Môn học: Nhập môn Mạng máy tính

LAB 6. BẮT GÓI TIN & DÒ TÌM MẬT KHẨU WPA/WPA2

Câu 1: Hãy trình bày những chuẩn bảo mật Wi-Fi phổ biến (WPE, WPA, WPA2, WPA3). Cho biết làm thế nào để xem wifi mình đang truy cập sử dụng chuẩn bảo mật nào? Kiểm tra xem máy bạn đang sử dụng chuẩn bảo mật wifi nào (thực hiện và chụp lại màn hình).

WEP (Wired Equivalent Privacy)

Tháng 9/1999, Wifi Alliance giới thiệu WEP như là phương thức bảo mật tiêu chuẩn cho wifi. Như cái tên của mình, WEP sử dụng giao thức bảo mật kết nối tương tự giao thức sử dụng với hệ thống mạng có dây. Ngay tại thời điểm ra mắt, WEP là một giải thuật bảo mật cho mạng không dây chuẩn IEEE 802.11, không hề là một chuẩn bảo mật mạnh do nó chỉ dùng 64 bit, mã hóa theo quy định của chính phủ mỹ với xuất khẩu công nghệ mã hóa. Sau này khi chuẩn WEP được cải tiến với 128, thậm chí 256 bit mã hóa, vẫn có những lỗ hổng rất lớn khác trong giao thức bắt tay giữa Client (máy trạm) và AP (Access Point-điểm truy cập) khiến WEP trở thành một chuẩn yếu và dễ dàng bị hack bởi các tin tặc. Ngoài ra, người ta còn dễ dàng hack được các wifi có chuẩn bảo mật yếu như WEP với các phiên bản miễn phí trên mạng. Vào năm 2004, IEEE tuyên bố ngừng hỗ trợ chuẩn WEP trong bảo mật wifi.

WPA (Wi-Fi Protected Access)

Năm 2003 Wifi alliance giới thiệu WPA với vai trò chuẩn bảo mật mới thay thế WEP với WPA-PSK (pre-shared) hiện nay là phiên bản phổ biến nhất. Cái rõ rệt của WPA so với WEP là khả năng kiểm tra tính toàn vẹn của gói tin (message integrity check) xác định liệu dữ liệu có bị Hacker đánh chặn và thay đổi trong quá trình

truyền dẫn giữa Client-AP hay không. Bên cạnh đó, giao thức TKIP (Temporal Key Integrity Protocol) cho phép gửi nhận dữ liệu an toàn hơn nhiều nhờ hệ thống kí tự riêng cho từng gói tin thay vì bộ kí tự cố định như WEP. Tuy vậy, do việc phân phối các bản cập nhật cho TKIP vẫn được diễn ra dựa trên hệ thống WEP cũ, vẫn còn đó những lỗ hổng mà hacker có thể khai thác.

WPA 2 (WiFi Protected Access II)

Năm 2006, WPA2 ra đời và chính thức thay thế WPA. Điểm cải tiến mạnh nhất của WPA2 là hỗ trợ giao thức AES (Advance Encryption Standard) thay cho TKIP. Ngoài việc sử dụng giao thức AES, thì WPA 2 còn sử dụng thêm giao thức mã hóa CCMP (CTR mode with CBC-MAC Protocol). Giao thức CCMP là một giao thức truyền dữ liệu và kiểm soát tính truyền dữ liệu thống nhất để bảo đảm cả tính bảo mật và nguyên vẹn của dữ liệu được truyền đi. Đến phiên bản này, gần như không còn lỗ hổng bảo mật hiện hữu nào để Hacker khai thác. Nhưng an toàn hơn không có nghĩa là an toàn tuyệt đối, với một máy tính đủ mạnh và thời gian, ngay cả chuẩn bảo mật mạnh như WPA2 cũng có thể bị bẻ khóa.

WPA 3 (WiFi Protected Access III)

WPA3 sở hữu một số cải thiện quan trọng cho bảo mật không dây hiện đại, bao gồm:

Bảo vệ khỏi các cuộc tấn công Brute Force: WPA3 sẽ bảo vệ người dùng, ngay cả khi họ dùng mật khẩu yếu, khỏi các cuộc tấn công Brute Force.

Bảo mật mạng công cộng: WPA3 bổ sung mã hóa dữ liệu cá nhân, theo lý thuyết, mã hóa kết nối của người dùng đến điểm truy cập không dây, dù có mật khẩu hay không.

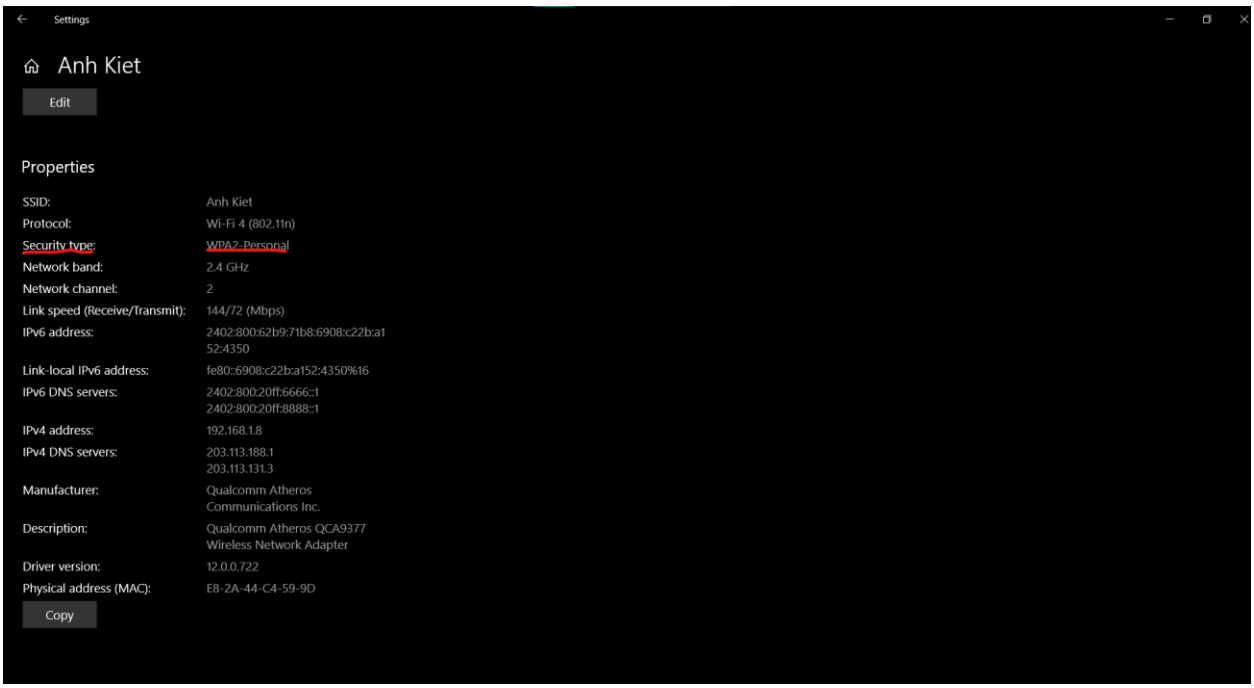
Bảo mật Internet of Things: WPA3 xuất hiện vào thời điểm các nhà phát triển thiết bị Internet of Things đang phải chịu áp lực rất lớn để cải thiện bảo mật cơ sở.

Mã hóa mạnh hơn: WPA3 bổ sung mã hóa 192-bit mạnh hơn nhiều, cải thiện đáng kể mức độ bảo mật.

Kiểm tra máy tính đang sử dụng chuẩn nào:

Chọn thanh mục wifi trên thanh taskbar và chọn mục Properties của wifi đang sử dụng

Sau khi chọn Properties thì sẽ hiện ra bảng Settings, cuộn xuống cuối cùng và kiểm tra mục Security Type, khi ấy sẽ thấy được phiên bản bảo mật wifi đang sử dụng là phiên bản nào (như hình là phiên bản WPA2)



Câu 2: Tìm hiểu về quá trình bắt tay 4 bước trong WPA/WPA2

Quá trình thực hiện bắt tay 4 bước sẽ gồm:

Bước 1: Điểm truy cập sẽ gửi một giá trị (ngẫu nhiên) đến máy khách khi được yêu cầu truy cập.

Bước 2: Máy khách tạo 1 khóa và gửi giá trị ngẫu nhiên dưới dạng mã của nó để xác nhận giá trị mà Điểm truy cập đã gửi.

Bước 3: Điểm truy cập tạo một khóa, (trong trường hợp cần thiết, Điểm truy cập sẽ gửi lại một khóa và một mã xác minh khác).

Bước 4: Máy khách gửi lại một tin nhắn xác nhận.

Câu 3: Brute force attack là gì? Nêu ưu và nhược điểm của phương pháp này? Hãy kể tên và mô tả những Phương pháp brute force phổ biến mà bạn biết?

Brute Force Attack là hình thức tấn công mạng, trong đó tin tặc sử dụng phần mềm để "trộn" các ký tự khác nhau thành mật khẩu đúng. Theo đó, chúng sẽ gửi các truy vấn đăng nhập vào file wp-login.php và thử mật khẩu. Quá trình này diễn ra liên tục cho đến khi tin tặc đăng nhập thành công. Việc bẻ khóa mật khẩu có thể mất từ vài giây cho đến vài ngày hoặc vài tháng, tùy vào độ phức tạp của mật khẩu. Hình thức tấn công Brute Force chính là để tìm ra mật khẩu và tài khoản của người quản trị cao nhất

Ưu điểm:

Phương pháp thủ công

Tính đơn giản của việc triển khai thuật toán

Có được nhiều bản hỗ trợ trên mạng

Nhược điểm:

Độ phức tạp của thuật toán rất lớn nếu mật khẩu đủ mạnh

Phụ thuộc vào tốc độ xử lý của máy tính

Thường tốn nhiều thời gian để dò mật khẩu mạnh

Các phương pháp Brute force phổ biến:

Simple Brute Force Attacks: Hacker cố gắng đoán một cách hợp lý thông tin đăng nhập của bạn – hoàn toàn không được hỗ trợ từ các công cụ phần mềm hoặc các phương tiện khác. Chúng có thể tiết lộ mật khẩu và mã PIN đơn giản. Ví dụ: mật khẩu được đặt là "guest12345".

Dictionary Attacks: Các cuộc tấn công từ điển là công cụ cơ bản nhất trong các cuộc tấn công brute force. Mặc dù không nhất thiết phải là các cuộc tấn công Brute Force, nhưng chúng thường được sử dụng như một thành phần quan trọng để bẻ khóa mật khẩu. Một số tin tặc chạy qua các từ điển không kết hợp và bổ sung các từ bằng các ký tự và chữ số đặc biệt hoặc sử dụng các từ điển từ đặc biệt, nhưng kiểu tấn công tuần tự này rất phức tạp.

Hybrid Brute Force Attacks: Hacker lợi dụng các thông tin bên ngoài và của bạn để một cách logic của họ để cố gắng lấy thông tin đăng nhập. Một cuộc tấn công hỗn hợp thường kết hợp các cuộc tấn công từ điển và brute force. Các cuộc tấn công này

được sử dụng để tìm ra mật khẩu kết hợp trộn các từ phổ biến với các ký tự ngẫu nhiên. Một ví dụ về cuộc tấn công vũ phu về bản chất này sẽ bao gồm các mật khẩu như NewYork1993 hoặc Spike1234.

Reverse Brute Force Attacks: Đây là một hình thức tấn công đảo ngược chiến lược tấn công bằng cách bắt đầu với một mật khẩu đã biết. Sau đó, hacker tìm kiếm hàng triệu tên người dùng cho đến khi họ tìm thấy một kết quả trùng khớp. Nhiều tên tội phạm trong số này bắt đầu với mật khẩu bị rò rỉ có sẵn trực tuyến từ các vi phạm dữ liệu hiện có.

Credential Stuffing: Nếu một hacker có tổ hợp tên người dùng và mật khẩu hoạt động cho một trang web, họ cũng sẽ thử nó cho rất nhiều trang web khác. Vì người dùng đã được biết là sử dụng lại thông tin đăng nhập trên nhiều trang web, họ là mục tiêu độc quyền của một cuộc tấn công như thế này.

Câu 4: Trình bày Phương pháp dictionary attack? Bạn biết gì về Phương pháp này? So sánh dictionary attack với brute force attack.

Là một kỹ thuật hay phương pháp sử dụng để vi phạm bảo mật máy tính của một máy được bảo vệ bằng mật khẩu hoặc máy chủ. Một từ điển nỗ lực tấn công để đánh bại một cơ chế xác thực bằng cách nhập một cách hệ thống mỗi từ trong một cuốn từ điển như một mật khẩu hoặc cố gắng để xác định khóa giải mã của một thông điệp được mã hóa hoặc tài liệu. các cuộc tấn công từ điển thường thành công vì nhiều người sử dụng và các doanh nghiệp sử dụng các từ thông thường như mật khẩu. Những lời nói bình thường có thể dễ dàng tìm thấy trong một cuốn từ điển, chẳng hạn như một cuốn từ điển tiếng Anh.

Phương pháp phổ biến nhất của chứng thực người dùng trong một hệ thống máy tính là thông qua một mật khẩu. Phương pháp này có thể tiếp tục trong nhiều thập kỷ hơn bởi vì nó là cách thuận tiện nhất và thực tiễn của chứng thực người dùng. Tuy nhiên, đây cũng là hình thức yếu nhất xác thực, bởi vì người dùng thường xuyên sử dụng các từ thông thường như mật khẩu. người sử dụng đối kháng như hackers và spammers tận dụng điểm yếu này bằng cách sử dụng một cuộc tấn công từ điển. Hacker và spam cố gắng đăng nhập vào hệ thống máy tính bằng cách cố gắng tất cả mật khẩu càng tốt cho đến khi một chính xác được tìm thấy.

Dictionary attack	Brute force attack
Giống nhau: Cả hai đều là các kiểu tấn công an ninh mạng phổ biến khi đó kẻ tấn công cố gắng đăng nhập vào tài khoản của người dùng bằng cách kiểm tra một cách có hệ thống và thử tất cả các mật khẩu và cụm mật khẩu có thể có cho đến khi tìm thấy mật khẩu chính xác. Các cuộc tấn công brute-force và dictionary là phổ biến, do số lượng lớn các cá nhân sử dụng lại các biến thể mật khẩu phổ biến.	
Sử dụng phương pháp phỏng đoán những từ có trong từ điển tiếng Anh, tiếng Việt,… từ đó có thể dò ra được mật khẩu Số lượng từ có giới hạn nên tốc độ xử lý nhanh hơn brute force Cần phải có chuẩn bị một bộ từ ngữ từ trước	Sử dụng thuật toán để để vét cạn tất cả các trường hợp của mật khẩu đó sử dụng Số lượng từ không giới hạn nên tốc độ xử lý chậm hơn Dictionary attack Không cần có bộ từ ngữ từ trước

Câu 5: Ở vai trò là 1 chuyên gia IT và người dùng mạng bạn sẽ áp dụng những phương pháp nào để bảo vệ mật khẩu của bản thân, bảo vệ hệ thống an ninh mạng chống lại brute force attack và dictionary attack? Hãy trình bày những phương pháp đó?

Đặt mật khẩu không nằm trong bộ từ điển hoặc quá thông dụng đối với người dùng thông thường.

Mật khẩu phải có độ mạnh nhất định dựa theo thang đo mật khẩu.

Thường xuyên thay đổi mật khẩu và chặn những truy cập lạ.

Giới hạn số lần truy cập nếu sai.

Sử dụng các công cụ quản lý mật khẩu đáng tin cậy như Google, Samsung, iCloud,…

Sử dụng công cụ quản lý đăng nhập do bên thứ ba quản lý như Facebook, Google,…

Câu 6: Ở trang 10 của lab 6 có trình bày: "Có thể sử dụng phương pháp dò tìm theo Wordlist hay thực hiện Brute-force để dò tìm mật khẩu Wi-Fi? Hãy so sánh ưu và nhược điểm của 2 phương pháp này.

Brute force

Ưu điểm: Đơn giản, dễ thiết lập, được hỗ trợ rất nhiều công cụ sẵn trên mạng

Khuyết điểm: Độ phức tạp thuật toán cao nếu mật khẩu đặt có độ mạnh cao tốn nhiều thời gian mới có thể tìm ra được mật khẩu

Word list

Ưu điểm: Có thể phỏng đoán từ ngữ dựa trên danh sách từ có sẵn, dễ dàng truy vấn được nahnh chóng.

Khuyết điểm: Không thể tìm được mật khẩu nếu như từ đó không nằm trong danh sách từ ngữ có sẵn.

Câu 7: Theo bạn, mình cần làm gì để bảo mật cho Wi-Fi của nhà mình? Hãy kể ra các cách bạn sẽ làm để tăng độ bảo mật cho Wi-Fi nhà mình?

Đặt mật khẩu không nằm trong bộ từ điển hoặc quá thông dụng đối với người dùng thông thường.

Mật khẩu phải có độ mạnh nhất định dựa theo thang đo mật khẩu.

Thường xuyên thay đổi mật khẩu và chặn những truy cập lạ.

Sử dụng các công cụ quản lý mật khẩu đáng tin cậy như Google, Samsung, iCloud,…

Sử dụng mật khẩu khó như: RetryUntilRevolution@27122002,...

Thang đo độ mạnh mật khẩu được trình bày dưới dạng thuật toán của ngôn ngữ C++:

Ứng dụng kiến thức từ môn Cấu trúc dữ liệu và Giải thuật (Data Structure and Algorithm)

```
#include <iostream>
#include <string.h>
using namespace std;
bool checkValid(string s)
{
	if (s.length() < 8)
		return false;
	for (int i = 0; i < s.length(); i++)
		if (s[i] == 46 or s[i] == 92 or s[i] == 47 or s[i] == ' ' or s[i] == ',')
			return false;
	return true;
}
bool check_Upper(string s, int i)
{
	if (s[i] >= 65 and s[i] <= 90)
		return true;
	return false;
}
bool check_Number(string s, int i)
{
	if (s[i] >= 48 and s[i] <= 57)
		return true;
	return false;
```

```
}

bool check_Symbols(string s, int i)
{
	if (s[i] == '!' or s[i] == '@' or s[i] == '#' or s[i] == '$' or s[i] == '%' or s[i] == '^' or s[i] == '&' or s[i] == '*' or s[i] == '?' or s[i] == '_' or s[i] == '~')
		return true;
	return false;
}
int main()
{
	string s;
	cin >> s;
	if (!checkValid(s)) cout << "KhongHopLe";
	else
	{
	//khai bao
		int Bonus_Combo = 0, Bonus_FlatLower = 0, Bonus_FlatNumber = 0;
	bool flagU = false, flagN = false, flagS = false;
		int Num_Excess = s.length() - 8;
		int Num_Upper = 0, Num_Numbers = 0, Num_Symbols = 0;
		int BaseScore = 40;
		int Bonus_Excess = 3;
		int Bonus_Upper = 4;
		int Bonus_Numbers = 5;
		int Bonus_Symbols = 5;
```

```
//check ky tu
for (int i = 0; i < s.length(); i++)
{
	if (check_Number(s, i))
	{
		Num_Numbers++;
		flagN = true;
	}
	if (check_Symbols(s, i))
	{
		Num_Symbols++;
		flagS = true;
	}

	if (check_Upper(s, i))
	{
		Num_Upper++;
		flagU = true;
	}
}
// tang giam
if (flagN == true and flagS == true and flagU == true) Bonus_Combo = 25;
else if ((flagN == false and flagS == true and flagU == true) or (flagN == true and flagS == false and flagU == true) or (flagN == true and flagS == true and flagU== false))
```

```
                Bonus_Combo = 15;
        if (flagU == false and flagN == false and flagS == false) Bonus_FlatLower = -15;
        if (Num_Numbers == s.length()) Bonus_FlatNumber = -35;


        //tinh diem
        int score = BaseScore + (Num_Excess * Bonus_Excess) + (Num_Upper * Bonus_Upper) + (Num_Numbers * Bonus_Numbers) + (Num_Symbols * Bonus_Symbols) + Bonus_Combo + Bonus_FlatLower + Bonus_FlatNumber;


        // check
        if (score < 50) cout << "Yeu";
        else if (score >= 50 and score < 75) cout << "Vua";
        else if (score >= 75 and score < 100) cout << "Manh";
        else if (score >= 100)cout << "RatManh";
    }
    return 0;
}
```