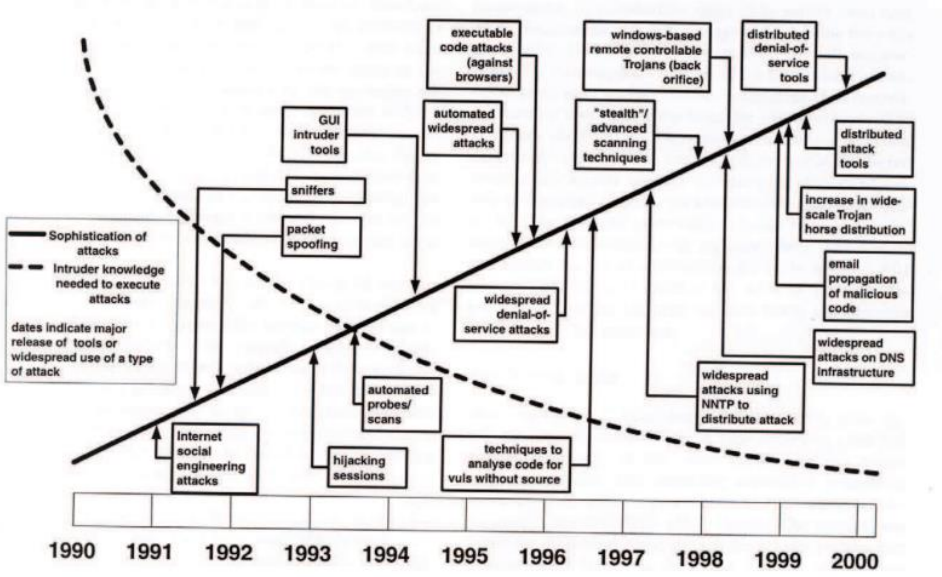
BAB I. PENDAHULUAN

A. Latar Belakang Masalah

Pesatnya perkembangan teknologi informasi saat ini menyebabkan meningkatnya pengiriman data dan informasi secara global. Selain tingginya manfaat yang dirasakan, tingkat risiko dan ancaman penyalahgunaan teknologi informasi juga semakin tinggi dan kompleks. Organisasi menjadi lebih rentan terhadap ancaman atau serangan jaringan atau keamanan informasi yang disebabkan oleh berbagai sumber baik dari aktivitas personil internal atau serangan peretas (Jouini, Rabai, & Aissa, 2014). Beraneka ragam ancaman atau serangan jaringan atau sistem informasi hadir berpotensi menggangu kinerja dan layanan organisasi seperti insider attacks, poor configurations, lack of contingency, masquerading, man-in-the-middle-attack, virus attack atau denial of service attack (Bhatia & Sehrawat, 2014).

Tanpa perlindungan yang memadai berupa keamanan jaringan atau sistem informasi, organisasi berisiko kehilangan aset informasi mereka. Keamanan jaringan atau sistem informasi adalah proses dimana aset informasi dilindungi mencakup perlindungan atas kerahasiaan, integritas, dan ketersediaan aset informasi tersebut (Alabady, 2009). Keamanan jaringan atau sistem informasi terdiri dari seperangkat kebijakan dan pelaksanaan yang diterapkan untuk mencegah dan memantau akses tidak sah, modifikasi dalam sistem, penyalahgunaan, atau penolakan jaringan komputer dan sumber daya yang dapat diakses jaringan (Pawar & Anuradha, 2015)

Dalam beberapa tahun terakhir, Internet dan jaringan secara keseluruhan telah mengalami peningkatan yang luar biasa dalam perannya dalam masyarakat kita terutama di sektor pemerintahan dan bisnis. Selama kali ini, kami juga menyaksikan serangan yang semakin canggih diluncurkan oleh penyusup, yang tentu saja dimotivasi oleh tujuan finansial dan politik. Jenis serangan dihasilkan menggunakan alat dan skrip eksploit yang: tersedia secara bebas di internet dan banyak digunakan oleh pengguna jahat pemula untuk meluncurkan serangan di dalam jaringan. Mc Hugh juga memberikan bukti lebih lanjut dengan menyatakan bahwa “siapa pun dapat menyerang situs Internet menggunakan yang tersedia” alat intrusi dan skrip eksploitasi yang memanfaatkan kerentanan yang diketahui secara luas (Mc Hugh dkk, 2000). Oleh karena itu peningkatan jumlah eksploitasi alat mungkin telah memengaruhi jumlah penyerang pemula di dalam internet.

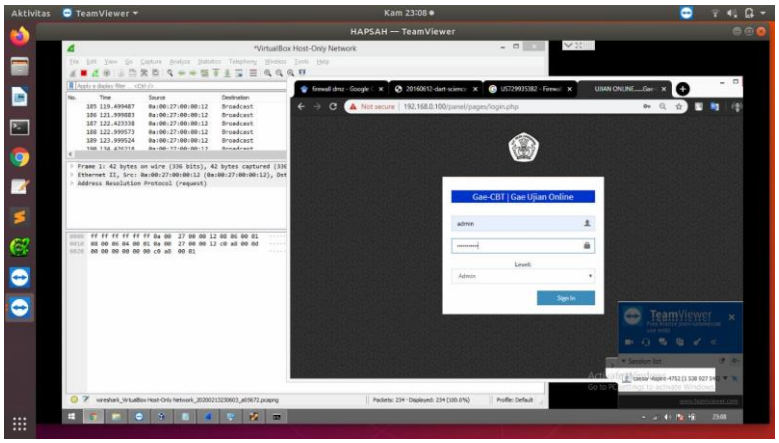


Gambar 1.1 Statistik serangan jaringan
(Faizal, Shahrin, Asrul, Fairuz & Robbie, 2008)

B. Masalah Penilitian

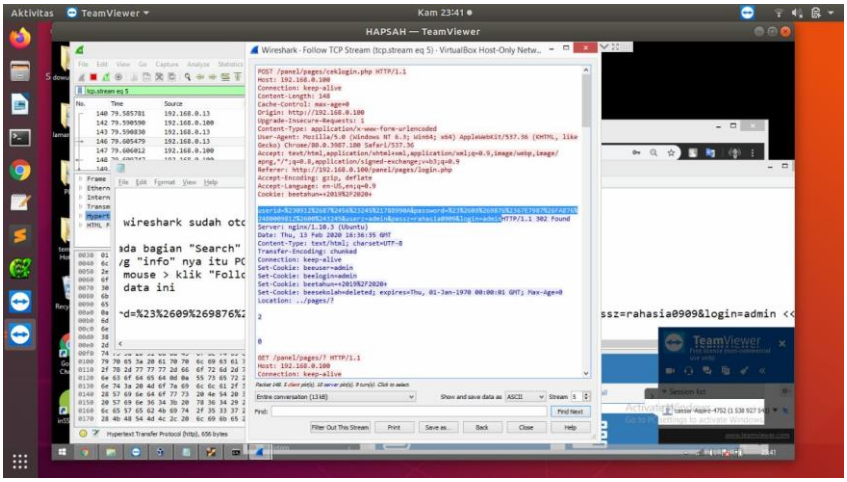
Para ahli jaringan menyatakan bahwa jaringan komputer di SMK Bina Informatika yang didalamnya terdapat komputer server lokal dinyatakan tidak aman karena hasil dari ujicoba serangan yang telah dijalankan terhadap jaringan tersebut adalah akun administrator ketika mengakses server terlacak.

Uji coba *packet sniffer* dengan cara merekam jejak *login* administrator. Pihak yang terlibat dalam ujicoba ini ialah, administrator dan ahli jaringan. Ketika ahli jaringan terhubung dengan jaringan yang dimana terdapat server didalamnya, kemudian ahli jaringan itu melakukan serangan sniffer kepada server dengan menggunakan tools wireshark. Pada saat administrator melakukan *login* akses di tampilan halaman *login* administrator dengan menekan tombol *login* setelah memasukan *username* dan *password*.



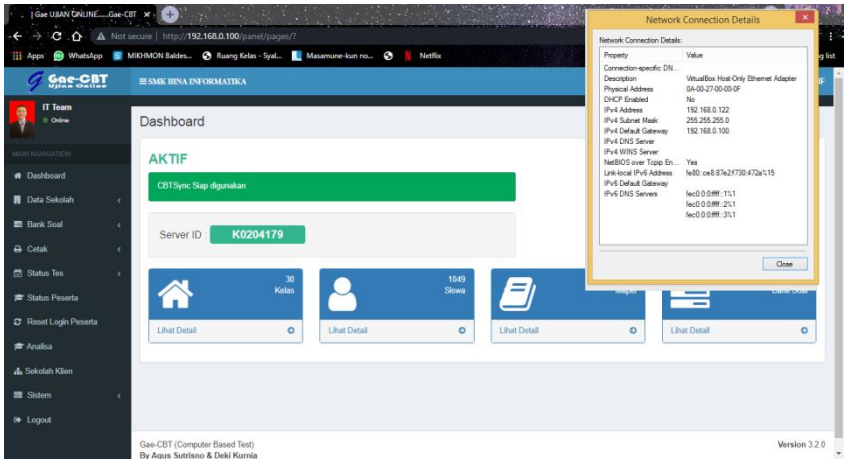
Gambar 1.2 ahli jaringan merekam jejak login administrator

Setelah administrator menekan tombol *login*, ahli jaringan akan mendapatkan berbagai informasi trafirk akses dari komputer yang sedang beraktivitas di lalulintas jaringan tersebut. Untuk mengatahui informasi akses *login* hanya cari baris “POST” pada menu info. POST adalah variabel fungsi standar dalam bahasa pemograman PHP. POST berfungsi untuk mengumpulkan jumlah data didalam form, seperti mengumpulkan nilai akses *login* di form *login*. Data yang ditransfer menggunakan metode POST terlihat samar atau bahkan tidak terlihat oleh orang lain namun tidak ada batasan pada keseluruhan informasi untuk mengirim. Namun untuk kasus serangan jaringan *packet sniffer* sebuah informasi yang dikumpulkan POST dapat terlihat informasi *login* berupa *username* dan *password* oleh *tools* pendukung.



Gambar 1.3 ahli jaringan mendapatkan informasi login administrator

Efek utama dari serangan jaringan komputer berupa bocornya data informasi yang tersimpan pada server. Selain itu untuk jenis serangan jaringan yang sangat berbahaya dapat mengakibatkan rusaknya data pada server, sehingga hal ini sangat merugikan pengguna ataupun *end user* yang sedang mengakses. Aktivitas mencuri data, membenani jaringan, merusak sistem keamanan, merubah informasi dan segala hal yang dapat merugikan pemilik data pada jaringan komputer adalah suatu tindak ilegal dan secara hukum pengadilan dapat dijatuhkan sangsi.



Gambar 1.4 ahli jaringan login halaman admin pada komputer siswa

Lemahnya kemanan server pada jaringan menyebabkan kerugian yang cukup besar, pengaruh dari kerugian tersebut berupa akun milik administrator yang diketahui oleh penyeludup **(Gambar 1.3)**, penyeludup mendapatkan informasi penting didalam halaman administrator yang berisi bank soal, kunci jawaban soal dan data penting lainnya. Data penting lainnya seperti daftar nama ujian siswa yang dapat dikendalikan untuk menghentikan ujian pada siswa tertentu atau menyeluruh, mengubah nilai hasil jawaban dan data penting lainnya yang tentunya sangat merugikan. **(Gambar 1.4)**

Demilitarized Zone (DMZ) merupakan mekanisme untuk melindungi sistem internal dari serangan pihak-pihak yang ingin memasuki sistem tanpa mempunyai hak akses. Dalam keamanan jaringan komputer, DMZ merupakan fisik atau logis *subnetwork* yang berisi dan mengekspos layanan eksternal/internal menghadap organisasi untuk jaringan yang lebih besar dan dipercaya.

Tujuan dari DMZ adalah menambahkan lapisan tambahan keamanan untuk organisasi jaringan area lokal (LAN), seorang penyerang eksternal hanya memiliki akses langsung ke peralatan di DMZ, daripada bagian lain dari jaringan terutama server. Nama DMZ ini berasal dari istilah "zona demiliterisasi", yaitu sebuah daerah antara negara-negara bangsa di mana operasi militer tidak diizinkan. (Saleh Dwiyatno, Gunardi Wira Putra, Erni Krisnaningsih, 2015)

Wireshark adalah *tools* yang dipergunakan untuk menganalisa protokol jaringan dan mengaudit keamanan jaringan. Terdapat beberapa kemampuan Wireshark untuk memblokir lalu lintas pada jaringan LAN, mencuri informasi autentikasi, dan melakukan penyadapan aktif terhadap protokol-protokol jaringan yang sifatnya umum.

SMK Bina Informatika merupakan salah satu sistem pendidikan guna

meningkatkan sumber daya manusia. Dari pendidikan yang diterima anak bangsa dibangku sekolah, akan mampu mengubah pola pikir dan daya kreativitas anak untuk menciptakan anak yang bermutu bagi nusa dan bangsa. Wilayah SMK Bina Informatika meliputi beberapa ruang jaringan yang saling terhubung, terdapat

ruang laboratorium komputer yang digunakan untuk pembelajaran praktek dan ujian praktek serta digunakan untuk program sekolah seperti ujian sekolah semesteran.

1. Identifikasi Masalah
    a. Keamanan server yang masih rentan diserang penyeludup.

        Tingkat kemanan server yang belum kuat untuk menahan serangan-serangan dari penyeludup mengakses atau masuk kedalam jaringan tanpa ada hak akses. (**Gambar 1.3)**
    b. Layanan server yang bebas pakai.

        Layanan server berupa webserver bebas pakai, artinya baik siswa atau admin dapat mengaskes server secara langsung. **(Gambar 1.4)**
2. *Problem Statement*

    Keberadaaan Server yang rentan terhadap serangan jaringan dikarenakan jaringan yang bebas pakai dan terbuka sehingga orang lain atau penyudup bisa masuk kedalam jaringannya.
3. *Research Question*

    Pertanyaan – pertanyaan yang mendukung seputar permasahalan keamanan jaringan diantaranya:
    a. Bagaimana Penerapan Metode DMZ Untuk Kemanan Jaringan komputer di SMK Bina Informatika Bogor.
    b. Seberapa efekif perenerapan DMZ untuk keamanan jaringan komputer di SMK Bina Informatika Bogor.

C. Maksud dan Tujuan Penilitian

1. Maksud

    Untuk melakukan Penerapan Metode *Demilitarized Zone* (DMZ) Untuk Kemanan Jaringan Pada Pelaksanaan Ujian Akhir Semester di SMK Bina Informatika Bogor.
2. Tujuan
    a. Meningkatkan keamanan jaringan.
    b. Meminimalisir tingkat serangan jaringan dari macam – macam teknik penyerangan jaringan komputer.
    c. Mengembangkan alur trafik jaringan yang aman.

d. Menambahkan kemanan server dan efektifitas penerapan DMZ untuk keamanan jaringan di SMK Bina Informatika Bogor.

D. Spesifikasi Produk Yang diharapkan

Terciptanya sebuah sistem lalulitas jaringan berserta kemanan jaringan yang dapat diterapkan disemua kalangan baik diperusahan dan khususnya Jaringan sekolah manapun.

E. Signifikansi Penilitian

1. Kegunaan Penilitan

   Mengembangkan teknik komputasi untuk Penerapan Keamanan jaringan melalui pendekatan metode DMZ.

2. Manfaat Penilitian
   a. Manfaat teoritis : sumbangan pengetahuan dalam penerapa metode DMZ untuk keamanan jaringan.
   b. Manfaat praktis : membuat kenyamanan penggunaan jaringan dari kerentanan serangan jaringan.
   c. Manfaat Kebijakan pengembangan : dapat dijadikan acuan untuk pengembangan jaringan dimana pun.

F. Asumsi dan Keterbatasan Penilitian

1. Asumsi
   a. Penyerangan jaringan Komputer menggunakan Teknik *packet sniffing* dengan menggunakan aplikasi Wireshark.
   b. Penerapan Metode *Demilitarized Zone* (DMZ) pada sistem oprasi Linux Ubuntu 14.04
   c. Penyerangan melalui komputer siswa.
2. Keterbatasan Penilitian
   a. Server yang digunakan menggunakan sistem oprasi virtual.
   b. Penempatan server pada jaringan yang masih jaringan berbasis lokal.

G. Definisi Istilah

1. Penyerangan Jaringan, kegiatan yang mengaganggu sistem data sekolah dan merugikan sekolah dengan berbagai teknik cara.
2. *Hypertext Tranfer Protocol* (HTTP) adalah protokol jaringan lapisan aplikasi yang dikembangkan untuk membantu proses transfer antar komputer melalui web. Protokol ini sangat terdapat celah dan rentan dari serangan jaringan.
3. Server dalam latar belakang diatas merupakan sebuah sistem komputer yang menyediakan jenis layanan (*service*). Layanan server digunakan untuk pengguna

seperti administrator dan siswa. tertentu dalam sebuah jaringan komputer kondisi server harus didukung dengan spesifikasi yang tinggi dan tidak lupa akan keamanan server sendiri harus tangguh.

4. LAN (*Local Area Network*) adalah sebuah jaringan komputer dalam skala kecil seperti jaringan lab pada objek penilitian tepatnya di SMK Bina informatika, biasanya jaringan komputer yang teradapat disuatu perusahaan, beberapa bagian dari perusahaan, bahkan 1 ruangan dari bagian perusahaan.