METODOLOGI RISET TEKNOLOGI INFORMASI

“TUGAS 2”

Dosen Pengampu : Ika Menarianti, S.Kom.,M.Kom.

Disusun oleh :

Ardiyansyah R

PMM220085

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK DAN INFORMATIKA

UNIVERSITAS PGRI SEMARANG

2022

TELAAH PUSTAKA

Topik Penelitian
Kemanan Sistem Jaringan
Judul Karya Ilmiah
1. Perancangan dan Analisis Sistem Keamanan Jaringan Komputer Menggunakan SNORT 2. Sistem Keamanan Jaringan *Local Area Network* Menggunakan Teknik *De-Militarized Zone*
Identifikasi Masalah
1. Perancangan dan Analisis Sistem Keamanan Jaringan Komputer Menggunakan SNORT a. Serangan dari pihak-pihak yang tidak bertanggung jawab atau disebut *hacker.* b. Banyak jenis serangan pada sistem komputer yang dituju, tapi jenis *port scanning* dan DoS merupakan jenis serangan yang sering dilakukan. c. Sistem keamanan *firewall* belum mampu menjamin keamanan sistem komputer sepenuhnya d. Sistem operasi Windows yang terkena virus *ransomeware* yang mengunci data pada PC e. Email yang berisi virus *worm* yang ingin mencuri data perusahaan. 2. Sistem Keamanan Jaringan *Local Area Network* Menggunakan Teknik *De-Militarized Zone* a. Kelemahan yang terdapat pada jaringan komputer jika tidak dilindungi dan dijaga dengan baik akan menyebabkan kerugian berupa kehilangan data, kerusakan sistem server, tidak maksimal dalam melayani user atau bahkan kehilangan aset-aset berharga institusi. b. Beberapa organisasi lebih mendahulukan tampilan dan lain sebagainya dibandingkan masalah keamanan. c. DDoS *attack*, serangan *hacker*, virus, trojan yang semuanya merupakan ancaman yang tidak bisa diabaikan. d. Serangan yang paling sering digunakan adalah *Port scanning* dan DoS
Ruang Lingkup Penelitian
1. Ruang lingkup penelitian pada jurnal pertama yaitu perancangan dan penganalisaan sistem keamanan komputer dengan menggunakan perangkat lunak SNORT pada PT. Primanufacture Indonesia. 2. Ruang lingkup penelitian pada jurnal kedua yaitu pengimplementasian sistem keamanan

jaringan LAN menggunakan teknik DMZ pada layanan server jaringan komputer Universitas Islam "45".

Metode Penelitian

1. Metode yang digunakan pada jurnal yang pertama adalah PPDIOO. PPDIOO adalah sebuah metode perancangan jaringan yang dirancang untuk mendukung berkembangnya jaringan. PPDIOO terdiri dari beberapa tahapan, yaitu *Prepare, Plan, Design, Implement, Operate*, dan *Optimize*.
2. Metode yang digunakan pada jurnal yang menggunakan metode pengembangan (*development research*) dengan pendekatan model 4D yaitu *Define* (pendefinisian), *Design* (perancangan), *Develop* (pengembangan/implementasiana), *Disseminate* (uji coba).

Langkah Penyelesaian

1. Perancangan dan Analisis Sistem Keamanan Jaringan Komputer Menggunakan SNORT
   a. *Prepare phase* : melakukan persiapan membangun sistem keamanan jaringan menggunakan SNORT, yaitu mulai mempersiapkan kebutuhan, konsep, dan strategi finansial.
   b. *Plane phase* : melakukan identifikasi hal-hal yang harus dipenuhi berdasarkan tujuan, fasilitas, dan kebutuhan pengguna.
   c. *Design phase* : melakukan desain jaringan yang terperinci yang akan memenuhi persyaratan teknis.
   d. *Implement phase* : melakukan instalasi dan konfigurasi yang sesuai dengan spesifik desain, dengan menginstal *software* dan konfigurasi dan pemilihan serangan yang diuji coba pada sistem jaringan komputer.
   e. *Operational phase* : mempertahankan ketahanan kegiatan jaringan, dimana pada fase ini meliputi pengolahan komponen jaringan, melakukan pemeliharaan sistem jaringan, mengelola kinerja jaringan, dan mengoreksi jika ada kesalahan pada jaringan. Pada fase ini, aplikasi SNORT dijalankan sesuai dengan rencana yang telah ditentukan.
   f. *Optimize phase* : Fase Optimalisasi, administrator jaringan mengidentifikasi dan menyelesaikan masalah yang sedang terjadi.
2. Sistem Keamanan Jaringan *Local Area Network* Menggunakan Teknik *De-Militarized Zone*
   a. Analisa kebutuhan : Tahap ini merupakan identifikasi masalah dari sistem

keamanan jaringan di Unisma. Dari masalah yang ada kemudian diselesaikan dengan implementasi metode DMZ pada jaringan local.

b. Perancangan : Dalam tahap perancangan dilakukan penentuan topologi dan konfigurasi jaringan.
c. Implementasi : Tahap implementasi merupakan tahap yang melakukan setting layanan DMZ pada server.
d. Pengujian : Tahap pengujian dilakukan untuk mengetahui sejauh mana implementasi dilakukan. Dalam penelitian dilakukan 2 pengujian yaitu pengujian tanpa menggunakan DMZ dan pengujian dengan menggunakan DMZ.

Hasil dan Pembahasan

1. Perancangan dan Analisis Sistem Keamanan Jaringan Komputer Menggunakan SNORT
   a. Hasil analisa pada penelitian terdapat penambahan *rules* yang dibuat untuk mendeteksi jika adanya ping ke komputer server dan jika ada yang melakukan percobaan serangan ke komputer server.
   b. Aplikasi SNORT mampu mencatat setiap paket yang telah dideteksi dalam bentuk *file* dan paket yang akan disimpan ke dalam *disk* komputer.
   c. Saat dilakukan penyerangan DDoS *attack*, maka grafik pada CPU sangat tinggi yang menyebabkan komputer akan berkerja secara lebih maksimal karena terlalu banyak paket yang menuju komputer server. Ketika penyerangan dari komputer *attack*er diberhentikan menyebabkan grafik performa dari komputer server lebih rendah dan komputer server dapat melakukan pemrosesan secara lebih stabil.
   d. Kesimpulannya bahwa sistem kemanan jaringan komputer yang menggunakan aplikasi SNORT dapat membantu administrator untuk meminimalisir terjadi serangan dari pihak-pihak yang tidak bertanggung jawab.
2. Sistem Keamanan Jaringan *Local Area Network* Menggunakan Teknik *De-Militarized Zone*
   a. Hasil yang diperoleh dari hasil pengujian yang telah dilakukan yaitu berupa data perbandingan *loging server* saat terjadi DoS *attack* dari tiga jenis pengujian DoS *attack* sebelum dan sesudah server diimplementasi teknik DMZ, hasil perbandingan tersebut
   b. Data Perbandingan ICMP *Flooding Attack* : perbandingan hasil loging ICMP *flooding attack* pada server tanpa DMZ rata-rata menunjukan jumlah *packet* yang diterima sebanyak 16391,4 *packet* dan rata-rata *packet* yang diterima saat DMZ

sebanyak 32,2 *packet*, sehingga didapatkan perbandingan penurunan jumlah *packet* saat terjadi DoS *attack* sebesar 16359,2 *packet* setelah implementasi teknik DMZ, artinya DMZ berhasil melakukan filter sebesar 16359,2 *packet* pada DoS *attack* tersebut.

c. Data Perbandingan UDP *Flooding Attack* : perbandingan hasil loging UDP *flooding attack* pada server tanpa DMZ rata-rata menunjukan jumlah *packet* yang diterima sebanyak 7640,7 *packet* dan rata-rata *packet* yang diterima saat DMZ sebanyak 34,2 *packet*, sehingga didapatkan perbandingan penurunan jumlah *packet* saat terjadi DoS *attack* sebesar 7606,5 *packet* setelah implementasi teknik DMZ, artinya DMZ berhasil melakukan filter sebesar 7606,5 *packet* pada DoS *attack* tersebut.

d. Data Perbandingan *Syn Flooding Attack* : hasil loging *Syn flooding attack* pada server tanpa DMZ rata-rata menunjukan jumlah *packet* yang diterima sebanyak 7386 *packet* dan rata-rata *packet* yang diterima saat DMZ sebanyak 7407,8 *packet*, sehingga didapatkan perbandingan jumlah *packet* yang hampir sama pada server sebelum dan setelah implementasi teknik DMZ, artinya DMZ tidak berhasil melakukan filter pada jenis DoS *Syn flooding attack* tersebut karena server masih terkena *flooding*.

e. Kesimpulannya adalah teknik jaringan DMZ dapat diimplementasikan pada sistem jaringan komputer dengan dbaikm dan implementasi teknik DMZ pada layanan server jaringan LAN dapat melakukan filter terhadap serangan DoS jenis ICMP *flooding attack* dan UDP *flooding attack*.

f. Saran yang diberikan yaitu penggunaan spesifikasi *hardware* yang maksimal dan memaksimalkan fungsi *firewall filtering* pada router *firewall* Mikrotik untuk memblokir *port* yang masih mungkin untuk disusupi.

URL Link

1. https://www.mendeley.com/catalogue/api/fulltext-resolver/44caec93-f6c1-364e-b02e-c4b296a016f3/?t=1668569238457
2. https://www.mendeley.com/catalogue/api/fulltext-resolver/8ed5cf82-1533-3cd9-be1e-8bc290ecfd14/?t=1668569321105