# PENERAPAN *NETWORK INTEGRATED SYSTEM* PADA ROUTER CISCO MENGGUNAKAN METODE AUTENTIKASI BERBASIS *LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)*

Anzalar Rhokman, M. Noor Al-Azam S.Kom., M.MT, Natalia Damastuti, S.T., M.T.

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Narotama
Jl. Arief Rachman Hakim 51, Sukolilo – Surabaya (60117)
Telp. (031) 594-6404, 599 – 5578
Website : http://www.narotama.ac.id
Email : info.narotama@gmail.com

**ABSTRAK**

Sistem otentikasi terpusat merupakan suatu sistem yang memusatkan semua proses otentikasi pada satu server khusus dimana pada *server* tersebut berisi data tentang *credential user*. Sebelum diciptakan sistem ini, proses otentikasi menggunakan sistem otentikasi lokal. Sistem otentikasi lokal memiliki beberapa kekurangan diantaranya sistem keamanan yang rendah sehingga rentan dengan tindak pencurian data, terbatasnya jumlah account user yang dapat dibuat dan kesulitan dalam memanajemen account user ketika jumlah perangkat semakin banyak. Saat ini sistem otentikasi terpusat telah banyak dipergunakan oleh berbagai perangkat berbasis jaringan diantaranya Cisco Router.

Cisco Router mendukung beberapa *software* otentikasi terpusat antara lain Kerberos, Tacacs, LDAP dan Radius. Pada penelitian ini akan dibangun sistem otentikasi terpusat dengan menggabungkan *software* Radius sebagai otentikator dan LDAP (*Lightweight Directory Access Protocol*) sebagai *database*. Dengan memanfaatkan sistem otentikasi terpusat berbasis LDAP, maka proses manajemen *user access* oleh administrator akan lebih mudah karena semua informasi terkumpul dalam satu *server* dan *credential user* dapat terlindungi. Dengan memanfaatkan keamanan *remote access* berbasis *Secure Shell* pada router cisco, maka kegiatan *remote* dapat dilakukan dari mana saja tanpa khawatir akan tindakan penyadapan karena semua data yang mengalir melalui jaringan akan di-enkripsi sehingga sulit untuk diketahui konten sebenarnya dari paket data tersebut.

*kata kunci: sistem otentikasi terpusat, radius, LDAP, Cisco Router, Remote Access, penyadapan*

# I. PENDAHULUAN

Pengguna aplikasi berbasis jaringan kini semakin banyak. Hal ini disebabkan karena kebutuhan manusia akan *sharing resources* semakin tinggi. Maraknya tindak pencurian data melalui media internet menuntut para *developer* untuk lebih meningkatkan kualitas keamanannya. Oleh sebab itu, dibutuhkan suatu sistem otentikasi terpusat dan aman sehingga dapat melindungi data dari tindak pencurian.

Penerapan otentikasi berbasis *Lightweight Directory Access Protocol (LDAP)* adalah salah satu cara yang dipilih oleh sebagian perusahaan berskala besar karena telah dibuktikan kehandalannya dalam memanajemen *user credential*. Otentikasi berbasis LDAP dapat diterapkan pada beberapa aplikasi berbasis jaringan seperti web *server*, samba *server*, *FTP (File Transfer Protocol) server* dan lain-lain.

Sistem otentikasi LDAP berbeda dengan sistem otentikasi lokal. Perbedaannya adalah jika sistem otentikasi lokal database *user login*-nya tersimpan pada *server* tersebut sehingga hanya memerlukan 1 koneksi saja yaitu antara pengakses dan *server*. Pada sistem otentikasi LDAP database *user login*-nya tersimpan pada *server* LDAP yang berfungsi khusus untuk memanajemen *user login*, jadi dibutuhkan 3 buah koneksi yaitu pengakses ke *server* service (samba, FTP dan lain-lain) dan *server* service ke LDAP. Jika *server* service tidak terkoneksi dengan *server* LDAP maka proses otentikasi tidak akan terjadi. LDAP juga mendukung fungsi *Single Sign-On (SSO)* yang memungkinkan pengakses dapat mengakses beberapa aplikasi yang memerlukan otentikasi hanya dengan 1 kali *login*.

Dahulu seorang administrator jaringan yang ingin mengakses perangkatnya (misalkan router cisco, huawei dan lain-lain) hanya bisa menggunakan koneksi console dengan kabel console yang dikonesikan secara langsung ke komputer. Seiring dengan semakin banyaknya perangkat jaringan dan cabang-cabang perusahaan maka cara tersebut dirasa kurang efektif karena cukup menghabiskan banyak waktu untuk *mobile*. Namun saat ini, telah diciptakan servis *remote protocol* yang berfungsi untuk mengontrol perangkat jaringan dari jarak jauh. Diantara servis *remote protocol* yang sering dipergunakan adalah telnet, Secure Shell (SSH), File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP) dan lain-lain.

Kemudahan akses ini ternyata tidak berjalan sebaik yang diharapkan, karena di dunia jaringan terdapat tindak kriminalitas yang bertujuan untuk mencuri hak akses dari administrator. Oleh sebab itu, dibutuhkan suatu sistem yang berfungsi untuk memanajemen dan mengamankan hak akses dari administrator agar terhindar dari tindak pencurian.

*Lightweight Directory Access Protocol (LDAP)* merupakan salah satu protokol yang handal dalam mengamankan hak akses. Saat ini LDAP telah banyak diimplementasikan oleh perusahaan-perusahaan berskala besar yang sangat memprioritaskan keamanan data dan jaringannya, terutama dari jaringan publik. Salah satu aplikasi yang dapat diintegrasikan dengan LDAP adalah Radius.

Radius memungkinkan *user* dan *service* untuk saling mengautentikasi dan menunjukkan identitasnya. Router cisco merupakan salah satu perangkat jaringan yang mendukung otentikasi berbasis LDAP.

Untuk itu pada skripsi ini akan membahas tentang membangun sistem otentikasi berbasis LDAP pada router cisco.

## II. TINJAUAN PUSTAKA

Jaringan komputer merupakan gabungan dua atau lebih perangkat komputer yang terhubung dalam satu jaringan, dimana pada jaringan tersebut pengguna dapat berbagi data *(file sharing)*, aplikasi dan penggunaan perangkat (*sharing device*) seperti printer, scanner dan lain- lainsehingga dapat digunakan secara bersama. Berdasarkan area lingkupnya sendiri, jaringan komputer dibagi menjadi beberapa macam yaitu *Local Area Network (LAN), Metropolitan Area Network (MAN)* dan *Wide Area Network (WAN)*. Namun pada penelitian ini akan lebih terfokus kepada sistem keamanan jaringan dan beberapa metode pengamanan yang digunakan.

## III. METODOLOGI PENELITIAN

Dalam penyusunan penelitian ini terdapat beberapa tahapan kerja, antara lain:

1. Tahap I (Persiapan)

   Tahap ini dimulai dengan mengkaji permasalahan yang sedang terjadi pada proses otentikasi router cisco, kemudian melakukan studi literatur untuk menemukan metode yang dapat digunakan dalam menyelesaikan permasalahan tersebut.

2. Tahap II (Penelitian Pendahuluan)

   Tahap ini dimulai dengan mencari informasi tentang perangkat dan aplikasi yang dibutuhkan dalam membangun sistem otentikasi berbasis LDAP pada router cisco.

3. Tahap III (Pelaksanaan)

   Tahap ini dimulai dengan melakukan instalasi CAS *server*, LDAP *server* dan persiapan router cisco, kemudian memastikan bahwa semua perangkat saling terhubung dengan melakukan test ping. Setelah itu dikakukan konfigurasi pada masing-masing perangkat agar semua sistem dapat saling terintegrasi.

4. Tahap IV (Pengujian)

   Tahap ini dilakukan tahap pengujian dimulai dari registrasi dan manajemen *user* pada LDAP *server*, proses otentikasi pada router cisco dan *log user login* pada CAS *server*.

5. Tahap V (Analisis Data)

   Tahap ini membahas tentang detail proses otentikasi yang terjadi antara LDAP *server*, CAS *server* dan router cisco serta *penetration test* untuk memastikan keamanan *user* sehingga dapat ditarik sebuah kesimpulan tentang hasil penelitian.

## IV. HASIL DAN PEMBAHASAN

Sistem otentikasi terpusat memudahkan administrator dalam memanajemen *user access* bagi setiap *user* dan dengan adanya sistem logging yang bagus dapat lebih memudahkan administrator dalam memantau setiap aktifitas *user*.

Dari hasil percobaan penyadapan yang dilakukan menggunakan software wireshark, terlihat bahwa akses *remote* dengan menggunakan *telnet service* dapat disadap dan dibaca dengan jelas isi paket datanya. Namun akses *remote* dengan menggunakan *ssh service* paket data yang ditangkap terlihat seperti huruf-huruf yang diacak sehingga meskipun paket data dapat disadap namun isinya tidak dapat terbaca. Hal ini disebabkan karena paket data yang dikirimkan melalui *telnet service* masih menggunakan *plain text*, namun pada *ssh service* paket data yang mengalir ke internet telah ter-enkripsi sehingga aman jika terjadi tindak penyadapan data

## V. PENUTUP

Setelah melakukan penelitian dan uji coba, maka dapat disimpulkan bahwa:

1. Dengan menggunakan sistem otentikasi terpusat administrator jaringan akan lebih mudah dalam mengelola *user access* bagi masing-masing user
2. Dengan menggunakan *remote service SSH*, keamanan user ketika melakukan *remote access* dari jaringan publik / internet akan terjaga karena data yang mengalir ke jaringan akan di-enkripsi / diacak sehingga sulit untuk dibaca oleh para penyadap.
3. Dengan adanya system logging yang baik, maka setiap aktivitas user dan perubahan yang terjadi pada perangkat jaringan (router cisco) dapat diketahui secara detail mulai dari tanggal, nama *user* yang mengakses dan perintah-perintah apa saja yang telah digunakan oleh *user* saat mengakses.

# DAFTAR PUSTAKA


Adicson Gmbh Team, 2011, *LogAnalyzer Basic*, Deutschland, Adicson IT-SolutionGmbh.

Cisco Team, 2010, *Cisco ASA Series General Operations CLI Configuration Guide*, United State, Cisco System.

Findlay A, 2011, *Best Practices in LDAP Security*, Maidenhead, Apache Software Foundation.

Hilmi F, 2012, *Analisis Performansi Otentikasi Single Sign On Pada Web Menggunakan LDAP*, Medan, JSM STMIK Mikroskil

Hilmi R dan Irawan B, 2011, *Integrasi Aplikasi Dengan Metode Single Sign On menggunakan Central Autentication Service (CAS) dan LDAP*, Surabaya, upn.ac.id

Justine Ellingwood, 2014, *Understanding the SSH Encryption and Connection Process*, New York, Digital Ocean Community.

Ratdhian Cipta Sukmana, 2006, Implementasi Transport Layer Security pada LDAP, Jakarta, Ilmu Komputer.

Reid A, 2011, *Using SSL to Secure LDAP Traffic to Microsoft Domain Controllers*, Melburne, SANS Institute InfoSec Reading Room

Sari R. F dan Hidayat S, 2006, *Integrasi Mekanisme Autentikasi Web Server Dengan Metode LDAP*, Jakarta, Jurnal Teknik Universitas Indonesia.

Schulzrine H dan Wang X, 2011, *Measurement and Analisys of LDAP Performance*, Yorktown Heights, Network System Department IBM.

Xiujuan H dan Zhenghui G, 2010, *Research of Security Identity Authentication Based on Campus Network*. Jiaohuo Henan, College of Computer Science and Technology Henan Polytechnic University.