- Tốn thời gian và là loại kiểm thử tốn kém

White box Pen-test

- Hoàn thiện sự hiểu biết về cơ sở hạ tầng
- Kiểm thử loại này mô phỏng các hoạt động của nhân viên của công ty
- Thông tin được cung cấp gồm:
  - Cơ sở hạ tầng của công ty
  - Loại hình mạng
  - Các triển khai an ninh hiện nay
  - IP address/ firewall/ IDS
  - Chính sách công ty làm và không nên làm

Grey box Pen-test

- Trong kiểm thử hộp xám, thử nghiệm thường có thông tin hạn chế
- Thực hiện đánh giá và kiểm tra an ninh bên trong
- Phương pháp bảo mật cho ứng dụng bằng cách kiểm tra tất cả các lỗ hổng mà hacker có thể tìm thấy và khai thác
- Thực hiện chủ yếu khi ki thuật kiểm thử bắt đầu kiểm tra hộp đen trên các hệ thống được bảo vệ tốt và có được một ít kinh nghiệm cần thiết để tiến hành xem xét kỹ lưỡng

Kiểm thử bên trong

- Việc kiểm thử sẽ được thực hiện từ một số các điểm truy cập mạng, đại diện cho mỗi phân đoạn logic và vật lý
- Ví dụ, điều này có thể bao gồm lớp và DMZ trong môi trường mạng nội bộ công ty hoặc kết nối các công ty đối tác
- Đánh giá an ninh nội bộ theo một phương pháp tương tự để kiểm tra bên ngoài, nhưng cung cấp một cái nhìn đầy đủ hơn về an ninh của trang web

Kiểm thử có thông báo (Announced Testing)

- Là một nỗ lực để đạt được sự thỏa hiệp với hệ thống trên máy khách với sự phối hợp toàn diện và kiến thức của các nhân viên IT
- Kiểm tra các cơ sở hạ tầng bảo mật hiện có lỗ hổng
- Đòi hỏi các nhân viên an ninh trong đội pentest thực hiện kiểm toán

Kiểm thử không thông báo (Unannounced Testing)

- Một thử nghiệm thỏa hiệp hệ thống mạng lưới khách hàng mà không cần thông tin của nhân viên an ninh
- Cho phép chỉ quản lý ở mức cao để được nhận biết các kiểm thử
- Kiểm tra an ninh cơ sở hạ tầng và đáp ứng của nhân viên công nghệ thông tin

Kiểm thử tự động

- Tự động kiểm tra có thể tiết kiệm thời gian và tiết kiệm chi phí trong một thời gian dài, tuy nhiên, nó không thể thay thế kinh nghiệm chuyên gia bảo mật chuyên nghiệp
- Như với công cụ quét lỗ hổng, có thể là có thể đưa ra kết quả đúng hoặc sai.
- Công cụ có thể học hỏi theo một biểu đồ, và cần phải cập nhập thường xuyên để có hiệu quả
- Với kiểm thử tự động, không tồn tại phạm vi kiểm tra cho bất kì thành phần kiến trúc

Kiểm thử thủ công

- Hướng dẫn kiểm thử là lựa chọn tốt nhất một tổ chức có thể chọn để hưởng lợi từ kinh nghiệm của một chuyên gia an ninh
- Mục đích của các chuyên gia là đánh giá tình trạng bảo mật của tổ chức từ góc độ của một kẻ tấn công
- Để tiếp cận hướng dẫn đòi hỏi có quy hoạch, kiểm tra thiết kế, lập kế hoạch, và tìm tài liệu hướng dẫn để nắm bắt kết quả của quá trình kiểm định

Module Flow

Khái niêm kiểm thử xâm nhập
Các hình thức kiểm thử xâm nhập
Kỹ thuật kiểm thử xâm nhập
Các giai đoạn kiểm thử xâm nhập
Lộ trình kiểm thử xâm nhập
Dịch vụ kiểm thử xâm nhập
Công cụ kiểm thử

Kỹ thuật kiểm thử xâm nhập phổ biến (1)

- **Nghiên cứu bị động**
  - Được sử dụng để thu thập tất cả các thông tin về cấu hình hệ thống của một tổ chức
- **Giám sát mã nguồn mở**
  - Tạo điều kiện cho tổ chức thực hiện các bước cần thiết để đảm bảo bí mật và tính toàn vẹn dữ liệu
- **Lập bản đồ mạng**
  - Được sử dụng để có thể nắm được cấu hình của mạng lưới đang được thử nghiệm
- **Giả mạo**
  - Thực hiện bằng cách sử dụng 1 máy tính để giả vờ là một máy khách
  - Được sử dụng ở đây để kiển thử xâm nhập nội bộ và bên ngoài
- **Network sniffing**
  - Được sử dụng để lấy được dữ liệu khi nó được truyền qua mạng

Kỹ thuật kiểm thử xâm nhập phổ biến (2)

- **Trojan tấn công**
  - Mã độc hoặc các chương trình thường được gửi qua mạng dưới dạng file đính kèm email hoặc chuyển qua tin nhắn vào phòng chat
- **Tấn công vét cạn**
  - Là phương pháp bẻ khóa phổ biến nhất từng được biết đến Network Sniffing
  - Được sử dụng để lấy được dữ liệu khi nó di chuyển qua mạng
  - Có thể quá tải hệ thống và ngăn chặn hệ thống đáp ứng các yêu cầu của pháp luật
- **Quét lỗ hổng**
  - Là một kiểm tra toàn diện các vùng của cơ sở hạ tầng mạng của tổ chức
- **Phân tích tình huống**
  - Là giai đoạn cuối cùng của thử nghiệm, đánh giá rủi ro của các lỗ hổng chính xác hơn

Sử dụng tên miền DNS và địa chỉ IP

1. Dữ liệu trên các máy chủ DNS liên quan đến mạng lưới các mục tiêu có thể được sử dụng để lập bản đồ mạng của một tổ chức đích
2. Việc chặn IP của một tổ chức có thể được thực hiện bằng cách tìm kiếm tên miền và thông tin liên lạc cho nhân viên
3. Các bản ghi DNS cũng cung cấp một số thông tin giá trị liên quan đến hệ điều hành hoặc ứng dụng được chạy trên máy chủ

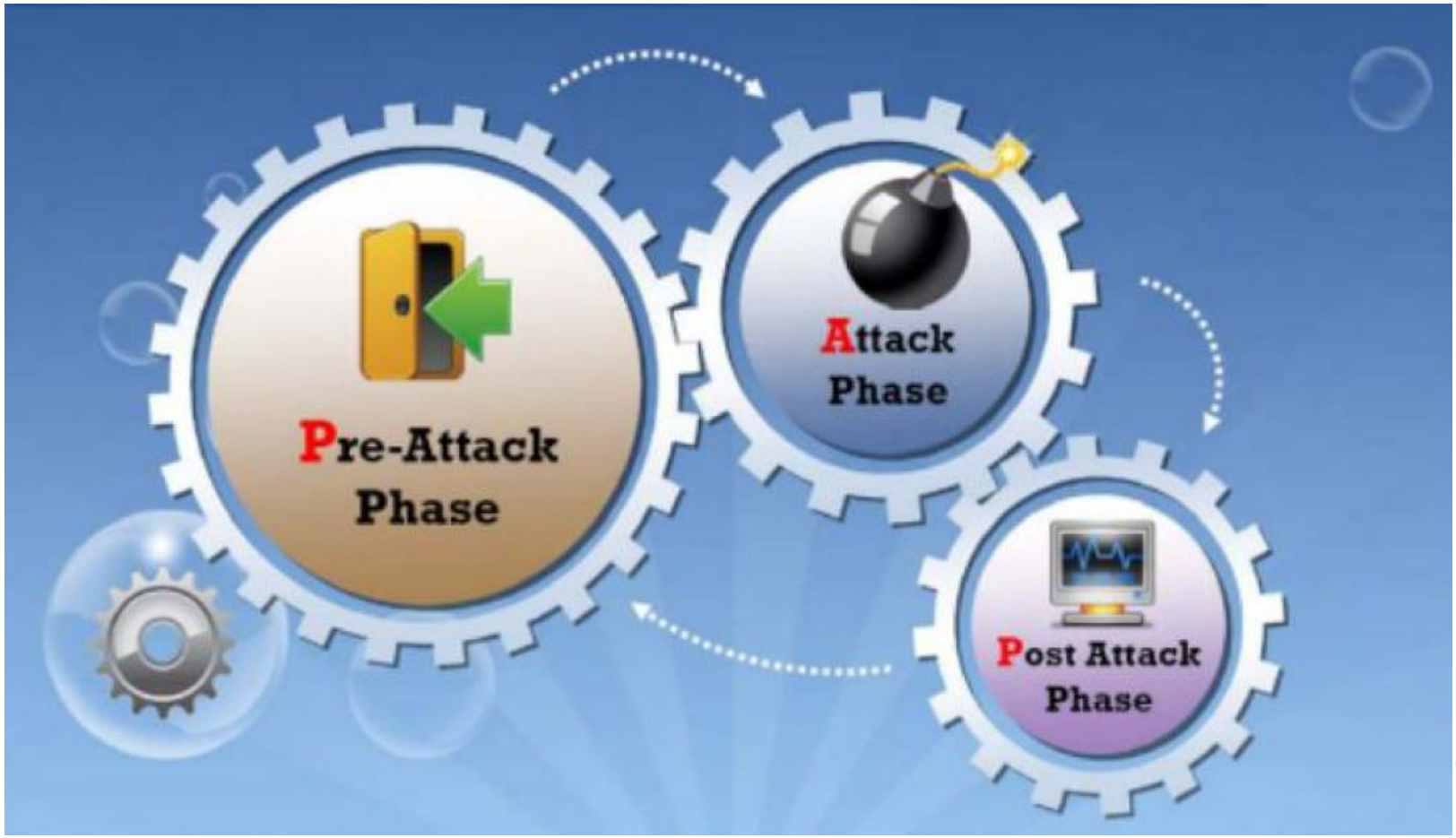
Liệt kê các thông tin về máy chủ trên mạng công khai có sẵn

- Việc liệc kê có thể được thực hiện bằng cách sử dụng công cụ quét port, giao thức IP, và lắng nghe các cổng TCP / UDP
- Nhóm kiểm thử sau đó có thể hình dung một sơ đồ mạng lưới chi tiết có thể được truy cập một cách công khai
- Trình thu thập dữ liệu trang web có thể phản ánh toàn bộ các trang web
- Thêm vào đó, các nỗ lực có thể cung cấp subnet đươc sàng lọc và một danh sách đầy đủ các loại được cho phép lưu thông trong và ngoài mạng

Module Flow

Khái niêm kiểm thử xâm nhập
Các hình thức kiểm thử xâm nhập
Kỹ thuật kiểm thử xâm nhập
Các giai đoạn kiểm thử xâm nhập
Lộ trình kiểm thử xâm nhập
Dịch vụ kiểm thử xâm nhập
Công cụ kiểm thử

Các giai đoạn của kiểm thử xâm nhập



Các giai đoạn trước khi tấn công (1)

- Giai đoạn trước khi tấn công là để cập đến chế độ của cuộc tấn công và mục tiêu phải đạt được
- Do thám được coi là giai đoạn trong giai đoạn trước khi tấn công để xác định vị trí, thu thập, xác định và ghi thông tin về mục tiêu
- Hacker tìm kiếm để tìm hiểu càng nhiều thông tin của nan nhân càng tốt
- Hacker thu thập thông tin theo những cách khác nhau cho phép chúng xây dựng kế hoạch tấn công.

Các giai đoạn trước khi tấn công (2)

- Có hai loại:
  - Trinh sát thụ động gắn với việc thu thập thông tin về mục tiêu từ các truy cập công cộng trong hoạt động trinh sát. Gồm kỹ thuật thu thập thông tin thông trên các nguồn công cộng, ghé thăm trên các trang web, phỏng vấn và bảng câu hỏi
  - Trinh sát chủ động: tiếp xúc trực tiếp với đối tượng

Thông tin lấy trong giai đoạn trước khi tấn công

- Thông tin cạnh tranh
- Thông tin đăng ký trên mạng
- Thông tin DNS và mail server
- Thông tinh hoạt động hệ thống
- Thông tin của người dùng
- Thông tin Chứng nhận xác thực
- Kết nối tương tự
- Thông tin liên lạc
- Thông tinh website
- Địa chỉ vật lý và logic của tổ chức
- Phạm vi sản phẩm và dịch vụ được cung cấp bởi công ty mục tiêu có trên mạng
- Bất kỳ thông tin nào khác có giá trị đều có thể khai thác

Giai đoạn tấn công

Xâm nhập vùng ngoài

Thu thập mục tiêu

Thực thi tấn công

Đặc quyền được nâng cao

Kiểm thử vòng ngoài

- Phương pháp kiểm thử cho an ninh vòng ngoài bao gồm những bước sau (nhưng không giới hạn):
  - Đánh giá báo cáo lỗi và quản lý lỗi với thăm dò ICMP
  - Kiểm thử danh sách kiểm soát truy cập bằng cách giả mạo các câu trả lời với các gói dữ liệu thủ công
  - Xác định ngưỡng từ chối dịch vụ bằng cách cố gắng kết nối lên tục dùng TCP, đánh giá các kết nối chuyển tiếp TCP và cố gắng kết nối sử dụng UDP.
  - Đánh giá các quy tắc lọc giao thức bằng cách cố gắng kết nối sử dụng các giao thức khác nhau chẳng hạn như SSH, FTP, và Telnet 9
  - Đánh giá khả năng của IDS bằng cách gởi mã độc hại (chẳng hạn như URL bị thay đổi) và quét các mục tiêu khác nhau để đáp ứng lưu lượng truy cập bất thường
  - Kiểm thử phản ứng của hệ thống an ninh vòng ngoài của web server bằng cách sử dụng nhiều phương pháp như POST, DELETE và COPY

Liệt kê các thiết bị

- Kiểm kê thiết bị là một tập hợp các thiết bị mạng cùng với một số thông tin liên quan về mỗi thiết bị được ghi lại trong một tài liệu
- Sau khi mạng đã được lập bản đồ và các tài sản kinh doanh được xác định, bước hợp lý tiếp theo là làm một bản kê cho các thiết bị
- Kiểm tra vật lý có thể được thực hiện bổ sung để đảm bảo rằng việc liệt kê các thiết bị đã được cố định

Hoạt động: Thu thập mục tiêu

- Thu thập một mục tiêu cần phải tập hợp các hoạt động được thực hiện bởi các tester với các đối tượng máy bị nghi ngờ sử dụng nhiều các thử thách xâm nhập chẳng hạn như quét lỗ hổng và đánh giá an ninh
- Phương pháp thử nghiệm để đạt được mục tiêu bao gồm (nhưng không hạn chế) như:
  - **Hoạt động của các cuộc tấn công thăm dò**: Sử dụng kết quả của việt quét mạng để thu thập thêm thông tin có thể dẫn đến một sự thỏa hiệp
  - **Quá trình chạy quét lỗ hổng**: Quá trình quét lỗ hổng được hoàn thành trong giai đoạn này
  - **Hệ thống đáng tin cậy và quá trình đánh giá độ tin cậy**: Cố gắng truy cập tài nguyên của máy bằng cách sữ dụng thông tin hợp pháp thu được thông qua kỹ thật giao tiếp hoặc các kỹ thuật khác

Hoạt động: kỹ thuật leo thang đăc quyền

- Một khi đã dành được mục tiêu, tester cố gắng khai thác hệ thống và truy cập các nguồn tài nguyên được bảo vệ. Các hoạt động bao gồm (nhưng không giới hạn):
  - Các tester có thể tận dụng lợi thế của các chính sách bảo mật kém và tận dụng lợi thế của email hoăc code web không an toàn để thu thập thông tin có thể dẫn đến sự leo thang các đặc quyền
  - Sử dụng các kỹ thuật như brute force để đạt được đặc quyền. Ví dụ về các công cụ bao gồm nhận quản trị và mật khẩu crackers
  - Sử dụng các Trojans và phân tích giao thức
  - Sử dụng thông tin thu thập được thông qua các kỹ thuật như kỹ thuật giao tiếp để truy cập trái phép vào các nguồn tài nguyên đặc quyền

Hoạt động: Thực thi, cấy ghép và xem lại

- **Kiểm soát hệ thống:**
  - Trong giai đoạn này, tester có được sự thỏa hiệp của hệ thống bằng cách thực hiện đoạn code bất kỳ
- **Thâm nhập vào hệ thống:**
  - Mục tiêu của quá trình thâm nhập hệ thống là để tìm mức độ lỗi của hệ thống an ninh
- **Thực hiện các khai thác:**
  - Thực hiện khai thác bằng các công cụ đã có sẵn hoặc bằng tay để sử dụng các lỗ hổng được xác định trong hệ thống của mục tiêu

Giai đoạn sau tấn công và hoạt động

- Giai đoạn này quan trọng đối với kiểm tra thâm nhập vì nó có trách nhiệm để khôi phục lại các hệ thống trước kia
- Các hoạt động bao gồm những bước sau:
  - Loại bỏ tất cả các tập tin đã tải lên trên hệ thống
  - Làm sạch tất cả các mục đăng ký và loại bỏ lỗ hổng
  - Loại bỏ tất cả các công cụ và khai thác từ các hệ thống thử nghiệm
  - Khôi phục lại mạng lưới thử nghiệm bằng cách loại bỏ chia sẻ và kết nối
  - Phân tích tất cả các kết quả và trình bày cùng với các tổ chức

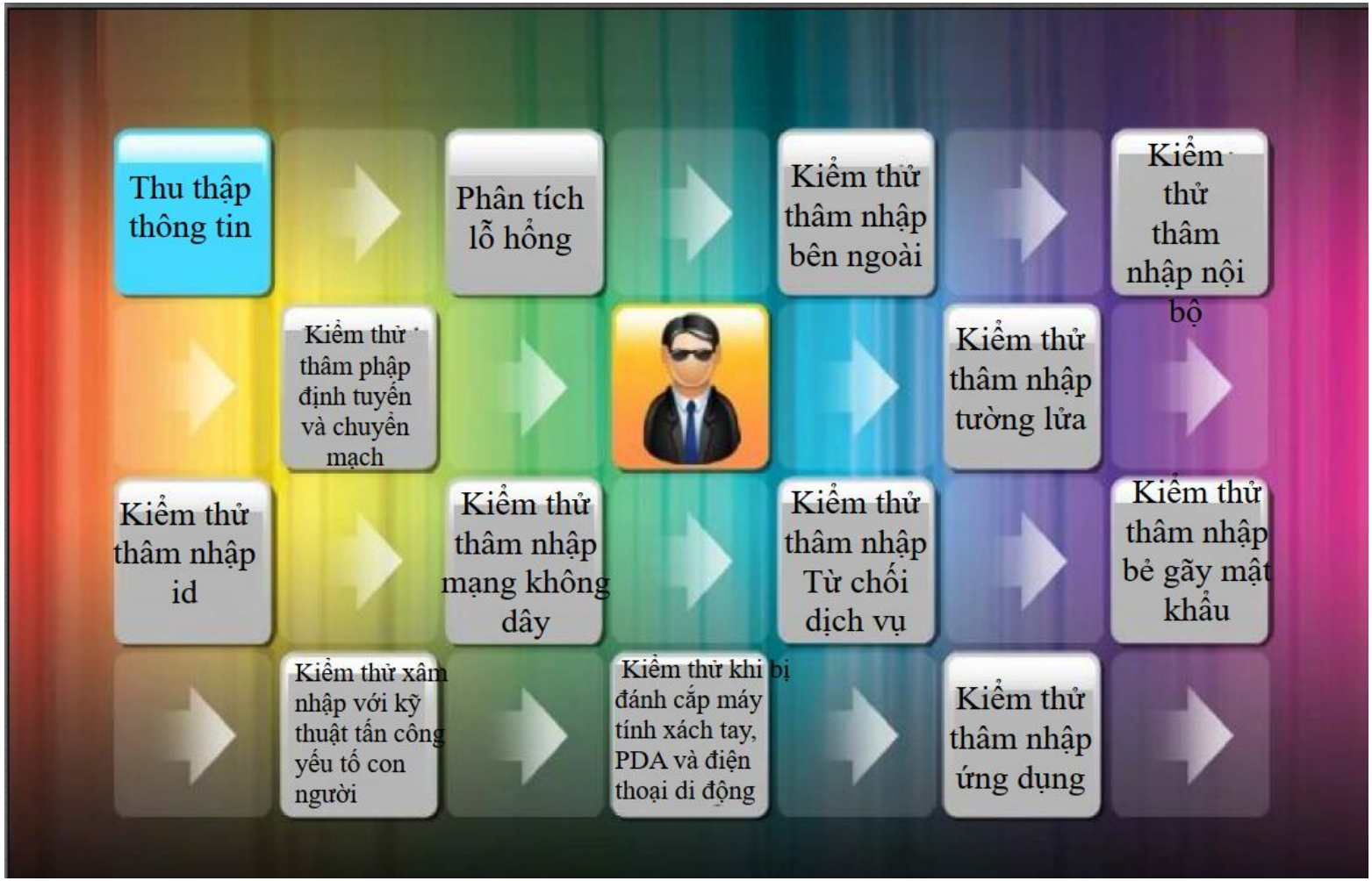
Kết quả của kiểm thử xâm nhập

- Báo cáo pen-test cho biết chi tiết của các sự cố trong các quá trình thử nghiệm và phạm vi hoạt động
- Bao gồm mục tiêu, quan sát, thực hiện các hoạt động, và báo cáo các sự cố
- Nhóm nghiên cứu cũng có thể đề nghị biện pháp khắc phục dựa trên các quy tắc tham gia

Module Flow

Khái niêm kiểm thử xâm nhập
Các hình thức kiểm thử xâm nhập
Kỹ thuật kiểm thử xâm nhập
Các giai đoạn kiểm thử xâm nhập
Lộ trình kiểm thử xâm nhập
Dịch vụ kiểm thử xâm nhập
Công cụ kiểm thử

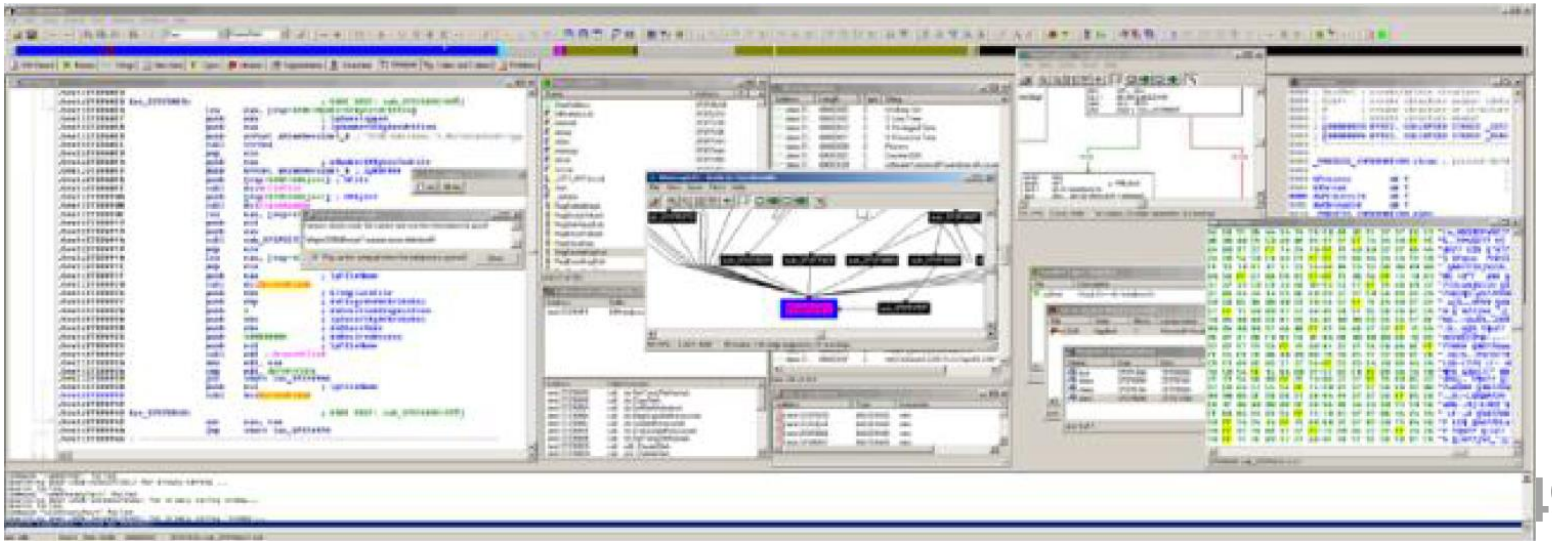
Lộ trình kiểm thử xâm nhập (1)



Lộ trình kiểm thử xâm nhập (2)

Đánh giá bảo mật ứng dụng

- Ngay cả trong một cơ sở hạ tầng được triển khai và bảo đảm, một ứng dụng yếu có thể tiếp cận với thông tin quan trọng của tổ chức là điều không thể chấp nhận được
- ứng dụng đánh giá an ninh được thiết kế để xác định và đánh giá các mối đe dọa cho tổ chức
- Thử nghiệm này giúp cho hệ thống chống lại người dùng có ý đồ không tốt, họ không thể truy cập, sửa đổi phá hủy dữ liệu hoặc các dịch vụ trong hệ thống



Kiểm thử ứng dụng Web (1)

Xác nhận đầu vào

- Kiểm tra bao gồm hệ điều hành chính, kịch bản chính, cơ sở dữ liệu chính, LDAP injection và cross-site scripting

Sự cải thiện đầu ra

- Các kiểm tra này bao gồm các phân tích các ký tự đặc biệt và xác minh kiểm tra trong ứng dụng lỗi

Điều khiển truy cập

- Kiểm tra quyền truy cập vào giao diện quản trị, sẽ gửi dữ liệu để thao tác các trường mẫu, cố gắng truy vấn URL, thay đổi các giá trị trên kịch bản phía máy khách và tấn công cookie

Kiểm thử ứng dụng Web (2)

Kiểm tra các lỗi tràn bộ đệm

- Kiểm tra bao gồm các cuộc tấn công chống lại tràn ngăn xếp, tràn khối xếp, và tràn chuỗi định dạng

Kiểm thử thành phần

- Kiểm tra kiểm soát an ninh trên các thành phần máy chủ ứng dụng web mà có thể phát hiện các ứng dụng lỗ hổng web

Từ chối dịch vụ

- Các kiểm tra khả năng ngăn chặn DoS

Kiểm thử dữ liệu và lỗi

- Kiểm tra các dữ liệu liên quan đến an ninh như lưu trữ dữ liệu trong bộ nhớ cache hoặc thông qua các dữ liệu bằng cách sử dụng HTML

Kiểm thử ứng dụng Web (3)

Kiểm tra bảo mật

- Các ứng dụng sử dụng giao thức an toàn và mã hóa, kiểm tra các sai sót trong cơ chế trao đổi khóa, chiều dài khóa đầy đủ, và các thuật toán.

Phiên quản lý

- Nó sẽ kiểm tra thời gian hiệu lực của thẻ phiên, chiều dài của thẻ, hết hạn của phiên thẻ từ sử dụng SSL đến không sử dụng SSL, sự hiện diện của bất kỳ thẻ phiên trong lịch sử trình duyện hoặc bộ nhớ cache, và ngẫu nhiên phiên ID (kiểm tra sử dụng dữ liệu người sử dụng trong việc tạo ID).

Mã xác nhận cấu hình

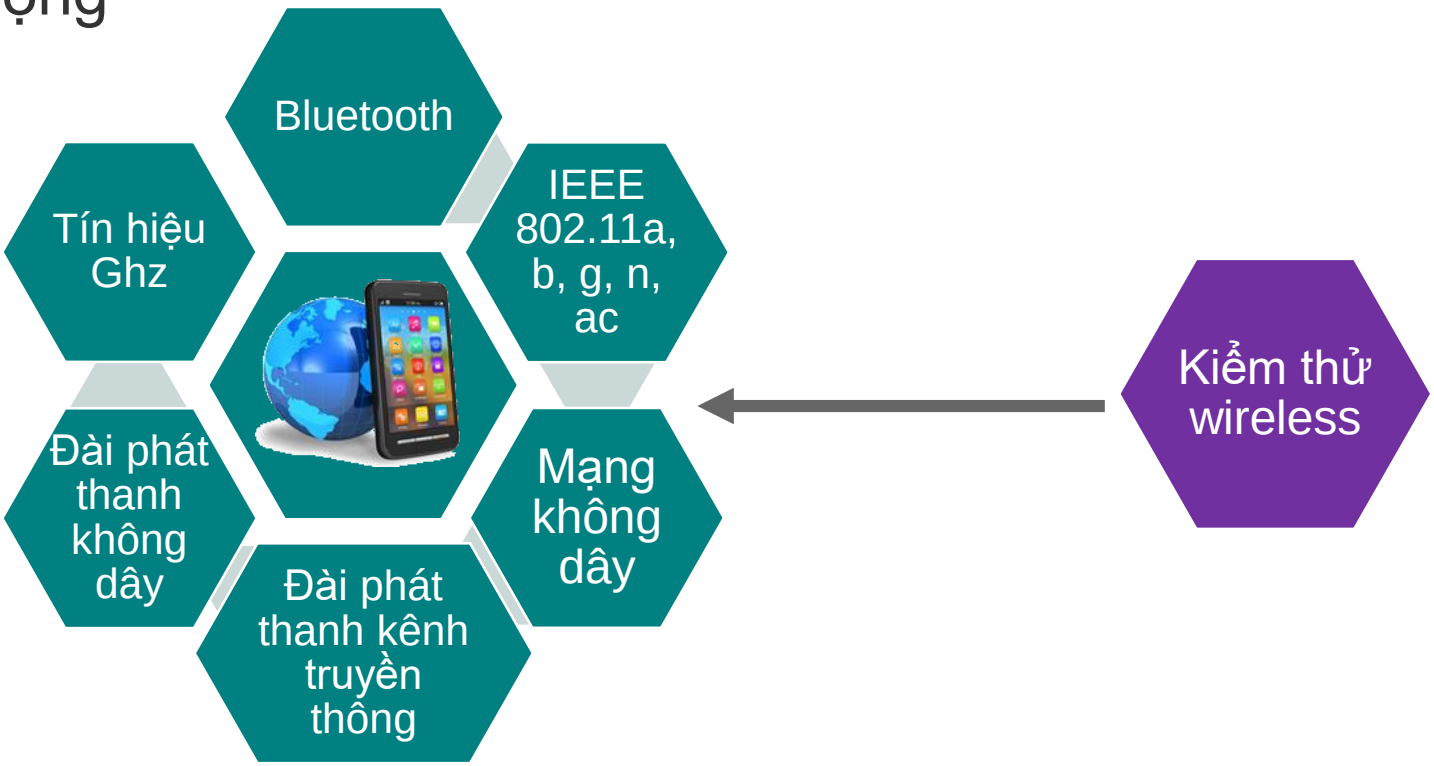
- Cố gắng để khai thác tài nguyên bằng cách sử dụng phương thức HTTP, kiểm tra các phiên bản nội dung có sẵn và kiểm tra các lỗ hổng được biết đến và khả năng tiếp cận các giao diện trong các máy chủ và các thành phần máy chủ.

Đánh giá an ninh mạng

- Nó quét trên môi trường mạng để xác định các lỗ hổng và giúp cải thiện chính sách bảo mật của doanh nghiệp
- Nó phát hiện ra lỗi an ninh mạng có thể dẫn đến dữ liệu hoặc thiết bị đang được khai thác hoặc bị phá hủy bởi các trojan, các cuộc tấn công từ chối dịch vụ, và sự xâm nhập khác
- Nó đảm bảo rằng việc thực hiện an ninh thực sự cung cấp sự bảo vệ mà doanh nghiệp yêu cầu khi bất kỳ cuộc tấn công diễn ra trên mạng, thường bởi "khai thác" một lỗ hổng hệ thống
- Nó được thực hiện bởi nhóm tìm cách đột nhập vào mạng hoặc máy chủ

Đánh giá wireless/Remote Access

- Đánh giá wireless/Remote Access giải quyết rủi ro về bảo mật với sự gia tăng ngày càng tăng của thiết bị di động



Kiểm thử mạng không dây

- Phương thức kiểm thử mạng không dây bao gồm:
  - Kiểm thử xem các điểm truy cập mặc định Service Set Identifier (SSID) có sẵn sang không?. Kiểm tra khả năng "SSID phát sóng" và khả năng kết nối với mạng LAN.
  - Kiểm tra các lỗ hổng trong quá trình truy cập vào mạng WLAN thông qua các wireless router, access point, or gateway. Nếu sử dụng khóa mã hóa Wired Equivalent Privacy (WEP) mặc định thì thông tin có thể được bắt và giải mã
  - Kiểm tra cho đèn hiệu broadcast của tất cả các access point và kiểm tra tất cả các giao thức có sẵn trên các điểm truy cập.
  - Kiểm tra mạng Layer 2 switch được sử dụng thay cho hub để kết nối đến các điểm truy cập
  - Mục đích chứng thực là để xem lại các quá trình xác thực trước đó nhằm kiểm tra để hạn chế truy cập trái phép
  - Giấy chứng nhận truy cập chỉ được cấp cho máy khách đăng ký địa chỉ MAC

Kiểm thử mạng – thiết bị lọc gói tin

- Mục tiêu của nhóm pen-test là để chắc chắn rằng tất cả lưu lượng truy cập hợp pháp đều đi qua thiết bị lọc.
- Kiểm thử máy chủ Proxy để đánh giá khả năng lọc ra các gói tin không mong muốn
- Kiểm thử cài đặt mặc định của tường lửa để đảm bảo rằng ID và mật khẩu mặc định của người sử dụng đã được thay đổi.
- Thực hiện các cuộc kiểm thử khác nhằm đánh giá khả năng bị tấn công từ đăng nhập từ xa

Mô phỏng từ chối dịch vụ

- Mô phỏng các cuộc tấn công DoS (từ chối dịch vụ) có thể là nguồn cường độ lớn
- Các cuộc tấn công DoS (từ chối dịch vụ) có thể được mô phỏng bằng cách sử dụng phần cứng
- Một số trang web trực tuyến mô phỏng các cuộc tấn công DoS
- Các kiểm thử kiểm tra sự hiệu quả của các thiết bị anti-Dos (phòng chống -từ chối dịch vụ)

Module Flow

Khái niêm kiểm thử xâm nhập
Các hình thức kiểm thử xâm nhập
Kỹ thuật kiểm thử xâm nhập
Các giai đoạn kiểm thử xâm nhập
Lộ trình kiểm thử xâm nhập
Dịch vụ kiểm thử xâm nhập
Công cụ kiểm thử

Dịch vụ kiểm thử xâm nhập

Hướng dẫn thực hiện:

Xác nhận rằng hạ tầng mạng đã được kiểm thử bởi một tổ chức thứ ba có thẩm quyền nhằm có được cái nhìn của một kẻ xâm nhập. Tổ chức có thể yêu cầu đánh giá các yếu tố an ninh mạng cụ thể và gợi ý biện phát khắc phục.

Đảm bảo trách nhiệm nghề nghiệp, hoàn tiền lại nếu thực hiện không đúng các thỏa thuận, chịu trách nhiệm cho các kết quả từ các hoạt động, hoặc các dịch vụ thực hiện không chuyên nghiệp
Nó còn được gọi là E&O bảo hiểm trách nhiệm nghề nghiệp

Kiểm tra thâm nhập bảo lãnh phát hành (underwriting penetration testing

Điều khoản cam kết

- Một tổ chức có thể phạt một pentester đã vi phạm bất kỳ lỗi nào được quy định rõ ràng cam kết
- Nêu rõ các điều khoản tham chiếu theo đó các cơ quan có thể tương tác với các tổ chức
- Có thể xác định mã của hành vi, các thủ tục

Quy mô dự án

- Xác định phạm vi của pentest là điều cần thiết để quyết định đó là một cuộc kiểm thử có mục tiêu hay kiểm tra một cách toàn diện
- Đánh giá toàn để phát hiện ra các lỗ hổng càng nhiều càng tốt trong toàn bộ tổ chức
- Một cuộc kiểm thử có mục tiêu sẽ tìm cách xác định các lỗ hổng trong hệ thống cụ thể và trong thực tiễn

Cấp độ thỏa thuận dịch vụ Pentest

Một thỏa thuận cấp độ dịch vụ (SLA) là một hợp đồng chi tiết về dịch vụ mà một người đảm nhận sẽ cung cấp

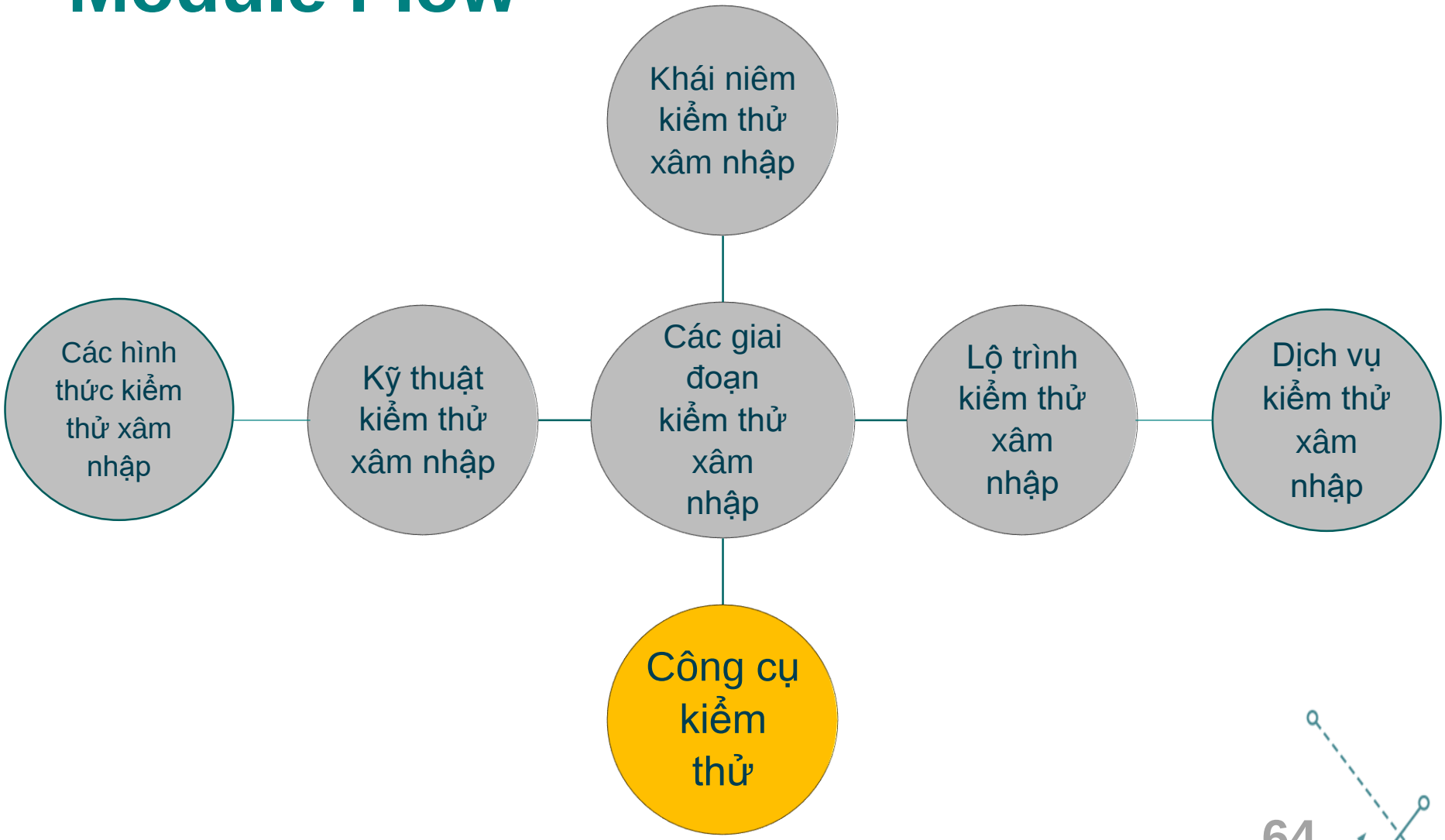
SLA xác định mức tối thiểu hành động của người kiểm thử và xác định những hành động nào sẽ thực hiện trong trường hợp có sự cố hay rối loạn nghiêm trọng

SLA thực hiện bởi các chuyên gia và có thể bao gồm cả các biện pháp khắc phục hậu quả và hình phạt

Tư vấn kiểm thử xâm nhập

- Thuê các chuyên gia đủ điều kiện để đánh giá chất lượng của kiểm thử xâm nhập
- Một cuộc kiểm thử xâm nhập vào một mạng công ty sẽ kiểm tra rất nhiều máy chủ khác nhau (và một số hệ điều hành khác nhau), kiến trúc mạng và cả chính sách và thủ tục
- Kỹ năng kiểm thử xâm nhập không thể có được nếu không có nhiều năm kinh nghiệm trong các lĩnh vực như phát triển, hệ thống quản lý, tư vấn, …
- Mỗi khu vực của mạng phải kiểm thử chuyên sâu

Module Flow

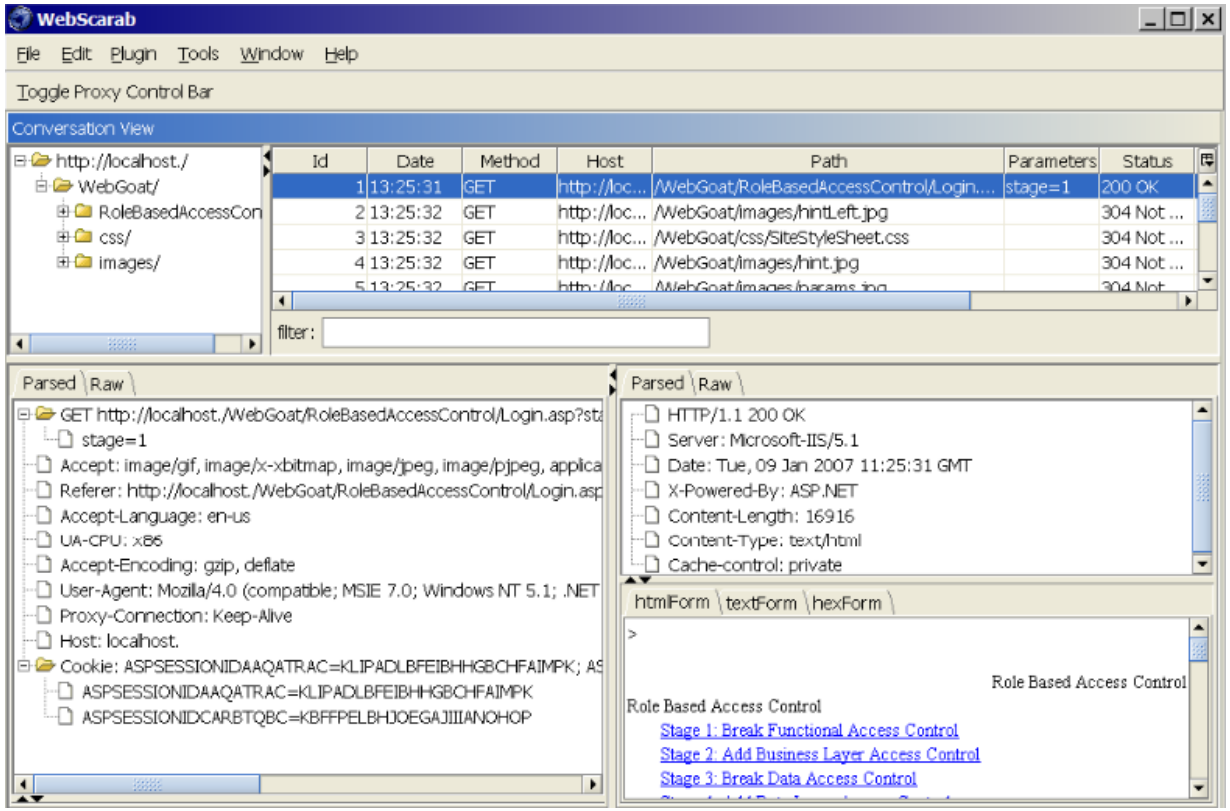

Khái niêm kiểm thử xâm nhập
Các hình thức kiểm thử xâm nhập
Kỹ thuật kiểm thử xâm nhập
Các giai đoạn kiểm thử xâm nhập
Lộ trình kiểm thử xâm nhập
Dịch vụ kiểm thử xâm nhập
Công cụ kiểm thử

Đánh giá các công cụ Pentest

- Các tiêu chí đánh giá:
  - Chi phí
  - Nền tảng
  - Dễ sử dụng
  - Khả năng tương thích
  - Khả năng báo cáo

Công cụ đánh giá bảo mật ứng dụng: WebScarab

- WebScarab là một framework cho việc phân tích các ứng dụng giao tiếp bằng cách sử dụng các giao thức HTTP và HTTPS



Công cụ đánh giá ứng dụng bảo mật

Acunetix
https://www.acunetix.com

Invicti (Netsparker)
https://www.invicti.com/

N-Stalker
http://www.nstalker.com

Skipfish
https://code.google.com

Wapiti
https://wapiti-scanner.github.io/

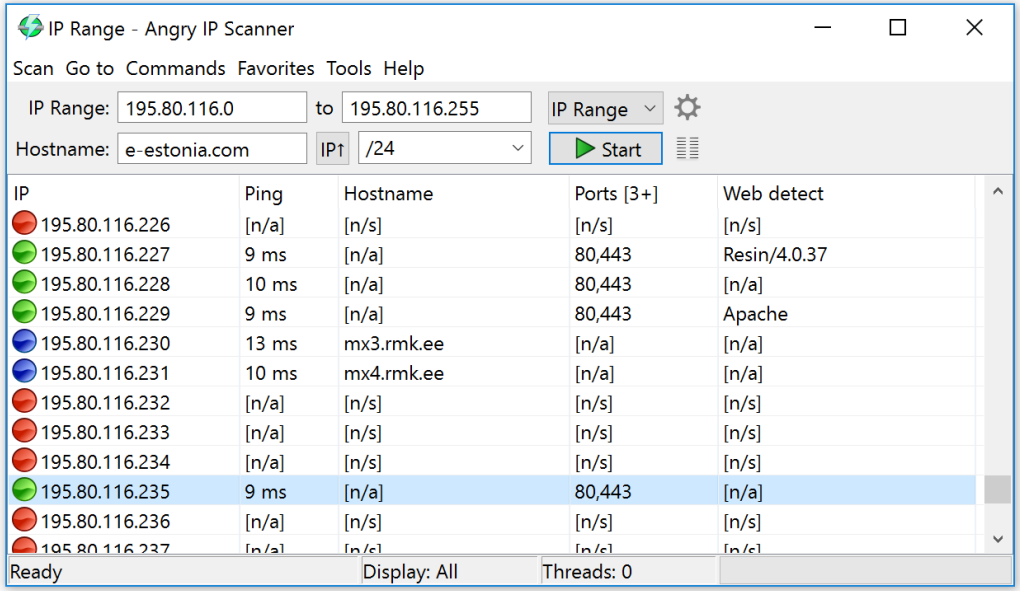
Openscap
https://www.open-scap.org/

Websecurify
https://websecurify.com/

Intruder
https://www.intruder.io/

Công cụ đánh giá an ninh mạng (1)

- **Angry IP scanner:**
  - Quét địa chỉ IP cũng như cổng trong phạm vi bất kỳ.
  - Các tính năng:
    - Thông tin NetBIOS
    - Phạm vi địa chỉ ip yêu thích
    - Phát hiện máy chủ Web
    - Tùy chỉnh mở



Công cụ đánh giá an ninh mạng (1)

- **GFI LANguard:**
  - là một an ninh mạng máy quét và giải pháp quản lý bản vá
  - GFI LANguard hỗ trợ trong các lĩnh vực :
    - Quản lý bản vá
    - Quản lý lỗ hổng
    - Mạng và phần mềm kiểm toán
    - Quản lý thay đổi
    - Phân tích rủi ro và tuân theo

Cộng cụ đánh giá truy cập không dây từ xa

- Kismet:
  - Đây là công cụ sniffer, wardriving cho chuẩn 802.11 lớp 2 mạng không dây: Wi-Fi, Bluetooth, Zigbee, RF…
  - là một framework cho việc chụp gói tin và phân tích 802.11 chạy trên Linux và MacOS
  - Xác định mạng lưới bằng cách thụ động thu thập các gói tin
  - Phát hiện mạng lưới ẩn và sự hiện diện của mạng nonbeaconing thông qua dữ liệu lưu lượng

Cộng cụ đánh giá truy cập không dây từ xa

Aircrack-ng
http://www.aircrack-ng.org

AirSnort
http://airsnort.shmoo.com/

KisMAC
https://kismac-ng.org/

Wireshark
https://www.wireshark.org/

Công cụ đánh giá an ninh hệ thống điện thoại (1)

- Omnipeek: là một mạng lưới cung cấp phân tích thời gian thực VoIP theo dõi và phân tích kết hợp với Ethernet, mạng không dây, LAN, WAN…

Công cụ đánh giá an ninh hệ thống điện thoại (2)

HackingVoIP
http://www.hackingvoip.com

VoIPShield
https://www.voipshield.com/

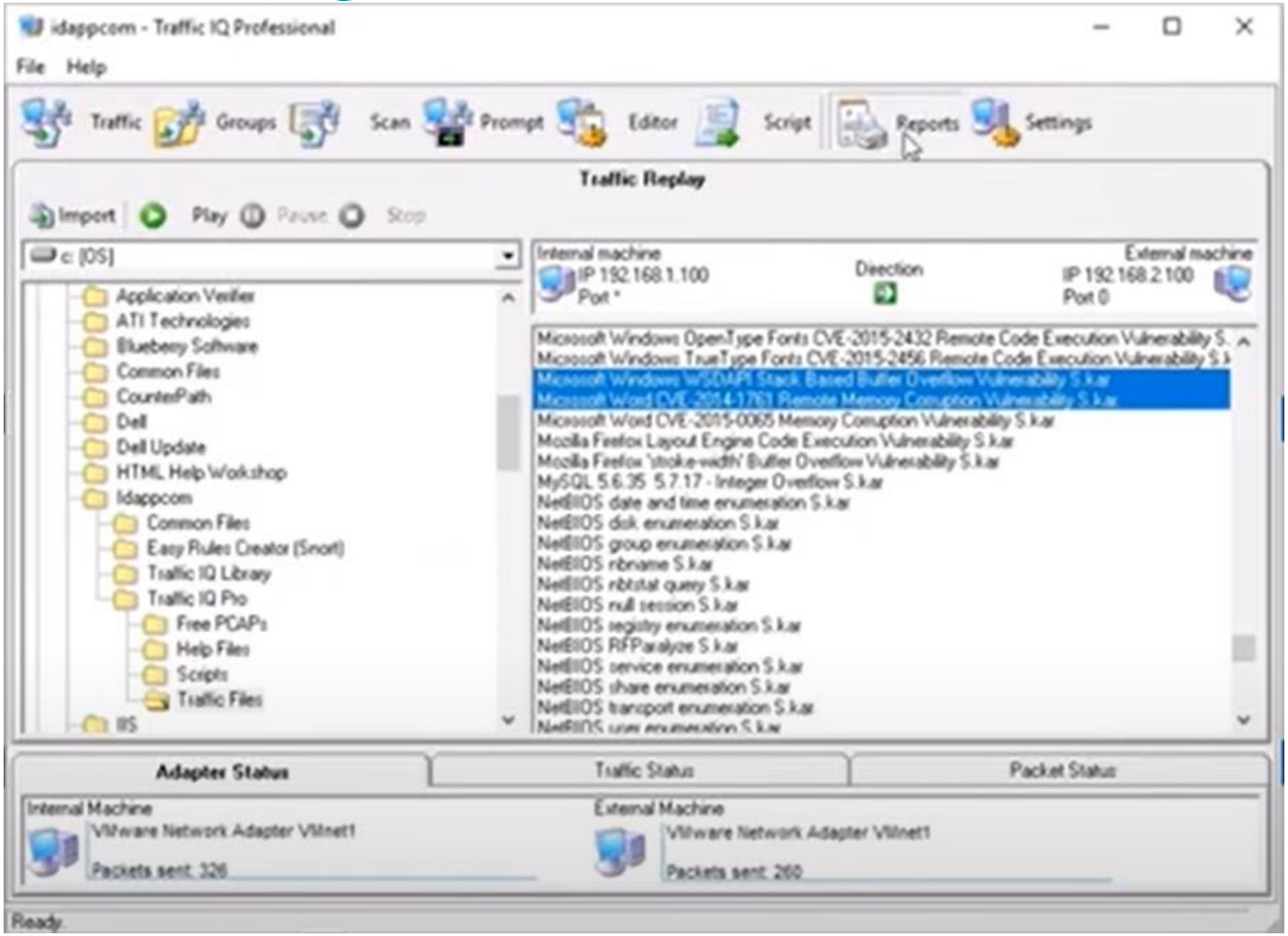
VoIPSA
https://www.voipsa.org

nsauditor
http://www.nsauditor.com/

Công cụ kiểm tra mạng – lọc thiết bị

- **Traffic IQ Pro:**
  - Công cụ này cho phép các chuyên gia bảo mật để kiểm toán và xác nhận hành vi của các thiết bị bảo mật bằng cách tạo ra lưu lượng truy cập ứng dụng tiêu chuẩn hoặc lưu lượng truy cập tấn công giữa hai máy ảo
  - Công cụ này có thể được sử dụng để đánh giá , kiểm toán , và kiểm tra các hành vi đặc điểm của bất kỳ thiết bị lọc gói tin không phải là proxy, bao gồm:
    - Tường lửa lớp ứng dụng
    - Hệ thống phát hiện xâm nhập
    - Hệ thống chống xâm nhập
    - Định tuyến và chuyển mạch

Traffic IQ Pro



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

KIỂM THỬ XÂM NHẬP

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

KIỂM THỬ XÂM NHẬP

Các môi trường phổ biến cho thực hành kiểm thử xâm nhập

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY

Biên soạn từ bài giảng: Nguyễn Ngọc Điệp, Bài giảng Kiểm thử xâm nhập, Học viện Công nghệ Bưu chính Viễn thông, 2021.

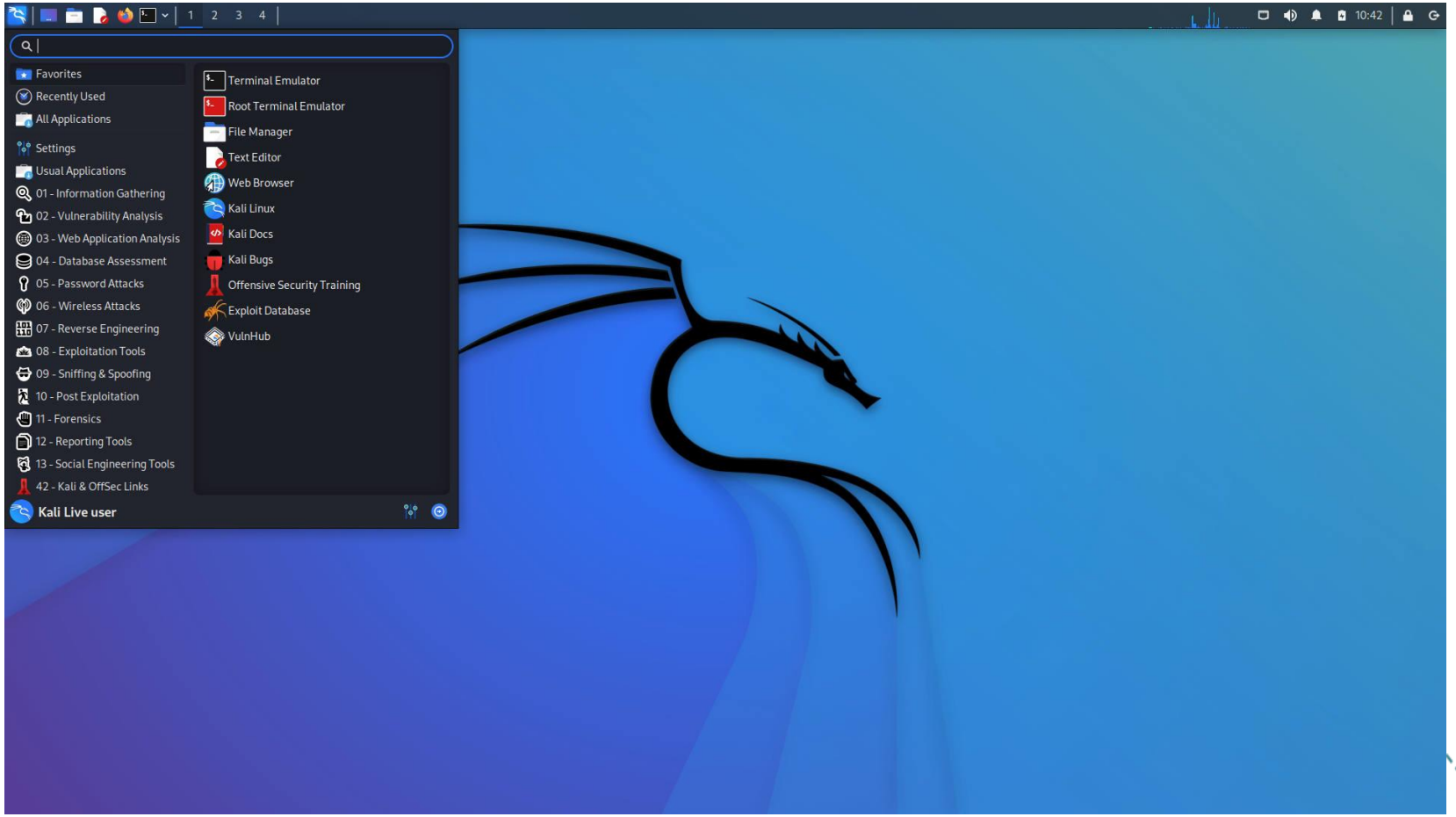
Nội dung

1. Kali Linux
2. Metasploit
3. Các công cụ khác

Kali Linux (1)

- **Kali Linux** (tên cũ: **BackTrack Linux)** là một bản phân phối của Linux dựa trên Debian mã nguồn mở hoàn toàn miễn, được phát triển với mục đích kiểm tra xâm nhập (**Penetration Testing)** và kiểm tra bảo mật nâng cao. Phiên bản đầu tiên được giới thiệu vào tháng 3/2013
- Công cụ Kali Linux chứa hàng trăm công cụ khác nhau hướng mục tiêu đến nhiệm vụ lớn là bảo mật thông tin hay những mục tiêu cụ thể hơn trong bảo mật như:
  - Nghiên cứu bảo mật
  - Kiểm tra thâm nhập
  - Kỹ thuật đảo ngược – Reverse Engineering
  - Pháp y máy tính – Computer Forensics
- Kali Linux là một giải pháp đa nền tảng, hỗ trợ truy cập và cung cấp cho những chuyên gia bảo mật thông tin cũng những người yêu thích máy tính bộ công cụ chuyên nghiệp hoàn toàn miễn phí.

Kali Linux (2)


1 2 3 4
10:42
Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
42 - Kali & OffSec Links
Terminal Emulator
Root Terminal Emulator
File Manager
Text Editor
Web Browser
Kali Linux
Kali Docs
Kali Bugs
Offensive Security Training
Exploit Database
VulnHub
Kali Live user

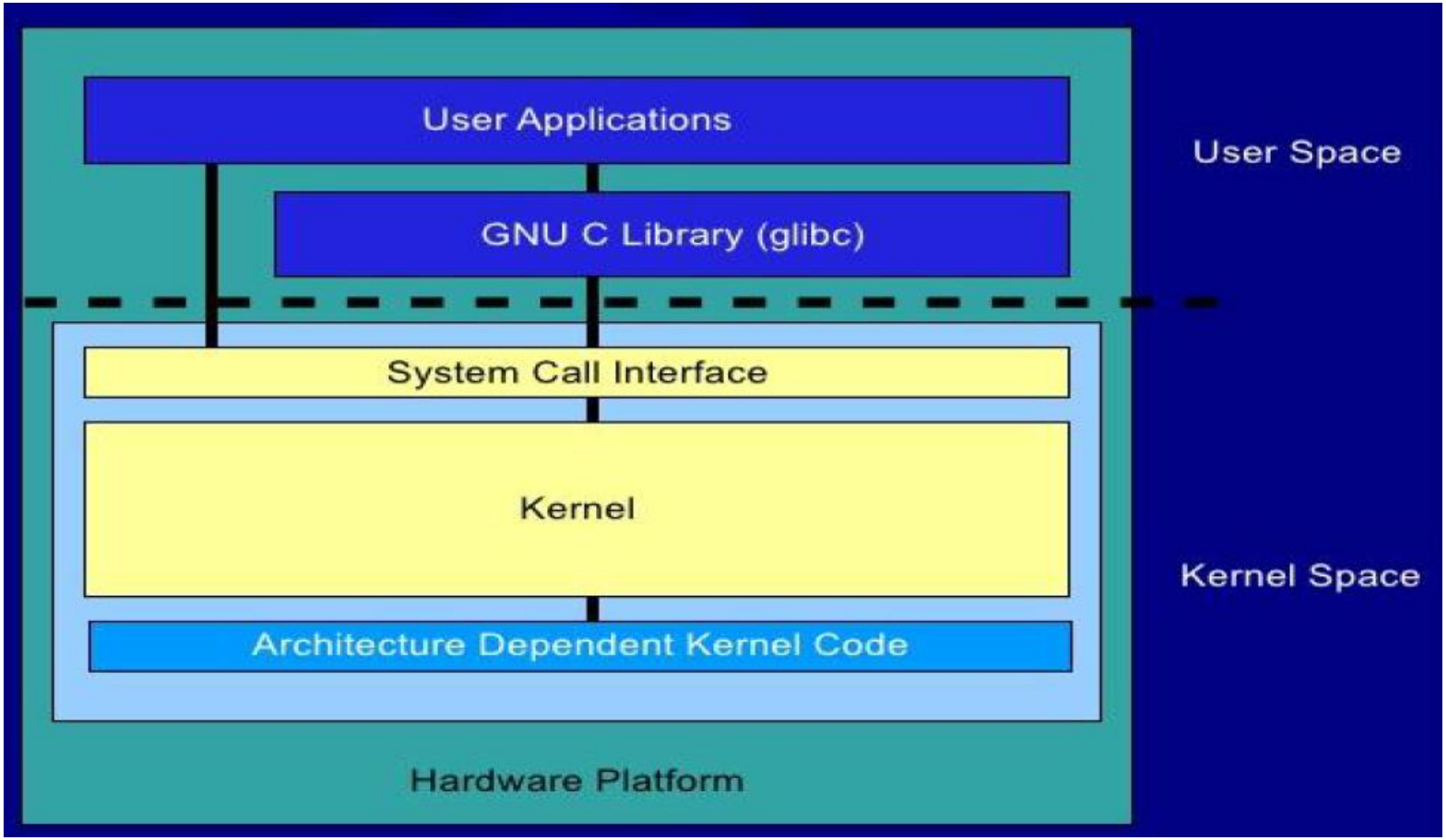
Ưu điểm và nhược điểm của Kali Linux

- **Ưu điểm của Kali Linux**
  - Có hơn 600 công cụ kiểm tra thâm nhập được cài đặt sẵn
  - Mã nguồn mở, khả năng tùy chỉnh cao, hoàn toàn miễn phí sử dụng
  - Hỗ trợ nhiều ngôn ngữ
  - Hỗ trợ nhiều thiết bị không dây (bộ vi xử lý ARM).
  - Môi trường phát triển an toàn.
  - Cây Git mã nguồn mở.
  - Tuân thủ Tiêu chuẩn Phân cấp Hệ thống Tập tin (FHS).
  - Gnu Privacy Guard (GPG) bảo mật các gói và kho lưu trữ đã ký.
- **Nhược điểm của Kali Linux**
  - Kali Linux dễ bị sử dụng sai mục đích
  - Định hướng của Kali Linux là dành cho các chuyên gia, không phải những người làm quen với Linux.
  - Không có sẵn các cấu hình bảo mật và các cấu hình khác cho người dùng bình thường
  - Một số phần mềm bên trong có thể hoạt động sai cách, bị chậm

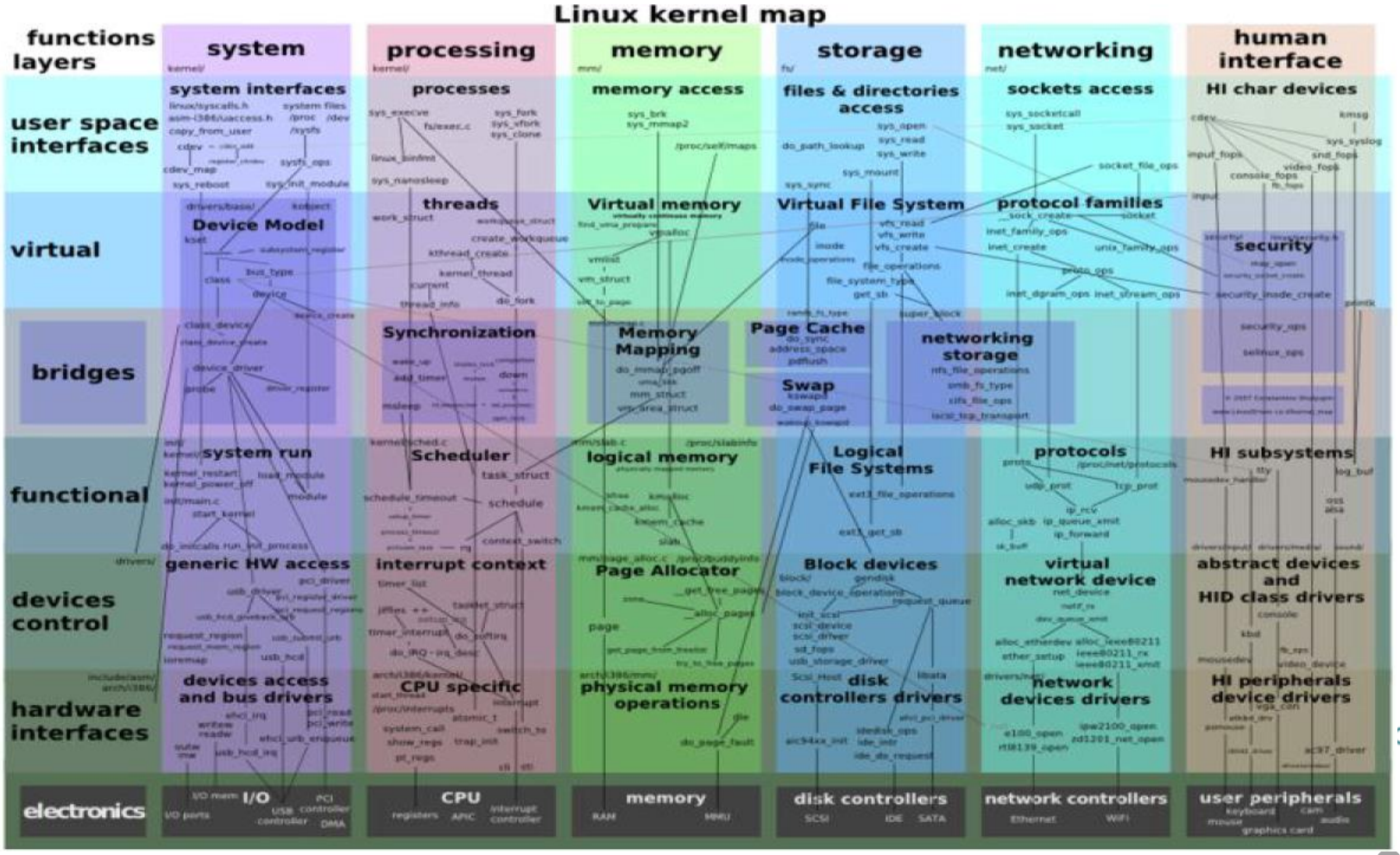
Yêu cầu phần cứng Kali linux

- Ổ cứng trống tối thiểu 20 GB để cài đặt tùy theo phiên bản, Phiên bản 2020.2 yêu cầu ít nhất 20 GB.
- RAM tối thiểu 2GB cho kiến trúc i386 và AMD64.
- có khả năng khởi động bằng ổ đĩa CD-DVD hoặc thẻ nhớ USB.
- Để có hiệu suất tốt nhất cần có tối thiểu là bộ xử lý Intel Core i3 hoặc AMD E1
- Thông số kỹ thuật phần cứng được đề xuất để có trải nghiệm mượt mà là:
  - Dung lượng ổ cứng 50 GB, ưu tiên SSD
  - Ít nhất 2GB RAM

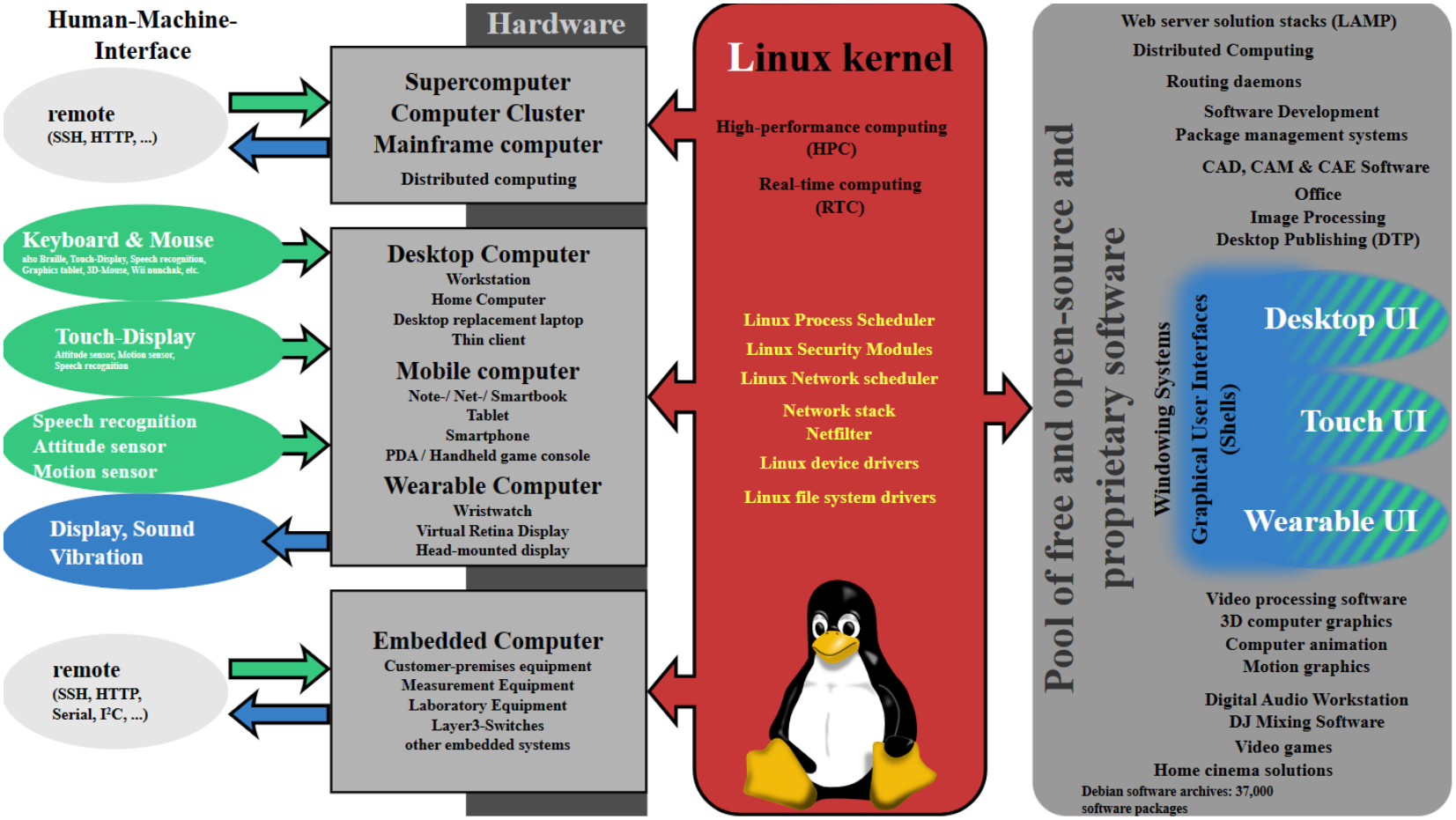
Kiến trúc cơ bản Linux



Nhân của Linux



Linux ubiquity



Các công cụ hỗ trợ trên Kali Linux (1)

Aircrack-ng
Autopsy
Armitage
Burp suite
BeEF
Cisco Global Exploiter
Ettercap
Hashcat
John the Ripper
Kismet
Lynis
Maltego
Metasploit framework
Nmap
Nikto
OWASP ZAP
Social engineering tools
Sqlmap
Wireshark
WPScan
Nessus
Zenmap
Hydra
Reverse engineering toolkit
Foremost
Volatility
VulnHub

Các công cụ hỗ trợ trên Kali Linux (2)

- Information Gathering (Thu thập thông tin)
- Vulnerability Analysis (phân tích lỗ hổng)
- Web Applications (Ứng dụng Web)
- Password Attacks (Tấn công mật khẩu)
- Wireless Attacks (Tấn công mạng không dây)
- Sniffing/Spoofing (Nghe lén/Giả mạo)
- Maintaining Access (Duy trì truy nhập).
- Reverse Engineering (Dịch ngược)

Các công cụ hỗ trợ trên Kali Linux (3)

- Stress Testing (Kiểm tra hiệu năng)
- Hardware Hacking (Tấn công các thiết bị phần cứng)
- Forensic (Điều tra số)
- Reporting Tools (Các công cụ báo cáo)
- System Services (Các dịch vụ hệ thống)

Metasploit: khái niệm cơ bản

- Xâm nhập hệ thống: Hành động tấn công trái phép vào một hệ thống máy tính từ xa thành công để giành được một số hình thức truy cập kiểm soát.
- Các phương pháp dùng để xâm nhập hệ thống:
  - Tấn công xác thực (Authentication Attacks)
  - Tấn công sử dụng kỹ thuật xã hội (Social Engineering Attacks)
  - Tấn công SQL Injection
  - Tấn công khai thác phần mềm (Software Exploitation Attacks)

Payload (1)

- Payload (tải trọng) thường được viết bằng Hợp ngữ (Assembly)
- Payload đối với an ninh máy tính là một phần của mã độc
- Phụ thuộc vào nền tảng và hệ điều hành
  - Ví dụ payload Win32 sẽ không hoạt động trong Linux (ngay cả khi bị khai thác cùng một lỗi).
- Các loại payload khác nhau tồn tại và chúng thực hiện các nhiệm vụ khác nhau
  - exec → Thực thi lệnh hoặc chương trình trên hệ thống từ xa
  - download_exec → Tải xuống tệp từ một URL và thực thi
  - upload_exec → Tải tệp cục bộ lên và thực thi
  - adduser → Thêm người dùng vào tài khoản hệ thống

Payload (2)

- Tuy nhiên, loại payload phổ biến nhất được sử dụng để khai thác lỗ hổng là mã shell (shellcode) hoặc còn gọi là shell payloads.
  - Các payload này rất hữu ích vì chúng cung cấp cho kẻ tấn công một shell tương tác có thể được sử dụng để kiểm soát hoàn toàn hệ thống từ xa
  - Thuật ngữ này được kế thừa từ Unix → /bin/sh
  - Đối với Windows, shell đề cập đến comment prompt → cmd.exe
- Có hai loại payload shell khác nhau;
  - Bind Shells → Tạo một socket, một cổng (port) được liên kết với nó và khi một kết nối được thiết lập với nó, nó sẽ sinh ra một shell.
  - Reverse Shells → Thay vì tạo một socket để lắng nghe, một kết nối được tạo và liên kết tới một IP và Cổng được xác định trước và một shell sau đó được chuyển tới Kẻ tấn công.

Metasploit Framework (1)

- Metasploit Framework (MSF) là một nền tảng để viết, thử nghiệm và sử dụng mã khai thác. Người dùng chính của Framework này là các chuyên gia thực hiện kiểm tra xâm nhập, phát triển shellcode và nghiên cứu lỗ hổng.

Metasploit Framework (2)

- MSF không chỉ là môi trường để phát triển khai thác mà còn là nền tảng để khởi chạy khai thác trên các ứng dụng trong thế giới thực. Nó có thể được đóng gói trong đó có triển khải khai thác các lỗ hổng thực sự và có thể gây ra thiệt hại thực sự nếu không được sử dụng một cách chuyên nghiệp.
- Thực tế là MSF là một công cụ nguồn mở và cung cấp một phương pháp đơn giản hóa như vậy để khởi động các cuộc tấn công nguy hiểm, nó đã và vẫn đang thu hút các hacker và script kiddies sử dụng để tạo thêm sự cố trên mạng và hệ thống.

Metasploit Framework (3)

- là một framework để cung cấp môi trường kiểm thử các hệ thống phần mềm và mạng.
- lưu trữ một cơ sở dữ liệu cho các lỗ hổng đã công bố, và cung cấp sẵn các công cụ để khai thác các lỗ hổng đó
- sử dụng công cụ này để tạo ra các payload kiểm thử các hệ thống
- xây dựng từ ngôn ngữ hướng đối tượng Perl, với những thành phần được viết bằng C, assembly, và Python
- có thể cài đặt trên Windows, Linux, Mac OS, nhưng phổ biến nhất vẫn là Linux. Kali Linux có cài đặt sẵn Metasploit
- hỗ trợ nhiều giao diện với người dùng. Msfconsole – giao diện dòng lệnh, giao diện đồ họa Armitage và giao diện Web.

Metasploit Framework (4)

- Có hai loại môi trường làm việc:
  - *Môi trường toàn cục* chứa các biến mang tính toàn cục, có tất cả các mô-đun khai thác
  - *Môi trường tạm thời* chỉ đưa các biến vào mô-đun khai thác đang nạp hiện tại, không ảnh hưởng đến các mô-đun khác

Metasploit Framework (5)

- Để sử dụng metasploit thường phải thực hiện các bước như sau:

1. chọn mô-đun khai thác (exploit), nghĩa là lựa chọn chương trình, dịch vụ có chứa lỗi mà Metasploit hỗ trợ để khai thác
2. cần kiểm tra những tùy chọn với lệnh “check” để xem đã được thiết lập chính xác chưa, rồi chọn mục tiêu (hệ điều hành) cần thực hiện
3. Sau khi chọn mục tiêu, cần chọn payload hay đoạn mã chạy trên hệ thống của nạn nhân
4. Cuối cùng là thực thi khai thác với lệnh *exploit*. Payload sau đó sẽ cung cấp thông tin về hệ thống đã được khai thác

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

KIỂM THỬ XÂM NHẬP

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

KIỂM THỬ XÂM NHẬP

Một số dạng kiểm thử xâm nhập

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY

Biên soạn từ bài giảng: Nguyễn Ngọc Điệp, Bài giảng Kiểm thử xâm nhập, Học viện Công nghệ Bưu chính Viễn thông, 2021.

Các nội dung tìm hiểu

- Social Engineering là gì?
- Tại sao Social Engineering lại hiệu quả
- Các giai đoạn trong một cuộc tấn công Social Engineering
- Các mục tiêu phổ biến của Social Engineering
- Các kiểu Social Engineering
- Các chiến thuật xâm nhập phổ biến và chiến lược phòng chống
- Social Engineering với tấn công mạo danh trên mạng xã hội
- Ảnh hưởng của mạng xã hội tới mạng doanh nghiệp
- Ăn cắp ID là gì?
- Thế nào là ăn cắp tính danh?
- Biện pháp đối phó Social Enginneering
- Thử nghiệm Social Engineering

Mục lục

1. **Khái niệm Social Engineering**
2. Kỹ thuật Social Engineering
3. Mạo danh trên mạng xã hội
4. Ăn cắp danh tính
5. Biện pháp đối phó với Social Engineering
6. Thử nghiệm xâm nhập

Không có bất kỳ bản vá lỗi nào đối với một con người ngu ngốc

Social Engineering là gì

- Tấn công vào yếu tố con người - Social Engineering là một nghệ thuật thuyết phục mọi người tiết lộ thông tin bí mật
- Social Engineering phụ thuộc vào những thứ mà mọi người không biết những thông tin về chúng và bất cẩn trong việc bảo vệ nó

Các hành vi dễ bị tấn công

- Sự tin tưởng là nền tảng cơ bản của tấn công Social Engineering
- Sự thiếu hiểu biết về Social Engineering và các hiệu ứng của nó trong đội ngũ nhân viên khiến cho các tổ chức là một mục tiêu dễ dàng
- Socal Engineers có thể đe doạ nghiêm trong đến việc mất mát trong trường hợp không tuân thủ những yêu cầu của tổ chức
- Social Engineers thu hút các mục tiêu tiết lộ thông tin bởi một cái gì đó đầy hứa hẹn
- Các mục tiêu sẽ được hỏi để trợ giúp và họ tuân theo những quy định mang tính nghĩa vụ được đưa ra

Những yếu tố làm doanh nghiệp dễ bị tấn công

Việc đào tạo hiểu biết về an toàn thông tin cho nhân viên còn thiếu

Thiếu những chính sách an ninh

Nhiều các đơn vị tổ chức

Dễ dàng truy cập thông tin

Tại sao Social Engineering lại hiệu quả

- Không có một phần mềm hay phần cứng nào có thể chống lại một cuộc tấn công Social Engineering
- Không có một phương pháp chắc chắn nào để đảm bảo an ninh một cách đầy đủ từ các cuộc tấn công Social Engineering
- Chính sách bảo mật mạnh cũng sẽ là liên kết yếu nhất và con người là yếu tố nhạy cảm nhất
- Rất khó để phát hiện ra Social Engineering

Những dấu hiệu của một cuộc tấn công

- Tấn công trên mạng Internet đã trở thành một ngành kinh doanh và Kẻ tấn công liên tục cố gắng để xâm nhập mạng và có các dấu hiệu sau:
  - Không cung cấp số gọi lại
  - Yêu cầu phi chính thức
  - Yêu cầu thẩm quyền và đe doạ nếu như không cung cấp thông tin
  - cho thấy sự vội vàng và vô tình để lại tên
  - Bất ngờ được khen tặng hoặc ca ngợi
  - Thấy khó chịu khi đặt câu hỏi

Các giai đoạn của một cuộc tấn công Social Engineering

- **Nghiên cứu mục tiêu**: Dumpster diving, trang web, nhân sự, lịch trình…
- **Lựa chọn nạn nhân**: Xác định những nhân viên không hài lòng về chính sách trong công ty mục tiêu
- **Phát triển mối quan hệ**: Phát triển mối quan hệ với những nhân viên đã được lựa chọn
- **Khai thác mối quan hệ**: Tập hợp thông tin tài khoản nhạy cảm, thông tin tài chính, và công nghệ hiện tại

Những ảnh hưởng lên tổ chức khi bị tấn công

- Mất sự riêng tư
- Tổn hại uy tín
- Những mất mát về kinh tế
- chính sách khủng bố
- Các vụ kiện và các thủ tục
- Tạm thời hoặc vĩnh viễn đóng cửa

Các phương pháp tấn công

Online

Kết nối Internet cho phép kẻ tấn công tiếp cận nhân viên từ một nguồn internet ẩn danh và thuyết phục họ cung cấp những thông tin thông qua một User đáng tin cậy

Telephone

Yêu cầu thông tin, thông thường bằng cách giả mạo người dùng hợp pháp, mà người đó có thể truy cập tới hệ thống điện thoại hoặc có thể truy cập từ xa vào hệ thống máy tính

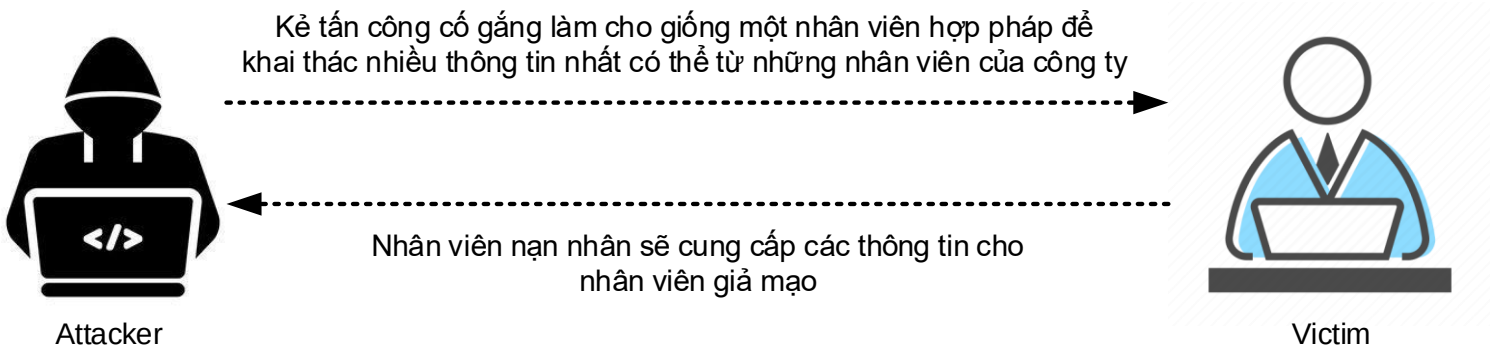
Tiếp cận trực tiếp

Trong việc tiếp cận đối tượng, kẻ tấn công sẽ lấy thông tin bằng cách trực tiếp hỏi đối tượng đó

Những mục tiêu chung của Social Engineering

- Nhân viên tiếp tân và nhân viên hỗ trợ
- Người dùng và khách hàng
- Người bán hàng của doanh nghiệp
- Người quản trị hệ thống
- Giám đốc hỗ trợ kỹ thuật

Những mục tiêu chung của Social Engineering: Nhân viên văn phòng



- Mặc dù có tường lửa tốt nhất, phát hiện xâm nhập, và hệ thống chống virut, thì bạn vẫn bị tấn công bởi những lỗ hổng bảo mật.
- kẻ tấn công có thể cố gắng tấn công Social Engineering lên những nhân viên văn phòng để thu thập những dữ liệu nhạy cảm như:
  - Những chính sách bảo mật
  - Những tài liệu nhạy cảm
  - Cấu trúc mạng văn phòng
  - Những mật khẩu

Mục lục

1. Khái niệm Social Engineering
2. **Kỹ thuật Social Engineering**
3. Mạo danh trên mạng xã hội
4. Ăn cắp danh tính
5. Biện pháp đối phó với Social Engineering
6. Thử nghiệm xâm nhập

Các kiểu Social Engineering

Human-based:

- Tập hợp những thông tin nhạy cảm bằng cách khai thác sự tin tưởng, sợ hãi và sự giúp đỡ

Computer-based:

- Social Engineering được thực hiện bởi sự giúp đỡ của máy tính

Human-based (1)

- **Mạo danh**
  - là giả mạo thành một người hay một vật nào đó. 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 ...

Human-based (2)

Giả làm một người sử dụng hợp pháp

- Nhận dạng và yêu cầu thông tin nhạy cảm “Chào ! Đây là John, từ bộ phận X, tôi đã quên password của tôi. Bạn có thể lấy lại nó dùm tôi được chứ ?”

Giả làm một khách hàng quan trọng (VIP)

- “Chào tôi là Kevin, tôi là thư kí giám đốc kinh doanh. Tôi đang làm một dự án cấp bách và bị mất mật khẩu hệ thống của mình. Bạn có thể giúp tôi được chứ?”

Giả làm nhân viên hỗ trợ kỹ thuật

- Nói như một nhân viên hỗ trợ kỹ thuật và yêu cầu ID và mật khẩu cho việc khôi phục dữ liệu “Thưa ngài, tôi là Mathew, nhân viên hỗ trợ kỹ thuật, công ty X, tối qua chúng tôi có một hệ thống bị sập ở đây do đó chúng tôi đến để kiểm tra có bị mất dữ liệu hay không. Ngài có thể cung cấp cho tôi ID và mật khẩu không?”

Human-based (3)

Ví dụ về việc hỗ trợ kỹ thuật

- "Một người đàn ông gọi đến bàn hỗ trợ của công ty và nói rằng ông ta đã quên mật khẩu của ông ta. Ông ta nói thêm rằng nếu ông ta bỏ lỡ mất dự án quảng cáo lớn trên thì sẽ bị sếp của ông ta đuổi việc. Nhân viên bàn trợ giúp cảm lấy tiếc cho anh ta và nhanh chóng resets lại mật khẩu, vậy là vô tình tạo ra một lối vào mạng bên trong của công ty".

Ví dụ về việc giả mạo cơ quan hỗ trợ (1)

- "Chào, tôi là John Brown. Tôi đang ở cùng với kiểm soát viên ngài Arthur Sanderson. Chúng tôi đã làm việc với công ty về một cuộc kiểm tra bất ngờ đối với bạn nhằm khắc phục các thảm họa xảy ra từ bạn.
- Bộ phận của bạn có 10 phút để chỉ cho tôi biết làm cách nào bạn khôi phục một website sau khi bị tai nạn

Human-based (4)

Ví dụ về việc giả mạo cơ quan hỗ trợ (2)

- "Chào, dịch vụ chuyển phát nhanh Aircon phải không? Chúng tôi nhận được cuộc gọi rằng phòng máy tính bị quá nóng và cần được kiểm tra hệ thống HVAC của bạn"
- Sử dụng hệ thống mang tên HVAC (hệ thống sưởi, thông gió và điều hòa nhiệt độ) có thể thêm độ tin cậy đủ để giả mạo một kẻ xâm nhập cho phép anh ta hoặc cô ta để đạt được quyền truy cập vào tài nguyên mục tiêu.

Human-based (5)

Eavesdropping

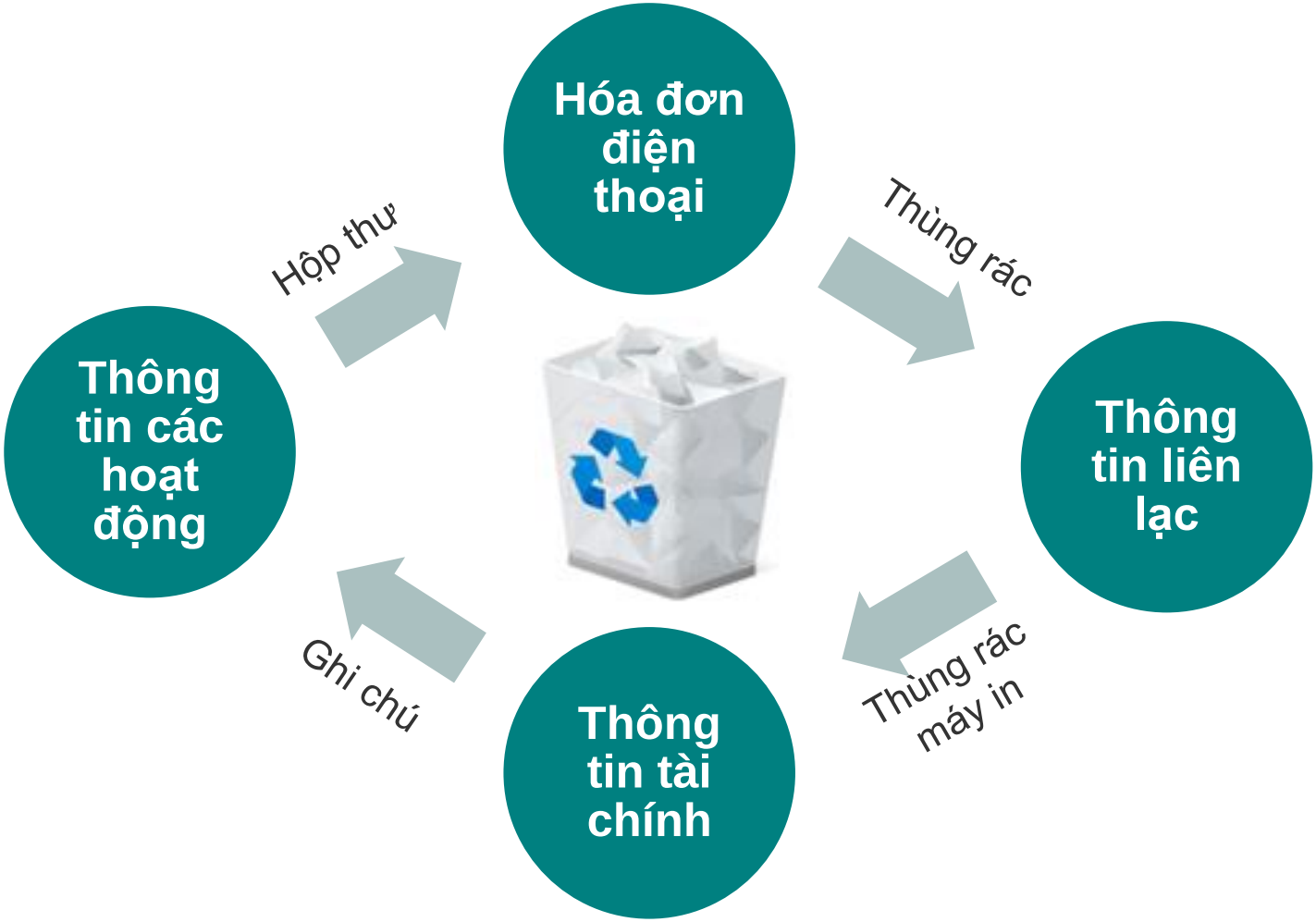
- Nghe lén hoặc nghe trái phép các cuộc hội thoại hoặc đọc tin nhắn
- Chặn lại bất kỳ các hình thức như âm thanh, video hoặc văn bản.
- Eavesdropping cũng sử dụng với những kênh truyền thông khác như đường dây điện thoại, email, tin nhắn tức thời …

Shoulder Surfing

- Shoulder Surfing là một quy trình mà kẻ tấn công sử dụng để tìm ra mật khẩu, số chứng minh nhân dân, số tài khoản ...
- Kẻ tấn công đứng đằng sau nhìn qua vai của nạn nhân hoặc thậm chí quan sát từ một khoảng cách xa bằng cách sử dụng ống nhòm, để có được thông tin.

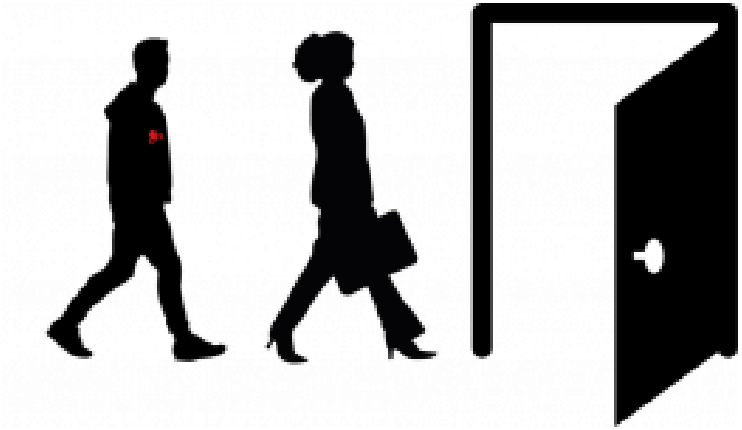
Human-based (6)

Dumpster Diving: là tìm kiếm kho báu của người khác trong thùng rác

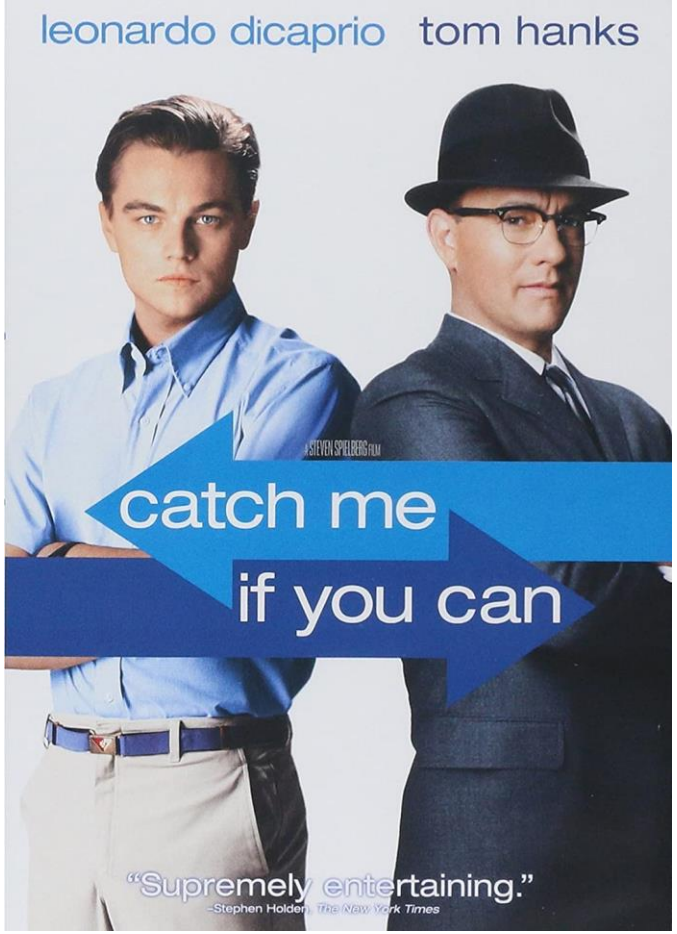


Human-based (7)

- **Piggybacking** và **Tailgating** là hai kĩ thuật khá 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. VD: Tôi quên thẻ ID ở nhà. Vui lòng hãy cho tôi đi cùng. Một người có thẩm quyền cho phép truy cập cho một người trái phép bằng cách cho cách cửa luôn được mở
  - **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. VD: sử dụng ID giả và theo sát người dùng khi đi qua điểm kiểm tra



Human-based (8)



Human-based (9)

Human-based (9)

- Mạo danh
- Eavesdropping
- Shoulder Surfing
- Dumpster Diving
- Piggybacking
- Tailgating

Computer-based

Những lá thư Hoax là những email cảnh báo các vấn đề cho người dùng về virut, Troijan, sâu có thể làm tổn hại đến hệ thống máy tính người sử dụng

Thu thập thông tin cá nhân bằng cách nói chuyện với người dùng trực tuyến đã được lựa chọn để lấy thông tin như họ tên, ngày sinh, số ID…

Pop-up Windows → Hoax Letters → Chain Letters → Instant Chat Messenger → Spam Email

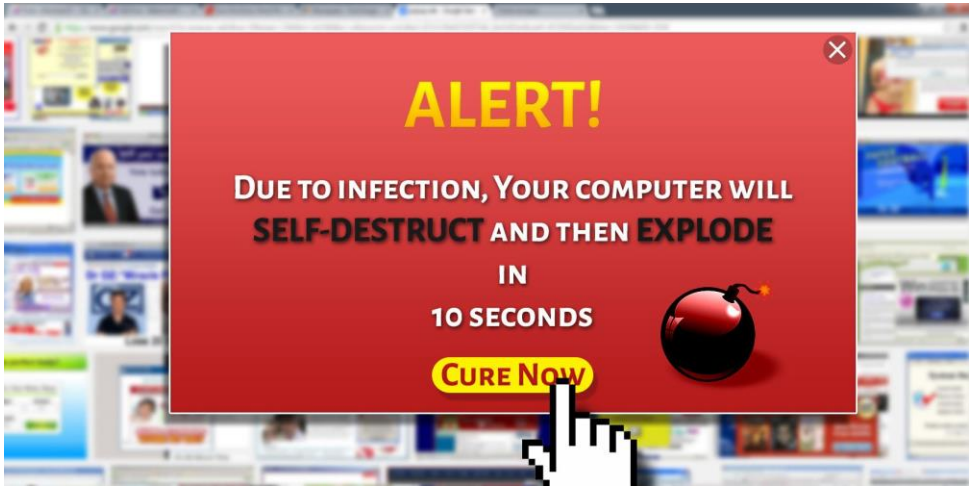
Một cửa sổ window tự động bật lên khi lướt web và yêu cầu thông tin của người dùng để đăng nhập hoặc đăng ký

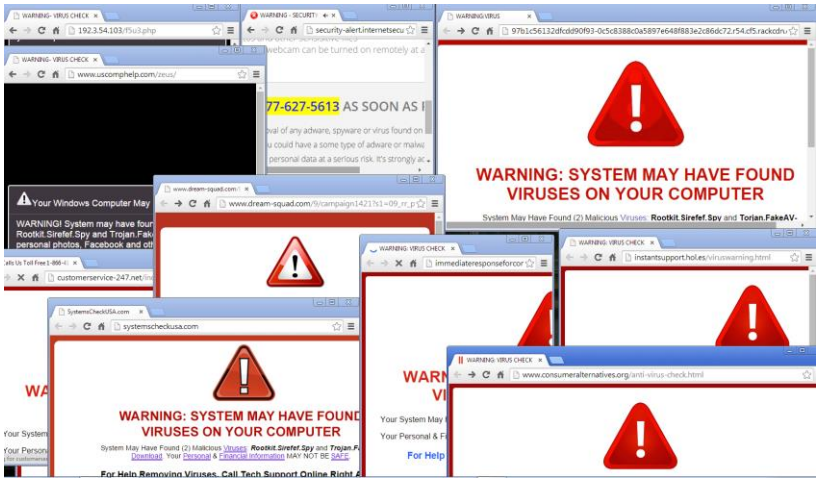
Chain Letters là những lá thư cung cấp quà tặng miễn phí như tiền hay phần mềm kèm theo điều kiện là người dùng phải chuyển tiếp thư này đến một số người khác.

Không liên quan, không mong muốn và những email không được yêu cầu này dùng để thu thập thông tin tài chính, các số an ninh, và thông tin mạng.

Computer-based: Pop-Ups

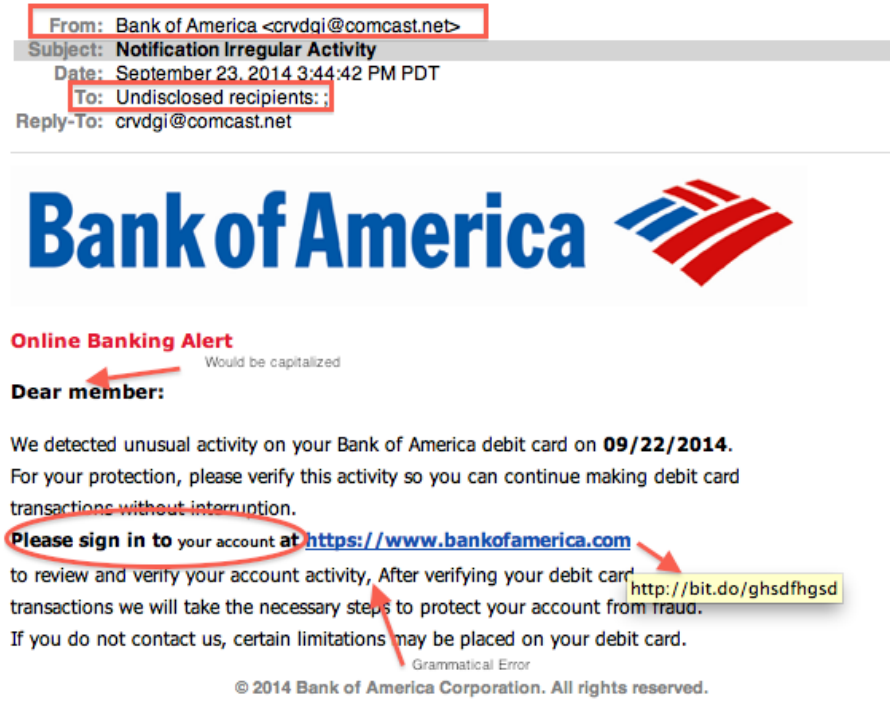
- Cửa sổ pop-ups lừa đảo bật lên khi click chuột vào một liên kết sẽ chuyển hướng chúng đến các trang web giả mạo yêu cầu thông tin cá nhân hoặc tải chương trình độc hại như Keyloggers, Troijan, hoặc phần mềm gián điệp





Computer-based: Phishing

- Một email giả bất hợp pháp tự nhận là đến từ một web hợp pháp và cố gắng để có được thông tin cá nhân hoặc tài khoản người dùng.
- Các email Phishing hoặc các Pop-Up chuyển hướng người dùng tới những trang web giả mạo bắt trước trang web đáng tin cậy và yêu cầu họ gửi thông tin các nhân của họ


From: Bank of America <crvdgi@comcast.net>
Subject: **Notification Irregular Activity**
Date: September 23, 2014 3:44:42 PM PDT
To: Undisclosed recipients: ;
Reply-To: crvdgi@comcast.net

Bank of America

Online Banking Alert

Would be capitalized

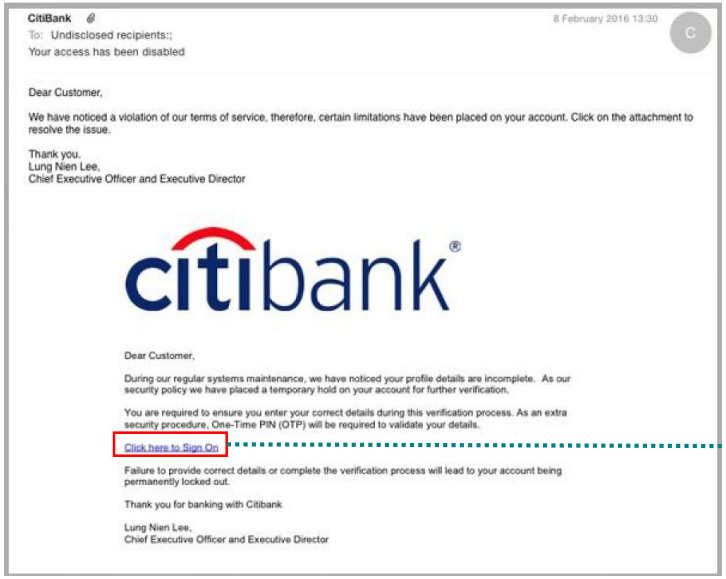
Dear member:

We detected unusual activity on your Bank of America debit card on **09/22/2014**.
For your protection, please verify this activity so you can continue making debit card transactions without interruption.
Please sign in to your account **at** https://www.bankofamerica.com
to review and verify your account activity, After verifying your debit card
http://bit.do/ghsdfhgsd
transactions we will take the necessary steps to protect your account from fraud.
If you do not contact us, certain limitations may be placed on your debit card.

Grammatical Error

© 2014 Bank of America Corporation. All rights reserved.

Computer-based: Phishing



CitiBank
8 February 2016 13:30
To: Undisclosed recipients;;
Your access has been disabled

Dear Customer,

We have noticed a violation of our terms of service, therefore, certain limitations have been placed on your account. Click on the attachment to resolve the issue.

Thank you.
Lung Nien Lee,
Chief Executive Officer and Executive Director

citibank®

Dear Customer,

During our regular systems maintenance, we have noticed your profile details are incomplete. As our security policy we have placed a temporary hold on your account for further verification.

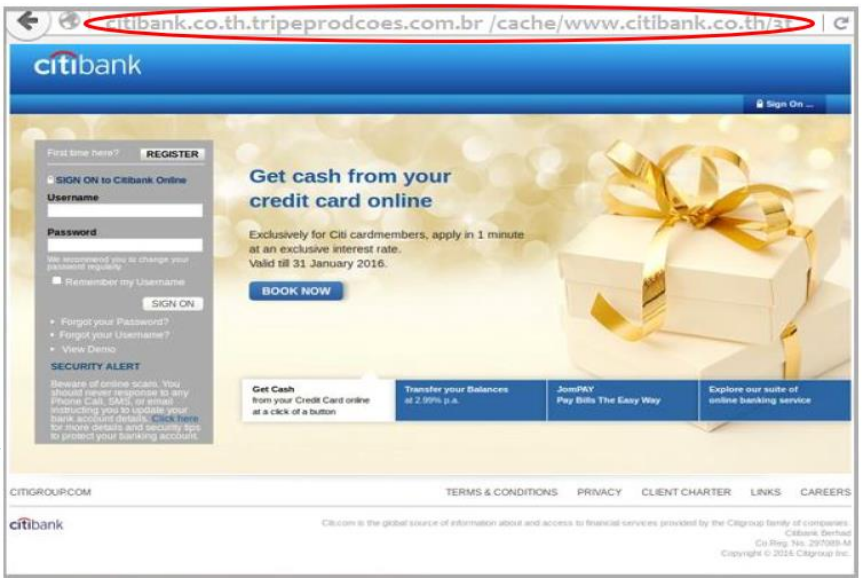
You are required to ensure you enter your correct details during this verification process. As an extra security procedure, One-Time PIN (OTP) will be required to validate your details.

Click here to Sign On

Failure to provide correct details or complete the verification process will lead to your account being permanently locked out.

Thank you for banking with Citibank

Lung Nien Lee,
Chief Executive Officer and Executive Director



Social Engineering sử dụng SMS

- Tracy nhận được một tinh nhắn SMS, mạo nhận từ bộ phận bảo mật tại ngân hàng XIM. Trong đó nói có việc khẩn cấp và Traycy nên gọi ngay một cuộc điện thoại ngay lập tức, cô lo lắng và đã gọi để kiểm tra tài khoản của mình.
- Cô đã gọi cho số đó và nghĩ đó là số điện thoại của dịch vụ khách hàng của ngân hàng XIM. Kẻ tấn công thông báo cuộc gọi đang được ghi âm đồng thời yêu cầu cô cung cấp thẻ tín dụng hoặc số thẻ ghi nợ
- Không có gì ngạc nhiên, Tracy đã tiết lộ những thông tin nhạy cảm do tin nhắn giả mạo trên gây ra

Tấn công Insider

Spying

- Nếu đối thủ cạnh tranh muốn gây ra thiệt hại cho một tổ chức, ăn cắp các bí mật quan trọng, hoặc tiêu diệt, họ chỉ cần tìm ra một công việc mà tổ chức này đang cần và cho người của mình tham gia, vượt qua vòng phỏng vấn, và họ đã có người của họ trong tổ chức đó.

Revenge

- việc trả thù chỉ cần có người bất mãn để trả thù và công ty đó sẽ bị tổn hại.
  - 60 % các cuộc tấn công xảy ra phía sau tường lửa
  - Một cuộc tấn công bên trong sẽ dễ dàng khởi động
  - Phòng chống là rất khó khăn
  - Những kẻ tấn công bên trong có thể dễ dàng thành công

Nhân viên bất mãn

- Hầu hết các trường hợp lạm dụng nội bộ có thể được khởi nguồn từ một cá nhân sống nội tâm, không có khả năng đối phó với căng thẳng hay xung đột, và cảm thấy thất vọng với công việc của mình, chính trị trong văn phòng và sự thiếu tôn trọng …
- Những nhân viên bất mãn có thể cung cấp những bí mật công ty và sở hữu trí tuệ có ích cho đối thủ cạnh tranh

Ngăn chặn mối đe dọa bên trong nội bộ

Các chiến thuật xâm nhập phổ biến và chiến lược phòng chống

Lĩnh vực rủi ro	Chiến thuật của kẻ tấn công	Chiến lược phòng chống
Điện thoại (bàn trợ giúp)	Mạo danh hoặc thuyết phục	Đào tạo nhân viên bàn trợ giúp không được tiết lộ mật khẩu cũng như các thông tin khác thông qua đường điện thoại
Lối ra vào	Không được phép truy cập vật lý	Quản lý thẻ an ninh chặt chẽ, đào tạo nhân viên, và nhân viên an ninh
Văn phòng	Shoulder surfing	Không nên gõ bất kỳ mật khẩu nào khi có bất kỳ người nào đang có mặt tại đó (nếu phải làm, thì nên nào việc đó rất nhanh).
Điện thoại(bàn trợ giúp)	Mạo danh các cuộc gọi trợ giúp	Gán một mã PIN cho mỗi nhân viên bàn hỗ trợ guiúp đỡ
Văn phòng	Lang thang qua các phòng tìm kiếm các phòng đang mở	Hộ tống tất cả các khách
Mail room	Chèn các bản ghi nhớ giả mạo	Khóa và theo dõi Mail Room
Phòng máy / phòng điện thoại riêng	Cố gắn truy cập, loại bỏ thiết bị, hoặc đính kèm một số giao thức để lấy dữ liệu mật	Giữ phòng điện thoại riêng, phòng server, vv. Đều được khóa và kiểm kê cập nhật thiết bị
Điện thoại và hệ thống PBX	Ăn cắp số điện thoại để truy cập	Kiểm soát các cuộc gọi ở nước ngoài và các cuộc gọi đường dài, dấu viết cuộc gọi, và từ chối chuyển cuộc gọi

Mục lục

1. Khái niệm Social Engineering
2. Kỹ thuật Social Engineering
3. **Mạo danh trên mạng xã hội**
4. Ăn cắp danh tính
5. Biện pháp đối phó với Social Engineering
6. Thử nghiệm xâm nhập

Social Engineering thông qua mạo danh trên các mạng xã hội

- Mạo danh có nghĩa là bắt chước hoặc sao chép các hành vi hoặc hành động của người khác
- Mã độc hại được sử dụng để thu thập thông tin bí mật từ các trang mạng xã hội và tạo ra các tài khoản với những tên khác nhau
- Kẻ tấn công sử dụng những hồ sơ khác nhau để tạo ra các mạng lớn những người bạn và triết xuất thông tin để sử dụng tấn công Social Engineering
- Kẻ tấn công cũng có thể sử dụng thông tin thu thập được để tiến hành các hình thức tấn công Social Engineering khác

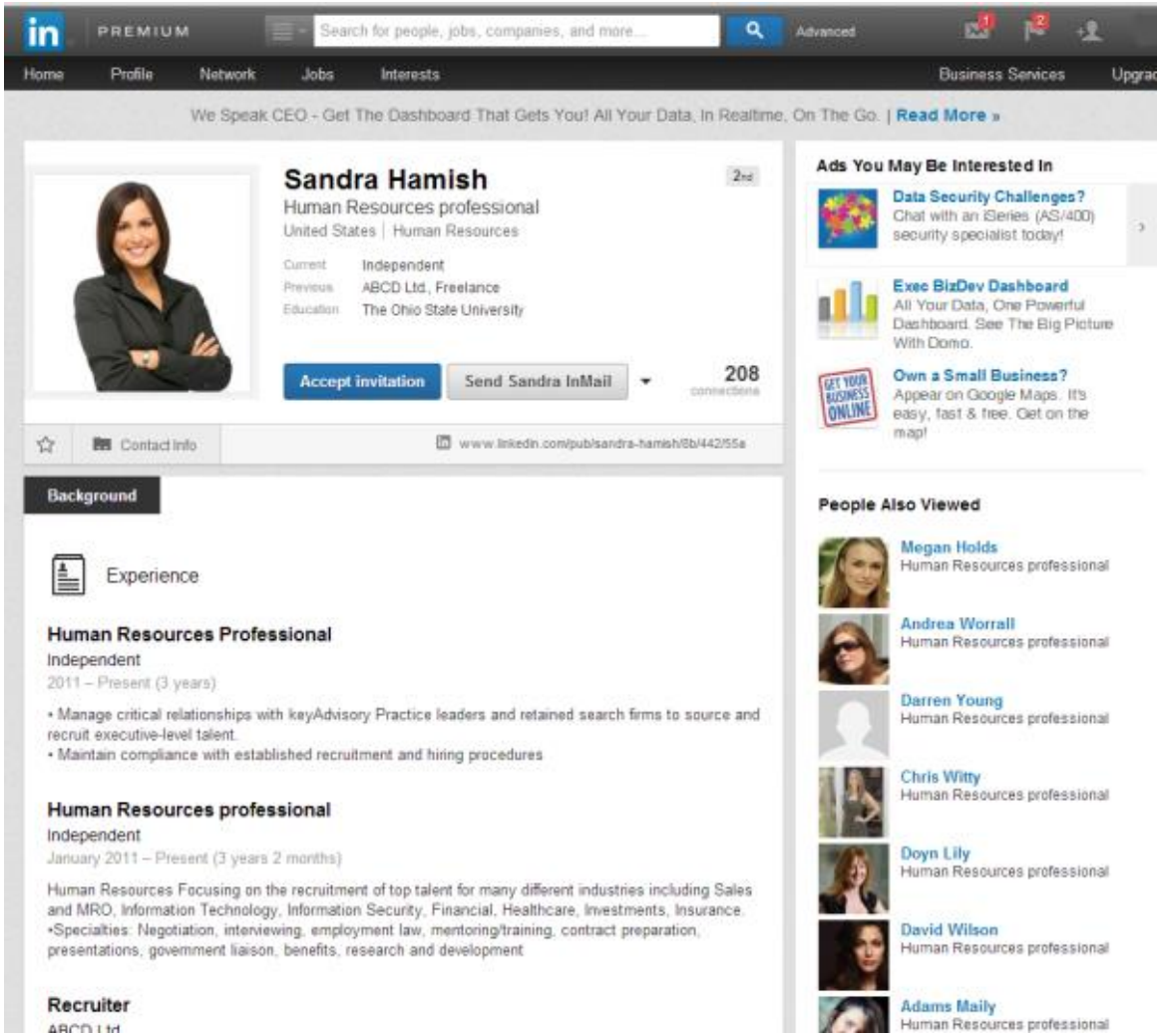
Chi tiết về tổ chức

Chi tiết nghề nghiệp

Địa chỉ liên lạc và kết nối

Chi tiết cá nhân

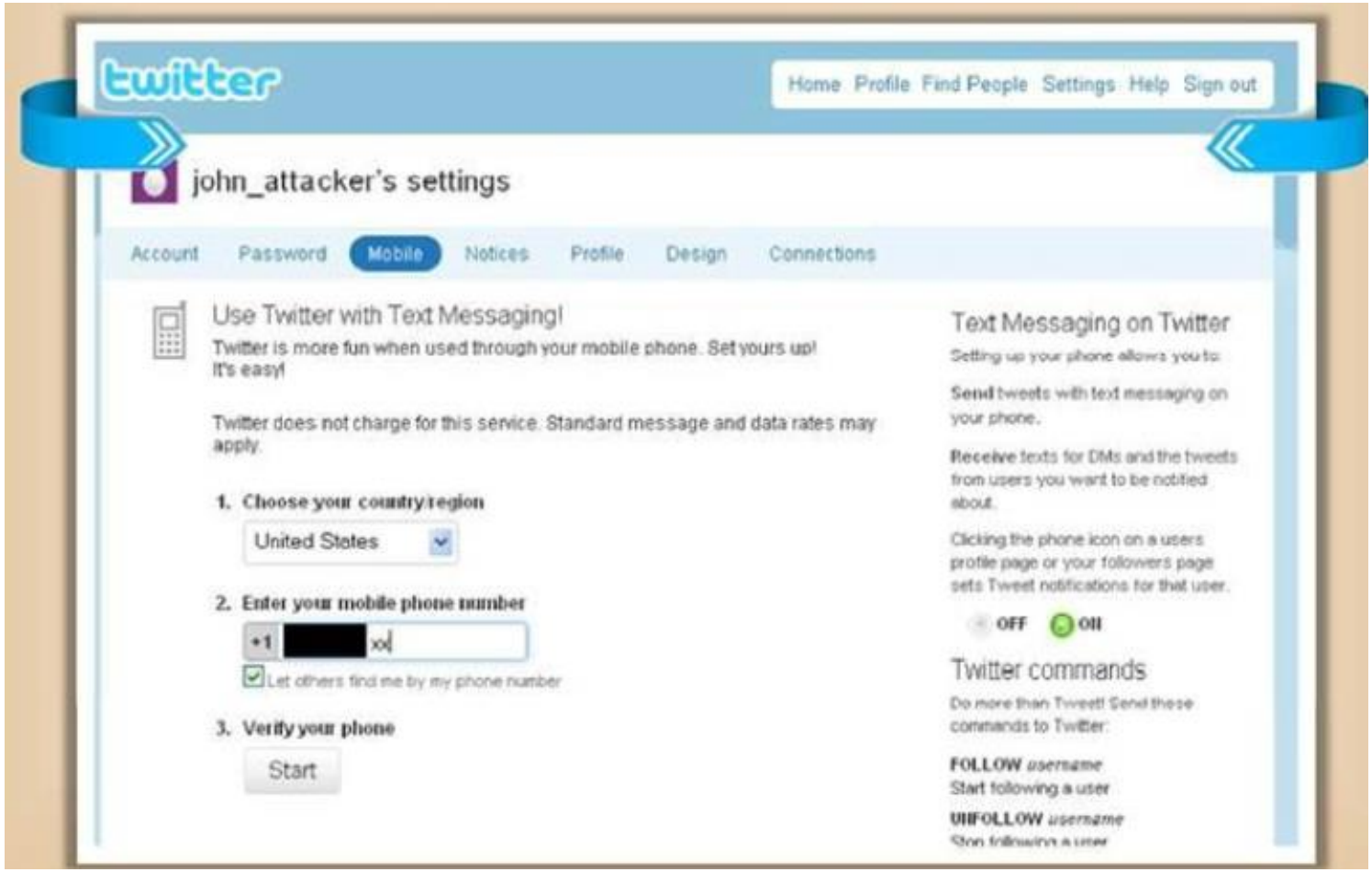
Social Engineering example: LinkedIn Profile



Social Engineering on Facebook

- Kẻ tấn công tạo ra một nhóm người sử dụng giả mạo trên facebook là “nhân viên“ của công ty
- Sử dụng identity giả, kẻ tấn công sau đó sẽ tiến tới “làm bạn”, hoặc mời, nhóm nhân viên giả mạo, nhóm nhân viên giả mạo này giả mạo là nhân viên của công ty
- Khi người sử dụng tham gia vào nhóm và họ sẽ cung cấp những thông tin về họ như ngày sinh, trường lớp, nguồn gốc, việc làm vợ chồng, tên …
- Bằng cách sử dụng những chi tiết của một nhân viên bất kỳ nào đó, kẻ tấn công có thể truy cập vào tòa nhà công ty.

Social Engineering on Twitter



Social Engineering on MySpace

Rủi ro của mạng xã hội với các mạng công ty

Ăn cắp dữ liệu

- Một trang trang web mạng xã hội là một cơ sở dữ liệu khổng lồ được truy cập bởi nhiều cá nhân, tăng nguy cơ khai thác thông tin

Không cố ý làm rò rỉ thông tin

- Trong trường hợp không có chính sách mạnh mẽ, nhân viên có thể vô tình gửi dữ liệu nhạy cảm về công ty của họ lên trên mạng xã hội

Tấn công mục tiêu

- Các thông tin trên các trang web sử dụng để thăm dò sơ bộ trong một cuộc tấn công mục tiêu

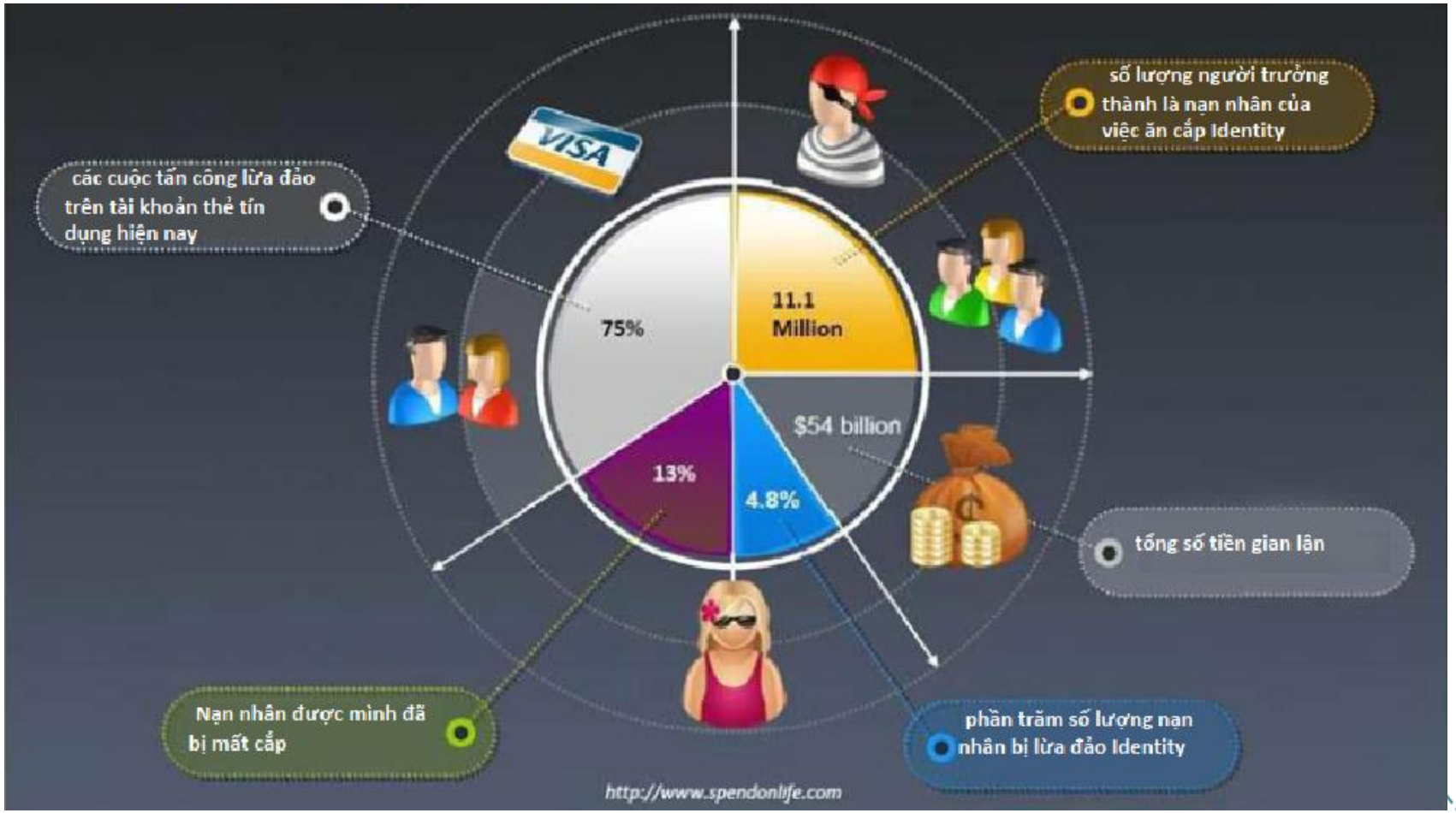
lỗ hổng hệ thống mạng

- Tất cả các trang mạng xã hội có thể để sai sót và lỗi và lộ có thể dẫn đến lỗ hổng trong mạng của công ty

Mục lục

1. Khái niệm Social Engineering
2. Kỹ thuật Social Engineering
3. Mạo danh trên mạng xã hội
4. **Ăn cắp danh tính**
5. Biện pháp đối phó với Social Engineering
6. Thử nghiệm xâm nhập

Số liệu thống kê tình trạng ăn cắp danh tính



Ăn cắp danh tính

Mất cắp thông tin cá nhân	Ăn cắp danh tính xảy ra khi một người nào đó bị ăn cắp tên của bạn và các thông tin cá nhân khác cho các mục đích gian lận
Bằng những phương pháp đơn giản	Không gian ảo đã làm cho việc ăn cắp Identity dễ dàng hơn để sử dụng thông tin cho các mục đính gian lận
Bị mất những con số an ninh xã hội	Ở một số nước sẽ rất nguy hiểm nếu mà kẻ mạo danh có được thông tin cá nhân, như số an ninh xã hội hoặc bằng lái xe

Làm thế nào để ăn cắp danh tính

Bước 1

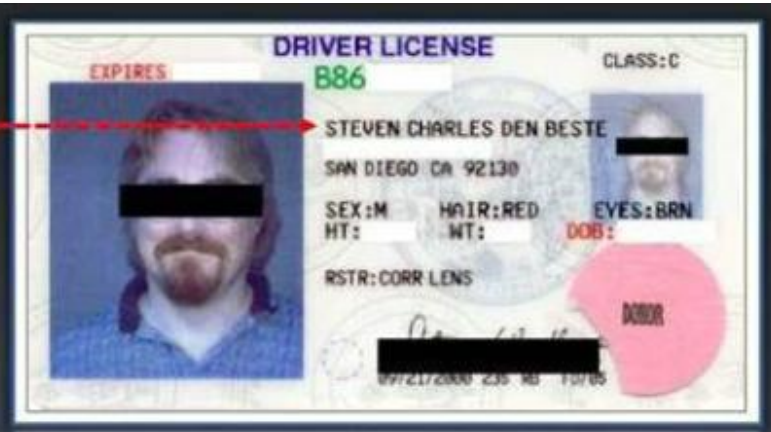
Kẻ tấn công ăn cắp hóa đơn điện thoại, hóa đơn nước hoặc hóa đơn điện của Steven sử dụng Dumpster Diving, Sotolen Email, hoặc ăn trộm tại chỗ.

Bước 2

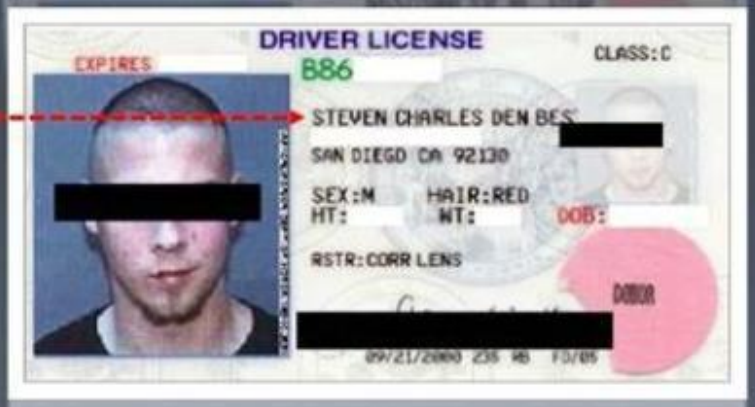
- Kẻ mạo danh (A) đến sở giao thông và nói rằng bị mất bằng lái xe
- Họ sẽ yêu cầu A cho bằng chứng xác nhận nhân thân như hóa đơn nước và hóa đơn điện
- A cho họ xem những hóa đơn đã lấy cắp
- A thông báo đã di chuyển từ địa điểm ban đầu nào (vd ở 1 bang khác)
- Nhân viên các bộ phận sẽ yêu cầu A hoàn thành hai việc cho việc thay đổi bằng lái xe và việc thứ hai cho sự thay đổi trên địa chỉ
- A sẽ cần một hình ảnh để cấp giấy phép lái xe
- Giấy phép lái xe thay thế của A sẽ được cấp với địa chỉ mới của nhà A
- Bây giờ A đã sẵn sàng với một danh tính mới.

So sánh

Ban đầu



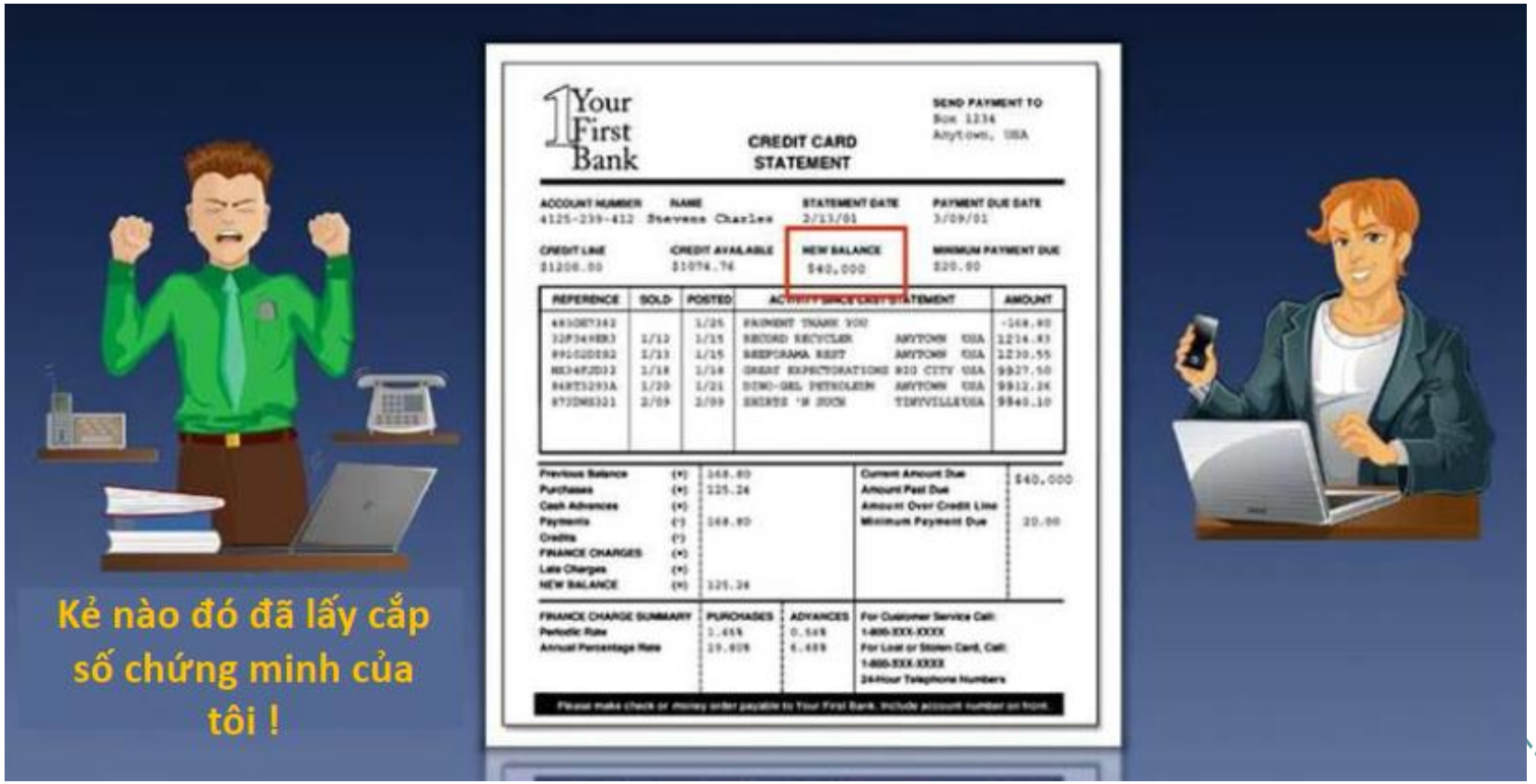
Tên tương tự : Steven Charles
Ăn cắp Identity



Bước 3

- A đi đến một ngân hàng trong đó đã có tài khoản của Steven Charles và cho họ biết A muốn mở một thẻ tín dụng mới
- A nói với ngân hàng là không nhớ số tài khoản và yêu cầu họ tìm nó bằng cách sử dụng địa chỉ và tên Steven
- Ngân hàng sẽ yêu cầu id của A: A cho họ thấy số id trên bằng lái xe, và nếu như họ chấp nhận, thẻ tín dụng của Steven sẽ được phát hành và sẵn sàng được sử dụng bởi A
- → A có thể sẵn sàng đi shopping rồi:
  - Thực hiện mua những mặt hàng giá trị với hàng ngàn đô la
  - Vay tiền mua xe
  - Làm một hộ chiếu mới
  - Mở mới một tài khoản ngân hàng
  - Đóng các dịch vụ tiện ích của A

Kết quả


Your First Bank
CREDIT CARD STATEMENT
SEND PAYMENT TO
Box 1234
Anytown, USA
ACCOUNT NUMBER
NAME
STATEMENT DATE
PAYMENT DUE DATE
CREDIT LINE
CREDIT AVAILABLE
NEW BALANCE
MINIMUM PAYMENT DUE
REFERENCE
SOLD
POSTED
AMOUNT
Kẻ nào đó đã lấy cắp số chứng minh của tôi !

Lấy cắp danh tính – vấn đề nghiêm trọng

- Lấy cắp danh tính là một vấn đề nghiêm trọng
- Số lượng và các hành vi vi phạm đã tăng lên
- Đảm bảo thông tin cá nhân tại nơi làm việc và tại nhà; kiểm tra các báo cáo thẻ tín dụng chỉ là một trong những cách để giảm thiểu nguy cơ mất cắp danh tính

Mục lục

1. Khái niệm Social Engineering
2. Kỹ thuật Social Engineering
3. Mạo danh trên mạng xã hội
4. Ăn cắp danh tính
5. **Biện pháp đối phó với Social Engineering**
6. Thử nghiệm xâm nhập

Biện Pháp Đối Phó với Social Engineering: Chính Sách

- Những chính sách và thủ tục tốt sẽ không hiệu quả nếu như chúng không được giảng dạy và trang bị cho các nhân viên của công ty.
- Sau khi được đào tạo, nhân viên phải ký một tuyên bố thừa nhận rằng họ hiểu các chính sách

Các chính sách về mật khẩu	Các chính sách an ninh vật lý
• Thay đổi mật khẩu định kỳ • Tránh mật khẩu đoán được • Tài khoản cần đươc năng chặn sau khi cố gắn đăng nhập thất bại • Mật khẩu phải có độ dài và tính phức tạp • Giữ bí mật mật khẩu	• Phát thẻ id, đồng phục • Hộ tống những khách mời • Hạn chế các khu vụ truy cập • Tiêu hủy, băm nhỏ những tài liệu không còn sử dụng • Tuyển dụng nhân viên an ninh

Biện Pháp Đối Phó với Social Engineering

Đào tạo	Nguyên tắc hoạt động
• Một chương trình đào tạo hiệu quả nên bao gồm tất cả những chính sách bảo mật và phương pháp để nâng cao nhận thức về Social Engineering	• Đảm bảo an ninh thông tin nhạy cảm và ủy quền sử dụng tài nguyên

Biện Pháp Đối Phó với Social Engineering

phân loại thông tin	• Phân loại các thông tin tối mật, độc quyền, sử dụng nội bộ, sử dụng công cộng
đặc quyền truy cập	• cần phải có quản trị viên, người sử dụng các tài khoản phải được ủy quyền thích hợp
Kiểm tra nhân viên và sử lý đình chỉ đúng đắn	• Trong nội bộ các tiềm tàng về hình sự và nhân viên bị thôi việc rất dễ dàng cho việc mua thông tin
tần xuất phản hồi thích hợp	• cần có những phản ứng thích hợp cho những trường hợp cố gắng sử dụng Social Engineering

Biện Pháp Đối Phó với Social Engineering

Xác thực hai yếu tố

- Thay vì mật khẩu cố định, sử dụng xác thực hai yếu tố cho những dịch vụ mạng có nguy cơ cao như VPN và Modem Pool

Phòng thủ Anti-Virus/Anti-Phishing

- sử dụng nhiều lớp để phòng chống virus như người dùng đầu cuối và mail gateway để giảm thiểu các cuộc tấn công Social Engineering

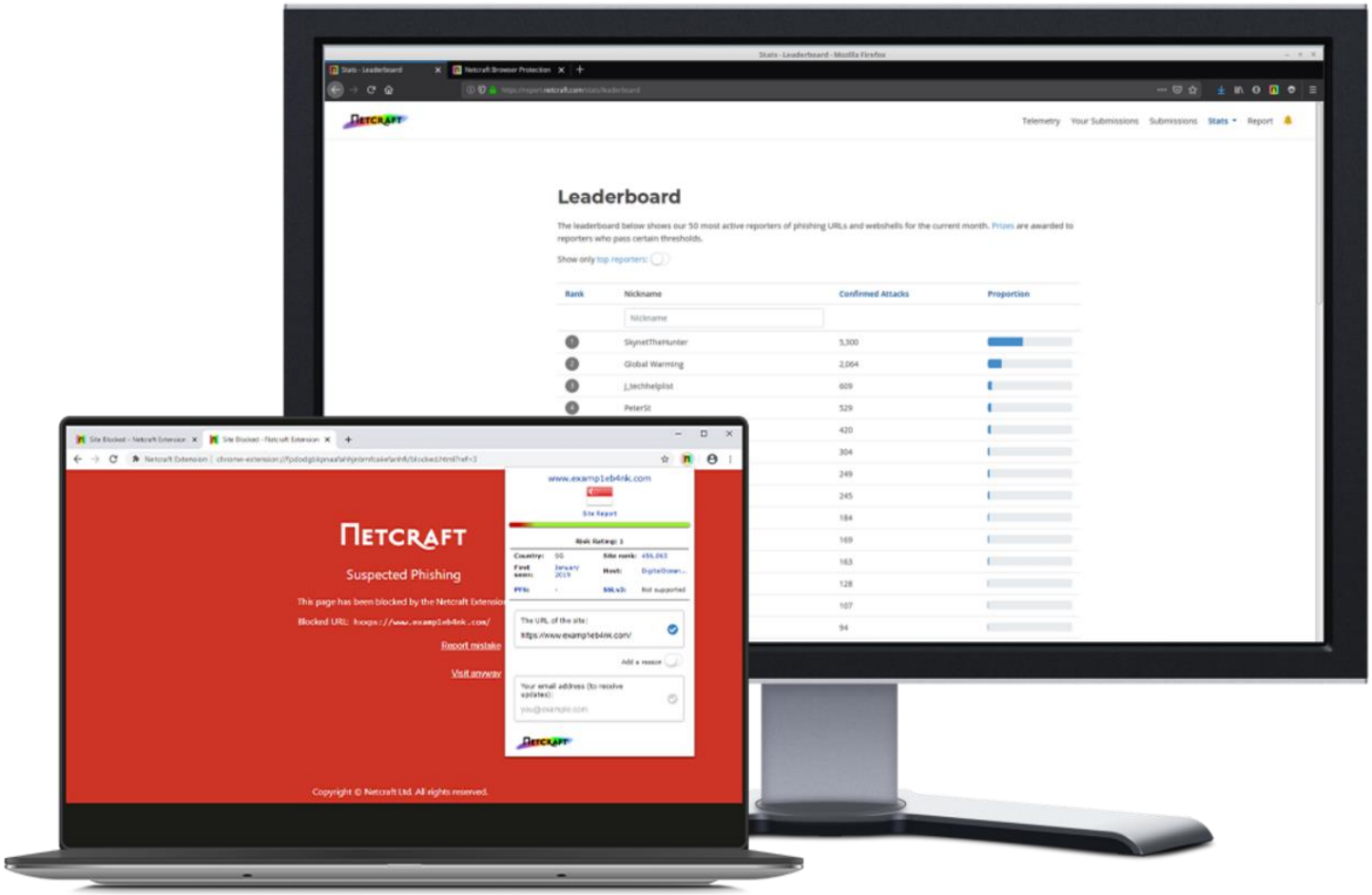
Thay đổi công tác quản lý

- việc thay đổi quy trình quản lý tài liệu sẽ bảo mật hơn

Làm thế nào để phát hiện các Email giả mạo

- Nó bao gồm các liên kết dẫn đến các trang web giả mạo yêu cầu nhập thông tin cá nhân khi click
- Email lừa đảo có vẻ đến từ một ngân hàng, tổ chức tài chính, công ty hoặc một mạng xã hội
- Giống như đến từ một người trong danh sách địa chỉ email
- Chỉ đạo để gọi một cuộc điện thoại để cung cấp số tài khoản số điện thoại cá nhân, mật khẩu hoặc các thông tin bí mật
- Bao gồm logo của các viên chức và các thông tin khác được lấy trực tiếp từ các trang web hợp pháp thuyết phục nạn nhân tiết lộ chi tiết cá nhân của mình

Thanh công cụ chống lừa đảo: Netcraft



Thanh công cụ chống lừa đảo: PhishTank

PhishTank® Out of the Net, into the Tank.

username
Register | Forgot Pa

Home | Add A Phish | Verify A Phish | Phish Search | Stats | FAQ | Developers | Mailing Lists | My Account

Join the fight against phishing

Submit suspected phishes. Track the status of your submissions.
Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:
http:// Is it a phish?

Recent Submissions

You can help! Sign in or register (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
8035246	https://ebisaplus.herokuapp.com/des/index.php	voldemor
8035245	https://amerikoolernet.w3spaces.com/	JackSparrow2016
8035244	https://att-101776.weeblysite.com/	prodigyabuse
8035243	https://att-103094.weeblysite.com/	prodigyabuse
8035242	http://att-103094.weeblysite.com/	prodigyabuse
8035241	https://bt-login-page-103284.weeblysite.com/	verifrom
8035240	http://bt-login-page-103284.weeblysite.com/	verifrom
8035239	https://sim-update.eu/verification/login.php	verifrom
8035238	https://sfresim.net/	verifrom
8035237	https://sfr-esim-desactivation.com/	verifrom
8035236	http://www.thefishfinder.com/mass/	r3gersec
8035235	https://youthful-golick.178-170-13-195.plesk.page/...	verifrom
8035233	https://virtual5.com.mx/mass/	r3gersec
8035232	http://positivistthings.org.uk/	Amarena98
8035231	https://funny-nobel.178-170-13-195.plesk.page/ad/w...	verifrom

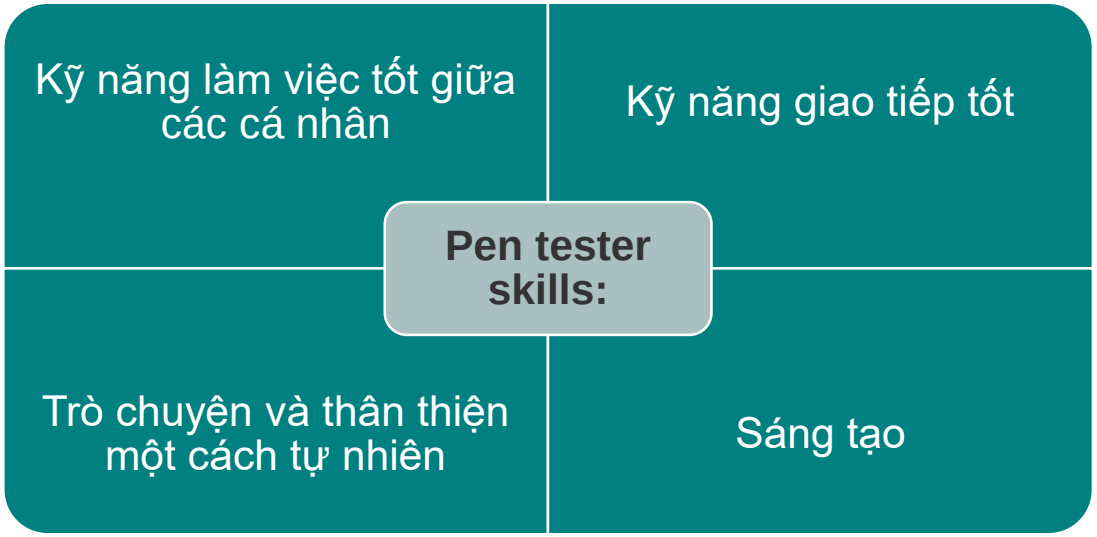
See more suspected phishes...

Biện pháp đối phó việc đánh cắp Identity

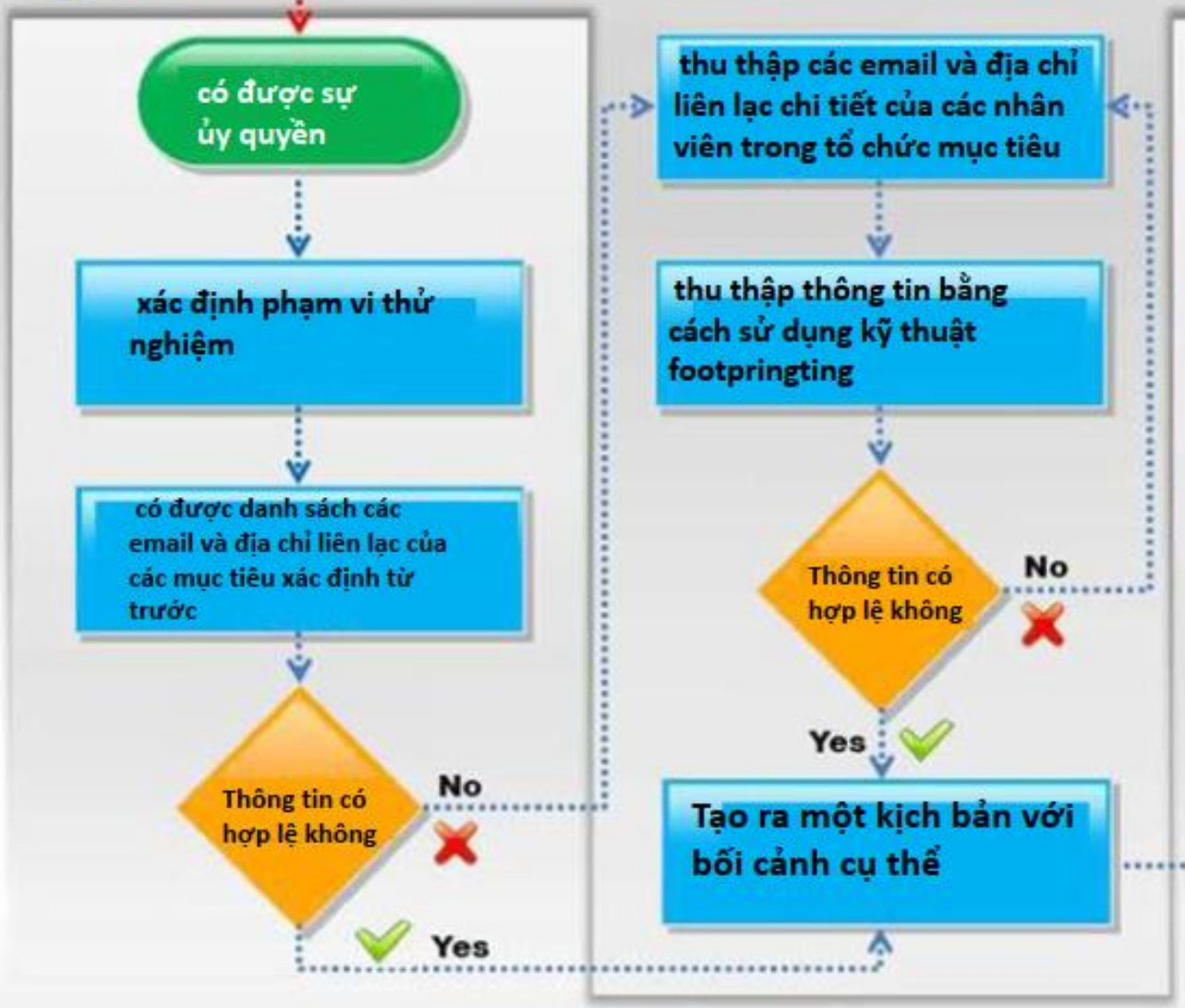
- ✓ Bảo đảm hoặc xé nhỏ tất cả các tài liệu có chứa thông tin cá nhân
- ✓ Luôn giữ cho hòm thư được an toàn, làm sạch chúng một cách nhanh chóng
- ✓ Đảm bảo rằng tên của mình không xuất hiện trong các danh sách của người tiếp thị
- ✓ Nghi ngờ và xác minh lại tất cả những yêu cầu cho dữ liệu cá nhân
- ✓ Xem xét các báo cáo thẻ tín dụng/ ghi nợ của mình một cách thường xuyên
- ✓ Không bao giờ để thẻ tín dụng/ ghi nợ của mình ngoài tầm nhìn
- ✓ Bảo vệ thông tin cá nhân của mình khi được công bố công khai
- ✓ Không bao giờ đưa ra bất cứ thông tin cá nhân nào trên điện thoại
- ✓ Không hiển thị số tài khoản hoặc số liên lạc trừ khi bắt buộc

Kiểm thử Social Engineering

- Mục tiêu của kiểm thử Social Engineering là để kiểm tra của yếu tố con người trong một chuỗi bảo mật trong tổ chức
- Kiểm thử Social Engineering thường được sử dụng để nâng cao trình độ nhận thức bảo mật giữa các nhân viên
- Người kiểm thử phải cẩn thận và chuyên nghiệp khi thử nghiệm Social Engineering vì nó có liên quan đến vấn đề pháp lý vi phạm quyền riêng tư và có thể dẫn đến các tình huống lúng túng

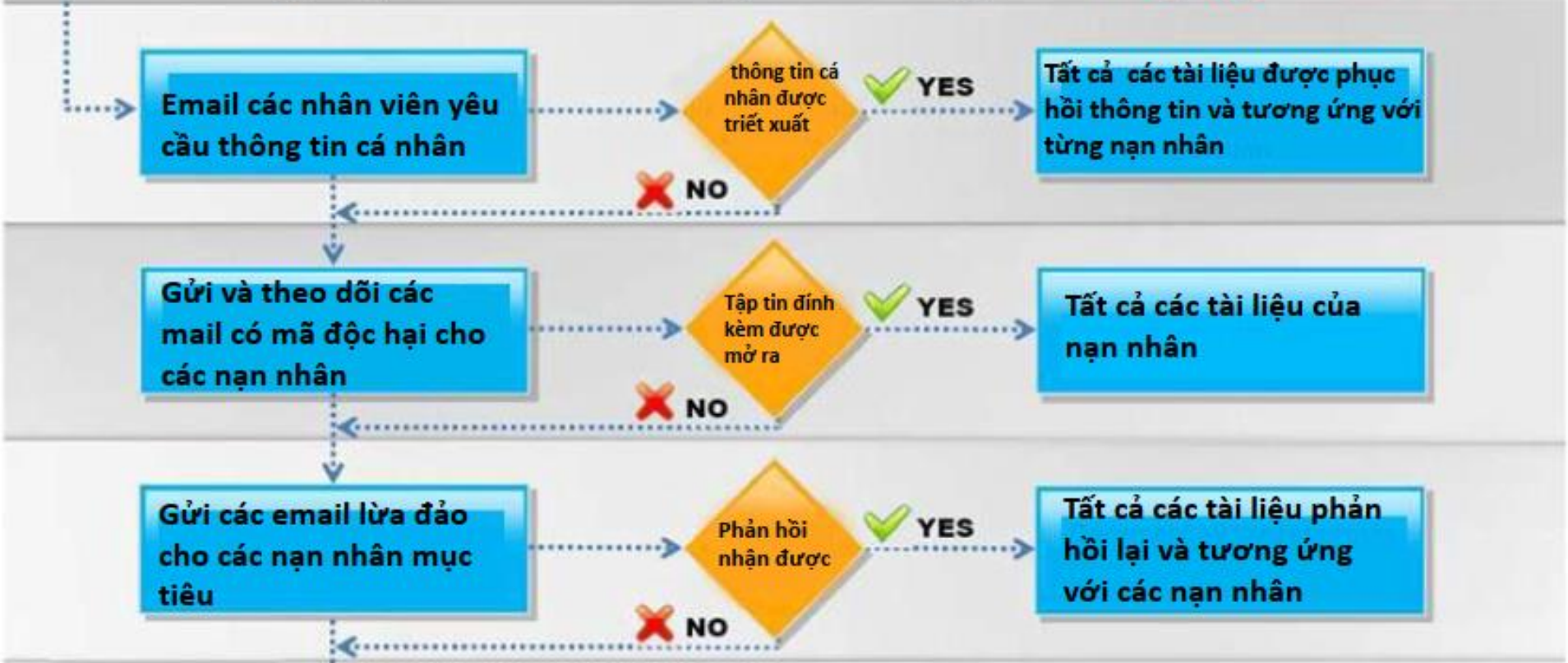


Thử nghiệm Social Engineering



- Có được sự ủy quyền quản lý rõ ràng và chi tiết sẽ giúp cho việc xác định phạm vi kiểm tra, chẳng hạn như danh sách các danh sách các phòng ban, nhân viên cần phải được kiểm tra, hoặc mức độ xâm nhập vật lý
- Thu thập địa chỉ email và chi tiết liên lạc của tổ chức mục tiêu và nguồn nhân lực (nếu không được cung cấp) bằng cách sử dụng cá kỹ thuật như Dumpster diving, đoán email, USENET và các trang web tim kiếm, công cụ bẫy email như Email Extractor
- Cố gắn triết xuất thông tin càng nhiều càng tốt về các mục tiêu đã xác định bằng cách sử dụng kỹ thuật footprinting
- Tạo ra một kịch bản dựa trên những thông tin thu thập được xem xet kết quả tích cực và tiêu cực của một cố gắng

Thử nghiệm Social Engineering: Sử Dụng Emails



- Email nhân viên yêu cầu thông tin cá nhân như tên người dùng mật khẩu bằng cách cải trang quản trị mạng, hỗ trợ kỹ thuật, hoặc bất kỳ ai từ các bộ phận khác nhau lấy lý do là có một trường hợp khẩn cấp
- Gửi email tới các mục tiêu có đính kèm file độc hại và theo rõi phản ứng của họ với file đính kèm đó bằng cách sử dụng công cụ như ReadNotify
- Gửi một email lừa đảo tới các mục tiêu như thế từ một ngân hàng và yêu cầu thông tin nhạy cảm từ họ (bạn cần phải có sự cho phép cần thiết cho việc này

Thử nghiệm Social Engineering: Sử Dụng Điện Thoại

Gọi một cuộc điện thoại đến mục tiêu đặt ra giả vờ như một đồng nghiệp và yêu cầu thông tin nhạy cảm

Gọi một cuộc điện thoại đến mục tiêu đặt ra giả vờ như một user quan trọng

Gọi một cuộc điện thoại đến mục tiêu đặt ra giả vờ như nhân viên hỗ trợ kỹ thuật và yêu cầu họ thông tin nhạy cảm

Đề cập đến một người quan trọng trong tổ chức và cố gắng thu thập dữ liệu

Gọi đến mục tiêu và cung cấp cho họ những phần thưởng thay thế cho thông tin cá nhân của họ

Đe dọa mục tiêu với những hậu quả nghiêm trọng (vd như tài khoản sẽ bị vô hiệu hóa) để có được thông tin

Sử dụng kỹ thuật Reverse Social Engineering sao cho các mục tiêu mang lại lại thông tin

Thử nghiệm Social Engineering: In Person

kết bạn với nhân viên trong quán ăn tự phục vụ và cố gắng để lấy thông tin

cố gắng vào cổng sau đeo một thẻ ID giả hoặc piggyback

cố gắng vào trụ sở giả như một kiểm toán viên bên ngoài

cố gắng nghe trộmtrên hệ thông , nhìn trộm và những người sử dụng

cố gắng vào trụ sở giả như một nhân viên kỹ thuật

tất cả các tài liệu tìm thấy nằm trong một báo cáo

- Thành công của bất kỳ kỹ thuật Social Engineering đều phục thuộc vào một người thử nghiệm bằng cách nào nó đưa ra một kịch bản thử nghiệm và kĩ năng giao tiếp của mình
- có vô số kỹ thuật Social Engineering dựa trên những thông tin có sẵn và phạm vi thử nghiệm. Luôn luôn xem xét các bước thử nghiệm có vấn đề pháp lý không

Tổng kết

- Social Engineering là nghệ thuật thuyết phục mọi người tiết lộ thông tin
- Social Engineering liên quan đến việc thu thập thông tin nhạy cảm hoặc các đặc quyền truy cập không phù hợp với người ngoài
- Kĩ thuật Computer-based đề cập đến việc sử dụng các phần mềm máy tính để lấy thông tin mong muốn
- Phòng thủ thành công phụ thuộc vào chính sách tốt và việc thi hành các chính sách đó có nghiêm túc và liên tục hay không

Quotes

"Nếu bạn nghĩ rằng công nghệ có thể giải quyết các vấn đề bảo mật, thì tức là bạn không hiểu gì về các vấn đề bảo mật của bạn và công nghệ là gì!"

Bruce Schneier,

Security Technologist and Author

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

KIỂM THỬ XÂM NHẬP

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

KIỂM THỬ XÂM NHẬP

Một số dạng kiểm thử xâm nhập: Kiểm thử vật lý

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY

Biên soạn từ bài giảng: Nguyễn Ngọc Điệp, Bài giảng Kiểm thử xâm nhập, Học viện Công nghệ Bưu chính Viễn thông, 2021.

Mục lục

1. **Giới thiệu kiểm thử vật lý (Physical penetration testing)**
2. Phương pháp thực hiện
3. Ví dụ
4. Tổng kết

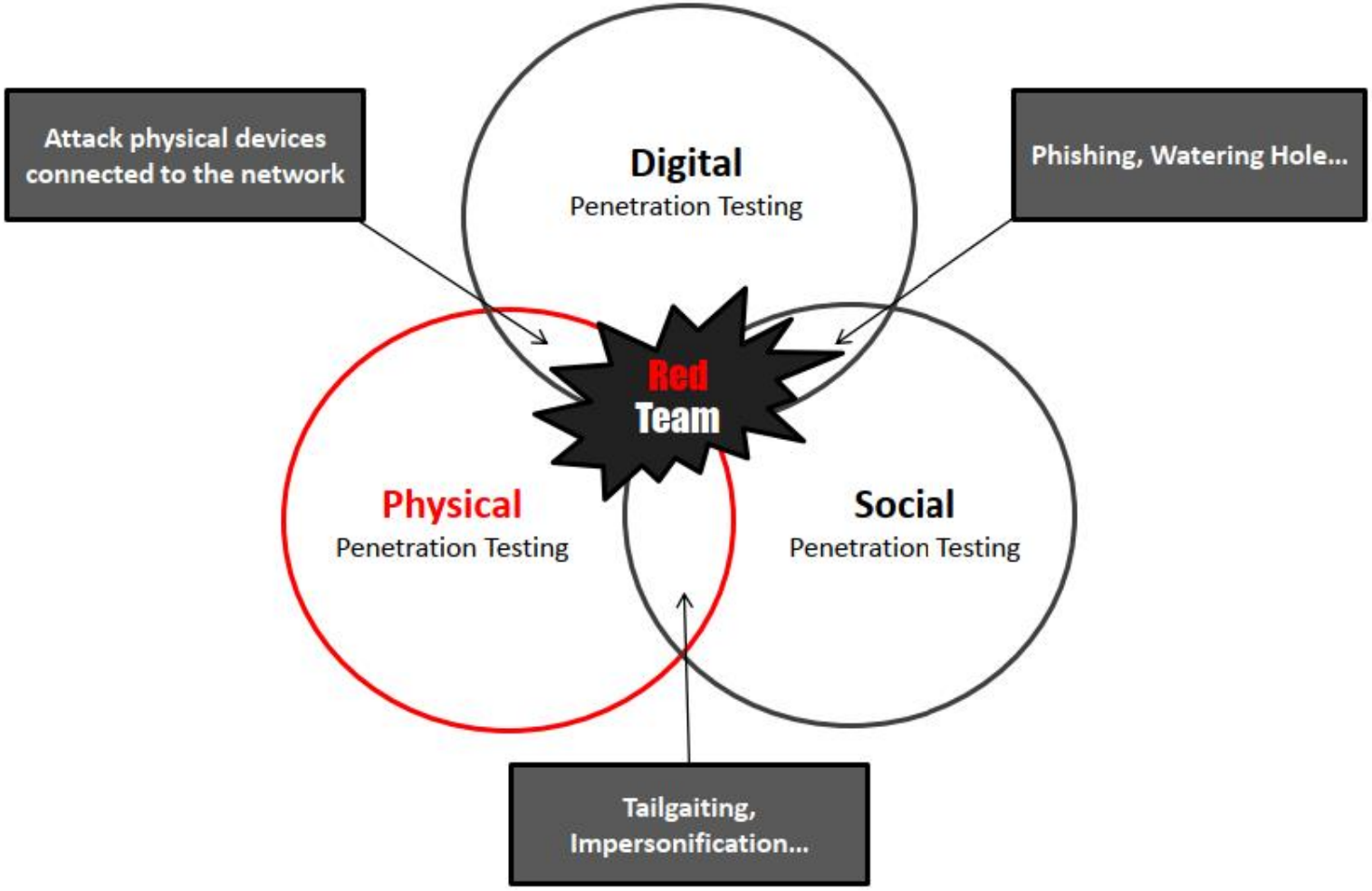
Khái niệm

- Xâm nhập vật lý là một phương pháp của tội phạm mạng nhằm truy nhập vào cơ sở hạ tầng mạng dữ liệu từ phía trong của công ty, từ đó có thể dễ dàng xâm nhập đến mục tiêu. Một khi kẻ tấn công có thể đi vào bên trong của các tổ chức mục tiêu, cơ hội tấn công là rất nhiều.
- Kiểm thử xâm nhập vật lý sẽ giúp đánh giá chính xác hiệu quả của các chính sách kiểm soát an toàn vật lý trong tổ chức.

Tại sao xâm nhập vật lý lại nguy hiểm

- Tất cả mọi biện pháp bảo mật sử dụng các hệ thống điều khiển kỹ thuật số như: tường lửa, hệ thống phát hiện xâm nhập IDS … đều sẽ vô dụng khi xâm nhập vật lý có thể thực hiên được.
- Sự vi phạm chính sách kiểm soát bên ngoài của tổ chức sẽ khác nhau tùy theo độ phức tạp của hệ thống và các thủ tục mà tổ chức đã áp dụng để ngăn chặn
- Các tổ chức vẫn còn chưa quan tâm đến kiểm thử vật lý.

Bảo mật tích hợp



Phân biệt các team

- Red team:
  - tập trung vào việc kiểm tra khả năng thâm nhập của các hệ thống khác nhau và mức độ bảo mật của chúng
  - giúp phát hiện, ngăn chặn và loại bỏ các điểm yếu trong khi tấn công các lỗ hổng bảo mật
  - sử dụng tất cả các kỹ thuật thâm nhập mạng và dữ liệu hiện có
- Blue team:
  - bảo vệ an ninh mạng cho tổ chức và phát hiện ra các lỗ hổng có thể xảy ra
  - Có trách nhiệm tăng cường phòng thủ mạng, đồng thời đảm bảo xử lý nhanh chóng các lỗ hổng trong trường hợp tin tặc tấn công mạng thành công

Mục lục

1. Giới thiệu kiểm thử vật lý (Physical penetration testing)
2. **Phương pháp thực hiện**
3. Ví dụ
4. Tổng kết

Các bước thực hiện

1. Xác định mục tiêu và phạm vi
2. Thu thập thông tin
3. Phân tích sơ bộ
4. Trinh sát (bị động và chủ động)
5. Đánh giá tình hình
6. Lên kế hoạch và phân tích
7. Luyện tập
8. Thực hiện tấn công

Lên kế hoạch và đánh giá (1)

- Xác định mục tiêu và phạm vi
- Thu thập thông tin
  - Tìm hiểu về tổ chức mục tiêu và xác định các tài sản của họ.
  - Tìm nơi cất giấu tài sản
- Phân tích sơ bộ

Lên kế hoạch và đánh giá (2)

- Trinh sát bị động
  - Tìm hiểu về địa điểm mục tiêu và địa hình xung quanh
  - Tìm hiểu đường lái xe
  - Tìm hiểu các cửa, lỗ hổng
  - Các đường thoát

Lên kế hoạch và đánh giá (3)

- Trinh sát chủ động
  - Giám sát nhân viên, bảo vệ
  - Đồng phục và huy hiệu
  - Xác định vị trí thang máy
  - Khu vực mù của máy ảnh và cảm biến
  - Dạo quanh khu vực công cộng bên trong tòa nhà
  - Xác định vị trí phòng họp
  - Mạng không dây
  - Bản đồ khẩn cấp
- Đánh giá tình hình
  - Đánh giá cơ hội trò chuyện với nhân viên
  - Thu thập thông tin về nhân viên

Thực hiện tấn công (1)

- **Vượt qua kiểm soát truy cập**
  - Lock Picking
  - Tailgating
  - Key pad
  - Biometric
  - Badges
    - Contactless
    - Smartcard
    - Magnetic
  - Not controlled physical Access
    - Windows
    - Garage

Thực hiện tấn công (1)

- **Vượt qua các cảm biến và báo động**
  - Cảm biến chuyển động
    - PIR
    - Quang điện
    - Siêu âm
  - Cảm biến từ tính
  - Chống nhiễu cho hệ thống thông tin liên lạc
- **Vượt qua hệ thống giám sát**
- **Sử dụng tấn công social engineering để có quyền truy cập vật lý**

Thực hiện tấn công (2)

- Khai thác và truy cập mạng công ty (Red Team)
  - Cửa hậu vật lý (PwnPlg, Raspberry …)
  - Thiết bị bên ngoài (Keylogger, Network Sniffer …)
  - Truy cập vào các máy tính không được bảo vệ (Kon-Boot …)
  - Chặn cuộc gọi (Điện thoại và VoIP)
  - Các thiết bị phần cứng
- Lấy thông tin bí mật

Thực hiện tấn công (2)

- Khai thác và truy cập mạng công ty (Red Team)
  - Cửa hậu vật lý (PwnPlg, Raspberry …)
  - Thiết bị bên ngoài (Keylogger, Network Sniffer …)
  - Truy cập vào các máy tính không được bảo vệ (Kon-Boot …)
  - Chặn cuộc gọi (Điện thoại và VoIP)
  - Các thiết bị phần cứng
- Lấy thông tin bí mật

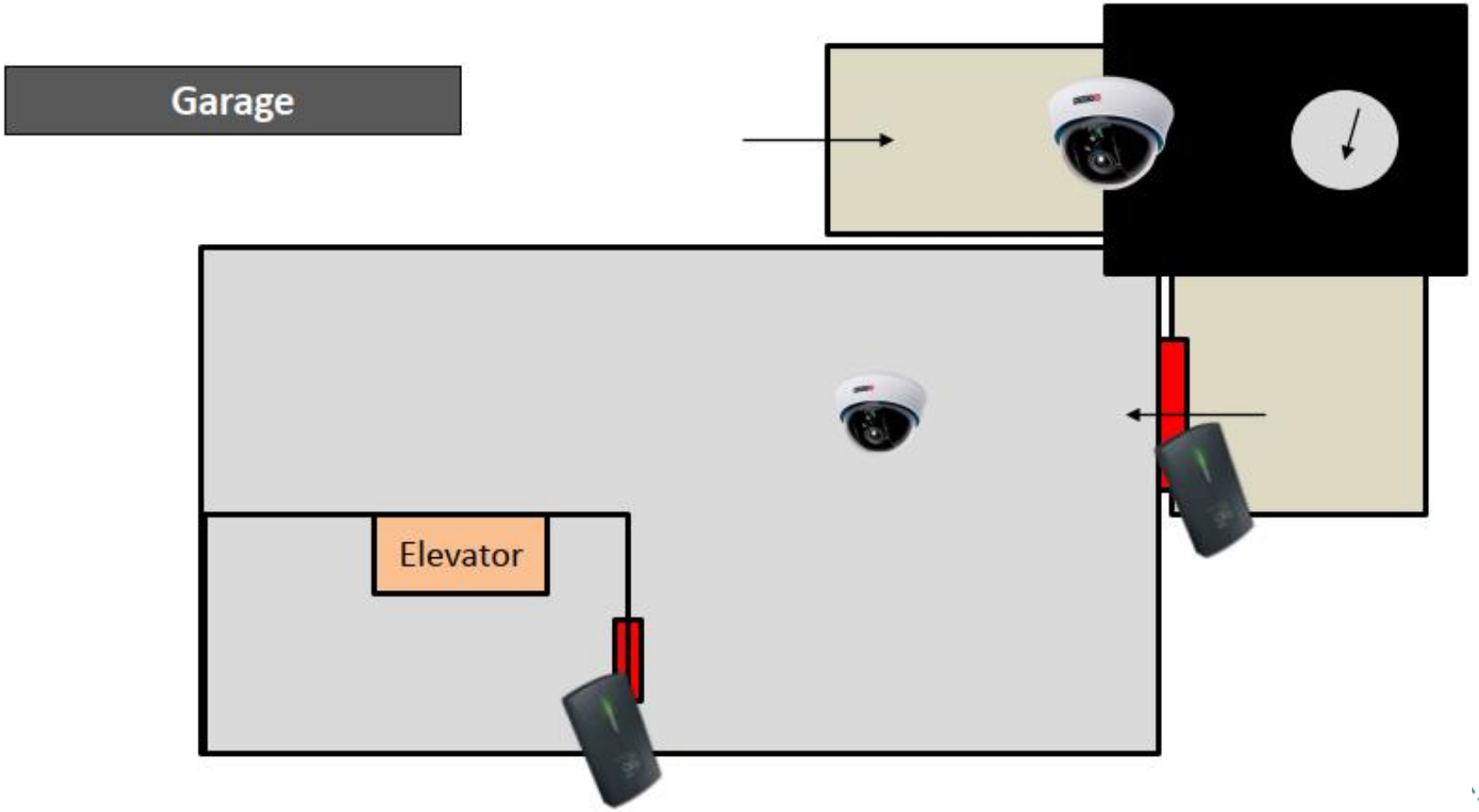
Mục lục

1. Giới thiệu kiểm thử vật lý (Physical penetration testing)
2. Phương pháp thực hiện
3. **Ví dụ**
4. Tổng kết

Ví dụ (1)

Ground floor

Ví dụ (2)

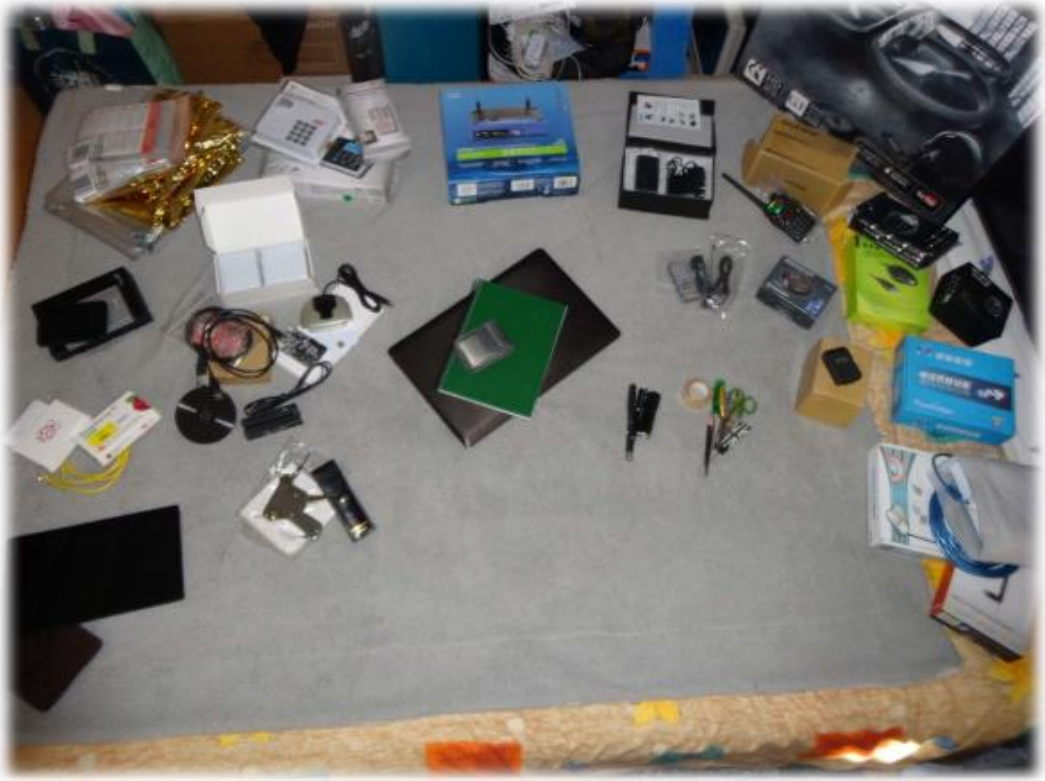


Ví dụ (3)

Objetive floor

Ví dụ (3)

Equipment



Ví dụ: Trinh sát (thụ động)

Using Google, Maps and Street

Ví dụ: Trinh sát (chủ động)

- Sử dụng drone

Ví dụ: Trinh sát (chủ động)

- Theo dõi ban đêm

VS

VD: thu thập thông tin

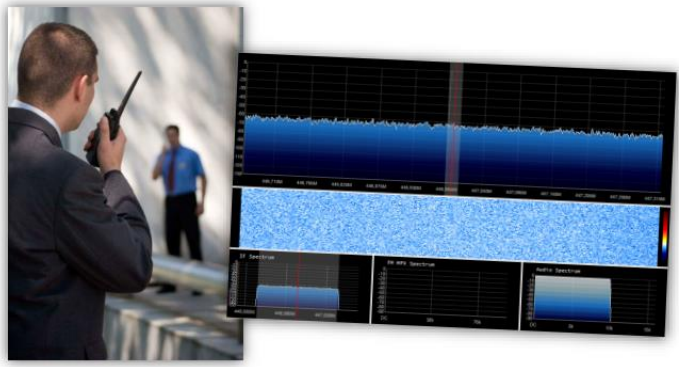
- Dumpster Diving

- Shoulder Surfing

VD: thu thập thông tin

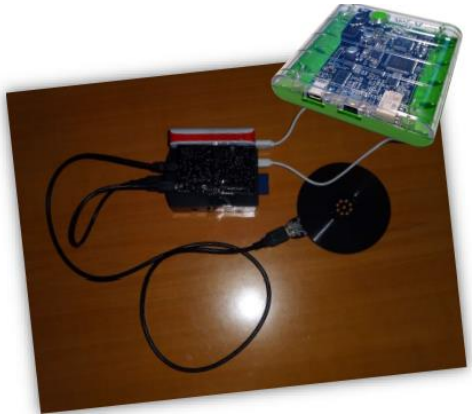
- Social Engineering

- Interception of radio communications



VD: Vượt qua kiểm soát truy cập

- Bypass of RFID Access Control



1. Read employ card
2. Clone employ card

If fail:
3. Analyze
4. Change content
   or
   Emulate / Brute Force

VD: Trinh sát nội bộ

- Reconnaissance of Internal Security Measures

VD: Vượt qua các biện pháp an ninh

- Bypass of Alarm System

- Bypass of Magnetic Sensor

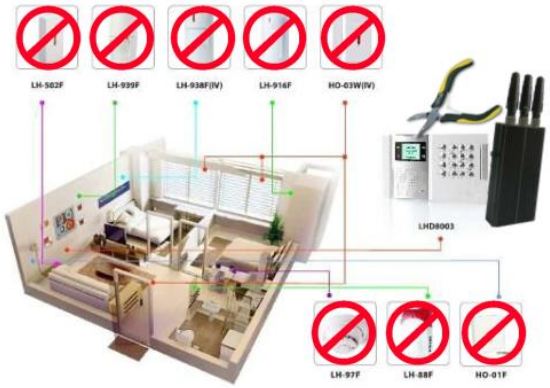
VD: Vượt qua các biện pháp an ninh

- Bypass of Motion Sensor

VD: Vượt qua các biện pháp an ninh

- Bypass of Photoelectric Sensor

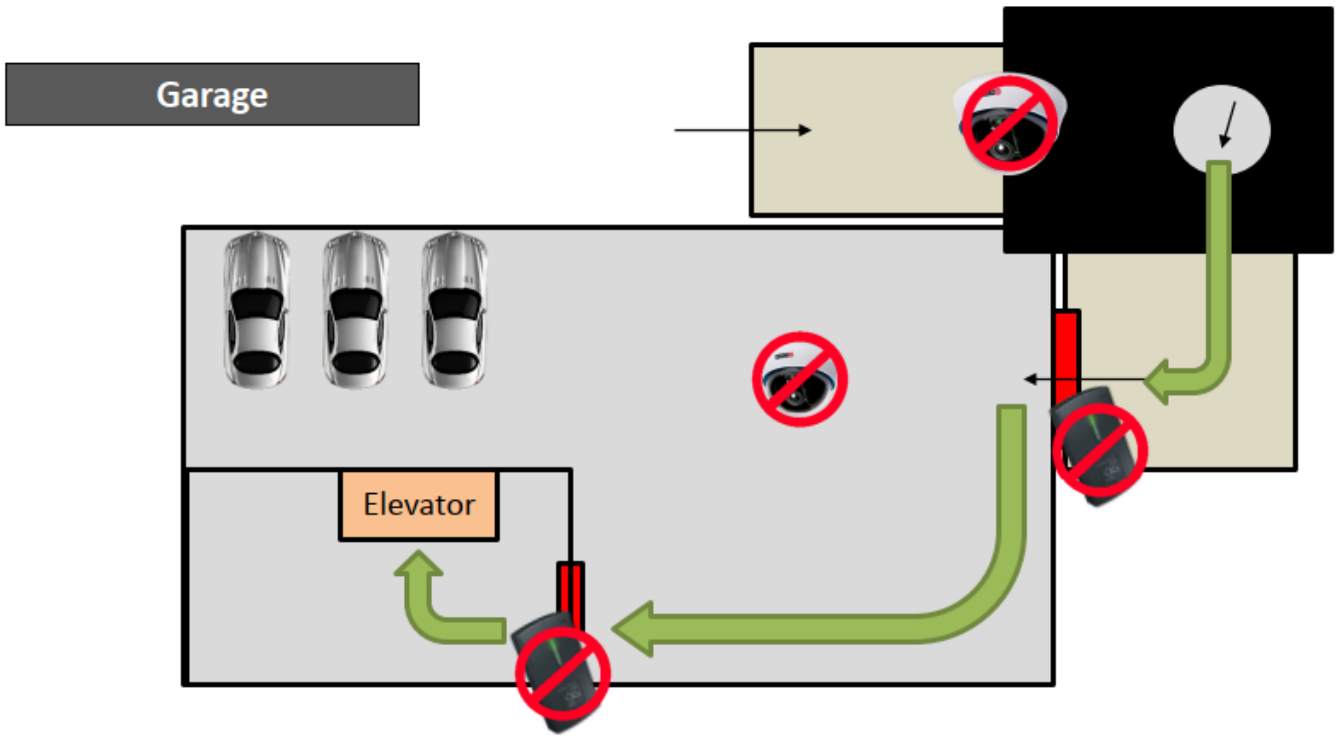
- Bypass of Alarm System



VD: Vượt qua các biện pháp an ninh

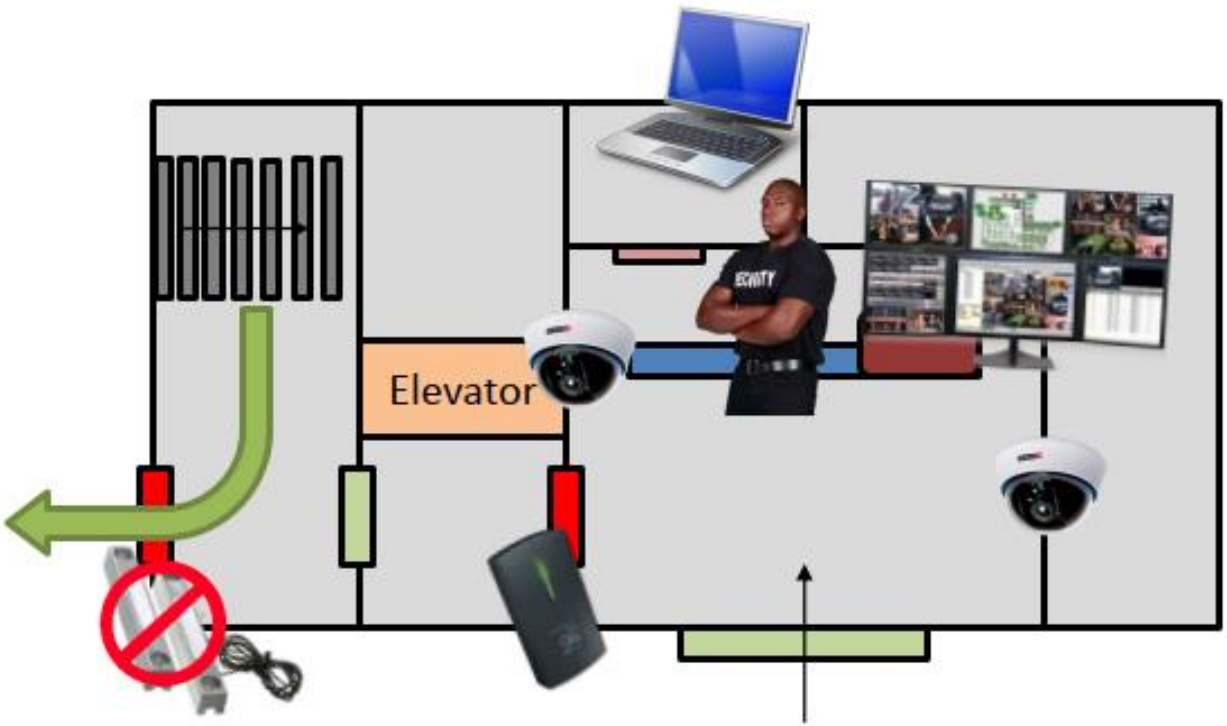
- Bypass of Magnetic Card / Keypad Access

Kết quả (1)



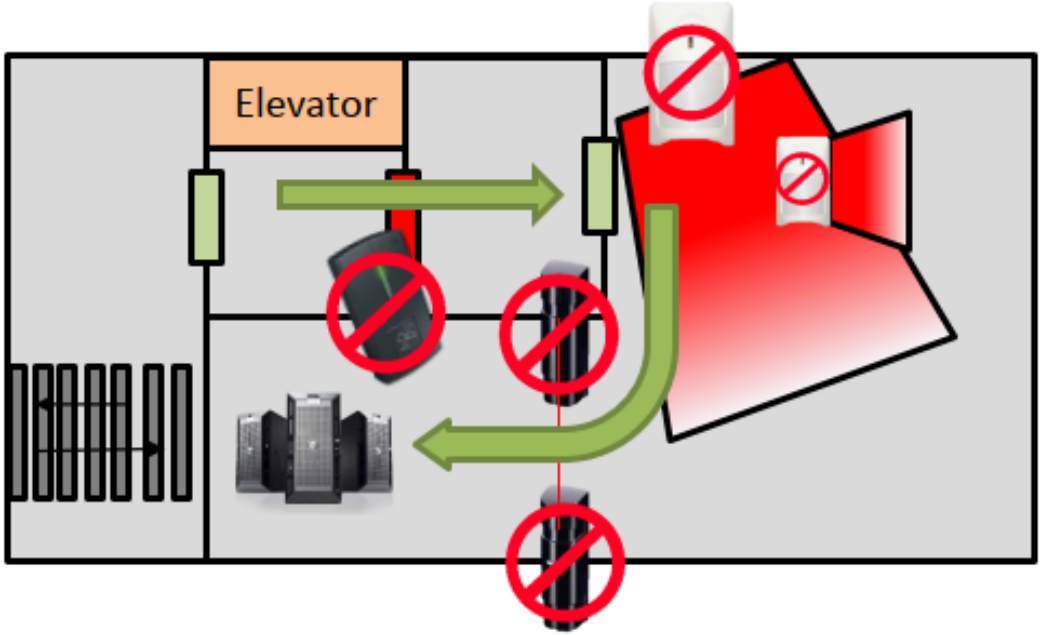
Kết quả (2)

Ground floor



Kết quả (3)

First Floor



Kết quả (4)

Ground floor

Mục lục

1. Giới thiệu kiểm thử vật lý (Physical penetration testing)
2. Phương pháp thực hiện
3. Ví dụ
4. **Tổng kết**

Tổng kết

- Đòi hỏi sự sáng tạo và tư duy bên trong việc thực hiện xâm nhập vật lý thực tế.
- Cách tiếp cận của Red Team như một giải pháp để tiến hành đánh giá bảo mật tích hợp toàn diện trong một tổ chức.