Học Viện Công Nghệ Bưu Chính Viễn Thông

Khoa Công Nghệ Thông Tin

BÁO CÁO MÔN HỌC

An Toàn Bảo Mật Hệ Thống Thông Tin

Chủ đề: Session Hijacking

Nhóm tín chỉ 6 (nhóm báo cáo 5)

Đỗ Đình Nhất - B16DCCN258

Đỗ Trọng Dũng - B16DCCN090

Nguyễn Đình Tiến - B16DCCN353

Nguyễn Văn Hiếu - B16DCCN146

Đóng góp của thành viên

Nhóm trưởng: Đỗ Đình Nhất

Thu thập và chuẩn bị tài liệu: Nguyễn Văn Hiếu

Báo cáo lý thuyết: Đỗ Trọng Dũng – Nguyễn Đình Tiến

Cài đặt môi trường thử nghiệm và demo: Đỗ Đình Nhất

Nội dung báo cáo:

1. Session là gì ?
2. Session Hijacking là gì?
3. Các dạng tấn công Session Hijacking.
4. Session Hijacking trong mô hình OSI
5. Session Hijacking mức ứng dụng.
6. Session Hijacking mức mạng.
7. Biện pháp bảo vệ và phương pháp ngăn chặn.
8. Demo thử nghiệm

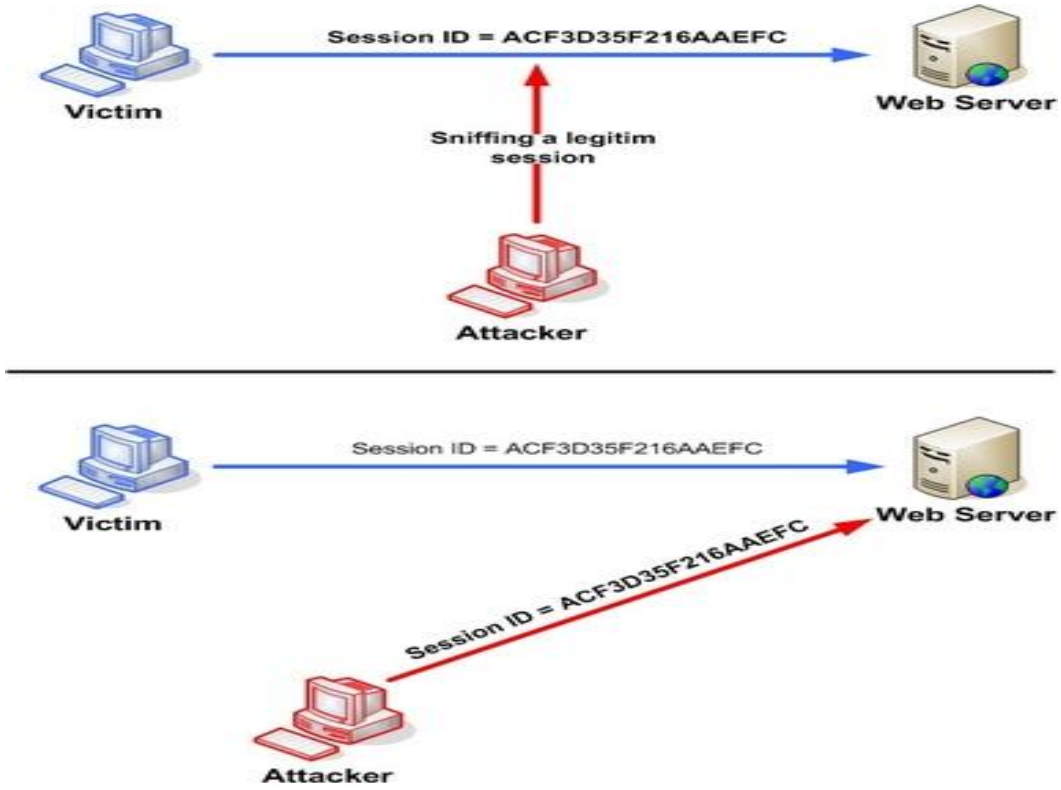
1. Session

- Session là 1 phiên làm việc trong đó người sử dụng giao tiếp với 1 ứng dụng. Session bắt đầu khi người sử dụng truy cập vào ứng dụng lần đầu tiên, và kết thúc khi người sử dụng thoát khỏi ứng dụng. Một session thường được gắn với 1 mã số định danh (Session ID) và 1 hash chứa 1 số thông tin nhất định của người dùng. Session được đặt thời gian tồn tại.
- Sử dụng một session: Session giống như một bộ nhớ có thể truy cập nhanh chóng được cung cấp cho người sử dụng ứng dụng đó, khi người sử dụng thoát thì session bị hủy. Bộ nhớ tạm có thể nằm trên hệ thống tệp trong các tệp văn bản, trên cơ sở dữ liệu hoặc trong bộ nhớ trong của chương trình đang thi hành ứng dụng.
- Cấu trúc 1 session:
    i. Session là một cấu trúc dữ liệu key-value.
    ii. Session có thể được lưu bên server hoặc trên client. Nếu ở máy khách, nó sẽ được lưu trữ bởi trình duyệt (hầu hết là trong cookie) và nếu nó được lưu trữ trên server, session_id sẽ được tạo và quản lí bởi server.

2. Session Hijacking

- Session Hijacking là hình thức tấn công vào phiên làm việc giữa client và server cách đánh cắp session của người sử dụng sau khi họ đã qua bước xác thực với máy chủ, sau đó sẽ chiếm quyền điều khiển của phiên làm việc này.
- Trong quá trình hoạt động, người dùng không cần phải chứng thực lại. Kẻ tấn công lợi dụng điều này để cướp session đang hoạt động của người dùng và làm cho người dùng không kết nối được với hệ thống. Sau đó kẻ tấn công mạo danh người dùng bằng session vừa cướp được, truy cập đến máy chủ mà không cần phải đăng nhập vào hệ thống.

- Khi cướp được session của người dùng, kẻ tấn công có thể vượt qua quá trình chứng thực dùng, có thể ghi lại phiên làm việc và xem lại mọi thứ đã diễn ra.



3. Các dạng tấn công Session Hijacking

Có hai dạng Session Hijacking:

- Chủ động: Hacker sẽ tìm các phiên làm việc đang hoạt động và chiếm đoạt nó thông qua các công cụ
- Thụ động: Các kẻ tấn công chỉ theo dõi và ghi lại tất cả những thông tin được gửi bởi người sử dụng hợp lệ (nghe lén).

4. Session Hijacking trong mô hình OSI

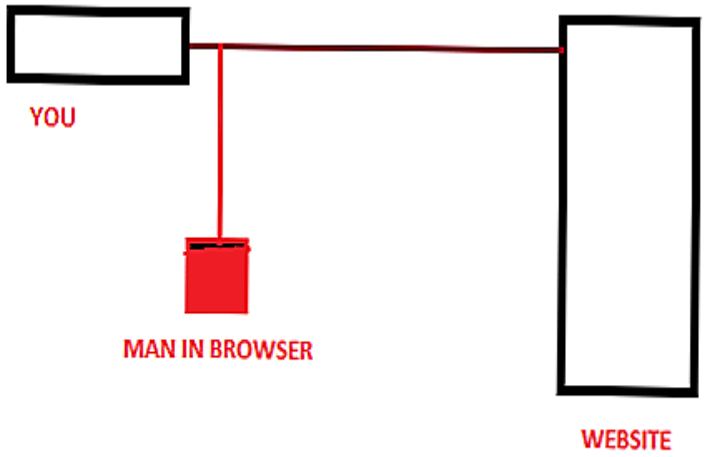
- Hijacking mức mạng: làm việc với tầng giao vận TCP/UDP để thông dịch các packets trong một phiên làm việc giữa client và server
- Hijacking mức ứng dụng: hacker giành quyền kiểm soát trên HTTP session thông qua session đã đánh cắp được

5. Session Hijacking mức ứng dụng

- Trong một cuộc tấn công Session Hijacking, session token bị đánh cắp hoặc session token hợp lệ được dự đoán để truy cập trái phép vào máy chủ web.
- Session token có thể bị đánh cắp bằng nhiều cách khác nhau:
    i. Thăm dò phiên (Session Sniffing)
        - Kẻ tấn công thăm dò để chiếm 1 token hợp lệ là "sessionID".
        - Tiếp theo, kẻ tấn công dùng token hợp lệ để truy cập trái phép vào máy chủ web.
    ii. Dự đoán session token(Predictable session token)
        - Dự đoán giá trị sessionID bằng cách phân tích và hiểu quy trình tạo ra sessionID, kẻ tấn công có thể dự đoán giá trị sessionID hợp lệ và có quyền truy cập vào ứng dụng.
        - Kẻ tấn công cần thu thập một số giá trị sessionID hợp lệ được sử dụng để xác định người dùng hoặc sử dụng sessionID được tạo bởi tên người dùng hoặc thông tin dự đoán khác, như dấu thời gian hoặc địa chỉ IP của máy khách.
        - Ví dụ:

            Bước 1: Kẻ tấn công chiếm một số các sessionID, dự đoán cấu trúc của các sessionID và phân tích để lấy ra những dữ liệu cần thiết.

            Bước 2: Kẻ tấn công phân tích mô hình của session ID chiếm được. Nhìn vào 1 session ID, kẻ tấn công dự đoán được thời gian vào ngày 25/09/2010 lúc 16:40.20
    iii. Tấn công Man in the browser (Man-in-the-browser attack)



- Tấn công sử dụng Trojan Horse để chặn và can thiệp ứng dụng đang dùng với các cơ chế bảo mật hay các thư viện được sử dụng.
- Tấn công MITB thường được sử dụng để nhắm tới nhưng giao dịch trực tuyến về tài chính (banking). Phầm mềm độc hại có thể chuyển tiền hoặc thanh toán, ngân hàng sẽ không thể phát hiện về việc tấn công nếu thông tin đăng nhập được nhập chính xác.
- Ví dụ:

  Hầu hết các trang web của ngân hàng chỉ yêu cầu ID của bạn và mã PIN (OTP) để đăng nhập. Một số trang web có thể sử dụng mật khẩu. Nhưng nếu cần login bằng thủ tục lạ như yêu cầu bạn số thẻ tín dụng của bạn, mã PIN,… thì chúng ta nên cảnh giác. Nếu điều đó xảy ra, cần đến ngân hàng để xác minh có thực sự cần dữ liệu đó.
- Các bước thực hiện cơ bản

  + B1: Trojan xâm nhập vào phần mềm của máy tính

  + B2: Trojan cài đặt mã độc hại và lưu vào cấu hình trình duyệt

  + B3: Sau khi người dùng khởi động lại trình duyệt, mã độc dưới hình thức tập tin mở rộng được tải.

  + B4: Các tập tin mở rộng đăng kí một xử lý cho mỗi lần truy cập trang web.

  + B5: Khi trang web được tải, đuôi mở rộng sử dụng các URL và phù hợp với một danh sách các các trang web được biết đến là mục tiêu tấn công.

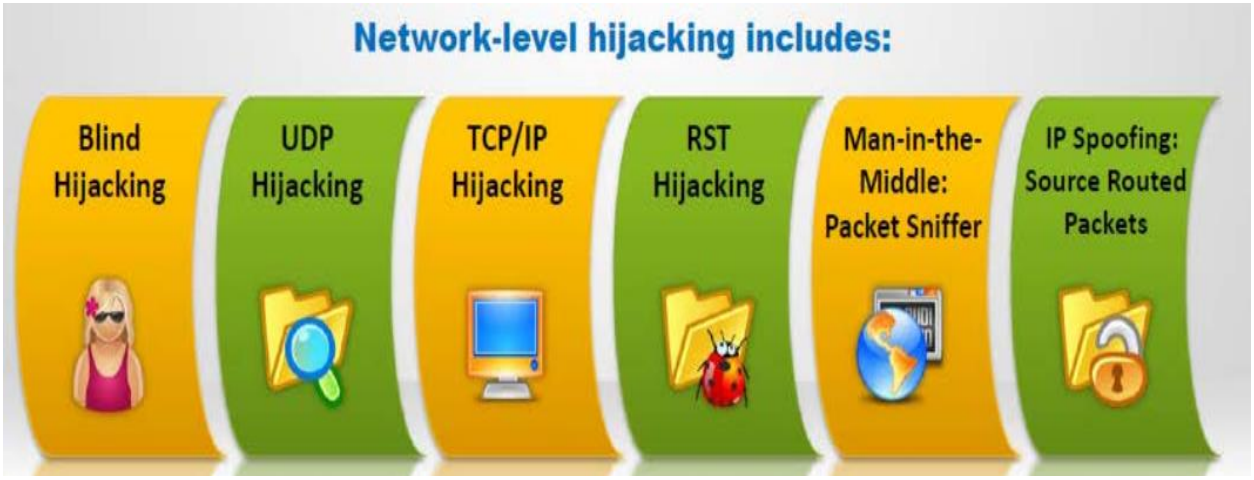
  + B6: Người sử dụng đăng nhập vào trang web.

+ B7: Nó đăng ký 1 nút xử lý sự kiện khi tải trang cụ thể là phát hiện một giao diện cụ thể và so sánh nó với danh sách mục tiêu của nó.
+ B8: Trình duyệt sẽ gửi các giao diện và giá trị điều chỉnh đến máy chủ.
+ B9: Khi người dùng nhấp vào nút, sử dụng giao diện DOM và lấy được tất cả các dữ liệu từ tất cả các trường thông tin trên giao diện và thay đổi các giá trị.
+ B10: Máy chủ nhận được các giá trị thay đổi nhưng không thể phân biệt giữa bản gốc và các giá trị được sửa đổi.
+ B11: Sau khi máy chủ thực hiện xử lí, 1 xác nhận được tạo ra.
+ B12: Trình duyệt nhận được xác nhận thay đổi xử lí.
+ B13: Trình duyệt hiển thi xác nhận với các chi tiết gốc
+ B14: Người sử dụng nghĩ rằng các xử lí ban đầu đã được nhận bởi máy chủ mà không có bất kỳ ngăn chặn nào.

iv. Tấn công Client side (Client-side attack)
- Là một loại của cuộc tấn công xen vào, trong đó các tập lệnh mã độc hại được xen vào các trang web.
- Mã độc hại có thể được nhúng trong một trang web và không tạo ra bất kỳ loại cảnh báo nào khi trang được xem trong mọi trình duyệt.

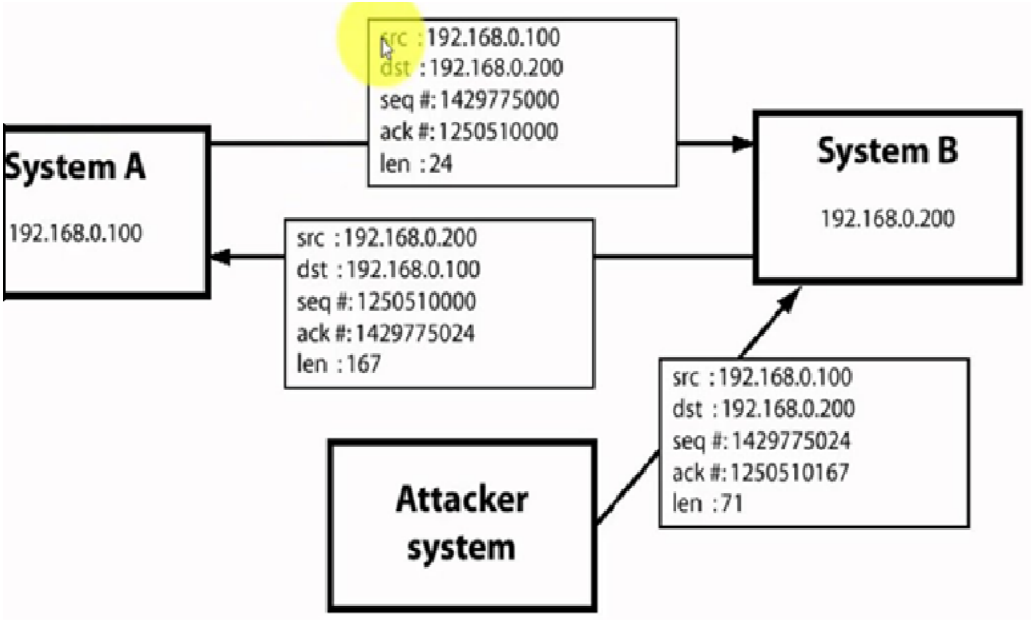
6. Session Hijacking mức mạng

- Tấn công mức mạng được thực hiện trên dữ liệu của giao thức chia sẻ bởi tất cả các ứng dụng web.
- Bằng cách tấn công các phiên mức mạng, kẻ tấn công tập hợp một số thông tin quan trọng được sử dụng để tấn công các phiên mức ứng dụng.



a. Tấn công TCP/IP

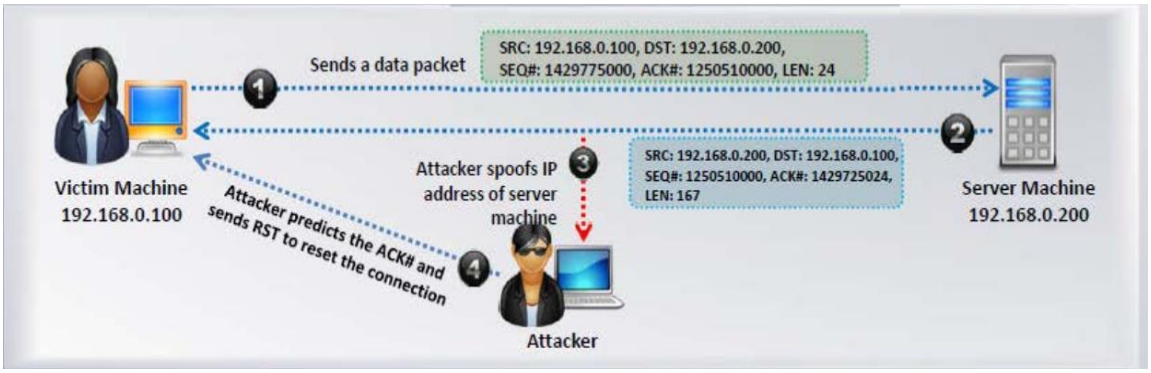
- Tấn công TCP/IP là một kỹ thuật tấn công sử dụng các gói tin giả mạo để tiếp nhận một kết nối giữa một nạn nhân và một máy mục tiêu.
- Trong cuộc tấn công, máy chủ tưởng rằng đang liên lạc với một khách hàng hợp lệ, nhưng thực tế là máy chủ đang liên lạc với một kẻ tấn công đã lấy được TCP.
- Để thực hiện tấn công chiếm TCP/IP, hacker và nạn nhân phải cùng mạng.



- Các bước thực hiện:
  - Bước 1: Kẻ tấn công thăm dò kết nối của nạn nhân và sử dụng IP của nạn nhân để gửi một gói giả mạo với chuỗi số dự đoán.
  - Bước 2: Host xử lí các gói tin giả mạo, tăng số tuần tự (sequence number) và gửi xác nhận đến địa chỉ IP của nạn nhân.
  - Bước 3: Máy tính nạn nhân sẽ không biết về các gói tin giả mạo, do đó nó bỏ qua gói ACK máy chủ và ngừng đếm số tuần tự. Vì vậy, máy chủ nhận được gói dữ liệu với tuần tự không chính xác.
  - Bước 4: Kẻ tấn công đánh dấu kết nối của nạn nhân với máy chủ vào trạng thái desynchoronized.
  - Bước 5: Kẻ tấn công theo dõi các chuỗi số và liên tục gửi các gói tin gải mạo đến từ IP của nạn nhân.

- Bước 6: Kẻ tấn công tiếp tục giao tiếp với máy chủ trong khi kết nối của nạn nhân bị treo.

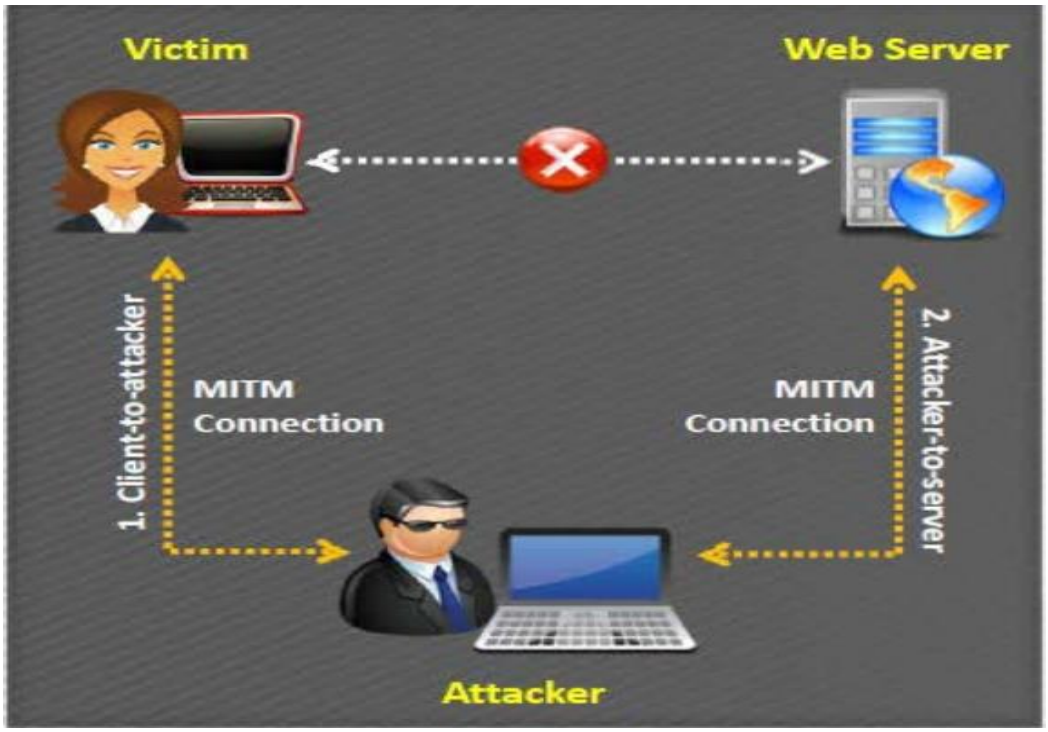
b. Tấn công RST



- Tấn công RST liên quan đến việc truyền 1 gói authetic - looking reset (RST) bằng cách sử dụng địa chỉ nguồn giả mạo và dự đoán số lượng xác nhận.
- Hacker có thể reset lại kết nối nếu kết nối sử dụng chính xác số xác nhận
- Nạn nhân tin rằng các nguồn thực sự gửi các gói tin thiết lập lại và thiết lập lại kết nối.
- Tấn công RST có thể được thực hiện bằng cách sử dụng một gói công cụ thủ công như gói Bulder Colasoft và công cụ phân tich TCP/IP như tcpdump.

c. Tấn công Man in the middle (MITM)

- Kiểu tấn công man-in-the-middle là dùng để xâm nhập vào một kết nối hiện tại giữa các hệ thống và chặn các tin nhắn được trao đổi.
- MITM giống như một kẻ nghe trộm. MITM hoạt động bằng cách thiết lập các kết nối đến máy tính nạn nhân và chuyển tiếp dữ liệu giữa chúng.
- Kẻ tấn công sử dụng các kĩ thuật khác nhau để chia kết nối thành 2 phần:
  - Nạn nhân đến hacker
  - Hacker đến máy chủ
- Trong trường hợp bị tấn công, nạn nhân tưởng là họ đang giao tiếp một cách trực tiếp với máy chủ, nhưng sự thực thì các luồng giao tiếp lại bị trung gian qua máy của kẻ tấn công. Hacker có thể đọc, sửa, chèn dữ liệu vào các giao tiếp giữa máy chủ và nạn nhân



- Một số hình thức tấn công MITM hay được sử dụng
    i. Tấn công giả mạo ARP Cache
    ii. DNS Spoofing
    iii. HTTP Session

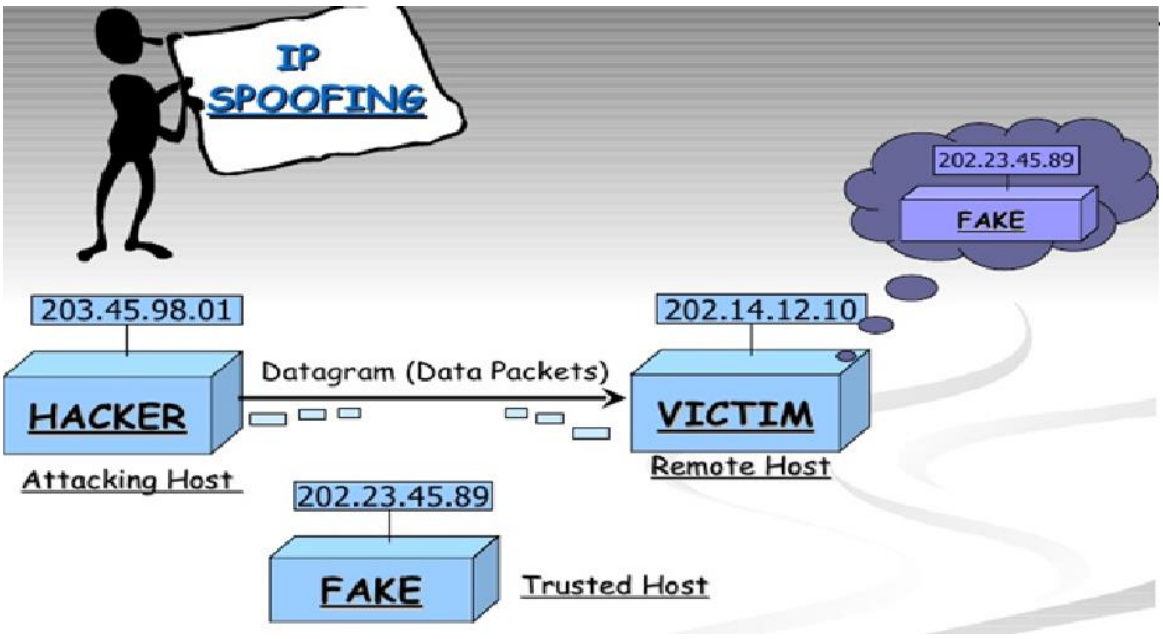
d. Tấn công mù

- Hacker có thể truyền các dữ liệu độc hại hoặc lệnh vào các thông tin liên lạc bị chặn trong phiên TCP ngay cả khi các định tuyến nguồn bị vô hiệu hóa.
- Hacker có thể gửi dữ liệu hoặc comments, nhưng không được truy cập để xem response.

e. Tấn công UDP

- Kẻ tấn công giả mạo đáp ứng UPD request của client trước khi máy chủ thực sự đáp ứng với nó.
- Kẻ tấn công sử dụng Man-in-the-Middle để chặn response của máy chủ cho client và gửi đáp ứng giả mạo của chính nó.

f. IP Spoofing – Source route packets:



- Kĩ thuật routing nguồn gói tin (Packet source routing) được sử dụng để giành quyền truy cập trái phép đến một máy tính với sự hỗ trợ của địa chỉ IP của nạn nhân đã chứng thực.
- Attacker giả mạo IP của nạn nhân vì vậy server quản lý session với host bị giả mạo, có thể chấp nhận các gói tin từ kẻ tấn công
- Khi session được sinh ra, kẻ tấn công thêm vào gói tin giả mạo trước khi host phản hồi tới server
- Gói tin gốc từ nạn nhân bị loại bỏ do server đã xử lý gói tin giả mạo có số tuần tự đã được sử dụng bởi hacker

7. Biện pháp bảo vệ và phương pháp ngăn chặn

a. Biện pháp bảo vệ

- Sử dụng Secure Shell (SSH) để tạo ra một kênh giao tiếp an toàn
- Cấp phép xác thực các tập tin cookie qua kết nối HTTPS
- Kết thúc phiên bằng chức năng log out
- Tạo ra các session ID sau khi đăng nhập thành công và chỉ chấp nhận session ID được sinh ra bởi server
- Hãy chắc chắn dữ liệu được mã hóa khi truyền
- Sử dụng phiên được sinh ra với chuỗi kí tự hoặc số ngẫu nhiên và độ dài lớn
- Cài đặt thời gian hết hạn ngắn cho session, hủy session ngay khi người dùng log out
- Hạn chế truy cập từ xa

b.Phương pháp ngăn chặn

- Đối với Developer
  - Giảm thời gian tồn tại của Session, Cookie
  - Tạo lại các session ID sau khi đăng nhập thành công để ngăn chặn cuộc tấn công cố định phiên
  - Ngăn chặn nghe lén trong hệ thống
  - Mã hóa dữ liệu và session key giao tiếp giữa người sử dụng và máy chủ

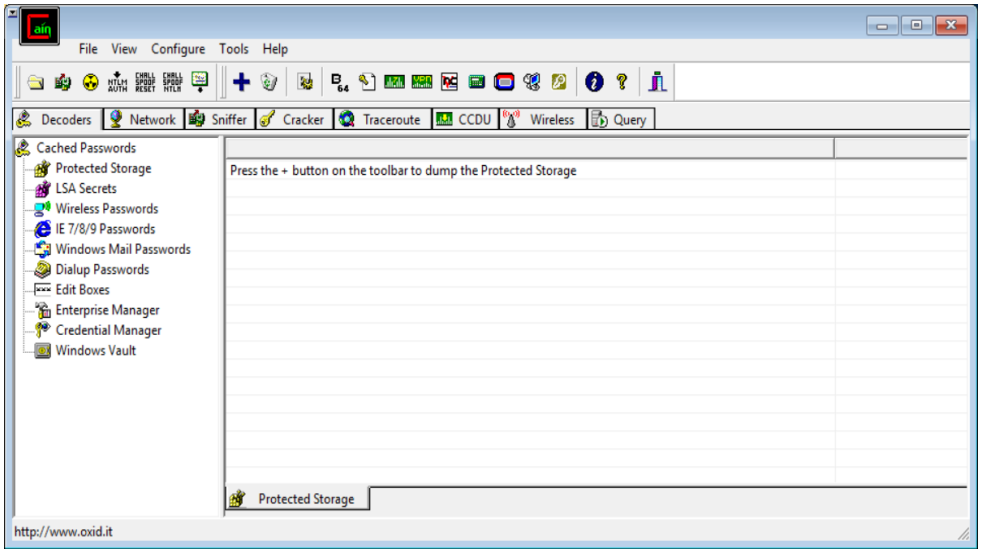
- Tạo các session có key-value dài, ngẫu nhiên, kí tự khó để tránh dễ dàng đoán được
- Sử dụng HTTPS cho website để mã hóa dữ liệu truyền đi

- Đối với người dùng
  - Không bấm vào các liên kết nhận được thông qua mail hay mạng xã hội
  - Sử dụng tường lửa để ngăn chặn các nội dung độc hại xâm nhập vào mạng
  - Cài đặt trình duyệt hạn chế các tập tin cookie
  - Hãy chắc chắn rằng các trang web được xác nhận bởi nơi đáng tin cậy
  - Đăng xuất khỏi trình duyệt bằng cách bấm vào nút đăng xuất thay vì đóng trình duyệt
  - Hạn chế trao đổi thông tin mật và nhạy cảm với trang web không có HTTPS
  - Hãy chắc rằng bạn xóa hết lịch sử, nội dung ngoại tuyến và cookie từ trình duyệt của bạn sau mỗi lần giao dịch bí mật và nhạy cảm

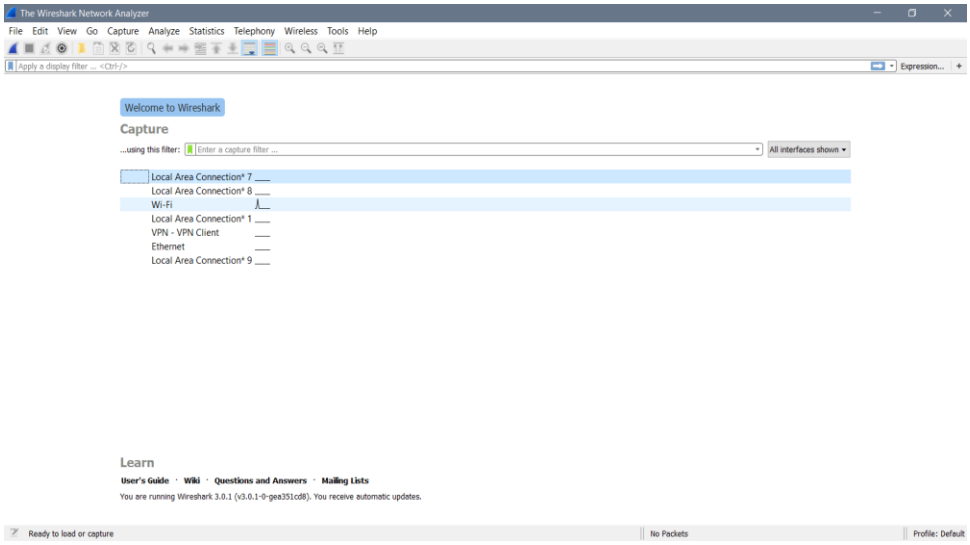
8. Demo thử nghiệm

- Tình huống: Nạn nhân sử dụng điện thoại kết nối cùng 1 mạng (cụ thể là Wifi) với hacker, truy cập vào website và thực hiện truy xuất thông tin được bảo vệ thông qua đăng nhập mật khẩu.
- Mục tiêu: Truy cập được vào trang được bảo vệ bởi tài khoản người dùng
- Các công cụ:
  1. Cain & Abel: Là phần mềm dùng để giải mã mật khẩu, crack mật khẩu đã mã hóa, nghe lén VoIP, sniffing mạng… Trong demo thử nghiệm, Cain & Abel được dùng để thực hiện tấn công Man In The Middle bằng

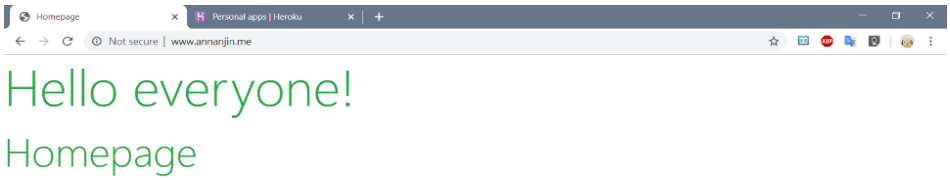
phương pháp APR Spoofing



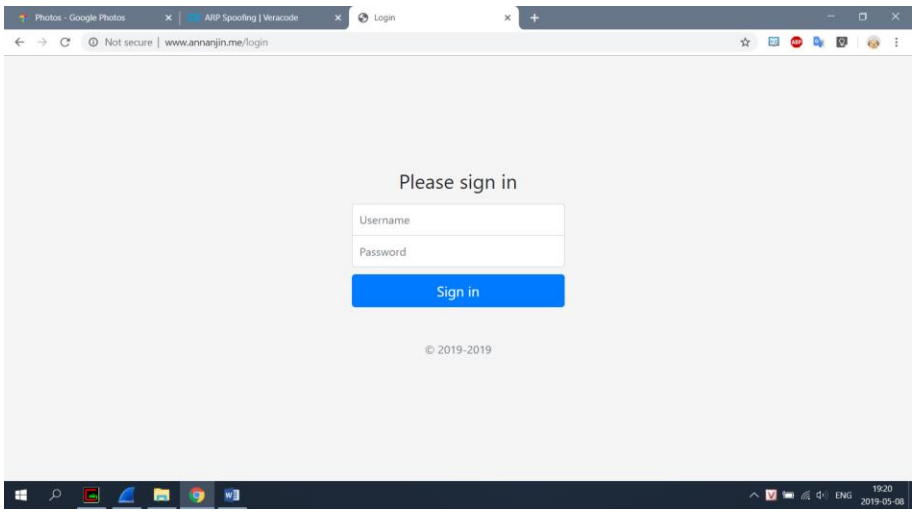
2. Wireshark: Sử dụng để xem thông tin về mạng, nghe lén gói tin trong mạng…



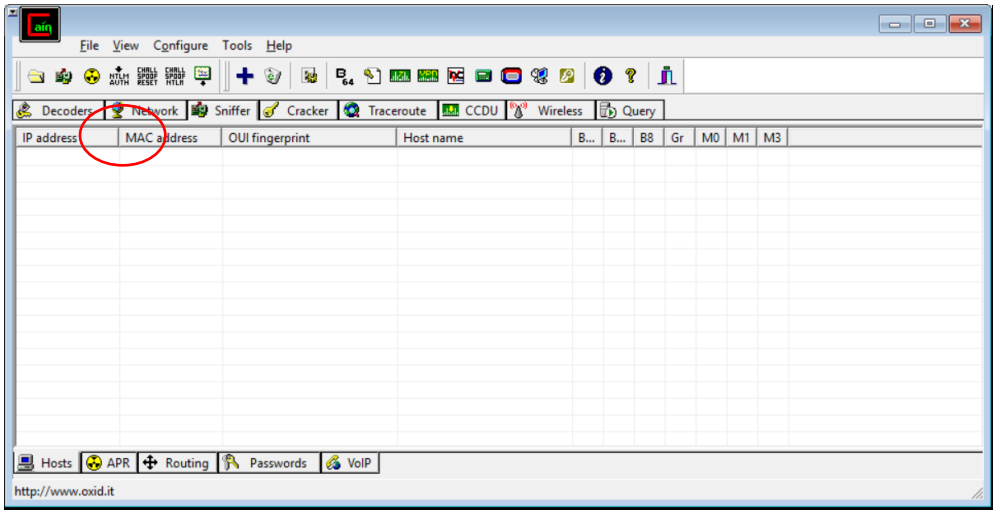
3. Trang web http://www.annanjin.me do nhóm xây dựng, gồm các trang đơn giản, phân quyền được bảo vệ bằng đăng nhập người dùng.



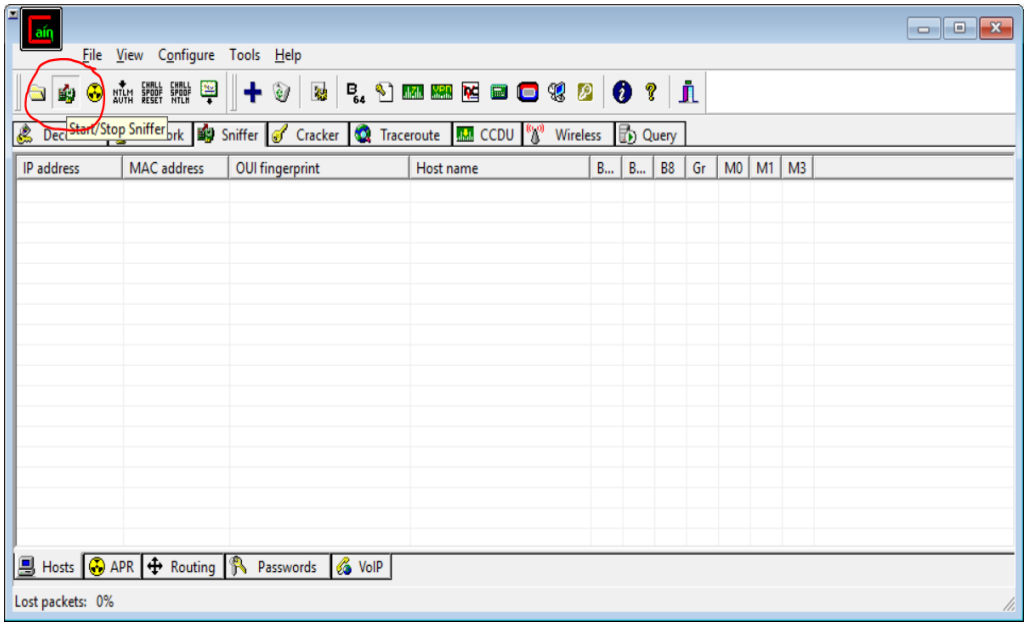
- Tóm tắt kĩ thuật: Hacker sử dụng chung mạng với nạn nhân, dò tìm địa chỉ MAC của nạn nhân và router, sử dụng kĩ thuật ARP Spoofing để giả mạo địa chỉ MAC, biến mình thành trung gian giữa nạn nhân và router (kĩ thuật Man in the middle), từ đó có thể nghe lén gói tin. Hacker xem xét các gói tin bắt được và đánh cắp session của nạn nhân và trang web, sử dụng session để truy cập trái phép thông tin nạn nhân
- Các bước thực hiện:
    1. Ban đầu, hacker thử truy cập trang được bảo vệ http://www.annanjin.me/protected nhưng bị từ chối và chuyển hướng về trang login.



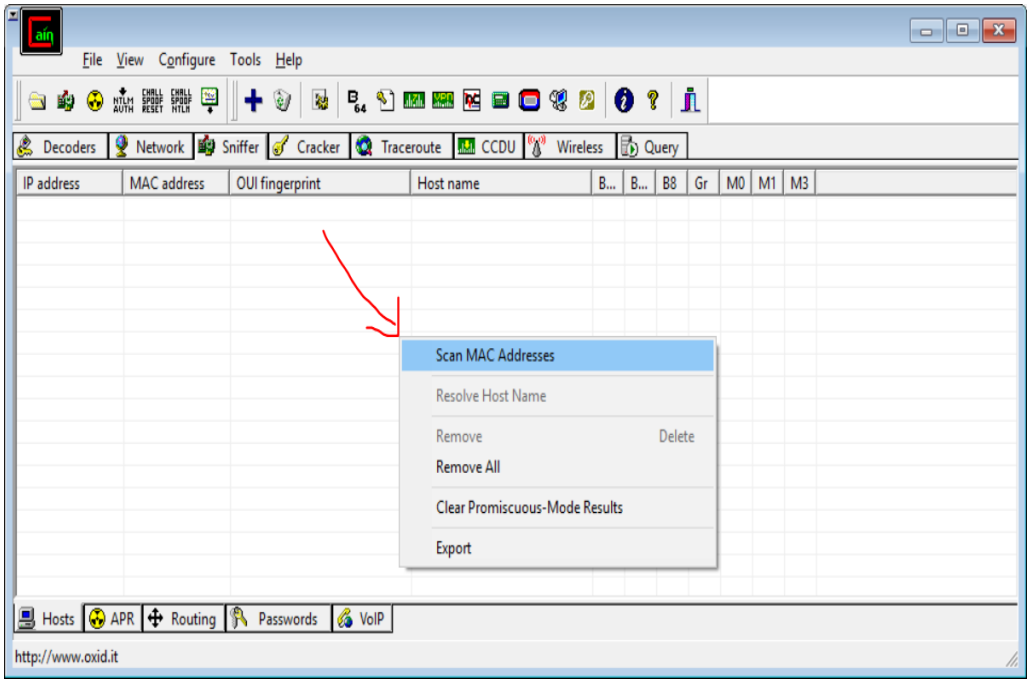
2. Mở Cain & Abel, mở tab Sniffer



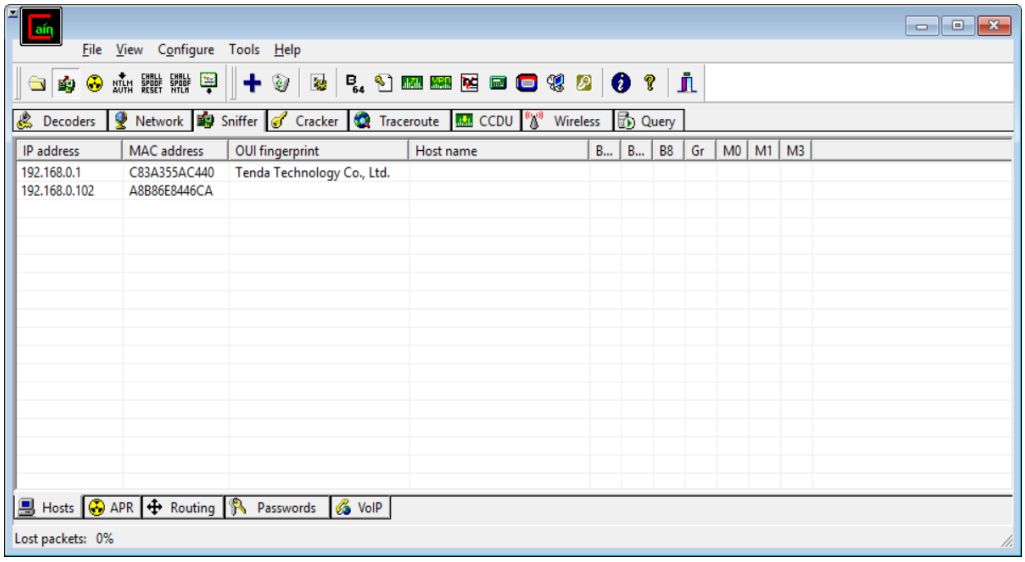
3. Bật bắt đầu sniffing



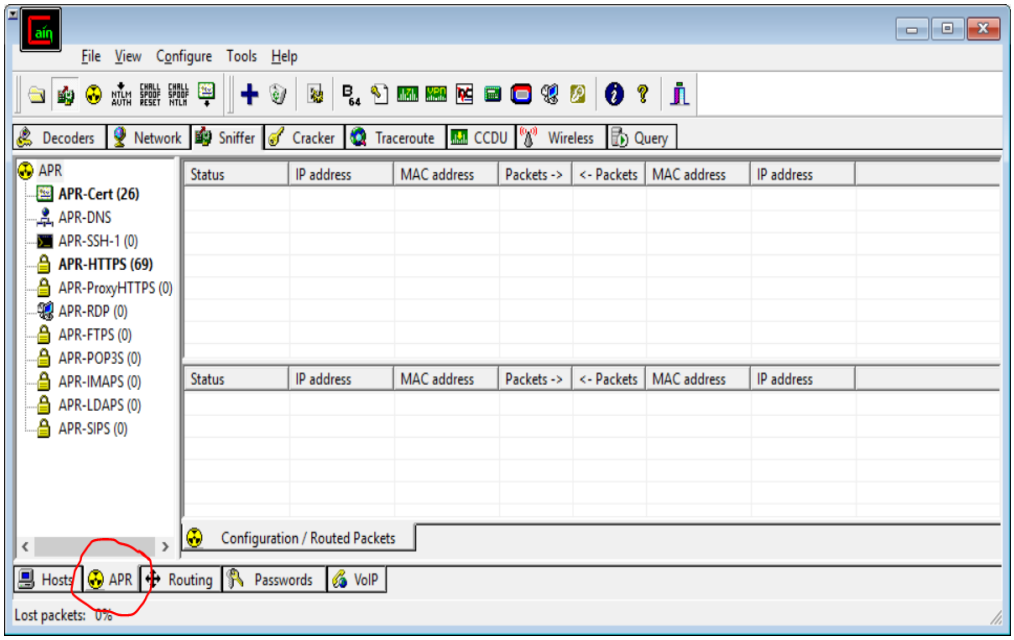
4. Scan các thiết bị trong mạng



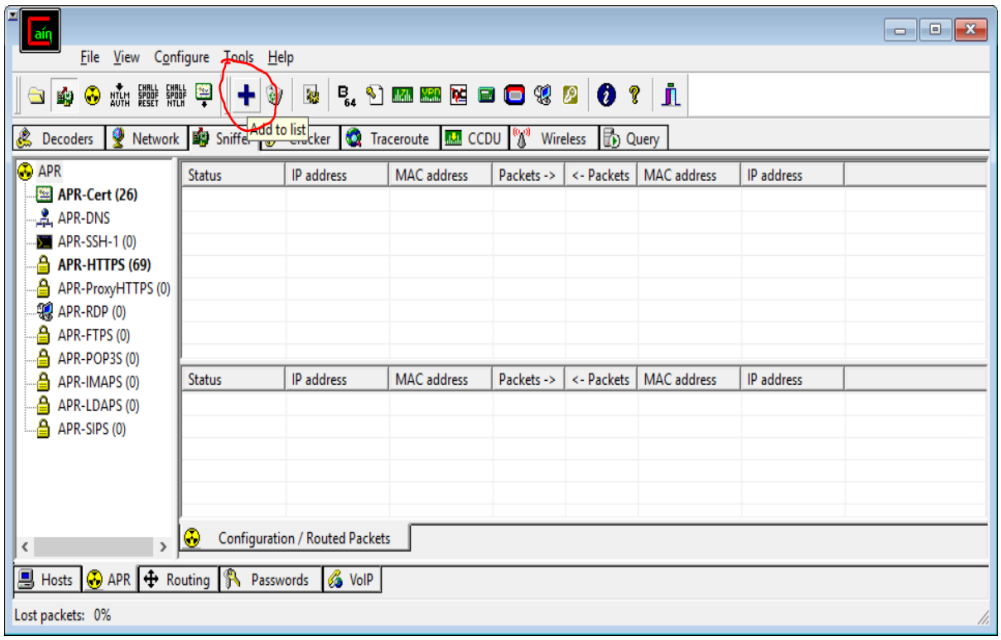
5. Kết quả thu được 2 thiết bị có 2 IP: 1 là của router wifi, 1 của nạn nhân



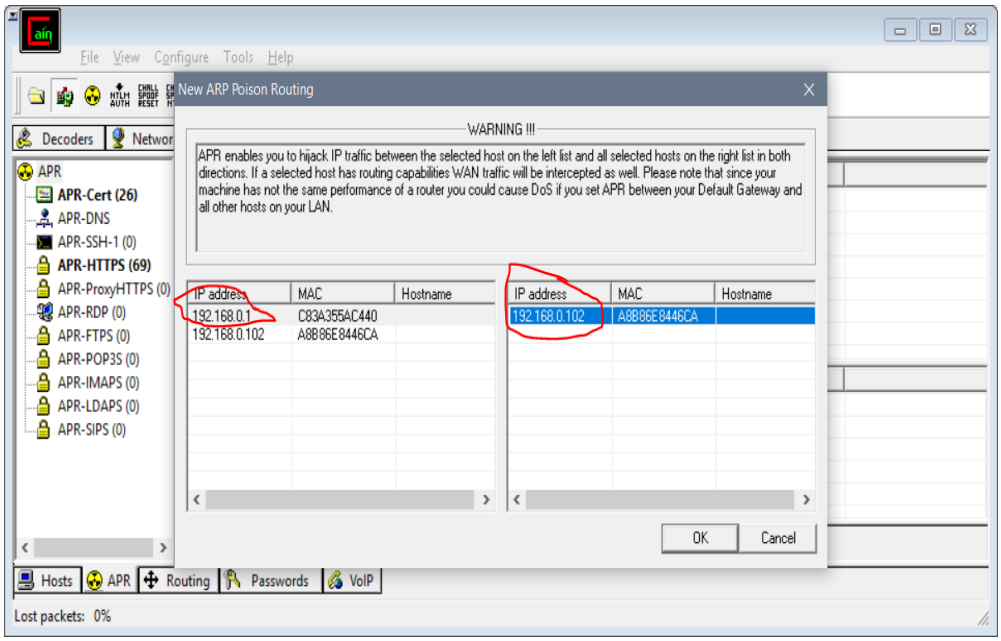
6. Sang tab APR (bên dưới)



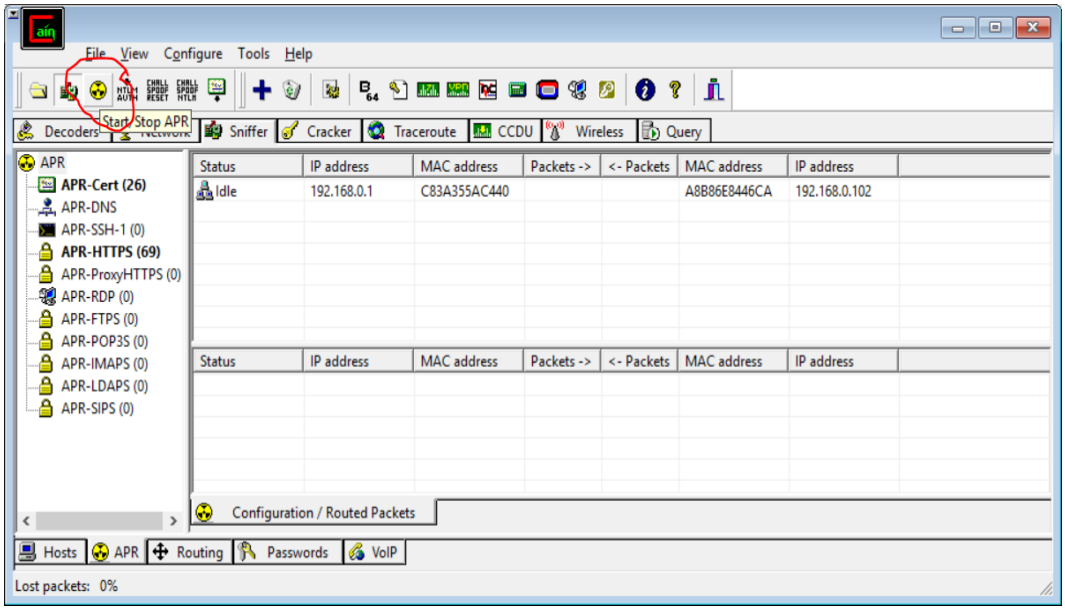
7. Thêm danh sách



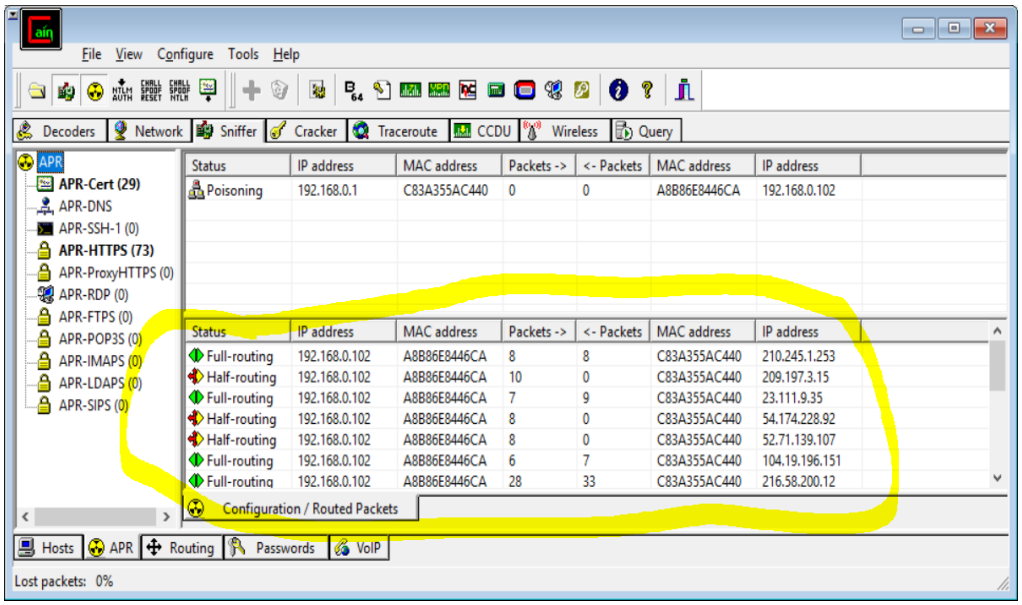
8. Thêm cặp host đầu-cuối. Sử dụng kĩ thuật ARP Spoofing, biến mình thành “Man in the middle”



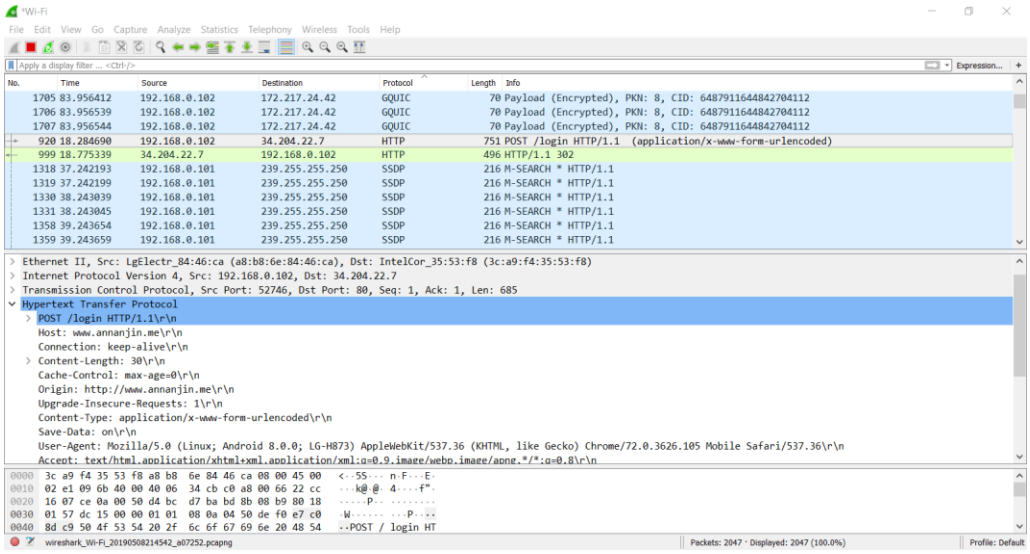
9. Bắt đầu ARP Poison



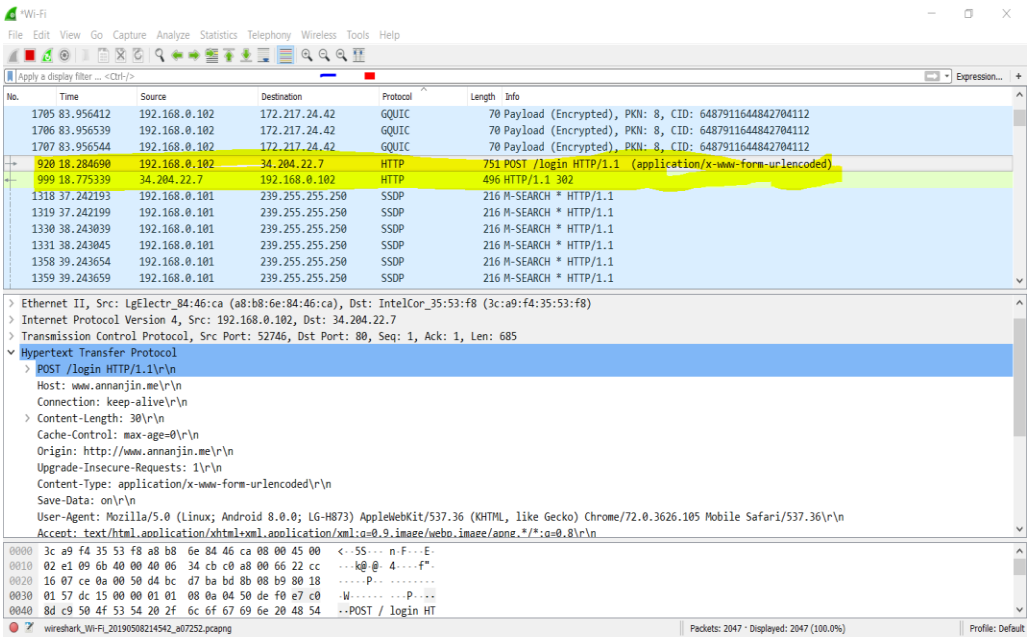
10. Khi nạn nhân truy cập mạng, hacker là kẻ trung gian vận chuyển gói tin giữa nạn nhân và router, vì vậy có thể truy xuất và điều khiển truy cập



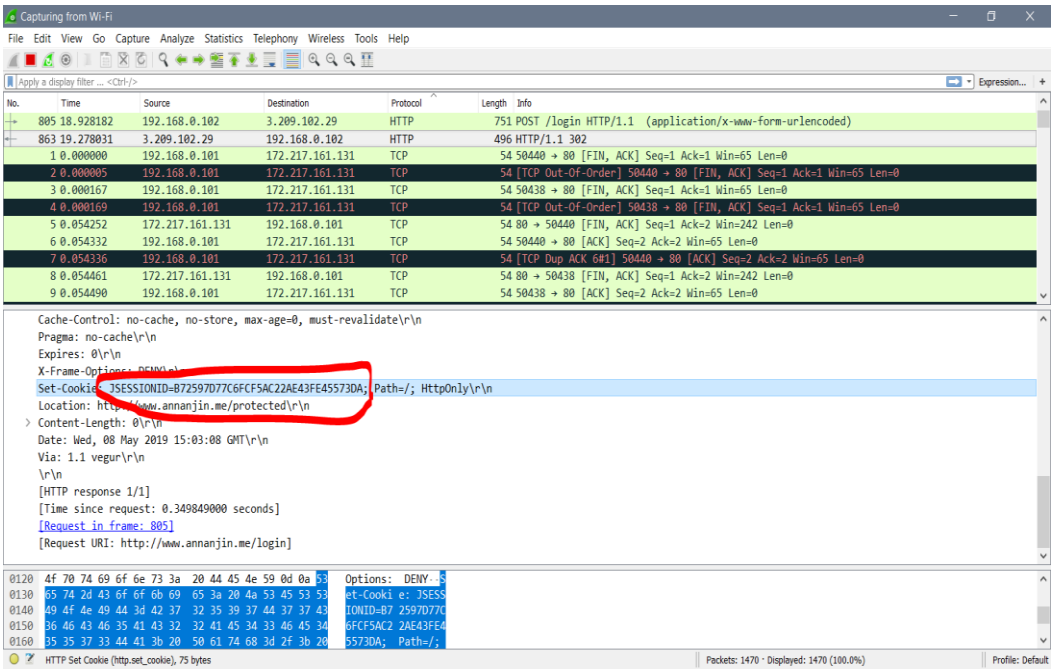
11. Ta sử dụng Wireshark để theo nghe lén các gói tin từ nạn nhân đến router và ngược lại



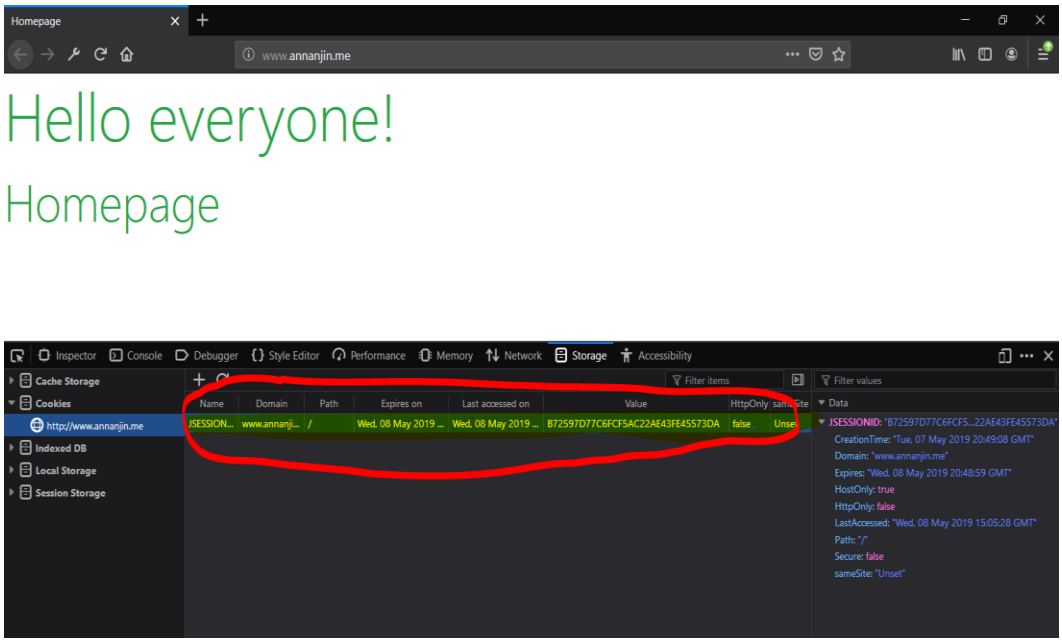
12. Ta bắt được gói tin từ nạn nhân truy cập đến trang web annanjin.me có IP 34.204.22.7 (được đánh dấu)



13. Đọc gói tin, ta tìm được Session ID của Session giữa nạn nhân và trang web



14. Sử dụng ngay Firefox có hỗ trợ thêm Cookie-Session để thêm value session bắt được



15. Thử truy cập trang được bảo vệ http://www.annanjin.me/protected Kết quả thành công, thông tin được bảo vệ đã bị truy cập trái phép