JIKSTRA Vol. 03, No. 01, April 2021
p-ISSN:2715-887X
e-ISSN:2747-2485

IMPLEMETASI KEAMANAN JARINGAN BERBASIS VPN DAN ANTI-DDOS DALAM MELINDUNGI SERVER LINUX DARI SERANGAN HAMMER

Raka Nugraha Pangestu[1],Herlina Harahap[2],Rismayanti[3]

[1,2,3]Program Studi Teknik Informatika, Fakultas Teknik dan Komputer, Universitas Harapan Medan.
[1]rakanugrahapangestu44@gmail.com,[2]herlinaharahap66@gmail.com,[3]risma.stth@gmail.com

ABSTRAK

Walaupun banyak metode keamanan yang dapat digunakan untuk menghalau serangan DDoS, namun untuk sekarang ini metode-metode tersebut bisa dibilang sudah kurang efektif, karena telah banyak hacker mengetahui bugs dari sistem atau metode-metode keamanan tersebut. Dari latar belakang masalah tersebut, sehingga dilakukan pengujian keamanan server linux, Linux Mint tanpa VPN dan Anti DDoS, mengimplementasikan keaman jaringan dari serangan hammer pada server linux Linux Mint dengan VPN dan Anti-DDoS, dan melakukan pengujian serangan DDoS dan VPN telah berhasil di implementasikan pada linux mint. Anti-DDoS dan VPN mampu untuk mencegah serangan DDoS pada server linux dengan cara memblokir IP yang tidak dikenal untuk mengakses server dan mengalihkan serangan ke virtual IP yang disediakan oleh VPN.

Kata Kunci: Anti DDoS, VPN, Hammer

ABSTRACT

Although there are many security methods that can be used to block DDoS attacks, for now these methods are arguably less effective, because many hackers have known bugs from the system or security methods. From the background of this problem, testing the security of Linux Mint servers, Linux Mint without VPN and Anti DDoS, implementing network security from hammer attacks on Linux Mint Linux servers with VPN and Anti-DDoS, and testing DDoS and VPN attacks have been successfully implemented. on linux mint. Anti-DDoS and VPN are able to prevent DDoS attacks on Linux servers by blocking unknown IPs from accessing the server and redirecting attacks to virtual IPs provided by the VPN.

Keyword:*Anti DDoS, VPN, Hammer*

1. PENDAHULUAN

Jaringan komputer dapat bersifat *private* atau publik. Jaringan *private* biasanya memerlukan *user* untuk memasukkan kredensial untuk mengakses jaringan. Biasanya, ini diberikan secara *manual* oleh *administrato*r jaringan atau diperoleh langsung oleh pengguna melalui kata sandi atau dengan kredensial lainnya [1].

Hal tersebut membuat banyak orang atau individu lebih memilih untuk membangun server pribadi mereka sendiri seperti ini sangat rentan dengan serangan DDoS seperti ini sangat rentan dengan serangan DDoS.

Walaupun bersifat pribadi, apabila sebuah sistem jaringan komputer tidak memiliki sistem keamanan, maka akan sangat mudah di retas oleh orang – orang yang

tidak bertanggung jawab. Salah satu serangan yang paling mudah dilakukan adalah dengan DDoS.DDoS adalah jenis serangan yang dilakukan dengan membanjiri lalu lintas jaringan internet pada server, sistem, atau jaringan. DDoS adalah serangan yang sangat populer dilakukan oleh banyak hacker.

Salah satu *scipt* yang sangat populer adalah hammer. Hammer merupakan salah satu *script* yang menggunakan bahasa *python* dan dikenal

sebagai salah satu *script* DDoS yang sangat baik dalam melakukan serangan DDoS.

Anti-DDoS merupakan salah satu sistem keamanan jaringan terbaru. Proyek Anti-DDoS adalah proyek perangkat lunak sumber terbuka yang dikembangkan untuk melindungi server dari serangan DdoS. Secara umum, serangan DDoS dilakukan untuk mendistrupsi kegiatan yang berhubungan dengan internet dengan cara menghabiskan sumber daya atau *resource* target, baik dengan membuat *crash/reboot/hang hardware*, menghabiskan *bandwidth* yang dibutuhkan oleh target untuk berkomunikasi dengan *client* lain [2].

Proyek Anti-DDoS adalah proyek perangkat lunak sumber terbuka yang dikembangkan untuk melindungi *server* dari serangan DDoS. Proyek ini ditulis mengguakan bahasa pemrograman bash dan php. Anti-DDoS bekerja dengan cara menulis aturan *iptables* ke dalam sistem operasi linux serta mengambil konfiguasi pertahanan yang diperlukan. Proyek Anti-DDoS hanya berfungsi pada sistem operasi linux dan 100% kompatibel untuk sistem operasi linux. Sedangkan untuk sistem operasi lain belum ada dukungan [3].

VPN merupakan teknologi komunikasi yang memungkinkan pengguna melakukan koneksi ke jaringan privatnya melalui internet secara aman dengan sistem tunneling, dan menggunakan jaaringan publik sebagai jalurnya [4].

Hammer adalah sebuah perangkat lunak berbentuk script dengan bahasa pemrograman python. *Hammer* berfungsi sebagai salah satu alat untuk melakukan serangan DDoS pada sebuah *server*. Secara umum, serangan DDoS dilakukan untuk mendistrupsi kegiatan yang berhubungan dengan internet dengan cara menghabiskan sumber daya atau *resource target*, baik dengan membuat *crash/reboot/hang hardware*, menghabiskan *bandwidth* yang dibutuhkan oleh target untuk berkomunikasi dengan *client* lain. Salah satu cara untuk melakukan penyerangan ini adalah membanjiri koneksi antara satu mesin dengan mesin lain dengan paket-paket dalam jumlah yang banyak [5].

2. METODE PENELITIAN

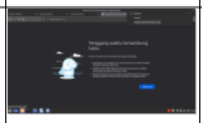
Adapun metode yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Lineratur dan Kajian Pustaka
   Metode ini digunakan untuk mendapatkan data yang diperlukan melalui buku, jurnal, dan internet.
2. Eksperimen
   Merupakan metode dengan mengadakan eksperimen atau pembuatan alat seperti instalasi dan konfigurasi pada layanan yang diterapkan.
3. Pengujian
   Metode ini merupakan uji coba terhadap keamanan menggunakan VPN dan Anti-DDoS dalam menegah serangan hammer.

3. HASIL PENELITIAN

Pengujian server dilakukan dengan cara melakukan akses melalui beberapa alamat IP yang ada pada server. Adapun hasil pengujian server dapat dilihat pada Tabel 1.

Tabel 1. Hasil Pengujian

No.	Jenis IP	Alamat IP	Port	Hasil	Status
1	Lokal PC	0.0.0.0	8000		Dapat Diakses
2	Lokal PC	127.0.0.1	8000		Dapat Diakses
3	Lokal Area	192.199.3.11	8000		Dapat Diakses
4	Publik Area	36.68.107.83	8000		Tidak Dapat Diakses
5	Virtual Area	27.122.12.232	8000		Tidak Dapat Diakses

IP 0.0.0.0:8000 merupakan IP lokal yang hanya dapat diakses melalui PC Server dan tidak dapat diakses melalui jaringan publik, saat diakses melalui jaringan lokal web sampel dapat berjalan normal dan Anti DDoS berjalan dengan normal.

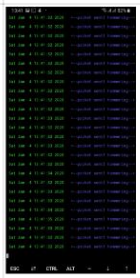
IP 127.0.0.1:8000 merupakan IP lokal yang hanya dapat diakses melalui PC Server dan tidak dapat diakses melalui jaringan publik, saat diakses melalui jaringan lokal web sampel dapat berjalan normal dan Anti DDoS berjalan dengan normal.

IP 192.199.3.11:8000 merupakan IP lokal yang dapat diakses melalui PC Client yang terdapat dalam 1 (satu) jaringan *router* dan tidak dapat diakses melalui jaringan publik, saat diakses melalui jaringan lokal web sampel dapat berjalan normal dan Anti DDoS berjalan dengan normal.

IP 36.68.107.83:8000 merupakan IP publik yang dapat diakses melalui PC Server, Client dan dapat diakses melalui jaringan publik, saat diakses melalui jaringan publik web sampel tidak dapat berjalan normal, hal ini dikarenakan VPN mengarahkan tujuan akses ke IP virtual.

IP 27.122.12.232:8000 merupakan IP virtual yang dapat diakses melalui PC Server, Client dan dapat diakses melalui jaringan publik, saat diakses melalui jaringan publik web sampel tidak dapat berjalan normal, hal ini dikarenakan VPN melindungi IP dari PC Server dari serangan pihak ketiga.

Tabel 2. Hasil Pengujian Serangan Hammer

No.	Jenis IP	Alamat IP	Port	Hasil	Keterangan
1	Lokal Area	192.199.3.11	8000		Tidak Berhasil Menembus Server
2	Publik Area	36.68.107.83	8000		Tidak Berhasil Menembus Server
3	Virtual Area	35.193.161.204	80		Tidak Berhasil Menembus Server

Pada Tabel 2. dapat dilihat bahwa pengujian serangan pada server menunjukkan bahwa serangan DDoS melalui hammer dapat berjalan dengan normal namun tidak menimbulkan efek down pada server. Hal ini membuktikan bahwa Anti DDoS dan VPN mampu melindungi server dari serangan DDoS. VPN membuat seolah-olah penyerang telah berhasil menembus dan melakukan serangan pada server, namun sebenarnya serangan tersebut dialihkan ke IP Virtual yang dibangun oleh VPN dan Anti DDoS memverifikasi setiap akses masuk yang tidak dikenal.

Implementasi VPN dengan *windscribe* langkah pertama adalah membuat akun baru di situs resmi *windscribe*. Setelah akun selesai dibuat, maka langkah selanjutnya dapat melakukan perintah konfigurasi dengan menambahkan key pada apt linux dengan perintah “sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-key FDC247B7”, selanjutnya menambahkan daftar sumber ke repositori linux dengan perintah “echo 'deb https://repo.windscribe.com/ubuntu bionic main' | sudo tee /etc/apt/sources.list.d/windscribe-repo.list”, melakukan pembaruan apt linux dengan perintah “sudo apt-get update”, dan melakukan instalasi windscribe dengan perintah “sudo apt-get install windscribe-cli”.

Setelah *windscribe* berhasil dipasang pada server linux mint, langkah selanjutnya adalah mengimplementasikan atau mengkonfigurasi *windscribe* sebagai VPN pada server linux mint dengan menjalankan perintah “*windscribe login*” pada

terminal yang kemudian di isi dengan informasi login yang telah ada dan selanjutnya adalah menjalankan perintah "*windscribe connect*" dan hasilnya telah berhasil dihubungkan ke VPN *windscribe* dan alamat IP yang tadinya adalah 36.68.107.83 berubah menjadi 27.122.12.236 yang tepatnya berada di Hongkong Victoria.

Implementasi Anti-DDoS dilakukan dengan cara menyisipkan script Anti-DDoS pada bagian <head website sampel pengujian. Peletakan *script* Anti-DDoS terletak pada bagian sebelum <head pada website sampel. Script tersebut akan berjalan apabila diakses melalui IP yang tidak dikenali. Dalam hal ini IP dapat ditentukan antara yang termasuk *whitelist* atau *blacklist*. Implementasi MyServer dalam penelitian ini adalah sebagai *server nginx* untuk menjalankan *website* sampel pada server linux mint. Adapun implementasi MyServer dapat dilakukan dengan menjalankan perintah "git clone https://github.com/Rajkumrdusad/MyServer.git" pada terminal linux yang berfungsi untuk menkloning repositori MyServer, langkah selanjutnya kemudian buka repositori yang telah berhasil di kloning tadi dengan perintah "cd MyServer", setelah itu ketikkan perintah "chmod +x install" untuk merubah ijin dari file instalasi MyServer, untuk melakukan instalasi dengan mengetikkan perintah "sh install". Melalui langkah tersebut diketahui bahwa MyServer telah berhasil terpasang pada server linux mint, dan untuk langkah selanjutnya adalah mengetikkan perintah "myserver start" untuk menjalankan MyServer.

Untuk menentukan IP dari server agar *website* nantinya dapat diakses melalui IP tersebut. Khusus dalam penelitian ini konfigurasi IP diatur menjadi 0.0.0.0 yang bertujuan agar semua IP terbuka dan dapat tertuju ke server, sehingga VPN juga dapat berfungsi pada server website di linux mint. Kemudian langkah selanjutnya adalah mengkonfigurasi PHP pada MyServer.

Implementasi hammer pada termux melalui beberapa tahap, yaitu tahap pertama adalah memasang python dan git pada termux. Adapun tahapan untuk memasang python dan git dapat dilakukan dengan perintah "pkg install python" dan kemudian ikuti perintah selanjutnya dan tunggu proses sampai selesai, kemudian memasang git ketikkan perintah "pkg install git" dan kemudian ikuti perintah selanjutnya dan tunggu proses sampai selesai. Tahap kedua, yaitu pemasangan hammer pada termux dengan mengetikkan perintah "git clone https://github.com/cyweb/hammer" dan tunggu proses sampai dengan selesai. Selanjutnya untuk menjalan hammer dapat mengetikkan perintah "cd hammer" dan mengubah ijin hammer dengan perintah "chmod +x hammer.py", lalu menjalankan hammer dengan perintah "python hammer.py -s [isi dengan IP target] -p [isi dengan port target] -t 135".

Pengujian server melalui IP pada lokal PC dan lokal area menunjukkan bahwa website sampel dapat diakses dengan normal, namun untuk akses melalui IP publik dan virtual sama sekali tidak terdapat respon dan website sampel tidak dapat diakses Hal tersebut bertujuan agar penyerang tidak mampu melakukan serangan DDoS terhadap server. IP 0.0.0.0:8000 merupakan IP lokal yang hanya dapat diakses melalui PC Server dan tidak dapat diakses melalui jaringan publik, saat diakses melalui jaringan lokal web sampel dapat berjalan normal dan Anti DDoS berjalan dengan normal. IP 127.0.0.1:8000 merupakan IP lokal yang hanya dapat diakses melalui PC Server dan tidak dapat diakses melalui jaringan publik, saat diakses melalui jaringan lokal web sampel dapat berjalan normal dan Anti DDoS berjalan dengan normal. IP 192.199.3.11:8000 merupakan IP lokal yang dapat diakses melalui PC Client yang terdapat dalam 1 (satu) jaringan router dan tidak dapat diakses melalui jaringan publik,

saat diakses melalui jaringan lokal web sampel dapat berjalan normal dan Anti DDoS berjalan dengan normal. IP 36.68.107.83:8000 merupakan IP publik yang dapat diakses melalui PC Server, Client dan dapat diakses melalui jaringan publik, saat diakses melalui jaringan publik web sampel tidak dapat berjalan normal, hal ini dikarenakan VPN mengarahkan tujuan akses ke IP virtual. IP 27.122.12.232:8000 merupakan IP virtual yang dapat diakses melalui PC Server, Client dan dapat diakses melalui jaringan publik, saat diakses melalui jaringan publik web sampel tidak dapat berjalan normal, hal ini dikarenakan VPN melindungi IP dari PC Server dari serangan pihak ketiga.

Untuk pengujian serangan pada server menunjukkan bahwa serangan DDoS melalui hammer dapat berjalan dengan normal namun tidak menimbulkan efek down pada server. Hal ini membuktikan bahwa Anti DDoS dan VPN mampu melindungi server dari serangan DDoS. VPN membuat seolah-olah penyerang telah berhasil menembus dan melakukan serangan pada server, namun sebenarnya serangan tersebut dialihkan ke IP Virtual yang dibangun oleh VPN dan Anti DDoS memverifikasi setiap akses masuk yang tidak dikenal.

4. KESIMPULAN

Berdasarkan hasil dari penelitian ini, maka dapat diuraikan kesimpulan sebagai berikut:

1. Sistem keamanan server linux menggunakan Anti-DDoS dan VPN telah berhasil di implementasikan pada linux mint.
2. Anti-DDoS dan VPN mampu untuk mencegah serangan DDoS pada server linux dengan cara memblokir IP yang tidak dikenal untuk mengakses server dan mengalihkan serangan ke virtual IP yang disediakan oleh VPN.

UCAPAN TERIMA KASIH

Ucapan terima kasih disampaikan kepada semua pihak yang telah berperan dalam membantu menyelesaikan jurnal ini yaitu, kepada orang tua & seluruh dosen fakultas teknik dan komputer. Sehingga, penulis dapat menyelesaikan jurnal ini dengan baik.

DAFTAR PUSTAKA

[1] D. Sopandi, *Instalasi dan Konfigurasi Jaringan Komputer*. Bandung: Informatika, 2017.

[2] M. S. Bagus Mardiyanto, Tutuk Indriyani and B. Mardiyanto, “Analisis Dan Implementasi Honeypot Dalam Mendeteksi Serangan Distributed Denial-Of-Services (DDOS) Pada Jaringan Wireless,” *Integer J.*, vol. Vol. 1, no. No. 2, 2016.

[3] R. D. Patisa, “Serangan DDoS Menggunakan Hammer | Formasi Berita.” 2019, Accessed: Nov. 22, 2019. [Online]. Available: https://formasiberita.blogspot.com/2019/11/serangan-ddos-menggunakan-hammer.html.

[4] A. R. Azwary, "Perbandingan Protokol L2tp Dengan Protokol PPTP Sebagai VPN Untuk Koneksi Antar Cabang," Universitas Sumatera Utara, 2015.
[5] Petunjuk Penulisan dan Kirim Artikel Jurnal Jikstra Mulai Penerbitan Tahun 2019.