**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG CƠ SỞ TP HCM**

**MÔN HỌC: AN TOÀN MẠNG**

**BÁO CÁO BÀI TẬP TÌM HIỂU VỀ WIRELESS SECURITY**

****

**NHÓM THỰC HIỆN: NHÓM 4**

**THÀNH VIÊN: MAI XUÂN Ý – N18DCAT105**

**NGUYỄN ĐỨC QUỲNH – N18DCAT065**

**NGUYỄN MẠNH THÌN – N18DCAT085**

**TRƯƠNG VĂN NAM – N18DCAT051**

**NGUYỄN MINH HẬU – N18DCAT019**

1. **Các bước hack WPA/WPA2 wifi, nêu mục đích các bước.**

Chuẩn bị :

* Wifi support monitor mode
* Công cụ aircrack-ng
  1. Khởi động wireless interface ở chế độ giám sát(monitor mode) ở một kênh access point.

Mục đích: đưa card mạng vào chế độ giám sát, qua đó theo dõi mọi gói tin truyền trong mạng.

* 1. Khởi động airodump-ng

Mục đích:thu thập thông tin bắt tay 4 bước của Access point.

* 1. Sử dụng aireplay-ng để hủy xác thực ứng dụng của wireless client.

Mục đích:Để wireless client thực hiện lại kết nối với AP, sau đó ta sẽ thu thập được thông tin bắt tay 4 bước.

* 1. Chạy aircrack-ng để lấy pre-shared key.

Mục đích:Lấy pre-shared key để chạy brute-force.

Tham khảo : https://www.aircrack-ng.org/doku.php?id=cracking\_wpa

# **Các bước Authentication với wireless**

* 1. Máy khách yêu cầu 1 khung xác thực
  2. Phản hồi khung xác thực cho máy khách chứa challenge text.
  3. Máy khách mã hóa challenge text bằng mã hóa WEP bằng khóa chung, sau đó gửi cho AP. AP sẽ giải mã bằng khóa chung và so sánh với challenge text ban đầu.
  4. Nếu khớp mã thì AP cho phép máy khách đó truy cập.

Thamkhảo:http://etutorials.org/Networking/wn/Chapter+8.+Wireless+Network+Security+Protecting+Information+Resources/Authentication/

1. **Nguyên lý tìm ra password**

* Sử dụng brute-force attack để thử từng mật khẩu trong 1 tập tin mật khẩu.

**Sử dụng naïve-hashcat**

cap2hccapx.bin name.cap name.hccapx

Đổi định dạng tập tin .cap sang hccapx có được từ quá trình airodump-ng.

Cài đặt naïve-hashcat và tải tập lib rockyou(hoặc tập tin tự tạo)

sudo git clone https://github.com/brannondorsey/naive-hashcat

cd naive-hashcat

curl -L -o dicts/rockyou.txt <https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt>

Khởi chạy naive-hashcat:

thay tất cả câu có phần "name" bằng tên tập tin ".cap":

HASH\_FILE=name.hccapx POT\_FILE=name.pot HASH\_TYPE=2500 ./naive-hashcat.sh

**Chờ mật khẩu mạng bị bẻ khóa.** Sau khi mật khẩu bị bẻ khóa, chuỗi ký tự sẽ được thêm vào tập tin "name.pot" trong thư mục "naive-hashcat”

hoặc trên màn khởi chạy naïve-hashcat.

**Đối với máy không có GPU**

* Sử dụng tập tin mật khẩu có sẵn hoặc tự thiết lập.

Curl -L -o rockyou.txt https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt

Sử dụng aircrack-ng để bắt đầu bẻ khóa

aircrack-ng -a2 -b MACADDRESS -w lib.txt -name.cap

-a2 : WPA2

-a :WPA

MAC: địa chỉ MAC lấy được từ 4 way handshake

-name.cap: tập tin lấy được từ quá trình airodump-ng

Mật khẩu sẽ hiện trong KEY FOUND! [ ]

* Mật khẩu sẽ không bị bẻ khóa nếu nó không nằm trong tập tin mật khẩu.

# **802.1X**

EEE 802.1X là một chuẩn điều khiển truy cập mạng dựa trên cổng (port), chứng thực trên tầng 2 mô hình OSI. Phần lớn các việc triển khai truy cập mạng dựa trên cổng là truy cập đến các mạng không dây (WLAN) và truy cập các mạng có dây (LAN). Mặc nhiên các cổng ở trạng thái “đóng”, nghĩa là sự truy cập không được cho phép luồng dữ liệu đi ngang qua.

Sau khi người dùng (user) hoặc thiết bị truy cập yêu cầu chứng thực bản thân nó, khi đó trạng thái cổng được thay đổi “mở”, nghĩa là cho phép luồng dữ liệu đi qua.

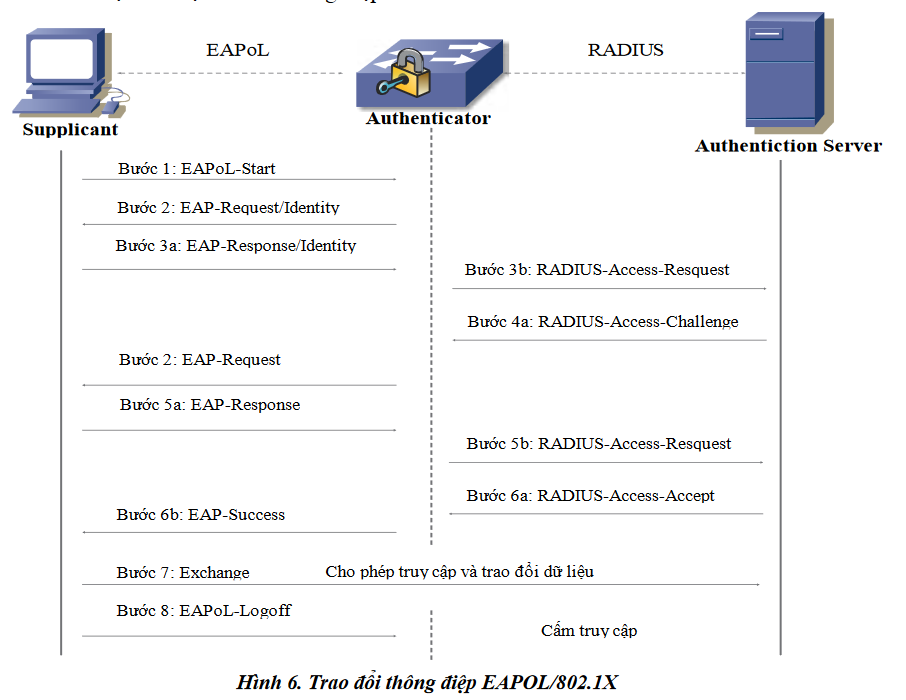
802.1X hạn chế các máy trạm (clients) không được xác thực kết nối đến hạ tầng mạng LAN hoặc WLAN dùng bởi sự điều khiển truy cập dựa trên máy chủ (Server) và máy trạm với giao thức chứng thực

Giao tiếp 802.1x ban đầu bắt đầu với một thiết bị hỗ trợ không được xác thực (wireless client device) cố gắng kết nối với một bộ xác thực (wireless base station). Base station phản hồi bằng cách cho phép một cổng chỉ truyền các gói EAP từ máy khách đến máy chủ xác thực nằm ở phía có dây của base station. Base station chặn tất cả các lưu lượng khác, chẳng hạn như gói HTTP, DHCP và POP3, cho đến khi base station có thể xác minh danh tính của khách hàng bằng máy chủ xác thực, chẳng hạn như RADIUS. Sau khi được xác thực, base station sẽ mở cổng của máy khách cho các loại lưu lượng khác dựa trên quyền truy cập do máy chủ xác thực nắm giữ.

EAP là một nền tảng sự chứng thực cho các thiết bị trong hệ thống mạng mà nó hỗ trợ nhiều phương pháp chứng thực. EAP cho phép hai thực thể trong hệ thống mạng trao đổi thông tin được chỉ định phương pháp chứng thực, các thực thể đó muốn sử dụng.

Quá trình:

* Máy khách gửi một thông báo bắt đầu EAP. Điều này bắt đầu một loạt các trao đổi tin nhắn để xác thực khách hàng;
* Base station trả lời bằng một thông báo nhận dạng yêu cầu EAP.
* Máy khách gửi một gói phản hồi EAP có chứa danh tính đến máy chủ xác thực.
* Máy chủ xác thực sử dụng một thuật toán xác thực cụ thể để xác minh danh tính của khách hàng.
* Máy chủ xác thực sẽ gửi thông báo chấp nhận hoặc từ chối đến trạm gốc.
* Base station gửi một gói tin thành công EAP đến máy khách.
* Nếu máy chủ xác thực chấp nhận máy khách, trạm gốc sẽ chuyển cổng của máy khách sang trạng thái được ủy quyền và chuyển tiếp lưu lượng bổ sung.



Tham khảo : <https://tckh.tvu.edu.vn/sites/default/files/magazinepdfs/tapchiso_10_03.pdf>

1. **WPA3/wifi6**

* WPA3 – Wifi Protection Access3 do Wifi Alliance phát triển, được phê duyệt trong năm 2018.
* Giao thức WPA3 cung cấp các tính năng mới cho mục đích sử dụng cá nhân và doanh nghiệp như Giao thức chế độ bộ đếm(Counter Mode Protocol) / Galois 256 bit (GCMP-256), Chế độ xác thực tin nhắn băm 384 bit ( HMAC - Hashed Message Authentication Mode) và Giao thức toàn vẹn truyền phát / đa phương tiện 256 bit (BIP /GMAC-256 - 256-bit Broadcast/Multicast Integrity Protocol ). Giao thức WPA3 cũng hỗ trợ các biện pháp bảo mật như bảo mật chuyển tiếp hoàn hảo(perfect forward secrecy).
* So với WPA2 thì WPA3 có các tính năng ưu việt hơn như:
  + **Xác thực đồng thời giao thức Equals** : Giao thức này được sử dụng để tạo bắt tay an toàn, trong đó thiết bị mạng sẽ kết nối với điểm truy cập không dây và cả hai thiết bị giao tiếp để xác minh xác thực và kết nối. Ngay cả khi mật khẩu của người dùng yếu, WPA3 cung cấp khả năng bắt tay an toàn hơn bằng cách sử dụng Wi-Fi DPP.
  + **Mã hóa dữ liệu được cá nhân hóa** : Khi đăng nhập vào mạng công cộng, WPA3 đăng ký một thiết bị mới thông qua một quy trình không phải là mật khẩu dùng chung. WPA3 sử dụng một hệ thống được gọi là Giao thức cấp phép thiết bị Wi-Fi (DPP) cho phép người dùng sử dụng thẻ NFC hoặc mã QR để cho phép các thiết bị trên mạng. Hơn nữa, bảo mật WPA3 sử dụng mã hóa GCMP-256 , so với mã hóa 128 bit được sử dụng trước đây.
  + **Bảo vệ chống tấn công brute-force mạnh mẽ hơn** : WPA3 bảo vệ chống lại các lần đoán mật khẩu ngoại tuyến bằng cách cho phép người dùng chỉ một lần đoán, khiến người dùng phải tương tác trực tiếp với thiết bị Wi-Fi, có nghĩa là họ sẽ phải có mặt trực tiếp mỗi khi muốn đoán mật khẩu . WPA2 thiếu mã hóa và quyền riêng tư tích hợp trong các mạng mở công cộng, khiến các cuộc tấn công brute-force trở thành một mối đe dọa lớn.
  + **Khóa phiên lớn hơn** : WPA3 sẽ hỗ trợ kích thước khóa phiên(session key) lớn hơn , bảo mật lên đến 192-bit trong các trường hợp sử dụng cho doanh nghiệp.

Tham khảo: <https://searchsecurity.techtarget.com/definition/WPA3>