Makalah Tugas Kuliah EL6115

Operasi Keamanan dan *Incident Handling*

OPERASI KEAMANAN PENGGUNAAN JARINGAN INTERNET ITB

Oleh

MUHAMMAD OGIN HASANUDDIN

NIM: 23215120

(Program Studi Magister Teknik Elektro)

SEKOLAH PASCASARJANA

SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA

INSTITUT TEKNOLOGI BANDUNG

2016

OPERASI KEAMANAN PENGGUNAAN JARINGAN INTERNET ITB

Oleh

MUHAMMAD OGIN HASANUDDIN

NIM: 23215120

(Program Studi Magister Teknik Elektro)

Makalah ini dibuat sebagai
persyaratan untuk lulus mata kuliah
EL6115 Operasi Keamanan dan *Incedent Response*
di
PROGRAM STUDI MAGISTER TEKNIK ELEKTRO
SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
INSTITUT TEKNOLOGI BANDUNG

Bandung, 21 April 2016

Dosen mata kuliah EL6115
Operasi Keamanan dan *Incident Response*,

Dr. Ir. Budi Rahardjo

ABSTRAK

OPERASI KEAMANAN PENGGUNAAN JARINGAN INTERNET ITB

Oleh

MUHAMMAD OGIN HASANUDDIN

NIM: 23215120

PROGRAM MAGISTER STUDI TEKNIK ELEKTRO

Layanan Akses Internet merupakan layanan yang diberikan ITB untuk mengakses Internet dari jaringan ITB. Untuk dapat menggunakan Layanan Akses Internet, pengguna harus memiliki akun INA dalam kondisi aktif. INA atau disebut juga akun AI3 merupakan satu-satunya akun yang bisa digunakan untuk mengakses layanan internet melalui jaringan kampus ITB, seperti email mahasiswa @students.itb.ac.id, area hotspot ITB, akses wireless network, internet proxy, VPN (Virtual Private Network) dan aplikasi internal di ITB lainnya. AI3 – ITB merupakan satuan unit kerja di bawah DSTI – ITB (Direktorat Sistem dan Teknologi Informasi – Institut Teknologi Bandung). Tugas utamanya adalah memantau dan memelihara jaringan komputer *backbone* kampus ITB.

Dalam penggunaanya, akun AI3 seharusnya tidak diketahui oleh pihak yang tidak berwenang, dari percobaan yang telah dilakukan dengan tool snipper pasangan *username* dan *password* dari akun AI3 dapat diketahui dengan mudah. Dikarenakan AI3 menggunakan metode *single authentication* maka hal tersebut sangat berbahaya bila pasangan username dan password diketahui oleh pihak yang tidak berwenang. Dari latarbelakang tersebut, makalah ini akan membahas masalah autentikasi (*single authentication*), pengaturan *hotstpot*, dan kebijakan dari persyaratan minimum untuk kemanan jaringan di perguruan tinggi.

Kata kunci: AI3 – ITB, autentikasi, pengaturan hostspot, kebijakan, operasi keamanan.

ABSTRACT

OPERASI KEAMANAN PENGGUNAAN JARINGAN INTERNET ITB

By

MUHAMMAD OGIN HASANUDDIN

NIM: 23215120

MAGISTER ELECTRICAL ENGINEERING STUDY PROGRAM

Internet Access Service is a service provided by ITB for accessing internet from ITB network. To use Internet Access Service from ITB, user must to have active INA account. INA, sometimes called AI3 account is the one and only account that can be use to access internet service through ITB campus network, such as students mail @students.itb.ac.id, ITB hotspot area, wireless network access, internet proxy, VPN (Virtual Private Network) and other ITB internal applications. AI3 – ITB is sub unit under DSTI – ITB (Departemen of Information Technology and System – Institut Teknologi Bandung). The main task of DSTI – ITB is monitoring and maintenance ITB backbone computer campus network.

In use, the account AI3 should not be known by an unauthorized person, from the experiments have been done with a couple snippets tool username and password of an account AI3 can be seen easily. Due to AI3 using a single authentication method then it is very dangerous if the pair username and password is known by unauthorized parties. From such background, this paper will discuss the issue of authentication (single authentication), hotstpot setting, and the policy of minimum requirements for network security at the college.

Keywords: AI3 – ITB, authentication, hotspot setting, policy, secure operation.

KATA PENGANTAR

Puji syukur penulis panjatkan pada Tuhan Yang Maha Esa, yang atas rahmat dan karunia-Nya penulis dapat menyelesaikan penulisan makalah yang berjudul "Operasi Keamanan Penggunaan Jaringan Internet ITB."

Selama penulisan makalah ini, penulis mendapat bantuan dan dukungan dari berbagai pihak. Untuk itu, penulis mengucapkan terima kasih kepada:

1. Dr.Ir. Budi Rahardjo, selaku dosen mata kuliah EL6115 Operasi Keamanan dan *Incident Response*, yang telah mencurahkan perhatian dan waktunya dalam memberikan bimbingan sehingga makalah ini dapat terselesaikan;
2. mamah, bapak, kakak-kakak dan calon istri tercinta, yang selalu memberikan semangat dan do'anya;
3. teman - teman *fasttrack*, yang telah saling membantu dan mengingatkan dalam pengerjaan makalah ini hingga dapat terselesaikan;
4. seluruh staf dan karyawan prodi Teknik Elektro ITB, yang telah memberikan banyak bantuan;
5. dan semua pihak yang membantu, yang tidak dapat penulis sebutkan satu persatu.

Penulis menyadari bahwa makalah ini bukanlah tanpa kelemahan, untuk itu penulis sangat mengharapkan kritik dan saran dari pembacanya.

Akhir kata, semoga makalah ini dapat bermanfaat.

Bandung, Mei 2016

Penulis

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR SINGKATAN DAN ISTILAH

SINGKATAN	Nama	Pemakaian pertama kali pada halaman
AI3	Asian Internet Interconnection Initiatives	i
SSO	Single Sing On	4
MRTG	Multi Router Traffic Grapher	6
SNORT	Intrusion Detection System Tool	13

BAB I

PENDAHULUAN

1.1 Latar Belakang

Semakin pesatnya perkembangan teknologi saat ini, pemanfaatan teknologi informasi menjadi bagian yang penting dalam sebuah perusahaan yang berskala nasional maupun internasional, tak terkecuali dalam lingkungan pendidikan seperti perguruan tinggi. Dalam perjalanannya, pelaksanaan kegiatannya harus dilakukan secara aman, dilihat dari berbagai aspek diantaranya: Infrastruktur, aplikasi, SDM, kelembagaan dan hukum.

Pemanfaatan teknologi dalam lingkungan perguruan tinggi memiliki aplikasi jaringan dan pelayanan beragam. Dalam lingkungan kampus ITB dikenal teknologi AI3, yang membuat mulai dari Dosen sampai dengan mahasiswa di wajibkan memiliki sebuah akun untuk dapat menikmati layanan akses internet ITB.

Satu akun ini dapat digunakan langsung untuk menikmati layanan akses internet, email, serta login langsung ke situs – situs resmi organisasi pendidikan seperti IEEE library dan ACM library, yang memungkinkan pengguna dapat mengunduh paper secara gratis.

Keamanan operasi pengguna AI3 dirasa perlu untuk mendukung keberjalanan sistem. Hal ini penting untuk mengenali bahwa sifat dari sistem Internet adalah memiliki aspek kekuatan dan, mungkin, aspek yang paling rapuh. Aturan operasi, seperti aturan etiket, bersifat sukarela dan, sebagian besar, tidak memiliki kekuatan hukum, kecuali mereka terjadi bertepatan dengan hukum nasional, pelanggaran yang dapat menyebabkan penuntutan. Sebuah set umum aturan untuk keberhasilan operasi dan semakin aman dari internet adalah sukarela, karena hukum berbagai negara tidak seragam mengenai jaringan data. Namun, untuk pelaksanaannya data yang tersebar di dalam jaringan harusnya dilindungi agar kejadian yang tidak diinginkan kelak terjadi.

Sebagai infrastruktur jaringan, AI3 harus memiliki mekanisme keamanan untuk melindungi data pengguna dan privasi. Dari pengamatan yang telah dilakukan pada akun AI3, dapat dilihat dengan mudah pasangan username dan password pengguna

menggunakan tools snipper. Hal ini tentu sangat rentan bila pasangan username dan password akun AI3 berseliweran dalam bentuk plain. Namun hal yang terjadi dalam lingkungan kampus ITB adalah tetap membiarkan pasangan username dan password pengguna dalam bentuk plain. Dalam makalah ini akan dibahas tentang autentikasi, pro dan kontra yang terjadi, pengaturan hotspot dan kebijakan tentang pengamanan jaringan kampus pendukung teknologi AI3.

1.2 Rumusan Masalah

Berdasarkan uraian pada latar belakang di atas, maka masalah utama yang diangkat pada makalah ini adalah sebagai berikut.

- Masalah terkait autentikasi.
- Pro dan Kontra terkait autentikasi.
- Persyaratan minimum untuk pengamanan jaringan untuk instansi pendidikan perguruan tinggi.

1.3 Tujuan Makalah

Tujuan yang ingin dicapai dari makalah ini adalah sebagai berikut.

- Membahsa ,asalah terkait autentikasi pada penggunaan akun AI3.
- Memberikan pengetahuan pada pengguna agar lebih berhati – hati dalam menggunakan akun AI3.

1.4 Batasan Masalah

Batasan masalah yang dirumuskan dalam makalah ini mencakup:

- Pembahasan tentang kebijakan ITB terkait model autentikasi yang digunakan
- Infrastruktur pendukung
- Aplikasi
- SDM
- Hukum

1.5 Metodologi

Berikut langkah – langkah yang dilakukan dalam pembuatan makalah ini.

1. Identifikasi masalah

   Proses identifikasi masalah meliputi tinjuan pustaka dan wawancara yang menghasilkan formulasi masalah.
2. Evaluasi

   Evaluasi yang dilakukan dicapai dengan menggunakan studi kasus atau dengan melakukan suatu survei yang berkaitan dengan solusi yang diberikan.

1.6 Sistematika Penulisan

Pembuatan makalah ini disusun dengan sistematika sebagai berikut.

BAB I. PENDAHULUAN

Pada bab ini dibahas mengenai latar belakang, perumusan masalah, tujuan dan manfaat penelitian, batasan masalah, metodologi pengerjaan, dan sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Pada bab ini dijabarkan dasar-dasar teori serta dokumen yang menjadi acuan dasar penulis dalam pembahasan makalah.

BAB III. PEMBAHASAN

Pada bab ini dijabarkan mengenai masalah autentikasi, pro dan kontra, pengaturan hotspot dan kebijakan tentang syarat minimum pengamanan jaringan dalam lingkungan kampus.

BAB IV. KESIMPULAN

Pada bab ini dijabarkan mengenai kesimpulan hasil yang didapat makalah ini, dan saran untuk pengembangan sistem selanjutnya.

BAB II

TINJAUAN PUSTAKA

Dalam bab II ini akan dibahas mengenai dasar teori serta dokumen yang menjadi acuan dasar penulis dalam pembahasan makalah. Teori yang dibahas meliputi single sign-on, infrastruktur AI3, dan kebijakan TI ITB.

2.1 Asian Internet Interconnection Initiatives (AI3)

Proyek AI3 dirancang untuk melakukan penelitian dalam teknologi yang dibutuhkan untuk menyediakan konektivitas internet berbasis satelit di bagian Asia [6]. Pada September 1996, Institut Teknologi Bandung (ITB) memasang Ku-Band peralatan stasiun bumi untuk akses satelit JCSAT-3 yang didukung oleh proyek AI3 dari Jepang. Ini adalah lompatan besar bagi lembaga pendidikan Indonesia untuk menghubungkan mereka ke Internet.

Indonesia memperluas layanan yang saat ini mencakup lebih dari 25 lembaga pendidikan di tingkat nasional, peregangan dari Sabang sampai Manado. Pada tahun 1998, jaringan ini dikenal sebagai A13 jaringan Indonesia dengan alamat kontak: ai3@itb.ac.id.

Sebuah strategi yang berhasil kami selalu menyarankan dalam mengembangkan jaringan di setiap universitas adalah untuk memberikan siswa kesempatan dan iman untuk mengembangkan dan pemeliharaan jaringan di teknis tingkat. Strategi ini terbukti. Para siswa yang memiliki lebih banyak waktu, semangat, dan energi selalu belajar baru teknologi dan menerapkannya untuk jaringan mereka [4].

2.2 *Single Sign On*

Kampus Portal menggunakan mekanisme otentikasi terpadu, dimana pengguna hanya menggunakan satu waktu dari nama dan otentikasi password dapat mencapai single sign on (SSO), maka mereka bisa menjelajah antara sistem informasi yang berbeda dari kampus dengan identitas yang unik, dan menggunakan sumber daya informasi sesuai dengan kewenangan didelegasikan dan peran identitas. Hal ini tidak hanya

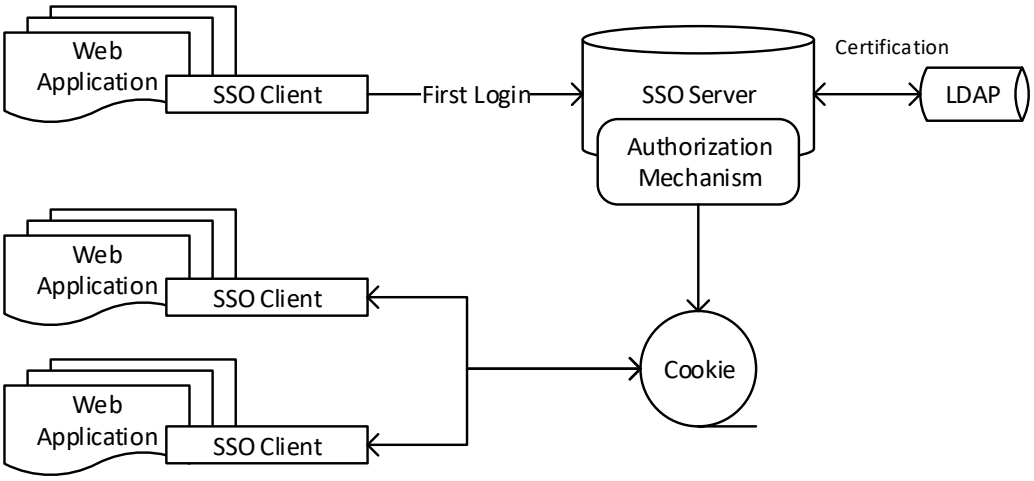
menghindari ketidaknyamanan yang disebabkan oleh menyiapkan beberapa account pengguna, tetapi juga meningkatkan efisiensi dan keamanan dalam penggunaan sumber daya data.

Fungsi Single sign-on (SSO) memungkinkan pengguna untuk login sekali untuk akses ke sistem aplikasi lainnya sesuai dengan hak akses pengguna, sehingga dapat meningkatkan kegunaan, keamanan dan stabilitas sistem informasi. Single sign-on merupakan bagian dari manajemen identitas pengguna. Ketika akses pengguna yang sama ke sumber daya yang dilindungi dalam aplikasi yang berbeda pada server yang sama, ia hanya perlu login sekali. Setelah verifikasi sistem keamanan, ia dapat mengakses ke sistem aplikasi lain pada server yang sama tanpa perlu login lagi untuk memverifikasi.

Mekanisme SSO adalah bahwa ketika pengguna mengunjungi sistem aplikasi A untuk pertama kalinya, pengguna diarahkan untuk login ke sistem otentikasi. Setelah menggunakan SSO, semua sistem aplikasi berbagi sistem otentikasi identitas. Sebuah sistem otentikasi terpadu merupakan salah satu tempat dari SSO. Fungsi utama dari sistem otentikasi adalah untuk membandingkan informasi login dengan database informasi pengguna untuk otentikasi login. Ketika otentikasi berhasil, sistem otentikasi harus menghasilkan tanda otentikasi terpadu (Tiket) dan kembali ke pengguna. Sistem otentikasi juga dapat mewujudkan verifikasi Ticket, sehingga untuk menilai efektivitas. Semua sistem aplikasi di portal dapat mengenali dan ekstrak informasi tiket, yang memungkinkan sistem aplikasi untuk mengenali pengguna log-in yang telah login sekali sebelum [9]. Sistem aplikasi harus dapat mengidentifikasi dan ekstrak Ticket. Melalui komunikasi dengan sistem otentikasi, secara otomatis dapat menilai apakah pengguna saat masuk, sehingga untuk menyelesaikan tanda tunggal pada. SSO proses otentikasi pengguna ditunjukkan pada Gambar II. 1.

Saat ini, ada banyak skema realisasi SSO, di antaranya mekanisme otentikasi umum SSO adalah: Kerberos, PKI, KryptoKnight dan Sesame, dll [10]. teknik yang umum digunakan adalah: Web Service dan Cookie, CAS (Authentication Sistem Tengah), dll SSO dalam sistem ini dapat mewujudkan manajemen terpadu dan verifikasi pengguna berdasarkan single sign-on Model CAS, dan dapat disesuaikan dan dikembangkan

sesuai dengan permintaan, yang lebih baik memenuhi kebutuhan premis menjamin keselamatan. CAS tidak hanya dapat menyediakan infrastruktur SSO ke beberapa aplikasi web, tetapi juga menyediakan fungsi SSO untuk aplikasi non-web dengan fungsi layanan fungsional web front-end. CAS dapat memusatkan otentikasi pengguna untuk aplikasi Web tunggal dan menyederhanakan manajemen password, karena itu meningkatkan keamanan.



Gambar II. 1 Proses Autentikasi Pengguna SSO [11]

Dari hasil wawancara yang telah dilakukan dengan pihak USDI (Pak Mugi), dikatakan bahwa ITB sendiri, untuk fitur SSO yang diimplementasikan menggunakan metode proxy-based.

Proxy-based Pseudo-SSO Systems

Dalam arsitektur pseudo-SSO berbasis proxy, komponen pseudo-SSO berada pada server proxy eksternal; seperti dalam kasus lokal, server eksternal ini memiliki akses ke kredensial pengguna, dan karenanya harus dipercaya untuk tujuan ini oleh pengguna. Autentikasi utama terjadi antara pengguna dan proxy pada awal sesi (dan mungkin setelah itu, jika proxy ingin melakukan re-autentikasi). Autentikasi pengguna berikutnya di SPs diarahkan ke, atau dicegat oleh, proxy, yang secara otomatis mengeksekusi protokol autentikasi SP tertentu termasuk memasok kredensial yang diminta. Properti kunci dari arsitektur ini adalah bahwa mesin lokal tidak pernah

memiliki akses ke kredensial SP tertentu pengguna; autentikasi untuk SPs terjadi secara langsung antara proxy dan SPs.

Proxy-based True SSO Systems

Dalam arsitektur SSO berbasis proxy benar, server eksternal mengambil peran ASP. Server eksternal ini bertindak sebagai broker antara pengguna dan SPs; pengguna terdaftar bisa mendapatkan keuntungan dari SSO di SPs yang mempertahankan hubungan kepercayaan dengan ASP. Perlu dicatat bahwa ASP sepele bisa berkedok pengguna terdaftar di setiap SP mengandalkan, hanya dengan menyampaikan sebuah pernyataan. Oleh karena itu, baik pengguna dan SPs harus percaya ASP untuk tujuan SSO. Perhatikan juga bahwa pengamatan ini berlaku untuk ASP di semua sistem SSO (lokal atau proxy yang berbasis) benar, serta untuk komponen pseudo-SSO di semua sistem pseudo-SSO.

2.3 Persoalan Operasi AI3

Bagian ini membahas beberapa isu operasi terkait dalam jaringan AI3 termasuk beberapa dilema terkait dengan lingkungan jaringan penelitian berbasis satelit yang besar. Ringkasan alat saat ini dan sistem yang sekarang digunakan dalam jaringan AI3 juga dibahas.

Operasi Pengaturan Jaringan saat ini

Grafik MRTG, menunjukkan lalu lintas dua arah dari AI3 Jepang untuk semua lembaga mitra, sekarang digunakan untuk memantau berbagai link [7]. Alat ini, bagaimanapun, tidak dapat menentukan lalu lintas tertentu (yaitu, tcp, udp, smtp, icmp, http) mengalir di setiap link, sehingga membuatnya sulit untuk mengevaluasi penggunaan link, yaitu, apakah itu benar-benar penelitian lalu lintas terkait atau lalu lintas Internet hanya komersial.

Operasi dan Implementasi AI3

Karena jaringan AI3 memiliki cakupan yang sangat luas, dengan setup jaringan yang berbeda di eachp lembaga artner, beberapa alat operasi yang sedang digunakan. Alat ini terpisah atau tersebar dan tidak ada server pusat dimana data pengukuran disimpan. alat yang berbeda yang sekarang digunakan untuk operasi AI3 adalah [8]:

- Software ComStream Monitoring - alat data logging dan monitoring untuk modem ComStream.
- Modem WatchDog - alat untuk memantau status dari SDM300A dan modem satelit NEC Nxtar.
- AI3 IPv6 / IPv4 Looking Glass - alat untuk pemantauan router dan konektivitas server, routing dan BGP peering untuk jaringan IPv6 dan IPv4.
- AI3 Traffic Repository – database agregat lalu lintas antara AI3 dan WIDE.
- MRTG Map - indeks dari semua grafik MRTG pemanfaatan link semua lembaga mitra AI3.
- Weather Map - digunakan dalam memvisualisasikan lalu lintas testbed jaringan AI3.

2.4 Kebijakan TI ITB

Kebijakan Teknologi Infromasi ITB dibuat untuk tujuan [14]:

- memberikan dukungan agar kegiatan akademik dan kegiatan non-akademik institut dapat berjalan secara lebih baik;
- menjamin penggunaan sumberdaya informasi institut dilaksanakan berdasar kan kriteria informasi yang berkualitas;
- mengantisipasi perkembangan kebutuhan sumberdaya informasi institut agar dapat direncanakan secara lebih baik;
- mendukung ketersediaan pelayanan teknologi informasi dan komunikasi bagi komunitas institut; dan
- melindungi aset institut yang berupa sumberdaya informasi

terdiri dari delapan bab yang berisikan pokok-pokok bahasan sebagai berikut.

- Bab I Pendahuluan
- Bab II Data dan Informasi
- Bab III Aplikasi
- Bab IV Infrastruktur Teknologi Informasi
- Bab V Sumberdaya Teknologi Informasi
- Bab VI Ketentuan Umum Penyelenggaraan aktivitas Teknologi Informasi
- Bab VII Pelanggaran dan Sanksi
- Bab VIII Ketentuan lain.

Pada Kebijakan TI ITB Bab IV mengenai Infrastruktur Teknologi Informasi, Pasal 22 Keamanan Infrastruktur Teknologi Informasi.

(1) Pengelola teknologi informasi harus menjamin keamanan pemanfaatan infrastruktur teknologi informasi dari segala kemungkinan resiko yang merugikan pengguna maupun institut.
(2) Standar dan prosedur keamanan infrastruktur teknologi informasi ditetapkan oleh unit pengelola teknologi informasi berdasarkan kriteria informasi berkualitas.
(3) Pemanfaatan infrastruktur teknologi informasi harus menjamin keselamatan pengguna yang menggunakan infrastruktur tersebut.

Pada Kebijakan TI ITB Bab VI mengenai Ketentuan umum penyelenggaraan aktivitas teknologi informasi, Pasal 35 Manajemen Keamanan.

(1) Kebutuhan keamanan harus didefinisikan dalam Service Level Agreement
(2) Kebutuhan eksternal lainnya dijelaskan lebih spesifik dalam kontrak, perundangan dan kebijakan internal yang terkait.
(3) Kebutuhan garansi kontinuitas layanan TI di ITB dituangkan dalam Service Level Agreement.

Pada Kebijakan TI ITB Bab VII mengenai Pelanggaran dan Sanksi, Pasal 38 Pelanggaran Privasi.

(1) Siapa saja yang memberitahukan rahasia pribadi seseorang berupa username atau password, yang diperolehnya secara profesional atau resmi tanpa hak, dinyatakan bersalah dengan hukuman atas pelanggaran ringan.
(2) Sanksi atas pelanggaran tersebut berupa pelayanan terhadap institut, atau denda, jika pelanggaran tersebut menyebabkan kerugian yang besar
(3) Pelanggaran atas standar dan prosedur keamanan infrastruktur teknologi informasi akan dikenakansanksi sesuai dengan aturan dan ketentuan yang berlaku.

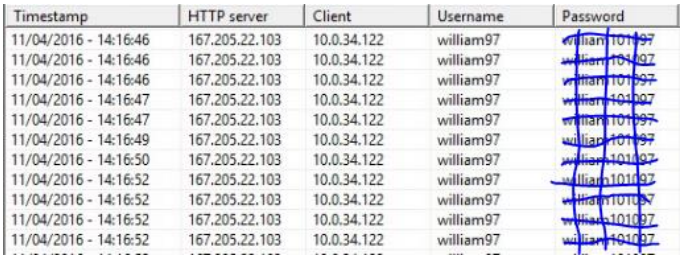
BAB III

PEMBAHASAN

Dalam bab III ini dijelaskan pembahasan yang mencakup Masalah Autentikasi AI3, pro dan kontra implementasi mekanisme autentikasi AI3, pengaturan hotspot serta kebijakan dan syarat minimum keamanan operasi pada jaringan internet sebuah perguruan tinggi.

3.1 Autentikasi akun AI3

Autentikasi AI3 dilakukan dengan menggunakan pasangan username dan password. Seorang pengguna dapat menikmati layanan internet bila ia memiliki akun atau mengetahui salah satu akun aktif yang dapat digunakan untuk dapat melewati autentikasi proxy. Di ITB, pasangan username dan password dapat dilihat dengan aplikasi seperti chain and abel berikut adalah tampilan untuk capture yang dilakukan chain and abel [13].



Timestamp	HTTP server	Client	Username	Password
11/04/2016 - 14:16:46	167.205.22.103	10.0.34.122	william97	[redacted]
11/04/2016 - 14:16:46	167.205.22.103	10.0.34.122	william97	[redacted]
11/04/2016 - 14:16:46	167.205.22.103	10.0.34.122	william97	[redacted]
11/04/2016 - 14:16:47	167.205.22.103	10.0.34.122	william97	[redacted]
11/04/2016 - 14:16:47	167.205.22.103	10.0.34.122	william97	[redacted]
11/04/2016 - 14:16:49	167.205.22.103	10.0.34.122	william97	[redacted]
11/04/2016 - 14:16:50	167.205.22.103	10.0.34.122	william97	[redacted]
11/04/2016 - 14:16:52	167.205.22.103	10.0.34.122	william97	[redacted]
11/04/2016 - 14:16:52	167.205.22.103	10.0.34.122	william97	[redacted]
11/04/2016 - 14:16:52	167.205.22.103	10.0.34.122	william97	[redacted]
11/04/2016 - 14:16:52	167.205.22.103	10.0.34.122	william97	[redacted]

Gambar III. 1 Pasangan password dan username dari program Chain and Abel.

Selain dapat dapat dilihat dengan aplikasi seperti penjelasan diatas, sering kali mahasiswa membagikan atau sharing dengan pengguna lain hal ini tentu dapat menimbulkan risiko keamanan.

3.2 Pro dan Kontra

Pada bagian ini dijelaskan pro dan kontra dari mekanisme single sign-on pada AI3.

Keuntungan Single Sign-on

Kebutuhan autentikasi pada setiap aplikasi menyebabkan masalah bagi pengguna yaitu mereka harus mengingat password untuk setiap sistem. Pada situasi ini, pengguna cenderung untuk menuliskan passwordnya pada catatan sehingga mereka dapat mengingatnya dengan mudah atau membuat password yang sama untuk beberapa aplikasi.

Hal tersebut meningkatkan risiko tertebaknya password oleh penyusup. Pada situasi ini, kita dapat mengimplementasikan fitur single sign-on (SSO) untuk meningkatkan pengalaman pengguna dan membuat sistem lebih aman. SSO merupakan cara untuk mengakses sistem software ganda, berhubungan namun bebas dengan cara pengguna masuk ke sistem dan meningkatkan akases ke semua sistem tanpa dimintai login ulang oleh setiap aplikasi. Berikut adalah beberapa keuntungan SSO [2]:

- Meningkatkan produktivitas organisasi. Pengguna tidak perlu masuk pada sistem login ganda dan tidak perlu mengingat pasangan username dan password untuk setiap aplikasi dan juga jumlah mengurangi jumlah panggilan untuk bantuan tentang password.
- Menyederhakana admin IT dengan mengurangi jumlah pasangan username dan password yang harus dikelola.
- Meningkatkan keamanan sistem.

Kerugian Single Sign-on

Selain mendatangkan manfaat, SSO juga dapat mendatangkan bencana. Dari cara pandang seperti ini, beberapa pengamat memperkirakan bahwa penggunaan SSO dapat menghemat biaya untuk memelihara password yang rumit yang dapat mencapai ratusan dolar setiap pengguna tiap tahun. Tetapi, implementasi SSO dalam sebuah jaringan yang heterogen adalah rumit, sehingga banyak administrator jaringan kurang begitu giat dalam mengimplementasikannya.

Contoh dari sistem SSO adalah protokol Kerberos, yang telah dimasukkan ke dalam sistem operasi Windows 2000 ke atas. Protokol yang sama dapat juga digunakan di dalam keluarga sistem operasi UNIX. Novell juga telah menawarkan fungsi SSO miliknya sendiri, yang disebut sebagai Novell Single Sign On (NSSO) yang dapat

digunakan dalam lingkungan Windows/NetWare. Beberapa perusahaan, seperti Entrust Technologies dan RSA Security menawarkan fungsi SSO yang berbasis kriptografi kunci publik.

3.3 Pengaturan Hotspot ITB

Hotspot adalah suatu area yang dilingkupi oleh sinyal WiFi sehingga mereka yang memiliki Laptop, PDA, Smartphone, dan perangkat WiFi lainnya bisa tersambung ke jaringan ITB. Di lingkungan ITB tersedia beberapa area Hotspot, baik yang dikelola oleh USDI maupun yang dikelola oleh unit kerja. Hotspot yang dikelola oleh USDI menggunakan SSID “Hotspot ITB” dan tidak menggunakan mekanisme pengamanan, sementara Hotspot yang dikelola unit kerja ada yang menggunakan mekanisme pengamanan tertentu.

USDI hanya menjamin keamanan akses internet via WiFi yang dikelola USDI. Keamanan koneksi internet via WiFi yang disediakan oleh pihak lain, bukan menjadi tanggung jawab USDI ITB [12].

Lokasi Hotspot ITB

- Kampus ITB - Ganesha
  - Aula Timur (2 lokasi)
  - Aula Barat (2 lokasi)
  - Campus Center Timur
  - Campus Center Barat
  - Labtek V: Ruang 7601 & Lantai 3
  - GKU Timur (3 lokasi)
  - TVST (3 lokasi)
  - Oktagon (2 lokasi)
  - Comlabs (2 lokasi)
  - Perpustakaan lantai 1
  - Perpustakaan lantai 2
  - Perpustakaan lantai 3
  - Perpustakaan lantai 4

    - Astronomi (2 lokasi)
    - PAU – CNRG
    - PAU - AI3
    - GKU Barat
- Rektorat ITB
    - Rapim A
    - Rapim B
    - Rektorat
    - Annex
    - LPPM
    - USDI
- Gedung BPI
    - Ruang Rapat Utama
    - Ruang Rapat Senat
    - Ruang Rapat MWA
- Kampus Jatinangor
    - Asrama Tower 1
    - Asrama Tower 2
    - Rektorat Lt.1
    - Rektorat Lt. 2
    - Rektorat Lt. 3
    - Gedung Mektan
    - Perpustakaan Lt.1
    - Perpustakaan Lt. 2
    - Perpustakaan Lt. 3
    - Perpustakaan Lt. 3 Ruang Rapat

Penggunaan

Untuk tersambung ke Hotspot ITB, berikut ini langkah-langkahnya:

- Aktifkan perangkat WiFi di Laptop, PDA, Smartphone, atau perangkat WiFi lain yang anda gunakan.

- Cari (Search/Scan) sinyal Wi-Fi yang ada pada area tersebut, kemudian pilih sambungan Wi-Fi dengan SSID Hotspot ITB.
- Isikan password: hotspotitb
- Sampai tahap ini anda sudah tersambung ke Jaringan ITB. Untuk bisa menjelajah Internet, anda perlu menyetel Proxy pada perangkat yang anda gunakan dan memiliki INA untuk autentikasi Proxy.

Password untuk dapat masuk terhubung ke hotspot itb tidak dirahasiakan, sehingga pasangan username dan password untuk autentikasi proxy seharusnya dirahasiakan.

3.4 Persyaratan Minimum Keamanan Jaringan untuk Lingkungan Kampus

Pemanfaatan internet untuk bidang pendidikan telah banyak membantu civitas akademika di lingkungan kampus dalam proses belajar mengajar. Selain memberikan dampak positif, penggunaan internet juga tak lepas dari efek negatif, antara lain issue keamanan jaringan lingkungan kampus.

Diperlukan audit dan investigasi jaringan kompuer kampus untuk menemukan celah kemanan dan memetakan serangan-serangan yang ada. Untuk proses audit, Indeks KAMI (SNI ISO 27000) digunakan sebagai standar keamanan komputer di Indonesia. Sedangkan untuk proses investigasi dapat menggunakan SNORT yang merupakan pendeteksi serangan pada jaringan komputer.

BAB IV

KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang didapat dari pembahasan dan saran untuk keamanan operasi penggunaan AI3.

4.1 Kesimpulan

Dari penjabaran pada Bab pembahasan, dapat ditarik kesimpulan sebagai berikut.

- Metode yang digunakan untuk mengaplikasikan AI3 ITB adalah proxy based SSO.
- Dalam implementasi pasangan username dan password akun AI3 dapat di ketahui dengan mudah menggunakan aplikasi yang tersedia.
- Pengaturan Hotspot ITB di tempatkan pada beberapa lokasi kampus, dengan password “hotspotitb”.

4.2 Saran

Berikut saran yang diajukan.

- Pasangan username dan password sebaiknya tidak dalam plain ketika berada dijaringan.
- Pasangan username dan password tidak diberikan pada orang lain (sharing akun).

DAFTAR PUSTAKA

[1] A. Pashalidis and C. J. Mitchell, "A Taxonomy of Single Sign-On System," in R. Safavi-Naini and J. Seberry (editors), Information Security and Privacy – 8th Australasian Conference, ACISP 2003, Wollongong, Australia, July 9-11 2013, Proceedings, Springer-Verlag (LNCS 2727), Berlin (2003), pp.249-264.

[2] Hongping Chen, Jinhong Li, and Qizhi Sun, "Campus Information Portal based on Portal Technology," in *Journal ACM Transactions on Information and System Security* (TISSEC), Article No. 10, Vol. 13 Issue 1, October 2009.

[3] Ashish G. Revar and Madhuri D. Bhavsar, "Securing user authentication using single sign-on in Cloud Computing," in *2011 Nirma University International Conference on Engineering*, December 2011.

[4] I. Fahmi, O. W. Purbo Mahmudin, N. Hasanah, and S. Suwandi, "Library Network in Indonesia," in Internet Workshop, 1999. IWS 99, pp. 268–271.

[5] S. Yamaguchi, T. Baba, and J. Murai, "Step beyond International Collaborations: our challenges in Asian Internet Interconnection Initiatives," in Proceedings Symposium 2003 on Application and the Internet Workshops, 2003, pp. 8–13.

[6] S. Yamaguchi and J. Murai, "Asian Internet Interconnection Initiatives," in 1996 Proceedings of INET, June 1996.

[7] AI3 MRTG Map. http://www.ai3.net/op/mrtg/.

[8] E. D. Vinas and T. Baba, "Characterization, analysis, and visualization of traffic in the Asian Internet Interconnection Initiatives (AI3) satelite-based research network test bed," in Proceedings Symposium on Application and the Internet Workshops, 2003, pp. 41–45.

[9] Hui Haoa and Hualin Qian, "Research and Design of Network Service System Unified Identity Authentication Model," Computer Science, vol.32, pp. 72–72, Sep. 2005.

[10] Runda Liu and Yunqiang Zhu, "A Simple Imlementation of Cross domain Single Sign on System," Computer Application, Vol.27, pp.288–291, Feb. 2007.

[11] Hongtao Hu and Zifang Guo, “The Application of cross-domain single sign-on in municipal portal,” in TENCON 2013. IEEE Region 10 Conference (31194), pp. 1–4.

[12] https://ditsti.itb.ac.id/hotspot-itb/.

[13] Steven Fewer, “ARP Poisoning An investigation into spoofing the Address Resolution Protocol,” Harmony Security, 2007.

[14] KEPUTUSAN REKTOR INSTITUT TEKNOLOGI BANDUNG NOMOR : 251/SK/K01/OT/2008 TENTANG KEBIJAKAN DAN ATURAN TEKNOLOGI INFORMASI INSTITUT TEKNOLOGI BANDUNG.