JETT
Jurnal Elektro Telekomunikasi Terapan [Bulan] [Tahun]

IMPLEMENTASI SISTEM KEAMANAN JARINGAN LOKAL MENGGUNAKAN HONEYPOT DIONAEA, DAN IDS, SERTA ANALISIS MALWARE MENGGUNAKAN *MALWARE ANALYSIS SYSTEM*

IMPLEMENTATION OF THE LOCAL NETWORK SECURITY SYSTEM USING A HONEYPOT DIONAEA, AND IDS, ALSO MALWARE ANALYSIS USING MALWARE ANALYSIS SYSTEM

Resevoa Moral Muhammad[1], Indrarini Dyah Irawati[2], Muhammad Iqbal[3]

[1,2,3]Universitas Telkom, Bandung

[1]**resevoa@student.telkomuniversity.ac.id,** [2]**indrarini@tass.telkomuniversity.ac.id,** [3]**iqbal@tass.telkomuniversity.ac.id**

Abstrak

Sistem keamanan jaringan sudah sangat banyak macamnya sesuai dengan keadaan dan kondisi yang bersangkutan. Sistem keamanan jaringan sangatlah penting perannya dalam menjaga suatu keamanan jaringan sehingga dapat mencegah terjadinya penyerangan dan melindungi kita ketika terjadi penyerangan. Sering terjadi penyerangan terhadap sebuah perangkat melalui suatu jaringan baik dalam hal pemberian malware, dan pencurian data. Proyek akhir ini berfokus pada sejauh mana IDS yang berbasis HIDS dapat mendeteksi serangan serangan yang umum terjadi dalam jaringan. Dengan bantuan Honeypot Dionaea yang dijadikan sebagai penarik perhatian penyerang, serta informasi apa saja yang akan didapatkan ketika melakukan malware analysis menggunakan Cuckoo Sandbox. Implementasi ini dilakukan dengan enam user aktif yang berada dalam satu jaringan dan memperhatikan apakah penyerang dapat terdeteksi oleh IDS atau tidak. Hasil dari proyek akhir ini didapatkan bahwa IDS yang berbasis HIDS memiliki kelebihan dalam memonitoring data digital namun tidak bisa mendeteksi serangan dalam ranah jaringan yang mempengaruhi trafik jaringan tersebut, serta Cuckoo Sandbox dapat memberikan informasi malware berupa jenis malware apa yang dianalisis, bagaimana tingkahlaku malware tersebut, dan bagaimana dampak malware tersebut pada sistem yang diserang.

Kata kunci : ***Honeypot, IDS, Malware, Malware Analysis System***

Abstract

Network security system has a lot of variety according to the circumstances and conditions concerned. A network security system is a very important role in maintaining network security to prevent attacks and protect us in the event of an attack. Frequent attacks on a device through a network both in terms of malware administration, and data theft. This final project focuses on the extent to which HIDS-based IDS can detect attacks that are common in the network. With the help of Honeypot Dionaea which serves as an attracter for attackers, as well as what information will be obtained when performing analysis malware using Cuckoo Sandbox. This implementation is carried out with six active users who are in one network and pay attention to whether the attacker can be detected by IDS or not. The result of this final project was obtained that HIDS-based IDS has the advantage of monitoring digital data but cannot detect attacks in network area that affect the network traffic, and Cuckoo Sandbox can provide malware information in the form of what types of malware are analyzed, how the malware behaves, and how the malware impacts the attacked system.

Keywords: ***Honeypot, IDS, Malware, Malware Analysis System***

1. PENDAHULUAN

Seiring berkembangnya teknologi, semakin berkembang pula ancaman dan gangguan yang dihadapi dalam kinerja teknologi tersebut. Kini seorang pemulapun dapat melakukan serangan kepada sebuah sistem dengan menggunakan alat penyerangan jaringan yang ada. Dengan alasan tersebut maka diciptakanlah sebuah system pendeteksi gangguan yang dikenal sebagai *Intrusion Detection System* (IDS). Selain IDS ada juga Honeypot yang berfungsi sebagai penjebak penyerang dan Cuckoo Sandbox yang melakukan analisis malware.

Penelitian ini dilakukan berdasarkan penelitian-penelitian yang pernah dilakukan sebelumnya. Pada penelitian [1] menyatakan bahwa Dionaea dapat digunakan sebagai server palsu atau tiruan sehingga dapat melindungi server asli ketika server tiruan tersebut mengalami serangan. Pengujian server tiruannya berbasis Dionaea menggunakan metasploit framework, dan melibatkan tiga teknik exploit. Berdasarkan hasil penelitiannya honeypot dapat menunjang keamanan jaringan, namun honeypot tidak dapat melindungi sistem operasi khususnya windows. Penelitian [2] menyatakan bahwa implementasi honeypot pada jaringan nirkabel *hotspot* akan memberikan tambahan kesulitan pada penyerang, serta kombinasi antara honeypot dan IDS memberikan sebuah sistem keamanan berlapis. Beradasarkan penelitian [3] Honeypot juga dapat melindungi dari serangan *brute force* dan *malware* dengan menyediakan *port-port* dan sistem palsu. Didalam sistem palsu tesebut penyerang dapat berinteraksi seperti layaknya sistem nyata. Serangan *brute force* dideteksi oleh honeypot kippo dan disimpan berupa *log* dalam *database* MySQL, untuk serangan *malware* akan dideteksi oleh Honeypot Dionaea dengan mensimulasikan beberapa antaralain port *FTP, HTTP, HTTPS, SMB, MySQL, Name.Serever, MSPRC.* Pada penelitian [4] Honeypot Dionaea mampu mengunduh malware rata-rata tiga kali sehari. Dengan persentase serangan 89% pada *port* 445, dan 11% pada *port* 80. Penelitian [5] menyatakan bahwa SNORT dan HoneyWeb merupakan dua buah metode yang cocok untuk dikolaborasikan dengan Honeypot, dikarenakan memberikan proses deteksi serangan dengan mudah dengan dilihat melalui *log*. Bedasarkan penelitian [6] menyatakan bahwa Honeypot memiliki log yang mencatat seluruh aktivitas yang terjadi, namun cukup sulit untuk melakukan *monitoring*. Snort juga mampu menjalankan tugasnya sebagai IDS namun snort masih lemah dalam menentukan mana yang merupakan *false positif* dan mana yang *false negative*. Cuckoo sandbox mempu bekerja sebagai *Malware Analysis Toolkit* dengan baik, dimana dapat menganalisa sebuah file yang disinyalir berbahaya dan membuat sebuah laporan nantinya.

Berdasarkan dari penelitian sebelumnya penelitian ini akan mencari tau sejauh mana IDS yang berbasis HIDS dapat mendeteksi serangan, mencoba melakukan skenario penyerangan yang berbeda untuk mengetahui batas kemampuan dari IDS yang digunakan, serta melakukan analisa lebih lanjut mengenai *malware* yang berhasil di tangkap untuk mengetahui informasi apa saja yang didapatkan dari *malware* tersebut.

2. DASAR TEORI

2.1 Honeypot

Honeypot merupakan suatu alat yang sengaja dibuat untuk diserang, dan diselidiki. Pada umumnya Honeypot berupa komputer, data, atau situs jaringan yang terlihat seperti bagian dari jaringan, namun sebenarnya terisolasi dan termonitor [1].

- *Low Interaction Honeypot*

  Honeypot yang didesain untuk mengemulasikan service seperti pada server asli. Penyerang hanya mampu memeriksa dan terkoneksi ke satu atau beberapa *port*.

- *High interaction Honeypot*

  Honeypot ini memiliki sistem operasi dimana penyerang dapat berinteraksi langsung dan tidak ada batasan yang membatasi interaksi tersebut. Menghilangkan batasan tersebut memiliki resiko yang tinggi karena penyerang dapat memiliki akses *root*.

2.2 Intrusion Detection System

Merupakan sebuah metode yang dapat digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan [7]. IDS dapat melakukan inspeksi terhadap lalu lintas *inbound* dan *outbound* dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti percobaan intrusi (penyusupan).

- *Network-based Intrusion Detection System* (NIDS)

  Semua lalu lintas yang mengalir ke jaringan akan dianalisis apakah ada upaya penyusupan pada sistem jaringan. NIDS biasanya terletak pada pintu masuk jaringan atau dimana sever berada. Kekurangan dari NIDS adalah cukup rumit diimplementasikan dalam jaringan yang menggunakan switch ethernet.

- *Host-based Interusion Detection System* (HIDS)

  Aktivitas suatu host jaringan akan dipantau, terlepas dari apakah ada upaya serangan atau gangguan. HIDS biasanya ditempatkan di server utaman di jaringan, seperti Firewall, server web, atau server yang terkoneksi ke internet.

2.3 Malware

Malware adalah sebuah perangkat lunak yang dibuat dengan tujuan memasuki dan terkadang merusak sistem komputer, jaringan, atau server tanpa diketahui oleh pemiliknya [8]. Tujuan malware tentu saja untuk menghancurkan atau mencuri data dari perangkat yang di masuki. *Malware* adalah perangkat lunak yang secara khusus dirancang untuk melakukan aktivitas perusak. Perangkat lunak perusak lainnya seperti trojan horse, virus, spyware, dan exploit. Tujuan pembuatan malware adalah untuk melakukan aktivitas berbahaya yang dapat berdampak negatif pada korban, seperti penyadapan dan pencurian informasi pribadi.

2.4 Malware Analysis

Analisis malware adalah proses untuk menentukan fungsi, sumber, dan dampak potensial dari sampel malware tertentu seperti virus, worm, trojan horse, rootkit, atau backdoor. Ada dua metode untuk melakukan Analisa terhadap malware, yaitu:

- *Dynamic Analysis*

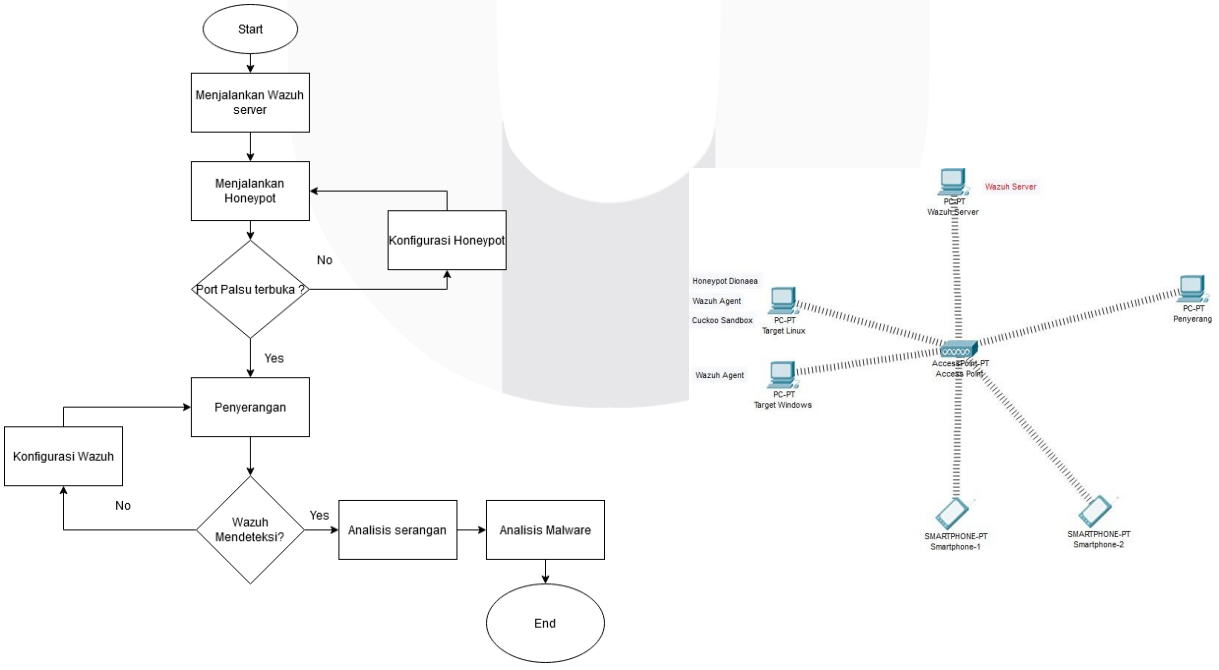
Merupakan suatu metode untuk menganalisis malware dengan membandingkan perilaku sistem sebelum malware dijalankan dengan perilaku sistem sesudah malware tersebut dijalankan. Metode analisis dinamik biasanya menggunakan software virtual seperti Virtualbox, VMware, dan lain-lain, sehingga apabila malware yang dijalankan menyebabkan kerusakan pada sistem, sistem utama tidak akan rusak oleh malware tersebut.

- *Static Analysis*

Merupakan metode yang digunakan untuk melakukan analisis malware dengan secara langsung mengamati kode sumber malware. Saat mengamati source code malware tersebut umumnya menggunakan Teknik Reverse Engineering.

3. Analisis

Pada BAB ini akan dilakukan analisis tentang informasi apa saja yang didapatkan dari hasil penyerangan pada bab sebelumnya. Gambar 1 menunjukkan diagram alir tentang bagaimana sistem ini bekerja, serta pada gambar 2 menunjukkan tentang topologi yang digunakan dalam sistem ini.

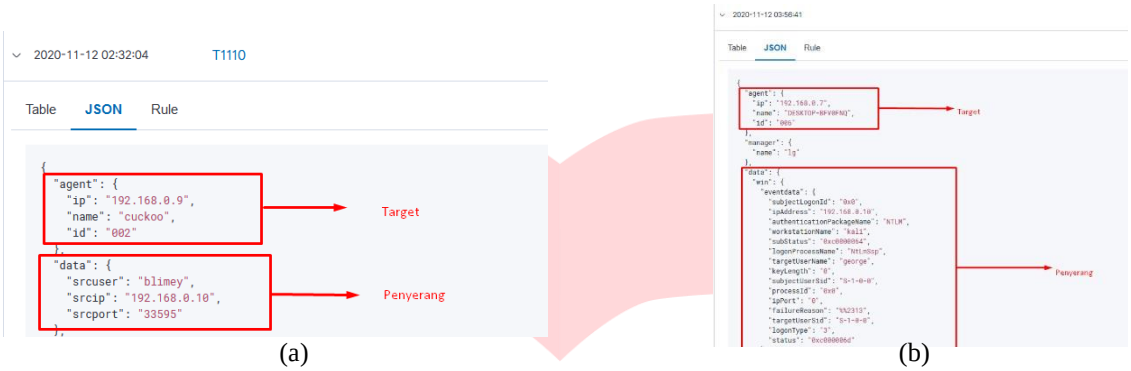


(a) (b)

Gambar 1 (a) Diagram Alir (b) Topologi

3.1 Bruteforce

Pada serangan pertama yaitu SSH Bruteforce didapatkan hasil dari Wazuh berupa informasi adanya *login* SSH secara paksa pada jam tertentu. Didapatkan juga informasi target yang diserang serta IP penyerang dan user yang digunakan untuk melakukan login SSH. Dilakukan juga serangan RDP Bruteforce, serangan ini mencoba untuk mendapatkan akeses komputer melalui cara *remote desktop*, informasi yang didapatkan dari wazuh antara lain berupa ip target yang di serang, ip penyerang, serta menggunakan user apa penyerang untuk melakukan rdp bruteforce.

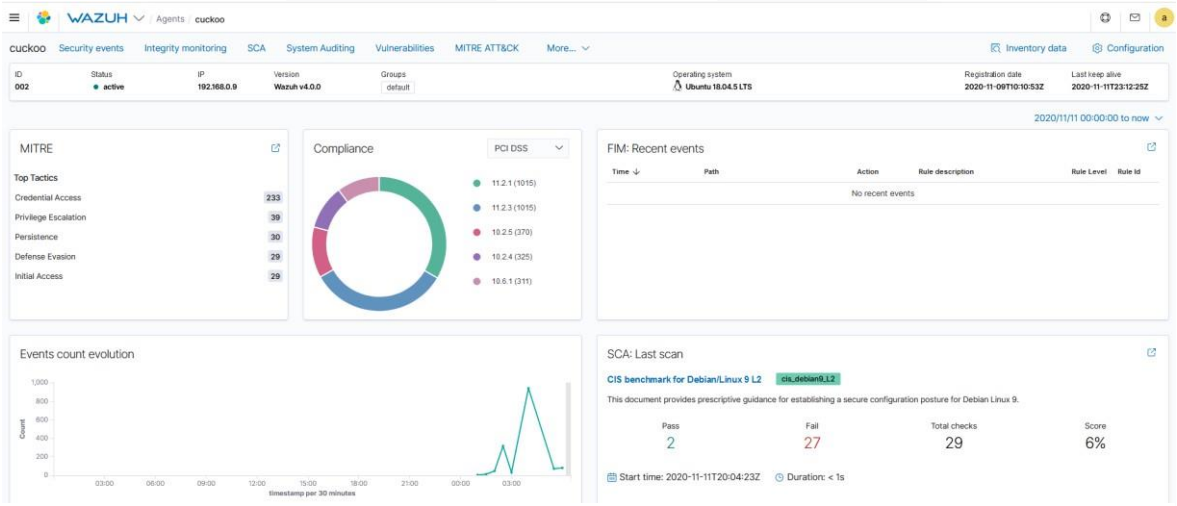


(a) (b)

Gambar 2 Informasi yang didapatkan dalam serangan *Bruteforce* (a) SSH *Bruteforce* (b) RDP *Bruteforce*

3.2 DoS

Pada serangan ketiga ini dilakukan penyerangan DoS disini memanfaatkan *port* 80 yang telah di buka oleh Honeypot Dionaea, namun hasil yang didapatkan oleh wazuh adalah tidak adanya aktivitas serangan yang terjadi.



Gambar 3 Tidak terdeteksinya serangan Bruteforce

Ini terjadi karena IDS yang berbasis HIDS memang lebih handal dalam melakukan monitoring data digital, disebutkan dalam situs Wazuh yang menyatakan bahwa wazuh merupakan salah satu

HIDS yang baik dimana melakukan analisis terhadap aktivitas log di tiap perangkat agen yang terdaftar namun beberapa masalah keamanan lebih sering terdeteksi dengan melakukan inspeksi terhadap tafik jaringan.

3.3 Integrity dan Vulnerability Monitoring

Integrity Monitoring adalah salah satu fitur Wazuh untuk memastikan data digital tersebut dapat dipercaya dan akurat isinya. Dalam percobaan ini dilakukan membuat file, mengedit, dan menghapus file. Semua kegiatan tersebut dapat terekam dengan baik oleh Wazuh. *Vulnerability Monitoring* pada wazuh disini melakukan pemindaian ke seluruh aplikasi yang ada di dalam agen yang terhubung dengan wazuh. Wazuh akan mendeteksi celah celah kemanan yang ada disetiap aplikasi yang ada.

Time	syscheck.path	syscheck.event
Nov 12, 2020 @ 04:46:03.862	c:\apple\test.txt	deleted
Nov 12, 2020 @ 04:45:57.868	c:\apple\test.txt	modified
Nov 12, 2020 @ 04:45:55.063	c:\apple\test.txt	added
Nov 12, 2020 @ 04:45:55.047	c:\apple\new text document.txt	deleted
Nov 12, 2020 @ 04:45:52.239	c:\apple\new text document.txt	added

Gambar 4 *Integrity Monitoring*

Most common rules

Rule ID	Description	Count
23506	CVE-2020-26154 affects libproxy1v5	1
23506	CVE-2020-26154 affects libproxy1-plugin-networkmanager	1
23506	CVE-2020-26154 affects libproxy1-plugin-gsettings	1
23506	CVE-2020-15683 affects thunderbird-gnome-support	1
23506	CVE-2020-15683 affects thunderbird	1

Export: Raw Formatted

1 2 3 4 »

Gambar 5 *Vulnerability Monitoring*

4. KESIMPULAN

Berdasarkan hasil perancangan, pengujian dan analisa yang telah dilakukan maka dapat diambil beberapa kesimpulan sebagai berikut :

1. Berdasarkan dari hasil pengujian sistem deteksi yang dilakukan oleh wazuh dapat bekerja dengan baik, khususnya dalam hal menjaga data digital.
2. IDS yang berbasis HIDS memiliki kelebihan dalam melakukan monitoring terhadap kegiatan log pada setiap agen yang terhubung.
3. Honeypot yang digunakan berfungsi sebagai penarik perhatian para penyerang dimana membuka beberapa port, namun sistem asli tidak terpengaruh dari penyerangan.

4. Informasi yang didapatkan dari analisis *malware* berupa jenis *malware*, tingkah laku dari *malware* tersebut, serta dampak yang ditimbulkan dari *malware* tersebut.

REFERENSI

[1] T. A. Cahyanto, H. Oktavianto, and A. W. Royan, "Analisis dan Implementasi Honeypot Menggunakan Dionaea Sebagai Penunjang Keamanan Jaringan," *JUSTINDO (Jurnal Sist. dan Teknol. Inf. Indones.*, vol. 1, no. 2, pp. 86–92, 2013.

[2] P. Soepomo, "Penerapan Sistem Keamanan Honeypot dan Ids pada Jaringan Nirkabel (Hotspot)," vol. 1, no. 1, pp. 111–118, 2013, doi: 10.12928/jstie.v1i1.2512.

[3] D. P. Agustino, Y. Priyoatmojo, and N. W. W. Safitri, "Implementasi Honeypot Sebagai Pendeteksi Serangan dan Melindungi Layanan Cloud Computing," *Konf. Nas. Sist. Inform. 2017*, pp. 196–201, 2017.

[4] P. Studi, T. Informatika, and F. Teknik, "MENGGUNAKAN DIONAEA (Malware Detection in the Network Using Dionaea) Harjono," vol. 14, no. 2, pp. 64–69, 2013.

[5] P. L. Restanti and D. Utomo, "Analisis Kolaborasi IDS SNORT dan HoneyPot," 2014.

[6] I. L. Pribadi, R. Munadi, and Y. Purwanto, "Implementasi Sistem Keamanan Jaringan Menggunakan Honeypot Dionaea, Ids, dan Cuckoo Sandbox," 2013.

[7] Sutarti, P. Pancaro, Adi, and I. Saputra, Fembi, "Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal," *J. PROSISKO*, vol. 5, no. 1, 2018, [Online]. Available: http://e-jurnal.lppmunsera.org/index.php/PROSISKO/article/download/584/592.

[8] A. Tedyyana and S. Supria, "Perancangan Sistem Pendeteksi Dan Pencegahan Penyebaran Malware Melalui SMS Gateway," *INOVTEK Polbeng - Seri Inform.*, vol. 3, no. 1, p. 34, 2018, doi: 10.35314/isi.v3i1.340.