CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 4, No. 1, Mei 2021, hlm. 33-37

PERANCANGAN INTRUSION DETECTION SYSTEM MENGGUNAKAN HONEYPOT PADA UNIVERSITAS BHAYANGKARA JAKARTA RAYA

Allan D Alexander[1], Ratna Salkiawati[2], Joni Warta[3]

[1, 2] Program Studi Informatika, Fakultas Ilmu Komputer, Univesitas Bhayangkara Jakarta Raya
Email: [1]allan@ubharajaya.ac.id , [2]ratna_tind@dsn.ubharajaya.ac.id,[3]joniwarta@dsn.ubharajaya.ac.id

(Naskah masuk: 12 Maret 2021, diterima untuk diterbitkan: 31 Mei 2021)

Abstrak

Internet sudah menjadi bagian vital dari sebuah institusi yang membawa keuntungan yang besar bagi penggunanya tetapi di sisi lain ada segelintir pengguna yang melakukan kegiatan yang mengambil keuntungan dari sistem lain dengan cara melakukan penyerangan menggunakan berbagai *software* yang berbahaya seperti virus, *worm, trojan horse, spyware* dan lainnya.Tujuan dari penelitian ini adalah untuk mengukur kuantitas dan kualitas serangan siber terhadap jaringan komputer Universitas Bhayangkara Jakarta Raya, dan juga melakukan pendataan serangan siber dengan mengunakan *honeypot*. *Honeypot system* sering digunakan sebagai bagian dari sistem pendeteksi serangan (IDS, *Intrusion Detection System*) yang mampu mendeteksi ancaman yang terjadi pada sebuah jaringan komputer, keuntungan dari *honeypot* tidak hanya mendeteksi berbagai serangan tetapi dapat juga membuat sebuah system yang berpura-pura memiliki titik kelemahan yang sangat tinggi sehingga mudah diserang oleh malware. Dan jika malware menjalankan aktifitasnya system *honeypot* akan mencatat dan hasil dari catatannya dapat dianalisa guna menangani dan pemulihan selama dan setelah serangan terjadi. Hasil dari penelitian ini adalah *honeypot system* dapat mendetesi berbagai serangan, baik yang dilakukan oleh malware maupun peretas, dan hasil dari pendeteksian yang dilakukan tidak hanya mengecoh serangan tetapi juga mencatat semua kegiatan yang dilakukan oleh penyerang, hal ini dapat dilihat dari catatan hasil *scanning port* yang merupakan langkah awal dari penyerangan sensor dapat mencatat dalam satu perintah "nmap" sensor dapat mencatat 1026 aktifitas yang dianggap sebagai serangan.

Kata kunci: *honeypot, malware, ancama siber, catatan aktifitas malware*

INTRUSION DETECTION SYSTEM DESIGN USING HONEYPOT AT BHAYANGKARA JAKARTA RAYA UNIVERSITY

Abstract

The internet has become a vital part of an institution that brings great benefits to its users but on the other hand, there are a handful of users who carry out activities that take advantage of other systems by attacking using various malicious software such as viruses, worms, trojan horses, spyware and The purpose of this study is to measure the quantity and quality of cyberattacks against computer networks at Bhayangkara University, Jakarta Raya, and also to collect data on cyber attacks using a honeypot. Honeypot systems are often used as part of an attack detection system (IDS, Intrusion Detection System) that can detect threats that occur on a computer network, the advantage of a honeypot is not only to detect various attacks but can also create a system that pretends to have weak points that so high that it is easily attacked by malware. And if the malware carries out its activities, the honeypot system will log and the results of the logs can be analyzed for handling and recovery during and after the attack occurs. The result of this research is that the honeypot system can detect various attacks, whether carried out by malware or hackers, and the results of the detection do not only outwit attacks but also record all activities carried out by attackers, can be seen from the port scanning results recorded. is the first step of the attack sensor can record in one command "nmap" sensor can record 1026 activities that are considered as attacks.

Keywords: *honeypot, malware, cyber threats, malware activity record*

1. PENDAHULUAN

Internet sudah menjadi bagian penting dari sebuah institusi karena membawa keuntungan yang sangat besar bagi penggunannya tetapi disisi lain ada sebagian pengguna internet yang melakukan aktifitas dengan cara mengambil keuntungan dari sistem yang dimiliki oleh orang lain dengan cara melakukan serangan dengan menggunakan program berbahaya yang dikenal dengan *malware* (*malicious software*) dan *malware* yang digunakan bisa dalam bentuk virus, worm, trojan horse, spyware dan lain-lain. Berdasarkan data yang dikeluarkan oleh Badan Siber dan Sandi Negara (BSSN) pada tahun 2018 terdapat 12,895,554 serangan siber yang terjadi di jaringan komputer Indonesia dan 513,863 diantaranya merupakan serangan *malware* (BSSN, 2018). Malware merupakan sebuah istilah yang umum digunakan untuk program yang mempunyai tujuan jahat, program tersebut termasuk serangan *virus*, *worm*, *adware*, kuda troya dan spyware, hal-hal tersebut memiliki bahaya yang sama bagi sistem (Easttom, 2016)

Universitas Bhayangkara Jakarta Raya (Ubhara Jaya) merupakan sebuah institusi dibawah Yayasan Brata Bakti yang memiliki kedekatan dengan POLRI, hubungan ini memiliki daya Tarik bagi penyerang karena mereka menyangka bahwa Ubhara Jaya adalah bagian dari POLRI dan dampaknya jaringan komputer Ubhara Jaya kerap mendapatkan serangan berupa malware bahkan pada Februari 2018 serangan tersebut sempat melumpuhkan jaringan dan sebagian sistem yang ada. Sangat disayangkan serangan yang terjadi tidak tercatat dengan baik karena pada saat serangan terjadi Ubhara Jaya belum memiliki sistem pencatatan serangan sehingga dianggap perlu untuk membangun sebuah sistem untuk mendeteksi dan mencatat serangan yang terjadi guna membuat perencanaan pencegahan, penanganan dan pemulihan serangan malware.

2. TINJAUAN PUSTAKA

Honeypot berfungsi mengalihkan perhatian penyerang, hal tersebut disebabkan penyusup menganggap diri mereka telah berhasil melakukan peretasan dan memperoleh informasi dari sebuah jaringan komputer, yang sebenarnya informasi yang diperoleh itu merupakan hal yang tidak penting dan sistem tersebut sudah di isolir (Diansyah et al., 2017) dan disisi lain aktifitas peretasan tersebut dicatat oleh *honeypot*.

Beberapa penelitian mengkalsifikasi *honeypot* menjadi *high-interaction* atau *low-interaction* dimana; *high-interaction honeypot* merupakan perangkat dengan sistem operasi dan aplikasi yang dipersiapkan untuk mendapatkan serangan sementara *low-interaction honepot* menggunakan sistem yang biasa saja speerti, linux yang menjalanka piranti lunak yang menirukan sistem operasi, perangkat jaringan dan layanan yang biasa terdapat dalam jaringan komputer (Scott, 2014).

Layanan yang dapat ditiru oleh honeypot diantaranya; Hypertext Transfer Protocol (HTTP), Secure Shell (SSH), layanan database MySql, dan Telnet, protokol-protokol terbetu dipilih karena bebrapa alasan yaitu;

a. HTTP merupakan protokol yang paling banyak penggunaannya, dan di internet banyak sekali sumber daya yang bisa digunakan untuk melakukan eksploitasi.
b. SSH memungkinkan terjadinya percobaan *brute force* terhadap akun yang ada pada beberapa komputer.
c. MySql merupakan DBMS yang mendukung protokol HTTP dan berfungsi sebagai penyedia informasi, karena fungsinya tersebut maka protokol ini tak luput menjadi sasaran penyerangan.
d. Telnet juga menjadi target peyerangan yang menarik perhatian para peretas karena sebagian besar peralatan jaringan dan perangkan IoT dikendalikan menggunakan protokol ini. (Britton et al., 2018)

Dionaea merupakan aplikasi *honeypot* yang memiliki kemampuan untuk mencatat dan mengorganisir karakteristik dari jejak serangan malware, infromasi serangan yang terjadi disimpan dalam sebuah database SQLite dimana SQLite merupakan sebuah piranti lunak yang menimplementasikan layanan *autonomous transactional* sehingga tidak memerlukan sebuah server khusus ataupun pengaturan. (Wafi et al., 2017)

MHN adalah singkatan dari *Modern Honey Network.* MHN merupakan proyek *open-source* yang dikembangkan oleh perusahaan keamanan siber yang bernama Threatstream dengan tujuan untuk membuat solusi piranti lunak yang mudah dikembangkan dan diadopsi. Aplikasi ini mendukung penggunaan *honeypot* baik bersifat internal maupun eksternal dalam skala besardan terdistribusi.(Jigneshkumar, 2016)(Anil Tom | Dr. M N Nachappa, 2020)

Beberapa topik penelitian yang terkait dengan honeypot diantaranya;

"Honeypot Based Intrusion Detection System with Snooping agents and Hash Tags" penelitian ini menyatakan bahwa *honeypot* mengalami modifikasi algoritma sehingga dapat meningkatkan kemampuannya dalam mendeteksi serangan.(Joshi & Kakkar, 2017) dan penelitian lainya dengan judul "*Survey on Security Using Honeypot"* menyatkan bahawa penerapan *honeypot* pada sebuah jaringan diharapkan mempu memonitor dan mencegah

terjadinya aktifitas yang berbahaya dalam jaringan.(Ashani et al., 2018)

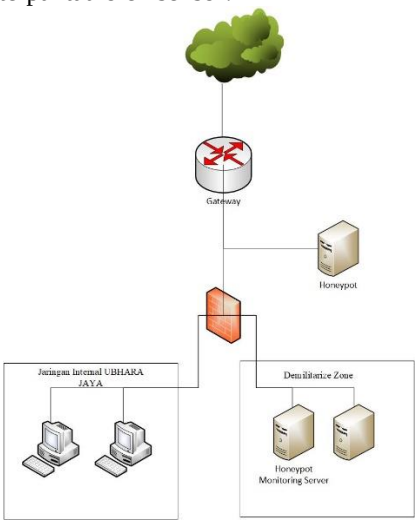
3. METODOLOGI

3.1. Perancangan Piranti Keras dan Jaringan

Sebelum melakukan implementasi penerapan *honeypot* pada jaringan perlu di rencanakan lokasi meletakan dan peralatan decoy yang akan digunakan sebagai tempat untuk menjalankan aplikasi *honeypot*, dan pada penetilian ini digunakan rapberry pi sebagai sensor untuk mengecoh penyusup dalam jaringan.

Gambar 1. Raspberry Pi 3B+ yang digunakan sebagai sensor

Setelah melakukan pemilihan piranti yang akan digunakan, tahap selanjutnya adalah penentuan lokasi peletakan piranti yang akan digunakan sebagai sensor malware dalam jaringan, untuk itu dipilih tempat yang sangat rentan terhadap serangan yaitu diantana gateway router dengan firewall yang memisahkan jaringan internet dengan jaringan DMZ (*Demilitarize Zone*) dan jaringan Internal Universitas Bhayangkara Jakarta Raya, dan untuk mencatat semua aktifitas yang terpantau oleh sensor.

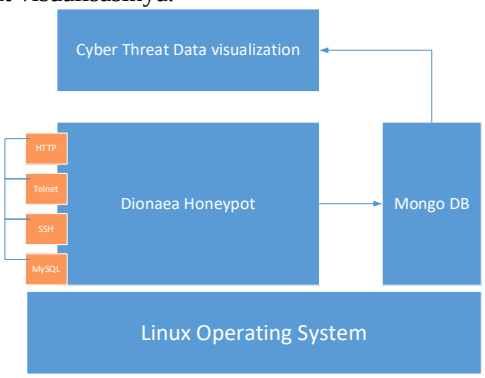


Gambar 2. Topologi jaringan Komputer UBHARA JAYA

3.2. Pemilihan Protokol Yang Akan Dipantau

Berdasarkan hasil studi pustaka yang telah dilakukan, maka disusunlah perencanaan implementasi piranti lunak yang akan digunakan sebagai *honeypot* dalam jaringan, untuk itu penulis memilih aplikasi Dionaea yang dianggap mampu menirukan kinerja protokol-protokol yang biasa mendapat serangan, protokol yang dimaksud adalah; http, telnet, ssh, dan mysql, dan dionaea berjalan diatas system operasi linux.

Hasil dari pemantauan aktifitas yang dilakukan oleh *honeypot* dikumpulkan dalam sebuah database yang pada tahap selanjutnya akan dikumpulkan untuk dibuat visualisasinya.



. Gambar 3. Arsitektur piranti lunak honeypot dan proses visualisasinya

4. PEMBAHASAN

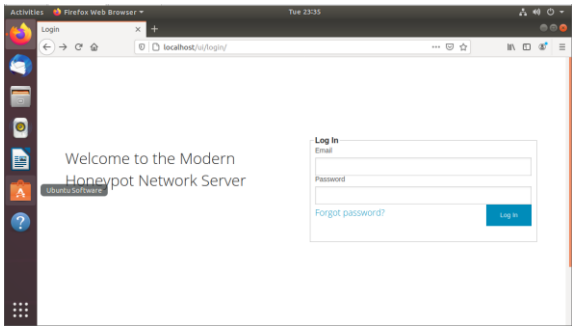
Tahapan selanjutnya adalah membuat percobaan dalam bentuk simulasi implementasi *honeypot* dalam jaringan virtual, hal ini perlu dilakukan guna menjaga agar tidak menggangu jaringan utama. Dalam percobaan ini penulis menggunakan jaringan virtual dengan menggunakan jaringan yang dibentuk oleh aplikasi vmware. Pada aplikasi ini dibuat bebrapa komputer virtual yang berfungsi sebagai; server *MHN*, sensor yang menjalankan aplikasi dionaea yang berjalan diatas sistem operasi Raspberry OS (sistem operasi dari raspbery pi), dan untuk melakukan uji penetrasi digunakan sistem operasi Kali Linux.

4.1. Persiapan MHN Server

MHN Server di jalankan diatas sistem operasi ubuntu dan untuk menggunakannya maka dilakukan proses intalasi dengan menggunakan perintah pada terminal, dan urutan peritah tersebut adalah;

```
$ sudo apt install git -y
$ cd /opt/
$ $ sudo git clone
https://github.com/pwnlandia/mhn.git
$ cd mhn/
$ sudo ./install.sh
```

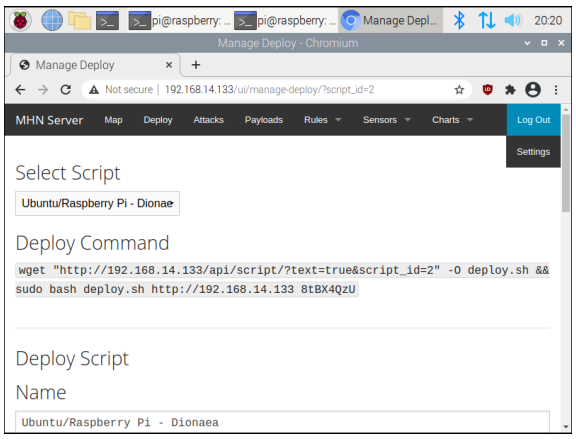
Setelah melakukan instalasi maka aplikasi MHN akan memerlukan beberapa input untuk konfigurasi. Dan tahap selanjutnya MHN server akan dapat diakses menggunakan antar muka web yang telah disediakan;



Gambar 4. Antarmuka MHN Server

4.2. Mempersiapkan Sensor Honeypot

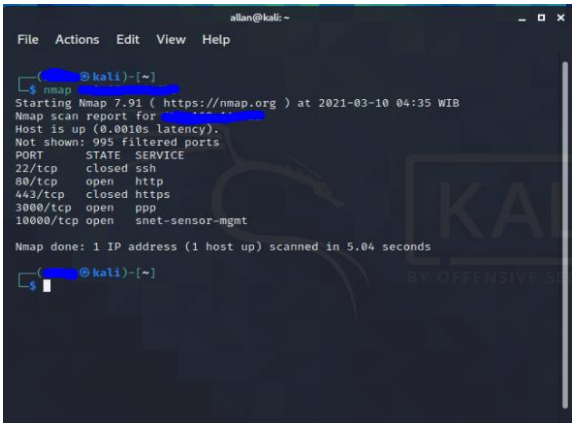
Setelah mempersiapkan MHN server, maka tahapan selanjutnya adalah pembuatan sensor, pada artikel ini peralatan yang digunakan sebagai sensor adalah Raspberry Pi 3B+ yang telah di install sistim operasi Raspberry OS. Dan untuk mempersiapkan sensor *honeypot* maka beberapa langkah yang yang perlu dilakukan yaitu; mengakses server MHN unttuk memperoleh shell script yang akan menginstall aplikasi Dionaea pada perangkat sensor dan mendaftarkan perangkat sensor pada server MHN.



Gambar 5. Shell Script yang diperoleh dari MHN Server

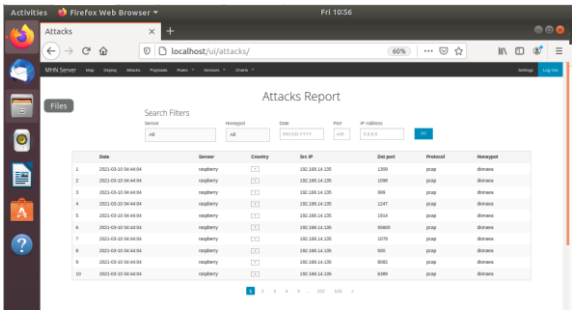
4.3. Uji Penetrasi

Langkah yang diambil selanjutnya adalah memastikan bahwa sensor bekerja dengan baik dengan cara melakukan uji penetrasi dengan menggunakan sistim operasi Kali linux dimana sistim operasi ini berisi berbagai aplikasi yang biasa digunakan untu melakukan uji penetrasi pada jaringan komputer dan juga sistem keamanan jaringan komputer. Tahap ini dilakukan beberapa pengujian penetrasi dilakukan pada sensor untuk melihat apakah sensor dapat mendeteksi serangan yang dialami.



Gambar 6. Uji penetrasi terhadap sensor

Dari hasil uji penetrasi didapati bahwa sensor memiliki beberapa layanan yang dengan sengaja dibuka dan hal ini akan menjadi perhatian bagi penyerang yang akan melakukan eksploitasi adapun layanan yang terbuka adalah HTTP yang terdapat pada port 80, PPP yang terdapat pada port 3000 dan layanan manajemen sensor yaitu pada port 10000 , namun disisi lain setiap aktifitas yang terjadi pada sensor akan dicatat oleh MHN server, beberapa aktifitas yang dicatat berupa informasi asal serangan, port yang menjadi target serangan, dan protokol yang diserang, pada percobaan ini dilakukan proses scanning pada sensor dengan menggunakan perintah npmap dan hasilnya sensor mencatat 1026 aktifitas yang dianggap sebagai serangan. Dan dari 1026 aktifitas tersebut sensor mampu mencatat beberapa informasi yaitu; waktu serangan, negara asal serangan, port yang diserang, protokol yang digunakan oleh penyerang dan sensor apa yang mendapatkan serangan.



Gambar 7. Catatan laporan serangan yang terjadi pada sensor

5. KESIMPULAN DAN SARAN

Perancangan yang telah dilakukan dapat mendetesi berbagai serangan, baik yang dilakukan oleh malware maupun peretas, dan hasil dari pendeteksian yang dilakukan tidak hanya mengecoh serangan tetapi juga mencatat semua kegiatan yang dilakukan oleh penyerang, hal ini dapat dilihat dari catatan hasil scanning port yang merupakan langkah awal dari penyerangan sensor dapat mencatat dalam satu perintah nmap sensor dapat mencatat 1026 aktifitas yang dianggap sebagai serangan, hal ini

membuktikan bahwa sensor memiliki sensitifitas yang cukup tinggi dalam mendeteksi serangan.

Pada tahap berikutnya diharapkan data serangan yang didapat dari penelitian ini untuk diolah dengan menggunakan teknik machine learning guna mendeteksi pola serangan dan membangun sistem honeypot yang berbasiskan kecerdasan buatan.

DAFTAR PUSTAKA

ANIL TOM | DR. M N NACHAPPA. (2020). A Study on Honeypots and Deceiving Attacker using Modern Honeypot Network. *International Journal of Trend in Scientific Research and Development*, *5*(1), 266–271.

ASHANI, A., NIRMAL, D., DOSHI, V., & PATIL, N. (2018). *Survey on Security Using Honeypot*. *12*, 41–43.

BRITTON, T., LIU-JOHNSTON, I., CUGNIÈRE, I., GUPTA, S., RODRIGUEZ, D., BARBIER, J., TRICAUD, S., School, H., & Project, H. (2018). *Analysis of 24 Hours Internet Attacks A Brief Overview of Malicious Traffic Targeting Featureless Servers on the Web*.

BSSN. (2018). *Laporan Tahunan 2018 Honeynet Project BSSN-IHP*.

DIANSYAH, T. M., FAISAL, I., PERDANA, A., SEMBIRING, B. O., & SINAGA, T. H. (2017). Analysis of Using Firewall and Single Honeypot in Training Attack on Wireless Network. *Journal of Physics: Conference Series*, *930*(1). https://doi.org/10.1088/1742-6596/930/1/012038

EASTTOM, C. (2016). *Computer Security Fundamentals*. Pearson.

JIGNESHKUMAR, S. M. (2016). Modern Honey Network. *International Journal of Research in Advent Technology*, *Special Issue*, 156–162.

JOSHI, V., & KAKKAR, P. (2017). Honeypot Based Intrusion Detection System with Snooping agents and Hash Tags. *International Journal of Computer Science and Information Technologies*, *8*(2), 237–242. www.ijcsit.com

SCOTT, C. (2014). Designing and Implementing a Honeypot for a SCADA Network. In *SANS Institute*. https://www.sans.org/reading-room/whitepapers/detection/designing-implementing-honeypot-scada-network-35252

WAFI, H., FIADE, A., HAKIEM, N., & BAHAWERES, R. B. (2017). Implementation of a modern security systems honeypot Honey Network on wireless networks. *2017 International Young Engineers Forum (YEF-ECE)*, 91–96. https://doi.org/10.1109/YEF-ECE.2017.7935647