METODE PENGUJIAN KEAMANAN FILE SERVER SEBAGAI LANGKAH DALAM MENENTUKAN KEBIJAKAN KEAMANAN DI CV. BRAINESIA

Naskah Publikasi

diajukan oleh

Edi Dwidayanto

07.11.1421

kepada

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2011

NASKAH PUBLIKASI

METODE PENGUJIAN KEAMANAN FILE SERVER SEBAGAI LANGKAH DALAM MENENTUKAN KEBIJAKAN KEAMANAN DI CV. BRAINESIA

disusun oleh

Edi Dwidayanto
07.11.1421

Dosen Pembimbing

Sudarmawan, S.T, M.T.
NIK. 190302035

Tanggal, 23 November 2011

Ketua Jurusan
Teknik Informatika

Sudarmawan, S.T, M.T.
NIK. 190302035

File Server Security Testing Methods
As A Step On Determining
The Security Policy
In CV. Brainesia

Metode Pengujian Keamanan File Server
Sebagai Langkah Dalam Menentukan
Kebijakan Keamanan
di CV. Brainesia

Edi Dwidayanto
Jurusan Teknik Informatika
STMIK AMIKOM YOGYAKARTA

ABSTARCT

The development of technology that is currently growing rapidly enable the development of software and hardware in a short time. The ability of a computer system can be measured through three reviews of brainware, software, and hardware. Without the alignment between those three things then the computer system can not be said to work optimally. Security is one important factor in a company. Without the guarantee of security will arise concerns the existence of wiretapping or theft of important company data. Security rights of access to information is of major concern to the CV. Brainesia.

Security method that should be done in accordance with the needs and without prejudice to the functions of the system. The solution offered is the testing process of implementing network security and begining from wireless security risks that may occurs. Testing continues on a server computer device. Testing is done by finding detile information such as ip address, open ports, services that are being worked, and the type of operating system is used. Based on the information obtained, the test continued with the search for security holes and exploits experimental system.

The results of the process undertaken is expected to assist CV. Brainesia know the vulnerabilities that are owned and prevention of violations of corporate data access. Existing network devices can also be configured better, so its performance can be improved and reliable.

Keywords*: security, permissions, information, patching, file servers*

1. Pendahuluan

Keamanan data merupakan salah satu masalah terbesar yang dihadapi oleh dunia usaha, penyedia jasa layanan internet dan pihak pengatur kebijakan serta penegak konsekuensi pelanggaran. Berkembangnya teknologi yang memudahkan manusia dalam melakukan akses terhadap suatu komputer *standalone* maupun jaringan komputer mengharuskan pihak pengelola suatu lembaga mampu untuk menentukan bagaimana kebijakan yang ditetapkan dan mampu memperkirakan tantangan yang akan dihadapi.

Keamanan merupakan sebuah proses yang berkelanjutan, dan bukan merupakan sebuah produk jadi sehingga penting artinya untuk melakukan pengujian terhadap kebijakan keamanan yang diambil guna meningkatkan keamanan perusahaan.

2. Landasan Teori

2.1 Konsep Dasar Jaringan Komputer

Jaringan komputer merupakan kelompok komputer dan perangkat terkait yang dihubungkan serta mampu berkomunikasi, berbagi file dan sumberdaya lain antar pengguna. Sebuah jaringan dapat terdiri dari jaringan *peer-to-peer*, perkantoran, departemen, dan LAN yang terhubung dengan banyak pengguna melalui kabel yang terinstal maupun dial-up. MAN dan WAN sebagai jaringan yang terhubung dalam wilayah geografis yang lebih luas.

2.1.1 Tipe Serangan

Serangan dapat didefinisikan sebagai penyerangan terhadap keamanan sistem oleh ancaman berkecerdasan atau aksi dengan metode dan teknik tertentu guna mengecoh sistem keamanan dan melanggar kebijakan keamanan sistem. Serangan yang terjadi secara garis besar dapat dikategorikan menjadi dua[1] :

1. *Active attacks*

   Serangan jenis ini merupakan serangan dengan metode penyerangan secara langsung pada target komputer, pada umumnya berupa serangan terhadap ketersediaan dan layanan komputer server sehingga dapat berdampak pada integritas dan keaslian informasi pada sistem.

2. *Passive attacks*

   Serangan jenis ini dilancarkan dengan tanpa mengganggu kondisi sistem. Metode yang dilakukan adalah dengan memantau lalu lintas paket data

[1] International Council of Electronic Commerce Consultants, Ethical Hacking (EC-Coucil Exam 312-50):Student Courseware.2004

yang ada kemudian dilakukan analisis berdasarkan frekwensi lalu lintas paket data tersebut.

Ditinjau dari sisi organisasi, serangan dapat juga dikategorikan menjadi dua, yaitu serangan dari pihak luar dan serangan dari pihak dalam.

1. Serangan dari pihak luar adalah serangan yang berasal dari luar organisasi, pihak yang tidak memiliki hak akses mencoba untuk melanggar kebijakan keamanan.
2. Serangan dari pihak dalam merupakan serangan yang dilancarkan oleh pihak dalam organisasi yaitu orang yang memiliki wewenang atau hak akses namun disalahgunakan atau seseorang yang mencoba menaikkan tingkat hak aksesnya.

2.1.2 Metode Pengamanan

Metode pengamanan yang dapat digunakan untuk mengamankan sebuah sistem sangat beragam, setiap organisasi memiliki cara dan metode masing-masing, namun secara garis besar, metode pengamanan yang dilakukan dapat dikategorikan sebagai berikut :

2.1.2.1 Authentikasi

Metode autentikasi paling umum digunakan adalah penggunaan *username* dan *password*. Pengguna dengan *username* dan *password* yang tepat akan terautentikasi dan dapat mengakses layanan. Jenis penggunaan metode ini ada bermacam, berikut ini ragam metode tersebut:

1. Tidak ada *username* / *password*
2. Statis *username* / *password*
3. *Expired username* / *password*
4. *One-Time Password* (OTP)

Metode autentikasi juga tergantung pada kualitas *password* yang digunakan. Penggunaan *password* yang baik minimal memiliki kriteria sebagai berikut :

1. *Username* dan *password* yang digunakan bukan berasal dari kata yang terdapat pada kamus bahasa.
2. *Username* dan *password* tidak terkait dengan pengguna seperti tanggal lahir atau alamat dan tidak menggunakan istilah-istilah umum yang sering dipakai.

3. *Username* dan *password* merupakan *password* yang kuat, yaitu memiliki kombinasi huruf kapital, angka, dan karakter. Panjang *password* yang dipakai minimal 8 karakter.

2.1.2.2 Enkripsi

Enkripsi merupakan proses merubah informasi dari bentuk yang dapat dimengerti menjadi bentuk yang tidak dapat dimengerti. Penerima informasi yang telah dienkripsi harus melakukan proses dekripsi atau membalikkan proses enkripsi agar pesan yang diterima dapat dimengerti.

Pesan yang akan dienkripsi dikenal dengan sebutan *plaintext* yang ditransformasikan berdasarkan sebuah kunci (*key*). Hasil dari proses enkripsi dikenal dengan *chipertext* yang kemudian ditransmisikan dari *sender* menuju *receiver*. Jika pada transmisinya pesan tersebut diambil oleh orang yang tidak berhak (*enemy*) maka *chipertext* tersebut tidak bisa secara langsung dimengerti, sehingga perlu mencari kunci sandi agar dapat diubah menjadi pesan yang dapat dimengerti. Ilmu untuk melakukan dekripsi *chipertext* disebut *cryptanalysis* dan ilmu yang mempelajari kriptografi disebut dengan *cryptology*.

2.1.2.3 Firewall

Fungsi utama dari firewall adalah untuk memusatkan akses control antara jaringan terpercaya dan jaringan tidak terpercaya. Firewall memiliki fungsi keamanan berikut[2] :

1. Melakukan pemblokiran terhadap lalulintas jaringan yang tidak diinginkan.
2. Mengarahkan lalulintas yang masuk pada sistem internal yang lebih dapat dipercaya.
3. Menyembunyikan sistem yang rentan, yang tidak mudah diamankan dari internet.
4. Membuat log lalulintas dari dan menuju jaringan pribadi.
5. Dapat memberikan sistem autentikasi yang kuat.

2.1.2.4 *Vulnerability Patching*

Melakukan penutupan lubang keamanan yang ditemukan guna mengurangi risiko kehilangan atau kerusakan sistem. Metode yang dilakukan diantaranya :

[2] S.K.Parmar, Cst, An Introduction to Security, hal. 130.

1. *Update* perangkat lunak

   Sistem operasi atau program aplikasi yang memiliki celah keamanan diperbaharui sehingga program aplikasi tersebut bebas dari celah keamanan yang telah diketahui.

2. Perangkat lunak keamanan

   Melakukan installasi perangkat lunak penunjang keamanan guna meningkatkan keamanan, dapat berupa perangkat keamanan host based maupun network based untuk mencegah atau memantau sistem yang bekerja.

2.2 Konsep Dasar Keamanan Informasi

2.2.1 Elemen Keamanan

Keamanan merupakan kondisi dimana informasi dan infrastruktur berada dalam kondisi baik, tidak terdeteksi adanya pencurian data dan tidak ada gangguan terhadap layanan informasi atau berada pada tingkat yang dapat ditoleransi. Elemen yang terkait dalam penerapan keamanan adalah :

1. Kerahasiaan

   Mampu menjaga kerahasiaan isi dan sumber informasi dari pihak yang tidak berhak.

2. Keaslian

   Informasi yang diberikan merupakan informasi yang terjamin keasliannya dan tidak mengalami perubahan dari sumber informasi.

3. Integritas

   Data dan informasi terjaga akurasi dan kelengkapannya.

4. Ketersediaan

   Menjamin bahwa informasi dapat diakses dan digunakan oleh pihak yang berwenang ketika dibutuhkan.

2.2.2 Standar Keamanan Informasi

Standar keamanan informasi diperlukan sebagai acuan mekanisme kebijakan yang akan dibuat, hal ini penting karena dengan mengikuti standar organisasi memiliki jaminan bahwa apa yang diputuskan telah memenuhi kriteria yang diakui.

Contoh organisasi yang mengeluarkan standar dalam kegiatan keamanan informasi adalah[3] :

[3] ESCAP/APCICT, Modul 6 Keamanan Jaringan dan Keamanan Informasi dan Privasi, hal. 24

1. ISO (International Standards Organisation)
   Fokus utama yang diambil pada standarisasi ini adalah keamanan administratif organisasi.
2. CISA (Certified Information System Auditor)
   Fokus utama pada standar ini adalah pada kegiatan audit dan pengendalian sistem informasi.
3. CISSP (Certified Information System Security Profesional)
   Fokus utama dari standar ini adalah pada keamanan teknis.

2.3 Kebijakan Keamanan

Kebijakan keamanan merupakan dokumen pokok yang menjelaskan detil jenis kegiatan yang diijinkan dan masih dalam batasan akses serta bentuk konsekuensi terhadap pelanggaran.

2.3.1 Penerapan Kebijakan Keamanan

Keputusan yang diambil seorang administrator dalam mengelola jaringan mencerminkan tingkat keamanan, fungsionalitas, dan kemudahan yang ditawarkan pada jaringan tersebut. Keputusan yang baik mengenai keamanan perlu untuk merujuk pada tujuan utama dari penerapan kebijakan tersebut. Sebagai contoh adalah pemilihan produk dari vendor, administrator perlu mempertimbangkan fitur yang ditawarkan dengan level keamanan yang telah diputuskan. Pertimbangan penerapan keputusan kebijakan keamanan tersebut harus mempertimbangkan aspek berikut[4] :

1. Layanan dibandingkan dengan keamanan
2. Kemudahan dibandingkan dengan keamanan
3. Biaya penerapan keamanan dibandingkan dengan risiko kehilangan

2.3.2 Tujuan Penerapan Kebijakan Keamanan

Kebijakan merupakan bagian dari perumusan standar panduan dalam kegiatan organisasi, pengaturan hak akses, mekanisme pelayanan jasa, dan respon terhadap adanya ancaman. Tujuan utama kebijakan keamanan adalah[5] :

1. Sebagai panduan pengelolaan pihak manajemen dan administrasi keamanan jaringan.
2. Melindungi sistem komputer perusahaan.
3. Memastikan integritas pelanggan dan mencegah akses yang tidak berhak.

[4] S.K.Parmar, Cst, An Introduction to Security, hal. 16.
[5] EC-Coucil, CEHv6 Module 49 Creating Security Policies, hal. 7.

4. Mengurangi risiko yang disebabkan oleh penggunaan secara ilegal sumberdaya sistem, kehilangan data penting dan kepemilikan serta untuk membedakan tingkatan hak akses pengguna.

2.3.3 Acuan Kebijakan Keamanan yang Baik

Kebijakan keamanan agar dapat dikatakan baik dan mampu dijadikan acuan solusi keamanan sistem harus memenuhi kriteria minimal berikut[6] :

1. Harus diimplementasikan pada administrasi sistem sebagai bagian dari prosedur, dipublikasikan sebagai sebagai panduan yang diterima atau dengan metode lain.
2. Harus ditegakkan dengan dukungan alat keamanan dan sanksi saat pencegahan secara teknis tidak dapat dilaksanakan.
3. Harus secara jelas didefinisikan tanggung jawab pengguna, administrator, dan pihak manajemen.

3. Metode Penelitian

3.1 Sejarah CV. Brainesia

CV. Brainesia merupakan perseroan komanditer yang bergerak pada pelayanan jasa hosting dan domain. Perusahaan ini didirikan pada 27 April 2011 dan beralamat di Baturan, RT 002/RW 019, Trihanggo, Gamping, Sleman, Yogyakarta.

Jenis usaha utama yang dijalankan adalah jasa hosting, domain dan pembuatan website. CV. Brainesia mencoba mengembangkan usaha dan membuat jaringan lokal LAN dan WLAN yang terkoneksi dengan file server yang berfungsi sebagai pusat data dan media pencetakan dokumen.

Tergolong sebagai perusahaan baru, maka CV. Brainesia membutuhkan perencanaan infrastruktur yang matang agar dalam masa pengembangannya dapat berjalan sesuai dengan perencanaan dan dapat mengurangi pemborosan yang mungkin terjadi saat penerapan infrastruktur. Faktor keamanan data perusahaan juga merupakan salah satu kata kunci yang harus diperhatikan, hal ini mengingat data server perusahaan terkoneksi pada jaringan komputer.

3.2 Identifikasi Masalah

Identifikasi permasalahan merupakan tahap awal dalam proses penentuan solusi yang tepat terhadap masalah yang dihadapi. Masalah yang dihadapi perlu ditindaklanjuti agar dapat ditemukan solusi ataupun alternatif solusi agar sistem yang dibangun dapat

[6] S.K.Parmar, Cst, An Introduction to Security, hal. 18.

berjalan sesuai dengan apa yang diharapkan dan tujuan dari penerapan teknologi dapat terlaksana.

Mempertimbangkan permasalahan-permasalahan yang ada maka dapat ditarik kesimpulan bahwa permasalahan yang dihadapi adalah CV. Brainesia memerlukan kepastian dan jaminan keamanan data perusahaan tidak diakses oleh pihak yang tidak berhak dan tetap memiliki fungsionabilitas perangkat pada jaringan lokal LAN dan WLAN.

3.3 Dugaan Penyelesaian Masalah

Memperhatikan uraian permasalahan diatas CV. Brainesia membutuhkan jaminan keamanan data perusahaan dan fungsionabilitas perangkat, maka dapat diusulkan solusi berupa pengujian keamanan baik pada komputer server, jaringan LAN dan jaringan WLAN kemudian merumuskan usulan kebijakan keamanan jaringan yang baru. Pengujian dilakukan dengan memfungsikan fitur-fitur keamanan yang dapat diaplikasikan pada infrastruktur yang dibangun kemudian dilakukan pengujian kelemahan yang mungkin terjadi pada fitur yang diaplikasikan, informasi yang didapat kemudian dilakukan analisis dan disimpulkan dalam bentuk usulan kebijakan perusahaan.

3.4 Alat dan Bahan Penelitian

3.4.1 Perangkat Keras

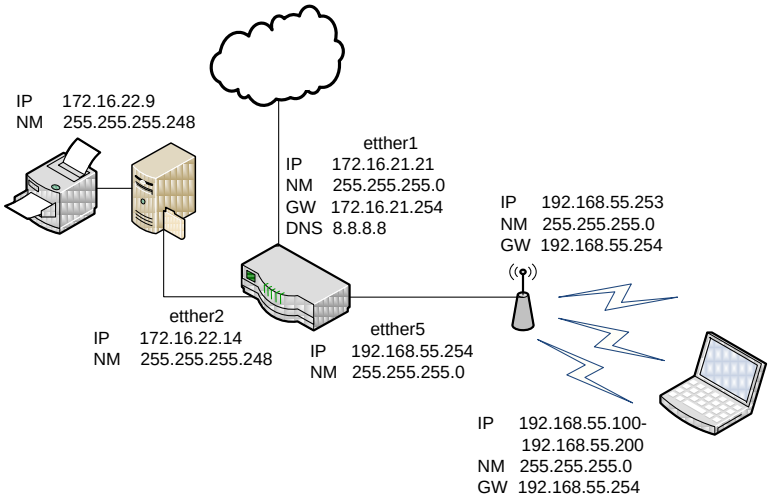
Perangkat keras yang digunakan dalam penelitian ini adalah sebagai berikut :

1. *Wireless Card* (Alfa AWUS036NH)
2. *Access Point* (Linksys WAG120N)
3. Router (Mikrotik RouterBoard 450G)
4. Komputer Server (Komputer Desktop)
5. Komputer *Tester* (Dell Studio XPS 1340)
6. Komputer *Client* (Acer Aspire 4920G)
7. Kabel UTP (CAT-6)

3.4.2 Perangkat Lunak

1. Mikrotik Router OS 4.14 Lisensi 5
2. Microsoft Windows Server 2003
3. Perangkat Antivirus Clamav
4. Backtrack Linux 5

3.5 Rancangan Topologi Jaringan



Gambar 3. 1 Topologi Jaringan

3.6 Metode Pengujian

Pengujian dilakukan untuk mengetahui masing-masing kemungkinan kelemahan pada komponen sistem yang diteliti. Metode pengujian dipakai adalah *Graybox testing*[7], dikenal juga dengan internal testing yaitu pengujian dengan asumsi serangan datang dari lingkungan network lokal. Pertimbangan akan kelebihan dan kekurangan dari komponen keamanan system, digunakan sebagai dasar penyusunan usulan kebijakan keamanan. Proses pengujian yang dilakukan adalah sebagai berikut :

1. Memastikan koneksi *client* dengan *access point*, DHCP, NAT, *File Sharing* dan *Printer Sharing* dapat bekerja dengan baik.
2. Bagian terlemah pada sistem ini adalah media *wireless* sehingga langkah pengujian keamanan dilakukan pada media *wireless* terlebih dahulu. Pengujian dilakukan dengan mode keamanan Hidden SSID, MAC Filter, WEP, dan WPA/WPA2.
3. Pengujian keamanan kedua dilakukan dengan *network mapping* dan mencari detil informasi komputer server. Informasi yang dicari berupa IP *address*, port terbuka, jenis service yang sedang berjalan, dan sistem operasi.
4. Melakukan pencarian jenis-jenis *vulnerability* yang dimungkinkan sesuai dengan informasi yang didapat dari komputer server.
5. Berdasarkan informasi yang telah dikumpulkan kemudian melakukan percobaan *exploitasi* celah keamanan yang didapatkan.

[7] EC-Coucil, CEHv6 Module 01 Introduction to Ethical Hacking, hal. 62.

4. Implementasi Dan Pembahasan

4.1 Pengujian Infrastruktur

Pengujian infrastruktur dilakukan guna memastikan sistem yang dikonfigurasi dapat bekerja sesuai dengan yang diharapkan. Pengujian bertahap dilakukan mulai koneksi *client* dengan *access point*, uji koneksi jaringan, dan uji *file sharing* dan *printer sharing*. Uji koneksi antara *client wireless* dengan *access point* dilakukan dengan mengaktifkan fitur-fitur keamanan yang diuji. Uji koneksi jaringan dilakukan dengan pengiriman paket ICMP *(Internet Control Message Protokol*) menggunakan program Ping kemudian dilakukan uji jalur paket data dengan program Traceroute. Uji *file sharing* dan *printer sharing* dilakukan dengan cara *client* mengakses layanan tersebut dari jaringan *wireless*.

4.2 Uji Keamanan

Pengujian keamanan dilakukan dua tahap, tahap pertama pada keamanan jaringan *wireless*, tahap kedua pada keamanan file server. Perangkat lunak yang digunakan merupakan perangkat lunak pilihan berdasarkan survey yang dilakukan oleh website http://sectools.org/ dan http://tools.securitytube.net/. Pengujian keamanan pada WLAN dilakukan dengan penerapan tingkat keamanan secara bertahap, mulai dari Hidden SSID, MAC Filter, WEP, dan WPA/WPA2. Pengujian keamanan file server dilakukan dengan tiga tahap yaitu *network mapping* (pemetaan jaringan), *vulnerability scanning* (mencari kelemahan sistem) dan penetration testing (percobaan penetrasi dan *exploitasi* sistem).

4.2.1 Keamanan Wireless Lan

Perbandingan penerapan metode keamanan jaringan wireless sesuai dengan hasil pengujian diatas adalah sebagai berikut :

1. Keamanan Hidden SSID dan MAC Filter

Tabel 4. 1 Perbandingan Perangkat Uji Keamanan Hidden SSID

Perangkat Uji	User Interface	Deteksi SSID	Deteksi MAC Address	Deteksi IP Address
airodump-ng	CLI	Ya	Ya	Tidak
Kismet	CLI	Ya	Ya	Ya
ssidsniff	CLI	Tidak	Ya	Tidak
Wireshark	GUI	Ya	Ya	Tidak

2. Keamanan WEP

Tabel 4. 2 Perbandingan Perangkat Uji Keamanan WEP

Perangkat Uji	User Interface	Key Recovery
aircrack-ng	CLI	Ya
Gerix wifi cracker	GUI	Ya

3. Keamanan WPA/WPA2

a. WPA

Tabel 4. 3 Perbandingan Perangkat Uji Keamanan WPA

Perangkat Uji	User Interface	Key Recovery	Waktu Key Recovery (10 x Uji)
aircrack-ng	CLI	Ya	2,59 menit
Cowpatty	CLI	Tidak	-
Gerix wifi cracker	GUI	Ya	2,59 menit
Pyrit	CLI	Ya	2,55 menit

b. WPA2

Tabel 4. 4 Perbandingan Perangkat Uji Keamanan WPA2

Perangkat Uji	User Interface	Key Recovery	Waktu Key Recovery (10 x Uji)
aircrack-ng	CLI	Ya	2,58 menit
Cowpatty	CLI	Ya	4 menit
Gerix wifi cracker	GUI	Ya	2,59 menit
Pyrit	CLI	Ya	2,53 menit

4.2.2 Keamanan File Server

Proses pengujian keamanan file server dilakukan dalam tiga tahap. Tahap pertama adalah melakukan pencarian informasi mengenai perangkat yang terkoneksi pada jaringan, kemudian mencari informasi detil perangkat yang terkoneksi. Informasi yang didapat, digunakan sebagai dasar untuk melakukan pencarian celah keamanan dan dengan mendapatkan daftar celah keamanan yang mungkin ada kemudian dilakukan pembuktian dengan melakukan percobaan *penetration testing* pada komputer server.

Pengujian ini dilakukan guna mengetahui langkah-langkah yang dapat dilakukan dan akibat yang mungkin terjadi jika sistem yang ada memiliki celah keamanan.

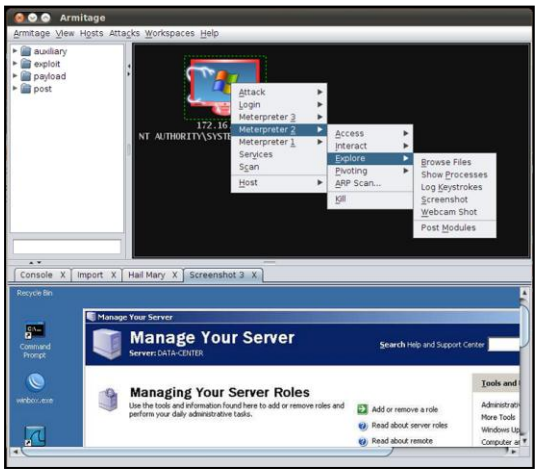
Hasil scanning Nmap terlihat perangkat dengan IP *address* 172.16.22.9 merupakan komputer Windows dengan kemungkinan Windows 2000/XP/2003 sedangkan IP address 192.168.55.253 merupakan perangkat Cisco Linksys yang dideteksi sebagai distribusi Linux, dan pada IP address 192.168.55.254 merupakan perangkat Routerboard yang dideteksi sebagai distribusi Linux.

4.2.2.1 *Vulnerability Scanning*

Proses *vulnerability scanning* dapat dilakukan dengan bermacam-macam cara diantaranya dengan mencari exploit secara manual dari informasi yang sudah didapat dan dapat pula dengan melakukan *vulnerability scanning* menggunakan perangkat lunak khusus untuk melakukan tugas tersebut. Pada pengujian ini dilakukan dengan menggunakan perangkat lunak Nessus. Hasil scanning Nessus menunjukkan bahwa pada komputer file server terdapat total anacaman keamanan sejumlah 49, dengan rincian prioritas high 9, medium 1, Low 25 dan open port sejumlah 14. Risiko tertinggi yaitu high ada pada CIFS port 445 yang merupakan port Microsoft NetBIOS *service*.

4.2.2.2 *Penetration Testing*

Terdapat banyak perangkat lunak yang dapat digunakan untuk melakukan proses *penetration testing* baik yang berbayar maupun tidak. Pada pengujian ini digunakan perangkat lunak Armitage yang merupakan salah satu metode untuk berinteraksi dengan metasploit framework.



Gambar 4. 1 Hasil Screenshoot Desktop Server

Adanya proses eksploitasi sistem yang berhasil tentunya dapat berdampak buruk pada perusahaan jika sistem tersebut sudah bekerja. Terlihat pada gambar 4. 1 Armitage berhasil mendapatkan screenshoot dari komputer server. Risiko yang lebih berat adalah penyerang dapat mengirim atau mendownload file pada komputer server, berinteraksi dengan remote desktop VNC, mengambil gambar webcam jika terpasang perangkat webcam, mematikan proses, dan merekam *keystroke* pada keyboard.

5. Penutup

5.1 Kesimpulan

Kesimpulan yang dapat diambil dari penulisan laporan skripsi ini antara lain sebagai berikut :

1. Langkah metode pengujian keamanan file server yang terhubung dengan perangkat wireless adalah dimulai dengan pengujian fitur keamanan perangkat wireless, pemetaan perangkat komputer yang terkoneksi, deteksi port dan service yang bekerja, deteksi kelemahan sistem, dan percobaan *exploitasi* kelemahan sistem.
2. Perangkat lunak yang efektif untuk digunakan adalah Kismet, airodump-ng, Pyrit, Nmap, Nessus, dan Armitage.
3. Fitur – fitur keamanan yang diterapkan tetap memiliki celah keamanan yang dapat ditemukan dikemudian hari, sehingga perlu adanya kombinasi penggunaan fitur keamanan guna meningkatkan kualitas keamanan sistem.
4. Keamanan merupakan proses yang berkelanjutan dan bukan merupakan produk jadi, dengan demikian penerapan usulan kebijakan keamanan pada CV. Brainesia bersifat dinamis dan menyesuaikan dengan perkembangan teknologi dan informasi.

5.2 Saran

Saran yang dapat diberikan dengan adanya penulisan laporan skripsi ini antara lain sebagai berikut :

1. Perlu adanya usaha membudayakan "*security aware*" guna mencegah tindakan-tindakan merugikan yang mungkin terjadi.
2. Perlu adanya penelitian lebih lanjut mengenai pencegahan serangan deauthentikasi pada perangkat *wireless* serta penelitian mengenai pengaturan seberapa jauh sinyal wireless dapat dipancarkan yang mungkin dapat diterapkan sebagai alternatif pengamanan.

3. Perlu adanya penelitian lanjut mengenai langkah-langkah pengujian keamanan jaringan yang mungkin dapat lebih dieksplorasi kembali, misalnya pengujian keamanan WPA pada jaringan wireless tanpa ada client sah yang terkoneksi.
4. Perlu adanya penelitian lebih lanjut mengenai *vulnerability research* pada sistem operasi maupun program aplikasi guna mengetahui kemungkinan adanya celah keamanan baru sehingga dapat dilakukan usaha pencegahan.

Daftar Pustaka

Antoniewicz, Brad.Whitepaper:802.11 Attacks.Foundstone Professional Service

Edney, Jon and A.Arbaugh, William.2003.Real 802.11 Security: Wi-Fi Protected Access and 802.11i,Addison Wesley,Boston,MA

ESCAP/APCICT.2009.Modul 6 Keamanan Jaringan dan Keamanan Informasi dan Privasi

E. Canavan, John.2001.Fundamentals of Network Security,Artech House,London

International Council of Electronic Commerce Consultants.2004.Ethical Hacking (EC-Coucil Exam 312-50):Student Courseware,OSB Publisher,New York

Liska, Allan.2002.The Practice of Network Security: Deployment Stategies for Production Environments,Prentice Hall PTR

Manzuik, Steve Pfeil, Ken Gold,Andre.2007.Network Security Assessment.Syngress Publishing, Inc, Rockland, MA

Michael Halvorsen, Finn and Haugen, Olav.2009.Cryptanalysis of IEE 802.11i TKIP.Norwegian University of Sience and Technology

Microsoft Corporation with Andy Ruth and Kurt Hudson.2003.Security+ Certification, Microsoft Press, Washington

S.K.Parmar, CSt.An Introduction to Security,Duncan, BC

http://www.securitytube.net/groups?operation=view&groupId=8

http://www.securitytube.net/groups?operation=view&groupId=9