ANALISIS IMPLEMENTASI ROUTING PROTOCOL AUTHENTICATION PADA JARINGAN MPLSVPN-L3VPN

Ceisar Maulana Shabirin[1], Rendy Munadi [2], Yudha Purwanto[3]

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

Abstrak

Nama : Ceisar Maulana Shabirin Pembimbing I : Dr. Rendy Munadi, Ir., MT. NIM : 1101091135 Pembimbing II: Yudha Purwanto. ST,. MT.

ANALISIS IMPLEMENTASI ROUTING PROTOCOL AUTHENTICATION PADA JARINGAN MPLSVPN-L3VPN

Semakin tingginya kebutuhan akan jaringan internet membuat terjadinya pengembangan untuk jaringan internet. Diantaranya high speed internet access dan secure network. Jaringan dengan tingkat keamanan yang tinggipun menjadi suatu keharusan untuk diperhatikan, kebocoran informasi data yang dilewatkan melalui jaringan adalah hal yang sangat dihindari, sehingga dapat disimpulkan akses internet cepat juga sangat membutuhkan kamanan jaringan yang memadai. MPLS (Multi Protocol Label Switching) adalah suatu metode forwarding yang mempersingkat waktu pembacaan destination address paket sehingga paket lebih cepat diteruskan ke hop selanjutnya. Karena itulah muncul juga MPLS VPN, dengan mengandalkan skalabilitas dan traffic engineering sebagai keamanan sisi confidentiality[10]. Bagaimana dengan informasi sistem peroutingan, maka kita dapat menggunakan Routing Protocol Authentication yang merupakan metode autentikasi yang dibuat untuk memberikan autentikasi pada tiap informasi routing yang berada di dalam paket. Sehingga mencegah adanya serangan pada paket informasi peroutingan[2].

Pada tugas akhir ini akan dibahas masalah keamanan pada sisi integrity dari man-in-the-middle-attack, menggunakan sistem autentikasi di setiap peer MPLS, dengan menggunakan teknologi Routing Protocol authentication.

Dari pengujian dapat disimpulkan bahwa informasi peroutingan sangat mudah untuk didapatkan sehingga membutuhkan autentikasi pada tiap header-nya yang kemudian dienkripsi dengan fungsi hash MD5. Dengan adanya autentikasi ini dibutuhkan waktu untuk melakukan cracking agar dapat mengirim paket spoof dari penyerang ke arah router sehingga penyerang dikenali sebagai bagian dari jaringan yang seharusnya. Dan MD5 sendiri masih mampu untuk melindungi paket, dengan menggunakan key atau password yang kuat dan dijaga kerahasiaannya.

Kata Kunci : MPLS, routing protocol authentication, man-in-the-middle, MPLSVPN.

Abstract

Name : Ceisar Maulana Shabirin 1st Advisor : Dr. Rendy Munadi, Ir., MT. NIM : 1101091135 2nd Advisor : Yudha Purwanto. ST,. MT. IMPLEMENTATION OF ANALYSIS OF ROUTING PROTOCOL AUTHENTICATION ON MPLSVPN-L3VPN

Increasingly high demand for the development of the Internet network to make Internet network . Among them high speed internet access and secure network . Network security level become a necessity for attention , information leakage data passed over the network is a very avoidable , so it can be concluded fast internet access is also urgently need to secure an adequate network . MPLS (Multi Protocol Label Switching) is a method of forwarding that shorten the time reading a destination address so that the package faster packet is forwarded to the next hop . Because that appears too MPLS VPN , relying on scalability and traffic engineering as the security confidentiality [10] . What information peroutingan system , then we can use the Routing Protocol Authentication is an authentication method that is designed to provide authentication of each routing information inside the package . So as to prevent any attacks on peroutingan information package [2].

In this thesis will discuss security issues in the integrity of the man-in - the-middle - attack , using the authentication system at each peer MPLS , Routing Protocol using authentication technology .

From the test it can be concluded that the information peroutingan very easy to obtain and thus require authentication on each of his header is then encrypted with the MD5 hash function . Given this authentication takes time to do the cracking that can send packets from the attacker to spoof the direction of the router so that the attacker identified as part of a network that is supposed to be . And MD5 itself is still able to protect the package , using the key or strong password and is kept confidential .

Keywords : MPLS , routing protocol authentication , man-in - the-middle , MPLSVPN

BAB I

PENDAHULUAN

1.1 Latar Belakang

Semakin tingginya kebutuhan akan jaringan internet membuat terjadinya pengembangan untuk internet. Diantaranya *high speed internet access* dan *secure network*. Dengan begitu kebutuhan akan jaringan internet yang terus meningkat akan dapat terpenuhi, hal ini mepengaruhi tuntutan agar jaringan backbone lebih cepat dan aman, Sehingga para ISP untuk memenuhi kebutuhan tersebut menggunakan teknologi MPLSVPN, karena MPLSVPN mendukung *traffic engineering* dan skalabilitas jaringan yang tinggi[10] dan memiliki juga toleransi yang baik pada jaringan[3] sehingga tidak terlalu mengganggu performansi jaringan yang ada. Dari sisi lain penggunaan VPN hanya menjaga jaringan pada sisi *confidentiality*-nya saja. Sehingga untuk sisi lainnya seperti *integrity* masih rentan akan serangan yang dapat menggangu jaringan, diantaranya adalah informasi sistem seperti peroutingan yang dapat dengan mudah dimodifikasi dan digunakan untuk mengganggu jaringan dengan misalnya mengubah peroutingan jaringan itu sendiri. Sehingga dibutuhkannya sistem keamanan yang dapat menjaga informasi ini, dan informasi ini dapat dilindungi dengan memberikan sistem autentikasi pada proses informasi sistem itu sendiri, dengan menggunakan *Routing Protocol Authentication* data routing yang ada akan diberikan kunci dan dienkripsi dengan algoritma MD5, sehingga menghasilkan *chipertext* yang hanya dapat didekripsi pada router yang dikenal dan memiliki kunci yang sama/benar, dan paket-paket yang tidak dikenal dapat dicegah masuk ke router, dengan begitu semua paket informasi routing yang merupakan paket untuk menyerang jaringan pada router akan ditolak

Pada Tugas akhir ini dibahas masalah keamanan MPLSVPN-L3VPN dari serangan *man-in-the-middle-attack*, dengan menggunakan *Authentication* pada *routing protocol*-nya. Penulis akan menganalisis implementasi ini untuk mencegah dari serangan pada informasi peroutingan yang digunakan pada jaringan yang dibangun dari serangan *man-in-the-middle* yang akan dilakukan dengan menggunakan tool LOKI dan *wireshark*. Dan hasil yang didapat adalah pemasangan *routing protocol*

authentication dapat mencegah terjadinya *spoofing* paket informasi yang tidak dikenal oleh router, dengan menggunakan kunci yang panjang dan unik, akan menyulitkan untuk melakukan serangan *brutforce* untuk mengetahui kuncinya.

1.2 Tujuan

Tujuan dari tugas akhir ini adalah:

1. Merancang dan membangun jaringan MPLSVPN-L3VPN.
2. Mengimplementasikan *Rouitng Protocol Authentication* pada komponen MPLSVPN-L3VPN.
3. Melakukan analisis integritas jaringan yang telah dibangun.
4. Melakukan serangan *man-in-the-middle* pada sisi CE, PE, dan P jaringan yang dibangun.
5. Melakukan analisis keamanan pada jaringan *backbone* MPLS VPN *layer* 3 dan diimplementasikan *Rouitng Protocol Authentication*, dan menganalisis Autentikasinya, dan juga menganalisis perubahan QOS setelah penerapan autentikasi pada *routing protocol*.

1.3 Rumusan Masalah

Rumusan masalah pada tugas akhir ini adalah:

1. Bagaimana membangun jaringan MPLS?
2. Bagaimana mengimplementasikan *routing protocol authentication* pada jaringan MPLS.
3. Bagaimana membangun hubungan untuk komunikasi baik dengan VoIP,?
4. Bagaimana melakukan *sniffing* pada jaringan MPLS yang telah dibangun?, dan melakukan *Spoofing* pada jaringan.
5. Bagaimana melakukan analisis QOS pada MPLS yang telah dibangun?

1.4 Batasan Masalah

Batasan masalah dari tugas akhir ini adalah:

1. Jaringan yang dibangun adalah jaringan *private*. hanya membahas informasi yang ada pada jaringan, berbasis Ipv4.
2. Menganalisis keamanan pada sisi integritas jaringan.
3. Menggunakan CISCO IOS di GNS3.
4. Menggunakan mekanisme MPLS, mekanisme *man-in-the-middle*.

5. Hanya membahas penggunaan VoIP.
6. Metode *spoofing* dan *cracking* dengan menggunakan LOKI.
7. Metode *sniffing* dan analisis QOS dengan menggunakan *Wireshark*.

1.5 Metodologi

Metodologi yang digunakan dalam pembuatan tugas akhir ini adalah:

1. Studi Literatur

   Melakukan pengumpulan literatur-literatur berupa jurnal, artikel, buku referensi, dan sumber lain untuk memahami dan mendalami konsep.
2. Perancangan dan Realisasi

   Merancang dan membangun jaringan backbone dengan 1 PC untuk 6 router cisco pada GNS3, 1 buah server, 2 pc *client*. 1 pc *attacke*r.
3. Pengujian dan Analisls implementasi.
4. Pengambilan kesimpulan dan penyusunan laporan.

1.6 Sistematika

Sistematika penulisan Tugas Akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Membahas tentang latar belakang masalah, tujuan, rumusan masalah, batasan masalah, metodologi, dan sistematika penulisan.

BAB II DASAR TEORI

Membahas teori tentang MPLS, VPN, Aspek keamanan, jenis serangan, *routing protocol* dan dengan *authentication*, VoIP, dan Quality of Service.

BAB III PERANCANGAN DAN IMPLEMENTASI

Merancang konfigurasi jaringan MPLS, menerapkan *Routing Protocol Authentication* pada jaringan MPLSVPN-L3VPN.

BAB IV PENGUJIAN DAN ANALISIS HASIL IMPLEMENTASI

Berisi tentang hasil pengujian dan analisis, analisis integritas jaringan dan tentang hasil dari *attack* dan pengaruh keamanan yang dipasang terhadap jaringan.

BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan yang didapat dari pembahasan dan analisis bab sebelumnya, serta saran yang dibutuhkan untuk pengembangan selanjutnya.

BAB V

KESIMPULAN dan SARAN

5.1 Kesimpulan

Berdasarkan hasil proses implementasi, pengujian, penelitian yang telah dilaksanakan. Maka dapa disimpulkan sebagai berikut:

1. Implementasi dari MPLSVPN-L3VPN berhasil dilakukan, terbukti dengan komunikasi VoIP yang dapat dilakukan dengan melewati jaringan yang telah dibangun tersebut.
2. Hasil dari analisis keamanan dengan menggunakan tool LOKI telah menunjukan bahwa implementasi *routing protocol authentication* pada jaringan MPLSVPN-L3VPN cukup aman, asalkan kunci yang digunakan pada jaringan lebih panjang dan lebih unik mengunakan semua karakter (huruf besar/kecil, simbol, angka), penyerang tidak mengetahui key yang terlewati, dan pengguna mengganti password-nya secara periodik, karena fungsi hash MD5 sudah umum digunakan sehingga sudah banyak developer yang menbuat program untuk *cracking* data yang ter-enkripsi tersebut, dan membuat proses *cracking* itu sendiri jadi lebih singkat.
3. Hasil pengukuran QOS menunjukan performansi yang baik setelah implementasi dan tidak membebani jaringan MPLSVPN itu sendiri[3]. sebelum dan ataupun sesudah implementasi, sistem autentikasi pada jaringan. Performasinya masih bisa dibilang baik. Terlihat dengan tidak melewati batas standar dari ITU-T, Cisco, dan thipon. Delay paling besar dimiliki BGP dan masih dibawah standar >11.7% dimana standar 0-150 ms, sehingga bila memang menjadi perubahan hanya akan menambah delay >11.7% dari delay aslinya.

5.2 Saran

Saran yang dapat diajukan untuk penelitian lebih lanjut adalah

1. Perlu dicobanya fungsi hash yang lain selain MD5 seperti SHA, Blowfish, atau lainnya.

2. Perlu dicobanya untuk mencari cara lain untuk melindungi integrity dari jaringan. Seperti firewall atau filtering pada jaringan.
3. Untuk penelitian selanjutnya digunakan tool yang lebih banyak dan kompleks untuk penyerangannya, mengkombinasikan semua tool memungkinkan untuk *attack* bagian integrity.

DAFTAR PUSTAKA

[1] Al-Saud K.A.; Hatim T.; M. Saleh. 2009. “A Performance Comparison of MD5 Authenticated Routing Traffic with EIGRP, RIPv2, and OSPF”. The International Journal Arab Journal of Information Technology, Vol 7, No. 4, October 2010.

[2] Alberth, N and Rickard von Essen. mei 2006. “Security In Internet Routing Protocols”. Linkoping Institute of Technology, 8 mei 2006.

[3] Alouneh, S and Sa’ed Abed, 2010, “Fault Tolerance and Security Isddues in MPLS Networks”, in proceeding ACS'10 Proceedings of the 10th WSEAS international conference on Applied computer science, Wincosin, USA, pp. 134-138 .

[4] Authukuri, P. 2012. “Multiprotocol Label Switching Layer 3 Virtual Private Networks with Open ShortestPath First protocol”. International Journal of Engineering Research and Aplication, Vol. 2, pp. 1638-16422, Maret-April 2012.

[5] B. Quinn. RFC3170. IP Multicast Application: chalanges and solutions. 2001.

[6] Behringer, Michael, dkk. *MPLS VPN Import/Export Verification. Cisco System Inc.* 2002.

[7] Cisco Networking Academy. *CCNA 4 Accessing The WAN*. Cisco System, Inc. 2007.

[8] Fischer, Thorsten. 2007. “MPLS Security Overview”. IRM Research White Paper.

[9] Gupta, R.K. Arvind K. Pankaj. Omjeet. 2013. “Analyzing Multi Protocol Label Switching Network”. International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, Juni 2013.

[10] Harb. Eng. Hussein M, *MPLS VPN*.ITU-D, Arab, 2009.

[11] Kaur, G and Dinesh Kumar. 2010, “MPLS Technology on IP Backbone Network”. International Journal of Computer Applications, Volume 5- No.1, Agustus 2010.

[12] Mehta, Tomy S. 2012. “PERANCANGAN DAN IMPLEMENTASI DATA LOSS PREVENTION PADA ZIMBRA MAIL SERVER BERBASIS UBUNTU ENTERPRISE CLOUD”. Institut Teknologi Telkom.

[13] Munadi. Rendy, *Teknik Switching*, Informartika, Bandung, Mei 2006.

[14] Mondal, Amit and Alexandar K. 2007. "A Poisioning-Resilent TCP Stack". IEEE International Conference. Oktober 2007.

[15] R. Rivest.*RFC 1321 The MD5 Message-Digest Algorithm. Internet Engineering Task Force*, 1992.

[16] Rakheja, P; P. Kaur; Anjali G;Aditi S. 2012. "Performance Analysis of RIP, OSPF, IGRP and EIGRP Routing Protocols in a Network". International Journal of Computer Application, Vol 48, No. 18, Juni 2012.

[17] ERNW,"Loki : Layer 3 will never be the same again ", [online] (https://www.ernw.de/research/loki.html, terakhir diakses 15 januari 2014).

[18] "loki", (http://c0decafe.de, terakhir akses tanggal 15 januari 2014)