1. Đặc tính an toàn thông tin + Ví dụ

- **Tính bí mật**: Chỉ người được phép mới truy cập (VD: mật khẩu email).
- **Tính toàn vẹn**: Dữ liệu không bị sửa đổi trái phép (VD: chữ ký số).
- **Tính sẵn sàng**: Dịch vụ luôn hoạt động (VD: website luôn truy cập được).
- **Tính xác thực**: Đảm bảo đúng danh tính người dùng (VD: đăng nhập 2 lớp).
- **Tính chống chối bỏ**: Không thể phủ nhận hành vi (VD: hóa đơn điện tử).

2. Phân biệt điểm yếu và lỗ hổng

Khái niệm	Giải thích	Ví dụ
Điểm yếu (Weakness)	Lỗi do thiết kế, cấu hình, phần cứng, phần mềm	Sử dụng mật khẩu mặc định, cấu hình sai
Lỗ hổng (Vulnerability)	Là điểm yếu có thể bị khai thác để tấn công	SQL Injection, Buffer Overflow

👉 Tóm lại:
Điểm yếu là nguyên nhân tiềm tàng,
Lỗ hổng là điểm yếu có thể bị hacker khai thác.

3. Phân biệt DoS và DDoS

- **DoS**: Một máy tấn công -> làm nghẽn dịch vụ.
- **DDoS**: Nhiều máy tấn công đồng thời -> làm tê liệt hệ thống.

4. 5 bước tấn công

1. Xác định mục tiêu
2. Trinh sát, thu thập thông tin
3. Cài cắm, ẩn náu
4. Lưu trữ, phát triển mã độc
5. Thực hiện tấn công

5. Đặc điểm các mô hình kiểm soát truy nhập

- Theo chính sách: Gán mức an ninh cho đối tượng.
- Theo luồng tin: Kiểm soát luồng dữ liệu giữa các mức.
- Theo phân quyền: Gán quyền cho chủ thể (thêm, sửa, xóa,...).

6. Khái niệm nén và mã hóa

- **Nén**: Giảm kích thước dữ liệu (VD: ZIP).
- **Mã hóa**: Biến đổi dữ liệu thành dạng không đọc được nếu không có khóa.

7. Nguyên lý nén RLC

Dựa trên việc **lặp lại liên tiếp** của một ký tự/màu.
Thay vì lưu: "AAAAAA" → lưu: "A6" (ký tự A, lặp 6 lần)
Hiệu quả khi dữ liệu có nhiều phần lặp (ảnh đen trắng, văn bản đơn giản)

8. Nguyên lý nén Huffman

1. Tính tần suất ký tự.
2. Tạo cây nhị phân từ tần suất.
3. Mã hóa: nhánh trái (0), nhánh phải (1).
   → Ký tự xuất hiện nhiều có mã ngắn.

9. Nguyên lý Shannon-Fano *(viết đúng là "Shannon-Fano Coding")*

- Tính xác suất các ký tự.
- Chia tập ký tự sao cho tổng xác suất 2 bên xấp xỉ bằng nhau.

- Gán mã nhị phân theo cây phân chia.

10. Cơ chế mã hóa bất đối xứng

- Dùng **cặp khóa**: công khai (public) và riêng tư (private).
- Mã hóa bằng khóa public → giải mã bằng private (và ngược lại).
  → Bảo mật và xác thực.

11. Cấu trúc cơ bản tường lửa

Chức năng: Kiểm soát lưu lượng ra/vào mạng

Cấu trúc cơ bản:

- **Giao thức (Protocol)**: TCP/UDP/ICMP
- **Cổng (Port)**: cổng nguồn và đích (VD: port 80 cho HTTP)
- **Địa chỉ IP**: nguồn và đích
- **Điều kiện**: thời gian, mức độ, nội dung

Ví dụ: Chặn tất cả truy cập từ ngoài vào port 22 (SSH)

12. Phân biệt HIDS và NIDS

Tiêu chí	**HIDS (Host-based)**	**NIDS (Network-based)**
Vị trí	Đặt tại máy chủ/thiết bị đầu cuối	Đặt tại mạng (switch, router, gateway)
Dữ liệu thu thập	File log, tiến trình, hành vi hệ thống	Gói tin di chuyển trong mạng
Ưu điểm	Nhận biết thay đổi hệ thống cụ thể	Phát hiện tấn công trên toàn mạng
Nhược điểm	Dễ bị bỏ sót nếu hacker xóa log	Khó phát hiện tấn công mã hóa

13. Hai cách phát hiện xâm nhập (IDS/IPS)

Phương pháp	**Chi tiết**
Dựa trên chữ ký (Signature-based)	So sánh với mẫu tấn công đã biết. Nhanh, chính xác nhưng không phát hiện được kiểu tấn công mới.
Dựa trên bất thường (Anomaly-based)	Xây dựng hành vi chuẩn → cảnh báo khi lệch chuẩn. Phát hiện được tấn công mới, nhưng có thể báo sai.

II. Bài tập

1. Cho chuỗi (VD: ptit@1234). Tính E?
   E = log2(R ^ l) = l * log2(R)

   l(length) = 9
   R = R1(Chữ hoa) + R2(Chữ thường) + R3(Số) + R4(Kí tự)
   = 0 + 3 + 4 + 1 (Thay @ bằng kí tự bất kì => R4 = 32)

2. Mô hình BLP/BiBa
   Si = { 3, 2, 2, 1 }
   Oj = { 3, 1, 2, 1 }

Vẽ ma trận truy nhập

L3 S1-----O1----------
L2 S2 ----O3----------S3

L1 S1-----O2-----O4------

3. Mô hình Index Henry????

$$I = \frac{Ri + Rr + Lt + Lm + Lp + 1}{Rt + Rm + Rp + Li + Lr + 1}$$

16 8 4 2 1 (Hệ số)

4. Tính Mel: Cho dải tần 300Hz -> 8000Hz. Tính 4 vector

- Đổi sang đơn vị Mel: M(f) = 1125 * ln(1 + f/700)

=> 300Hz = 401.25 (Mel1)

8000Hz = 2835 (Mel2)

- Số khoản = Số vector + 1 = n

$$\text{delta} = \frac{\text{Mel2} - \text{Mel1}}{n} = 221$$

- m[i] = { 401, 401 + 221 = 622, 622 + 221 = 843,....., Mel2 }
- Chuyển về tần số:

h[i] = 700 * [exp(m[i] / 1125 - 1)]

h[i] = { 300, 517, 782,...., 8000 }

- Tính vector:

$$f[i] = \text{floor}\left[\frac{(FFT\_size + 1) * h[i]}{f\_R}\right]$$

f_R = 2 * f_Max

=> f[i] = { 9, 16, 25, 35, 47, 63 }

--9----16------25----------35--------------47----------------63

5. Cho K = '123'

Counter = 3min 20s

Block = 5

IN/OUT = 1

Hash = Tổng % 256

Tính OTP 4 số?

- Đổi ra giây: C1 = 3 * 60 + 20 = 200

C = C1/30 = 7 (Chuyển sang hệ 16)

- K = '123' = (31, 32, 33) (Chuyển sang hệ 16)

=> (31, 32, 33, 00, 00) (Thêm cho đủ 5 byte)

- KQ1 = K XOR IN

31 32 33 00 00

= XOR

01 01 01 01 01

= 30 33 32 01 01 + 00 00 00 00 07 (Nối với C)

=> f(KQ1) = 158 % 256 = 9E (Hệ 16)

- KQ2 = K XOR OUT
= 30 33 32 01 01

KQ2 = KQ2 + KQ1 (Nối với KQ1)
= { 30, 33, 32, 01, 01, 9E }

=> f(KQ2) = sum(Byte) % 256 = 309 % 256 = 53 = 35 (Hệ 16)

- f(KQ2) = { 00, 00, 00, 00, 35 } (Hệ 16)
Lấy 4 byte cuối = 53
OTP = 53 % 10000 = 0053