ISBN : 978-979-3577-28-4

PROSEDING

SEMNASTIK DAN MAGMA

Seminar Nasional Teknologi Informasi Komunikasi dan Manajemen

Universitas Bina Darma

Seminar Nasional 2014

SEMINAR NASIONAL

Kualitas Hidup Melalui Aplikasi IT & Manajemen

Penerbit :
PPP-UBD Press

ASPIKOM

APTIKOM

Penerbit Salemba

TELKOMSEL

BNI

ANALISIS PERBANDINGAN KEAMANAN SISTEM SINGLE SIGN ON MENGGUNAKAN CAS BERBASIS LDAP DAN RADIUS

Nyimas Sopiah, Rusmala Santi, Winda Nurmulyani

Fakultas Ilmu Komputer
Universitas Bina Darma
Jl. A. Yani No. 12, Palembang 30624, Indonesia

Abstrak

Single sign on merupakan teknologi yang mengizinkan pengguna untuk melakukan otentikasi pada beberapa aplikasi web hanya menggunakan satu username dan satu password. Pengguna cukup melakukan login sekali agar bisa mengakses beberapa aplikasi web yang terintegrasi. Single sign on menyediakan fasilitas Central Authentication Service (CAS) sebagai portal penghubung antara pengguna dan aplikasi web. Beberapa aplikasi web akan didaftarkan di server CAS. Server CAS membutuhkan backend sebagai pusat penyimpanan username dan password pengguna. Server CAS mendukung backend LDAP dan RADIUS, yang akan dibandingkan kemanannya dari serangan sniffing. Sehingga didapatkan hasil, sistem single sign on menggunakan CAS dengan LDAP sebagai backend lebih rentan terhadap serangan sniffing. Backend RADIUS bisa menjadi pilihan yang lebih aman terhadap serangan sniffing untuk sistem single sign on.

1 PENDAHULUAN

Keamanan credential (username dan password) pengguna merupakan salah satu faktor yang sangat penting dalam sebuah aplikasi web. Apalagi aplikasi web yang telah terintegrasi ke dalam sebuah sistem single sign on. Untuk itu, aplikasi web tersebut membutuhkan tempat penyimpanan yang aman dari serangan yang akan mengancam keselamatan dan keutuhan data pengguna, seperti serangan sniffing. Dimana sniffer akan dengan mudah mengetahui password pengguna yang melakukan login.

1.1 Latar Belakang

Berkembangnya protokol Hypertext Transfer Protocol (HTTP) menjadi daya tarik tersendiri bagi pengembang aplikasi untuk membangun aplikasi berbasis teknologi web atau yang biasa disebut web based application. Hampir semua komunitas, seperti perusahaan ataupun lembaga pendidikan menggunakan aplikasi berbasis web. Aplikasi berbasis web biasanya menyertakan proses otentikasi terhadap penggunanya. Proses otentikasi adalah dengan melakukan pengisian user id dan password pada from login. Jadi semakin banyak aplikasi web yang dikembangkan oleh sebuah perusahaan, maka semakin banyak pula proses otentikasi yang dilakukan pengguna . Untuk itu

dibutuhkan sebuah sistem single sign on yang mengintegrasikan semua aplikasi web sehingga proses otentikasi menjadi lebih sederhana karena pengguna cukup memiliki satu akun untuk mengakses semua aplikasi web.

Salah satu produk single sign on adalah Central Authentication Service yang digunakan sebagai portal penghubung antara pengguna dengan aplikasi web. Central Authentication Service merupakan tempat proses otentikasi dilakukan, terdapat dua backend yang digunakan untuk memvalidasi pengguna yang sah yaitu LDAP dan RADIUS. Masing-masing backend memiliki kelebihan dan kekurangan dalam beberapa hal, salah satunya keamanan credential pengguna.

Untuk itu penulis merasa perlu untuk membandingkan keamanan sistem single sign on menggunakan CAS berbasis LDAP dan RADIUS, sehingga harapannya ditemukan solusi backend yang lebih baik untuk mengamankan credential user dari serangan sniffing.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, penulis merumuskan permasalahan dalam penelitian ini adalah bagaimana membandingkan keamanan sistem single sign on menggunakan CAS berbasis LDAP dan RADIUS?

1.3 Batasan Masalah

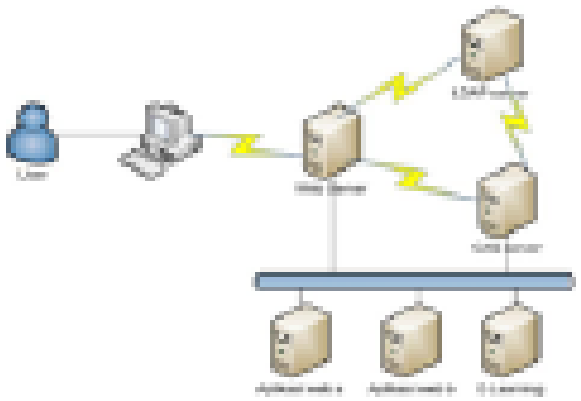
Untuk mempermudah proses penyelesaian masalah pada penelitian ini agar lebih fokus dan terarah maka penulis membatasi permasalahan dalam penelitian ini yaitu LDAP dan RADIUS digunakan sebagai backend sistem single sign on, parameter perbandingan yang digunakan adalah hanya dari segi keamanan credential pengguna dari serangan sniffing dan aplikasi web yang diuji cobakan ke dalam sistem single sign on adalah e-learning menggunakan moodle.

2 METODOLOGI PENELITIAN

Metode penelitian yang digunakan pada penelitian ini adalah action research (penelitian tindakan). Penelitian tindakan memiliki beberapa tahapan, untuk menemukan permasalahn dalam penelitian ini penulis harus mengetahui permasalahan yang ada dengan cara melakukan diagnosing pada objek penelitian. Selanjutnya setelah ditemukan permasalahan, penulis mulai merencanakan tindakan yang tepat untuk menyelesaikan permasalahan. Setelah melakukan perencanaan, penulis menerapkan rencana tindakan yang telah dibuat sebelumnya. Setelah proses penerapan selesai, selanjutnya adalah proses mengevaluasi dari hasil tindakan yang telah diterapkan kemudian selanjutnya untuk diambil pelajaran dari penelitian yang penulis lakukan.

Berikut ini merupakan rancangan penelitian sistem single sign on yangver CAS sebagai pintu gerbang untuk mengakses aplikasi web dengan server LDAP sebagai backendnya. Jadi sebelum pengguna bisa mengakses aplikasi web, pengguna akan melakukan otentikasi pada halaman server CAS, kemudian server CAS akan memeriksa apakah pengguna sudah terdaftar di server LDAP atau tidak. Apabila pengguna sudah

terdaftar maka pengguna akan diberikan akses ke halaman web yang diminta.



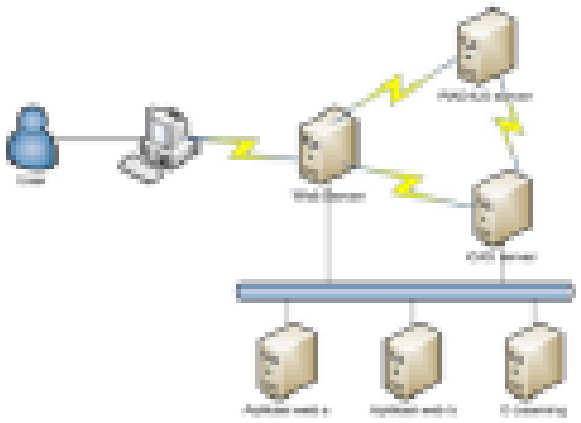
Selanjutnya, berikut ini merupakan rancangan sistem single sign on menggunakan server CAS dengan server RADIUS sebagai backendnya. Dimana masing-masing backend yang digunakan akan dibandingkan kinerja nya dalam hal keamanan terhadap serangan sniffing. Untuk sistem kerja dari kedua sistem tersebut tetap sama, yang membedakan hanya backend nya saja (tempat penyimpanan username dan password pengguna).

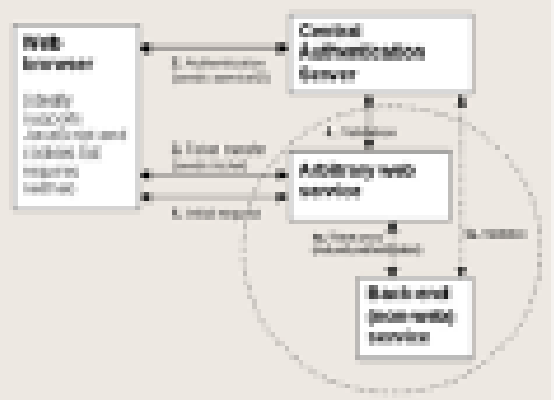
2.1 Single Sign On

Menurut Wallmark (2011) single sign on adalah sebuah istilah yang digunakan untuk menggambarkan bagaimana beberapa aplikasi web bisa menggunakan cara yang sama untuk mengidentifikasi pengguna yang akan melakukan login.

Single sign on adalah teknologi yang mengizinkan pengguna jaringan agar dapat mengakses sumber daya dalam jaringan hanya dengan menggunakan satu akun saja. Dengan menggunakan sistem single sign on pengguna cukup melakukan satu kali proses otentikasi untuk mendapatkan izin akses terhadap semua layanan aplikasi web yang terdaftar di sistem single sign on.

2.2 Central Authentication Service





Menurut JASIG (2011) Central Authentication Service merupakan sebuah sistem otentikasi yang aslinya dibuat oleh Universitas Yale yang menyediakan jalan aman pada aplikasi web untuk mengotentikasi seorang pengguna. Berikut ini merupakan gambaran umum proses dari central authentication service.

Jadi central authentication service merupakan salah satu produk single sign on yang menyediakan layanan otentikasi terpusat. Central Authentication Service bisa menggunakan server LDAP dan server RADIUS sebagai backend, yaitu sebagai tempat penyimpanan username dan password pengguna secara terpusat. Dimana server CAS akan memvalidasi pengguna yang sah melalui server LDAP atau server RADIUS.

2.3 Lightweight Directory Access Protocol (LDAP)

Menurut Imam (2013:75) Lightweight Directory Access Protocol adalah protokol yang mendefinisikan bagaimana data direktori dapat diakses melalui jaringan. LDAP biasa digunakan untuk menyimpan informasi secara terpusat. Penggunaan LDAP di dalam sistem akan membuat pencarian infromasi menjadi mudah dan terintegrasi dan sangat mudah.

2.4 Remote Access Dial In User Service (RADIUS)

Menurut Imam (2013:123) RADIUS merupakan suatu protokol yang digunakan secara luas untuk mengotentikasi pengguna jaringan. Secara sederhana RADIUS menyediakan fungsi otentikasi, otorisasi dan akunting atau lebih dikenal dengan AAA (Authentication, Authorization, and Accounting) untuk menggunakan layanan di jaringan.

2.5 Sniffing

Menurut Efvy (2011:89) dalam sebuah jaringan tentunya terdapat banyak paket data yang hilir mudik. Data tersebut bisa apa saja, mulai dari informasi waktu, ip address, jenis protokol dan nama jaringan. Bahkan terkadang termasuk pula informasi sensitif seperti cookies, username maupun password. Paket data atau informasi yang berteberan tersebut bisa dicapture atau ditangkap. Tindakan capture data ini disebut dengan sniffing. Salah satu tool yang bisa digunakan untuk melakukan sniffing adalah wireshark. Wireshark merupakan salah satu network tool analyzer yang nyaman digu-

nakan dan lebih menarik (Iwan Sofana:324).

3 HASIL DAN PEMBAHASAN

Dari hasil penelitian melakukan sniffing paket data pada sistem single sign on menggunakan CAS berbasis LDAP dan RADIUS didapatkan hasil yaitu ada perbedaan pada masing-masing backend. Untuk backend LDAP, saat pengguna mengakses sistem single sign on, sniffer bisa dengan mudah membaca username pengguna tetapi untuk passwordnya tidak terbaca, akan tetapi saat melakukan sniffing pada protokol LDAP, sniffer juga bisa mengetahui user id dan password admin. Sedangkan, untuk hasil sniffing paket data sistem menggunakan backend RADIUS, sangat berbeda dengan LDAP. Pada saat pengguna melakukan login melalui halaman CAS, maka pengguna akan melewati proses otentikasi yang dilakukan oleh server RADIUS, yaitu dengan cara memeriksa apakah pengguna sudah terdaftar di database RADIUS. Disinilah RADIUS akan melakukan fungsi sebagai AAA. Hasil sniffingnya nya menunjukkan bahwa sniffer hanya mengetahui username pengguna yang login, tanpa mengetahui password pengguna dan admin. Karena passwordnya terenkripsi.

4 KESIMPULAN

Dari hasil penelitian ini dapat disimpulkan bahwa keamanan sistem single sign on menggunakan CAS dengan LDAP sebagai backend sangat rentan terhadap serangan sniffing, karena penyerang bisa mengetahui user id dan password admin server LDAP. Hal ini bisa membuat penyerang mengetahui semua username dan password pengguna yang tersimpan di server LDAP. Keamanan sistem single sign on menggunakan CAS dengan RADIUS sebagai backend cukup aman dari serangan sniffing, penyerang hanya bisa mengetahui username pengguna, tanpa mengetahui passwordnya karena terenkripsi.

4.1 SARAN

Untuk keamanan koneksi pengguna sistem single sign on berbasis CAS dengan LDAP sebagai backend bisa diujicobakan menggunakan TLS encryption agar alur koneksinya tidak mudah terbaca oleh penyerang.

5 Referensi

1. http://www.jasig.org/cas diakses pada tanggal 1 desember 2013

2. Wallmark, Mattias. (2011). Central Authentication Service http://www.it.umu.se/english/services/central-username/central-autentication-service/ diakses pada tanggal 24 Nopember 2013

3. Maurizio, Storani. (2008). Central Authentication Service-CAS : concepts and examples 2008 http://mauriziostorani.wordpress.com/2008/08/23/central-authentication-service-cas-concepts-and-examples/ . diakses pada tanggal 24 Nopember 2013

4. Cartealy, Imam. 2013. Linux Networking. Jasakom

5. https://wiki.jasig.org/display/CASUM/End-to-end+Windows+Example diakses pada tanggal 7 Januari 2014

6. Sofana, Iwan. 2011. Teori dan Modul Praktikum Jaringan Komputer. Bandung : Modula