MỤC LỤC

[Bài 1: TRIỂN KHAI GIAO THỨC PAP 2](#_Toc192688451)

[1.1. Mô hình 2](#_Toc192688452)

[1.1.1. Triển khai PAP 1 chiều 2](#_Toc192688453)

[1.1.2. Triển khai PAP 2 chiều 6](#_Toc192688454)

[1.2. Tổng kết 8](#_Toc192688455)

[BÀI 2: TRIỂN KHAI GIAO THỨC CHAP 8](#_Toc192688456)

[2.1. Cấu hình 8](#_Toc192688457)

[2.2. Tổng kết 12](#_Toc192688458)

[BÀI 3: TRIỂN KHAI GIAO THỨC KERBEROS 13](#_Toc192688459)

[3.1. Triển khai hệ thống sử dụng xác thực kerberos 13](#_Toc192688460)

[3.1.1. Mô hình 13](#_Toc192688461)

[3.1.2. Triển khai hệ thống 13](#_Toc192688462)

[3.2. Sử dụng MIT Kerberos 18](#_Toc192688463)

[3.4. Triển khai máy chủ dịch vụ và máy chủ Kerberos riêng biệt 22](#_Toc192688464)

[3.5. Tổng kết 28](#_Toc192688465)

# Bài 1: TRIỂN KHAI GIAO THỨC PAP

## 1.1. Mô hình

**A red line with black numbers

Description automatically generated**

- HMD1: Router đóng vai trò máy chủ xác thực, kiểm tra thông tin đăng nhập và cấp quyền truy cập nếu hợp lệ.

- HMD2: Router đóng vai trò thiết bị khách, gửi thông tin đăng nhập để xác thực.

- Kết nối: HMD1 và HMD2 kết nối trực tiếp qua cổng serial s0/0.

- Dải địa chỉ IP: 192.168.1.0/24.

### 1.1.1. Triển khai PAP 1 chiều

A screenshot of a computer

Description automatically generated- Cấu hình HMD1:

- Cấu hình HMD2:

A screen shot of a computer

Description automatically generated

- Kiểm tra kết nối:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

- Cấu hình PPP trên cổng serial s0/0 của HMD2 (Client gửi username/password)

A black background with yellow text

Description automatically generated

* Dùng lệnh “encapsulation PPP” để cấu hình PPP (Point-to-Point Protocol)

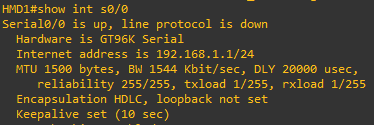
- Kiểm tra cấu hình cổng serial s0/0 của router HMD2

A screen shot of a computer

Description automatically generated

* “Encapsulation PPP”: Giao thức PPP đã được khởi tạo trên cổng serial s0/0 của HMD2
* “LCP REQsent”(Link Control Protocol Request sent): Giao thức kiểm soát kết nối đang trong giai đoạn kết nối PPP vì chưa nhận được phản hồi từ bên HMD1 do chưa cấu hình
* “loopback not set”

- Kiểm tra cấu hình cổng serial s0/0 của router HMD1 khi chưa cấu hình



* HMD1 chưa được cấu hình PPP

A black background with yellow text

Description automatically generated- Cấu hình PPP trên cổng serial s0/0 của HMD1 (Server xác thực)

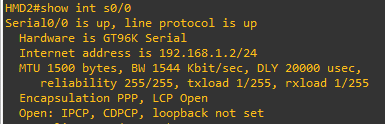
- Kiểm tra cấu hình cổng serial s0/0 của router HMD1 khi đã cấu hình

A screenshot of a computer

Description automatically generated

* “LCP Open”: Hoàn tất thương lượng, đường link PPP được thiết lập.

- Kiểm tra cấu hình cổng serial s0/0 của router HMD2 khi HMD1 đã cấu hình



* “LCP Open”: Hoàn tất thương lượng, đường link PPP được thiết lập

A screen shot of a computer

Description automatically generated- Khai báo thông tin xác thực cho router HMD2

* “ppp authentication pap”: kích hoạt quá trình xác thực PAP

A screenshot of a computer screen

Description automatically generated- HMD2 gửi username/password để xác thực với HMD1

- Shutdown cổng serial s0/0 rồi sử dụng câu lệnh “*debug ppp authentication*” để xem đầu ra xác thực PPP thời gian thực

A screen shot of a computer

Description automatically generated

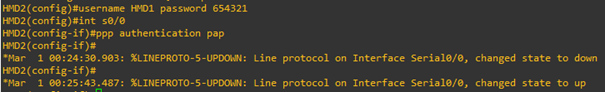
A screenshot of a computer

Description automatically generated- No shutdown để quan sát toàn bộ quá trình xác thực

* Se0/0 PPP: Using default call direction, Treating connection as a dedicated line
* Router HMD1 bắt đầu quá trình PPP trên cổng Serial0/0, coi đây là kết nối điểm-điểm (dedicated line).
* Authorization required / PAP: I AUTH-REQ id 2 len 16 from "HMD2"
* HMD1 yêu cầu xác thực
* “AUTH-REQ from HMD2”: router HMD2 đang gửi username/password để xác thực.
* PAP: Authenticating peer HMD2
* HMD1 tiến hành kiểm tra thông tin đăng nhập của HMD2.
* Sent PAP LOGIN Request / Received LOGIN Response PASS
* HMD1 gửi yêu cầu đăng nhập đến cơ sở dữ liệu
* Nhận lại “Response PASS” nghĩa là xác thực thành công
* Sent LCP AUTHOR Request / Received AAA AUTHOR Response PASS
* Sau khi xác thực thành công, router tiếp tục thực hiện bước authorization (ủy quyền). Nếu AAA được bật, router sẽ gửi yêu cầu đến AAA(Authentication, Authorization, Accounting).
* “Response PASS” báo rằng HMD2 được phép sử dụng kết nối.
* Sent CDPCP AUTHOR Request/Sent IPCP AUTHOR Request
* CDPCP (Cisco Discovery Protocol Control Protocol)
* IPCP (IP Control Protocol)

### 1.1.2. Triển khai PAP 2 chiều

- Cấu hình tương tự HMD2 như HMD1



- HMD1 gửi username/password để xác thực với HMD2

A screenshot of a computer screen

Description automatically generated

- Shutdown cổng serial s0/0 rồi sử dụng câu lệnh “*debug ppp authentication*” để xem đầu ra xác thực PPP thời gian thực

A screen shot of a computer

Description automatically generated

- No shutdown để quan sát toàn bộ quá trình xác thực

A screenshot of a computer program

Description automatically generated

- Các gói tin wireshark bắt được

A screenshot of a computer

Description automatically generated

* No 1201 – 1251 : PAP 1 chiều
* No 2266 – 2366: PAP 2 chiều (Hai router xác thực qua lại)

A screenshot of a computer

Description automatically generated

* Số thứ tự: 2268
* Độ dài khung: 9 bytes
* Kiểu đóng gói: PPP
* Authenticate-Ack phản hồi xác nhận thành công nếu thông tin đúng với mã hex “c0 23 02”.
* Authenticate-Nak phản hồi xác nhận không thành công với mã hex “c0 23 03”
* Message: Trống(không có thông báo báo lỗi)

A screenshot of a computer

Description automatically generated

* Authenticate-Request gửi yêu cầu xác thực từ client tới server với mã hex “c0 23 01”
* Trong đó, mật khẩu được gửi dưới dạng plain-text, dễ bị tấn công nghe lén

## 1.2. Tổng kết

- PAP là một giao thức xác thực đơn giản, dễ triển khai nhưng không an toàn vì thông tin xác thực được gửi đi dưới dạng plain-text.

- Lý thuyết về PAP phản ánh chính xác cách hoạt động của nó trong thực tế. Tuy nhiên, khi triển khai, ta thấy rõ được điểm yếu bảo mật nên khi bắt buộc phải dùng PAP thì ta nên kết hợp với giao thức bảo mật khác để mã hoá đường truyền hoặc dữ liệu.

- Khi triển khai giao thức thì còn có các giao thức phụ khác kèm theo như là CDPCP, IPCP.

# BÀI 2: TRIỂN KHAI GIAO THỨC CHAP

## 2.1. Cấu hình

- Cấu hình địa chỉ IP của 2 router như chương 1. Tuy nhiên, mật khẩu của 2 router cần giống nhau vì giao thức CHAP sẽ sử dụng hàm băm để băm mật khẩu.

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

* **“**ppp authentication chap”: Kích hoạt quá trình xác thực CHAP

- Shutdown cổng serial s0/0 rồi sử dụng câu lệnh “*debug ppp authentication*” để xem đầu ra xác thực PPP thời gian thực

A screen shot of a computer

Description automatically generated

A screen shot of a computer

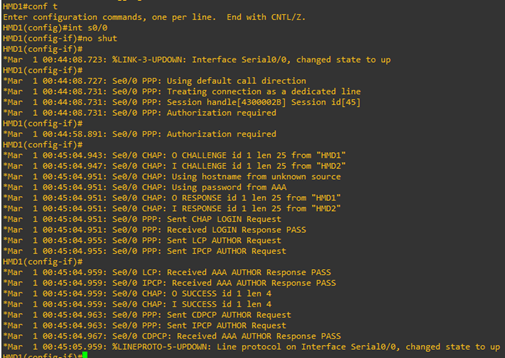
Description automatically generated

- No shutdown để quan sát toàn bộ quá trình xác thực

A screenshot of a computer

Description automatically generated

* HMD2 gửi Challenge tới HMD1 (O CHALLENGE - Outgoing)
* HMD2 nhận Challenge từ HMD1 (I CHALLENGE - Incoming)
* “Using password from AAA” : Cả hai thiết bị sử dụng thông tin xác thực từ AAA (Authentication, Authorization, Accounting)
* HMD2 gửi Response chứa mật khẩu dạng hash đến HMD1(O RESPONSE – Outgoing)
* HMD2 nhận Response từ HMD1 (I RESPONSE – Incoming)
* “sent CHAP LOGIN Request”: Thiết bị gửi CHAP LOGIN Request
* “Received LOGIN Response PASS”: Nhận phản hồi PASS (đăng nhập thành công)



- Tương tự như HMD2, vì cả hai thiết bị đang thực hiện xác thực CHAP hai chiều

- Các gói tin wireshark bắt được

A screenshot of a computer

Description automatically generated

* Ta thấy password đã được băm nên sẽ an toàn hơn giao thức PAP

A screenshot of a computer

Description automatically generated

* “C2 23”: Mã giao thức dành cho CHAP trong PPP
* “Challenge (1)”: Gói tin challenge, HMD1 đang yêu cầu HMD2 chứng minh danh tính và có mã là 01. (c2 23 01)
* A screenshot of a computer

  Description automatically generatedValue trong challenge: là giá trị ngẫu nhiên (nonce) do HMD1 tạo ra
* A screenshot of a computer

  Description automatically generated“Success (3)”: Gói tin success, xác nhận xác thực thành công và có mã là 03 (c2 23 03)
* “Response (2)”: Gói tin response, HMD2 gửi phản hồi để xác minh danh tính và có mã là (c2 23 02)
* Ngoài ra còn có gói tin Failure (xác thực thất bại) với mã là (c2 23 04)
* Value trong response: là giá trị hash MD5(Identifier + Password + ChallengeValue)

## 2.2. Tổng kết

* CHAP là giao thức xác thực không truyền mật khẩu dạng rõ nhưng vẫn lưu mật khẩu dạng rõ và yêu cầu mật khẩu phải giống nhau trên cả hai thiết bị
* CHAP sử dụng xác thực hai chiều, đảm bảo cả hai bên đều xác minh danh tính lẫn nhau, nâng cao mức độ bảo mật so với PAP.
* Các gói tin thu thập được từ Wireshark hoàn toàn khớp với quy trình xác thực CHAP theo lý thuyết, cho thấy phương thức này hoạt động đúng như mong đợi.
* Khi triển khai giao thức thì còn có các giao thức phụ khác kèm theo như là CDPCP, IPCP.
* CHAP là một lựa chọn tốt để xác thực trong mạng PPP vì có tình bảo mật hơn PAP.
* CHAP có tốc độ chậm hơn PAP

**BẢNG SO SÁNH PAP VÀ CHAP**

| **Tiêu chí** | PAP (Password Authentication Protocol) | CHAP (Challenge Handshake Authentication Protocol) |
| --- | --- | --- |
| **Bảo mật** | - Mật khẩu được gửi dưới dạng plain-text (dễ bị tấn công nghe lén). - Không có cơ chế bảo vệ dữ liệu xác thực. | - Mật khẩu được băm (hash) trước khi gửi, đảm bảo an toàn hơn. - Sử dụng cơ chế Challenge-Response để xác thực. |
| **Hiệu suất** | - Nhanh hơn do quy trình xác thực đơn giản. | - Chậm hơn do quy trình băm và xác thực phức tạp hơn. |
| **Trường hợp sử dụng** | - Phù hợp với môi trường có độ tin cậy cao, ít rủi ro bảo mật. | - Phù hợp với môi trường yêu cầu bảo mật cao. |

# BÀI 3: TRIỂN KHAI GIAO THỨC KERBEROS

## 3.1. Triển khai hệ thống sử dụng xác thực kerberos

### 3.1.1. Mô hình

A close-up of a line

Description automatically generated

- Máy client: Windows 10

- Máy server: Windows Server 2008

### 3.1.2. Triển khai hệ thống

- Đặt địa chỉ IP cho máy Client: 10.5.14.105/24

- Đặt địa chỉ IP cho máy Server: 10.5.14.5/24

A screenshot of a computer

Description automatically generatedA screenshot of a computer screen

Description automatically generated

- Thiết lập cho Server và Client kết nối chung 1 LAN

- Tạo domain hoangminhduong.com mới

A screenshot of a computer

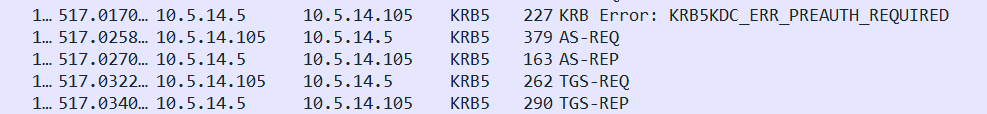
Description automatically generated

- Kết nối Client với Server

A white rectangular object with a black border

Description automatically generated with medium confidence

- Vậy là ta đã triển khai xong hệ thống và bắt được các gói tin bằng wireshark



- Có tổng cộng 5 loại gói tin:

+ AS-REQ: Authentication Server Request

+ AS-REP: Authentication Server Reply

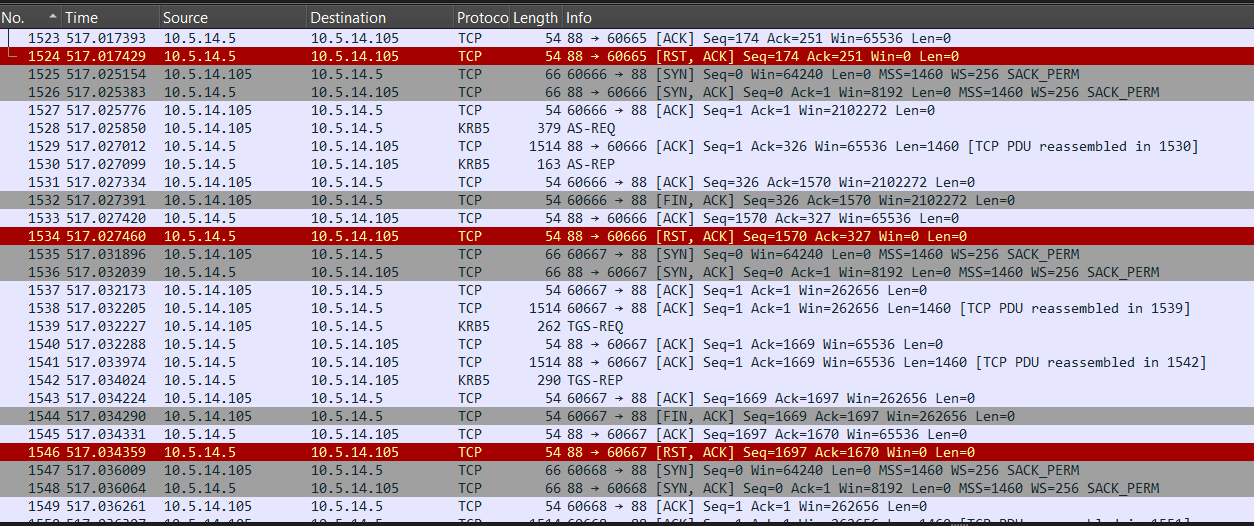
+ TGS-REQ: Ticket Granting Server Request

+ TGS-REP: Ticket Granting Server Reply

+ KRB Error

5 loại gói tin này thể hiện tương tác giữa Client với KDC (Key Distribution Center) với mục đích là lấy được phiếu dịch vụ (ST – Service Ticket) và yêu cầu dịch vụ từ Server

- Ta còn thấy được các kết nối TCP sử dụng bắt tay ba bước



- Gói tin AS-REQ được gửi từ Client tới Server để yêu cầu xác thực

A screenshot of a computer program

Description automatically generated

* Record mark: 321 bytes – Tổng kích thước gói tin là 321 bytes
* pvno (Protocol Version Number): Phiên bản Kerberos (5)
* msg-type: loại tin (AS-REQ) và số thể lớp ứng dụng (10)
* padata: truyền tải thông tin bổ sung trong các yêu cầu hay phản hồi  
  xác thực
  + PA-ENC-TIMESTAMP: Mã hoá timestamp để tránh tấn công replay
  + PA-PAC-REQUEST: Truyền tải yêu cầu truy cập
* kdc-options: flag cho phiếu kết quả (40810010 là kết hợp từ các flag  
  nhỏ hơn đại diện cho từng kết quả)
* cname: chứa tên người dùng đang xác thực (administrator)
* realm: miền xác thực Kerberos, có thể là tên Server hay Domain
* sname: chứa tên dịch vụ đang được yêu cầu
* till: thời gian hết hạn của phiếu yêu cầu (TGT)
* rtime: thời gian tối đa mà phiếu yêu cầu (TGT) tồn tại trước khi phải  
  gia hạn
* nonce: Số tạo ngẫu nhiên, duy nhất và được sử dụng trong các tin nhắn  
  Keberos
* etype: Các loại mã hoá được yêu cầu
* address: IP của Client

- Gói tin AS-REP được phản hồi từ KDC tới Client sau khi nhận AS-REQ

A screenshot of a computer program

Description automatically generated

* Ticket: Chứa các thông tin về phiếu yêu cầu TGT
  + tkt-vno: Số phiên bản định dạng phiếu
  + realm: Vùng quản trị logic (thường dùng tên là DNS được tạo)
  + enc-part: Phiếu được mã hoá
* enc-part: Khoá phiên được mã hoá

- Tương tự với gói tin TGS-REQ và TGS-REP

A screenshot of a computer program

Description automatically generated

Máy khách sử dụng TGT trong AS-REP để yêu cầu một Ticket Granting Service (TGS) ticket từ máy chủ phân phối dịch vụ (Ticket Granting Server - TGS). Gói tin TGS-REQ chứa TGT và yêu cầu truy cập tới một dịch vụ cụ thể (service principal).

* + msg-type: krb-tgs-req (12), xác nhận đây là yêu cầu lấy vé TGS.
  + sname(ServiceName): yêu cầu vé dịch vụ cho giao thức CIFS (dùng để truy cập chia sẻ tệp) trên máy WIN-7ROPA2V06NT thuộc domain hoangminhduong.com

A screenshot of a computer program

Description automatically generated

- Máy chủ phân phối dịch vụ (TGS) kiểm tra thông tin trong TGT và phản hồi với gói tin TGS-REP chứa TGS ticket được mã hóa bằng khóa chia sẻ giữa máy khách và TGS. TGS ticket này sẽ được sử dụng để yêu cầu truy cập vào dịch vụ cụ thể .

## 3.2. Sử dụng MIT Kerberos

- Download phiên bản dành cho windows trên trang chủ

A screenshot of a computer program

Description automatically generated

- Cài đặt file cấu hình MIT Kerberos

Những thiết lập cho Kerberos được chỉ định thông qua một config file. Ta có thể điều chỉnh những thiết lập của Kerberos bằng cách điều chỉnh config file ở đường dẫn mặc đỉnh ở dưới. (Mặc định thư mục này bị ẩn nên cần phải hiển thị file ẩn để tìm được file này)

A screenshot of a computer

Description automatically generated

- Cấu hình config

A screenshot of a computer program

Description automatically generated

* Libdefaults: Những thiết lập sử dụng thư viện (lib) Kerberos V5
  + default\_realm: Vùng Kerberos mặch định
  + dns\_lookup\_kdc = true: Hệ thống sẽ tra cứu KDC qua DNS, thay vì chỉ dựa vào file cấu hình
  + ticket\_lifetime = 24h: Vé Kerberos (TGT) có hiệu lực trong 24 giờ
  + renew\_lifetime = 7d: Vé có thể được gia hạn lên đến 7 ngày
  + forwardable = true & proxiable = true: Vé có thể được chuyển tiếp hoặc ủy quyền
  + udp\_preference\_limit = 0: Bật TCP thay vì UDP để giao tiếp với KDC
  + default\_tkt\_enctypes = rc4-hmac  
    default\_tgs\_enctypes = rc4-hmac  
    → Sử dụng RC4-HMAC làm thuật toán mã hóa chính
  + default\_ccache\_name = FILE:C:\krb5\krbcache: Đường dẫn lưu trữ cache vé Kerberos
  + default\_keytab\_name = FILE:C:\krb5\krb5.keytab: File chứa keytab cho dịch vụ Kerberos
* Realms: Cấu hình KDC
  + hoangminhduong.com: là miền đang sử dụng
  + kdc = 10.5.14.5: Địa chỉ IP của KDC (Key Distribution Center)
  + admin\_server = 10.5.14.5 : Máy chủ quản trị KDC
  + default\_domain = hoangminhduong.com: Xác định miền Kerberos
* Domain\_realm: Mapping miền
* Mapping giữa tên miền DNS và realm Kerberos.
* Dấu chấm trước .hoangminhduong.com cho phép tất cả subdomains (ví dụ: sub.hoangminhduong.com)
* Logging: Cấu hình log
* Ghi log vào các file:

krb1ds.log: Log mặc định.

krb5kdc.log: Log của KDC.

kadmin.log: Log của Admin Server.

- Cập nhật biến môi trường cho cache

A screenshot of a computer program

Description automatically generated

- Sử dụng chức năng Get Ticket trên MIT Kerberos Manager

A screenshot of a computer

Description automatically generated

Ngay sau khi thực hiện bước trên, ta sẽ thấy Client sẽ thực hiện AS-REQ tới Server và được phản hồi AS-REP. Còn TGS có thể sẽ xuất hiện ngay hoặc một lúc mới xuất hiện (tuỳ vào việc Client có yêu cầu dịch vụ nào không, hoặc đến thời hạn phải làm mới ticket – renew ticket). Ta cũng có thể mô phỏng dịch vụ renew ticket  
bằng nút Renew Ticket bên cạnh nút Get Ticket

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

## 3.4. Triển khai máy chủ dịch vụ và máy chủ Kerberos riêng biệt

- Tạo một tài khoản trên Server

A screenshot of a computer

Description automatically generated

- Mở cổng TCP 88 trên tường lửa, và làm tương tự với UDP 88

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

- Thêm 2 phương thức xác thực Windows Authentication và Basic Authentication

A screenshot of a computer

Description automatically generated

- Tạo một web site mới (vào IIS Manager, chuột phải vào Sites => Add Website)

A screenshot of a computer

Description automatically generated

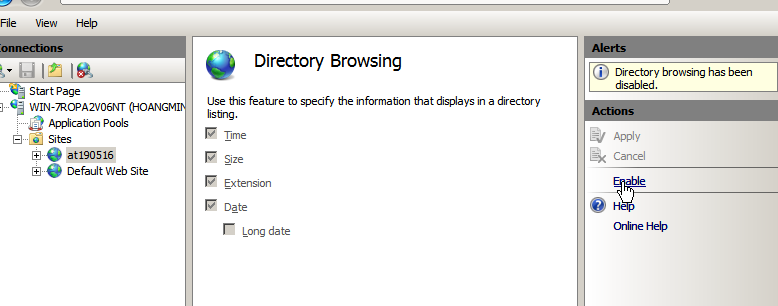
A screenshot of a computer

Description automatically generated

- Một bảng cấu hình sẽ xuất hiện:

* Site name: Tên trang
* Physical path: Chọn folder sẽ được hiển thị  
  trên trang (hãy tạo một folder trên server và cấp  
  quyền cho user dịch vụ - at190516)
* Binding: Cấu hình giao thức, IP, port, Host  
  name cho website (Host name không bắt buộc)
* Connect as: Những truy cập vào trang web sẽ  
  được coi như là người dung được chỉ định, ở đây ta  
  sẽ chỉ định user dịch vụ (at190516)

- Sau khi thiết lập website ta sẽ quay lại menu, mở Directory Browsing để bật chức năng hiển thị Folder trên website bằng cách chọn Enable



- Thiết lập xác thực: Quay lại menu chính và chọn Authentication. Tắt phương thức đang bật là Anonymous Auth và bật phương thức Windows Auth

A screenshot of a computer

Description automatically generated

- Mở port cần thiết trên tường lửa

A screenshot of a computer

Description automatically generated

- Kiểm tra:

Dùng client truy cập vào trình duyệt, nhập vào thanh địa chỉ http://<IP server dịch vụ>:<port nếu cần> Ngay sau khi nhập, website sẽ yêu cầu cung cấp thông tin xác thực của người dùng. Sau khi xác thực thành công, ta sẽ vào được website như ảnh bên dưới

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

- Kiểm tra gói tin Wireshark, ta thấy được mọi xác thực Kerberos là do Server Kerberos đảm nhận, Server dịch vụ sẽ chỉ cung cấp dịch vụ web

A screenshot of a computer screen

Description automatically generated

## 3.5. Tổng kết

- Qua mô hình triển khai giao thức Kerberos ta thấy được quá trình xác thực, trao đổi gói tin đều khớp với lý thuyết qua các giai đoạn.

- Kerberos đảm bảo tính an toàn cho hệ thống xác thực bằng cách:

* Xác thực hai chiều: Cả client và server đều cần chứng minh danh tính trước khi giao tiếp.
* Chống tấn công phát lại (Replay Attack): Dữ liệu chứa dấu thời gian, kết hợp với nonce ngẫu nhiên giúp ngăn kẻ tấn công sử dụng lại thông tin cũ.
* Bảo vệ mật khẩu: Mật khẩu người dùng không bao giờ được truyền trực tiếp trên mạng, thay vào đó là các token được mã hóa.
* Tập trung quản lý quyền truy cập: Tất cả xác thực diễn ra thông qua KDC, giúp quản lý dễ dàng hơn so với các mô hình truyền thống.

- Kerberos là giao thức xác thực mạnh mẽ nhất trong ba giao thức, sử dụng mô hình xác thực tập trung với vé (ticket) và mã hóa khóa đối xứng, giúp đảm bảo tính bảo mật và tính toàn vẹn trong quá trình truyền dữ liệu.