ANALISIS KEAMANAN JARINGAN *WIRELES LAN* DI DINAS PERPUSTAKAN DAN KEARSIPAN KOTA PEKANBARU

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana
Pada Fakultas Teknik
Universitas Islam Riau

OLEH:

JUAN FERNANDES
143510607

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS ISLAM RIAU
PEKANBARU
2021

LEMBAR PENGESAHAN PEMBIMBING SKRIPSI

Nama	:	Juan Fernandes
NPM	:	143510607
Fakultas	:	Teknik
Program Studi	:	Teknik Informatika
Jenjang Pendidikan	:	Strata Satu (S1)
Judul Skripsi	:	Analisis Keamanan Jaringan Wireles LAN Di Dinas Perpustakaan Dan Kearsipan Kota Pekanbaru .

Format sistematika dan pembahasan materi pada masing-masing bab dan sub bab dalam skripsi ini telah dipelajari dan dinilai relatif telah memenuhi ketentuan-ketentuan dan kriteria - kriteria dalam metode penulisan ilmiah. Oleh karena itu, skripsi ini dinilai layak dapat disetujui untuk disidangkan dalam ujian komprehensif.

Pekanbaru, 17 Desember 2021

Disahkan Oleh

Ketua Prodi Teknik Informatika	**Dosen Pembimbing**
Dr. APRI SISWANTO, S.Kom., M.Kom	**Dr. APRI SISWANTO, S.Kom., M.Kom**

LEMBAR PENGESAHAN
TIM PENGUJI UJIAN SKRIPSI

Nama	:	Juan Fernandes
NPM	:	143510607
Fakultas	:	Teknik
Program Studi	:	Teknik Informatika
Jenjang Pendidikan	:	Strata Satu (S1)
Judul Skripsi	:	Analisis Keamanan Jaringan Wireles LAN Di Dinas Perpustakaan Dan Kearsipan Kota Pekanbaru .

Skripsi ini secara keseluruhan dinilai telah memenuhi ketentuan-ketentuan dan kaidah-kaidah dalam penulisan penelitian ilmiah serta telah diuji dan dapat dipertahankan dihadapan tim penguji. Oleh karena itu, Tim Penguji Ujian Skripsi Fakultas Teknik Universitas Islam Riau menyatakan bahwa mahasiswa yang bersangkutan dinyatakan **Telah Lulus Mengikuti Ujian Komprehensif Pada Tanggal 17 Desember 2021** dan disetujui serta diterima untuk memenuhi salah satu syarat guna memperoleh gelar Sarjana Strata Satu Bidang Ilmu **Teknik Informatika.**

Pekanbaru, 17 Desember 2021

Tim Penguji

1. **Dr. Evizal Abdul Kadir, S.T., M.Eng** — **Sebagai Tim Penguji** (.....)
2. **Rizdqi Akbar Ramadhan, S.Kom., M.Kom** — **Sebagai Tim Penguji** (.....)

Disahkan Oleh

Ketua Prodi Teknik Informatika	**Dosen Pembimbing**
Dr. APRI SISWANTO, S.Kom., M.Kom	**Dr. APRI SISWANTO, S.Kom., M.Kom**

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Dengan segala kerendahan hati Penulis haturkan rasa syukur dalam kehadirat Allah SWT,yang telah memberikan limpahan rahmat dan karunia-Nya yang berupa kemampuan, kesehatan dan juga kesempatan kepada Penulis untuk menyelesaikan proposal tugas akhir "Analisis Keamanan Jaringan Wireless Lan di Dinas Perpustakaan dan Kearsipan Kota Pekanbaru" ini.

Terimakasih kepada semua pihak yang telah membantu penulis dalam proses pembuatan skripsi ini, karena berkat dan dorongan dari berbagai pihak penulis dapat menyelesaikan skripsi ini, rasa terimakasih penulis ucapkan kepada :

1. Kedua orang tua Penulis yang telah memberikan motivasi, nasehat, serta didikannya sampai saat ini hingga penulis dapat kuliah dan menyelesaikan proposal tugas akhir ini.
2. Kepada Bapak Dr. Eng, Muslim, S.T., M.T Dekan Fakultas Teknik Universitas Islam Riau.
3. Bapak Dr. Apri Siswanto S.Kom., M.Kom selaku Ketua Program Studi Teknik Informatika Universitas Islam Riau.

4. Bapak Apri Siswanto, S.Kom., M.Kom selaku pembimbing yang telah memberikan pengajaran, arahan, dan telah sabar dalam memberikan bimbingan di sela-sela kesibukan beliau.
5. Bapak dan Ibu Dosen UIR yang telah banyak memberikan ilmunya selama penulis menduduki bangku perkuliahan khususnya bagi Bapak dan Ibu Dosen Program Studi Teknik Informatika
6. Kepada seluruh staff TU Teknik yang telah membantu kelancaran dalam proses penyelesaian skripsi

Demikian yang dapat saya sampaikan semoga dapat bermanfaat bagi seluruh pembaca. Akhir kata, apabila terdapat kesalahan ketik atau format penulisan yang tidak sesuai pada skripsi ini, dengan rendah hati penulis memohon maaf atas segala kekuarangan.

Wassalamu'alaikum Wr. Wb.

Pekanbaru, 17 Desember 2021

Juan Fernandes
NPM : 143510607

ANALISIS KEAMANAN JARINGAN WIRELES LAN DI DINAS PERPUSTAAN DAN KEARSIPAN KOTA PEKANBARU

Juan Fernandes
NPM 143510607

Program Studi Teknik Informatika

Universitas Islam Riau

Email : juanfernandes@student.uir.ac.id

ABSTRAK

Keamanan jaringan komputer kini dipandang sebagai salah satu tugas dan masalah penting yang harus dibenahi untuk melindungi aset-aset dan berbagai informasi. Keamanan jaringan adalah proses pencegahan yang dilakukan oleh penyerang untuk terhubung ke dalam jaringan komputer melalui akses yang tidak sah, atau penggunaan secara illegal dari komputer dan jaringan. Faktor-faktor penyebab resiko dalam jaringan komputer meliputi kelemahan manusia *(human error),* kelemahan perangkat keras komputer, kelemahan sistem operasi jaringan dan kelemahan sistem jaringan komunikasi. *Honeypot* merupakan salah satu jenis keamanan jaringan yang mampu mengidentifikasi penyerangan sehingga cocok diusulkan untuk diimplementasikan pada Dinas Perpustakaan dan Kearsipan Kota Pekanbaru. *Honeypot* adalah sumber daya keamanan yang mempunyai nilai jika sistem disusupi atau diserang. *Honeypot* adalah system palsu yang didesign mirip dengan sistem asli dengan tujuan untuk diserang dan disusupi. *Honeypot* hanyalah sistem palsu sehingga *traffic* dari dan kedalam *honeypot* akan sedikit dan bahkan tidak ada sama sekali. Saat ada interaksi / *traffic* pada *honeypot*, itu dapat dicurigai sebagai aktifitas akses yang tidak sah atau illegal. Dengan begitu, *honeypot* dapat menjadi alat bantu keamanan jaringan serta monitoring terhadap *traffic* jaringan. Hasil dari penelitian ini adalah penggunaan *Honeypot* sangat membantu dalam proses skema keamanan jaringan. Karena *honeypot* dapat menipu *hacker* dalam percobaan masuk ke *system* admin dengan membuat halaman web atau protocol web palsu. *IDS Snort* yang digunakan untuk mencatat aktifitas server juga dapat digunakan dengan baik. Hasil Analisa dapat dijadikan acuan untuk lebih memperkuat jaringan *wireless* sehingga keamanan dan kerahasian data dapat terjaga dengan baik.

Kata Kunci: keamanan jaringan, *Honeypot, IDS*

ANALYSIS OF WIRELES LAN NETWORK SECURITY AT THE CITY OF PEKANBARU LIBRARY AND CIVIL SERVICES

Juan Fernandes
NPM 143510607

Program Studi Teknik Informatika

Universitas Islam Riau

Email : juanfernandes@student.uir.ac.id

ABSTRACT

Computer network security is now seen as one of the important tasks and problems that must be addressed to protect assets and various information. Network security is the prevention process carried out by attackers to connect to computer networks through unauthorized access, or illegal use of computers and networks. The factors that cause risk in computer networks include human weakness (human error), computer hardware weaknesses, network operating system weaknesses and communication network system weaknesses. Honeypot is one type of network security that is able to identify attacks so it is suitable to be proposed to be implemented at the Pekanbaru City Library and Archives Service. A honeypot is a security resource that has value if a system is compromised or attacked. A honeypot is a fake system designed to resemble the original system with the aim of being attacked and compromised. Honeypot is just a fake system so that the traffic to and from the honeypot will be little or no. When there is interaction / traffic on the honeypot, it can be suspected of being an unauthorized or illegal access activity. That way, the honeypot can be a tool for network security and monitoring of network traffic. The results of this study are the use of Honeypot is very helpful in the process of network security schemes. Because honeypots can trick hackers into trying to get into the admin system by creating fake web pages or web protocols. IDS Snort which is used to record server activity can also be used properly. The results of the analysis can be used as a reference to further strengthen the wireless network so that data security and confidentiality can be maintained properly.

Keywords: network security, Honeypot, IDS

DAFTAR ISI

Hal

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dalam jaringan komputer berkembang sangat pesat dan fleksibel. Internet merupakan jaringan komputer yang lazim digunakan karena kemudahan aksesnya. Satu hal yang membedakan aplikasi jaringan komputer dengan teknologi lainnya adalah tidak adanya batasan dimensi ruang dan waktu. Seluruh informasi dapat tersebar luas dan cepat melalui internet. Oleh karna sifat dari internet adalah *public*, informasi yang disebarkan dapat bersifat terbuka. Sifat *public* pada internet banyak dimanfaatkan sebagai celah serangan oleh orang yang tidak bertanggung jawab. Hal ini akan beresiko terhadap persebaran informasi yang bersifat *private* (tertutup). Seiring dengan pesatnya perkembangan teknologi tersebut, semakin besar pula ancaman dan gangguan terhadap kinerja dalam teknologi tersebut. Untuk itu, keamanan jaringan merupakan aspek penting yang harus diperhatikan.

Keamanan jaringan komputer kini dipandang sebagai salah satu tugas dan masalah penting yang harus dibenahi solusinya untuk melindungi aset-aset dan berbagai informasi. Keamanan jaringan adalah proses pencegahan yang dilakukan oleh penyerang untuk terhubung ke dalam jaringan komputer melalui akses yang tidak sah, atau penggunaan secara illegal dari komputer dan jaringan. Faktor-faktor penyebab resiko dalam jaringan komputer meliputi kelemahan manusia (*human error*), kelemahan perangkat keras komputer, kelemahan sistem operasi jaringan dan kelemahan sistem jaringan komunikasi.

Teknologi yang digunakan untuk menangkal serangan tersebut sebenarnya telah ada, namun perkembangannya telah mencapai batas. Penggunaan teknologi tersebut menjadi tidak efisien karena tidak dapat menjamin keakuratan keamanannya. Salah satu teknik dalam mempertahankan keamanan adalah menggunakan *firewall*. *Firewall* adalah sistem atau perangkat yang mengizinkan lalulintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Umumnya, sebuah *firewall* diimplementasikan pada pintu gerbang (*gateway*) antara jaringan lokal dan jaringan lainnya (Prasetyo, 2008). Jenis Keamanan jaringan ini banyak diimplementasikan pada banyak intansi dan perusahaan. Salah satu instansi yang mengimplementasikannya adalah Dinas Perpustakaan dan Kearsipan Kota Pekanbaru.

Dinas Perpustakaan dan Kearsipan Kota Pekanbaru adalah instansi yang bergerak dibidang perpustakaan, arsip, dan dokumentasi. Dinas tersebut menyediakan perpustakaan yang dibuka untuk umum bernama perpustakaan Kota Pekanbaru. Seluruh fasilitas dan layanan yang ada di perpustakaan Soeman HS disediakan oleh dinas tersebut. Aktifitas di Dinas Perpustakaan dan Kearsipan Kota Pekanbaru iau banyak berorientasi pada jaringan internet (*jaringan wireless*). Divisi Otomasi, Preservasi, Kerjasama dan Jaringan Perpustakaan adalah divisi yang menjamin jalannya jaringan internet yang ada di Dinas Perpustakaan dan Kearsipan Kota Pekanbaru.

Divisi Otomasi, Preservasi, Kerjasama dan Jaringan Perpustakaan merupakan divisi yang bertugas dalam memastikan ketersediaan jaringan internet,

melaksanakan pengelolaan pangkalan data perpustakaan lingkup provinsi, pengelolaan *website* dan jaringan internet perpustakaan serta mengembangkan format komunikasi antar perpustakaan di Kabupaten/kota se- Kota Pekanbaru, pelestarian koleksi perpustakaan, dan melaksanakan kerjasama dan jaringan perpustakaan. Tugas yang diemban divisi ini berhubungan langsung dengan memastikan keamanan *database* dan jaringan perpustakaan sehingga resiko besar terhadap serangan kemanan jaringan menjadi ancaman yang serius.

Namun sistem keamanan yang ada di divisi ini bersifat *firewall*. *Firewall* memang dianggap mampu dalam menghadapi serangan, namun tidak mampu mengidentifikasi pelaku serangan dan menjebak penyerang. *Firewall* hanya mampu memberikan peringatan-peringatan saat ada aktivitas yang dianggap mencurigakan. Sementara itu, pengumpulan informasi tentang penyerang dan pola serangan yang diberikan bisa menjadi referensi dalam meningkatkan keamanan, mengetahui celah keamanan yang gampang disusupi, dan mengetahui solusi paling efektif dalam menangani masalah keamanan jaringan. *Honeypot* merupakan salah satu jenis keamanan jaringan yang mampu mengidentifikasi penyerangan sehingga cocok diusulkan untuk diimplementasikan pada Dinas Perpustakaan dan Kearsipan Kota Pekanbaru.

Honeypot adalah sumber daya keamanan yang mempunyai nilai jika sistem disusupi atau diserang. Pada dasarnya *honeypot* merupakan suatu alat untuk mendapatkan informasi dari penyerang. *Honeypot* merupakan sistem yang dirancang untuk diperiksa dan diserang (Andros Refan, Lucas, 2014). *Honeypot* adalah system palsu yang didesign mirip dengan sistem asli dengan tujuan untuk

diserang dan disusupi. *Honeypot* hanyalah sistem palsu sehingga *traffic* dari dan kedalam *honeypot* akan sedikit dan bahkan tidak ada sama sekali. Saat ada interaksi / *traffic* pada *honeypot*, itu dapat dicurigai sebagai aktifitas akses yang tidak sah atau illegal. Dengan begitu, *honeypot* dapat menjadi alat bantu keamanan jaringan serta monitoring terhadap *traffic* jaringan. *Honeypot* memiliki berbagai jenis, contohnya *honeywall, honeyd, honeynet* dan MHN (*Modern Honey Network*).

Atas dasar hal diatas, penelitian tentang perancangan dan implementasi MHN dilakukan. Penelitian ini bertujuan sebagai alat bantu keamanan jaringan guna mengurangi terjadinya serangan serangan berupa *scanning* dan pencarian celah kelemahan lainnya di Dinas Perpustakaan dan Kearsipan Provinsi Riau. Pengimplementasian jenis *honeypot* disesuaikan dengan pertimbangan kondisi dan kemudahan yang diberikan dalam pengaplikasiannya. Untuk melakukan perancangan dan implementasi *honeypot* di Dinas Perpustakaan dan Kearsipan Provinsi Riau, maka dibuatlah skripsi ini dengan judul "*Analisis Keamanan Jaringan Wireles Lan di Dinas Perpustakaan dan Kearsipan Kota Pekanbaru*"

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas dapat dirumuskan beberapa permasalahan, yaitu :

1. Bagaimana Keamanan Jaringan Wireles Lan Di Dinas *Perpustakaan dan Kearsipan Kota Pekanbaru*
2. Membangun dan mengimplementasikan MHN pada jaringan data *wireless* di Dinas Perpustakaan dan Kearsipan Kota Pekanbaru.

3. Bagaimana pengujian atau pembuktian bahwa Keamanan Jaringan Wireles Lan dapat berjalan dan membantu meningkatkan keamanan jaringan.

1.3 Identifikasi Masalah

Berdasarkan pernyataan masalah diatas dapat ditentukan tujuan yang akan dicapai yaitu mengimplementasikan MHN untuk keamanan jaringan data *wireless* di Dinas Perpustakaan dan Kearsipan Kota Pekanbaru.

1.4 Batasan Masalah

Untuk mencapai objektif terdapat beberapa batasan masalah pada skripsi ini, yaitu :

1. Implementasi dilakukan pada divisi Otomasi, Preservasi, Kerjasama dan Jaringan Perpustakaan.
2. Sistem Operasi yang digunakan adalah Ubuntu 14.
3. Sistem *honeypot* yang dibangun mempunyai kategori atau jenis *research honeypot*.
4. Perancangan dan pengimplementasian *honeypot* dilakukan pada jaringan yang sudah ada.
5. Pengimlementasian MHN menggunakan Snort.
6. Pengujian serangan dilakukan dalam beberapa skenario, yaitu menggunakan *port scanning*, DoS, DDoS, *brute force attack*.

1.5 Tujuan Penelitian

1. Mengimplementasikan MHN untuk keamanan jaringan data *wireless* di Dinas Perpustakaan dan Kearsipan Kota Pekanbaru.

2. Mendeteksi serangan keamanan jaringan dari pihak yang tidak bertangung jawab.

1.6 Manfaat Penelitian

Adapun manfaat yang ingin dicapai dari penelitian ini adalah:

1. Dapat membantu peningkatan keamanan jaringan.
2. Bagi peneliti memberi pengetahuan tentang bagaimana membuat sebuah penelitian yang dapat memaksimalkan pengunaan Keamanan jaringan.

BAB II

STUDI PUSTAKA DAN LANDASAN TEORI

2.1 Studi Kepustakaan

Hasil penelitian terdahulu merupakan referensi untuk melakukan penelitian ini. Dalam penelitian tersebut terdapat kesamaan permasalahan penelitian. Penelitian terdahulu juga menjadi salah satu acuan dalam melakukan penelitian sehingga dapat menambahkan teori yang digunakan dalam mengkaji penelitian yang dilakukan.

1. Penelitian yang dilakukan oleh Ahmad Fikri Nurrahman (2013) yang mengimplementasikan *virtual* jenis *low interaction honeypot* dengan menggunakan dionaea untuk mendukung keamanan jaringan. Penelitian ini bertujuan untuk membantu dalam mengatasi serangan *port scanning* dan eksploitasi. Seluruh komputer *virtual* dengan spesifikasi kebutuhan perangkat keras yang terbatas dapat bekerja sesuai dengan skenario yang telah ditentukan. Tahap awal penetrasi dilakukan dengan *port scanning* terhadap *port* yang terbuka lalu melakukan eksploitasi terhadap *port* tersebut. Pada saat terjadinya serangan Nmap, Dionaea mencatat semua kegiatan yang dilakukan oleh Nmap. Tiap serangan terhadap *port* tertentu diberikan *attackid* sehingga dapat diketahui detil tiap serangan dan jumlahnya. Serangan terhadap layanan palsu Dionaea telah berhasil diimplementasikan dengan menggunakan BackTrack (Nurrahman, 2013).
2. Penelitian yang dilakukan oleh Sutarti dan Khairunnisa (2017). Dalam penelitian ini, dilakukan peracangan dan analisis keamanan jaringan nirkabel dari serangan DDos berbasis *honeypot*. Perancangan ini

menggunakan dioneae *honeypot*. Tujuan dari penelitian memberi alat bantu keamanan jaringan pada PDAM Tirta Al Bantani yang hanya menggunakan *firewall* sebagai ketahanan jaringan sebelumnya. Setelah dioneae diimplementasikan, uji serangan *port scanning* dan DoS dilakukan. Hasil penelitian menyatakan bahwa serangan spam, malware, Ddos Attack, scanner, dan virus dapat ditangkap oleh *server honeypot* dan gagal masuk ke sistem (Sutarti, 2017).

3. Penelitian yang dilakukan oleh Bagus Mardiyanto(2016), Tutuk Indriyani, I Made Suartana. Dalam penelitian ini, dilakukan analisa dan implementasi *honeypot* dalam mendeteksi serangan DDoS pada jaringan *wireless*. Jenis *honeypot* yang di implementasikan adalah honeyd. Honeyd yang telah dikonfigurasi digunakan untuk membuat dan menjalankan *virtual host* dalam jaringan komputer dan mendeteksi serangan-serangan yang dilakukan oleh *attacker*. Uji coba dilakukan dengan *host scanning* dan *port scanning*, serangan Ddos TCP flood, serangan Ddos HTTP flood, serangan Ddos UDP flood, serangan Ddos ke *server* sebelum konfigurasi *IPtables*, serangan Ddos ke server setelah konfigurasi *iptables*. Didapatkan kesimpulan bahwa honeyd dapat mendeteksi serangan Ddos secara *real time* dan dengan Penggunaan *IPtables* sebagai *firewall* serangan DDoS dapat dibelokkan ke IP yang tidak digunakan (Mardiyanto, 2016).
4. Penelitian yang dilakukan Triawan Adi Cahyanto(2016), Hardian Oktavianto, Agil Wahyu Royan. Dalam penelitian ini dilakukan analisis dan implementasi *honeypot* menggunakan dionaea sebagai penunjang

keamanan jaringan. Pengimplementasian menggunakan *honeypot* jenis dioneae. Pengujian menggunakan *port scanning* serta eksploitasi layanan menggunakan teknik e*xploit* yang terdapat pada *Metasploit Framework*. Pengujian *server* tiruan tersebut berbasis Dionaea menggunakan Metasploit Framework, dan melibatkan tiga teknik exploit yaitu MS04_011_LSASS, MS03_026_DCOM, dan MySQL_Payload. Berdasarkan simulasi serangan yang sudah dikerjakan, dapat diketahui bahwa penggunaan dioneae dapat menunjang keamanan jaringan dengan berperan sebagai *server* palsu atau *server* tiruan sehingga dapat melindungi *server* asli ketika *server* tiruan tersebut mengalami serangan. Namun *honeypot* tidak dapat melindungi sistem operasi khususnya windows (Cahyanto, 2016).

5. Penelitian yang dilakukan oleh Harjono dan Agung Purwo Wicaksono (2013). Dalam penelitian ini, jenis honeypot yang diimplementasian adalah honeyd. Honeyd ditempatkan pada segmen jaringan internal, dengan konfigurasi untuk menirukan empat *host* dengan sistem operasi dan layanan yang berbeda-beda. Dari penelitian ini didapatkan sejumlah serangan kepada honeyd yang berasal dari sejumlah *host* dengan alamat IP *private* dari dalam jaringan internal. Hal tersebut menunjukkan bahwa penyerang berasal dari dalam jaringan internal. Rata-rata dalam satu hari jumlah serangan yang menuju honeyd sebanyak 10 kali serangan. Empat *host* yang disimulasikan honeyd mendapatkan jumlah serangan yang relatif sama besar. Serangan yang terdeteksi oleh honeyd adalah serangan dilakukan secara otomatis oleh malware (Harjono, 2013).

6. Penelitian yang dilakukan oleh Lukito Prima Aidin, Surya Michradi Nasution dan Fairuz Azmi (2016). Penelitian mengimplementasikan High Interaction Honeypot pada server dengan menggunakan *High Interaction Analysis Tools* (HIHAT). Berdasarkan hasil pengujian, dapat disimpulkan bahwa honeypot high interaction HIHAT dapat mengemulsikan dan mencatat serangan *directory buster brute fource*, RFI, dan SQL *Injection* namun masih belum mengemulsikan serangan DoS dengan sempurna. Dari hasil DoS, HIHAT pada *honeypot* mengalami *delay* saat mendapatkan *request* yang banyak secara bersama namun semua request tetap diproses tanpa adanya *packet loss* (Aidin, 2016).
7. Penelitian yang dilakukan oleh Shah Manthan Jigneshkuma (2016). Dalam peneltian ini, dijelaskan mengenai MHN yakni arsitektur MHN, sensor-sensor MHN, HPFeeds, Mnemosyne, MHN Web Application. Hasil dari penelitian ini adalah MHN *server* mampu mengatasi kekurangan *honeypot*. Manfaat yang diberikan oleh MHN adalah mudah di implementasikan, dikonfigurasikan dan dirawat serta mengurangi resiko (Jigneshkuma, 2016).
8. Penelitian yang dilakukan oleh Satish Mahendra Kevat (2017). Dalam penelitian ini, dijelaskan mengenai *honeypot*, penempatan *honeypot*, dan membangun *virtual honeypot*. Pertimbangan dalam mengimplementasikan honeypot dalam jurnal ini adalah tujuan penggunaan (peringatan dini atau analisis forensik), tingkat interaksi, digunakan langsung pada sistem atau melalui emulasi, administrator

honeypot, pembaharuan data. Masalah hukum pada honeypot adalah jebakan, privasi, dan *liability*. *Honeypot* dianggap mampu meningkatkan keamanan jaringan dan perkembangan *honeypot* sedemikian rupa agar penyerang dapat percaya dengan sistem asli perlu dipertimbangkan (Kevat, 2017).

9. Penelitian yang dilakukan oleh Snehil Vidwarshi, Atul Tyagi, Rishi Kumar (2015). Dalam jurnal ini dibahas secara lengkap tentang sejarah, berbagai jenis, aplikasi, kelebihan dan kekurangan dan manfaat *honeypot*. Kesimpulan dari penjabaran dalam penelitian ini adalah *honeypot* dapat digunakan dalam banyak model dasar sistem deteksi dan dapat membantu peningkatan keamanan jaringan (Vidwarshi, 2015).
10. Penelitian yang dilakukan oleh Tengku. Mohd. Diansyah, Ilham Faisal, Adidtya Perdana, Boni Octaviani Sembiring, dan Tantri Hidayati Sinaga (2017). Dalam penelitian ini, jenis honeypot yang digunakan adalah honeyd yang memiliki resiko lebih kecil karena tidak langsung melibatkan sistem asli. Kesimpulan yang didapat dari penelitian ini adalah *honeypot* dan *firewall* dapat bekerja sama dalam menahan serangan. Penyerang tidak dapat masuk dengan mudah karena penyerang masuk kedalam perangkap *honeypot* yang telah dibuat. *Honeypot* juga berhasil medeteksi aktivitas mencurigakan dan menangkap IP penyerang dan disimpan dalam folder yang terpisah pada perangkap *honeypot server* (Diansyah, 2017).
11. Penelitian yang dilakukan oleh Navneet Kambow dan Lavleen Kaur Passi (2014). Penelitian ini menjelaskan mengenai pengantar *honeypot*,

kepentingannya dalam keamanan jaringan, jenis *honeypot*, kelebihan, kekurangan, dan masalah hukum yang terkait dengan *honeypot*. Dijelaskan juga mengenai kekurangan sistem deteksi intrusi dalam keamanan jaringan dan bagaimana *honeypot* meningkatkan arsitektur keamanan jaringan. Dalam jurnal ini dibahas juga mengenai perbedaan jenis *honeypot*, tingkat interaksi dan resiko yang terkait dengan *honeypot* (Kambow, 2014).

12. Penelitian yang dilakukan oleh Jashanpreet Singh Toor dan Abhinav Bhandari (2017). Dalam penelitian ini, honeypot jenis pentbox diimplementasikan pada *server* ubuntu. Pentbox dikonfigurasikan secara manual pada *port* 80 dan hanya bisa dijalankan pada sudo previleges. *Port* 80 merupakan nomor *port* yang ditetapkan oleh *internet communication protocol* untuk *Hypertext Transfer Protoco*l (HTTP). Wireshark pada *honeypot* digunakan untuk monitoring trafik jaringan dan *capture* data. Dapat disimpulkan bahwa setelah service berjalan, pentbox akan merekam setiap koneksi yang dilakukan. *Honeypot* hanya melihat aktivitas mencurigakan dan hampir semuanya merupakan sebuah serangan. Setiap sistem yang mencoba terhubung pada *server honeypot*, maka server *honeypot* tersebut merekam informasi yang terjadi (Toor, 2017).

2.2 Landasan Teori

2.2.1 Jaringan Komputer

Jaringan Komputer adalah sekelompok komputer otonom yang saling berhubungan antara satu dengan lainnya menggunakan *protocol* komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, program-program, penggunaan bersama perangkat keras seperti printer, harddisk, dan sebagainya (Barus, 2015). Jaringan komputer adalah sistem yang menggunakan Teknik komunikasi data, tetapi lebih mementingkan arti dari tiap bit saat proses pengiriman data sampai diterimanya data secara sempurna di komputer yang menjadi tujuannya. Menurut Sopandi (2008) banyak manfaat yang diperoleh dalam suatu jaringan komputer yaitu:

1. Jaringan komputer memungkinkan seseorang dapat mengakses *file* yang dimilikinya(*upload*) atau *file* yang telah diizinkan untuk diakses(*download*), dimanapun dan kapanpun.
2. Jaringan memungkinkan proses pengiriman data dapat berlangsung cepat dan efisien.
3. Jaringan komputer memungkinkan adanya *sharing hardware* antar *client*.
4. Jaringan komputer memungkinkan seseorang berhubungan dengan orang lain di berbagai negara dengan berupa teks, gambar, audio, dan video secara *real time*.
5. Jaringan komputer dapat menekan biaya operasional, seperti pemakaian kertas, pengiriman surat atau berkas, telepon serta pembelian *hardware* jaringan.

Jaringan adalah sistem yang terdiri dari media komunikasi, perangkat keras dan perangkat lunak yang diperlukan untuk menghubungkan antara dua atau lebih sistem komputer dan peralatan. Jaringan menjadi sangat penting karena pada dasarnya digunakan untuk berbagai alasan. Pertama, jaringan komputer memungkinkan organisasi lebih fleksibel dan dapat diselesaikan dengan cepat dalam kondisi bisnis. Kedua jaringan memungkinkan perusahaan membagi *hardware*, aplikasi komputer dan *database* dari suatu komputer ke komputer lain dalam satu organisasi. Ketiga jaringan komputer memungkinkan pekerja dan timnya yang secara geografis berjauhan untuk interaksi yang lebih efektif dan efisien. Informasi berupa data akan mengalir dari suatu komputer ke komputer lainnya atau dari satu komputer ke perangkat lain, sehingga masing-masing komputer yang terhubung tersebut biasa bertukar data atau berbagi perangkat keras. Jaringan komputer dibangun untuk membawa sebuah informasi secara tepat tanpa adanya kesalahan dari sisi pengirim (*transmitter*) maupun sisi penerima (*receiver*) melalui media komunikasi (Sharon dkk, 2014).

Jaringan komputer merupakan gabungan antara teknologi komputer dan teknologi komunikasi. Gabungan teknologi ini melahirkan pengolahan data yang dapat didistribusian, mencakup pemakaian *database*, *software* aplikasi dan perangkat keras secara bersaman. Jaringan komputer adalah sekelompok komputer otonom yang saling berhubungan satu dengan yang lain menggunakan *protocol* komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, aplikasi, dan perangkat keras secara bersama-sama. Dapat disimpulkan bahwa jaringan komputer adalah gabungan antara teknologi komputer dan teknologi komunikasi yang saling berkaitan satu sama lain (Saputra, 2012).

2.2.2 Jaringan Wireless

Seiring dengan perkembangan teknologi serta kebutuhan untuk akses jaringan yang *mobile* (bergerak) yang tidak membutuhkan kabel sebagai media tranmisinya, maka muncullah *Wireless Local Area Network* (*Wireless* LAN/WLAN). Jaringan lokal tanpa kabel atau WLAN adalah suatu jaringan area lokal tanpa kabel dimana media transmisinya menggunakan frekuensi radio (RF) dan infrared (IR), untuk memberi sebuah koneksi jaringan ke seluruh pengguna dalam area disekitarnya. Area jangkauannya dapat berjarak dari ruangan kelas ke seluruh kampus atau dari kantor ke kantor yang lain dan berlainan gedung. Peranti yang umumnya digunakan untuk jaringan WLAN termasuk di dalamnya adalah PC, Laptop, PDA, telepon seluler, dan lain sebagainya. Teknologi WLAN ini memiliki kegunaan yang sangat banyak. Contohnya, pengguna *mobile* bisa menggunakan telepon seluler mereka untuk mengakses *e-mail*. Sementara itu para pelancong dengan *laptop*-nya bisa terhubung ke internet ketika mereka sedang di bandara, kafe, kereta api dan tempat publik lainnya.

Setiap teknologi pasti ada kelebihan dan kelemahan yang ditawarkan kepada pengguna, untuk teknologi *wireless* mempunyai kelebihan dan kelemahan antara lain:

Kelebihan yang ditawarkan *wireless*:

1. Mobilitas
    a. Bisa digunakan kapan saja.
    b. Kemampuan akses data pada jaringan *wireless* itu *real time*, selama masih di area *hotspot*.

2. Kecepatan Instalasi
    a. Proses pemasangan cepat.
    b. Tidak perlu menggunakan kabel.
3. Fleksibel, bisa menjangkau tempat yang tidak mungkin dijangkau kabel.
4. Jangkauan luas
5. Biaya pemeliharannya murah (hanya mencakup stasiun bukan seperti pada jaringan kabel yang mencakup keseluruhan kabel).
6. Infrastrukturnya berdimensi kecil.
7. Mudah dikembangkan.
8. Mudah dan murah untuk direlokasi dan mendukung portabelitas.

Kelemahan teknologi *wireless*:

1. Transmit data kecil, sedangkan jika menggunakan kabel akan lebih cepat.
2. Alatnya cukup mahal.
3. Mudah terjadi gangguan antara pengguna yang lain (interferensi gelombang)
4. Kapasitas jaringan terbatas.
5. Keamanan data kurang terjamin.
6. *Intermittence* (sinyal putus-putus)
7. Mengalami gejala yang disebut *multipath* yaitu propagasi radio dari pengirim ke penerima melalui banyak jalur yang LOS.
8. Mempunyai *latency* yang cukup besar dibandingkan dengan media transmisi kabel.

WLAN, mewakili *local area network wireless*, seperti lab atau perpustakaan, untuk membentuk suatu jaringan atau koneksi ke Internet. Jaringan sementara dapat dibentuk oleh beberapa pemakai membutuhkan *access point* (Hartono, 2011).

2.2.3 Definisi Alat Bantu Keamanan Jaringan Komputer

Alat adalah benda yang dipakai untuk mengerjakan sesuatu. Selain itu dapat juga memiliki arti benda yang dipakai untuk mencapai maksud tertentu. Aman berarti bebas dari bahaya, bebas dari gangguan (pencuri, hama, dsb), terlindung atau tersembunyi; tidak dapat diambil orang. Sedangkan keamanan berarti keadaan aman. 3 macam keamanan sistem, yaitu:

1. Keamanan eksternal / *external security* berkaitan dengan pengamanan fasilitas komputer dari penyusup dan bencana seperti kebakaran /kebanjiran
2. Keamanan interface pemakai / *user interface security* berkaitan dengan indentifikasi pemakai sebelum pemakai diijinkan mengakses program dan data yang disimpan
3. Keamanan internal / *internal security* berkaitan dengan pengamanan beragam kendali yang dibangun pada perangkat keras dan sistem operasi yang menjamin operasi yang handal dan tak terkorupsi untuk menjaga integritas program dan data.(Candra, 2014)

Dasar keamanan jaringan komputer adalah komputer yang terhubung ke *network*, mempunyai ancaman yang lebih besar daripada komputer yang tidak

terhubung kemanapun. Maka ditarik kesimpulan bahwa keamanan jaringan komputer adalah usaha-usaha yang berhubungan dengan keamanan suatu jaringan komputer dan dilakukan untuk mengamankan jaringan komputer tersebut.

Keamanan jaringan merupakan sebuah topik dengan cakupan yang sangat luas dan sangat kompleks. Materi keamanan jaringan idealnya diberikan oleh seseorang yang sangat terlatih, sangat berpengalaman, dan sangat ahli di bidang jaringan komputer. Tidak hanya mengetahui secara konsep namun juga sudah terjun langsung menangani berbagai persoalan security. Orang-orang semacam ini sudah mengerti benar seluk beluk jaringan komputer secara teori dan praktik. (Sofana, 2014).

Di dalam keamanan jaringan terdapat pula resiko jaringan komputer yang merupakan segala bentuk ancaman baik fisik maupun *logic* yang langsung atau tidak langsung mengganggu kegiatan yang sedang berlangsung dalam jaringan. Resiko dalam jaringan komputer disebabkan oleh beberapa faktor yaitu:

1. Kelemahan manusia.
2. Kelemahan perangkat keras computer.
3. Kelemahan sistem operai jaringan.
4. Kelemahan sistem jaringan komnikasi (Adi dkk, 2014).

Berdasarkan arti kata diatas, maka dapat disimpulkan bahwa alat bantu keamanan jaringan adalah benda yang digunakan untuk membantu dalam usaha pengamanan jaringan komputer dari berbagai serangan dan ancaman oleh beberapa faktor.

2.2.4 Aspek Keamanan Komputer

Keamanan komputer meliputi beberapa aspek, diantaranya adalah *privacy, integrity, authentication, availability, acess control,* dan *non-repudation* (Ariyus, 2006: 2).

1. Privacy atau confidentiality

   Aspek ini berhubungan dengan menjaga informasi dari orang yang tidak berhak mengakses informasi tersebut. *Privacy* kearah data-data yang bersifat pribadi, sedangkan *confidentitialy* berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk tujuan tertentu. Serangan terhadap aspek *privacy* misalnya dengan melakukan penyadapan (*sniffer*) terhadap hal yang bukan menjadi haknya. Salah satu upaya dalam menangani permasalahan *privacy* dan *confidentiality* adalah dengan menggunakan teknologi kriptografi (Prasetyo, 2008).

2. Integrity

   Aspek ini menekankan bahwa tidak boleh ada perubahan data tanpa seizin pemilik informasi. Adanya virus, trojan house, atau pemakai lain yang mengubah informasi tanpa izin merupakan ancaman yang perlu dihadapi. Contoh masalah integrity ini *email* yang ditangkap (*intercept*) ditengah jalan lalu diubah isinya (*altered, tempored, modified*) dan kemudian diteruskan kealamat yang dituju. Salah satu cara mengatasi masalah ini adalah dengan enkripsi dan *digital signature* (Prasetyo, 2008).

3. Authentication

Aspek ini berhubungan dengan metode untuk memastikan bahwa informasi tersebut betul-betul asli dan pihak yang mengakses atau memberikan informasi tersebut juga asli. Contoh dari *authentication* adalah dengan menjaga keaslian data melalui *digital signature*. Contoh lain adalah dengan pembatasan terhadap orang orang yang dapat mengakses informasi tersebut (Prasetyo, 2008).

4. Availability

Aspek ini berhubungan dengan ketersediaan informasi dan data saat dibutuhkan. Aspek ini berakibat fatal jika tidak di perhatikan dengan baik dan saat terjadi serangan oleh orang yang tidak bertanggung jawab. Contoh serangan pada aspek ini adalah DoS(Denial Of Service) dimana suatu server tidak bias melayani kebutuhan sebab mendapatkan banyak kiriman permintaan sehingga menmbulkan keadaan *hang*, *down*, bahkan *crash* (Prasetyo, 2008).

5. Access Control

Aspek ini berhubungan dengan cara pengaturan akses terhadap suatu informasi. Hal ini biasanya berhubungan dengan klasifikasi data(*private,public, confidential, top secret*) dan user(*guest, admin, top manager*, dsb), serta mekanisme *authentication* dan juga *privacy*. Access control biasanya dilakukan dengan userid/password atau dengan menggunakan mekanisme lain seperti kartu dan biometrics (Prasetyo, 2008).

6. Non-repudiation

Aspek ini bertujuan untuk menjaaga agar seseorang tidak dapat menyangkal telah melakukan suatu transaksi. Sebagai contoh seseorang yang mengirim *email* tidak dapat menyangkal bahwa sudah mengirim *email*. Hal ini sangat penting dalam *electronic commerce*. Aspek ini dapat diamankan secara umum dengan penggunaan *digital signature*, *certifiates*, dan teknologi kriptografi (Prasetiyo, 2008).

2.2.5 Aspek Ancaman Keamanan Komputer

Serangan terhadap keamanan komputer dapat dilihat dari sudut peranan komputer atau jaringan komputer yang berfungsi sebagai penyedia informasi. Ada empat jenis serangan yakni interruption, interception, modification, dan fabrication (Stallings, 2003).

1. Interruption

Serangan ini menyebabkan perangkat system menjadi rusak atau tidak dapat digunakan lagi sehingga menimbulkan ketidaktersediaan. Serangan ditujukan untuk aspek *availability* dari suatu sistem.

Sebagai contoh, pemutusan jalur komunikasi sehingga komunikasi yang dikirimkan oleh suatu pihak tidak sampai kepada pihak yang dituju. Contoh serangannya adalah DoS (Denial of Service).

2. Interception

Ketika Pihak yang Tidak berwenang berhasil mengakses aset atau informasi yang bukan miliknya. Serangan ini menyerang aspek *confidentialy*. Pihak yang tidak berwenang bias berbentuk orang,

program komputer, dan komputer. Contoh serangan ini adalah penyadapan (*wiretapping*) untuk meng-*capture* data pada jaringan.

3. Modification

   Ketika pihak berwenang bukan hanya mengakses terhadap aset tersebut, namun juga dapat merubahnya. Serangan ini menyerang aspek *integrity*. Sebagai contoh adalah merubah nilai suatu data, merubah isi *website* orang lain tanpa sepengetahuan pemiliknya.

4. Fabrication

   Ketika pihak yang tidak berwenang memasukan sesuatu kedalam suatu system. Serangan ini menyerang aspek *authenticity*. Sebagai contoh adalah *email*, yaitu dengan memasukan *email* palsu dalam jumlah banyak kedalam suatu jaringan.

2.2.6 Serangan pada Keamanan Jaringan

Ada banyak aktifitas atau jenis serangan terhadap system keamanan jaringan. Beberapa yang akan dibahas adalah:

1. Port Scanning

   Sebuah *port* scan, adalah alat yang digunakan untuk scan *port* TCP dan UDP dan melaporkan status mereka. *Port scanner* menggunakan beberapa *protocol* seperti TCP, UDP dan ICMP. *Port scanning* memungkinkan individu memeriksa dan menentukan layanan apa yang berjalan pada komputer target. *Port* digunakan oleh kedua *protocol* yaitu TCP dan UDP. Meskipun beberapa aplikasi dapat membuat *port* tersebut

untuk beroperasi pada *port* yang tidak standar, nomor *port* telah ditetapkan oleh standar yang ada(Sons, 2014)

2. DoS

   DoS merupakan salah satu serangan yang banyak ditemui dalam dunia *networking* saat ini. Pengguna tidak pernah tahu kapan akan mendapat serangan ini. Serangan DoS dapat terjadi kapan saja pada jaringan dan dapat ditujukan kepada siapa saja, bahkan ke personal. Namun biasanya yang paling sering terkena dampaknya adalah *server-server* besar seperti *yahoo, google,* serta perbankan yang secara langsung memberikan pelayanannya melalui jaringan. Serangan ini biasanya bertujuan untuk mematikan pelayanan dari komputer atau jarïngan yang diserang. Korban yang terkena serangan ini tidak dapat memberikan pelayanan yang seharusnya. Serangan DoS ini dapat menghambat bahkan mematikan pelayanan pada sebuah sistem sehingga pengguna yang sah tidak dapat menerima atau mendapatkan pelayanan yang seharusnya. (Komputer, 2010)

3. DDoS

   Distributed Denial of Service (DDoS) merupakan salah satu jenis serangan *Denial of Service* yang menggunakan banyak *host* penyerang sekaligus untuk menyerang satu buah *host* target dalam sebuah jaringan. Boleh dibilang serangan DoS bersifat “satu lawan satu”. Tentu saja hal ini akan membutuhkan waktu yang lama supaya bisa membanjiri *host* target. Dengan DDoS serangan bisa dilakukan oleh beberapa komputer sekaligus yang efeknya lebih berbahaya daripada DoS. Banyaknya

komputer yang menyerang sebuah sistem merupakan kelebihan yang menyebabkan betapa berbahayanya DDoS. Komputer-komputer tersebut bisa saja dilakukan oleh sebuah komunitas dengan komputernya masing-masing dan menyerang pada satu waktu yang telah ditentukan. Atau bisa juga menggunakan *computer zombie* (kompter perantara), yaitu istilah yang digunakan untuk komputer yang dikontrol oleh orang lain untuk ikut melakukan DDoS. *Zombie* ini biasanya dieksploitasi menggunakan *Trojan Horse* (Zam, 2011)

4. Brute Force

Algoritma *brute-force* adalah algoritma yang memecahkan masalah dengan pemikiran yang sangat sederhana, langsung, dan dengan cara yang jelas/lempang. Algoritma ini mampu digunakan dalam meretas semua kemungkinan *password* dengan masukkan karakter dan panjang *password* tertentu sehingga dapat menghasilkan banyak kemungkinan kombinasi *password*. Serangan *brute-force* adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin. Secara sederhana, sistem serangan *brute-force* adalah sistem menebak *password* dan mencoba semua kombinasi karakter yang mungkin. Serangan *brute-force* digunakan untuk menjebol akses ke suatu *host* (*server/workstation/network*) atau kepada data yang ter-enkripsi. Metode ini dipakai para *cracker* untuk mendapatkan *account* secara tidak sah, dan sangat berguna untuk memecahkan enkripsi

2.2.7 Honeypot

Honeypot adalah sumber sistem informasi yang biasanya didesain bertujuan untuk mendeteksi, menjebak, dalam usaha percobaan penetrasi kedalam sistem (Joshi & Sardana, 2011). Suatu sistem yang terdiri dari beberapa *honeypot* disebut juga *honeynet*. Apabila *attacker* melakukan penyerangan kedalam sistem atau *server*, maka *honeypot* yang menyerupai *server* asli akan mengalami penyerangan terlebih dahulu, sedangkan sistem dan *server* asli tetap aman dibelakang *honeypot*. Komputer tersebut melayani serangan yang dilakukan oleh *attacker* dalam melakukan penetrasi terhadap *server* tersebut. *Honeypot* akan memberikan data palsu apabila ada hal aneh yang yang akan masuk ke dalam sistem atau *server*. Secara teori *honeypot* tidak akan mencatat trafik yang legal. Sehingga dapat dilihat bahwa yang berinteraksi dengan *honeypot* adalah *user* yang menggunakan sumber daya sistem yang digunakan secara ilegal. Bagi *attacker* yang tidak berpengalaman, bisa jadi akan mengira mudah berhasil meretas sistem/*server* yang asli. Namun sejatinya segala tindakan, *tool*, dan teknik yang digunakannya didalam melakukan penyerangan, telah tercatat dan dipelajari oleh *Sysadmin* bersangkutan melalui data dan informasi yang disajikan oleh *honeypot* (Pratama, 2014).

Dalam bahasa sederhana, *honeypot* adalah sistem atau komputer yang sengaja dikorbankan untuk menjadi target serangan *hacker*. Oleh sebab itu setiap interaksi dengan *honeypot* patut diduga sebagai aktivitas penyusupan. Misal, jika ada orang yang melakukan *scanning* jaringan untuk mencari komputer yang *vulnerable* (rentan), saat ia mencoba koneksi ke *honeypot* tersebut, maka *honeypot* akan mendeteksi dan mencatatnya, karena seharusnya tidak ada *user* yang

berinteraksi dengan *honeypot*. Keunggulan *hacker* adalah anonimitas. *Honeypot* merupakan senjata orango-rang baik yang membuat situasi menjadi lebih imbang. Tidak seperti IDS atau *firewall*, *honeypot* tidak menyelesaikan suatu masalah tertentu, tetapi memiliki kontribusi terhadap keseluruhan keamanan (Spitzner, 2003).

2.2.8 Kategori Honeypot

Setiap *honeypot* dirancang berdasarkan tujuan yang berbeda-beda oleh para pengembangnya.

1. Production Honeypot

   Digunakan untuk mendeteksi, mencegah, menanggulangi dan mengurangi tingkat resiko yang ditimbulkan akibat serangan tertentu pada system keamanan jaringan komputer (Prasetyo, 2008).

2. Research Honeypot

   Mendapatkan berbagai macam informasi tentang penyerangan dari para *blackhat community* sehingga para administrator dapat mempelajari informasi tersebut untuk dijadikan referensi dalam mengamankan system jaringan komputer pada masa yang akan datang (Prastyo, 2008).

2.2.9 Tingkatan honeypot

1. Low-Involvment Honeypot

   Low involvment honeypot merupakan *honeypot* dengan tingkat interaksi *honeypot*, yang didesain untuk mengemulasikan *service* (layanan) seperti *server* yang asli. Penyerang hanya mampu memeriksa dan terkoneksi ke

satu atau beberapa *port* (Laksana dkk, 2017). *Low Involvement Honeypot* merupakan yang paling mudah diinstal dan dipelihara karena desainnya yang sederhana dan fungsionalitas dasar. Normalnya teknologi ini hanya meniru berbagai macam *service*. Contohnya, *honeypot* dapat meniru *server* Unix dengan beberapa *service* yang berjalan, seperti Telnet dan FTP.

Honeypot tingkat ini mensimulasikan hanya sejumlah bagian layanan seperti *network stack*. Penyusup tidak bias memperoleh akses penuh ke *honeypot*. Meskipun terbatas, tetapi berguna untuk memperoleh informasi mengenai probing jaringan atau aktivitas worm (Utdirartatmo,2005).

Kelebihan *low involvement honeypot* yaitu:

a. Mudah diinstall, dikonfigurasi, dikembangkan, dan dimaintain.
b. Mampu mengemulasi suatu layanan seperti http, ftp, telnet, dan lainnya.
c. Berfungsi untuk mendeteksi serangan, khususnya pada proses *scanning* atau percobaan pembukaan koneksi pada suatu layanan.

Kekurangan low involvement honeypot:

a. Layanan yang diberikan hanya berupa emulasi, sehingga penyerang tidak dapat berinteraksi secara penuh dengan layanan yang diberikan atau sistem operasinya secara langsung.
b. Informasi yang didapatkan dari penyerang sangat sedikit.

c. Apabila serangan dilakukan oleh *real person* bukan *automated tools* mungkin akan segera menyadari bahwa yang sedang dihadapi merupakan mesin *honeypot*, karena keterbatasan layanan yang bisa diakses (Utdirartatmo,2005).

2. Medium Involvement Honeypot

Medium involvement honeypot menyediakan kemampuan interaksi yang lebih bila dibandingkan dengan *low involvement honeypot* namun fungsionalitasnya masih dibawah *high involvement honeypot*. Contohnya, *honeypot* dapat dibuat untuk meniru Microsoft IIS *web server* termasuk fungsionalitas tambahan yang biasa terdapat pada dirinya. IIS *web server* yang ditiru dapat dirubah sesuai dengan keiginan penyerang. Ketika koneksi HTTP dibuat oleh *honeypot*, ia akan merespon sebagai IIS *web server* dan memberikan peluang kepada penyerang.

Kelebihannya *medium involvement honeypot*:

a. Memiliki kemampuan yang lebih banyak untuk berinteraksi dengan penyerang dibandingkan *low-involvement honeypot* namun tidak sebanyak *high-involvement honeypot*.
b. Emulasi layanan dapat ditambahkan berbagai macam fitur tambahan sehingga seakanakan penyerang benar-benar sedang berinteraksi dengan layanan yang sebenarnya.

Kekurangan Medium Involvement Honeypot:

a. Sistem tersebut cukup kompleks.

b. Memerlukan usaha lebih untuk maintain dan pengembangan sistem tersebut sehingga akses yang diberikan kepada penyerang benar-benar terjamin tingkat keamanannya namun tetap dapat memberikan suasana sistem yang nyata bagi penyerang sehingga penyerang tersebut tidak curiga bahwa aktivitasnya sedang dimonitor (Utdirartatmo,2005).

3. High-Interaction Honeypot

High-interaction honeypot terdapat system opeasi dimana penyerang dapat berinteraksi langsung dan tidak mempunyai batasan yang dapat membatasi interaksi tersebut. Dengan kata lain jenis honeypot ini membuat *server* palsu yang menyerupai dengan *server* asli, sehingga penyerang tidak mencurigai saat terjadi penyerang (Laksana dkk, 2017). *High involvement honeypot* adalah teknologi *honeyspot* yang paling ekstrim. Ia memberikan informasi yang sangat banyak mengenai penyerang tapi memerlukan waktu untuk mendapatkannya. Tujuan dari *high involvement honeyspot* adalah memberikan akses sistem operasi yang nyata kepada penyerang dimana tidak ada batasan yang ditentukan. *High involvement honeypot* sangatlah sulit dan menghabiskan waktu untuk dinstal dan dikonfigurasikan. Berbagai macam teknologi yang berbeda terlibat disini seperti firewall atau Intrusion Detection Sistem (IDS) haruslah disesuaikan dengan seksama. Pemeliharaannya pun menghabiskan waktu, seperti menmperbaharui *rulebase firewall* dan *signature database* IDS serta mengawasi *honeyspot* terus menerus. *High-*

involvement honeypot akan menjadi solusi yang baik apabila diimplementasikan dengan benar, dan begitu pula kebalikannya jika *high-involvement honeypot* tidak diimplementasikan dengan benar maka penyerang dapat mengambil alih dan ia akan menjadi *boomerang* yang berbahaya. *Honeypo*t juga dapat dibedakan menjadi dua. Pertama adalah physical, yaitu mesin sungguhan dalam jaringan dengan alamat IP sendiri. Dan Virtual yaitu *honeypots* yang disimulasikan oleh mesin lain yang merespon pada *traffic* jaringan yang dikirim ke *virtual honeypot*. Suatu *honeypots* merupakan sumber sistem informasi yang menghasilkan nilai palsu pada saat terjadi penggunaan sumber daya yang tidak sah tidak diizinkan (Candra, 2014).

2.2.10 Penempatan Honeypot

1. Internal

Penempatan *honeypot* didalam jaringan internal adalah cara yang baik untuk membuat system *early-werning* yang akan memberi informasi akan ancaman yang datang dari luar dan dalam jaringan lokal. Penempatan *honeypot* pada lokasi ini akan menambah resiko pada jaringan *private* karena bila *honeypot* berhasil disusupi dan diambil alih maka penyerang akan mendapatkan akses menuju jaringan *private* dari *honeypot*, dengan kata lain *honeypot* akan dapat digunakan sebagai batu loncatan untuk menyerang jaringan *private* (Prasetyo, 2007).

2. Eksternal

Lokasi ini merupakan penempatan yang paling tepat jika ingin mendeteksi penyerangan dari luar, karena *honeypot* secara langsung terkoneksi pada internet sehingga mudah ditemukan dan diserang. Penempatan *honeypot* diluar jaringan komputer lokal akan mengurangi resiko terhadap jaringan internal dan *honeypot* akan dapat dengan mudah ditemukan. Biasanya honeypot diletakan didepan *firewall* terluar dari suatu topologi jaringan komputer. Kelebihan dari penempatan *honeypot* dilokasi ini adalah *honepot* akan dianggap sama seperti sistem eksternal sehingga akan mengurangi resiko terhadap jaringan *private* ,apabila *honeypot* berhasil disusupi atau diambil alih oleh penyerang. Kekurangan dari penempatan ini adalah trafik-trafik tidak sah yang dicatat oleh *honeypot* tidak akan tercatat dan membangkitkan *alert* oleh *firewall* dan IDS sehingga informasi sangat berkurang. Kekurangan lainnya apabila penyerang berasal dari dalam jaringan lokal sehingga sulit mendeteki serangan tersebut (Prasetyo, 2007).

3. DMZ (*Demilitarized Zone*)

Penempatan *honeypot* dilokasi ini merupakan solusi terbaik untuk mengimplementasikan *honeypot*. Hal ini disebabkan karena DMZ terletak diantara jaringan internal dan jaringan eksternal. Pada *gateway* biasanya terdapat pengamanan sama seperti *firewall* sehingga trafik tidak sah yang menuju *honeypot* akan melewati *firewall* akan tercatat di *firewall log* dan menambah informasi yang terkumpul. Kelemahan

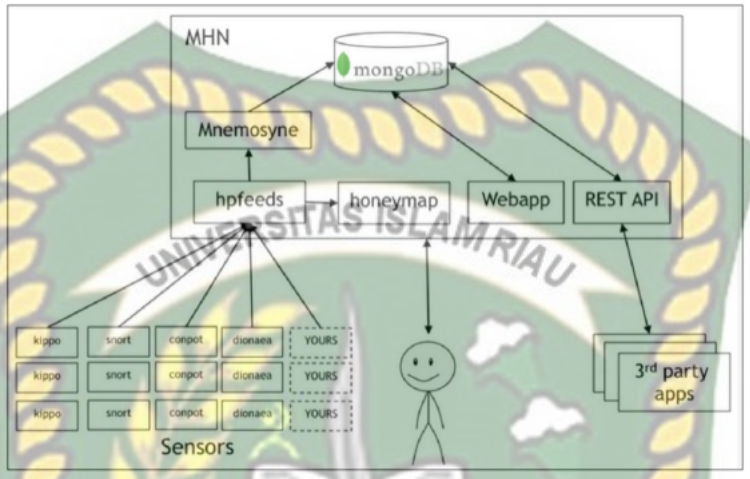
penempatan ini adalah sistem lain yang berada di DMZ harus di amankan dari *honeypot* karena bila *honeypot* berhasil disusupi dan diambil alih maka kemungkinan *honeypot* tersebut dapat digunakan untuk menyerang sistem lain yang berada di DMZ (Prasetyo, 2007).

2.2.11 MHN

MHN adalah *software open source* yang dibuat oleh perusahaan ThreatStream, yang bertujuan untuk mempermudah menginstalasi *honeypot*. Adapun kegunaan dari MHN ini adalah mengelola dan menganalisa data dari *honeypot* tersebut dan mempermudah membangun *honeypot* baru dan mengambil data. Ada beberapa *honeypot* yang sudah terintergrasi oleh Modern Honey Network (MHN) antara lain hpfeed, nmomesyne, honeymap, MongoDB, dionaea, conpot, snort, kippo, glastopf, amun, dan wordpot (Laksana dkk, 2017). MHN adalah sistem manajemen *honeypot* yang memungkinkan beberapa sensor *honeypot* seperti: *Snort* dan yang lainnya untuk membuat jaringan pertahanan yang aktif dan berfungsi secara keseluruhan dalam beberapa menit. MHN menggunakan satu set sensor untuk mengumpulkan data-data yang terkait dengan penyerangan pada jaringan. MHN menganalisis penyerangan dan memetakan parameter serangan menjadi tampilan *World Map* dengan tetap menjaga banyaknya jumlah informasi tentang penyerangan, sehingga membuatnya sangat visual dan intuitif.

MHN membuat penerapan dan pengelolaan *honeypot*s menjadi lebih mudah dan sangat sederhana. Dari pengelolaan yang lebih mudah, MHN selalu memberikan produk *honeypot* terbaru. MHN benar-benar *software* gratis *open*

source yang mendukung penyebaran dan pengelolaan *honeypot* eksternal dan internal pada skala besar. MHN menggunakan standar HPFeeds. Gambar 2.1 berikut ini adalah arsitektur *Modern Honey Network*:



Gambar 2.2. Arsitektur *Modern Honey Network*

*Honeypot*s belum belum dianggap sebagai pertahanan secara keseluruhan, terutama karena manajemen proses yang rumit disediakan untuk keamanan bagi suatu perusahaan. MHN adalah proyek *open source* untuk membuat active-defense yang memanfaatkan lebih banyak *honeypot* dan banyak digunakan untuk keamanan perusahaan(Wafi, 2016).

2.2.12 Intrusion Detection System

Intrusion Detection System adalah sebuah alarm keamanan yang dikonfigurasi untuk melakukan pengamatan terhadap access point (Affandi, 2016). aktifitas host. dan kegiatan penyusupan. Cara paling sederhana untuk mendefinisikan IDS mungkin tergantung dari bagaimana mendeskripsikan IDS sehagai tool spesial yang dapat membaca dan mengintepretasikan isi dari file-file

log dari router, firewall serve,r dan perangkat jaringan lainnya. Secara lebih Jurnal Teknologi Informasi Vol. 4 No. 2 100 spesifik, Intrusion Detection System adalah sebuah sistem yang dapat mendeteksi adanya penggunaan tak ter-autorisasi (unauthorized use) pada sebuah sistem jaringan.

IDS yang digunakan dalam penelitian menggunakan snort merupakan salah satu contoh program Network-based Intrusion Detection System, yaitu sebuah program yang dapat mendeteksi suatu usaha penyusupan pada suatu sistem jaringan komputer. Snort bersifat open source dengan lisensi GNU General Purpose License sehingga software ini dapat dipergunakan untuk mengamankan sistem server tanpa harus membayar biaya lisensi.

2.2.13 Tools Pengujian

1. Nmap

   Nmap (*Network Mapper*) adalah sebuah program *open source* yang berguna untuk mengeksplorasi jaringan. Nmap didesain untuk dapat melakukan scan jaringan yang besar, juga dapat digunakan untuk melakukan *scan host* tunggal. Nmap menggunakan paket IP untuk menentukan *host-host* yang aktif dalam suatu jaringan *port-port* yang terbuka, sistem operasi yang dipunyai, tipe *firewall* yang dipakai. Fungsi utama dari Nmap adalah sebagai *port scanning*, menurut definisinya *scanning* adalah kegiatan *probe* dalam jumlah yang besar dengan menggunakan *tool* secara otomatis, dalam hal ini adalah Nmap. Sebuah *scanner* sebenarnya adalah *scanner* untuk *port* TCP/IP, yaitu sebuah program yang menyerang *port* TCP/IP dan servis-servisnya (telnet, ftp, http, dan lain - lain) dan mencatat respon dari komputer target. Dengan

cara ini, user program *scanner* dapat memperoleh informasi yang berharga dari *host* yang menjadi target (Rosnelly & Pullungan, 2011).

2. Snort

   Sebuah program yang dapat mendeteksi suatu usaha penyusupan pada suatu sistem jaringan komputer. Snort bersifat open source dengan lisensi GNU.

3. HoneyPy

   HoneyPy adalah suatu program yang dibuat menggunakan bahasa pemrograman *python* dan sangat "*powerfull*" dalam berinteraksi untuk memanipulasi paket di jaringan.

BAB III

METODOLOGI PENELITIAN

3.1 Gambaran Umum Objek Penelitian

Berdasarkan dengan penghantar pendahuluan, batasan penelitian, dan tinjauan pustaka yang dijelaskan pada bab-bab sebelumnya, penelitian yang akan dilakukan adalah merancang dan mengimplementasikan *modern honey network* (*snort*) untuk alat bantu keamanan jaringan data *wireless* di Dinas Perpustakaan dan Kearsipan Kota Pekanbaru yang sebelumnya hanya berupa *firewall*.

Masalah jaringan yang sering di alamai dinas Dinas Perpustakaan dan Kearsipan Kota Pekanbaru adalah gangguan pada saat pencarian buku yang hendak di cari oleh pengunjung, sering kali mendapatkan gangguan jaringan akibat tidak adanya konsentrasi atau server jaringan yang khusus untuk komputer pencarian buku

3.2 Metodologi Penelitian

Metode penelitian di bidang ilmu computer adalah peneitian di bidang Ilmu Komputer yang merupakan ilmu yang sangat kompleks, sedemikian luasnya bidang ini sehingga penelitian dalam bidang ini juga menjadi demikian luasnya. Berbagai jurnal penelitian dalam bidang Ilmu Komputer menggunakan beberapa Metode. Dari beberapa penelitian pada Ilmu Komputer terlihat bahwa penelitian di bidang ini dapat dikategorikan menjadi 2 (dua) yakni :

a. Penelitian berfokus pada Metode Penelitian

b. Penelitian berfokus pada suatu bidang area penelitian

Metode pengambilan data merupakan proses untuk mendapat atau mencari data untuk melakukan penelitian. Data yang dikumpulkan merupakan data yang mendukung untuk melakukan perancangan alat yang dibutuhkan dan penempatan implementasi MHN. Adapun data-data yang dibutuhkan, yaitu:

3.3 Teknik Pengumpulan Data

3.3.1 Studi Literatue

Studi literatur merupakan pembelajaran materi materi terkait, baik itu penelitian terdahulu yang digunakan sebagai pembeda dengan penelitian saat ini. Materi tersebut berasal dari berbagai referensi atau sumber–sumber ilmiah lainnya seperti jurnal ilmiah, buku–buku yang terkait dengan skripsi.

1. Data Primer

   Data primer merupakan data yang diperoleh langsung dari objek yang akan diimplementasikan, objek yang akan dianalisis ialah Dinas Perpustakaan dan Kearsipan Kota Pekanbaru dengan menerapkan MHN dengan bantuan aplikasi proxmox, sistem operasi ubuntu dan juga *software* MHN dengan snort.

2. Data Sekunder

   Data sekunder merupakan data pendukung yang didapatkan melalui jurnal dan skripsi nasional bahkan internasional dari penelitian terdahulu. Hal ini bertujuan untuk mendapatkan teori yang sesuai dengan penelitian terkait sehingga penelitian tersebut memiliki landasan yang kuat.

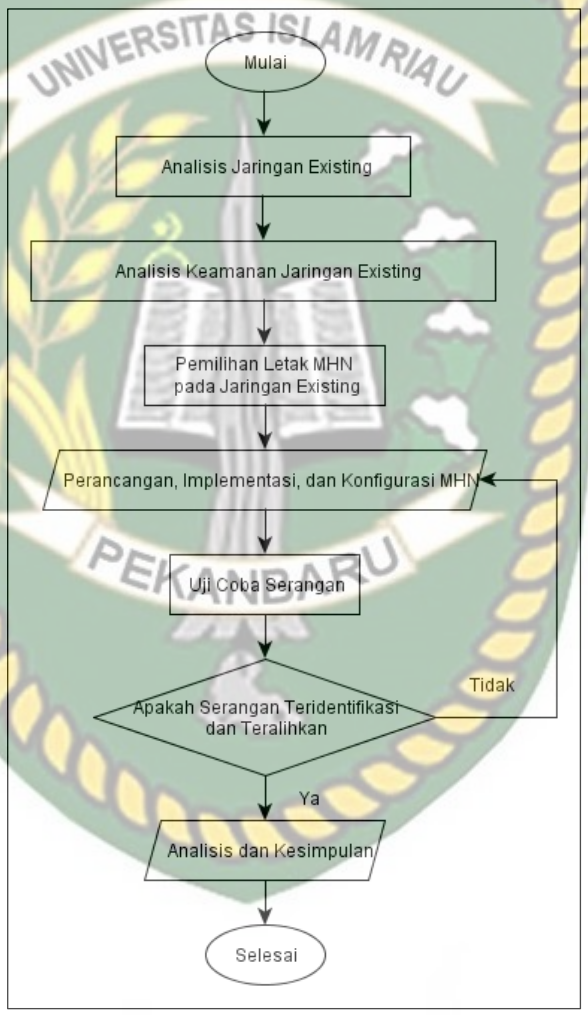
3.3.1 Studi Bimbingan

Dalam melaksanakan penelitian ini penulis melakukan studi bimbingan dengan cara berdiskusi dan meminta saran dengan dosen pembimbing serta

pembimbing lapangan untuk menyelesaikan masalah masalah yang terjadi saat melaksanakan penelitian.

3.4 Tahapan Teknik Penelitian

Diagram alir berguna untuk memudahkan untuk proses penelitian dari tahap awal hingga selesai dan mudah untuk menganalisa. Langkah kerja pada diagram alir dapat dilihat pada gambar 3.1.



Gambar 3.1 Alur Kerja Penelitian

3.5 Alat Penelitian

Adapun *software* dan *hardware* yang dibutuhkan dalam penelitian berikut adalah :

3.5.1 Perangkat Keras

a. Router Mikrotik

Tipe: RB1100AHX2

Spesifikasi: CPU Freescale P2020 1066Mhz *Dual Core* RAM 1.5GB *Main Storage* 64MB Ethernet 13 Ports.

Jumlah: 1 buah

b. Switch

Tipe: D-Link DES-1008A

Jumlah: 1 buah

c. Komputer *Server*

Spesifikasi: Intel(R) Xeon(R) CPU E5-1607 v2 RAM 16GB

Jumlah: 1 buah

d. Komputer Penyerang

Spesifikasi: Processor Intel Core i5-6200U RAM: 4GB HDD: 1 TB

Jumlah : 1 buah

3.5.2 Perangkat lunak

Untuk *software*, dibedakan menjadi 2 yakni *software* pada *server*, dan *software* pada komputer penyerang.

1. Perangkat Lunak Server

   a. *Ubuntu server* 14.04 *LTS*

   Spesifikasi: *Processor* 2 *core*, RAM 2GB, *Hard disk* 32GB.

   b. *Snort*

   c. *HoneyPy*

   d. *honeypy web*

2. Perangkat Lunak pada Computer Attacker

   a. Aplikasi Nmap

3.6 Skema Perencanaan / Scenario Penelitian

Adapun skema penelitian yang akan dilakukan dalam penelitian ini adalah sebagai berikut:

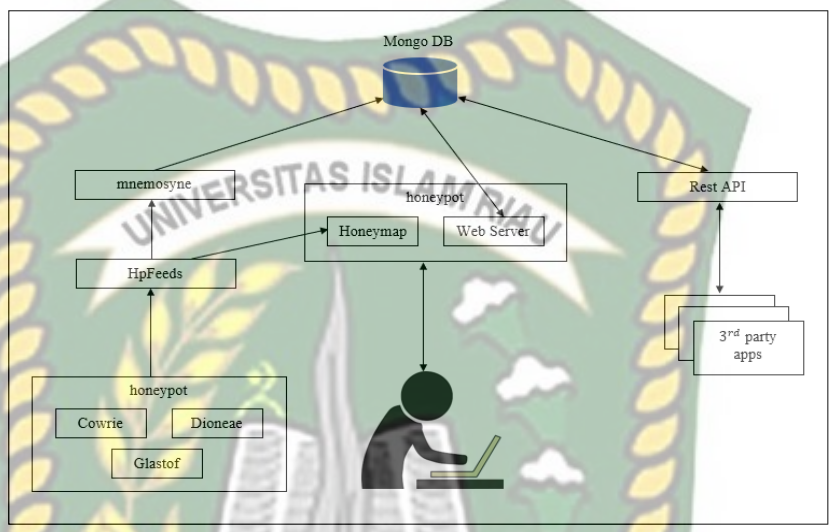
3.6.1 Analisi Jaringan Existing

Dinas Perpustakaan dan Kearsipan Kota Pekanbaru memiliki 2 buah ISP untuk memberikan layanan internet kepada pengguna. Terdapat 4 buah router, 4 buah switch, 2 access point di gedung A, dan 2 access point digedung C dan 6 buah access point ditiap lantai gedung B. Jenis keamanan yang sudah berlaku di Dinas Perpustakaan dan Kearsipan Kota Pekanbaru adalah *firewall*. Serangan yang datang hanya bisa dideteksi dan memunculkan peringatan tanpa adanya identifikasi pelaku serangan dan juga pengamanan dengan aplikasi deepfrezz pada PC yang bisa digunakan oleh pengunjung. Padahal serangan yang masuk dapat membahayakan data-data dalam *database* maupun sistem yang berlaku di sana. Untuk itu, identifikasi pelaku, informasi-informasi serangan *port*, dan berbagai informasi lain dibutuhkan dalam mengatasi permasalahan serangan keamanan jaringan yang terjadi. MHN dapat membantu meningkatkan lapisan keamanan jaringan di Dinas Perpustakaan dan Kearsipan Kota Pekanbaru.

3.6.2 Arsitektur Honeypot

Pada penelitian ini, digunakan aplikasi Snort yang dapat mengembangkan dan mengelola *honeypot* secara cepat dan mudah, sebab Snort memiliki *interface web* yang memudahkan admin untuk melakukan fungsi

tersebut. Tidak hanya itu, Snort juga merupakan aplikasi berbasis *open source* yang mendukung pengembangan dan pengelolaan *honeypot* yang dapat didistribusikan dalam skala besar, eksternal maupun internal. Gambar 3.2 berikut menunjukan tampilan dari Snort.



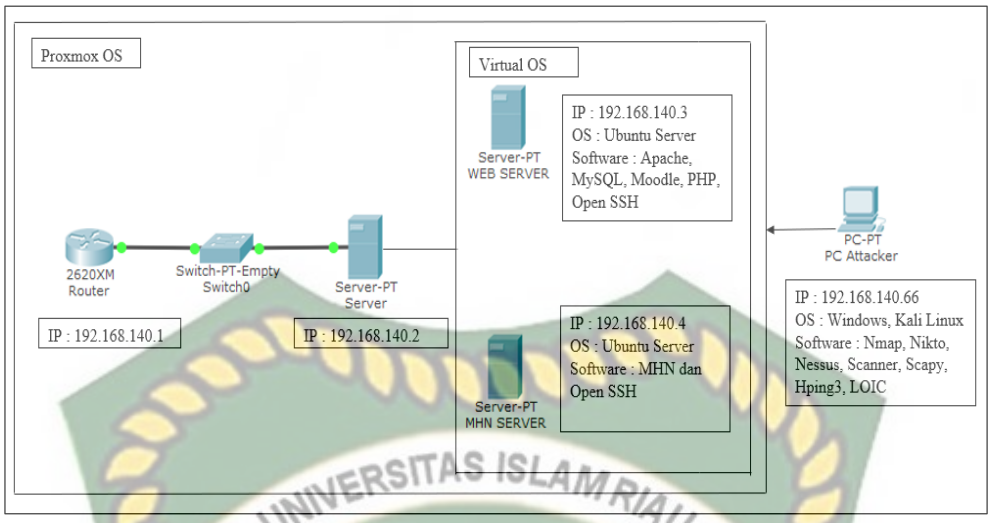
Gambar 3.3 Arsitektur *Honeypot*

Berdasarkan gambar 3.3 diatas, dapat disimpulkan bahwa aktifitas jaringan yang mencurigakan pada *web server* yang sebelumnya telah diinstall *honeypot*. Pada gambar tersebut terdapat *honeymap* dilingkungan *honeypot* yang tidak masuk kedalam *database honeypot* sebab tugas dari *honeymap* adalah memetakan *honeypot*.

3.6.3 Perancangan Honeypot

Honeypot dirancang agar memungkinkan terjadinya serangan. Perancangan ini menggunakan *server virtual* proxmox. *Honeypot* ini dibangun dengan menggunakan dari paket Snort sehingga *honeypot* ini tidak langsung terpasang pada *host*, melainkan pada *server*.

Gambar 3.4 berikut ini adalah skema dari perancangan MHN di Dinas Perpustakaan dan Kearsipan Kota Pekanbaru:



Gambar 3.4 Perancangan *Honeypot*

Dari gambar 3.4, dapat dijelaskan bahwa perancangan MHN berupa:

1. Sever telah ter-*install software* Snort, yang dalam Snort tersebut telah terinstal dua sistem operasi Ubuntu *server*
2. Untuk mendapatkan IP yang berbeda, jaringan dari kedua *virtual server*(*web server* dan MHN *server*) dikonfigurasikan menjadi *bridge*.
3. *MHN server* menanamkan sistem *honeypot* pada *web server*.
4. *Web server* dan MHN *server* diakses melalui Snort untuk dikonfigurasikan.
5. IP kedua *virtual server* dijadikan publik, sehingga dapat diakses oleh semua orang.
6. Pengujian dilakukan dengan serangan pada jaringan *wireless*.

3.6.4 Perancangan dan konfigurasi

1. Instalasi Snort

   Instalasi Snort dilakukan pada *server*. Didalam *software* Snort ini akan dijadikan tempat untuk menginstal dua *server* ubuntu, untuk mencatat lalu lintas server.

2. Instalasi Web Server

   Pada penelitian kali ini, *web server* yang akan dibuat adalah *web sever*. Setelah semua komponen terinstall.

3. Installasi dan Konfigurasi MHN Server

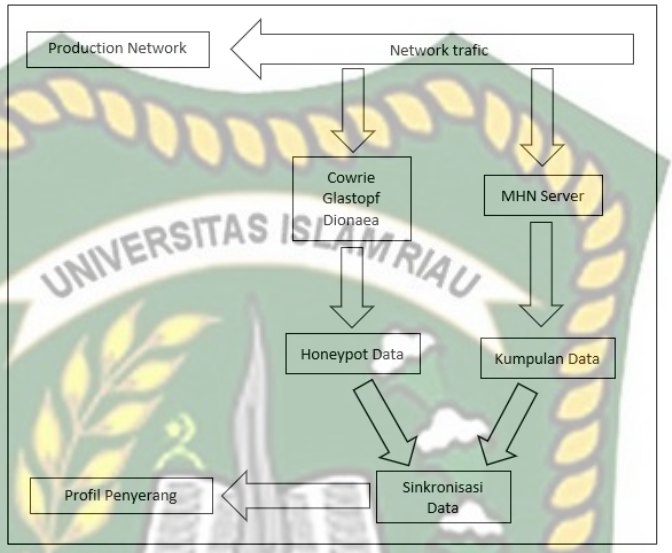
   Instalasi MHN dilakukan pada proxmox. Sebelumnya, komponen-komponen untuk menjalankan MHN *server* harus dipastikan telah terinstal. Setelah dilakukan installasi MHN *server*, *service-service honeypot* diinstall pada jaringan lokal terlebih dahulu dan nantinya jaringan tersebut akan diubah menjadi jaringan *public* dengan melakukan konfigurasi Mnemosyne. Selanjutnya konfigurasi MHN *server* baru bisa dikerjakan.

4. Implementasi Honeypot

   Implementasi *honeypot* langsung dilakukan pada *web server* dengan mengakses dan merujuk pada MHN *server web* melalui *browser*. Dalam hal ini *honeypot* yang akan diimplementasi adalah cowrie, glastopf, dan dionaea.

3.6.5 Alur Penangkapan Serangan pada Honeypot

Gambar 3.5 berikut menunjukann alur dari penangkapan serangan pada *honeypot*:



Gambar 3.5 Alur penangkapan serangan pada honeypot

Berdasarkan gambar 3.5 diatas maka alur serangan pada honeypot dapat dijelaskan sebagai 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 *input* kebagian *production network* dan 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*. Kedua, paket tersebut diproses web server yang didalamnya telah diinstall kumpulan honeypot (snort). Berikut tabel 3.1 keterangan jenis honeypot dan port yang ditanganinya:

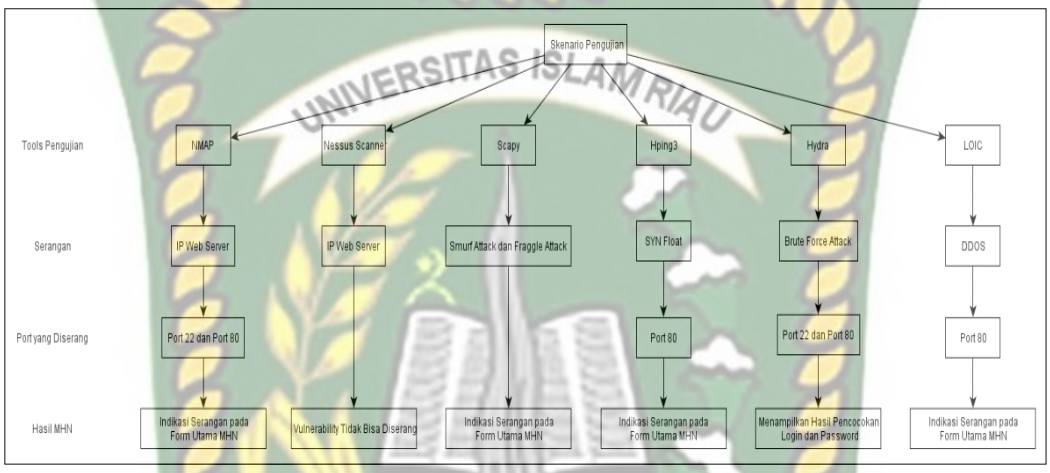
Tabel 3.1 *Honeypot* dan *port* yang ditanganinya

MHN	PORT
Snort	Port SSH
Snort	Port HTTP
Snort	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
	tcp/5060 : SIP *Protocol*
	tcp/69 : TFTP

2. Paket yang masuk dan diproses oleh *honeypot* dianggap sebagai *intrusion* dan nantinya dimasukan dalam data *honeypot* serta diolah menjadi sekumpulan data.
3. Paket yang telah diproses oleh MHN server dianggap sebagai aktivitas yang mencurigakan lalu dikumpulkan dan diolah menjadi sekumpulan data.
4. Data yang sudah diolah dari MHN *server* dan *honeypot* disinkronisasikan dan menghasilkan data penyerangan.

3.6.6 Pengujian Terhadap Serangan

Pengujian terhadap honeypot yang telah diimplementasi meliputi *port scanning*, DoS melalui *ping of death*, DDoS, dan juga *brute force attack*. Serangan dilakukan seperti pada gambar 3.6 dibawah:



Gambar 3.6 *Tools* Pengujian Serangan

Berdasarkan gambar 3.6 diatas, maka penyerangan dilakukan dengan menggunakan aplikasi *open source* seperti:

a. Nmap

Pengujuan menggunakan Nmap untuk melakukan *port scanning* yang diarahkan menuju IP *web server*. Pengujian ini dilakukan terhadap *honeypot-honeypot* yang dipasang pada *web server*. Pengujian *port scanning* dilakukan pada port 22 untuk menguji cowrie, dan *port* 80 untuk menguji glastopf.

b. Honeypy

Pengujian selanjutnya menggunakan *Software honeypy* yang ditujukan pada *honeypot*. Pengujian dilakukan dengan memasukkan IP computer target yakni IP *web server*.

c. LOIC

LOIC digunakan untuk melakukan serangan DDOS. DDoS merupakan salah satu jenis serangan *Denial of Service* yang menggunakan banyak *host* penyerang sekaligus untuk menyerang satu buah *host* target dalam sebuah jaringan. DDOS merupakan jenis serangan yang berbahaya karena dapat melumpuhkan aktifitas sistem. Pengujian dilakukan terhadap *web server* yang telah dipasang honeypot melalui *port* 80.

3.7 Analisa Hasil

Hasil yang akan didapatkan dalam pengimplementasian *Modern Honey Network* adalah pengalihan serangan, serangan tersebut dapat teridentifikasi, informasi yang diterima penyerang dapat dipalsukan dan serangan dapat dihindari. Dengan demikian, keamanan jaringan pada Dinas Perpustakaan dan Kearsipan Kota Pekanbaru dapat meningkat.

3.7.1 Penulisan Laporan

Proses akhir dalam penelitian ini adalah membuat laporan yang berisi uraian-uraian dan hasil yang didapat dalam melaksanakan penelitian. Laporan ini nantinya akan digunakan sebagai syarat untuk menyelesaikan program S1 Teknik Informatika Universitas Islam Riau. Pengerjaan laporan ini dibuat menjadi 2 tahapan, di mana tahap pertama yaitu pembuatan proposal yang berisi bab 1,2,3 untuk seminar proposal dan laporan akhir yang digunakan untuk seminar hasil.

BAB IV

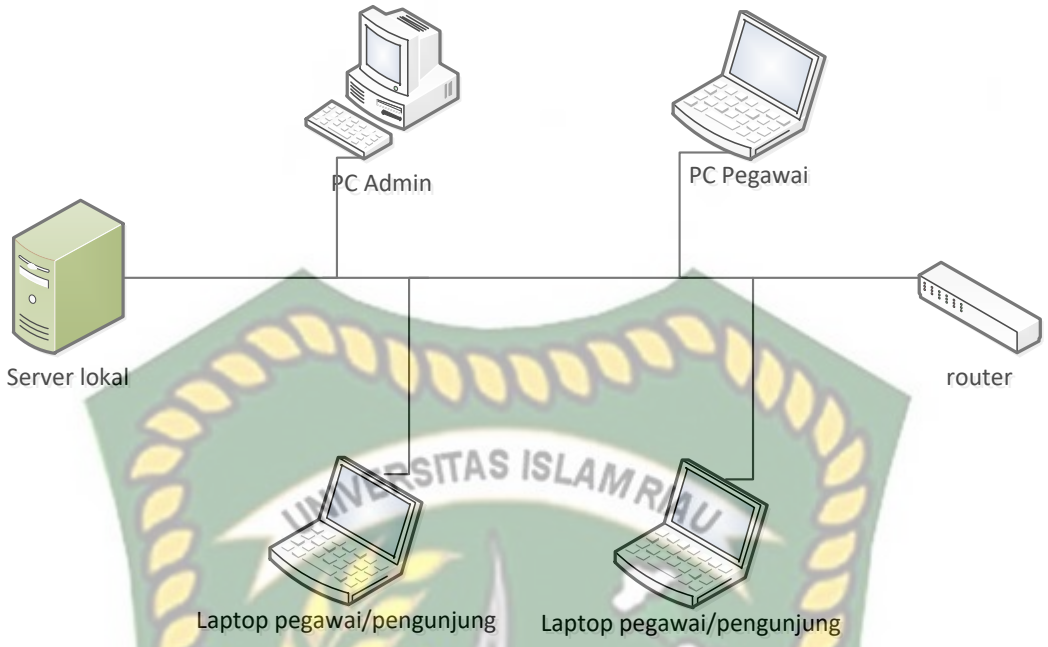
HASIL DAN PEMBAHASAN

4.1 Implementasi Perangkat Keras

Implementasi sistem ini dilakukan dengan spesifikasi perangkat keras dan lunak sebagai berikut:

1. Spesifikasi perangkat keras yang dipakai yaitu:
   a. Laptop Server dan Client Prosessor (minimal) Intel Pentium.
   b. RAM minimal 4 GB dan HardDisk minimal 320 Gb.
   c. Router Mikrotik Versi Hap Lite.
   d. Kabel RJ45 3 buah.
2. Spesifikasi perangkat lunak yang dipakai yaitu:
   a. Ubuntu 14.
   b. Nmap.
   c. Snort
   d. HoneyPy
   e. Honeypy Berbasis Web
   f. Winbox

Konfigurasi jaringan pada Perpustakaan Daerah Pekanbaru menggunakan topologi star yang terdiri dari router dan Komputer server. Berikut ini adalah gambaran topologi jaringan pada Perputakaan Daerah Pekanbaru.



Gambar 4.1 Topologi Jaringan

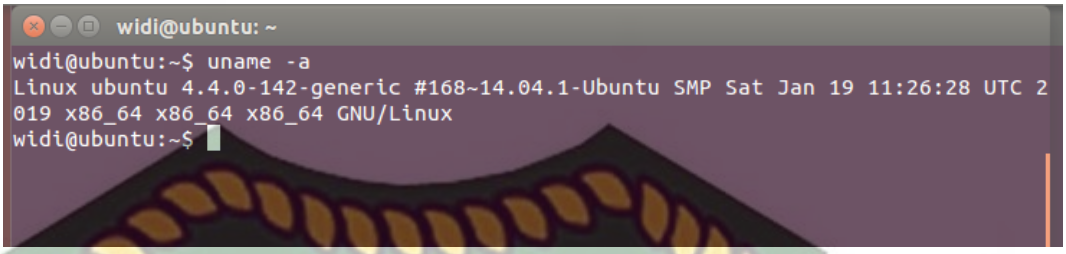
Pada gambar 4.1 mikrotik di hubungkan dengan dua kabel LAN yang masing-masing digunakan untuk koneksi ke modem wifi Indihome (putih) dan koneksi ke LAN laptop atau PC (biru).

4.2 Implementasi Pada Komputer Server

Pada penelitian yang dilakukan oleh penulis akan menganalisa keamanan jaringan pada Perpuskaan Daerah Pekanbaru. Dalam penelitian Analisa dilakukan dengan menguji dasar penyarangan jaringan yang dapat dilakukan dengan scanning, Ddos Attack atau sniffing.

Maka pada penelitian ini penulis akan menggunakan HoneyPot yang dimaksudkan untuk mengecohkan hacker penyerang dalam menyerang computer server. Honeypot yang akan dipasang pada computer server akan menggunakan software HoneyPy yang dibangun dengan menggunakan Bahasa python. Berikut ini adalah proses pemasangan HoneyPot pada computer server. Komputer server yang terpasang di Perpustakaan menggunakan system operasi Ubuntu Versi 14.

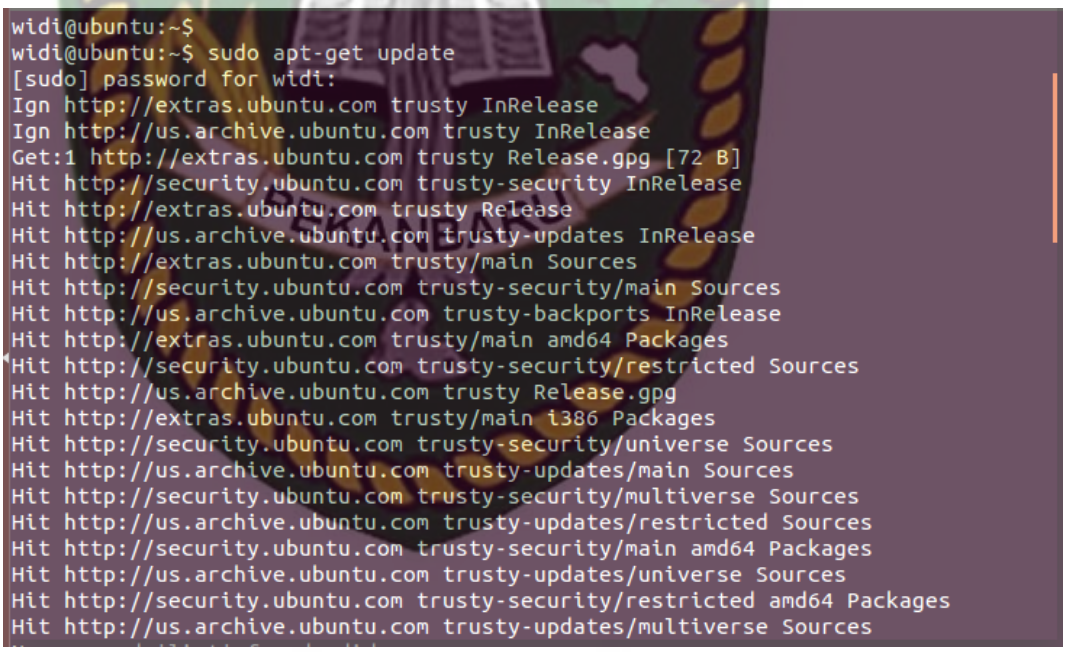
1. Pengecekan versi OS yang digunakan pada computer server. Berikut ini adalah proses pengecekan OS di computer server.



Gambar 4.2 Cek Os Server

Pada gambar 4.2 dijelaskan bahwa computer server menggunakan system operasi Ubuntu versi 14.04.1.

2. Menginstall Git pada computer server yang digunakan untuk pengambilan kode atau paket dari github.



```
wd@ubuntu:~$ sudo apt-get install git
[sudo] password for wd:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  git-man liberror-perl
Suggested packages:
  git-daemon-run git-daemon-sysvinit git-doc git-el git-email git-gui gitk
  gitweb git-arch git-bzr git-cvs git-mediawiki git-svn
The following NEW packages will be installed:
  git git-man liberror-perl
0 upgraded, 3 newly installed, 0 to remove and 61 not upgraded.
Need to get 3,459 kB of archives.
After this operation, 22.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://us.archive.ubuntu.com/ubuntu/ trusty/main liberror-perl all 0.17-1.
1 [21.1 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu/ trusty-updates/main git-man all 1:1.9
.1-1ubuntu0.10 [700 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu/ trusty-updates/main git amd64 1:1.9.1
-1ubuntu0.10 [2,737 kB]
```

Gambar 4.3 Install Git

3. Jika sudah melakukan penginstalan git maka selanjutnya pengambilan paket HoneyPy dan honeypy di github yang digunakan untuk proses honeypot di computer server. Berikut ini adalah hasil pengambilan paket Honeypy dan honeypie.

```
wd@ubuntu:~$ git clone http://github.com/foospidy/HoneyPy
Cloning into 'HoneyPy'...
remote: Enumerating objects: 2687, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 2687 (delta 1), reused 0 (delta 0), pack-reused 2681
Receiving objects: 100% (2687/2687), 2.82 MiB | 1.47 MiB/s, done.
Resolving deltas: 100% (1594/1594), done.
Checking connectivity... done.
wd@ubuntu:~$
```

```
wd@ubuntu:~$ git clone http://github.com/shipcod3/honeypy
Cloning into 'honeypy'...
remote: Enumerating objects: 106, done.
remote: Total 106 (delta 0), reused 0 (delta 0), pack-reused 106
Receiving objects: 100% (106/106), 338.29 KiB | 0 bytes/s, done.
Resolving deltas: 100% (48/48), done.
Checking connectivity... done.
wd@ubuntu:~$
```

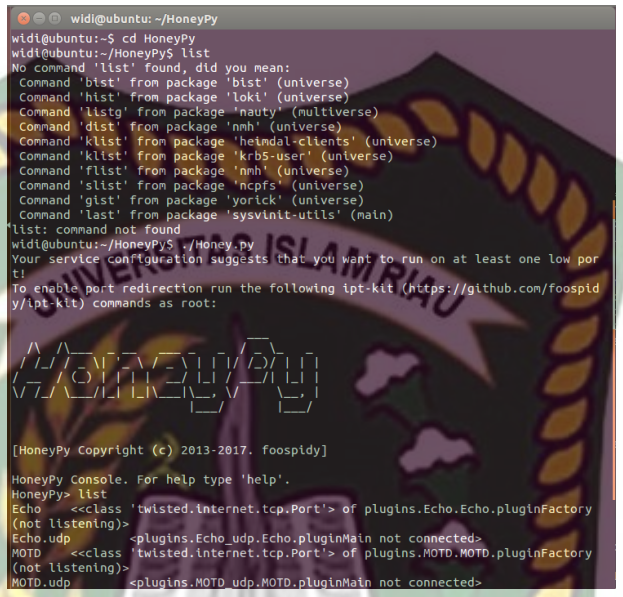
Gambar 4.4 Clone HoneyPy dan honeypy

Hasilnya dapat dilihat dengan menggunakan sintak ls pada terminal.

```
wd@ubuntu:~$ ls
Desktop    Downloads         honeypy  Music     Public     Videos
Documents  examples.desktop  HoneyPy  Pictures  Templates
wd@ubuntu:~$
```

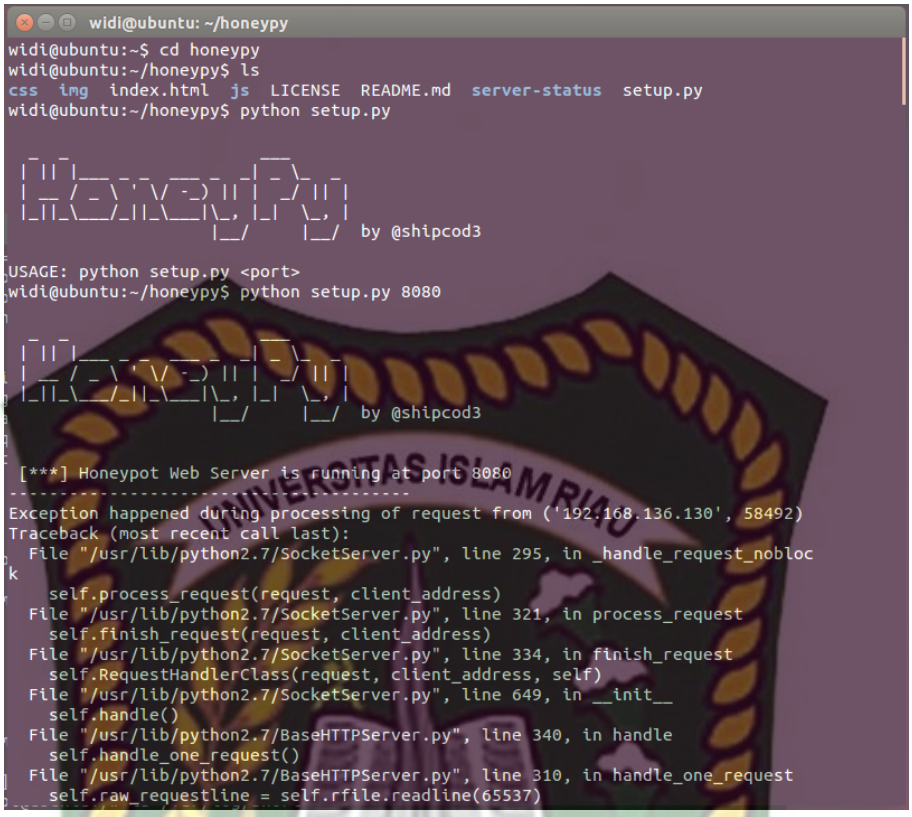
Gambar 4.5 Hasil Clone

4. Setelah melakukan penginstallan honeypot selanjutnya jalankan honeypot yang sudah dimasukan dengan sintak ./Honey.py setelah masuk ke folder HoneyPy.



Gambar 4.6 *Jalankan HoneyPot*

Kemudian lakukan pengaktifan port 8080 untuk mengecoh hacker agar mengira banyak port terbuka di sisi server.



Gambar 4.7 Menjalankan honeypi Port 8080

Proses setting honeypot di computer sudah selesai selanjutnya penulis akan melakukan uji coba penyerangan dari computer client. Inti dari pemasangan honeypot adalah agar dapat mengecoh hacker yang berusaha memasuki computer server, dan admin computer server dapat melihat interaksi percobaan serangan yang dilakukan oleh hacker.

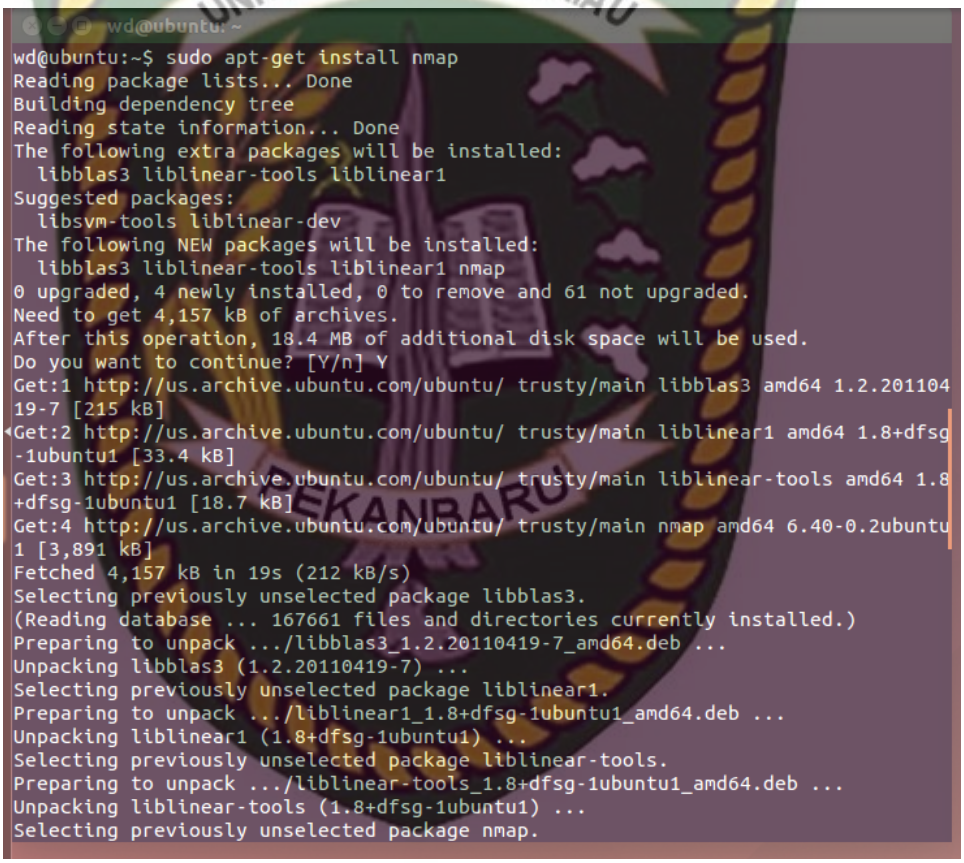
4.3 Implementasi Komputer Client

Pada computer client penulis akan mencoba melakukan beberapa serangan ke computer server dengan melakukan scanning, brute force attack dan Ddos Attack.

Komputer client akan menggunakan system operasi ubuntu karena mudah digunakan dan open source serta mempunyai tampilan yang baik dan friendly. Berikut ini adalah proses percobaan penyerangan yang dilakukan oleh penulis.

1. Scanning

   Percobaan pertama akan menggunakan nmap untuk scanning pada sisi computer server. Nmap akan diinstall terlebih dahulu dengan menggunakan sudo apt-get install nmap. Berikut hasilnya :



Gambar 4.8 Penginstallan Nmap Ubuntu

Setelah Langkah penginstalan Nmap selesai selanjutnya melakukan scanning untuk memperoleh alamat ip tujuan dan port yang terbuka. Berikut ini adalah proses scanning.

```
wd@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:b9:fe:7e
          inet addr:192.168.136.130  Bcast:192.168.136.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feb9:fe7e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4753 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2687 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5738956 (5.7 MB)  TX bytes:210743 (210.7 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:112 errors:0 dropped:0 overruns:0 frame:0
          TX packets:112 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:10603 (10.6 KB)  TX bytes:10603 (10.6 KB)
```

Gambar 4.9 Cek IP Komputer

Pengecekan IP computer sendiri dilakukan untuk mengetahui ip address dan rangenya. Pada kasus diatas ip address sudah dapat ditemukan yaitu 192.168.136.130. Jadi untuk proses scanning dapat menggunakan range IP 192.168.136.0/24 agar dapat diketahui IP address yang terhubung dengan jaringan yang sama.

```
wd@ubuntu:~$ nmap -n -sn 192.168.136.0/24

Starting Nmap 6.40 ( http://nmap.org ) at 2021-09-11 21:31 PDT
Nmap scan report for 192.168.136.2
Host is up (0.0022s latency).
Nmap scan report for 192.168.136.128
Host is up (0.00053s latency).
Nmap scan report for 192.168.136.130
Host is up (0.00022s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.32 seconds
wd@ubuntu:~$ nmap -n 192.168.136.128

Starting Nmap 6.40 ( http://nmap.org ) at 2021-09-11 21:32 PDT
Nmap scan report for 192.168.136.128
Host is up (0.0018s latency).
All 1000 scanned ports on 192.168.136.128 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
wd@ubuntu:~$ nmap -n 192.168.136.2

Starting Nmap 6.40 ( http://nmap.org ) at 2021-09-11 21:32 PDT
Nmap scan report for 192.168.136.2
Host is up (0.00066s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

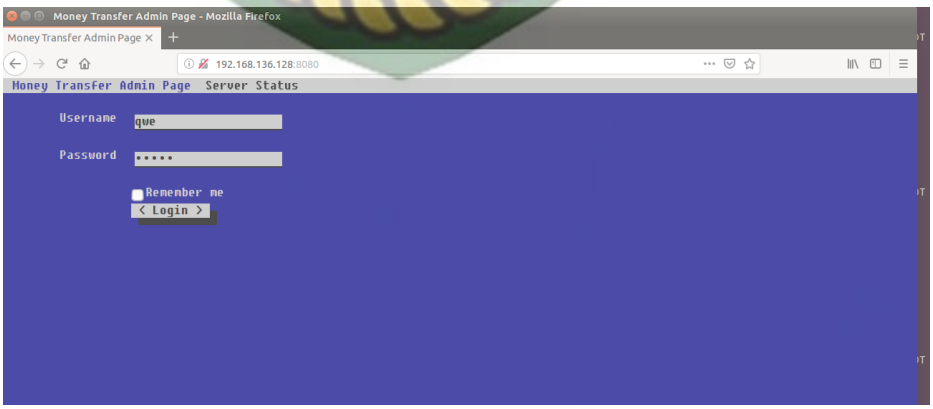
Gambar 4.10 Hasil scanning

Dari hasil scanning diatas didapatkan ada 4 IP yang terhubung dengan jaringan wireless yang sama. 192.168.136.130 merupakan IP client sehingga IP Address yang lain adalah salah satunya IP address computer

server. Untuk mengetahui target serangan maka akan dilakukan cek port pada masing-masing IP dan port yang banyak terbuka akan digunakan untuk proses penyerangan. Berikut ini adalah hasil scanning port pada IP Address 192.168.136.128.

Gambar 4.11 Cek Port yang terbuka

Salah satu port terbuka adalah port 8080 yang sudah dibuat oleh computer server. Sehingga jika hacker akan mengakses port tersebut maka hanya dengan membuka browser, karena port 8080 adalah port apache.

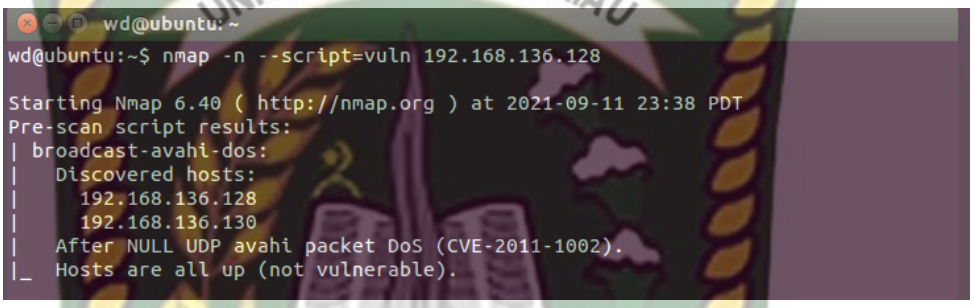


Gambar 4.12 Hasil port 8080 dari Firefox

Dengan tampilan ini maka hacker mengira ini adalah layanan transfer atau login ke system. Padahal yang sebenarnya adalah port palsu yang disiapkan oleh admin dikomputer server.

2. Brute Force

Pada penyerangan berikut ini penulis akan menguji coba menggunakan serangan brute force attack yang mengggunakan nmap script untuk proses penyerangan. Berikut hasilnya.

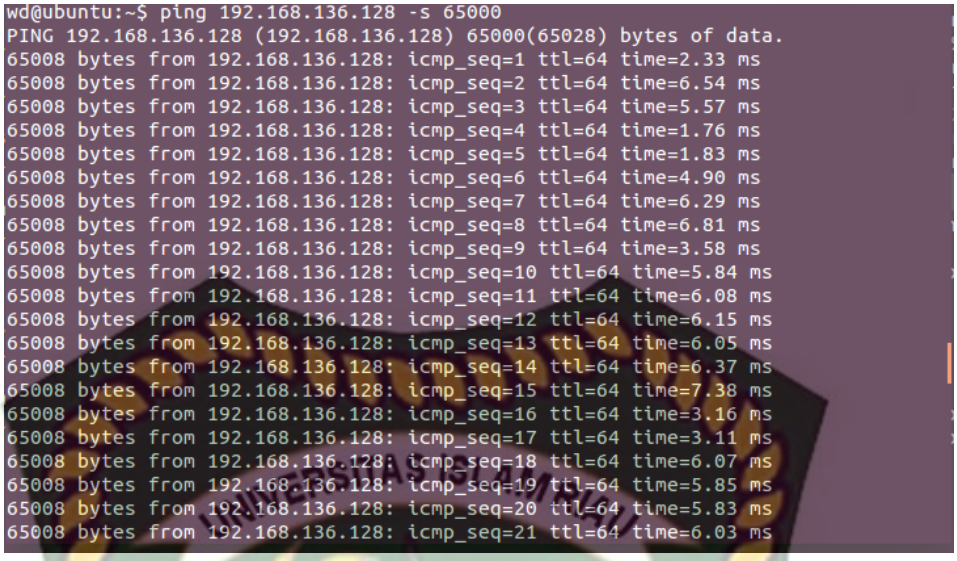


Gambar 4.13 Hasil Brute Force

Hasil yang ditampilkan tidak memberikan respon apapun karena memang yang digunakan oleh computer server adalah port palsu sehingga tidak memberikan informasi apapun.

3. Ddos Attack

Percobaan serangan terakhir menggunakan Ddos Attack yang menggunakan serangan ping ipaddress sebanyak mungkin agar computer server down. Berikut ini adalah proses ddos attack.



Gambar 4.14 Ddos Attack

Hasil serangan ddos attack memungkin server down karena pengiriman paket data yang banyak. Dalam kasus ini penyerangan dilakukan dengan pengiriman ping sebanyak 65000 kali.

4. Man in the middle attacks

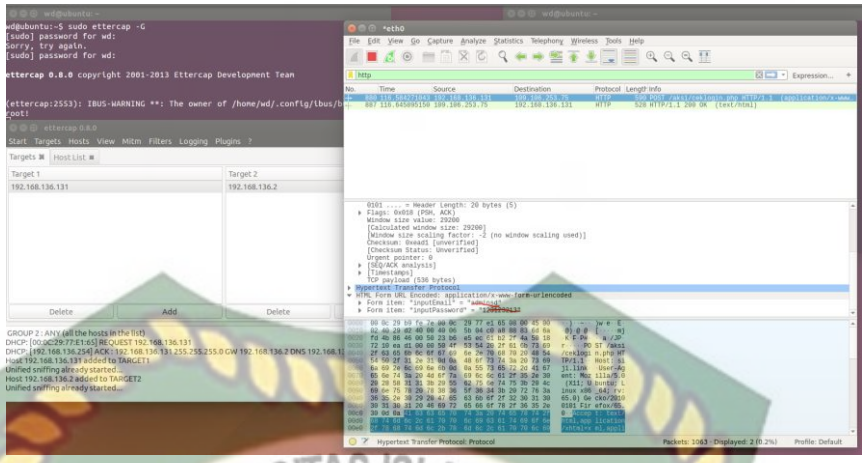
Percobaan serangan berikutnya adalah *Man in the middle attack* yaitu penyerang dapat memodifikasi lalu lintas yang lewat antara dua pihak. *Man in the middle attack* terjadi jika sistem tidak mampu membedakan komunikasi dengan penerima asli. Penyerang dapat membuat jaringan Wi-Fi palsu dan begitu pengguna terhubung ke jaringan itu, penyerang dapat melihat aktivitas pengguna yang dilakukan pengguna secara *online*. Pembuatan wifi palsu menggunakan bantuan router wifi usb seperti dibawah ini.

Gambar 4.15 Router Wifi USB

Proses berikutnya melakukan pengamatan yang masuk jaringan wifi yang sama dengan bantuan ettecap pada ubuntu. Seperti berikut ini.

Gambar 4.16 MITM

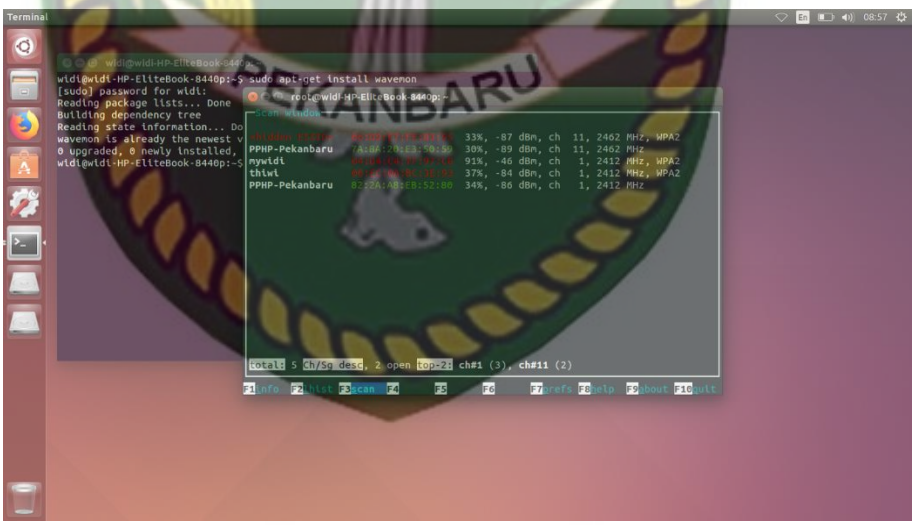
Berikut ini hasil sniffing dengan menggunakan mitm dan hasil yang didapat dari user login pada suatu website dan tertangkap username dan password dari user yang login. Berikut hasil pemantauan jaringan dengan MITM.



Gambar 4.17 Hasil MITM

5. *Discovery dan Probing Tools*

Alat Discovery dan Probing membantu penyerang untuk menemukan jaringan wifi yang memiliki keamanan yang lemah. Ada banyak alat yang membantu penyerang untuk menemukan titik akses keamanan rendah. Berikut ini prosesnya pencarian wifi.

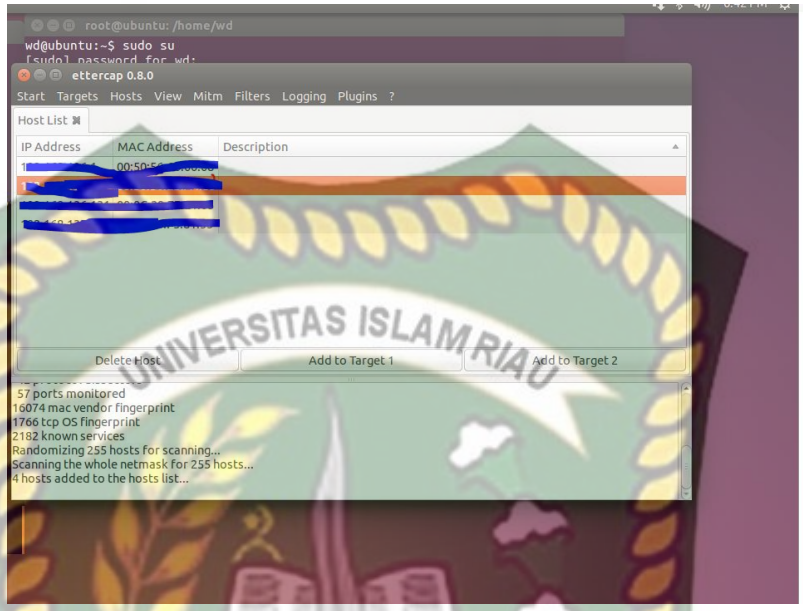


Gambar 4.18 Pencarian Wifi dengan Wavemon

6. *MAC identity spoof attacks*

Alamat Mac yang secara terbuka di udara. Penyerang dapat menangkap alamat mac dari pengguna WLAN, AP, sakelar, dan komponen router

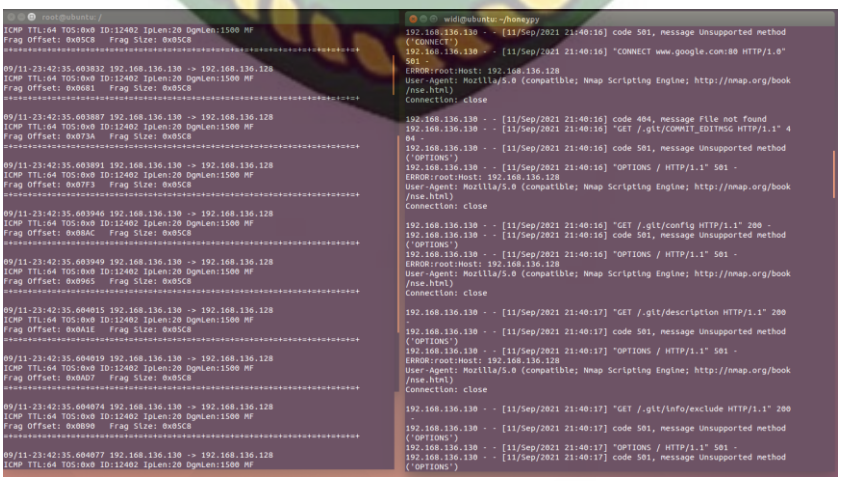
resmi. Setelah menangkap alamat mac, ada banyak program yang dapat menipu alamat mac ini dan dengan mudah.



Gambar 4.19 Pencarian Alamat Mac

4.4 Hasil Pengujian

Hasil pengujian serangan yang dilakukan oleh computer client adalah berhasil mengecohkan hacker dengan bantuan honeypot. Hasil rekap penyerangan computer client kepada computer server sebagai berikut :



Gambar 4.20 Hasil Penyerangan

Hasil penyerangan yang dilakukan hacker mendapatkan log ativitas di klien karena menggunakan IDS (Intruction Detection System) dengan Snort yang mencatat aktivitas penyerangan yang dilakukan oleh computer client/hacker.

4.5 Kesimpulan Hasil Pengujian

Data hasil yang diinginkan tercapai berdasarkan pada percobaan yang dilakukan. Semua menu sistem pada admin dapat berjalan dengan baik. Berikut ini rincian kesimpulan hasil percobaan sistem :

1. Proses keamanan jaringan dengan honeypot dapat berjalan dengan baik.
2. Log aktivitas server dapat diketahui dengan bantuan *IDS Snort* yang mencatat masuknya percobaan serangan yang berlebihan.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil analisa data keamanan jaringan wireless di Perpustakaan Daerah Pekanbaru ini dapat disimpulkan yaitu:

1. Penggunaan Honeypot sangat membantu dalam proses skema keamanan jaringan. Karena honeypot dapat mengecohkan hacker dalam percobaan masuk ke system admin dengan membuat halaman web atau protocol web palsu.
2. IDS Snort yang digunakan untuk mencatat aktifitas server juga dapat digunakan dengan baik. Hasil Analisa dapat dijadikan acuan untuk lebih memperkuat jaringan wireless sehingga keamanan dan kerahasian data dapat terjaga dengan baik.

5.2 Saran

Saran dari penulis untuk analisa data keamanan jaringan wireless di Perpustakaan Daerah Pekanbaru lebih lanjut adalah:

1. Penelitian berikutnya dapat menggunakan teknik IDS yang lain sehingga dapat melihat hasil perbedaannya.
2. Mengembangkan aplikasi untuk proses keamanan jaringan yang dapat dipantau menggunakan aplikasi mobile.

DAFTAR PUSTAKA

Adi, W. N. S. K., Iskandar, M., & Borris, H. (2014). *Analisa Dan Perancangan Keamanan Jaringan Dengan Menggunakan Snort Di Kementrian Komunikasi Dan Informatika*. Jakarta: Universitas Binus

Aidin, Lukito Prima dkk. 2016. *Implementasi High Interaction Honeypot Pada Server*. Bandung: e-Proceeding of Engineering : Vol.3, No.2 Agustus 2016 | Page 2172. ISSN : 2355-9365

Andros Refan, Lukas. 2014. *Implementasi Honeypot Dengan Raspberry Pi Sebagai Alat Bantu Pendeteksi Keamanan Jaringan Dan Penangkap Malware*. Jakarta: Jurnal Teknik dan Ilmu Komputer Vol. 04 No. 13, Jan – Mar 2015

Ar, Abdul Aziz. (2012). *Evaluasi Penerapan Autentikasi Pengguna Wireless Lan Berbasis Radius Server Universitas Bina Darma*. Palembang: Universitas Bina Darma

Ariyus, Dony. 2007. *Computer Security*. Yogyakarta. Penerbit Andi

Arief, Muhammad. 2012. *Implementasi Honeypot Dengan Menggunkan Dionaea Dijaringan Hotspot FIZZ*. Bandung: Politeknik Telkom

Barus, Eldifa Fajar. 2015. *Simulasi Membangun Jaringan Komputer dengan Cisco Packet Tracer*. Medan: Universitas Sumatera Utara

Cahyanto, Triawan Adi dkk. 2016. *Analisis dan Implementasi Honeypot Menggunakan Dionaea Sebagai Penunjang Keamanan Jaringan*. Jember: JUSTINDO , Jurnal Sistem & Teknologi Informasi Indonesia, Vol. 1, No. 2, Agustus 2016

Candra, Bayu Setia. 2014. *Analisis penerapan jaringan keamanan menggunakan ids dan honeypot*. Semarang: Universitas Dian Nuswantoro

Diansyah, Tengku Mohammad dkk, 2017. *Analysis Of Using Firewall And Single Honeypot InTraining Attack On Wireless Network*. Medan: International Conference on Information and Communication Technology (IconICT) IOP Publishing

Fadjrin, Akbar, Jahnsen Gultom. 2013. *Cloud Computing Server Menggunakan Proxmox Pada CV. Cipta Solusi Sejahtera*. Palembang: STMIK PalComTech Palembang

Jigneshkuma, Shah Manthan. 2016. *Modern Honey Network*. International Journal of Research in Advent Technology (E-ISSN: 2321-9637) Special Issue

National Conference “NCPCI-2016”, 19 March 2016; India

Harjono, Agung Purno. 2013. *Honeyd untuk Mendeteksi Serangan Jaringan di Universitas Muhammadiyah Purwokerto*. JUITA ISSN: 2086-9398 Vol. II Nomor 4, Nopember 2013; Purwokerto

Hartono, R. 2011. *Pengantar Jaringan Wireless*.

Kambow, Navneet, Lavleen Kaur Passi. 2014. *Honeypots: The Need of Network Security*. (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6098-6101. India

Komputer, W. (2010). *Tutorial 5 Hari Belajar Hacking dari Nol*. Yogyakarta: CV Andi

Laksana, Dimas Danang dkk. 2017. *Implementasi Honeypot Dengan Modern Honey Network*. Bandung: e-Proceeding of Applied Science: Vol.3, No.3 Desember 2017 | Page 1815. ISSN : 2442-5826

Mardiyanto, Bagus dkk. 2016. *Analisis Dan Implementasi Honeypot Dalam Mendeteksi Serangan Distributed Denial-Of-Services (DDOS) Pada Jaringan Wireless*. 32 Integer Journal, Vol 1, No 2, September 2016: 32-42

McCaughey, Ryan J. 2017. *Deception Using An SSH Honeypot*. California: Naval Postgraduate School Monterey

Nurrahman, Ahmad Fikri. 2013. *Implementasi Virtual Low-Interaction Honeypot Dengan Dionaea Untuk Mendukung Keamanan Jaringan*. Semarang: Journal of Informatics and Technology, Vol 2, No 4, Tahun 2013, p 28-37

Oktavianto, Digit. *Cuckoo Malware Analysis*. Birmingham: packt, 2013.

Prabowo, Yunan Arie. 2014. *Penggunaan Nmap Dan Hping 3 Dalam Menganalisa Keamanan Jaringan Pada B2P2TO2T*. Surakarta: Universitas Muhammadiyah Surakarta

Pramudita, K. E. (2010). *Brute Force Attack dan Penerapannya pada Password Cracking*. Bandung: Makalah IF3051 Strategi Algoritma – Sem. I Tahun 2010/2011

Prasetyo, Heru. 2008. *Perancangan dan Implementasi Sistem Honeypot Sebagai Alat Bantu Keamanan Jaringan Komputer pada PT. IP Teknologi Komunikasi*. Jakarta: Universitas Islam Negeri Syarif Hidayatullah

Saputra, Adhe. 2012. *Pengembangan Jaringan Wireless Local Area Network (WLAN) Menggunakan Metode PPDIOO*. Palembang: Binadarma.

Sharon, Desmon, Sapri, Reno Supardi. 2014. *Membangun Jaringan Wireless Local Area Network (WLAN) Pada CV. BIQ BENGKULU*. Bengkulu: Jurnal Media Infotama Vol. 10 No.1, hlm 36-37

Sofana, I. (2014). *Cisco CCNA & Jaringan Komputer* (Revisi). Bandung: Informatika

Sons, J. W. &. (2014). *CASP CompTIA Advanced Security Practitioner Study Guide*. (J. Kellum, Ed.). Canada: Indiana

Sopandi, Dede. 2008. Instalasi dan Konfigurasi Jaringan Komputer. Bandung: Informatika

Stallings, William. 2003. Data and Computer Communications. Prentice Hall.

Sunardi, A., Chandradinata, A., & Darmawan, C. (2012). *Implementasi Dan Evaluasi Honeypot Dionaea Dan Glastopf Di Id-SIRTII*. Jakarta: Binus University

Suryono, Tito, Mohammad Faruq Afif. 2012. *Pembuatan Prototype Virtual Server Menggunakan Proxmox VE untuk Optimalisasi Resouces Hardware di NOC FKIP UNS*. International Journal on Networking Security Volume 1 No. 1 November 2012

Sutati, Khairunnisa. 2017. *Perancangan Dan Analisis Keamanan Jaringan Nirkabel Dari Serangan DDoS (Distributed Denial Of Service) Berbasis Honeypot*. Banten: Jurnal PROSISKO Vol. 4 No. 2 September 2017. ISSN: 2406-7733

Toor, Jashanpreet Singh, Abhinav Bhandari. 2017. *Deployment of Low Interaction Honeypot in a Private Network*. India: International Journal of Advanced Research in Computer Science Volume 8, No. 7, July – August 2017

Utdirartatmo, Firrar. 2005. *Trik Menjebak Hacker dengan Honeypot*. Yogyakarta. Penerbit Andi

Vidwarshi, Snehil dkk, 2015. *a Discussion About Honeypots And Different Models Based on Honeypots*. India: International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-3, Issue-8, Aug.-2015

Wafi, Habibul. 2016. *Implementasi Sistem Keamanan Honeypot dengan Modern Honey Network pada Jaringan Wireless*. Jakarta: Universitas Islam Negeri Syarif Hidayatullah

Zam, E. (2011). *Buku Sakti Hacker*. Jagakarsa: MediaKita