ANALISIS DAN IMPLEMENTASI HIGH INTERACTION HONEYPOT PADA SERVER

SKRIPSI

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

DISUSUN OLEH:

ROYAN FIRDAUS
133510311

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UINIVERSITAS ISLAM RIAU
PEKANBARU
TAHUN 2020

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

LEMBAR PENGESAHAN PEMBIMBING SKRIPSI

Nama	:	Royan Firdaus
NPM	:	133510311
Fakultas	:	Teknik
Program Studi	:	Teknik Informatika
Jenjang Pendidikan	:	Strata Satu (S1)
Judul Skripsi	:	Analisis dan Implementasi High Interaction Honeypot Pada Server.

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, 22 Desember 2020

Disahkan Oleh

Ketua Prodi Teknik Informatika	**Dosen Pembimbing**
Dr. ARBI HAZA NASUTION, B.IT(Hons)., M.IT	**APRI SISWANTO, S.Kom., M.Kom**

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

LEMBAR PENGESAHAN
TIM PENGUJI UJIAN SKRIPSI

Nama	:	Royan Firdaus
NPM	:	133510311
Fakultas	:	Teknik
Program Studi	:	Teknik Informatika
Jenjang Pendidikan	:	Strata Satu (S1)
Judul Skripsi	:	Analisis dan Implementasi High Interaction Honeypot Pada Server.

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 22 Desember 2020** dan disetujui serta diterima untuk memenuhi salah satu syarat guna memperoleh gelar Sarjana Strata Satu Bidang Ilmu **Teknik Informatika.**

Pekanbaru, 22 Desember 2020

Tim Penguji

1. **Dr. Evizal, S.T., M.Eng** — **Sebagai Tim Penguji I** (.....)
2. **Panji Rachmat Setiawan, S.Kom., MMSI** — **Sebagai Tim Penguji II** (.....)

Disahkan Oleh

Ketua Prodi Teknik Informatika	**Dosen Pembimbing**
Dr. ARBI HAZA NASUTION, B.IT(Hons)., M.IT	**APRI SISWANTO, S.Kom., M.Kom**

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

LEMBAR PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Royan Firdaus

Tempat/Tgl Lahir : Buluh Rampai, 17 November 1995

Alamat : Buluh Rampai Indragiri Hulu Riau

Adalah mahasiswa Universitas Islam Riau yang terdaftar pada:

Fakultas : Teknik

Program Studi : Teknik Informatika

Jenjang Pendidikan : Strata-1 (S1)

Dengan ini menyatakan dengan sesungguhnya bahwa skripsi yang saya tulis adalah benar dan asli hasil dari penelitian yang telah saya lakukan dengan judul "**Analisis dan Implementasi High Interaction Honeypot Pada Server**".

Apabila di kemudian hari ada yang merasa dirugikan atau menuntut karena penelitian ini menggunakan sebagian hasil tulisan atau karya orang lain tanpa mencantumkan nama penulis yang bersangkutan, atau terbukti karya ilmiah ini bukan karya saya sendiri atau plagiat hasil karya orang lain, maka saya bersedia menerima sanksi sesuai dengan peraturan perundangan yang berlaku.

Demikian surat pernyataan ini saya buat dengan sesungguhnya untuk dapat digunakan sebagaimana mestinya.

Pekanbaru, 30 Desember 2020

Yang membuat pernyataan,



(ROYAN FIRDAUS)

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

LEMBAR IDENTITAS PENULIS

NPM	: 133510311
Nama	: Royan Firdaus
Tempat/Tgl Lahir	: Buluh Rampai, 17 November 1995
Alamat Orang Tua	: Buluh Rampai, Kec. Seberida, Kab. Indragiri Hulu, Riau, Indonesia
Nama Orang Tua	: Yayat Supriyatna
No HP / Telp	: 082268291583
Jurusan	: Teknik Informatika
Fakultas	: Teknik
Masuk Th.Ajaran	: 2013
Wisuda Th.Ajaran	: 2020
Judul Skripsi	: Analisis dan Implementasi High Interaction Honeypot Pada Server

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

HALAMAN PERSEMBAHAN

Assalamu'alaikum Wr.Wb.

Alhamdulillah, puji syukur penulis ucapkan kepada Allah Subhanahu wata'ala yang maha kuasa atas segala rahmat dan karunia-Nya yang telah diberikan kepada penulis sehingga dapat menyelesaikan tugas akhir skripsi dengan judul **"Analisis dan Implementasi High Interaction Honeypot Pada Server".**

Tugas akhir skripsi ini disusun untuk memenuhi persyaratan mencapai derajat strata-1 (S-1) di jurusan Teknik Informatika Fakultas Teknik Universitas Islam Riau.Penulis menyadari bahwa tanpa bantuan dari pihak-pihak lain, usaha yang penulis lakukan dalam menyelesaikan laporan skripsi ini tidak akan membuahkan hasil yang berarti. Dalam kesempatan ini penulis menyampaikan ucapan terima kasih kepada :

1. Kepada yang teristimewa ayahanda Yayat Supriyatna, Ibunda Yanti selalu memberi motivasi, selalu mendo'akan penulis agar dapat sukses dan bisa menggapai cita-cita.
2. Kepada saudara-saudaraku Muhammad Tedi Hidayat, Rika Rian Hidayat yang selalu memberikan motivasi dan mendoakan penulis dalam menyelesaikan tugas akhir.
3. Kepada Seluruh Dosen Teknik Informatika yang telah memberikan ilmu dan bimbingannya kepada saya khususnya kepada Bapak Apri Siswanto, S.Kom., M.Kom sebagai Pembimbing, Bapak Dr. Evizal, S.T., M.Eng,

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Bapak Panji Rachmat Setiawan, S.Kom., MMSI sebagai penguji dan Ibu Ana Yulianti, ST., M.Kom.

4. Kepada sahabat-sahabatku , Derio Danda Prayoga, ST, Imam Riva'ie, ST , Ardi Pranata, SIP, Roni Desi Priono, ST , Zainal Arifin, ST, terimakasih atas semangat, motifasi dan kebersamaannya. Kepada seluruh teman-teman angkatan 2013 yang telah begitu banyak membantu dan berjuang bersama selama kuliah, khususnya teman seperjuangan di Teknik Informatika Universitas Islam Riau.
5. Serta semua pihak yang telah membantu penulis yang tidak dapat penulis sebutkan satu persatu, terima kasih atas keikhlasannya, mudah-mudahan Allah SWT membalas segala kebaikan kalian semua.

Akhir kata penulis mohon maaf atas kekeliruan dan kesalahan yang terdapat dalam skripsi ini dan berharap semoga skripsi ini dapat memberikan manfaat bagi pembaca.

Pekanbaru, 22 Desember 2020

Royan Firdaus
133510311

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

KATA PENGANTAR

Alhamdulillahi robbil alamin, marilah kita bersyukur atas kehadirat Allah SWT, yang telah memberikan rahmat dan hidayah-nya kepada kita semua sehingga penulis mampu menyelesaikan Laporan Hasil ini dengan baik. Shalawat beriring salam kita junjungkan kepada Nabi Muhammad SAW, karena beliau telah membawa umat dari zaman jahiliyah ke zaman yang terang ini.

Dalam Penelitian yang berjudul **"Analisis dan Implementasi *High Interaction Honeypot* Pada *Server*"** ini disusun dan ditulis dalam rangka melaksanakan kurikulum Program Studi Teknik Informatika dalam penyelesaian tugas akhir di bidang ilmu Teknik Informatika.

Penulis menyadari bahwa penyusunan dalam Tugas Akhir ini jauh dari kata kesempurnaan. Untuk itu, Penulis mengharapkan kritik dan saran yang bersifat membangun demi peningkatan kemampuan penulis dimasa yang akan datang.

Akhir kata semoga Hasil Tugas Akhir ini dapat memberikan manfaat dan sumbangan wawasan bagi kita semua, Amiin.

Pekanbaru, 22 Desember 2020

Royan Firdaus

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

DAFTAR ISI

Halaman

Kata Pengantar ..... **i**

Daftar Isi ..... **ii**

Daftar Gambar ..... **v**

Daftar Tabel ..... **vii**

Abstrak ..... **viii**

Abstract ..... **ix**

BAB I Pendahuluan **1**

1.1 Latar Belakang 1

1.2 Identifikasi Masalah 2

1.3 Rumusan Masalah 2

1.4 Batasan Masalah 2

1.5 Tujuan Penelitian 3

1.6 Manfaat Penelitian 3

BAB II Landasan Teori **5**

2.1 Studi Kepustakaan 5

2.2 Dasar Teori 8

2.2.1 Keamanan Jaringan Komputer 8

2.2.1.1 Tujuan Keamanan Jaringan Komputer 8

2.2.1.2 Langkah Pengamanan Jaringan Komputer 9

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

2.2.1.3 Pengamanan Sistem 11

2.2.2 Ancaman 13

2.2.2.1 Macam Ancaman Pada Jaringan 13

2.2.3 *Honeypot* 14

2.2.4 *Router* 15

2.2.5 Protocol 15

2.2.5.1 *Tranmission Control Protocol / Internet Protocol (TCP/IP)* 15

2.2.5.2 *IP Addressing* 16

2.2.5.3 Kelas-kelas Alamat IP 16

2.2.5.4 Subnetting 17

2.2.5.5 *User Datagram Protocol (UDP)* 17

2.2.6 *Web Server* 17

2.3 Hipotesis 18

BAB III Metode Penelitian 19

3.1 Metodologi Penelitian 19

3.2 Alat dan Bahan Penelitian yang Digunakan 20

3.2.1 Prangkat Keras (*Hardware)* 20

3.2.2 Prangkat Lunak (*Software)* 20

3.3 Pengembangan Dan Perancangan Sistem 21

3.3.1 Perancangan Topologi 21

3.3.2 Perancangan Program 22

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3.3.3 Skenario yang Digunakan pada Implementasi 23

3.4 Parameter Kerja Sistem Jaringan 24

3.5 Kerangka Pemodelan 26

BAB IV Hasil Dan Pembahasan 27

4.1 Hasil 27

4.2 Pembahasan 29

4.2.1 Peralatan Penerapan *Honeypot* 29

4.2.2 Pengujian Penerapan *Honeypot* 31

BAB V Penutup 42

5.1 Kesimpulan 42

5.2 Saran 42

Daftar Pustaka .....

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

DAFTAR GAMBAR

1. Gambar 3.1 Metode Penelitian Tugas Akhir 19
2. Gambar 3.2 Topologi UIR (Roni Kharisma, 2017) 21
3. Gambar 3.3 Rancangan *Server Honeypot* 22
4. Gambar 3.4 Rancangan Pengalihan *Attacker ke Server* 23
5. Gambar 3.5 *Flowchar* Sistem Penyusupan *Router* 26
6. Gambar 4.1 *Cracking Password Word List Airmon-Ng* 28
7. Gambar 4.2 Komputer 1 sebagai *server* 30
8. Gambar 4.3 Komputer 2 sebagai *Honeypot* 31
9. Gambar 4.4 Komputer 3 *Attacker* 31
10. Gambar 4.5 Instalasi *Pentbox* 1.8 Pada Dikomputer 2 32
11. Gambar 4.6 Proses *setting honeypot* membuka *port* 33
12. Gambar 4.7 pemilihan *port* yang akan dibuka 34
13. Gambar 4.8 *Scanning Nmap* pada Jaringan 35
14. Gambar 4.9 Hasil *Scanning IP* 172.0.0.1/24 35
15. Gambar 4.10 *Nmap* Mencoba *Scanning* IP Yang Tersedia 36
16. Gambar 4.11 *Nmap* Deteksi *Firewall* IP *Address* 192.168.01.100 37
17. Gambar 4.12 *Nmap Scanning* Sistem Operasi 37
18. Gambar 4.13 Nmap Mendapat *Script* Dari *Scanning* 38
19. Gambar 4.14 *Nmap* Mencoba *Scanning Port* 4444 39
20. Gambar 4.15 Hasil *Log Port* 82 *Honeypot* 39
21. Gambar 4.16 Hasil *log port* 80 *honeypot* 40

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

22. Gambar 4.17 Hasil *Log Port* 4444 *Honeypot* 41

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

DAFTAR TABEL

1. Tabel 2.1 Pembagian Kelas Alamat *IP* 16
2. Tabel 3.1 IP Addresss Topologi 22
3. Tabel 3.2 *IP Address* Rancangan Topologi Jaringan *Server Honeypot* 23
4. Tabel 3.3 Pengalihan *Request* oleh *Router* 24

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Analisis dan Implementasi High Interaction Honeypot Pada Server

(Royan Firdaus)

Program Studi Teknik Informatika Fakultas Teknik Universitas Islam Riau

Email: royanfirdaus@student.uir.ac.id

Keamanan jaringan komputer merupakan bagian dari sebuah sistem yang sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. *Server* merupakan sebuah sistem yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. *Server* menjalankan perangkat lunak yang dapat mengontrol akses terhadap jarigan dan sumber daya yang berada dalam jaringan tersebut. *Honeypot* adalah sebuah sistem palsu yang dirancang menyerupai sistem sebenarnya yang dibangun untuk mengecoh *attacker* dalam melancarkan penyusupan, dengan kata lain ketika seorang *attacker* ingin menguasai sebuah *server* maka dia akan menyerang *server* tiruan yang telah dibangun dan tidak akan sampai ke *server* yang sebenarnya. Tujuan dari *honeypot* sendiri bukan hanya untuk membelokan serangan, akan tetapi *honeypot* juga akan mengumpulkan informasi mengenai cara dan juga perangkat-perangkat *maleware* apa saja yang digunakan seorang *attacker* ketika ingin mengambil alih sebuah *server*. *Output* pada analisis dan implementasi ini yaitu mengalihkan penyusupan *attacker* pada *server honeypot* dan mengetahui pola penyusupan.

Kata Kunci: Keamanan Jaringan Komputer, *Server*, *Honeypot*

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Analysis and Implementation High Interaction Honeypot on the Server

(Royan Firdaus)

Informatics Engineering study Program, Faculty of Engineering, Islamic University of Riau

Email: royanfirdaus@student.uir.ac.id

Computer network security is part of a system that is very important to maintain data validity and integrity and ensure the availability of services for its users. Server is a system that provides certain types of services in a computer network. The server runs software that can control access to networks and resources on the network. Honeypot is a fake system that is designed to resemble the real system that was built to trick attackers into launching an infiltration, in other words when an attacker wants to control a server, he will attack the mock server that has been built and will not reach the real server. The purpose of the honeypot itself is not only to deflect attacks, but the honeypot will also collect information about the methods and also what maleware devices an attacker uses when he wants to take over a server. The output of this analysis and implementation is to divert the attacker's infiltration on the honeypot server and find out the intrusion pattern.

Keyword : Computer network security, Server, Honeypot

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan komputer merupakan bagian dari sebuah sistem yang sangat penting untuk menjaga *validitas* dan *integritas* data serta menjamin ketersediaan layanan bagi penggunanya. Keamanan menjadi konsentrasi dan fokus utama seiring dengan ketergantungan masyarakat akan teknologi informasi. Terjadinya kasus penyusupan maupun ancaman tersebut sudah sering terjadi terhadap sistem keamanan jaringan pada *server* yang tidak dirawat dengan baik.

Server merupakan sebuah sistem yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. *Server* menjalankan perangkat lunak yang dapat mengontrol akses terhadap jarigan dan sumber daya yang berada dalam jaringan tersebut. Dengan memperkuat keamanan pada *server* berbagai ancaman keamanan dapat diminimalkan dengan memaksimalkan identifikasi celah keamanan sedini mungkin.

Kombinasi dan perpaduan keamanan *software* dan perangkat *hardware* merupan solusi keamanan teknologi informasi yang komprehensif. Implementasi sistem *honeypot* merupakan solusi keamanan yang komprehensif meskipun *honeypot* hanya memiliki ruang lingkup deteksi dan respon, namun dapat merekam semua kemungkinkan celah keamanan. *Honeypot* adalah sistem yang dibuat seperti desain sistem aslinya agar sengaja diserang atau disusupi, sehingga informasinya dapat dieksplor untuk melakukan tindakan pencegahan selanjutnya.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Oleh karena itu, sesuai dengan latar belakang diatas peneliti mengusulkan membuat penelitian yaitu "Analisa dan Implementasi *High Interaction Honeypot* Pada *Server* ".

1.2 Identifikasi Masalah

1. Kelalaian administrator dalam mengelola *server* dapat terjadi timbulnya ancaman keamanan pada jaringan.
2. Perlunya sistem yang dapat mempelajari pola serangan yang terjadi supaya *server* dapat menangani ketika terjadinya serangan.

1.3 Rumusan Masalah

Adapun rumusan masalah penelitian ini yaitu :

1. Bagaimana merancang suatu sistem keamanan *honeypot* dan mengimplementasikan pada jaringan sehingga dapat meningkatkan keamanan pada *server*.
2. Apakah dengan menguji beberapa tipe serangan pada sistem yang telah dibangun telah cukup untuk membuktikan *honeypot* memang handal, tidak terkecoh terhadap serangan dan mampu mempelajari pola penyusup.
3. Sejauh mana informasi yang diberikan oleh *log* dapat membantu dalam mendeteksi, mempelajari dan menindak lanjuti serangan.

1.4 Batasan Masalah

Dalam penelitian ini penulis membatasi masalah yaitu :

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

1. Hanya membahas perancangan dan implementasi teknologi *honeypot* pada jaringan *wireless* tanpa *proxy* dan *firewall*.
2. Tidak membahas perbandingan sistem keamanan teknologi *honeypot* dengan sistem keamanan yang lain.
3. Serangan yang diterapkan berupa *port scanning* dan *hacking* (metode *bruteforce*).
4. Software yang digunakan adalah software mikrotik (winbox v3.11) dan hardware mikroik (mikrotik RB951-2ND).

1.5 Tujuan Penelitian

Adapun penelitian ini bertujuan untuk :

1. Menjadikan *honeypot* sebagai sistem pertahanan pada jaringan komputer.
2. Dapat menjadikan *honeypot* sebagai sebuah *server* palsu dalam sebuah jaringan komputer.
3. Dapat membantu *server* dalam menangani terjadinya suatu serangan maupun pencurian data.

1.6 Manfaat Penelitian

Adapun manfaat yang akan diharapkan dari penelitian ini adalah :

1. Mempermudah dalam mendeteksi ketika adanya aktivitas penyusupan pada sistem keamanan jaringan.
2. Mengetahui karakteristik dan aktivitas apa saja yang terjadi pada sistem keamanan jaringan.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3. Mengetahui kelayakan dan kehandalan sistem keamanan menggunakan *honeypot* pada jaringan *wireless*.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

BAB II

LANDASAN TEORI

2.1 Studi Kepustakaan

Adapun beberapa tinjauan pustaka ini dilakukan untuk memberi pengetahuan penulis terhadap penelitian yang dilakukan oleh para peneliti terdahulu. Dengan melakukan tinjauan pustaka ini mendapatkan referensi yang bisa membantu penulis untuk menyelesaikan penelitian ini.

Dalam penelitian yang dilakukan oleh Moh Dahlan, Anastasya Latubessy, dan Mukhamad Nurkamid (2015), bahwa beliau melakukan penelitian keamanan jaringan *web server* pada *website* Universitas Muria Kudus dari penyusupan *possibility sql injection*. Metode yang digunakan dalam penelitian beliau dalam menangani keamanan jaringan *web server* menggunakan *intruder detection system* (IDS). Sistem beliau menerapkan aturan *possibility injection* pada *tools* yang dipasang pada *Web Server* Universitas Muria Kudus menggunakan *software Snort* sebagai identifikasi terhadap ancaman yang masuk pada *web server*.

Dalam melakukan pengujian terhadap keamanan *web server* tersebut, SQL injection adalah kerentanan yang sering terjadi ketika penyusupan memiliki kemampuan untuk mempengaruhi *structured query language* (SQL) query yang melewati suatu aplikasi ke-*database back-end*. Hasil dari penelitian beliau berupa

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

alert sebagai alternatif peringatan keamanan dari penyusupan (*intruder*) yang masuk kejaringan.

Selanjutnya menurut Nazwita dan Siti Ramadhani (2017), beliau melakukan penelitian keamanan *web server* dan *database server* dari penyusupan seperti *Port Scanning* dan *Brute Force*. *Port Scanning* merupakan aktivitas untuk mendapatkan informasi yang menyeluruh mengenai status *port* (biasanya *port* TCP) pada suatu *host*, dan sedangkan *Brute Force* merupakan suatu aktivitas yang bertutujuan untuk mendapatkan password dari *user* yang menjadi target. Dalam penelitian beliau menangani sistem keamanan *web server* dan *database server* menggunakan metode *Intrusion Detection and Prevention System* (IDPS) open source yang merupakan generasi lanjutan dari IDS dan IPS.

Suricata merupakan perangkat lunak pendeteksi dan sekaligus pencegahan gangguan ancaman dari IDPS. Dalam penelitian beliau menganalisa penyusupan dari port scanning menggunakan *nmap* dan *brute force* menggunakan *brutus* dapat diketahui oleh administrator. *Rule* yang diterapkan pada suricata telah bekerja dengan baik dan membantu tugas dari *network* admin untuk melakukan tindakan prefentif terhadap ancaman dari *attacker*.

Sejalan dengan itu, Menurut Roni Karisma (2017), bahwa beliau melakukan penelitian keamanan jaringan pada *Router* Mikrotik dari penyusupan *Port Scanning* dan *Brute Force*. Adapun metode keamanan jaringan yang digunakan dalam

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

penelitian beliau yaitu dengan sistem keamanan dari Intrusion Prevention System (IPS) sebagai monitor trafik jaringan yang merupakan kombinasi antara fasilitas blocking *capabilities* dari *Firewall*.

Dalam penelitian beliau menerapkan sistem IPS pada *Server* Mikrotik dan uji coba melakukan penyusupan *port scanning* dengan Nmap menggunakan aplikasi *Zenmap* dan *brute force* dengan aplikasi *Brutus*. Sebelum menerapkan sistem IPS pada *Server* Mikrotik dalam penelitian beliau memperlihatkan terjadi log aktivitas yang ingin masuk secara paksa ke *server* mikrotik namun belumbisa dicegah oleh mikrotik. Dalam pengujian setelah menerapkan IPS pada *Server* Mikrotik mampu mencegah penyusupan dari port scanning *nmap* dengan *zenmap* dan *brute force pass mode = combo list* dengan *brutus*. Adapun beliau memyimpulkan penyusupan terdeksi tergantung pada pola penyusupan yang ada didalam *rule* IPS tersebut. Untuk itu pengolahan *filter rule*s pada perangkat IPS harus secara rutin melakukan pengecekan *rules*.

Berdasarkan beberapa studi kasus dari jurnal penelitan tersebut akan berkaitan dengan penelitian yang dilakukan oleh penulis. Perbedaan penelitian yang akan dilakukan penulis yaitu dari segi metode keamanan jaringan. Adapun kelebihan dan kekurangan penelitian sebelumnya yang menyarankan keamanan dengan metode lain. Penulis akan melakukan penelitian sistem keamanan menggunakan *Honeypot*, *honeypot* merupakan sistem keamanan untuk mengelabuhi dan membaca pola

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

penyusupan *attacker* dalam melancarkan penyusupan ke *server*. *Honeypot* akan diterapkan pada *Server* Mikrotik.

2.2 Dasar Teori

2.2.1 Keamanan Jaringan Komputer

Keamanan jaringan secara umum adalah komputer yang terhubung ke *network*, mempunyai ancaman keamanan lebih besar daripada komputer yang tidak terhubung ke mana-mana. Keamanan jaringan (*network security*) dalam jaringan komputer sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Tugas keamanan jaringan dikontrol oleh administrator jaringan. Ariyus, (2007: 3).

2.2.1.1 Tujuan keamanan Jaringan Komputer

Fuaddi (2017), adapun pentingnya keamanan jaringan adalah untuk menjamin beberapa aspek agar tetap terjaga aspek-aspek tersebut diantaranya :

1. *Availablility*

   Adalah terjaminya ketersedian data yang terus ada. Situs yang down karena penyusupan DDoS menunjukkan rendahnya tingkat keamanan pada aspek *availabilility*.

2. *Reability*

   Adalah kehandalan sebuah jaringan komputer dalam menjaga data-data yang keluar dan masuk jaringan komputer tetap dalam keadaan aman.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3. *Confidentiality*

   Adalah kemampuan sebuah jaringan komputer untuk dapat merahasiakan setiap lalu lintas data yang masuk dan keluar sehimgga seorang penyusup tidak dapat membaca data-data tersebut.

2.2.1.2 Langkah Pengamanan Jaringan Komputer

Dalam proses pengamanan jaringan komputer ada beberapa tahap yang perlu dilakukan oleh pihak yang bertanggung jawab diantaranya adalah :

1. Persiapan (preparation)

   Persiapan menjadi awal dari segala macam kegiatan sebelum memulainya. Persiapan yang dilakukan diantaranya.

   a. Persiapan personal

      Persiapan personal dalam hal ini diberatkan pada orang yang bertugas mengamankan atau tim pengamanan. Tim penanganan yang baik adalah sumber daya yang berharga dalam proses penaganan masalah yang akan terjadi.

   b. Persiapan alat (*tool*)

      Persiapan tool merupakan kegiatan untuk mempersiapkan alat/teknologi yang diperlukan dalam proses penanganan insiden keamanan pada jaringan.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

c. Persiapan dokumentasi

Beberapa dokumentasi yang perlu untuk dipersiapkan diantaranya daftar ip address, topologi jaringan beserta ip address terbarunya, peninjauan *Disaster Recovery Plan* (DRP) serta memastikan manajemen senior dan tim hukum memahami pentingnya penanganan dari penyusupan pada jaringan termasuk peran mereka.

d. Persiapan komponen keamanan n*etwork*

Merupakan komponen yang digunakan untuk menjaga keamanan pada jaringan komputer diantaranya anti malware, firewall, VPN.

2. Tahap Identifikasi

Menyelidiki dan memahami sifat terhadap suatu penyusupan dan target dari penyusupan tersebut adalah hal yang dilakukan pada tahap identifikasi contohnya kinerja jaringan yang buruk, layanan lambat atau tidak dapat di akses, sistem yang tiba-tiba crash merupakan tanda-tanda yang patut dicurigai sebagai sebuah penyusupan sebelum dilakukannya proses penahanan dan pemulihan.

3. Tahap penahanan

Rencana penahanan yang telah ditentukan sebelum terjadinya penyusupan akan meningkatkan kecepatan respon dari kerusakan akibat penyusupan yang terjadi pada jaringan. Dimana strategi penahanan akan berbeda-beda tergantung pada sistem yang akan dikelola.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

4. Tahap *Eradication*

   Tahap ini merupakan tahapan analisa lebih dalam (forensik) pada tahap ini dilakukan analisa terhadap *log* file pada *server*, peralatan aktif jaringan, IDS, *firewall*, sistem *file*, dan aplikasi. Kualitas forensik akan semakin baik bila kualitas dan kuantitas dari barang bukti semakin baik serta banyak.

5. Tahap *Recovery*

   Pada tahap ini dilakukan proses pemulihan sistem setelah dilakukannya proses penahanan dan proses eradication tahapan recovery akan semakin cepat dan tepat bila tim yang melakukan perbaikan memahami karakteristik penyusupan dengan sangat baik.

6. Tahap *Follow Up*

   Tahapan ini pelaporan atas penyusupan yang telah terjadi serta penangannya dan tahapan dari penaganan tersebut, pembelajaran atas apa yang telah terjadi, peningkatan terhadap sistem untuk mencegah hal yang sama tidak terulang kembali, pembaruan dokumen-dokumen terkait seperti Standari Operasi Prosedur (SOP), Prosedur Operasi Darurat (POD), Disaster Recovery Plan (DRP).

2.2.1.3 Pengamanan Sistem

Dalam menjaga sistem yang dibuat tetap terjaga aman seorang administrator dapat melakukan beberapa cara dalam sistemnya diantaranya adalah :

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

1. Autentikasi

   Adalah proses pengenalan sisitim operasi, user, kegiatan, aplikasi yang terhubung ke dalam jaringan komputer. Proses ini diawali pada saat user melakukan login menggunakan *username* dan *password.*

2. Enkripsi

   Adalah proses perubahan sebuah data menjadi bentuk-bentuk tertentu sehingga tidak dapat dibaca secara langsung dan harus melakukan proses dekripsi agar data tersebut dapat dibaca secara normal oleh user.

3. *Account Locking*

   Melakukan penguncian sebuah akun jika setelah beberapa kali gagal dalam melakukan proses login.

4. *Password Aging & Expiration*

   Adalah pemberian umur kepada password. Jika password sudah melebihi batas waktu administrator akan memberitahukan untuk merubah password kembali.

5. Otorisasi

   Adalah pemberian hak akses terhadap suatu resource kepada seseorang. Dengan begitu seseorang akan diberi batasan untuk mengakses resource-resouce yang tidak diberikan kepadanya.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

2.2.2 Ancaman

Utomo (2006: 111), pada dasarnya ancaman datang dari seseorang yang mempunyai keinginan memperoleh akses ilegal kedalam suatu jaringan komputer. Oleh karena itu, harus ditentukan siapa saja yang diperbolehkan mempunyai akses legal kedalam sistem, dan ancaman-ancaman yang dapat mereka timbulkan. Ada beberapa tujuan yang ingin dicapai oleh penyusup dan sangat berguna apabila dapat membedakan tujuan-tujuan tersebut pada saat merencanakan sistem keamanan jaringan komputer.

2.2.2.1 Macam Ancaman Pada Jaringan

Dalam melakukan tindakan penyusupan pada sebuah jaringan komputer seorang penyusup akan melakukan beberapa hal terhadap targetnya diantaranya sebagai berikut :

1. Interupsi

   Teknik ini bekerja dengan mencegh agar pesan atau data yang dikirimkan seseorang sampai pada tujuan.

2. Intersepsi

   Teknik ini bekerja dengan menagkap pesan atau data yang dikirimkan seseorang kepada orang lain (*spionase*).

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3. Modifikasi

   Teknik ini bekerja dengan membelokan pesan yang dikirimkan ke komputer penyusup kemudian si penyusup akan mengubah pesan tersebut setelah itu pesan yang telah diubah dikirimkan kepada penerima sebenarnya.

4. Fabrikasi

   Teknik ini bekerja dengan memberikan pesan palsu kepada target dimana pesan si pengirim akan dicegat oleh penyusup kemudian penyusup akan mengirimkan pesan buatannya kepada si penerima seolah-olah itu adalah pesan yang asli.

2.2.3 *Honeypot*

Honeypot adalah sebuah sistem palsu yang dirancang menyerupai sistem sebenarnya yang dibangun untuk mengecoh *attacker* dalam melancarkan penyusupannya, dengan kata lain ketika seorang *attacker* ingin untuk menguasai sebuah *server* maka dia akan menyerang *server* tiruan yang telah dibangun dan tidak akan sampai ke *server* yang sebenarnya. *Honeypot* sendiri bertujuan bukan hanya untuk membelokan penyusupan, akan tetapi *honeypot* juga akan mengumpulkan informasi mengenai cara dan juga perangkat-perangkat *maleware* apa saja yang digunakan seorang *attacker* ketika ingin mengambil alih sebuah *serve*r. Fuaddi, (2017).

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

2.2.4 *Router*

Router merupakan sebuah *device* atau alat yang dapat menghubungkan dua atau lebih jaringan komputer yang berbeda. Secara umum *router* adalah suatu alat pada jaringan komputer yang bekerja di *network layer* pada lapisan *OSI*. Dalam *Router* ini terdapat *routing table* yaitu table yang berisi alamat-alamat jaringan yang dibutuhkan untuk memenuhi tujuan dari paket-paket data yang akan dilewatkan pada suatu jaringan tersebut. Gin-Gin Yugianto, (2012).

2.2.5 Protocol

Protocol adalah aturan-aturan dan prosedur untuk melakukan komunikasi. Ketika beberapa komputer dalam sebuah jaringan hendak melakukan komunikasi dengan komputer lain, aturan-aturan atau prosedur komunikasi harus dilakukan terlebih dahulu. Zaenal Arifin, (2005).

2.2.5.1 *Transmission Control Protocol / Internet Protocol* (*TCP/IP*)

Zaenal Arifin (2005) TCP/IP (*Tranmission Control Protocol/Internet Protocol*) merupakan sebuah *protocol suite standard* yang menyediakan komunikasi dalam sebuah lingkungan (sistem operasi) yang beragam. TCP/IP bersifat *routeable* dan merupakan *protocol* yang biasa di dalam jaringan *global* (*enterprise*). Terdapat beberapa *protocol* yang berjalan menggunakan *protocol TCP/IP*, diantaranya:

1. FTP (*File Transfer Protocol*) – digunakan untuk melakukan mekanisme pengiriman file.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

2. SMTP (*Simple Mail Transfer Protocol*) – digunakan untuk pengiriman *email*, dan lain-lain.

2.2.5.2 *IP Addressing*

Gin-Gin Yugianto (2012) alamat *IP* merupakan kode *biner* 32 bit dan dibagi menjadi dua bagian identifikasi sebagai berikut :

1. Bagian identifikasi *NetID*, menunjukan identitas jaringan komputer tempat *host* – *host* (komputer) yang dihubungkan.
2. Bagian identifikasi *Host* ID, memberikan suatu pengenalan unik pada setiap *host* (komputer) sutau jaringan komputer.

2.2.5.3 Kelas-kelas Alamat IP

Gin-Gin Yugianto (2012) mengggunakan suatu sistem alamat logika untuk mengenali *host*. Alamat logika disebut juga alamat *TCP/IP* yang menyediakan beberapa keuntungan *routing*, yang dapat disegerhanakan karena informasi alamat haringan dikodekan pada alamat *IP*.

Tabel 2.1 Pembagian Kelas Alamat *IP*

Kelas	*Range*	maksimal *network*	Jumlah *host*
A	113.46.5.6 -126.1.5.5	127	12777214
B	128.0.12.5 -191.255.1.1	16384	65534
C	192.168.0.10 – 223.255.255.0	2097152	254

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

2.2.5.4 *Subnetting*

Subnetting Merupakan cara untuk membagi jaringan menjadi jaringan-jaringan yang lebih kecil dengan cara mengubah *subnet mask*, yaitu dengan cara meminjam *bit host* menjadi *bit network*. Teknik *subnet* menjadi penting bila sebuah jaringan memiliki alokasi *IP* yang terbatas. Gin-Gin Yugianto, (2012).

2.2.5.5 *User Datagram Protocol* (UDP)

Merupakan protokol *transport* yang digunakan secara luas pada urutan kedua. Seperti *transmission control protocol* (TCP), UDP menggunakan *port* dan menyediakan konektivitas *end-to-end* antara aplikasi *client* dan *server*. UDP merupakan protokol yang kecil dan efisien. Tetapi, berbeda dengan TCP, UDP tidak menjamin pengiriman datanya, aplikasi harus mengimplementasikan mekanisme *error recovery*-nya sendiri jika memerlukan mekanisme tersebut. Hal ini membuatnya cocok untuk beberapa aplikasi, tetapi tidak untuk beberapa yang lain. Menurut Gin-Gin Yugianto, (2012).

2.2.6 *Web Server*

Web server adalah *software* yang menjadi tulang belakang dari *world wide web* (www) yang pertama kali tercipta sekitar tahun 1980an**.** *Web server* menunggu permintaan dari *client* yang menggunakan *browser* seperti *Netscape Navigator, Internet Explorer, Mozilla Firefox,* dan program browser lainnya. Jika ada permintaan dari browser, maka *web server* akan memproses permintaan itu kemudian memberikan hasil prosesnya berupa data yang diinginkan kembali ke browser. Evy Nurmiati, (2012).

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Web server mempunyai sebutan format standar yaitu SGML (S*tandar General Markup Language*). menampilkan gambar tersebut, dan jika ada akan menampilkan alternatifnya saja. *Web server* dalam berkomunikasi dengan *client*-nya (*web browser*) mempunyai protokol sendiri, yaitu HTTP (*hypertext transfer protocol*). Dengan protokol ini, komunikasi antar *web server* dengan *client*-nya dapat saling dimengerti dan lebih mudah. Seperti telah dijelaskan diatas, format data pada *world wide web* adalah SGML. Tapi para pengguna internet saat ini lebih banyak menggunakan format HTML (*hypertext markup language*) karena penggunaannya lebih sederhana dan mudah dipelajari.

Contoh standarisasi *web server* antara lain :

1. Spesifikasi HTML, CSS, DOM dan XHTML (W3C)
2. Spesifikasi Javascript (ECMA)
3. URL, HTTP (IETF) dalam bentuk dokumen RFC

2.3 Hipotesis

Dengan dilakukannya penelitian tentang "Analisa dan Implementasi *High Interaction Honeypot* Pada *Server*" maka diharapkan akan membantu membangun keamanan jaringan dan mengetaui kelebihan dan kelemahannya sistem keamanan *honeypot* dengan baik.

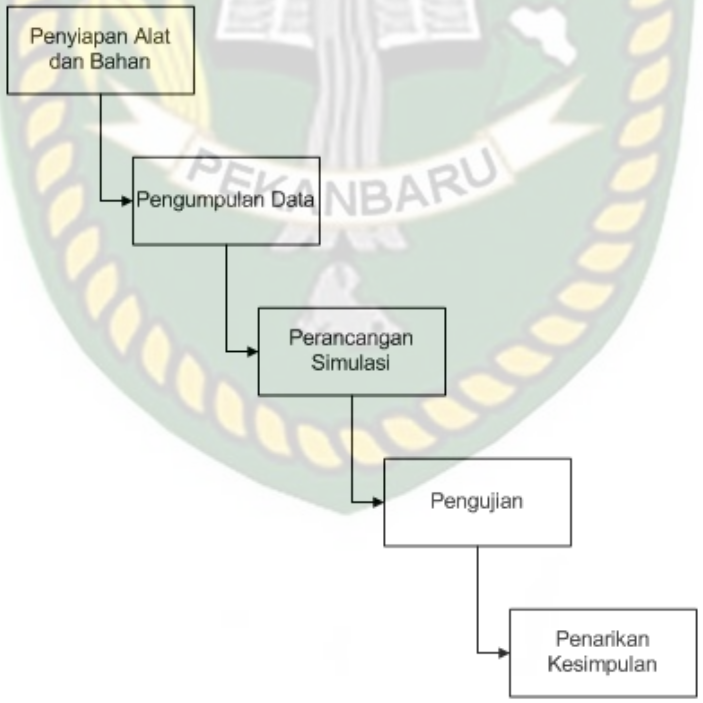
Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

BAB III

METODOLOGI PENELITIAN

3.1 Metodologi Penelitian

Metodologi penelitian mendefinisikan tahapan dan prosedur yang dilakukan dalam penelitian ini menjelaskan dan memperkenalkan simulasi pengembangan sistem keamanan *honeypot* secara umum, adapun tahapan dari penelitian ini adalah penyiapan alat dan bahan, pengumpulan data, pengembangan dan perancangan simulasi, parameter kerja, kerangka pemodelan, evaluasi hasil penelitian dan penarikan kesimpulan. Seperti pada gambar 3.1 berikut ini.



Gambar 3.1 Metode Penelitian Tugas Akhir

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3.2 Alat dan Bahan Penelitian yang Digunakan

Untuk mendapatkan hasil seperti yang diinginkan dalam perancangan sistem pendukung keputusan ini tentunya membutuhkan beberapa komponen penunjang dalam proses pengerjaannya, antara lain sebagai berikut :

3.2.1 Perangkat Keras (*Hardware*)

Adapun peralatan perangkat keras dari penelitian yaitu :

1. Spesifikasi *Minimum* Laptop *Intel Core* i3
2. *RAM* 2GB
3. *Harddisk* 320GB
4. *CPU* 1.2 GHz
5. *Router* Mikrotik RB951-2nD
6. *Ethernet* minimal 10/100Mbps
7. *Support Firewall*, NAT dan PAT
8. Kabel *UTP serial cross*
9. *PC Client* dan *Server*

3.2.2 Perangkat Lunak (*Software*)

Adapun peralatan perangkat lunak dari penelitian yaitu :

1. Sistem operasi : *Microsoft Windows* 7, *Kali linux 2020*
2. Bahasa Pemograman : *Winbox* (*Scripting*)
3. Tool yang digunakan : - *Microsoft Office Visio Proffesional* 2007

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

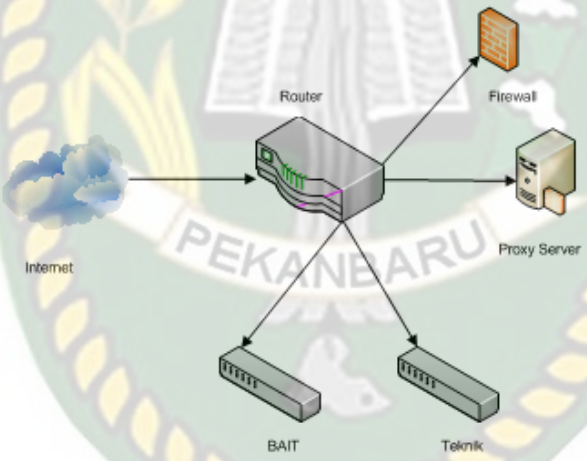
- Pentbox 1.8, Nmap

3.3 Pengembangan dan Perancangan Sistem

Adapun tahap pengembangan dan perancangan simulasi sebagai berikut :

3.3.1 Perancangan Topologi

Dalam membangun sebuah jaringan perlunya sebuah rancangan topologi jaringan untuk mengatur dan mempermudah mengetahui lalu lintas jaringan yang dibangun. Topologi yang digunakan dalam penelitian ini yaitu Topologi *Star*. (Roni, 2017).



Gambar 3.2 Topologi UIR (Roni Kharisma, 2017)

Adapun topologi yang digunakan dalam penelitian diambil dari topologi jaringan UIR (Universitas Islam Riau). Kemudian IP address pada topologi jaringan tersebut sebagai berikut.

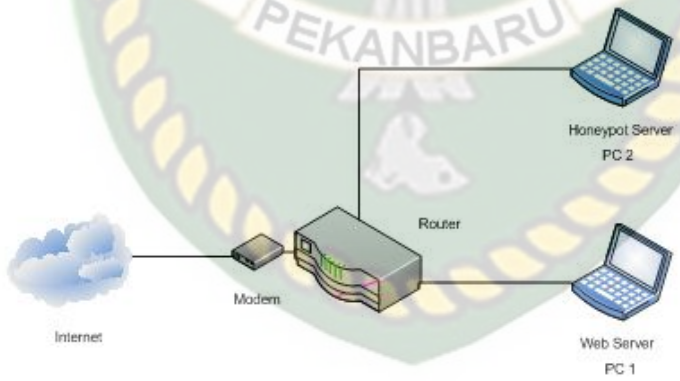
Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Tabel 3.1 *IP Address* Topologi (Roni Karisma, 2017)

	Interface	IP Address	Subnet Mask	Gateway
GATEWAY	Fa0/0	192.168.137.2	255.255.255.0	192.168.137.1
	Fa0/1	192.168.0.1	255.255.255.0	
BAIT	Fa0/1	10.0.255.254	255.255.255.0	
TEKNIK	Fa0/0	172.16.12.1	255.255.255.0	

3.3.2 Perancangan Program

Pada implementasi jaringan dibawah ini terdapat 2 PC, PC 1 berfungsi sebagai *server* dengan sistem operasi *windows 7 ultimate* dan *winbox*, PC 2 berfungsi sebagai *honeypot server* dengan sistem operasi *kali linux 2020*.



Gambar 3.3 Rancangan *Server Honeypot*.

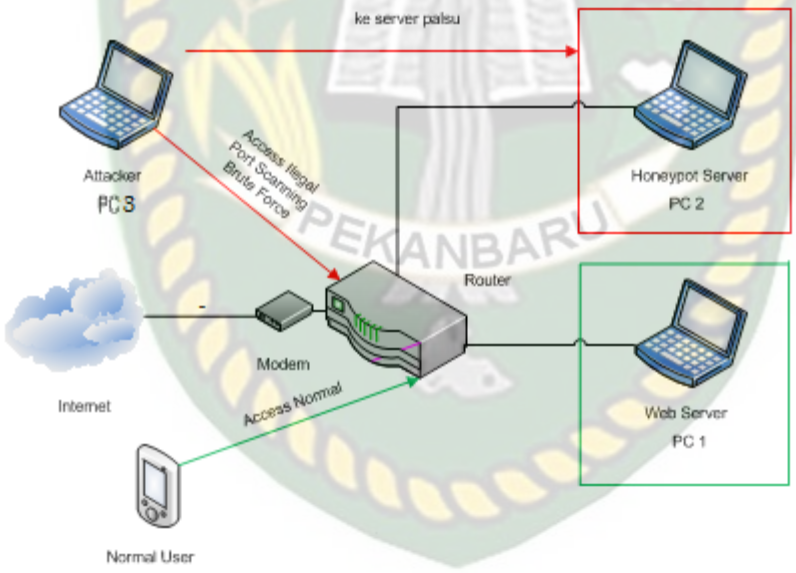
Adapun untuk *IP address* pada rancangan topologi *server honeypot* sebagai berikut.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Tabel 3.2 *IP Address* Rancangan Topologi Jaringan *Server Honeypot*

Device	IP Address	Subnet Mask	Gateway
Router	107.0.0.1	255.255.255.0	192.168.0.1
Honetpot Server	192.168.0.100	255.255.255.0	192.168.0.1
Web Server	198.168.0.104	255.255.255.0	192.168.10.1

3.3.3 Skenario yang Digunakan pada Implementasi



Gambar 3.4 Rancangan Pengalihan *Attacker ke Server*

Dari implementasi diatas dapat dilihat bahwa *attacker* akan mencoba *scanning* dari perangkat *router* untuk mencari komputer *server* dari perangkat tersebut. Namun sebelumnya pada *honeypot server* sudah diatur sebagaimana *server* aslinya, dan

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

memberikan peluang buat penyusup dengan membuka beberapa *port*. *Port* yang dibuka pada *honeypot server* bertujuan untuk meyakinkan *attacker* bahwa *honeypot serve*r berpeluang sebagai *server* asli padahal sebaliknya yang nanti disusupi *attacker* adalah *server* palsu dari *honeypot server*.

Selanjutnya untuk pengalihan *address* pada jaringan *server honeypot* ini peneliti sudah menentukan *request* maupun *port* yang akan dialihkan ke *server honeypot* tersebut antara lain sebagai berikut.

Tabel 3.3 Pengalihan *Request* oleh *Router*

Device	Request	Destination port	Destination IP	Direction IP	Direction Port
Web Server	http	80	192.168.0.103	192.168.0.104	81
Honeypot	http xfer krb524	80 82 4444	192.168.0.103	192.168.1.2	80 82 4444

3.4 Parameter Kerja Sistem Jaringan

1. *Prevention* (pencegahan)

   Kebanyakan dari ancaman akan dapat ditepis dengan mudah, walaupun keadaan yang benar-benar 100% aman belum tentu dapat dicapai.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Akses yang tidak diinginkan kedalam jaringan komputer dapat dicegah dengan memilih dan melakukan konfigurasi layanan (*service*) yang berjalan dengan hati-hati.

2. *Observation* (observasi)

   Ketika sebuah jaringan komputer sedang berjalan, dan sebuah akses yang tidak diinginkan dicegah, maka proses perawatan dilakukan. Perawatan jaringan komputer harus termasuk melihat isi log yang tidak terpantau. Sistem *honeypot* dapat digunakan sebagian dari proses observasi tetapi menggunakan *honeypot* tidak merujuk kepada ketidak pedulian pada informasi log yang disediakan.

3. *Response* (respon)

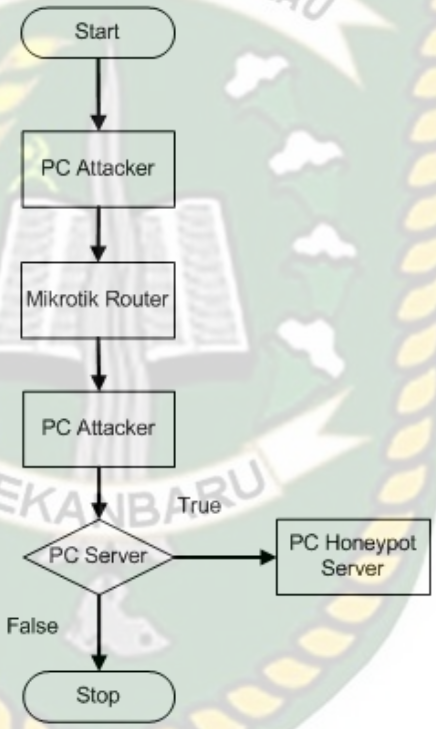
   Bila sesuatau yang tidak diinginkan terjadi dan keamanan suatu sistem telah berhasil disusupi, maka personil perawatan harus segera mengambil tindakan tergantung pada proses produktifitas dan masalah yang menyangkut dengan keamanan maka tindakan yang tepat harus segera dilaksanakan. Bila sebuah proses sangat vital pengaruhnya kepada fungsi sistem yang telah disusupi telah dibiarkan berjalan, maka harus dipertimbangkan untuk direncanakan perawatan pada saat yang tepat. Ini merupakan masalah yang sulit dikarenakan tidak seorangpun akan segera tahu apa yang menjadi celah begitu sistem telah disusupi.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

4. *Sniffing* (penyadap)

   Tindakan penyadapan yang dilakukan dalam jaringan komputer dengan tujuan untuk dapat mencuri data-data pribadi ataupun *account* lain yang bersifat pribadi.

3.5 Kerangka Pemodelan



Gambar 3.5 *Flowchart* Sistem Penyusupan *Router*

Pada gambar 3.4 diatas menjelaskan kerangka pemodelan mulai dari user mengakses sistem login ke *router* menggunakan username dan password yang sudah ditentukan namun dengan cara request normal atau tidak norma user mengakses sistem tersebut,

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

maka router akan mengirimkan log ke server asli jika user mengakses dengan normal dan sebaliknya jika tidak dianggap normal maka akan dialihkan ke *server honeypot.*

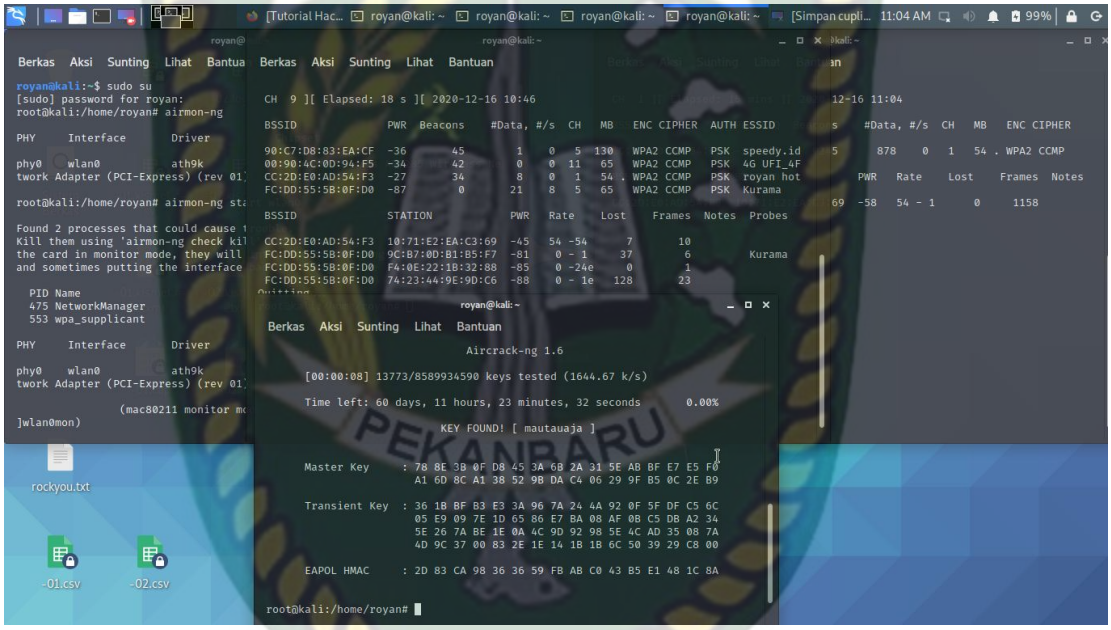
Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

BAB IV

HASIL DAN PEMBAHASAN

4.1 Hasil

Hasil dari proses dengan metode *Word List* menggunakan *rockyou.txt* bertujuan untuk mendapatkan *password* enkripsi *wpa2* pada sebuah jaringan *hotspot* mikrotik.



Gambar 4.1 *Cracking Password Word List Airmon-ng*.

Berikut ini keterangan dari konfigurasi *airmon-ng* berdasarkan Gambar 4.1 :

1. *Airmon-ng* = menjalankan *airmon-ng* pada *user root kali linux*.
2. *Airmon-ng start wlan0* = mengaktifkan *wlan0* sebagai monitoring jaringan.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3. *Airmon-ng check kill* = perintah proses merekam scanning jaringan dan akan memutuskan jaringan *internet*.
4. *Airodump-ng wlan0mo*n = perintah yang ada pada airmon-ng untuk menampilkan hasil informasi dari scan jaringan disekitar dan tekan *ctrl+c* untuk menghentikan setelah mendapatkan BSSID dari jaringan disekitar.
5. *Airodump-ng -c 1 –bssid CC:2D:E0:AD:54:F3 -w /home/royan/Destop/ wlan0mon* = perintah ini memilih channel dan bssid dari hasil *scan* menulis penyimpannya di Destop.
6. *Aircrack-ng -a2 -b CC:2D:E0:AD:54:F3 -w /home/royan/Destop/rockyou.txt /home/royan/Destop/*.cap* = perintah -a2 metode *aircrack-ng* untuk meretas *handshake* yang udah didapatkan tadi pada *scan* dan yang metode yang digunakan adalah *wpa2*, -b merupakan bssid komputer dan diganti dengan router bssid sasaran. setelah itu -w kita masukkan ke *word list* yang berdada pada Destop dan *.*cap* menangkap *passwor*d dari *word list rockyou.txt* sampai menemukannya.

Hasil dari *cracking* gambar 4.1 diatas merupakan contoh dari *attacker* melakukan *brute force* pada jaringan tanpa diketahui oleh pemilik dari penyedia jaringan tersebut. Peroses tersebut menggunakan sistem operasi *kali linux 2020.3* dan dapat dilihat dari hasil peroses illegal tersebut tidak memerlukan waktu yang lama untuk meretas *password* dari *hotspot wifi* mikrotik. *Airmon-ng* sebuah aplikasi berbasis

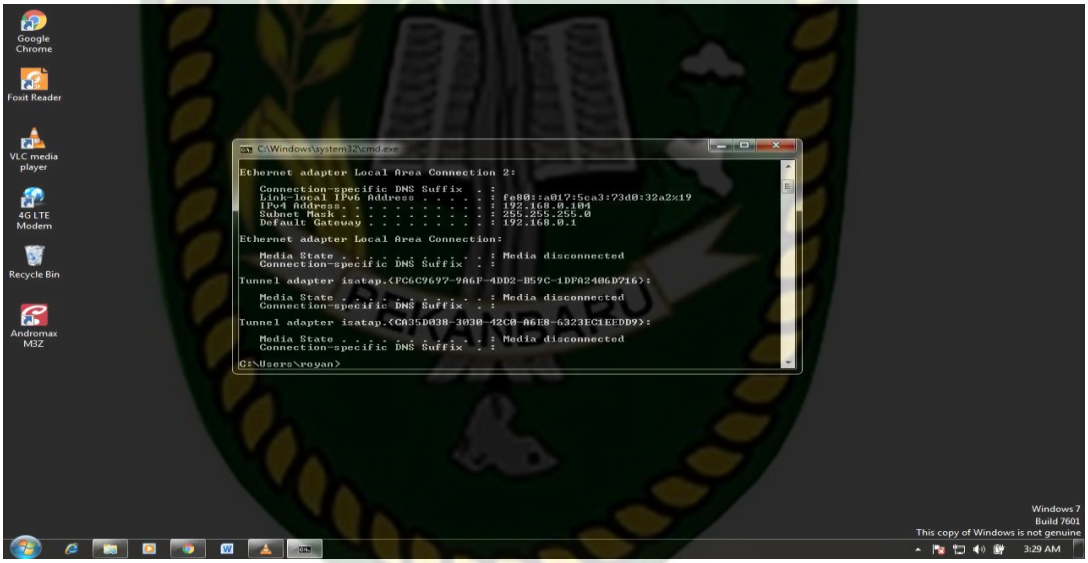
Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

word list yang berada di sistem operasi kali linux biasanya digunakan untuk *cracking* sistem keamanan *wpa/wpa2*.

4.2 Pembahasan

4.2.1 Peralatan Penerapan *Honeypot*

Pengujian *honeypo*t sebagai pengalihan attacker pada *server* asli. Dalam pengujian menggunakan 3 perangkat komputer. Adapun pengujian komputer *server* menggunakan sistem operasi *windows 7 ultimate* dengan *ip address* 192.168.0.104.

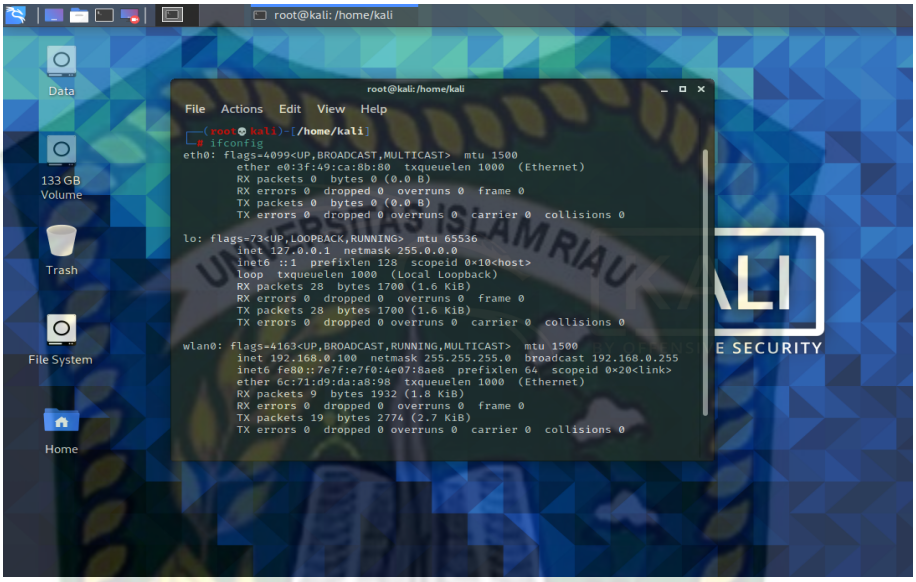


Gambar 4.2 Komputer 1 sebagai *serve*r.

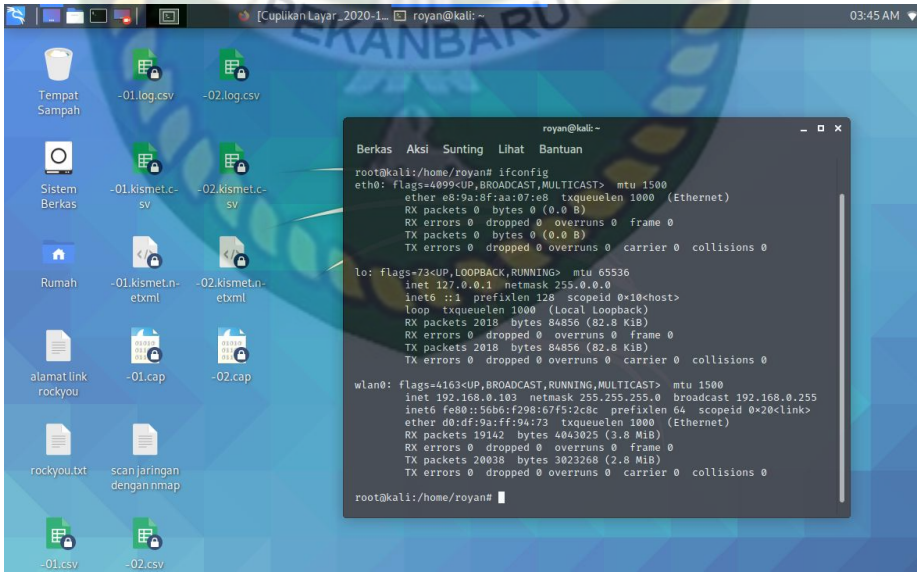
Kemudian untuk komputer 2 akan digunakan sebagai *honeypot* yang fungsinya sebagai pengecoh serangan agar tidak berinteraksi langsung dengan computer *server*

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

jaringan yang aslinya. Komputer 2 menggunakan sistem operasi *kali linux 2020.4* dengan *ip address* 192.168.0.100.



Gambar 4.3 Komputer 2 sebagai *Honeypot*.



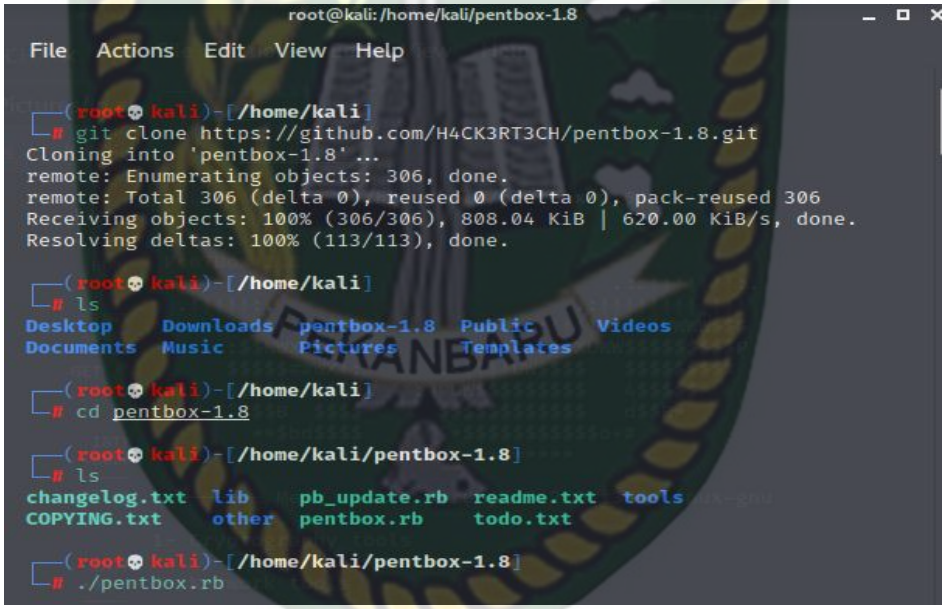
Gambar 4.4 Komputer 3 *Attacker*.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Selanjutnya komputer 3 akan digunakan sebagai attacker kesistem jaringan untuk mendapatkan informasi dari jaringan komputer-komputer yang terhubung. Sistem operasi yang digunakan *kali linux 2020.3* dengan *ip address* 192.168.0.103.

4.2.2 Pengujian Penerapan *Honeypot*

Berikut ini dilakukan setelah penerapan *honeypot* pada sebuah jaringan komputer dalam menjalankan perannya sebagai layaknya sebuah *server*. Adapun *tool* yang digunakan adalah *pentbox-1.8* sebagai *honeypot*.

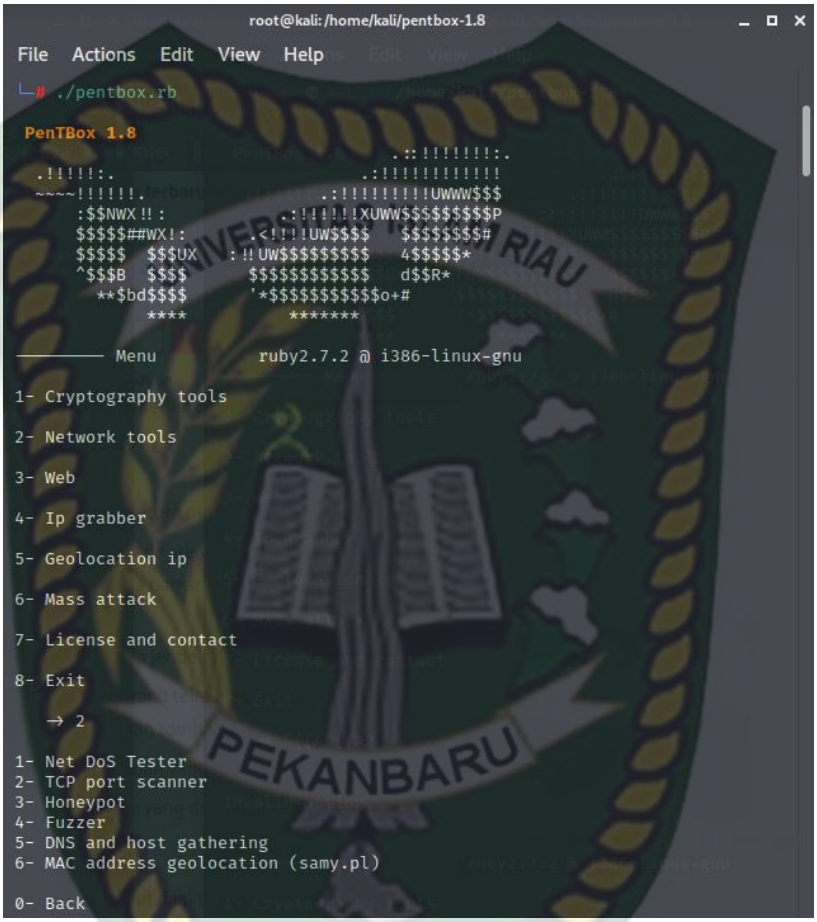


Gambar 4.5 Instalasi Pentbox 1.8 Pada Dikomputer 2.

Pentbox merupakan keamanan *open source* yang digunakan untuk untuk menguji stabilitas keamanan sistem. Aplikasi ini dibuat sudah sebaik mungkin karena mempermudah penggunanya tanpa harus melakukan setting yang rumit.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

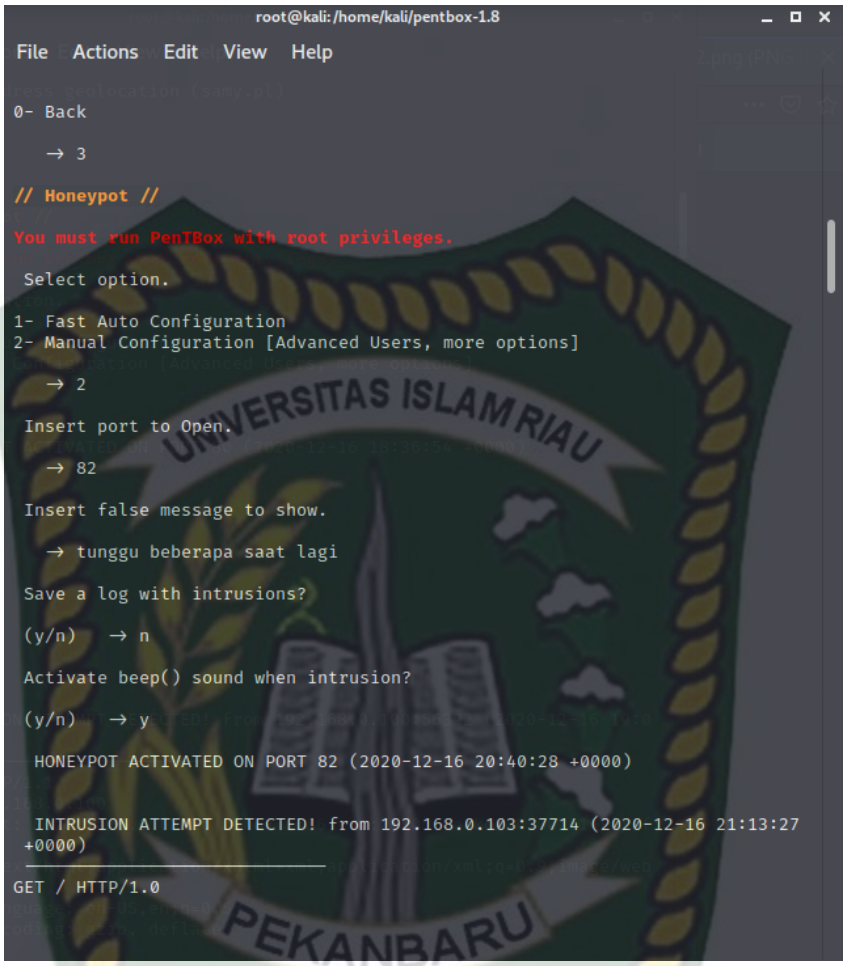
Disini penulis melakukan uji coba honepot dengan membuka beberapa port yang akan diuji dalam penyusupan nanti oleh sipenyusup.



Gambar 4.6 Proses setting honeypot membuka *port*.

Setelah menjalankan pentbox 1.8 muncul beberapa pilihan yang tersedia. Karena yang diujikan adalah honeypot untuk keamanan jaringan jadi penulis memilih Network tools. Kemudian menjalankan pilihan Honeypot yang berada pada Gambar 4.6.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

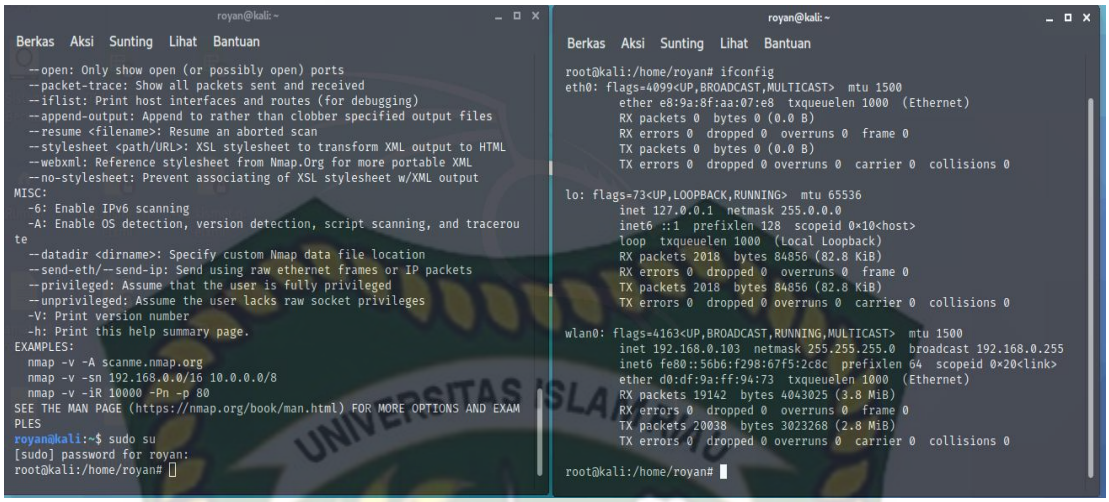


Gambar 4.7 pemilihan port yang akan dibuka.

Adapun dalam setting honeypot dilakukan membuka beberapa port yaitu port 80,82 dan 4444. Untuk hasil dari honeypot pada setiap log berapa pada Gambar 4.15, 4.16 dan Gambar 4.17.

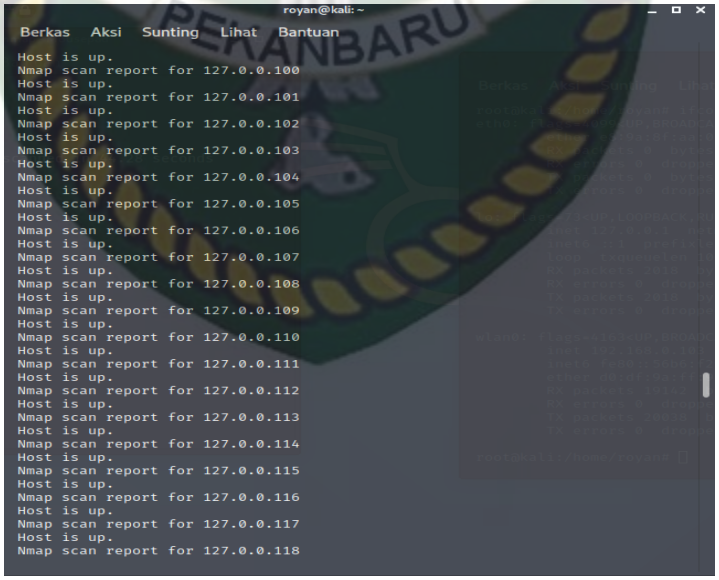
Kemudian berikut ini penyusupan yang dilakukan oleh komputer 3 ke jaringan untuk mendapatkan informasi menngunakan aplikasi Nmap.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 4.8 Scanning Nmap pada Jaringan.

Komputer 3 menemukan ip dari scanning akses jaringan yang sebelumnya sudah terhubung pada jaringan tersebut. Pada gambar 4.9 penyusup mencoba scanning ip 127.0.0.1 yang merupan perangkat penyedia jaringan.

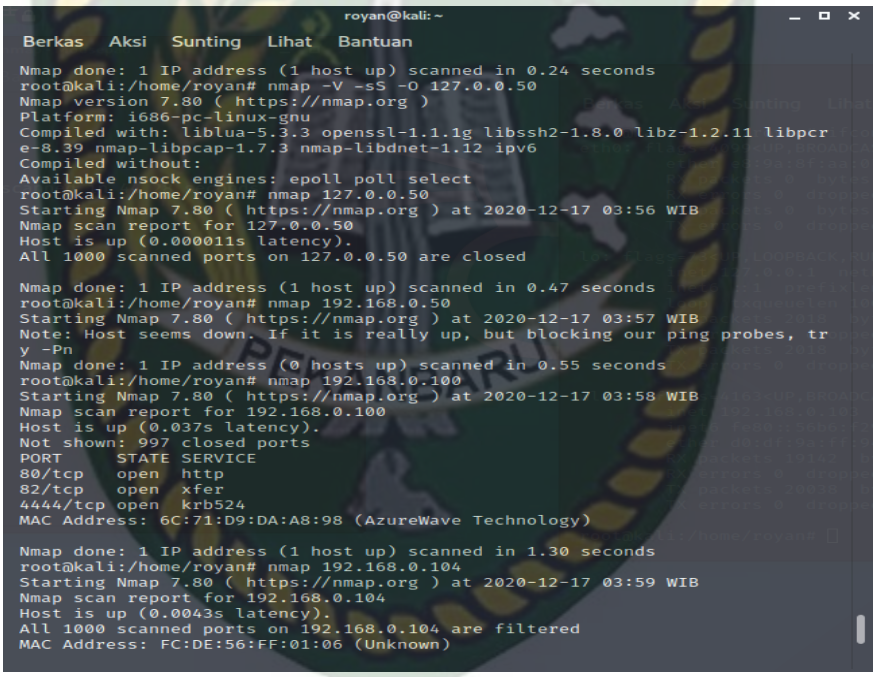


Gambar 4.9 Hasil Scanning IP 172.0.0.1/24.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Deteksi scanning perangkat jaringan ip 127.0.0.1 mendapatkann hasil batasan ip berapa saja yang bisa terhubung perangkat tersebut *syntax* : *nmap -sn* 127.0.0.1/24.

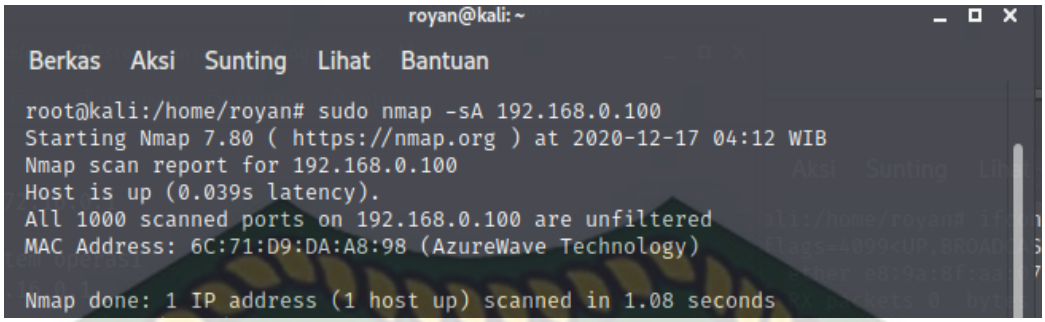
Dari hasil deteksi penyusup mengambil tindakan untuk mencoba menemukan ip dari *server* jaringan tersebut. Yang mana nantinya akan menggali informasi maupun melakukan tindakan merugikan bagi server. Pada gambar 4.10 penyusup mulai mencoba scanning beberapa *ip address* dari batasan *ip* yang tersedia pada perangkat jaringan.



Gambar 4.10 *Nmap* Mencoba *Scanning IP* Yang Tersedia. .

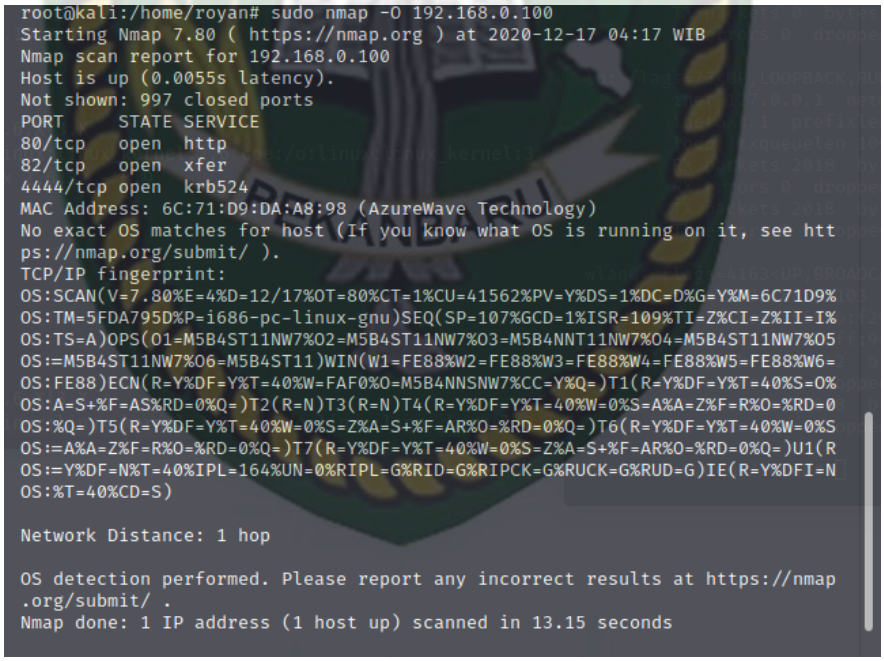
Gambar 4.10 hasi deteksi *port scanning* terdapat ada 1 *ip address* yang dianggap *server* oleh penyusup dengan *ip address* 192.168.0.100.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 4.11 *Nmap* Deteksi *Firewall IP Address* 192.168.01.100.

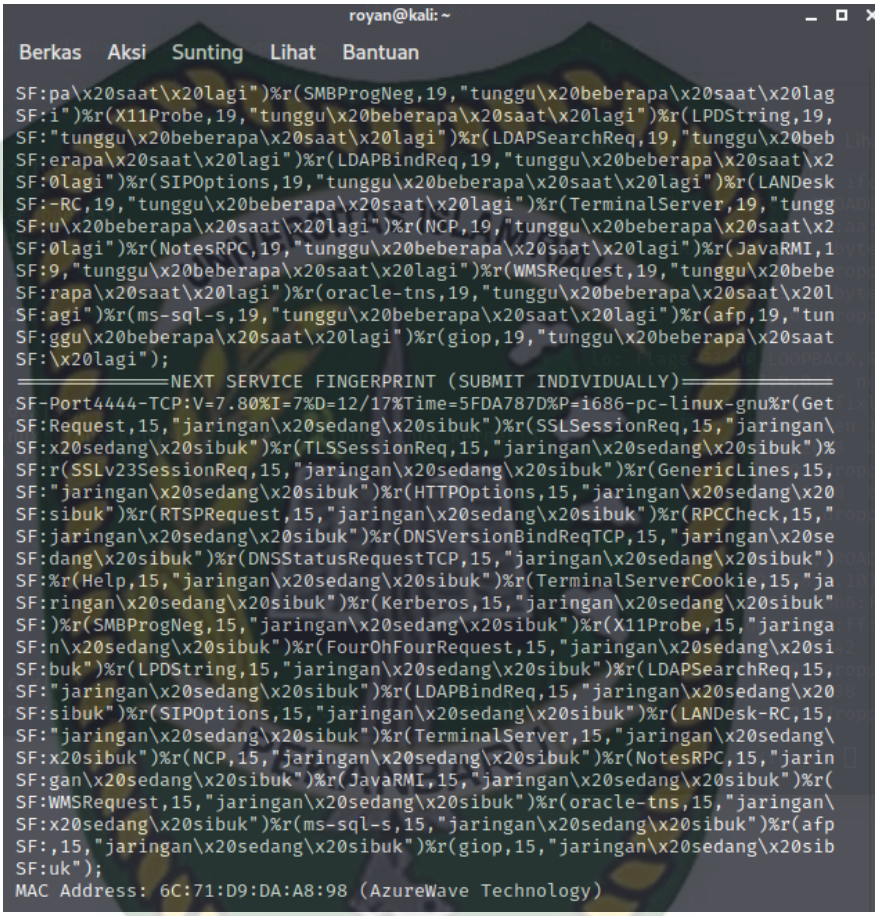
Pada gambar 4.11 *attacker* memutuskan untuk menelusuri informasi dari ip 192.168.0.100. karena dianggap mempunyai potensi sebagai *ip server* dan mencoba *scanning firewall* pada *ip* tersebut. *Syntax : sudo nmap -sA* 192.168.0.100.



Gambar 4.12 *Nmap Scanning* Sistem Operasi.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

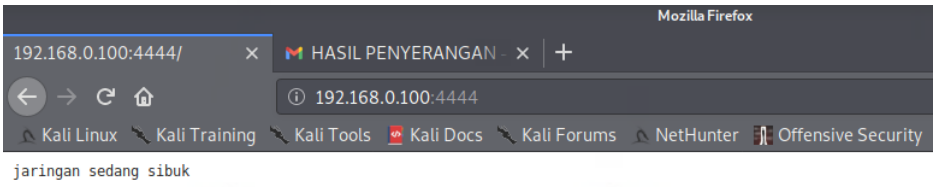
Pada gambar 4.12 *attacker* mencoba kembali ingin mengetahui sistem operasi dari *ip address* 192.168.0.100 dan mendapatkannya yaitu linux-gnu.



Gambar 4.13 *Nmap* Mendapat *Script* Dari *Scanning*.

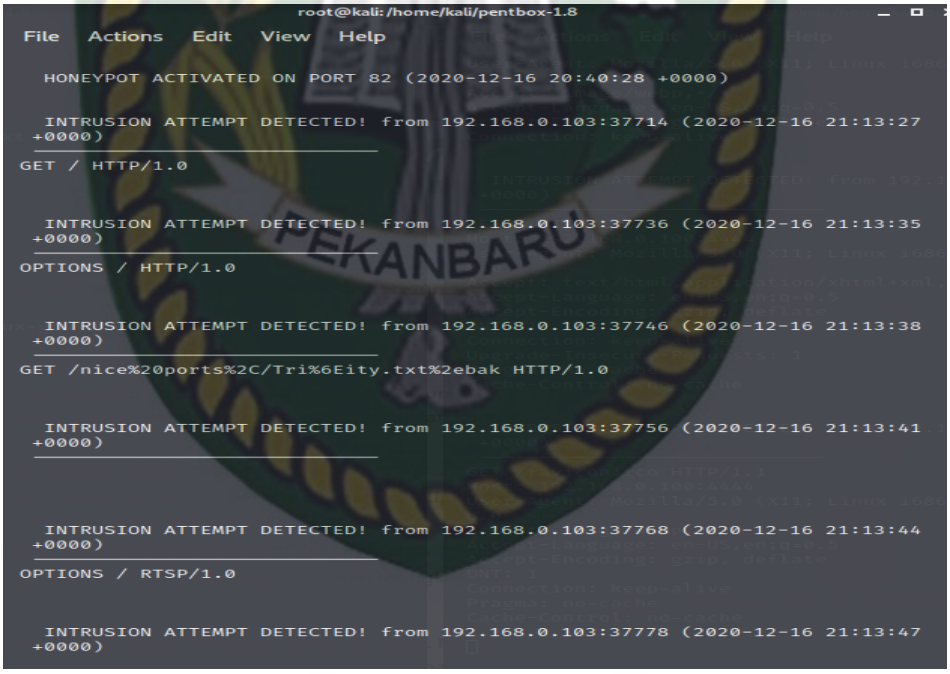
Adapun didalam scanning sistem operasi tersebut *attacker* menemukan script yang dibuat *honeypot* pada *pentabox* sebelumnya. Disini *attacker* belum mengetahui bahwa yang *ip* yang ditelusuri informasinya adalah *honeypo*t.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 4.14 *Nmap* Mencoba *Scanning Port* 4444.

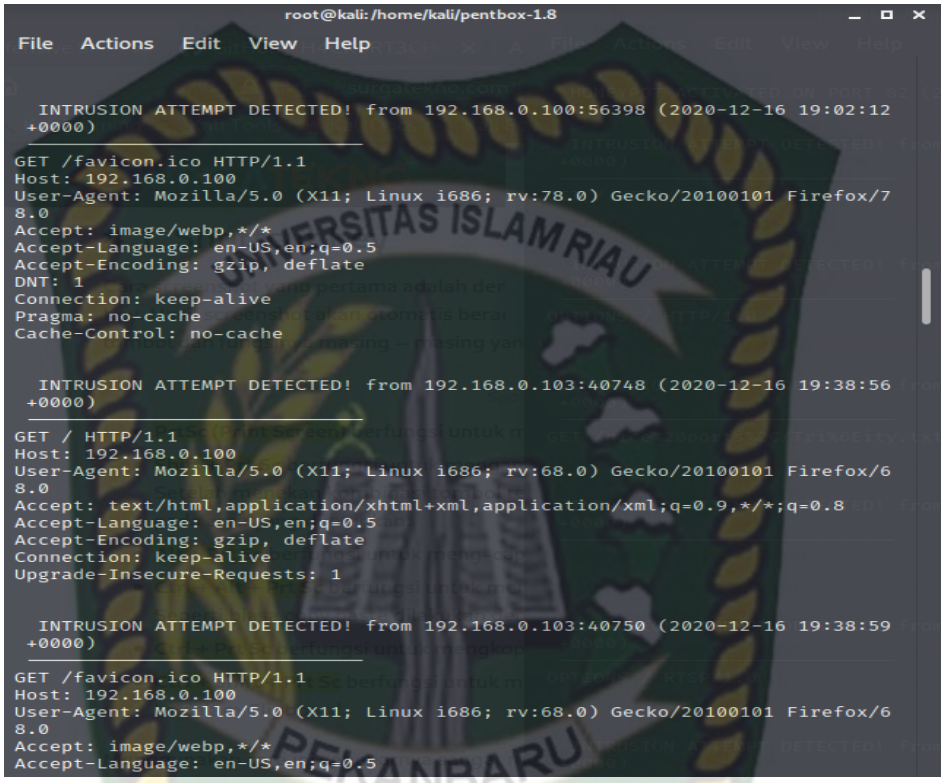
Pada gambar 4.14 *attacker* mencoba melakukan layanan TCP/DCP pada ip 192.168.0.100 dan hasilnya seperti di gambar 4.14 tersebut.



Gambar 4.15 Hasil *Log Port* 82 *Honeypot*.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Gambar 4.15 hasil laporan log dari port 82 *honeypot* yang sudah diatur sebelumnya dan mendapatkan hasil informasi.



Gambar 4.16 Hasil *log port* 80 *honeypot.*

Pada gambar 4.16 hasil *log port* 80 *honeypot* menampilkan *log* adanya tindakan illegal yang berusaha menggali informasi dari *ip* 192.168.0.100.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 4.17 Hasil *Log Port* 4444 *Honeypot*.

Berikutnya hasil laporan *log honeypot* pada *port* 4444 gambar 4.17 mendapatkan informasi adanya tindakan mengirimkan *bug* pada sistem agar jalur akses data *down*.

Analisis dari hasil pengujian yang dilakukan tersebut. Terlihat *honeypot* sudah memberikan pembuktian bahwa sistem *honeypo*t tersebut dapat berinteraksi dengan *attacker*. *Honeypot* sendiri dapat menentukan apa yang akan diserang oleh *attacker* nantinya.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan dalam penelitian yang berjudul Analisis dan Implementasi *High Interction Honeypot* Pada *Server* maka dapat disimpulkan sebagai berikut :

1. *Honeypot* merespon dengan cepat ketika ada penyusupan pada celah *port* yang telah dibuka pada sistem sebagai pengalihan *attacker*.
2. *Log honeypot* mendeteksi informasi perangkat yang digunakan oleh penyusup.
3. *Honeypot* hanya bekerja ketika ada ancaman pada komputer *honeypot* itu sendiri, jika *attacker* menyusup ke *server* asli maka honeypot tidak dapat mendeteksi adanya ancaman penyusupan.

5.2 Saran

Dari hasil pengujian aplikasi *honeypo*t dapat dikembangkan lebih lanjut dan bisa ditambahkan sistem keamanan lainnya seperti penambahan keamanan dengan IDS maupun IPS. Agar menjadi sistem keamanan pendeteksi lebih lanjut dan akurat dalam menangangi ancaman penyusupan yang dapat merugikan keamanan data.

.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

DAFTAR PUSTAKA

Ariyus, Dony. 2007. *Intrusion Detection System*. Yogyakarta: Andi Yogyakarta.

Ferdiansyah, Doddy. 2013. Pemanfaatan Teknologi *Honeypot* Dalam Meningkatkan *Availability* Pada Sistem Jaringan. Jurnal Teknik Universitas Pasundan. Vol. 15, No. 1.

Dahlan, Moh, Anastasya Latubessy, dan Mukhamad Nurkamid. 2015. Analisa Keamanan *Web Server* Terhadap Serangan *Possibility SQL Injection*. Jurnal Teknik Elektro Universitas Muria Kudus.

Nazwita, dan Siti Ramadhan. 2017. Analisis Sistem Keamanan *Web Server* dan *Database Server* Menggunakan *Suricata*. Sains Dan Teknologi UIN Sultan Syarif Kasim Riau.

Nurmiati, Evy. 2012. Analisis dan Perancangan *Web Server* Pada *Handphone*. Vol. 5, No. 2.

Prasetyo, Dimas. 2011. Perancangan Kolaborasi Sistem Deteksi Intruksi Jaringan Tersebar dengan *Honeypot* menggunakan *Metode elert Correlation*. *E-journa*l Teknik Elektro dan Komputer UNSRAT Manado. Vol. 3. No. 2.

Randy, Mentang, et al. 2015, Perancangan dan Analisis Keamanan Jaringan *Nirkabel* Menggunakan *Wireless Intrusion Detection System*. *E-journal* Teknik Elektro dan Komputer UNSRAT Manado. Volume 5. No 7.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Karisma, Roni. 2017. Simulasi Implementasi *Intrusion Prevention System* Pada Router Mikrotik, Jurnal Teknik Informatika Universitas Islam Riau.

Yugianto, Gin-Gin, dan Rachman Oscar. 2012. *Router* Teknologi, Konsep, Konfigurasi, dan *Troubleshooting*. Informatika Bandung.

Zulkarnaen, Disky. 2010. Implementasi *Honeypot* Sebagai Alat Bantu Deteksi Keamanan Jaringan Pada Kantor Pengawasan dan Pelayanan Bea dan Cukai Tipe A2 Palembang. Jurnal Teknik Informatika STMIK PalComTech Palembang. Vol. 4, No. 13.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :