DETEKSI PAKET SNIFFING PADA WIRELLES MENGGUNAKAN ARP WATCH

Aditya Ariyanto
D3 Manajemen Informatika, Fakultas Teknik, Universitas Negeri Surabaya, aditya.ariyanto27@gmail.com

Asmunin
Jurusan Teknik Informatika, Fakultas Teknik, Universitas Negeri Surabaya, asmunin@unesa.ac.id

Abstrak

Di era yang serba maju ini banyak tersebar luas fasilitas publik wireless access point secara gratis dan tanpa adanya keamanan jaringan sehingga banyak sekali ancaman atau serangan yang bisa dilakukan oleh pihak yang tidak bertanggung jawab dan akan merugikan pengguna fasilitas access point, sehingga privasi pengguna akan diketahui oleh para pihak yang tidak bertanggung jawab,

Permasalahan keamanan jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para pihak yang tidak bertanggung jawab, baik menggunakan jaringan Local Area Network (LAN) maupun wireless LAN. Salah satu ancaman yang akan di terima oleh pengguna fasilitas access point adalah serangan packet Sniffing.

Untuk mengatasi permasalahan ancaman keamanan jaringan di perlukan sebuah mekanisme keamanan jaringan untuk mendeteksi serangan packet sniffing dengan indikasi ARP spoofing pada jaringan menggunakan ARP Watch dan selanjutnya dibuat sebuah laporan pada tugas akhir "Deteksi Packet Sniffing Pada Wireless Menggunakan ARP Watch"

Kata Kunci : *Local Area Network (LAN), packet Sniffing, ARP Watch*

.

PENDAHULUAN

Teknologi *wireless* (tanpa kabel/nirkabel) saat ini berkembang pesat terutama dengan hadirnya perangkat teknologi dan komunikasi. Komputer, Notebook, dan Handphone mendominasi pemakaian teknologi *wireless*..

Di era yang serba maju ini banyak tersebar luas fasilitas publik *wireless access point* secara gratis dan tanpa adanya keamanan jaringan sehingga banyak sekali ancaman atau serangan yang bisa dilakukan oleh pihak yang tidak bertanggung jawab dan akan merugikan pengguna fasilitas *access point*, sehingga privasi pengguna akan diketahui oleh para pihak yang tidak bertanggung jawab,

Permasalahan keamanan jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para pihak yang tidak bertanggung jawab, baik menggunakan jaringan *Local Area Network (LAN)* maupun *wireless LAN*. Salah satu ancaman yang akan di terima oleh pengguna fasilitas *access point* adalah serangan *packet Sniffing.*

Untuk mengatasi permasalahan ancaman keamanan jaringan di perlukan sebuah mekanisme keamanan jaringan untuk mendeteksi serangan *packet sniffing* dengan indikasi *ARP spoofing* pada jaringan menggunakan *ARP Watch* dan selanjutnya dibuat sebuah laporan pada tugas akhir *"Deteksi Packet Sniffing Pada Wireless Menggunakan ARP Watch"*.

KAJIAN PUSTAKA

Jaringan Komputer

Menurut definisi, jaringan komputer adalah himpunan "interkoneksi" antara sejumlah komputer *autonomous.* Dalam bahasa popular dapat dijelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer (dan perangkat lain seperti printer, hub, dan sebagainya) yang saling terhubung satu sama lain melalui media perantara. Media perantara ini bisa berupa media kabel ataupun media tanpa kabel (nirkabel/wireless). (Syafrizal, hal : 2, 2005).

Fungsi dari jaringan komputer adalah untuk berbagi perangkat keras (*hardware*), perangkat lunak *(software)*, berbagi saluran komunikasi (internet), berbagai data dengan mudah, mencetak pada printer yang sama dan memudahkan komunikasi antar pemakai jaringan. Membangun jaringan komputer diperlukan adanya klasifikasi jaringan komputer, topologi (hubungan antar perangkat keras di dalam jaringan 8komunikasi data), komponen *hardware* dan s*oftware*, TCP/IP(*protocol)* yang digunakan, pemberian alamat komputer yang terhubung ke jaringan, dan model komunikasi data yang sesuai dengan arsitektur layer OSI (*Open System Interconnection*). (Elson Feza Satyagrahaprabu : 2008).

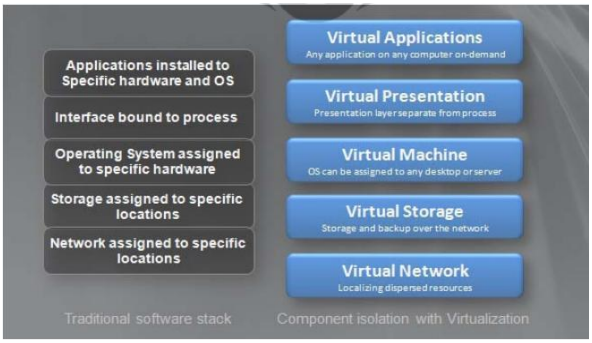
Virtualisasi

Pengertian virtualisasi dalam IT secara essensia melakukan isolasi terhadap satu sumber daya komputasi dengan yang lainnya. Dengan memisahgkan layer-layer yang berbeda dalam logic stack dimungkinkan

fleksibilitas yang lebih tinggi karena tidak diperlukan lagi konfigurasi tiap-tiap elemen untuk dapat bekerja bersama-sama.

Salah satu jalan yang paling baik untuk memahami virtualisai adalah dengan melighat ke mesin virtual, sistem operasi dan aplikasi dikemas bersama-sama untuk selanjutnya dilakukan *hosted* pada *server* fisikal yang menjalankan sistem operasi *host* atau *virtual layer.*

Virtual layer adalah sebuah layer perangkat lunak tipis yang menyediakan *basic interface* dengan perangkat keras. Konsep terpenting untuk memudahkan pemahaman adalah bahwa mesin virtual (OS + Aplikasi) dioperasikan secara independen dari OS pada *server*fisikal seakan–akan berada pada *discreate hardware*-nya sendiri. Hal ini memungkinkan beberapa mesin virtual dijalankan pada sebuah *server* fisikal. Untuk memperoleh gambaran *hardware/software tradisional stack* dan *logic stack virtual* dapat dilihat pada Gambar 2.1



2.1 Gambar Virtualisasi

Packet Sniffing

Packet sniffer adalah suatu mekanisme, baik perangkat lunak maupun perangkat keras yang digunakan untuk memperoleh informasi yang melewati jaringan komputer yang menggunakan protokol apa saja *(Ethernet, TCP/IP,IPX* atau yang lain). Kegunaan dari *packet sniffer* adalah membuat *NIC (Network Interface Card),* dalam hal ini *ethernet* dalam *mode promiscuous* sehingga dapat menangkap semua trafik di dalam jaringan. *Mode promiscuous* adalah mode di mana semua *workstation* pada jaringan komputer "mendengar" semua trafik, tidak hanya trafik yang dialamatkan kepada *workstation* itu sendiri. Jadi *workstation* pada *mode promiscuous* dapat "mendengarkan" trafik dalam jaringan yang dialamatkan kepada *workstation* lain.

Trafik jaringan ini (dengan tidak bergantung kepada protokol yang digunakan) terdiri dari paket-paket (dapat berupa data *IP* atau paket - paket *ethernet*) yang dipertukarkan oleh komputer - komputer pada tingkat yang sangat rendah dari sistem operasi antarmuka jaringan. Trafik ini kemungkinan mengandung data yang sangat penting, dan *sniffer* di desain untuk menangkap data tersebut untuk keperluan lebih lanjut (Purbo, 2011).

ARP

ARP adalah sebuah protokol dalam *TCP/IP Protocol Suite* yang bertanggung jawab dalam melakukan resolusi alamat IP ke dalam alamat Media *Access Control* (*MAC Address*). Pada kenyataannya, masih sedikit solusi yang tepat untuk mendeteksi maupun untuk mencegah aktivitas *sniffing* ini. Sistem deteksi penyusup jaringan yang ada saat ini umumnya mampu mendeteksi berbagai jenis serangan tetapi tidak mampu mengambil tindakan lebih lanjut Beberapa aksi *sniffing* lebih menakutkan lagi, biasanya *cracker* melakukan *sniffing* di tempat-tempat rawan, misalnya seorang karyawan melakukan *sniffing* di perusahaan tempat dia bekerja, atau seorang pengunjung warnet melakukan *sniffing* untuk mencuri password email, bahkan mencuri data transaksi bank melalui informasi kartu kredit.

Akibatnya tingkat kriminal *cyber* (cyber crime) meningkat dan merugikan banyak pihak cara untuk mengatasi *sniffing* aktif ini dapat dilakukan dengan pembentukan ARP *Static Table* sehingga *hacker* tidak dapat mengubah ARP dengan metode *ARP Poisoning*, Namun ada kendala dalam pembentukan ARP *static table*, yaitu tidak dapat mengetahui antara *IP/MAC address* mana yang fiktif (hasil ARP Poisoning) dan *IP/MAC* address yang asli.

ARP Spoofing

Address Resolution Protocol (ARP) spoofing, juga dikenal sebagai *ARP Poison Routing (APR),* adalah suatu teknik yang digunakan untuk menyerang *Ethernet* kabel atau jaringan nirkabel. *ARP Spoofing* dapat memungkinkan seorang penyerang untuk mengendus frame data pada jaringan area lokal (LAN), memodifikasi lalu lintas, atau menghentikan lalu lintas sama sekali (dikenal sebagai *denial of service attack*). Serangan hanya dapat digunakan pada jaringan yang benar - benar memanfaatkan ARP dan bukan metode lain resolusi alamat.

Solusi untuk mencegah *IP spoofing* adalah dengan cara mengamankan packet - packet yang ditransmisikan dan memasang *screening policies*. Enkripsi *Point – to - point* juga dapat mencegah user yang tidak mempunyai hak untuk membaca data/packet. Autentikasi dapat juga digunakan untuk menyaring *source* yang legal dan bukan *source* yang sudah di spoof oleh *attacker*. Dalam pencegahan yang lain, Admininistrator dapat menggunakan signature untuk paket - paket yang berkomunikasi dalam networknya sehingga meyakinkan bahwa paket tersebut tidak diubah dalam perjalanan.

Anti Spoofing rules (peraturan anti spoof) yang pada dasarnya memberitahukan server untuk menolak packet yang datangnya dari luar yang terlihat datangnya dari dalam, umumnya hal ini akan mematahkan setiap serangan spoofing.

METODE

Analisa Sistem

Penelitian ini menggunakan aplikasi ARP watch yang digunakan untuk mendeteksi adanya serangan pada jaringan public. ARP Watch ini akan memonitor aktifitas etherner dan menyimpan informasi yang didapat dalam bentuk pasangan IP dan alamat MAC. Selain itu penulis menggunakan Mikrotik sebagai access point.

Pada penelitian ini dilakukan teknik untuk mendeteksi adanya paket yang telah di sisipi paket yang tidak dikenal, setelah itu Arp Watch akan langsung mendeteksi dan segera melakukan pemblokan terhadap aktifitas tersebut.

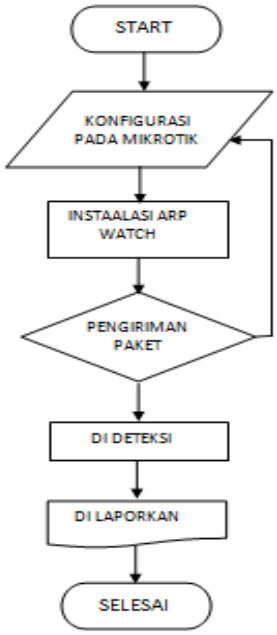
Desain Sistem

Desain sistem pada penelitian ini dilakukan agar aplikasi atau sistemyang nantinya dibangun tepat sesuai dengan yang ingin dicapai. dalam penelitian ini diperlukan beberapa infrastruktur dan komponen diantaranya adalah:

1. 3 buah komputer dengan sistem operasi Windows XP
2. 1 buah Mikrotik
3. Aplikasi yang digunakan : ArpWatch, Ethercap, Wireshark

3.1. Gambar Topologi Jaringan

Perancangan Sistem



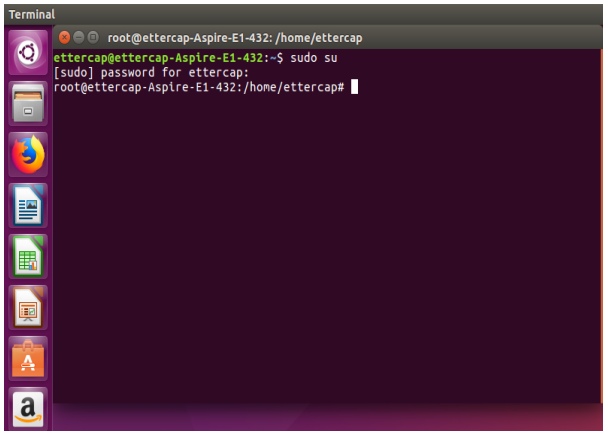
3.2 Gambar Desain Sistem

Penjelasan pada flowchart di atas adalah :

1. Dilakukankan konfigurasi dasar pada mikrotik, konfigurasi ini akan digunakan sebagai access point.
2. Instalasi ARP Watch pada komputer admin, pada komputer ini bertujuan sebagai administrator dari mikrotik.
3. Pada tahapan pengiriman paket, ini bertujuan untuk menyerang salah satu klien yang terhubung dengan mikrotik..
4. Deteksi, tahapan ini berfungsi untuk mendeteksi adanya kiriman yang mencurigakan dan terhubung dengan access point. Tahapan ini bisa dicegah dengan menggunakan Arp Watch sehingga bila paket tersebut masih lolos maka adanya kesalahan pada saat konfigurasi Arp Watch
5. Dilaporkan, pada tahapan ini mikrotik akan melaporkan melalui email atau melalui sms gateway pada klien yang akan di serang.

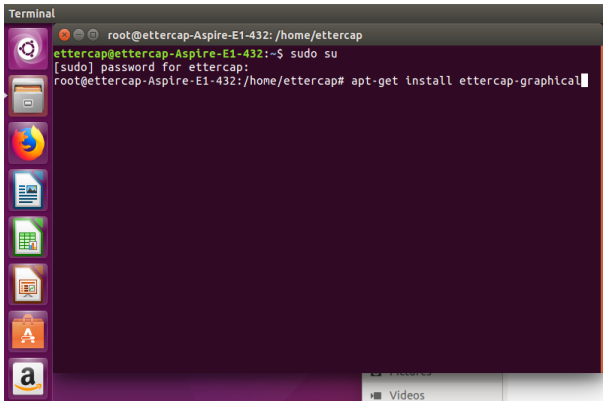
HASIL DAN PEMBAHASAN

Pertama kita ketikan sudo su dan masukan paswword ubuntu kita untuk menginstall ettercap nya



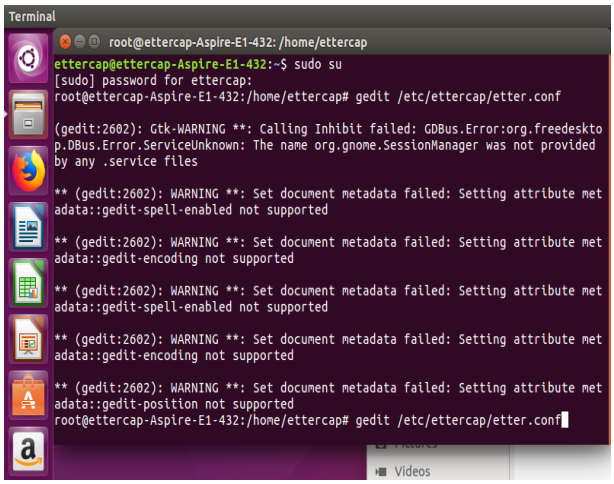
4.1 Gambar Tampilan Terminal Ubuntu

setelah itu kita instaal ettercap dengan mengetikan apt-get *install ettercap-graphical*,disini saya menggunakan ettercap graphichal untuk menjalakan program saya



4.2 Gambar Proses instalasi ettercap pada ubuntu

ketikan *gedit /etc/ettercap/etter.conf* untuk mengkonfigurasi ettercap kita



4.3 Gambar Konfigurasi Ettercap

dan hasilnya akan seperti ini disini hapus konfigurasi tanda pagar (#) di if you use iptables untuk konfigurasinya

PENUTUP

Simpulan

1. Pada penelitian kali ini penulis berhasil melakukan percobaan melakukan serangan menggunakan arp pada system operasi Ubuntu.
2. Diperlukan percobaan berulang kali agar arp dapat memantau aktifitas dari perangkan yang akan di serang.
3. Dalam mendeteksi serangan *packet sniffing* dengan indikasi *arp spof* menggunakan *arpwatch*. Agar *arpwatch* dapat memonitoring jaringan di perlukan konfigurasi pada *arpwatch* agar ketika terjadi serangan *packet sniffing* pada jaringan internet maka secara otomatis *arpwatch* akan memberikan *alert.*

Saran

1. Masih diperlukan percobaan berulang kali agar hasil yang diharpkan dapat sempurna.
2. Dibutuhkan lebih banyak refrensi dan materi yang cukup agar serangan yang di buat dapat berjalan lebih baik.

DAFTAR PUSTAKA

Satyagrahaprabu, Elson Feza. 2008. Monitoring Sistem Kerja dan Pengembangan Jaringan Komputer (Networking) Rumah Sakit Moewardi Bagian Bedah Menggunakan Simulasi The Dude. Skripsi. Fakultas Teknik, Jurusan Teknik Elektro, UMS

(http://www.download.portalgaruda.org/article.php?article=10706&val=750)(online 12/11/16, 14.2)

(https://www.dropbox.com/s/6uwmy5x5j9k67wi/OWP-2011112-buku-keamanan-jaringan.pdf?dl=0)(online 13/11/16, 12.50)

(https://www.id.scribd.com/document/320666135/analisa-paket-pdf)(online 12/11/16, 13.38)

https://www.academia.edu/6775927/Keamanan_Sistem_Informasi_Studi_Spoofing_TUGAS_Ini_Diajukan_sebagai_salah_satu_syarat_Kelulusan_matakuliah_Pada_Program_Studi_Sistem_Informasi_Manajemen_Informatika_Fakultas_Teknik_dan_Ilmu_Komputer (online 02/01/17, 12.59)