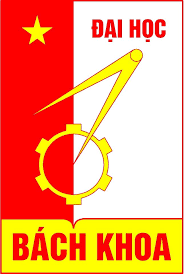
TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

Viện Công nghệ thông tin và truyền thông



**Báo cáo BTL: Tìm hiểu về xác thực Kerberos**

**Môn: Nhập môn An Toàn Thông Tin**

**Nhóm XX:**

|  |  |
| --- | --- |
| Họ và Tên | MSSV |
| Lương Tiến Mạnh | 20173254 |
| Mạc Quang Huy | 20173169 |
| Hồ Quốc Khánh | 20173191 |
| Đỗ Hoàng Nam | 20173270 |

**Hà Nội, ngày 31 tháng 5 năm 2020**

**NỘI DUNG TRÌNH BÀY**

**CHƯƠNG I: GIỚI THIỆU VỀ KEREROS 3**

* 1. **LỊCH SỬ PHÁT TRIỄN KERBEROS 3**
  2. **ỨNG DỤNG KERBEROS TRONG MÔI TRƯỜNG CÔNG NGHỆ SHAREPOINT .5**
  3. **CÁC PHẦN MỀM ỨNG DỤNG 16**

**CHƯƠNG II: NGUYÊN TẮC HOẠT ĐỘNG KERBEROS 17**

* 1. **MÔ HÌNH VÀ GIẢI THÍCH HOẠT ĐỘNG TÓM TẮT KERBEROS 17**
  2. **NGUYÊN TẮC HOẠT ĐỘNG CỦA KERBEROS 18**

**CHƯƠNG III: KẾT QUẢ THỰC NGHIỆM KERBEROS 24**

* 1. **HÌNH CHỤP DEMO QUÁ TRÌNH CÀI ĐẶT 24**
  2. **GIẢI THÍCH GÓI TIN LẤY ĐƯỢC TỪ WIRESHARK 33**

**Tài liệu tham khảo…………………………………………………………...…...36**

**CHƯƠNG I: GIỚI THIỆU VỀ KEREROS**

Kerberos là một giao thức mật mã dùng để xác thực trong các mạng máy tính theo mô hình client -server hoạt động trên những đường truyền không an toàn. Giao thức Kerberos có khả năng chống lại việc nghe lén hay gửi lại các gói tin cũ và đảm bảo tính toàn vẹn dữ liệu. Giao thức được xây dựng trên mật mã khóa đối xứng (vừa mã hóa vừa giải mã) và cần đến bên thứ 3 mà cả 2 phía tham gia giao dịch tin tưởng. Được phát triển trong dự án Athena của học viện công nghệ MIT.

* 1. **LỊCH SỬ PHÁT TRIỄN KERBOS**

Học viện công nghệ Massachusetts(Massachusetts Institute of Technology viết tắt là MIT) là học viện nghiên cứu và giáo dục ở thành phố Cambridge , Massachusetts Hoa Kỳ. MIT trở thành nổi tiếng trong khoa học công nghệ cũng như trong các lĩnh vực khác trong đó có quản lý, kinh tế, ngôn ngữ, khoa học chính trị và triết họctrong các lĩnh vực tiềm năng nhất và trường đào tạo là  Lincoln Laboratory và phòng trí tụy nhân tạo và khoa học vi tính, phòng thực hành truyền thông MIT, học viện Whitehead và trường quản lý Sloan của MIT  
Học viện kỹ thuật Massachusetts(MIT) phát triển Kerberos để bảo vệ các dịch vụ mạng cung cấp bởi dự án tên của giao thức được đặt tên của con chó 3 đầu Cerberus canh gác cổng địa ngục trong thần thọai hy lạp giao thức được phát triển dưới nhiều phiên bản trong đó phiên bản trong đó phiên bản từ 1 đến 3 chỉ dùng trong nội bộ MIT.

Các tác giả chính của phiên bản 4 Steve Miller và Clifford Neuman, đã xuất bản giao thức công chúng vào cuối thập niên 1980, mặc dù mục đích chính của họ là chỉ phục vụ cho dự án Athena. phiên bản 5 do John Kohl và Clifford Neuman thiết kế xuất hiện trong tài liệu RFC 1510 vào năm 1993 (được thay thế bởi RFC 4120 vào năm 2005) với mục đích sữa lỗi phiên bản 4 MIT đã cung cấp các phiên bản thực hiện Kerberos miễn phí dưới giấy phép tương tự như dùng cho các sản phẩm BDS.

Chính phủ Hoa Kỳ đã cấm xuất khẩu Kerberos vì nó sử dụng thuật tóan DES(56 bit) tuy nhiên trước khi chính sách xuất khẩu của Hoa Kỳ thay đổi (năm 2000) đã có phiên bản KTH-KRB viết tại Thụy Điển thực hiện Kerberos được phân phối rộng rãi bên ngòai Hoa Kỳ, phiên bản này dựa trên một phiên bản khác có tên là eBones, eBones dựa trên một phiên bản được xuất khẩu của MIT thực hiện Kerberos 4 (patch-level 9) gọi là Bones(lọai bỏ các hàm mật mã và các lạnh gọi chúng) Eric Young một lập trình viên người Australia đã phục hồi lại các lệnh gọ hàm và sử dụng các hàm mật mã trong thư viện của anh ta, một phiên bản khác thực hiện Kerberos 5 Heimdal cũng được thực hiện bởi nhóm đã xuất bản KTH-KRB.

Các hệ điều hành Windows 2000, Windows XP và Windows Server 2003 sử dụng một phiên bản thực hiện Kerberos làm phương pháp mặc định để chứng thực những bổ sung của Microsoft và bộ giao thức được đề cập trong tài liệu RFC 3244 (Microsoft Windows 2000 Kerberos Change Password and Set Password Protocols) hệ điều hành Mac OSX cũng sử dụng Kerberos trong các phiên bản máy khách và máy chủ của mình.

Năm 2005 nhóm làm việc IETF về Kerberos đã cập nhật các đặc điểm kỹ thuật tại địa chỉ các cập nhật gần đây bao gồm:

* RFC 3961 các quy định về mật mã hóa và kiểm tra tổng
* RFC 3962 mật mã hóa AES cho Kerberos 5
* RFC 4120 phiên bản mới về tiêu chuẩn Kerberos V5(The Kerberos Network Authentication Service (V5) phiên bản này thay thế phiên bản RFC 1510 làm rõ các vấn đề của giao thức và cách sử dụng
* RFC 4121 phiên bản mới của tiêu chuẩn GSS-API (Cơ cấu GSS-API của Kerberos Version 5: Version 2)

DES( Data Encryption Standard) là một phương pháp mật mã hóa được FIPS( tiêu chuẩn xử lý thông tin liên bang hoa kỳ) chọn làm chuẩn chính thức vào năm 1976 sau này chuẩn này được sử dụng rộng rãi trên phạm vi thế giới, thuật tóan này đã gây ra rất nhiều tranh cãi do nó bao gồm các thành phần thiết kế mật độ dài khóa tương đối ngắn và nghi ngờ cơ quan an ninh quốc gia Hoa Kỳ(NSA) có thể bẻ khóa, do đó DES được các nhà nghiên cứu rất kỹ lưỡng đã thúc đẩy hiểu biết hiện đại về mật mã khối và các phương pháp mã tương ứng hiện nay DES được xem là không đủ an tòan cho nhiều ứng dụng, nguyên nhân chủ yếu là độ dài 56bit của khóa là quá nhỏ

* 1. **ỨNG DỤNG KERBEROS MÔI TRƯỜNG CÔNG NGHỆ SHAREPOINT**

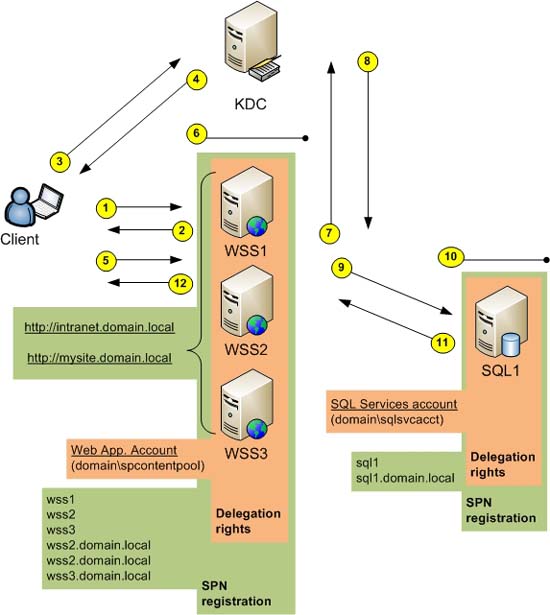
Microsoft Windows Sharepoint Services (WSS) 3.0 và Microsoft Office Sharepoint Server (MOSS) 2007 được thiết kế để tập trung các thông tin và giúp các thành viên trong các nhóm có thể cộng tác với nhau một cách hiệu quả. Người dùng có thể truy cập vào tất cả thông tin nằm trong các tài khoản cá nhân riêng lẻ nếu được cho phép từ website Sharepoint.

Trong bài này, chúng tôi sẽ giới thiệu cho các bạn những một số vấn đề cơ bản để sử dụng Kerberos trong môi trường Sharepoint. Bạn sẽ tìm thấy nhiều hướng dẫn cấu hình cho các kịch bản khác nhau và một số mẹo ở đây và chúng tôi hy vọng bài viết này có thể cung cấp được cho các bạn một cái nhìn tổng quan đối với môi trường của riêng mình.

**Việc sử dụng Kerberos trong Sharepoint?**

Kerberos là một giao thức an toàn cho phép thẩm định theo thẻ nếu yêu cầu máy khách đến Trung tâm phân phối khóa - Key Distribution Center (KDC) có các chứng chỉ người dùng hợp lệ và tên dịch vụ - Service Principal Name (SPN) hợp lệ. Kerberos là kiểu thẩm định được ưa thích trong Sharepoint vì tốc độ, sự an toàn hơn và giảm được số lượng lỗi với username và password hơn so với NTLM. Nếu website Sharepoint sử dụng dữ liệu bên ngoài (nằm trên các máy chủ khác với bản thân máy chủ Sharepoint của bạn) cho cơ sở dữ liệu SQL thông qua các webpart thì máy chủ cần có Kerberos để ủy nhiệm các chứng chỉ máy khách.  
Vậy những gì xảy ra giữa máy khách và các máy chủ khi bạn truy cập một website có cho phép Kerberos? Chúng tôi đã tạo một tóm tắt mang tính tổng quan để thể hiện những gì sẽ xảy ra đằng sau kịch bản. Kịch bản được thể hiện trong hình 1 này được tạo từ Windows Sharepoint Services 3.0.

Hình 1: Kerberos trong luồng Sharepoint



* Máy khách truy cập http://intranet.domain.local bằng các chứng chỉ nặc danh
* WSS Server trả về lỗi IIS error 401.2 nhưng cũng trả về một WWWAuthenticate header.
* Máy khách yêu cầu thẻ cho SPN được tạo bởi trình duyệt Internet nội bộ: HTTP/intranet.domain.local
* KDC trả về thẻ nếu SPN được phát hiện. Điều này được mã hóa bằng khóa chủ tài khoản đã được đăng ký cho SPN (domain\spcontentpool).
* Máy khách thẩm định với thẻ cho ứng dụng web.
* Tài khoản Web App giải mã thẻ và hợp lệ hóa nó.
* Tài khoản Web App yêu cầu thẻ cho SPN được tạo bởi SQL Client: MSSqlSvc/sql1.domain.local:1433.
* KDC trả về thẻ nếu SPN được tìm thấy. Điều này được mã hóa bằng khóa chủ của tài khoản đã được đăng ký cho SPN (domain\sqlsvsacct).
* Dịch vụ ứng dụng web thẩm định với cơ sở dữ liệu QLS bằng thẻ tài khoản ứng dụng web và đóng vai người dùng bằng các quyền ủy nhiệm.
* Tài khoản dịch vụ SQL giải mã thẻ và hợp lệ nó.
* SQL Server trả về dữ liệu yêu cầu cho WSS Server.
* WSS Server trả về webpage.

Nếu Kerberos không được cấu hình để truyền thông SQL, bạn hãy nhảy từ bước 6 đến bước 12. Nhớ rằng việc cho phép thẻ chỉ xảy ra ở lần đăng nhập đầu tiên và cho đến khi timeout.

**Cấu hình Kerberos cho Sharepoint**

Đầu tiên chúng tôi khuyên các bạn tạo một cài đặt thử nghiệm trước khi cấu h́nh lại môi trường sản xuất. Biết vấn đề này sẽ rất khó cho bạn nhưng nếu có các máy chủ ảo, bạn hoàn toàn có thể xây dựng các máy chủ test một cách nhanh chóng và dễ dàng. Điều này cũng cho phép bạn so sánh cấu hình cuối cùng nếu có vấn đề gì đó không làm việc như mong đợi.

Chính vì vậy chúng tôi cần phải tách bỏ NTLM trên các ứng dụng web của mình và cấu hình để sử dụng Kerberos. Đầu tiên bạn vô hiệu hóa giao thức truyền thông này giữa các máy chủ frontend và backend. Sau đó kích hoạt Kerberos giữa các máy khách và các ứng dụng web riêng biệt để quản lý sự thẩm định thông qua máy chủ Sharepoint (có thể gọi nó là sự thẩm định dual- hoặc double-hop).

Hãy xem xét danh sách cần phải thực hiện cho các thiết lập này.

* Thu thập các thông tin cần thiết và tạo người dùng Sharepoint
* Kích hoạt Kerberos để truyền thông SQL
* Cấu hình Service Principal Names (SPNs) trong Active Directory
* Cấu hình “sự tin tưởng về ủy nhiệm” đối với các tài khoảng computer và user
* Cấu hình *Component Services* trên các máy chủ Sharepoint
* Kích hoạt Kerberos cho các ứng dụng web và Shared Service Provider (SSP)
* Test môi trường Sharepoint

**Thu thập các thông tin cần thiết**

Để thực hiện một cách dễ dàng và không gây hại cho các hệ thống đang hoạt động, chúng ta cần phải có tất cả các block đã sẵn sàng. Giả sử môi trường của bạn đang chạy Active Directory và mỗi máy chủ đều có một địa chỉ IP duy nhất. Điều này phải được đăng ký trong máy chủ DNS và không có sự nhân bản tồn tại trong các vùng tra cứu thuận và ngược để Kerberos làm việc. Thêm vào đó tất cả các máy chủ và máy khách phải được đặt thời gian đúng như Kerberos sử dụng để hợp lệ hóa các thẻ và sự truy cập cho máy chủ DNS bên trong.

Trước khi cài đặt, Sharepoint sẽ tạo những người dùng thích hợp trong Active Directory. Nếu bạn đã tạo các tài khoản cần thiết này, hãy đọc các phần tiếp sau nó.

Đây là một danh sách các thông tin cần thiết cho việc thiết lập Kerberos trong môi trường Sharepoint.

* Lớp dịch vụ của SPN  
  (HTTP cho các ứng dụng web WSS/MOSS. MSSQLSvc cho SQL Server mặc định)
* Tên host của SPN
* Fully Qualified Domain Name (FQDN) cho tất cả các ứng dụng wen và máy chủ
* Số cổng hoặc SPN của bạn (không có cổng nào cho các ứng dụng web WSS và MOSS. 1433 cho SQL).
* Các tài khoản Active Directory cho SPN (dịch vụ và các tài khoản ứng dụng)

**Kích hoạt Kerberos trong truyền thông SQL**

Microsoft khuyên nên thực hiện bước này trước khi cài đặt Microsoft Sharepoint để bảo đảm rằng sự truyền thông SQL sẽ làm việc. Cơ sở dữ liệu cấu hình được định vị trong máy chủ SQL và nếu kết nối bị đứt thì bạn cần sửa nó trước khi các site Sharepoint được thiết lập và chạy trở lại. Nếu bạn thay đổi sự thẩm định sau khi cài đặt ban đầu, phải tắt các dịch vụ Sharepoint để tránh mất dữ liệu.

Kích hoạt Kerberos giữa các máy chủ frontend Sharepoint cho máy chủ SQL của bạn bởi:

* Cấu hình SPN
* Cấu hình sự tin cậy cho việc ủy nhiệm nếu bạn cần đóng vai người dùng trong các dịch vụ khác.

Không cần thiết kích hoạt Kerberos trong việc truyền thông SQL nếu bạn chỉ cần thẩm định các máy khách cho frontend Sharepoint, không cần các dịch vụ khác như kết nối dữ liệu, Excel Services/SQL Reporting.

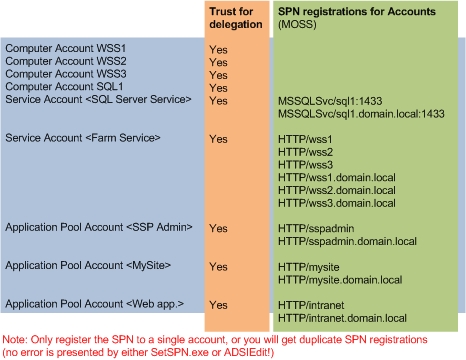
**Cấu hình Service Principal Names (SPNs) trong Active Directory**

Việc bản đồ hóa Service Principal Name được sử dụng bởi Kerberos để cho phép sự ủy nhiệm của một dịch vụ nhằm thủ vai một tài khoản dịch vụ của người dùng nào đó. Một SPN gồm có Service Class, hostname và đôi khi một số cổng. Một số ví dụ ở đây là **HTTP/intranet.domain.local** và **MSSqlSvc/sql1.domain.local:1433**. Bạn nên đăng ký cả hai hostname và FQDN cho các ứng dụng web của mình mặc dù thường chỉ sử dụng một trong chúng.

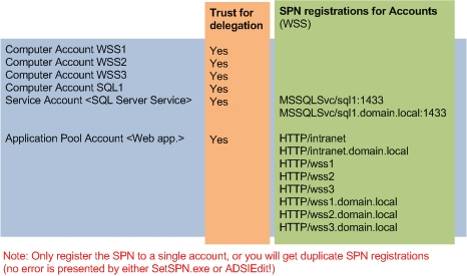
Để cấu hình Service Principal Name, bạn có thể sử dụng một vài công cụ. Chúng tôi sử dụng thành phần SetSPN-tool được cài đặt trong Windows Server 2008 mặc định. Với Windows Server 2003, thành phần này có thể tìm thấy trong phần các công cụ hỗ trợ trên cài đặt CD-ROM hoặc trong phần resource kit có thể download từ Microsoft. Bạn cũng có thế sử dụng ADSIedit để cấu hình SPN, tuy nhiên thao tác này khiến bạn mất đôi chút công việc để điều hướng thông qua Active Directory, việc edit các hạng mục và thay đổi *ServicePrincipalName* của chúng.

Lệnh đăng ký một SPN: **setspn.exe –A HTTP/intranet.domain.local DOMAIN\Account**  
Lệnh liệt kê SPN cho một tài khoản: **setspn.exe –L DOMAIN\Account**  
Lệnh xóa một SPN: **setspn.exe –D HTTP/intranet.domain.local DOMAIN\Account**

Sử dụng các bảng trong hình 2 và 3 để xem các đăng ký cần thiết cho SQL trong kịch bản MOSS và WSS



Hình 2: Sự ủy nhiệm và SPN cho MOSS

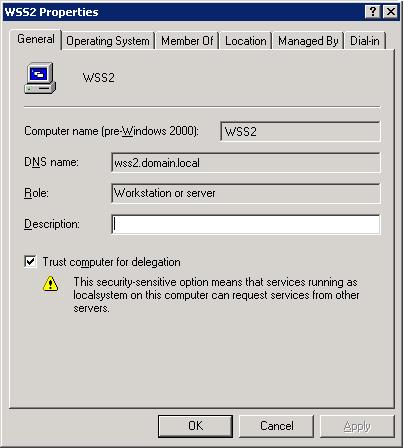


Hình 3: Sự ủy nhiệm và SPN cho WSS

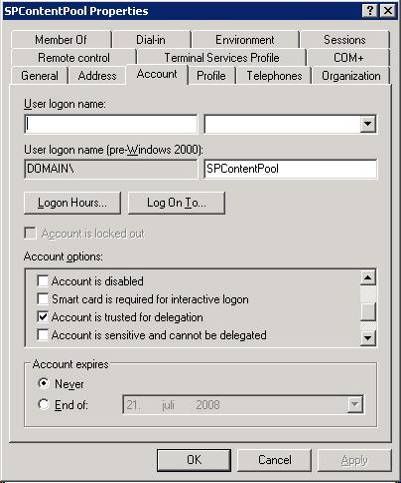
**Cấu hình sự tin cậy cho các ủy nhiệm trên các tài khoản computer và user**

Lúc này bạn cần quản lý được các quyền ủy nhiệm trong Active Directory. Điều này có thể được thực hiện cho các tài khoản máy tính và người dùng như những gì bạn có thể xem trong bảng trên. Trong *Active Directory Users and Computers,* kích chuột phải vào tài khoản, chọn thuộc tính và kiểm tra phần tin cậy của sự ủy nhiệm (xem các thông tin trong hình 4 và 5 bên dưới). Văn bản hay thủ tục có thể khác trong các phiên bản của Windows Server.

Hình 4: Ủy nhiệm cho tài khoản máy tính



Hình 5: Ủy nhiệm các tài khoản người dùng



Xem trong hình 2 và 3 về các tài khoản để cấu hình sự ủy nhiệm trong kịch bản.

**Cấu hình các dịch vụ thành phần trên máy chủ Sharepoint**

Các tài khoản ứng dụng web cần phải có các quyền hợp pháp bằng không bạn sẽ nhận được một lỗi DCOM với mã sự kiện là 10017 trong bản ghi sự kiện của mình và được môt tả trong Microsoft KB920783:

*“The application-specific permissions settings do not grant Local Activation permission for the COM Server application with CLSID {CLSID} to the user DomainName\UserName SID {SID}. This security permission can be modified using the Component Services administration tool.”*

Với việc thiết lập bảo mật thích hợp cho các tài khoản, bạn chỉ cần vào Control Panel, *Component Services*, Computers, My Computer, DCOM Config và chỉnh sửa các thuộc tính của “IIS WAMReg Admin Service”. Chỉnh sửa “Launch and Activate” trong tab Security và trao quyền “Local Activation” cho các tài khoản ứng dụng (xem trong hình 2 và 3).

Khi bạn ở trong Component Services, thiết lập “Default Impersonation Level” là “Delegate” bằng cách chỉnh sửa thuộc tính của “My Computer”.

**Kích hoạt Kerberos cho các ứng dụng web và Shared Service Provider (SSP)**

Cấu hình cơ bản của bạn sẽ được thực hiện lúc này. Để sử dụng Kerberos bạn phải kích hoạt thông qua *Central Administration* cho các ứng dụng web của bạn. Chúng ta có thể chọn giữa NTLM và Kerberos cho các ứng dụng web riêng biệt trên trang *Authentication Providers* mà bạn sẽ tìm thấy trong panel *Application Management*. Theo đường dẫn này để cấu hình:

* Central Administration, Application Management, Authentication providers
* Chọn ứng dụng web của bạn cần sử dụng Kerberos cho, ví dụ:



* Kích “Default”
* Chọn hay tích vào tùy chọn Kerberos



Hãy khởi động lại IIS với **iisreset /noforce** trong nhắc lệnh trên các máy chủ front end của bạn.  
Trong MOSS, Shared Service Provider của bạn cũng phải được cấu hình và bạn thực hiện trong một nhắc lệnh. Lệnh **SetSharedWebServiceAuthn** không tồn tại trong WSS. Điều hướng đến thư mục 12-hive (thường nằm trong *C:\Program Files\Common Files\Microsoft Shared\web server extensions\12\bin*) và chạy lệnh: **stsadm.exe -o SetSharedWebServiceAuthn –negotiate**

**Test môi trường Sharepoint**

Lúc này vào phần đang tồn tại của hoạt động: Bảo đảm rằng mọi thứ đều làm việc như mong đợi.

Kiểm tra bản ghi đăng nhập bảo mật cho các sự kiện đăng nhập của Kerberos. Kiểm tra tài khoản miền đã được sử dụng. Nếu tài khoản có một đăng nhập lỗi, hãy kiểm tra những thứ dưới đây:

* Ngày và thời gian có được thiết lập đúng trên tất cả máy chủ
* Tài khoản không bị khóa trong miền
* Dịch vụ hoặc ứng dụng đang hoạt động với đúng tài khoản
* Ủy nhiệm được cấu hình đúng trên các tài khoản máy tính và người dùng
* SPN được cấu hình đúng trong Active Directory
* Không có sự nhân bản trên các máy chủ tồn tại trong vùng DNS thuận và ngược
* Các máy chủ DNS được chỉ định đúng trên tất cả các máy chủ

**Các vấn đề về phiên bản đối với Internet Explorer**  
Nếu bạn sử dụng các cổng không phải mặc định trên máy chủ IIS Virtual của mình, hãy bảo phiên bản Internet Explorer mà bạn đang sử dụng là Internet Explorer 6 hoặc đã được vá và được cấu hình để có các cổng trong SPN. *Central Administration* sẽ gồm một số cổng không mặc định. Lưu ý ở đây là bạn sẽ không thấy thông báo lỗi nói rằng lỗi này là do sử dụng một phiên bản không thích hợp của Internet Explorer

**Kết luận**

Microsoft Windows Sharepoint có thể được sử dụng trong các môi trường phức tạp, nơi sự thẩm định bảo mật với Kerberos cần thiết. Bài viết này được cung cấp cho các bạn với hy vọng giải thích một số vấn đề về bức trang lớn của Kerberos trong cài đặt Sharepoint. Các công cụ và các cấu hình cơ bản đều có sẵn để bạn có thể bắt đầu việc sử dụng các tính năng tuyệt vời của Sharepoint với thẩm định dual-hop.

* 1. **CÁC PHẦN MỀM ỨNG DỤNG**
* OpenSSH (với Kerberos v5 hoặc cao hơn).
* NFS (kể từ NFSv3) PAM (với mô đun pam\_krb5).
* SOCKS (kể từ SOCKS5).
* Apache (với mô đun mod auth kerb).
* Devecot IMAP4 và POP3.
* Hệ thống X Windows.

**CHƯƠNG II: NGUYÊN TẮC HOẠT ĐỘNG KERBEROS**

**2.1 MÔ HÌNH VÀ GIẢI THÍCH HOẠT ĐỘNG TÓM TẮT KERBEROS**

* MÔ HÌNH



*Hub*

*Switch*

**Service Server (SS)**

**Client A**

Client B

**Key Distribution Center - KDC**

***Authentication Server (AS)***

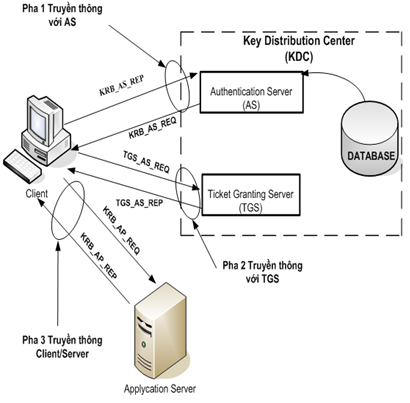
***Ticket Granting Server (TGS)***

* GIẢI THÍCH HOẠT ĐỘNG TÓM TẮT KERBEROS

*Từ Mô Hình trên, người dùng Client A* gửi yêu cầu *chứng thực* tớiAS*, Máy chủ chứng thực (AS)* tra trên *dữ liệu* mình có thông tin *Client A* và cho phép *Client A* giao tiếp tới cổng *TGS (Trung Tâm Cấp Vé)*. Sau đó, *Client* A sẽ gửi yêu cầu tới *Máy Chủ Cấp Vé TGS* rằng mình đã được *chứng thực* bởi *AS* cấp phép*,* yêu cầu để *nhận Vé Chấp Thuận từ TGS*. *TGS* xem và xác minh đúng là *AS* đã xác thực, thì sẽ cấp cho *Client* 1 tấm vé được vào cổng *Dịch Vụ Máy Chủ (SS)*. Client sẽ vào SS và *xác thực* với *SS* rằng mình đã được *Chấp Thuận* bởi trong tay có tấm vé vào cổng. Cuối cùng *Client* sẽ gửi yêu cầu mình muốn tới *Dịch Vụ Máy Chủ SS*. *Máy Chủ Dịch Vụ* sẽ chấp thuận yêu cầu và cho Client A trò chuyện với Client B.

**2.2 NGUYÊN TẮC HOẠT ĐỘNG CỦA KERBEROS**

**Một phiên giao dịch (giản lược) của Kerberos : 3 giai đoạn và 6 bước trao đổi.**



SƠ ĐỒ HOẠT ĐỘNG CỦA KERBEROS

**Giai đoạn 1:**

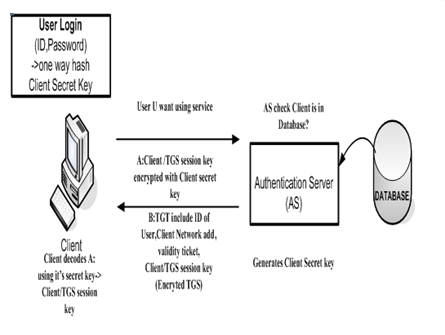
🖎Người sử dụng *Client* nhập *Username* và *Password* để tiến hành *đăng nhập*.

🖎*Phần mềm* máy *Client* mã hóa *Password* với *hàm băm một chiều*, kết quả mã hóa sẽ làm khóa bí mật của người sử dụng client*.*

🖎*Phần mềm máy khách client* gửi một gói tin không mã hóa (username, địa chỉ mạng của người sử dụng) đến máy chủ AS (máy chủ chứng thực) để yêu cầu chứng thực. Lưu ý: là cả khóa bí mật của người sử dụng client lẫn *Password* đều không gửi tới AS.

🖎*AS* kiểm tra xem username của client có nằm trong cơ sở dữ liệu *database* của mình không, nếu *có* thì *gửi 2 gói tin* sau tới *người sử dụng*:

* Gói tin A: gồm (Thời gian, thời hạn, yều cầu cần của client và “Khóa phiên TGS/Client”) được mật mã hóa với khóa bí mật của người sử dụng chỉ có người sử dụng mới mở được gói tin A.
* Gói tin B: là “Vé chấp thuận” (bao gồm username, địa chỉ mạng của người sử dụng, thời gian, thời hạn của vé và “Khóa phiên TGS/Client”) được mật mã hóa với khóa bí mật của TGS.



HÌNH MÔ TẢ GIAI ĐOẠN 1

**Giai đoạn 2:**

🖎Khi nhận được 2 gói tin A và B, phần mềm máy khách Client giải mã gói tin A (với khóa bí mật của người sử dụng Clientvà sẽ có được khóa phiên TGS/Client là khóa vào cổng TGS, và bao gồm thời gian, thời hạn, yêu cầu cần của Clientở bên trong gói tin A. Chứng minh là AS là thật không giả mạo

🖎 Khi có khóa vào cổng dịch vụ TGS, người sử dụng gửi 2 gói tin sau tới TGS:

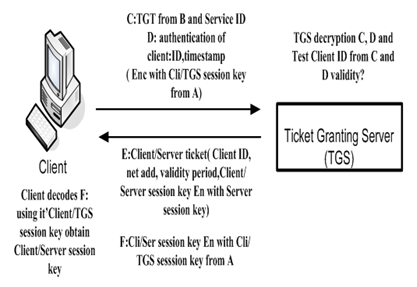
* Gói tin C: Bao gồm “Vé chấp thuận” từ gói tin B, gói tin này client không mở được vì dùng khóa riêng của TGS, nhằm để chứng minh client có được là do AS cấp cho
* Gói tin D: Phần nhận thực (bao gồm username và thời điểm yêu cầu), mật mã hóa với “Khóa phiên TGS/Client ” lấy được từ bước trước.

🖎 Khi nhận được 2 gói tin C và D, TGS giải mã C với khóa bí mật của TGS giải mã D với khóa phiên TGS/Client.

🖎 TGS so sánh username từ gói tin C và gói tin D đã giải mã, so sánh giữa thời điểm yêu cầu và thời hạn sử dụng của vé, nếu thỏa mãn thì gửi 2 gói tin sau tới người sử dụng:

* Gói tin E: là “Vé vào dich vụ máy chủ SS như hình trên là Aplication Server” (bao gồm username, địa chỉ mạng người sử dụng, thời hạn sử dụng và “Khóa phiên Server/Client“) mật mã hóa với khóa bí mật của máy chủ cung cấp dịch vụ SS. Chỉ có SS mới mở được , client không mở được.
* Gói tin F: gồm “Khóa phiên Server/Client” mật mã hóa với “Khóa phiên TGS/Client ”, Client sẽ mở ra lấy được Khóa phiên Server/Client để vào cổng Máy Chủ Dịch vụ SS.

HÌNH MÔ TẢ GIAI ĐOẠN 2



**Giai đoạn 3:**

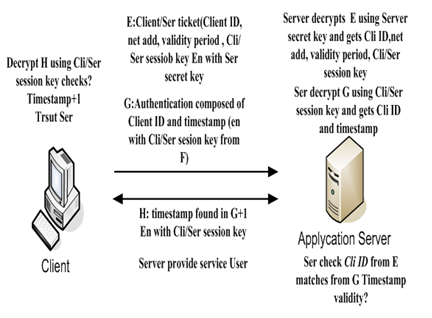
🖎Khi nhận được 2 *gói tin E* và *F*, người sử dụng đã có đủ thông tin để nhận thực vào cổng với máy chủ cung cấp dịch vụ SS.

🖎 Phần mềm máy khách giải mã *gói tin F* để lấy khóa phiên Server/Client. Khóa này sẽ vào cổng máy chủ cung cấp dịch vụ SS.

🖎 Người sử dụng tạo *gói tin G*: bên trong gồm: chỉ danh người sử dụng, thời điểm yêu cầu dịch vụ, được mã hóa với khóa phiên Server/Clientđã lấy được ở trên.

🖎 Gửi tới máy chủ cung cấp dịch vụ SS*gói tin G* và *gói tin E* mà client không mở được do mã hóa với khóa bí mật riêng của SS, thu được từ bước trước để chứng minh là người sử dụng có được chứng thực với SS.

HÌNH MÔ TẢ GIAI ĐOẠN 3



**CHƯƠNG III: KẾT QUẢ THỰC NGHIỆM KERBEROS**

Do Kerberos là một giao thức Chứng Thực mặc định của các hệ điều hành Windows 2000, Windows Xp, Windows Server 2003, Windows Server 2008....,

Nên Chúng em sẽ áp dụng việc chứng thực này bằng cách:

Máy Server: Chúng em nâng cấp lên Domain Controller với Windows Server 2008

Máy Client: Chúng em sẽ join vào Domain và đăng nhập với Windows 10

* 1. **QUÁ TRÌNH CÀI ĐẶT THỰC NGHIỆM KERBEROS**

Máy Server:

Click phải My Network Places -> Properties -> Click phải Card Cross chọn Properties ->chọn Internet Protocol

TCP/IP -> Properties cấu hình IP: 192.168.56.2

Subnet Mask: 255.255.255.0

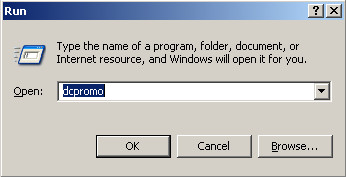
Gateway để trống

DNS: 192.168.56.2 -> OK -> OK

A screenshot of a cell phone

Description automatically generated

Start -> Run -> gõ dcpromo -> OK

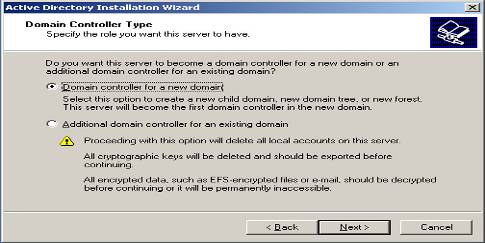


Hộp thoại Welcome to…> Click Next

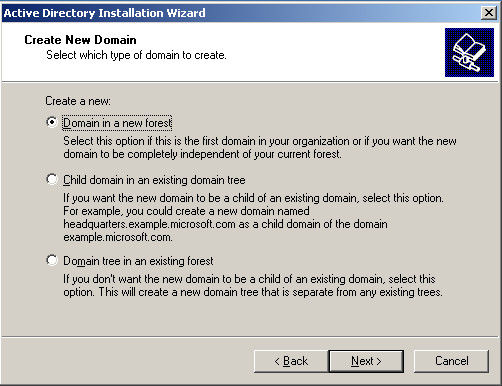


Hộp thoại Operating System…> Next

Hộp thoại Domain Controller Type -> chọn Domain Controller for a new domain -> Next



Hộp thoại Create New Domain -> chọn Domain in a new forest -> Next



Hộp thoại New Domain Name -> nhập -> Next

Hộp thoại NetBIOS Domain Name -> Next

Hộp thoại Database and … -> Next

Hộp thoại Shared Volume -> Next

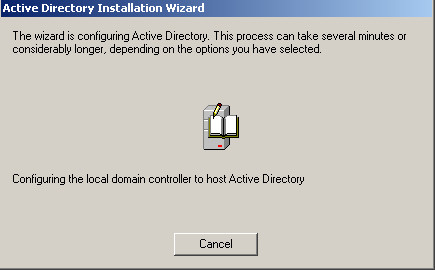
Hộp thoại DNS Registration Diagnostics -> Next

Hộp thoại Permission -> chọn Permission compatible only with -> Next

Hộp thoại Directory Services…-> Next

Hộp thoại Summary -> Next

Hệ thống tiến hành quá trình nâng cấp Domain Controller



Nâng cấp hoàn tất -> Finish chọn Restart để khởi động lại Server



**Kết quả trên máy server :**

A screenshot of a social media post

Description automatically generated

Máy Client:

Cấu hình IP:

A screenshot of a cell phone

Description automatically generated

Sau khi cấu hình IP của máy client. Kiểm tra bằng cách thực hiện lệnh ping từ máy này sang máy kia:

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Click phải My Computer -> chọn System Properties -> Tab Computer Name -> Change.

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

Hộp thoại Computer Name Change -> chọn More. Nhập tên đầy đủ của máy server

A screenshot of a cell phone

Description automatically generated

Hộp thọai Computer Name Change -> chọn **Domain** nhập **kerberos.net -**> OK.

A screenshot of a cell phone

Description automatically generated

Nhập username và password của máy server:

A screenshot of a cell phone

Description automatically generated

Chọn Ok. Sẽ đăng nhập vào Domain **3.2 GIẢI THÍCH GÓI TIN LẤY ĐƯỢC TỪ WIRESHARK**

**Hình chụp lọc ra gói tin Kerberos:**

A screenshot of a computer

Description automatically generated

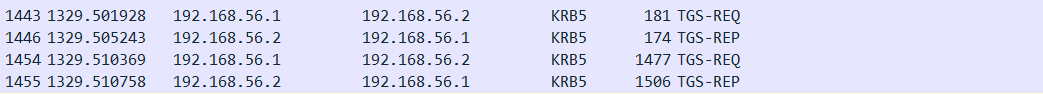
**Giải thích gói tin:**

* client ip 192.168.56.1 gửi yêu cầu request lên server ip 192.168.56.2 để AS chứng thực thông tin user id của client,
* server ip 192.168.56.2 hồi đáp yêu cầu reply tới client thông báo là đã kiểm tra trong database xác thực có user id của client.

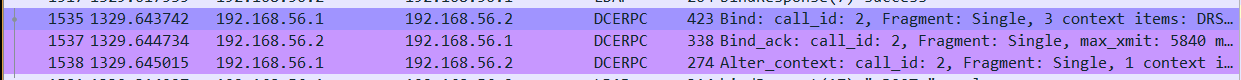
A screenshot of a cell phone

Description automatically generated

* Client gửi thông tin yêu cầu request cấp vé chấp thuận TGS để vào được các dịch vụ mà client muốn.
* Server hồi đáp reply lại yêu cầu của client cấp vé chấp thuận.



* khi có vé chấp thuận dịch vụ được cấp , thì client sẽ gọi thủ tục hệ thống phát triễn và phân phối mạng máy tính DCERPC , để đăng nhập kết nối vào tài khoản domain khi join domain.



* Server khi nhận được cuộc gọi trên sẽ kiểm tra xem có đúng dns không. Nếu đúng thì sẽ chấp thuận cho phép client kết nối.
* khi được chấp thuận vào môi trường domain. Client sẽ thay đổi cuộc gọi tới các user trong domain để kết nối.



* Client sẽ gửi yêu cầu request dịch vụ SMB( Server Message Block) đòi phiên cài đặt hệ thống tập tin để cung cấp chia sẻ tập tin, máy in, cổng nối tiếp.
* Server hồi đáp response phiên cài đặt của client thành công
* Client gửi yêu cầu request tới LDAP yêu cầu truy cập các dịch vụ thư mục mà Client cần.
* Server hồi đáp response thành công.



Tài liệu tham khảo:

* <https://www.youtube.com/watch?v=faX4d-iV58c>
* <http://kerberos.net/>
* <https://letonphat.wordpress.com/2010/10/21/quy-trnh-ho%E1%BA%A1t-d%E1%BB%99ng-kerberos/>