PENGGUNAAN SPOOFING DAN SSH FORWARDING UNTUK KEAMANAN SERTA FILTRASI DATA PADA JARINGAN

Selamet Hariadi
Jurusan Teknik Informatika Fakultas Sains & Teknologi
Universitas Islam Negeri "Maulana Malik Ibrahim" Malang
Email*: met_hariadi@yahoo.co.id*

Abstrak - *Teknologi Internet memang sungguh fenomenal & memberikan efek yang baik bagi penggunanya. Namun seiring perkembangannya, transportasi data melalui jaringan memang rawan disadap orang yang lain. Spoofing merupakan salah satu cara untuk melihat dan membuat backdoor dari sebuah jaringan. SSH Forwarding pada penggunaanya adalah pada efektivitas pengiriman data agar tepat pada data server atau client yang dituju. Penggabungan spoofing & SSH Forwarding dimaksudkan agar data yang direquest dari client dapat lebih privasi atau menjaga sifat keamanan dan penggunaan spoofing pada server lokal ditujukan agak ada filtrasi data atau address yang akan disampaikan ke client yang meminta*

Kata Kunci: Internet, Spoofing, SSH Forwarding, Keamanan Data , Filtrasi Data

1. PENDAHULUAN

Perkembangan teknologi yang begitu cepat harus dapat ditunjang dengan fasilitas atau alat yang sesuai juga dengan kebutuhan kecepatan informasi saat ini. Munculnya telepon memang sangat membantu manusia dalam berkomunikasi, namun seiring dengan kebutuhan sekarang ini, rasanya teknologi telepon belum cukup memahami.

Perkembangan internet atau intranet di belahan dunia ini sangat membantu dalam pertukaran informasi antar manusia di lain tempat. Teknologi jaringan diadaptasi guna mempermudahnya. Sistem ini memerlukan arus timbal balik antar manusia. Pertukaran data atau adanya permintaan (request) dan respon inilah yang sering terjadi dalam sebuah jaringan baik yang besar maupun yang bertaraf lokal.

Setiap pengguna jaringan yang akan berhubungan atau mengakses pihak lain di dalam jaringan tersebut atau di luar jaringan lokalnya pastilah melalui pihak-pihak sebagi penyambungnya. Pihak-pihak inilah yang kadang kita sebut server sebagai pusat jalur dari banyak jaring informasi di dalam jaringannya.

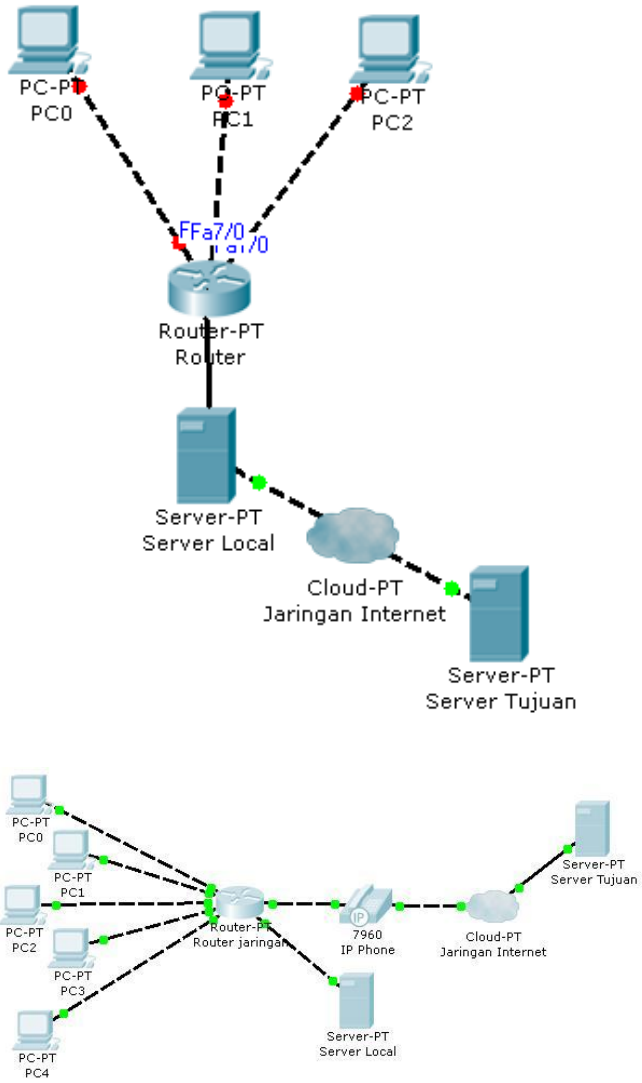
Penggunaan internet sebagai media komunikasi & informasi kadang riskan terganggu oleh pihak-pihak lain yang hanya main-main atau tujuan lain yang merusak jaringan kita sendiri. spoofing telah menjadi metode penyerangan yang menarik bagi pihak-pihak yang tak bertanggung jawab itu untuk mengumpulkan informasi yang berharga dari kita maupun server kita.

Masalah inilah yang penulis angkat disini. Masalah tentang pengamanan jaringan kita dari pihak lain yang tak berkempentingan. Masalah tentang pencurian data atau backdoor (pintu belakang, maksudnya server tujuan yang dimanipulasi leawt jalur lain padahal kita menginginkan lewat jalur yang benar)

Masalah yang berikutnya adalah kadang adanya kesulitan dari server lokal atau gate away kita (yang menghubungkan dengan jaringan internet) dalam

membendung atau memfilter alamat-alamat atau kata kata tertentu dari suatu informasi di internet.

Oleh karena itulah, penulis mencoba membuat gambaran sistem jaringan terdistribusi dengan menggunakan SSH forwarding sebagai enkripsi pengamanan & spoofing yang digunakan untuk membendung atau memfilter alamat-alamat atau kata kata tertentu dari suatu informasi di internet.



Gambar 1. Sistem Alur Data Umum

2. KAJIAN PUSTAKA

2.1 Spoofing

Dengan semakin banyaknya orang yang terus menggunakan web untuk mendapatkan atau tukar-menukar informasi, web spoofing telah menjadi metode penyerangan yang menarik bagi hackers untuk mengumpulkan informasi yang berharga. Web spoofing memungkinkan penyerang untuk menciptakan “shadow copy” dari seluruh World Wide Web. Akses ke web bayangan diarahkan ke mesin penyerang yang memungkinkan penyerang untuk memonitor seluruh aktivitas pengguna termasuk mendapatkan dan mengubah informasi yang ditransfer melalui web tersebut. Serangan yang demikian memberikan metode bagi penyerang untuk mendapatkan informasi yang bersifat pribadi password, nomor rekening, alamat, nomor telepon dan lain-lain. Sebagai tambahan, serangan ini dapat digunakan untuk memberikan informasi palsu yang menyesatkan pengguna sehingga menyebabkan salah satu tipe dari “Denial of Service” attack dengan meniadakan akses pengguna ke informasi web site yang diinginkan.[1]

IP spoofing adalah salah satu teknik yang digunakan untuk mendapatkan akses secara ilegal ke komputer lain. Hacker mengirimkan data ke komputer lain dengan alamat IP yang seakan-akan berasal dari komputer yang dikenal.[2]

IP spoofing adalah serangan dimana seorang penyerang pretends untuk mengirim data dari alamat IP selain sendiri. Lapisan IP yang menganggap bahwa sumber alamat IP pada setiap paket yang diterimanya sama dengan alamat IP sebagai sistem yang sebenarnya dikirim paket - ia tidak otentikasi. Banyak protokol tingkat tinggi dan aplikasi ini juga membuat asumsi, sehingga seolah-olah ada yang dapat memalsukan sumber alamat IP paket (dinamakan "spoofing" alamat) bisa mendapatkan hak istimewa yang tidak sah.[3]

2.2 SSH Forwarding

SSH adalah program untuk login pada suatu remote system dan untuk menjalankan perintah - perintah pada

remote system. Hal yang paling aman untuk melindungi dari paket sniffer adalah dengan mematikan servis remote login seperti telnet atau rlogin. Namun terkadang koneksi tersebut diperlukan untuk berbagai keperluan, sehingga dibutuhkan program remote login yang aman. Program alternatif yang aman digunakan untuk melakukan remote login adalah Secure Shell (SSH). Dengan SSH semua data terkirim dalam bentuk terenkripsi termasuk dalam melakukan otentikasi seperti login dan password, sehingga terlindung dari serangan sniffing, dns spoofing, atau cara-cara lain.

SSH merupakan arsitektur client/server. Program server SSH di-install dan dijalankan oleh system administrator, tugasnya untuk menerima atau menolak koneksi yang masuk ke komputer tersebut. User kemudian mejalankan program client SSH, biasanya dilakukan dari komputer lain, untuk membuat permintaan kepada server SSH. Seluruh komunikasi antara client dan server terenkripsi dan terlindungi dari modifikasi. [4]

3. PENGGUNAAN SPOOFING

Penggunaan Spoofing baik itu ip Spoofing ataupun web Spoofing sangat erat kaitannya dengan TCP/IP (Transmission Control Protocol/Internet Protocol). Jadi, akan sangat erat dengan tipe pemrograman connection-oriented. Antara client dan server memiliki hungungan komunikasi terbuka dan aktif saat aplikasi mulai dieksekusi sampai aplikasi ditutup.[5]

Dalam banyak kajian literatur yang penulis dapat, spoofing memang lebih diidententikkan dengan hacker atau orang yang mendapatkan akses ilegal dari pengguna internet yang lain. Karena pengunaannya yang digunakan untuk mendapatkan akses secara ilegal dari client atau pengguna. Orang yang mendapat akses ilegal ini mengirimkan data ke komputer lain dengan alamat IP yang seakan-akan berasal dari komputer yang dikenal.

Agar bisa melakukan spoofing, hacker terlebih dulu harus mencari sasaran yang akan dijadikan korban sebagai sumber spoofing, kemudian merubah / intercept paket header data dan dikirimkan ke komputer yang menjadi target.

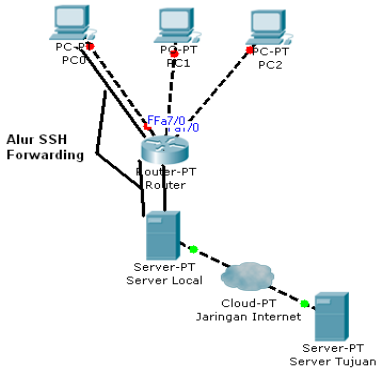
Secara ringkas cara kerja dari spoofing yakni setelah menulis ulang URL maka terjadi langkah-langkah berikut pada waktu serangan spoofing :

1. Pengguna merequest sebuah URL dari web browser.
2. Sever penyerang mendapatkan halaman yang diinginkan dari web server yang sebenarnya.
3. Web server yang sebenarnya menyediakan halaman tersebut ke server yang dimiliki oleh penyerang.
4. Server penyerang menulis ulang halaman yang dimaksud.
5. Server penyerang memberikan versi halaman yang sudah ditulis ulang kepada pengguna.

4. SSH FORWARDING

Port forwarding pada intinya adalah memerintah kan router untuk melakukan forward suatu port kepada port lain, baik sesama komputer maupun terhadap komputer yang berbeda.[4]. Secara ringkas penggunaan SSH Forwarding adalah:

1. Dalam penggunaannya SSH Forwarding, client & juga server harus sama-sama aplikasi untuk SSH dan aplikasi ini harus aktif.



Gambar 2. Penggunaan SSH Forwading

2. Seperti tampak pada gambar di atas penggunaan SSH dari client akan mengirimkan berupa plaintext yang kemudian diteruskan ke router lalu berjalan ke gateway. Jadi permasalahan seperti client lain dalam jaringan tersebut yang sengaja akan membuat backdoor akan kesulitan dengan penggunaan SSH Forwarding ini.

Dikatakan forwarding karena SSH ini akan mengembalikan atau menyalurkan data berupa plaintext tadi ke depan atau muka jaringan yang dituju.

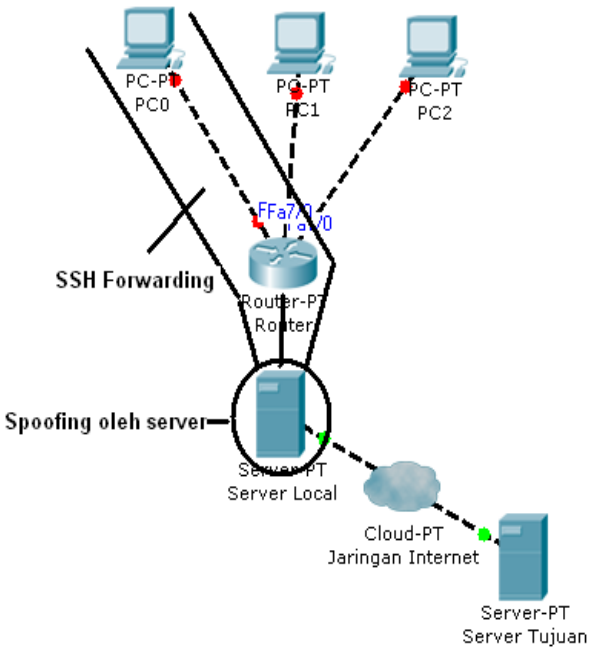
5. DESAIN SISTEM

5.1 Penggunaan Spoofing & SSH Forwading

Seperti telah dijelaskan tadi, penggunaan spoofing adalah lebih pada analisa jaringan atau bisa semacam pengaksesan data dari server yang dimintai data yang difilter dahulu dengan spoofing lalu diteruskan ke client yang meintanya.

Sedangkan SSH Forwarding lebih pada penyaluran informasi yang hanya server local dan client yang meminta respon saja yang dapat berkomunikasi, sehingga client lain yang akan merusak tersampainya informasi ke client yang meminta respon akan kesulitan karena menggunakan data berupa plaintext dengan SSH Forwarding yang menuju jaringan yang dituju si pengirim pesan.

Untuk penggabungan Spoofing & SSH Forwarding ini penulis coba membuat efektivitas spoofing & SSH Forwarding pada jaringan lokal. Seperti gambar 3 di atas, proses alir datanya dimulai dari computer client yang akan relakukan permintaan atau request ke server melalui browsernya untuk disambungkan ke jaringan internet. Dengan menggunakan data berupa SSH yang telah di plaintext-kan jadi data bisa lebih privasi untuk jaringan lokal tersebut.



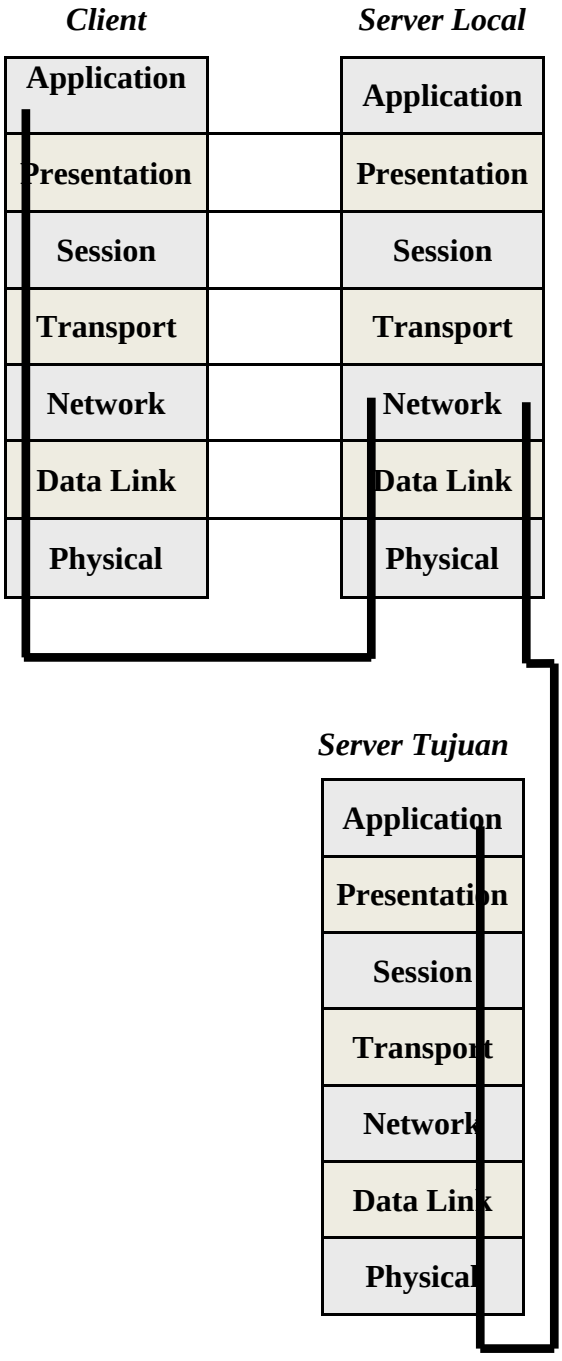
Gambar 3. Alur data dengan SSH Forwading & Spoofing

Setelah jaringan mengkonvergensikan data SSH dari client yang meminta tadi maka server lokal akan mencarikan lalu menghubungkan via jaringan internet. Setelah informasi datang ke server lokal, maka data akan diolah terlebih dahulu oleh server apakah data ini layak diteruskan ke client dengan cara spoofing. Bila ada di daftar hitam server local maka server local akan mengirimkan respon ke client yang merquest tadi dengan alamat address yang lain (yang telah disediakan server lokal).

5.2 Desain Pada OSI Layer

Pada perjalanan data akan melalu pertama kali di aplication Layer yang terdiri dari bermacam-macam protocol[6]. Lalu bila ada konversi data dari EBDIC ke ASCII akan melalui layer ini. Setelah itu layer sesion yang digunakan untuk kendali dilaog. Selanjutnya pada layer transport data dipecak menjadi bagian yang lebih kecil lalu diteruskan ke layer network dengan pemberian address dimana tempat kerja IP Address. Setelah itu masuk ke ethernet di layer data link. Layer terakhir adalah phisical yang memecah data tadi

menjadi aliran listrik. Pengiriman data via router lalu server local tadi akan menggunakan SSh Forwarding untuk pengamanan data.



Gambar 4. Alur data pada OSI Layer

Di layer milik server lokal, maka data akan disambut hanya pada layer network untuk dilakukan identifikasi lalu data informasi ini akan dikirim ke server tujuan via jaringan internet, setelah kembali akan dilakukan spoofing di layer 3 milik server lokal. Setelah spoofing selesai, maka data siap dikirim ke client yang merequest dengan SSH Forwarding lagi.

6. KESIMPULAN

Dari pemanfaatan Spoofing dengan SSH Forwarding pada penjelasan di atas dapat disimpulkan bahwa penggunaan spoofing tidak hanya untuk mereka yang mau mengrusak aliran data client, namun dapat pula sebagai filter dari server lokal dari request clientnya.

Untuk melindungi aliran data dari client atau server, SSH Forwarding merupakan cara yang cukup baik untuk menganggulangi penyusupan atau penyalahgunaan aliran data pada client yang berhak menerimanya.

Penggunaan Spoofing dan SSH Forwarding dalam jaringan local akn membantu pengamanan data serta pemfilteran atu penyaringan data yang berhak di dapat oleh client yang meminta.

DAFTAR PUSTAKA

[1] Hendry. *Web Spoofing*. 2009.

[2] Harry. *IP Spoofing*. Didapat dari hr2009.blogspot.com diakses tanggal 05 Mei 2009.

[3]Chambers, Chris dkk. TCP/IP Security. Ohio State University Columbus. Ohio

[4]Kafianto, Arief. *Dynamic SSH Port Forwarding : Implementasi Protokol Kriptografi yang Membuat ARP Spoofing Menjadi Sia-Sia*. Sekolah Tinggi Sandi Negara.

[5]Santoso, Budi. *Belajar Sendiri Pemrograman Client/Server dengan Java 2*. 2003 PT. Elex Media Komputindo. Jakarta

[6] Tim peneliti Dan pengembangan Wahana Komputer. *Konsep Jaringan Komputer dan Pengembangannya*. 2003. Penerbit Salemba Infotek. Jakarta.