Journal of SAKIRA (*Secure And Knowledge-Intelligent Research in Cybersecurity And Multimedia*) e-ISSN 3046-773X

Vol.1, No.2, December 2023, pp. 57~64

Implementation of Live Forensic Virtual Router for Network Traffic Comparison

Firmansyah[1], Hendri Purnomo[2], Yusuf Hendra Pratama[3], Bayu Wibisana[4],
Ilmu Komputer, Universitas Islam Al-Azhar

f.firman@unizar.ac.id

Article Info

Article history:

Received November 6, 2023
Revised November 10, 2023
Accepted November 17, 2023

Keyword:

Virtual Router, Client, Forensic, Analyzing.

ABSTRACT

An entrepreneur or a service provider in the internet network world, will certainly find clients with different characters. Clients who are not technology blind, especially routers, sometimes want full access to the router, or some clients who ask to add a router to be able to directly access the router in full. Virtual Router allows clients to process their own network, as if the client has a router. Network forensics has the ability to reconstruct events using a system that stores all data traffic activities on the network, so that investigations can be carried out by looking back at events that have occurred and analyzing events that occurred in the past. Wireshark can review data packages in real time. This means that the wireshark application will monitor all incoming and outgoing data packets through a predefined interface and the next will display the results of the data package.

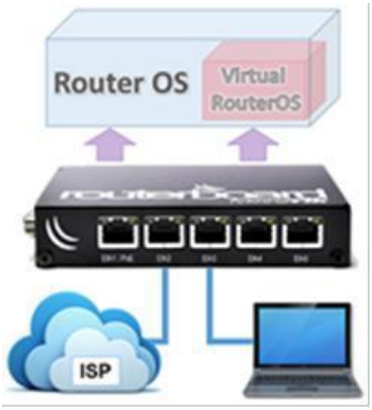
I. PENDAHULUAN

Indonesia memiliki aturan soal perlindungan data pribadi di era digital. Aturan itu dituangkan dalam bentuk Peraturan Menteri (Permen) No 20 Tahun 2016 tentang Perlindungan Data Pribadi (PDP) yang ditetapkan 7 November 2016, diundangkan dan berlaku sejak 1 Desember 2016. Aturan itu dinyatakan Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Perlindungan Data Pribadi dalam Sistem Elektronik mencakup perlindungan terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan Data Pribadi. Data Pribadi hanya dapat diolah dan dianalisis sesuai kebutuhan Penyelenggara Sistem Elektronik yang telah dinyatakan secara jelas saat memperoleh dan mengumpulkannya. Untuk keperluan proses penegakan hukum. Penyelenggara Sistem Elektronik wajib memberikan Data Pribadi yang terdapat dalam Sistem Elektronik atau Data Pribadi yang dihasilkan oleh Sistem Elektronik atas permintaan yang sah dari aparat penegak hukum berdasarkan ketentuan peraturan perundang-undangan. Hal tersebut di atas mengawali penyelenggaran sistem dan transaksi elektronik tentang perlindungan data pribadi dalam sistem elektronik. Dalam dunia teknologi informasi dewasa ini sering kita mendengar istilah virtulisasi atau *virtualization* dalam Bahasa Inggris. Teknik virtualisasi merupakan teknik untuk menciptakan versi virtual (bukan fisik) dari sistem operasi komputer, sumber daya jaringan computer, maupun perangkat penyimpanan [1], [2]. Untuk sumber daya jaringan, dapat membangun router virtual, switch virtual, server virtual maupun topologi virtual [3], [4]. Perangkat-perangkat jaringan virtual tersebut bisa saja berada pada satu perangkat fisik saja. Bagi penggemar Router MikroTik, dengan teknik virtualisasi, dapat memiliki beberapa unit Router MikroTik, meskipun hanya memiliki sebuah RouterBoard [5], [6], [7]. Ada banyak keuntungan menerapkan virtualisasi pada infrastruktur jaringan. Keuntungan yang paling utama adalah penghematan dan pemangkasan biaya infrastruktur jaringan. Sebagai contoh, jika harus membeli 8 (delapan) unit router, padahal sebenarnya bisa memiliki router-router tersebut di dalam sebuah RouterBoard [8], [9], [10], [11], [12].

Virtual router merupakan fitur MikroTik yang memungkinkan untuk menjalankan operating system baru

e-ISSN 3046-773X

secara virtual baik untuk penerapan virtualisasi router maupun virtualisasi topologi jaringan. Hampir sama seperti aplikasi VMware atau VirtualPC. Dengan Virtual router sebuah routerboard mikrotik akan mampu menjalankan beberapa RouterOs dalam bentuk virtualisasi selain Router OS dengan Virtual router dapat juga dijalankan sebuah OS lain misalkan sistem operasi Linux Openwrt. Untuk itu dengan Virtual router memungkinkan dalam satu router bisa digunakan untuk berbagai hal misal membangun RouterOs Virtual, membagun Server Virtual, juga bisa membangun topologi jaringan. Selain itu bisa digunakan untuk menyederhanakan konfigurasi yang apabila disatukan akan sangat sulit atau bahkan membingungkan, contohnya untuk load balancing dua ISP sekaligus bandwidth manager sekaligus juga firewall ditambah pula VPN, akan sangat bijaksana bila dipisah-pisahkan dan dijalankan pada Virtual router dalam sebuah hardware Mikrotik.



Gambar 1Topologi Virtual router

Untuk mengelola jaringan dengan skala besar tersebut maka jaringan (network) itu harus dipisahkan menjadi beberapa jaringan kecil. Mengatur beberapa jaringan kecil yang berisi puluhan host, tentu akan lebih mudah daripada mengatur sebuah jaringan yang berisi ratusan bahkan ribuan host. Teknik memisahkan jaringan ini dapat diimplementasikan untuk jaringan (LAN), jaringan skala menengah (MAN) maupun jaringan besar (WAN/Internet). Setelah jaringan tersebut dipisahkan menjadi beberapa jaringan kecil, maka pekerjaan selanjutnya adalah menghubungkan kembali jaringan-jaringan kecil tersebut. Dalam topologi jaringan di sebuah laboratorium memiliki ruangan untuk Praktikum, Server, Teknisi, dan Dosen. Setiap ruangan memiliki kebutuhan dan Access Control Lists (ACLs) berbeda. ACLs pada Laboratorium Komputer Jaringan Komputer terpusat pada router server, ACLs yang banyak dan terpusat dapat menyebabkan traffic padat. Pemisahan ACLs berdampak pada penggunaan router yang lebih banyak dan menyebabkan biaya berlebih untuk pembelian router, pemakaian listrik dan penggunaan ruang penyimpanan. Permasalahan tersebut dapat diatasi dengan virtualisasi. Router Mikrotik dapat menerapkan virtualisasi dengan Virtual router yang berdampak pada penghematan biaya pembelian hardware router, penggunaan listrik, dan tempat penyimpanan. Virtualisasi router menggunakan Virtual router dapat menghemat biaya pembuatan jaringan komputer, pemakaian energi listrik dan penggunaan tempat dibandingkan router non-virtualisasi (Galang dkk, 2017).

Pengumpulan data Network Forensic menggunakan sebuah tool yang bisa menyimpan semua kejadian data- data lalu lintas jaringan [13], [14], [15]. Salah satu tool yang mampu memenuhi kebutuhan Network Forensic yaitu Snort. Snort merupakan tool cross platform yang mampu diinstall pada Windows, Mac OS, dan Linux. Snort merupakan tool yang open source dan update dari Snort dapat diakses oleh semua pengguna. Snort merupakan tool yang berbasis Intrusion Detection System (IDS) yang dapat memonitor jaringan yang berdampak serangan, selain itu juga menyimpan serangan tersebut pada Log. Tujuan dari penelitian ini yaitu mengimplementasikan snort serta menganalisis Log snort dengan menggunakan Network Forensik, yaitu melakukan inverstigasi dari data serangan yang tersimpan pada Log snort. Pada implementasi akan dibangun sebuah topology star.Identifikasi Masalah.

II. METODE

Objek Penelitian

Objek penelitian ini yaitu berkaitan tentang *Network Forensic* untuk menemukan kejahatan di dunia maya seperti *cyber crime*. Kejahatan dilakukan secara digital, namun tetap saja meninggalkan bukti atau "jejak". Pada bab ini akan membahas mengenai proses-proses *Network Forensic.* Alat danbahan dapat dilihat pada Tabel 1.

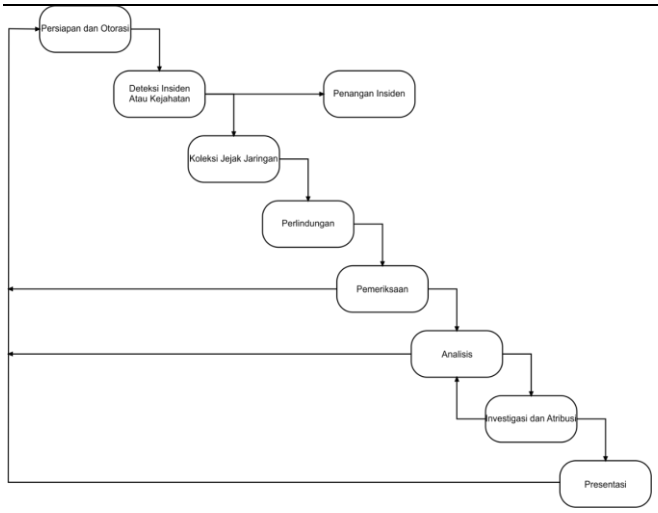
Tabel 1. Alat dan Bahan

No	Alat dan Bahan	
	Hardware	Software
1	Mikrotik RB951Ui	Snort IDS
2	Access Point TP-Link WA5210	Winbox v3.19
3	Modem ADSL	Apache Server for Windows 2.4.9
4	Laptop Core i5, RAM 4GB	Microsoft Windows 10
5	PC dan laptop	Ubuntu 16.04

Perancangan Sistem

Forensik sebagian besar menangani kejahatan yang dilakukan sebelumnya, fokusnya untuk mencegah kejahatan di masa depan. Forensik jaringan merupakan salah satu ilmu forensik digital yang melingkupi penemuan dan invesitgasi materi (data) yang ditemukan pada perangkat digital. Model Proses Forensik yang digunakan oleh peneliti ditunjukkan pada Gambar 1.

e-ISSN 3046-773X



Gambar 2. Diagram Alir Penelitian

***Preparation And Authorization* (Persiapan dan Otorisasi)**

Network Forensik bisa diterapkan jika dimana network security tools seperi system deteksi instrusi, packet analyzer, dan firewall ditempatkan di beberapa titik jaringan. Otorisasi sangat diperlukan untuk memantau lalu lintas jaringan, selain itu aturan keamanan diterapkan dengan baik sehingga tidak menyalahi privasi individu dan organisasi.

***Detection and Incident/Crime (Deteksi* insiden / kejahatan)**

Alert yang disinyalkan oleh security tools menunjukkan serangan dan tahap selanjutnya akan di analisis. Sifat serangan ditentukan dari berbagai parameter. Validasi dilakukan untuk menilai dan mengkonfirmasi dugaan penyerangan. Hal ini dilakukan untuk menentukan apakah penyelidikan dilanjutkan atau mengabaikan alert sebagai false alarm.

***Incident Response* (Penanganan Insiden)**

Respon terhadap serangan keamanan terdeteksi berdasarkan informasi yang dikumpulkan untuk memvalidasi dan mengevaluasi kejadian. Respon dimulai tergantung pada jenis serangan dan diarahkan oleh or ganisasi atau kebijakan hukum yaitu rencana untuk mencegah serangan dan recover kerusakan, pada saat yang bersamaan keputusan apakah penyelidikan dilanjutkan atau tidak. Fase ini berlaku untuk kasus- kasus dimana investigasi dimulai pada saat serangan berlangsung dan tidak dapat dilakukan setelah notifikasi serangan.

***Collection of Network Traces* (Koleksi Jejak Jaringan)**

Network trace dikumpulkan oleh security tools. Pada tahap ini melakukan pencarian bukti dan pengumpulan bukti, pengenalan terhadap bukti-bukti penyerangan dan pengumpulan bukti.

***Preservation and Protection* (Presentasi dan Ulasan)**

Data asli yang diperoleh dan log disimpan pada perangakat backup. Memastikan akurasi data, salinan dari data yang akan di analisis. Hal ini dilakukan agar penyelidikan dilakukan dapat dibuktikan lagi sehingga memenuhi persyaratan hukum.

***Examination* (Pemeriksaan)**

Data yang diperoleh membentuk dataset dan dapat dianalisis serta dipetakan. Pemeriksaan dilakukan agar informasi penting tidak hilang atau tercampur dengan data lain. Data akan diklasifikasikan, informasi dan data yang tidak penting dihapus.

***Analysis* (Analisis)**

Bukti-bukti dikumpulkan dan dianalisis pola serangan yang digunakan penyerang. Beberapa parameter penting yang berhubungan dengan pembentukan koneksi, protokol, sistem operasi, fragmentasi paket semua dianalisis untuk mengetahui cara penyeranh. Hasil dari tahap ini adalah validasi dari aktivitas yang mencurigakan.

***Investigation and Attribution* (Investigasi dan Atribusi)**

Bukti-bukti informasi yang diperoleh dari hasil analisis digunakan untuk mengidentifikasi:

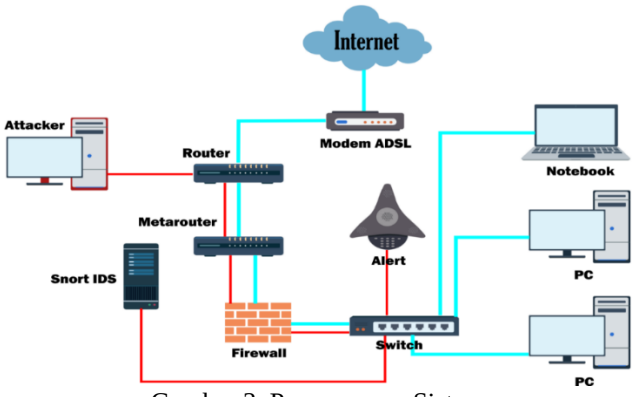
1) Serangan apa yang terjadi?
2) IP siapa yang melakukan serangan?
3) Kapan serangan terjadi?
4) Dimana serangan itu terjadi?
5) Bagaimana serangan tersebut bisa terjadi?
6) Mengapa itu terjadi?

***Presentation* (Presentasi dan Review)**

Semua hasil di sajikan dengan bahasa yang dimengerti serta menjelaskan berbagai prosedur yang digunakan sampai pada kesimpulan dari proses penyidikan. Dokumentasi penyidikan juga disertakan agar bisa digunakan untuk mencegah kejadian serangan yang sama di masa yang akan datang.

Topologi Jaringan

Topologi yang digunakan untuk eksperimen adalah topologi star. Terdapat 1 Server sebagai Snort, 2 PC dan 1 Laptop sebagai client yang terhubung dengan Switch. Gambar 3.2 merupakan desain perancangan sistem yang digunakan untuk esperimen.



Gambar 3. Perancangan Sistem

Pada eksperimen ini 1 PC akan melakukan serangan kepada server Snort, selain itu 2 PC dan 1 laptop hanya sebagai client biasa yang mengirimkan packet data ke PC Snort dan ke PC lainya. Ketika terdapat packet datang melalui switch maka akan terdeteksi oleh detection engine yang sudah terinstall Snort sebagai IDS di cocokan dengan rules yang sudah di set. Packet tersebut dicek apakah packet sesuai

e-ISSN 3046-773X

dengan rules. Ketika packet tersebut mengandung konten serangan maka akan tersimpan di Log Snort dan akan memunculkan alarm. Namun ketika packet tersebut tidak mengandung konten serangan maka packet tersebut di discard (diabaikan) dan langsung dikirimkan.

III. HASIL DAN PEMBAHASAN

Pada bagian ini menjelaskan hasil yang didapatkan selama penelitian yang telah dilakukan berdasarkan perumusan dan tujuan penelitian, yaitu:

1. Melakukan pengaturan Virtual Router
2. Melakukan analisis forensik pada virtual router.
3. Melakukan analisis perbandingan

Pengaturan Virtual Router

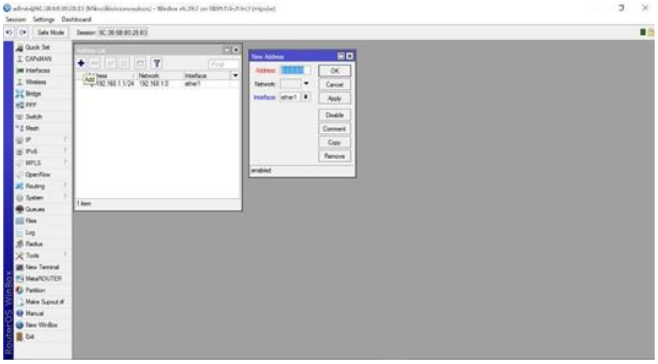
Sub bab ini menyajikan implementasi sistem, meliputi spesifikasi perangkat yang digunakan untuk mengembangkan Perbandingan Algoritma Proses *Stemming* Pada Sistem Deteksi *Error* Kata Bahasa Indonesia, implementasi fungsional dan implementasi antarmuka.

Melakukan pengaturan IP network

Sebelum melakukan setting virtual router pada bagian ini terlebih dahulu melakukan setting IP yang akan gunakan untuk clien yang akan terkoneksi dengan mikrotik . menentukan IP yang akan jadikan sebagi IP public yang berikan kepada Clien. Berikut cara setting network IP pada mikrotik router board.

Gambar 4. Setting IP Networ di Virtual Box

Pada Gambar 4. Menjelaskan tentang bagaimana cara melakukan Settingan IP Network di Virtual Box. Kemudian di virtual box bisa melakukan setting IP, penentuan kelas dan penentuan klasifikasi IP.



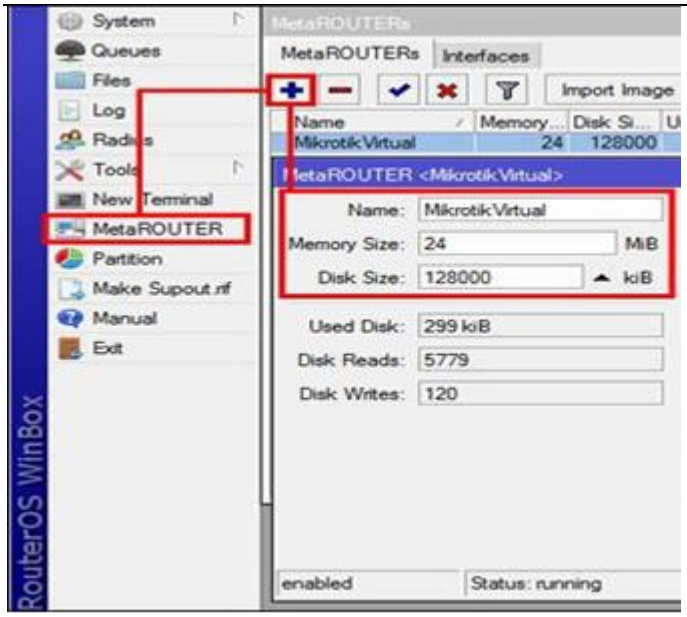
Gambar 5. Pembuatan IP address

Pada Gambar 5 menjelaskan tentang pembuatan IP Address pada sebuah virtual router. Jika kita perhatikan pada router master terdapat ip address 10.10.10.1 di interface virtual, dan pada virtual router terdapat ip address 10.10.10.2 di interface ether1. Dengan ip address inilah nanti router master dan virtual router akan saling interkoneksi. Agar virtual router dapat terkoneksi ke internet, kita setting router master sebagai gateway. Cara setting juga sama persis ketika kita setting router fisik. Begitu juga dengan setting NAT, DNS nya.

4.1.2 Melakukan Setting Virtual router

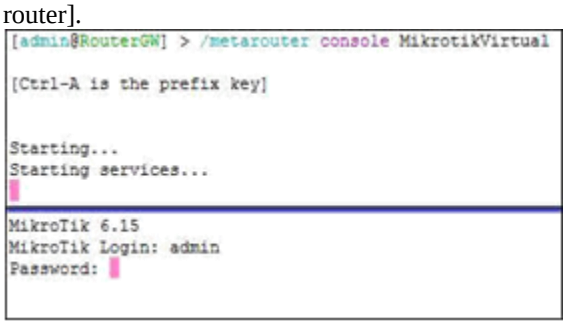
Pada saat berbisnis di dunia internet, tentu kita akan banyak menemui pelanggan yang bermacam kriteria. Beberapa user yang cukup mengenal MikroTik terkadang menginginkan akses full ke router kita, atau paling tidak mereka membutuhkan router lagi untuk bisa memanagement jaringan secara full. Sebenarnya kita sebagai penyedia jasa bisa saja memberikan router lagi, namun tentu akan membutuhkan biaya yang lebih besar. Atau pada kasus lain misalnya kita hendak melakukan lab jaringan yang membutuhkan lebih dari satu router. Salah satu solusi hemat adalah dengan memanfaatkan fitur Virtual router. Virtual router merupakan fitur MikroTik yang memungkinkan untuk menjalankan operating system baru secara virtual. Hampir sama seperti aplikasi VMware atau VirtualPC pada Windows. Virtual router bisa kita gunakan untuk menjalankan Operating System didalam OS MikroTik yang sedang berjalan. Pada bagian ini menjelaskan bagaimana melakukan seting virtual router, berikut langkah yang bisa lakukan Pertama, masuk ke menu Virtual router. Klik tombol + untuk menambahkan virtual router. Disini ada 3 parameter yang perlu ditentukan, "Name" diisi dengan nama Virtual Router sesuai kebutuhan Anda. Kemudian Parameter RAM dan Hardisk juga diisi seuai kebutuhan. Parameter lainnya bisa dibiarkan bernilai default.

e-ISSN 3046-773X



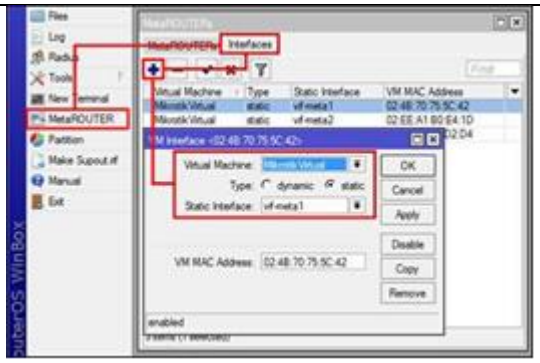
Gambar 6. Membuat Virtual router

Pada Gambar 6. menjelaskan tentang bagaimana membuat virtual router. Virtual Router di Virtual router akan berjalan saat tombol Apply di eksekusi. Operating System secara otomatis akan menggunakan RouterOS Mikrotik dan versi yang dijalankan sama dengan versi RouterOS Router Mikrotik. Virtual Router ini hanya bisa diakses secara console dengan perintah : /virtual router console [nama-virtual-router].



Gambar 7. Console Meta router

Pada Gambar 7. menjelaskan tentang console virtual router. Langkah selanjutnya adalah membuat virtual Ethernet yang nanti akan digunakan oleh virtual router untuk dapat berkomunikasi dengan router master atau bahkan device lain dalam jaringan.



Gambar 8. Setting Virtual Ethernet

Pada Gambar 8. Menjelaskan tentang setting virtual Ethernet. Satu virtual ether akan digunakan oleh virtual router untuk dapat berkomunikasi dengan Router Master client.

Gambar 9. setting interface virtual router

Pada Gambar 9. menjelaskan tentang bsetting interface virtual router. Langkah berikutnya adalah melakukan seting interface virtual router. Virtual router ini digunakan untuk membuat viritual interface router seperti pada Gambar 4.6. Setting berikutnya adalah pada opsi "Virtual Machine" pilih di virtual router mana virtual ethernet akan digunakan, pilih Type static Static Interface. Pada contoh diatas, akan mensetting virtual router dengan dua interface ethernet. Satu ethernet untuk kominikasi virtual router ke internet, satu lagi untuk komunikasi ke client. Untuk memastikannya, coba remote virtual router secara console kemudian tampilkan interface ethernet. Interface ether1 di virtual router sudah bisa komunikasikan dengan interface pada router master, caranya cukup setting ip address satu segmen antara interface virtual di router master dengan interface ether1 di virtual router. Sedangkan ether2 virtual router, masih belum bisa berkomunikasi dengan perangkat lain atau client, supaya bisa berkomunikasi perlu bridging dengan interface yang terkoneksi secara fisik dengan jaringan client.

Pengambilan Data Virtual router

Pada bagian ini akan menjelaskan langkah-langkah Pengambialan data pada virtual router dengan melakukan interkoneksi antar ether yang sudah setting menjadi virtual router pada tahap setting diatas. Langkah berikutnya adalah

e-ISSN 3046-773X

melakukan koneksi pengambilan data di virtual router. Pertama lakukan setting IP di computer client yang akan melakukan Pentest. langkah pertama membuat client meta router

```
[admin@RouterGW] /metarouter> add name=client1 memory-size=32
[admin@RouterGW] /metarouter> print
Flags: X - disabled
 #   NAME                          MEMORY-SIZE DISK-SIZE    USED-DISK     STATE
 0   client1                       32MiB       0kiB         189kiB        runni
[admin@RouterGW] /metarouter>
```

Gambar 10. Create Client Virtual router

Pada Gambar 10 menjelaskan tentang create client virtual router .Setelah membuat client meta router selanjutnya melakukan koneksi antar client meta router.

```
[admin@RouterGW] /ip address> add address=10.0.1.1/24 interface=vif1
[admin@RouterGW] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         BROADCAST       INTERFACE
 0 D 10.5.8.68/24       10.5.8.0        10.5.8.255      ether1
 1   10.0.1.1/24        10.0.1.0        10.0.1.255      vif1
[admin@RouterGW] /ip address>
```

Gambar 11. Koneksi Virtual router Client

Pada Gambar 11. menjelaskan tentang koneksi virtual router client. Setalah Client ter interkoneksi baru melakukan seting pengambilan paket data antar client dalam meta router.

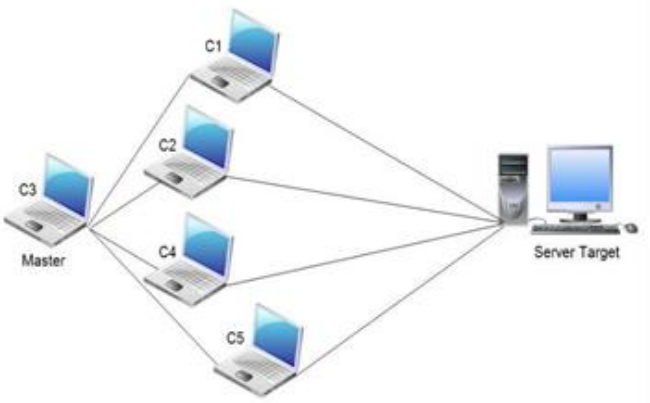
```
[admin@Client1] /interface ethernet> p
Flags: X - disabled, R - running, S - slave
 #    NAME                                                MTU   MAC-ADDRESS       ARP
 0 R  ether1                                              1500  02:49:68:55:08:E8 enabled
 1 R  ether2                                              1500  02:16:16:90:EF:0E enabled
[admin@Client1] /interface ethernet> set 0 name=public
[admin@Client1] /interface ethernet> set 1 name=local
[admin@Client1] /interface ethernet> print
Flags: X - disabled, R - running, S - slave
 #    NAME                                                MTU   MAC-ADDRESS       ARP
 0 R  public                                              1500  02:49:68:55:08:E8 enabled
 1 R  local                                               1500  02:16:16:90:EF:0E enabled
[admin@Client1] /interface ethernet>

[admin@Client1] /ip address> add address=10.0.1.2/24 interface=public
[admin@Client1] /ip address> add address=10.0.2.1/24 interface=local
[admin@Client1] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         BROADCAST       INTERFACE
 0   10.0.1.2/24        10.0.1.0        10.0.1.255      public
 1   10.0.2.1/24        10.0.2.0        10.0.2.255      local

[admin@Client1] /ip route> add gateway=10.0.1.1
[admin@Client1] /ip route> print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #     DST-ADDRESS        PREF-SRC        G GATEWAY              DISTANCE INTERFACE
 0 A S 0.0.0.0/0                          r 10.0.1.1                    1 public
 1 ADC 10.0.1.0/24        10.0.1.2                                      0 public
 2 ADC 10.0.2.0/24        10.0.2.1                                      0 local
[admin@Client1] /ip route>

[admin@Client1] /ip firewall nat> add action=masquerade out-interface=public chain=srcnat
```

Gambar 12. Pengambilan Paket data Virtual router

Pada Gambar 12. menjelaskan tentang pengambilan paket data pada virtual router sehingga cara ini bisa digunakan pada saat kita melakukan praktek pengambilan data lewat virtual router.

Skenario Pengujian Serangan DoS (*Denial of Service*)

DoS (*Denial of Service*) adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.



Gambar 13. Konsep serangan DoS

Pada Gambar 13. menjelaskan tentang konsep serangan Dos . Dalam sebuah serangan Denial of Service, penyerang akan mencoba untuk mencegah akses seorang pengguna terhadap sistem atau jaringan dengan menggunakan beberapa cara, yakni sebagai berikut:

1. Membanjiri lalu lintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan. Teknik ini disebut sebagai traffic flooding.
2. Membanjiri jaringan dengan banyak request terhadap sebuah layanan jaringan yang disedakan oleh sebuah host sehingga request yang datang dari pengguna terdaftar tidak dapat dilayani oleh layanan tersebut. Teknik ini disebut sebagai request flooding.
3. Mengganggu komunikasi antara sebuah host dan kliennya yang terdaftar dengan menggunakan banyak cara, termasuk dengan mengubah informasi konfigurasi sistem atau bahkan perusakan fisik terhadap komponen dan server.

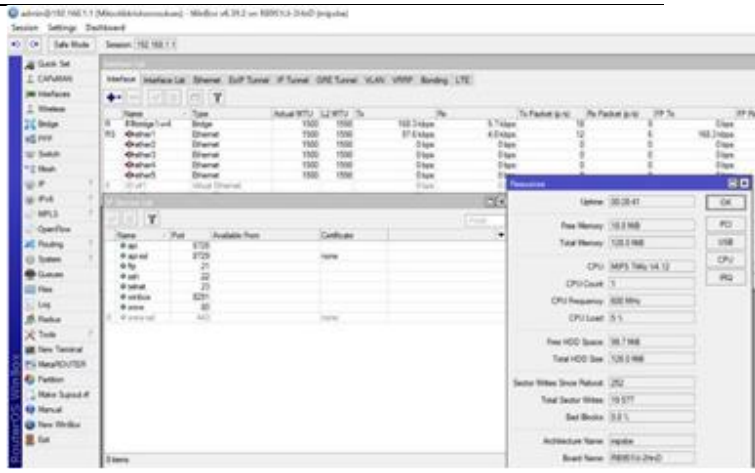
Bentuk serangan Denial of Service awal adalah serangan SYN Flooding Attack, yang pertama kali muncul pada tahun 1996 dan mengeksploitasi terhadap kelemahan yang terdapat di dalam protokol Transmission Control Protocol (TCP). Serangan-serangan lainnya akhirnya dikembangkan untuk mengeksploitasi kelemahan yang terdapat di dalam sistem operasi, layanan jaringan atau aplikasi untuk menjadikan sistem, layanan jaringan, atau aplikasi tersebut tidak dapat melayani pengguna, atau bahkan mengalami crash. Beberapa tool yang digunakan untuk melakukan serangan DoS pun banyak dikembangkan setelah itu (bahkan beberapa tool dapat

e-ISSN 3046-773X

diperoleh secara bebas), termasuk di antaranya Bonk, LAND, Smurf, Snork, WinNuke, dan Teardrop.

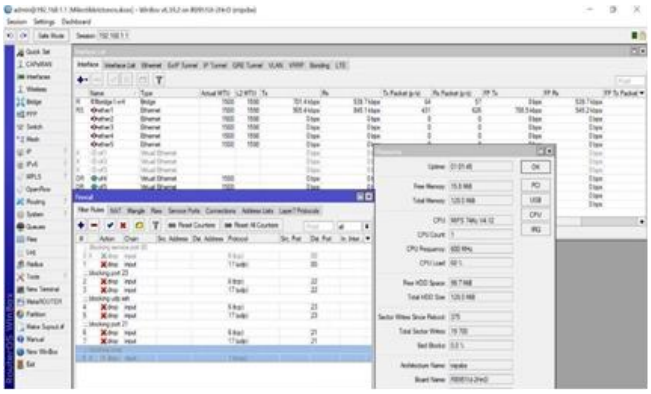
Gambar 14. Simulasi Serangan DOS dengan Ping ICMP

Pada Gambar 14. menjelaskan tentang bsimulasi serangan DoS dengan Ping ICMPMeskipun demikian, serangan terhadap TCP merupakan serangan DoS yang sering dilakukan. Hal ini disebabkan karena jenis serangan lainnya (seperti halnya memenuhi ruangan hard disk dalam sistem, mengunci salah seorang akun pengguna yang valid, atau memodifikasi tabel routing dalam sebuah router) membutuhkan penetrasi jaringan terlebih dahulu, yang kemungkinan penetrasinya kecil, apalagi jika sistem jaringan tersebut telah diperkuat.Sebuah serangan Denial of Service adalah teknik hacking untuk membuat down atau lumpuh situs atau server dengan membanjiri situs atau server dengan banyak lalu lintas atau packet data sehingga server tidak dapat memproses semua permintaan dalam real time atau bersamaan dan akhirnya down atau lumpuh. Berikut langkah langkah sekenario penyerangan mikrotik .



Gambar 15. Simulasi traffic Sebelum terjadi serangan

Pada Gambar 15. menjelaskan tentang simulasi traffic sebelum terjadi serangan DoS. Keadaan traffic sebelum terjadi serangan menunjukan memori data dan cpu yang bergerak belum signifikan terjadinya tansaksi DoS akan Memepengarui kinerja dari mikrotik dimana dengan adanya serangan Dos CPU akan mengalami kenaikan akses yang signifikan hal ini akan menyebabkan kinerja dari paket data akan down.



e-ISSN 3046-773X

Gambar 16. Hasil Serangan DoS

Pada gambar 16. menjelaskan tentang hasil serangan DoS. Setelah terjadi serangan resource pad traffic paket datanya amenjadi naik baik dari space memorinya hingga CPU load akan naik secara signifikan hal ini yang menyebab kan down dalam network traffic maupun down computer yang diserang.

IV. KESIMPULAN

Hasil penelitian menunjukkan bahwa Live Forensik pada Virtual Router memberikan hasil yang konsisten dengan analisis forensik pada lalu lintas jaringan langsung. Keberhasilan implementasi ini memberikan manfaat signifikan dalam mengurangi dampak pengumpulan data terhadap lingkungan produksi dan mempercepat deteksi serta respons terhadap kejadian keamanan jaringan. Penelitian ini memberikan kontribusi pada pengembangan metode forensik digital yang dapat diterapkan dalam lingkungan virtual, khususnya menggunakan Virtual Router. Implikasi praktis dari penelitian ini mencakup peningkatan efisiensi dan efektivitas analisis forensik dalam mengatasi ancaman keamanan jaringan modern.

DAFTAR PUSTAKA

[1] C. M. Galang, S. Eko, and A. Imam, "Teknik Virtualisasi Router Menggunakan Metarouter Mikrotik (Studi Kasus: Laboratorium Jaringan Komputer Politeknik Negeri Lampung)," *Politeknik Negeri Lampung*, 2017.

[2] A. Asmunin and A. Hermawan, "Penerapan dan Analisis Virtualisasi Router Menggunakan RouterOS," *Multinetics*, vol. 2 (1), pp. 31–34, 2016, doi: 10.32722/vol2.no1.2016.pp31-34.

[3] R. Towidjojo and Herman, *Mikrotik MetaROUTER*. Jasakom, 2016. [Online]. Available: http://www.jasakom.com

[4] F. F. A. Firmansyah and R. Umar, "Analisis Forensik Metarouter pada Lalu Lintas Jaringan Klien," *Edu Komputika*, vol. 6, no. 2, pp. 54–59, 2019.

[5] Y. Wang, E. Keller, B. Biskeborn, J. van der Merwe, and J. Rexford, "Virtual routers on the move," p. 231, 2008, doi: 10.1145/1402958.1402985.

[6] F. Baumgartner, T. Braun, E. Kurt, and A. Weyland, "Virtual routers: A tool for networking research and education," *Computer Communication Review*, vol. 33, no. 3, pp. 127–135, 2003, doi: 10.1145/956993.957008.

[7] F. Firmansyah, A. Fadlil, and R. Umar, "Identifikasi Bukti Forensik Jaringan Virtual Router Menggunakan Metode NIST," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 5, no. 1, pp. 91–98, Feb. 2021, doi: 10.29207/resti.v5i1.2784.

[8] A. Luse and J. Rursch, "Using a virtual lab network testbed to facilitate real-world hands-on learning in a networking course," *British Journal of Educational Technology*, vol. 52, no. 3, 2021, doi: 10.1111/bjet.13070.

[9] S. Xiao, "VR Open Computer Network Virtual Laboratory Based on Big Data Technology," *J Phys Conf Ser*, vol. 1648, no. 4, p. 042105, Oct. 2020, doi: 10.1088/1742-6596/1648/4/042105.

[10] N. Nelmiawati, N. C. Kushardianto, A. H. Tohari, Y. P. Hasibuan, and D. E. Kurniawan, "Rancang Bangun Lab Komputer Virtual Berbasis Cloud Computing Menggunakan Openstack Pada Jaringan Terpusat," *JOURNAL OF APPLIED INFORMATICS AND COMPUTING*, vol. 2, no. 1, 2018, doi: 10.30871/jaic.v2i1.821.

[11] X. QI, "The Construction and Research of Computer Network Laboratory Based on Virtual Simulation Technology," *DEStech Transactions on Engineering and Technology Research*, no. amma, 2017, doi: 10.12783/dtetr/amma2017/13368.

[12] S. Vighnesh, "A Virtual Laboratories for Computer Network," *Int J Res Appl Sci Eng Technol*, vol. 6, no. 4, 2018, doi: 10.22214/ijraset.2018.4349.

[13] S. A. Mandowen, "Analisis forensik komputer pada lalu lintas jaringan," *Jurnal Sains*, vol. 16 (1), pp. 14–20, 2016.

[14] F. H. P. Y. Firmansyah, "Analisis Simulasi Mitigasi Ancaman ARP Dan Round Trip Time Pada Lalu Lintas DHCP VTP," *Progresif: Jurnal Ilmiah Komputer*, vol. 19, no. 1, pp. 137–144, Feb. 2023.

[15] A. Ramli, S. Sriyono, and H. Ramza, "Analisa Kecepatan Lalu Lintas Data Jaringan Local Area Network Menggunakan Graphical Network Simulator 3 (GNS-3)," *Electrical Engineering Acta*, vol. 1, no. 1, pp. 13–19, May 2021, doi: 10.22236/ate.v1i1.6946.