Analisis dan Implementasi Keamanan Jaringan File Transfer Protocol (FTP) Menggunakan Intrusion Prevention System (IPS) pada Mikrotik

Andriyan Dwi Putra*[1], Muhammad Thorriq Ridho Bey Alghozy [2]
[1]Sistem Informasi Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
[2]Informatika Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
E-mail: ***[1]andriyan.putra@amikom.ac.id**, [2]muhammad.2903@students.amikom.ac.id

Abstrak

Perkembangan teknologi pada bidang komunikasi dan informasi mengalami peningkatan yang pesat, dampak dari kemajuan ini terlihat didalam pengolahan data. Pengolahan data dilakukan melalui media transmisi elektronik, media tersebut dikenal dengan File Transfer Protocol (FTP), FTP digunakankan sebagai media transfer data atau file dalam lingkup suatu jaringan. FTP merupakan salah satu pilihan yang tepat dalam penyimpanan file, karena proses upload dan download bisa digunakan secara cepat dan efektif. Namun dengan perkembangan teknologi yang pesat ini banyak alat atau tools yang dapat digunakan untuk melakukan tindakan kejahatan seperti brute force FTP, port scanning, dan DDoS (ICMP flood). Maka dibutuhkan sebuah sistem yang mampu melakukan tindakan prevention dan digunakanlah metode Intrusion Prevention System (IPS). IPS mempunyai fungsi untuk mengamati, mengidentifikasi tindakan mencurigakan, dan melakukan monitoring serta pencegahan serangan dengan memblokir semua ancaman secara otomatis. Karena itu IPS bisa disebut sebagai gabungan dari IDS yang melakukan moniroting dan prevention layaknya firewall. Maka dari itu IPS dapat diterapkan pada router MikroTik sebagai metode keamananya untuk mencegah serangan ke FTP server yang terdapat di router MikroTik.Dari percobaan serangan seperti bruteforce FTP, port scanning, dan DDoS (ICMP flood). Didapat hasil yaitu serangan Brute Force FTP tidak mampu membobol akses akun FTP dengan tingkat keberhasilan 0, Port Scanning juga tidak mampu melanjutkan serangan, walaupun pada port 21 beberapa kali terscan karena IPS mendrop serangan. Pada serangan ICMP Flood dapat membebani server pada saat belum menerapkan IPS dengan tingkat CPU load 63%-100% dan setelah menerapkan IPS CPU load hanya 13%-36% yang membuat server tetap stabil.

Kata Kunci: *Brute Force* FTP, ICMP *Flood, Port Scanning, Intrusion Prevention System* (IPS), *File Transfer Protocol* (FTP).

1. PENDAHULUAN

Perkembangan teknologi pada bidang komunikasi serta informasi mengalami peningkatan yang pesat, salah satu dampak dari kemajuan ini terlihat didalam sistem pengolahan data yaitu media transmisi elektronik, media tersebut dikenal dengan sebutan komunikasi data. Penggunaan komunikasi data biasanya dilakukan ketika akan menjalankan pertukaran data pada jaringan komputer. Kegiatan tersebut memerlukan sebuah protokol yang bisa menjalankan kegiatan pertukaran data, protokol itu disebut *File Transfer Protocol* (FTP) [1]. Namun dengan perkembangan teknologi yang pesat ini banyak tools yang dapat digunakan untuk melakukan tindakan kejahatan seperti *bruteforce* FTP, *port scanning*, dan *Internet Control Message protocol Flooding* (ICMP *flooding*). Pada sistem keaman FTP terdapat suatu kelemahan yaitu pada data

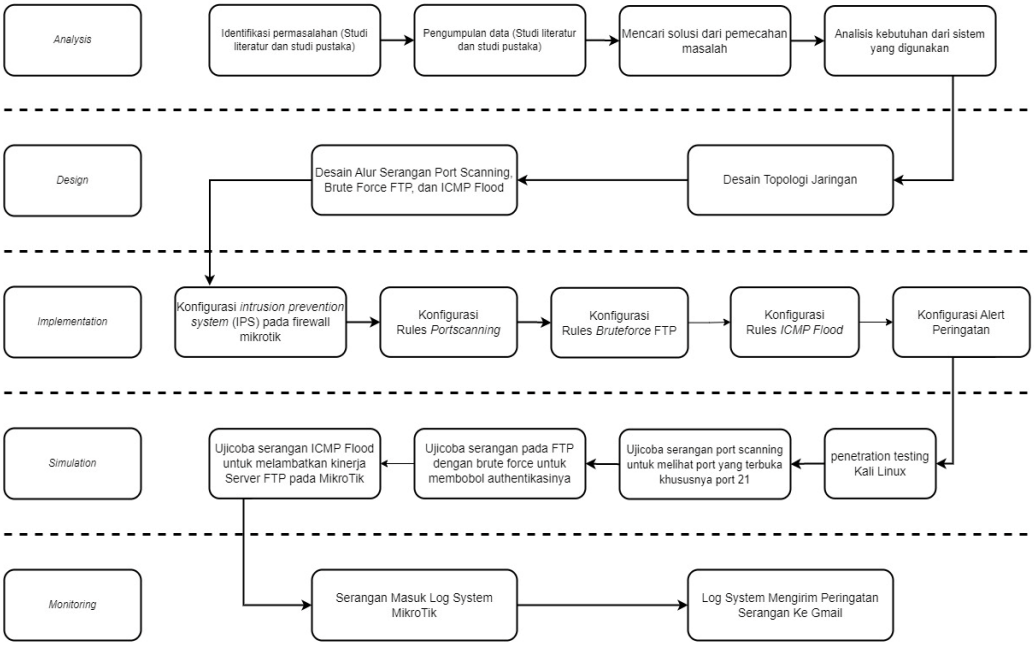
username dan password yang tidak di enkripsi pada saat melakukan proses login. Dengan keadaan tersebut membuat FTP menjadi rentan terhadap serangan oleh hacker[2].

Maka dari permasalahan diatas dibutuhkan sistem keamanan jaringan yang dapat melindungi FTP serta untuk menangkal dan mencegah dari potensi serangan. Keamanan Jaringan menjadi suatu komponen yang sangat penting dalam menjaga keabsahan dan kelengkapan suatu informasi data beserta penggunanya [3]. Untuk itu diperlukan sebuah sistem yang cocok untuk mencegah dan mengidentifikasi serangan, maka digunakanlah metode *Intrusion Prevention System* (IPS) [4]. Metode IPS mempunyai fungsi untuk mengamati *traffic* data yang berjalan secara real-time pada jaringan serta mengidentifikasi semua tindakan yang mencurigakan [5]. IPS merupakan upgrade dari metode sebelumnya yaitu *Intrusion Detection System* (IDS), pada metode IDS hanya bisa melakukan monitoring saja dan pada metode IPS bisa melakukan pencegahan serangan dengan memblokir semua ancaman secara otomatis dan bisa memonitoring serangan [6]

Dengan demikian metode IPS berperan selayaknya *firewall* yang dapat menerima atau mencegah semua paket yang mencoba masuk lalu digabungkan dengan monitoring jika terdapat data yang mencurigakan karena konsep dari *firewall* yaitu jika ada traffic data yang masuk menuju ke jaringan *firewall* akan melakukan tindakan pemeriksaan dan pengawasan pada *traffic* tersebut [7]. Maka jika terjadi sebuah kegiatan yang mencurigakan dan diindentifikasi sebagai serangan maka IPS akan melakukan tindakan pencegahan dengan memblokir serangan dengan cara memblock dan drop IP Address penyerang dan hasil dari serangan dapat ditampilkan pada log sistem MikroTik dan dapat dikirim dengan Gmail untuk sebagai monitoring alert peringatan dini untuk administrator ketika terjadi serangan pada FTP [8].

2. METODE PENELITIAN

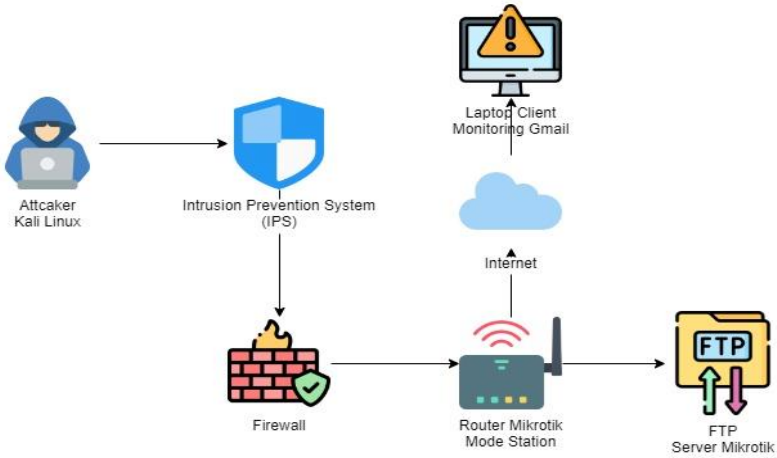
Alur penelitian merupakan tahapan – tahapan dalam melaksanakan kegiatan penelitian. Dengan memakai alur penelitian peneliti dapat melakukan penelitian secara terstruktur. Pada penelitian yang dilakukan sekarang peneliti menggunakan metode NDLC (*Network Development Life Cycle*), adapun tahapanya seperti pada gambar dibawah ini.



Gambar 1. Alur NDLC Penelitian

1. *Analysis* (Analisis): Pada tahap ini peneliti melakukan analisa permasalahan dengan mengidentifikasi permasalahan, caranya dengan membaca studi literatur berupa jurnal yang berada pada google schoolar atau sinta. Setelah mendapatkan permasalahan selanjutnya membuat solusi dari permasalahan tersebut dan melakukan analisa kebutuhan alat dan bahan yang digunakan untuk melaksanakan penelitian.
2. *Design* (Desain): Pada tahap ini peneliti membuat desain model gambaran alur penelitian, alur kerja sistem dan rancangan sistem keamanan yang akan dibuat untuk mencegah *attacker* melakukan penyerangan pada perangkat atau sistem.
3. *Implementation* (Implementasi): Pada tahap ini peneliti melakukan implementasi sistem keamanan bedasarkan rancangan keamanan yang sudah dibuat sebelumnya seperti, Konfigurasi rules IPS pada *firewall* router MikroTik dan konfigurasi alert monitoring serangan.
4. *Simulation* (Simulasi): Pada tahap ini peneliti melakukan simulasi penyerangan terhadap keamanan jaringan yang telah dibuat pada *firewall* dengan tujuan mengetahui apakah sistem keamanan IPS yang telah dibuat berhasil mencegah serangan atau tidak serta sistem alertnya berjalan secara real-time atau tidak.
5. Monitoring: Pada tahap monitoring ini peneliti melakukan monitoring dengan mengamati kinerja dari *intrusion prevention system* (IPS), pengamatan tersebut memiliki tujuan apakah metode IPS dapat mengatasi serangan *brute force* FTP, *Port Scaning* dan *ICMP Flood*. Hasil dari serangan tersebut akan masuk pada log MikroTik dan diintergrasikan ke Gmail sebagai alert serangan.

2.1. *Alur Sistem Kerja Serangan dan Pencegahan*



Gambar 2. Alur Serangan dan Pencegahan

Alur kerja system serangan yang pertama seorang attacker akan menghubungkan komputer atau laptop dengan jaringan lalu melakukan percobaan penyerangan terhadap FTP yang terdapat pada router Mikrotik dengan serangan port scanning, brute force FTP, dan ICMP flood. Tetapi jika IPS yang berada pada firewall Mikrotik dapat mengidentifikasi kegiatan tersebut sebagai tindakan kejahatan maka IPS akan melakukan tugasnya dengan cara menganalisa paket data yang masuk, lalu memastikan apakah paket data yang masuk itu merupakan serangan atau bukan melalui rules yang telah dibuat, jika terdeteksi sebagai serangan maka IPS melakukan prevention otomatis dengan cara memblock dan mendrop IP Address attacker dan hasil dari

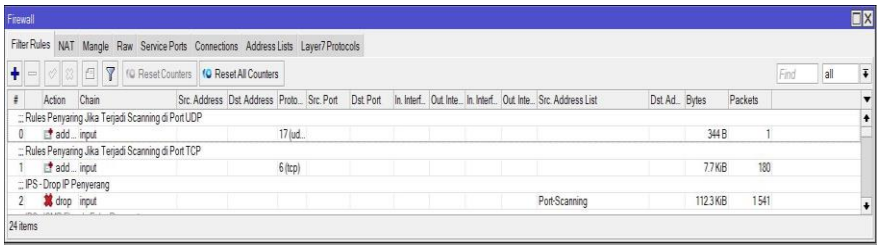
serangan tersebut akan masuk pada sistem log MikroTik lalu dari sistem log akan dikirim sebagai monitoring alert peringatan pada gmail administrator.

3. HASIL DAN PEMBAHASAN

3.1. Implementasi Intrusion Prevention System(IPS) pada firewall mikrotik

1. Rules IPS Port Scanning

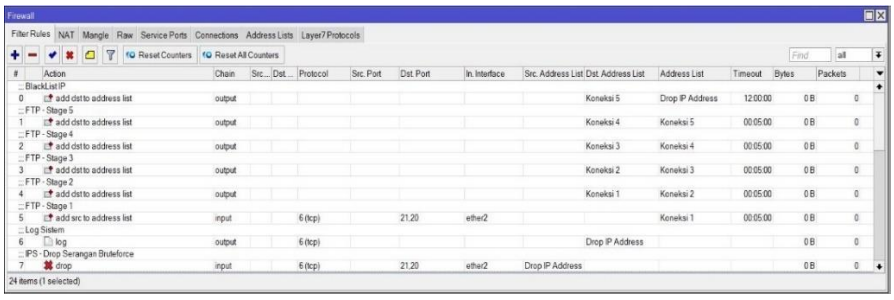
   Jika ada *attacker* yang melakukan percobaan penyerangan dengan menscan port TCP dan jumlah port yang discan lebih dari 21 pada *port scanning* detection (PSD), maka IP *attacker* dari perangkat yang digunakan untuk menyerang akan masuk kedalam *Address list* selama 12jam dan log sistem, yang selanjutnya IP tersebut akan langsung di blacklist dan di drop secara otomatis. Hasil dari penyerangan akan masuk ke log sistem lalu dikirim ke gmail untuk memberitahu adminitrator bahwa ada alert serangan.



Gambar 3. Rules *Port Scanning*

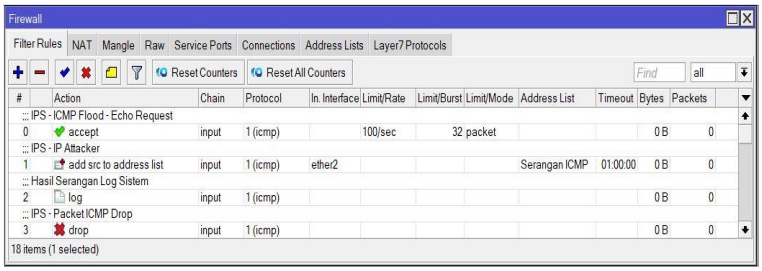
2. Rules IPS *Brute force* FTP

   Merupakan rules yang dipakai untuk mendeteksi serangan *brute force FTP* pada router MikroTik, pada rules ini peneliti memberi kesempatan login sampai 5 kali dan jika terjadi kegagalan login maka *IP Address* akan tercatat pada *Address list*. Artinya setiap kegagalan dalam percobaan login akan diberi waktu 5 menit, jika dalam waktu 5 menit itu melakukan percobaan login sampai 5 kali dan gagal maka sistem menganggap sebagai ancaman serangan, maka IP *attacker* akan di blacklist dan di drop selama 12 jam.



Gambar 4. Rules *Bruteforce* FTP

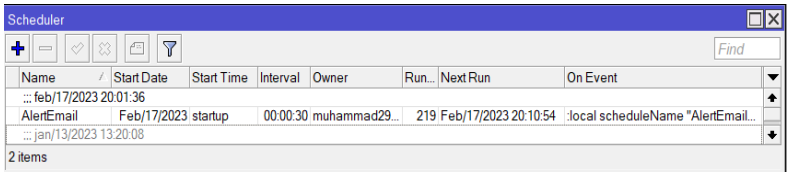
3. Rules IPS ICMP *Flood*



Gambar 5. Rules *Bruteforce* FTP

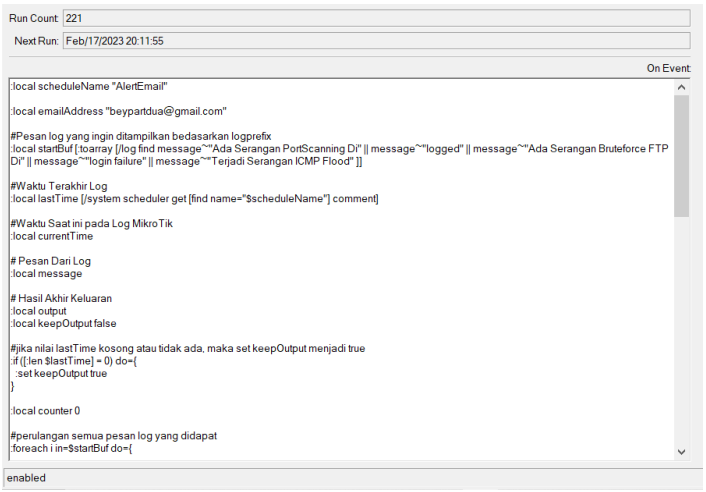
Merupakan rules yang dipakai untuk mendeteksi serangan ICMP *Flood* pada router MikroTik, pada rules ini peneliti memberi ketentuan jika terdapat ICMP *flood* dengan permintaan "*echo request*" pada server, lalu mencocokan paket hingga mencapai batas limit/rate. Pada rules yang sudah diatur dengan limit/rate 100 dan burst 32, burst merupakan jumlah awal paket yang akan dikirimkan. Brust bisa terjadi ketika data rate lebih kecil. Jika permintaan *echo request* melebihi batas rate yang telah ditentukan maka rules IPS akan berjalan dan IP yang mengirim *echo request* akan masuk pada *address list*. Lalu IP tersebut akan diblacklist dan didrop selama 1 jam, supaya jika terjadi permintaan *echo request* dengan jumlah yang banyak dengan IP Address yang sama maka server tidak terbebani dan tidak menjadi down.\

3.2. Implementasi scheduler di Mikrotik



Gambar 6. Scheduler Alert Mikrotik

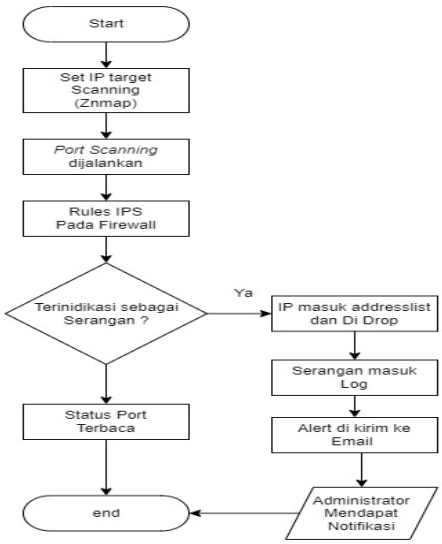
Scheduler merupakan salah satu fitur dari router MikroTik, fitur ini digunakan untuk membuat sistem penjadwalan yang bisa membaca pesan log prefix dari *firewall fillter rules* yang telah dibuat. Pada penelitian ini peneliti memanfaatkan *scheduler* untuk diimplementasikan sistem *alert* serangan yang dintergrasikan langsung dengan Gmail, pada sistem scheduler ini peneliti mengatur alert dengan interval atau jangka waktu rules dijalankan setiap 30 detik.



Gambar 7. Scheduler Alert Mikrotik

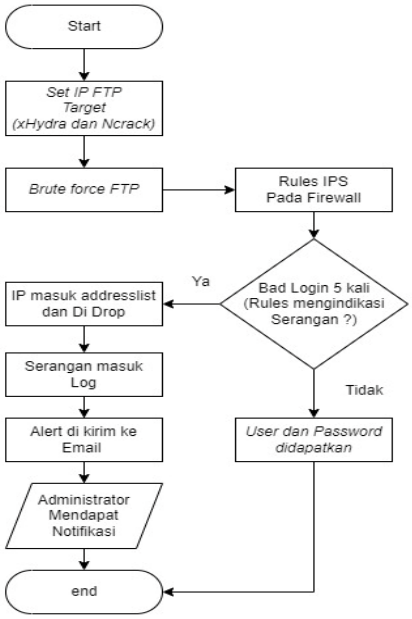
3.3. Flowchart Penyerangan

1. Flowchart Serangan *Port Scanning*



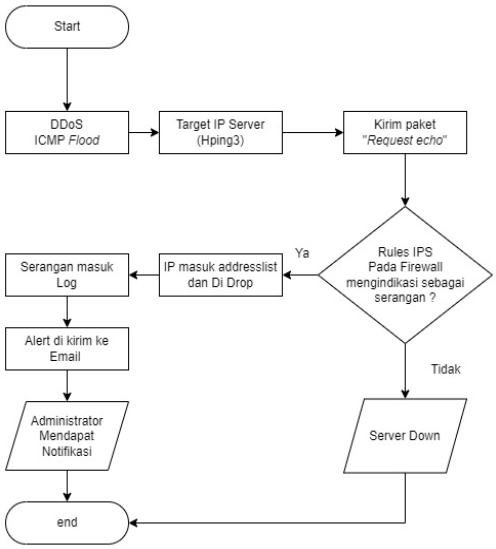
Gambar 8. Flowchart *Port Scanning*

2. Flowchart Serangan *Bruteforce* FTP



Gambar 9. Flowchart *Bruteforce* FTP

3. Flowchart Serangan ICMP *Flood*



Gambar 10. Flowchart ICMP *Flood*

3.4. Hasil Pengujian Serangan

1. Pengujian Serangan Port Scanning Dengan Tools Znmap
   Pada pengujian *port scanning* akan dilakukan percobaan serangan sebanyak 30 kali supaya dapat mengetahui apakah IPS mampu untuk memblokir *ports scanning* dan memonitoring secara *real-time*, pengujian *portscannig* dilakukan menggunakan profile *quick scan plus*.

Tabel 1 Pengujian Serangan Port Scanning Memakai Znmap

Pengujian Serangan	Durasi Waktu Scanning	Status Port	Hasil Serangan (IPS)	Waktu Log	Waktu Peringatan Monitoring	Rentan Waktu Alert
Percobaan Ke-1	55.82 Detik	Port Tidak Terlihat	Memblokir Serangan	10:18:07	10:18:24	17 Detik
Percobaan Ke-2	34.51 Detik	Port Tidak Terlihat	Memblokir Serangan	10:53:16	10:53:23	7 Detik
Percobaan Ke-3	3.03 Detik	Port Tidak Terlihat	Memblokir Serangan	11:00:29	11:00:29	1 Detik
Percobaan Ke-4	2.06 Detik	Port Tidak Terlihat	Memblokir Serangan	11:10:14	11:10:24	10 Detik
Percobaan Ke-5	56.82 Detik	Port 21 Terlihat	Memblokir Serangan	12:34:35	12:34:37	2 Detik
Percobaan Ke-6	56.23 Detik	Port Tidak Terlihat	Memblokir Serangan	12:42:28	12:42:29	1 Detik
Percobaan Ke-7	55.23 Detik	Port Tidak Terlihat	Memblokir Serangan	12:51:39	12:51:45	6 Detik
Percobaan Ke-8	57.54 Detik	Port Tidak Terlihat	Memblokir Serangan	12:55:24	12:55:27	3 Detik
Percobaan Ke-9	56.79 Detik	Port 21 Terlihat	Memblokir Serangan	12:58:41	12:58:43	2 Detik
Percobaan Ke-10	56.04 Detik	Port Tidak Terlihat	Memblokir Serangan	13:04:48	13:04:50	2 Detik
Percobaan Ke-11	55.58 Detik	Port Tidak Terlihat	Memblokir Serangan	13:08:40	13:08:42	2 Detik
Percobaan Ke-12	59.87 Detik	Port Tidak Terlihat	Memblokir Serangan	13:12:38	13:12:40	2 Detik
Percobaan Ke-13	50.54 Detik	Port Tidak Terlihat	Memblokir Serangan	13:25:50	13:25:52	2 Detik
Percobaan Ke-14	55.85 Detik	Port Tidak Terlihat	Memblokir Serangan	13:33:58	13:34:00	2 Detik
Percobaan Ke-15	5.69 Detik	Port Tidak Terlihat	Memblokir Serangan	13:45:49	13:45:51	2 Detik
Percobaan Ke-16	4.32 Detik	Port Tidak Terlihat	Memblokir Serangan	13:48:30	13:48:32	2 Detik
Percobaan Ke-17	56.45 Detik	Port Tidak Terlihat	Memblokir Serangan	13:50:25	13:50:27	2 Detik
Percobaan Ke-18	14.27 Detik	Port Tidak Terlihat	Memblokir Serangan	14:00:22	14:00:23	1 Detik
Percobaan Ke-19	12.27 Detik	Port 21 Terlihat	Memblokir Serangan	14:08:00	14:08:04	4 Detik
Percobaan Ke-20	59.20 Detik	Port Tidak Terlihat	Memblokir Serangan	14:18:45	14:18:48	3 Detik
Percobaan Ke-21	58.46 Detik	Port 21 Terlihat	Memblokir Serangan	14:27:47	14:27:51	4 Detik
Percobaan Ke-22	61.09 Detik	Port Tidak Terlihat	Memblokir Serangan	14:35:05	14:35:09	4 Detik
Percobaan Ke-23	58.42 Detik	Port 21 Terlihat	Memblokir Serangan	14:40:31	14:40:35	4 Detik

Percobaan Ke-24	66.75 Detik	Port Tidak Terlihat	Memblokir Serangan	14:45:58	14:46:03	5 Detik
Percobaan Ke-25	126.53 Detik	Port Tidak Terlihat	Memblokir Serangan	14:49:18	14:49:27	9 Detik
Percobaan Ke-26	55.63 Detik	Port 21 Terlihat	Memblokir Serangan	15:05:52	15:05:55	3 Detik
Percobaan Ke-27	57.13 Detik	Port 21 Terlihat	Memblokir Serangan	15:11:39	15:11:42	3 Detik
Percobaan Ke-28	59.68 Detik	Port Tidak Terlihat	Memblokir Serangan	15:15:37	15:15:41	4 Detik
Percobaan Ke-29	61.05 Detik	Port Tidak Terlihat	Memblokir Serangan	15:19:49	15:19:56	7 Detik
Percobaan Ke-30	58.86 Detik	Port Tidak Terlihat	Memblokir Serangan	15:26:45	15:26:50	5 Detik

2. Pengujian Serangan *Bruteforce* FTP Dengan Tools Ncrack
   Pada pengujian serangan *bruteforce* FTP dilakukan uji percobaan serangan sebanyak 30 kali supaya dapat mengetahui apakah IPS mampu untuk mencegah dan memblokir serangan *bruteforce* FTP dan memonitoring secara *real-time*. Pada pengujian nantinya akan disiapkan 36 list password palsu dan 1 password asli untuk diujicoba menggunakan ncrak. Hasil dari pengujian serangan akan ditampilkan dalam bentuk tabel.

Tabel 2 Pengujian Serangan Port Scanning Memakai Ncrack

Pengujian Serangan	Durasi Waktu Penyerangan	Hasil Serangan (IPS)	Waktu Log	Waktu Peringatan Monitoring	Rentan Waktu Alert
Percobaan Ke-1	60.20 Detik	Memblokir Serangan	17:03:48	17:04:14	27 Detik
Percobaan Ke-2	42.10 Detik	Memblokir Serangan	17:19:29	17:19:44	15 Detik
Percobaan Ke-3	42.15 Detik	Memblokir Serangan	17:23:18	17:23:45	27 Detik
Percobaan Ke-4	42.10 Detik	Memblokir Serangan	17:32:29	17:32:39	10 Detik
Percobaan Ke-5	42.13 Detik	Memblokir Serangan	17:35:21	17:35:45	24 Detik
Percobaan Ke-6	42.14 Detik	Memblokir Serangan	17:40:18	17:40:45	27 Detik
Percobaan Ke-7	42.16 Detik	Memblokir Serangan	17:44:13	17:44:15	2 Detik
Percobaan Ke-8	42.07 Detik	Memblokir Serangan	17:47:54	17:47:59	5 Detik
Percobaan Ke-9	42.07 Detik	Memblokir Serangan	17:50:36	17:50:45	9 Detik
Percobaan Ke-10	42.10 Detik	Memblokir Serangan	17:53:04	17:53:15	11 Detik
Percobaan Ke-11	45.08 Detik	Memblokir Serangan	17:55:30	17:55:42	12 Detik
Percobaan Ke-12	42.23 Detik	Memblokir Serangan	17:57:59	17:58:14	15 Detik
Percobaan Ke-13	42.13 Detik	Memblokir Serangan	17:59:40	17:59:45	5 Detik
Percobaan Ke-14	42.10 Detik	Memblokir Serangan	18:01:35	18:01:43	8 Detik
Percobaan Ke-15	42.24 Detik	Memblokir Serangan	18:04:08	18:04:13	5 Detik

Percobaan Ke-16	42.19 Detik	Memblokir Serangan	18:06:33	18:06:44	11 Detik
Percobaan Ke-17	42.29 Detik	Memblokir Serangan	18:09:05	18:09:14	9 Detik
Percobaan Ke-18	45.08 Detik	Memblokir Serangan	18:13:09	18:13:14	5 Detik
Percobaan Ke-19	42.25 Detik	Memblokir Serangan	18:15:31	18:15:45	14 Detik
Percobaan Ke-20	45.08 Detik	Memblokir Serangan	18:17:58	18:18:13	15 Detik
Percobaan Ke-21	42.11 Detik	Memblokir Serangan	18:20:31	18:20:44	13 Detik
Percobaan Ke-22	42.11 Detik	Memblokir Serangan	18:22:42	18:22:55	13 Detik
Percobaan Ke-23	45.34 Detik	Memblokir Serangan	18:25:17	18:25:28	11 Detik
Percobaan Ke-24	42.09 Detik	Memblokir Serangan	18:27:35	18:27:42	7 Detik
Percobaan Ke-25	45.46 Detik	Memblokir Serangan	18:29:58	18:30:13	14 Detik
Percobaan Ke-26	45.14 Detik	Memblokir Serangan	18:33:06	18:33:15	9 Detik
Percobaan Ke-27	42.15 Detik	Memblokir Serangan	18:35:40	18:35:56	16 Detik
Percobaan Ke-28	42.15 Detik	Memblokir Serangan	18:40:44	18:40:52	8 Detik
Percobaan Ke-29	45.35 Detik	Memblokir Serangan	18:43:48	18:43:58	10 Detik
Percobaan Ke-30	45.14 Detik	Memblokir Serangan	18:46:55	18:47:10	15 Detik

3. Pengujian Serangan *Brute force* FTP Dengan xHydra
   Pengujian serangan bruteforce FTP nantinya akan dilakukan percobaan serangan masih sama sebanyak 30 kali supaya dapat mengetahui apakah IPS mampu untuk memblokir bruteforce FTP dan memonitoring secara *real-time*. Pada pengujian nantinya akan disiapkan 36 list password palsu dan 1 password asli untuk diujicoba menggunakan tools xHydra. Hasil dari pengujian serangan akan ditampilkan dalam bentuk tabel.

Tabel 3 Pengujian Serangan *Brute force* Dengan Tools xHydra

Pengujian Serangan	Durasi Waktu Penyerangan	Hasil Serangan (IPS)	Waktu Log	Waktu Peringatan Monitoring	Rentan Waktu Alert
Percobaan Ke-1	67 Detik	Memblokir Serangan	16:07:09	16:07:10	3 Detik
Percobaan Ke-2	92 Detik	Memblokir Serangan	16:16:16	16:16:18	2 Detik
Percobaan Ke-3	129 Detik	Memblokir Serangan	16:19:00	16:20:02	2 Detik
Percobaan Ke-4	172 Detik	Memblokir Serangan	16:23:39	16:23:41	2 Detik
Percobaan Ke-5	172 Detik	Memblokir Serangan	16:29:00	16:29:03	3 Detik
Percobaan Ke-6	5 Detik	Memblokir Serangan	16:32:35	16:32:45	10 Detik
Percobaan Ke-7	158 Detik	Memblokir Serangan	16:38:11	16:38:15	4 Detik
Percobaan Ke-8	114 Detik	Memblokir Serangan	16:44:07	16:45:15	8 Detik
Percobaan Ke-9	67 Detik	Memblokir Serangan	10:14:46	10:14:50	4 Detik
Percobaan Ke-10	70 Detik	Memblokir Serangan	10:17:16	10:17:20	4 Detik

Percobaan Ke-11	109 Detik	Memblokir Serangan	10:20:00	10:20:03	3 Detik
Percobaan Ke-12	68 Detik	Memblokir Serangan	10:23:33	10:23:36	3 Detik
Percobaan Ke-13	82 Detik	Memblokir Serangan	10:44:50	10:44:51	1 Detik
Percobaan Ke-14	116 Detik	Memblokir Serangan	10:48:03	10:48:18	15 Detik
Percobaan Ke-15	128 Detik	Memblokir Serangan	10:51:53	10:51:56	3 Detik
Percobaan Ke-16	82 Detik	Memblokir Serangan	10:55:16	10:55:21	5 Detik
Percobaan S Ke-17	97 Detik	Memblokir Serangan	10:58:21	10:58:27	6 Detik
Percobaan Ke-18	97 Detik	Memblokir Serangan	11:01:09	11:01:15	6 Detik
Percobaan Ke-19	85 Detik	Memblokir Serangan	11:07:28	11:07:35	7 Detik
Percobaan Ke-20	74 Detik	Memblokir Serangan	11:10:24	11:10:29	5 Detik
Percobaan Ke-21	109 Detik	Memblokir Serangan	11:12:59	11:13:06	5 Detik
Percobaan Ke-22	67 Detik	Memblokir Serangan	11:16:07	11:16:12	5 Detik
Percobaan Ke-23	137 Detik	Memblokir Serangan	11:19:50	11:19:51	1 Detik
Percobaan Ke-24	75 Detik	Memblokir Serangan	11:27:27	11:27:38	11 Detik
Percobaan Ke-25	78 Detik	Memblokir Serangan	11:33:31	11:33:36	5 Detik
Percobaan Ke-26	97 Detik	Memblokir Serangan	11:37:11	11:37:23	12 Detik
Percobaan Ke-27	128 Detik	Memblokir Serangan	15:24:42	15:24:50	8 Detik
Percobaan Ke-28	115 Detik	Memblokir Serangan	15:28:55	15:29:03	8 Detik
Percobaan Ke-29	94 Detik	Memblokir Serangan	15:32:10	15:32:20	10 Detik
Percobaan Ke-30	134 Detik	Memblokir Serangan	15:35:40	15:35:50	10 Detik

4. Pengujian Serangan ICMP *Flood* Dengan Tools Hping3

Pada pengujian Serangan ICMP *Flood* akan menggunakan tools Hping3, Pengujian serangan akan diarahkan menuju router MikroTik dengan memberi permintaan paket "*echo request*" dalam jumlah yang banyak, tujuan dari serangan tersebut yaitu membuat router MikroTik yang didalamnya terdapat FTP server menjadi lambat dalam merespon *request* dari *client* atau membuat MikroTik menjadi *down* karena *resource* menjadi sangat besar. Pengujian dilakukan sebanyak 15 kali sebelum penerapan IPS dan 15 kali sesudah menerapkan IPS, lalu dalam pengujian jumlah pengiriman paket "ICMP" diatur menjadi 3 tahap yaitu 300.000 paket, 500.000 paket, 700.000 paket dengan speed --*faster* pada hping3.

Tabel 4 Pengujian Serangan ICMP Flood Sebelum Penerapan IPS

Pengujian Serangan	Metode Serang	Packet	CPU Load
Percobaan Ke-1	ICMP *Flood*	300000	71%
Percobaan Ke-2	ICMP *Flood*	300000	77%
Percobaan Ke-3	ICMP *Flood*	300000	64%
Percobaan Ke-4	ICMP *Flood*	300000	66%

Percobaan Ke-5	ICMP *Flood*	300000	70%
Percobaan Ke-6	ICMP *Flood*	500000	61%
Percobaan Ke-7	ICMP *Flood*	500000	63%
Percobaan Ke-8	ICMP *Flood*	500000	82%
Percobaan Ke-9	ICMP *Flood*	500000	68%
Percobaan Ke-10	ICMP *Flood*	500000	75%
Percobaan Ke-11	ICMP *Flood*	700000	72%
Percobaan Ke-12	ICMP *Flood*	700000	76%
Percobaan Ke-13	ICMP *Flood*	700000	81%
Percobaan Ke-14	ICMP *Flood*	700000	100%
Percobaan Ke-15	ICMP *Flood*	700000	99%

Tabel 5 Pengujian Serangan ICMP Flood Sesudah Penerapan IPS

Pengujian Serangan	Metode Serang	Packet	CPU Load	Hasil Serangan (IPS)	Waktu Log	Waktu Peringatan Monitoring	Rentan Waktu Alert
Percobaan Ke-1	ICMP *Flood*	300000	18%	Memblokir Serangan	17:47:11	17:47:34	23 Detik
Percobaan Ke-2	ICMP *Flood*	300000	20%	Memblokir Serangan	20:14:36	20:14:56	20 Detik
Percobaan Ke-3	ICMP *Flood*	300000	29%	Memblokir Serangan	20:21:22	20:21:39	17 Detik
Percobaan Ke-4	ICMP *Flood*	300000	21%	Memblokir Serangan	20:59:05	20:59:10	5 Detik
Percobaan Ke-5	ICMP *Flood*	300000	20%	Memblokir Serangan	21:03:18	21:03:28	10 Detik
Percobaan Ke-6	ICMP *Flood*	500000	13%	Memblokir Serangan	21:15:23	21:15:28	5 Detik
Percobaan Ke-7	ICMP *Flood*	500000	19%	Memblokir Serangan	21:21:11	21:21:26	5 Detik
Percobaan Ke-8	ICMP *Flood*	500000	15%	Memblokir Serangan	21:24:58	21:25:13	15Detik
Percobaan Ke-9	ICMP *Flood*	500000	25%	Memblokir Serangan	21:32:35	21:32:40	5 Detik
Percobaan Ke-10	ICMP *Flood*	500000	24%	Memblokir Serangan	22:15:19	22:15:24	5 Detik
Percobaan Ke-11	ICMP *Flood*	700000	13%	Memblokir Serangan	22:21:09	22:21:24	13 Detik
Percobaan Ke-12	ICMP *Flood*	700000	16%	Memblokir Serangan	22:28:18	22:28:28	10 Detik
Percobaan Ke-13	ICMP *Flood*	700000	17%	Memblokir Serangan	22:33:09	22:33:24	13 Detik
Percobaan Ke-14	ICMP *Flood*	700000	23%	Memblokir Serangan	22:37:49	22:37:54	5 Detik
Percobaan Ke-15	ICMP *Flood*	700000	36%	Memblokir Serangan	22:44:23	22:44:27	4 Detik

4. KESIMPULAN

Dari hasil penelitian yang dilakukan oleh peneliti dengan judul analisis dan implementasi kemanan jaringan *file transfer protocol* (FTP) menggunakan *intrusion prevention* system (IPS)

pada MikroTik. Sistem yang dibangun dapat berjalan dengan lancar dan berjalan dengan baik sesuai dengan tujuan dari penelitian ini. Adapun kesimpulan yang didapatkan yaitu sebagai berikut :

1. Dari pengujian yang dilakukan menggunakan 3 serangan yaitu : *Brute force* FTP, DDoS ICMP *flood*, dan *Port scanning*. Mendapatkan hasil sebagai berikut : Pertama serangan *brute force* FTP menggunakan tools ncrack dan xHydra dengan pengujian sebanyak 30 kali, lalu durasi waktu serangan rata-rata yang diperlukan yaitu 50,41 detik dan 100,6 detik. Hasil yang didapatkan setelah menerapkan rules IPS pada *firewall* yaitu serangan *brute force* FTP tidak mampu mendapatkan akses username dan password FTP atau tingkat keberhasilanya adalah 0. Kedua pada serangan *port scanning* menggunakan aplikasi znmap dengan pengujian sebanyak 30 kali, lalu rata-rata waktu yang diperlukan scanning yaitu 103.3 detik. Didapatkan hasil dari 30 kali pengujian 7 kali status pada port 21 terbuka, walaupun status port 21 terbuka rules IPS pada *firewall* masih tetap berjalan dan melakukan prevention dengan memblacklist dan mendrop IP penyerang maka serangan yang dilakukan tetap gagal. Ketiga pada serangan DDoS ICMP *flood* menggunakan tools Hping3 dengan pengujian 15 kali sebelum dan sesudah menerapkan IPS, hasil yang didapat yaitu sebelum menerapkan rules IPS CPU load saat terjadi serangan naik dari 63% - 100% yang membuat server menjadi lambat saat menerima request client dan server down. Hasil setelah menerapkan rules IPS pada *firewall* CPU load hanya naik 13% - 36% saat terjadi serangan yang membuat server tetap stabil walaupun terjadi serangan dan membuat request client ke server tetap berjalan lancar.
2. Respon time yang dibutuhkan untuk melakukan prevention dan mengirim pesan alert peringatan ke gmail untuk administrator menggunakan percobaan pengujian 3 serangan dengan menerapkan sistem IPS pada *firewall* MikroTik didapatkan hasil respon time yaitu 2 Detik – 5 Detik, hasil respon time tersebut bisa digolongkan sebagai *real-time*

DAFTAR PUSTAKA

[1] A. T. P. Tambunan, A. P. Lubis, and S. Anggraini, “Perancangan Sistem Keamanan File Transfer Protocol Dengan Secure Socket Layer Pada Server Centos 7,” *J-Com (Journal Comput.*, vol. 1, no. 2, pp. 95–102, 2021, doi: 10.33330/j-com.v2i1.1206.

[2] S. Khadafi, Y. D. Pratiwi, and E. Alfianto, “KEAMANAN FTP SERVER BERBASISKAN IDS DAN IPS,” vol. 6, no. 1, pp. 11–24, 2021.

[3] H. Alamsyah, R. -, and A. Al Akbar, “Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System,” *JOINTECS (Journal Inf. Technol. Comput. Sci.*, vol. 5, no. 1, p. 17, 2020, doi: 10.31328/jointecs.v5i1.1240.

[4] A. R. A. F. E. Laila, “Implementasi Intrusion Prevention System (IPS) Pada Keamanan Jaringan Dengan Notifikasi Berbasis Telegram di Jurusan Teknik Komputer,” *J. Lap. Akhir Tek. Komput.*, vol. 1, no. 1, pp. 10–17, 2021.

[5] S. Suryayusra and D. Irawan, “Perbandingan Intrusion Prevention System (Ips) Pada Linux Ubuntu Dan Linux Centos,” *J. Teknol. Inf. Mura*, vol. 12, no. 02, pp. 131–144, 2020, doi: 10.32767/jti.v12i02.1023.

[6] T. Prasetyo, “Pengamanan Jaringan Komputer Dengan Intrusion Prevention System (IPS) Berbasis Sms Gateway,” vol. 2, no. 6, pp. 1–13, 2022.

[7] E. S. R. O. B. Langobelen, Y. Rachmawati, and C. Iswahyudi, “Analisis Dan Optimasi Dari Simulasi Keamanan Jaringan Menggunakan Firewall Mikrotik Studi Kasus Di Taman Pintar Yogyakarta,” *J. JARKOM*, vol. 7, no. 2, pp. 95–102, 2019.

[8] A. Harbani and M. Apriani, “Pengembangan Notifikasi Email Untuk Keamanan Port Menggunakan Metode Port Knocking,” *Teknois J. Ilm. Teknol. Inf. dan Sains*, vol. 8, no.

2, pp. 25–36, 2019, doi: 10.36350/jbs.v8i2.12.

[9] S. Khadafi, S. Nurmuslimah, and F. K. Anggakusuma, "Implementasi Firewall Dan Port Knocking Sebagai Keamanan Data Transfer Pada Ftp Server Berbasiskan Linux Ubuntu Server," *Nero*, vol. 4, no. 3, pp. 181–188, 2019, [Online]. Available: https://nero.trunojoyo.ac.id/index.php/nero/article/view/137

[10] R. E. Susanti, A. W. Muhammad, and W. A. Prabowo, "Implementasi Intrusion Prevention System (IPS) OSSEC dan Honeypot Cowrie," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 11, no. 1, pp. 73–78, 2022, doi: 10.32736/sisfokom.v11i1.1246.

[11] Zulkarnain, "Analisis Keamanan FTP server Menggunakan Serangan Man-In-The-Middle Attack," *Telcomatics*, vol. 5, no. 1, pp. 12–18, 2020, doi: 10.37253/telcomatics.v5i1.851.

[12] A. Muhaimi, I. P. Hariyadi, and A. Juliansyah, "Analisa Penerapan Intrusion Prevention System (IPS) Berbasis Snort Sebagai Pengaman Server Internet Yang Terintegrasi Dengan Telegram," *J. Bumigora Inf. Technol.*, vol. 1, no. 2, pp. 167–176, 2019, doi: 10.30812/bite.v1i2.611.

[13] R. Kurniawan and F. Prakoso, "Implementasi Metode IPS (Intrusion Prevention System) dan IDS (Intrusion Detection System) untuk Meningkatkan Keamanan Jaringan," *Sentinel*, vol. 3, no. 1, pp. 231–242, 2020, doi: 10.56622/sentineljournal.v3i1.20.

[14] M. Ilham Ilahi, S. Pd, MTCNA, *ADMINISTRASI INFRASTRUKTUR JARINGAN.pdf*. Surabaya, 2020. [Online]. Available: https://www.google.co.id/books/edition/ADMINISTRASI_INFRASTRUKTUR_JARINGAN/r8LxDwAAQBAJ?hl=id&gbpv=0

[15] Rakhmat Dwi Jayanto, "Rancang Bangun Sistem Monitoring Jaringan Menggunakan Mikrotik Router OS," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 3, no. 4, pp. 391–395, 2019.

[16] A. . R. S. Bayu, "Implementasi Keamanan. Jaringan. Lan Menggunakan. Mikrotik. Dengan$ Metode. Firewall. Filtering* 1,2," vol. 3, no. 1, 2022.

[17] H. Suhendi and W. D. Cahyo, "JARINGAN MENGGUNAKAN SNORT SEBAGAI INTRUSION PREVENTION SYSTEM (IPS) PADA JARINGAN INTERNET," vol. 03, no. 02, pp. 60–68, 2021.