

ANALISIS DAN IMPLEMENTASI METODE DMZ (DEMILITARIZED ZONE) UNTUK KEAMANAN JARINGAN PADA LPSE KOTA PALEMBANG

Muhammad Diah Maulidin¹, Muhamad Akbar, M.I.T.², Siti Sa'uda, M.Kom.³

¹Mahasiswa Informatika, ^{2,3}Dosen Fakultas Ilmu Komputer Universitas Bina Darma
Jl. A Yani No. 12 Plaju, Palembang 30624

Email: dedekthamrin@gmail.com¹, muhamad.akbar@binadarma.ac.id², sitisauda@mail.binadarma.ac.id³

Abstract. The internet network administration needs at least a security that can protect critical data from hacking attacks, one of which is the use of a firewall. At the office of the Sekretariat Daerah Kota Palembang, there is one unit that regulates the procurement of goods / services, namely Layanan Pengadaan Secara Elektronik (LPSE). Analysis is performed on the network infrastructure in LPSE Kota Palembang, there is access to the LPSE website and the email website that can be accessed through a public IP address, domain and private IP address. Public dan private IP addresses can be susceptible to network security, if there is someone who wants to try to access the LPSE server website and email server, by exploiting loopholes open port, so that a person who accesses from the internet may try to hack, exploit and get the information network that is in LPSE Kota Palembang. With the existence of the problem, the necessary techniques are applied to the firewall DMZ in router Mikrotik.

Keywords: firewall, DMZ, *router* Mikrotik

Abstrak. Jaringan internet di pemerintahan setidaknya membutuhkan keamanan yang dapat melindungi data-data penting dari serangan peretas, salah satunya adalah penggunaan *firewall*. Pada kantor Sekretariat Daerah Kota Palembang terdapat satu unit yang mengatur pengadaan barang/jasa pemerintah secara elektronik yaitu Layanan Pengadaan Secara Elektronik (LPSE). Analisis yang dilakukan pada infrastruktur jaringan di LPSE Kota Palembang, terdapat akses *website* LPSE dan *website email* LPSE yang dapat diakses melalui *ip address* publik, *domain* dan *ip address* lokal. *IP address* publik dan lokal dapat rentan dengan keamanan jaringan, apabila ada seseorang yang ingin mencoba mengakses *server* website LPSE dan *server* email, dengan memanfaatkan celah *port* yang terbuka, sehingga seseorang yang mengakses dari internet dapat mencoba untuk meretas, mengeksploitasi

dan mendapatkan informasi jaringan yang berada di LPSE Kota Palembang. Dengan adanya masalah tersebut maka diperlukan teknik DMZ yang diterapkan pada *firewall* di *router* Mikrotik.

Kata kunci: *firewall*, DMZ, *router* Mikrotik

1. Pendahuluan

1.1 Latar Belakang

Keamanan jaringan internet merupakan salah satu aspek yang dapat dikembangkan dalam suatu jaringan di pemerintahan yang dapat melindungi data-data penting dari serangan peretas, yang dapat mengganggu kinerja pegawai untuk melayani masyarakat, salah satunya adalah penggunaan *firewall*. Pada kantor Sekretariat Daerah Kota Palembang terdapat satu unit yang mengatur pengadaan barang/jasa pemerintah secara elektronik yaitu Layanan Pengadaan Secara Elektronik (LPSE). LPSE melayani proses pengadaan barang/jasa pemerintah secara elektronik menggunakan teknologi informasi dan transaksi elektronik sesuai peraturan perundang-undangan yang berlaku.

Analisis yang dilakukan pada infrastruktur jaringan di LPSE, terdapat perangkat jaringan yaitu *server website* LPSE Kota Palembang yang berisi aplikasi Sistem Pengadaan Secara Elektronik (SPSE) dengan alamat lpse.palembang.go.id, *server email*, *router* dan *switch*. Akses internet yang ada di LPSE menggunakan *dedicated line*, terhubung ke *router* Mikrotik yang menghubungkan *switch* menuju *access point* atau akses *wireless*. Terdapat juga komputer yang ditempatkan di ruang *bidding & training room* (tempat pelatihan aplikasi SPSE) dan di ruang kerja yang terhubung ke internet melalui akses *wireless*.

Pada infrastruktur jaringan di LPSE Kota Palembang, terdapat akses *ip address* publik dan *ip address* lokal yang dapat mengakses perangkat jaringan yaitu *server website* LPSE dan *website email* LPSE. *Server* tersebut dapat diakses *user* melalui *domain* <http://lpse.palembang.go.id> untuk *website* LPSE dan *domain* <http://mail.lpse.palembang.go.id> untuk *website email* LPSE. Jika *user* yang berada di internal LPSE mengakses *domain server* LPSE dan *server email* LPSE, akan diarahkan ke *ip address* lokal. Jika *user* yang berada di eksternal (internet) mengakses *domain server* LPSE dan *server email* LPSE, akan diarahkan ke *ip address* publik. *IP address* lokal dan *ip address* publik dapat rentan dengan keamanan jaringan, apabila ada seseorang yang ingin mencoba mengakses *server website* LPSE dan *server email*, dengan memanfaatkan celah *port* yang terbuka, sehingga seseorang yang mengakses dari internet dapat mencoba untuk meretas, mengeksploitasi dan mendapatkan informasi jaringan yang berada di LPSE melalui celah *port* yang terbuka di *server website* dan *server email*. Dengan adanya masalah keamanan jaringan yang telah disebutkan di atas, peneliti mencari tahu bagaimana cara mengamankan keamanan jaringan di LPSE dan menemukan metode atau teknik DMZ yang dapat diterapkan melalui *firewall* di *router* Mikrotik yang digunakan di LPSE.

1.2 Perumusan Masalah

Adapun rumusan masalah dalam penelitian ini adalah “Bagaimana meningkatkan keamanan jaringan dengan teknik atau metode DMZ pada LPSE (Layanan Pengadaan Secara Elektronik) Kota Palembang?”

1.3 Tujuan Penelitian

Tujuan dari penelitian ini yaitu mengetahui informasi jaringan yang telah diterapkan di LPSE Kota Palembang dan meningkatkan keamanan jaringan di bagian *firewall* dengan teknik DMZ (*Demilitarized Zone*) yang dibuat berdasarkan tiga konsep yaitu NAT (*Network Address Translation*), PAT (*Port Addressable Translation*) dan *Access List*.

1.4 Batasan Masalah

Batasan masalah dalam penelitian ini adalah menganalisis keamanan jaringan internal dan eksternal yang diterapkan pada perangkat jaringan (*server website* dan *server email*) di LPSE Kota Palembang dan mengimplementasikan teknik DMZ (*Demilitarized Zone*) dengan membuat aturan (*policy*) pada *firewall* yang diterapkan melalui router Mikrotik di LPSE Kota Palembang.

1.5 Metode Penelitian

Metode penelitian yang digunakan untuk penelitian ini adalah metode penelitian tindakan atau *action research*^[1]. Tahapan *action research* yang dilakukan, yaitu melakukan diagnosis (*diagnosing*), membuat rencana tindakan (*action planning*), melakukan tindakan (*action taking*), melakukan evaluasi (*evaluating*) dan refleksi atau pembelajaran (*learning*).

2. Landasan Teori

2.1 Firewall

Firewall adalah suatu sistem yang mengendalikan aliran *traffic* antara jaringan dan memberikan suatu mekanisme untuk melindungi *hosts* yang ada di belakang *firewall*. *Firewall* juga bisa kita gunakan untuk mengendalikan aliran *traffic* yang mengakses *public resources* yang diletakkan pada DMZ.^[2]

2.2 DMZ

Firewall DMZ (*Demilitarized Zone*) – atau jaringan perimeter adalah jaringan *security boundary* yang terletak diantara suatu jaringan *corporate/private* LAN dan jaringan *public* (internet). Perimeter (DMZ) network didesain untuk melindungi server pada jaringan LAN *corporate* dari serangan *hackers* dari internet^[2].

DMZ berisi perangkat diakses untuk lalu lintas internet, seperti Web (HTTP) server, server FTP, SMTP (e-mail) server dan DNS server. *Demilitarized zone* digunakan untuk mengamankan jaringan internal dari akses eksternal. DMZ dapat dibuat menggunakan MikroTik Router. Secara umum DMZ dibangun berdasarkan tiga buah konsep, yaitu: NAT (*Network Address Translation*), PAT (*Port Addressable Translation*), dan *Access List*. NAT berfungsi untuk menunjukkan kembali paket-paket yang datang dari “real address” ke alamat internal. Kemudian PAT berfungsi untuk menunjukkan data yang datang pada particular port, atau range sebuah port dan protocol (TCP/UDP atau lainnya) dan alamat IP ke sebuah particular port atau range sebuah port ke sebuah alamat internal IP. Sedangkan *access list* berfungsi untuk mengontrol secara tepat apa yang datang dan keluar dari jaringan dalam suatu pertanyaan^[3].

2.3 Nmap

Nmap merupakan singkatan dari Network Mapper merupakan sebuah *tools open source* yang berfungsi untuk eksplorasi dan audit keamanan jaringan. Nmap menggunakan paket IP raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang

diberikan, sistem operasi (dan versinya) apa yang digunakan, apa jenis *firewall/filter* paket yang digunakan, dan sejumlah karakteristik lainnya.^[4]

3. Analisis dan Perancangan

Analisis dan implementasi jaringan yang dilakukan berdasarkan tahapan *action research*^[1]. Pada bagian Analisis dan Perancangan, tahapan yang dilakukan yaitu sebagai berikut.

3.1 Melakukan Diagnosis (*diagnosing*)

Tahapan ini menjelaskan perangkat komputer, *software* atau *tools* yang digunakan dan menganalisis jaringan pada objek penelitian (LPSE Kota Palembang) dengan mengikuti tahapan analisis kebutuhan (*requirements analysis*) sistem jaringan yang dijelaskan oleh McCabe^[5].

3.2 Membuat Rencana Tindakan (*action planing*)

Tahapan ini menganalisis informasi jaringan pada objek penelitian (LPSE Kota Palembang) menggunakan *tools* Nmap dan menjelaskan hasil *scan tools* tersebut.

4. Hasil dan Pembahasan

Pada bagian Hasil dan Pembahasan, dijelaskan tahapan ketiga dan keempat dari *action research* yaitu tahapan melakukan tindakan (*action taking*) dan tahapan melakukan evaluasi (*evaluating*).

4.1 Melakukan Tindakan (*action taking*)

Tahapan ini menjelaskan implementasi teknik DMZ dengan mengkonfigurasi *firewall* di *router* Mikrotik dengan melihat hasil *scan tools* Nmap sebelum menerapkan teknik DMZ pada *server website* LPSE dan *server email*. Setelah didapatkan dari *tools* Nmap, terdapat celah *port* yang terbuka di setiap *server* yang harus ditutup atau difilter, dengan harapan teknik DMZ dapat diimplementasikan untuk menutup celah tersebut. Implementasi yang diterapkan yaitu mengkonfigurasi jaringan pada *router* Mikrotik di bagian *firewall* menggunakan program Winbox.

4.2 Melakukan Evaluasi (*evaluating*)

Tahapan ini menjelaskan hasil dari implementasi yang dilakukan yaitu menerapkan teknik DMZ dengan menutup celah *port* di *server website* dan *server email* yang telah dikonfigurasi pada *router* Mikrotik. Pada tahapan ini juga akan dilakukan kembali *scan tools* Nmap pada perangkat jaringan (*server website* dan *server email*) setelah diterapkan teknik DMZ dan membandingkan hasil *scan* dari *tools* Nmap sebelum menerapkan teknik DMZ, dan setelah menerapkan teknik DMZ.

Berikut ini adalah perbedaan dari hasil *scan tools* Nmap sebelum penerapan DMZ dan hasil *scan tools* Nmap setelah penerapan DMZ.

Sebelum penerapan DMZ				Setelah Penerapan DMZ			
PORT	STATE	SERVICE	VERSION	PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)	22/tcp	filtered	ssh	
25/tcp	open	smtp	Postfix smtpd	25/tcp	filtered	smtp	
80/tcp	open	http	Apache/2.2.16 ((Debian))	80/tcp	open	http	Apache/2.2.16 ((Debian))
8080/tcp	open	http	Apache/2.2.16 ((Debian))	8080/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1
8081/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1	8081/tcp	filtered	blackice-icecap	

Gambar 1. Perbandingan Hasil Scan Nmap Internal Website LPSE

Sebelum penerapan DMZ				Setelah Penerapan DMZ			
PORT	STATE	SERVICE	VERSION	PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.0.5	21/tcp	filtered	ftp	
25/tcp	open	smtp	Postfix smtpd	25/tcp	filtered	smtp	
80/tcp	open	http	Apache/2.2.3 ((CentOS))	80/tcp	open	http	Apache/2.2.3 ((CentOS))
8080/tcp	open	http	Apache/2.2.3 ((CentOS))	8080/tcp	open	http	Apache/2.2.3 ((CentOS))
8081/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1	8081/tcp	filtered	blackice-icecap	

Gambar 2. Perbandingan Hasil Scan Nmap Internal Website Email LPSE

Sebelum penerapan DMZ				Setelah Penerapan DMZ			
PORT	STATE	SERVICE	VERSION	PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)	22/tcp	filtered	ssh	
25/tcp	open	smtp	Postfix smtpd	25/tcp	filtered	smtp	
80/tcp	open	http	Apache/2.2.16 ((Debian))	80/tcp	open	http	Apache/2.2.16 ((Debian))
8080/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1	8080/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1
8081/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1	8081/tcp	filtered	blackice-icecap	

Gambar 3. Perbandingan Hasil Scan Nmap Eksternal Website LPSE

Sebelum penerapan DMZ	Setelah Penerapan DMZ
<pre> Not shown: 978 closed ports PORT STATE SERVICE VERSION 21/tcp open ftp vsftpd 2.0.5 25/tcp open smtp postfix smtpd _smtp-commands: mail.lpse.palembang.go.id, PIPELINING, SIZE 10240000, VRFY, ETR _ssl-cert: Subject: commonName=mail.lpse.palembang.go.id/organizationName=Zimbr _Issuer: commonName=mail.lpse.palembang.go.id/organizationName=Zimbra Collabor _Public Key type: rsa _Public Key bits: 1024 _Not valid before: 2014-12-17T11:36:18+00:00 _Not valid after: 2015-12-17T11:36:18+00:00 _MD5: e762 3ae8 3989 8cd5 2d55 2f93 0f72 2db9 _SHA-1: a2bb 8ba2 9d6a 75d8 30a3 6868 a365 5b6b ee4b e018 _ssl-date: 2015-08-07T16:04:58+00:00; +7947ms1 from local time. 53/tcp open domain Mikrotik RouterOS named or OpenDNS Updater 80/tcp open http Apache httpd 2.2.3 ((CentOS)) _http-generator: ERROR: Script execution failed (use -d to debug) _http-methods: No Allow or Public header in OPTIONS response (status code 302) _http-title: Did not follow redirect to http://mail.lpse.palembang.go.id:8080 110/tcp open pop3 Zimbra Collaboration Suite pop3d _pop3-capabilities: EXPIRE(31 USES) XOLIP S/SL5 SASL(PLAIN) TOP UII 113/tcp open rcpbind 2 (RCS #1000000) _rcpinfo: _program version port/proto service _100000 2 111/tcp rcpbind _100000 2 111/udp rcpbind _100024 1 895/udp status _100024 1 896/tcp status 139/tcp open netbios-ssn Samba smb2 3.X (workgroup: WORKGRO 143/tcp open imap-proxy nginx imap proxy _imap-capabilities: BINARY QRESYNC completed LIST-EXTENDED NAMESI WITHIN ID SORT SEARCHRES I18NLEVEL=1 CHILDREN LOGINDISABLED0001 445/tcp open netbios-ssn Samba smb2 3.X (workgroup: WORKGRO 465/tcp open ssl/smtp postfix smtpd _smtp-commands: mail.lpse.palembang.go.id, PIPELINING, SIZE 1024 _ssl-cert: Subject: commonName=mail.lpse.palembang.go.id/organiz _Issuer: commonName=mail.lpse.palembang.go.id/organizationName=Z _Public Key type: rsa _Public Key bits: 1024 _Not valid before: 2014-12-17T11:36:18+00:00 </pre>	<pre> Not shown: 978 closed ports PORT STATE SERVICE VERSION 21/tcp filtered ftp 25/tcp filtered smtp 53/tcp open domain Mikrotik RouterOS named or OpenDNS Updater 80/tcp open http Apache httpd 2.2.3 ((CentOS)) _http-generator: ERROR: Script execution failed (use -d to debug) _http-methods: No Allow or Public header in OPTIONS response (status code 302) _http-title: Did not follow redirect to http://mail.lpse.palembang.go.id:8080 110/tcp filtered pop3 111/tcp filtered rcpbind 139/tcp filtered netbios-ssn 143/tcp filtered imap 145/tcp filtered microsoft-ds 445/tcp filtered smtp 587/tcp filtered submission 993/tcp filtered imaps 995/tcp filtered pop3s 2222/tcp filtered EtherNet/IP-1 3306/tcp filtered mysql 5222/tcp filtered xmpp-client 5269/tcp filtered xmpp-server 7025/tcp filtered vmsvc-2 7777/tcp filtered cbt 8080/tcp open http Zimbra http config _http-methods: GET HEAD POST TRACE OPTIONS _Potentially risky methods: TRACE _See http://nmap.org/nse/doc/scripts/http-methods.html _http-open-proxy: Proxy might be redirecting requests _http-title: Zimbra Web Client Log In 6881/tcp filtered blackice-ircop 10000/tcp filtered snet-sensor-mgmt </pre>

Gambar 4. Perbandingan Hasil Scan Nmap Eksternal Website Email LPSE

4.3 Refleksi atau Pembelajaran (*learning*)

Tahapan ini merupakan bagian akhir untuk mendapatkan kesimpulan dan saran dari penerapan teknik DMZ yang telah diterapkan di LPSE Kota Palembang. Tahapan ini dijelaskan lebih rinci pada bagian akhir Kesimpulan dan Saran.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Penerapan teknik DMZ di *firewall* diharapkan akan dapat memfilter *port* yang terbuka dan menutup celah keamanan di perangkat jaringan (*website* LPSE dan *website email* LPSE yang telah di-*scan* menggunakan *tools* Nmap, atau *tools* lain yang dapat memetakan jaringan (*host discovery*) dari jaringan yang diakses melalui internal maupun eksternal.

5.2 Saran

Penerapan teknik DMZ dapat memberikan alternatif keamanan jaringan kepada *administrator* jaringan agar dapat menerapkan teknik DMZ pada perangkat jaringan selain *server website* LPSE dan *server website email* LPSE.

Daftar Pustaka

- [1] Davison, R. M., Martinsons, M. G. & Kock (2004), *Principles of canonical action research*, Information Systems Journal 14, h. 65-86.
- [2] Hariono, A. (2009), *Apa Itu Port Router*. Diakses 13 Mei 2015, dari <http://www.jaringan-komputer.cv-sysneta.com/port-router>
- [3] Wahyudi, W. (2013), *Konfigurasi MikroTik DMZ (Demilitarized Zone)*. Diakses 14 Mei 2015, dari <http://sapikuda.com/jaringan/membuat-mikrotik-dmz/>
- [4] Panduan Referensi Nmap t. t., *Panduan Referensi Nmap Man Page, Bahasa Indonesia*. Diakses 22 Mei 2015, dari <https://nmap.org/man/id/>
- [5] McCabe, J. D. (2007), *Network Analysis, Architecture, and Design*, Morgan Kaufmann Publishers, United States. Diakses 20 Mei 2015, dari Google Books.