ANALISIS KEAMANAN JARINGAN *SINGLE SIGN ON* (SSO) DENGAN *LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL* (LDAP) MENGGUNAKAN METODE MITMA

Amarudin[1)], Widyawan[2)], Warsun Najib[3)]

Jurusan Teknik Elektro dan Teknologi Informasi
Universitas Gadjah Mada
Jl. Grafika No 2 Fakultas Teknik UGM, Yogyakarta 55283, Indonesia
Email:amarudin_s2te_12@mail.ugm.ac.id[1)], widyawan@gmail.com[2)], warsun@ugm.ac.id[3)]

Abstrak

Abstrak—Perkembangan aplikasi web secara tidak langsung menuntut pengguna aplikasi untuk dapat mengelola user dan password sistem aplikasi dengan baik agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Berbagai metode security user account telah disusulkan untuk memecahkan masalah-masalah tersebut. Diantaranya dengan menerapkan Authentication SSO (Single Sign On) dengan menggunakan Protocol LDAP (Lightweight Directory Access Protocol), dan database server MySQL.

Dalam penelitian ini meggunakan metode MITMA (Man In The Midle Attack) dan penggunaan tools hacking (Wireshark Versi 1.10.2, Pingflood.exe dan Ping Monitor Free Setup.exe) dalam pengujiannya. Hasil pengujian menunjukkan bahwa informasi IP korban maupun trafiknya dapat diketahui dan diidentifikasi dengan mudah melalui tools hacking dengan akurasi sebesar 85,71%.

Penelitian ini tentunya bermanfaat untuk mengetahui tingkat keamnan jaringan yang terintegrasi dengan SSO menggunakan protokol LDAP dan bisa dijadikan acuan untuk menguji model jaringan yang lain.

Kata kunci: *User account, authentication, single sign on (SSO), password, LDAP, MySQL, hacking.*

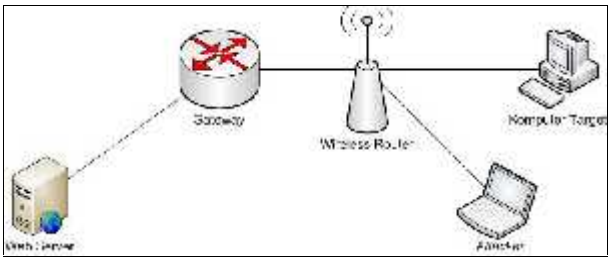
1. Pendahuluan

Perkembangan internet terus semakin pesat sehingga memungkinkan sebagian besar lembaga formal maupun non formal untuk terlibat didalamnya. Beberapa prinsip sederhana yang dimiliki internet adalah mudah dan menyenangkan untuk digunakan bagi penggunanya, dengan demikian fungsi internet semakin multifungsi [1].

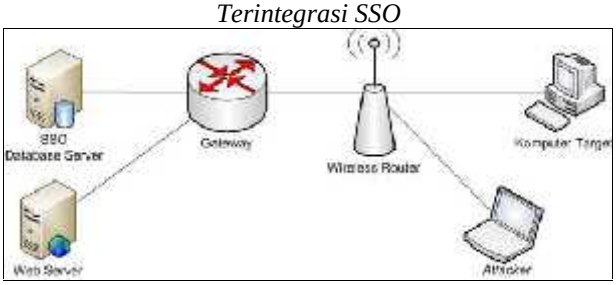
Seiring dengan maraknya penggunaan internet tersebut sehingga melibatkan jumlah *user* dalam penggunaan internet semakin bertambah banyak. Namun dengan semakin banyaknya jumlah *user*, secara tidak langsung malah menimbulkan masalah baru bagi *user* itu sendiri maupun admin sebagai pengelola *user* [2]. Salah satu masalah yang dihadapi *user* adalah banyak *user* yang lupa dengan *user account* dan *password* yang dimilikinya karena harus mengingat semua *user name* dan *password* untuk sistem-sistem tersebut [3, 4]. Selain dari itu tingkat keamanan *user account* semakin rentan dari serangan *hacker* [5]. Sepertihalnya *security* dalam *internet banking* membutuhkan keamanan kerahasiaan, integritas, dan privasi data yang luar biasa sehingga telah menjadi topik pembahasan yang semakin serius dalam *security networking* [6]. Selain dari itu muncul masalah baru bagi admin, yaitu masalah sulitnya admin dalam mengelola *user account*.

Selama beberapa dekade ini telah banyak dikembangkan berbagai cara untuk mempermudah pengelolaan dan meningkatkan keamanan *user acoount*, diantaranya dengan cara menerapkan pemanfaatan *Centralized Cookiebased SSO* (CC-SSO) [2], *Single Sign On* untuk *Cloud* [7]. Dalam rangka untuk meningkatkan efisiensi *user*, keamanan sistem informasi, dan produktifitas IT [8], maka perlu diimplementasikan otentikasi dengan SSO menggunakan LDAP (*Light Weight Directory Access Protocol*) [9]. Dengan adanya penerapan SSO ini diharapkan admin dapat mengelola setiap *user account* dengan efisien, mudah dan aman. Selain dari itu, setiap *user* tidak perlu susah payah dalam mengingat *user account* dan *password* yang dimiliknya.

Beberapa jaringan yang terintegrasi dengan SSO, telah menggunakan LDAP sebagai protokol untuk otentikasi [10], dan menggunakan Database Server MySql sebagai databasenya [11]. Apakah dengan menggunakan LDAP sudah relevan untuk diterapkan dalam otentikasi SSO, maka untuk mengetahui tingkat keamanan otentikasi SSO menggunakan LDAP tersebut, perlu dilakukan analisis tingkat keamanannya. Dengan demikian perlu dilakukan pengujian dengan cara *hacking* (*attacking* /*sniffing*) pada jaringan yang belum terintegrasi dengan SSO maupun pada sistem yang sudah terintegrasi dengan SSO yang menggunakan LDAP dan Database Server MySQL sebagai databasenya. Dari pengujian yang dilakukan, diharapkan dapat memperoleh tingkat efisiensi *user account* dan mengetahui tingkat keamanan SSO menggunakan LDAP. Gambaran umum dalam pengujiannya seperti pada Gambar 1.1 dan Gambar 1.2 berikut ini.



Gambar 1.1 *Pengujian Sistem Jaringan Tanpa Terintegrasi SSO*



Gambar 1.2 *Pengujian Sistem Jaringan Terintegrasi dengan SSO*

2. Tinjauan Pustaka

Pengujian keamanan jaringan komputer sudah banyak dilakukan dengan berbagai macam platform yang ada, maka dalam tinjauan pustaka ini hanya meninjau beberapa penelitian awal yang digunakan untuk menguji keamanan sistem jaringan komputer terintegrasi dengan SSO menggunakan LDAP.

Beberapa penelitian terkait pengujian keamanan sistem jaringan komputer SSO menggunakan LDAP antara lain adalah penelitian yang dilakukan oleh Yana Hendriana [12], yang menganalisis implementasi VPN pada CV Pangestu Jaya. Penelitiannya dilakukan dengan skenario uji kelayakan berdasarkan kebutuhan *user*. Pengujian-pengujian yang dilakukan adalah Pengujian Konektivitas, Pengujian Transfer Data, *Attacking* VPN dengan DoS (*Denial Of Services*), *Hacking* VPN dengan *ARP Poisoning* di Linux Backtrack. Hasil eksperimen pengujian *attacking* dengan *Denial of Service* (DoS) menggunakan *tools* pingflood ternyata berhasil mematikan *service*/ layanan pada VPN server. Selain itu pengujian *hacking*/*ARP Poisioning* untuk mendapatkan *user name* dan *password* dengan menggunakan *tools* yang ada pada Linux Backtrack juga berhasil menembus akses *login client* ke server.

Sedangkan penelitian yang telah dilakukan oleh Marti Widya Sari [13], melakukan penelitian analisis keamanan jaringan *Virtual Private Network* (VPN) pada sistem online microbanking di BMT Al Ikhlas Yogyakarta dengan cara menguji jaringan VPN menggunakan *tools* WireShark. Dalam penelitiannya dilakukan dengan dua tahap pengujian, pengujian pertama dilakukan pada jaringan tanpa menggunakan VPN, sedangkan pengujian kedua dilakukan pada jaringan menggunakan VPN Hamachi, dalam hal ini menggunakan aplikasi *Honeypot* (Honeyd, Dionaea) sebagai VPN. Dari hasil pengujian diperoleh perbandingan bahwa menggunakan VPN Hamachi (Honeypot) lebih aman dibandingkan tanpa VPN. Namun aplikasi VPN yang digunakan masih berupa *tools free* dan pengelolaan sistemnya masih dipegang oleh vendor pembuat sistem, sehingga untuk keamanan data dari pihak vendor sistem perlu dipertimbangkan lagi.

Dari penelitian yang telah dilakukan tersebut diperoleh metode pengujian keamanan jaringan yang sama sehingga dapat digunakan dalam pengujian keamanan jaringan *Single Sign On* (SSO) menggunakan LDAP yang belum pernah dilakukan dalam penelitian sebelumnya.

3. Landasan Teori

3.1. *Single Sign On* (SSO)

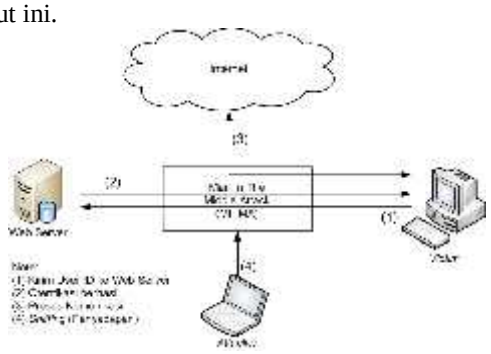
SSO adalah sebuah mekanisme yang membuat *user* hanya perlu mengingat satu *user name* dan *password* yang autentik untuk membuka beberapa layanan sekaligus. SSO perlu terautentikasi sekali, kemudian autentikasi akan terjadi otomatis ketika *user* membuka website lain melalui sebuah *session* [14].

3.2. *Lightweight Directory Access Protocol* (LDAP)

Lightweight Directory Access Protocol (LDAP) merupakan sebuah standar yang digunakan komputer dan perlengkapan jaringan untuk mengakses informasi umum melalui jaringan. Kemampuan untuk menyediakan akses data dalam jaringan tidak membuat LDAP berdiri sendiri terhadap protokol-protokol lain untuk mengakses data seperti *Hypertext Transfer Protocol* (HTTP). Sejumlah fitur dan vendor telah membuat LDAP dapat digunakan untuk mengakses dan meng-*update* berbagai tipe informasi [14].

3.3. *Man In The Middle Attack* (MITMA)

MITMA adalah sebuah aksi *sniffing* yang memanfaatkan kelemahan *switch* dan kesalahan penangannan *ARP chache* dan TCP/IP oleh Sistem Operasi [15]. Ide awalnya adalah menempatkan komputer *hacker* ditengah dua komputer yang sedang berhubungan sehingga paket data harus melalui komputer *hacker* agar paket data tersebut bisa dilihat atau disadap oleh *hacker*. Kemudian *hacker* mengarahkan *ARP chache* komputer korban (*victim*) dan komputer tujuan (*web server*) untuk menjadikan komputer *hacker* sebagai router. Ilustrasi Metode MITMA dapat dilihat seperti pada Gambar 3.1 berikut ini.



Gambar 3.1 *Ilustrasi Man-In-The-Middle Attack*

3.4. *ARP chance*

Adalah sebuah file yang digunakan untuk menyimpan alamat-alamat ip dan *mac address* dari komputer-komputer yang pernah berhubungan dengannya, dan jika suatu saat terjadi perbedaan ip antara *ARP chance*, dengan contoh DNS server, maka yang digunakan adalah alamat ip yang ada pada *ARP chance* tersebut [14].

4. Metode Penelitian

Dalam proses *snifing* (penyadapan), dalam penelitian ini menggunakan metode MITMA (*Man In The Middle Attack*). Yang dikerjakan dengan cara *experimen* melalui konfigurasi sebuah sistem aplikasi *web base* yang terkoneksi dengan SSO menggunakan LDAP. Kemudian sistem SSO tersebut dievaluasi keamanannya melalui eksperimen *hacking* (*attacking/sniffing*) untuk mengetahui apakah jaringan yang terintegrasi dengan SSO menggunakan LDAP sudah aman dari *sniffing* (penyadapan) atau belum.

4.1. Bahan Penelitian

Adapun spesifikasi bahan yang dibutuhkan adalah data-data yang berupa informasi mengenai perangkat *hardware* maupun *software* yang digunakan dalam membangun sistem jaringan terintegrasi dengan SSO menggunakan LDAP.

4.2. Alat Penelitian

Adapun alat-alat penelitian yang dibutuhkan antara lain:

1) Perangkat Keras (*Hardware*)
   Perangkat keras dalam penelitian ini menggunakan beberapa komputer, antara lain:
   a. Sistem Jaringan SSO dengan LDAP yang sudah digunakan di Lab Jaringan JTET UGM.
   b. CPU (*Central Processing Unit*) yang berfungsi sebagai server sistem baru yang akan diintegrasikan dengan sistem SSO pada Lab Jaringan JTETI UGM, dengan spesifikasi Processor Intel Pentium Core 2 Duo, RAM 4 GB, Hard Disk 1 TB, dengan OS Windows Server 2003.
   c. Laptop dengan spesifikasi Processor Intel Pentium Dual Core 1,8 GHz, RAM 3 GB, Hard Disk 320 GB, dengan OS Linux Bactrack, yang berfungsi sebagai komputer *hacker* berbasis Linux.
2) Perangkat Lunak (*Software*)
   Sedangkan daftar *software* yang digunakan antara lain:
   a. *Wireshark* versi 1.10.2
      Wireshark adalah salah satu *network analysis tools* atau packet *snifer*. Packet *snifer* sendiri diartikan sebagai sebuah program atau *tools* yang memiliki kemampuan untuk mencegat dan melakukan pencatatan terhadap *traffic* data dalam jaringan.
   b. *Software* Pingflood.
      Software Pingflood.exe hanya bisa berjalan pada komputer berbasis Windows dan *software* ini digunakan untuk mengirimkan paket Pingflood dengan jumlah yang besar, sehingga server akan mengalami *connection time-out/down* pada koneksinya.
   c. *Cain & Abel* versi 4.9.43
      Cain & Abel adalah sebuah *software* yang dapat digunakan untuk melakukan *hacking* via LAN (*snifing*). Tekniknya disebut dengan *Man In The Middle Attack* (MITMA).

4.3. Spesifikasi Jaringan

Berdasarkan data hasil *interview* dengan Admin jaringan JTETI, Bp Javilun, bahwa sistem jaringan SSO yang digunakan di JTETI UGM adalah menggunakan LDAP (*Light Weight Directory Access Protocol*). Pengujian keamanan jaringan SSO dilakukan di Lab Jaringan JTETI UGM secara lokal dengan WIFI/HOTSPOT yang sama dengan komputer *client* (*Laptop*) yang terhubung ke Server (Windows Server 2003), karena aksi *hacking* khususnya *arp poisoning* untuk menyadap *user name* dan *password* dapat dengan mudah dilakukan pada jaringan lokal. Sedangkan aksi *attacking* bisa dilakukan dimana saja pada semua jaringan yang terkoneksi ke jaringan internet, karena aksi *attacking* ini biasanya dilakukan untuk menyerang *ip public* komputer target.

4.4. Tempat Penelitian

Tempat penelitian dilakukan di beberapa lokasi yang masih terkoneksi dengan jaringan internet yang ada di wilayah JTETI UGM dengan menggunakan media internet maupun media Modem.

4.5. Jalan Pengujian

Untuk melakukan testing atau tahap pengujian keamanan jaringan SSO, dilakukan langkah-langkah sebagai berikut:

a. Instalasi *Software*
   Melakukan instalasi aplikasi-aplikasi yang diperlukan dalam *hacking/sniffing*.
b. Pengujian Konektifitas
   Pengujian ini dilakukan karena kebutuhan *user* untuk melakukan koneksi ke server, sehingga dapat melakukan pertukaran data.
c. Pengujian Transfer Data
   Pengujian ini dilakukan untuk mengetahui apakah transfer data antara *user/client* sudah dapat memenuhi kebutuhan *user*.
d. Pengujian Keamanan
   Pengujian ini dilakukan karena proses ini merupakan salah satu tujuan dari analisis keamanan jaingan SSO menggunakan LDAP, dengan melakukan *attacking/sniffing* (*hacking*).

Dalam pengujian keamanan jaringan yang terintegrasi dengan SSO LDAP, belum ditemukan standar yang baku. Dengan demikian disusun sekenario uji keamanan jaringan berdasarkan kebutuhan *user* dengan Metode MITMA. Pengujian-pengujian yang dilakukan adalah sebagai berikut:

3.5.1. Pengujian Konektifitas

Pengujian koneksi jaringan SSO LDAP antar server JTETI dengan *client*, dilakukan dengan cara pemantauan *route print*, *ping* dan *trace route* ke komputer server JTETI. Hal ini dilakukan dengan menggunakan *tools commend promt* yang dilakukan berulang kali untuk mengetahui konektifitas jaringan.

3.5.2. Pengujian Transfer Data

Pengujian trasfer data berupa file, serta memantau kestabilannya dengan beban file antara 5 sampai 80 MB. Pengujian ini menggunakan *tools* Ping Monitor Free Setup.exe.

3.5.3. *Attacking* Server SSO LDAP dengan DoS (*Denial Of Service*)

Denial Of Service (DoS) dilakukan *attack* dengan cara mengirim sebuah paket kepada alamat IP yang hendak diserang konektivitasnya dan menunggu respon dari alamat IP tujuan menggunakan Pingflood. Dengan cara ini diharapkan dapat membanjiri (*flood*) jaringan dengan jumlah paket yang sangat besar atau dengan sengaja menghabiskan sumber daya yang memang terbatas, sehingga berakibat *request time out* seperti *pending network connection*. Experimen ini menggunakan program aplikasi Pingflood.exe yang dijalankan pada *dos prompt*.

3.5.4. Identifikasi

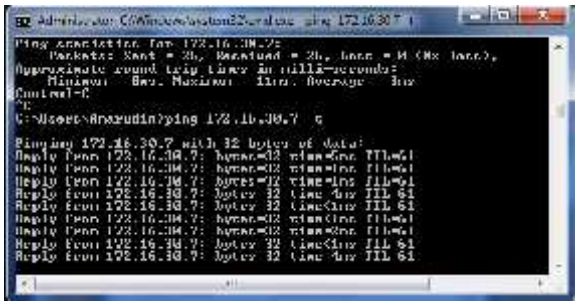
Dalam proses identifikasi ini dilakukan dengan cara pengamatan langsung (*observasi*) di lab Jaringan JTETI dengan maksud untuk mendapatkan data-data yang akurat dan sesuai dengan pokok permasalahan yang sedang terjadi di lapangan. Dalam melakukan pemantauan, menggunakan *software Cain & Abel* versi 4.9.43 atau *Wireshark* versi 1.10.2 sebagai *software* penguji jaringan yang dapat menggambarkan situasi yang sebenarnya terjadi jika saat ada serangan *hacker*. Kemudian dilakukan analisis terhadap masalah yang ada dengan melakukan evaluasi pada jaringan yang sudah terintegrasi dengan SSO maupun yang tidak terintegrasi.

5. Hasil dan Pembahasan

Dalam pengujian *network security*, belum ditemukan standar yang baku. Namun setelah melakukan *experimen* dengan menggunakan Metode MITMA, bisa diperoleh hasil pengujian sebagai berikut ini:

4.1. Pengujian Konektifitas

Pengujian Konektifitas ini dilakukan dengan cara ping ke IP *client* (target), dengan ketentuan harus mengetahui IP target terlebih dahulu. Untuk mengetahui IP target, dilakukan dengan cara men-scan jaringan melalui *tools* aplikasi Wireshark (Gambar 5.5). Hasil ping ke IP target adalah “Replay from 172. 16.30.7” seperti pada Gambar 5.1 berikut ini.



Gambar 5.1 *Ping ke IP Server*

4.2. Pengujian Transfer Data

Hasil pengujian yang dilakukan menggunakan *tools* Ping Monitor Free Setup.exe adalah seperti pada Gambar 5.2 berikut ini.

Gambar 5.2 *Hasil Pengujian dengan Tools Ping Monitor Free Setup.exe*

4.3. *Attacking* Server SSO LDAP dengan DoS

Experimen ini menggunakan program aplikasi Pingflood.exe yang dijalankan pada *dos prompt*. Langkah-langkah pengujiannya sebagai berikut:

1. Copy aplikasi pingflood tersebut kedalam *hardisk* di direktori Windows C:\WINDOWS.
2. Setelah pengkopian selesai cek apakah aplikasi tersebut sudah bisa digunakan. Caranya aktifkan Command Prompt dan ketik **pingflood** pada Command Promp tersebut, jika berhasil maka akan ada tampilan seperti Gambar 5.3 berikut ini.

Gambar 5.3 *Pingflood berhasil dijalankan*

3. Kemudian untuk pengujiannya gunakan format perintah dari ping flood: **pingflood <victim> [option].**
   Contoh:**pingflood 172.16.30.7 -n 100 -d 50 -s 15000**
   Penjelasan:
   pingflood, artinya mengaktifkan aplikasi ping flood.

172.16.30.7, adalah IP korban yang akan diserang menggunakan ping flood.
-n, artinya jumlah paket yang berjumlah 100.
-d, artinya delay tiap pengiriman paket.
-s 15000, artinya ukuran data yang dikirim sebesar 15000 bytes.

4. Setelah mengetahui IP address korban yang akan diserang, sebagai contoh (172.16.30.7). Aktifkan Command Prompt klik start > run > tulis cmd. Lakukan pengujian ping ke modem korban, caranya ketik ping 172.16.30.7.
5. Pengujian diatas menunjukan pengujian ping berhasil dan keadaan normal tidak ada paket yang *loss*. Rata-rata waktu tempuh 0 *mili second*.
6. Kemudian coba Ping flood ke korban caranya: Ketik pada command Prompt pingflood 10.190.x.x seperti pada Gambar 5.4 berikut ini.

Gambar 5.4 *Hasil Attacking dengan Pingflood.exe*

Akan terlihat perbedaan yang sangat segnifikan antara keadaan normal dengan keadaan pada saat dilakukan ping flood atau serangan *Distributed Denial of Service* (DDoS). Hal ini bisa dilihat perbedaannya pada saat melakukan ping flood selama lebih kurang 1-3 menit, dengan cara melakukan ping ke modem korban. Dengan demikian akan terlihat banyaknya jumlah paket yang *loss*. Selama proses ping flood ini, pada komputer korban akan dibanjiri kiriman paket data sehingga komputer korban tidak bisa beroperasi seperti normalnya.

4.4. Identifikasi

Tahap ini dilakukan untuk menganalisis trafik yang sedang berjalan dalam jaringan yang terintegrasi dengan SSO menggunakan *tools Wireshark*, seperti pada Gambar 5.5 berikut ini.

Gambar 5.5 *Hasil identifikasi dengan tools Wireshark*

Berdasarkan hasil identifikasi menggunakan *tools* Wireshark, beberapa informasi IP dan *trafic*-nya masih teridentifikasi oleh aplikasi. Misalnya pada IP 10.42.10.193 yang sedang mengakses Dropbox melalui protokol DB-LSP-DISC, dan IP 10.42.10.69 sedang mengakses http://paprirus2.te.ugm.ac.id melalui protokol HTTP. Untuk jaringan yang aman dari *sniffing*, seharusnya trafiknya tidak teridentifikasi dari *tools* dan dengan informasi trafik "NOTIFY" dengan protokol SSDP (*Simple Service Dicovery Protocol*) [13]. Hasil analisis pengujian *snifing* protokol menggunakan *tools* Wireshark pada jaringan SSO, bisa dilihat pada Tabel 1 berikut ini.

Tabel 1. *Hasil Analisis Sniffing Protokol pada Jaringan SSO dengan tools Wireshark*

No	IP Asal	IP Tujuan	Protokol	Hipotesa	Hasil Uji (T/F)	Kesimpulan	Keterangan
1	74.125.200.104	10.42.201.185	TCP	T	T	Diterima	Protokol Tidak Aman
2	10.42.200.72	10.42.203.255	NBNS	T	T	Diterima	Protokol Tidak Aman
3	10.42.202.46	10.42.203.255	DB-LSP-DISC	T	T	Diterima	Protokol Tidak Aman
4	AskeyCom_ff:c9:88	Broadcast	ARP	T	T	Diterima	Protokol Tidak Aman
5	10.42.200.60	239.255.255.250	SSDP	T	F	Ditolak	Protokol Aman
6	10.42.201.185	10.42.203.255	BROWSER	T	T	Diterima	Protokol Tidak Aman
7	fe80::3520:e19b:41c4:d9f7	ff02::1:ffea:1a6f	ICMPv6	T	T	Diterima	Protokol Tidak Aman
8	10.42.200.1	10.42.201.185	ICMP	T	T	Diterima	Protokol Tidak Aman
9	173.194.117.15	10.42.201.185	TLSv1	T	F	Ditolak	Protokol Aman
10	10.42.16.183	255.255.255.255	UDP	T	T	Diterima	Protokol Tidak Aman
11	10.42.16.101	10.42.16.255	CUPS	T	T	Diterima	Protokol Tidak Aman
12	10.42.16.204	10.42.16.187	NBSS	T	T	Diterima	Protokol Tidak Aman
13	10.42.16.187	10.42.16.204	LANMAN	T	T	Diterima	Protokol Tidak Aman
14	fe80::cd65:5850:ddb4:967c	ff02::1:2	DHCPv6	T	T	Diterima	Protokol Tidak Aman

Penjelasan dari **Tabel 1.** Hasil Analisis *Sniffing* Protokol pada Jaringan SSO dengan *tools* Wireshark adalah sebagai berikut:

Pada kolom Hipotesa berisi *True* (T) semua dengan maksud bahwa hipotesa/asumsi awal, setiap Protokol dapat diidentifikasi (di *Hecking*). Sedangkan pada kolom Hasil Uji berisi *True* (T) jika pengujian sesuai dengan Hipotesa atau berhasil mengidentifikasi trafik Protokol. Dan pada kolom Kesimpulan "Diterima". Jika pengujian tidak sesuai dengan Hipotesa atau tidak berhasil

mengidentifikasi trafik Protokol, maka pada kolom Hasil Uji berisi *False* (F) dengan Kesimpulan "Ditolak".

Berdasarkan pengujian identifikasi yang dilakukan pada 14 Protokol, diperoleh hasil uji *True*=12, dan *False*=2. Dengan demikian diperoleh hasil pengujian dengan akurasi *True*=85,71%, dan *False*=14,29%. Dari hasil pengujian (*Hacking*) sebesar 85,71% ini, menunjukkan bahwa setiap protokol masih rentan dari *Sniffing*, kecuali pada Protokol SSDP dan TLSv1 yang tidak dapat ditembus/diidentifikasi oleh *tools* Wireshark.

6. Kesimpulan

Berdasarkan hasil pengujian keamanan jaringan yang terintegrasi dengan SSO maupun yang tidak terintegrasi dengan SSO, bahwa informasi berupa IP korban maupun trafiknya dapat diketahui dengan mudah melalui *tools hacking* (Wireshark.exe) dengan akurasi sebesar 85,71%. Dengan demikian, hasil dari *sniffing* (penyadapan) ip dan trafik target tersebut, dapat digunakan untuk melacak identitas target. Misalnya untuk mendapatkan *user* dan *password* yang digunakan untuk login ke server yang terintegrasi dengan SSO menggunakan LDAP.

7. Saran

Untuk penelitian lebih lanjut, disarankan untuk meningkatkan *security* pada jaringan, misalnya dengan mengimplementasikan *Virtual Private Network* (VPN) atau protokol lain yang dapat digunakan untuk meningkatkan sekuritas pada jaringan yang terintegrasi dengan SSO dengan protokol LDAP. Selain dari itu perlu juga dilakukan penelitian lebih lanjut dalam *hacking* untuk mendapatkan *user name* dan *password*.

Daftar Pustaka

[1] K. Soohoo, "Multi-function Internet appliances," in *Wescon/97. Conference Proceedings*, 1997, pp. 14-18.

[2] M. E. Chalandar, P. Darvish, and A. M. Rahmani, "A centralized cookie-based single sign-on in distributed systems," in *Information and Communications Technology, 2007. ICICT 2007. ITI 5th International Conference on*, 2007, pp. 163-165.

[3] Z. Gaozheng, C. Mengdong, and S. Mou, "Authorization model of SSO for a distributed environment based on the attributes," in *Internet Technology And Secured Transactions, 2012 International Conferece For*, 2012, pp. 784-789.

[4] S. Dae-Hee, L. Im-Yeong, C. Soo-Young, and K. Choon-Soo, "Single sign-on authentication model using MAS(multiagent system)," in *Communications, Computers and signal Processing, 2003. PACRIM. 2003 IEEE Pacific Rim Conference on*, 2003, pp. 692-695 vol.2.

[5] G. Manimaran, "Internet infrastructure security," in *High Performance Interconnects, 2004. Proceedings. 12th Annual IEEE Symposium on*, 2004, p. 109.

[6] P. Subsorn and S. Limwiriyakul, "A Case Study of Internet Banking Security of Mainland Chinese Banks: A Customer Perspective," in *Computational Intelligence, Communication Systems and Networks (CICSyN), 2012 Fourth International Conference on*, 2012, pp. 189-195.

[7] P. Murukutla and K. C. Shet, "Single Sign on for Cloud," in *Computing Sciences (ICCS), 2012 International Conference on*, 2012, pp. 176-179.

[8] J. Montelius and B. Pehrson, "Web Single Sign-On System For WRL Company," *Department of Internetworking Royal Institute of Technology (KTH), IT-University Stockholm, Sweden*, p. 12, 2005.

[9] W. Latu. (2010, 29). *Penggunaan Sistem Single Sign On dengan LDAP*. Available: http://purpalacious.arieflatu.net/2009/08/penggunaan-sistem-single-sign-on-dengan-ldap/

[10] G. Huntington. (2006, 29). *SSO and LDAP Authentication*. Available: http://www.authenticationworld.com/Single-Sign-On-Authentication/SSOandLDAP.html

[11] M. Achour, F. Betz, A. Dovgal, N. Lopes, H. Magnusson, G. Richter, D. Seguy, and J. V. P. D. Group. (2013, 30). *HTTP authentication with PHP*. Available: http://php.net/manual/en/features.http-auth.php

[12] Y. Hendriana, "Evaluasi Implementasi Keamanan Jaringan Virtual Private Network (VPN) (Studi Kasus Pada CV.Pangestu Jaya," S2, Sistem Komputer dan Informatika (SKI), Universitas Gadjah Mada, Yogyakarta, 2012.

[13] M. W. Sari, "Analisis Keamanan Jaringan Virtual Private Network (VPN) pada Sistem Online Microbanking (Kasus di BMT Al Ikhlas Yogyakarta," S2, Magister Teknologi Informasi, Universitas Gadjah Mada, Yogyakarta, 2011.

[14] P. P. Nugroho, "Pengembangan Model Single Sign-On untuk layanan Internet dan Proxy IPB," S1, Ilmu Komputer Institut Pertanian Bogor, 2012.

[15] Baling-balingbambu. (2011). *Ini pengertian Tantang Man In Middle Attack* Available: http://balingbambu-baling-balingbambu.blogspot.com/2011/05/ini-pengertian-tantang-man-in-middle.html

Biodata Penulis

Amarudin, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Teknik Informatika STMIK TEKNOKRAT Lampung, lulus tahun 2011. Sedang menempuh pendidikan Program Pasca Sarjana S2 Jurusan Teknik Elektro dan Teknologi Informasi (JTETI) Universitas Gajah Mada Yogyakarta.

Widyawan, memperoleh gelar Sarjana Teknik (S.T), Jurusan Teknik Elektro Universitas Gajah Mada Yogyakarta, lulus tahun 1999. Memperoleh gelar *Master of Science* (M.Sc), NIHES, Erasmus University, Rotterdam, The Netherland, tahun 2002–2003. Memperoleh gelar (Ph.D), *Adaptive Wireless System*, Electronic Dept., CIT, Ireland, tahun 2005 – 2009.Saat ini menjadi Dosen di Jurusan Teknik Elektro dan Teknologi Informasi (JTETI) UGM, dan sebagai Kepala PSDI UGM Yogyakarta.

Warsun Najib, memperoleh gelar Sarjana Teknik (S.T), Jurusan Teknik Elektro Universitas Gadjah Mada Yogyakarta, lulus tahun 1997. Kursus bahasa Norwegia di Høgskolen I Volda, Norway, tahun 200-2001. Memperoleh gelar *Master of Science* (M.Sc) di Teknologi Informasi & Komunikasi Agder University College, Norway, tahun 2001-2003. Cork Institute of Technology, Irlandia, Program PhD: Kerangka Teknologi Lokalisasi Indoor, tahun 2007 s.d.sekarang. Dan saat ini menjadi Dosen di Jurusan Teknik Elektro dan Teknologi Informasi (JTETI) UGM Yogyakarta.