Analisis dan Implementasi Metode Demilitarized Zone (DMZ) untuk Keamanan Jaringan pada LPSE Kota Palembang

Muhammad Diah Maulidin[1], Muhamad Akbar[2], Siti Sa'uda[3]
[1,3] Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Bina Darma Palembang, Indonesia
[1]dedekthamrin@gmail.com, [2] muhamad.akbar@binadarma.ac.id

Abstract. Jaringan internet di pemerintahan 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 addresspublik 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. Maka diperlukan teknik DMZ yang diterapkan pada firewall di router Mikrotik.

Keywords: DMZ, Firewall, LPSE, Router Mikrotik.

1 Pendahuluan

Keamanan jaringan internet merupakan salah satu aspek yang dapat dikembangkan dalam suatu jaringan di pemerintahan 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). LPSE melayani proses pengadaan barang/jasa pemerintah secara elektronik dan transaksi elektronik sesuai peraturan perundang-undangan yang berlaku.

Infrastruktur jaringan di LPSE, terdapat perangkat jaringan yaitu *server website* LPSE Kota Palembang yang berisi aplikasi Sistem Pengadaan Secara Elektronik (SPSE), *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 *server website* LPSE dan *website email* LPSE. Jika *user* berada di *internal* LPSE mengakses *domain server* LPSE dan *server email* LPSE, akan diarahkan ke *ip address* lokal. Jika *user* 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 tersebut, 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.

Firewall adalah suatu sistem yang mengendalikan aliran *traffic* antara jaringan dan memberikan suatu mekanisme untuk melindungi *hosts* yang ada di belakang *firewall*. *Firewall* bisa kita gunakan untuk mengendalikan aliran *traffic* yang mengakses *public resources* yang diletakkan pada DMZ [1]. *Firewall* DMZ (*Demilitarized Zone*) – atau jaringan perimeter adalah jaringan *security boundary* yang terletak diantara suatu jaringan *corporate*/*private* LAN dan jaringan publik (*internet*). Perimeter (DMZ) *network* didesain untuk melindungi *server* pada jaringan LAN *corporate* dari serangan *hackers* [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 menunjukan 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 mengontrol secara tepat apa yang datang dan keluar dari jaringan dalam suatu pertanyaan [3].

Network Mapper (Nmap) merupakan 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].

2 Metode Penelitian

Metodologi penelitian yang dilakukan berdasarkan tahapan *action research* [5]. Tahapan yang dilakukan yaitu sebagai berikut. : 1) Melakukan Diagnosis (*Diagnosing*). Tahapan ini menjelaskan perangkat komputer, software atau tools yang

digunakan dalam penelitian, menganalisis jaringan pada objek penelitian (LPSE Kota Palembang) dengan mengikuti tahapan analisis kebutuhan (*requirements analysis*) sistem jaringan yang dijelaskan oleh McCabe [6], membuat spesifikasi kebutuhan berdasarkan analisis kebutuhan (requirements analysis), membuat peta ruangan, membuat daftar perangkat teknologi informasi (TIK) dan membuat topologi jaringan, 2) Membuat Rencana Tindakan (*Action Planning*). Tahapan ini menganalisis informasi jaringan pada objek penelitian (LPSE Kota Palembang) menggunakan tools Nmap dan menjelaskan hasil *scan tools* tersebut, 3) Melakukan Tindakan (*Action Taking*). Tahapan ini menjelaskan 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 Nmap, terdapat celah *port* yang terbuka di setiap *server* yang harus ditutup atau di-*filter*. Implementasi yang diterapkan yaitu mengkonfigurasi jaringan pada router Mikrotik di bagian firewall menggunakan program Winbox, 4) 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)sebelum menerapkan teknik DMZ, dan setelah menerapkan teknik DMZ, dan 5) Refleksi atau Pembelajaran (*Learning*). Tahapan ini merupakan bagian akhir untuk mendapatkan kesimpulan dari penerapan teknik DMZ yang telah diterapkan di LPSE Kota Palembang. Tahapan ini dijelaskan lebih rinci pada bagian akhir yaitu Kesimpulan.

3 Hasil dan Pembahasan

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

3.1 Evaluasi Scan Nmap *Internal Website* LPSE

Sebelum menggunakan DMZ ditemukan 8 (delapan) *port* terbuka. Selanjutnya setelah diterapkan DMZ, 5 (lima) *port* dapat di-*filter*, sedangkan 3 (tiga) *port* masih terbuka.

Tabel 1. Perbandingan Hasil *Scan* Nmap *Internal Website* LPSE

No	Port	Service	State Sebelum Penerapan DMZ	State Setelah Penerapan DMZ
1	22/tcp	ssh	Open	Filtered
2	25/tcp	smtp	Open	Filtered
3	53/tcp	domain	Open	Open
4	80/tcp	http	Open	Open
5	5432/tcp	postgresql	Open	Filtered

No	Port	Service	State Sebelum Penerapan DMZ	State Setelah Penerapan DMZ
6	8009/tcp	ajp13	Open	Filtered
7	8080/tcp	http	Open	Open
8	8081/tcp	http	Open	Filtered

3.2 Evaluasi Scan Nmap *Internal Website Email* LPSE

Sebelum menggunakan DMZ ditemukan 22 (dua puluh dua) *port* terbuka. Selanjutnya setelah diterapkan DMZ, tinggal 3 (tiga) *port* yang masih terbuka.

Tabel 2. Perbandingan Hasil *Scan* Nmap *Internal Website Email* LPSE

No	Port	Service	State Sebelum Penerapan DMZ	State Setelah Penerapan DMZ
1	21/tcp	ftp	Open	Filtered
2	25/tcp	smtp	Open	Filtered
3	53/tcp	domain	Open	Open
4	80/tcp	http	Open	Open
5	110/tcp	pop3	Open	Filtered
6	111/tcp	rpcbind	Open	Filtered
7	139/tcp	netbios-ssn	Open	Filtered
8	143/tcp	imap-proxy	Open	Filtered
9	445/tcp	netbios-ssn	Open	Filtered
10	465/tcp	ssl/smtps	Open	Filtered
11	587/tcp	smtp	Open	Filtered
12	993/tcp	ssl/imap-proxy	Open	Filtered
13	995/tcp	ssl/pop3	Open	Filtered
14	2222/tcp	ssh	Open	Filtered
15	3306/tcp	mysql	Open	Filtered
16	5222/tcp	jabber	Open	Filtered
17	5269/tcp	jabber	Open	Filtered
18	7025/tcp	lmtp	Open	Filtered
19	7777/tcp	cbt?/socks5	Open	Filtered
20	8080/tcp	http	Open	Open
21	8081/tcp	http-proxy	Open	Filtered
22	10000/tcp	http	Open	Filtered

3.3 Evaluasi Scan Nmap *External Website* LPSE

Sebelum menggunakan DMZ ditemukan 6 (enam) *port* terbuka. Selanjutnya setelah diterapkan DMZ, 5 (lima) *port* dapat di-*filter*, sedangkan 2 (dua) *port* masih terbuka.

Tabel 3. Perbandingan Hasil *Scan* Nmap *External Website* LPSE

No	Port	Service	State Sebelum Penerapan DMZ	State Setelah Penerapan DMZ
1	22/tcp	ssh	Open	Filtered
2	25/tcp	smtp	Filtered	Filtered
3	80/tcp	http	Open	Open
4	5432/tcp	postgresql	Open	Filtered
5	8009/tcp	ajp13	Open	Filtered
6	8080/tcp	http	Open	Open
7	8081/tcp	http	Open	Filtered

3.4 Evaluasi Hasil Scan Nmap External Website Email LPSE

Sebelum menggunakan DMZ ditemukan 22 (dua puluh dua) *port* terbuka. Selanjutnya setelah diterapkan DMZ, tinggal 2 (dua) *port* yang masih terbuka.

Tabel 3. Perbandingan Hasil *Scan* Nmap *External Website* LPSE

No	Port	Service	State Sebelum Penerapan DMZ	State Setelah Penerapan DMZ
1	21/tcp	ftp	Open	Filtered
2	25/tcp	smtp	Filtered	Filtered
3	53/tcp	domain	Open	Filtered
4	80/tcp	http	Open	Open
5	110/tcp	pop3	Open	Filtered
6	111/tcp	rpcbind	Open	Filtered
7	139/tcp	netbios-ssn	Open	Filtered
8	143/tcp	imap-proxy	Open	Filtered
9	389/tcp	ldap	Open	Filtered
10	445/tcp	netbios-ssn	Open	Filtered
11	465/tcp	ssl/smtps	Open	Filtered
12	587/tcp	smtp	Open	Filtered
13	993/tcp	ssl/imap-proxy	Open	Filtered
14	995/tcp	ssl/pop3	Open	Filtered
15	2222/tcp	ssh	Open	Filtered
16	3306/tcp	mysql	Open	Filtered
17	5222/tcp	jabber	Open	Filtered
18	5269/tcp	jabber	Open	Filtered
19	7025/tcp	lmtp	Open	Filtered
20	7777/tcp	cbt?/socks5	Open	Filtered
21	8080/tcp	http	Open	Open
22	8081/tcp	http-proxy	Open	Filtered
23	10000/tcp	http	Open	Filtered

4 Kesimpulan

Informasi jaringan yang telah diterapkan pada LPSE Kota Palembang) adalah terdapat celah keamanan pada port service perangkat jaringan (*server website* LPSE dan *server website* mail LPSE) yang aksesnya terbuka, dimana informasi celah keamaman pada perangkat jaringan didapat dari *scan tools* Nmap.

Konfigurasi jaringan *firewall* yang ditingkatkan menggunakan metode/teknik DMZ berdasarkan *Network Address Translation* (NAT) dengan menentukan *ip address* lokal dan publik dari perangkat jaringan (*server website* LPSE dan *server website mail* LPSE), dan *Port Addressable Translation* (PAT) dengan menentukan *port service* yang aksesnya di-*filter* atau ditutup dan *Access List* dengan membolehkan hak akses administrator jaringan yang dapat mengakses port tertentu, seperti port 22 ssh untuk memperbaiki jika terdapat kendala atau gangguan pada *server* jaringan.

Daftar Pustaka

1. K. Grinsing. (2009). *Apa Itu Port Router*. Available: http://www.jaringan-komputer.cv-sysneta.com/port-router
2. K. Grinsing. (2010). *Memahami Firewall DMZ*. Available: http://www.jaringan-komputer.cv-sysneta.com/memahami-firewall-dmz
3. W. Wahyudi, "Konfigurasi MikroTik DMZ (Demilitarized Zone)," ed, 2013.
4. G. Lyon. (2009). *Panduan Refensi Nmap (Man Page, bahasa Indonesia)*. Available: https://nmap.org/man/id/
5. R. Davison*, et al.*, "Principles of canonical action research," *Information Systems Journal,* vol. 14, pp. 65-86, 2004.
6. J. D. McCabe, *Network analysis, architecture, and design*: Morgan Kaufmann, 2010.