ANALISIS ASPEK KEAMANAN INFORMASI JARINGAN KOMPUTER (Studi Kasus: STIMIK Kupang)

Jemi Yohanis Babys[1)], Kusrini[2)], Sudarmawan[3)]
[1, 2, 3)]Magister Teknik Informatika STMIK AMIKOM Yogyakarta
Jln. Ring Road Utara, Condong Catur, Depok, Sleman, Yogyakarta
Email : [1)]betajemz@gmail.com, [2)]kusrini@amikom.ac.id, [3)]sudarmawan@amikom.ac.id

Abstrak
Jaringan komputer sebagai backbone dari teknologi informasi diharapkan dapat menyediakan layanan yang aman bagi penggunanya sehingga informasi-informasi penting seorang pengguna jaringan tidak dapat dicuri atau diakses oleh pengguna lain yang tidak berhak mengaksesnya. Oleh karena itu dalam suatu jaringan komputer perlu dilakukan analisis aspek confidentiality yang merupakan salah satu aspek dari keamanan informasi. Analisis ini bertujuan untuk mengukur tingkat kerahasian informasi pengguna jaringan komputer. Analisis ini dilakukan dengan cara melakukan ekspoitasi terhadap celah keamanan pada salah satu port yang terbuka di setiap client/hosts melalui internal jaringan komputer untuk mencuri informasi-informasi pengguna pada client/host yang dieksploit. Berdasarkan analisis yang dilakukan ditemukan kelemahan-kelemahan keamanan, baik itu pada tools pengamanan jaringan yang digunakan pada setiap client/host maupun pada instalasi jaringannya. Berdasarkan kelemahan-kelemahan keamanan tersebut ditemukan juga solusi-solusi untuk mengamankan jaringan, solusi-solusi tersebut akan direkomendasikan guna pengembangan jaringan yang lebih baik lagi. Solusi-solusi yang dihasilkan adalah sebagai berikut: (1) Melakukan segmentasi pada jaringan menggunakan VLAN dengan metode Access Control Lists (ACL) dan Port Security; (2) Melakukan instalasi firewall disetiap client/host dalam jaringan untuk melindungi setiap port yang terbuka pada sistem operasi yang digunakan, dalam penelitian ini menunjukan bahwa aplikasi McAfee 8.8 mampu melindungi port yang terbuka.

Kata Kunci: Jaringan komputer, Keamanan informasi, Eksploitasi *port*.

1. PENDAHULUAN

Dalam membangun suatu jaringan komputer salah satu hal penting yang harus dipahami dan diperhatikan dengan baik adalah mengenai keamanan informasi, salah satu aspek penting dalam keamanan informasi adalah aspek *confidentiality*, aspek ini menjamin kerahasiaan informasi pengguna jaringan komputer sehingga informasi tersebut tidak dapat diakses oleh pihak-pihak yang tidak memiliki hak untuk mengaksesnya (Syafrizal, 2007). Banyak terjadinya tindakan pencurian informasi-informasi pengguna seperti *username* dan *password* dari suatu akun atau data-data penting disebabkan oleh karena tidak adanya perlindungan terhadap aspek *confidentiality* dalam suatu jaringan komputer, hal ini tentunya akan berakibat fatal terhadap pengguna jaringan tersebut. Oleh karena itu perlu dilakukan analisis yang bertujuan untuk mengukur tingkat kerahasiaan informasi pengguna dalam suatu jaringan komputer guna pengembangan jaringan tersebut menjadi lebih baik lagi dalam hal perlindungan terhadap kerahasiaan informasi pengguna.

2. TINJAUAN PUSTAKA

Keamanan informasi terdiri dari perlindungan terhadap aspek-aspek berikut (Syafrizal, 2007):

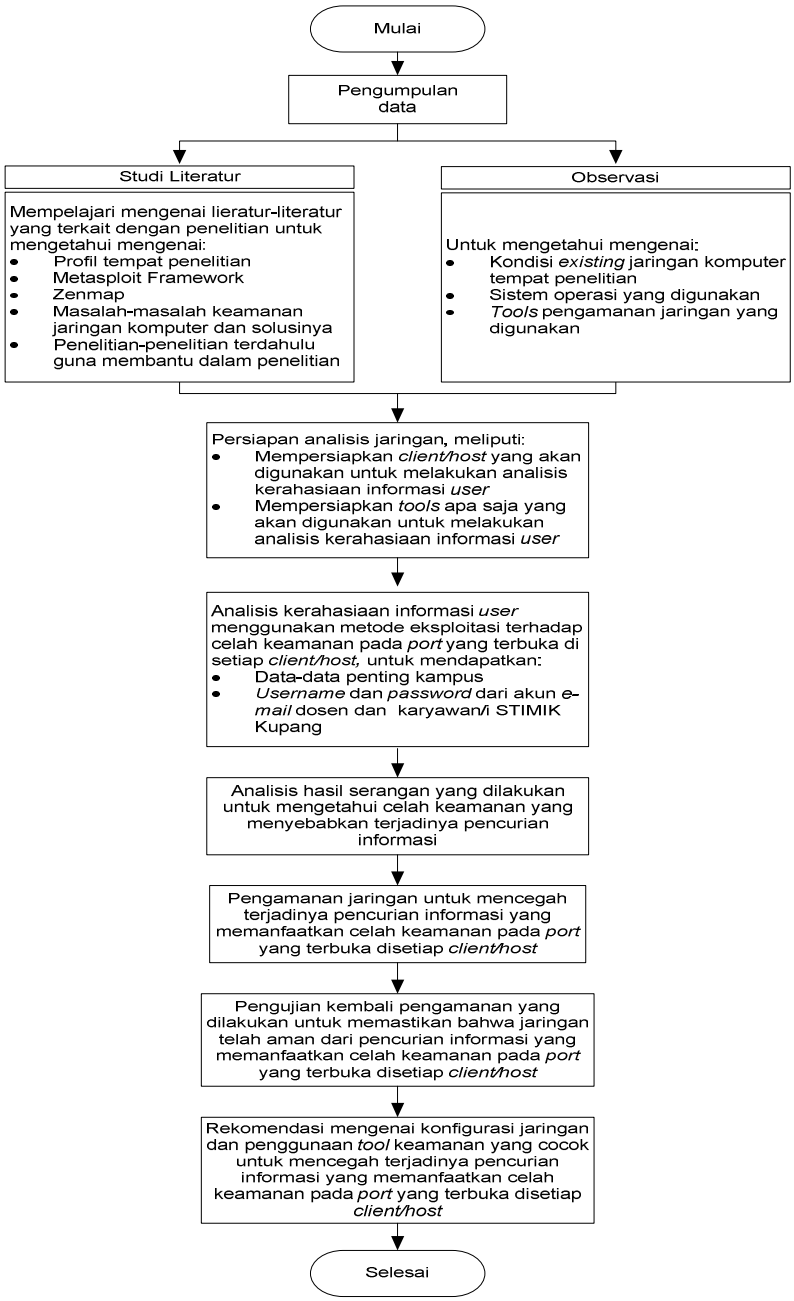
a. *Confidentiality* (kerahasian), artinya informasi dari pengguna jaringan komputer terjamin kerahasiaannya sehingga pihak yang tidak memiliki hak untuk mengakses informasi tersebut tidak dapat mengaksesnya.
b. *Integrity* (keutuhan), artinya informasi yang dikirim akan sampai kepada pihak yang tepat secara utuh tanpa di *intercept* oleh pihak ketiga dengan maksud untuk melakukan manipulasi terhadap informasi tersebut.
c. *Availability* (ketersediaan), artinya *user* dapat mengakses informasi yang dibutuhkan melalui layanan yang tersedia tanpa terjadi gangguan.

Telah banyak penelitian yang dilakukan mengenai keamanan informasi, penetian-penelitian tersebut bertujuan untuk meningkatkan keamanan informasi itu sendiri, seperti yang dilakukan oleh Wira Dimuksa dan Sukadi dalam jurnalnya yang berjudul Pengaman Data Kepolisian Pacitan Menggunakan Metode Kriptografi dan Anti *Keylogger*, penelitian ini menghasilkan aplikasi pengaman data yang menggunakan metode kriptografi AES dan pada aplikasi ini juga dilengkapi dengan *virtual keyboard* untuk menghindari jebakan *keylogger*. Aplikasi ini berfungsi untuk mengamankan data atau informasi dari tindakan pencurian data atau informasi pada Kepolisian Pacitan. Selain itu penelitian mengenai keamanan jaringan juga dilakukan oleh Ida Bagus Verry Hendrawan Manuaba yang membahas mengenai Evaluasi Keamanan Akses Jaringan Komputer Nirkabel pada kantor pusat Fakultas Teknik Universitas Gadjah Mada, pada penelitian ini dilakukan pengujian keamanan akses pada jaringan nirkabel dengan menggunakan serangan MAC *address spoofing*, *authentication attack*, *man in the middle attack*, DoS, *eavesdropping*, dan WEP *cracking*. Berdasarkan pengujian yang dilakukan tersebut

menghasilkan suatu model keamanan jaringan nirkabel sehingga dapat meningkatkan keamanan akses terhadap jaringan nirkabel.

3. METODE PENELITIAN

Penelitian ini melakukan analisis untuk mengukur tingkat kerahasiaan informasi pengguna jaringan komputer dengan cara melakukan eksploitasi terhadap celah keamanan pada *port* yang terbuka disetiap *client/hosts* melalui internal jaringan dengan menggunakan *tools* Zenmap dan Metasploit Framework yang terdapat pada sistem operasi Linux Backtrack 5 R1. Zenmap digunakan untuk melakukan *scanning port* pada *client/host* target untuk mengetahui *port-port* yang terbuka dan Metasploit Framework digunakan untuk melakukan eksploitasi terhadap celah keamanan pada *port* yang terbuka. Berikut adalah gambar yang menunjukan alur dari penelitian yang dilakukan:

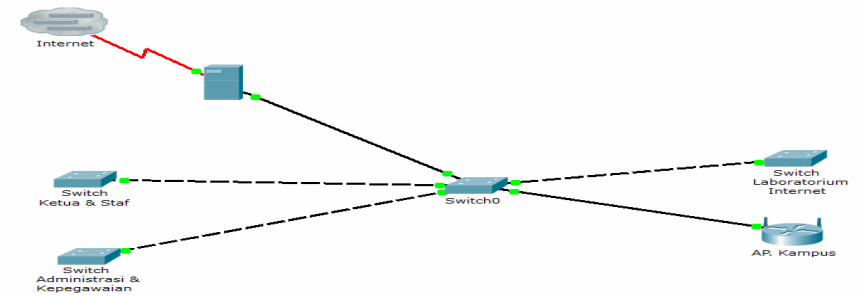


Gambar 1. Alur penelitian

4. HASIL DAN PEMBAHASAN

4.1 Jaringan Komputer STIMIK Kupang

Berikut adalah gambaran umum jaringan *local area network* STIMIK Kupang yang terkoneksi internet:



Gambar 2. Gambaran umum jaringan *local area network* STIMIK Kupang yang terkoneksi internet

Tabel 1. Daftar penggunaan *client/hosts* disetiap bagian

Bagian	Jumlah Hosts
Ketua dan Staf	5
Administrasi dan Kepegawaian	15
Laboratorium Internet	19

Pembagian IP *address* pada jaringan LAN yang menggunakan kabel untuk terhubung ke internet menggunakan sistem DHCP dan hanya menggunakan satu blok IP *address* yaitu 192.168.10.0/24. Setiap komputer menggunakan sistem operasi Windows XP, menggunakan aplikasi antivirus Smadav, AntiARP dan Avira AntiVir untuk mengamankan komputer. Spesifikasi komputer yang digunakan dalam jaringan bervariasi yaitu komputer dengan processor Intel Core 2 Duo 2.40 GHz dengan spesifikasi RAM 2 GB dan komputer Intel Pentium IV 2.60 GHz dengan spesifikasi RAM 1 GB.

4.2 Persiapan Analisis

Mempersiapkan *client/host* yang telah terinstall sistem operasi Linux Backtrack 5 R1 dan memastikan bahwa Zenmap dan Metasploit telah terinstall didalamnya dan dapat berjalan dengan baik.

4.3 Analisis Kerahasiaan Informasi User

4.3.1 Koneksi ke Jaringan

Koneksi kedalam jaringan dilakukan dengan mengkoneksikan *client/host* yang telah dipersiapkan sebelumnya kedalam jaringan melalui kelebihan *port* pada switch laboratorium internet STIMIK Kupang dan mengkonfigurasi IP *address* pada sistem operasi Linux Backtrack 5 R1 dengan menggunakan DHCP pada *network adapter* yang digunakan untuk mendapatkan IP *address*.

4.3.2 Port Scanning

Berikut adalah rekapitulasi data hasil dari *scanning port* menggunakan Zenmap yang dilakukan ke 15 (lima belas) *hosts* yang digunakan oleh bagian administrasi dan kepegawaian yang dianggap terdapat data-data atau informasi-informasi penting kampus.

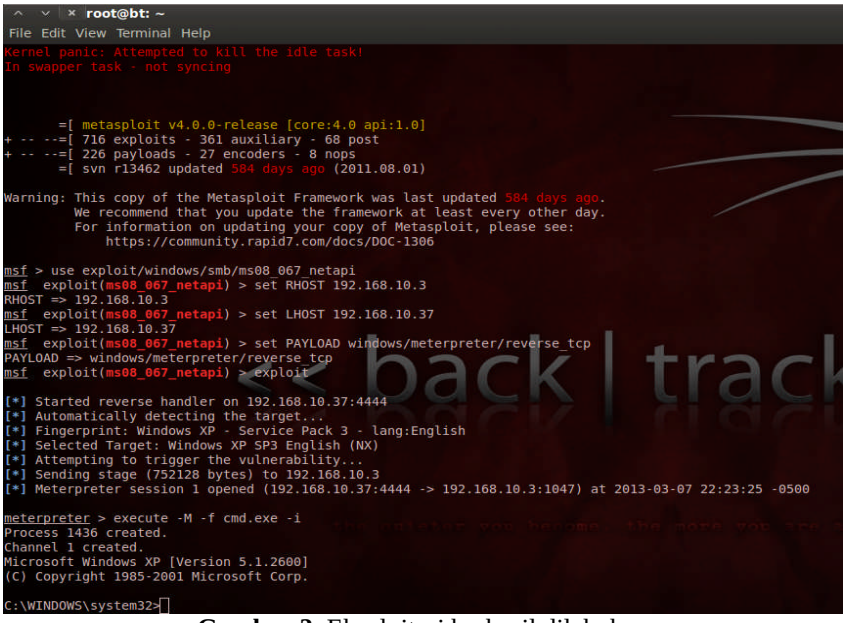
Tabel 2. Data hasil scanning port menggunakan Zenmap

No.	Hosts	Port Yang Terbuka
1	192.168.10.2/24	139, 445
2	192.168.10.3/24	139, 445
3	192.168.10.4/24	139, 445
4	192.168.10.5/24	139, 445
5	192.168.10.6/24	139, 445
6	192.168.10.7/24	139, 445
7	192.168.10.8/24	139, 445
8	192.168.10.9/24	139, 445
9	192.168.10.10/24	139, 445
10	192.168.10.11/24	139, 445
11	192.168.10.12/24	139, 445
12	192.168.10.13/24	139, 445
13	192.168.10.14/24	139, 445
14	192.168.10.15/24	139, 445
15	192.168.10.16/24	139, 445

Dari hasil *scanning* diatas rata-rata ditemukan 2 (dua) *port* yang terbuka yaitu *port* 139 dan *port* 445. *Port* 445 merupakan *port* yang digunakan oleh protokol *Server Message Block* (SMB) untuk melakukan tugas-tugas seperti *sharing file* dan *printer* dalam suatu jaringan komputer, *port* 445 sangat rentan terhadap serangan *worm* dan tindakan eksploitasi apabila dibiarkan terbuka (Speedguide.net, 2013).

4.3.3 Eksploitasi

Berdasarkan hasil *scanning* menggunakan Zenmap, maka akan dilakukan eksploitasi ke salah satu *host* yaitu *host* 192.168.10.3/24 melalui *port* 445 dengan menggunakan *tool* Metasploit Framework. Berikut adalah hasil yang diperoleh dari eksploitasi yang dilakukan ke *host* target dengan IP *address* 192.168.10.3/24.



Gambar 3. Eksploitasi berhasil dilakukan

Dari hasil analisis yang dilakukan menggunakan *tool* Metasploit Framework menunjukan bahwa terdapat celah keamanan pada *port* 445 yang terbuka, sehingga menyebabkan eksploitasi berhasil dilakukan. Dengan berhasilnya seorang *intruder* menyusup kedalam suatu sistem komputer *user* dalam suatu jaringan dengan memanfaatkan celah keamanan yang ada, maka tentunya *intruder* tersebut dapat mencuri informasi dengan menjalankan *keylogger* dan men-*download file-file* penting *user*, dan atau menanamkan *malware* kedalam sistem komputer *user* tersebut.

4.4 Analisis Kelemahan Keamanan

1. *Tools* keamanan yang digunakan pada setiap *client/host* bukan *personal* firewall tapi hanya antivirus dan anti ARP *spoofing* sehingga tidak bisa melindungi *port-port* yang terbuka pada komputer yang terhubung ke jaringan dari tindakan eksploitasi terhadap *port* yang terbuka. Salah satu hal yang harus dilakukan adalah dengan menginstal *firewall* untuk dapat melindungi *port-port* yang terbuka.
2. Terdapat kelemahan pada instalasi jaringan, kelemahan yang ditemukan seperti berikut:
   a. Pembagian IP *address* yang tidak sesuai dengan kebutuhan atau terjadi kelebihan IP *address* sehingga kelebihan IP *address* tersebut bisa dimanfaatkan oleh seorang *intruder* untuk terkoneksi ke jaringan,
   b. Tidak adanya perlindungan pada setiap *port* yang terdapat pada sebuah switch akan menyebabkan seseorang dapat mengkoneksikan komputernya kedalam sebuah jaringan melalui kelebihan *port* pada switch tersebut, dan
   c. Tidak adanya batasan hak akses tiap *user* dalam jaringan.

4.5 Pengamanan Jaringan

1. Salah satu program yang berfungsi sebagai *firewall* dan juga anti virus adalah McAfee yang dalam penelitian ini akan digunakan atau diinstal pada setiap *hosts* yang terhubung ke jaringan untuk melindungi *port-port* yang terbuka dan juga untuk melidungi komputer dari virus. Versi McAfee yang digunakan adalah McAfee 8.8
2. Untuk mengatasi permasalahan instalasi jaringan ini maka yang akan dilakukan adalah dengan mensegmentasi jaringan menggunakan Virtual Local Area Network (VLAN) dengan metode *Access Control Lists* (ACL) dan *port security*. Perangkat-perangkat yang akan digunakan dalam membangun VLAN ini adalah Cisco router 2621XM, Cisco switch 2950-24, perangkat akses point Linksys-WRT300N, Kabel UTP

dan konektor RJ-45. VLAN yang dibangun akan dibagi menjadi 12 (dua belas) VLAN. Berikut adalah tabel perencanaan dari VLAN yang akan dibangun.

Tabel 3. Perencanaan VLAN

Pengguna	VLAN ID	Interface Port	Status/ Mode	IP Address	Jlh PC
Router					
Switch Core-STIMIK	-	Fa0/0	-	-	-
Internet	-	Se0/0	-	-	-
Switch Core					
Router	-	Fa0/3	Trunk	-	-
Switch Pegawai	-	Fa0/2	Trunk	-	-
Switch Mahasiswa	-	Fa0/1	Trunk	-	-
-	-	Fa0/4 s/d 24	Shutdown	-	-
Switch Pegawai					
Switch Core	-	Fa0/1	Trunk	-	-
Hotspot Pegawai	110	Fa0/2	Access	192.168.10.0/30	-
Switch Pegawai I	-	Fa0/3	Trunk	-	-
-	-	Fa0/4 s/d 24	Shutdown	-	-
Switch Pegawai I					
Switch Pegawai	-	Fa0/1	Trunk	-	-
Ketua	101	Fa0/2	Access	192.168.1.0/30	1
Pembantu Ketua	102	Fa0/3 s/d 5	Access	192.168.2.0/29	3
Keuangan	103	Fa0/6	Access	192.168.3.0/30	1
Ketua Jurusan	104	Fa0/7 s/d 8	Access	192.168.4.0/29	2
BAAK	105	Fa0/9	Access	192.168.5.0/30	1
BAU	106	Fa0/10	Access	192.168.6.0/30	1
Dosen	107	Fa0/11 s/d 19	Access	192.168.7.0/28	9
UPT Perpustakaan	108	Fa0/20	Access	192.168.8.0/30	1
UPT Komputer	109	Fa0/21	Access	192.168.9.0/30	1
-	-	Fa0/22 s/d 24	Shutdown	-	-
Switch Mahasiswa					
Switch Core	-	Fa0/1	Trunk	-	-
Hotspot Mahasiswa	112	Fa0/2	Access	192.168.12.0/30	-
Switch Mahasiswa I	-	Fa0/3	Trunk	-	-
		Fa0/4 s/d 24	Shutdown		
Switch Mahasiswa I					
Switch Mahasiswa	-	Fa0/1	Trunk	-	-
Laboratorium Internet	111	Fa0/2 s/d 20	Access	192.168.11.0/27	19
-	-	Fa0/21 s/d 24	Shutdown	-	-

Pembagian *interface port* pada switch yang akan di konfigurasi dengan *port security* adalah seperti pada tabel berikut:

Tabel 4. Perencanaan port security

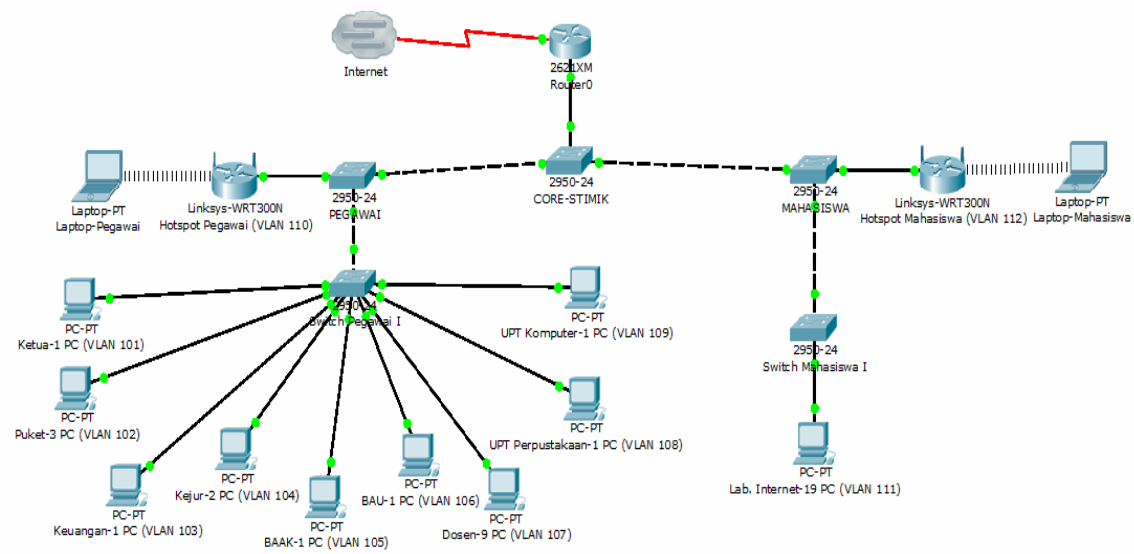
Switch	Port Security (Interface Fast Ethernet)
Switch Pegawai I	Fa0/2 s/d 21
Switch Mahasiswa I	Fa0/2 s/d 20

Rules yang digunakan untuk membatasi hak akses *user* dalam jaringan menggunakan ACL adalah sebagai berikut:

a. VLAN 101 dan 102 saling terkoneksi dan tidak bisa mengakses/diakses oleh VLAN lain dalam jaringan
b. VLAN 104, 105, 106, dan 107 saling terkoneksi dan tidak bisa mengakses/diakses oleh VLAN lain dalam jaringan
c. VLAN 103 tidak bisa mengakses/diakses oleh VLAN lain dalam jaringan
d. VLAN 108 tidak bisa mengakses/diakses oleh VLAN lain dalam jaringan
e. VLAN 109 tidak bisa mengakses/diakses oleh VLAN lain dalam jaringan
f. VLAN 110 tidak bisa mengakses/diakses oleh VLAN lain dalam jaringan

g. VLAN 111 tidak bisa mengakses/diakses oleh VLAN lain dalam jaringan
h. VLAN 112 tidak bisa mengakses/diakses oleh VLAN lain dalam jaringan

Berikut adalah hasil rancangan VLAN sebagai solusi dari permasalahan keamanan pada instalasi jaringan yang ditemukan, yang dirancang menggunakan *software* simulator jaringan Cisco Packet Tracer.

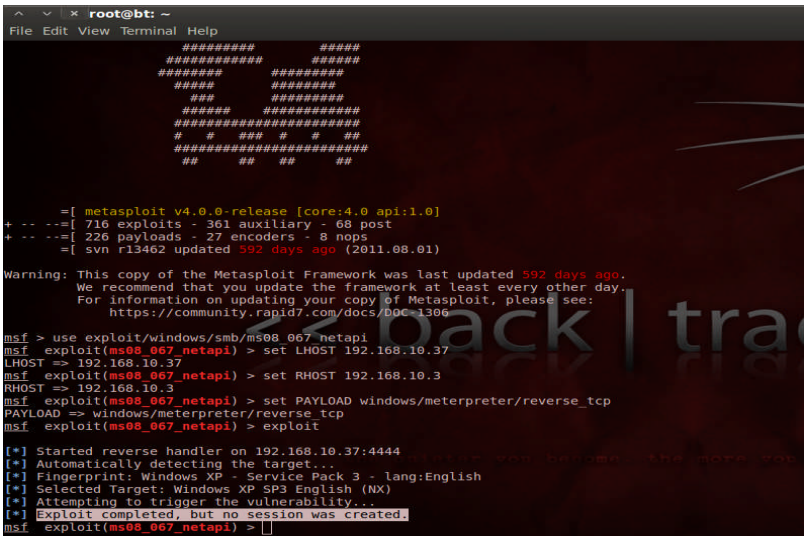


Gambar 4. Rancangan VLAN

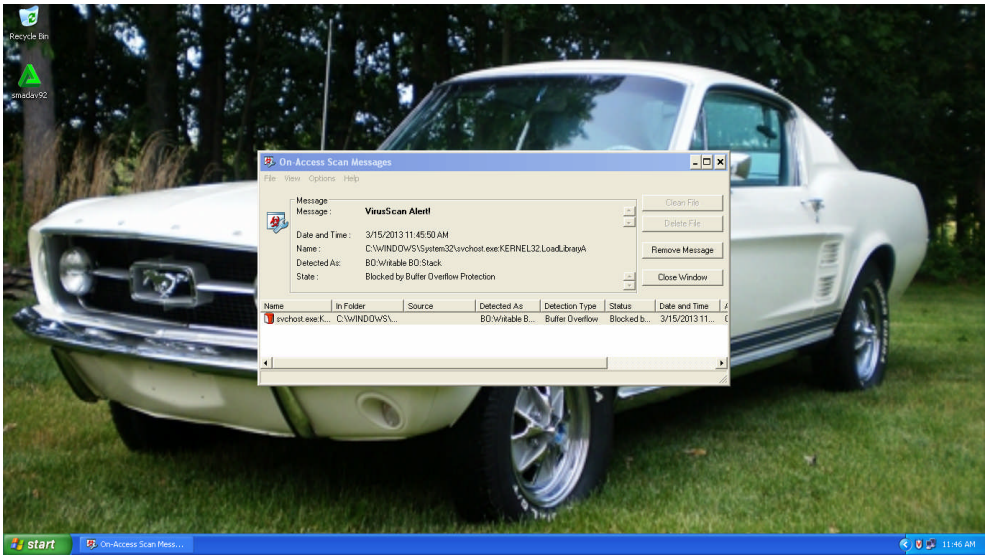
4.6 Pengujian Kembali Keamanan

4.6.1 Firewall

Dari pengujian yang dilakukan, seperti yang terlihat pada gambar 5 yang menampilkan pesan: *exploit completed, but no session was created* dan gambar 6 yang menunjukan McAfee memblok eksploitasi, menunjukan bahwa eksploitasi tidak berhasil dilakukan karena program McAfee yang diinstall telah melindungi komputer *user* dengan baik.



Gambar 5. Eksploitasi gagal



Gambar 6. McAfee memblok eksploitasi

4.6.2 Rancangan VLAN

Pengujian rancangan VLAN ini dilakukan dengan melakukan *ping* untuk memastikan bahwa ACL dan *port security* telah bekerja dengan baik. Berikut adalah data hasil rekapitulasi berdasarkan pengujian yang telah dilakukan yang menunjukan bahwa ACL dan *port security* telah bekerja dengan baik:

1. ACL

Tabel 5. Rekapitulas hasil pengujian ACL

VLAN	101	102	103	104	105	106	107	108	109	110	111	112	INTERNET
101													
102													
103													
104													
105													
106													
107													
108													
109													
110													
111													
112													

Keterangan :
- Access permit :
- Access deny :

2. Port security

Tabel 6. Rekapitulasi hasil pengujian port security

Switch	Interface (Fa0/)																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Pegawai I																								
Mahasiswa I																								

Keterangan :
- Port security :
- Non port security :

4.7 Rekomendasi

Berdasarkan analisis kerahasiaan informasi pengguna jaringan komputer yang telah dilakukan menggunakan *tools* Zenmap dan Metasploit Framework yang terdapat pada sistem operasi Linux Backtrack 5 R1, telah ditemukan kelemahan keamanan pada jaringan yaitu pada *tools* keamanan jaringan yang digunakan dan pada instalasi jaringan. Berdasarkan kelemahan keamanan tersebut ditemukan juga solusi-solusi yang diperoleh untuk mengamankan jaringan. Solusi-solusi tersebut akan direkomendasikan guna pengembangan jaringan yang lebih baik lagi, berikut adalah rekomendasi yang dihasilkan untuk mengamankan jaringan:

a. Melakukan segmentasi pada jaringan menggunakan VLAN dengan metode ACL dan *port security* untuk mengamankan jaringan, dan
b. Melakukan instalasi firewall disetiap *hosts* yang terkoneksi ke jaringan untuk melindungi setiap *port* yang terbuka pada sistem operasi yang digunakan *user*. Dalam penelitian ini menunjukan bahwa aplikasi McAfee 8.8 mampu melindungi *port* yang terbuka.

5. KESIMPULAN

Untuk mengamankan atau menjaga kerahasiaan informasi pengguna pada jaringan *local area network* yang menggunakan kabel sebagai media transmisi dari tidakan eksploitasi terhadap celah keamanan pada *port* yang yang terbuka disetiap *client/host* yang dilakukan melalui internal jaringan dapat dilakukan dengan beberapa hal, diantaranya adalah:

a. Dengan menginstal *personal* firewall di setiap *client/host* untuk melindungi *port-port* yang terbuka. Dalam penelitian ini menunjukan bahwa McAfee 8.8 mampu melindungi *port-port* yang terbuka dari tindakan eksploitasi, dan
b. Dengan melakukan segmentasi pada jaringan menggunakan VLAN dengan menggunakan metode ACL untuk membatasi hak akses tiap *user* dalam jaringan dan *port security* untuk mengamankan *port-port* pada switch.

DAFTAR PUSTAKA

Dimuksa, W.; Sukadi., 2012, *Pengaman Data Kepolisian Menggunakan Metode Kriptografi Dan Anti Keylogger*, Jurnal Speed 13, ISSN: 1979-9330 (Print) - 2088-0154 (Online) - 2088-0162 (CDROM), Vol. 9, Issue. Agustus, 2012

Hendriana, Y., 2012, Evaluasi Implementasi Keamanan Jaringan Virtual Private Network (VPN) (Studi Kasus Pada CV. PANGESTU JAYA), Tesis, Magister Teknologi Informasi, Universitas Gadjah Mada, Yogyakarta

Speedguide.net, 19 April 2013, http://www.speedguide.net/port.php?port=445

Syafrizal, M., 2007, *ISO 17799: Standar Sistem Manajemen Keamanan Informasi*, Seminar Nasional Teknologi 2007 (SNT 2007), ISSN: 1978-9777, Issue. 24 November, 2007