Lê Ngọc Kiều Anh - 22520047

**BÀI TẬP AN TOÀN MẠNG BUỔI 12**

**Câu 1. Nêu các đặc điểm của SSID**

***Trả lời:***

SSID (Service Set Identifier) là tên mạng không dây (Wi-Fi) được dùng để xác định một mạng trong số các mạng Wi-Fi có sẵn. Các đặc điểm chính của SSID bao gồm:

- SSID là một chuỗi ký tự dài tối đa **32 ký tự** (gồm cả chữ cái, số, và ký tự đặc biệt).

**- Mỗi mạng Wi-Fi sẽ có một SSID** để người dùng dễ dàng nhận diện và kết nối.

**- Dễ dàng thay đổi**: người quản trị mạng có thể thay đổi SSID của mạng không dây bất kỳ lúc nào để phân biệt với mạng khác hoặc vì lý do bảo mật.

**- Công khai hoặc ẩn:**

+ SSID có thể được cấu hình ở chế độ broadcast, cho phép mọi thiết bị trong phạm vi tìm thấy mạng.

+ SSID cũng có thể được cấu hình ẩn để tăng tính bảo mật, nhưng điều này không bảo vệ mạng hoàn toàn.

**- Bảo mật:** dù SSID không phải là yếu tố bảo mật chính, nhưng tên mạng quá đơn giản (như “admin” hoặc “default”) có thể bị tấn công dễ dàng hơn.

**- Phạm vi phủ sóng:** SSID thuộc về một mạng không dây cụ thể nên chỉ khả dụng trong pham vi phủ sóng của router hay điểm truy cập.

**Câu 2. Tại sao nói WEP là phương thức mã hóa yếu?**

***Trả lời:***

WEP (Wired Equivalent Privacy) là giao thức bảo mật mạng Wi-Fi ra đời từ năm 1997. Tuy nhiên, nó được coi là yếu vì những lý do sau:

- WEP sử dụng khóa mã hóa tĩnh (40-bit hoặc 104-bit): khóa này không thay đổi trong suốt thời gian kết nối dẫn đến việc dễ bị tấn công khi kẻ xấu thu thập đủ lượng dữ liệu bằng cách sử dụng các công cụ như Aircrack-ng.

**- IV (Initialization Vector) dễ đoán**: IV được sử dụng để đảm bảo mỗi gói dữ liệu có mã hóa khác nhau, nhưng trong WEP, IV quá ngắn (24-bit) và dễ lặp lại, giúp hacker dễ phân tích và giải mã dữ liệu.

**- Không kiểm tra tính toàn vẹn dữ liệu hiệu quả**: WEP sử dụng thuật toán kiểm tra CRC-32 để phát hiện lỗi trong dữ liệu, nhưng thuật toán này không đủ mạnh để chống lại các tấn công sửa đổi dữ liệu.

**- Không bảo vệ chống lại tấn công Replay(tái sử dụng gói dữ liệu đã được truyền trước đó): gây gián đoạn hoặc chiếm quyền điều khiển kết nối.**

**- Yêu cầu người dùng nhập khóa mã hóa chung (shared key) nên khi 1 thiết bị bị xâm nhập, toàn bộ mạng sẽ bị nguy hiểm.**

**Câu 3. Lập bảng tổng hợp các chuẩn mã hóa mạng không dây (tên, giải thuật mã hóa, đặc điểm, phương thức hoạt động, độ an toàn,…).**

***Trả lời:***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tên** | **Giải thuật mã hóa** | **Đặc điểm** | **Phương thức hoạt động** | **Độ an toàn** |
| **802.11a** | **WEP, WPA** | **- Băng thông lên đến 54 Mbps.  - Hoạt động ở tần số 5 GHz, ít nhiễu hơn 2.4 GHz.** | **Sử dụng phổ tần số 5 GHz để truyền tín hiệu Wi-Fi.** | **Trung bình nếu dùng WEP.** |
| **802.11b** | **WEP, WPA** | **- Băng thông tối đa 11 Mbps.  - Sử dụng tần số 2.4 GHz, dễ bị nhiễu từ các thiết bị khác.** | **Sử dụng tần số không cần cấp phép (unlicensed).** | **Yếu nếu dùng WEP.** |
| **802.11g** | **WEP, WPA, WPA2** | **- Băng thông tối đa 54 Mbps.  - Sử dụng tần số 2.4 GHz, có thể thay thế 802.11b.** | **Tương thích ngược với 802.11b, tăng tốc độ.** | **Tốt nếu dùng WPA2.** |
| **802.11i** | **WPA2 (AES)** | **- Tăng cường bảo mật so với WEP và WPA.  - Sử dụng chuẩn mã hóa AES (mạnh hơn TKIP).** | **Cung cấp mã hóa AES cho các mạng WLAN hiện có.** | **Rất cao nếu dùng WPA2.** |
| **802.11n** | **WPA, WPA2** | **- Băng thông trên 100 Mbps (tối đa 600 Mbps).  - Hỗ trợ MIMO để tăng tốc độ và vùng phủ sóng.** | **Sử dụng đồng thời tần số 2.4 GHz và 5 GHz.** | **Cao nếu dùng WPA2.** |
| **802.16 (WiMAX)** | **AES** | **- Được thiết kế cho mạng MAN (Metropolitan Area Networks).  - Hỗ trợ truyền dữ liệu xa và băng rộng.** | **Sử dụng truyền dẫn băng rộng không dây cho các khu vực lớn.** | **Cao (ứng dụng doanh nghiệp).** |
| **Bluetooth** | **Không mã hóa, hoặc AES** | **- Tầm phủ sóng ngắn (~10 mét).  - Tốc độ thấp (1-3 Mbps), chủ yếu cho thiết bị cầm tay.** | **Kết nối nhanh qua giao thức không dây năng lượng thấp.** | **Trung bình nếu không mã hóa.** |
| **WEP** | **RC4** | **Khóa 40 bit hoặc 104 bit.** | **Mã hóa gói tin bằng RC4.** | **Rất yếu, dễ bị tấn công.** |
| **WPA** | **TKIP + RC4** | **- Cải tiến từ WEP.  - Dùng khóa động (temporal key).** | **Thay đổi khóa liên tục.** | **Trung bình, nhưng lỗi thời.** |
| **WPA2** | **AES (CCMP)** | **- Sử dụng thuật toán AES mạnh mẽ.  - Chuẩn bảo mật cao.** | **Thay thế TKIP bằng CCMP.** | **Cao, tiêu chuẩn phổ biến.** |
| **WPA3** | **AES (GCMP-256)** | **- Bảo vệ chống tấn công brute force.  - OWE cho mã hóa mở.** | **Sử dụng mã hóa mạnh hơn.** | **Rất cao, chuẩn mới nhất.** |