paper

by Ery Jullev

Submission date: 21-Aug-2021 05:12PM (UTC+0700)
Submission ID: 1633965119
File name: 122-Article_Text-600-2-10-20191110.pdf (1.32M)
Word count: 3143
Character count: 19305

Kombinasi Port Knocking Dan VPN Guna Pengamanan Akses Secure Shell Pada Cloud Computing

Ery Setiyawan Jullev Atmadji*[1], Bekti Maryuni Susanto[2], Khusnul Hotima[3]
[1,2,3] Jurusan Teknologi Informasi, Politeknik Negeri Jember;
e-mail: ***[1]Ery@polije.ac.id**, [2]bekti@polije.ac.id, [3]khusnul_k@polije.ac.id,

Abstract* - *One form of cloud computing that is commonly used is virtualization, vitalization technology allows sharing resources on one server computer so will reduce the cost of implementing an information system. Data security issues are one aspect that has become a focus in developing information systems and cloud computing, two security threats in cloud computing, namely data loss or leakage and account or service piracy. In order to prevent those two security loopholes, several security models were made, one of which was port knocking by using VPN networks which was a development of network security to prevent data theft using port 22. Using VPN can reduce packet tapping from outside parties who want to retrieve data, and utilize iptables can reject an IP address that is not registered in accessing port 22 and performing a remote server. Port knocking is used as the client entrance to do a remote server through port 22 using a tap configured by the server. This mechanism allows the client to access port 22 even though port 22 is closed, because port knocking also has the principle "open the port if the client requires and close the port again if the client is finished". Thus using IP from tun vpn server and port knocking will make it difficult for outsiders to access the server.

Kata kunci - *Port Knocking, VPN, Cloud Computing, Port.*

Abstrak* - *Salah satu bentuk cloud computing yang lazim digunakan adalah virtualisasi, teknologi virtualisasi memungkinkan melakukan share resource pada satu komputer server sehingga akan menekan biaya implementasi sebuah sistem informasi. Isu keamanan data merupakan salah satu aspek yang menjadi fokus dalam pengembangan sistem informasi dan cloud computing, dua ancaman keamanan pada cloud computing yaitu kehilangan atau kebocoran data dan pembajakan account atau service. Guna mencegah dua celah keamanan tersebut maka dibuatlah beberapa model keamanan salah satunya adalah port knocking pada jaringan VPN yang merupakan pengembangan dari keamanan jaringan guna mencegah pencurian data menggunakan port 22. Penggunaan VPN dapat mengurangi penyadapan paket dari pihak luar yang ingin mengambil data, serta memanfaatkan iptables dapat menolak ip address yang tidak terdaftar saat mengaksess port 22 serta melakukan remote server. Port knocking digunakan sebagai pintu masuk client untuk melakukan remote server melalui port 22 dengan menggunakan ketukan yang telah dikonfigurasi oleh server. Mekanisme ini memungkinkan client dapat mengakses port 22 walau dalam keadaan port 22 tertutup, karena port knocking juga memiliki prinsip "buka port jika klient membutuhkan dan tutup port kembali jika klient sudah selesai". Dengan demikian menggunakan ip dari tun0 vpn server dan port knocking akan sedikit menyulitkan pihak luar untuk melakukan pengaksesan server.

Kata kunci – *Port Knocking, VPN, Cloud Computing, Port.*

I. PENDAHULUAN

Pemanfaatan Teknologi Informasi pada dunia bisnis berkembang dengan sangat cepat khususnya pada pemanfaatan *cloud computing*. Teknologi pada cloud computing yang lazim digunakan adalah virtualisasi, teknologi virtualisasi memungkinkan melakukan *share resource* pada satu komputer server sehingga akan menekan biaya implementasi sebuah sistem informasi [1].

Salah satu teknologi *cloud* yang sering digunakan adalah berbagi sumber daya atau yang lebih sering dikenal dengan nama *resource sharing*. Pada *resource sharing* memiliki permasalahan pada keamanan data yang timbul apabila data tersebut ditransmisikan melalui jaringan dengan sumber terbuka [2].

Dalam melakukan akses pada sebuah mesin virtual, pengguna dapat melakukan akses melalui shell / command prompt yang terhubung pada jaringan internet terbuka, hal inilah yang menjadikan focus pada penelitian ini.

Isu keamanan data merupakan salah satu aspek yang menjadi fokus dalam pengembangan sistem informasi dan cloud computing, dua ancaman keamanan pada cloud computing yaitu kehilangan atau kebocoran data dan pembajakan account atau service [3]. Dua ancaman tersebut sangat krusial karena mempengaruhi

reputasi, kepercayaan mitra, karyawan, dan juga pelanggan sehingga mempengaruhi bisnis [4].

Guna mengatasi permasalahan tersebut maka dibutuhkan sebuah model atau mekanisme yang mampu melakukan pengamanan pada system cloud computing, beberapa keamanan yang pernah digunakan adalah Telnet maupun rlogin, namun keduanya masih memungkinkan penetrasi dari orang-orang yang tidak bertanggung jawab, hal ini dikarenakan mekanisme tersebut tidak melakukan enkripsi terhadap data sebelum dikirim ke server [5].

Salah satu teknologi yang mampu melakukan enkripsi data sebelum mengirimkan ke server adalah Secure Shell (SSH) [3]. Pada SSH, Administrator akan menyediakan layanan Service Remote Access sehingga server dapat diakses. Dengan adanya layanan tersebut maka keadaan port harus terbuka secara terus-menerus, hal ini akan mengakibatkan masalah baru oleh karena itu administrator dapat menggunakan salah satu aplikasi dari firewall yaitu Iptables [6].

Pada penelitian ini akan difokuskan pada efektifitas dari penggabungan antara port knocking dan iptables yang sebagai salah satu model keamanan pada cloud computing.

II. RUMUSAN MASALAH

Berdasarkan latar belakang tersebut,maka permasalahan yang dapat diambil pada penelitian ini yaitu bagaimana membangun sistem keamanan pada SSH dengan menggunakan port knocking pada cloud server pada jaringan VPN (Virtual Private Network) serta melakukan evaluasi hasil kerja dari port knocking di VPN.

III. TINJAUAN PUSTAKA

Beberapa penelitian terdahulu yang mendasari penelitian ini adalah yang dilakukan oleh wahyu purnama [7] yang mengatakan bahwasanya perlindungan pada para administrator pengguna dan pengelolaaan router meningkat dengan akses login harus melalui firewall tindakan tarpit melanjutkan layanan akses login dengan pelabuhan mengetuk, dan lakukan tidak perlu tambahan aplikasi diinstall pada komputer yang digunakan untuk mengakses router, kelamahan pada penelitian ini adalah bahwa kinerja ketika membaca filter firewall pada router diturunkan tetapi tidak terlalu drastic.

Selain itu penelitian yang dilakukan oleh rois awang rimbayani yang memfokuskan pada authentikasi remote server dengan port knocking juga membahas tentang celah keamanan pada kemanan server pada akhir penelitian ini penulis menyatakan terbentuk sistem autentikasi yang cukup aman karena ditupnya port yang sangat penting, yaitu port SSH dari port knocking para pengelola jaringan lebih terbantu selama proses autentikasi ke server yang ia kelola. Dengan demikian akan membuat para attacker harus berusaha lebih keras lagi untuk bisa menembus ke dalam sistem [8].

Pada penelitian yang dilakukan oleh Mohammad Bastian Alifi tentang pengamanan server dengan port knocking dengan menggunakan RSA didapatkan kesimpulan berupa keamanan system dapat ditingkatkan tetapi mempunyai kelemahan yaitu menutup semua port yang terhubung ke internet sehingga koneksi dari luar dapat ditahan, namun dengan menutup semua port maka apabila diperlukan remote akses pada jarak jauh hal ini tidak dapat dilakukan [9].

Guna mengurangi permasalahan pada penelitian-penelitian diatas maka penelitian ini berpusat pada bagaimana melakukan pengamanan remote access SSH dengan menggunakan metode port knocking dan iptables sehingga diharapkan dapat lebih mengamankan proses remote pada komputer server tujuan.

IV. METODE PENELITIAN

Dalam penggabungan antara port knocking dan iptables pada SSH. penulis menggunakan beberapa metode yang meliputi proses studi literature dan pengumpulan kebutuhan, perancangan topologi, konfigurasi iptables dan port knocking pada server, konfigurasi jaringan VPN, serta model pengujian. Berikut urutan metode-metode di atas sebagai berikut.

A. Perancangan Topologi Jaringan

Pada penelitian ini, komputer Client akan mengakses jaringan internet melalui sebuah modem dan akan diteruskan kepada iptables sebagai filtering terhadap ip address yang diperbolehkan masuk ke server, jika memang iptables mengijinkan dan mengenali setiap ketukan yang dilakukan oleh client maka selanjutnya port knocking akan menerima perintah untuk membuka atau menutup port yang dibutuhkan oleh client [10]. Struktur jaringan pada lingkungan pengujian ditunjukkan pada Gambar 1. Selain menggunakan jaringan internet lokal biasa, sistem ini juga dapat mengakses jaringan melalui VPN, dengan client dan server memiliki ip sendiri yang dapat terhubung antar server dan client melalui jaringan VPN. Dengan jaringan VPN maka server dan client dapat memiliki jalur lalu lintas sendiri dalam jaringan internet yang dilewati. Ip tunneling VPN juga dapat melakukan ketukan terhadap port knocking di server. Setelah itu maka client akan dapat meremote server menggunakan ip tunneling.

Gambar 1 Struktur jaringan Pada Lingkungan Pengujian

B. Pengujian

Ujicoba dilakukan dengan menggunakan beberapa skema pengujian, mulai dengan uji coba dengan knocking hingga evaluasi terhadap port knocking pada jaringan VPN.

a. Pengujian pertama dilakukan port knocking
   Pengujian pertama adalah melakukan proses port knocking pada port yang yang telah ditentukan dalam hal ini port yang dilakukan pengujian adalah prot 22 sebagai port default dari SSH.
b. Uji coba VPN server dengan menggunakan client
   Pada tahap pengujian ini client telah mendapatkan sertifikat yang telah dibuat sebelumnya oleh server. Setelah itu client menjalankan sertifikat tersebut untuk mendapatkan ip tunneling dari VPN server. Komputer client akan melakukan pengecekan ip terlebih dahulu guna memastikan bahwa ip tunneling dari VPN sudah didapat. VPN pada client telah diperoleh serta melakukan koneksi VPN untuk memastikan terhubungnya VPN server dan client.

C. Evaluasi terhadap VPN dan port knocking

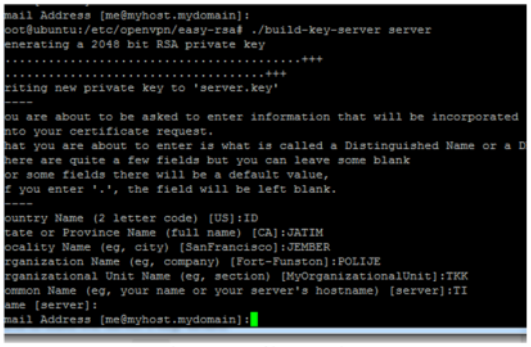
Pada pengujian ini akan dilakukan proses pengujian port knocking pada jaringan private, hal ini diperlukan guna menguji kehandalan dari port knocking itu sendiri

III. Hasil dan Pembahasan

Sebelum melakukan pengujian dengan menggunakan port knocking ada beberapa hal yang harus di perhatikan, salah satunya adalah dalam menentukan setup lingkungan uji untuk koneksi VPN, dalam penelitian ini lingkungan VPN yang digunakan adalah dengan menggunakan openvpn yang telah digabungkan dengan RSA, lingkungan ini diyakini lebih aman daripada OpenVPN standard.

VPN sendiri adalah protokol yang digunakan sebagai jembatan untuk melakukan koneksi antar komputer melalui jaringan publik. Dengan menggunakan vpn maka kemungkinan untuk adanta peretasan data dapat diminimalisir, hal pertama yang harus dilakukan adalah melakukan installasi terhadap openvpn dan openssl, serta memasukan file "./easy-rsa" ke direktori "openvpn " selanjutkan mengganti file tujuan yang ada pada file "vars" dengan "/etc/openvpn /easy-rsa". Konfigurasi File VARS untuk VPN ditunjukkan pada Gambar 2. Dalam konfigurasi vpn dan akses vpn dibutuhkan file sertifikat sebagai koneksi client untuk meminta layanan openvpn pada server. Sertifikat tersebut sebagai kunci server dan client untuk terkoneksi pada jaringan server. Terdapat beberapa perintah untuk membangun file sertifikat diantaranya sertifikat untuk server dan klient. Sertifikat untuk server ditunjukkan pada Gambar 3.

Gambar 2 Konfigurasi File VARS untuk VPN



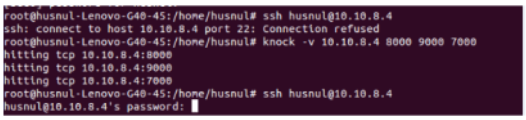
Gambar 3 Sertifikat untuk server

VPN server membutuhkan file konfigurasi yang berekstensi .conf dan file tersebut terdapat pada direktori "openvpn". File tersebut yang akan membaca sertifikat yang telah dibangun sebelumnya serta memberikan ip tunneling terhadap klient yang ingin mengakses melalui vpn. Selanjutnya guna menggabungkan ip tunneling vpn dan ip eth0 pada jaringan lokal server dapat dilakukan dengan menambahkan line akhir pada "contrab –e" dengan line "iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE". Selanjutnya adalah membuat file konfigurasi untuk klient dengan akhiran ".ovpn" yang akan tersimpan pada direktori "/keys".

Setelah proses pembuatan VPN dan *Knocking* selesai selanjutnya adalah melakukan pengujian pada sistem, pada pengujian ini lingkungan pengujian menggunakan server virtualisasi serta client tunggal yaitu ubuntu 14.04 LTS desktop. Skenario dalam pengujian port knocking ini dengan melakukan akses terlebih dahulu tanpa menggunakan port knocking setelah itu client akan terdeteksi bisa mengakses server virtualisasi. Pengujian dengan menggunakan terminal pada ubuntu,wireshark.

Pada pengujian mengaktifkan port knocking dengan cara melakukan penolakan (reject) semua ip yang mencoba masuk dengan memanfaatkan iptables. Maka akan dapat dilihat ketika menggunakan terminal pada

ubuntu ssh server sudah tidak bisa diakses, gambar capture ssh di wireshark juga berubah warna menjadi hitam, warna hitam diibaratkan bahwa port atau protokol dalam keadaan blok atau invalid.



Gambar 4 Percobaan ketukan pada server

Pada gambar 4 Client mencoba melakukan ketukan terhadap server dengan menggunakan ip VPN server untuk melakukan koneksi terhadap port 22 namun port 22 dalam kondisi tertutup, hal itu dikarenakan merupakan port untuk SSh ke server. Ketika melakukan ketukan dengan benar maka ssh dengan ip 10.10.8.4 dapat diakses oleh client yang memiliki ip yang berubah-ubah sesuai dengan ip yang diberikan oleh server jaringan.

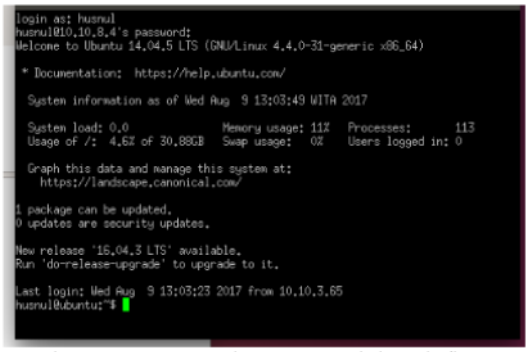
Sedangkan apabila ingin melakukan aktifitas ssh melalui VPN maka melakukan ketukan terlebih dahulu. Sebelumnya ketukan telah ditentukan oleh server pada konfigurasi di server virtualisasi, ketukan tersebut merupakan kunci untuk memasuki pada port 22. Setelah melakukan pengetukan pada port 22 server. Maka ip tun0 client akan dapat mengakses port 22 melalui terminal ubuntu maupun wireshark. Pada wireshark harus masuk terlebih dahulu di interface tun0 untuk mengetahui port 22 berjalan atau masih dalam keadaan terblokir.

Ketika sudah melakukan ketukan maka ip tun0 sudah dapat mengakses ssh pada server serta dapat melakukan aktifitas remote server melalui aplikasi putty yang terdapat pada komputer client.

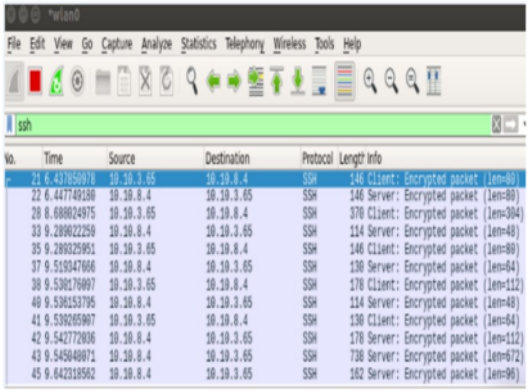
Selanjutnya adalah melakukan pengujian dengan memamntau paket yang keluar dan masuk pada lingkungan pengujian, pada tahapan ini peralatan yang digunakan adalah *wireshark* yang merupakan salah satu alat untuk melakukan pemantauan pada jaringan.

Pada gambar 5 menunjukkan bahwa sebelum port knocking diaktifkan server masih dapat diakses menggunakan aplikasi putty,sehingga server dapat dengan mudah diremote dan client dapat melakukan aktifitas yang ingin dilakukan pada server,namun dengan keberadaan server dalam kondisi seperti ini dapat memicu pihak luar untuk dapat masuk pula ke server. Sehingga perlu adanya port knocking sebagai model keamanan khususnya mengamankan port.

Pada gambar 6 merupakan hasil awal dari wireshark ketika tidak diaktifkan port knocking diserver. Sehingga client masih dapat masuk dan mengakses server serta meremote server melalui putty. Putty digunakan untuk meremote server melalui port 22, karena menggunakan server virtualisasi jadi membutuhkan putty untuk melakukan aktifitas di server. Client dapat menggunakan ip address wlan guna melakukan koneksi ke server, sedangkan server menggunakan ip eth0 untuk memberikan ip DHCP untuk client. Berikut merupakan gambar dari hasil tampilan wireshark.



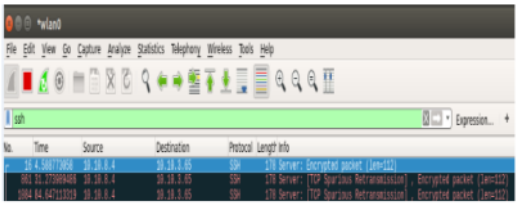
Gambar 5 Remote server dengan putty sebelum aktifkan port knocking



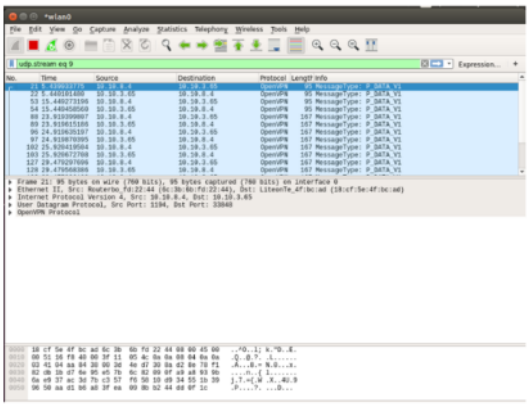
Gambar 6 wireshark sebelum aktifkan port knocking

Pada gambar 7 wireshark menunjukan tampilan yang berbeda dan memiliki warna yang berbeda dari sebelumnya. Warna yang ditampilkan oleh wireshark adalah warna hitam yang mengindikasikan bahwa protocol ssh dalam keadaan memiliki masalah (TCP spurious retransmission(transmisi yang dipalsukan)). Permasalahan ini terjadi karena telah diaktifkannya port knocking pada server, sehingga monitoring pada port 22 di wireshark pun telah berubah menjadi warna hitam.

Pada gambar 8 merupakan tampilan ketika VPN pada server dan client telah diaktifkan, sehingga protocol yang muncul pun adalah protocol openvpn. Dalam protocol ini tidak dapat dilakukan pemanggilan paket-paket yang dibutuhkan untuk ditampilkan seperti paket 22 yang menjadi sasaran dalam penelitian ini. Dalam tampilan tersebut hanya mempersingkat info yang ada dan tidak seperti ketika tidak menggunakan VPN. Berikut merupakan hasil gambar ketika openvpn aktif.



Gambar 7 hasil wireshark setelah port knocking diaktifkan



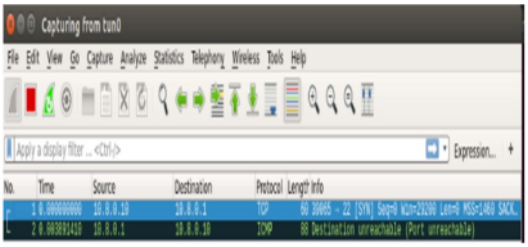
Gambar 8 hasil wireshark dari openvpn

Pada gambar 9 merupakan hasil dari capture tun0 yang ada pada jaringan ini. Dalam tampilan tersebut akan muncul monitoring aktifitas yang terjadi pada jaringan VPN. Pada tampilan diatas merupakan tampilan dari ip tunneling yang mencoba akses ke port 22 di server. Namun terhalang dengan port knocking yang telah diaktifkan sebelumnya. Sehingga tampilan yang muncul menjadi warna hitam yang memiliki arti sebagai permasalahan yang terjadi di protocol jaringan.

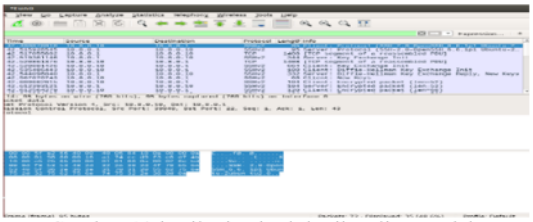
Pada gambar 10 ketika VPN client sudah melakukan ketukan maka tampilan pada tunneling di wireshark pun akan berubah menjadi warna biru muda yang merupakan warna ketika lalu lintas pada UDP berlangsung. Dengan seperti itu maka client dapat melakukan pengaksesan dan remote terhadap ssh server. Dan melakukan aktifitas pada server sesuai dengan kebutuhan.

Pada gambar 11 dalam melakukan sebuah ketukan pada komputer server dengan menggunakan ip address dari jaringan yang sama. Ketukan yang berupa sequence dapat dilihat dengan mudah oleh pihak ke-tiga dan mengetahui kombinasi ketukan yang dilakukan oleh client terhadap port 22 server. Sehingga tidak cukup aman jika hal tersebut dibiarkan serta terdapat celah keamanan pada port 22 sehingga dapat diakses dengan mudah oleh pihak lain yang tidak bertanggung jawab. Oleh karena itu digunakan jaringan VPN untuk membuat sendiri jaringan pribadi yang dalam cakupan lalu lintas jaringan yang dilewati oleh user baik koneksi ke server maupun sebaliknya. Jaringan VPN hanya akan dapat dilewati oleh baik oleh client maupun server yang memiliki akses ip yang diperikan melalui konfigurasi yang disebuk dengan ip tunneling. Ip tersebut akan digunakan untuk mengakses server dan port 22 serta sebagai mekanisme keamanan pada lalu lintas jaringan yang sedang digunakan.

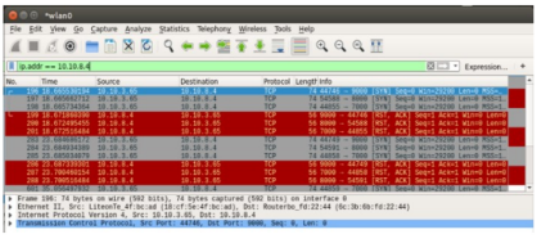
Dengan memanfaatkan wireshark maka akan didapatkan tampilan lalu lintas yang sedang berlangsung antar server dan client pada jaringan VPN, Oleh karena itu protocol yang ditampilkan pun akan menunjukan protocol openvpn sesuai dengan yang digunakan oleh server dan client. Pada jaringan VPN tidak akan membaca paket-paket yang diakses oleh client ke server maupun sebaliknya.



Gambar 9 hasil wireshark tun0 ketika port knocking diaktifkan



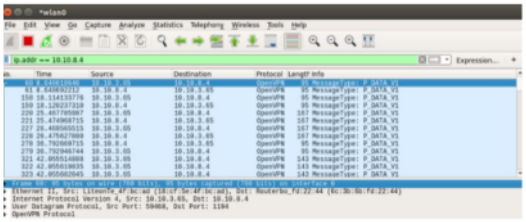
Gambar 10 hasil wireshark ketika client sudah melakukan ketukan



Gambar 11 hasil sequence pada wireshark

Gambar 12 menunjukkan hasil sequence pada jaringan VPN yang menggunakan protocol OpenVPN menunjukan bahwa ketika client melakukan ketukan terhadap port 22 pada server maka tampilan yang ada pada wireshark tetap dalam posisi protocol openvpn,

tidak adanya info seperti ketika client melakukan ketukan terhadap port 22 server tanpa menggunakan VPN. Maka dengan ini penggunaan metode port knocking dalam jaringan VPN bisa dikatakan lebih aman dibanding dengan menggunakan metode port knocking dalam jaringan terbuka.



Gambar 12 hasil sequence pada jaringan VPN

IV. KESIMPULAN

Dari hasil penelitian dan analisa maka dapat ditarik kesimpulan bahwa melakukan akses ssh melalui interface tun0 dengan protocol VPN tanpa menggunakan port knocking dapat dilakukan namun data yang terkirim masih dapat dilihat melalui wireshark.

Sedangkan ketika port knocking telah diaktifkan untuk keadaan tanpa VPN sebelum melakukan ketukan maka akan menghasilkan *destination unreachable* (port unreachable) serta pada terminal client pun SSH pun akan muncul *connection refused* yang berarti koneksi tidak dikenali

Namun pada saat menggunakan jaringan VPN serta client telah melakukan ketukan maka melalui wireshark dapat dilihat lalu lintas yang ada melalui jaringan telah terenkripsi namun tetap dapat melakukan remote melalui SSH.

Sehingga dapat ditarik kesimpulan bahwa salah satu cara dalam melakukan keamanan pada saat melakukan remote pada server dapat dilakukan dengan mengkombinasikan port knocking dengan VPN sehingga data yang dikirimkan melalui jaringan akan terenkripsi sehingga menyulitkan dalam melakukan pencurian data.

DAFTAR PUSTAKA

[1] E. Kurniawan, "PENERAPAN TEKNOLOGI CLOUD COMPUTING DI UNIVERSITAS Studi Kasus : Fakultas Teknologi Informasi UKDW," *Eksis*, vol. 08, no. 01, pp. 29–36, 2015.

[2] C. Aditama and A. Priadana, "IMPLEMENTATION AND PERFORMANCE ANALYSIS OF PRIVATE CLOUD USING OPENSTACK SWIFT DAN RCLONE," vol. III, no. Ix, pp. 317–322, 2018.

[3] V. Farhat, B. Mccarthy, and R. Raysman, "Cyber Attacks : Prevention and Proactive Responses," pp. 1–12, 2011.

[4] B. Nugraha, "Analisis Teknik-Teknik Keamanan Pada Cloud Computing dan NEBULA (Future Cloud): Survey Paper," vol. 02, no. 02, pp. 35–42, 2016.

[5] Simaremare, "Pengembangan Sistem Keamanan Jaringan Intranet UGM Menggunakan Metode IPS (Intrusion Prevention System)," *Ugm*, pp. 0–6, 2007.

[6] RSA Security, "Implementing a secure virtual private network," *Elektron*, vol. 20, no. 9, pp. 38–41, 2003.

[7] W. Purnama, "ANALISIS DAN PERANCANGAN SISTEM PENGAMANAN AKSES OTENTIKASI MENGGUNAKAN METODE PORT KNOCKING DAN FIREWALL ACTION TARPIT PADA MIKROTIK RB951-2n," 2014.

[8] M. D. Adisetya and R. Munadi, "PERANCANGAN SISTEM KEAMANAN SERVER DENGAN AUTENTIKASI PORT KNOCKING," 2010.

[9] R. Anggoro, J. T. Informatika, and F. T. Informasi, "IMPLEMENTASI REMOTE SERVER MENGGUNAKAN METODE PORT KNOCKING DENGAN ASYMMETRIC ENCRYPTION," 2010.

[10] I. Sembiring, "Perancangan dan Implementasi Sistem Keamanan Jaringan dengan Metode Port Knocking untuk Mencegah Http Attack Vulnerability Artikel Ilmiah," no. 672010275, 2014.

paper

ORIGINALITY REPORT

10%	9%	2%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to LL Dikti IX Turnitin Consortium Student Paper	2%
2	officialsitemaunk.blogspot.com Internet Source	2%
3	digilib.uin-suka.ac.id Internet Source	1%
4	pt.scribd.com Internet Source	1%
5	www.pekerjadata.com Internet Source	<1%
6	id.123dok.com Internet Source	<1%
7	Submitted to Harrisburg Christian School Student Paper	<1%
8	jtit.polije.ac.id Internet Source	<1%
9	repositori.usu.ac.id Internet Source	<1%

10	"Analisis Keamanan Lalu Lintas Paket Data Pada Ubuntu Menggunakan Metode Attack Centric", 'Ikatan Ahli Informatika Indonesia (IAII)' Internet Source	<1 %
11	core.ac.uk Internet Source	<1 %
12	eprints.umm.ac.id Internet Source	<1 %
13	www.coursehero.com Internet Source	<1 %
14	netlearning2002.org Internet Source	<1 %
15	www.sciencegate.app Internet Source	<1 %
16	www.bola-mania.net Internet Source	<1 %
17	www.scribd.com Internet Source	<1 %
18	www.ijsr.net Internet Source	<1 %

Exclude quotes	On	Exclude matches	< 3 words
Exclude bibliography	On		