ANALISIS SERANGAN HACKER MENGGUNAKAN *HONEYPOT HIGH INTERACTION* (*HIHAT)*

Wahyu Purnama Sari
Fakultas Teknik, Program Studi Informatika
Universitas Langlangbuana
Jl. Karapitan 116, Bandung
wahyu.purnama@unla.ac.id

I Nyoman Adhi Palguna Putra
Fakultas Teknik, Program Studi Informatika
Universitas Langlangbuana
Jl. Karapitan 116, Bandung
adhiikuvukiland@gmail.com

ABSTRAK

Informasi merupakan asset perusahaan yang harus dijaga kerahasiaannya dari akses pihak-pihak yang tidak bertanggungjawab. Aspek keamanan informasi yang harus dilindungi mencakup *Confidentiality, Integrity* dan *Availability*. Berbagai serangan dan ancaman dapat dilakukan untuk mengambil alih asset informasi yang diinginkan. *Hacker* merupakan seseorang yang memiliki kemampuan untuk menembus sistem keamanan sebuah perusahaan. Ada beberapa jenis serangan *hacker* biasa dilakukan yaitu *SQL Injection, Cross Site Scripting (XSS), Brute Force, Distributed-Denial-of-Service (DDoS), Inclusion, Code Injection* dan lain-lain. *Honeypot* merupakan teknologi keamanan yang bertujuan mengidentifikasi, mencari celah keamanan dan berkontribusi aktif ketika terjadi aktifitas penyusupan keamanan teknologi informasi. *Honeypot High Interaction (Hihat)* dapat merekam dan mengumpulkan informasi serangan lebih spesifik dan lebih banyak. Jenis serangan yang terekam oleh *Honeypot Hihat* ini kemudian dianalisa untuk mengetahui jenis serangan yang paling banyak masuk ke perusahaan XYZ.

Kata Kunci: *Honeypot*; *Hihat;* Analisis; Hacker; Keamanan*; SQL Injection dan XSS.*

ABSTRACT

Information is a corporate asset that should be kept confidential access to parties who are not responsible. Aspects of the security of the information to be protected includes the Confidentiality, Integrity and Availability. A wide range of attacks and threats can be made to take over the assets of the desired information. A hacker is someone who has the ability to penetrate security systems of a company. There are several types of hacker attacks performed, i.e. SQL Injection, Cross Site Scripting (XSS), Brute Force, Distributed-Denial-of-Service (DDoS), Inclusion, Code Injection and more. Honeypot is a security technology that aims to identify, find security gaps and contribute actively when there are security intrusions on information technology activities. High Interaction Honeypot (Hihat) may record and collect information more specific attacks and more. The type of attack that was recorded by the Honeypot Hihat is then analyzed to find out the type of attack that most got into XYZ Company.

Keywords: Honeypot; Hihat; Analysis; Hacker; Security; SQL Injection and XSS.

I. PENDAHULUAN

Internet sebagai salah satu jaringan konektifitas terluas didunia memberikan banyak kemudahan-kemudahan dalam berbagai aspek kehidupan manusia. Dimana hampir semua fungsi organisasi dapat dilakukan di dunia virtual, seperti bisnis, perbankan, pendidikan, pemerintahan, kesehatan dan masih banyak lainnya. Kemudahan dan fasilitas yang ditawarkan oleh jaringan berbasis internet menjadikan internet saat ini sebagai kebutuhan utama yang tidak bisa dipisahkan dari kehidupan sehari-hari baik secara individu ataupun organisasi.

Banyak organisasi atau perusahaan yang kemudian melibatkan teknologi informasi dan internet sebagai bagian tak terpisahkan dari aktivitas operasionalnya, tentunya hal ini akan mendatangkan dampak teror yang luar biasa terhadap penyerangan sistem jaringan dan komputer yang dimiliki. Banyak jenis kejahatan siber terjadi karena rendahnya sistem keamanan dari *website* sistem perusahaan, sehingga pelaku kejahatan siber dapat dengan leluasa mengambil alih asset perusahaan dengan modus tertentu.

Perusahaan XYZ merupakan perusahaan yang menggunakan web server untuk layanan operasional perusahaan. Perusahaan XYZ Seringkali mendapatkan serangan dari pelaku kejahatan dengan berbagai macam serangan. Serangan-serangan inilah yang kemudian dianalisa untuk mengetahui jenis serangan yang dilakukan oleh *hacker*.

II. LANDASAN TEORI

Analisis

Menurut Keraf [4], "Analisa adalah sebuah proses untuk memecahkan sesuatu ke dalam bagian-bagian yang saling berkaitan satu sama lainnya". Sedangkan Komarudin [1], mengatakan bahwa

analisis merupakan suatu kegiatan berfikir untuk menguraikan suatu keseluruhan menjadi komponen sehingga dapat mengenal tanda-tanda dari setiap komponen, hubungan satu sama lain dan fungsi masing-masing dalam suatu keseluruhan yang terpadu.

Hacker

Jika ada seseorang menggunakan teknologi *hacking* untuk kejahatan maka dia akan mengotori ilmu dan teknologi *hacking*. Beberapa contoh cara kerja *hacker* adalah sebagai berikut:

a. *Spoofing*, bentuk pemalsuan dimana identitas pemakai disamarkan atau dipalsukan.
b. *Scanner*, program yang mampu mendeteksi kelemahan komputer di jaringan lokal atau di jaringan dengan lokasi lain.
c. *Sniffer*, kata lain dari *Network Analyzer* berfungsi sebagai alat untuk memonitor jaringan komputer. Alat ini dapat dioperasikan hampir pada seluruh tipe protokol pada *Ethernet*, *Transmission Control Protocol/Internet Protocol (TCP/IP)*, *Internetwork Packet Exchange (IPX)* dan lainnya.
d. *Password Cracker*, program yang digunakan untuk membuka enkripsi *password* atau sebaliknya, tetapi sering digunakan untuk mematikan sistem pengamanan *password*.
e. *Destructive Device*, sekumpulan program antivirus yang dibuat khusus untuk menghancurkan data-data, diantaranya *E-mail Bombs*, dan lainnya.

Dalam websitenya, idsirtii.co.id [3] menjelaskan ada 4 (empat) alasan mengapa para *hacker* melakukan aksi *hacktivism*nya.

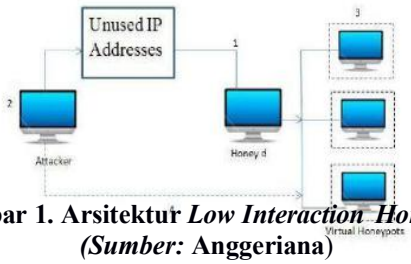
1. *Thrill Seekers* adalah aktivitas seseorang untuk mencari sensasi diri. Perlu diperhatikan, generasi yang lahir setelah tahun 85-an telah terbiasa dengan keberadaan komputer di lingkungannya, berbeda dengan mereka yang lahir di masa-masa sebelumnya. Jika generasi lama merasakan sebuah sensasi diri yang menyenangkan dengan cara bermain catur, mengisi teka teki silang, bermain kartu truft, menyelesaikan misteri cerita detektif, dan lain sebagainya maka generasi baru mendapatkan sensasi diri yang sama dengan cara utak-atik atau ngoprek komputer, bermain *game*, dan tentu saja melakukan kegiatan hacking.
2. *Organized Crime* adalah Organisasi untuk melakukan kejahatan. Bukan rahasia umum bahwa di negara-negara maju misalnya, telah banyak berkeliaran para *hacker* profesional yang tugasnya adalah melakukan kejahatan terorganisasi.
3. *Terrorist Groups* adalah untuk menjalankan aktivitas terorisme. Di jaman modern ini para teroris melihat bahwa internet dan dunia maya merupakan lahan dan media yang cukup efektif untuk melakukan aktivitas teror dimana-mana. Sasaran *terrorist hacker* biasanya adalah *critical infrastructure* alias obyek-obyek vital sebuah negara seperti perusahaan listrik, instalasi militer, pusat transportasi publik, sentra-sentra keamanan negara, jaringan keuangan perbankan, dan lain sebagainya.
4. *Nation-States* adalah untuk alasan intelijen. Seperti diketahui bersama, setiap negara pasti memiliki jaringan intelijen di dalam dan di luar negeri untuk keperluan pertahanan dan keamanan nasional. Karena saat ini seluruh percakapan, interaksi, komunikasi, diskusi, kooperasi, transaksi, dan negosiasi dilakukan dengan memanfaatkan teknologi informasi dan internet, maka kegiatan intelijen-pun mulai masuk ke ranah ini.

Honeypot

Anggeriana [2], *Honeypot* merupakan teknologi keamanan yang bertujuan mengidentifikasi, mencari celah keamanan dan berkomprimasi aktif ketika terjadi aktifitas penyusupan keamanan teknologi informasi. Secara fungsional dari teknologi *honeypot* terdiri dalam banyak variasi dan umumnya terbadi dalam dua kategori yaitu *honeypot* interaksi rendah (*low interaction honeypot*) dan *honeypot* berinteraksi sensitif (*high interaction honeypot*).

Low Interaction Honeypot

Anggeriana [2], *Low Interaction Honeypot* adalah sebuah *honeypot* yang didesain untuk menyerupai jaringan infrastruktur pada server asli. Penyerang hanya mampu memeriksa dan terkoneksi ke satu atau beberapa *port*. Contoh sederhana dari *honeypot* jenis ini dalah pembuatan sebuah *service* yang mendengarkan dan mencatat setiap koneksi yang terjadi pada sebuah *port*. *Low Interaction Honeypot* bersifat koneksi satu arah karena dari satu sisi-sisi *honeypot,* hanya mendengarkan dan mencatat koneksi yang terjadi tanpa memberikan balasan kepada koneksi tersebut. Hal ini akan mengurangi resiko karena tidak akan ada sistem yang akan diambil alih Arsitektur *low interaction honeypot* dapat dilihat pada gambar 1.



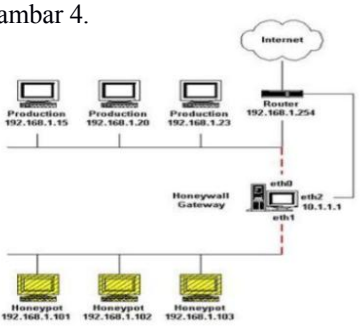
Gambar 1. Arsitektur *Low Interaction Honeypot* (*Sumber:* Anggeriana)

High Interaction Honeypot

Pada *High Interaction Honeypot* terdapat sistem operasi dimana terjadi interaksi secara langsung dengan *hacker* dan tidak ada batasan yang membatasi interaksi tersebut. Dengan dihilangkannya batasan-batasan tersebut, maka tingkat resiko yang dihadapi semakin tinggi karena *hacker* dapat memiliki akses *root*. Pada saat yang sama, kemungkinan

pengumpulan informasi semakin meningkat dikarenakan kemungkinan serangan yang tinggi. Informasi tersebut dapat berupa pola serangan, program yang digunakan, motivasi dan lain-lain.

High interaction honeypot harus diawasi secara terus menerus, pengawasan ini diperlukan karena apabila *high interaction honeypot* telah diambil alih dan dimanfaatkan oleh penyerang maka *honeypot* tersebut dapat menjadi ancaman bagi jaringan yang ada. Arsitektur *high interaction honeypot* dapat dilihat pada gambar 4.



Gambar 2. Arsitektur *High Interaction Honeypot* (*Sumber:* Anggeriana)

Perbandingan *Low Interaction* dan *High Interaction Honeypot*

Masing-masing kategori dari *honeypot* tersebut memiliki keunggulan, keunggulan yang dimiliki *low interaction honeypot* yaitu, skala pembangunan dan skala pemeliharaan kategori sederhana, karena *honeypot low interaction* didesain hanya untuk mengumpulkan informasi penyerang dan menjadi target utama penyerang sehingga dampak resiko minimum dari sistem utama dapat dicapai.

Sedangkan keunggulan dari *high interaction honeypot* yaitu, merekam dan mengumpulkan informasi lebih spesifik dari *low interaction honeypot*, *behavior* penyerang dan penelusuran jaringan *protocol* secara spesifik dari penyerang saat terjadinya insiden penyerangan atau penyusupan. Perbandingan antara *low interaction honeypot* dan *high interaction honeypot* dapat dilihat pada Tabel 1.

Tabel 1. Perbandingan *Low Interaction dan High Interaction*

Low Interaction Mensimulasi sistem operasi dan servis	***High Interaction*** Sistem Operasi dan servis sungguhan tanpa emulasi
1. Mudah diinstal dan *deploy*, konfigurasi software biasanya sederhana. 2. Resiko minimal, emulasi mengontrol apa yang bisa dilakukan penyusup. 3. Menangkap jumlah informasi terbatas.	1. Menangkap informasi lebih banyak. 2. Bisa cukup kompleks. 3. Resiko tinggi, penyusup bisa berinteraksi dengan sistem operasi sungguhan

III. METODE

Metode penelitian yang digunakan adalah penelitian deskriptif, dimana peneliti memusatkan perhatian kepada serangan-serangan yang terjadi pada server di perusahaan XYZ. Pengumpulan data untuk proses analisa dilakukan dengan cara observasi dan wawancara untuk mendapatkan informasi yang akurat. Seperti diketahui *hacker* paling gencar mencari data-data vital perusahaan supaya dapat menyebarluaskan data atau untuk memeras perusahaan. Secara gamblang penulis menganalisis sistem aplikasi berdasarkan data rahasia yang biasanya dicari oleh para *hacker* untuk diambil datanya Dari hasil observasi yang dilakukan, ditemukan fakta bahwa serangan-serangan yang terjadi pada server perusahaan XYZ adalah *SQL Injection, Cross Site Scripting (XSS) dan Deface.*

IV. HASIL DAN DISKUSI

Sistem yang digunakan pada analisis saat ini mencakup beberapa aspek dalam software dan juga hardware yang mumpuni dikarenakan kebutuhan sistem yang sangat besar, aplikasi dapat berjalan apabila terdapat server yang dapat berjalan dengan optimal sehingga dapat mensupport software yang digunakan. Berdasarkan banyaknya ancaman data yang diretas melalui aplikasi website yang tidak terintegrasi keamanannya maka dilakukan analisa dengan memasang *Honeypot High Interaction (HIHAT)* di beberapa aplikasi yang sudah disebutkan sebelumnya. Adapun ringkasan spesifikasi server yang digunakan untuk memasang Honeypot *HIHAT* yaitu menggunakan sistem operasi *Ubuntu (Linux)* juga menggunakan beberapa software yang menunjang seperti *PHP, JAVA, MySQL, dll*. Perangkat keras yang digunakan diwajibkan untuk dapat standby 7x24 jam supaya server dapat tetap beroperasi tanpa ada hambatan yang dapat membuat server menjadi *down.*

Analisis Serangan

Pada tahap awal aplikasi *Honeypot* HIHAT menu yang dimiliki salah satunya adalah *overview* dari serangan yang terjadi, pada analisa ini dilakukan analisa dari beragam jenis serangan yang terbaca oleh *Honeypot HIHAT*. Pada analisa ini ditunjukkan *script* berdasarkan tiga jenis serangan yang dilakukan *hacker* yang ditampilkan pada tabel 1 sd tabel 3.

1. *SQL Injection*

   Pada serangan *SQL Injection* terdapat *script* untuk mengetahui user dalam sebuah aplikasi yang dapat dilihat pada tabel 1.

Tabel 2. *Script* penyerangan penggunakan *SQL Injection*

Perintah	***Script***
OR	*admin OR 1=1 dan ' or ''='' or ''='*
UNION	*UNION select username,password from users--*
DROP	*Blah; UserId = 105; DROP TABLE users;*

Perintah diatas merupakan perintah yang paling banyak dideteksi oleh *Honeypot HIHAT,* akan

dijelaskan dibawah ini pengertian dari masing-masing perintah yang terbaca, yaitu:

a. Perintah *or* dan *scriptnya* bisa diartikan sebagai *username* dan *or* akan menghasilkan nilai satu sehingga hasil query *SQL* ini akan menghasilkan nilai *true.*

b. Perintah *UNION* merupakan perintah untuk menggabungkan lebih dari dua tabel atau biasa disebut dengan *join* beberapa tabel yang ingin dibaca saat melakukan serangan ataupun dalam keadaan sedang melakukan *query* untuk pemanggilan data.

c. Perintah *DROP* biasa digunkan untuk menghapus *field* atau data yang banyak dimanfaatkan oleh *database administrator* tetapi juga biasa digunakan untuk menghapus tabel target oleh para *hacker* dan *blah;* merupakan *script* yang akhirannya diberikan tanda titik koma (*;)* yang artinya *command* dibelakangnya diabaikan.

Rekaman data serangan pada aplikasi HIHAT ditunjukkan pada gambar 3.

Gambar 3. Data serangan yang direkam oleh *Honeypot HIHAT*

Pada menu overview terdapat keterangan:

1. Modul keuangan telah diserang
2. IP Address penyerang 192.168.43.43
3. Browser yang digunakan adalah *Mozilla Firefox*
4. Waktu terjadinya serangan adalah tanggal 11-10-2017 Pukul 20:57:48
5. Jenis serangan yang terjadi adalah *SQL Injection*
6. *URL* atau alamat yang dijadikan target saat menyerang adalah http://192.168.43.208/keuangan/index.php
7. *Script* serangan yang digunakan adalah *OR '1'='1* pada form *Login*
8. Tercatat *cookie* atau session terakhir dari *web*site.

Pada menu overview gambar 1 hanya menunjukkan ringkasan dari serangan yang masuk, selanjutnya pada menu details akan menunjukkan lebih banyak keterangan dari serangan yang masuk seperti ditunjukkan pada gambar 4.

Gambar 4.* Detail Informasi Serangan *SQL Injection

2. *Cross-Site Scripting (XSS)*
   Script serangan *XSS* akan ditunjukan pada tabel 2.

Tabel 2 *Script* penyerangan menggunakan *XSS*

Perintah	*Script*
<*script*>	`<script>alert('XSS');</script>`
<IMG>	`<img src="http://website.com/image.jpg" " alt="">`

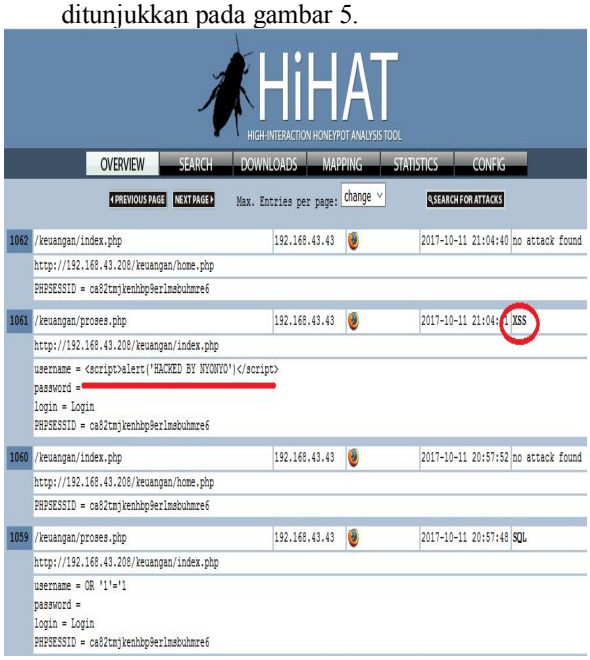
Serangan *XSS* termasuk serangan yang banyak digunakan oleh *hacker,* salah satunya menggunakan perintah <*script*>, untuk itu akan dijelaskan pengertian dari *script XSS* diatas:

a. Perintah <*script*> merupakan salah satu bahasa pemrograman *javascript* yang dapat memunculkan *alert* atau peringatan yang dapat dimanfaatkan oleh *hacker* utuk mengubah tampilan atau menyusup kedalam halaman *web*.

b. Perintah <*img src=””*> memiliki tujuan untuk mengubah tampilan dari halaman *web*site yang diserang untuk mengelabui atau merusak tampilan dari halaman *website* target sehingga ketika ada user yang masuk

ke halaman tersebut dapat diketahui oleh teknik tersebut.

Rekaman data serangan pada aplikasi HIHAT ditunjukkan pada gambar 5.



Gambar 5. Honeypot* merekam aktivitas serangan *XSS

Pada menu overview terdapat keterangan:

1. Modul keuangan telah diserang
2. *IP Address* penyerang 192.168.43.43
3. *Browser* yang digunakan adalah *Mozilla Firefox*
4. Waktu terjadinya serangan adalah tanggal 11-10-2017 Pukul 21:04:01
5. Jenis serangan yang terjadi adalah *XSS*
6. *URL* atau alamat yang dijadikan target saat menyerang adalah http://192.168.43.208/keuangan/index.php atau *form Login*
7. *Script* serangan yang digunakan adalah <*script*>alert('*HACKED* BY NYONYO');</*script*> pada field username di dalam form *Login*
8. Tercatat *cookie* atau *session* terakhir dari *web*site.

Pada menu details akan menunjukkan lebih banyak keterangan dari serangan yang masuk seperti ditunjukkan pada gambar 4.

Gambar 4. Detail Informasi Serangan *SQL Injection*

V. KESIMPULAN

Dari analisa yang telah dilakukan pada serangan dan perilaku hacker menggunakan *High interaction HIHAT* dapat ditarik beberapa kesimpulan diantaranya:

a. Dengan melakukan pemeliharaan sistem aplikasi melalui perbaikan *script* dan memasang *tools* pada *server* untuk mendeteksi serangan oleh *hacker* seperti memasang *Honeypot* pada server.
b. Dengan menerapkan aplikasi *Honeypot* dapat membantu memonitor dan merekam *web* server dari serangan-serangan *hacker* yang mencoba masuk seperti melakukan *SQL Injection*, *XSS*, *Code Injection* dan percobaan untuk melakukan *Inclusion*.

DAFTAR PUSTAKA

[1] Komarrudin. 2005. Ensiklopedia Manajemen, Alumni. Bandung.
[2] Anggeriana, H. 2012. Perancangan Keamanan Cloud Computing Melalui Honeypot Sistem. Surakarta.

Sumber Online

[3] Idsitrii. http://idsirtii.com diakses pada 1 September 2017 pada pukul 10.00
[4] Keraf, Gorys. 2013. http://pengertiandefinisi.com, diakses pada 26 Agustus 2017 pada pukul 23.44.