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

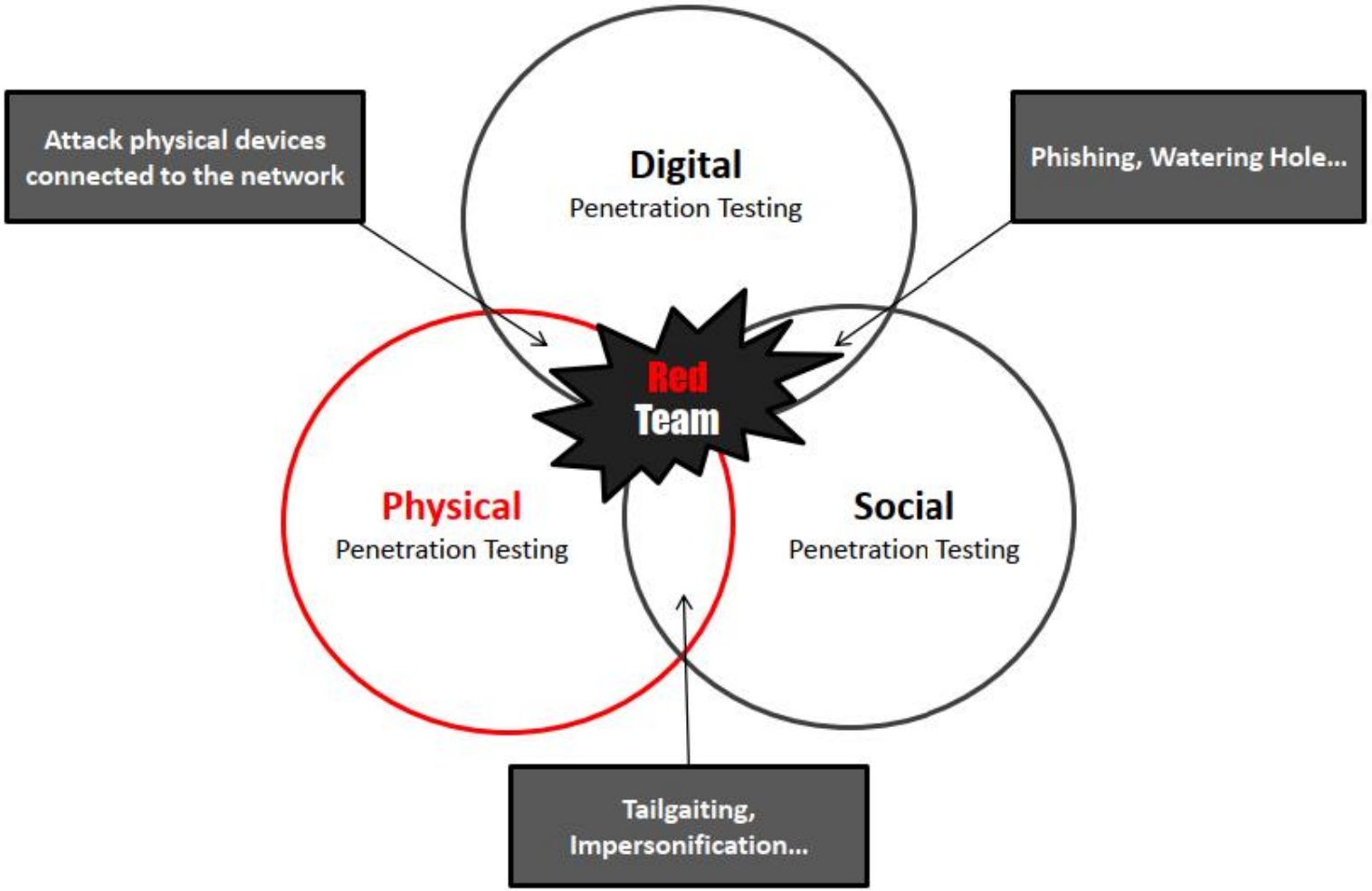
Khái niệm

- 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

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)

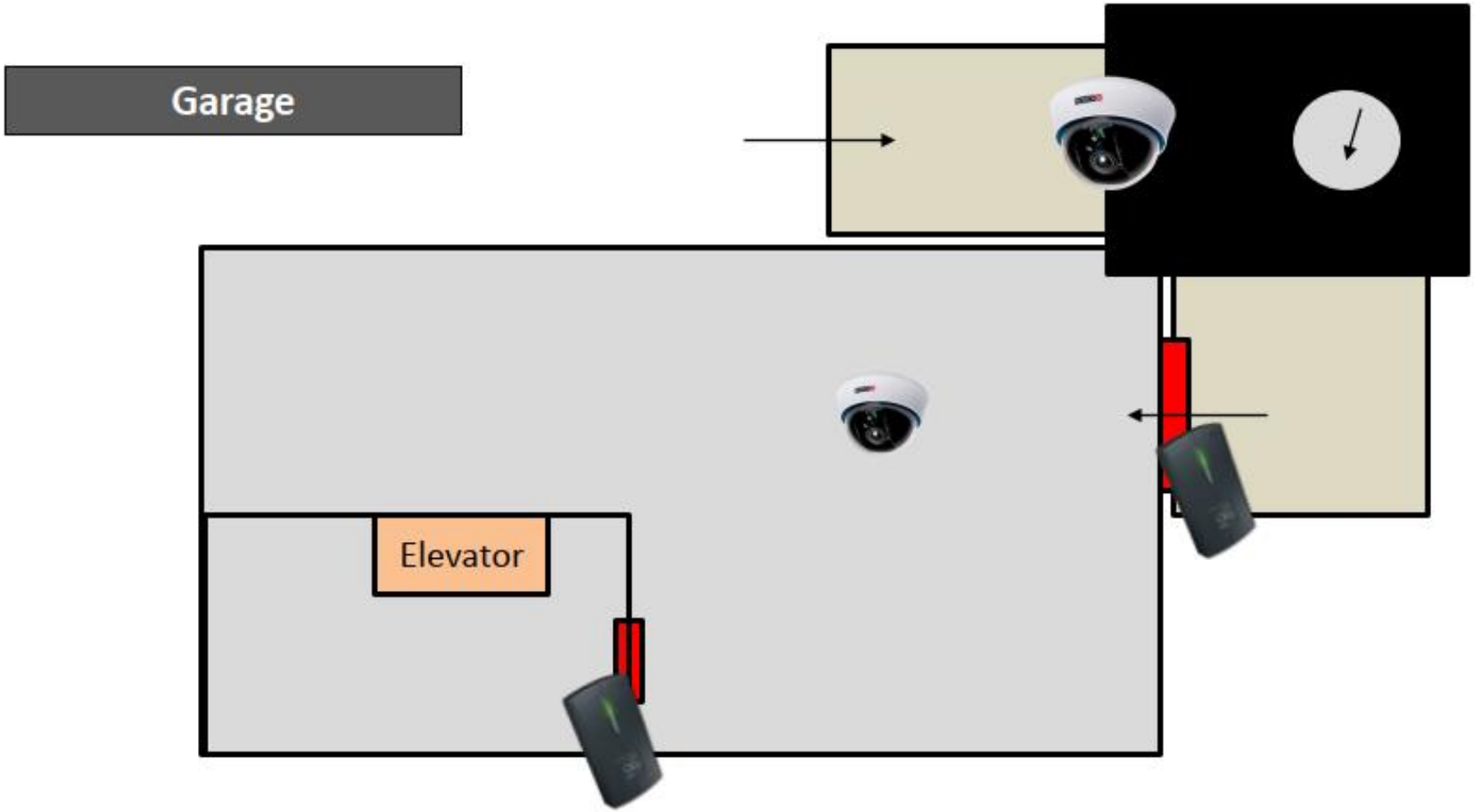
- Khai thác và truy cập mạng công ty (Red Team)
  - Cửa hậu vật lý (PwnPlg, Raspberry …)
  - Thiết bị bên ngoài (Keylogger, Network Sniffer …)
  - Truy cập vào các máy tính không được bảo vệ (Kon-Boot …)
  - Chặn cuộc gọi (Điện thoại và VoIP)
  - Các thiết bị phần cứng
- Lấy thông tin bí mật

Mục lục

Ví dụ (1)

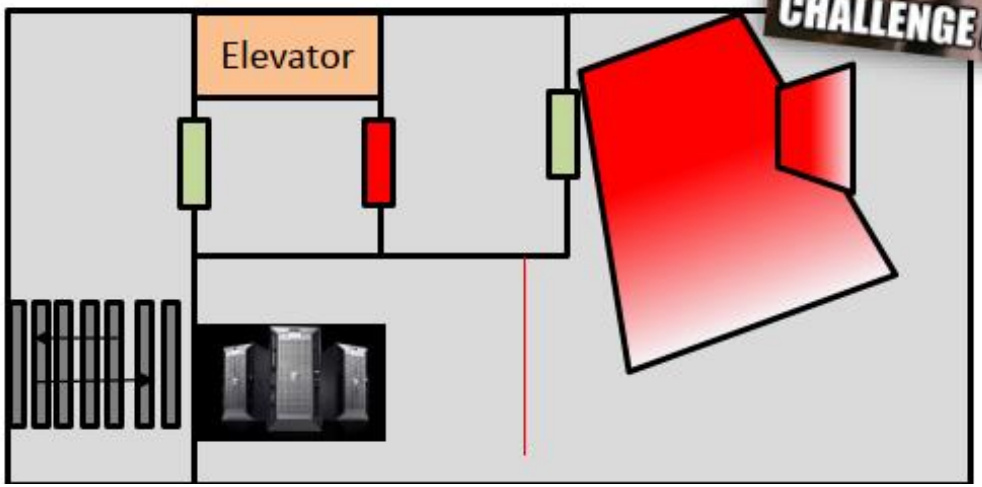
Ground floor

Ví dụ (2)



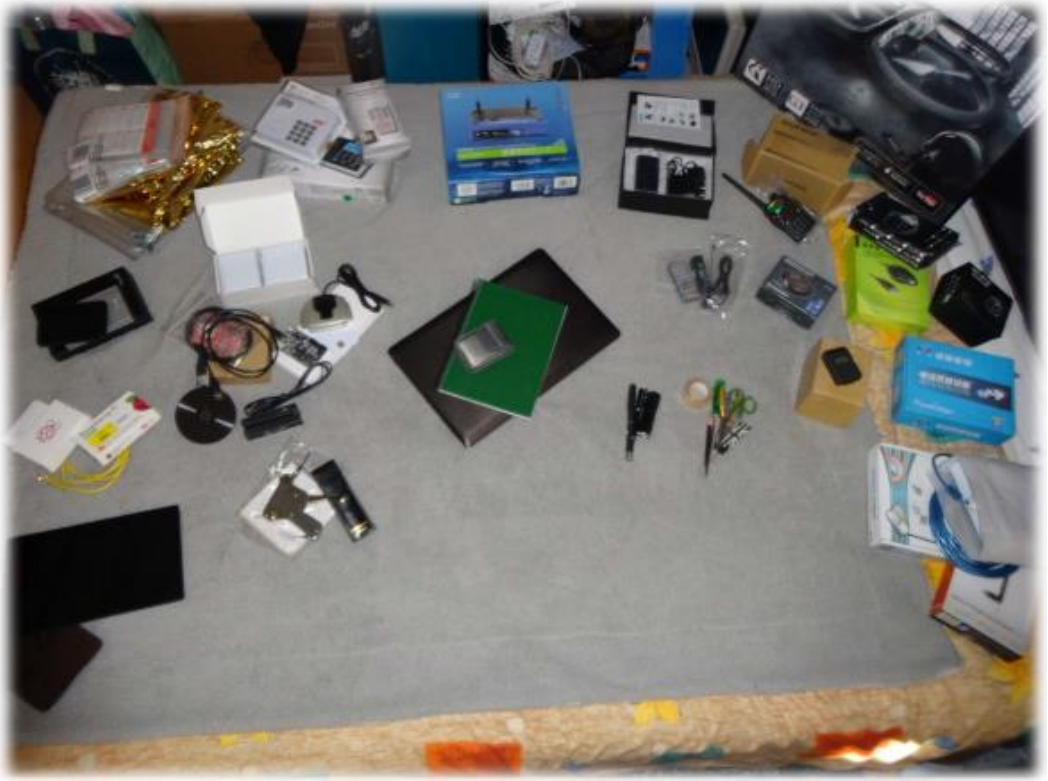
Ví dụ (3)

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

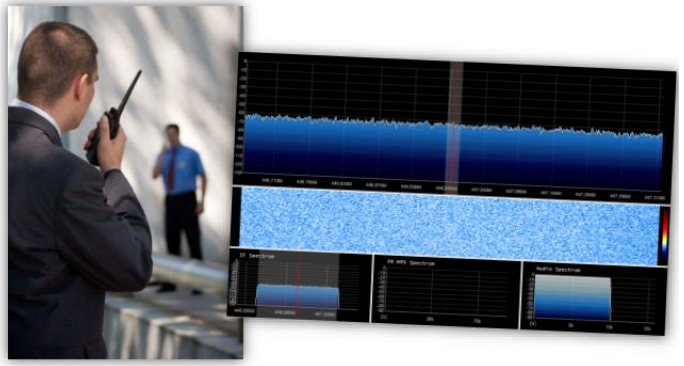
- Dumpster Diving

- Shoulder Surfing

VD: thu thập thông tin

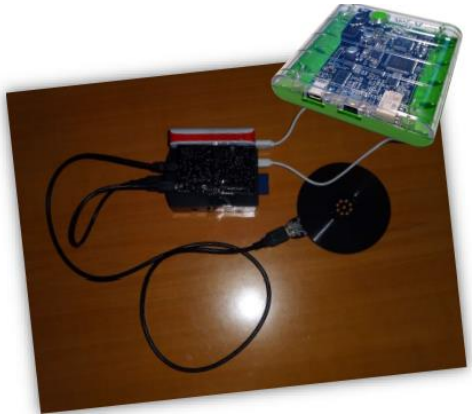
- Social Engineering

- 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

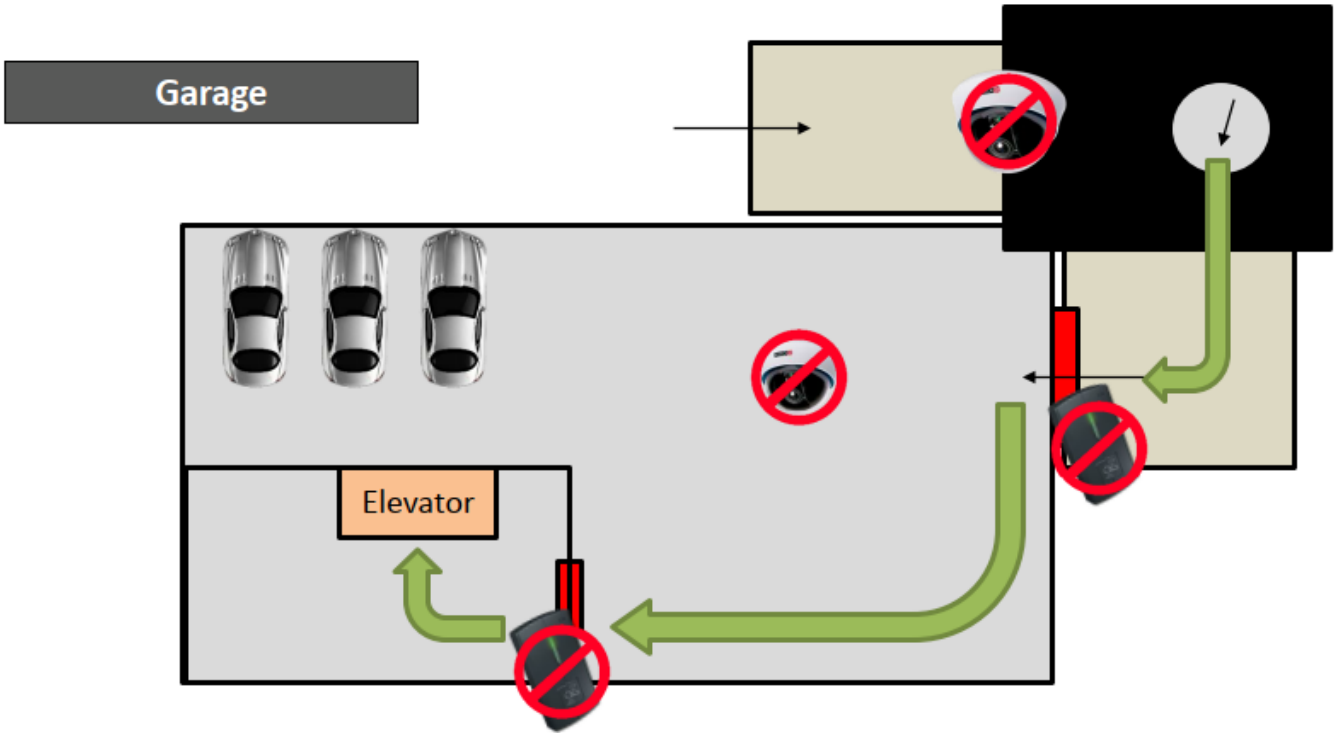
- Bypass of Photoelectric Sensor

- Bypass of Alarm System

VD: Vượt qua các biện pháp an ninh

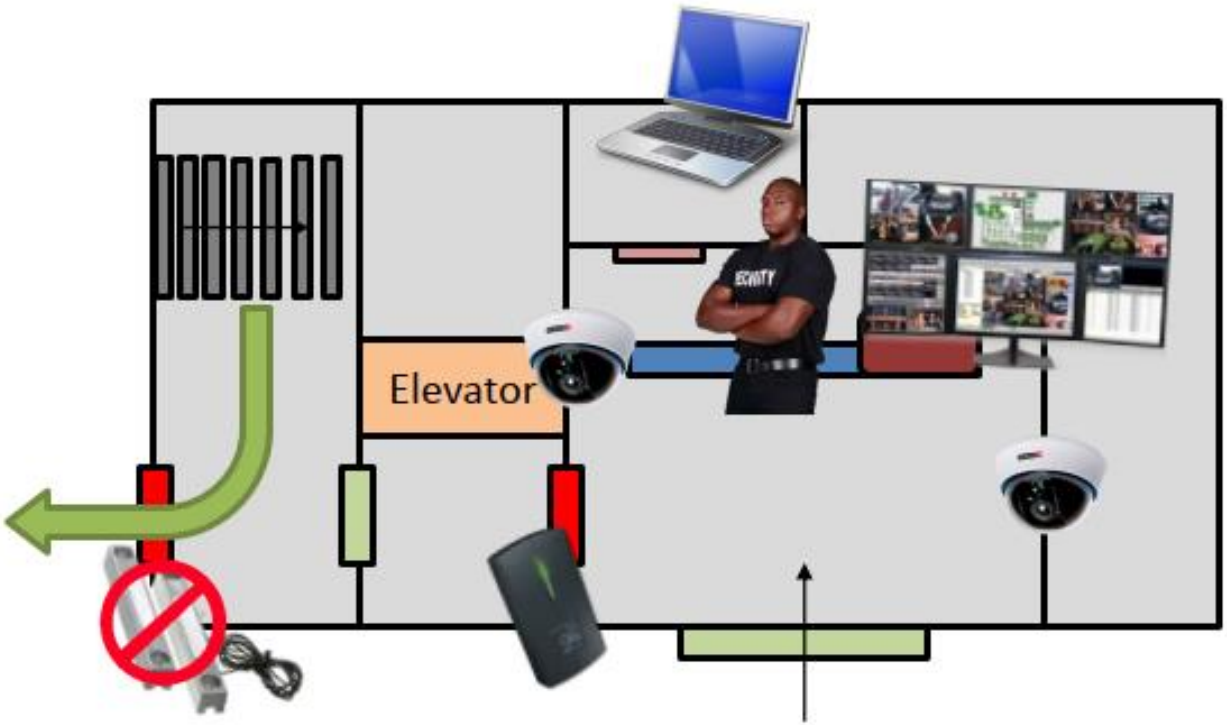
- Bypass of Magnetic Card / Keypad Access

Kết quả (1)



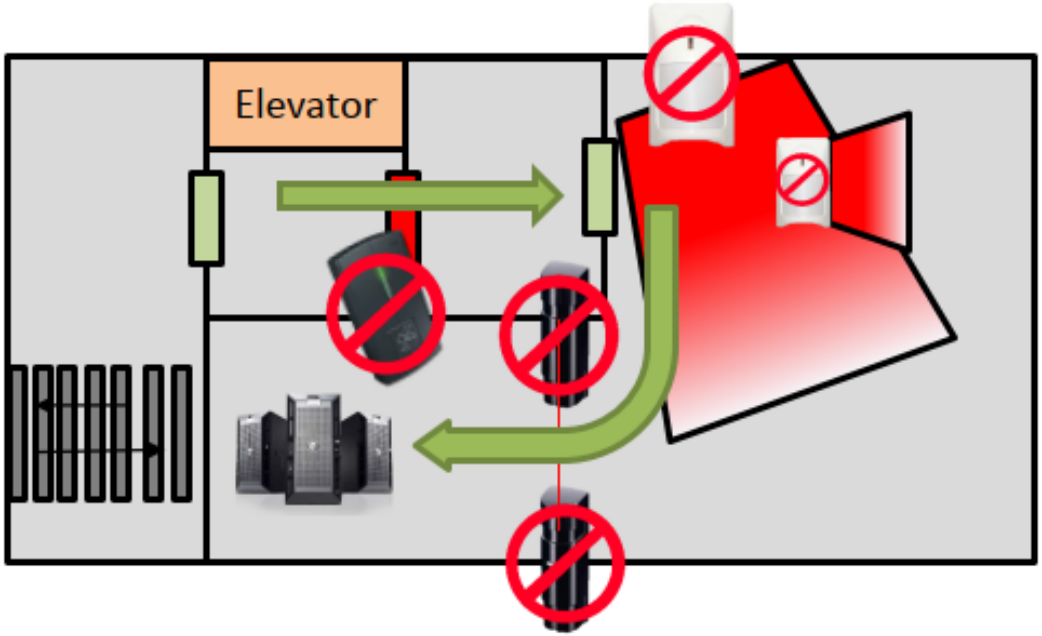
Kết quả (2)

Ground floor



Kết quả (3)

First Floor



Kết quả (4)

Ground floor

Mục lục

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.