IMPLEMENTASI HIGH INTERACTION HONEYPOT PADA SERVER

IMPLEMENTATION OF HIGH INTERACTION HONEYPOT TO SERVER

Lukito Prima Aidin[1], Surya Michrandi Nasution[2], Fairuz Azmi[3]

[1,2,3]Prodi S1 Sistem Komputer, Fakultas Teknik, Universitas Telkom
[1]primalukito@students.telkomuniversity.ac.id,[2]michrandi@telkomuniversity.ac.id,
[3]azme27@telkomuniversity.ac.id

Abstrak

Teknologi internet saat ini tidak lepas dari banyak masalah ataupun celah keamanan. Banyaknya celah keamanan ini dimanfaatkan oleh orang yang tidak berhak untuk mencuri data-data penting. Kasus serangan terjadi karena pihak yang diserang juga tidak menyadari pentingnya keamanan jaringan untuk diterapkan pada sistem yang dimilki.

Honeypot adalah suatu sistem yang didesain menyerupai production system asli dan dibuat dengan tujuan untuk diserang / disusupi. Honeypot diimplementasikan menggunakan honeypot jenis high interaction yaitu high interaction analysis tools serta menggunakan software pendukung lainnya. Uji coba ketahanan dilakukan dengan cara penyerangan langsung untuk mengetahui keamanan dari system.

Hasil dari penelitian ini adalah high interaction honeypot yang diimplementasikan pada server yang akan memberikan sebuah sistem keamanan berlapis dengan menipu dan mendeteksi serangan serta ditujukan untuk keamanan web server.

Kata kunci: honeypot, high interaction, web server, keamanan.

Abstract

Today's internet technology is not free from many problems or security holes. This security hole could be exploited by an unauthorized person to steal important data. The case of the attacks occurred because the party that was attacked also did not realize the importance of network security to be applied to the system.

Honeypot is a system that is designed to resemble the original production system and is made with the intention to be attacked / compromised. Honeypot implemented using high interaction honeypot as well as using other supporting software. Durability test conducted with direct attacks to determine the safety of the system.

The outcome of this research is a high interaction honeypot implemented to server which will provide secured system to deceive and detect attacks, and is intended for web server security.

Keywords: honeypot, high interaction, web server, security.

1. Pendahuluan

Perkembangan teknologi internet telah menjadikannya salah satu media utama pertukaran informasi. Tidak semua informasi bersifat terbuka untuk umum. Karena internet merupakan jaringan komputer yang bersifat publik, maka diperlukan suatu usaha untuk menjamin keamanan informasi tersebut. Di satu sisi, telah banyak usaha- usaha untuk menjamin keamanan suatu informasi. Di sisi lain, tetap saja ada pihak- pihak dengan maksud tertentu yang berusaha untuk menembus sistem keamanan tersebut. Untuk saat ini saja, penyerangan terhadap aplikasi web telah melebihi 60% [14]. Oleh karena itu, diperlukan suatu sistem yang mampu mendeteksi usaha-usaha dan pola penyusupan tersebut.

Honeypot adalah suatu sistem yang didesain menyerupai production system asli dan dibuat dengan tujuan untuk diserang / disusupi. Karena honeypot bukan merupakan production system asli, maka hanya sedikit atau bahkan tidak ada sama sekali trafik jaringan yang berasal dari atau menuju honeypot. Oleh karena itu, semua trafik honeypot patut dicurigai sebagai aktivitas yang tidak sah atau tidak terautorisasi. Hal tersebut memungkinkan untuk dilakukan pendeteksian terhadap usaha-usaha tersebut dengan cara melakukan pengawasan (monitoring) terhadap sistem honeypot.

Server adalah sebuah sistem yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. *Server* dapat digunakan untuk implementasi sistem *high interactin honeypot* yang dibuat untuk sengaja diserang tanpa mengakibatkan resiko atau dampak buruk bagi *web server* sesungguhnya. Oleh sebab itu dipersiapkan suatu pengamanan untuk *web server* yaitu sistem *high interaction honeypot* yang di implementasikan pada *web*

server palsu untuk menjadi perangkap dari penyerang serta membantu mengamankan *web server* yang sesungguhnya.

2. Tinjauan Pustaka

2.1. *Website*

Website adalah suatu metode untuk menampilkan informasi di internet, baik berupa teks, gambar suara maupun *video* yang interaktif dan mempunyai kelebihan untuk menghubungkan (*link*) satu dokumen dengan dokumen lainnya (*hypertext*) yang dapat diakses melalui *web browser* [22]. Salah satu hal yang paling sering diserang di dunia digital adalah *website*. Penyerangan terhadap aplikasi *web* telah melebihi 60% dari total serangan [14]. Oleh karena itu diperlukan pengamanan yang lebih untuk mencegah hal-hal yang tidak diinginkan.

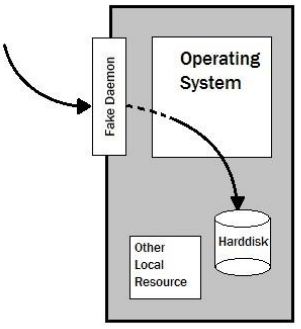
2.2. *Honeypot*

Honeypot adalah suatu sistem yang sengaja dikorbankan untuk menjadi sasaran penyerangan dari peretas. *Honeypot* juga berguna untuk membuang-buang sumber daya penyerang atau mengalihkan penyerangan dari sesuatu yang lebih berharga. Sistem tersebut dapat melayani serangan yang dilakukan oleh peretas dalam melakuan penetrasi terhadap server tersebut [2]. *Honeypot* juga dapat diterapkan untuk memperoleh informasi - informasi dari kegiatan peretas, serta mengetahui metode yang digunakan dalam menyerang suatu sistem sehingga dapat dilakukan tindakan pencegahan terhadap sistem yang dilindungi sebenarnya. Pada tahap awal, biasanya peretas akan melakukan *scanning* terhadap jaringan untuk mencari komputer yang *vulnerable*. Jika penyerang melakukan koneksi ke *honeypot*, maka *honeypot* akan segera mendeteksi dan mencatat tindakan tersebut, karena seharusnya tidak ada *user* yang berinteraksi dengan *honeypot*.

2.2.1. Jenis *Honeypot*

Perbedaan jenis *honeypot* ini adalah berdasarkan *level of involvement* (tingkat keterlibatan). *Level of involvement* membedakan derajat interaksi penyerang dengan sistem *honeypot*. Berdasarkan tingkat keterlibatan ini, *honeypot* dapat dikategorikan menjadi tiga yaitu:

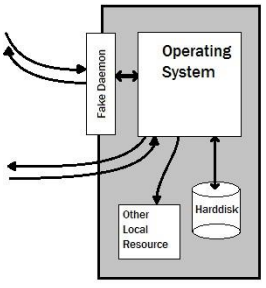
1. *Low Interaction Honeypot*, yaitu jenis *honeypot* yang hanya menyediakan tiruan atau emulasi dari layanan tertentu saja. Tidak ada sistem operasi nyata yang dapat dipakai sebagai tempat operasi penyerang untuk low interaction honeypot. *Honeypot* jenis ini relatif lebih mudah dan cepat untuk di terapkan.



Gambar 1. *Low Interaction Honeypot*

Dari gambar 1, pada *low interaction honeypot* hanya mengemulasikan layanan dan melakukan *logging* yang selanjutnya akan dicatat pada *harddisk* namun tidak melakukan akses ke resource lain.

2. *High interaction honeypot*, menyediakan sistem penuh untuk berinteraksi. Ini berarti *high interaction honeypot* tidak hanya melakukan tiruan dari layanan, fungsi, maupun *operating system* saja. Honeypot jenis ini memberikan sistem dan layanan nyata layaknya sistem yang sesungguhnya. Oleh karena itu, penyerang dapat melakukan control penuh pada sistem honeypot. HIHAT adalah contoh dari *high interaction honeypot* aplikasi *web*. HIHAT mengubah aplikasi PHP menjadi *honeypot* dengan derajat interaksi yang tinggi [10].



Gambar 2. *High Interaction Honeypot*

Dari gambar 2 menjelaskan bahwa *honeypot high interaction* menggunakan seluruh sistem operasi sebagai medianya termasuk sumber daya yang ada di dalamnya.

3. *Medium Interaction Honeypot*, *honeypot* jenis ini memberikan ilusi dari operasi sistem palsu yang dapat berkomunikasi dengan penyerang [7]. Kemudian melakukan pencatatan aktivitas dari si penyerang. Honeytrap adalah salah satu contoh dari *medium interaction honeypot*.

2.3. Web Server

Server adalah sebuah sistem komputer yang menyediakan jenis layanan dalam sebuah jaringan komputer. Server didukung dengan kapasitas memori yang cukup besar dan dilengkapi dengan suatu sistem operasi khusus. Server juga dapat menjalankan perangkat lunak yang dapat mengontrol akses terhadap jaringan dan sumber daya yang berada didalam jaringan tersebut. Server memiliki aplikasi yang menggunakan arsitektur klien contohnya adalah DHCP server, Mail Server, HTTP Server, FTP Server, dan DNS Server.

2.4. High Interaction Analysis Tools

High interaction analysis tools (hihat) merupakan software untuk memonitoring honeypot dan berbasis web. High interaction analysis tools memberikan design menarik untuk mendukung proses pemantauan honeypot dan menganalisis data yang diperoleh.

Sebuah web service seperti PHPNuke, PHPMyAdmin, dan OSCOmmerce menjadikan honeypot berfungsi dengan baik, yang menawarkan keamanan lengkap dari aplikasi untuk pengguna tapi melakukan pencatatan dan pemantauan yang komprehensif di balik layar.

High interaction analysis tools juga dilengkapi pencatat log secara berkala dan terperinci. High interaction analysis tools ini dapat mencatat ip peretas secara baik dan dapat memvisualisasikan berapa jumlah hits yang dilakukan oleh peretas dan file apa yang diakses oleh peretas. Sedangkan prinsip kerja yang dilakukan high interaction analysis tools adalah menjawab respon yang dilakukan oleh peretas dengan respon yang diharapkan oleh peretas. Peretas mengirimkan permintaan berbahaya lalu honeypot akan memproses request dan menulis ke database lalu memberi balasan pada penyerang. Setelah dilakukan identifikasi jenis serangan maka high interaction analysis tools akan mengasilkan respon untuk mensimulasukan hasil dari serangan yang berhasil. Serangan diterima dan diproses untuk memberikan respon yang akurat.

3. Perancangan dan Implementasi Sistem

3.1. Gambaran Umum Sistem

Secara sistematis, infrastruktur *honeypot* Cubieboard serta *web server* asli yang dirancang dan diimplementasikan memiliki topologi fisik seperti gambar seperti berikut ini

Gambar 3. Gambaran Umum Sistem

Berdasarkan gambar 4, sistem *honeypot low interaction* dan *honeypot high interaction* diterapkan pada satu jaringan yang sama dengan *web server* asli.

3.2. Server Honeypot

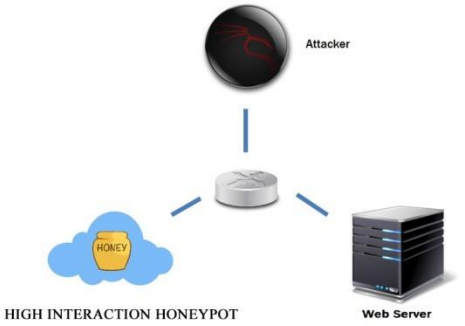
Penggunaan Server sebagai media *honeypot* memiliki beberapa keuntungan yaitu:

1. *Open Source*
2. Proses instalasi mudah.
3. Bisa digunakan di berbagai *platform* dan *embedded system*.

4. Pengujian dan Analisis

4.1. Gambaran Pengujian dan Analisis

Pada bagian pengujian dan analisis, menguji dan menganalisa kemampuan *honeypot* yang dibuat pada Cubieboard. Metode yang digunakan adalah *directory buster brute force*, RFI, DoS, dan SQL *Injection*.
Untuk kebutuhan pengujian dan analisa, menggunakan topologi yang lebih sederhana seperti yang ditunjukkan pada gambar 5. Penyerang, *server honeypot*, serta *web server* utama dikoneksikan kedalam satu jaringan yang sama. Pengujian dilakukan menggunakan *tools* yang ada pada kali linux, seperti DirBuster, Metasploit, SQLMap, dan DoS yang tersedia untuk perangkat yang memiliki platform Java.



Gambar 4. Topologi Pengujian

Pengujian *high interaction honeypot* pada server ditempatkan pada satu jaringan dengan penyerang digunakan untuk memudahkan dalam percobaan emulasi kemampuan dari *honeypot* hihat pada Cubieboard.

4.2. Directory Buster Brute Force

Directory buster brute force adalah metode untuk menemukan *file* dari sebuah *web* dan direktori di dalamnya menggunakan serangan *brute force*. DirBuster dapat menemukan direktori web baik menggunakan *list* nama direktori maupun dengan *brute force* murni. DirBuster merupakan *client* HTTP ditulis menggunakan bahasa perograman Java yang menggunakan *list* direktori umum yang ditemukan dan mengirimkan permintaan ke masing-masing direktori [20]. Beberapa hasil *crawling* menggunakan DirBuster ditunjukkan pada tabel 1.

Tabel 1 Hasil Directory Buster Brute Force

Found	Response Code	Content Length
/	200	317
/cgi-bin/	403	539
/icons/	200	195
/doc/	403	535
/icons/small/	200	195
/twiki	200	1074
/twiki/readme.text	200	4726
/twiki/license.text	200	20096
/twiki/TwikiDocumentation.html	200	461323
/twiki/TwikiHistory.html	200	53645
/twiki/bin/	403	541
/twiki/templates/	403	547
/twiki/bin/search/	200	201

/twiki/bin/view/Main/	200	201

4.3. SQL Injection

SQL Injection menggunakan SQLmap untuk menguji kinerja dari *honeypot*. Tes ini berfungsi untuk mengetahui *username* atau *password* ari *web* tersebut

Tabel 2. Hasil SQL Injection

ID	Request	IP	Hit	Attack
5489	/tikiwiki/tiki-index.php	192.168.0.13	PHPSESSID = f0f61ba57ad892c9d03371a25b525675	No Attack Found
5488	/tikiwiki/tiki-index.php	192.168.0.13	PHPSESSID = f0f61ba57ad892c9d03371a25b525675	No Attack Found
5487	/tikiwiki/tiki-index.php	192.168.0.13	Page=HomePage UNION ALL SELECT NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL--	SQL
5486	/tikiwiki/tiki-index.php	192.168.0.13	Page=HomePage UNION ALL SELECT NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL--	SQL

Dari tabel 2, kita dapat menyimpulkan bahwa TikiWiki tidak dapat diserang menggunakan SQL Injection tetapi karena penyerangan dilakukan di *honeypot* maka *honeypot* mendeteksi bahwa telah terjadi serangan yang di lakukan oleh peretas yaitu SQL.

4.4. Remote File Intrusion

Metasploit adalah suatu software untuk melakukan penyerangan yang biasa disebut dengan *Remote File Inclusion* yaitu digunakan untuk menjalankan suatu *file* didalam *web server*. Hasil yang diproses oleh honeypot dijelaskan didalam tabel 3.

Gambar 7. Pengujian Remote File Inclusion

ID	Request	IP	Hit	Attack
5491	/tikiwiki/tiki-graph_formula.php	192.168.0.13	0 = x.expm1.passthru(chr(101) . chr(99). chr(104). chr(111). Chr(32). Chr(89). Chr(89). Chr(59). Chr(99). Chr(97). Chr(116). Chr(32). Chr(100). Chr(98). Chr(47). Chr(108). Chr(111). Chr(99). Chr(97). Chr(108). Chr(46). Chr(112). Chr(104). Chr(112). Chr(59). Chr(101). Chr(99). Chr(104). Chr(111). Chr(32). Chr(89). Chr(89))	INCLUSION
5490	/tikiwiki/tiki-graph_formula.php	192.168.0.13	0 = x.expm1.passthru(chr(101) . chr(99). chr(104). chr(111). Chr(32). Chr(89). Chr(89). Chr(59). Chr(99). Chr(97). Chr(116). Chr(32). Chr(100). Chr(98).	INCLUSION

			Chr(47). Chr(108). Chr(111). Chr(99). Chr(97). Chr(108). Chr(46). Chr(112). Chr(104). Chr(112). Chr(59). Chr(101). Chr(99). Chr(104). Chr(111). Chr(32). Chr(89). Chr(89))	

4.5 Denial of Service

Denial of Service adalah cara umum dalam melakukan penyerangan yaitu dengan mengirim *file log* sebanyak mungkin dalam waktu bersamaan sehingga dapat menyebabkan *server* tersebut *down*. Tabel 3 akan menampilkan hasil DoS tersebut.

Tabel 3 Hasil Log DoS

ID	Request	IP	Time	Attack
5583	/tikiwiki/tiki-index.php	192.168.0.13	2016-06-15 09:19:58	No Attack Found
5582	/tikiwiki/tiki-index.php	192.168.0.13	2016-06-15 09:19:58	No Attack Found
5581	/tikiwiki/tiki-index.php	192.168.0.13	2016-06-15 09:19:58	No Attack Found
5580	/tikiwiki/tiki-index.php	192.168.0.13	2016-06-15 09:19:58	No Attack Found
5579	/tikiwiki/tiki-index.php	192.168.0.13	2016-06-15 09:19:58	No Attack Found

Tes DoS pada Honeypot tidak dapat disimulasikan oleh honeypot sebagai serangan dikarenakan DoS bisa dinggap sebagai kumpulan user yang mengakses honeypot tersebut secara bersamaan sehingga terjadi *lagging* dan mengakibatkan server down dan tidak dapat digunakan. Tabel 3 adalah beberapa hasil serangan DoS yang tercatat pada honeypot.

5. Kesimpulan

Dari hasil percobaan yang telah penulis lakukan dan analisa yang ada dapat disimpulkan bahwa:

1. Implementasi *high interaction honeypot* yang dipasang pada *server* yang berupa berhasil dilakukan dengan menggunakan High Interaction Analysis Tools sebagai *high interaction honeypot* untuk aplikasi *web*.
2. Berdasarkan hasil pengujian, dapat disimpulkan bahwa *honeypot high interaction* HIHAT dapat mengemulasikan dan mencatat serangan *directiory buster brute force*, RFI, dan SQL Injection namun masih belum dapat mengemulasikan serangan DoS dengan sempurna.
3. Dari hasil DoS, HIHAT pada *honeupot* mengalami *delay* saat mendapatkan *request* yang banyak secara bersamaan namun semua *request* tetap diproses tanpa adanya *packet loss*.

Daftar Pustaka

[1] Boparai, A., Ruhl, R., & Lindskog, D. 2012. The Behavioral Study of Low Interaction Honeypots: Dshield and Glastopf in Various Web Attacks. *Unpublished*.

[2] Diebold, P., Hess, A., & Schafer, G. 2005. A Honeypot Architecture for Detecting and Analyzing Unknown Attacks. *14th Kommunikation in Verteilten Systemen*.

[3] Harjono, & Wicaksono, A. P. 2013. Honeyd untuk Mendeteksi Serangan Jaringan di Universitas Muhammadiyah Purwokerto. *JUITA*, 225-229.

[4] Husnan, S. 2013. *Implementasi Honeypot untuk Meningkatkan Sistem*. Surakarta: Universitas Muhammadiyah Surakarta.

[5] Khairil, Riyanto, N. P., & Rosmeri. 2013. Membangun Webserver Intranet dengan Linux. *Jurnal Media Infotama, 9*, 1-24.

[6] Kim, H.-k., Kim, T.-h., & Kiumi, A. 2008. Using Honeypots to Secure E-Government Networks. *Advances in Security Technology*, 79-88.

[7] Mahajan, S., Adagale, A. M., & Sahare, C. 2016. Intrusion Detection System Using Raspberry PI Honeypot in Network Security. *IJESC International Journal of Engineering Science and Computing*, 2792-2795.

[8] Maheswara, A. C. 2013. *Implementasi Honeyd sebagai Alat Bantu Pengumpulan Serangan Aktifitas Serangan Jaringan*. Bandung: Politeknik Telkom.

[9] Muhammad, A. 2011. *Implementasi Honeypot dengan Menggunakan Dionaea di Jaringan Hotspot Fizz*. Bandung: Politeknik Telkom.

[10] Muter, M., Freiling, F., Holz, T., & Matthews, J. 2008. *A Generic Toolkit for Converting Web Applications Into High-Interaction Honeypots*. University of Manheimm.

[11] Narote, S., & Khanna, S. 2014. Advanced Honeypot System for Analysing Network Security. *International Journal of Current Research and Academic Review*, 65-70.

[12] Prasad, B. R., Abraham, A., Abhinav, A., Gurlahosur, S. V., & Srinivasa, Y. 2011. Design and Efficient Deployment of Honeypot and Dynamic Rule Based Live Network Intrusion Collaborative System. *International Journal of Network Security & Its Applications (IJNSA)*, 52-65.

[13] Rao, S. S., Hedge, V., Maneesh, B., M., J. P., & Suresh, S. 2013. Web Based Honeypots Network. *International Journal of Scientific and Research Publications*, 1-5.

[14] Rist, L., Vetsch, S., Kobin, M., & Mauer, M. 2010. Know Your Tools: Glastopf a Dynamic, Low Interaction Web Application Honeypot. *The Honeynet Project KYT Paper*.

[15] Sajjadi, S. M., & Pour, B. T. 2013. Study of SQL Injection Attacks and Countermeasures. *International Journal of Computer and Communication Engineering*, 539-542.

[16] Singh, A., Pahal, M., & Goyat, N. 2013. A Review Paper On Firewall. *International Journal for Research in Applied Science Engineering Technology (IJRASET)*, 4-8.

[17] Srilatha, B., Susmitha, B., & Srinivasu, N. 2013. Honeypots for Network Security. *International Journal of P2P Network Trends and Technology*, 172-177.

[18] Sumarno, & Bisosro, S. 2010. Solusi Network Security dari Ancaman SQL Injection dan Denial of Service (DoS). *TEKNOLOJIA, 5*, 19-29.

[19] Suresh, K., Yadav, K. K., Srijit, R., & Bhat, K. P. 2014. Hybrid Honeypot - System for Preserving Privacy in Networks. *International Journal of Advanced Research in Computer Science Engineering and Information Technology*, 375-387.

[20] Swarup, R. 2014. Practical Use of Infosec Tools. *ISSA Journal - Developing and Connecting Cybersecurity Leaders Globally*, 14-21.

[21] Utdirartatmo, F. 2006. *Trik Menjebak Hacker dengan Honeypot*. Yogyakarta: ANDI.

[22] Yuhefizar. 2008. *10 Jam Menguasai Komputer*. Jakarta: PT. Elex Media Komputindo.