Câu 1.

* SSID là 1 token để định dạng 1 mạng Wifi (802.11): theo mặc định đây là một phần của tiêu đề gói được gửi qua mạng cục bộ không dây (wlan).
* SSUD chỉ giữ bí mật trên các mạng đóng và không có hoạt động nào, điều này gây bất tiện cho người dùng hợp pháp.
* Chế độ truy cập không an toàn cho phép khách hàng kết nối với điểm truy cập bằng SSID đã cấu hình, SSID trống hoặc SSID được cấu hình là "bất kỳ”
* Nếu SSID của mạng bị thay đổi, cần phải cấu hình lại SSID trên mọi mạng vì mọi người dùng mạng đều cấu hình SSID vào hệ thống của họ.
* Nó hoạt động như một mã định danh được chia sẻ duy nhất giữa các điểm truy cập và máy khách.
* Các điểm truy cập SSID phát các tín hiệu vô tuyến mà máy khách nhận được liên tục nếu được kích hoạt.
* Một vấn đề về quản lý khóa được tạo ra cho quản trị viên mạng vì SSID là khóa bí mật thay vì khóa chung.
* SSID là một chuỗi ký tự duy nhất, có độ dài tối đa 32 ký tự. Ký tự có thể là chữ cái, chữ số và các ký tự đặc biệt như dấu chấm, dấu cách, dấu gạch ngang.
* SSID được sử dụng để xác định một mạng Wi-Fi. Khi người dùng tìm kiếm mạng Wi-Fi, họ sẽ thấy danh sách các SSID có sẵn trong khu vực.
* SSID được phát sóng bởi các điểm truy cập Wi-Fi. Điều này cho phép các thiết bị Wi-Fi khác tìm thấy mạng và kết nối với nó.
* SSID có thể được thay đổi bởi người quản trị mạng. Điều này có thể được thực hiện để tăng cường bảo mật hoặc để thay đổi tên mạng.

Câu 2:

1. Khoa ngắn: WEP sử dụng khóa có độ dài chỉ 40 hoặc 104 bit, làm cho nó dễ bị dò tìm và tấn công brute force (cố gắng tất cả các khả năng kết hợp khóa một cách tuần tự).
2. Quy trình khởi tạo không an toàn: Quy trình khởi tạo khóa của WEP có các lỗ hổng bảo mật, làm cho nó dễ bị tấn công và phá vỡ.
3. Khoá mã hoá tĩnh: các gói mã hóa không tránh được hiện tượng bị chặn, kẻ nghe trộm hoàn toàn có thể chặn đủ số lượng gói tin đã mã hoá để tìm ra được khoá giải mã là gì
4. WEP sử dụng phương thức mã hóa dòng RC4. Phương thức mã hóa này có một số lỗ hổng có thể được khai thác để bẻ khóa WEP.
5. Thiếu tính nhất quán trong phân phối khóa: WEP không cung cấp cơ chế hiệu quả cho việc phân phối khóa an toàn, làm cho nó dễ bị tấn công trực tiếp hoặc thông qua quy trình quản lý khóa yếu.

Câu 3:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tên | Giải thuật mã hóa | Đặc điểm | Phương thức hoạt động | Độ an toàn |
| WEP | RC4 | - Khóa ngắn (40/104 bit) | - Sử dụng IV (Initialization Vectors), khởi tạo không an toàn | Rất yếu, không được khuyến khích sử dụng |
| WPA | TKIP, RC4 | - Sử dụng phương pháp tạm thời | - Thay đổi khóa theo thời gian, sử dụng MIC (Message Integrity Code) | Tốt hơn WEP nhưng vẫn có thể bị bẻ khóa bằng các phương pháp tiên tiến |
| WPA2 | AES-CCMP | - Sử dụng AES, một giải thuật mã hóa mạnh mẽ | - Thay đổi khóa theo thời gian, sử dụng CCMP | An toàn đối với hầu hết các ứng dụng Wi-Fi |