TELCOMATICS, Vol.6 No. 1, Juni 2021, pp.11-16
eISSN: 2541-5867
DOI: 10.37253/telcomatics.v6i1.4990

Analisa Keamanan *Web Server* terhadap Serangan *Distributed Denial of Service* menggunakan *Modevasive*

Muhamad Dody Firmansyah
Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas, Internasional Batam, Kota Batam
E-mail: dodyfirmansyah.dodi@gmail.com,

ABSTRAK

Perkembangan teknologi informasi khususnya dalam keamanan digital baik itu berupa website adalah merupakan aspek yang sangat penting sekali dalam hal untuk upaya pencegahan terjadinya hal yang tidak diingikan seperti tim hacker yang sering melakukan kejahatan didunia maya dengan metode phising, ddos attacking, dan banyak sekali metode yang digunakan untuk melakukan kejahatan cyber di internet. Teknik serangan yang paling populer dijumpai seperti, Cross Site Scripting, Sql Injection, phising dan attack ddos. Teknik serangan hacker yang terhubung dan dipakai adalah teknik dalam Ddos (*Distributed Denial of Service)*. Setelah mengumpulkan banyak pembuktian mengetahui teknik Distributed Denial of Service ini ialah teknik gangguan hacker sering kali di lakukan oleh orang yang ahli dari jarak jauh, Peneliti menemukan adanya Analisa Keamanan Web Server belum sepenuhnya efektif bisa di atasi dengan adanya serangan Distribited Denial of Service Dari pemasalahan tersebut oleh karena itu peneliti melakukan penelitian Analisa keamanan web dengan menggunakan Modevasive.

Katakunci: Keamanan Internet, *Ddos Attack, Phising, Cybercrime,* Keamanan web server, *Distributed Denial Of Service, Modevasive, Penetration Test, Cyber Attack*

ABSTRACT

Development of information Web technology Service, especially on digital security, whether in the form of a website, is a very important aspect in terms of efforts to prevent unwanted things from happening, such as a team of hackers who often commit crimes in cyberspace with the phishing method, ddos attacking, and various methods used. to commit cyber crimes on the internet. The most popular attack techniques are found, such as, Cross Site Scripting, Sql Injection, phishing and ddos attacks. The most frequently used hacker attack technique is the Distributed about Denial-of-Service technique. After collecting a lot of evidence, knowing that Tehcnic Distributed Denial of Service is a hacked attack technique carried out by remote experts, the researcher found that the Web Server Security Analysis was not yet fully effective, it could be overcome by the Distributed Denial of Service attack. Based on the background description problems above, the authors are interested in conducting research using Modevasive.

Keywords: Internet Security, Ddos Attack, Phishing, Cybercrime, Security Webserver, Distributed Denial Of Service, Modevasive, Penetration Test, Cyber Attack

I. PENDAHULUAN

Perkembangan website di dunia saat ini sangat pesat sekali, Keamanan informasi dalam sebuah *website* menjadi yang paling sangat penting dan menjadi bagian utama bagi seorang *web development* dan tidak lepas bagi sebuah profesi keamanan sistem informasi yang sangat andil dalam melakukan pengecekan, pengamanan dan ketahanan dalam sebuah *website* [5].

Webserver sarana penunjang untuk kebutuhan dalam sebuah rangkaian keamanan untuk menggabungkan data *client* dalam induk jaringan *web server*, kemudian dari *request client* bisa memperoleh sebuah informasi yang di hubungkan melalui koneksi *web server*. Sistem keamanan dalam perantara konektivitas dapat terhubung sehingga mengandung sebuah informasi maupun berupa data-data yang bersifat *privacy* / sangat rahasia.

TELCOMATICS, Vol.6 No.1, 2021, pp.11-16
eISSN : 2541-5867
DOI: 10.37253/telcomatics.v6i1.4990

Pada saaat ini banyak terdapat sebuah aplikasi berbasis pengelolaan *web* atau *tools* yang bisa membuat kita mudah untuk memproses suatu data pada jaringan *server*, maka oleh karena itu jika kita memiliki aplikasi yang sangat penting yang ingin untuk mendapatkan pengelolaan kedalam jaringan *system* (Handi Prasetyo, 2016).

Hacker dengan senang bisa melakukan serangan dengan menggunakan metode tersebut dengan mudah dan leluasa mengubah *server*. *Denial Distribute of Service* adalah sebuah sistem penyerangan dimana bisa melumpuhkan *web* dan akan membuat akibat atau dampak dalam sebuah *resource*/sumber yang kita punya sebuah oleh *web* terhadap jaringan *server* hingga mengakibatkan dampak membuat sebuah fungsi dengan baik.

Berdasarkan hasil dari deskripsi pada latar belakang tsesebut, jadi dapat disimpilkan tujuan dari penelitian yang kita capai dalam penelitian adalah untuk mempraktekkan mengenai ilmu pengetahuan dan [4]. teknologi mengenai Analisa Keamanan *Web Server* Terhadap Serangan *Distributed Denial of Service* Menggunakan *Modevasive*

II. LANDASAN TEORI

Berikut ini adalah untuk melihat lalu kita akan menganalisa dalam keamanan dalam sebuah jaringan di dalam sebuah *website server* maka ada beberapa teori yang di landaskan dalam artikel ini.

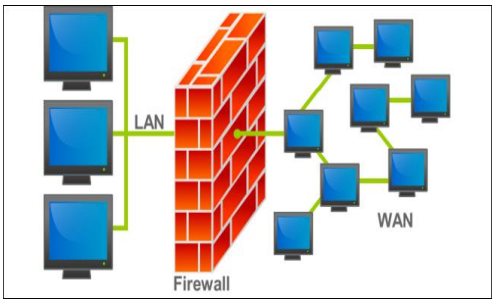
A. Sistem Keamanan Jaringan

Keamanan jaringan PC *(Personal Computer)* merupakan hal prioritas dalam sistem *security* jaringan dalam *computer*. Hal ini berkaitan dengan banyaknya aplikasi yang terlibat apabila tidak dijaga maka akan terganggu ketidakstabilan koneksi kedalam sebuah perangkat *computer* itu sendiri sehingga bisa menyebabkan *software* menjadi *crash* dan rusak inilah yang menjadi penyebabnya.[4]. Adapun beberapa perlindungan yang harus dilakukan agar bisa memfilter, membatasi dan tidak menerima nya adalah dengan membuat suatu segmen atau sebuah jaringan hubungan pribadi yang jaringan nya di atau ruang lingkupanya sendiri, segmen tersebut bisa di lihat pada jaringan LAN *(Local Area Network)* dan juga pengaturan *firewall* yang harus di pahami, yang dibagi menjadi dua jenis:

1. Dalam konfigurasi ini tidak bisa di akses dan tidak bisa masuk dalam sistem. semua yang akses akan mencoba melewati batas sistem yang di cegah oleh namanya dinding keamanan *firewall* yang kita sebut dengan pertahanan
2. Semua yang ada konsep terkonfigurasi dengan adanya filter baik akses masuk dan keluar pada sistem sehingga mempunyai syarat-syarat jika ingin masuk dan keluar oleh sistem pada batas – batas yang di perbolehkan oleh sebuah sistem yang kita sebut sebagai *firewall (Permitted).*

B. Firewall

Menurut [4], *Firewall* adalah sebuah sistem keamanan dalam entitas jaringan *computer* yang terbentuk dari dinding-dinding yang kuat sebagai pertahanan dari *server* yang ada dalam sebuah jaringan *internet*.



Gambar 1. Ilustrasi Firewall

Gambar 1 merupakan ilustrasi firewall. Firewall saat ini banyak sekali digunakan untuk Iptables dengan pengganti ipchains dan mendukung sistem kernel dari 2.4 serta memiliki fitur yang sangat banyak disbanding dengan ipchain, diantaranya: (a) *Connection's tracking capability*: adalah kemampuan kita untuk mengecek apakah paket kita bekerja dengsn menggunakan ICMP dan UDP didalam sebuah koneksi tcp. (b) Menyederhanakan lagi dari paket dalam melakukan beberapa macam negoisasi (*input, output* atau *forward*). (c) Lalu ada *Rate-limited connection* dan *logging capability*. Dimana kita bisa membatasi usaha-usaha koneksi sebagai Tindakan atas segala preventif serangan *Syn flood denial of services* (DOS).

eISSN: 2541-5867
DOI: 10.37253/telcomatics.v6i1.4990

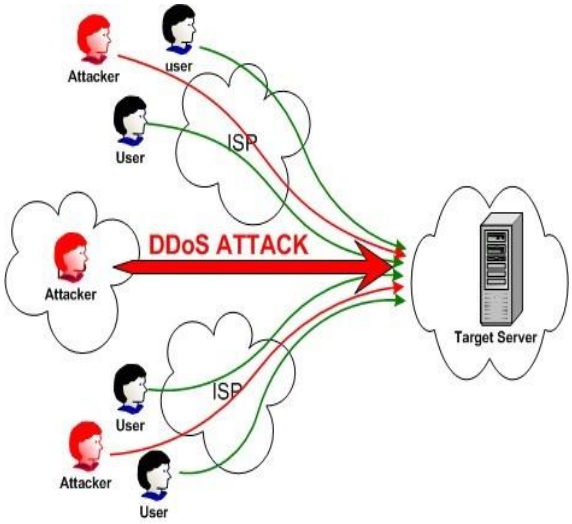
C. Web Application Firewall ModEvasive

Wireless Application Firewall (WAF) merupakan sebuah metode menggunakan memakai *Modsecurity* menjadi solusi buat pengamanan web server. WAF merupakan modul open source buat *web server Apache* yg dikembangkan sang SpiderLabs, Trustwave. WAF adalah produk open source, menggunakan lisensi perdeo yg memungkinkan dikembangkan sang poly pengguna. Mod-Security bisa melindungi pelaksanaan web berdasarkan aneka macam agresi & memungkinkan pemantauan kemudian lintas HTTP tanpa poly melakukan perubahan dalam infrastruktur yg ada Konsep pada kembali Web Application Firewall (WAF) sangat seperti menggunakan bagaimana firewall tradisional bekerja [11]. Firewall bekerja menurut suatu set anggaran yg dikonfigurasi dalam firewall atau yg dianggap menggunakan rule. Aturan ini yg selektif mengizinkan atau menolak kemudian lintas jaringan. Aturan dalam Web Application Firewall (WAF) secara spesifik didesain buat menyaring kemudian lintas jaringan menggunakan memakai protokol HTTP.

D. DDoS (*Distributed Denial of Service*)

DDoS adalah merupakan merupakan galat satu agresi yg terjadi pada global maya. Dimana penyerang berusaha buat menciptakan perangkat, server atau jaringan nir mampu dipakai sang pengguna [4]. Biasanya agresi ini dilakukan menggunakan cara membanjiri perangkat [9]. server yg ditargetkan menggunakan kemudian lintas yg tinggi [5].

Gambar 2 merupakan lustrasi serangan DDOS. Secara konsep adapun cara melakukan penyerangan dengan adanya *control* dalam sebuah [6] jaringan yang sedang *online* berupa jaringan *online* seperti perangkat PC *(Personal Computer)* atau *Device Portable* yang sedang *online* yang mempunyai *malware.* Dengan adanya ganguan ini setiap *device PC (Personal Computer)* menjadi sebuah *bot* inilah disebut dengan yang nama nya *botnet.* Jadi *Botnet* yang udah dibuat, dan juga yang menyerang dapat mengatur intruksi mesin-mesin dengan mengirimkan perintah *bot* ke *node* melalu *mode remote* dengan *control* [8].



Gambar 2. Berikut Ilustrasi Serangan DDOS

Ada banyak hal mengenai serangan *ddos.* Berikut adalah kejadian yang disebabkan oleh serangan ddos adalah sebagai berikut:

1. UDP Flood
   User Diagram Protocol adalah UDP adalah jenis serangan yang memanfaatkan protokol UDP dengan mengurangi sambungan *(connectionless)* untuk menyerang target. Dalam analisis ini menggunakan metode penelitian deskriptif untuk memperoleh data secara langsung dengan melakukan teknik *flooding.*
2. ICMP (Ping) Flood
   ICMP adalah *intruksi Ping Flood* yang dikenal dengan istilah kebanjiran perintah ping dengan serangan yang banyak penolakan, dimana penyerang ini membanjiri korban dengan menyebutkan paket *"echo dengan intruksi request" (ping)* ini menyerang dengan korban sangat merespon paket terhadap [1]. ICMP atau yang kita kenal dengan paket ICMP jadi banyak sekali memakan besar kebutuhan *bandwith* nya yang posisi *in* / masuk nya bandwidth
3. SYN Flood
   Syn Flood ini adalah sebuah bentuk penyerangan dengan *server* yang ada di internet jika kita bisa paham *frase* yang di pakai kita dapat mengetahui sebagai banjirnya SYN. karena permintaan SYN secara besar kepada *server* yang mengakibatkan *server* banjir inilah yang dinamakan *flood*

TELCOMATICS, Vol.6 No.1, 2021, pp.11-16
eISSN : 2541-5867
DOI: 10.37253/telcomatics.v6i1.4990

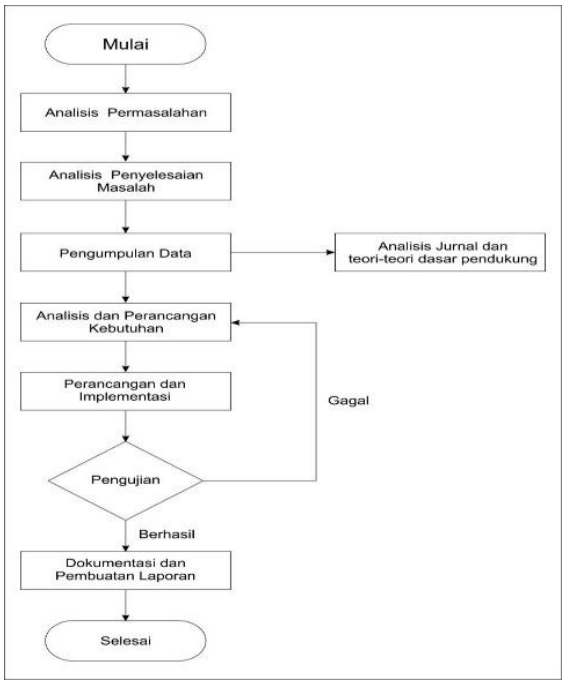
E. Apache Benchmark

Apache benchmark adalah *tool* untuk menganalisa pengukuran *performance apache*, dengan menggunakan tool *apache benchmark* dapat melihat fitur yang ada dalam menangani *kapabilitas request* dari *client-client* tersebut

III. METODOLOGI PENELITIAN

A. Alur Penelitian

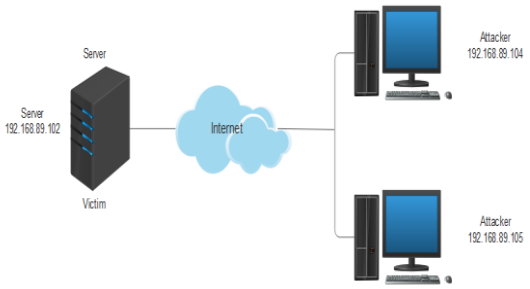
Alur penelitian berisi langkah-langkah yang digunakan dalam penelitian ini agar terstruktur dengan baik. Dengan sistematika ini proses penelitian dapat dipahami dan diikuti oleh pihak lain. Penelitian yang dilakukan untuk merancang sistem keamanan *web* yang handal diperoleh dari pengamatan data-data yang ada. Adapun langkah-langkah yang dilakukan untuk mencapai tujuan dari penelitian ini adalah seperti dibawah ini. Metode pengembangan yang digunakan dalam penelitian ini yaitu pada Gambar 3 dibawah ini:



Gambar 3. Diagram Alur Penelitian

B. Topologi jaringan

Jaringan adalah suatu cara untuk membuat sejumlah komputer saling berhubungan satu sama lain, baik menggunakan kabel maupun yang *nirkabel*. Biasanya, tujuan topologi jaringan adalah demi kemudahan pertukaran informasi. Berikut ini adalah Topologi Jaringan yang digambarkan oleh penelitian sebagai berikut:



Gambar 4. Topologi Jaringan

IV. IMPLEMENTASI PENELITIAN

A. Implementasi Serangan

Ada beberapa hal yang disiapkan demi melakukan analisis, berikut ini adalah rancangan bangun dari sistem *Distributed denial of service* seperti yang ditunjukkan pada Gambar 5.

```
root@debian:/home/yopi# apt-get install libapache2-mod-evasive
Reading package lists... Done
Building dependency tree
Reading state information... Done
libapache2-mod-evasive is already the newest version (1.10.1-3).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Gambar 5. Install Modevasive

Penginstalan modul untuk Apache untuk memberikan tindakan mengelak dari aktivitas HTTP DoS atau serangan DDoS atau serangan brute force

```
<IfModule mod_evasive20.c>
    DOSHashTableSize    3097
    DOSPageCount        2
    DOSSiteCount        50
    DOSPageInterval     1
    DOSSiteInterval     1
    DOSBlockingPeriod   10

    DOSEmailNotify      you@yourdomain.com
    #DOSSystemCommand    "su - someuser -c '/sbin/... %s ...'"
    DOSLogDir           "/var/log/mod_evasive"
</IfModule>
```

Gambar 6. Konfigurasi Mod Evasive

Gambar 6 menjelaskan penginstalan konfigurasi Mod Evasive dengan penjelasan

eISSN: 2541-5867
DOI: 10.37253/telcomatics.v6i1.4990

sebagai berikut. Tambahkan kode dibawah ini pada file /usr/local/apache/conf/includes/post_virtualhost _2.conf

bisa lewat console/ssh atau lewat WHM. Apache Configuration > Include Editor -> Post VirtualHost Include (pilih versi 2.2.xx).

```
root@debian:/home/yopi# mkdir /var/log/mod_evasive
```

Gambar 7. Direktori Modevasive

Gambar 7 menjelaskan mengenai direktori modevasive adalah sebagai berikut:

Kode yang diberikan _Uncomment #DOSLogDir _untuk mengaktifkan _logging _pada setiap aktivitas yang terjadi di Apache. Contoh, kita akan menggunakan _/var/log/mod_evasive _sebagai direktori tempat penyimpanan.

```
root@debian:/home/yopi# chmod 777 /var/log/mod_evasive
```

Gambar 8. Akses Folder Modevasive

Gambar 8 menjelaskan mengenai akses folder modevasive adalah sebaagai berikut : Cara akses folder dikarenakan mod_evasive ini dapat melakukan monitoring http request (incoming), (2).maka buat folder /var/log/mod_evasive dengna menggunakan perintah mkdir/var/log/mod_evasive lalu berikan otorisasi terhadap folder tersebut agar mo evasive dapat menulis.

```
root@debian:/home/yopi# a2enmod evasive
Module evasive already enabled
root@debian:/home/yopi# /etc/init.d/apache2 restart
[ ok ] Restarting apache2 (via systemctl): apache2.service.
```

Gambar 9. Cek Installan Modevasive

Gambar 9 menjelaskan mengenai cek penginstalan modevasive adalah sebaagai berikut: Cek apakah ModSecurity sudah enabled. Sebelum me-restart Apache2 cek apakah modules sudah diload dengan baik. Buka terminal dan lakukan sudo a2enmod headers

```
root@debian:/home/yopi# apt-get install apache2-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2-utils is already the newest version (2.4.25-3+deb9u7).
apache2-utils set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Gambar 10. Installasi Apache Benchmark

Gambar 10 menjelaskan mengenai installasi Apache Benchmark adalah sebaagai berikut : Untuk sistem operasi berbasis Debian/Ubuntu, bisa menggunakan command berikut: $ sudo apt install apache2-utils.Perlu diketahui, apabila kita sudah menginstal Apache 2 di sistem tersebut, maka apache2-utils belum terpasang di dalammnya. Jika apache2-utils sudah diinstal, kita dapat menggunakan Apache Bench pada Bash dengan perintah ab.

B. Uji coba Serangan

Langkah ini akan mencoba untuk melakukan serangan ke *webserver* yang telah di konfigurasi menggunakan *modevasive*:

```
root@debian:/home/yopi# ab -n 1000 -c 100 http://192.168.89.102:80/
This is ApacheBench, Version 2.3 <$Revision: 1757674 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking 192.168.89.102 (be patient)
Completed 100 requests
Completed 200 requests
Completed 300 requests
Completed 400 requests
Completed 500 requests
Completed 600 requests
Completed 700 requests
Completed 800 requests
Completed 900 requests
Completed 1000 requests
Finished 1000 requests


Server Software:        Apache/2.4.25
Server Hostname:        192.168.89.102
Server Port:            80

Document Path:          /
Document Length:        289 bytes

Concurrency Level:      100
Time taken for tests:   0.443 seconds
Complete requests:      1000
Failed requests:        12
   (Connect: 0, Receive: 0, Length: 12, Exceptions: 0)
Non-2xx responses:      988
Total transferred:      595072 bytes
HTML transferred:       413944 bytes
Requests per second:    2257.46 [#/sec] (mean)
Time per request:       44.297 [ms] (mean)
Time per request:       0.443 [ms] (mean, across all concurrent requests)
Transfer rate:          1311.87 [Kbytes/sec] received

Connection Times (ms)
              min  mean[+/-sd] median   max
Connect:        0   18   5.2     18      30
Processing:     5   24  13.6     21     104
Waiting:        5   20   6.4     20     100
Total:         17   42  12.3     40     118
```

Gambar 11. Uji Coba Serangan Ddos

Gambar 11 merupakan hasil uji coba serangan DDOS dengan penjelasan sebagai berikut:

1. Honeyd Adalah kegiatan yang dilakukan untuk memberikan servis seperti pada perangkat komputer asli kepada pengguna attacker dan juga dapat mendeteksi terhadap serangan Ddos secara up to date. Dengan Penggunaan

TELCOMATICS, Vol.6 No.1, 2021, pp.11-16
eISSN : 2541-5867
DOI: 10.37253/telcomatics.v6i1.4990

Iptables sehingga firewall bisa dibelokkan ke ip yang tidak digunakan.

2. Beban rata-rata kinerja cpu sebelum terjadi serangan sebesar 15.25% Setelah adanya serangan beban rata-rata kinerja cpu naik menjadi 45.98% setelah adanya pembelokkan serangan dengan iptables beban rata-rata kinerja cpu menurun menjadi 30.83%.

VI. KESIMPULAN

Dari implementasi *tool* yang dilakukan dalam peneltian ini maka peneliti merumuskan dan mencatatkan hasilnya dibawah ini:

1. Untuk memperoleh *secure* tingkat tinggi dalam perusahaan maka dalam menyimpan data harus dalam bentuk yang sangat protektif misalnya di sisipkan enkripsi / password sebagaimana mestinya keamanan yang disimpan di sistem *cloud computing* seperti *Dropbox, Google Drive,* dan seperti *AWS Cloud*, agar bisa mem*backup* data pada sistim keamanan teknologi informasi [3]..
2. Hasil Analisa keamanan *web* ini bisa menguji ketahanan *web* terhadap gangguan serangan *hacker*
3. Peneliti menjabarkan dengan Teknik *tools penetration testing* dalam keamanan *web* ini agar bisa terhindar dari serangan apapun.
4. Disarankan menggunakan *support tools* untuk melindungi sistem keamanan *web* terjaga dengan baik dan terhindar dari serangan.

V. DAFTAR PUSTAKA

[1] Anugrah, Klarisa. (2016). Pengenalan OSI Layer Kata Kunci : Pengenalan OSI Layer. 1–5.

[2] Hermawan, R. (2015). Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (DDOS). Faktor Exacta, 5(1), 1–14.

[3] Hidayat, T. (2014). Penerapan Teknologi Augmented Reality Sebagai Model Media Edukasi Kesehatan Gigi Bagi Anak. Creative Information Technology Journal, 2(1), 77–92.

[4] Prasetyo Handi. (2016). Analisa Keamanan Web Server Menggunakan Web Application Firewall Modsecurity. Artikel Ilmiah. 1–20.

[5] Metasari, D., & Irsyadi, F. Y. (2014). Analisis Keamanan Website.

[6] Muhammad Dedy harianto, I. R. (2014). 210977-Analisis-Dan-Optimalisasi-Jaringan-Menggunakan Teknik Load Balancing. 2, 1370–1378.

[7] Putera, A., & Siahaan, U. (2018). Cybercrime Offenses & Jurisdiction Power. 5(1), 6–9.

[8] Putra, F. widya. (2018). Analisis Keamanan Website Dari Serangan Sql Injection Menggunakan Web Application Firewall.

[9] Putra, R. S., Mayasari, R., Bogi, N., Karna, A., Elektro, F. T., & Telkom, U. (2018). Implementasi dan menganalisa keamanan dalam jaringan Virtual Hips Snort dalam kondisi penyerangan Ddos.(3), 4958–4965.

[10] Richard Pangalila, Agustinus Noertjahyana, J. A. (2015). Penetration Testing Server Sistem Informasi Manajemen Dan Website Universitas Kristen Petra. Jurnal Infra, 3(2), pp.271-p.276.

[11] Rizky, D., Laitupa, H., & Rizal, M. F. (2015). Implementation of Modsecurity as a Web Application Security Monitoring System in Real Time. EProceedings of Applied Science, 1(3), 2132–2134.

.