UJI COBA SISTEM KEAMANAN JARINGAN MENGGUNAKAN *HONEYPOT* DAN SIEM PADA JARINGAN KOMPUTER PT. GLORIA MAJU CAHAYA

TUGAS AKHIR

NAMA : MOHAMAD IQBAL
NIM : 41517120057

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2022

UJI COBA SISTEM KEAMANAN JARINGAN MENGGUNAKAN *HONEYPOT* DAN SIEM PADA JARINGAN KOMPUTER PT. GLORIA MAJU CAHAYA

Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

NAMA : MOHAMAD IQBAL
NIM : 41517120057

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2022

LEMBAR PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini:

NIM	: 41517120057
Nama	: Mohamad Iqbal
Judul Tugas Akhir	: Uji Coba Sistem Keamanan Jaringan Menggunakan *Honeypot* dan Siem Pada Jaringan Komputer PT.Gloria Maju Cahaya

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan di dalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 19 Januari 2022

MOHAMAD IQBAL

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Mohamad Iqbal
NIM	:	41517120057
Judul Tugas Akhir	:	Uji Coba Sistem Keamanan Jaringan Menggunakan *Honeypot* dan Siem Pada Jaringan Komputer PT.Gloria Maju Cahaya

Dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Non Eksklusif** (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul di atas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti/Non Eksklusif ini Universitas Mercu Buana berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya.

Selain itu, demi pengembangan ilmu pengetahuan di lingkungan Universitas Mercu Buana, saya memberikan izin kepada Peneliti di Lab Riset Fakultas Ilmu Komputer, Universitas Mercu Buana untuk menggunakan dan mengembangkan hasil riset yang ada dalam tugas akhir untuk kepentingan riset dan publikasi selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 19 Januari 2022

MOHAMAD IQBAL

SURAT PERNYATAAN LUARAN TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Mohamad Iqbal
NIM	:	41517120057
Judul Tugas Akhir	:	Uji Coba Sistem Keamanan Jaringan Menggunakan *Honeypot* dan Snort Pada Jaringan Komputer PT.Gloria Maju Cahaya

Menyatakan bahwa :

1. Luaran Tugas Akhir saya adalah sebagai berikut :

No	Luaran	Jenis		Status	
1	Publikasi Ilmiah	Jurnal Nasional Tidak Terakreditasi		Diajukan	
		Jurnal Nasional Terakreditasi			
		Jurnal Internasional Tidak Bereputasi		Diajukan	
		Jurnal Internasional Bereputasi			
	Submit/dipublikasikan di :	Nama Jurnal	:		
		ISSN	:		
		Link Jurnal	:		
		Link File Jurnal Jika Sudah di Publish	:		

2. Bersedia untuk menyelesaikan seluruh proses publikasi artikel mulai dari submit, revisi artikel sampai dengan dinyatakan dapat diterbitkan pada jurnal yang dituju.
3. Diminta untuk melampirkan scan KTP dan Surat Pernyataan (Lihat Lampiran Dokumen HKI), untuk kepentingan pendaftaran HKI apabila diperlukan

Demikian pernyataan ini saya buat dengan sebenarnya.

Mengetahui
Dosen Pembimbing TA

Emil R. Kaburuan, Ph.D

Jakarta, 19 Januari 2022

Mohamad Iqbal

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41517120057
Nama	:	Mohamad Iqbal
Judul Tugas Akhir	:	Uji Coba Sistem Keamanan Jaringan Menggunakan *Honeypot* dan Siem Pada Jaringan Komputer PT.Gloria Maju Cahaya

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 19 Januari 2022

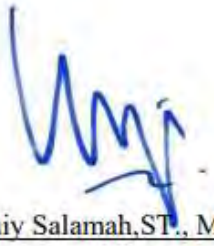
(Vina Ayumi S.Kom.,M.Kom)

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41517120057
Nama	:	Mohamad Iqbal
Judul Tugas Akhir	:	Uji Coba Sistem Keamanan Jaringan Menggunakan *Honeypot* dan Siem Pada Jaringan Komputer PT.Gloria Maju Cahaya

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 2 Februari 2022



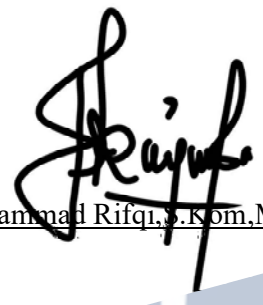
(Umniy Salamah,ST., MMSI)

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41517120057
Nama	:	Mohamad Iqbal
Judul Tugas Akhir	:	Uji Coba Sistem Keamanan Jaringan Menggunakan *Honeypot* dan Siem Pada Jaringan Komputer PT.Gloria Maju Cahaya

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta,19 Januari 2022



(Muhammad Rifqi,S.Kom,M.Kom)

LEMBAR PENGESAHAN

NIM	:	41517120057
Nama	:	Mohamad Iqbal
Judul Tugas Akhir	:	Uji Coba Sistem Keamanan Jaringan Menggunakan *Honeypot* dan Siem Pada Jaringan Komputer PT.Gloria Maju Cahaya

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 19 Januari 2022

Menyetujui,

(Emil R. Kaburuan, Ph.D)
Dosen Pembimbing

Mengetahui,

(Wawan Gunawan, S.Kom, MT)
Koord. Tugas Akhir Teknik Informatika

(Emil R. Kaburuan, Ph.D.)
Ka. Prodi Teknik Informatika

ABSTRAK

Nama	:	Mohamad Iqbal
NIM	:	41517120057
Pembimbing TA	:	Emil R. Kaburuan, Ph.D
Judul	:	Uji Coba Sistem Keamanan Jaringan Menggunakan *Honeypot* dan *Siem* Pada Jaringan Komputer PT.Gloria Maju Cahaya

Keamanan informasi terlalu penting di zaman teknologi sekarang ini. Penyimpanan dan penyebaran informasi saat ini sudah tidak memakai media kertas, tapi banyak memakai teknologi komputer dan internet. Dengan berkembangnya teknologi internet dapat mempermudah pekerjaan dan juga dapat memberikan efisiensi waktu dan tempat tetapi dengan segala manfaatnya yang besar internet tidak serta merta membuat para pengguna merasa aman. di samping kemudahan akses, terdapat pula potensi serta gangguan berbahaya pada jaringan ancaman yang mengintai misalnnya Jenis serangan yang terjadi pada server meliputi *port scan detection, brute force dan Denial-of-Service (DoS)*. Oleh karena itu, dibutuhkan pendeteksi dan pertahanan untuk melawan serangan terhadap jaringan untuk melindungi informasi penting dalam jaringan. Sejalan dengan perkembangan teknologi informasi, peralatan-peralatan pendukung jaringan komputer masih sangat diperlukan. Peralatan tersebut pun kini menjadi komponen penting dalam pembangunan jaringan komputer. Perkembangan teknologi keamanan jaringan saat ini sudah terdapat teknik mendeteksi serangan jaringan seperti *honeypot dan Siem. Honeypot* terdiri dari sistem pencegahan intrusi (*Interruption counteractive action framework*) yang terletak di taraf Penyedia Layanan Internet. *IPS* kemudian membentuk jaring pengaman untuk melindungi data pergerakan yg dipilih. evaluasi *honeypot* mempromosikan reproduksi luas dan gugusan data pasti diperkenalkan, yang membagikan aktivitas *honeypot* serta *overhead* yang rendah. *Honeypot* mengantisipasi agresi semacam itu serta mengurangi server. *IDS* yang berlaku umumnya dimodulasi untuk membedakan agresi sistem tingkat otoritas yang diketahui. Spontanitas ini membentuk sistem *honeypot* kuat melawan serangan pada jaringan *Security information and event management* (*SIEM*) akan memberikan keamanan yang mengadopsi metodologi yang dipergunakan untuk meng korelasi log, peristiwa, mengalir dari komputasi perangkat, sistem dan layanan terdistribusi dengan baseline keamanan (kegiatan pengguna serta aplikasi, kegiatan basis data dan kegiatan jaringan.

Kata kunci:
Honeypot, Security information and event management (*SIEM*), *Denial-of-Service (DoS)* , *port scan detection, brute force ,*ilmu komputer, universitas mercu buana

ABSTRACT

Name	:	Mohamad Iqbal
Student Number	:	41517120057
Counselor	:	Emil R. Kaburuan, Ph.D
Title	:	Uji Coba Sistem Keamanan Jaringan Menggunakan *Honeypot* dan *Siem* Pada Jaringan Komputer PT.Gloria Maju Cahaya

Information security is too important in today's technological age. Currently, the storage and dissemination of information does not use paper media, but uses computer and internet technology a lot. With the development of internet technology, it can make work easier and can also provide time and place efficiency, but with all its great benefits the internet does not necessarily make users feel safe. In addition to the ease of access, there is also the potential and dangerous interference on the network of threats that lurk, for example. Types of attacks that occur on servers include port scan detection, brute force and Denial-of-Service (DoS). Therefore, it takes detection and defense against attacks against the network to protect important information on the network. In line with the development of information technology, computer network support equipment is still very much needed. The equipment is now an important component in the construction of computer networks. The development of network security technology currently includes techniques for detecting network attacks such as honeypot and Siem.

Honeypot consists of an intrusion prevention system (Interruption counteractive action framework) located at the Internet Service Provider level. The IPS then forms a safety net to protect the selected movement data. Honeypot evaluation promotes extensive reproduction and definite data sets are introduced, which provides honeypot activity and low overhead. Honeypot anticipates such attacks and reduces servers. The prevailing IDS is generally modulated to discriminate against known authority level system aggressions. This spontaneity establishes a robust honeypot system against attacks on the network. Security information and event management (SIEM) will provide security that adopts the methodology used to correlate logs, events, flows from computing devices, distributed systems and services with a security baseline (user and application activity, activity). database, network activity.

Keywords:
Honeypot, Security information and event management (SIEM), Denial-of-Service (DoS), port scan detection, brute force, computer science, mercu buana university

KATA PENGANTAR

Puji syukur kita Puji syukur kita panjatkan kepada Tuhan Yang Mahas Esa karena atas berkat dan rahmat-Nya penulis dapat menyelesaikan penyusunan Tugas Akhir ini yang berjudul "UJI COBA SISTEM KEAMANAN JARINGAN MENGGUNAKAN *HONEYPOT* DAN SIEM PADA JARINGAN KOMPUTER PT. GLORIA MAJU CAHAYA" tepat pada waktunya.

Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, penulisan laporan tugas akhir ini tidak dapat diselesaikan. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Keluarga yang selalu support dan mendoakan
2. Bapak Emil R. Kaburuan, Ph.D selaku dosen pembimbing Tugas Akhir Teknik Informatika.
3. Bapak Emil R. Kaburuan, Ph.D selaku Ketua Program Studi Teknik Informatika Fakultas Ilmu Komputer Universita Mercu Buana.
4. Seluruh Dosen Universitas Mercu Buana Fasilkom.
5. Bapak Anto Wijaya selaku Direktur Utama PT Gloria Maju Cahaya yang telah memberikan izin kepada penulis untuk melakukan penelitian di perusahaan yang bapak pimpin
6. Teman-teman Mahasiswa dan Mahasiswi Universitas Mercu Buana.

Akhir kata, penulis berharap Laporan Tuga Akhir ini dapat bermanfaat bagi Mahasiswa Universitas Mercu Buana khususnya dan pembaca pada umumnya.

Jakarta, 19 Januari 2022

Mohamad Iqbal

DAFTAR ISI

NASKAH JURNAL

PENDAHULUAN

Keamanan informasi terlalu penting di zaman teknologi sekarang ini. Penyimpanan dan penyebaran informasi saat ini sudah tidak memakai media kertas, tapi banyak memakai teknologi komputer dan internet. PT. Gloria Maju Cahaya membangun jaringan internet yang dipergunakan untuk mengakses server, yang terdiri dari database server, web application server, dan untuk mengakses aplikasi tersebut PT. Gloria Maju Cahaya membuat akses yaitu melalui akses yang terkoneksi dengan internet. Menurut hasil wawancara dengan bapak Andi Wijaya sebagai staff, pada PT. Gloria Maju Cahaya sering kali terjadi gangguan seperti, akses pada server yang sangat berat, yang tidak dapat diakses dan terkadang tidak dapat masuk ke dalam database server, disebabkan komputer yang terkoneksi pada infrastruktur jaringan dan memiliki akses ke server tidak terjamin bebas virus, spyware, malware, dan semacamnya.

Dari indikasi-indikasi tersebut terdapat kemungkinan jika server tersebut terkena virus dari komputer-komputer yang terkoneksi pada server atau terjadi serangan pada server, baik seperti trojan, DoS attack ataupun DDoS, malware atau yang biasa di sebut perangkat perusak. Apabila terjadi gangguan pada server maka penginputan data akan terganggu dan akan berakibat keterlambatan dikarenakan laporan pada aplikasi dikunci dengan tanggal penginputan dan sangat berbahaya apabila data yang terdapat pada server menjadi rusak atau corrupt.

Perkembangnya teknologi internet dapat mempermudah pekerjaan dan juga dapat memberikan efisiensi waktu dan tempat tetapi dengan segala manfaatnya yang besar internet tidak serta merta membuat para pengguna merasa aman. di samping kemudahan akses, terdapat pula potensi serta gangguan berbahaya pada jaringan ancaman yang mengintai misalnnya Jenis serangan yang terjadi pada server meliputi port scan detection, brute force dan Denial-of-Service (DoS). Oleh karena itu, dibutuhkan pendeteksi dan pertahanan untuk melawan serangan terhadap jaringan untuk melindungi informasi penting dalam jaringan. Sejalan dengan perkembangan teknologi informasi, peralatan-peralatan pendukung jaringan komputer masih sangat diperlukan. Peralatan tersebut pun kini menjadi komponen penting dalam pembangunan jaringan komputer.

Jumlah ancaman dan serangan keamanan cyber selalu meningkat setiap saat, dan seringkali standar keamanan seperti IDS (Intrusion Detection Systems), access control system dan firewall tidak cukup untuk mengamankan server dari penyerang. Karena itu, seorang administrator harus terus belajar dan menganalisis ancaman baru dan metode serangan untuk melawan dan memproteksi dari penyerang dunia maya. Jenis serangan yang terjadi pada server meliputi mencari port yang aktif pada server (port scan detection), membuka akses ke port tertentu (port knocking), percobaan login dengan mencoba kata sandi yang cocok

(brute force) dan serangan DDoS (Distributed Denial of Service).

Honeypot dan Siem dipilih sebagai bentuk dari perbandingan untuk mengatasi serangan pada server ,honeypot mempelajari bagaimana penyerang menembus ke dalam informasi sistem keamanan. Honeypot menjadi alat keamanan siber fundamental untuk mendeteksi, mencegah dan merekam ancaman baru yang digunakan oleh penyerang untuk menembus sistem.Sedangkan *Security Information and Event Management (SIEM) Security Information and Event Management* atau biasa disebut dengan SIEM untuk mendeteksi berbagai ancaman dan insiden dari keamanan dengan mengumpulkan Log real-time dan melakukan analisis sejarah Log keamanan dari berbagai jenis tipe log dan berasal dari berbagai sumber data dari perangkat yang berbeda-beda.

Security information and event management (*SIEM*) akan memberikan keamanan yang mengadopsi metodologi yang dipergunakan untuk meng korelasi log, peristiwa, mengalir dari komputasi perangkat, sistem dan layanan terdistribusi dengan baseline keamanan (kegiatan pengguna serta aplikasi, kegiatan basis data, kegiatan jaringan.

Ancaman serangan *cyber* seperti serangan *brute force* dan DDoS dapat dengan mudah menyerang server. DoS merupakan serangan yang bertujuan untuk mematikan target dengan cara memadati jalur data dengan paket yang ilegal, sedangkan DDoS adalah serangan yang melakukannya secara serempak dengan jumlah komputer yang lebih banyak dengan target yang sama. Serangan DoS memiliki dampak yaitu server akan mengalami down time selama serangan berlangsung. Brute force merupakan ancaman dari penyerang yang mencoba untuk login dengan menggunakan protokol SSH dan Telnet untuk mengungkap password login. Serangan brute force merupakan serangan yang menggunakan algoritma untuk memecahkan masalah yang secara langsung, sederhana dan dengan cara yang jelas. Penyelesaian masalah password dengan menggunakan algoritma brute force dapat dengan mudah mencari password dengan mengkombinasikan

menyediakan akses yang tidak diinginkan ke dalam jaringan komputer perusahaan; (2) *integrity* (integritas) – jaringan komputer yang dapat diandalkan juga berdasar pada fakta bahwa data yang tersedia apa yang

Keamanan jaringan komputer sendiri sering dipandang sebagai hasil dari beberapa faktor yang bervariasi tergantung pada bahan dasar, tetapi Secara normal setidaknya beberapa hal di bawah ini diikutsertakan: (1) *confidentiality* (kerahasiaan) – ada beberapa jenis informasi yang tersedia di dalam sebuah jaringan komputer. Setiap data yang berbeda pasti mempunyai grup pengguna yang berbeda pula dan data dapat dikelompokkan sehingga beberapa pembatasan kepada penggunaan data harus ditentukan. Pada umumnya data yang terdapat di dalam suatu perusahaan bersifat rahasia dan tidak boleh diketahui oleh pihak ketiga yang bertujuan untuk menjaga rahasia perusahaan dan strategi perusahaan. *Backdoor*, sebagai contoh, melanggar kebijakan perusahaan dikarenakan

sudah seharusnya. Jaringan komputer mau tidak mau harus terlindungi dari serangan yang dapat merubah data selama dalam proses transmisi. *Man-in-the-Middle* merupakan jenis serangan yang dapat merubah integritas dari sebuah data yang mana penyerang (*attacker*) dapat membajak *session* atau memanipulasi data yang terkirim; (3) *availability* (ketersediaan) – ketersediaan data atau layanan dapat dengan mudah dipantau oleh pengguna dari sebuah layanan. Ketidaktersediaan dari sebuah layanan dapat menjadi sebuah halangan untuk maju bagi sebuah perusahaan dan bahkan dapat berdampak lebih buruk lagi, yaitu penghentian proses produksi. Sehingga untuk semua aktifitas jaringan, ketersediaan data sangat penting untuk sebuah sistem agar dapat terus berjalan dengan benar (Kelompok 123P, 2005).

Pada beberapa referensi yang dibaca oleh peneliti yaitu jurnal – jurnal terkait mengenai *Honeypot,*

Hasil penelitian ini adalah kombinasi antara *Honeypot* dan *Siem*,diharapkan kombinasi ini dapat memberikan sebuah sistem keamanan *Honeypot* adalah *security resource* yang sengaja dibuat untuk diselidiki, diserang, atau dikompromikan (Firrar Utdirartatmo, 2005:1). Pada umumnya *honeypot* berupa komputer, data atau situs jaringan yang terlihat seperti bagian dari jaringan, tetapi terisolasi dan dimonitor. Uji Coba *honeypot* menggunakan jenis *low-interaction* yaitu *HoneyPy*. *Honeypot* dibangun menyerupai sistem yang sesungguhnya dan dilengkapi dengan *vulnerability* yang sudah diketahui sehingga *attacker* dapat teralih perhatiannya dari sistem utama yang akan diserang dan beralih menyerang ke sistem palsu *honeypot* tersebut.

Subjek penelitian ini adalah penerapan sistem keamanan jaringan komputer. Metode yang digunakan dalam penelitian ini adalah Studi Pustaka (*Library Research*). Analisis dilakukan untuk mendapatkan hasil serta data yang bisa dijadikan sebagai acuan guna menerapkan suatu sistem keamanan jaringan hotspot berbasis *honeypot* dan *Security information and event management* (*SIEM*).
yang berlapis dengan menipu dan memberi informasi mengenai *track record* atau aktivitas yang terjadi.

LANDASAN TEORI

Dalam penyusunan skripsi ini penulis sedikit banyak terinspirasi dan mereferensi dari penelitian-penelitian sebelumnya yang berkaitan dengan latar belakang masalah pada skripsi ini.

" Implementasi *Honeypot* Sebagai sistem keamanan jaringan pada *Virtual Private Server*" Perbandingan keuntungan menggunakan *Honeypot* dari pada *Firewall*, diketahui bahwa apabila menggunakan perangkat keamanan jaringan firewall harus mengeluarkan biaya yang besar seperti pembayaran software yang dilakukan secara berlangganan, sedangkan *Honeypot* tidak memerlukan biaya karena bersifat *open source.*

Penelitian yang dilakukan oleh Citra Arfanudin, Bambang Sugiantoro, Yudi Prayudi,2019," Analisis Serangan Router Dengan *Security Information And Event Management (SIEM)* Dan Implikasinya Pada Indeks Keamanan Informasi"
Penggunaan *SIEM* untuk melakukan monitoring keamanan terbukti dapat memberikan informasi mengenai serangan yang terjadi pada router kepada *security officer*. Akan tetapi tidak semua serangan dapat di kenali oleh *SIEM*. Hanya serangan *DHCP Starvation, DHCP Rogue, SSH Bruteforce dan FTP Bruteforce* dikenali oleh *SIEM*. Sedangkan untuk serangan *Mac Flooding, ARP-Poisoning, CDP Flooding dan Syn Flooding* tidak dapat dikenali oleh *SIEM* karena router tidak mengirim log ke *SIEM*.

2.1 Linux

Gambar 2. Linux

Linux adalah *operating system* (OS) atau sistem operasi yang berbasis GNU/Linux yang bersifat *Open Source* dan memiliki banyak varian seperti Debian, Slackware, Open Suse, Archlinux, Redhat dan sebagainya.

2.2 Honeypot

Honeypot bisa diklasifikasikan sesuai penerapannya (penggunaan / tindakan) dan sesuai taraf keterlibatannya. sesuai penerapan, *honeypot* dapat diklasifikasikan menjadi:

- *Honeypot* Produksi
- penelitian *Honeypot*.

Honeypot produksi mudah digunakan, hanya menangkap isu terbatas, dan dipergunakan terutama oleh perusahaan. *Honeypot*s produksi ditempatkan di dalam jaringan produksi menggunakan server produksi lain oleh organisasi untuk meningkatkan status keamanan mereka secara keseluruhan. umumnya, *honeypot*s produksi merupakan *honeypot*s hubungan rendah, yang lebih simpel diterapkan. Mereka menyampaikan lebih sedikit informasi tentang serangan atau penyerang daripada penelitian *honeypot*.

Penelitian *honeypot* dijalankan buat mengumpulkan informasi tentang motif dan strategi komunitas topi hitam yang menargetkan jaringan yang tidak sama. *Honeypot*s ini tidak menambah nilai langsung ke organisasi eksklusif; sebaliknya, mereka digunakan buat meneliti ancaman yg dihadapi organisasi dan buat mempelajari cara melindungi menggunakan lebih baik dari ancaman tersebut. *Honeypot*s penelitian rumit buat digunakan dan dipelihara, menangkap berita ekstensif, serta digunakan terutama oleh organisasi penelitian, militer, atau pemerintah.

*honeypot*s adalah senjata melawan spammer, sistem deteksi

honeypot adalah senjata balasan yang digunakan oleh spammer. Karena sistem deteksi kemungkinan akan menggunakan karakteristik unik dari *honeypot*s tertentu untuk mengidentifikasinya, seperti pasangan nilai properti dari konfigurasi *honeypot* default, banyak *honeypot*s yang sedang digunakan memanfaatkan serangkaian karakteristik unik yang lebih besar dan lebih menakutkan bagi mereka yang ingin mendeteksi. dan dengan demikian mengidentifikasi mereka. Ini adalah keadaan yang tidak biasa dalam perangkat lunak, situasi di mana "versionitis" (sejumlah besar versi dari perangkat lunak yang sama, semuanya sedikit berbeda satu sama lain) dapat bermanfaat. Ada juga keuntungan dalam menerapkan beberapa *honeypot*s yang mudah dideteksi.

Fred Cohen , penemu Perangkat Penipuan, berpendapat bahwa setiap sistem yang menjalankan *honeypot*nya harus memiliki port penipuan yang dapat digunakan musuh untuk mendeteksi *honeypot*.Cohen percaya bahwa ini mungkin menghalangi musuh.

3.2 Security information and event management (SIEM)

Security information and event management (*SIEM*) adalah sub-bagian dalam bidang keamanan komputer , di mana produk dan layanan perangkat lunak menggabungkan manajemen informasi keamanan (SIM) dan manajemen acara keamanan (SEM). Mereka menyediakan analisis *real-time* dari peringatan keamanan yang dihasilkan oleh aplikasi dan perangkat keras jaringan.

Vendor menjual *SIEM* sebagai perangkat lunak, peralatan, atau sebagai layanan terkelola, produk ini juga digunakan untuk mencatat data keamanan dan menghasilkan laporan untuk tujuan kepatuhan .

Istilah dan inisialisme *SIEM* diciptakan oleh Mark Nicolett dan Amrit Williams dari Gartner pada tahun 2005.

Akronim SEM , SIM dan *SIEM* terkadang digunakan secara bergantian, tetapi umumnya mengacu pada fokus utama produk yang berbeda:

1. Manajemen log : Fokus pada pengumpulan dan penyimpanan sederhana dari pesan log dan jejak audit
2. Manajemen informasi keamanan (SIM): Penyimpanan jangka panjang serta analisis dan pelaporan data log.
3. Manajer peristiwa keamanan (SEM): Pemantauan waktu nyata, korelasi peristiwa, pemberitahuan, dan tampilan konsol.
4. Informasi keamanan dan manajemen acara (*SIEM*): Menggabungkan SIM dan SEM dan memberikan analisis *real-time* dari peringatan keamanan yang dihasilkan oleh perangkat keras dan aplikasi jaringan.
5. Layanan Keamanan Terkelola: (MSS) atau Penyedia Layanan Keamanan Terkelola: (MSSP): Layanan terkelola yang paling umum tampaknya berkembang seputar konektivitas dan bandwidth, pemantauan jaringan, keamanan, virtualisasi , dan pemulihan bencana.
6. Keamanan sebagai layanan (SECaaS) : Layanan keamanan ini sering kali mencakup antara lain otentikasi , anti-virus , anti-malware / *spyware*, deteksi intrusi , pengujian

Penetrasi, dan manajemen peristiwa keamanan.

Dalam praktiknya, banyak produk di area ini akan memiliki campuran fungsi ini, sehingga akan sering terjadi tumpang tindih - dan banyak vendor komersial juga mempromosikan terminologi mereka sendiri.

Seringkali vendor komersial memberikan kombinasi yang berbeda dari fungsi-fungsi ini yang cenderung meningkatkan *SIEM* secara keseluruhan. Manajemen log saja tidak memberikan wawasan waktu nyata tentang keamanan jaringan, *SIEM* sendiri tidak akan menyediakan data lengkap untuk analisis ancaman yang mendalam. Ketika *SIEM* dan manajemen log digabungkan, lebih banyak informasi tersedia untuk dipantau *SIEM*.

METODE PENELITIAN

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian kuantitatif,dimana spesifikasinya adalah sistematis,terencana dan terstruktur dengan jelas sejak awal hingga pembuatan desain penelitian.

1. Metode Pengumpulan Data

Metode yang dilakukan bertujuan agar hasil dari penelitian dan analisa lebih terarah serta data yang diperoleh lebih akurat. Kelengkapan data yang diperoleh dapat memberikan kontribusi dalam proses penyusunan skripsi ini,dan memberikan waktu yang lebih singkat.

Adapun beberapa metode yang dilakukan dalam pengumpulan data terdiri dari :

2. Studi Pustaka

Metode dengan pengumpulan data dengan cara membaca berdasarkan keputusan dari buku,jurnal maupun makalah yang mana di maksudkan untuk mendapatkan teori yang mengenai masalah yang ingin diteliti serta mencari sumber data di internet dan perpustakaan

3. Metode Observasi

Pengumpulan data dengan pengamatan secara langsung pada objek yang diteliti untuk memperoleh informasi yang tepat dan sistematis. Meliputi instalasi ,konfigurasi,tool yang di pakai dan pengujian koneksi terhadap internet.

KERTAS KERJA

Ringkasan

Kertas kerja ini merupakan material kelengkapan artikel jurnal dengan judul di atas. Kertas kerja berisi semua material hasil penelitian Tugas Akhir yang tidak dimuat/atau disertakan di artikel jurnal. Di dalam kertas kerja ini disajikan:

1. Literature review
2. Analisis dan Perancangan sistem
3. Konfigurasi
4. Tahapan eksperimen
5. Hasil eksperimen secara keseluruhan.