ANALISA KEAMANAN INTERNET MENGGUNAKAN NESSUS DAN ETHEREAL UNIVERSITAS PUTRA INDONESIA "YPTK" PADANG

Rizki Nurdin[1]

ABSTRACT

With the existence of this information will be easily obtained, the exchange of data that occurs in the virtual world will increase. In addition to the development of this technology, unwittingly evolved also crimes that occur in cyberspace that can harm users who access these sites, ranging from the delivery of viruses, spamming or other types of crime. So that institutions connected in an Internet network will be very vulnerable to network security at the institution. This is given that the productivity of an institution or company will depend on the performance of the network in it. Damage that occurs in a network will result in data exchange that occurs on the network will slow or even damage the network system. Therefore a mechanism that is used to analyze network security is required. Computer network security systems connected to the Internet must be planned and well understood in order to protect the resources within the network effectively.

Keywords : Nessus and Ethereal, Internet Security

INTISARI

Dengan adanya hal ini informasi apapun akan dengan mudah didapatkan, pertukaran data yang terjadi di dunia maya tersebut akan semakin bertambah. Di samping perkembangan teknologi ini, tanpa disadari berkembang pula kejahatan yang terjadi di dunia maya yang mampu merugikan *user* yang mengakses situs-situs tersebut, mulai dari pengiriman virus, pengiriman *spam* atau jenis kejahatan lainnya. Sehingga institusi yang terhubung dalam suatu jaringan internet akan sangat rentan dengan keamanan jaringan pada institusi tersebut. Hal ini mengingat bahwa produktivitas suatu institusi atau perusahaan akan sangat bergantung pada kinerja jaringan di dalamnya. Kerusakan yang terjadi pada suatu jaringan akan mengakibatkan pertukaran data yang terjadi pada jaringan tersebut akan melambat atau bahkan merusak sistem jaringan tersebut. Oleh karena itu dibutuhkan mekanisme yang digunakan untuk menganalisa keamanan jaringan. Sistem keamanan jaringan komputer yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif.

Kata Kunci: Nessus dan Ethereal, Keamanan Internet

[1]Dosen UPI YPTK Padang

PENDAHULUAN

Perkembangan teknologi informasi khususnya pada *World Wide Web* (WWW) yaitu sistem informasi dalam bentuk teks, gambar, suara, dan lain-lain direpresentasikan dalam bentuk *hypertext* yang merupakan salah satu contoh nyata perkembangan teknologi informasi.

Perkembangan sistem informasi *saat* ini sangat pesat sekali. Perkembangan ini ditandai dengan berkembangannya situs-situs yang berisi informasi baik seputar ilmu pengetahuan dan teknologi, hiburan, permainan, kesehatan atupun berisi curahan hati pembuat situs.

PENDEKATAN PEMECAHAN MASALAH

Analisis Jaringan

Analisys merupakan tahap pertama dimana *system engineering* menganalisis hal-hal yang diperlukan dalam pelaksanaan proyek pembuatan atau pengembangan system dalam bidang komunikasi dan komputerisasi (Jack Febrian: 2004).

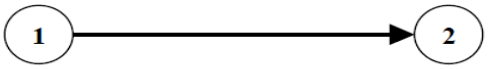
Secara umum dapat dikatakan bahwa analisis jaringan digunakan untuk membantu menyelesaikan masalah-masalah yang muncul dari serangkaian pekerjaan.

Analisis jaringan ini pertama kali dikembangkan oleh perusahaan jasa konsultan manajemen Boaz, Allen dan Hamilton yang dibuat untuk keperluan perusahaan pesawat terbang *lockhead*. *Metode* yang biasanya digunakan sering disebut dengan PERT yang merupakan singkatan dari *program evaluation and review tachnique*. Tanpa bermaksud meniru, ada juga metode CPM (*Critical Path Method*) yang dapat digunakan untuk menyelesaikan masalah jaringan ini.

Perbedaan utamanya adalah, CPM lebih menekankan pada efisiensi biaya pelaksana serangkaian pekerjaan, dengan mempercepat salah satu atau beberapa kegiatan dalam rangkaian pekerjaan tersebut.

Beberapa istilah dalan analisis jaringan antara lain adalah:

1. Aktivitas, adalah suatu pekerjaan yang membutuhkan pengorbanan sumberdaya (waktu, tenaga dan biaya). Aktivitas ini biasanya disimbolkan dengan anak panah.
2. Kejadian, adalah permulaan atau akhir dari sebuah aktivitas, dan disimbolkan dengan sebuah lingkaran.



Gambar 1. Permulaan Atau Akhir Dari Sebuah Aktivitas

3. Jalur kritis adalah sebuah jalur yang waktu penyelesaian serangkaian pekerjaannya paling besar/panjang.
4. *Earliest Start Time* (ES), adalah waktu paling cepat untuk memuali sebuah aktivitas.
5. *Lates Start Time* (LS), adalah waktu paling lambat untuk memulai sebuah aktivitas.
6. *Earliest Finish Time* (EF), adalah waktu peling cepat untuk selesainya sebuah aktivitas.
7. *Latest Finish Time*, adalah waktu paling lambat untuk menyelesaikan sebuah aktivitas.

Beberapa Hal yang penting dalam analisis jaringan adalah:

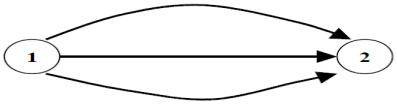
1. Sebelum suatu aktivitas dimulai, semua aktivitas yang mendahuluinya (yang menjadi syarat) harus sudah selesai dikerjakan terlebih dahulu.

2. Anak panah yang menjadi simbol sebuah aktivitas hanya menunjukkan arah dan uruturutan kejadian, jadi panjang pendek dan bentuknya tidak akan memberi pengaruh apapun.
3. Lingkaran, yang merupakan simbol dari kejadian, diberi nomor sedemikian rupa sehingga tidak memiliki nomor yang sama dan sebaiknya berurutan, sehingga dapat menggambarkan urutan kejadian. Biasanya nomor yang lebih kecil diletakkan di kejadian awal (permulaan anak panah).
4. Dua buah kejadian (lingkaran) hanya dapat dihubungkan dengan satu anak panah.
5. Sebuah rangkaian pekerjaan hanya dapat dimulai dan diakhiri dengan sebuah kejadian (lingkaran).

Namun demikian, seringkali suatu kasus jaringan dihadapkan pada kondisi dimana poin 4 dan 5 di atas, tidak dapat dihindari, sehingga untuk mengatasinya harus dibuatkan atau dibantu dengan sebuah aktivitas *dummy*.

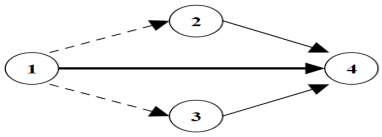
Aktivitas *dummy* adalah aktivitas yang sebenarnya tidak ada, sehingga tidak memerluakan pengorbanan sumber daya. Jadi manfaat dari aktivitas *dummy* adalah:

a. Untuk menghindari terjadinya kondisi dimana dua kajian dihubungkan oleh lebih dari satu anak panah



Gambar 2. Aktivitas *Dummy*

Dengan aktivitas *dummy* akan menjadi :



Gambar 2.3 Hasil Aktivitas *Dummy*

b. Untuk memenuhi ketentuan, di mana serangkaian kejadian hanya dapat dimulai dan diakhiri dengan satu kejadian (lingkaran).
c. Untuk menunjukkan urutan kejadian atau aktivitas yang sebenarnya.

Konsep Keamanan Jaringan Internet

Internet telah berkembang ke seluruh pelosok dunia secara global dan tidak mempunyai batas-batas negara lagi, kejahatan yang mungkin timbul masih tetap mempunyai ciri dan cara yang bergantung kepada negara/daerah tempat sipelaku berada, yaitu cara perpikir, cara pandang, moral, norma kehidupan dan pergaulan, bahkan bahasa pun sangat mempengaruhinya serta fakto-faktor lokal lainnya. Pintu dan tingkat kecanggihan kejahatan ditingkat *global* berkembang bersama perkembangan jaman dan kebudayaan lokal.

Sebagai salah satu contoh perkembangan internet, kita bisa melihat salah satunya di Jepang. Pertumbuhan pemakai internet di Jepang adalah seperti garis *linier* (deret hitung), naik secara pasti dari tahun ke tahun, dan ditahun 1999, telah mencapai 15 juta orang lebih, atau 1/10 jumlah penduduk Jepang. Kemudian, dilihat dari pemakaian internet untuk apa, yang terbanyak adalah untuk e-mail dan untuk mencari informasi secara gratis (masing-masing 98.5% dan 98%). Setelah itu untuk *mailing-list*, belanja secara *on-line* lewat internet, untuk membuat *homepage* perusahaan ataupun pribadi, menduduki peringkat berikutnya. *On-line*

shopping hanya menduduki rangking ke-4 (38.4%), menandakan bahwa belanja lewat internet masih belum dilirik oleh kebanyakan orang, mungkin karena mereka masih ragu-ragu tentang keamanan belanja di dunia maya (Agus Fanar Syukri: 2003).

Bahwa sebenarnya internet belumlah benar-benar aman. Ada 2 alasan utama ketidakamanan internet adalah sebagai berikut:

1. Internet adalah wilayah bebas *tak bertuan*, tak ada pemerintahan & hukum yang mengaturnya. Manajemen dan perlindungan keamanan masing-masing jaringan diserahkan sepenuhnya kepada penanggungjawab jaringan (*administrator* jaringan internet). Dan pada kenyataannya, tidak semua administrator jaringan, mengerti dengan baik tentang keamanan internet.
2. Masih banyaknya '*hole'* (lubang) di sistem komputer dan jaringan yang dapat dimanfaatkan oleh *cracker* demi keuntungan/kepuasan nafsu pribadinya.

Pada era *global* ini, keamanan sistem informasi berbasis internet harus sangat diperhatikan, karena jaringan komputer internet yang sifatnya publik dan *global* pada dasarnya tidak aman. Pada saat data terkirim dari suatu terminal asal menuju ke terminal tujuan dalam internet, data itu akan melewati sejumlah terminal yang lain yang berarti akan memberi kesempatan pada *user internet* yang lain untuk menyadap atau mengubah data tersebut. Sistem keamanan jaringan komputer yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif. Apabila ingin mengamankan suatu jaringan maka harus ditentukan terlebih dahulu tingkat ancaman (*threat*) yang harus diatasi, dan resiko yang harus diambil maupun yang harus dihindari. Berikut ini akan dibahas mengenai ancaman (*threat*) , kelemahan, dan *policy* keamanan (*security policy*) jaringan.

Insiden Keamanan Jaringan

Menurut G. J. Simons, keamanan informasi adalah "bagaimana kita dapat mencegah penipuan (*cheating*) atau paling tidak mendeteksi adanya penipuan disebuah system yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik.

Security attack, atau serangan terhadap keamanan sistem informasi, dapat dilihat dari sudut peranan komputer atau jaringan komputer yang fungsinya adalah sebagai penyedia informasi. Menurut W. Stallings ada beberapa kemungkinan serangan (*attack*):

1. *Interruption*: Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (*availability*) dari sistem. Contoh serangan adalah "*denial of service attack*".
2. *Interception*: Pihak yang tidak berwenang berhasil mengakses aset atau informasi. Contoh dari serangan ini adalah penyadapan (*wiretapping*).
3. *Modification*: Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari *website* dengan pesan-pesan yang merugikan pemilik *website*.
4. *Fabrication*: Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesanpesan palsu

seperti *e-mail* palsu ke dalam jaringan komputer.

Insiden keamanan jaringan adalah suatu aktivitas terhadap suatu jaringan komputer yang memberikan dampak terhadap keamanan sistem yang secara langsung atau tidak bertentangan dengan *security policy* sistem tersebut. Secara garis besar, insiden dapat diklasifikasikan menjadi: *probe*, *scan*, *account compromize*, *root compromize*, *packet sniffer*, *denial of service*, *exploitation of trust*, *malicious code*, dan *infrastructure attacks*. Berikut ini akan dibahas mengenai jenis jenis insiden tersebut

Nessus

Sekarang sudah bisa diketahui beberapa jenis serangan dan gangguan kejahatan yang terjadi di dalam jaringan komputer perusahaan, dan beberapa metode umum yang sering dilakukan untuk menyerang IT aset anda. Hal ini sangat penting untuk dipelajari karena *nessus* perlu disesuaikan dengan kondisi infrastruktur jaringan yang ada di perusahaan dan model bisnis dengan asset teknologi informasi. Cara cepat untuk menentukan apakah dibutuhkan *nessus* adalah dengan menjawab beberapa pertanyaan berikut ini.

1. Apakah anda memiliki data, yang jika berada ditangan orang lain akan berakibat fatal, dapat mengakibatkan mimpi buruk bagi citra perusahaan atau data finansial mengenai keuntungan dan kerugian *costumer* dan *clients*.
2. Apakah anda memiliki data jika data itu dicuri dapat melumpuhkan operasi anda dan kredibilitas perusahaan anda.

Ethereal

Penganalisa dengan *ethereal* merupakan pendeteksi lalu lintas jaringan dengan men-*capture* paket dalam jaringan secara langsung dan menayangkan isi dari paket tersebut. Dimulai dengan instal paket *ethereal* dari *repositori* “universe” dan pilih *applications* -> internet -> *ethereal*.

Ethereal adalah sebuah *network protocol analyzer* yang dapat didapatkan secara gratis. *Ethereal* dapat berjalan pada sistem operasi *linux* dan *window*. *Ethereal* memberikan ringkasan dan informasi yang mendetail mengenai paket yang “ditangkap”.

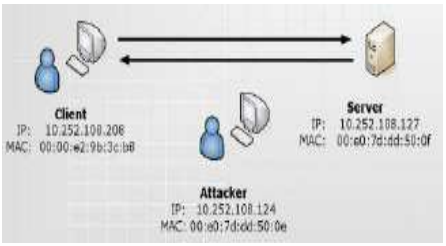
Berikut ini adalah fitur-fitur yang dimiliki oleh *ethereal*-0.9.14:

1. Data dapat langsung ditangkap dari koneksi jaringan secara langsung.
2. *Ethereal* dapat membaca *file-file* yang ditangkap oleh *tcpdump, NAI’s Sniffer, Sniffer Pro, Sunsnoop, atmsnoop,* dan lain-lain.
3. Data langsung dapat dibaca dari Ethernet, FDDI , PPP, Token Ring, IEEE 802.11, *classical IP over ATM,* dan *loopback interface.*
4. Data yang ditangkap dapat dilihat secara grafis.
5. 393 *protocol* dapat dikenali oleh *ethereal*.
6. *Output* dapat disimpan atau diprint sebagai *plain text* atau sebagai *Post Script*.

a. Prinsip Kerja Ethereal

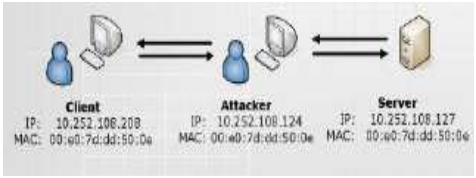
Sniffer adalah program yang membaca dan menganalisa setiap protokol yang melewati mesin di mana program tersebut diinstal. Secara default, sebuah komputer dalam jaringan (*workstation*) hanya mendengarkan dan merespon paket-paket yang dikirimkan kepada mereka. Namun

demikian, kartu jaringan (*network card*) dapat di*set* oleh beberapa program tertentu, sehingga dapat memonitor dan menangkap semua lalu lintas jaringan yang lewat tanpa peduli kepada siapa paket tersebut dikirimkan. Aktifitasnya biasa disebut dengan *sniffing*. Untuk dapat membaca dan menganalisa setiap protokol yang melewati mesin, diperlukan program yang bisa membelokkan paket ke komputer attaker. Biasa disebut serangan *spoofing*. Attaker akan bertindak sebagai *Man-In-the-Middle* (*MIM*).



Gambar 2.5 Koneksi Tcp Sebelum *Spoofing*

Gambar di atas mengilustrasikan koneksi TCP yang sebenarnya, tanpa ada sebuah *host* yang bertindak sebagai *MIM*. Kemudian *host attacker* menjalankan program *spoofing*, berarti host *attacker* akan bertindak sebagai *host* yang dilewati data antara *host client* dan *host server*.

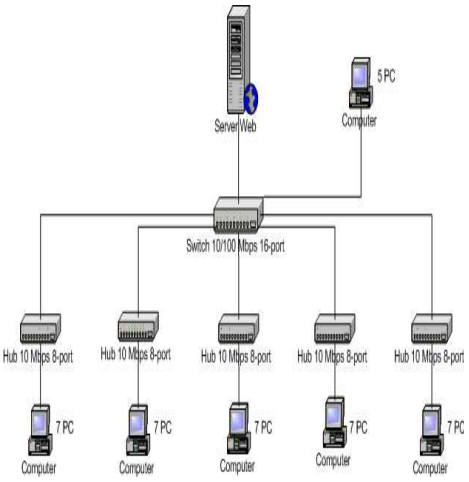


Gambar 2.6 Koneksi TCP Setelah *Spoofing*

Setelah host *attacker* menjadi host yang berada di tengah-tengah dari dua *host* yang saling berkomunikasi, kemudian *attacker* melakukan analisa *traffic* dengan menjalankan program *ethereal*. Dengan menganalisa *traffic* TCP yang sudah *tercapture*, *attacker* dapat mengetahui apa saja yang dilakukan oleh *host client* terhadap *host server*.

b. Arsitektur Sistem Ethereal

Dua puluh *user* dalam waktu yang relatif bersamaan dengan menggunakan *browser Internet Explorer* 6.0 mengakses alamat http://192.168.1.1 (*url server web*). Seluruh *user* dikondisikan tidak melakukan aktivitas lain selain mengakses alamat http://192.168.1.1. Paket data dan *bandwidth* jaringan yang berhasil direkam oleh *ethereal* terlihat pada gambar 10 dan Gambar 11. Terlihat pada gambar 10 di atas bahwa rata-rata *bandwidth* LAN yang terpakai sekitar 3 kbps.



Gambar 2.8 Struktur LAN Uji Coba Menggunakan Ethereal

Komputer *server web* yang menjalankan aplikasi terhubung secara *local area network* (LAN) dengan empat

puluh komputer *user* melalui *switch* 10/100 Mbps, seperti terlihat pada gambar 2.8. Setting IP (*Internet Protocol*) *Address* untuk komputer *server web* dalam pengujian ini adalah 192.168.1.1 atau http://lab.igm.ac.id, sedangkan halaman *web* default.htm yang nanti akan diakses oleh pengguna diletakkan pada direktori \explorer.

ANALISA *NESSUS* DAN *ETHEREAL*

Nessus merupakan salah satu *software* favorit yang digunakan untuk memproteksi *network* dari serangan *hacker*. Proteksi tambahan ini cukup memadai untuk menghindari serangan *hacker* pada umumnya.

Sebagai *software open source* untuk perlindungan gangguan yang lumayan populer dan tersedia gratis. *Nessus* hadir untuk melindungi jaringan-jaringan dengan cara mendeteksi dan mencegah gangguan. *Nessus* adalah sebuah program yang berfungsi sebagai *security scanner* yang akan mengaudit jaringan yang dituju lalu menentukan kelemahan-kelemahan dari jaringan yang dituju.

Nessus merupakan suatu software yang berfungsi sebagai vulnerability scanner dan sudah digunakan oleh 75,000 organisasi / perusahaan di seluruh dunia. Pengertian Vulnerability scanner disini adalah kemampuan dari software ini untuk melihat celah keamanan (security hole) pada suatu sistem baik yang terkait dengan sistem operasi maupun aplikasi yang terpasang pada suatu sistem.

Projek "Nessus" diawali oleh Renaud Deraison pada tahun 1998 dengan tujuan menyediakan software untuk melakukan pengecekan keamanan / security audit pada suatu sistem dimana software ini bersifat remote, free, powerful, up-to-date dan mudah untuk digunakan.

Lisensi :

1. Free. Update database terbaru akan diberikan 1 minggu setelah security hole terbaru ditemukan.
2. Komersil. Update database terbaru akan diberikan sesegera mungkin setelah security hole terbaru ditemukan. Adanya support untuk troubleshooting dari produk ini dan lain sebagainya.

Nessus dapat dijalankan pada sistem operasi :

1. Linux : Fedora FC4 & 5, Red Hat Enterprise 3 & 4, SuSE 9.3 & 10, Debian 3.1 (i386).
2. FreeBSD : FreeBSD 5 & 6 (i386).
3. Solaris : Solaris 9 & 10 (sparc).
4. Mac OS X : Mac OS X 10.4 (intel & ppc).
5. Windows : Windows 2000, XP and 2003 (32 bits).

Installasi

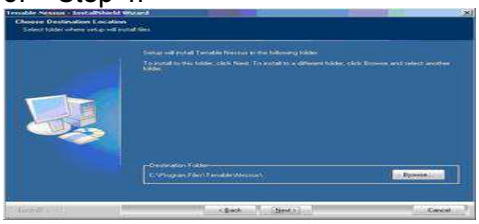
Instalasi software di tutorial ini dijalankan pada Microsoft Windows. Download software berikut: **Nessus** http://www.nessus.org/download/.

1. Double klik pada software yang di download.
2. Step 1.

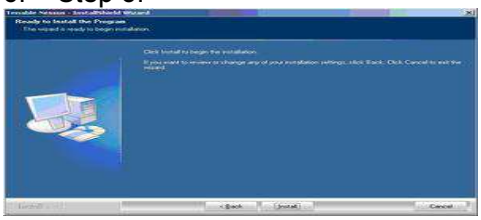
3. Step 2.

4. Step 3

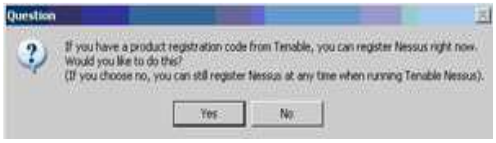
5. Step 4.



6. Step 5.

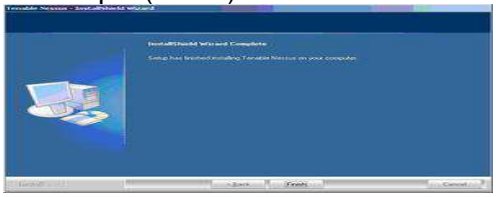


7. Step 6 (Registrasi software). Registrasi software ini dibutuhkan untuk update database Nessus. Dapat dilakukan sebelum atau sesudah instalasi software.



8. Step 7 (Instalasi Plugins).

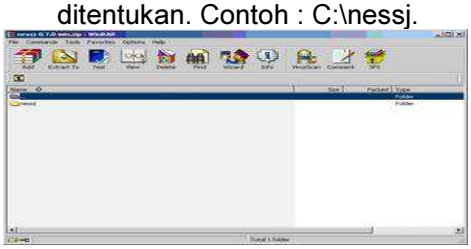
9. Step 8 (Finish).



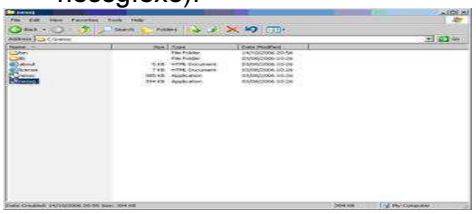
Nessus Client & Reporting

http://www.pss.intekras.com/tools/nessj/#download.

1. Unzip file nessj-0.7.0-win.zip ke folder / direktori yang telah ditentukan. Contoh : C:\nessj.



2. Hasil unzip : c:\nessj (perhatikan nessg.exe).



Pemakaian Nessus

Dalam melakukan scanning, Nessus dapat langsung dijalankan pada server / host yang telah terinstall software Nessus atau dapat pula scanning secara remote menggunakan Nessus Client. Pada Tutorial ini akan ditekankan kegiatan scanning secara remote ke Nessus Server. Sebelum menjalankan Nessus Server pastikan terlebih dahulu Nessus sudah di registrasi. Jalankan Product registration apabila belum dilakukan.

Start —> Programs —> Tenable Network Security —> Nessus —> Product Registration.

Masukkan code aktifasi apabila sudah mendaftar sebelumnya. Apabila ingin membuat code aktifasi, daftarkan ke http://www.nessus.org/register.

Langkah selanjutnya adalah membuat User yang akan digunakan untuk login ke Nessus Server secara remote menggunakan Nessus Client.

Start —> Programs —> Tenable Network Security —> Nessus —> User Management.

Membuat User Nessus.

User Nessus telah dibuat.

Menjalankan Nessus Server :

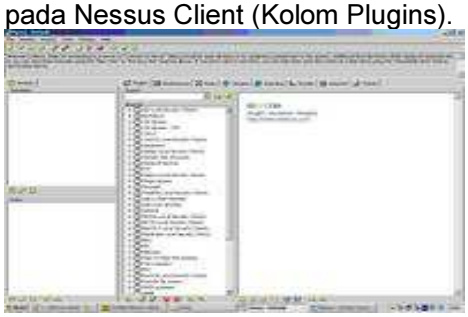
Start —> Programs —> Tenable Network Security —> Nessus —> Tenable Nessus.

Akses ke Nessus Server menggunakan Nessus Client (NESSG.EXE) :
Jalankan / double klik nessg.exe.

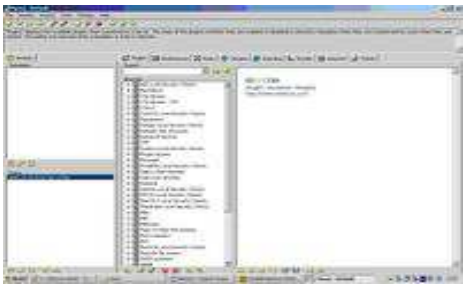
Protocol : *TLSv1*
Server : *Ip address dari Nessus Server*
Port : *Port dari Nessus Server (default 1241)*
User : *someuser*
Password : *somepassword*

Tampilan Nessus Client saat pertama kali running. Klik Ok untuk menerima key certificate.

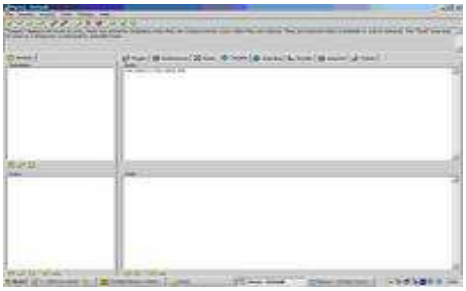
Tampilan Plugins yang terpasang pada Nessus Client (Kolom Plugins).



Agar Nessus Client dapat memberikan informasi yang dibutuhkan setelah melakukan scanning, maka plugins ini perlu diaktifkan sebelum proses scanning dilaksanakan.



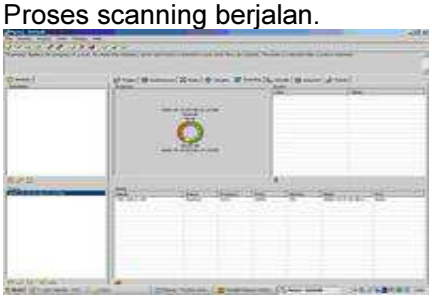
Proses scanning dilakukan dengan memasukkan ip address / range ip address dari target yang akan di scan (Kolom Targets). Contoh: sebuah virus dengan ip address 152.102.20.5



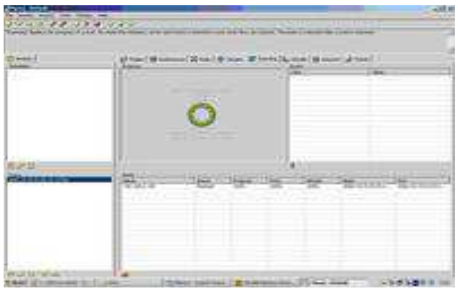
Setelah ip address / range ip address dimasukkan, lakukan proses scanning (Kolom Scanning).

Action —> *Start Scan* atau dengan kombinasi tombol *Ctrl* + *Shift* + *R*.

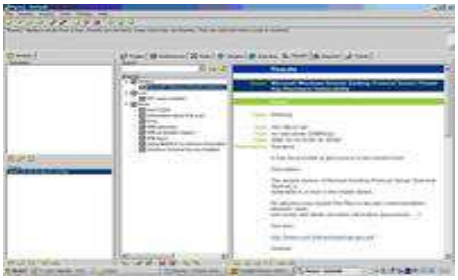
Proses scanning berjalan.



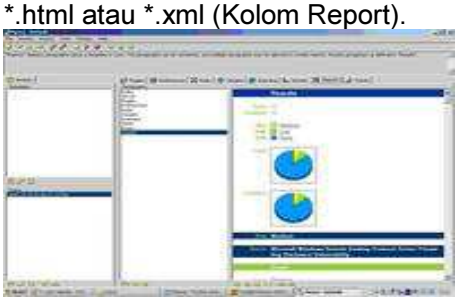
Proses scanning selesai.



Hasil scanning menggunakan Nessus Client (Kolom Result).Kolom disebelah kanan memberikan informasi detail mengenai security hole / lubang keamanan yang ditemukan dan langkah-langkah yang perlu dilakukan untuk menutup security hole tersebut. Hacker dapat memanfaatkan informasi dari Nessus ini untuk melakukan penyerangan ke sistem yang memiliki security hole.



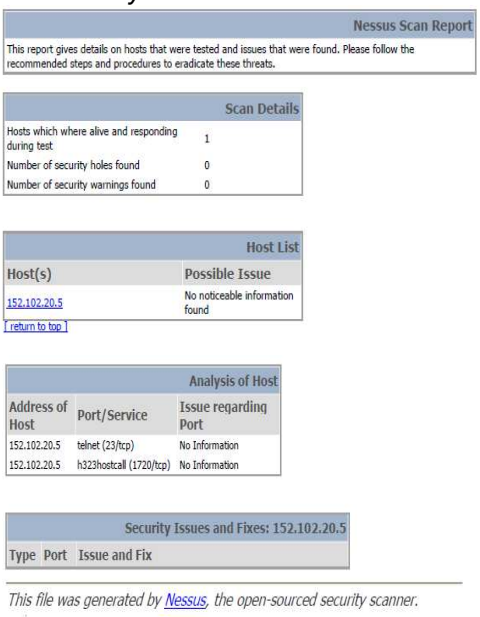
Hasil dari scanning dapat dibuat menjadi suatu report dan diexport ke *.html atau *.xml (Kolom Report).



Dengan menggunakan software Nessus, IT Security Officer dapat melakukan audit terhadap sistem yang mereka miliki dan memberikan gambaran mengenai langkah-langkah yang perlu dilakukan untuk mengamankan sistem mereka.

Hasil Analisa Pengujian Keamanan Nessus

Nessus adalah sebuah program yang berfungsi sebagai *security scanner,* pada bagian ini akan diperlihatkan hasil scan dari Nessus. Berikut ini adalah hasil scan dari host 152.102.20.5, dapat dilihat pada host ini tidak terdapat *vulnerability.*



Nessus Scan Report

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details

Hosts which where alive and responding during test	1
Number of security holes found	0
Number of security warnings found	0

Host List

Host(s)	Possible Issue
152.102.20.5	No noticeable information found

[return to top]

Analysis of Host

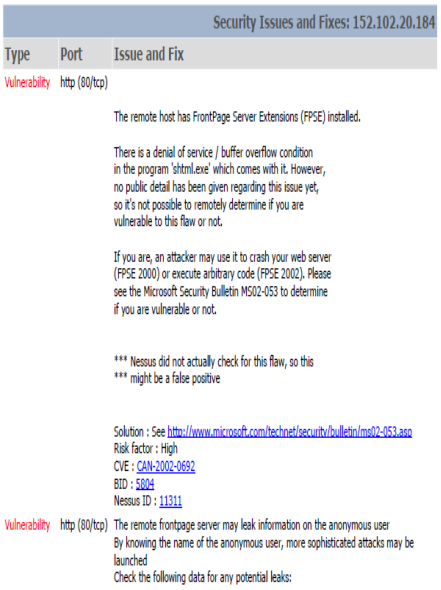
Address of Host	Port/Service	Issue regarding Port
152.102.20.5	telnet (23/tcp)	No Information
152.102.20.5	h323hostcall (1720/tcp)	No Information

Security Issues and Fixes: 152.102.20.5

Type	Port	Issue and Fix

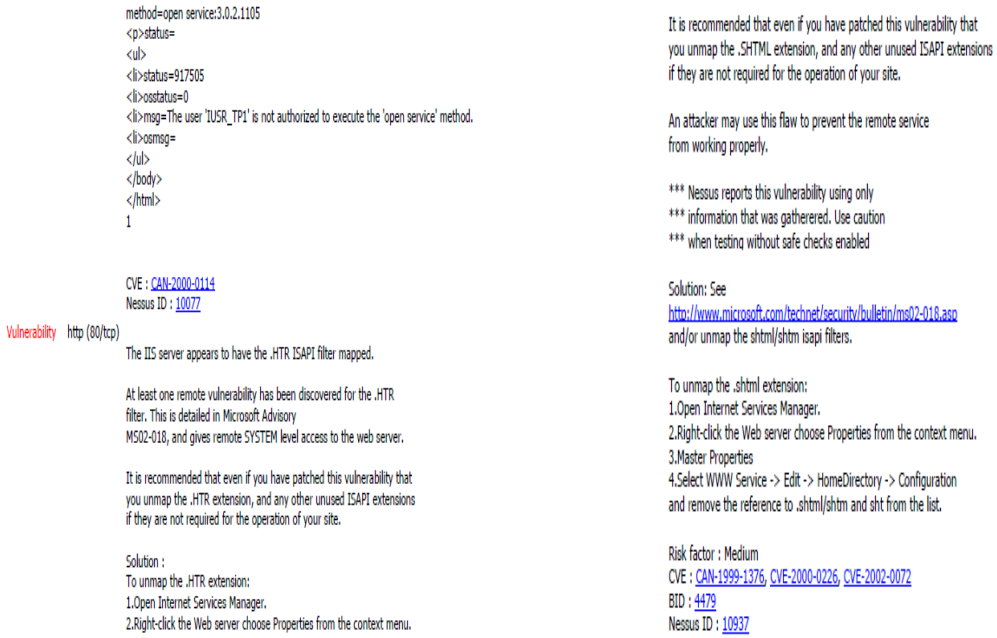
This file was generated by Nessus, the open-sourced security scanner.

Berikut ini akan diperlihatkan sebuah contoh dari host, yaitu host dengan IP 152.102.20.5, yang memiliki *vulnerabiliiy* pada port 80:



Security Issues and Fixes: 152.102.20.184

Type	Port	Issue and Fix
Vulnerability	http (80/tcp)	The remote host has FrontPage Server Extensions (FPSE) installed. There is a denial of service / buffer overflow condition in the program 'shtml.exe' which comes with it. However, no public detail has been given regarding this issue yet, so it's not possible to remotely determine if you are vulnerable to this flaw or not. If you are, an attacker may use it to crash your web server (FPSE 2000) or execute arbitrary code (FPSE 2002). Please see the Microsoft Security Bulletin MS02-053 to determine if you are vulnerable or not. *** Nessus did not actually check for this flaw, so this *** might be a false positive Solution : See http://www.microsoft.com/technet/security/bulletin/ms02-053.asp Risk factor : High CVE : CAN-2002-0692 BID : 5804 Nessus ID : 11311
Vulnerability	http (80/tcp)	The remote frontpage server may leak information on the anonymous user By knowing the name of the anonymous user, more sophisticated attacks may be launched Check the following data for any potential leaks:



method=open service:3.0.2.1105
<p>status=

status=917505
osstatus=0
msg=The user 'IUSR_TP1' is not authorized to execute the 'open service' method.
osmsg=

</body>
</html>
1

CVE : CAN-2000-0114
Nessus ID : 10077

Vulnerability http (80/tcp)

The IIS server appears to have the .HTR ISAPI filter mapped.

At least one remote vulnerability has been discovered for the .HTR filter. This is detailed in Microsoft Advisory MS02-018, and gives remote SYSTEM level access to the web server.

It is recommended that even if you have patched this vulnerability that you unmap the .HTR extension, and any other unused ISAPI extensions if they are not required for the operation of your site.

Solution :
To unmap the .HTR extension:
1.Open Internet Services Manager.
2.Right-click the Web server choose Properties from the context menu.
3.Master Properties
4.Select WWW Service -> Edit -> HomeDirectory -> Configuration and remove the reference to .htr from the list.

Risk factor : High
CVE : CVE-2002-0071
BID : 4474
Nessus ID : 10932

Vulnerability http (80/tcp)

The remote WebDAV server may be vulnerable to a buffer overflow when it receives a too long request.

An attacker may use this flaw to execute arbitrary code within the LocalSystem security context.

*** As safe checks are enabled, Nessus did not actually test for this
*** flaw, so this might be a false positive

Solution : See http://www.microsoft.com/technet/security/bulletin/ms03-007.asp
Risk Factor : High
CVE : CAN-2004-0109
BID : 7116
Nessus ID : 11412

Vulnerability http (80/tcp)

The IIS server appears to have the .SHTML ISAPI filter mapped.

At least one remote vulnerability has been discovered for the .SHTML filter. This is detailed in Microsoft Advisory MS02-018 and results in a denial of service access to the web server.

It is recommended that even if you have patched this vulnerability that you unmap the .SHTML extension, and any other unused ISAPI extensions if they are not required for the operation of your site.

An attacker may use this flaw to prevent the remote service from working properly.

*** Nessus reports this vulnerability using only
*** information that was gatherered. Use caution
*** when testing without safe checks enabled

Solution: See
http://www.microsoft.com/technet/security/bulletin/ms02-018.asp
and/or unmap the shtml/shtm isapi filters.

To unmap the .shtml extension:
1.Open Internet Services Manager.
2.Right-click the Web server choose Properties from the context menu.
3.Master Properties
4.Select WWW Service -> Edit -> HomeDirectory -> Configuration and remove the reference to .shtml/shtm and sht from the list.

Risk factor : Medium
CVE : CAN-1999-1376, CVE-2000-0226, CVE-2002-0072
BID : 4479
Nessus ID : 10937

Penjelasan dari hasil *report* mengenai *vulnerability* di atas akan diuraikan di bawah ini:

a. Host dengan IP152.102.20.5 memiliki *Front Page Server Extension (FPS)* yang terinstal di dalamnya, yang dapat menyebabkan *denial of service(DOS)/buffer overflow* di dalam program shtml.exe.
b. *Frontpage server* pada host dengan IP 152.102.20.5 sangat mungkin untuk membocorkan informasi pada *anonymous user*, yang dapat menyebabkan serangan yang membahayakan host.
c. *IIS server* pada host dengan IP 152.102.20.5 mempunyai .HTR ISAPI *filter mapped.* Sedikitnya ada sebuah *vulnerability* yang disebabkan oleh .HTR *filter*. Hal ini dapat diatasi dengan cara melakukan *unmap* pada *extension* pada HTR. *Server* ini juga mungkin mempunyai .SHTML ISAPI *filter mapped*. Sama seperti .HTR, sedikitnya ada sebuah *vulnerability* yang disebabkan oleh SHTML *filter.*

d. WebDAV *server* mungkin mempunyai *vulnerability* ketika menerima *request* yang terlalu panjang.

Instalasi *Ethereal*

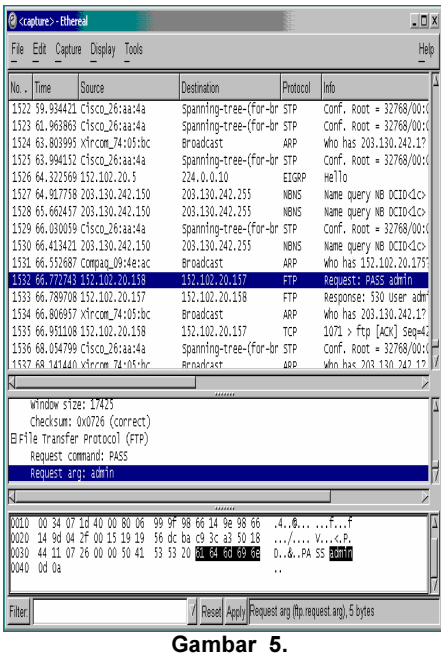
Ethereal adalah sebuah protokol analyzer jaringan yang free, yang berjalan pada sistem operasi Windows, Linux/Unix dan komputer Mac. Ethereal mampu menganalisa lebih dari 500 protokol.

Untuk instalasi Ethereal, Anda perlu memiliki akses ke komputer yang mendukung Ethereal dan packet capture library *libpcap*. Jika *libpcap* belum diinstal, Anda perlu meng-instalnya sebelum menggunakan Ethereal.

Donwload dan instal Ethereal dan (jika perlu) software *libpcap*. Jika perlu, download dan instal software *libpcap*. Pointer ke software *libpcap* disediakan dari halaman download Ethereal. Untuk mesin Windows, software libpcap dikenal sebagai *WinPCap* dan dapat ditemukana di http://winpcap.polito.it. Pergi ke http://www.ethereal.com dan download dan instal binary Ethereal untuk komputerAnda.

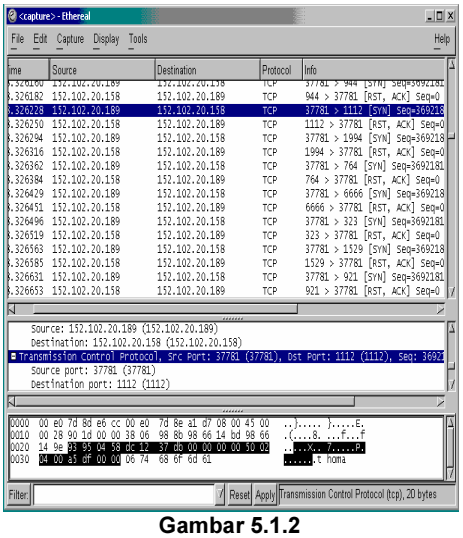
Hasil Analisa Pengujian Keamanan *Ethereal*

Seperti yang telah disebutkan di atas bahwa ethereal berfungsi untuk menangkap paket data langsung dari jaringan, dan juga memberikan informasi mengenai paket data yang ditangkap. Berikut ini akan diperlihatkan hasil *capture* dari ethereal.



Gambar 5.

Pada tampilan di atas dapat dilihat bahwa dengan menggunakan ethereal dapat diketahui password yang dalam contoh ini untuk mendapatkan akses mengadakan FTP *session* dengan 152.102.20.157. Dari contoh di bawah ini dapat dilihat bahwa host 152.102.20.189 sedang melakukan *scanning* terhadap host 152.102.20.158.19.2.



Gambar 5.1.2

Dari hasil-hasil *capture* di atas dapat terlihat bahwa output dari ethereal terbagi atas tiga bagian, yaitu:

1. Bagian pertama menampilkan keseluruhan paket data yang ditangkap oleh ethereal, bagian ini memberikan informasi mengenai waktu ditangkapnya paket data oleh ethereal setelah program ethereal dijalankan, asal paket data berasal, tujuan dari paket data, protokol yang dipergunakan, dan memberikan informasi paket data yang ditanglap secara umum.
2. Bagian kedua menampilkan informasi dari paket data secara lebih mendetail.
3. Bagian ketiga menampilkan nilai heksa dari paket data yang ditangkap.

KESIMPULAN

Nessus adalah sebuah program yang berfungsi sebagai *security scanner* yang akan mengaudit jaringan yang dituju lalu menentukan kelemahan-kelemahan dari jaringan yang dituju.

Nessus berjalan dengan mengambil sistem informasi dan menganalisanya untuk memeriksa sesuatu yang tidak biasa/lazim terhadap suatu *event* yang terjadi di*server*/jaringan. Ada beberapa cara bagaimana *nessus* bekerja. Cara yang paling populer adalah dengan menggunakan pendeteksi berbasis *signature* (seperti halnya yang dilakukan oleh beberapa anti virus), yang melibatkan pencocokan lalu lintas jaringan dengan basis data yang berisi cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang.

Teknik lain yang digunakan adalah dengan memantau berkas-berkas sistem operasi, yakni dengan cara melihat apakah ada percobaan untuk mengubah beberapa sistem operasi utama berkas *log*. Teknik ini sering diimplementasikan didalam *nessus*, selain tentunya melakukan pemindaian terhadap *log* sistem untuk memantau apakah terjadi kejadian yang tidak biasa

Kelebihan *nessus* yang menonjol adalah *plugin-based*, artinya *nessus* memiliki *plugin* (modul) yang digunakan untuk proses *scan* dan *plugin-plugin* ini dapat dibuat sendiri bagi yang ingin dengan menggunakan bahasa pemrograman C atau dengan NASL (*Nessus Scripting Language*). Selain dengan jalan membuat sendiri, *nessus* juga menyediakan *plugin online* yang secara rutin di*update* dan biasa *didownload* dengan aplikasi 'nessus-update-plugins' yang menyatu dengan *source* program *nessus*

Kelemahan *nessus* adalah apabila penyusup masuk ke jaringan, *nessus* tidak bisa mengaktifkan alarm secara otomatis sehingga *user* tidak mengetahui apabila ada penyusup masuk kejaringan internet.

Ethereal adalah sebuah *network protocol analyzer* yang dapat didapatkan secara gratis. *Ethereal* dapat berjalan pada sistem operasi *linux* dan *window*. *Ethereal* memberikan ringkasan dan informasi yang mendetail mengenai paket yang "ditangkap". Penganalisa dengan *ethereal* merupakan pendeteksi lalu lintas jaringan dengan men-*capture* paket dalam jaringan secara langsung dan menayangkan isi dari paket tersebut.

Kelebihan dari ethereal adalah data dapat langsung ditangkap dari koneksi jaringan secara langsung, e*thereal* dapat membaca *file-file* yang ditangkap oleh *tcpdump, NAI's Sniffer, Sniffer Pro, Sunsnoop, atmsnoop,* dan lain-lain, 393 *protocol* dapat dikenali oleh *ethereal*, dan o*utput* dapat disimpan atau diprint sebagai *plain text.*

Kelemahan dari ethereal adalah open source ini hanya sekedar memantau lalu lintas jaringan internet saja dan apabila penyusup masuk ethereal tidak bisa melakukan pemblokiran penyusup tersebut.

DAFTAR PUSTAKA

[1] A.S, Rosa dan M. Shalahuddin. 2013. "*Rekayasa Perangkat Lunak".* Informatika: Bandung.

[2] Haviluddin. 2011. *Memahami Penggunaan UML (Unified Modelling Language).* Jurnal Informatika Mulawarman Vol 6 No. 1

[3] Jakimi, A. dan Koutbi, M. 2009. "*An Object Oriented Approach to UML Scenarios Engineering and Code Generation*". International Journal of Computer Theory and Engineering, Vol. 1, No. 1,1793-8201.

[4] Kaur, A. 2012 *Application of UML in RealTime Embedded Systems.* International Journal of Software Engineering & Applications (IJSEA), Vol.3, No.2.

[5] Kyung, S. J. dan Jung, W. W. 2014. "*Development of Object-Oriented Analysis and Design Methodology for Secure Web Applications*". International Journal of Security and ItsApplications Vol.8, No.1

[6] Lee, S. 2012." *Unified Modeling Language (UML) for Database Systems and Computer Applications",* International Journal of Database Theory and Application Vol. 5, No. 1.

[7] Sathiyaraj, R., Yadav, N.S., Prabhakar, M. 2012. "Modeling Real Time Scheduler in OOAD Using UML", International Journal Of Research In Educational Methodology. Council For Innovative Research Vol.2, No.1 : ISSN:2278-7690