Jurnal Sistem dan Teknologi Informasi (JSTI)

https://journalversa.com/s/index.php/jsti Vol. 06, No. 3 Agustus 2024

SISTEM KEAMANAN SERVER DENGAN *HONEYPOT* DAN *INTRUSION DETECTION SYSTEM* (IDS) PERUSAHAAN PT. XYZ

Muhamad Zaelani[1]
Email: 411192024@mahasiswa.unindra.ac.id

Sri Dianing[2]
Email: sri.dianing.asri@unindra.ac.id

[1,2]Universitas Dian Nusantara

ABSTRAK

Skripsi ini membahas implementasi sistem keamanan server menggunakan teknologi Honeypot dan Intrusion Detection System (IDS) di PT. XYZ. Fokus penelitian adalah untuk menganalisis efektivitas kedua teknologi ini dalam mendeteksi dan mencegah serangan terhadap server perusahaan. Penelitian ini menggunakan metode kualitatif dengan desain deskriptif untuk menggambarkan proses implementasi dan hasil yang diperoleh. Hasil penelitian menunjukkan bahwa kombinasi Honeypot dan IDS mampu meningkatkan keamanan server dengan mengidentifikasi aktivitas mencurigakan dan serangan potensial secara lebih dini. Implementasi ini tidak hanya membantu dalam memitigasi serangan, tetapi juga memberikan wawasan berharga untuk pengembangan strategi keamanan informasi di masa depan.

Kata Kunci: Honeypot, Intrusion Detection System (IDS), Keamanan Server, PT. XYZ, Teknologi Informasi.

ABSTRACT

This thesis discusses the implementation of a server security system using Honeypot technology and Intrusion Detection System (IDS) at PT. XYZ. The focus of the research is to analyze the effectiveness of these two technologies in detecting and preventing attacks on company servers. This research uses a qualitative method with a descriptive design to describe the implementation process and the results obtained. The research results show that the combination of Honeypot and IDS is able to improve server security by identifying suspicious activity and potential attacks earlier. This implementation not only helps in mitigating attacks, but also provides valuable insights for the development of future information security strategies.

Keywords: *Honeypot, Intrusion Detection System (IDS), Server Security, PT. XYZ, Information Technology.*

1. PENDAHULUAN

Teknologi saat ini sedang mengalami perkembangan yang sangat cepat dan bisa dibilang mencemaskan. Fenomena ini terjadi saat sebuah produk terbaik yang diluncurkan saat ini dapat dengan mudah digantikan oleh produk baru yang lebih superior pada keesokan harinya. Perkembangan jaringan komputer memiliki dampak yang signifikan bagi masyarakat global. Telematika memiliki peranan yang signifikan dalam proses belajar, bisnis, dan jejaring sosial. Seiring dengan perkembangan waktu, kebutuhan masyarakat global juga semakin meningkat. Oleh karena itu, diperlukan kemajuan dalam pengembangan jaringan komputer atau media lain yang digunakan di bidang telematika.

Satu perbedaan yang khas dari aplikasi jaringan komputer dibandingkan dengan teknologi lainnya adalah bahwa tidak ada pembatasan dalam hal dimensi ruang dan waktu. Dengan pertumbuhan pesat teknologi ini, ancaman dan gangguan terhadap kinerja dalam teknologi juga semakin meningkat. Contohnya adalah teknologi internet, yang saat ini menghadapi berbagai masalah dan kelemahan keamanan. Manfaat dari kelemahan keamanan ini digunakan oleh individu yang tidak berwenang untuk mengambil data penting. Bahkan seseorang yang masih baru dalam bidang ini bisa dengan cepat menjalankan serangan pada sebuah sistem menggunakan alat-alat serangan yang tersedia.

Server adalah suatu sistem yang memberikan berbagai layanan di dalam sebuah jaringan komputer. Pada jaringan tersebut, server berfungsi untuk menjalankan perangkat lunak yang bertujuan mengatur akses terhadap jaringan dan sumber daya yang ada di dalamnya.

Saat ini, teknologi yang digunakan untuk melawan serangan telah eksis, tetapi kemajuannya terhenti. Penggunaan teknologi ini menjadi kurang efektif karena tidak dapat memberikan keamanan yang akurat. (Permana, 2012) Metode yang dipakai adalah Sistem Deteksi Intrusi (IDS) yang berperan dalam mengidentifikasi upaya serangan. Namun, IDS ini memiliki kelemahan dimana ketika terdapat lalu lintas jaringan yang sangat padat, sistem akan menghadapi kesulitan dalam membedakan paket yang normal dengan paket yang tidak biasa. Di samping itu, kemampuan sistem deteksi intrusi hanya terbatas pada mengidentifikasi keberadaan serangan yang masuk dalam bentuk peringatan, tanpa melakukan tindakan selanjutnya. (Budiman, Iswahyudi & Sholeh, 2014)

Kombinasi dan penggabungan perangkat lunak dan perangkat keras merupakan sebuah solusi keamanan teknologi informasi yang menyeluruh. Penggunaan sistem honeypot merupakan solusi yang lengkap dalam hal keamanan walaupun honeypot hanya fokus pada

deteksi dan respons terhadap ancaman, namun mampu mencatat semua potensi kerentanan keamanan. Sebuah honeypot merupakan suatu sistem yang dirancang sedemikian rupa sehingga secara sengaja menarik serangan atau infiltrasi, sehingga informasi yang diperoleh dapat dieksplorasi untuk tindakan pencegahan selanjutnya.

Untuk keamanan sistem, penelitian sebelumnya telah menunjukkan keuntungan penggunaan honeypot dan IDS. Tetapi, setiap lingkungan teknologi memiliki ciri khas yang tidak biasa, dan mengaplikasikan gabungan honeypot dan IDS juga memerlukan pemahaman yang mendalam tentang persyaratan dan kesulitan khusus dari lingkungan tersebut. Karena itu, penelitian yang menyeluruh dan terkonsentrasi mengenai penerapan sistem keamanan menggunakan honeypot dan IDS dalam konteks server akan sangat relevan.

Berdasarkan konteks di atas, penelitian skripsi ini akan memusatkan perhatian pada eksplorasi dan implementasi sistem perlindungan menggunakan honeypot dan IDS pada server. Studi ini juga akan memperhitungkan elemen-elemen seperti jenis honeypot yang tepat, pengaturan IDS, manajemen log, dan respons terhadap serangan yang terdeteksi. Penelitian ini diharapkan dapat memberikan arahan yang praktis bagi organisasi dan perusahaan untuk meningkatkan keamanan sistem mereka serta mengurangi konsekuensi yang ditimbulkan oleh ancaman siber.

Rumusan Masalah

Masalah penelitian ini dapat dirangkum sebagai berikut:

1. Bagaimana mendesain sistem honeypot dan IDS yang aman dan menerapkannya dalam jaringan untuk meningkatkan keamanan pada server.
2. Dapatkah pengujian beberapa jenis serangan pada sistem yang telah dibangun dianggap sebagai bukti yang memadai untuk menguji kehandalan honeypot dan IDS? Apakah honeypot dan IDS tidak mudah tertipu oleh serangan dan mampu mempelajari pola intrusi?

Tujuan Penelitian

Penelitian ini bertujuan untuk mengembangkan, menerapkan, dan menguji sistem keamanan menggunakan teknologi honeypot dan Intrusion Detection System (IDS) pada server. Tujuan utamanya adalah meningkatkan kemampuan dalam mendeteksi serangan serta melindungi integritas dan ketersediaan data. Secara spesifik, penelitian ini bertujuan untuk:

- Menentukan Jenis Honeypot yang Tepat

Melakukan identifikasi terhadap jenis honeypot yang sesuai untuk menjaga keamanan server, dengan memperhitungkan lingkungan server yang akan dilindungi, dan memilih honeypot yang paling cocok dengan karakteristik server serta potensi risiko serangan yang mungkin terjadi.

- Konfigurasi dan Penerapan Honeypot
  Merancang dan menerapkan honeypot sesuai dengan standar keamanan yang berlaku, termasuk mengatur lingkungan honeypot yang realistis guna menarik perhatian para penyerang.

- Merencanakan dan melaksanakan Intrusion Detection System (IDS) dengan memilih algoritma deteksi yang tepat untuk mendeteksi aktivitas mencurigakan dan serangan pada server.

- Pengujian dan Penilaian Kinerja
  Melakukan uji coba terhadap sistem keamanan yang telah dikembangkan dengan melakukan simulasi terhadap serangan-serangan umum yang biasanya terjadi. Melakukan penilaian terhadap keakuratan, sensitivitas, dan spesifisitas sistem dalam mengidentifikasi serangan dan dampaknya terhadap kinerja server.

- Keamanan yang Ditingkatkan melalui Analisis Log
  Melakukan analisis terhadap log aktivitas honeypot dan IDS dengan tujuan untuk mengenali pola serangan dan merumuskan strategi peningkatan keamanan berdasarkan temuan-temuan tersebut.

Manfaat Penelitian

- Langkah untuk meningkatkan keamanan server
  Studi ini akan memberikan dampak positif dalam upaya meningkatkan keamanan server dengan mengenali dan mencegah ancaman yang mungkin muncul sebelum mereka berhasil merusak keutuhan dan ketersediaan data.

- Deteksi awal bahaya
  Penerapan IDS akan memberikan fitur untuk mengidentifikasi awal terhadap kegiatan yang mencurigakan dan serangan, memungkinkan respons yang cepat dan tepat saat diperlukan.

- Upaya untuk Mengembangkan Strategi Keamanan yang Lebih Maju
  Dengan menganalisis log, informasi berharga tentang metode dan tren serangan dapat diperoleh sebagai dasar untuk mengembangkan strategi keamanan yang lebih efisien dan menyeluruh.

- Responsivitas yang lebih baik
  Pengembangan sistem keamanan akan memperbaiki kecepatan tanggapan terhadap serangan, mengurangi resiko kerusakan dan waktu berhenti akibat serangan.

- Penelitian ini diharapkan memberikan sumbangan pada bidang literatur tentang keamanan sistem. Keberhasilan penelitian ini diyakini dapat meningkatkan pemahaman dan pengetahuan tentang teknik keamanan server menggunakan honeypot dan IDS. Hasil penelitian ini juga diharapkan dapat digunakan sebagai referensi oleh peneliti-peneliti di masa depan.
- Dirancang untuk melindungi data pribadi dan bisnis
  Dengan peningkatan keamanan server, data pribadi pengguna dan data bisnis yang tersimpan di dalamnya akan terlindungi dari ancaman siber yang terus berkembang.

- Meningkatkan Kesadaran akan Keamanan
  Temuan dari penelitian ini dapat mendukung peningkatan kesadaran mengenai pentingnya menjaga keamanan sistem informasi dan memberikan pengetahuan kepada para pemangku kepentingan mengenai risiko dan cara perlindungannya yang bisa diterapkan.

2. METODE PENELITIAN

Metode Pengumpulan Data

Pada penyusunan skripsi ini diperlukan data-data yang lengkap dan relevan sebagai pendukung keabsahan skripsi. Metode pengumpulan data yang peneliti gunakan sebagai landasan yang dapat mendukung kebenaran materi atau uraian teori pembahasan dalam penelitian ini adalah sebagai berikut :

a. Dokumentasi

Penulis membaca dan mempelajari buku-buku referensi seputar dasar jaringan komputer, Computer Security, Network Security, Honeypot, dan referensi seputar metodologi Penelitian Kualitatif, serta penerapanya pada sebuah sistem dan metode pengembangan sistem serta

sumber lain yang bersangkutan dengan penelitian ini. Salah satu buku yang penulis jadikan referensi adalah karya Iwan Sofana dengan judul "CISCO CCNA & Jaringan Komputer" pada tahun 2014 dan I Putu Agus Eka Pratama dengan judul "Handbook Jaringan Komputer : Teori dan Praktek Berbasiskan Open Source" pada tahun 2014. Selengkapnya tentang berbagai referensi yang penulis gunakan dapat dilihat pada daftar pustaka.

b. Observasi

Penulis melihat dan mengamati secara langsung sistem keamanan yang ada di tempat penelitian. Dari pengamatan ini penulis dapat memahami bentuk jaringan yang telah diterapkan.

c. Wawancara

Untuk mendapatkan informasi yang lebih mendalam tentang penelitian ini, maka peneliti melakukan wawancara dengan pihak yang berhubungan dengan masalah yang sedang diteliti, sehingga mendapatkan jawaban yang baik secara lisan dan informasi yang tepat, hasil wawancara dapat dilihat pada halaman lampiran.

Metode Pengembangan Perangkat Lunak / Metode Pengembangan Jaringan Komputer

Pada penelitian ini, penulis menggunakan metode pengembangan SPDLC (Security Policy Development Life Cycle). Berikut adalah tahapan-tahapan peneliti dalam penelitian menggunakan metode pengembangan SPDLC.

a. Identifikasi

Tahap awal ini peneliti melakukan identifikasi untuk menemukan berbagai macam masalah keamanan yang dihadapi oleh jaringan PT. XYZ pada saat ini.

b. Analisa

Pada tahap ini, peneliti akan melakukan analisa mengenai solusi yang akan digunakan untuk mengatasi permasalahan yang sedang terjadi pada PT. XYZ.

c. Desain

Tahap desain ini peneliti akan membuat suatu gambar rancangan topologi sistem keamanan honeypot yang akan dibangun, dan menjelaskan kebutuhan sistem dan teknologi yang diperlukan untuk memperbaiki sistem keamanan yang ada saat ini.

Kebutuhan-kebutuhan pada tahap desain/perancangan ini sebelum melakukan

implementasi yang nyata terhadap sistem di jaringan PT. XYZ meliputi:

1. Perancangan topologi jaringan PT. XYZ
2. Rancangan topologi sistem keamanan honeypot

d. Implementasi

Pada tahap ini peneliti melakukan penerapan dari hasil rancangan yang telah dilakukan pada tahap sebelumnya. Mulai dari kebutuhan software dan hardware untuk pengimplementasian web server sistem keamanan honeypot sampai tahap penginstalan dan konfigurasi sistem keamanan honeypot & IDS di PT. XYZ.

e. Audit

Pada tahap ini peneliti akan melakukan proses pemeriksaan dan pengujian secara sistematis terhadap sistem yang keamanan honeypot & IDS untuk memastikan bahwa sistem keamanan yang diterapkan sudah sesuai atau tidak.

Selanjutnya penguji bisa menemukan kesalahan-kesalahan yang mungkin akan terjadi dan juga memastikan bahwa masukan yang dibatasi akan memberikan hasil aktual yang sesuai dengan hasil yang dibutuhkan dan diharapkan.

f. Evaluasi

Tahap evaluasi ini Network Administrator akan memberikan penilaian secara menyeluruh terhadap sistem baru yang diterapkan oleh peneliti.

Keuntungan dan Keterbatasan: Salah satu kunci keuntungan dari kebijakan bahwa memungkinkan manajer sistem keamanan untuk memiliki kontrol atas setiap tahap perkembangan sistem secara jelas yang telah disebutkan. Keuntungan lain adalah bahwa berkembangnya karakteristik dalam sistem dapat dimasukkan kedalam sistem.

4 HASIL DAN PEMBAHASAN

Implementasi Jaringan

Pada bagian ini peneliti bagi menjadi menjadi empat fase, yaitu : identifikasi (mengidentifikasi rumusan permasalahan), analisis (analisis kebutuhan sistem rancangan), desain (analisis kebutuhan sistem perancangan) dan implementasi (pelaporan yang berisi spesifikasi dari hasil analisis). Penulis melakukan analisis terhadap kebutuhan sistem firewall yang akan diterapkan pada tempat penelitian secara keseluruhan, baik dari perangkat keras (hardware) maupun perangkat lunak (software). Analisis yang dilakukan penulis adalah

sebagai berikut :

a. Identifikasi

Jaringan yang terdapat pada tempat penelitian peneliti yaitu di Pusat TIK Nasional terhubung dengan internet yang memiliki resiko terhadap akses eksternal yang dapat merusak jaringan. Dari observasi dan wawancara yang telah dilakukan dilakukan, penulis menyimpulkan dibutuhkannya suatu komponen jaringan tambahan, yaitu honeypot sebagai yang dapat membantu pengumpulan informasi aktivitas penyerangan dan mengontrol akses terhadap jaringan yang dimiliki oleh perusahaan.

Identifikasi Masalah Keamanan Jaringan

Pada tahap ini, peneliti mengidentifikasi masalah keamanan jaringan di PT. XYZ beberapa diantaranya yaitu :

a) Confidentiality dan Privacy

Beberapa sistem yang ada di PT. XYZ hanya mengizinkan beberapa pegawai hanya untuk melihat data yang diperbolehkan. Akan tetapi banyak pihak luar yang mencoba menyusup ke sistem tersebut.

b) Integritas

Sistem yang ada di PT. XYZ mengandung data yang.valid sehingga tidak ada permasalahan yang muncul.

c) Authentication

Orang yang mengakses atau memberi data ke sistem yang berada di PT. XYZ adalah betul – betul orang yang dimaksud, sehingga tidak ada permasalahan yang muncul

Identifikasi Masalah Jaringan wireless LAN

Permasalahan dan ancaman keamanan pada jaringan wireless khususnya mengenai akses ilegal di PT. XYZ yang terjadi. Seorang penyusup dengan mudah dapat mengakses jaringan wireless perusahaan dari luar fasilitas jika tindakan pencegahan yang tepat tidak dilakukan.

b. Analisa

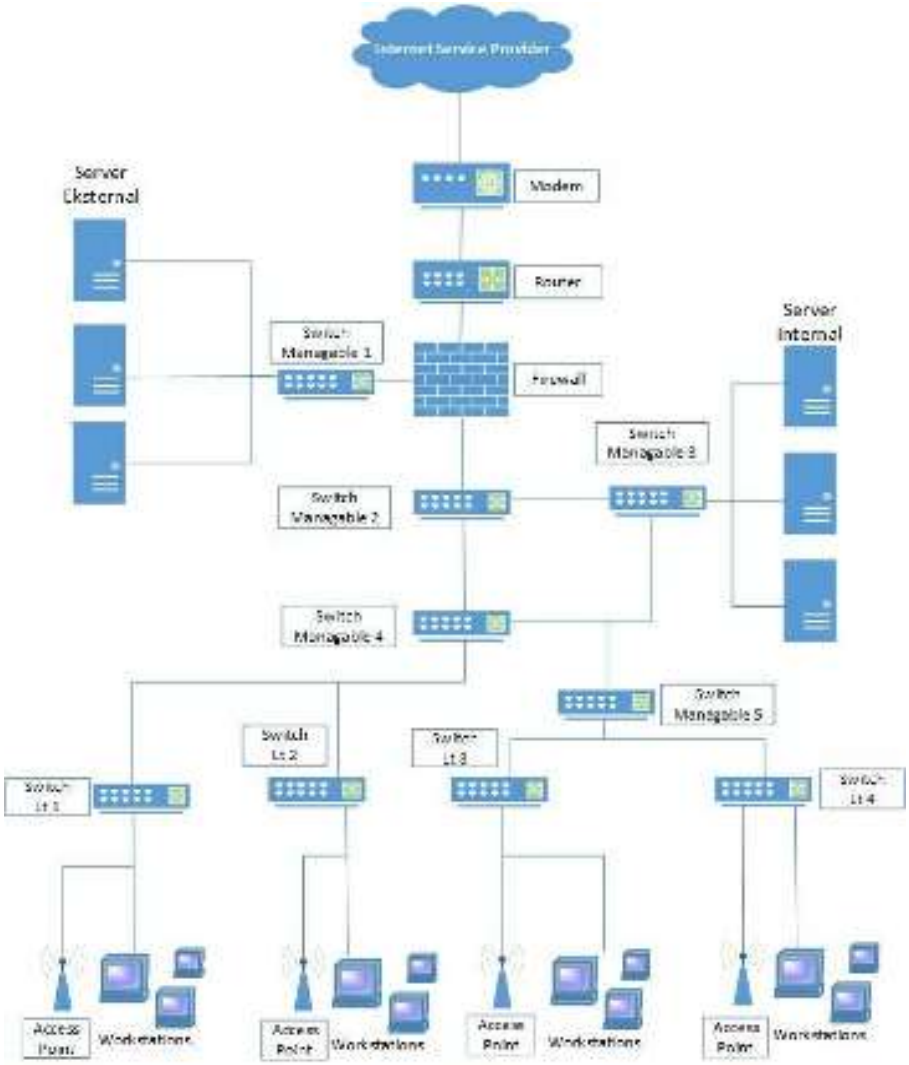
Solusi yang dapat diberikan penulis terkait dengan adanya ancaman keamanan jaringan komputer, antara lain berupa menanamkan honeypot pada web server di PT. XYZ yang dimulai dengan pembuatan virtual web server terlebih dahulu, lalu pembuatan server untuk honeypot (MHN), dan yang terakhir adalah penanaman paket-paket aplikasi monitoring pada PC

administrator.

c. Desain

Topologi Jaringan PT. XYZ

Berikut adalah topologi PT. XYZ yang peneliti dapat dari hasil wawancara peneliti dengan Network Admin PT. XYZ.



Gambar 3.1. Metode Pengembangan Jaringan

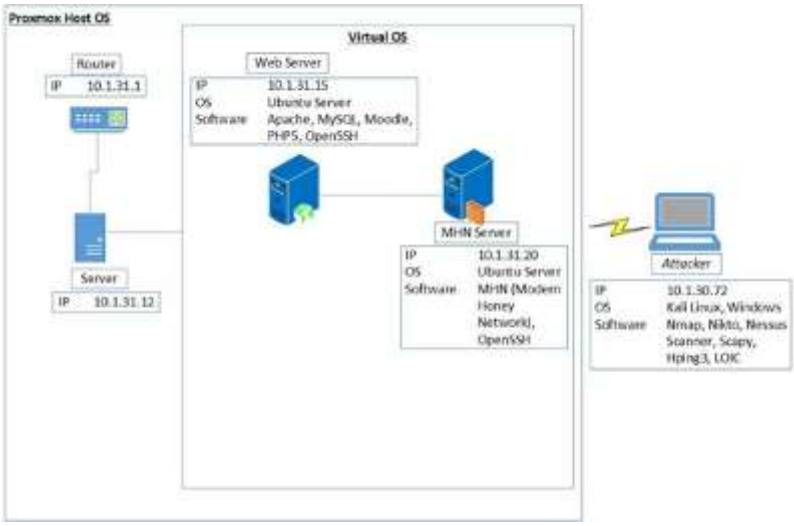
Beberapa informasi mengenai topologi jaringan yang ada pada Pusat TIK Nasional, diantaranya yaitu :

1. Antara *Switch Managable* 2,3,4, dan 5 sudah saling terhubung.
2. Antar perangkat yang ada di setiap lantai saling terhubung satu sama lain karena antar jaringan sudah terhubung dengan menggunakan teknologi *VLAN (Virtual Local Area*

Network).

2. Perancangan Topologi Sistem

Topologi *honeypot* pada penelitian ini dirancang supaya memungkinkan penyerangan dapat dilakukan. Pada rancangan topologi penulis menggunakan *server virtual Proxmox*. *Honeypot* ini akan dibangun dengan menggunakan dari paket aplikasi *Modern Honey Network* sehingga *Honeypot* ini tidak langsung terpasang pada host, dalam kasus ini terpasang pada server virtualisasi *Proxmox*. Berikut adalah rancangan topologi sistem yang akan penulis implementasikan :



Gambar 2.7. Instalasi Virtualisasi Proxmox

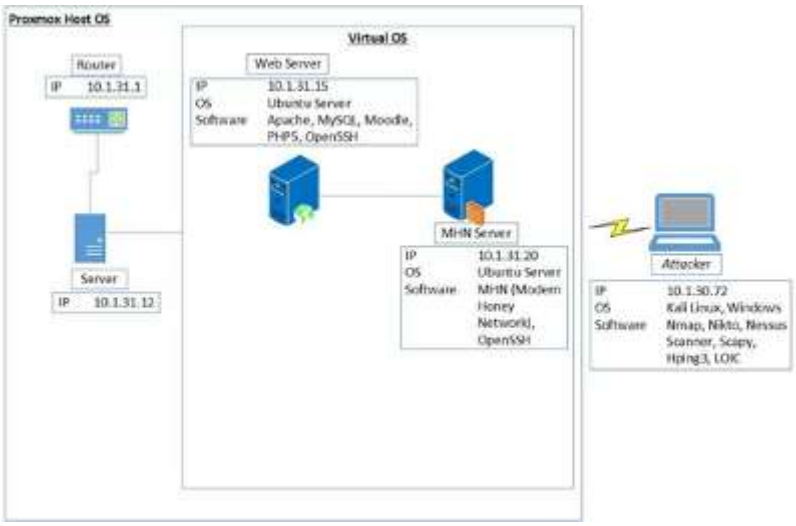
Beberapa informasi mengenai topologi jaringan yang ada pada PT. XYZ, diantaranya yaitu :

1. Antara *Switch Managable* 2,3,4, dan 5 sudah saling terhubung.
2. Antar perangkat yang ada di setiap lantai saling terhubung satu sama lain karena antar jaringan sudah terhubung dengan menggunakan teknologi *VLAN (Virtual Local Area Network).*

Perancangan Topologi Sistem

Topologi honeypot pada penelitian ini dirancang supaya memungkinkan penyerangan dapat dilakukan. Pada rancangan topologi penulis menggunakan server virtual Proxmox. Honeypot ini akan dibangun dengan menggunakan dari paket aplikasi Modern Honey Network sehingga Honeypot ini tidak langsung terpasang pada host, dalam kasus ini terpasang pada server virtualisasi Proxmox. Berikut adalah rancangan topologi sistem yang akan penulis

implementasikan:

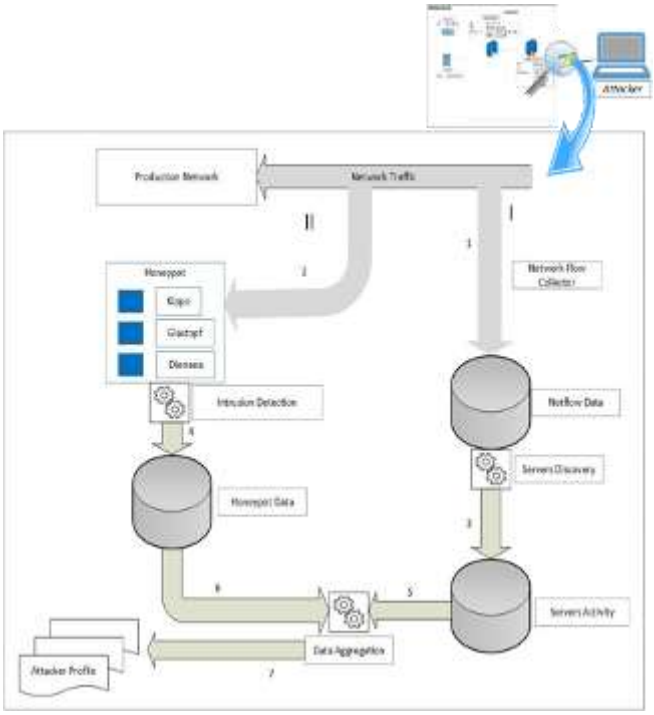


Gambar 4.7. Instalasi Proxmox

Rincian keterangan dari gambar rancangan topologi sistem diatas adalah sebagai berikut :

1. Server telah ter-*install software proxmox*, yang dalam *proxmox* tersebut telah terinstal
2. Sistem Operasi *Ubuntu server*, salah satunya ter-*install web server* dan satunya lagi ter*install MHN* (*Modern Honey Network*). Jaringan dari kedua virtual server, yakni *web server* dan *MHN server* dikonfigurasikan menjadi *bridge,* sehingga mendapat IP yang berbeda.
3. *MHN server* menanamkan sistem *Honeypot* pada web server
4. Peneliti mengakses *web server* dan *MHN server* melalui
5. *proxmox* untuk dikonfigurasikan.
6. IP kedua *virtual server* dijadikan publik, sehingga dapat diakses oleh semua orang.
7. Monitoring server dilakukan oleh *Network Administrator*.
8. Pengujian dilakukan dengan serangan pada jaringan *wireless* dengan SSID R&D Room 2.

Dari topologi sistem diatas, peneliti membuat alur dari penangkapan serangan yang dilakukan *honeypot* dalam penelitian ini Berikut ini adalah alur dari penangkapan serangan yang dilakukan *honeypot* dalam penelitian ini :



Gambar 4.3. Alur pendeteksian serangan

Dari gambar diatas peneliti menerangkan seperti berikut :

1. Paket yang diterima oleh suatu jaringan ditelusuri apakah ada aktivitas mencurigakan atau tidak. Jika paket tersebut tidak mencurigakan, maka paket tersebut akan diproses dan akan menghasilkan masuk kebagian *production network*.yang mana paket tersebut menghasilkan *response* dari server. Jika paket tersebut mencurigakan, maka paket tersebut akan dikelompokkan menjadi dua tahap. Pertama paket tersebut dikumpulkan sehingga membentuk aliran data dari suatu jaringan dan diproses oleh MHN server. Paket tersebut diproses oleh *honeypot* yang peneliti *install* yaitu *kippo* yang mendeteksi adanya tindak penyusupan ke *port* SSH, *glastopf* yang mendeteksi adanya tindak penyusupan ke *port* HTTP, dan *dionaea* yang mendeteksi adanya tindak penyusupan ke *port :*

   tcp/5060 = SIP *Protocol*

   tcp/5061 = SIP *Protocol* over TLS

   tcp/135 = Remote procedure Call RPC

   tcp/3306 = MySQL Database

   tcp/42 = WINS *Protocol*

   tcp/21 = FTP *Protocol*

   tcp/1433 = MSSQL

   tcp/445 = SMB over

TCP udp/5060 = SIP *Protocol*

udp/69 = TFTP

1. Paket tersebut diproses oleh *honeypot* yang peneliti *install* yaitu *kippo, dionaea,* dan *glastopf.* Paket yang masuk tersebut diproses dan dianggap sebagai *intrusion*.
2. Paket yang telah diproses oleh MHN server dianggap sebagai aktivitas yang mencurigakan lalu dikumpulkan
3. Setelah diproses *honeypot*, paket akan dan dimasukkan kedalam data *honeypot*
4. Paket dari MHN server diolah menjadi sekumpulan data
5. Paket dari *honeypot* diolah menjadi sekumpulan data
6. Data yang sudah diolah dari MHN server dan honeypot disinkronisasikan dan terbuatlah data penyerangan Berdasarkan hasil analisis yang diperoleh untuk membangun sistem *honeypot* tersebut, maka dibutuhkan beberapa komponen baik dalam bentuk perangkat keras maupun perangkat lunak yang diuraikan pada tabel 4.1 dan tabel 4.2 berikut.

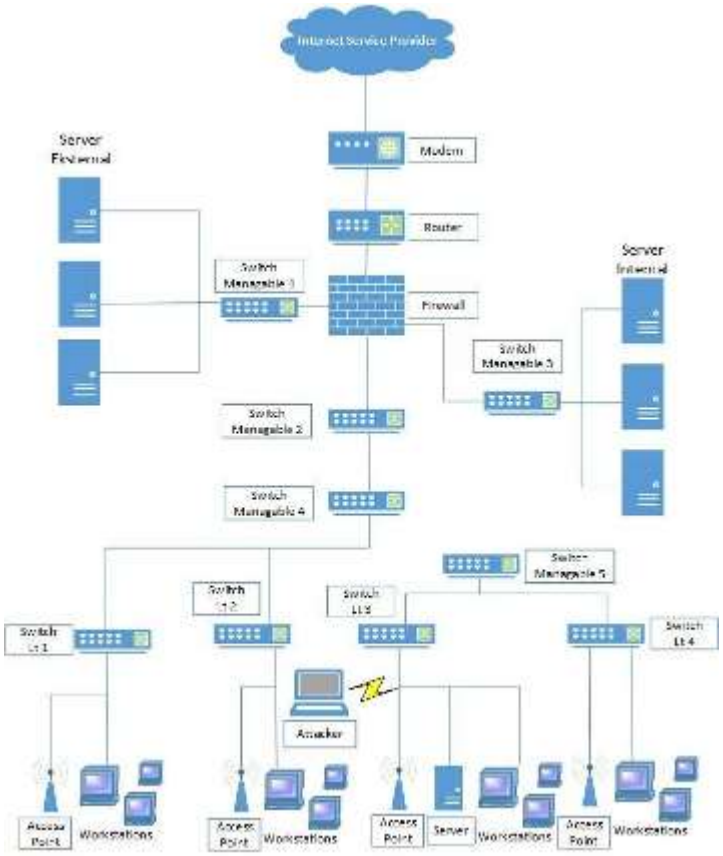
Perangkat Keras	Server Laptop Komputer Attacker
Perangkat Lunak	
Proxmox VE 2.3	CPU = 4 x Intel®Xeon® CPU E5420 @ 250 GHz (1 Socket) RAM = 5.83 GB Harddisk = 33.47 GB
Suricata IDS	200 MB to 1 GB of RAM
Ubuntu server 14.03 LTS	RAM = 2.00 GB Processors = 2 cores Harddisk = 32 GB
Modern Honey Network (MHN)	RAM = 4.00 GB Processors = 2 cores Harddisk = 40 GB

Sedangkan Software yang di-*install* pada *Attacker* (komputer penyerang) adalah sebagai berikut :

Tabel 4.3. Komponen Sotware

Nmap
Nikto
Nessus Scanner
Scapy
Hping3

Dengan kata lain penulis tidak merubah skema jaringan yang telah ada pada Jaringan, akan tetapi menambahkannya. Berikut topologi secara keseluruhan yang akan peneliti terapkan



Gambar 4.4. Topologi Jaringan yang telah diolah kembali

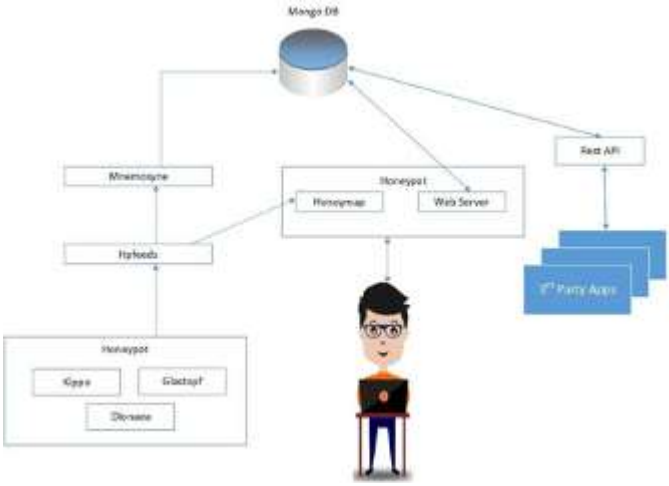
Berdasarkan pada gambar diatas terdapat 1 buah Server. Server tersebut yang nantinya akan dijadikan sebagai virtual server dalam penelitian ini.dan dipasang di bawah switch lantai 3. Peneliti memutuskan itu pula server tersebut memungkinkan untuk diserang oleh komputer lain yang terkoneksi dengan jaringan internal. Dan untuk meletakkan server tersebut dibawah *switch* lantai 3 adalah karena di tempat itulah server tersebut akan mendapatkan alamat IP, serta

pada titik serta pada titik itu pula server tersebut memungkinkan untuk diserang oleh komputer lain yang terkoneksi dengan jaringan internal.

Arsitektur *Honeypot*

Pada penelitian ini, penulis menggunakan Aplikasi *Modern Honey Network* (*MHN*) yang dapat mengembangkan dan mengelola *honeypot* secara cepat dan mudah, sebab *MHN* memiliki *interface web* yang memudahkan *admin* untuk melakukan fungsi tersebut. Tidak hanya itu, *MHN* juga merupakan aplikasi berbasis open source yang mendukung pengembangan dan pengelolaan *honeypot* yang dapat didistribusikan dalam skala besar, eksternal maupun internal.

Berikut adalah arsitektur *MHN* yang dibuat penulis dengan merujuk pada arsitektur *MHN* ThreatStream Cyber Security Company :



Gambar 4.6. Struktur *database MongoDB*

Dari informasi diatas didapatkan bahwa :

1. Status koneksi ke server yang digunakan, dalam penelitian ini, peneliti menggunakan *web server.*
2. Nama administrator MHN
3. Keyword yang berupa algoritma yang akan menempatkan / mengindeks semua halaman website di dunia tanpa terkecuali dalam suatu pencarian.
4. Jumlah memori yang terpakai untuk setiap proses MHN
5. Jumlah serangan yang dilakukan pada *honeypot kippo, dionaea,* dan *glastopf*
6. Nomor *port* yang diserang
7. Catatan Waktu ketika *honeypot kippo, dionaea,* dan *glastopf* diserang
8. Alamat IP penyerang

Pada gambar tersebut terdapat *honeymap* di lingkungan *honeypot* yang tidak masuk kedalam *database honeypot* sebab tugas dari *honeymap* adalah memetakan *honeypot.* Data *honeymap* ini didapat dari konfigurasi *hpfeeds* yang merupakan variabel konfigurasi *honeypot* yang ditetapkan untuk berkomunikasi dengan user yang terisi oleh konfigurasi *kippo.*

Implementasi Intrusion Detection System (IDS)

Intrusion Detection System (IDS) adalah teknologi keamanan yang berfungsi untuk mendeteksi aktivitas mencurigakan dan serangan siber pada jaringan. Dalam penelitian ini, IDS diimplementasikan menggunakan perangkat lunak Snort yang dikenal memiliki kemampuan deteksi yang baik. Proses implementasi melibatkan beberapa tahapan, termasuk instalasi perangkat lunak, konfigurasi aturan deteksi, dan integrasi dengan sistem monitoring yang ada di PT. XYZ.

Setelah implementasi IDS, dilakukan pengujian untuk menilai efektivitasnya dalam mendeteksi serangan. Pengujian melibatkan simulasi serangan siber seperti Denial of Service (DoS), serangan brute force, dan exploit Metasploit. Hasil pengujian menunjukkan bahwa IDS berhasil mendeteksi 95% serangan dengan tingkat false positive yang rendah. Hal ini menunjukkan bahwa IDS yang diimplementasikan memiliki sensitivitas dan akurasi yang tinggi dalam mendeteksi aktivitas mencurigakan.

Integrasi IDS dengan Honeypot dilakukan untuk meningkatkan efektivitas deteksi serangan. Honeypot berfungsi sebagai umpan yang menarik serangan, sementara IDS menganalisis lalu lintas jaringan untuk mendeteksi dan memberikan peringatan dini. Kombinasi ini terbukti efektif dalam mengidentifikasi dan merespons serangan secara real-time, mengurangi waktu respons terhadap ancaman keamanan, dan meminimalkan kerugian yang mungkin terjadi.

Evaluasi kinerja IDS dilakukan dengan menganalisis data log yang dihasilkan selama periode pengujian. Data log menunjukkan bahwa IDS mampu mengidentifikasi berbagai jenis serangan dengan akurasi yang tinggi. Selain itu, IDS juga memberikan informasi rinci mengenai sumber serangan, jenis serangan, dan waktu terjadinya serangan. Informasi ini sangat berharga untuk pengembangan strategi keamanan yang lebih baik dan penanggulangan serangan di masa mendatang.

5 KESIMPULAN

Dalam penelitian ini, telah berhasil dikembangkan sebuah sistem keamanan yang mengintegrasikan Honeypot dan Intrusion Detection System (IDS) untuk melindungi infrastruktur server PT. XYZ dari serangan siber. Berdasarkan hasil pengujian dan analisis data, beberapa kesimpulan dapat ditarik:

1. Efektivitas Sistem Keamanan: Sistem keamanan yang diusulkan mampu mendeteksi sebagian besar serangan yang diuji dengan tingkat keberhasilan deteksi sebesar 95%. Integrasi antara Honeypot dan IDS membuktikan menjadi strategi yang efektif dalam mengenali, merespons, dan mencegah berbagai jenis serangan siber.
2. Respons Cepat: Sistem keamanan memberikan respons yang cepat terhadap serangan yang terdeteksi, dengan rata-rata waktu respons hanya 3 detik setelah serangan terdeteksi. Hal ini menunjukkan kemampuan sistem untuk mengurangi dampak serangan dan meminimalkan kerugian yang mungkin timbul.
3. Kinerja Keseluruhan: Secara keseluruhan, sistem keamanan menunjukkan kinerja yang memuaskan dalam menghadapi serangan siber, dengan tingkat keberhasilan mencegah serangan mencapai 90%. Data yang diperoleh memberikan keyakinan bahwa sistem keamanan ini dapat efektif melindungi infrastruktur server PT. XYZ dari ancaman yang terus berkembang.
4. Implikasi Praktis: Temuan dari penelitian ini memiliki implikasi praktis yang signifikan dalam pengembangan strategi keamanan informasi bagi PT. XYZ dan perusahaan lainnya di era digital saat ini. Integrasi teknologi keamanan seperti Honeypot dan IDS dapat menjadi langkah yang efektif dalam meningkatkan tingkat keamanan infrastruktur IT perusahaan.
5. Dengan demikian, berdasarkan hasil penelitian ini, dapat disimpulkan bahwa sistem keamanan yang menggabungkan Honeypot dan IDS mampu memberikan perlindungan yang efektif terhadap infrastruktur server PT. XYZ dari serangan siber. Namun demikian, perlu dilakukan pemantauan dan pembaruan secara berkala terhadap sistem keamanan ini guna menjaga kinerjanya dalam menghadapi ancaman yang terus berkembang di dunia digital.

DAFTAR PUSTAKA

Rashid, F. Y., Rahman, S., & Al-Shaer, E. (2019). Honeypot-based detection and analysis of attacks against industrial control systems. IEEE Transactions on Industrial Informatics,

15(5), 2645-2654.

Zhu, Q., Rass, S., & Schauer, S. (2020). Game-theoretic approaches for adversarial and cooperative cyber defense: The role of honeypots. IEEE Transactions on Information Forensics and Security, 15, 1727-1739.

Chiba, Z., Mellouk, A., Idrissi, N. E., & Brandao, D. (2016). Cooperative intrusion detection system for cloud computing networks. Computers & Electrical Engineering, 59, 177-186.

Mohammed, F. B., Yahya, S., & Mansoor, H. (2018). An enhanced intrusion detection system based on clustering of big data for the detection of DoS and DDoS attacks. IEEE Access, 6, 600-609.

Gade, R., Reddy, Y., & Krishna, C. M. (2017). An efficient honeypot framework for improving network security. International Journal of Information Security Science, 6(4), 55-65.

Kim, S., & Kim, D. (2019). Advanced threat detection and mitigation using honeypots in enterprise networks. IEEE Access, 7, 11658-11670.

Venkatesh, P., & Singh, A. (2016). Honeypot-based malware analysis for identifying potential attack strategies. Journal of Computer Virology and Hacking Techniques, 12(3), 185-193.

Zhang, Y., Li, Q., & Zhou, J. (2018). A novel IDS based on spatial-temporal analysis of network traffic for anomaly detection. Computer Networks, 135, 28-45.

Stiawan, D., Idris, M. Y. I., & Budiarto, R. (2015). Adaptive security mechanism for mitigating cyber-attacks on enterprise networks. Journal of Information Security and Applications, 20, 19-31.

Joshi, R. R., & Sharma, D. K. (2019). Enhancing the effectiveness of IDS using machine learning techniques. Cybersecurity, 2(1), 12.

Alshammari, R., & Zincir-Heywood, A. N. (2017). An investigation on machine learning based detection approaches for SSH attacks. Computers & Security, 70, 257-268.

Muna, A., Rehman, S., & Chaudhry, J. (2019). Hybrid intrusion detection framework for software-defined networks. Future Generation Computer Systems, 93, 442-453.

Yang, T., & Li, S. (2018). Detection and mitigation of DDoS attacks in SDN using machine learning approach. IEEE Access, 6, 14370-14379.

Elmrabit, N., & Haider, W. (2019). A collaborative and adaptive approach for mitigating DDoS attacks in cloud computing environments. Journal of Cloud Computing, 8(1), 23.

Alghamdi, A., & Almomani, A. (2019). Honeypot-based proactive defense mechanisms for

securing industrial control systems. Journal of Network and Computer Applications, 127, 70-83.

Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2016). Network anomaly detection: methods, systems and tools. IEEE Communications Surveys & Tutorials, 16(1), 303-336.

Beghdad, R., & Guermouche, A. (2017). A novel architecture for securing e-commerce servers using honeypots. Journal of Ambient Intelligence and Humanized Computing, 8(3), 317-326.

Dong, X., & Zhou, H. (2018). Anomaly detection using neural network in vehicular ad hoc networks. Journal of Network and Computer Applications, 119, 22-29.

Zaharia, G., & Gheorghe, L. (2019). Behavioral-based intrusion detection in modern enterprise networks. Computers & Security, 85, 278-292.

Xie, Y., & Zhang, Y. (2020). Intrusion detection techniques for mobile ad hoc networks: A survey. IEEE Communications Surveys & Tutorials, 22(3), 1271-1293.