Kiểm thử & đánh giá an toàn hệ thống thông tin

Social Engineering
Pentesting Methodology

1 Tổng quan

2 Quy trình thực hiện

1 Tổng quan

2 Quy trình thực hiện

SE Pentesting

- Kỹ nghệ xã hội (Social engineering - SE) là nghệ thuật khai thác thông tin dựa trên yếu tố con người
- Kiểm thử kỹ nghệ xã hội được thực hiện nhằm:

- Thực hiện kiểm tra nhận thức nhân sự trong tổ chức đối với vấn đề an toàn thông tin
- Sử dụng để nâng cao nhận thức người dùng trong tổ chức trước những cuộc tấn công thực tế

SE Pentesting

❑**Đối tượng:**

– Users/clients

– Quản trị viên hệ thống

– Nhân viên lễ tân

– Nhân viên hỗ trợ kỹ thuật

– Nhà cung cấp

❑**Tại sao có thể thực hiện SE?**

- Thiếu đào tạo nhận thức về ATTT
- Đánh vào yếu tố lòng tin, lòng tham của con người
- Thiếu chính sách đảm bảo
- Khó bị phát hiện
- Không có giải pháp chắc chắn trước SE

SE Pentesting

- Kỹ năng yêu cầu để thực hiện SE pentesting:
  - Kỹ năng giao tiếp tốt
  - Sáng tạo
  - Nói chuyện tự nhiên & thân thiện

Black Box or White Box

- Hộp trắng:
  - Pentester được cung cấp mọi thông tin về địa chỉ, số điện thoại, email, vị trí của đối tượng
- Hộp đen
  - Pentester cần thu thập thông tin dựa trên các kỹ thuật OSINT

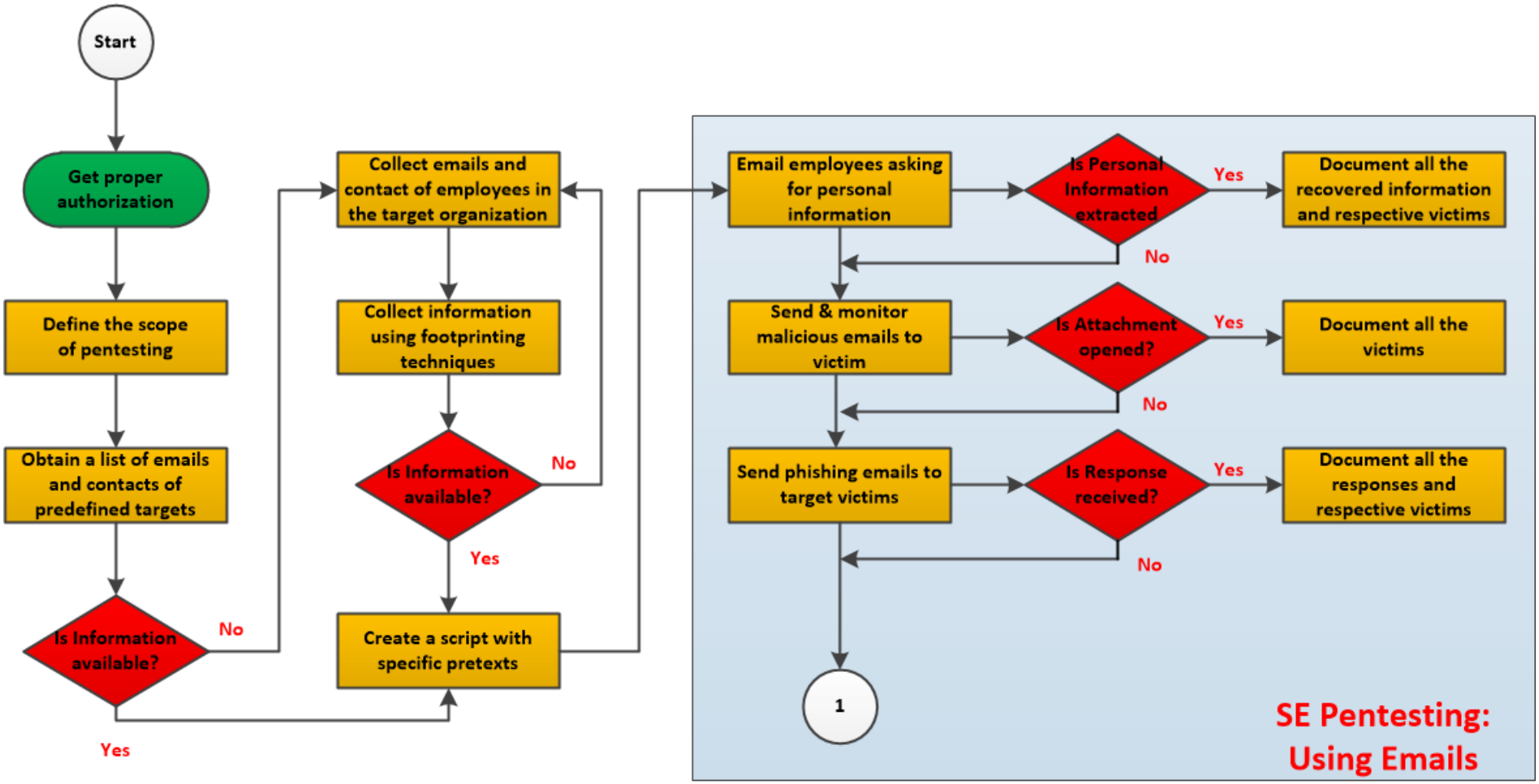
1 Tổng quan

2 Quy trình thực hiện

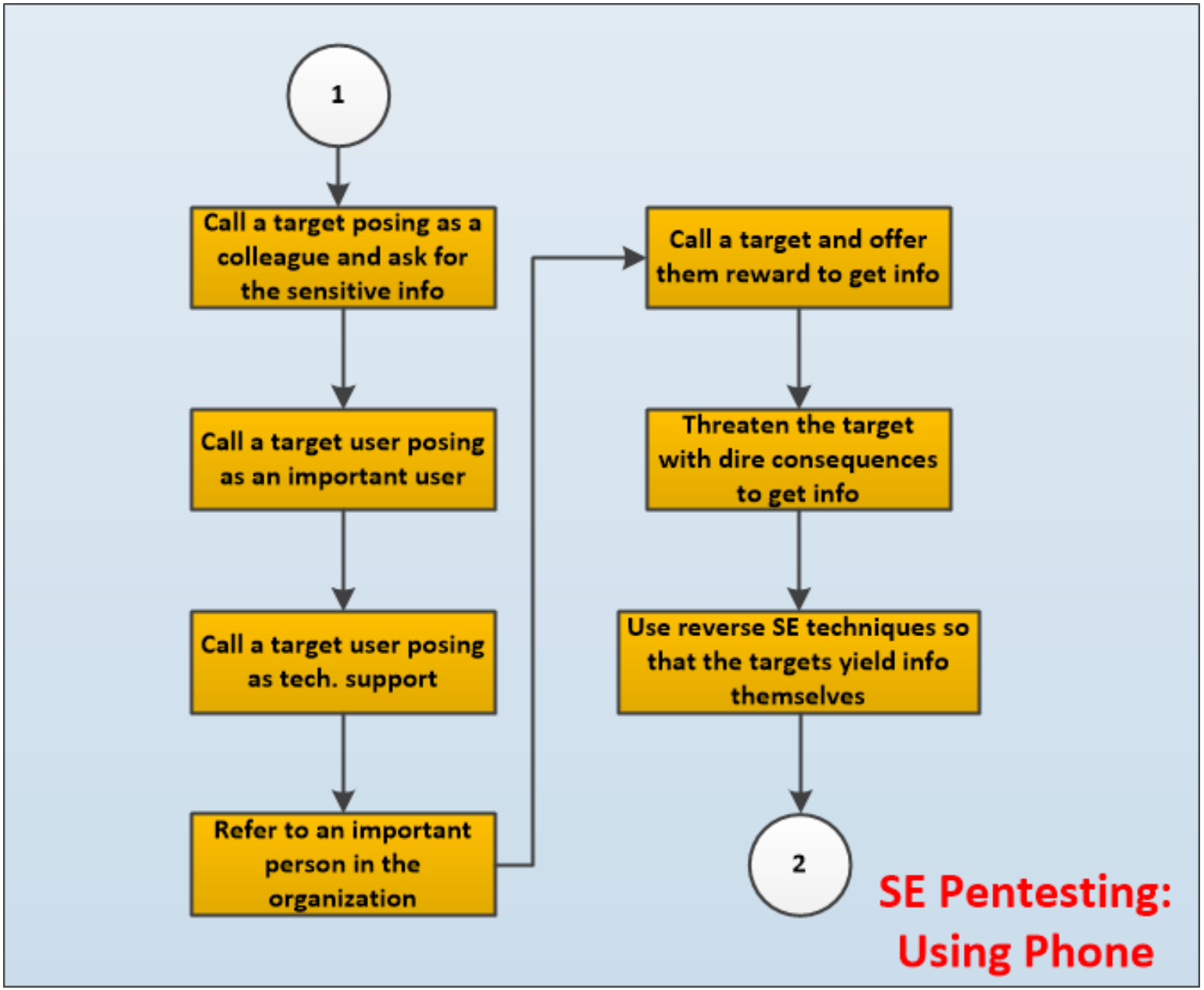
Phases of a SE Pentesting

- Tìm kiếm thông tin về tổ chức
- Xác định phạm vi kiểm thử, lựa chọn đối tượng
- Phát triển mối quan hệ
- Khai thác mối quan hệ

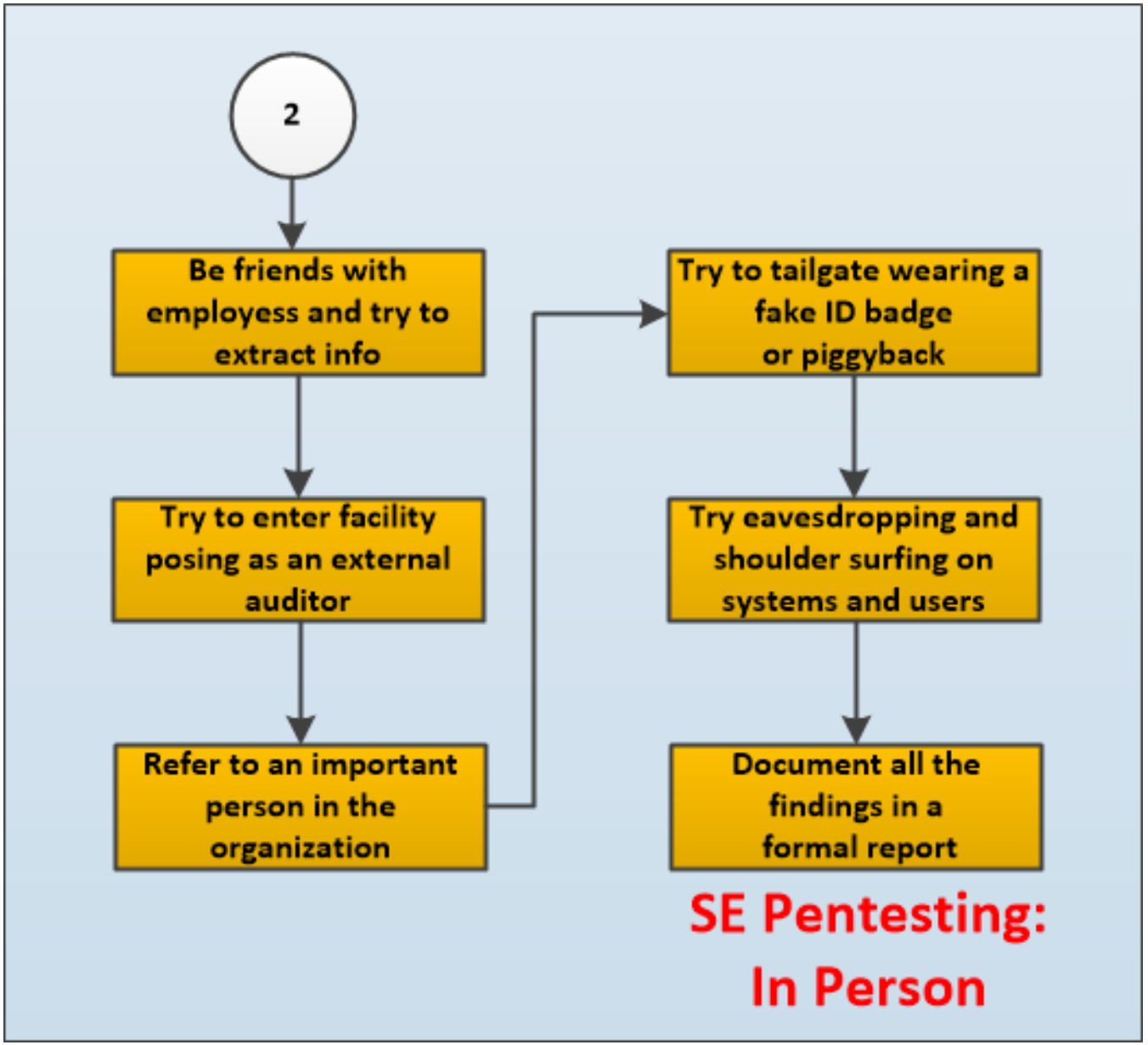
SE Pentesting Steps



SE Pentesting Steps (cont'd)



SE Pentesting Steps (cont'd)



SE Pentesting Techniques

❑Human-based SE

- Impersonation, Tailgating, Vishing, Dumpster Diving, Eavesdropping, Shoulder Surfing, Piggybacking

❑Technical-base SE

- Phishing, Pop-ups, Spam Mail, Public Malicious Apps, Using Fake Security Application

Human-based SE Pentesting

Impersonation

- Thực hiện giả mạo cá nhân, người dùng hợp lệ trong tổ chức thông qua email, điện thoại (vishing), tin nhắn từ đó chiếm đoạt các thông tin nhạy cảm của người dùng khác:

- Giả mạo người dùng đầu cuối
- Giả mạo lãnh đạo, nhân vật cấp cao của tổ chức
- Giả mạo nhân viên hỗ trợ, nhân viên kỹ thuật, nhân viên lắp đặt, sửa chữa…

Physical Attack Vector

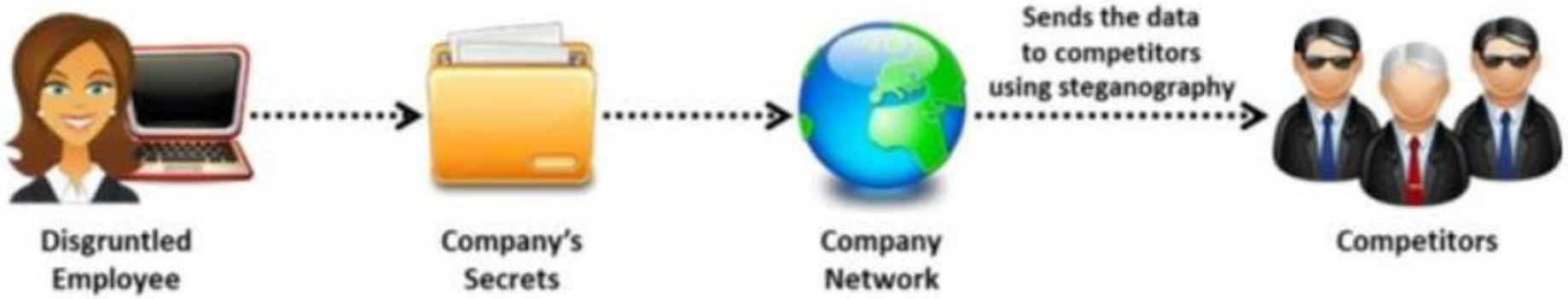
- Thực hiện nghe lén các cuộc nói chuyện điện thoại, hội nghị truyền hình, đọc trộm tin nhắn (Eavesdropping)
- Xem trộm các thông tin đăng nhập (password, PIN…) từ sau lưng (Shoulder Surfing)
- Tìm kiếm thông tin có giá trị tại mặt thùng rác, mặt bàn, sticky note xung quanh nơi làm việc (Dumpster Diving)
- Thử "làm rơi" các thiết bị như USB, lén cắm vào máy tính tại tổ chức…(Dropping media)

Physical Attack Vector

- Thử sử dụng Fake ID để xâm nhập vào văn phòng/ khu vực hạn chế của tổ chức
- Sử dụng kỹ thuật Piggybacking/Tailgating để vào khu vực hạn chế

Physical Attack Vector

- Tìm kiếm, lôi kéo các cá nhân bất mãn với tổ chức



Technical-based SE Pentesting

Computer-based SE Pentesting

- **Pop-up windows:**

- Cửa sổ yêu cầu người dùng nhập thông tin cá nhân

- **Hoax Letter:**

- Thông tin cảnh báo về virus, trojan đã lây nhiễm trên máy nạn nhân

- **Chain Letters:**

- Emails gợi ý về nhận tiền, quà miễn phí, thông báo trúng thưởng

- **Instant Chat**

-Sử dụng các kênh chat để thu thập thông tin

- **Spam Email**

- Gửi email chứa mã độc để thu thập thông tin

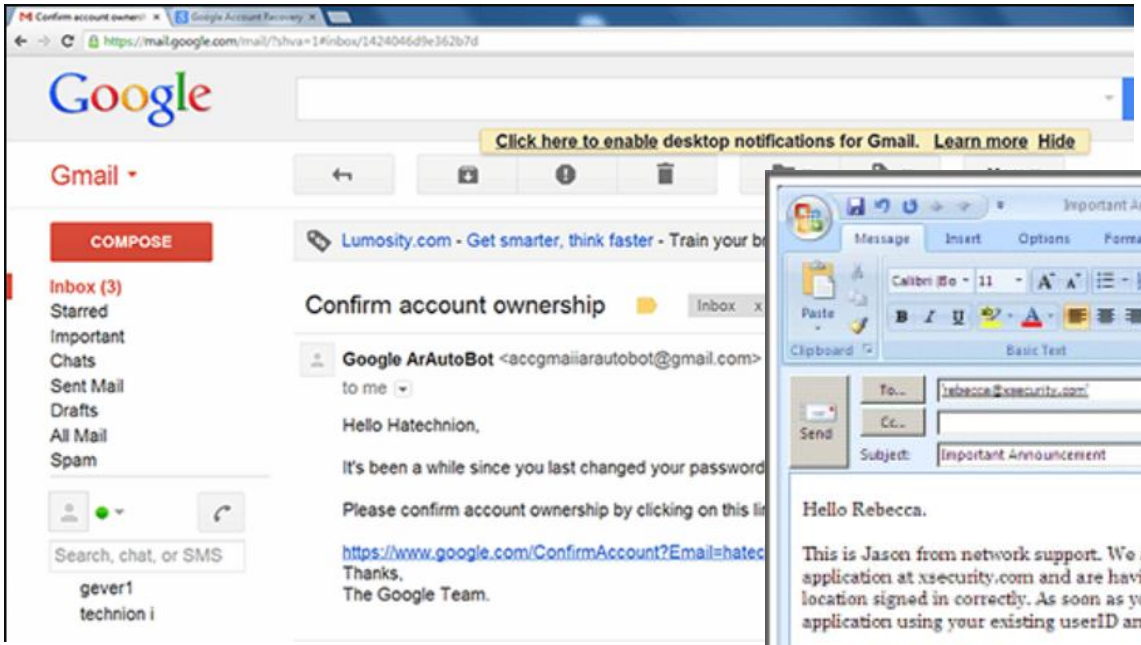
Phishing

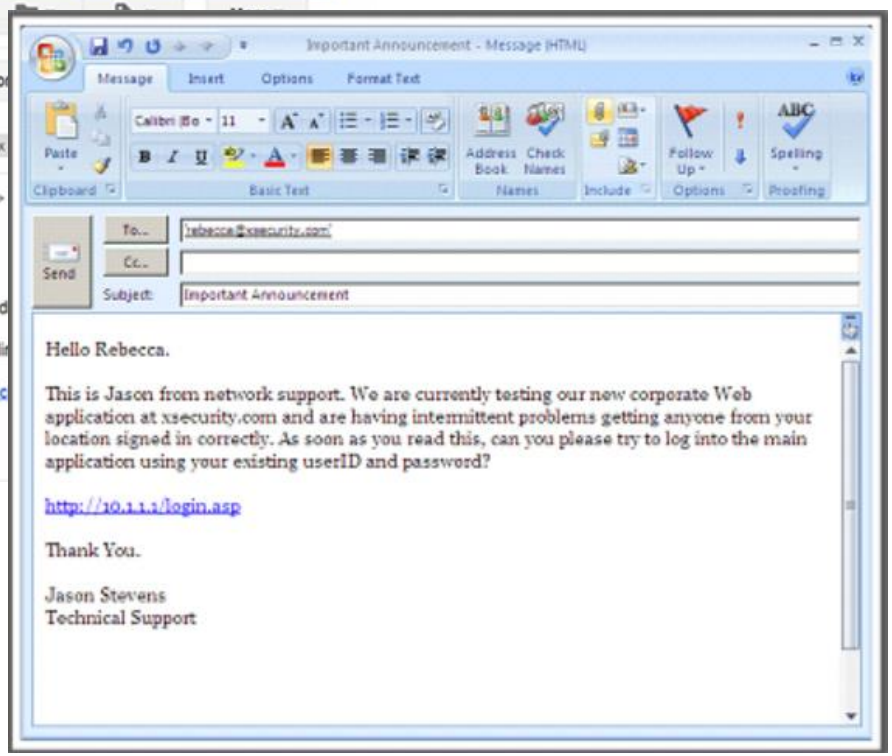
- Là hành vi giả mạo ác ý nhằm lấy được các thông tin nhạy cảm như bằng cách giả dạng thành một chủ thể tin cậy
- Phân loại:

- Spear Phishing
- Whaling
- Pharming
- Spimming

Phishing

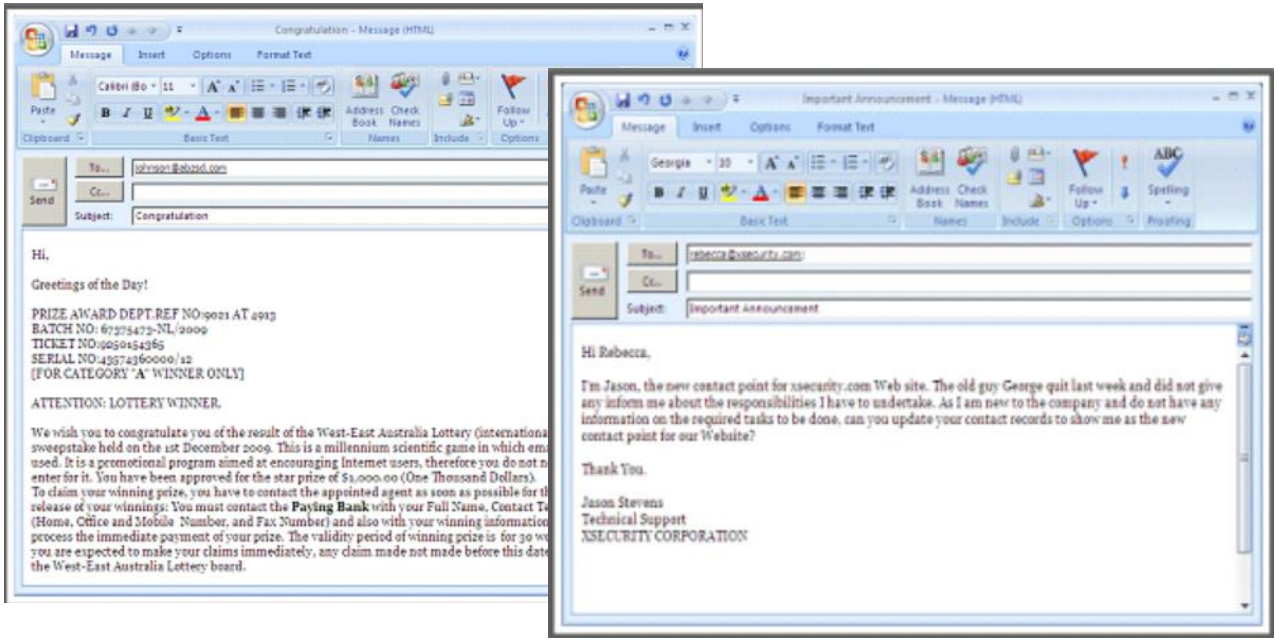
- Tạo một website giả mạo website của tổ chức
- Gửi email cho một vài cá nhân trong tổ chức với đường link tới website giả mạo





Phishing

- Gửi các thông báo giả (trúng sổ xố, quà tặng) tới users và yêu cầu hộ cung cấp thông tin, email, địa chỉ, password..thông qua online form
- Gửi mạo người quản trị hệ thống và gửi email yêu cầu người dùng truy cập vào link để cấp lại mật khẩu (lý do: mật khẩu cũ hết hạn, nghi ngờ bị lộ…)



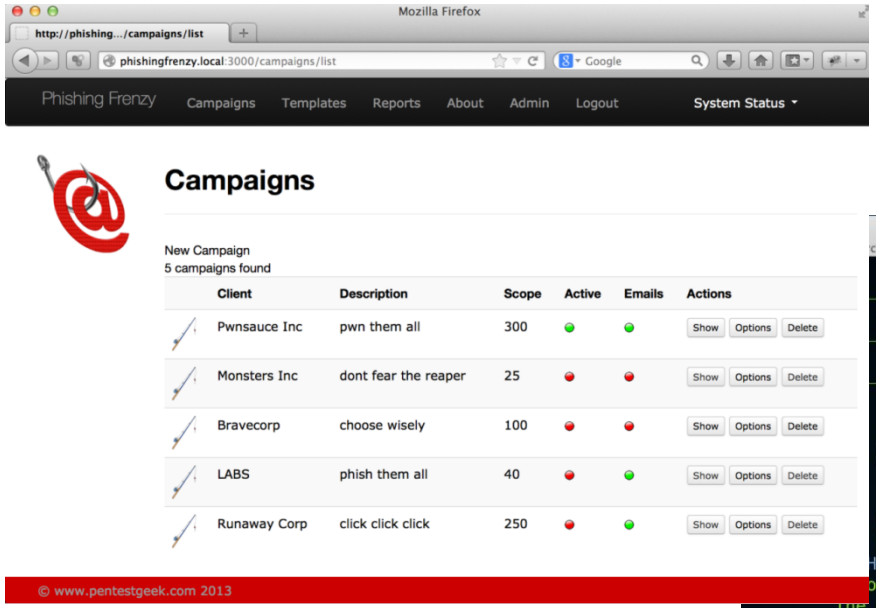
Phishing

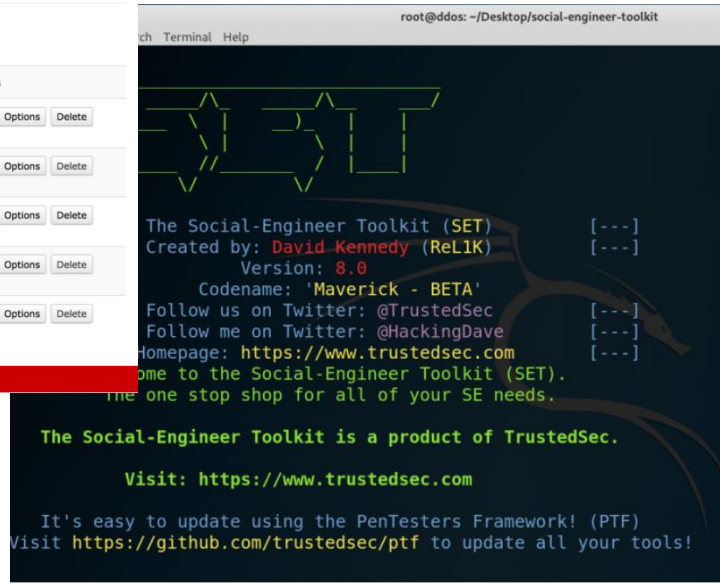
- Sử dụng fake websites để chuyển hướng người dùng nhằm thu thập các thông tin bí mật
- Lừa người dùng click vào các pop-ups
- Gửi email chưa link độc hại gần giống với link thật của tổ chức
- Ví dụ:

- Các trang download tài liệu giả yêu cầu thông tin user
- www.vietcombank.com.vn // www.vietcombank.com

Launch a Phishing Campaign

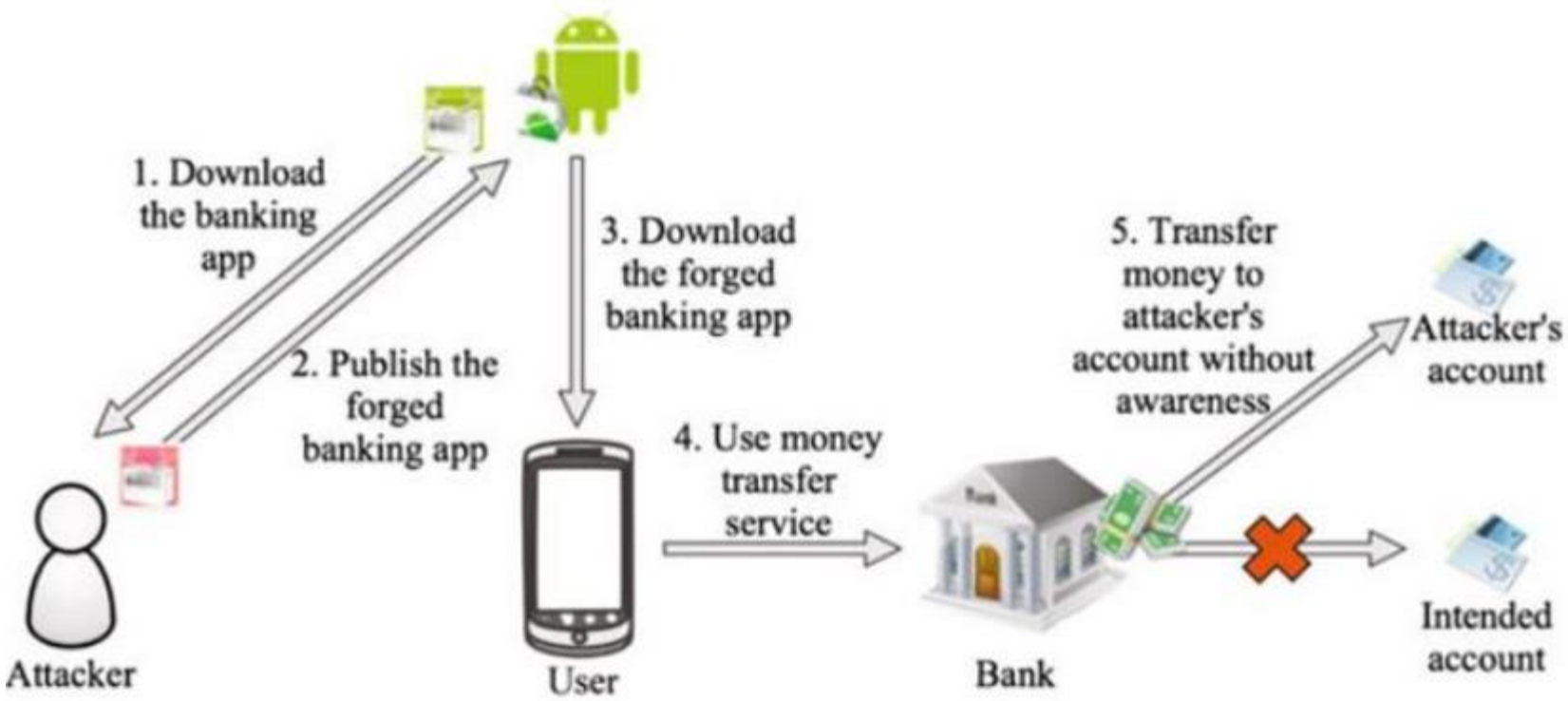
- Pentester có thể sử dụng các công cụ sau
  - Phising Frenzy, LUCY, SE Toolkit (SET), SpeedPhish Framework (SPF), GoPhish, King phisher…





Mobile-based SE Pentesting

- ❑Publishing Malicious Apps
- ❑Repackaging Legitimate Apps
- ❑Fake Security Application
- ❑SMS Phishing



Document the Result

- Ghi lại tất cả các thông tin thu thập được để chuẩn bị cho các loại hình tấn công tiếp theo

Thảo luận

SE Pentesting countermeasures?

Countermeasures & Recommendations

- Đào tạo nâng cao nhận thức về an toàn thông tin cho nhân viên trong tổ chức để không tiết lộ các thông tin nhạy cảm qua điện thoại, email…
- Triển khai các giải pháp giới hạn vật lý như sử dụng ID, xác thực sinh trắc học, thuê bảo vệ, camera
- Đảm bảo "trash" được xử lý cẩn thận, giám sát các khu vực, cần trang bị các khóa vật lý
- Thực hiện đào tạo nhận thức nhiều lần, lặp đi lặp lại và kiểm tra thường xuyên các kết quả đào tạo
- …

Thank you & Any questions?