PENINGKATAN KEAMANAN JARINGAN TERHADAP SERANGAN MALWARE MENGGUNAKAN TEKNIK HONEYPOT DIONAEA

Agus Hariyanto[1)], Surateno[2)]

Jurusan Teknologi Informasi, Politeknik Negeri Jember
Jalan Mastrip PO BOX 164 Jember

[1)]agus_hariyanto@polije.ac.id, [2)]surateno@polije.ac.id

Abstract

Handling for network security issues require a defense system that uses a firewall, antivirus and intrusion detection systems in the network (network intrusion detection system / NIDS). Security-related attacks through the network with malware could use the honeypot Dionaea. In this research honeypot implementation Dionaea as a shadow server as a diversion attack, while the model of the attack through the network first scan and attack by malware. It is expected that the system is implemented capable of handling network security attacks. Scenario testing in this study were carried out attacks on the system via the internal network and external networks / public use nmap and metasploit. Besides testing in realtime against attack from outside. This model of data retrieval is done for 3 days in a span of 7:00 to 3:00 p.m. On testing over a local network, the public and the public in realtime obtained the system has detected attacks. In the public backlash in realtime leads on port 1433 for MSSQL service, so it requires more handling for systems that use the service.

Keywords— honeypot dionaea, keamanan jaringan , malware, metasploit, scanning port.

PENDAHULUAN

Keamanan jaringan adalah bagian terpenting dalam sebuah sistem organisasi yang secara tidak langsung tergantung dengan teknologi informasi (TI). Penyerangan terhadap sebuah sistem sebanyak 62,7 % lebih didasarkan pada *cyber crime*,28 % oleh hacker, 5,3 % cyber spionase serta 4% cyber war [hackmagedon]. Sedangkan target penyerangan adalam sistem layanan online yang mencapai 29,3 % dari kebanyakan target. Teknik yang banyak digunakan untuk menyerang keamanan sistem adalah melalui malware sebanyak 41,3 %.[1]

Penanganan untuk masalah keamanan jaringan tersebut memerlukan sistem pertahanan yang menggunakan firewall , antivirus dan sistem pendeteksi penyusupan dalam jaringan (network intrusion detection system / NIDS). Teknik yang banyak digunakan dalam pengelolaan jaringan adalah menggunakan NIDS, tetapi terdapat kelemahan yaitu sistem NIDS hanya memantau dan mencatat proses terkait penyerangan terhadap sistem. Terdapat kemampuan untuk menahan serangan tetapi belum ada solusi terhadap penyerangan, solusi dilakukan oleh administrator sistem jaringan.[5]

Alternatif lain dari penanganan adalah menggunakan teknik sistem penanganan keamanan secara proaktif (proactive monitoring). Terkait keamanan jaringan dengan penyerangan melalui malware dapat menggunakan honeypot dionaea.

Pada penelitian ini dilakukan implementasi honeypot dionaea sebagai server bayangan sebagai pengalih serangan, sedangkan model penyerangan melalui scan jaringan terlebih dahulu dan penyerangan melalui malware. Diharapkan sistem yang diimplementasikan mampu menangani serangan keamanan jaringan tersebut.[2]

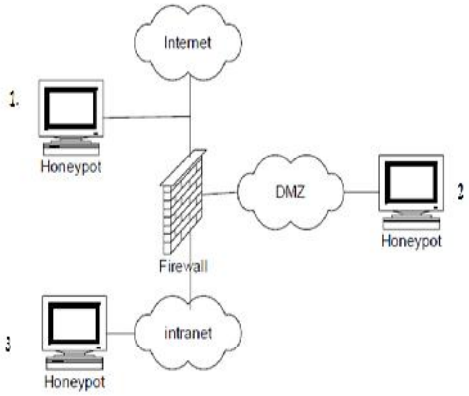
TINJAUAN PUSTAKA

Sistem keamanan jaringan ditentukan oleh empat komponen yaitu ketersediaan informasi, kerahasiaan informasi, keutuhan

data, serta keabsahan kepemilikan data atau informasi tersebut. Untuk itu diperlukan sebuah rancangan yang tepat dengan cakupan empat komponen tersebut .

Salah satu mekanisme pengamanan jaringan adalah menempatkan salah satu bagian layanan atau server yang dijadikan umpan bagi pihak penyerang atau hacker, dan selanjutnya di analisa pola penyerangan yang digunakan sebagai dasar dalam sistem pertahanan dan pendeteksi serangan. Teknik pengamanan tersebut dikenal dengan teknik honeypot[4].

Honeypot biasanya diletakkan sebelum firewall atau gateway pada sebuah sistem, baik pada akses jaringan intranet, internet dan DMZ, seperti pada gambar 1. Hal ini dilakukan untuk memperbanyak akses informasi penyerangan dari semua jalur keluar dan masuknya data di sistem jaringan.



Gambar 1. Lokasi honeypot pada sistem keamanan jaringan.

Honeypot digolongkan menjadi 3 berdasar model sistem nya yaitu Low Interaction, Medium Interaction serta High Interaction. Pada Low Interaction, model sistem yang digunakan berupa layanan(service) yang diemulasikan sesuai di server. Pada Medium Interaction, model sistem dibuat sesuai seutuhnya dengan sistem server yang ada. Dan pada High Interaction, sistem memberikan hak akses langsung pada server asli tetapi tedapat proteksi pada service tertentu dan beresiko tinggi terhadap serangan[6] .

Pada penelitian ini dilakukan menggunakan model Low Interaction dengan teknik Dioanea,dengan mekanisme pemberian bug software sebagai umpan bagi malware agar mengeksploitasi service layanan jaringan yang ada sehingga didapatkan salinan code dari malware tersebut yang diproses menjadi informasi terkait pola dan mekanisme penyerangan. Informasi tersebut dapat diakses menggunakan format teks atau berbasis web. [3] .

METODE PENELITIAN

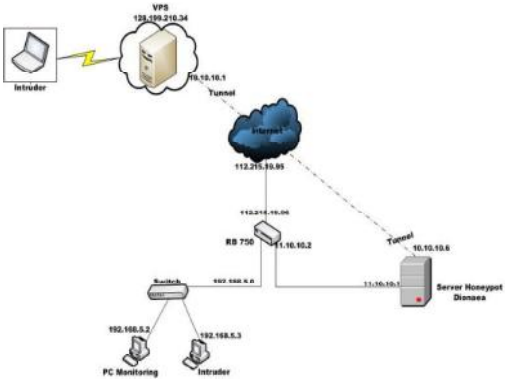
Metode penelitian yang dilakukan adalah dengan melakukan kegiatan analisa kebutuhan , perancangan sistem jaringan, impelemtasi sistem jaringan serta uji coba sistem.

Pada kegiatan analisa kebutuhan dilakukan pengumpulan data dan informasi terkait lhoneypot dioanea serta kebutuhan sistem untuk proses implementasi, sehingga didapatkan kebutuhan sistem sesuai dengan tabel 1.

Tabel 1. Kebutuhan Sistem Jaringan

No	Kebutuhan	Spesifikasi
1	Sistem Operasi Server	Ubuntu
2	Honeypot	Dionaea
3	Klien	Intruder Intranet dan Online
4	VPS	Pengujian Online
5	Mikrotik	Routerboard

Pada kegiatan perancangan sistem jaringan didapatkan desain topologi jaringan seperti pada gambar 2. Dimana honeypot dionea akan ditanam pada sebuah server ubuntu sebagai umpan untuk proses exploitasi hingga scanning port oleh penyerang. Sedangkan penyerang melalui jaringan lokal dan online. Bagi penyerang jaringan online melalui tunelling pada server VPS ke server lokal.



Gambar 2. Topologi Sistem Jaringan.

Pada kegiatan implementasi sistem dilakukan konfigurasi pada sistem. Layanan

dasar jaringan terlebih dahulu diinstall yaitu ssh,ftp dan http , karena nanti port tersebut akan digunakan oleh dionaea. Sedangkan untuk Server yang sudah terinstal jangan dilengkapi terlebih dahulu dengan beberapa aplikasi atau layanan (service) jaringan seperti http, ftp, ssh dan lainya. Selanjutnya dilakukan implementasi dionaea pada server serta konfigurasi melalui iptables untuk memonitoring port yang diserang dengan mengarahkan port agar bisa dicek oleh dionaea.

Pada saat terdapat interaksi terhadap honeypot dionaea maka secara otomatis sistem akan mendeteksi sebagai tindakan penyusupan dan akan direkam oleh honeypot. Hasil dari rekaman tersebut yang dianalisa guna diambil tindakan selanjutnya.

Pada tahapan pengujian dilakukan dengan mekanisme pengujian melalui jaringan lokal dan publik / online. Pengujian menggunakan tool nmap dan metasploit yang dilakukan selama 3 hari pengujian . Dengan data penyerangan yang masuk akan direkam sebagai bahan analisa penyerangan.

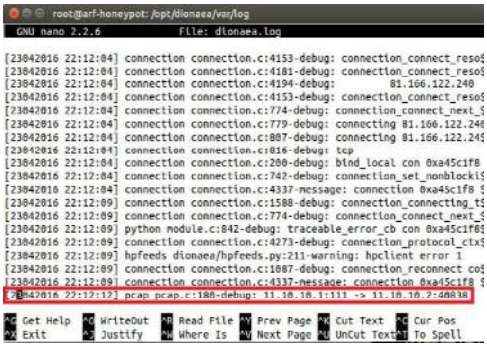
HASIL DAN PEMBAHASAN

Skenario ujicoba pada penelitian ini adalah dilakukan penyerangan terhadap sistem melalui jaringan internal dan jaringan luar / publik menggunakan nmap dan metasploit. Selain itu dilakukan pengujian secara realtime terhadap penyerangan dari luar. Pengambilan data model ini dilakukan selama 3 hari pada rentang waktu 07.00-15.00 . Sedangkan port samaran dari honeypot dionaea yang digunakan adalah sesuai dengan tabel 2.

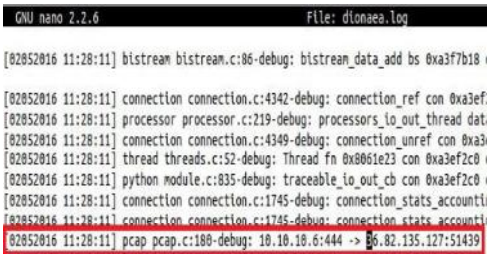
Tabel 2. Port Samaran Honeypot Dionaea

No	PORT	Layanan
1	443	SSL
2	445	SMB
3	5060	SIP
4	135	EPMAPPER
5	3306	MYSQL
6	42	NAME SERVER
7	80	HTTP
8	21	FTP
9	1433	MSSQL

Pada pengujian scanning jaringan menggunakan aplikasi zenmap , dilakukan scanning terhadap sistem jaringan baik dari dalam dan luar jaringan yang terdeteksi seperti gambar 3 dan gambar 4.

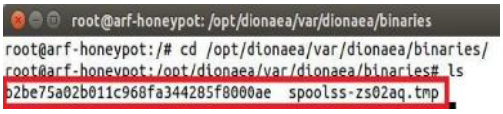


Gambar 3. Hasil Log Sistem Scanning Port dari Jaringan Lokal.



Gambar 4. Hasil Log Sistem Scanning Port dari Jaringan Publik.

Pengujian selanjutnya dilakukan eksploitasi terhadap layanan yang ada pada sistem dionaea, pada pengujian ini dilakukan pada layanan sharing file pada port 445 atau lebih dikenal dengan layanan Service Messages Block (SMB) . Pada pengujian ini mengunakan aplikasi metasploit dan sistem berhasil mendeteksi penyerangan serta menyalin code malware pada direktori karantina sistem. Hasil penyimpanan malware dari penyerangan jaringan lokal dan publik terlihat pada gambar 5 dan gambar 6.



Gambar 5. File hasil karantina metasploit dari jaringan lokal.

Gambar 6. File hasil karantina metasploit dari jaringan publik.

Pada pengujian yang terakhir adalah membuka sistem jaringan agar bisa secara langsung menyerang melalui jaringan publik. Sehingga semua yang online di internet dapat menyerang kedalam sistem. Penyerangan dari publik dapat terdeteksi seperti pada gambar 7.

Gambar 7. File hasil karantina metasploit dari jaringan publik secara realtime.

Sedangkan rekap data penyerangan dari jaringan publik secara realtime adalah sesuai pada tabel 3. Pada tabel 3 terlihat bahwa penyerangan terbanyak pada port MSSQL dan paling sedikit pada port SSL.

TABEL 3
JUMLAH SERANGAN TERDETEKSI

No	Port/Layanan	Jumlah Serangan
1	443/SSL	4
2	445/SMB	8
3	5060/SIP	4
4	135/EMAPPER	20
5	3306/Mysql	3
6	42/Name Server	5
7	80/HTTP	30
8	21/FTP	26
9	1433/MSSQL	60

KESIMPULAN

Sistem honeypot dionaea telah berhasil terimplentasi pada sistem keamanan jaringan dalam menangkal malware. Dalam hal ini sistem telah memberikan samaran layanan palsu serta tercatat kedalam log sistem. Data tersebut yang akan dijadikan acuan dalam menganalisa serangan.

Pada pengujian melalui jaringan lokal, publik serta publik secara realtime didapatkan sistem telah mendeteksi serangan. Pada serangan publik secara realtime banyak mengarah pada port 1433 untuk layanan MSSQL , sehingga diperlukan penanganan lebih bagi sistem yang menggunakan layanan tersebut.

Dalam penelitian lanjutan diharapkan menggunakan terdapat kombinasi antara sistem honeypot dan intrusion prevention system (IPS) , sebagai kolaborasi ampuh terhadap serangan sistem. Selain itu diperbanyak model penyerang sebagai ujicoba kehandalan sistem seperti menggunakan aplikasi brute force, flooding serta sistem penyerangan yang lain.

DAFTAR PUSTAKA

[1] (2016) February 2016 Cyber Attacks Statistics [Online].Tersedia: http://www.hackmageddon.org/

[2] Chandra A., Lalitha K., " Honey Pots: A New Mechanism for Network Security", Problems and Application in Engineering Research Paper, Vol 4, Spesial Issue 01, 2013.

[3] Kambow N., Passi L. K. , " Honeypots: The Need of Network Security", International Journal of Computer Science and Information Technologies , Vol 5(5) , 2014.

[4] Kumar R. , Kaur Er.T , "A Study on Statistical Analysis on Security Attack Logs" , International Journal of Advanced Research in Computer Science and Software Engineering, Volumen4, Issue 9, September 2014.

[5] Ourida S.B. Boubaker, "Impelentation of an Intrusion Detection System," IJCSI International Journal of Computer Science Issues Vol 9, Issue 2, No 1 , May 2012 .

[6] Zemene M. S., AvadhaniP. S. , "Honeypot System for local network atttackes ", IRACST-International Journal of Computer Science dan Information & Security , Vol 6, No. 2 Mar-April 2016.