Implementasi *Intrusion Prevention System* (IPS) OSSEC dan Honeypot Cowrie

Risa Eri Susanti[1], Arif Wirawan Muhammad[2], Wahyu Adi Prabowo[3]*
Fakultas Informatika, Program Studi Teknik Informatika [1][2][3]
Institut Teknologi Telkom Purwokerto
Purwokerto, Jawa Tengah, Indonesia
16102066@ittelkom-pwt.ac.id[1], arif@ittelkom-pwt.ac.id[2], wahyuadi@ittelkom-pwt.ac.id [3]*

***Abstract*—The development of increasingly sophisticated technology is widely used as a crime, such as data theft, data falsification to damage systems and networks. With these problems, a layered security system is needed to maintain the integrity of the data and the system so that it remains intact. The OSSEC security system which is integrated with the cowrie honeypot aims to slow down attacks, where these systems work together to provide logs to take action against attackers. OSSEC works like a firewall that can allow or block. Meanwhile, this cowrie honeypot works like a real server to trap attackers as if they succeeded in carrying out an attack. In this study, the system that has been designed can handle attacks such as SSH brute force, Man in The Middle (MITM) attack, and Distributed Denial of Service (DDoS). From network security using IPS OSSEC and Honeypot Cowrie can handle existing attacks well. Based on the log, the detection accuracy can reach 100% percentage.**

***Keywords—Intrusion Prevention System* (IPS), *Open Source Security* (OSSEC), Honeypot Cowri**

***Abstrak*—Perkembangan teknologi yang semakin canggih ini banyak digunakan sebagai tindak kejahatan, seperti pencurian data, pemalsuan data hingga merusak sistem maupun jaringan. Dengan adanya permasalahan tersebut, dibutuhkan sistem pengamanan berlapis untuk menjaga integritas data maupun sistem agar tetap utuh. Pengamanan sistem OSSEC yang diintegrasikan dengan honeypot cowrie ini bertujuan untuk menekan waktu penyerangan, dimana pada sistem ini saling bekerja sama untuk memberikan log untuk melakukan tindakan terhadap penyerang. OSSEC bekerja layaknya firewall yang dapat melakukan *allow* maupun *block*. Sedangkan honeypot cowrie ini bekerja layaknya server asli untuk menjebak penyerang seolah-olah berhasil melakukan penyerangan. Dalam penelitian ini, sistem yang telah dirancang agar dapat menangani adanya serangan seperti Port Scanning, SSH *brute force, Man in The Middle* (MITM) *attack*, dan *Distributed Denial of Service* (DDoS). Dari hasil perbandingan serangan dengan confusion matrix ini OSSEC yang diintegrasikan dengan honeypot cowrie memiliki tingkat akurasi yang besar terhadap serangan DDoS, Berdasarkan log, akurasi deteksi dapat mencapai persentase 100%.**

***Kata Kunci—Intrusion Prevention System* (IPS), *Open Source Security* (OSSEC), Honeypot Cowri**

I. PENDAHULUAN

Pada perkembangan internet saat ini, keamanan jaringan merupakan suatu hal yang sangat penting untuk menjaga validitas dan integritas data [1], namun ada beberapa orang yang memanfaatkan keamanan jaringan untuk hal negatif, seperti halnya tindakan serangan siber [2], [3]. Ancaman keamanan informasi oleh serangan siber, disebabkan karena kondisi keamanan jaringan tersebut rentan dari serangan internet[4]. Pelaku penyerangan memanfaatkan kelemahan dari suatu sistem untuk kepentingan pribadi dan merugikan pihak lain seperti serangan *port scanning*, SSH, *brute force*, *Man In The Middle* (MITM) Attack, dan *Distributed Denial of Service* (DDoS) [5] . Hal ini diperlukan agar sistem memiliki keamanan jaringan yang dapat mendeteksi, mencegah dan mencatat dari aktivitas serangan *port scanning*, SSH *brute force*, MiTM dan DDoS (ICMP *flood*, TCP *flood* dan UDP *flood*) [6]. Keamanan secara berlapis dapat membantu keamanan jaringan dengan mengintegrasikan *Intrusion Prevention System* (IPS) dan Honeypot. Pemanfaatan dari metode IPS ini digunakan untuk mendeteksi, mengidentifikasi, menganalisis dan mencegah ancaman yang masuk ke dalam sistem [7]. Metode ini bertindak seperti layaknya firewall yang akan melakukan *allow* dan *block* [8]. IPS memiliki beberapa jenis namun yang digunakan yaitu *Network- based Intrusion Prevention System* (NIPS) [9]. NIPS bekerja secara *inline* dengan perlindungan *proaktif* yang berarti melakukan *sniffing* untuk menahan semua trafik jaringan pada *in-line* model dan menganalisis aktivitas dan kode yang mencurigakan [9]. Banyak aplikasi yang digunakan untuk melakukan pencegahan dengan metode NIPS, salah satunya adalah *Open Source Security* (OSSEC) [10]. OSSEC ini berguna untuk memberikan *alert* secara *real-time* kepada *router* terhadap penyusup yang melakukan serangan [11], selain itu teknik yang dilakukan dalam mendeteksi adanya serangan dengan menggunakan *signature-based* [12], dimana dalam mendeteksi serangan melalui pola atau paket data yang terdeteksi kemudian dibandingkan dengan data atau paket yang sudah tersimpan dalam *database rule* yang telah ada[13].

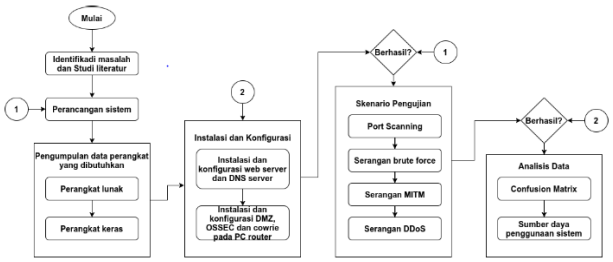
Dalam melakukan pemantauan aktivitas serangan, Honeypot juga merupakan salah satu solusi untuk mengetahui bagaimana seorang penyerang beraksi untuk mendapatkan informasi [14]. Honeypot merupakan alat yang dapat menipu penyerang

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i1.1246, Copyright ©2020
Submitted : August 31, 2021; Revised : March 31, 2022; Accepted : April 1, 2022; Published : April 5, 2022

dengan membuat sistem yang sama persis dari sistem aslinya, sehingga ketika penyerang melakukan penetrasi maka dirinya menganggap telah berhasil masuk ke dalam sistem aslinya, padahal kenyataannya penyerang telah diarahkan masuk ke dalam server virtual [14]. Terdapat beberapa aplikasi Honeypot yang tersedia secara *open source* namun yang akan digunakan adalah Honeypot Cowrie. Honeypot Cowrie termasuk dalam jenis *medium interaction*, dimana Honeypot Cowrie mampu menganalisis dan mencatat aktivitas yang dilakukan oleh penyerang dalam jaringan menggunakan layanan *Secure Shell* (SSH) [15], [16], dengan adanya permasalahan tersebut, maka dilakukan penelitian keamanan secara berlapis menggunakan OSSEC dan honeypot cowrie.

II. METODOLOGI PENELITIAN

Diagram alur penelitian dilakuka secara sistematis dengan beberapa tahapan yang dijelaskan pada gambar 1.

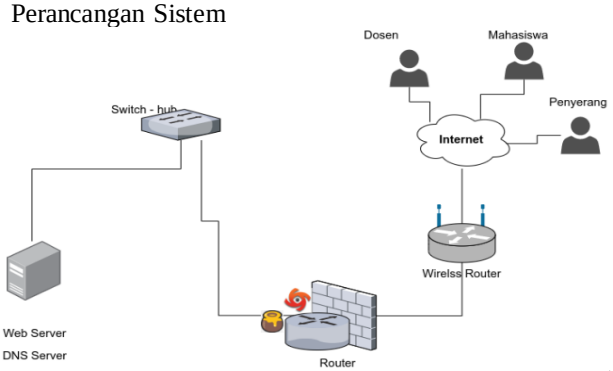


Gambar 1. Diagram Alur Penelitian

A. Studi literatur

Peneliti mengidentifikasi permasalahan dengan mengumpulkan referensi yang dibutuhkan sebagai dasar dalam tahapan penelitian, dan referensi yang digunakan oleh peneliti menggunakan jurnal terdahulu yang masih berhubungan dengan penelitian ini sebagai acuan. Selain menggunakan jurnal terdahulu peneliti juga menggunakan buku elektronik untuk memperluas pengetahuan dalam metode yang digunakan.

B. Perancangan Sistem



Gambar 2. Perancangan Sistem

Pada Gambar 2. perancangan simulasi sistem dilakukan untuk menentukan alamat *Internet Protocol* serta untuk menentukan perangkat yang dibutuhkan, seperti perangkat lunak dan perangkat keras.

C. Analisis Kebutuhan Sistem

1. Kebutuhan Perangkat Lunak

a) PC Router

PC Router menggunakan sistem operasi ubuntu *desktop* yang diuji untuk melakukan pengamanan, administrasi jaringan dan membuat log serangan secara *realtime* dengan menggunakan *tools* yang terpasang yaitu DMZ, OSSEC dan Cowrie.

b) Server

Server ini terdapat dua service yaitu DNS server serta web server, dimana layanan DNS melakukan instalasi bind9 serta web server melakukan instlasi apache2, Mysql, Php dan PhpMyadmin. Keduanya dirancang menggunakan sistem operasi ubuntu live server versi 20.04.

c) Penyerang

Pada saat melakukan penetrasi, penyerang menggunakan sistem operasi Kali Linux. Terdapat beberapa *tools* yang digunakan oleh penyerang dalam melakukan penetrasi diantaranya *tool* hydra untuk serangan *brute force*, SetToolkit untuk serangan *Man in The Middle* (MiTM) *Atack* dan *Low Orbit Ion Cannon* (LOIC) untuk serangan *Distributed Denial of Service* (DDoS).

d) *Client* (*user*)

Pada penelitian ini *user* menggunakan operasi sistem Ubuntu desktop. Pengguna ini adalah dosen dan mahasiswa, dimana keduanya bukan termasuk penyerang yang akan melakukan serangan. Adanya pengguna pada penelitian ini untuk membuktikan bahwa terdapat perbedaan antara penyerang dengan penguna ketika mengakses sebuah *web server*.

2. Kebutuhan Perangkat Keras

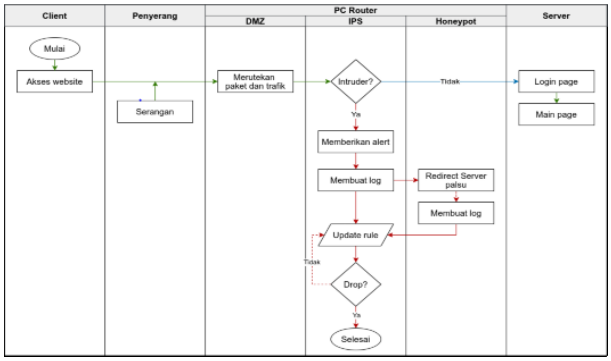
Pada tabel 1 beberapa perangkat keras yang dibutuhkan dalam implementasi OSSSEC dan Honeypot Cowrie.

Tabel 1.Kebutuhan Perangkat Keras

No	Perangkat	Unit	Deskripsi
1	Laptop	2	Satu laptop sebagai PC router, server dan pengguna. Sedangkan laptop kedua sebagai penyerang
2	Switch-hub	1	Media penghubung Router, Wireless Router, Switch untuk dilakukan *broadcast* paket
3	Wireless Router	1	Penyedia internet dari ISP dan penyedia NAT ke *local computer*
4	USB Wireless Adapter	2	Media penerima sinyal *hotspot* dan penguat sinyal, serta pengakses jaringan eksternal pada VM

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i1.1246, Copyright ©2020
Submitted : August 31, 2021; Revised : March 31, 2022; Accepted : April 1, 2022; Published : April 5, 2022

D. Skenario Pengujian Sistem



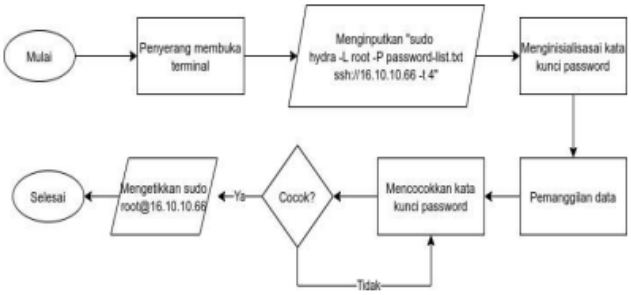
Gambar 3.Skenario Pengujian Sistem

Berdasarkan *activity* diagram pada gambar 3 dapat dijelaskan, bahwa antara pengguna dan penyerang memiliki skenario alur yang berbeda. Dimana saat pengguna dan penyerang akan melakukan akses *server*, keduanya melewati DMZ yang tugasnya merutekan paket dan trafik yang lewat. Setelah itu IPS bertugas melakukan allow maupun *block* terhadap paket dan trafik yang tidak sesuai dengan signature Based. Berikutnya melakukan predecoding dengan membaca *field* yang berisi kode-kode paket dan trafik yang lewat supaya dapat melakukan pembuatan decoder maupun rules. IPS ini membuat akses kontrol dengan melihat konten, layanan, *port*, IP address dan lainnya. Selanjutnya proses data yang telah terkumpul akan disesuaikan dengan metode signature Based atau berdasarkan rules yang telah dibuat. Apabila ada kecocokan data serangan dengan rules, maka IPS akan menghasilkan file log. Namun, jika tidak terjadi adanya serangan, maka paket dan trafik diarahkan ke arah login page hamsakuy.com pada server yang menjadi target penyerangan. File *log* yang dihasilkan akan diparsing untuk memantau adanya serangan. Serangan yang masih berkelanjutan akan diarahkan ke honeypot untuk mendapatkan log yang relevan dengan IPS. Sehingga IPS dapat melakukan update rules untuk melakukan drop paket yang dilakukan penyerang baik melalui IP address, port, maupun user.

E. Pengujian Penyerangan

Pada pengujian penyerangan ini sistem akan diuji dengan berbagai serangan. Serangan yang dilakukan yakni SSH *brute force*, *Man In The Middle* (MITM) *Attack* dan *Distributed Denial of Service* (DDoS).

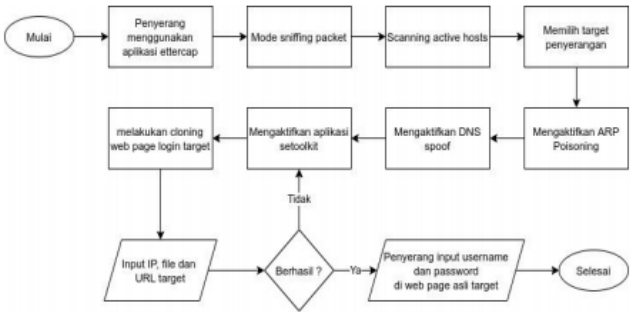
1. Skenario serangan SSH *brute force*



Gambar 4. Diagram Alur Serangan SSH *Brute Force*

Pada penyerangan SSH *brute force* ini penyerang berusaha untuk mendapatkan *username* dan *password* yang dimiliki server menggunakan aplikasi Hydra, dimana aplikasi ini berbasis *command prompt*. Penyerang berusaha menebak *password* dengan menginputkan perintah sesuai dengan gambar 4. Setelah perintah diinputkan maka aplikasi Hydra akan menginisiasi kata kunci *password* yang kemudian dilakukan pemanggilan data. Hydra akan mencocokkan kata kunci *password*, jika terdapat kecocokan pada *password-list*.txt maka penyerang akan melakukan serangan ssh *brute force* terhadap server menggunakan mode *root*. Namun, apabila kata kunci password tidak mengalami kecocokan, maka akan mencocokkan kata kunci password kembali

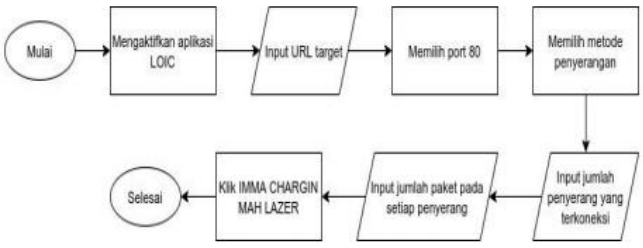
2. Skenario serangan *Man In The Middle* (MITM) *attack*



Gambar 5. Diagram Alur Serangan MiTM

Pada Gambar 5 penyerangan MITM ini terdapat beberapa tahapan penyerang dalam melakukan serangan. Tahap awal dari serangan ini dengan menggunakan aplikasi Ettercap yang digunakan untuk melakukan *sniffing packet*. Selanjutnya melakukan *scanning* pada *host* yang aktif dengan dilanjutkan memilih target penyerangan dan mengaktifkan ARP *poisoning* serta DNS *spoof*. Setelah selesai dilakukan, maka selanjutnya mengaktifkan aplikasi setToolkit dan melakukan duplikasi web *page login*, selanjutnya penyerang menginputkan IP, *file* dan URL target. Jika penyerangan yang dilakukan berhasil, maka penyerang menginputkan *username* dan *password* pada *webpage* asli target.

3. Skenario serangan *Distributed Denial of Services* (DDoS)



Gambar 6. Diagram alur serangan DDoS

Berdasarkan Gambar 6 penyerangan DDoS ini dilakukan dengan menggunakan aplikasi LOIC. Penggunaannya pun terdapat beberapa tahapan, dimana tahap pertama ini penyerang

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i1.1246, Copyright ©2020
Submitted : August 31, 2021; Revised : March 31, 2022; Accepted : April 1, 2022; Published : April 5, 2022

akan mengaktifkan aplikasi LOIC. Penyerang akan menginputkan URL *website* dengan IP 16.10.10.66 sebagai target penyerangan. Selanjutnya akan memilih *port* 80 serta memilih metode penyerangan. Selanjutnya akan memilih 3 metode yakni TCP, ICMP dan UDP. Dari metode tersebut digunakan untuk melakukan penyerangan TCP SYN *flood*, ICMP *flood*, dan UDP *flood*. Berikutnya penyerang menentukan banyaknya user pada kolom *threads* serta menentukan banyaknya *threads* pada setiap user. Tahapan yang terakhir yaitu memulai serangan DDoS.

III. HASIL DAN PEMBAHASAN

Pada tahap ini melakukan uji coba serangan, dengan melakukan parsing log OSSEC yang dikonfigurasi secara NIPS. Pada tahap ini penyerang melakukan pengujian serangan *port scanning*, SSH *brute force*, MiTM dan DDoS yang dilakukan pada waku yang berveda dengan menggunakan beberapa *tools* atau aplikasi yang disebutkan secara berurutan yaitu Nmap, hydra, Ettercap, setoolkit dan LOIC. Sebelum melakukan deteksi serangan, terdapat beberapa proses yang dilakukan agar OSSEC dapat menampilkan *alert* terhadap serangan. Tahap pertama, pada tabel 2 dengan melakukan *predecoding* dengan menentukan *date/time*, *hostname*, *program_name* serta *log* yang dihasilkan sebelum di *parsing* oleh OSSEC. Pada tabel 3 untuk tahap berikutnya adalah dengan membuat *decoder* untuk melakukan pemanggilan kode yang sesuai dengan *tag order*. Kemudian melakukan pencocokan dengan *rule* yang telah dibuat.

Tabel 2. *predecoding*

Field	Description
date/time	Aug 10 04:25:03
hostname	-
program_name	TCP
log	Detected to hamsakuy.com (16.10.10.66) [port 53] from 192.168.36.32

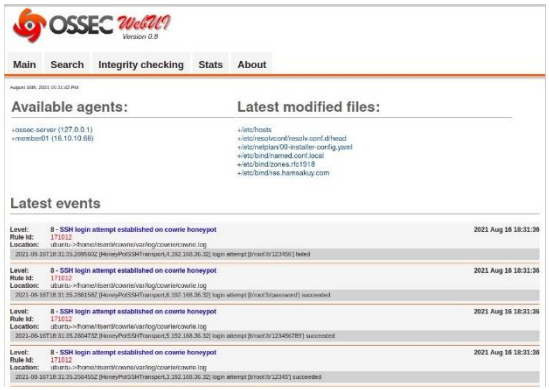
Tabel 3. *Decoding*

Field	Description
url	hamsakuy.com
dstip	16.10.10.66
srcip	192.168.36.32

Pada gambar 7, hasil implementasi didapatkan serangan port scanning dapat di deteksi dengan baik. Simulasi pertahanan sistem menggunakan OSSEC dapat mendeteksi adanya port scanning. Berdasarkan alert tersebut, sistem dapat mendeteksi serangan yang menggunakan protokol TCP. Selain itu alamat IP penyerang dapat terdeteksi pada log, sehingga sistem dapat mengenali pola atau kode yang akan di drop sebagai contoh kode source IP. Berikut merupakan perintah untuk mengktifkan mode drop dari active response

Gambar 7. Deteksi Serangan *Port Scanning*

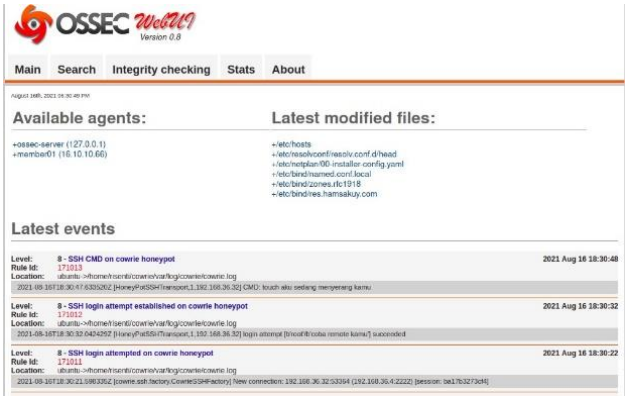
Pada gambar 8 merupakan pendeteksian ketika penyerang menggunakan *tool* hydra dalam melakukan penyerangan. Dapat dilihat bahwa honeypot cowrie dapat merekam jejak penyerang. Penyerang yang masuk ke dalam server akan langsung dikenali oleh OSSEC karena antara OSSEC dan honeypot Cowrie saling terintegras. Aplikasi OSSEC ini sudah mendukung pengamanan yang bersifat *third party*, dimana OSSEC dapat diintegrasikan dengan aplikasi lain untuk melakukan monitoring jaringan. Sehingga paket maupun trafik jaringan yang menuju ke server dapat terlindungi. Berdasarkan *alert* tersebut, sistem dapat mendeteksi serangan yang menggunakan *source port* 22.



Gambar 8. Deteksi Serangan *Brute Force*

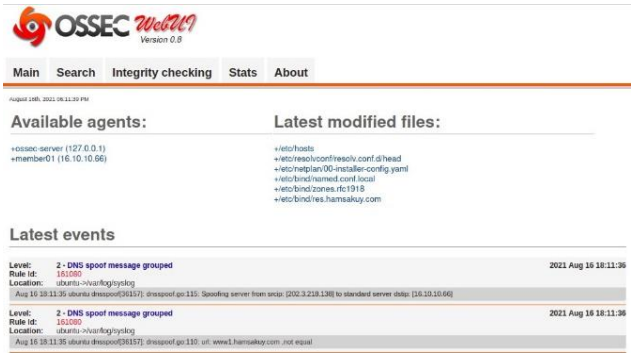
Pada gambar 9 OSSEC dapat mendeteksi adanya serangan ARP poisoning pada saat penyerang mencoba masuk maupun merubah *station*, dimana *station* ini berfungsi untuk menghubungkan perangkat satu dengan yang lainnya dalam satu jaringan LAN yang biasa disebut dengan alamat MAC. Selain menggunakan tool Ettercap, penyerang menggunakan setoolkit. Setoolkit ini berfungsi untuk melakukan duplikasi *web page login* dengan menyerupai aslinya. OSSEC dapat memberikan *alert* pada serangan ARP *poisoning* dengan memunculkan *alert* bahwa telah terjadi serangan. OSSEC dapat mengetahui adanya serangan dengan mengubah alamat MAC pada *gateway* dan server.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i1.1246, Copyright ©2020
Submitted : August 31, 2021; Revised : March 31, 2022; Accepted : April 1, 2022; Published : April 5, 2022



Gambar 9. Deteksi Serangan ARP *Poisoning*

Pada gambar 10 *Alert* yang dihasilkan menunjukan bahwa terdapat serangan DNS *spoof*, namun serangan ini hanya dapat memberikan *alert* dan tidak dapat melakukakn *allow* ataupun *block*. Hal ini karena serangan DNS *spoof* tidak memiliki sumber data yang spesifik. Hal ini dikarenakan pada saat penyerang mengalihkan website hamsakuy.com menuju website penyerang, server mengalami *down* dengan menampilkan alamat IP 202.3.218.138 dan kemudian dapat di akses kembali. Namun, setelah diakses kembali *website* berubah menjadi milik penyerang



Gambar 10. Deteksi Serangan DNS Spoof

OSSEC dapat mendeteksi adanya ICMP *flood*, UDP *flood* dan TCP *flood* dengan memberikan *alert* dengan pesan PING *flood detected*. Pada saat terjadi adanya serangan, OSSEC dapat melakukan deteksi adanya serangan dengan memberikan *alert* serta memberikan source IP dan *Alert* penyerang sehingga dapat dilakukan *block* maupun *drop* penyerang menggunakan *active response*. Hasil pertahanan dari semua serangan dengan menggunakan pengamanan OSSEC dan Honeypot Cowrie dapat dilihat pada tabel 4.

Tabel 4. Hasil Deteksi Serangan

Tipe Serangan	Alert	Log	Active Response
Port Scanning	Terdeteksi	Terdeteksi	Berhasil
SSH brute force	Terdeteksi	Terdeteksi	Berhasil
ARP Poisoning	Terdeteksi	Terdeteksi	Berhasil
DNS Spoofing	Terdeteksi	Terdeteksi	Gagal
ICMP flood	Terdeteksi	Terdeteksi	Berhasil
TCP flood	Terdeteksi	Terdeteksi	Berhasil
UDP flood	Terdeteksi	Terdeteksi	Gagal

IV. KESIMPULAN

OSSEC dapat dijadikan IPS dikarenakan adanya *active response* untuk melakukan dan *block* penyerang berdasarkan IP address. OSSEC ini tidak dapat mencegah adanya serangan DNS *Spoof* dan DDoS UDP *flood* dikarenakan protokol UDP akan menghasilkan IP public baik yang masuk dan keluar jaringan PC Router dan PC *server* yang mengakibatkan sulitnya memperkirakan IP publik milik penyerang. Pengamanan jaringan dengan menggunakan OSSEC memiliki kekurangan, yaitu *delay* dalam *parsing* log pada *third party*. Namun, dalam hal ini pengamanan OSSEC yang diintegrasikan dengan honeypot cowrie lebih unggul dalam serangan SSH *brute force* yang telah dilakukan.

DAFTAR PUSTAKA

[1] M. Warkentin and C. Orgeron, “Using the security triad to assess blockchain technology in public sector applications,” *International Journal of Information Management*, vol. 52, 2020, doi: 10.1016/j.ijinfomgt.2020.102090.

[2] N. Ahmad and M. Habib, “Analysis of Network Security Threats and Vulnerabilities: by Development & Implementation of a Security Network Monitoring Solution,” *Researchgate*, no. January 2010, p. 93, 2010.

[3] M. Zuzčák and M. Zenka, “Expert system assessing threat level of attacks on a hybrid SSH honeynet,” *Computers and Security*, vol. 92, p. 101784, 2020, doi: 10.1016/j.cose.2020.101784.

[4] D. P. Sharma *et al.*, “Dynamic Security Metrics for Software-Defined Network-based Moving Target Defense,” *Journal of Network and Computer Applications*, vol. 170, no. April, p. 102805, 2020, doi: 10.1016/j.jnca.2020.102805.

[5] H. Wang *et al.*, “DDoS Attack in Software Defined Networks: A Survey,” *Neural Regeneration Research*, vol. 7, no. 14, 2017.

[6] T. Ray, “DDoS defence: new tactics for a rising shadow industry,” *Network Security*, vol. 2020, no. 4, pp. 6–7, 2020, doi: 10.1016/S1353-4858(20)30041-6.

[7] C. Cai, S. Mei, and W. Zhong, “Configuration of intrusion prevention systems based on a legal user: the case for using intrusion prevention systems instead of

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i1.1246, Copyright ©2020
Submitted : August 31, 2021; Revised : March 31, 2022; Accepted : April 1, 2022; Published : April 5, 2022

intrusion detection systems," *Information Technology and Management*, vol. 20, no. 2, pp. 55–71, 2019, doi: 10.1007/s10799-018-0291-6.

[8] Y. Arta, A. Syukur, and R. Kharisma, "Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik," *IT JOURNAL RESEARCH AND DEVELOPMENT*, vol. 3, no. 1, pp. 104–114, 2018, doi: 10.25299/itjrd.2018.vol3(1).1346.

[9] A. Guezzaz, A. Asimi, and Y. Asimi, "A hybrid NIPS based on pcapsocks sniffer and neural MLP," in *Advances in Intelligent Systems and Computing*, 2018, vol. 640, pp. 253–266. doi: 10.1007/978-3-319-64719-7_22.

[10] "Instant OSSEC Host-based Intrusion Detection," *Network Security*, vol. 2013, no. 9, p. 4, 2013, doi: 10.1016/s1353-4858(13)70099-0.

[11] C. Gayathri Harshitha, M. Kameswara Rao, and P. Neelesh Kumar, "A novel mechanism for host-based intrusion detection system," in *Advances in Intelligent Systems and Computing*, 2020, vol. 1045, pp. 527–536. doi: 10.1007/978-981-15-0029-9_42.

[12] M. A. Jabbar and R. Aluvalu, "A Signature-based Intrusion Detection System for the Internet of Things," in *Smart Cities Symposium 2018*, 2018, vol. 2018, no. CP747, pp. 51 (6 pp.)-51 (6 pp.).

[13] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks," *Electronics (Switzerland)*, vol. 8, no. 11, 2019, doi: 10.3390/electronics8111210.

[14] M. Baykara and R. Das, "A novel honeypot based security approach for real-time intrusion detection and prevention systems," *Journal of Information Security and Applications*, vol. 41, pp. 103–116, 2018, doi: 10.1016/j.jisa.2018.06.004.

[15] D. A. P. Putri and A. Rachmawati, "Honeypot cowrie implementation to protect ssh protocol in ubuntu server with visualisation using kippo-graph," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 6, pp. 3200–3207, 2019, doi: 10.30534/ijatcse/2019/86862019.

[16] I. Barak, "Critical infrastructure under attack: lessons from a honeypot," *Network Security*, vol. 2020, no. 9, pp. 16–17, 2020, doi: 10.1016/S1353-4858(20)30106-9.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i1.1246, Copyright ©2020
Submitted : August 31, 2021; Revised : March 31, 2022; Accepted : April 1, 2022; Published : April 5, 2022