ANALISIS DAN IMPLEMENTASI SISTEM REDUNDANT HOT STANDBY NETWORK SECURITY MENGGUNAKAN METODE INTRUSION PREVENTION SYSTEM (IPS) DAN CAPTIVE PORTAL PADA JARINGAN NIRKABEL

Shidqy Riyasa[1], Asep Mulyana[2], Yudha Purwanto[3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Semakin maraknya penggunaan teknologi nirkabel pada tempat-tempat umum (seperti cafe, restaurant, hotel dan perkantoran) membuat mayoritas pengusaha berlomba-lomba menyediakan akses internet gratis berbasis nirkabel di tempat usahanya. Namun tidak sedikit administrator jaringan tersebut tidak memperhatikan masalah keamanan, sehingga dapat menjadi sebuah celah dan dimanfaatkan oleh seorang "hacker" untuk merusak atau mengganggu layanan dari server setempat. Tentunya akan merugikan perusahaan tersebut karena pelanggan yang menggunakan fasilitas internet di tempat tersebut merasa terganggu atau bahkan merasa dirugikan. Oleh karena itu tugas akhir ini mencoba untuk menginovasikan sebuah sistem keamanan untuk melindungi server di tempat-tempat umum yang memiliki akses nirkabel untuk menggunakan layanannya. Sistem keamanan utama dari tugas akhir ini merupakan sistem firewall IPS (Intrusion Prevention System) yang dibantu oleh teknologi Captive Portal yang dirancang secara redundansi.

Alat authentikasi yang biasa dipakai di jaringan nirkabel adalah captive portal. Captive portal memakai standar web browser untuk memberi seorang user nirkabel kesempatan untuk mengauthentikasi dirinya, biasanya berupa username & password. Captive portal biasanya dipakai di jaringan terbuka yang tak punya metode authentikasi lain (seperti WEP atau MAC filter). Di jaringan publik atau semi-publik, teknik enkripsi seperti WEP dan WPA tidak berguna. Tidak ada cara untuk menyebarkan publik atau kunci yang dipakai bersama kepada masyarakat tanpa membahayakan keamanan dari kunci tersebut. Sistem autentikasi yang disediakan oleh Captive Portal memungkinkan untuk dirusak sehingga seorang "Hacker" mampu melakukan penyerangan terhadap server yang memang dituju olehnya. Oleh karena itu digunakanlah teknologi keamanan Intrusion Prevention System yang mampu melakukan blocking terhadap trafik yang dicurigai sebagai serangan dan mampu merusak atau mengganggu layanan server setempat.

Pada implementasi sistem ini, sudah diujicobakan pada berbagai macam serangan, seperti Port Scanning, DoS, dan DDoS yang merupakan salah satu tipe serangan yang mengeksploitasi sistem dimana akan dikirimkan request dalam jumlah besar, sistem yang tidak mampu menangani banyak request tersebut akan habis sumber daya sistemnya sehingga kinerja sistem secara utuh akan terganggu. Oleh karena itu, digunakanlah Captive Portal untuk mencegah masuknya pengguna ilegal dan redundansi firewall IPS yang membuat jaringan lebih tahan terhadap serangan pembanjiran trafik.

Kata Kunci : Captive Portal, Intrusion Prevention System, Wireless, Redundant, DDoS

Abstract

Increasingly the use of wireless technology in public places (such as cafes, restaurants, hotels and offices) make the majority of entrepreneurs are competing to provide wireless internet access based on his place of business. But not a few of the network administrator does not aware about security issues, so it may be a gap which can be exploited by a "hacker" to damage or disrupt the service of the local server. Surely it would be harm for the company because the customers who use the internet facilities at the site was disturbed or even feel aggrieved. Therefore, this thesis tries to innovate a security system to protect the server in public places that have wireless access to use their services. The main security system of this thesis is a system firewall IPS (Intrusion Prevention System) assisted by Captive Portal technology which is designed of redundancy.

Authentication tool which commonly used in wireless networks is a captive portal. Captive portal using a standard web browser to give a user access a chance to authenticate themselves, usually in the form username and password. Captive portals are usually used in open network with no other authentication methods (such as WEP or MAC filters). In the public network or a semi-public, techniques such as WEP and WPA encryption is not useful. There is no way to deploy a public or shared key to the public without jeopardizing the security of the key. Authentication system provided by the Captive Portal is possible to destroyed so that a "Hacker" are able to attack the server that is intended by it. Therefore, the security technology in this thesis is used Intrusion Prevention System which capable of doing some blocking for the traffic suspected of attacks and could damage or interfere with the local server services.

In the implementation of this system has been tested on a variety of attacks, such as port scanning, DoS and DDoS, which is one type of attacks that exploit the system where the request is sent in large quantities, the system is not able to handle the many requests the system will run out of resources so the performance of the system as a whole will suffer. Therefore, the Captive Portal is used to to prevent the entry of unauthorized users and IPS firewall redundancy that makes the network more resistance to flooding attack traffic.

Keywords : Captive Portal, Intrusion Prevention System, Wireless, Redundant, DDoS

BAB I
PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

Banyak pengguna internet yang mulai menggunakan jaringan internet nirkabel sebagai jalur akses penggunaan layanan internet, namun tingkat keamanan sistem jaringan nirkabel tidak begitu kuat. Sehingga dibutuhkan jaringan keamanan dan manajemen sistem jaringan nirkabel yang dapat memberi keamanan bagi penggunanya. Menggunakan fasilitas nirkabel ini tidaklah sepenuhnya aman dari serangan *hacker*, karena jaringan nirkabel ini tidak menggunakan enkripsi pada saat berlangsungnya komunikasi data. Sehingga memungkinkan terjadinya *hacking* seperti *Port Scanning, DoS* dan DDoS mengakibatkan kerugian bagi pengguna layanan jaringan internet nirkabel ini, contohnya pada saat kita melakukan transaksi e-banking dan menggunakan akses nirkabel, maka dibutuhkan keamanan di sisi akses masuk nirkabel yaitu akses poin, maupun keamanan di sisi server e-banking untuk melakukan sistem redundan dan sistem *blocking* saat keamanan jalur akses masuk tidak berfungsi. Salah satu cara meredam terjadinya penyusupan melalui akses jaringan nirkabel adalah menggunakan *Captive Portal* sebagai mesin autentikasi di sisi akses poin dan *Intrusion Prevention System* (IPS) di sisi server penyedia layanan.

Dengan adanya masalah tersebut diharapkan keamanan akses jaringan nirkabel dapat diperkuat dan dihasilkan sebuah rancangan infrastruktur jaringan nirkabel yang memadukan *Captive Portal* dengan *Intrusion Prevention System* (IPS) pada rangkaian redundansi *Hot Standby* yang dapat mendeteksi dan melakukan proteksi secara dini jika ada serangan berupa trafik yang berbahaya (*intruder traffic*) maupun saat server

penyedia layanan sedang down. Sehingga keamanan dan kenyamanan para pengguna akses nirkabel dapat terjamin.

1.2 RUMUSAN MASALAH

Rumusan masalah dari penelitian tugas akhir ini adalah sebagai berikut:

1. Bagaimana performansi IPS ini ketika dikombinasikan dengan sistem *Captive Portal* untuk manajemen dan keamanan jaringan.
2. Captive Portal yang akan diintergrasikan pada distro linux harus dapat kompatibel dan dapat berjalan dengan stabil.
3. Perancangan *Captive Portal* ini diharapkan dapat seefektif mungkin dalam sistem kerjanya sehingga mengurangi beban sistem IPS saat menerima serangan.
4. Perancangan pada sebuah sistem redundansi diharapkan dapat bersifat siaga jika terjadi berbagai serangan maupun saat server mangalami *failure* atau *down*.
5. Perancangan IPS harus mampu menangkal terjadinya serangan Port Scanning, DoS, dan DDoS.

1.3 TUJUAN

1. Menghasilkan sistem manajemen akses internet yang terintegrasi menjadi suatu sistem keamanan jaringan yang bersifat *redundant hot-standby* untuk mendapatkan kondisi *high availability system* .
2. Analisis performansi dan kemanan sistem yang berhasil dilakukan dengan kombinasi antara *Intrusion Prevention System* (IPS) dan *Captive Portal.*
3. Membuat sebuah sistem keamanan ganda yang kuat untuk akses sebuah server yang diakses melalui jaringan nirkabel.
4. Dapat mengkonfigurasi *snort* yang merupakan jenis dari (IDS) *Intrussion Detection System* agar dapat menjadi sebuah sistem keamanan jaringan yang dapat mendeteksi dan memblok intrusi dalam jaringan secara otomatis.
5. Menyediakan jaringan akses yang aman dan terauthentikasi menuju *server* penting seperti untuk penggunaan transaksi bank menuju *server* bank pada tempat-tempat umum seperti cafe, hotel, dan lainnya.

1.4 BATASAN MASALAH

Pada penelitian tugas akhir ini akan dilakukan beberapa batasan masalah, diantaranya adalah sebagai berikut:

1. Server yang digunakan adalah *Web Server* dan *DNS Server* pada *Operating System Ubuntu*
2. Arsitektur Jaringan IPS dan *Captive Portal* ini menggunakan wireless router sebagai akses poin dan penyedia layanan hotspot.
3. IPS yang digunakan adalah *Snort + BlockIT*
4. Uji coba Distributed Denial of Service (DDoS) menggunakan TFN2000 (Tribe Flood Network 2000)
5. Uji coba Denial of Service (DoS) menggunakan software LOIC (Low Orbit Ion Cannon)
6. Uji coba yang dilakukan dengan menggunakan teknik *port scanning* nmap sebagai teknik *hacking*nya.
7. Tidak membahas mengenai pembuatan *web* dan konten-kontentnya.

1.5 METODE PENELITIAN

Beberapa metode yang digunakan pada penelitian tugas akhir ini adalah:

1. Melakukan studi pustaka, untuk mengumpulkan literatur dan proses pembelajaran materi melalui buku maupun jurnal-jurnal ilmiah dari berbagai sumber yang digunakan sebagai acuan penelitian tugas akhir ini.
2. Menentukan pemodelan sistem dan parameter-parameter yang digunakan untuk simulasi sehingga menghasilkan data-data pendukung penelitian.
3. Melakukan pengambilan data-data parameter dari penelitian yang telah dilakukan sebelumnya sebagai data pendukung pada penelitian tugas akhir ini.

1.6 SISTEMATIKA PENULISAN

Sistematika yang digunakan dalan penulisan proyek akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Berisi latar belakang masalah, maksud dan tujuan, perumusan masalah, batasan masalah, pemodelan sistem, metode penyelesaian masalah, dan sistematika penulisan.

BAB II DASAR TEORI

Pada bab ini dikemukakan berbagai teori yang mendukung dalam pembuatan proyek ini diantaranya *Captive Portal*, *Intrusion Prevention System*, *Redundant Hot-standby*.

BAB III PERANCANGAN

Berisi tentang tahap-tahap perancangan dan tahap-tahap implementasi awal sistem.

BAB IV ANALISIS HASIL IMPLEMENTASI

Bab ini membahas hasil uji performansi dari Sistem keamanan yang akan dibuat.

BAB V KESIMPULAN DAN SARAN

Berisi tentang kesimpulan akhir dan saran pengembangan Tugas Akhir.

KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Dari hasil implementasi serta pengambilan data dan analisis mengenai sistem keamanan Captive Portal dan Redundansi IPS pada jaringan nirkabel yang diujikan menggunakan beberapa skenario, maka dapat diambil kesimpulan sebagai berikut :

1. *Captive Portal* mampu mengurangi adanya trafik yang dengan sengaja maupun tidak sengaja untuk merusak maupun mengganggu layanan dari *server*, karena dibatasi oleh sistem *log in*, yang memaksa pengguna untuk mempunyai akun yang legal dan terdaftar di server. *Captive Portal* juga mampu mengenkripsi data *(password)* yang ditransmisikan melalui media nirkabel maupun media kabel sehingga keamanan data lebih terjamin.
2. Pada serangan DoS dan Port Scanning menggunakan software LOIC (Low Orbit Ion Cannon) dan NMAP, nampak bahwa IPS dapat langsung memblok IP source dalam waktu kurang dari 1 menit yang ditujukan kepada server sehingga IP tersebut tidak bisa melakukan koneksi lagi ke *server*.
3. Pada serangan ICMP *Flood* mempunyai minimal *requirement* untuk menjaga *server* agar tidak terjadi *down* yaitu dengan jumlah paket minimal 3.600.000.000 dan jumlah *client* dua buah.
4. Pada serangan UDP *Flood* mempunyai minimal *requirement* untuk menjaga *server* agar tidak terjadi *down* yaitu dengan jumlah paket minimal 3.711.821.222 dan jumlah *client* dua buah.
5. Pada serangan TCP/SYN *Flood* berbeda dengan pengujian lainnya, TCP/SYN *flooding attack* lebih mementingkan jumlahnya *client zombie* yang digunakan untuk membuat server menjadi *down* sehingga dapat dikatakan TCP/SYN *attack* lebih mementingkan kuantitas.
6. Waktu perpindahan yang dibutuhkan oleh sistem redundansi *server active* menuju *server standby* ketika terjadi *down*, membutuhkan waktu rata-rata sekitar 14.059 detik. Hal ini sangat dipengaruhi oleh spesifikasi *hardware* yang digunakan.

5.2 SARAN

Penulis mengharapkan penelitian ini dapat dikembangkan lebih lanjut diantaranya:

1. Untuk implementasi lebih lanjut diharapkan dapat dilakukan pengembangan pengujian *web server* atau secara layanannya yang dibuat *redundant* dengan IDS, atau biasa disebut AIRIDS.
2. Untuk implementasi lebih lanjut sebaiknya ditambah fitur WPA2 pada *server* RADIUS untuk memperkuat *Captive Portal* agar sistem keamanan dari sisi wireless dapat semakin aman
3. Pengembangan pada sisi webnya yaitu adanya konten yang mampu memberikan gambaran secara langsung bentuk layanan yang diberikan melaui jaringan nirkabel.
4. Menggunakan metode redundansi *load balancing* dengan konsep kerja *together as one*, agar pembagian beban *server* semakin baik lagi.

DAFTAR PUSTAKA

[1] **Affan, Frastuzi. "***Analisis Dan Implementasi Sistem Redundant Firewall Menggunakan Metode Intrusion Prevention System*" Tugas Akhir Institut Teknologi Telkom. 2011

[2] **E-Reports. "*Distributed System Intruder Tool Trinoo and Tribe Flood Network*".** https://e-reports-ext.llnl.gov/pdf/238327.pdf (22 Januari 2013)

[3] **Hedrinote.** "*Tutorial Hacking menggunakan Netcat*". http://hendrinote.blogspot.com/2010/02/tutorial-hacking-menggunakan-netcat.html (16 Januari 2013)

[4] **Instrument, national.** "Redundant System Basic Concepts*"*.http://www.ni.com/white-paper/6874/en .(20 September 2012)

[5] **Konoharakureah**. " Belajar Konfigurasi Basic HSRP (Hot StandbyRouter Protocol)". http://www.scribd.com/doc/48849587/Belajar-Konfigurasi-Basic-HSRP. (19 september 2012)

[6] **Lubis , Laila Nuzha.** "*Implementasi Pencegahan Serangan Interruption Jenis Flooding Terhadap Keamanan Layanan Video Streaming Dan Transfer File*". Politeknik Telkom. 2011

[7] **Muhamad, Faris**. *"Analisa Serangan DDoS Pada Server Ubuntu Yang Beroperasi Dalam Wireless Local Area Network".* Tugas akhir, Institut Teknologi Telkom. 2010

[8] **Nanopaw.** *"Setting IP failover heartbeat dan Pacemaker".* http://www.zivtech.com/blog/setting-ip-failover-heartbeat-and-pacemaker-ubuntu-lucid. (14 November 2012)

[9] **Redra, Fredy**, 2010, "Install Easyhotspot dan Konfigurasi Freeradius seta Coova Chili di Ubuntu 10.04 LTS Server Edition". Diambil tanggal 22 november 2012 dari http://ndra.gmib26.net/2010/06/install-easyhotspotdan- konfigurasi-freeradius-serta-coova-chilli-di-ubuntu-10-04-ltsserver-edition/

[10] **S'to**. "Seni Teknik Hacking Uncensored". Jasakom.2009

[11] **S'to. "**Certified Ethical Hacker". Jasakom. 2009

[12] **Thomas, Tom.** "*Network Security First-Step"***.** Penerbit Andi. Yogyakarta

[13] **Xeon**. "**Captive Portal (Coova chilli + Yfi Manager Hotspot)".** http://opensource.telkomspeedy.com/forum/viewtopic.php?id=8439. (1 Oktober 2013)

[14] **Zen, Muhammad**. “Menyerang dan Bertahan, mengetahui bagaimana hacker beraksi dan membangun pertahanan yang kuat pada sistem dan jaringan komputer” modul 5a hacking and defense.