

**IMPLEMENTASI KEAMANAN JARINGAN KOMPUTER
MENGUNAKAN IP TABLES DAN BRO IDS (INTRUSION
DETECTION SYSTEM) DENGAN NOTIFIKASI EMAIL
PADA LABORATORIUM ELEKTRO UNIVERSITAS
HANGTUAH SURABAYA**

SKRIPSI



Oleh:

KIKI BAHRUM SUHARNO

1234010126

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"
JAWA TIMUR
2019**

DOSEN PEMBIMBING 1 : CHRYSTIA AJI PUTRA, S.KOM, M.KOM
DOSEN PEMBIMBING 2 : HENNI ENDAH WAHANANI, ST, M.KOM
PENYUSUN : KIKI BHRUM SUHARNO
NPM : 1234010126

ABSTRAK

Pada penelitian ini, penulis membuat keamanan jaringan menggunakan *IP Tables* untuk melakukan *filter* lalu lintas pada jaringan dan sistem *Intrusion Detection System (IDS) Bro* untuk mendeteksi adanya serangan yang terjadi pada jaringan komputer yang dilakukan oleh penyerang. Dan sistem operasi yang digunakan adalah *ubuntu*.

Pada penelitian ini, penulis menerapkan *IP Tables* dan *Intrusion Detection System* di laboratorium elektro universitas hang tua dengan melakukan instalasi dan konfigurasi aplikasi *Bro* untuk mendeteksi serangan yang dapat merusak jaringan komputer, serangan yang digunakan berupa *Port Scanning*, *SSH Bruteforce attack* dan *SYN Flood*. Serangan tersebut dilakukan ke *device* yang terhubung pada jaringan tersebut, Serta melakukan konfigurasi *Postfix* agar dapat mengirimkan notifikasi pendeteksian serangan secara langsung melalui *email*.

Hasil dari penelitian ini menyatakan bahwa *Bro* mampu mendeteksi serangan berdasarkan jumlah *log* dan *notice* serangan yang diterima dan mengirimkan pemberitahuan deteksi serangan melalui *email* agar bisa meminimalisir serangan yang terjadi pada jaringan komputer di laboratorium elektro universitas hangtuh surabaya.

Kata kunci : *Bro, IPTables, IDS, SYN Flood, Port Scanning, SSH Bruteforce attack, ubuntu, Email.*

KATA PENGANTAR

Syukur Alhamdulillah kami panjatkan kehadiran Allah SWT yang telah memberikan rahmat serta hidayah-Nya sehingga penyusunan Laporan Skripsi ini dapat diselesaikan.

Laporan Skripsi ini disusun untuk memenuhi syarat dalam memperoleh gelar sarjana komputer, program studi Teknik Informatika. Judul yang diambil dalam penulisan Skripsi ini adalah :

**“IMPLEMENTASI KEAMANAN JARINGAN KOMPUTER
MENGUNAKAN IP TABLES DAN BRO IDS (INTRUSION DETECTION
SYSTEM) DENGAN NOTIFIKASI EMAIL PADA LABORATORIUM
ELEKTRO UNIVERSITAS HANGTUAH SURABAYA ”**

Penulis menyadari bahwa penulisan Laporan Skripsi ini masih belum sempurna. Oleh karena itu, saran dan kritik yang membangun akan penulis terima dengan senang hati.

Akhir kata semoga Laporan Skripsi ini dapat memberikan manfaat bagi para mahasiswa khususnya dan pengetahuan pada umumnya.

DAFTAR ISI

ABSTRAK	I
KATA PENGANTAR.....	II
DAFTAR ISI.....	V
DAFTAR GAMBAR.....	VIII
DAFTAR TABEL	XII
BAB I PENDAHULUAN.....	2
1.1. Latar Belakang.....	2
1.2. Perumusan Masalah	4
1.3. Batasan Masalah.....	5
1.4. Tujuan	5
1.5. Manfaat	6
1.6. Sistematika Penulisan	7
BAB II TINJAUAN PUSTAKA.....	9
2.1. Penelitian Terdahulu	9
2.1.1. Vern Paxson (San Antonio, Texas, January 26-29, 1998).....	9
2.1.2. Ganesh Kumar Varadarajan (15 Oct 2012).....	9
2.2. Dasar Teori.....	10
2.2.1. Ubuntu.....	10
2.2.2. IP Tables	13
2.2.2.1. Tabel Filter	13
2.2.2.2. Tabel NAT	14
2.2.2.3. Table Mangle	14
2.2.3. Jaringan Komputer	15

2.2.4. IDS	22
2.2.4.1 Network Based Intrusion Detection System (NIDS)	24
2.2.4.2. Host-based Intrusion Detection System (HIDS)	25
2.2.5. Intrusion Prevention System (IPS).....	25
2.2.5.1. Signature-based Intrusion Detection System	27
2.2.5.2. Anomaly Based Intrusion Detection System	27
2.2.5.3. Host Based Intrusion Prevention System (HIPS)	28
2.2.5.4. Network Based Intrusion Prevention System (NIPS).....	28
2.2.6. BRO	29
2.2.7. Port Scanning	29
2.2.8. SSH Bruteforce Attack.....	30
2.2.9. SYN Flood	30
2.2.10. Simple Mail Protocol (SMTP)	34
BAB III METODOLOGI PENELITIAN	35
3.1. Alur Penelitian	35
3.1.1. Studi Pustaka.....	36
3.1.2. Perancangan Sistem	36
3.1.3. Pengujian Sistem.....	36
3.1.4. Analisa Serangan.....	37
3.1.5. Kesimpulan	37
3.2. Rancangan Penelitian.....	37
3.2.1. Definisi Kebutuhan Sistem	37
3.2.2. Rancangan Jaringan	39
3.2.3. Rancangan Sistem	40

3.3. Skenario Pengujian Serangan.....	42
3.3.1. Skenario Serangan Port Scanning	43
3.3.2. Skenario Serangan SSH Bruteforce Attack	44
3.3.3. Skenario Serangan SYN Flood	45
3.4. Analisa Serangan.....	46
BAB IV HASIL DAN PEMBAHASAN	48
4.1. Instalasi Sistem	48
4.1.1. Instalasi Bro	48
4.1.2. Instalasi Postfix	50
4.2. <i>Konfigurasi Sistem</i>	51
4.2.1. Konfigurasi Bro.....	51
4.2.2. Konfigurasi Postfix	53
4.3. Implementasi Serangan dan Pendeteksian	55
4.3.1. Serangan dan Pendeteksian Port Scanning	56
4.3.2. Serangan Pendeteksian Bruteforce Attack.....	60
4.3.3. Serangan dan Pendeteksian SYN Flood.....	64
4.4. Implementasi Pencegahan Serangan.....	75
4.4.1. Pencegahan Serangan Port Scanning	75
4.4.2. Pencegahan Serangan SSH Bruteforce Attack.....	76
4.4.3. Pencegahan Serangan SYN Flood.	77
BAB V KESIMPULAN DAN SARAN	82
5.1. Kesimpulan	82
5.2. Saran.....	82
DAFTAR PUSTAKA	84

DAFTAR GAMBAR

Gambar 2.1. Perancangan Sistem <i>Intrusion Detection System</i> (IDS) (Anif, HWS, & Huri, 2015).....	23
Gambar 2.2. Perancangan Sistem <i>Wireless Intrusion Detection Prevention System</i> (IDPS) (Scarfone & Mell, 2007).....	26
Gambar 2.3. Alur Three-Way Handshake (Setiawan, 2015).	31
Gambar 3.1. Alur Rancangan Penelitian.....	35
Gambar 3.2. Skenario Rancangan Jaringan	39
Gambar 3.3. Alur Instalasi dan Konfigurasi Bro	40
Gambar 3.4. Alur Instalasi dan Konfigurasi <i>Postfix</i>	41
Gambar 3.5. Alur Serangan <i>Port Scanning</i>	43
Gambar 3.6. Alur Serangan <i>SSH Bruteforce Attack</i>	44
Gambar 3.7. Alur Serangan <i>SYN Flood</i>	45
Gambar 3.8. Alur Analisa Serangan	46
Gambar 4.1. Instalasi Paket <i>Bro</i>	48
Gambar 4.2. Proses <i>Download Bro</i>	49
Gambar 4.3. Membuka <i>Folder Bro</i>	49
Gambar 4.4. Pemeriksaan Berkas Bro	49

Gambar 4.5. Perintah Instalasi <i>Bro</i>	50
Gambar 4.6. Perintah Instalasi dan Pemasangan Paket <i>Postfix</i>	50
Gambar 4.7. Konfigurasi <i>Rules Networks.cfg</i>	51
Gambar 4.8. Konfigurasi <i>Rules Broctl.cfg</i>	51
Gambar 4.9. Konfigurasi <i>Node</i>	52
Gambar 4.10. Konfigurasi Mengaktifkan <i>IDS Bro</i>	52
Gambar 4.11. Perintah Masuk Berkas Konfigurasi <i>Main.cf</i>	53
Gambar 4.12. Konfigurasi <i>Main.cf</i>	53
Gambar 4.13. Konfigurasi <i>Sasl_Passwd</i>	54
Gambar 4.14. Perintah <i>Postfix</i> Mengirim <i>Email</i>	54
Gambar 4.15. Perintah Untuk Melihat <i>Log</i> Serangan Pada <i>Bro</i>	55
Gambar 4.16. Perintah Untuk Melihat <i>log Notice</i> Serangan Pada <i>Bro</i>	55
Gambar 4.17. Perintah Serangan <i>Port Scanning</i>	56
Gambar 4.18. <i>Hasil</i> Serangan <i>Port Scanning</i>	57
Gambar 4.19. <i>Hasil</i> Pendeteksian <i>Port Scanning</i> pada Log <i>Bro</i>	58
Gambar 4.20. <i>Hasil</i> Pendeteksian Notice <i>Port Scanning</i> pada Log <i>Bro</i>	59
Gambar 4.21. <i>Notifikasi Email</i> Terhadap Serangan <i>Port Scanning</i>	60
Gambar 4.22. <i>Perintah serangan SSH Bruteforce Attack</i>	61
Gambar 4.23. <i>Hasil serangan SSH Bruteforce Attack</i>	61

Gambar 4.24. Hasil efek serangan SSH Bruteforce Attack.....	62
Gambar 4.25. Hasil Pendeteksian Serangan SSH Bruteforce Pada log Bro.....	63
Gambar 4.26. Hasil Pendeteksian Notice Serangan SSH Bruteforce pada log Bro	63
Gambar 4.27. Notifikasi Email Terhadap Serangan SSH Bruteforce Attack.....	64
Gambar 4.28. Perintah Serangan SYN Flood	65
Gambar 4.29. Monitoring Grafik CPU Usage Sebelum terkena Serangan.....	66
Gambar 4.30. Perintah Serangan SYN Flood Percobaan Pertama	66
Gambar 4.31. Hasil Serangan SYN Flood Percobaan Pertama	67
Gambar 4.32. Hasil Grafik Efek CPU Usage SYN Flood Percobaan Pertama	68
Gambar 4.33. Perintah Serangan SYN Flood Percobaan Kedua	68
Gambar 4.34. Hasil Serangan SYN Flood Percobaan Kedua	69
Gambar 4.35. Hasil Grafik Efek CPU Usage SYN Flood Percobaan Pertama	69
Gambar 4.36. Perintah Serangan SYN Flood Percobaan Kedua	70
Gambar 4.37. Hasil Serangan SYN Flood Percobaan Ketiga.....	71
Gambar 4.38. Hasil Grafik Efek CPU Usage SYN Flood Percobaan Ketiga	71
Gambar 4.39. Hasil Percobaan Serangan SYN Flood.....	72
Gambar 4.40. Hasil Pendeteksian Serangan SYN Flood pada Bro.	73
Gambar 4.41. Notifikasi serangan SYN Flood pada Email.....	74

Gambar 4.42. <i>Rule IP Tables</i> Pencegahan Serangan <i>Port Scanning</i>	75
Gambar 4.43. Hasil Serangan <i>Port Scanning</i> Setelah Dilakukan Pencegahan	75
Gambar 4.44. Hasil Serangan <i>SSH Bruteforce</i> Setelah Dilakukan Pencegahan ...	76
Gambar 4.45. Hasil efek serangan <i>SSH Bruteforce Attack</i> Setelah Pencegahan ..	77
Gambar 4.46. <i>Rule IPTables</i> Pencegahan Serangan <i>SYN Flood</i> pada Bro.	77
Gambar 4.47. Hasil Percobaan Pertama Serangan <i>SYN Flood</i> Setelah Dilakukan Pencegahan	78
Gambar 4.48. Hasil Percobaan Kedua Serangan <i>SYN Flood</i> Setelah Dilakukan Pencegahan	78
Gambar 4.49. Hasil Percobaan Ketiga Serangan <i>SYN Flood</i> Setelah Dilakukan Pencegahan	79
Gambar 4.50. Hasil Diagram Grafik Pencegahan Serangan <i>SYN Flood</i>	80
Gambar 3.1. Alur Rancangan Penelitian.....	35
Gambar 3.2. Skenario Rancangan Jaringan	39
Gambar 3.3. Alur Instalasi dan Konfigurasi Bro	40
Gambar 3.4. Alur Instalasi dan Konfigurasi <i>Postfix</i>	41
Gambar 3.5. Alur Serangan <i>Port Scanning</i>	43
Gambar 3.6. Alur Serangan <i>SSH Bruteforce Attack</i>	44
Gambar 3.7. Alur Serangan <i>SYN Flood</i>	45
Gambar 3.8. Alur Analisa Serangan	46

DAFTAR TABEL

Tabel 3.1 Kebutuhan Perangkat Keras.....	38
Tabel 3.2 Kebutuhan Perangkat Lunak.....	38
Tabel 4.1. Alamat IP Penyerang, Target dan Metode Serangan.....	55
Tabel 4.2. Jumlah Percobaan Serangan <i>Syn Flood</i>	66
Tabel 4.3. Hasil Percobaan Serangan SYN Flood	72
Tabel 4.4. Hasil Pendeteksian Serangan Pada <i>IDS Bro</i>	74
Tabel 4.5. Hasil Pencegahan Serangan <i>SYN Flood</i>	80

UCAPAN TERIMA KASIH

Alhamdulillah puji syukur kepada Allah SWT, karena atas rahmat dan limpahan beliau penulis dapat menyelesaikan penulisa laporan tugas akhir Selama melaksanakan pengerjaan tugas akhir dan dalam menyelesaikan laporan skripsi ini, penulis telah banyak menerima bimbingan, pengarahan, petunjuk dan saran, serta fasilitas yang membantu hingga akhir dari penulisan laporan ini. Untuk itu penulis menyampaikan ucapan terimakasih yang sebesar-besarnya kepada :

1. Kedua orang tua dan keluarga yang telah memberikan doa, kasih sayang, serta semangat.
2. Ibu Dr. Ir. Ni Ketut Sari, MT selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jawa Timur.
3. Bapak Budi Nugroho ,S.Kom ,M.Kom selaku Ketua Jurusan Teknik Informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur.
4. Bapak Chrystia Aji Putra, S.Kom, M.Kom selaku Dosen Pembimbing pertama skripsi yang telah membimbing penulis selama pelaksanaan dan penyusunan laporan skripsi.
5. Ibu Henni Endah W, S.T, M.Kom selaku Dosen Pembimbing kedua skripsi yang telah membimbing penulis selama pelaksanaan dan penyusunan laporan skripsi.
6. Bapak Hendra Maulana, S.Kom selaku Koordinator Tugas Akhir / PIA Universitas Pembangunan Nasional “Veteran” Jawa Timur.

7. Bapak Ali Sabrian selaku Koordinator Laboratorium Elektro Universitas Hang Tuah Surabaya.
8. Bapak dan Ibu dosen Teknik Informatika yang tidak dapat disebutkan satu persatu. Terima kasih banyak, berkat beliau semua penulis mendapat banyak ilmu dan wawasan yang berguna pada kemudian hari
9. Bapak dan Ibu Staff Universitas Pembangunan Nasional “Veteran” Jawa Timur yang membantu penulis dalam proses tugas akhir.
10. Wahyu Ferdyanto, An Say,Fathoni, Johni, Adhit,Zainul, Fando, Bangga Aje, Arif, cak no, mbak lilik, Rizky (tumo), Ramadhan, Wisang.
11. Teman - teman Teknik Informatika UPN “Veteran” Jawa Timur tidak bisa penulis sebutkan satu persatu.