|  |  |
| --- | --- |
| logomobile.png | BỘ GIÁO DỤC VÀ ĐÀO TẠO  **TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM**  **KHOA CÔNG NGHỆ THÔNG TIN** |

**BÁO CÁO CUỐI KÌ**

TÌM HIỂU PHƯƠNG PHÁP TẤN CÔNG

**SESSION HIJACKING**

SINH VIÊN THỰC HIỆN: **LÊ PHẠM THÁI AN**

MSSV: 1811062048 LỚP: 18DTHB3

**NGUYỄN VĂN THIỆT**

MSSV: 1811061029 LỚP: 18DTHB3

**ĐỖ ĐÌNH LỘC**

MSSV: 1811060974 LỚP: 18DTHB3

TP. HỒ CHÍ MINH, 29 tháng 4 năm 2021

|  |  |
| --- | --- |
|  | BỘ GIÁO DỤC VÀ ĐÀO TẠO  **TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM**  **KHOA CÔNG NGHỆ THÔNG TIN** |

BÁO CÁO CUỐI KÌ

TÌM HIỂU PHƯƠNG PHÁP TẤN CÔNG

**SESSION HIJACKING**

MÔN HỌC: **BẢO MẬT THÔNG TIN**

SINH VIÊN THỰC HIỆN: **LÊ PHẠM THÁI AN**

MSSV: 1811062048 LỚP: 18DTHB3

**NGUYỄN VĂN THIỆT**

MSSV: 1811061029 LỚP: 18DTHB3

**ĐỖ ĐÌNH LỘC**

MSSV: 1811060974 LỚP: 18DTHB3

GVHD: **THS.TỐNG THANH VĂN**

TP. HỒ CHÍ MINH, 29 tháng 4 năm 2021

# Mục Lục

[Mục Lục 3](#_Toc70588785)

[LỜI NÓI ĐẦU 1](#_Toc70588786)

[Chương 1: Tổng quan về công cụ thực hiện đề tài 2](#_Toc70588787)

[1.1. Tổng quan về Vmware workstation 2](#_Toc70588788)

[1.2. Giới thiệu về WIRESHARK 3](#_Toc70588791)

[1.3. Cookie 5](#_Toc70588795)

[1.3.1. Cookie là gì? 5](#_Toc70588804)

[Chương 2: Nội dung lý thuyết 7](#_Toc70588806)

[2.1. Phương pháp tấn công SESSION HIJACKING 7](#_Toc70588808)

[2.1.1. Giới thiệu SESSION là gì ? 7](#_Toc70588809)

[2.2. Giới thiệu về SESSION HIJACKING 10](#_Toc70588812)

[2.2.1. Nguyên nhân có thể thai thác lỗi Session Hijacking: 11](#_Toc70588819)

[2.2.2. Mối nguy hiểm từ Hijacking 11](#_Toc70588820)

[2.2.3. Các kỹ thuật SESSION HIJACKING chính : 11](#_Toc70588821)

[2.2.4. Các loại tấn công : 12](#_Toc70588822)

[2.2.5. Phương thức hoạt động của Session Hijacking 12](#_Toc70588823)

[2.2.6. Các Công Cụ Tấn Công Session Hijacking : 12](#_Toc70588824)

[2.3. Các phương pháp chống tấn công : 12](#_Toc70588828)

[2.3.1. Dành cho người dùng 13](#_Toc70588841)

[2.3.2. Dành cho lập trình viên 13](#_Toc70588848)

[2.3.3. Dành cho quản trị server 13](#_Toc70588856)

[Nội dung Demo 14](#_Toc70588857)

[3 Demo chi tiết 15](#_Toc70588858)

**MỤC LỤC HÌNH ẢNH**

[Hình 1 *Ứng dụng bắt gói tin Wireshark* 15](#_Toc70588273)

[Hình 2 : Start ứng dụng bắt đầu nghe lén 16](#_Toc70588274)

[Hình 3: Các thông tin truyền và nhận 17](#_Toc70588275)

[Hình 4-Máy nạn nhân đang đăng nhập daotao.hutech.edu,vn 18](#_Toc70588276)

[Hình 5: Máy nạn nhân đã đăng nhập thành công trang daotao.hutech.edu.vn 19](#_Toc70588277)

[Hình 6 : Kiểm tra thông tin đăng nhập bắt được của máy nạn nhân 20](#_Toc70588278)

[Hình 7: Máy tấn công mở edit cookie 21](#_Toc70588279)

[Hình 8: Máy tấn công đăng nhập thành công vào phiên của nạn nhân 21](#_Toc70588280)

# LỜI NÓI ĐẦU

Đồ án môn học với những ngôn ngữ lập trình khá phổ biến với sinh viên khoa Công Nghệ Thông Tin như ngôn ngữ Java để tự thống kê kiến thức và lên ý tưởng cho những đồ án của mình. Đó là yêu cầu và cũng như thách thức đối với sinh viên khi làm quen với thực hành từ nhữnh lý thuyết sách vở.

Trong môi trường mạng máy tính, một lượng tin hay một khối dữ liệu khi được gửi từ người gửi đến người nhận thường phải đi qua nhiều trạm với nhiều người sử dụng khác nhau không ai đảm bảo rằng thông tin dữ liệu ấy sẽ được an toàn tuyệt đối trước khi đến với người nhận.

Chúng ta đã nghe nhiều về những mối đe dọa từ Internet đối với sự riêng tư của chúng ta hay những kẻ chuyên đánh cắp mật khẩu, những kẻ săn tin chuyên nghiệp và cả những kẻ quấy rối, chúng sẽ không bao giờ để yên cho chúng ta.

Chính vì vậy hôm nay với sự hướng dẫn của thầy Tống Thanh Văn nhóm chung em sẽ trình bày về phương thức tấn công SESSION HIJACKING bao gồm các hình thức tấn công cũng như những cách phòng tránh bản thân bị tấn công .

Xuất phát từ những lý do trên, cùng với sự hướng dẫn của Giảng viên Tống Thanh Văn, chúng em vận dụng những kiến thức đã được học vào thực tiễn, tìm hiểu và đưa ra các biện pháp phòng tránh cho người dùng và cách tối ưu hóa nó.

Chúng em xin chân thành cảm ơn !

# Tổng quan về công cụ thực hiện đề tài

## Tổng quan về Vmware workstation



VMware Workstation là một phần mềm ảo hóa desktop mạnh mẽ dành cho các nhà phát triển/kiểm tra phần mềm và các chuyên gia IT cần chạy nhiều HĐH một lúc trên một máy PC. Người dùng có thể chạy các HĐH Windows, Linux, Netware hay Solaris x86 trên các máy ảo di động mà không cần phải khởi động lại hay phân vùng ổ cứng. VMware Workstation cung cấp khả năng hoạt động tuyệt vời và nhiều tính năng mới như tối ưu hóa bộ nhớ và khả năng quản lý các thiết lập nhiều lớp.

Các tính năng thiết yếu như mạng ảo, chụp ảnh nhanh trực tiếp, kéo thả, chia sẻ thư mục và hỗ trợ PXE khiến VMware Workstation trở thành công cụ mạnh mẽ nhất và không thể thiếu cho các nhà doanh nghiệp phát triển tin họcvà các nhà quản trị hệ thống.

Với hàng triệu khách hàng và hàng loạt các giải thưởng quan trọng trong 7 năm qua, VMware Workstation đã được chứng minh là một công ghệgiúp tăng năng suất và sựlinh họat trong công việc. Đây là một công cụ không thể thiếu cho các nhà phát triển phần mềm và các chuyên gia IT trên toàn thế giới.

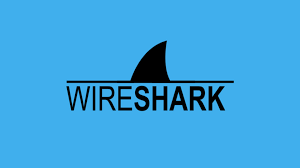
VMware Workstation họat động bằng cách cho phép nhiều HĐH và các ứng dụng của chúng chạy đồng thời trên một máy duy nhất. Các HĐH và ứng dụng này được tách ra vào trong các máy ảo. Những máy ảo này cùng tồn tại trên một phần cứng duy nhất. Các layer ảo của VMware sẽ kết nối các phần cứng vật lývới các máy ảo, do đó mỗi máy ảo sẽcó CPU, bộ nhớ, các ổ đĩa, thiết bị nhập/xuất riêng.

**Tính năng cho người dùng:**

* Thiết lập và thử nghiệm các ứng dụng đa lớp, cập nhật ứng dụng và các miếng vá cho HĐH chỉ trên một PC duy nhất.
* Dễ dàng phục hồi và chia sẻ các môi trường thử nghiệm được lưu trữ; giảm thiểu các thiết lập trùng lặp và thời gian thiết lập.
* Làm cho việc học tập trên máy tính thuận lợi hơn do sinh viên luôn đuợc sử dụng máy với tình trạng “sạch sẽ” và thử nghiệm với nhiều HĐH, ứng dụng cá các công cụ trên những máy ảo an toàn và độc lập.
* Chạy các bản demo phần mềm với các thiết lập phức tạp hoặc đa lớp trên một chiếc laptop.
* Tăng tốc độ giải quyết các rắc rối của người dùng cuối dựa trên một thư việncác máy ảo được thiết lập sẵn



## Giới thiệu về WIRESHARK



[Wireshark](https://bizflycloud.vn/tin-tuc/wireshark-la-gi-tinh-nang-va-cai-dat-wireshark-20181124105016443.htm) là một bộ phân tích gói mạng (network packet analyzer). Một network packet analyzer sẽ cố gắng nắm bắt các network packets và cố gắng hiển thị dữ liệu gói đó càng chi tiết càng tốt.

Một network packet analyzer được sử dụng như một thiết bị đo lường, dùng để kiểm tra những gì đang xảy ra bên trong cáp mạng (network cable), không khác gì chức năng của một vôn kế được thợ điện sử dụng để kiểm tra những gì đang xảy ra bên trong cáp điện.

Trước đây, các công cụ này thường hoặc là rất tốn kém, hoặc độc quyền, hoặc cả hai. Tuy nhiên, với sự ra đời của Wireshark, tất cả những điều đó đã thay đổi.

Wireshark có lẽ là một trong những máy phân tích gói mã nguồn mở tốt nhất hiện nay (open source packet analyzer).

**Mục đích :**

Sử dụng Wireshark nhằm các mục đích sau:

- Network administrators sử dụng Wireshark để khắc phục sự cố mạng.

- Các kỹ sư Network security sử dụng Wireshark để kiểm tra các vấn đề bảo mật.

- Các kỹ sư QA sử dụng Wireshark để xác minh các network applications.

- Các developers sử dụng Wireshark để gỡ lỗi triển khai giao thức.

- Mọi người sử dụng Wireshark để học internals giao thức mạng.

Không chỉ các tình huống trên, Wireshark cũng có thể hữu ích trong nhiều tình huống khác nữa.

**Tính năng :**

- Có sẵn cho UNIX và Windows.

- Chụp dữ liệu gói trực tiếp từ giao diện mạng.

- Mở các tệp có chứa dữ liệu gói được bắt bằng tcpdump/ WinDump, Wireshark và một số chương trình packet capture khác.

- Nhập các gói từ các tệp văn bản có chứa các hex dumps của packet data.

- Hiển thị các gói với thông tin giao thức rất chi tiết.

- Lưu dữ liệu gói bị bắt.

- Xuất một số hoặc tất cả các gói trong một số định dạng capture file.

- Lọc các gói tin trên nhiều tiêu chí.

- Tìm kiếm các gói trên nhiều tiêu chí.

- Colorize gói hiển thị dựa trên bộ lọc.

- Tạo các số liệu thống kê khác nhau.



## Cookie



### Cookie là gì?

****

Cookie là một đoạn văn bản ghi thông tin được tạo ra và lưu trên trình duyệt của máy người dùng. Cookie thường được tạo ra khi người dùng truy cập một website, cookie sẽ ghi nhớ những thông tin như tên đăng nhập, mật khẩu, các lựa chọn do người dùng lựa chọn đi kèm. Các thông tin này lưu trong máy tính thường được dùng để nhận ra người dùng khi truy cập một trang web. Cookie là những tập tin mà trang web gửi đến máy tính của người dùng. .

Khi người dùng truy cập đến một trang web có sử dụng cookie, web server của trang đó sẽ tự động gửi cookie đến máy tính của người dùng. Những cookie này tự động được tổ chức trong hệ thống máy tính. Khi truy cập đến các trang web sử dụng được cookie đã lưu, những cookie này tự động gửi thông tin của người dùng về cho chủ của nó (người tạo ra cookie). Tuy nhiên những thông tin do cookie ghi nhận không được tiết lộ rộng rãi, chỉ có website chứa cookie mới có thể xem được những thông tin này. Cookie được xem là một thành phần không thể thiếu được với những website có khối lượng dữ liệu lớn, có số lượng người dùng đông, và có những chức năng đi kèm với thành viên đăng ký. Phần lớn các website này là các website thương mại điện tử.

Cookie có thể tiết lộ bí mật về người dùng. Các trình duyệt hiện đại cho phép đề phòng việc các cookie tiết lộ bí mật bằng các cài đặt chế độ cấm gửi ngược lại hay là hỏi ý kiến người dùng máy trước khi gửi thông tin cho ai. Tuy khối lượng thông tin mà một cookie nắm không nhiều nhưng lại đóng một vai trò hết sức quan trọng đặc biệt thời đại bùng nổ của Internet marketing.

Cookie thường được xóa hoặc hủy bỏ sau một thời gian nhất định.

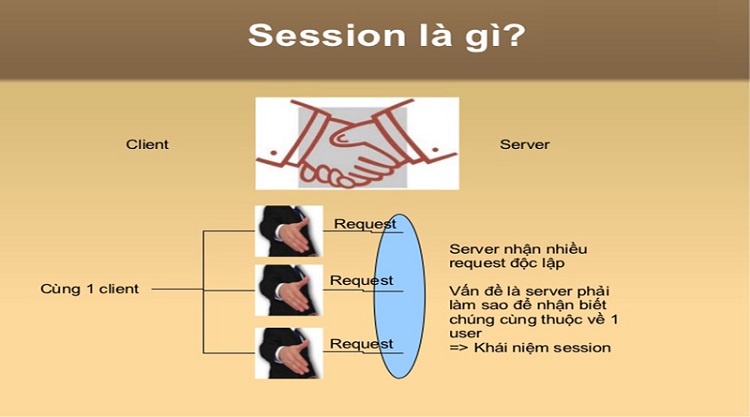


# Nội dung lý thuyết



## Phương pháp tấn công SESSION HIJACKING

### Giới thiệu SESSION là gì ?



Session có nghĩa là phiên làm việc. Khi bạn đi làm thì phiên làm việc của bạn được tính từ lúc bạn đặt chân vào công ty cho tới lúc ra về. Đối với máy tính thì một session được tính từ **lúc bạn truy cập một website, ứng dụng thông qua một trình duyệt web, cho tới lúc thoát khỏi nó.**

Lúc này, trình duyệt web sẽ gửi một yêu cầu truy cập tới máy chủ (server) của website/ứng dụng đó và khởi tạo một phiên làm việc trên server. Session này tồn tại ngay cả khi bạn chuyển sang trang khác hay mục khác của website/ứng dụng. Cuối cùng, session chỉ hết hiệu lực khi bạn rời khỏi trang, đóng ứng dụng, hoặc hết thời hạn cho phép (timeout) được lập trình viên quy định sẵn.

Với mỗi người dùng truy cập vào website/ứng dụng, họ được ghi nhận bởi một session có một mã số sessionID riêng biệt. Tất nhiên là các session chỉ được tắt theo đúng tiêu chí trên, vì thế có thể tồn tại hàng trăm session cùng một lúc. Với số lượng lớn như vậy, nếu các session chứa quá nhiều thông tin thì sẽ ảnh hưởng đến khả năng chịu tải của server. Cho nên, trong mỗi session chỉ **lưu lại các thông tin cơ bản**như: thông tin đăng nhập, thời gian truy cập, thông tin giỏ hàng (trong các trang TMĐT)…

Một ví dụ điển hình của session là khi bạn sử dụng dịch vụ internet banking của các ngân hàng, nếu thoát khỏi trang rồi quay lại thì bạn bắt buộc phải đăng nhập lần nữa. Hoặc nếu bạn đã đăng nhập nhưng không làm gì hết sau một khoảng thời gian, session của bạn cũng tự động hết hiệu lực.

Cookie có nhiều điểm tương đồng với session nên rất dễ gây hiểu lầm. Tuy nhiên, có 2 nét khác biệt nổi bật nhất giữa session và cookie: **(1) session được lưu trên server còn cookie được giữ trong máy tính của bạn**, vì lẽ đó **(2) session không thể được truy cập và hiệu chỉnh bởi người dùng**.

Cookie là một **tệp tin tạm thời lưu trên ổ cứng máy tính, chứa các thông tin về hoạt động sử dụng website/ứng dụng**của người dùng.

Lần đầu tiên bạn truy cập vào website/ứng dụng nào đó, server sẽ gửi về và lưu tạm trên máy tính của bạn một tệp tin cookie(1). Lần ghé thăm tiếp theo, trình duyệt sẽ gửi tệp cookie(1) đó lên server để phân tích các hoạt động trước đó của bạn. Sau đó, server sẽ lại gửi về một tệp cookie(2) khác, bao gồm thông tin có trong tệp cookie(1) cũ và thông tin mới được thêm vào.

Vòng lặp cứ thế tiếp diễn cho đến khi cookie hết hạn timeout hoặc khi bạn xóa nó đi (thông qua các công cụ dọn rác trình duyệt và máy tính). Và ngày nay hầu như tất cả các cookie đều tồn tại vĩnh viễn (persistant cookie) trong ổ cứng của bạn, còn không thì là tồn tại trong một thời gian rất rất dài, phục vụ cho mục đích theo dõi và thu thập dữ liệu người dùng.

Tác dụng của cookie là cho phép nhà phát triển **nắm được thông tin sử dụng website/ứng dụng của người dùng, từ đó áp dụng vào các công nghệ khác** như: quảng cáo, gợi ý, thống kê…

Nếu bạn chưa hiểu rõ về cookie, thì có thể thử làm một thử nghiệm sau: truy cập vào một trang TMĐT bất kỳ ([**Tiki**](https://tiki.vn/), [**Lazada**](https://www.lazada.vn/)), nhấp vào xem một sản phẩm nào đó. Sau đó, bạn vào Faceboook và bắt đầu lướt, bạn sẽ có thể thấy những sản phẩm vừa xem ngay trong những khung quảng cáo của Facebook. Tất nhiên là bạn cần phải tắt tất cả các chức năng chặn theo dõi và quảng cáo của trình duyệt trước thì mới có thể thực hiện được việc này.

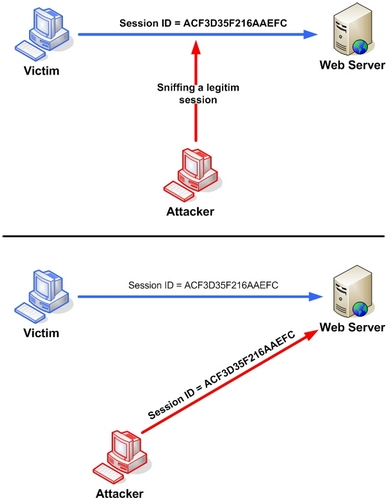
Như đã nói ở trên, cookie được lưu trên máy tính của bạn, và vì vậy, **có thể bị truy cập và chỉnh sửa.** Các hacker có thể lợi dụng cookie để chiếm lấy các thông tin nhạy cảm và tấn công cả hai bên: website và người dùng. Là lập trình viên, quản trị viên của website/ứng dụng, bạn nên thiết kế sao cho cookie không được lưu giữ những dữ liệu quan trọng của cả doanh nghiệp lẫn khách hàng.

Là người dùng, bạn nên quản lý các cookie được lưu trên máy tính, chỉnh sửa hoặc xóa bỏ các cookie chứa thông tin nhạy cảm. Ngoài hacker ra thì các nhà cung cấp dịch vụ cũng rất thèm khát dữ liệu cá nhân của bạn và có thể sử dụng chúng vào các mục đích không hề có lợi cho bạn.

|  |  |
| --- | --- |
| Session | Cookie |
| Session được lưu trữ trên server máy chủ | Cookie được lưu trữ trên máy tính của người dùng |
| Dữ liệu của session không dễ dàng được thay đổi | Dữ liệu của cookie dễ dàng đươc thay đổi vì lưu ở phía máy người dùng |
| Session sẽ mất đi khi người dung kết thúc phiên làm việc đó | Cookie có thể được lưu trữ trong một khoảng thời gian dài sau khi hết hạn thời gian hiệu lực |



## Giới thiệu về SESSION HIJACKING



**Session Hijacking** là quá trình chiếm lấy một session đang hoạt động, nhằm mục đích vượt qua quá trình chứng thực truy cập bất hợp lệ vào thông tin hoặc dịch vụ của một hệ thống máy tính..Khi một user thực hiện kết nối tới server qua quá trình xác thực, bằng cách cung cấp ID người dùng và mật khẩu của mình. Sau khi người dùng xác thực, họ có quyền truy cập đến máy chủ A và hoạt động bình thường. 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 ngườidùng 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. Đối với cơ quan pháp lý, có thể dung làm bằng chứng để truy tố, đối với kẻ tấn công, có thể dùng thu thập thông tin như ID người dùng và mật khẩu. Điều này gây nhiều nguy hại đến người dùng.



### Nguyên nhân có thể thai thác lỗi Session Hijacking:

- Không cấu hình Account Lockout cho Session ID không hợp lệ

- Thuật toán phát sinh Session ID yếu

- Không xác định thời gian hết hạn Session

- Kích thước Session ID nhỏ

- Truyền thông dạng Clear text

### Mối nguy hiểm từ Hijacking

- Hầu hết các biện pháp đối phó không làm việc trừ khi bạn dùng mã hóa

- Chiếm quyền điều khiển là dễ dàng khởi động

- Mối đe dọa đánh cắp nhận dạng, mất thông tin, gian lận,…

- Hầu hết các máy tính sử dụng giao thức TCP/IP dễ dàng bị tấn công

- Có thể bảo vệ và chống lại nó chỉ 1 phần, trừ khi chuyển qua giao thức bảo mật khác

### Các kỹ thuật SESSION HIJACKING chính :

**Brute Forcing :** Kẻ tấn công cố thử các ID khác nhau cho đến khi thành công

**Stealing :** Kẻ tấn công dùng các kỹ thuật khác nhau để lấy cắp các Session ID

**Calculating :** Sử dụng các ID không được tạo ra ngẫu nhiên, kẻ tấn công cố gắng tính toán các Session ID

### Các loại tấn công :

Tấn công chủ động : kẻ tấn công tìm kiếm phiên làm việc và chiếm quyền làm việc của nó

Tấn công thụ động : kẻ tấn công chiếm quyền điều khiển 1 phiên, nhưng ngừng lại, xem và ghi lại tất cả các lưu lượng truy cập được gửi ra

### Phương thức hoạt động của Session Hijacking

Quá trình tấn công Session Hijacking gồm có ba bước như sau :

- Dò Tìm Session : Hacker sẽ dò tìm các session đang mở và tính toán giá trị tuần tự của gói tin tiếp theo.

- Tái Đồng Bộ Kết Nối : Hacker gởi các tín hiệu TCP reset (RST) hay FIN để yêu cầu khởi động lại quá trình kết nối đồng thời đóng phiên làm việc cũ.

- Chèn Các Packet Tấn Công : lúc này hacker sẽ gởi đến máy chủ những gói tin TCP với số hiệu tuần tự đã được tính toán thích hợp với phiên làm việc do đó máy chủ sẽ chấp nhận những thông tin này giống như là các dữ liệu hợp lệ tiếp theo của người dùng bị tấn công. Nghĩa là, khi này các hacker có thể gởi đi một thông điệp trên chính Wall của nạn nhân bằng tài khoản Facebook của người bị tấn công

### Các Công Cụ Tấn Công Session Hijacking :

Có khá nhiều công cụ có thể tiến hành tấn công Session Hijacking đã được phát triển trước đây như Juggernaut chuyên sniff các TCP session trong môi trường mạng hoạt động với hub. Hoặc Hunt với chức năng giả mạo địa chỉ MAC với cơ chế ARP spoofing, reset và giám sát các kết nối, nghe lén đường truyền. 7 Hiện nay, nhiều công cụ mạnh mẽ khác được phát triển giúp cho hacker có thể tiến hành tấn công Session Hijacking dễ dàng hơn. Trong số đó phải kể đến Burp Suite, ứng dụng có mặt trong danh sách 125 công cụ bảo mật hàng đầu hiện nay có khả năng thay đổi dữ liệu trên quá trình truyền, đánh cướp session hay giả mạo cả các chứng chỉ điện tử dùng trong xác thực https



## Các phương pháp chống tấn công :

Để phòng chống không bị tấn công Session Hijacking thì chúng ta cần phòng tránh bị nghe lén, một khi hacker không thể nghe lén được thì cũng không thể tấn công vào session của người dùng. Một trong các giải pháp đế tránh các sniffer chính là mã hóa dữ liệu, mã hóa đường truyền với các kỹ thuật như dùng Secure Shell (SSH thay cho Telnet thông thường) khi quản trị từ xa hay áp dụng Secure Socket Layer (SSL dùng cho truyền thông qua HTTPS ). Ngoài ra chúng ta có thể ngăn không cho hacker tương tác vào đường truyền cũng giúp loại bỏ nguy cơ bị tấn công này, với những giải pháp hữu hiệu như dùng mạng riêng ảo (VPN), hay áp dụng IPSEC. Nhiều ý kiến còn cho rằng khi truy cập internet ở môi trường công cộng hãy dùng các thiết bị DCOM 3G cũng giảm đáng kể nguy cơ mất mát dữ liệu. Sau đây là một số khuyến nghị nhằm ngăn ngừa Session Hijacking :











### Dành cho người dùng

- Huấn luyện cho người dùng, nâng cao nhận thức an toàn thông tin.

- Sử dụng các thông tin truy cập khác nhau cho các tài khoản khác nhau.



### Dành cho lập trình viên

- Sử dụng mã hóa.

- Ứng dụng các giao thức an toàn.



### Dành cho quản trị server

- Hạn chế các kết nối đầu vào.

- Giảm các truy cập từ xa.

- Có chế độ xác thực mạnh mẽ.

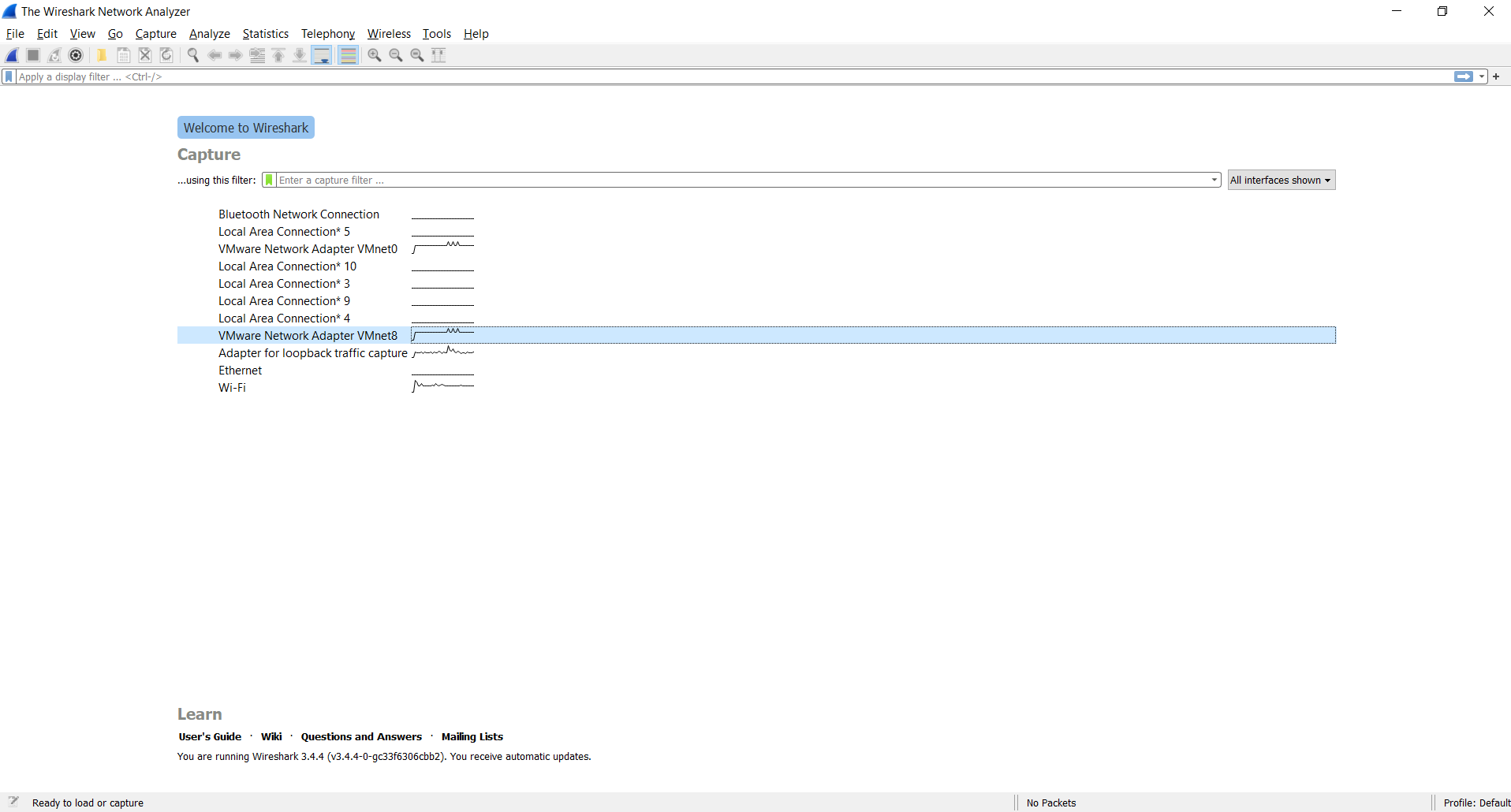
# Nội dung Demo

Thông tin thiết bị

* Máy hacker : ASUS Windows 10 64 bit
* Máy nạn nhân : máy ảo Windows 10 64 bit

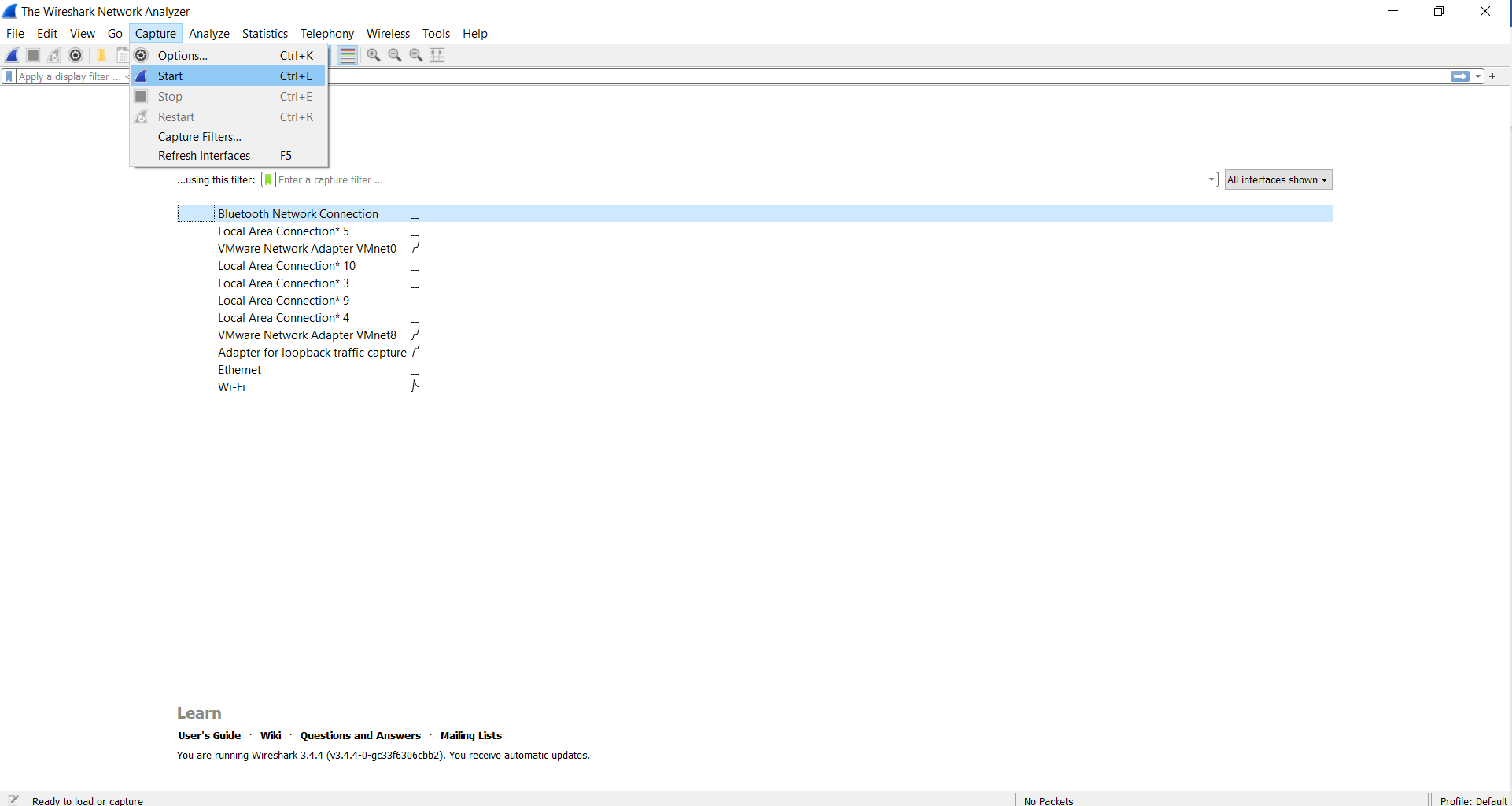
## Demo chi tiết

Tải và cài đặt ứng dụng WireShark để bắt các gói tin trên mạng.

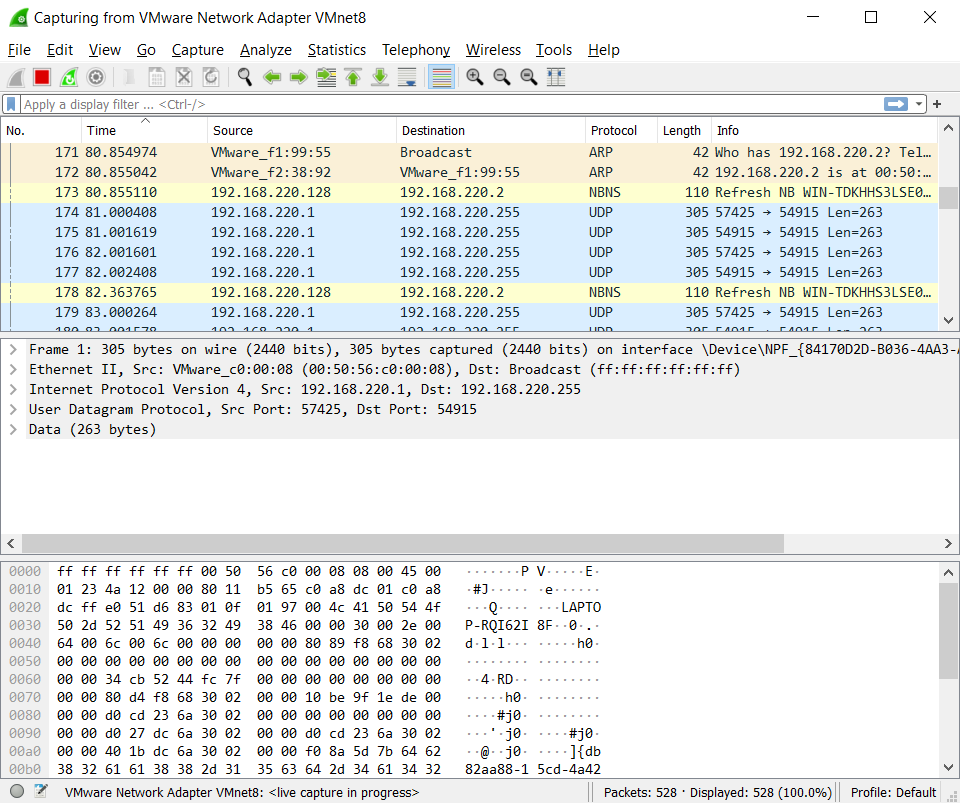


Hình 1 *Ứng dụng bắt gói tin Wireshark*

Capture > Start để bắt đầu theo dõi các gói tin



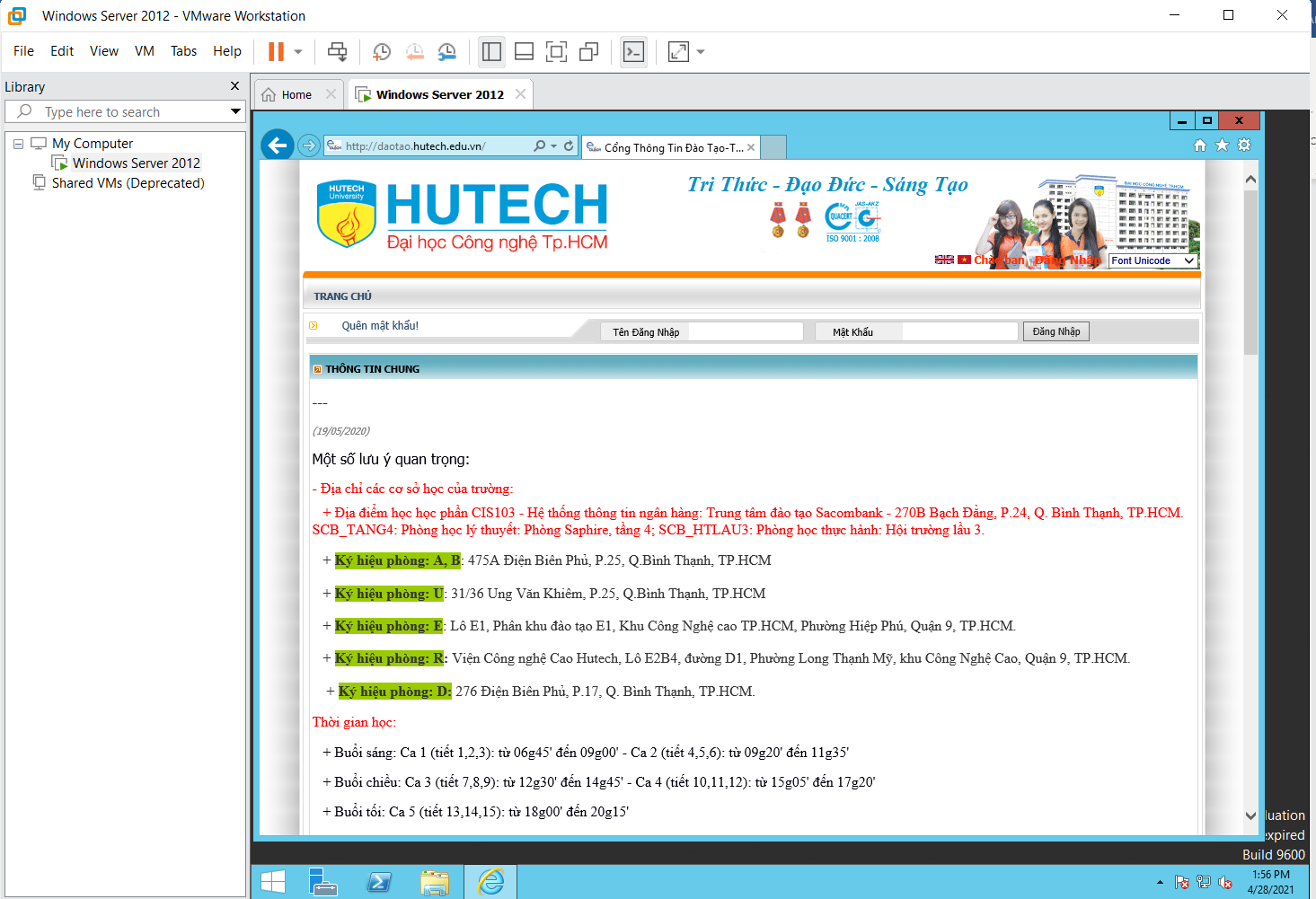
Hình 2 : Start ứng dụng bắt đầu nghe lén



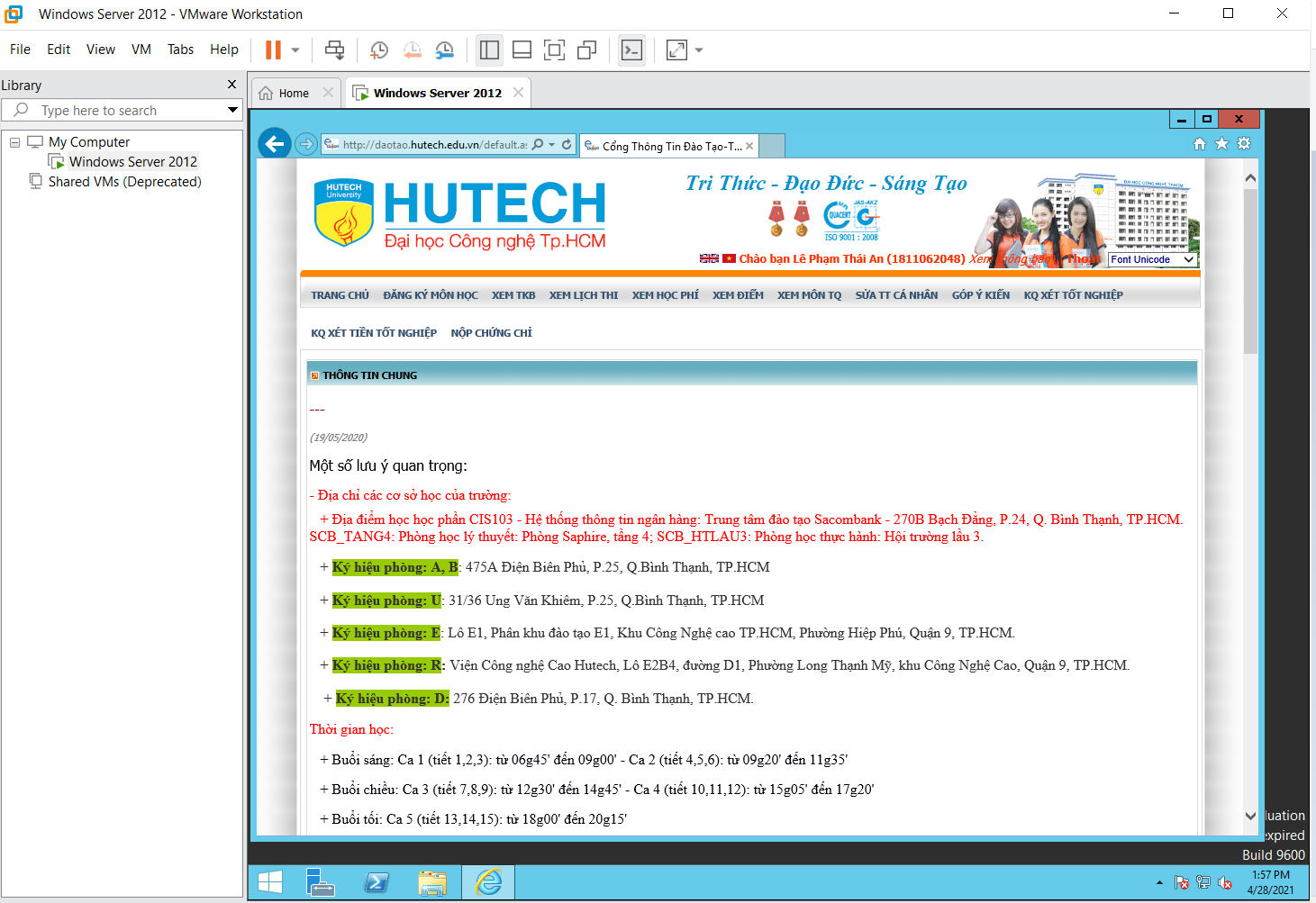
Hình 3: Các thông tin truyền và nhận

Trường hợp hacker có được thông tin địa chỉ IP máy nạn nhân và cùng dung chung một mạng.

Máy nạn nhân đăng nhập thông tin vào website daotao.hutech.edu.vn



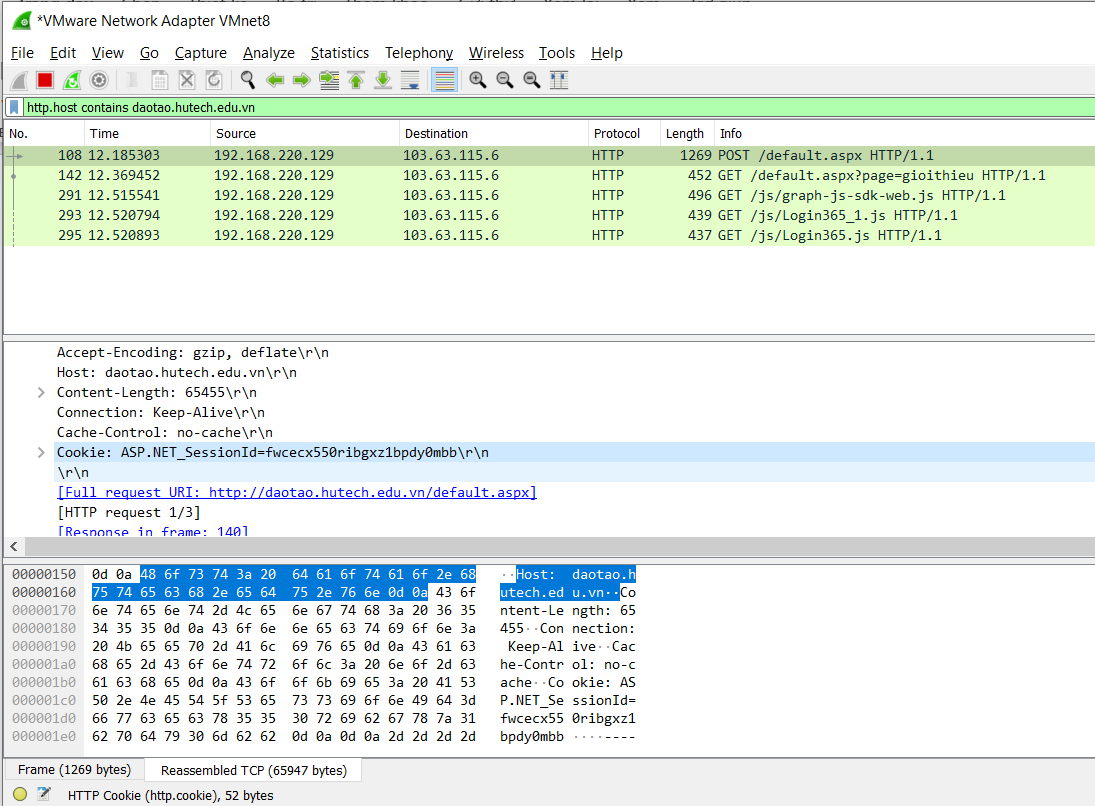
Hình 4-Máy nạn nhân đang đăng nhập daotao.hutech.edu,vn

**

Hình 5: Máy nạn nhân đã đăng nhập thành công trang daotao.hutech.edu.vn

Sau khi nạn nhân đăng nhập vào web ***daotao.hutech.edu.vn***

Hacker kiểm tra và bắt được gói tin POST chuyển đi từ máy nạn nhân

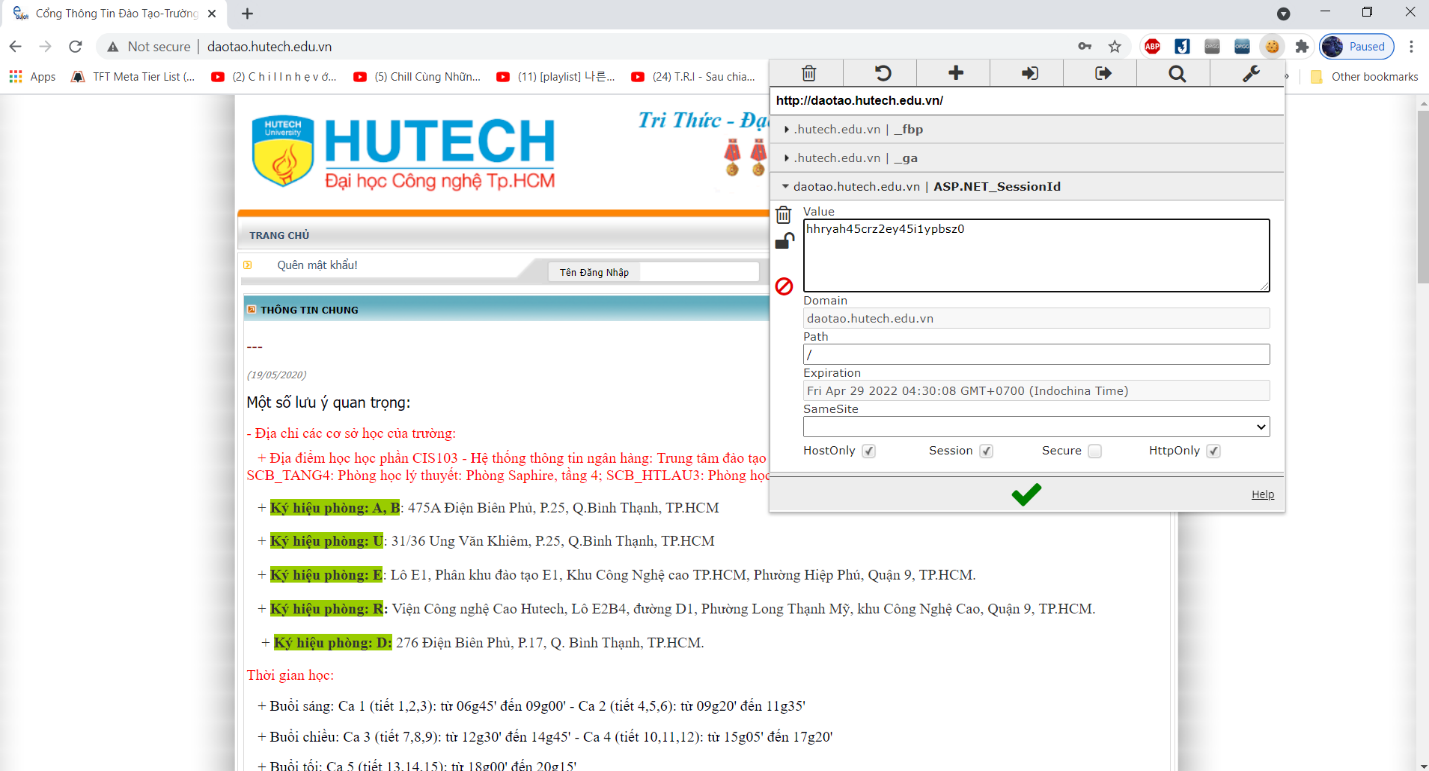


Hình 6 : Kiểm tra thông tin đăng nhập bắt được của máy nạn nhân

Bắt được SessionID của nạn nhân khi đăng nhập website thongtindaotao.sgu.edu.vn là

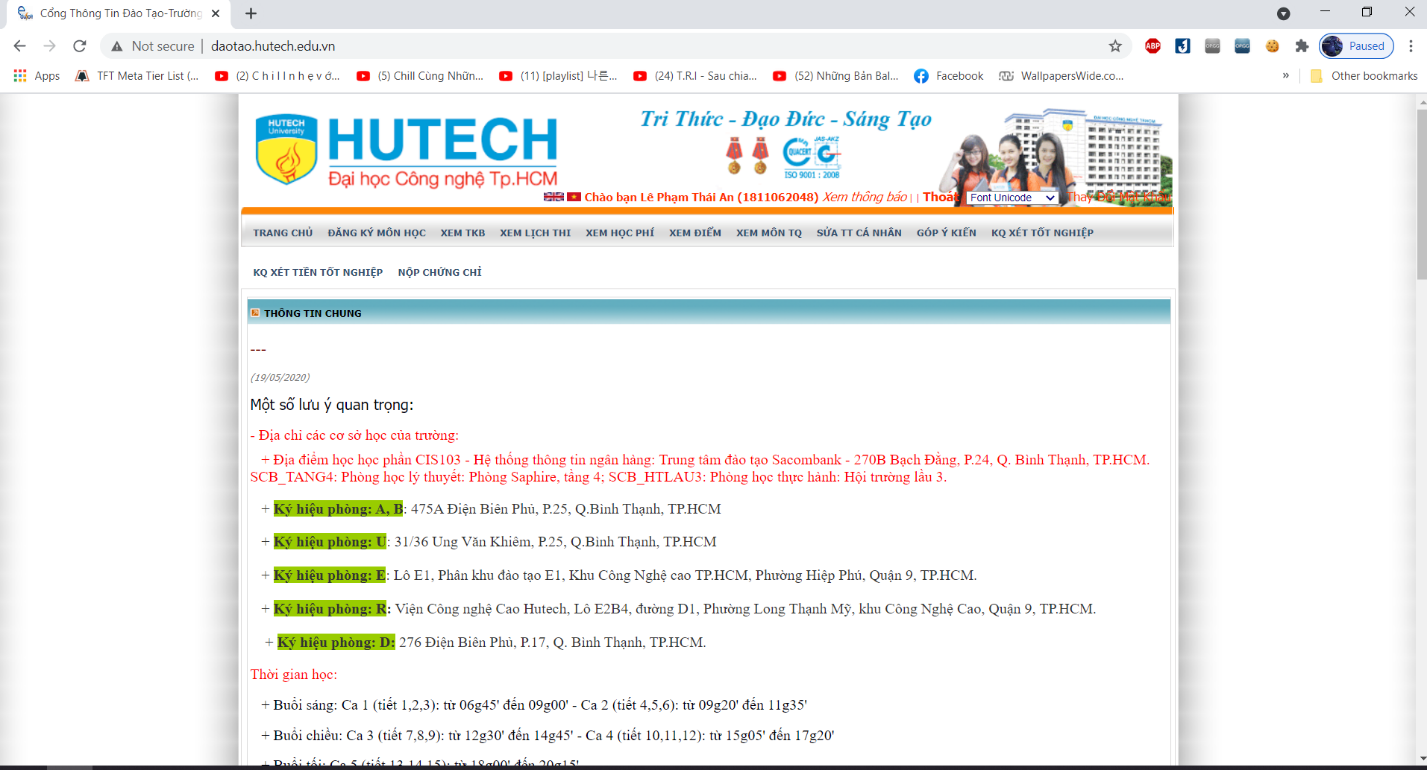
**ASP.NET\_SessionId=fwcecx550ribgxz1bpdy0mbb**

Hacker vào trang web daotao.hutech.edu.vn , trên trình duyệt tải extension của Google chrome để thay đổi giá trị cookie



Hình 7: Máy tấn công mở edit cookie

Nhập sessionId vào khung giá trị, nhấn Apply và tiến hành F5 load lại trang, hacker đã đăng nhập được vào phiên làm việc hiện tại này của nạn nhân.

******

Hình 8: Máy tấn công đăng nhập thành công vào phiên của nạn nhân

Tài liệu tham khảo

[1] Cache, session, cookie là gì? Phân biệt cache, session và cookie : <https://bitly.com.vn/lEX5a>

[2] Tìm hiểu về tấn công Man in the Middle (MITM) – Session Hijacking (<https://quantrimang.com/tim-hieu-ve-tan-cong-man-in-the-middle-chiem-quyen-dieu-khien-session-67520>)

[3] Tấn công Session Hijacking (<https://www.youtube.com/watch?v=dJ1hETRveqU>)