Traffic Analysis

**I. Network Security**

+ Là tập hợp các hoạt động bảo vệ dữ liệu, ứng dụng, thiết bị và hệ thống được kết nối mạng

+ Tập trung: thiết kế hệ thống, vận hành/quản lý kiến trúc/cơ sở hạ tầng để cung cấp khả năng truy cập, tính toàn vẹn, tính liên tục và độ tin cậy của mạng

+ Phân tích lưu lượng (Traffic Analysis): miền phụ của network security; điều tra dữ liệu mạng

**II. Network Security và Network Data**

**1. Network Security**

**a) Base Network Security Control Levels:**

+ Physical: Ngăn chặn truy cập trái phép vào các thiết bị mạng, bảng cáp, khóa và tất cả các thành phần được liên kết

+ Technical: Ngăn chặn truy cập trái phép vào dữ liệu mạng (tunneling,…), triển khai các lớp bảo mật

+ Administrative: Kiểm soát bảo mật hành chính, đảm bảo tính nhất quán trong các hoạt động bảo mật như tạo chính sách, cấp độ truy cập và quy trình xác thực

**b) Main approaches:**

+ Access Control: Kiểm soát đảm bảo xác thực, ủy quyền

+ Threat Control: Phát hiện, ngăn chặn hoạt động bất thường, độc hại

\* Access Control key elements (yếu tố chính)

+ Firewall protection: Kiểm soát lưu lượng mạng bằng các quy tắc được xác định trước; ngăn chặn lưu lượng đáng ngờ (mối đe dọa độc hại ) ở lớp ứng dụng

+ NAC (network access control):

- Kiểm soát tính phù hợp của thiết bị trước khi truy cập mạng (thông số kỹ thuật, cấu hình,…)

+ IAM (Identify and Access Management): Kiểm soát, quản lý danh tính tài sản và quyền truy cập người dùng vào hệ thống dữ liệu và tài nguyên trên mạng

+ Load Balancing: Kiểm soát sử dụng tài nguyên => phân phối tài nguyên phù hợp, cải thiện luồng xử lý

+ Network Segmentation (Phân đoạn mạng): Tạo + kiểm soát phạm vi + phân đoạn mạng => cô lập mức độ truy cập của người dùng, nhóm và tài nguyên chung => bảo vệ dữ liệu trong mạng lớn

+ VPN: Tạo, kiểm soát giao tiếp được mã hóa giữa các thiết bị qua mạng (cho truy cập từ xa)

+ Zero Trust Model: Đề xuất cấu hình, triển khai quyền truy cập ở mức tối thiểu (cấp quyền khi cần thiết)

\* Thread Control key elements

+ IDS/IPS(hệ thống phát hiện xâm nhập): Kiểm tra lưu lượng và tạo cảnh báo (IDS) hoặc thiết lập lại kết nối (IPS) khi phát hiện bất thường mối đe dọa

+ DLP (Phòng ngừa mất dữ liệu): Kiểm tra lưu lượng truy cập (nội dung + ngữ cảnh dữ liệu trên đường truyền), chặn trích xuất dữ liệu nhạy cảm

+ Endpoint protection: Bảo về thiết bị đầu cuối bằng sử dụng phương pháp nhiều lớp (mã hóa, diệt virus, DLP, IDS/IPS)

+ Cloud Security: Bảo vệ cloud không rò rỉ dữ liệu (VPN,…)

+ SIEM (Security Event and Information Management): Phát hiện mối đe dọa, tuân thủ và quản lý sự cố bảo mật thông qua dữ liệu sẵn có (log) = phân tích sự kiện bối cảnh, để xác định các điểm bất thường, mối đe dọa và lỗ hổng

+ SOAR (Tự động hóa và phản hồi điều phối bảo mật): phối hợp, tự động hóa các tác vụ giữa nhiều người, công cụ và dữ liệu trong 1 nền tảng duy nhất => xác định các mối đe dọa bất thường, mối đe dọa lỗ hổng

+ Phân tích lưu lượng, phát hiện và phản hồi mạng: Kiểm tra lưu lượng => xác định bất thường

Hoạt động quản lý bảo mật mạng:

A screenshot of a white board

Description automatically generated

Dịch vụ bảo mật được quản lý (MSS)

A screenshot of a computer

Description automatically generated