Analisis Penerapan *Virtual Private Network* Menggunakan Tools Hacking

Amarudin[1], Sampurna Dadi Riskiono[2]
[1,2] Teknk Elektro/Universitas Teknokrat Indonesia, Bandar Lampung, Indonesia
[1,2] Jl. ZA Pagaralam, No 9-11, Labuhanratu,Bandar Lampung

e-mail : **[1]amarudin @teknokrat.ac.id, [2]sampurna.go@teknokrat.ac.id**

Abstrak—**Akhir-akhir ini sudah mulai banyak perusahaan yang memanfaatkan protokol *Virtual Private Network* (VPN) sebagai media akses/komunikasi antar jaringan interlokal. VPN adalah sebuah protokol keamanan jaringan yang dapat digunakan sebagai salah satu cara untuk meningkatkan keamanan jaringan dari sisi transmisi data. Dengan pemanfaatan VPN, koneksi antar jaringan dapat terbentuk secara virtual walaupun tidak terbentuk secara fisik. Selain itu, dengan memanfaatkan protokol VPN, *user* (*client*) dapat mengkases Server secara *private* melalui jaringan *public*. Dengan demikian komunikasi antara *Client* dan *Server* terjaga dari *Sniffing* (penyadapan) dari pihak yang tidak bertanggung jawab. Akan tetap tingkat keamanan yang dihasilkan dari penerapan VPN ini perlu dilakukan pengkajian yang lebih dalam. Sehingga tingkat keamanannya dapat diketahui apakah sudah termasuk dalam kategori aman ataukah masih ada peluang bug yang membahayakan dari penetrasi. Dalam penelitian ini dilakukan pengujian *Scanning* dan *Sniffing* pada penerapan VPN menggunakan *toos hacking* yaitu Nmap dan Wireshark. Sedangkan pengujian performansi *service* pada VPN Server, dilakukan pengujian *Denial of Service* (DoS) menggunakan *tools hacking* yaitu LOIC. Adapun objek penelitian ini adalah perangkat Mikrotik RouterOS yang digunakan pada Universitas Teknokrat Indonesia. Hasil penelitian yang didapatkan bahwa komunikasi data antar jaringan (antara VPN Server dan VPN Client) dapat terenkripsi dengan baik. Akan tetapi dari segi konektifitas antar jaringan sangat dipengaruhi oleh performansi *bandwidth* yang digunakan oleh sistem jaringan tersebut. Selain itu berdasarkan hasil pengujian performansi *service* pada VPN Server didapatkan hasil bahwa *service* pada VPN Server dapat dimatikan pada *request* (ping) sebesar 1.899.276 *request*. Hal ini dipengaruhi oleh spesifikasi perangkat Mikrotik RouterOS yang digunakan. Adapun untuk penelitian selanjutnya perlu dilakukan pengujian performansi konektifitas menggunakan bandwith yang lebih besar dan untuk menguji performansi *service* VPN Server menggunakan spesifikasi perangkat Mikrotik yang lebih baik.**

Kata Kunci—*Network Security, Virtual Private Network, Tools Hacking, Denial of Service, Snifing*.

I. PENDAHULUAN

MMempelajari teknologi informasi adalah salah satu hal yang juga perlu dilakukan oleh pegiat komunikasi karena komunikasi tidak bisa dilepaskan dengan perkembangan teknologi informasi. Di Indonesia pun hal yang sama juga terjadi. Ada beberapa hal yang membuat mengapa mempelajari teknologi informasi di Indonesia menjadi penting, salah satunya adalah agar perkembangan dan potensi yang akan terjadi kelak di negara Indonesia ini bisa dimpelajari [1]. Sebagaimana yang dipaparkan oleh kominfo Bandarlampung, bahwa pengguna internet di Indonesia hingga saat ini telah mencapai 82 juta orang. Dengan capaian tersebut, Indonesia berada pada peringkat ke-8 di dunia [2]. Seiring dengan pesetnya perkembangan teknologi informsi ini, mulai banyak perusahaan atau lembaga formal maupun non formal yang memanfaatkan jaringan komputer sebagai sarana komunikasi. Akan tetapi, perkembangan teknologi informasi ini akan membawa dampak negatif jika dalam penggunaanya tidak disertai dengan pengelolaan yang baik. Salah satunya adalah akan

Received August 29th, 2019; Revised September 3rd, 2019; Accepted September 8th, 2019

munculnya peluang penyalahgunaan informasi dari pihak-pihak yang tidak bertanggung jawab alias hacker. Hacker (peretas) adalah orang yang mempelajari, menganalisis, memodifikasi, menerobos masuk ke dalam komputer dan jaringan komputer, baik untuk keuntungan atau dimotivasi oleh tantangan [3]. Selain adanya hacker yang mengancam terhadap keamanan sistem informasi, ada beberapa hal lain yang dapat mengancam keamanan sistem informasi tersebut, yaitu adanya serangan virus mematikan yang disebut dengan serangan *ransomware*. Virus ini sempat menggegerkan dunia pada tahun 2017. Verus tersebut telah menyerang berbagai perangkat jaringan dengan cara melumpuhkan berbagai perangkat dan jaringan komputer di berbagai negara di dunia. Diantaranya mengganggu produksi pabrik mobil Perancis, Renault, mengusik sistem Bank Sentral Rusia, serta mengacaukan sistem jaminan kesehatan nasional Inggris [4].

Untuk mengantisipasi adanya berbagai macam serangan keamanan jaringan, perlu dilakukan penelitian dan pengembangan sistem keamanan. Salah satunya adalah melakukan peningkatan keamanan sistem dengan cara membangun keamanan media transmisi yang digunakan. Salah satu protokol yang dapat digunakan untuk meningkatkan keamanan media transmisi dalam jaringan komputer yaitu protokol *Virtual Private Networ* (VPN). VPN merupakan sebuah metode yang digunakan untuk membangun jaringan yang menghubungkan antar node jaringan secara aman/terenkripsi dengan memanfaatkan jaringan publik (Internet/WAN). Contoh implementasinya adalah pada sebuah network yang terdiri dari beberapa kantor di lokasi yang berbeda, jika kemudian dibangun *link wireless* atau fiber optik maka akan membutuhkan biaya besar, padahal bisa jadi antar kantor tersebut berada di kota atau bahkan pulau yang berbeda. Dengan VPN, maka bisa membangun sebuah link antar kantor dengan memanfaatkan jaringan internet yang sudah ada. Link yang terbentuk diamankan dengan enkripsi sehingga meminimalisir kemungkinan data akan diakses oleh orang yang tidak bertanggung jawab [5]. Oleh karena itu, performansi dalam penerapan VPN ini perlu dianalisis dengan tujuan untuk mengetaui tingkat keamanan yang dihasilkan dalam enkripsi maupun dekripsi, serta untuk mengetahui tingkat performansi *service* yang ada pada VPN Server.

II. LANDASAN TEORI

A. Virtual Private Network

Pengembangan keamaan jaringan pada media transmisi dapat dibangun menggunakan protokol VPN. Sehingga untuk mengakses jaringan lokal dapat menggunakan atau memanfaatkan jalur publik [5]. Secara garis besar, cara kerja protokol VPN ini terdiri dari dua fungsi pokok. Pertama, berfungsi sebagai enkripsi dan dekripsi data. Dan fungsi kedua, dapat memanfaatkan jalur *public* (internet) seolah-olah menjadi jalur *private* (lokal). Salah satu *service* yang digunakan dalam membangun konfigurasi VPN ialah menggunakan *Point to Point Tunnel Protocol* (PPTP). Sebuah koneksi PPTP terdiri dari Server dan Client. PPTP ini ada dalam Mikrotik RouterOS yang bisa difungsikan baik sebagai server maupun client atau bahkan diaktifkan keduanya bersama dalam satu mesin yang sama. *Feature* ini sudah termasuk dalam *package* PPP sehingga perlu dicek di menu *system package* apakah paket tersebut sudah ada di router atau belum. Fungsi PPTP Client juga sudah ada di hampir semua OS, sehingga bisa menggunakan Laptop/PC sebagai PPTP Client [6]. Pemanfaatan VPN ini ialah digunakan sebagai salah satu alternatif cara dalam mengamankan jaringan dari pihak yang tidak bertanggung jawab yang biasanya disebut dengan hacker.

B. Hacker dan Cracker

Hacker (peretas) adalah orang yang mempelajari, menganalisis, memodifikasi, menerobos masuk ke dalam komputer dan jaringan komputer, baik untuk keuntungan atau dimotivasi oleh tantangan [3]. Berbeda halnya dengan hacker, cracker melakukan kegiatan hacking dengan niat yang buruk, seperti mencuri sebuah data, menghancurkan program yang sudah ada, atau merusak keamanan suatu sistem. Para cracker biasanya menggunakan alat tertentu dalam proses hackingnya sehingga banyak dari cracker tidak tahu cara mengembalikan sistem yang sudah di rusak. Karena niatnya yang buruk dari awal mereka tidak mempedulikan nasib dari pembuat/pemilik suatu sistem keamanan atau program tersebut [7].

C. Reconnaissance

Reconnaissance adalah langkah untuk mengumpulkan semua informasi tentang target. Langkah ini sangat penting, karena akan menentukan strategi apa dan *tools* apa saja yang akan digunakan dalam melakukan pengujian sistem keamanan [8].

D. Scanning

Scanning adalah tahap untuk mengetahui IP dari komputer target, Sistem Operasi komputer target, layanan apa saja yang tersedia dan celah keamanan apa saja yang ada pada komputer target [8]. Dengan diketahuinya layanan yang digunakan target, maka akan bisa lebih mudah untuk melakukan ke tahap exploitasi sistem. Dalam tahap melakukan *scanning* biasanya menggunakan aplikasi Nmap yang berfungsi untuk mengetahui sistem operasi target, *service* yang digunakan, port berapa saja yang terbuka, dan celah keamanan (*vulnerability*) apa saja yang ada pada komputer target.

E. Sniffing

Sniffing adalah pekerjaan menyadap paket data yang lalu-lalang di sebuah jaringan. Paket data ini bisa berisi informasi mengenai apa saja, baik itu *user name*, apa yang dilakukan pengguna melalui jaringan, termasuk mengidentifikasi komputer yang terinfeksi virus, sekaligus melihat apa yang membuat komputer menjadi lambat dalam jaringan. Bisa juga untuk menganalisa apa yang menyebabkan jaringan macet. Jadi bukan sekedar untuk kejahatan, karena semuanya tergantung penggunanya, tapi umumnya dilakukan karena iseng [9]. *Sniffing* merupakan cara untuk melihat paket-paket berupa data yang keluar maupun masuk pada sebuah jaringan komunikasi. Sebagai contohnya komputer yang terhubung dengan jaringan LAN atau pada WLAN, kemudian paket-paket tersebut disusun ulang sehingga data yang dikirimkan oleh pihak tertentu dapat dilihat oleh orang yang melakukan *sniffing*. Sniffing juga bisa digunakan untuk pertahanan jaringan. Pertahanan yang dimaksud yaitu dengan cara melakukan penganalisaan paket-paket yang lewat pada suatu jaringan. Apakah paket tersebut berbahaya atau tidak, mengandung virus atau tidak yang mungkin dapat mengancam performa jaringan itu sendiri [10].

F. Exploitation

Exploitation adalah sebuah kegiatan penyerangan pada sistem komputer, yang dilakukan oleh penyusup dengan tujuan utama untuk memanfaatkan kerentanan tertentu yang ada pada sistem. Eksploitasi keamanan ada dalam berbagai bentuk dan ukuran. Beberapa kerentanan keamanan berbasis web yang paling umum termasuk serangan *SQL injection, cross-site scripting* dan *cross-site request forgery*, serta penyalahgunaan kode otentikasi yang rusak atau kesalahan konfigurasi keamanan. Eksploitasi komputer dapat ditandai dengan hasil serangan yang terjadi, seperti *denial of service, remote code execution, privilege escalation*, pengiriman malware atau tujuan jahat lainnya. Eksploitasi komputer juga dapat ditandai dengan jenis kerentanan yang dieksploitasi, termasuk *eksploitasi buffer overflow, code injection*, atau jenis kerentanan validasi masukan lainnya dan serangan *side-channel*. [11].

G. Denial of Service (DoS)

Denial of Service (DoS) adalah jenis serangan yang tujuannya adalah mencegah pengguna yang sesungguhnya menikmati layanan yang diberikan server. Server sesuai namanya adalah pelayan yang harus selalu siap melayani permintaan pengguna, yang umumnya beroperasi 24 jam tanpa henti. Contohnya adalah web server yang bertugas melayani pengunjung web menyediakan informasi dalam bentuk halaman html. Dalam kondisi normal, pengunjung dapat meminta *resource* dari web server untuk ditampilkan dalam *browser*-nya, namun bila web server terkena serangan DoS maka pengunjung tidak bisa menikmati layanan web server [12].

H. Wireshark

Salah satu aplikasi yang paling banyak digunakan oleh para hacker maupun cracker antara lain Wireshark, Ettercap, IPScan, LOIC, dan lain-lain. Wireshark adalah program penganalisa

jaringan yang sangat populer saat ini, walaupun program ini kebanyakan dikenal bukan karena fungsi utamanya melainkan karena sering digunakan untuk keperluan hacking pemula. Dengan kata lain bahwa Wireshark adalah program *Network Protocol Analyzer* alias penganalisa protokol jaringan yang lengkap. Program ini dapat merakam semua paket yang lewat serta menyeleksi dan menampilkan data tersebut sedetail mungkin, misalnya postingan komentar di blog atau bahkan *username* dan *password* [13].

I. Nmap

Nmap (*Network Mapper*) adalah sebuah aplikasi atau *tool* yang berfungsi untuk melakukan *port scanning*. Nmap dibuat oleh Gordon Lyon, atau lebih dikenal dengan nama Fyodor Vaskovich. Aplikasi ini digunakan untuk meng-audit jaringan yang ada. Dengan menggunakan *tool* ini, maka dapat melihat host yang aktif, port yang terbuka, Sistem Operasi yang digunakan, dan *feature-feature scanning* lainnya. Pada awalnya, Nmap hanya bisa berjalan di sistem operasi Linux, namun dalam perkembangannya sekarang ini, hampir semua sistem operasi bisa menjalankan Nmap [14].

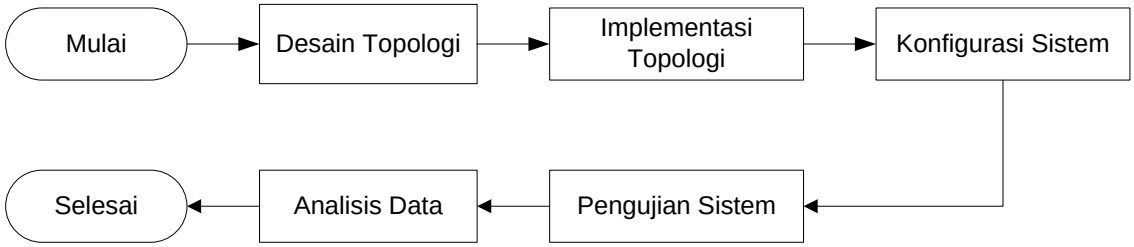
J. Mikrotik

Mikrotik adalah sebuah sistem operasi dan perangkat lunak yang dapat digunakan pada sebuah komputer sehingga dapat difungsikan sebagai *router network.* Adapun fitur yang dimiliki Mikrotik mencakup berbagai fitur yang bermanfaat untuk membuat IP *network* dan jaringan *wireless.* Sehingga perangkat ini sangat cocok jika digunakan oleh ISP, *provider hotspot* dan warnet [15]. Adapun *hardware* dari mikrotik bisa berupa Router Bord maupun Router PC. Salah satu contoh Router Board bisa dilihat pada Gambar 1.

Gambar 1. Router Board RB450 [16]

III. MOTODE

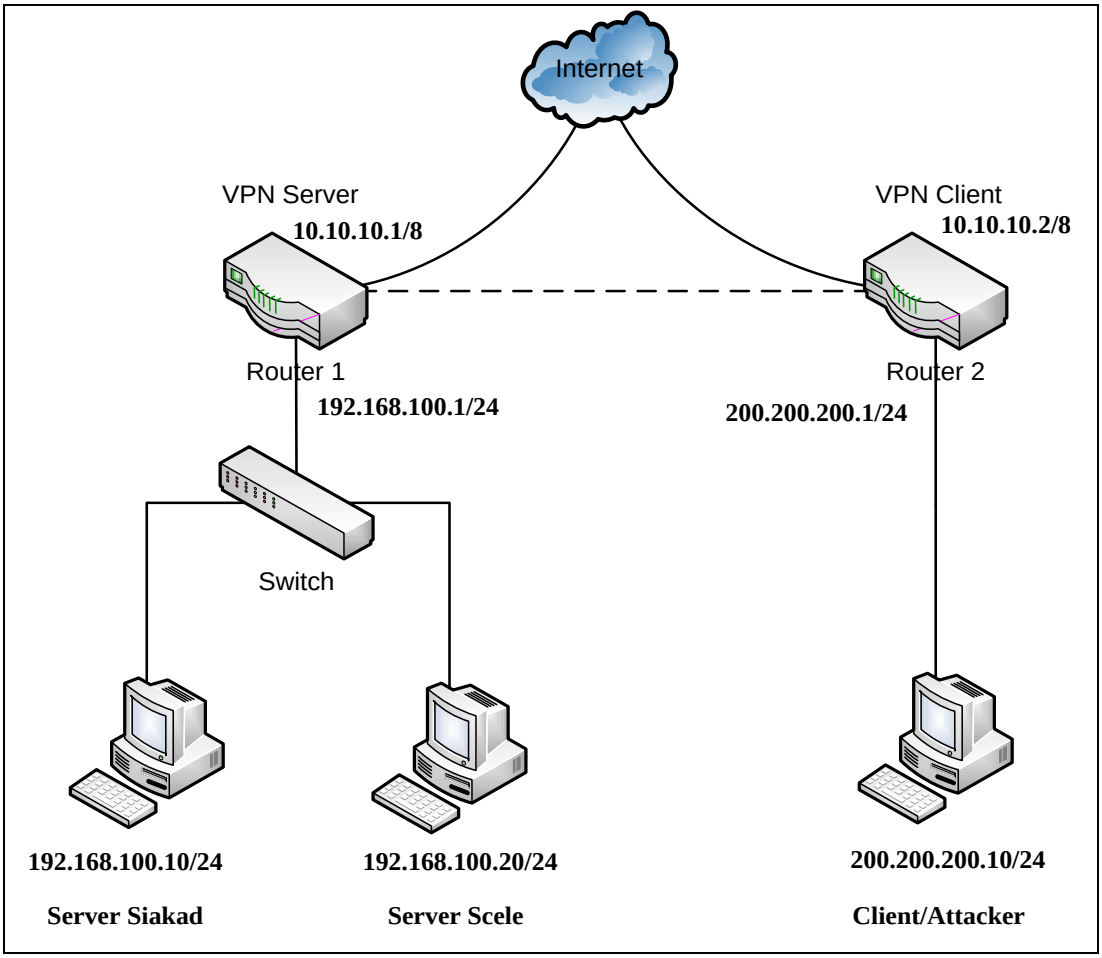
Tahapan penelitian yang dikerjakan dalam penelitian ini terdiri dari empat tahap yaitu: tahap desain topologi, implementasi topologi, konfigurasi sistem keamanan, pengujian sistem dan analisis data. Adapun tahapan penelitian tersebut dapat dilihat pada Gambar 2.



Gambar 2. Tahapan Penelitian

A. Desain Topologi

Dalam tahap ini dilakukan perancangan topologi jaringan menggunakan Simulator GNS. Dari hasil perancangan topologi ini, dapat dilakukan analisa kebutuhan yang diperlukan dan model pengujian yang akan dilakukan. Adapun topologi yang telah dibangun bisa dilihat pada Gambar 3.



Gambar 3. Desain Topologi Jaringan Virtual Private Network

B. Implementasi Topologi

Pada tahap ini melakukan implementasi/penerapan desain topologi yang sudah dibangun kedalam perangkat jaringan fisik, yakni pada perangkat Mikrotik RouterOS (RB450) dengan spesifikasi: CPU AR7130 300MHz, RAM 32 MB, LAN Port 5, License Level 5.

C. Konfigurasi Sistem

Pada tahap ini melakukan konfigurasi VPN Server dan VPN Client. Berdasarkan hasil eksperimen yang dilakukan oleh peneliti, bahwasanya konfigurasi penerapan Virtual Private Network (VPN) tidak begitu kompleks dan tidak rumit, sehingga bisa dengan mudah untuk diterapkan dimana saja bagi yang ingin menerapkan protokol VPN ini pada jaringan yang dibangunnya [17].

D. Pengujian Sistem

Pada umumnya ada empat langkah yang dilakukan untuk menguji sistem keamanan, yaitu: *Reconaissance, Scanning, Exploitation,* dan *Maintaining Access.* Adapun teknik *scanning* yang dilakukan dalam pengujian ini antara lain: TCP Scan, Syn Scan, UDP Scan, Xmas Scan, dan Null scan. Adapun parameter pengujian sistem bisa dilihat pada Tabel 1.

Tabel 1. Parameter Pengujian Sistem

No	Metode Pengujian	*Tools* yang Digunakan	Target Pengujian
1	*Scanning*	Nmap 7.80	Celah *Vulnerability*
2	*Sniffing*	Wireshark 3.0.4	Enkripsi Paket Data
3	*Denail of Service (DoS)*	LOIC_2.0.0.4-1	Performansi *Service* VPN Server

E. Analisis Data

Analisis data dilakukan dengan cara mengumpulkan data dari hasil eksperiman pengujian sistem yang telah dilakukan dan kemudian mengambil informasi baru berdasarkan dari analisis yang telah dilakukan.

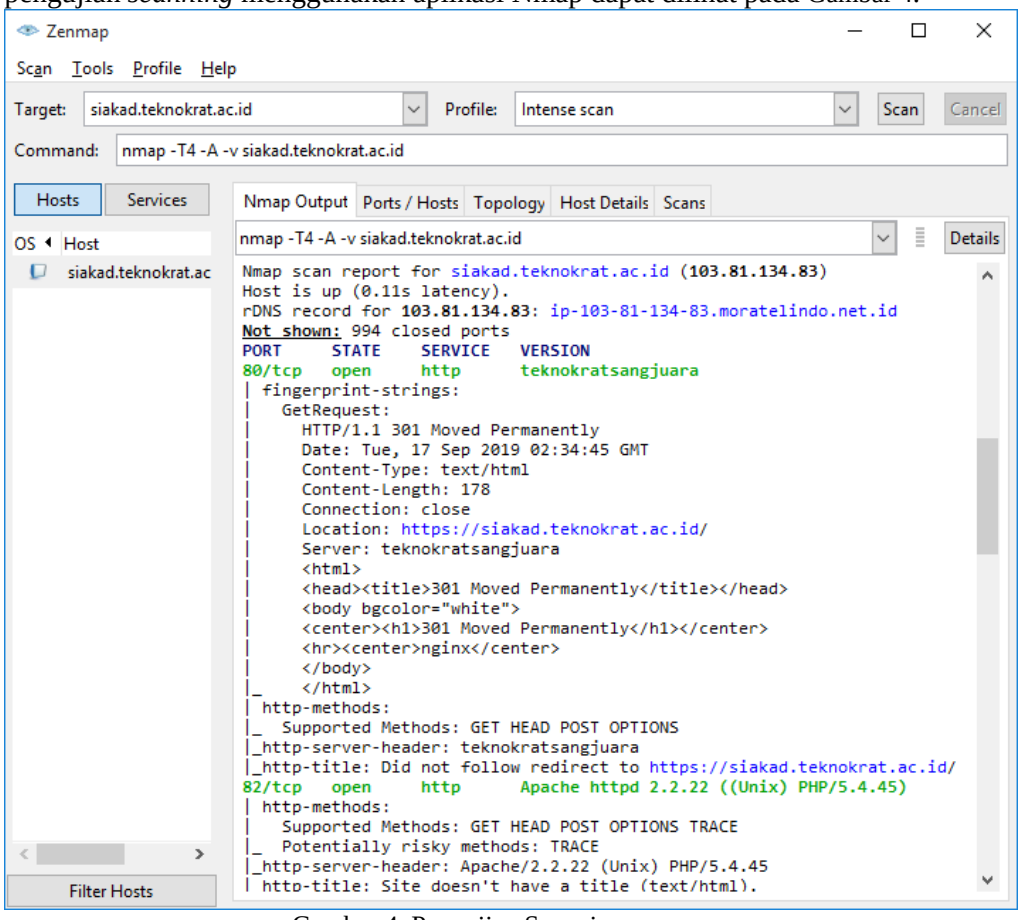
IV. IMPLEMENTASI MODEL DAN PEMBAHASAN

A. Pengujian Sistam

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan, diperoleh data sebagai berikut ini:

1. Pengujian *Scanning*

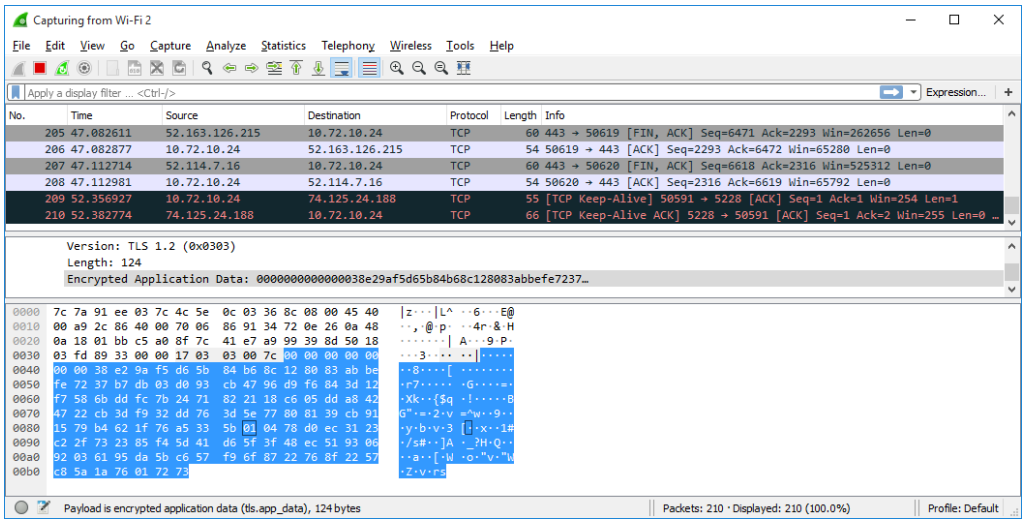
   Pengujian *scanning* ini dilakukan dengan tujuan untuk mendapatkan informasi yang ada pada target (Server Siakad). Adapun *tools* yang digunakan ialah aplikasi Nmap. Berdasarkan hasil eksperiman *scanning*, didapatkan hasil bahwa port yang aktif dan IP address target masih dapat terbaca dengan baik. Sehingga proses pengujian ini dapat dilanjutkan ke tahap selanjutnya yakni pengujian *sniffing* dan DoS. Adapun tampilan pengujian *scanning* menggunakan aplikasi Nmap dapat dilihat pada Gambar 4.



Gambar 4. Pengujian Scanning

2. Pengujian *Sniffing*

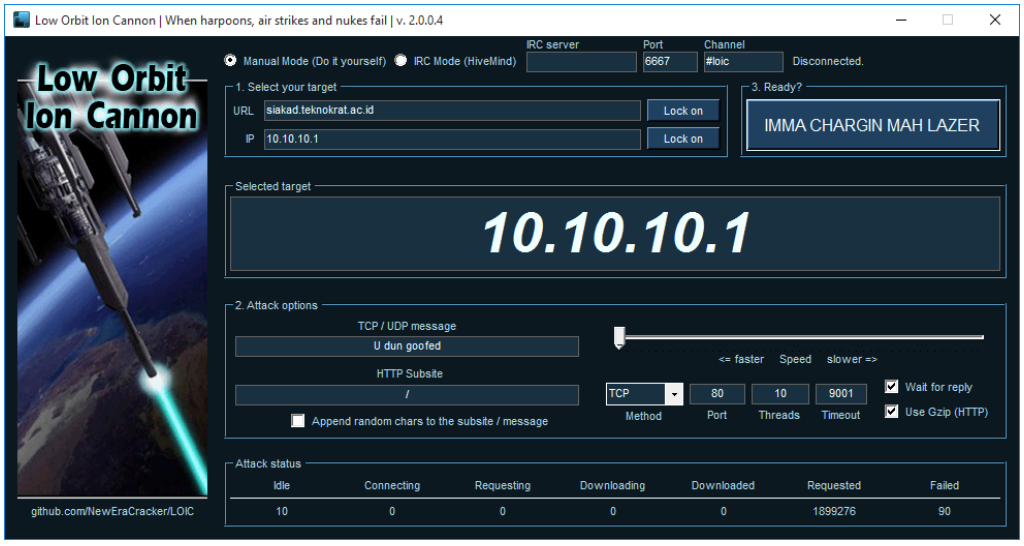
Pada pengujian *sniffing* ini dilakukan pengujian dengan cara melakukan monitoring Traffic menggunakan aplikasi Wireshark. Berdasarkan hasil pengujian, diperoleh hasil bahwa packet data yang ditrasmisikan dari client ke server dapat dienkripsi dengan baik sehingga data hasil *sniffing* tidak dapat terbaca langsung oleh *user* (attacker). Adapun tampilan monitoring trafik ke server siakad dalam pengujian *sniffing* ini dapat dilihat pada Gambar 5.



Gambar 5. Monitoring Trafik dari Client ke Server Siakad

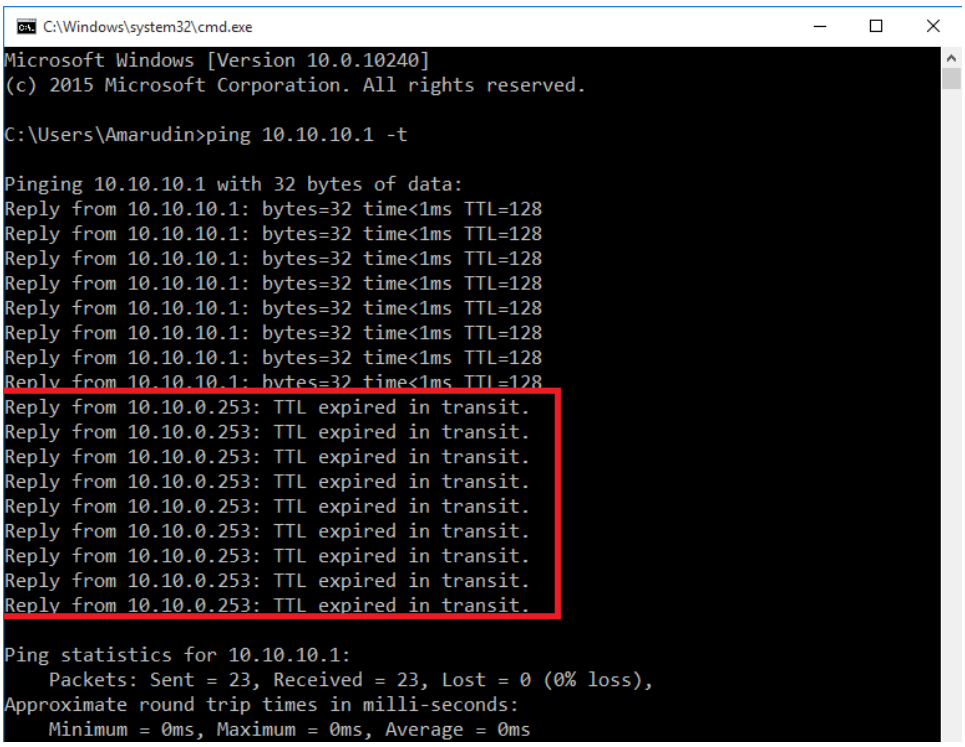
3. *Denail of Service* (DoS)

Pengujian DoS pada *service* VPN server, dilakukan dengan memanfaatkan *tools* hacking yang sudah ada yaitu LOIC_2.0.0.4-1. Adapun tampilan aplikasi LOIC saat *running* bisa dilihat pada Gambar 6.



Gambar 6. LOIC saat *running*

Kondisis *service* VPN server saat diakses sebelum dilakukan DoS, masih berjalan normal. Namun pada saat dilakukan DoS menggunakan LOIC sampai pada *request ping* ke 1.899.276, *service* VPN server mengalami masalah saat diakses. Adapun tampilan aksses VPN server saat sebelum error dan setelah error, dapat dilihat pada Gambar 7.



Gambar 7. Kondisi *service* VPN server saat DDoS

B. *Analisis Data Hasil Pengujian*

Berdasarkan hasil pengujian, didapatkan data sebagaimana yang ditampilkan pada Tabel 2.

Tabel 2. Hasil Pengujian

No	Metode Pengujian	*Tools*	Hasil Pengujian
1	*Scanning*	Nmap 7.80	- Open Port: 8080, 443, 80, 82, 212. - IP Address: 103.81.134.83. - Provider :moratelindo.net.id. - Sitem Operasi: Linux Ubuntu 2.7. - Server name: teknokratsangjuara. - Web Server: PHP/5.4.45. - DNS: siakad.teknokrat.ac.id.
2	*Sniffing*	Wireshark 3.0.4	Protocol : TCP (*Encrypted*) *User* dan *Password*: *Encrypted*
3	*Denail of Service (DoS)*	LOIC_2.0.0.4-1	*Service* VPN Server done: 1.899.276 request

V. KESIMPULAN

Pemanfaatan *Virtual Private Network* (VPN) yang dilakukan sangat bergantung pada kecepatan internet pada VPN server maupun VPN client serta perangkat attacker (*user*). Sedangkan performansi *service* yang digunakan pada VPN Server masih kurang bagus ketika diuji dengna DoS walaupun kecepatan internet yang digunakan pada Universitas Teknokrat Indonesia sudah cukup stabil. *Service* pada VPN Server dapat dimatikan pada *request* (ping) sebesar 1.899.276 request. Hal ini dipengaruhi oleh spesifikasi perangkat Mikrotik RouterOS yang digunakan. Adapun untuk penelitian selanjutnya sebaiknya perlu dilakukan pengujian performansi konektifitas menggunakan bandwith yang lebih besar dan untuk menguji performansi *service* VPN Server menggunakan spesifikasi perangkat Mikrotik yang lebih baik.

DAFTAR PUSTAKA

[1] Bimo, "Perkembangan Teknologi Informasi di Indonesia - PakarKomunikasi.com," 2019. [Online]. Available: https://pakarkomunikasi.com/perkembangan-teknologi-informasi-di-indonesia. [Accessed: 12-Aug-2019].

[2] Kominfo, "Kementerian Komunikasi dan Informatika," 2019. [Online]. Available: https://kominfo.go.id/index.php/content/detail/3980/Kemkominfo%3A+Pengguna+Internet+di+Indonesia+Capai+82+Juta/0/berita_satker. [Accessed: 12-Jul-2019].

[3] F. E. Rasjid, "Hacker Dan Cracker | Universitas Surabaya (UBAYA)," 2018. [Online]. Available: https://www.ubaya.ac.id/2018/content/articles_detail/148/Hacker-dan-Cracker.html. [Accessed: 12-Jul-2019].

[4] Admin, "Serangan Virus Ransomware Wannacry Gegerkan Dunia," *Jawapos*, 2017. [Online]. Available: https://www.jawapos.com/oto-dan-tekno/teknologi/31/12/2017/serangan-virus-ransomware-wannacry-gegerkan-dunia/. [Accessed: 12-Aug-2019].

[5] Mikrotik, "Mikrotik.ID : Pemilihan Tipe VPN," 2019. [Online]. Available: https://mikrotik.id/artikel_lihat.php?id=61. [Accessed: 12-Jul-2019].

[6] A. Yoga, "Mikrotik.ID : Konfigurasi VPN PPTP pada Mikrotik," *Mikrotik*, 2018. [Online]. Available: http://www.mikrotik.co.id/artikel_lihat.php?id=43. [Accessed: 01-May-2019].

[7] I. Efendi, "Perbedaan Hacker dan Cracker | IT-Jurnal.com," 2019. [Online]. Available: https://www.it-jurnal.com/perbedaan-hacker-dan-cracker/. [Accessed: 13-Aug-2019].

[8] Julismail, "Kajian 3: Scanning Network | Jul Ismail," 2019. [Online]. Available: https://julismail.staff.telkomuniversity.ac.id/scanning-network/. [Accessed: 16-Aug-2019].

[9] L. N. Niswati, "Sniffing? Cain & Abel Saja! : IlmuKomputer.Com," 2007. [Online]. Available: https://ilmukomputer.org/2007/03/27/sniffing-cain-abel-saja/. [Accessed: 16-Jul-2019].

[10] K. N. Fitria, "'Sniffing' Password dengan Wireshark," pp. 1–4, 2007.

[11] Noname, "Mengenal Apa itu Exploit (Komputer) - Definisi TI Berita Bebas," 2019. [Online]. Available: https://www.beritabebas.com/definisi/computer-exploit/. [Accessed: 16-Aug-2019].

[12] R. Wicaksono, "Memahami Serangan Denial of Service – Ilmu Hacking," 2009. [Online]. Available: https://www.ilmuhacking.com/web-security/memahami-serangan-denial-of-service/. [Accessed: 15-Aug-2019].

[13] Anonim, "Pengertian dan Fungsi Wireshark, sisi Hacker vs Administrator Jaringan," 2017. [Online]. Available: https://meretas.com/wireshark-adalah/. [Accessed: 05-Aug-2019].

[14] Wikipedia, "Nmap - Wikipedia bahasa Indonesia, ensiklopedia bebas," 2019. [Online]. Available: https://id.wikipedia.org/wiki/Nmap. [Accessed: 17-Jun-2019].

[15] Salman, "Weblet Importer," 2019. [Online]. Available: http://salmantkj48.blogspot.com/2015/02/pengertian-mikrotik-fungsinya.html. [Accessed: 10-Jun-2019].

[16] Mikrotik, "Jual MikroTik RB450 - harga bersaing, spesifikasi lengkap, kualitas dan aftersales terjamin," *Jogjabolic*, 2019. [Online]. Available: http://www.jogjabolic.id/shop/mikrotik-rb450/. [Accessed: 11-Aug-2019].

[17] A. Amarudin and S. D. Riskiono, "Analisis dan Desain Jalur Transmisi Jaringan Alternatif Menggunakan Virtual Private Network (VPN)," *J. Teknoinfo*, vol. 13, no. 2, pp. 100–106, 2019.

UCAPAN TERIMAKASIH

Terima kasih kepada Direktorat Riset dan Pengabdian kepada Masyarakat (DRPM) Dikti yang telah mendanai kegiatan penelitian ini yakni pada skema Penelitian Dosen Pemula (PDP) sesuai dengan SK Penetapan Pemenang Hibah PDP nomor: T/140/E3/RA.00/2019 tanggal 25 Februari 2019 dan Kontrak Pelaksanaan Penelitian Nomor: 005/LPPM-UTI/FTIK/PDPMONO/V/2019 tanggal 2 Mei 2019.

Terima kasih juga peneliti sampaikan kepada LPPM Universitas Teknokrat Indonesia yang telah memfasilitasi kegiatan penelitia ini khususnya tim Pusat TIK atas fasilitas perangkat dan laboratorium yang telah digunakan.

Amarudin, S.Kom., M.Eng. adalah lulusan Akademi Manajemen Informatika dan Komputer (AMIK Teknokrat) tahun 2007. Gelar Sarjana Komputer (S.Kom.) diraih di STMIK Teknokrat, Lampung tahun 2011. Gelar *Master of Engineering* (M.Eng.) diraih di Fakultas Teknik Jurusan Teknik Elektro dan Teknologi Informasi Universitas Gadjah Mada tahun 2014. Bidang penelitian yang sedang ditekuni saat ini adalah *Network Security, Machine Learning.* Penulis juga aktif melakukan penelitian dan naskah-naskahnya telah diterbitkan di beberapa jurnal nasional serta masih aktif sebagai anggota perkumpulan peneliti dunia di *www.researchgate.net*. Penulis saat ini berdinas sebagai Dosen di Universitas Teknokrat Indonesia pada Prodi Teknik Elektro.

Sampurna Dadi Riskiono, S.Kom., M.Eng. adalah lulusan Akademi Manajemen Informatika dan Komputer (AMIK Teknokrat) tahun 2006. Gelar Sarjana Komputer (S.Kom.) diraih di STMIK Teknokrat, Lampung tahun 2012. Gelar *Master of Engineering* (M.Eng.) diraih di Fakultas Teknik Jurusan Teknik Elektro dan Teknologi Informasi Universitas Gadjah Mada tahun 2017. Bidang penelitian yang sedang ditekuni saat ini adalah *Network Security, Machine Learning.* Penulis juga aktif melakukan penelitian dan naskah-naskahnya telah diterbitkan di beberapa jurnal nasional serta masih aktif sebagai anggota perkumpulan peneliti dunia di *www.researchgate.net*. Penulis saat ini berdinas sebagai Dosen di Universitas Teknokrat Indonesia pada Prodi Teknik Elektro.