Methotika : Jurnal Ilmiah Teknik Informatika
ISSN : 2776 – 5792
Vol. 4, No. 2, Oktober 2024, pp. 21-31
http://ojs.fikom-methodist.net/index.php/methotika

Analisis Dan Implementasi IPS Dengan Metode Honeypot Di IDS Untuk Keamanan VPS Dari Serangan DDoS Dan Brute Force

Josafat Simamora[1], Naikson F. Saragih[2], Fati G.N. Larosa[3], Asaziduhu Gea[4]
[1,2,3]Fakultas Ilmu Komputer, Universitas Methodist Indonesia

Info Artikel

Histori Artikel:
Received, Agus 9, 2024
Revised, Sep 20, 2024
Accepted, Sep 11, 2024

Keywords:
VPS,
IDS,
IPS,
Honeypot,
DDoS.

ABSTRAK

Kehadiran Virtual Private Servers (VPS) sebagai platform hosting telah menjadi target utama serangan cyber, terutama serangan Distributed Denial of Service (DDoS) dan serangan Brute Force yang dapat mengakibatkan kerugian besar dalam hal ketersediaan dan integritas layanan. Untuk mengatasi tantangan ini, penelitian ini mengusulkan pendekatan yang mengintegrasikan Sistem Deteksi Intrusi (IDS) dengan Sistem Pencegah Intrusi (IPS) yang mengadopsi teknik Honeypot. Pendekatan ini bertujuan untuk mendeteksi dan mencegah serangan DDoS dan Brute Force secara efektif. Metode Honeypot digunakan untuk menarik serangan yang berpotensi dan menganalisis pola serangan yang terdeteksi, sementara IPS bertanggung jawab untuk merespons serangan dengan mengimplementasikan kebijakan perlindungan yang sesuai. Pengujian dan evaluasi dilakukan menggunakan simulasi serangan yang realistis, serta pengujian langsung di lingkungan VPS yang aktif. Hasil eksperimen menunjukkan bahwa pendekatan yang diusulkan mampu meningkatkan keamanan VPS dengan mengurangi kemungkinan keberhasilan serangan DDoS dan Brute Force, serta memberikan deteksi yang lebih cepat dan respons yang lebih efektif terhadap ancaman tersebut. Dengan demikian, penelitian ini memberikan kontribusi yang signifikan dalam upaya memperkuat keamanan infrastruktur berbasis VPS dari serangan cyber yang semakin kompleks dan berbahaya.

Penulis Koresponden:
Josafat Simamora,
Fakultas Ilmu Komputer,
Universitas Methodist Indonesia, Medan,
Jl. Hang Tuah No.8, Medan - Sumatera Utara.
Email: josafat@gmail.com

1. PENDAHULUAN

Keamanan jaringan pada komputer sangatlah penting untuk menjaga kerahasiaan data dan informasi yang terdapat pada server. Penerapan server sudah banyak dimanfaatkan baik untuk kepentingan pribadi, usaha, organisasi dan berbagai kebutuhan lainnya. Server menjadi solusi untuk mengelola dan memonitoring data penyimpanan yang luas serta mempermudah dalam menyimpan dan menghubungkan data antar komputer dengan lebih cepat. Khususnya pada era kemajuan teknologi saat ini yaitu pada teknologi *Virtual Private Server* (VPS) yang semakin dimudahkan dengan adanya berbagai macam layanan dari penyedia VPS baik lokal maupun non lokal yang

memiliki sumber daya terdedikasi khusus untuk satu pengguna serta sudah terisolasi pada masing-masing servernya. VPS merupakan sebuah server fisik yang dibagi menjadi beberapa server *virtual.* Selain itu VPS juga berpotensi lebih aman karena memililki *full* akses dalam pengoprasiannya sehingga bisa diterapkan *tools-tools* keamanan pada VPS. Banyaknya data penting yang di simpan di VPS mengundang banyak *attacker* yang berniat untuk menyerang. Dengan demikian jaringan komputer membutuhkan sebuah keamanan yang cukup kuat agar para *attacker* tidak mudah untuk melumpuhkan *server*. Tujuan dari keamanan jaringan komputer adalah untuk menjaga stabilitas, integritas, dan validitas data [1]**.**

Website Fakultas Ilmu komputer https://fikom-methodist.com yang digunakan pada saat ini untuk supleman simak UMI sesuai kebutuhan khususnya FIKOM UMI terus dikembangkan secara berkelanjutan. Website ini berada pada web hosting telah mengalami beberapa serangkaian serangan dan upaya pengamanan yang dilakukan dengan menerapkan akses dengan SSH, penambalan beberapa celah keamanan telah dilakukan. Namun upaya pengamanan yang bisa dilakukan pada web hosting memiliki keterbatasan. Untuk memaksimalkan keamanan dan ketahanan siber, maka website ini perlu dilakukan migrasi ke VPS. Dengan dilakukannya migrasi ke VPS, maka berbagai upaya keamanan untuk mencapai ketahanan siber dari serangan DDoS bisa dilakukan.

Sistem deteksi penyusup jaringan yang ada di VPS Fikom UMI pada saat ini belum seutuhnya berjalan dengan baik. Di VPS Fikom UMI pada saat ini sudah memiliki sistem keamanan seperti NMAP, Fail2ban, Snort, Port Knocking, dan Webuzo. Oleh karena itu penerapan metode *HoneyPot* sangat berpengaruh penting disini karena *HoneyPot* akan membantu menyempurnakan *Intrusion Detection System*(IDS) dalam melakukan deteksi serangan [2]. Pada umum nya attacker mengunakan berbagai macam jenis serangan, salah satunya jenis serangan yang paling sering digunakan adalah *Distributed Denial Of Service (Ddos) dan Brute Force.*

Serangan *Distributed Denial of Service* (DDoS) sebuah serangan yang terdistribusi dan mengimplikasikan beberapa komputer untuk mencoba saling membantu menyerang suatu *host, host* yang melakukan serangan DDoS di sebut juga*zombie* (Faiz et al., 2022). Serangan *Distributed Denial-of- Service* (DDoS) ini cukup populer dikalangan para hacker atau sering digunakan karena serangan ini memiliki banyak jenis dan memiliki konsep yang sederhana, yaitu membuat lalu lintas server berjalan dengan berat sehingga tidak bisa lagi menampungkoneksi dari user lain (overload).

Serangan *Brute force* adalah serangan yang memecahkan masalah dengan mencari *password cracking* yang *valid* dengan mencari semua kemungkinan *password* yang sudah disediakan dengan masukan karakter dan panjang *password* tertentu hal ini mencoaba untuk mengkombinasi *password* [3].

Untuk mendeteksi serangan DDOS dan Brute Force tersebut, dilakukan dengan menggunakan metode HoneyPot, Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) yang dapat mendeteksi dan memblokir jika adanya serangan dan penyusupan pada sever. HoneyPot digunakan untuk memancing perhatian para hacker, HoneyPot sengaja dibuat dengan tingkat keamanan yang rendah. Salah satunya dengan penggunaan port yang rentan terhadap pemindaian port. Kemudian port yang lemah tersebut dibiarkan terbuka agar hacker terpancing untuk menyerangnya. Honeypot adalah umpan atau perangkap yang dipasang secara khusus untuk memikat peretas dengan tujuan menangkap atau melacak peretas saat serangan terjadi. Honeypot berfungsi sebagai perangkap bagi peretas yang ingin memasuki web server, ketika peretas mencoba memasuki web server maka honeypot akan mengirimkan pemberitahuan kepada administrator bahwa telah terjadi penerobosan system.

2. METODE PENELITIAN

2.1 Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS) dikenal sebagai sistem deteksi intrusi dan pencegahan [4]. IPS adalah sebuah aplikasi perangkat lunak atau perangkatkeras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan dan dapat langsung mencegah serangan tersebut [5]. IPS memiliki dua jenis yaitu [6] *Network Intrusion Prevention System* (NIPS) dan *Host Intrusion Prevention System* (HIPS)

2.2 Intrusion Detection System (IDS)

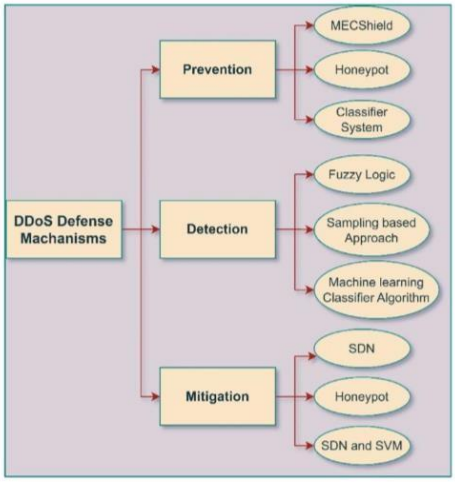
Intrusion Detection System (IDS) adalah sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan [7]. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan *traffic* jaringan, maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan [8].

2.3 Virtual Private Server (VPS)

Virtual Private Server (VPS) adalah tipe web hosting yang sumber dayanya berasal dari satu server fisik, yang kemudian terbagi lagi menjadi beberapa server virtual yang lebih kecil. Dalam hal ini, masing-masing server virtual berjalan seperti dedicated server [9]

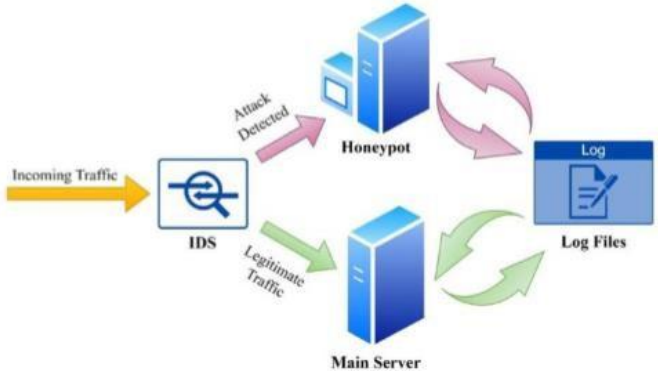
2.4 Honeypot

HoneyPot adalah umpan atau perangkap yang dipasang secara khusus untuk memikat peretas dengan tujuan menangkap atau melacak peretas saat serangan terjadi. Honeypot berfungsi sebagai perangkap bagi peretas yang ingin memasuki web server, ketika peretas mencoba memasuki web server maka honeypot akan mengirimkan pemberitahuan kepada administrator bahwa telah terjadi penerobosan system [10][11]. Honeypot dapat menangkal serangan DDoS dengan skema seperti pada Gambar 1.



Gambar 1 Skema Pertahanan DDoS [12]

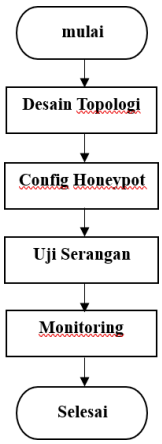
Honeypot produksi digunakan untuk melindungi server dari serangan DDoS secara *real time*. *Setup* honeypot dapat dibedakan menjadi dua bagian untuk proses pertahanan serangan DDoS. Adapun mekanisme pertahanan DDoS dengan honeypot seperti pada Gambar 2 [12].



Gambar 2. Skema Pertahanan Ddos Dengan Honeypot [12]

2.5 Framewok Penelitian

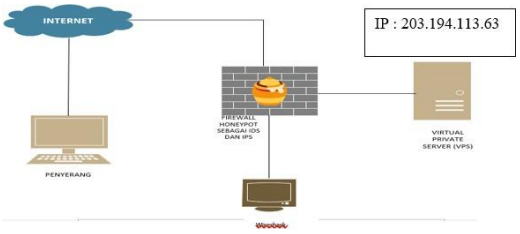
Framework penelitian yaitu kerangka penelitian yang akan membantu penulis dalam melakukan proses penelitian sehingga mendapatkan hasil yang diinginkan seperti pada gambar 3.



Gambar 3. Kerangka Kerja Penelitian

2.5.1 Perancangan Topologi Jaringan

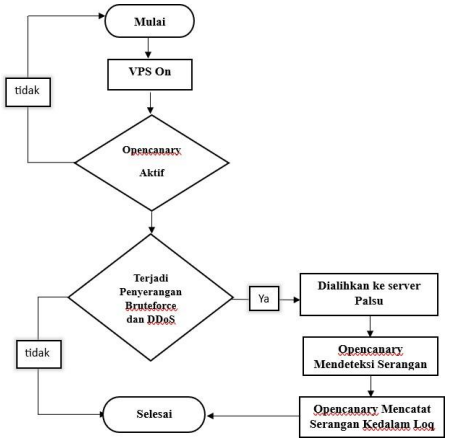
Pada topologi sistem usulan diatas Virtual Private Server (VPS) sudah menggunakan keamanan Honeypot. Pada gambar topologi diatas dapat dilihat server tidak terhubung secara langsung dengan internet. Terdapat Firewall yang melindungi Virtual Private Server (VPS) dari akses internet secara langsung dengan keamanan jaringan menggunakan metode Honeypot dan juga dilengkapi dengan Wireshark yang berfungsi untuk membantu IDS untuk mendeteksi dan memonitoring penyerang serta mengidentifikasi penyerang, alamat IP, Tanggal dan waktu serta port yang diserang seperti pada gambar 4:



Gambar 4 Gambaran Topologi Jaringan Diusulkan

2.5.2 Perancangan Skenario Serangan

Setelah uji coba serangan pertama maka akan dilakukan uji coba serangan kedua. Yaitu serangan terhadap VPS tetapi VPS sudah memiliki firewall Honeypot sebagai Ids dengan Ips didalamnya seperti pada Gambar 5.

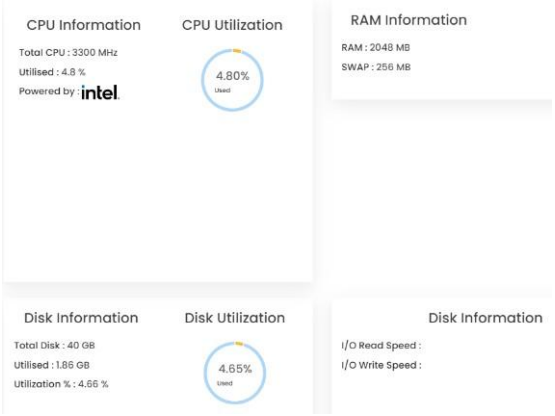


Gambar 5 Skenario Serangan

3. HASIL DAN PEMBAHASAN

3.1 Pengujian Sistem

Dalam hal ini sistem yang telah dianalisa dan dikonfigurasi dilanjutkan dengan sistem dioperasikan dan melakukan pengujian untuk melihat hingga sampai mana sistem yang dibuat dapat berjalan dengan baik hingga tujuan. Dalam proses Implementasi dan analisis keamanan VPS dari serangan DDoS dan *brute force* menggunakan *honeypot opencanary*. Sebelum dilakukan serangan, berikut adalah informasi kondisi awal CPU VPS:



Gambar 6 Kondisi Awal CPU Serta *Disk* VPS

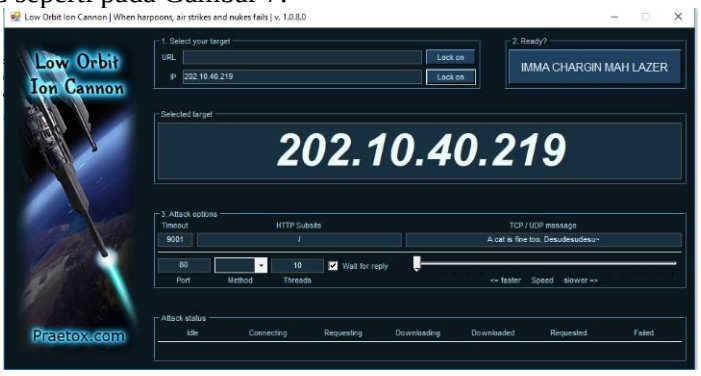
Berdasarkan pada Gambar 6, kondisi CPU VPS berada pada pemakaian 4.80% sedangkan kondisi *Disk* berada pada pemakian 4.66%. Agar pengujian lebih terarah dan dapat menghasilkan kesimpulan yang tepat, maka berikut adalah skenario pengujian dari keamanan VPS dengan *Honeypot Opencanary* dari serangan DDoS dan *brute force* seperti pada Tabel 1.

Tabel 1 Skenario Pengujian Serangan VPS

No	Jenis Serangan	Keamanan VPS	Jumlah Pengujian
1	DDoS	*Honeypot Opencanary*	5 Serangan
2	*Brute Force* Web Server	*Honeypot Opencanary*	5 Serangan
3	*Brute Force* SSH	*Honeypot Opencanary*	5 Serangan
4	*Brute Force* FTP	*Honeypot Opencanary*	5 Serangan

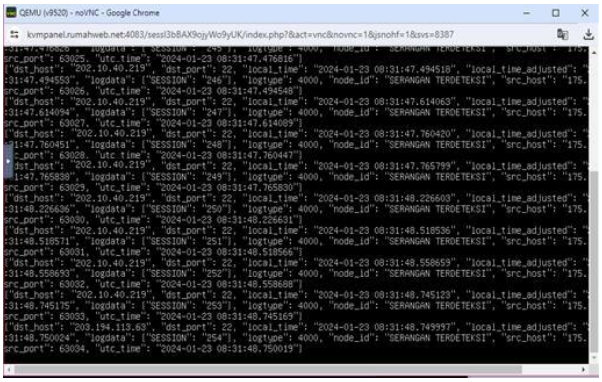
3.1.1 Pengujian Serangan Distributed Denial of Service (DDoS)

Pengujian ini akan melakukan penyerangan dari serangan DoS (*Distributed Denial of Service*) TCP *flooding* jumlah yang sangat besar ke server sehingga dapat mampu membuat sebuah server *crash* atau server tidak bekerja dengan baik. Serangan DDoS dilakukan dengan aplikasi LOIC, dimana aplikasi ini akan membajiri paket TCP yang terbuka. Berikut adalah hasil pengujian serangan DDoS dengan LOIC seperti pada Gambar 7.



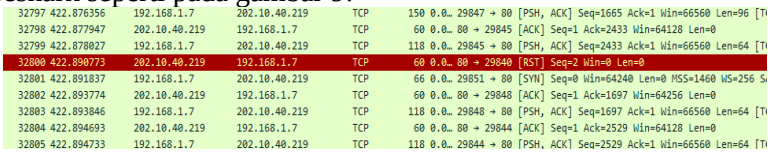
Gambar 7 DDoS TCP *Flooding*

Berikut adalah log serangan DDos pada *honeypot* seperti pada Gambar 8.



Gambar 8 *Log* Serangan DDoS Pada *Honeypot-1*

Berdasarkan log, *packet* serangan DDoS membanjiri *honeypot*. Berdasarkan tanda yang diberikan, diketahui serangan berasal dari IP 175.158.36.16 dengan tujuan IP 202.10.40.219 pada Tanggal 23/01/2024 dan jam 08:31:37, port=22, *Session* dari 245 hingga 254. *Honeypot Opencanary* berhasil mendeteksi serangan.*Honeypot Opencanary* berhasil mendeteksi serangan. Berikut adalah tangkapan serangan dari wireshark seperti pada gambar 9:



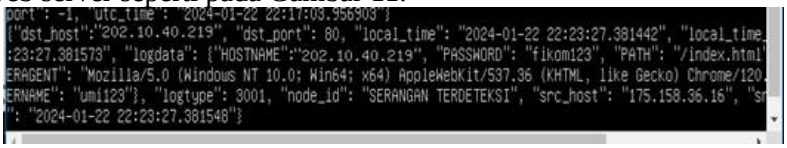
Gambar 9 Tangkapan *Wireshark* Serangan DDoS

3.1.2 Pengujian Serangan Brute Force Web Server

Serangan *brute force* adalah serangan yang mencoba akses *password* secara brutal (berkali-kali) dari suatu sistem. Pada penelitian ini, *honeypot* membuat ruang virtual palsu dengan alamat http://202.10.40.219/index.html. Selanjutnya melakukan serangan dengan menebak *username* dan *password* sistem pada halaman *login honeypot* seperti pada Gambar 10.

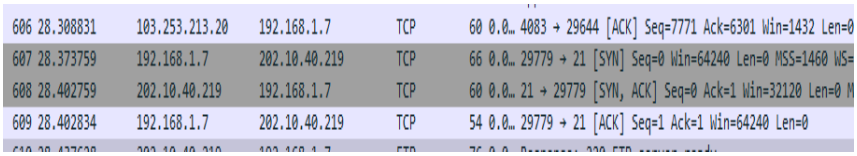
Gambar 10 Menebak Username Dan Password

Berdasarkan pada gambar di atas, ketika penyerangan melakukan *sign in* maka sistem keamanan *honeypot* akan mendeteksi adanya percobaan serangan dalam web server VPS. Berikut adalah *log* serangan pada web server seperti pada Gambar 11.



Gambar 11 *Log* Serangan Pada Web Server

Berdasarkan pada gambar log serangan web server diketahui serangan berasal dari IP 175.158.36.16 dengan tujuan IP 202.10.40.219 pada Tanggal 22/01/2024 dan jam 22:23:27, port=80, *browser crome* serta sistem operasi *windows*. *Username* yang diinputkan adalah umi123 sedangkan *password*nya fikom123. *Honeypot Opencanary* berhasil mendeteksi serangan. Berikut adalah tangkapan serangan dari wireshark seperti pada gambar 12:

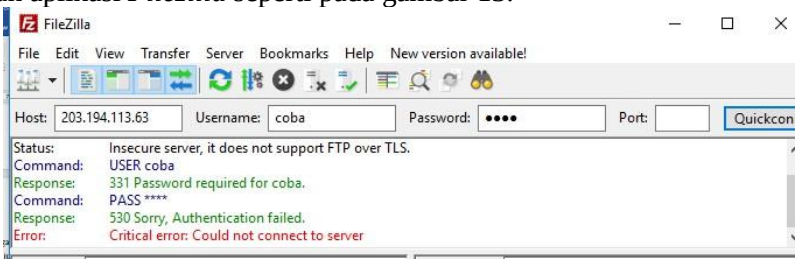


Gambar 12 Tangkapan *Wireshark* Serangan Web Server

Berdasarkan dari 2 contoh serangan, untuk serangan selanjutnya dilakukan dengan cara yang sama.

3.1.3 Pengujian Serangan Brute Force FTP

Serangan *brute force* FTP adalah serangan yang mencoba akses *password* secara brutal (berkali-kali) dari suatu sistem *File Transfer Protocol* (FTP). Pada penelitian ini pengujian serangan dilakukan dengan aplikasi *Filezilla* seperti pada gambar 13:

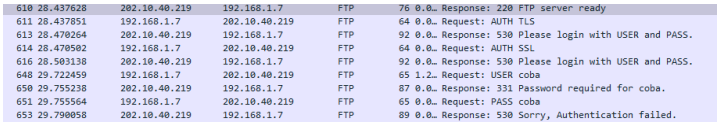


Gambar 13 Menebak *Username* Dan *Password Filezilla*

Berdasarkan pada gambar 13, ketika penyerangan melakukan koneksi maka sistem keamanan *honeypot* akan mendeteksi adanya percobaan serangan dalam FTP VPS. Berikut adalah *log* serangan pada *File Transfer Protocol* (FTP)seperti pada Gambar 14.

Gambar 14 *Log* Serangan Pada *File Transfer Protocol* (FTP)-1

Berdasarkan pada gambar log serangan *File Transfer Protocol* (FTP) diketahui serangan berasal dari IP 175.158.36.16 dengan tujuan IP 202.10.40.219 pada Tanggal 22/01/2024 dan jam 22:40: 59, port=21, *browser crome* serta sistem operasi *windows*. *Username* yang diinputkan adalah coba sedangkan *password*nya coba. *Honeypot* .Berikut adalah hasil tangkapan dari *wireshark* seperti pada gambar 15:

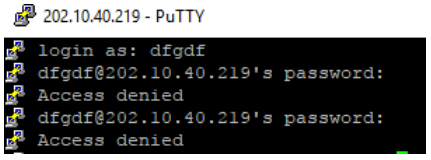


Gambar 15 Tangkapan *Wireshark* Serangan FTP

Berdasarkan dari 2 contoh serangan, untuk serangan selanjutnya dilakukan dengan cara yang sama.

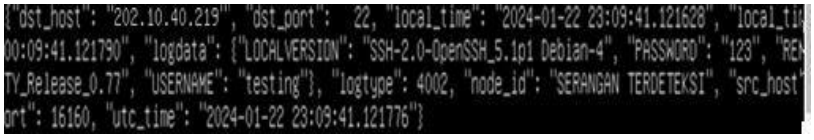
3.1.4 *Pengujian Serangan Brute Force SSH*

Serangan *brute force* SSH adalah serangan yang mencoba akses *password* secara brutal (berkali-kali) dari suatu sistem *Secure Shell* (SSH). Pada penelitian ini pengujian serangan dilakukan dengan aplikasi *putty* seperti pada gambar 16:



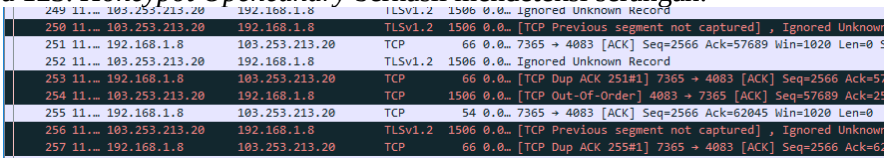
Gambar 16 Menebak *Username* Dan *Password* Putty

Berdasarkan pada gambar 16, ketika penyerangan melakukan koneksi maka sistem keamanan *honeypot* akan mendeteksi adanya percobaan serangan dalam SSH VPS. Berikut adalah *log* serangan pada *Secure Shell* (SSH) seperti pada Gambar 17.



Gambar 17 *Log* Serangan Pada *Secure Shell* (SSH)-1

Berdasarkan pada gambar log serangan *Secure Shell* (SSH) diketahui serangan berasal dari IP 175.158.36.16 dengan tujuan IP 202.10.40.219 pada Tanggal 22/01/2024 dan jam 23:09:41, port=22, *browser crome* serta sistem operasi *windows*. *Username* yang diinputkan adalah testing sedangkan *password*nya 123. *Honeypot Opencanary* berhasil mendeteksi serangan.



Gambar 18 Tangkapan *Wireshark* Serangan SSH

Berdasarkan dari 2 contoh serangan, untuk serangan selanjutnya dilakukan dengan cara yang sama.

3.2 Hasil Laporan Hasil Serangan DDoS

Berikut adalagh laporan hasil serangan DDoS pada VPS dengan keamanan *honetpot opencanary* seperti pada Tabel 2.

Tabel 2 Laporan Hasil Penyerangan DDoS

No	Tanggal dan Waktu	IP Penyerang	IP Tujuan	Jenis Serangan	Keterangan
1	23/01/2024 08:31:27	175.158.36.16	202.10.40.219	*DDoS*	*Terdeteksi/Kill IP*
2	23/01/2024 08:33:17	175.158.36.16	202.10.40.219	*DDoS*	*Terdeteksi/Kill IP*
3	23/01/2024 08:37:43	175.158.36.16	202.10.40.219	*DDoS*	*Terdeteksi/Kill IP*
4	23/01/2024 08:43:15	175.158.36.16	202.10.40.219	*DDoS*	*Terdeteksi/Kill IP*
5	23/01/2024 08:49:23	175.158.36.16	202.10.40.219	*DDoS*	*Terdeteksi/Kill IP*

Berdasarkan laporan penyerangan, diketahui bahwa *honeypot opencanary* mampu mendeteksi dan menangkis serangan DDoS sehingga keamanan VPS lebih terjaga.

3.3 Hasil Laporan Hasil Serangan Brute Force

Berikut adalagh laporan hasil serangan *brute force* Web Server, FTP dan SSH pada VPS dengan keamanan *honetpot opencanary* seperti pada Tabel 3.

Tabel 3 Laporan Hasil Penyerangan *Brute Force*

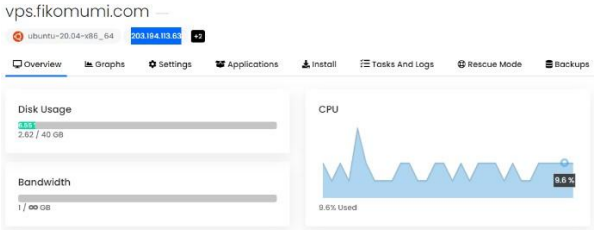
No	Tanggal dan Waktu	IP Penyerang	IP Tujuan	Jenis Serangan	Keterangan
1	22/01/2024 22:23:27	175.158.36.16	202.10.40.219	*Brute Force Web Server*	*Terdeteksi/Kill IP*
2	22/01/2024 22:24:64	175.158.36.16	202.10.40.219	*Brute Force Web Server*	*Terdeteksi/Kill IP*
3	22/01/2024 22:35:41	175.158.36.16	202.10.40.219	*Brute Force Web Server*	*Terdeteksi/Kill IP*
4	22/01/2024 22:36:11	175.158.36.16	202.10.40.219	*Brute Force Web Server*	*Terdeteksi/Kill IP*
5	22/01/2024 22:37:57	175.158.36.16	202.10.40.219	*Brute Force Web Server*	*Terdeteksi/Kill IP*

No	Tanggal dan Waktu	IP Penyerang	IP Tujuan	Jenis Serangan	Keterangan
6	22/01/2024 22:40:59	175.158.36.16	202.10.40.219	*Brute Force FTP*	*Terdeteksi/Kill IP*
7	22/01/2024 22:45:13	175.158.36.16	202.10.40.219	*Brute Force FTP*	*Terdeteksi/Kill IP*
8	22/01/2024 22:47:11	175.158.36.16	202.10.40.219	*Brute Force FTP*	*Terdeteksi/Kill IP*
9	22/01/2024 22:48:12	175.158.36.16	202.10.40.219	*Brute Force FTP*	*Terdeteksi/Kill IP*
10	22/01/2024 23:08:37	175.158.36.16	202.10.40.219	*Brute Force FTP*	*Terdeteksi/Kill IP*
11	22/01/2024 23:09:41	175.158.36.16	202.10.40.219	SSH Brute Force	*Terdeteksi/Kill IP*
12	22/01/2024 23:12:44	175.158.36.16	202.10.40.219	SSH Brute Force	*Terdeteksi/Kill IP*
13	22/01/2024 23:16:57	175.158.36.16	202.10.40.219	SSH Brute Force	*Terdeteksi/Kill IP*
14	22/01/2024 23:23:23	175.158.36.16	202.10.40.219	SSH Brute Force	*Terdeteksi/Kill IP*
15	22/01/2024 23:35:45	175.158.36.16	202.10.40.219	SSH Brute Force	*Terdeteksi/Kill IP*

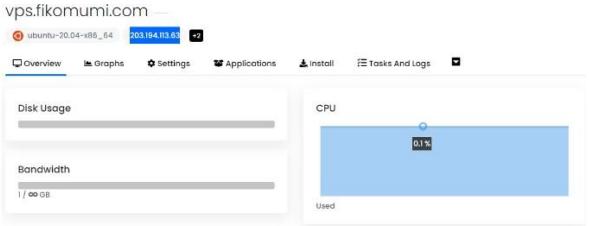
Berdasarkan laporan penyerangan, diketahui bahwa *honeypot opencanary* mampu mendeteksi dan menangkis serangan *brute force* web server, FTP dan SSH sehingga keamanan VPS lebih terjaga.

3.4 Kondisi CPU VPS Sebelum dan Sesudah Serangan

1. Kondisi CPU Pada Serangan DDoS
   Berikut adalah kondisi CPU VPS ketika terjadi serangan DDoS seperti pada Gambar 19



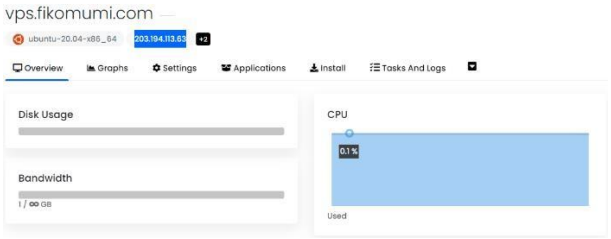
   Berdasarkan pada gambar 19, kondisi CPU VPS ketika Serangan DDoS adalah 9.6% pemakaian, peningkatan CPU sangat cukup signifikan, hal ini disebabkan *honeypot* bekerja ekstra untuk mendeteksis serangan DDoS dari server virtual.
2. Kondisi CPU Pada Serangan *Brute Force* Web Server
   Berikut adalah kondisi CPU VPS ketika terjadi serangan *brute force* web server seperti pada Gambar 20.



Gambar 20 CPU VPS Pada Serangan *Brute Force* Web Server

Berdasarkan pada gambar 20, kondisi CPU VPS ketika Serangan *Brute Force* Web Server adalah 0.1% pemakaian, peningkatan CPU sangat tidak signifikan, hal ini disebabkan *honeypot* bekerja dengan meniru server asli.

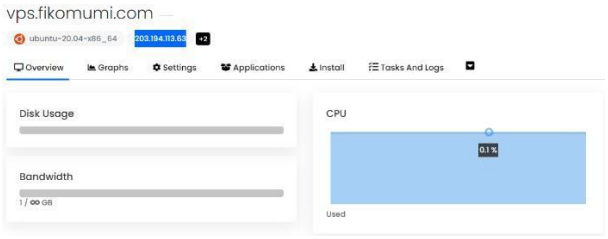
3. Kondisi CPU Pada Serangan *Brute Force* FTP
   Berikut adalah kondisi CPU VPS ketika terjadi serangan *Brute Force* FTP seperti pada Gambar 21.



Gambar 21 CPU VPS Pada Serangan *Brute Force* FTP

Berdasarkan pada gambar 21, kondisi CPU VPS ketika Serangan *Brute Force* FTP adalah 0.1% pemakaian, peningkatan CPU sangat tidak signifikan, hal ini disebabkan *honeypot* bekerja dengan meniru server asli.

4. Kondisi CPU Pada Serangan *Brute Force* SSH
   Berikut adalah kondisi CPU VPS ketika terjadi serangan *Brute Force* SSH seperti pada Gambar 22.



Gambar 22 CPU VPS Pada Serangan *Brute Force* SSH

Berdasarkan pada gambar 22, kondisi CPU VPS ketika *Brute Force* SSH adalah 0.1% pemakaian, peningkatan CPU sangat tidak signifikan, hal ini disebabkan *honeypot* bekerja dengan meniru server asli.

4. KESIMPULAN

Honeypot bekerja dengan mengvisualisikan server asli kedalam bentuk palsu dengan cara memasang *web server login* yang palsu, sehingga penyerang terkelabui dan teperangkap. Penyerangan dengan DDoS dan *brute force* tidak mengenai server VPS sebenarnya.Penerapan IPS *honeypot Opencanary* di IDS mampu bekerja efektif memberikan pemberi peringatan secara *realtime* adanya kegiatan penyerangan terhadap *sever* VPS hal ini dibuktikan dengan berhasilnya melakukan *Kill* IP setiap penyerangan. Dampaknya keamanan VPS lebih baik serta kondisi awal CPU 0.1% dan setelah penyerangan kondisi CPU tetap berapa pada 0.1% pemakaian. Honeypot opencanary mampu mendeteksi dan memanipulasi serangan ddos dan brute force pada web server dengan mengalihkan ke server palsu melalui port 80,22,21 sehingga server vps lebih terjamin keamanannya dari user yang tidak memiliki Otoritas.

REFERENSI

[1] A. D. Djayali, Muhammad Muzammil, and Abjan Samad, “Implementasi Aplikasi Meeting Online Pada Virtual Private Server di Masa Pandemi,” *Simkom*, vol. 6, no. 1, pp. 23–33, 2021, doi: 10.51717/simkom.v6i1.52.

[2] R. Dwi Yulian Prakoso, “Implementasi Low Interaction Honeypot Dan Port Knocking Untuk Meningkatkan Keamanan Jaringan,” *Perwira J. Sci. Eng.*, vol. 2, no. 1, pp. 16–23, 2022, doi: 10.54199/pjse.v2i1.96.

[3] P. Dewa Made Julijati, “Analisis Perbandingan Serangan Hydra, Medusa Dan Ncrack Pada

Password Attack," vol. 4, no. 4, pp. 461–466, 2022.
[4] A. Muhaimi, I. P. Hariyadi, and A. Juliansyah, "Analisa Penerapan Intrusion Prevention System (IPS) Berbasis Snort Sebagai Pengaman Server Internet Yang Terintegrasi Dengan Telegram," *J. Bumigora Inf. Technol.*, vol. 1, no. 2, pp. 167–176, 2019, doi: 10.30812/bite.v1i2.611.
[5] D. T. Yuwono, "Analysis Performance Intrusion Detection System in Detecting Cyber-Attack on Apache Web Server," *IT J. Res. Dev.*, vol. 6, no. 2, pp. 169–178, 2022, doi: 10.25299/itjrd.2022.7853.
[6] G. Tambunan, K. Kuningan, K. Setiabudi, and K. Jakarta, "Implementasi Keamanan Ids / Ips Dengan Snort Dan," *Semin. Nas. Mhs. Ilmu Komput. dan Apl. Jakarta-Indonesia, 28 Januari 2020 IMPLEMENTASI*, pp. 10–16, 2020.
[7] J. Sidabutar, "Analisis Keamanan Server Menggunakan IDS dan Router Firewall Server Dari Serangan DDOS," *J. Inform. Pengemb. IT*, vol. 1, no. 2, 2020.
[8] B. Wijaya and A. Pratama, "Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (Ids) Berbasis Snort," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 9, no. 1, pp. 97–101, 2020, doi: 10.32736/sisfokom.v9i1.770.
[9] A. Hidayat and D. Prabowo, "Implementation of Virtual Private Server (VPS) Using Digital Ocean Cloud Server on BMT. Mentari East Lampung," *Jtksi*, vol. 03, no. 03, pp. 116–121, 2020.
[10] W. A. Sulaksono and C. E. Suharyanto, "Implementasi Honeypot Sebagai Sistem Keamanan Jaringan Pada Virtual Private Server," *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 5, no. 1, pp. 90–95, 2020.
[11] T. Natanegara, Y. Muhyidin, and D. Singasatia, "Implementasi Honeypot Cowrie Dan Snort Sebagai Alat Deteksi Serangan Pada Server," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 7, no. 3, pp. 1871–1877, 2023, doi: 10.36040/jati.v7i3.6989.
[12] P. Kumari and A. K. Jain, "A comprehensive study of DDoS attacks over IoT network and their countermeasures," *Comput. Secur.*, vol. 127, 2023, doi: 10.1016/j.cose.2023.103096.