

ABSTRAK

Dalam perkembangan komputer, banyak sekali lubang-lubang keamanan yang selama ini dianggap remeh oleh banyak pihak. Dalam perusahaan-perusahaan besar keamanan jaringan merupakan aset yang sangat berharga, karena rahasia perusahaan terjaga dengan aman didalamnya.

Proyek ini akan membahas tentang pembuatan *IDS Server* yang dilengkapi dengan *web*. *Web* ini berguna untuk mengatur *server* tersebut secara keseluruhan. Keamanan jaringan tingkat tinggi yang ditawarkan oleh *snort*, *Barnyard*, serta *BASE* menjadi pasangan yang sempurna dalam pengamanan jaringan. *Snort* sebagai pendeteksi penyerang, *Barnyard* mempunyai kemampuan *logging* dengan cepat, serta *BASE* sebagai penampil hasil *logging* tersebut dalam bentuk *web Based*.

Sebuah *PC* dengan 2 *NIC (Network Interface Card)*, dan *software-software* yang *open source* digunakan untuk menekan harga seminim mungkin untuk membuat sebuah *firewall* dan sebuah *server* pelacak *intrusion* yang efisien dan *powerfull*. *Server* ini dilengkapi juga dengan aplikasi *web* yang dibuat dengan bahasa pemrograman *web PHP* yang akan membantu dalam mengendalikan *server*.

ABSTRACT

During IT world progress, many security holes has been ignored by many company. In big enterprises, network security is a valuable asset, because company secret is safe in it.

This project will be discuss about the making of IDS Server who have web added on it. This web is using for take full control server from far. High level network security which over by snort, Barnyard, and BASE will be best partner in network security. Snort as intruder detection, Barnyard who has ability of fast logging, and BASE as show the result of that logging in web Based display.

A PC with 2 NIC (Network Interface Card), and open source softwares is used to minimize budget to built powerfull and efficient firewall and Intrusion detection system server. This server is equip by web application which made by PHP web language which will help the controlling of the server.

DAFTAR ISI

LEMBAR PENGESAHAN TUGAS AKHIR.....	i
LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS.....	ii
SURAT PERNYATAAN ORISINALITAS KARYA	iii
KATA PENGANTAR.....	iv
ABSTRAK.....	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL	xii
BAB I. PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	2
1.3. Tujuan	3
1.4. Batasan Masalah.....	3
1.5. Systematika Pembahasan.....	4
1.6. Time Schedule	5
BAB II. DASAR TEORI	6
2.1. Teknologi yang Digunakan	6
2.1.1. Debian GNU/Linux.....	6
2.1.2. Apache.....	7
2.1.3. PHP Hypertext Preprocessor	7
2.1.4. Hubungan PHP dengan HTML.....	8
2.1.5. MySQL	9
2.1.6. Bekerja dengan PHP dan MySQL.....	10
2.1.7. Software Snort dan ACID	11
2.1.8. Software ADOdb	14
2.1.9. Software Basic Analysis and Security Engine (BASE).....	15
2.1.10. Software Barnyard	15
2.2. Pengertian Networking	16
2.2.1. Local Area Network (LAN)	16
2.3. Network Defence.....	17
2.3.1. Network Segmentation	17
2.3.2. Firewall	18
2.3.3. Mengenai Port	19
2.3.4. Deteksi Penyusupan (Intrusion Detection).....	19
BAB III. ANALISA DAN PEMODELAN	21
3.1. Pendahuluan.....	21
3.2. Pemodelan <i>System</i> dan <i>Hardware</i>	21
3.2.1. Hardware yang digunakan.....	22
3.2.2. Instalasi System Operasi Linux Debian 4.0, beserta Software yang Lain ..	22
3.2.3. Pemilihan Topologi Jaringan.....	23
3.3. Perancangan instalasi	25
3.4. Desain antar muka.....	26
3.4.1. Use Case Diagram	27
3.5. Perancangan <i>System</i> Keamanan.....	27

3.5.1.	Keamanan pada System Operasi (Versi Kernel yang digunakan)	28
3.5.2.	Keamanan pada Software Web Server (Versi Apache yang digunakan) ...	28
3.5.3.	Keamanan pada Software MySQL (versi MySQL yang digunakan)	28
3.5.4.	Keamanan pada Software PHP (Versi PHP yang digunakan)	29
3.5.5.	Keamanan pada Software Web Based yang berjalan	29
BAB IV. PERANCANGAN DAN IMPLEMENTASI		31
4.1.	Instalasi dan Konfigurasi	31
4.1.1.	Konfigurasi Debian	31
4.1.2.	Instalasi firewall	33
4.1.3.	Instalasi Snort dan Rule Snort (VRT Rules)	34
4.1.4.	Konfigurasi dan Menjalankan Program Snort.....	35
4.1.5.	Konfigurasi MySQL Server	37
4.1.6.	Konfigurasi Snort dengan MySQL Server.....	39
4.1.7.	Instalasi Apache-SSL Web Server.....	40
4.1.8.	Install dan Konfigurasi Basic Analysis and Security Engine (BASE)	41
4.1.9.	Install Barnyard dan Konfigurasi Snort.....	44
4.1.10.	Script Startup untuk Snort dan Barnyard	47
4.2.	Pembuatan Web	48
4.2.1.	Desain.....	48
4.2.2.	Check Alert.....	50
4.2.3.	Show Alert	51
4.2.4.	Restart Service	52
4.2.5.	Make Shell Bash	53
4.2.6.	Run Shell Bash.....	56
4.2.7.	Edit User	57
4.2.8.	Help & Support	58
BAB V. PENGUJIAN		59
5.1.	Whitebox Testing.....	59
5.1.1.	Pengujian pada Pemograman Shell.....	59
5.1.2.	Pengujian pada System	64
5.2.	Blackbox Testing	65
5.2.1.	Pengujian pada login.php	65
5.2.2.	Pengujian pada menu.php.....	66
5.2.3.	Pengujian pada sensor.php	66
5.2.4.	Pengujian pada restart.php	66
5.2.5.	Pengujian pada makesbash.php	67
5.2.6.	Pengujian pada stwizz.php	67
5.2.7.	Pengujian pada runsbash.php	68
5.2.8.	Pengujian pada editusr.php.....	68
5.2.9.	Pengujian pada help.php.....	69
BAB VI. KESIMPULAN DAN SARAN		70
6.1.	Kesimpulan dengan Hasil Evaluasi	70
6.2.	Saran dengan Hasil Evaluasi	70
DAFTAR PUSTAKA		72
LAMPIRAN		76
Instalasi Linux Debian untuk Transparent Firewall.....		76
Curriculum Vitae		87

DAFTAR GAMBAR

Gambar 2.1 Topologi-topologi jaringan dari situs (cisco.netacad.net)	16
Gambar 3.1 Topologi jaringan	23
Gambar 3.2 <i>Use case diagram</i>	27
Gambar 4.1 Konfigurasi pada <i>/etc/apt/sources.list</i>	32
Gambar 4.2 Tampilan lokkit (1)	33
Gambar 4.3 Tampilan lokkit (2)	34
Gambar 4.4 Konfigurasi interfaces pada <i>/etc/network/interfaces</i>	37
Gambar 4.5 <i>logging snort</i> telah masuk kedalam <i>database</i>	38
Gambar 4.6 Import table <i>snort</i> kedalam <i>database MySQL</i>	39
Gambar 4.7 Menghilangkan komentar pada <i>/etc/PHP5/Apache2/PHP.ini</i>	41
Gambar 4.8 Aplikasi <i>BASE</i> yang telah berjalan sempurna	42
Gambar 4.9 Menghilangkan komentar pada <i>/etc/PHP5/cls/PHP.ini</i>	43
Gambar 4.10 Menghilangkan komentar ada <i>output</i> di <i>/etc/snort/snort.conf</i>	45
Gambar 4.11 Isi file <i>/etc/snort/bylog.waldo</i>	46
Gambar 4.12 Isi file <i>/etc/init.d/snort-barn</i>	47
Gambar 4.13 Menu login awal <i>web</i>	48
Gambar 4.14 Halaman menu	49
Gambar 4.15 Halaman <i>check alert</i>	50
Gambar 4.16 Halaman <i>show alert</i>	51
Gambar 4.17 Halaman <i>restart service</i>	52
Gambar 4.18 Halaman <i>make shell bash</i>	53
Gambar 4.19 Halaman wizard (1)	54
Gambar 4.20 Halaman wizard (2)	55
Gambar 4.21 Halaman <i>run shell bash</i>	56
Gambar 4.22 Halaman <i>edit user</i>	57
Gambar 4.23 Halaman <i>help & support</i>	58
Gambar 5.1 Halaman <i>web</i> pada <i>restart.php</i>	60
Gambar 5.2 <i>Restarting</i> pada <i>networking</i>	60
Gambar 5.3 <i>Restarting</i> pada <i>Apache-ssl</i>	61
Gambar 5.4 <i>Restarting</i> pada <i>snort-barn</i>	62
Gambar 5.5 <i>Restarting</i> pada <i>MySQL</i>	62
Gambar 5.6 <i>Restarting</i> pada <i>Apache2</i>	63
Gambar 5.7 <i>ps aux</i> kepada <i>snort</i>	64
Gambar 5.8 <i>ps aux</i> kepada <i>barnyard</i>	65
Gambar Lampiran.1. <i>Booting Linux Debian</i> menu awal	76
Gambar Lampiran.2. Memilih bahasa yang akan digunakan	76
Gambar Lampiran.3. Memilih <i>keyboard layout</i>	77
Gambar Lampiran.4. Konfigurasi <i>network</i>	77
Gambar Lampiran.5. Memasukan <i>hostname</i>	78
Gambar Lampiran.6. Membuat partisi 1	78
Gambar Lampiran.7. Membuat partisi 2	79
Gambar Lampiran.8. Membuat partisi 3	79
Gambar Lampiran.9. Membuat partisi 4	79

Gambar Lampiran.10. Membuat partisi 5	80
Gambar Lampiran.11. Membuat partisi 6	80
Gambar Lampiran.12. Membuat partisi 7	80
Gambar Lampiran.13. Membuat partisi 8	81
Gambar Lampiran.14. Membuat partisi 9	81
Gambar Lampiran.15. Membuat partisi 10	81
Gambar Lampiran.16. Mengatur settingan waktu.....	82
Gambar Lampiran.17. Memasukkan <i>password root</i>	82
Gambar Lampiran.18. Verifikasi password root	82
Gambar Lampiran.19. Membuat user baru 1	83
Gambar Lampiran.20. Membuat user baru 2	83
Gambar Lampiran.21. Membuat user baru 3	84
Gambar Lampiran.22. Membuat user baru 4	84
Gambar Lampiran.23. Membuat user baru 5	84
Gambar Lampiran.24. Menginstall <i>Linux</i> 1.....	85
Gambar Lampiran.25. Menginstall <i>Linux</i> 2.....	85
Gambar Lampiran.26. Menginstall <i>Linux</i> 3.....	85
Gambar Lampiran.27. Menginstall <i>Linux</i> 4.....	86
Gambar Lampiran.28. Menginstall <i>Linux</i> 5.....	86

DAFTAR TABEL

Tabel 1.1 <i>Time schedule</i> penulis	5
Tabel 5.1 Tabel pengujian pada <i>login.php</i>	65
Tabel 5.2 Tabel pengujian pada <i>menu.php</i>	66
Tabel 5.3 Tabel pengujian pada <i>sensor.php</i>	66
Tabel 5.4 Tabel pengujian pada <i>restart.php</i>	66
Tabel 5.5 Tabel pengujian pada <i>makesbash.php</i>	67
Tabel 5.6 Tabel pengujian pada <i>stwizz.php</i>	68
Tabel 5.7 Tabel pengujian pada <i>runsbash.php</i>	68
Tabel 5.8 Tabel pengujian pada <i>editusr.php</i>	69
Tabel 5.9 Tabel pengujian pada <i>help.php</i>	69