PENERAPAN KEAMANAN JARINGAN MENGGUNAKAN SISTEM *SNORT* DAN *HONEYPOT* SEBAGAI PENDETEKSI DAN PENCEGAH *MALWARE*

SKRIPSI

Diajukan Oleh :

Zakia Fuada
NIM. 190212006

Bidang Peminatan : Teknik Komputer Jaringan

Mahasiswa Fakultas Tarbiyah dan Keguruan

Program Studi Pendidikan Teknologi Informasi

UNIVERSITAS ISLAM NEGERI AR-RANIRY

FAKULTAS TARBIYAH DAN KEGURUAN

PROGRAM STUDI PENDIDIKAN TEKNOLOGI INFORMASI

2023 M/ 1444 H

SKRIPSI

PENERAPAN KEAMANAN JARINGAN MENGGUNAKAN SISTEM *SNORT* DAN *HONEYPOT* SEBAGAI PENDETEKSI DAN PENCEGAH *MALWARE*

Oleh :

Zakia Fuada

NIM. 190212006

Mahasiswa Fakultas Tarbiyah dan Keguruan

Program Studi Pendidikan Teknologi Informasi

Bidang Peminatan : Teknik Komputer dan Jaringan (TKJ)

Disetujui Oleh

Pembimbing I	Pembimbing II
(Mira Maisura, M.Sc)	(Aulia Syarif Aziz, S.Kom., M.Sc)
NIP. 198605272019032011	NIP. 199305212022031001

PENERAPAN KEAMANAN JARINGAN MENGGUNAKAN SISTEM *SNORT* DAN *HONEYPOT* SEBAGAI PENDETEKSI DAN PENCEGAH *MALWARE*

SKRIPSI

Telah diuji oleh Panitia Ujian Munaqasyah Skripsi Fakultas Tarbiyah dan Keguruan UIN Ar-Raniry Banda Aceh dan Dinyatakan Lulus serta diterima sebagai salah satu beban studi Program Sarjana (S-1) dalam Pendidikan Teknologi Informasi

Pada:

Kamis, 09 November 2023

25 Rabiul Akhir 1445 H

Darussalam – Banda Aceh

Panitia Ujian Munaqasyah Skripsi

Ketua	Sekretaris
(Mira Maisura, M. Sc.)	(Aulia Syarif Aziz, S.Kom., M.)
NIP.198605272019032011	NIP. 199305212022031001
Penguji 1	Penguji 2
(Raihan Islamadina, S. T., M.T.)	(Baihaqi, M. T.)
NIP. 198901312020122011	NIDN. 1321028801

Mengetahui,
Dekan Fakultas Tarbiyah dan Keguruan UIN Ar-Raniry
Darussalam Banda Aceh

Prof. Safrul Mulak, S.Ag., M.A., M.Ed., Ph.D
NIP. 19730102 199703 1 003

LEMBAR PERNYATAAN KEASLIAN KARYA ILMIAH

Yang bertanda tangan di bawah ini:

Nama	: Zakia Fuada
NIM	: 190212006
Program Studi	: Pendidikan Teknologi Informasi
Fakultas	: Tarbiyah dan Keguruan
Judul Skripsi	: Penerapan Keamana Menggunakan Sistem *Snort* dan *Honenypot* Sebagai Pendeteksi Dan Pencegah *Malware*

Dengan ini menyatakan bahwa dalam penulisan skripsi ini, saya:

1. Tidak menggunakan ide orang lain tanpa mampu mengembangkan dan memper tanggung jawabkan.
2. Tidak melakukan plagiat terhadap naskah karya orang lain.
3. Tidak menggunakan karya orang lain tanpa menyebutkan sumber asli atau tanpa izin pemilik karya.
4. Tidak memanipulasi dan memalsukan data.
5. Mengerjakan karya ini dan mampu bertanggung jawab atas karya ini.

Bila dikemudian hari ada tuntutan dari pihak lain atas karya saya, dan telah melalui pembuktian yang dapat dipertanggungjawabkan dan ternyata memang ditemukan bukti bahwa saya telah melanggar pernyataan ini, maka saya siap dikenai sanksi berdasarkan atauran yang berlaku di Fakultas Tarbiyah dan Keguruan UIN Ar-Raniry Banda Aceh.

Demikian surat pernyataan saya buat dengan sesungguhnya.

Banda Aceh, 22 September 2023

Zakia Fuada

ABSTRAK

Nama : Zakia Fuada

NIM : 190212006

Fakultas/Prodi : Tarbiyah dan Keguruan/Pendidikan Teknologi Informasi

Judu : Penerapan Keamanan Jaringan Menggunakan Sistem *Snort* Dan *Honeypot* Sebagai Pendeteksi Dan Pencegah *Malware*

Bidang Peminatan : Teknik Komputer dan Jaringan

Jumlah Halaman : 57 Halaman

Pembimbing I : Mira Maisura, M.Sc

Pembimbing II : Aulia Syarif Aziz, S.Kom., M.Sc

Kata Kunci : Keamanan, Jaringan, Pendeteksi

Seiring berkembangnya teknologi informasi khususnya keamanan jaringan komputer dan layanan-layanannya yang mempermudah pekerjaan-pekerjaan manusia sehari-hari, akan tetapi di sisi lain timbul masalah yang sangat serius, yakni faktor keamanannya. Manusia sudah sangat tergantung dengan sistem informasi, akan tetapi statistik insiden keamanan meningkat tajam. Hal ini secara umum terjadi karena kepedulian terhadap keamanan sistem informasi masih sangat kurang.

Penelitian ini menggunakan metode *action research* adalah metode penelitian yang digunakan untuk menguji, mengembangkan. *Diagnosis* pada tahap ini dilaksanakan analisa kebutuhan, analisa permasalahan yang muncul analisa keiginan user dan topologi yang sedang berjalan. *Action Planing* pada tahapan ini dari peneliti memahami masalah dan akan melakukan penerapan konfigurasi *snort* dan *honeypot* menggunakan sistem operasi *linux ubuntu* untuk menyelesaikan

masalah keamanan jaringan pada *laboratorium* multifungsi UIN Ar-Raniry. *Intervention* pada tahap ini peneliti melakukan *implementasi snort* dan *honeypot.*

Honeypot adalah sebuah sistem atau komputer yang sengaja dijadikan umpan untuk menjadi target serangan dari penyerang (attacker), sehingga penyerang akan terjebak oleh umpan *Honeypot*. *Snort* adalah sebuah sistem yang digunakan untuk mendeteksi adanya serangan pada sebuah komputer atau *server. Snort* merupakan pilihan yang tepat untuk dipadukan dengan *Honeypot* karena dengan perpaduan ini maka penyerang dapat terjebak oleh *room* palsu buatan *honeypot* serta data dari penyerang akan dapat langsung terbaca oleh *Snort.* Dari hasil sistem *honeypot* dan snort ini memberikan informasi bahwa penyerang berhasil melakukan login ke dalam port ftp/21 menggunakan usernama dan *password* dari serangan *hydra.* Alamat *ip address* dan waktu serangan yang dilakukan penyerang juga tercatat pada sistem *honeypot* dan *snort.*

KATA PENGANTAR

Alhamdulillahirabbil'alamin. Dengan mengucapkan puji syukur kehadirat Allah SWT, yang telah memberi kesehatan, kesempatan, serta taufiq dan hidayah, sehingga penulis dapat menyusun skripsi ini. Shalawat serta salam yang tercurahkan kepada baginda Nabi besar Muhammad S.A.W yang merupakan sosok yang amat mulia yang menjadi panutan setiap muslim serta telah membuat perubahan yang besar di dunia ini. Berkat rahmat dan hidayah yang Allah berikan sehingga penulis dapat menyelesaikan skripsi ini yang berjudul: "PENERAPAN KEAMANA JARINGAN MENGGUNAKAN SISTEM *SNORT* DAN *HONEYPOT* SEBAGAI PENDETEKSI DAN PENCEGAH *MALWARE"*.

Pada kesempatan ini, penulis mengucapkan terimakasih yang sebesar-besarnya kepada :

1. Yang teristimewa dan yang tercinta sosok lelaki cinta pertama dan panutan penulis Ayahanda Adnan. Beliau memang tidak sempat menyelesaikan pendidikan di bangku perkuliahan karena beberapa faktor dan halangan, namun beliau mampu mendidik penulis, memberikan motivasi dan semangat tiada henti hingga penulis dapat menyelesaikan studi hingga sarjana.
2. Pintu Syurgaku, Ibunda tercinta Dra. Akbari penulis ucapkan beribu terima kasih telah mengasuh, mendidik, membimbing, membina, memberikan semangat serta doa-doa tulus yang diberikan selama ini. Terimakasih atas motovasi dan nasihat yang diberikan selama ini walaupun terkadang pikiran kita tidak sejalan. Terimakasih atas

kebesaran hati dan kesabaran menghadapi sikap kekanak-kanakan penulis. Ibu adalah sosok yang menjadi penguat dan pengingat paling hebat. Terimakasih sudah menjadi tempat pulang bu.

3. Bapak Prof Dr. H. Mujiburrahman M.Ag. Selaku Rektor Universitas Islam Negeri (UIN) Ar-Raniry.
4. Bapak Safrul Muluk, MA., M.Ed., Ph.D. Selaku Dekan Fakultas Tarbiyah dan Keguruan Universitas Islam Negeri (UIN) Ar-Raniry
5. Ibu Mira Maisura, M.Sc selaku Ketua Prodi Studi Pendidikan Teknologi Informasi atas kesempatan dan bantuan yang diberikan kepada penulis dalam melakukan penelitian dan memperoleh informasi yang diperlukan selama penulisan skripsi ini.
6. Ibu Mira Maisura, M.Sc sebagai Dosen Pembimbing I yang telah memberikan arahan dan semangat dalam penyusunan skripsi ini.
7. Bapak Aulia Syarif Aziz,S.kom,M.Sc. sebagai Dosen Pembimbing II yang telah memberikan arahan dan semangat dalam penyusunan skripsi ini.
8. Bapak//Ibu Dosen program studi Pendidikan Teknologi Informasi yang telah mendidik dan memberikan bimbingan selama masa perkuliahan.
9. Kakak Yulianti tercinta yang turut juga mendoakan penulis untuk menyelesaikan skripsi ini dan kepada seluruh keluarga yang telah memberikan semangat dan dukungan kepada penulis sehingga penulis dapat menyelesaikan skripsi ini.

10. Sahabat dan teman-teman Mahasiswa Prodi Pendidikan Teknologi Informasi seangkatan tahun 2019 yang saling bekerja sama dan saling membantu, memberi masukan untuk penulis.

11. *Last but not least, I wanna thank me, I wanna thank me for believing in me, I wanna thank me for doing al this hard work, I wanna thank me for having no days off, I wanna thank me for never quitting*. Perempuan sederhana namun terkadang sulit dimengerti isi kepalanya, diri saya sendiri, Zakia Fuada. Seorang perempuan yang berumur 22 tahun saat menyelesaikan karya tulis ini namun terkadang sifatnya seperti anak kecil pada umumnya. Kamu hebat bisa sampai di tahap ini dan tetap berdiri menghadapi segala lika-liku drama perskripsian ini, walaupun terkadang jenuh, bosan dan sudah buntu ingin berhenti namun kamu tetap bertahan dan tetap menyelesaikannya.

Pada fase perskripsian ini, kadangkala kita lupa akan arti kebaikan, kebenaran, kesetiaan, persahabatan, ketenangan dan cinta, karena terlalu banyak sandiwara yang menghadiri. Tetapi satu hal yang harus diingat, "*Dunia tidak pernah kekurangan orang-orang baik, hanya saja kita yang terlalu sering bertemu dengan orang jahat.*"

-Dedi Irawan

Meskipun telah berusaha menyelesaikan Skripsi ini sebaik mungkin, penulis menyadari bahwa skripsi ini masih ada kekurangan. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun dari para pembaca guna menyempurnakan segala kekurangan dalam penyusunan

Skripsi ini. Akhir kata, penulis berharap semoga Skripsi ini berguna bagi para pembaca dan pihak-pihak lain yang berkepentingan. Semoga Allah SWT meridhai penulisan ini dan senantiasa memberikan Rahmat dan hidayah-Nya kepada kita semua. Aamiin ya rabbal'alamin.

Banda Aceh, 12 Oktober 2023
Penulis,

Zakia Fuada

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Seiring berkembangnya teknologi informasi khususnya keamanan jaringan komputer dan layanan-layanannya yang mempermudah pekerjaan-pekerjaan manusia sehari-hari, akan tetapi di sisi lain timbul masalah yang sangat serius, yakni faktor keamanannya. Manusia sudah sangat tergantung dengan sistem informasi, akan tetapi statistik insiden keamanan meningkat tajam. Hal ini secara umum terjadi karena kepedulian terhadap keamanan sistem informasi masih sangat kurang. Sistem pelaporan pertahanan terhadap aktivitas gangguan yang ada saat ini umumnya dilakukan secara manual oleh administrator. Hal ini mengakibatkan integritas sistem bergantung pada ketersediaan dan kecepatan administrator [1].

Seorang adiministrator jaringan bertanggung jawab penuh atas segala sesuatu ketersedian dan kerahasiaan informasi. Tidak hanya itu, pemeliharaan perangkat keras maupun perangkat lunak, analisis masalah, pemantauan kinerja jaringan. Sehingga dibutuhkan sebuah sistem security yang bisa membantu kerja sang administrator.

Snort merupakan tool atau aplikasi *open source* dari *Intrusion Detection System* (IDS). *Snort* dirancang untuk beroperasi pada *command line* dan telah diintegrasikan ke beberapa aplikasi pihak ketiga serta mendukung *cross platform*.

Snort menganalisis semua lalu lintas jaringan untuk melakukan sniffing dan mencari beberapa jenis penyusupan maupun serangan dalam sebuah jaringan [2].

Honeypot adalah *system* atau komputer yang sengaja "dikorbankan" untuk menjadi sasaran serangan *hacker*. Sistem dapat memberikan layanan untuk setiap serangan yang ditembus peretas ke dalam server. Metode ini dirancang untuk memungkinkan administrator server yang akan diserang untuk mengetahui teknik infiltrasi yang dilakukan oleh *hacker*, dan diharapkan dapat melindungi server yang sebenarnya. *Honeypo*t dapat didefinisikan sebagai sumber daya sistem informasi yang dapat digunakan untuk mendeteksi kasus penggunaan sumber daya yang tidak sah secara hokum [3].

Malware adalah perangkat lunak yang dirancang untuk menyusup atau merusak sistem *computer*. *Malware* termasuk virus, *worm*, *trojan horse*, sebagian besar *rootkit*, *spyware*, *ransomware*. Ekstraksi data log secara visual dapat menampilkan pola distribusi serangan port scanning, sehingga mencerminkan perilaku penyerang di jaringan. Melalui visualisasi ini, dapat membantu administrator jaringan mengambil tindakan preventif untuk melindungi jaringan yang mereka kelola [4].

Indonesia sendiri menjadi salah satu negara di Asia Pasific dengan jumlah serangan malware tertinggi. Tujuan dari penelitian ini yaitu menggunakan sistem *snort* dan *honeypot* untuk memonitoring terjadinya serangan tehadap *malware* dan *attacker* yang masuk pada jaringan kampus. Dapat digunakan sebagai salah satunya sistem untuk melindungi keamanan jaringan [5].

Penelitian ini menggunakan metode *action research* adalah metode penelitian yang digunakan untuk menguji, mengembangkan. *Diagnosis* pada tahap ini dilaksanakan analisa kebutuhan, analisa permasalahan yang muncul analisa keiginan user dan topologi yang sedang berjalan. *Action Planing* pada tahapan ini dari peneliti memahami masalah dan akan melakukan penerapan konfigurasi *snort* dan *honeypot* menggunakan sistem operasi *linux ubuntu* untuk menyelesaikan masalah keamanan jaringan pada *laboratorium* multifungsi UIN Ar-Raniry. *Intervention* pada tahap ini peneliti melakukan *implementasi snort* dan *honeypot*. [6].

Oleh karena itu, sesuai dengan permasalahan yang telah dikemukakan, maka penulis mencoba membahas suatu masalah dengan judul "**Penerapan Keamanan Jaringan Menggunakan Sistem *Snort* dan *Honeypot* Sebagai Pendeteksi dan Pencegah Malware''.**

1.2 Rumusan Masalah :

Rumusan masalah penelitian adalah sebagai berikut:

1. Bagaimana cara meningkatkan keamanan server menggunakan sistem *snort* dan *honeypot* sebagai pendeteksi dan pencegahan *malwere*?
2. Bagaimana cara mengetahui penyusup dan serangan yang sering terjadi di dalam jaringan internet?

1.3 Tujuan Masalah

Tujuan penelitian adalah sebagai berikut:

1. Untuk mengetahui cara meningkatkan keamanan server dari serangan yang akan terjadi menggunakan *honeypot* dan memperoleh notifikasi serangan yang terjadi dengan menggunakan *snort.*
2. Untuk mengetahui penyusup dan serangan yang sering terjadi di dalam jaringan internet.

1.4 Manfaat Penelitian

Hasil penelitian dapat memberikan manfaat, antara lain:

1. Manfaat Teoritis

   Dapat memberikan informasi bagi peneliti serta menambah wawasan dalam bidang keamanan jaringan menggunakan *snort* dan *honeypot* dan bisa menjadi refrensi untuk membantu para peneliti dan pengembang dalam membuat sisitem keamanan jaringan di masa yang akan datang.

2. Manfaat Praktis

   a. Manfaat bagi peneliti

      Menambah ilmu pengetahuan serta wawasan mengenai keamanan jaringan menggunakan *Intrusion Prevention System* (IPS) dan *Honeypot*, serta mendapatkan pengelaman dan ilmu pengetahuan di dunia kerja selama penelitian, dapat mempersiapkan diri sebelum masuk ke dalam lingkungan dunia kerja dari pengalaman dan ilmu pengetahuan yang di dapat selama penelitian.

   b. Manfaat Bagi Kampus

      Manfaat dari penelitian ini yaitu meningkatkan keamanan jaringan server dengan mengimplementasikan deteksi penyerang server

dengan menggunakan *Snort* dan menerapkan teknik pengalihan serangan/jebakan untuk penyerang dengan *Honeypot*.

1.5 Relevansi Penelitian Terdahulu

Tabel 1.1 Penelitian terkait

No	Judul	Obyek penelitian	Hasil Penelitian
1	Kusnadi. 2018. Analisis Keamanan Jaringan Menggunakan Sistem Snort dan Honeypot Sebagai Pendeteksi dan Pencegah Malware	menggunakan aplikasi snort dan honeypot di install pada computer yang tersambung dengan jaringan kampus Universitas Udayana Sudirman	Penelitian ini menggunakan PC sebagai tempat instalasi sistem dengan operating sistem Ubuntu 16.04, ram 4GB, dan kapasitas harddisk 500GB. Instalasi snort membutuhkan 42,3 MB dengan format file penyimpanan adalah alert.csv, dan pada honeypot membutuhkan 32.7 MB dengan format dionaea.csv. PC yang telah terinstall snort dan honeypot di hubungkan pada server dengan IP 103.29.196.157, yang dimana jaringan akan melewati sistem snort dan honeypot sebelum masuk kedalam server. Terdapat lokal host dengan port yang berbeda, dimana beberapa port dalam lokal host tersebut di buat oleh honeypot bertujuan untuk mengelabui penyerang.
2	Mustofa, M. M., Aribowo, E. 2015 Penerapan network intrusion detection systemmenggunakan snort berbasis database mysql pada	NDLC (Network Development Life Cycle)	Untuk pengujian dilakukan dari sisi attacker dan server snort. Dalam pengujian pertama attacker akan mencoba melakukan manufer tarhadap jaringan dan kemudian di deteksi oleh server snort dan snort

	hotspot kota		akan menampilkan informasi hasil deteksi
3	Usy Azhar, 2013 Analisis network security snort menggunakan metode intrusion detection system (ids) untuk optimasi keamanan jaringan komputer	Intrusion Detection System (IDS)	Sistem yang akan diuji adalah sistem yang sudah dibangun pada komputer server yaitu sistem keamanan Snort. Pada penelitian ini yang akan uji adalah keamanan Snort. Terdapat tiga Skenario pengujian sistem keamanan Snort, yaitu sebagai berikut. Menguji Keamanan Sistem Snort terhadap Serangan DoS metode TCP Flooding. Menguji Keamanan Sistem Snort terhadap Serangan DoS metode UDP Flooding.
4	Abdul Latif, 2018 Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT	PT. Promanufacture Indonesia	Penelitian ini dilakukan dengan menghubungkan beberapa komputer yaitu terdiri dari komputer server,client, dan attacker. Komputer servertelah diinstal softwareSNORT yang berfungsi untuk menangkap paket yang menuju ke komputer server tersebut, Sedangkan komputer attacker telah diinstal software hping3 yang berfungsi untuk melakukan serangan DDOS Attack ke server. Pada jaringan kali ini disambungkan menggunakan switch. Berikut langkah-langkah yang dilakukan pada penelitian ini.
5	Ahmad Fauzan, 2014 Rancang bangun	Dinas Lingkungan Hidup Pemerintah	Sistem yang dibangun dapat mendeteksi adanya

	aplikasi deteksi dan penanganan serangan ddos dan Port Scanning Memanfaatkan snort pada jaringan komputer	Kota Batam	intrusi berupa serangan DDoS yang diakukan oleh Intruder menggunakan PING melalui command prompt dan serangan Port Scanning yang dilakukan menggunakan tools Nmap.Pemanfaatan Snort sebagai pendeteksi intrusi dan Barnyard2 sebagai perekam log Snort ke dalam database sangat membantu administrator dalam melakukan analisa dan membaca jenis serangan yang terjadi.Penggunaan SMS Gateway pada sistem mempermudah administrator dalam mendapatkanperingatan dini server.

1.6 Perbedaan dan pembaruan penelitian ini.

Pembaruan yang membedakan penelitian ini dengan penelitian sebelumnya terletak pada metode yang di gunakan penelitian terdahulu menggunakan metode NDLC *(Network Development Life Cycle*) sedangkan metode yang saya gunakan di penelitian ini menggunakan metode *action research*, dan perbedaan berikutnya terletak di lokasi penelitian. Penelitian sebelumnya di lokasi Universitas Udayana sedangkan penelitian saya di lokasi Kampus UIN Ar- raniry Banda Aceh.

1.7 Sistematika Penulisan

Penyajian penelitian ini dibagi dalam beberapa bab dengan tujuan untuk menunjukkan penyelesaian masalah yang sistematis. Pembagian bab adalah sebagai berikut :

Bab I PENDAHULUAN

Bab ini terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, penelitian relevan dan sistematika penulisan skripsi. Bab ini menjelaskan tentang permasalahan penelitian.

Bab II Landasan Teori

Bab ini berisi teori yang di ambil dari buku-buku panduan dan referensi lain yang terkait dengan penelitian yang dilakukan oleh penulis.

Bab III Metode Penelitian

Dalam bab ini penulis mengemukakan tentang metode penelitian yang dilakukan oleh penulis dalam keamanan jaringan menggunakan snort dan honeypot. Agar sistematis, bab metode penilitian meliputi :

A. Metode Penelitian
B. Tempat dan Waktu Penelitian
C. Teknik Pengumpulan data
D. Metode Pengembangan system

Bab IV Hasil dan Pembahasan

Bab ini terdiri dari gambaran hasil penelitian dan analisa. Baik dari secara kuantitatif dan statistik, serta pembahasan hasil penelitian. Agar tersusun dengan baik diklasifikasikan ke dalam :

A. Hasil Penelitian

B. Pembahasan

Bab V Penutup

Bab ini berisi kesimpulan yang didapat selama pembuatan laporan tugas akhir serta saran-saran yang akan menjadi masukan bagi penulis serta bisa berguna bagi orang yang membaca.

BAB II
LANDASAN TEORI

2.1 Jaringan Komputer

2.1.1 Pengertian Jaringan Komputer

Jaringan komputer adalah suatu sistem yang terdiri dari komputer-komputer yang dirancang untuk berbagi sumber daya (printer, prosesor), berkomunikasi (email,pesan instan) dan mengakses data (browser web). Tujuan jaringan sebuah komputer harus dapat mencapai tujuannya di setiap bagian jaringan komputer meminta dan menyediakan layanan. Pihak peminta atau penerima layanan disebut klien (klien) dan menyediakan atau mengirim layanan disebut server(Server). Model ini disebut sistem client-server dan hampir selalu digunakan semua aplikasi jaringan komputer [7].

Tujuan dari jaringan komputer adalah untuk melakukan komunikasi data, sharing data maupun pemakaian sumber daya bersama seperti printer dan 7 media penyimpanan sekunder. Komunikasi data sendiri memiliki tujuan yang lebih khusus, yaitu:

a. Memungkinkan pengiriman data dalam jumlah besar efisien, ekonomis, dan tanpa kesalahan dari suatu tempat ke tempat yang lain.
b. Memungkinkan penggunaan sistem komputer dan peralatan pendukung dari jarak jauh (remote).
c. Memungkinkan penggunaan komputer secara terpusat maupun secara tersebar sehingga mendukung manajemen dalam hal kontrol, baik desentralisasi ataupunsentralisasi.

d. Mempermudah kemungkinan pengelolaan dan pengaturan data yang ada dalam berbagai macam sistem komputer.

e. Mengurangi waktu untuk pengelolaan data.

f. Mempercepat penyebarluasan informasi.

g. Komunikasi data berkaitan dengan pertukaran data diantara dua perangkat yang terhubung secara langsung yang memungkinkan adanya pertukaran data antar kedua pihak.

2.1.2 Jenis Jaringan Komputer

Secara umum jaringan komputer dibagi atas lima jenis, yaitu:

a. Local Area Network (LAN)

Local Area Network (LAN), merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan workstation dalam kantor suatu perusahaan atau pabrik-pabrik untuk memakai bersama sumberdaya (misalnya printer) dan saling bertukarinformasi [8].

b. Metropolitan Area Network (MAN)

Metropolitan Area Network (MAN), pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel [9].

c. Wide Area Network (WAN)

WAN adalah singkatan dari istilah teknologi informasi dalam bahasa Inggris: Wide Area Network merupakan jaringan komputer yang mencakup area yang besar sebagai contoh yaitu jaringan komputer antar wilayah, kota atau bahkan negara, atau dapat didefinisikan juga sebagai jaringan komputer yang membutuhkan router dan saluran komunikasi publik. WAN digunakan untuk menghubungkan jaringan lokal yang satu dengan jaringan lokal yang lain, sehingga pengguna atau komputer di lokasi yang satu dapat berkomunikasi dengan pengguna dan komputer di lokasi yang lain. Wide Area Network (WAN), jangkauannya mencakup daerah geografis yang luas, seringkali mencakup sebuah negara bahkan benua [10].

d. Internet

Sebenarnya terdapat banyak jaringan didunia ini, seringkali menggunakan perangkat keras dan perangkat lunak yang berbeda-beda. Orang yang terhubung ke jaringan sering berharap untuk bisa berkomunikasi dengan orang lain yang terhubung ke jaringan lainnya. Keinginan seperti ini memerlukan hubungan antar jaringan yang seringkali tidak kampatibel dan berbeda. Biasanya untuk melakukan hal ini diperlukan sebuah mesin yang disebut gateway guna melakukan hubungan dan melaksanakan terjemahan yang diperlukan, baik perangkat keras maupun perangkat lunaknya. Kumpulan jaringan yang terinterkoneksi inilah yang disebut dengan internet [11].

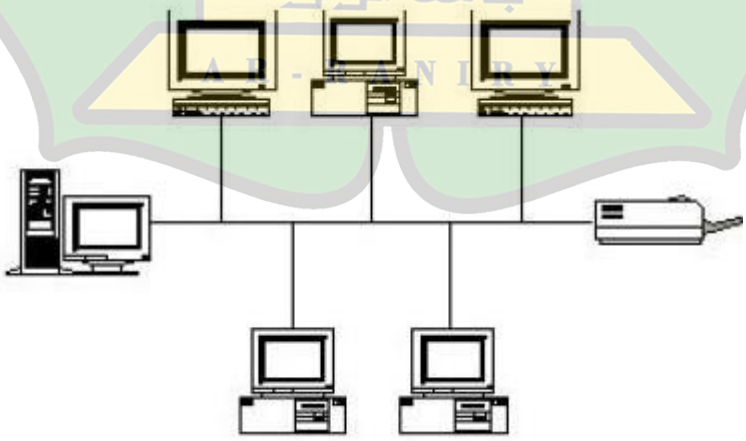
e. Jaringan Tanpa Kabel

Jaringan tanpa kabel merupakan suatu solusi terhadap komunikasi yang tidak bisa dilakukan dengan jaringan yang menggunakan kabel. Misalnya orang yang ingin mendapat informasi atau melakukan komunikasi walaupun sedang berada diatas mobil atau pesawat terbang, maka mutlak jaringan tanpa kabel diperlukan karena koneksi kabel tidaklah mungkin dibuat di dalam mobil atau pesawat. Saat ini jaringan tanpa kabel sudah marak digunakan dengan memanfaatkan jasa satelit dan mampu memberikan kecepatan akses yang lebih cepat dibandingkan dengan jaringan yang menggunakan kabel [12].

2.1.3 Topologi Jaringan Komputer

Topologi jaringan komputer adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Cara yang saat ini banyak digunakan adalah bus, token-ring,star dan peer-to-peer network. Masing-masing topologi ini mempunyai ciri khas, dengan kelebihan dan kekurangannya sendiri [13].

a. Topologi BUS



Gambar 2. 1 ***topologi bus***

Topologi bus terlihat pada skema di atas. Terdapat keuntungan dan kerugian dari tipe ini yaitu:

1) Keuntungan

a) Hemat kabel

b) Layout kabel sederhana

c) Mudah dikembangkan

d) Jarak LAN tidak terbatas.

e) Kecepatan pengiriman tinggi.

f) Tidak diperlukan pengendalian pusat.

2) Kerugian

a) Deteksi dan isolasi kesalahan sangat kecil

b) Kepadatan lalu lintas

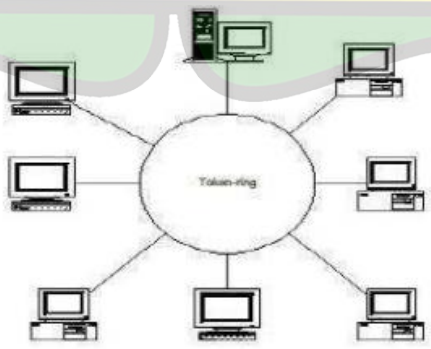
c) Bila salah satu client rusak maka jaringan tidak dapat berfungsi

d) Diperlukan repeater jarak jauh.

e) Jika lalu lintas data terlalu banyak dan tinggi dapat terjadi kemacetan pada pengiriman data.

f) Operasional jaringan LAN bergantung pada setiap terminal.

b. Topologi RING



Gambar 2. 2 Topologi Ring

Topologi RING terlihat pada skema berikut ini. Metode token-ring (sering disebut ring saja) adalah cara menghubungkan komputer sehingga berbentuk ring (lingkaran). Setiap simpul mempunyai tingkatan yang sama. Jaringan akan disebut sebagai loop, data dikirimkan kesetiap simpul dan setiap informasi yang diterima simpul diperiksa alamatnya apakah data itu untuknya atau bukan. Terdapat keuntungan dan kerugian dari tipe ini yaitu:

1) Keuntungan:

a) Hemat kabel

b) Laju data (transfer rate) tinggi.

c) Dapat melayani lalu lintas data yang padat.

d) Tidak diperlukan host,relatif lebih murah.

e) Dapat melayani berbagai media pengiriman.

f) Komunikasi antar terminal mudah.

g) Waktu yang diperlukan untuk mengakses data optimal.

2) Kerugian:

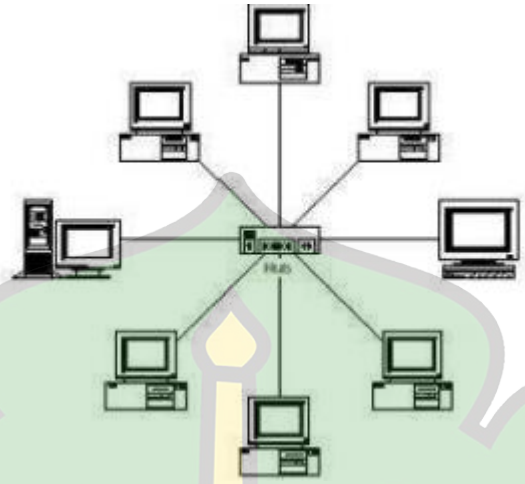
a) Peka pada masalah

b) Pengembangan jaringan lebih kaku

c) Penambahan atau pengurangan terminal sangat sulit.

d) Kerusakan pada media pengiriman dapat menghentikan kerja seluruh jaringan.

c. Topologi STAR



Gambar 2. 3 Topologi Star

Merupakan kontrol terpusat, semua link harus melewati pusat yang menyalurkan data tersebut kesemua simpul atau client yang dipilihnya.Simpul pusat dinamakan stasium primer atau server dan lainnya dinamakan stasiun sekunder atau client server.Setelah hubungan jaringan dimulai oleh server maka setiap client server sewaktu-waktu dapat menggunakan hubungan jaringan tersebut tanpa menunggu perintah dari server. Terdapat keuntungan dan kerugian dari tipe ini yaitu:

1) Keuntungan:

a) Paling fleksibel

b) Pemasangan/perubahan stasiun sangat mudah dan tidak mengganggu bagian jaringan lain

c) Kontrol terpusat

d) Kemudahan deteksi dan isolasi kesalahan/kerusakan

e) Kemudahaan pengelolaan jaringan

2) Kerugian:

a) Boros kabel

b) Perlu penanganan khusus

c) Kontrol terpusat (HUB) jadi elemen kritis

2.2 Perangkat keras Jaringan Komputer

Perangkat jaringan merupakan alat atau piranti yang digunakan untuk membangun suatu sistem jaringan. Masing-masing perangkat jaringan memiliki fungsi dan tujuan tersendiri didalam suatu sistem jaringan. Pemilihan perangkat-perangkat jaringan yang diperlukan dapat disesuaikan dengan kebutuhan sistem jaringan yang akan dibangun. Meskipun terdapat aneka ragam jenis jaringan komputer yang berbeda, tapi tetap memiliki perangkat keras yang umum seperti kabel atau perangkat WiFi, ethernet card, hub atau switch, repeater, bridege dan lain-lain.

1) Router

Router sering digunakan untuk menghubungkan beberapa network. Baik network yang sama maupun yang berbeda dari segi teknologinya. Seperti menghubungkan network yang menggunakan topologi Bus, Star, dan Ring. Router juga digunakan untuk membagi network besar menjadi beberapa buah subnetwork (network-network kecil). Setiap subnetwork seolah-olah terisolir dari network lain. Hal ini dapat membagi-bagi traffic yang akan berdampak positif pada performa network. Sebuah router memiliki kemampuan routing. Artinya router secara langsung dapat mengetahui kemana rute perjalanan informasi (yang

disebut packet) akan dilewatkan. Apakah ditujukan untuk host lain dalam satu network ataukah berbeda network. Jika paket-paket ditujukan untuk host pada network yang sama maka router akan menghalangi paket-paket keluar, sehingga paket-paket tersebut tidak membanjiri network yang lain [14].

2) Router OS

RouterOS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer manjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan wireless, cocok digunakan oleh ISP dan provider hotspot.

3) Routerboard

Router embedded produk dari mikrotik. Routerboard seperti sebuah komputer mini yang terintegrasi karena dalam satu board tertanam prosesor, ram, rom, dan memori flash. Routerboard menggunakan os RouterOS yang berfungsi sebagai router jaringan, bandwidth management, proxy server, dhcp, dns server dan bisa juga berfungsi sebagai hotspot server. Mikrotik pada standar perangkat keras berbasiskan Personal Computer (PC) dikenal dengan kestabilan, kualitas kontrol dan fleksibilitas untuk berbagai jenis paket data dan penanganan proses rute atau lebih dikenal dengan istilah routing. Mikrotik yang dibuat sebagai router berbasiskan PC banyak bermanfaat untuk sebuah ISP yang ingin menjalankan beberapa aplikasi mulai dari hal yang paling ringan hingga tingkat lanjut. Contoh aplikasi yang dapat diterapkan dengan adanya Mikrotik selain routing adalah aplikasi kapasitas akses (bandwidth) manajemen, firewall, wireless access point

(WiFi), backhaul link, sistem hotspot, Virtual Private Network (VPN)server dan masih banyak lainnya [15].

a. Bridge

Bridge atau kadangkala disebut transparent bridge merupakan perangkat network yang digunakan untuk menghubungkan dua buah LAN atau membagi sebuah LAN menjadi dua buah segmen. Tujuannya adalah 10 untuk mengurangi traffic sedemikian rupa sehingga dapat meningkatkan performa network.

b. Repeater

Repeater termasuk satu dari perangkat keras jaringan komputer yang dipasang di titik-titik tertentu dalam jaringan untuk memperbaharui sinyal yang ditransmisikan agar mencapai kembali kekuatan dan bentuknya semula guna memperpanjang jarak tempuh. Repeater berfungsi untuk menguatkan sinyal.

1) Network Interface Card

Kartu Jaringan (NIC) merupakan salah satu dari perangkat keras yang menyediakan media untuk menghubungkan antar komputer. Kebanyakan kartu jaringan adalah kartu internal, yaitu kartu jaringan yang di pasang pada slot ekspansi di dalam komputer. Kartu jaringan yang banyak terpakai saat ini adalah: kartu jaringan Ethernet, LocalTalk konektor, dan kartu jaringan Token Ring.

c. Kabel

Setiap jenis kabel mempunyai kemampuan dan spesifikasinya yang berbeda, oleh karena itu dibuatlah pengenalan tipe kabel. Ada beberapa jenis kabel yang dikenal secara umum,yaitu twisted pair (UTP / unshielded twisted pairdanSTP/shieldedtwisted pair), coaxial cable dan fiber optic. Berikut akan dijelaskan beberapa macam kabel yang serring digunakan dalam jaringan.

2.3 Perangkat Lunak Jaringan Komputer

1. *Snort*

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 (Snort team 2009). Suatu sistem IDS harus bersifat lintas platform, mempunyai sistem footprinting yang ringan, dan mudah dikonfigurasi oleh administrator sebuah sistem yang membutuhkan implementasi dari solusi kemananan dalam waktu yang singkat [16].

Implementasi tersebut dapat berupa seperangkat software yang dapat diasosiasikan dalam melakukan aksi untuk merespon sistuasi keamanan tertentu. Selain itu. sebuah sistem IDS juga harus powerfull dan cukup fleksibel untuk digunakan sebagai bagian permanen dari suatu sistem jaringan. Snort memenuhi kriteria tersebut, yaitu dapat dikonfigurasi dan dibiarkan berjalan untuk periode

yang lama tanpa meminta pengawasan atau perawatan bersifat administratif sebagai bagian dari sistem keamanan terpadu sebuah infrastruktur jaringan. Snort iuga dapat berjalan pada semua platform sistem operasi di mana libpcap dapat berjalan.

2 Honeypot

Honeypot adalah server atau sistem jaringan yang dipasang sebagai umpan untuk memikat hacker saat akan melakukan upaya penyerangan atau peretasan. Honeypot dirancang agar terlihat seperti target yang menarik dan diletakan di sekitar server asli. Sehingga dapat mengelabui hacker dan menyerang target yang salah. Selain dapat mengecoh target serangan peretas, honeypot juga dapat membantumu memprediksi serangan sajak awal dan memberikan respons yang diperlukan. Setelah serangan tersebut masuk ke dalam perangkap honeypot, kamu dapat mengumpulkan informasi penting tentang jenis serangan hingga metode yang digunakan. Dengan begitu, ketika serangan tersebut datang kembali, kamu dapat mengantisipasinya. Meskipun hanya bersifat tiruan, honeypot juga memerlukan file maupun pengoperasian yang mirip dengan server asli. Hal ini karena honeypot yang diciptakan semirip mungkin dengan server asli akan memberikan performa yang maksimal [17].

a. Cara Kerja *Honeypot*

Honeypot dibuat semirip mungkin dengan sistem komputer pada umumnya, lengkap dengan aplikasi maupun data yang dapat menarik perhatian hacker. Seperti misalnya honeypot yang meniru sistem keuangan perusahaan dan lain sebagainya. Untuk memancing perhatian peretas, honeypot sengaja dibuat

dengan tingkat keamanan yang rendah. Salah satunya dengan penggunaan port yang rentan terhadap pemindaian port. Kemudian port yang lemah tersebut dibiarkan terbuka agar hacker terpancing untuk menyerangnya [18].

Perlu dipahami jika honeypot bukanlah bentuk *cyber security* yang dapat mencegah serangan hacker secara langsung. Tujuan diciptakannya honeypot adalah untuk membantu menyempurnakan *Intrusion Detection System* (IDS)–*software* yang dapat mendeteksi jaringan keamanan–agar dapat mengatasi serangan dengan lebih baik lagi. Ada dua tahap utama dalam honeypot: ***production*** dan ***research***. Pada tahap produksi, honeypot fokus sebagai server yang menyamar dan mengelabui peretas. Sedangkan pada tahap penelitian, honeypot akan melakukan penelitian terhadap serangan yang berhasil masuk ke dalam honeypot.

b. Kelebihan dan Kekurangan *Honeypot*

Honeypot datang dengan beberapa kelebihan dan kekurangan yang bisa jadi bahan pertimbangan sebelum memasangnya pada jaringan komputer.

1. Kelebihan *Honeypot*

a. Mengumpulkan data secara aktual dari serangan yang sebelumnya masuk ke dalam perangkap *honeypot;*
b. Mendeteksi serangan dengan cukup akurat**,** karena honeypot bukanlah sistem jaringan yang dapat dengan mudah diakses pengguna umum. Hanya hacker dengan niat menyerang yang akan mengaksesnya;

c. Biaya yang lebih hemat, karena honeypot dapat menjadi investasi jangka panjang dalam mencegah serangan dan tidak memerlukan banyak sumber daya;

d. Menangkap aktivitas berbahaya, bahkan jika penyerang menggunakan enkripsi.

2. Kekurangan *Honeypot*

a. Data yang terbatas, karena honeypot hanya mengumpulkan data saat terjadi serangan;

b. Jaringan yang terisolasi, sehingga terkadang hacker dapat mencurigainya sebagai *honeypot*;

c. Dapat menempatkan server asli dalam risiko, meskipun honeypot adalah jaringan yang terisolasi, namun secara tidak langsung sistem jaringan tersebut terhubung dengan server asli. Sehingga ketika honeypot diserang, server asli tetap perlu diamankan.

3. **Jenis *Malware***

a. Virus

Menurut Septiani, (2016), Virus merupakan program komputer yang bersifat mengganggu dan merugikan pengguna komputer. Virus adalah Malware pertama yang dikenalkan sebagai program yang memiliki kemampuan untuk mengganggu kinerja sistem komputer. Hingga saat ini biasanya masyarakat lebih populer dengan kata virus komputer dibandingkan dengan istilah Malware sendiri. Biasanya virus berbentuk file eksekusi exe (executable) yang baru akan beraktivitas bila user

mengaktifkannya. Setelah diaktifkan virus akan menyerang file yang juga bertipe executable (.exe) atau juga tipe file lainnya sesuai dengan perintah yang dituliskan pembuatnya [19].

b. Worm

Menurut Septiani, (2016), Worm yang berarti cacing merupakan Malware yang cukup berbahaya. Worm mampu untuk menyebar melalui jaringan komputer tanpa harus tereksekusi sebelumnya. Setelah masuk ke dalam sistem komputer, Worm memiliki kemampuan untuk mereplikasi diri sehingga mampu memperbanyak jumlahnya di dalam sistem komputer. Hal yang diakibatkan dari aktivitas Worm adalah merusak data dan memenuhi memory dengan Worm lainnya hasil dari penggandaan diri yang dilakukannya. Replikasi ini membuat memory akan menjadi penuh dan dapat menngakibatkan aktivitas komputer menjadi macet (hang). Kebiasaan komputer menjadi hang dapat menjadi gejala awal terdapatnya Worm pada komputer tersebut. Contoh Worm yang populer akhir-akhir ini adalah Conficker [20].

c. Trojan Horse

Menurut Septiani, (2016), Teknik Malware ini terinspirasi dari kisah peperangan kerajaan Yunani kuno yang juga diangkat ke Hollywood dalam film berjudul ‘Troy’. Modus dari Trojan Horse ini adalah menumpangi file biasa yang bila sudah dieksekusi akan menjalankan aktivitas lain yang merugikan sekalipun tidak menghilangkan fungsi utama file yang ditumpanginya. Trojan Horse merupakan Malware 29 berbahaya, lebih dari

sekedar keberadaannya tidak diketahui oleh pengguna komputer. Trojan dapat melakukan aktivitas tak terbatas bila sudah masuk ke dalam sistem komputer. Kegiatan yang biasa dilakukan adalah merusak sistem dan file, mencuri data, melihat aktivitas user (spyware), mengetahui apa saja yang diketikkan oleh user termasuk password (keylogger) bahkan menguasai sepenuhnya komputer yang telah terinfeksi Trojan Horse [21].

d. Spyware

Menurut Septiani, (2016), Spyware merupakan Malware yang dirancang khusus untuk mengumpulkan segala informasi dari komputer yang telah dijangkitinya. Kegiatan Spyware jelas sangat merugikan user karena segala aktivitasnya yang mungkin menyangkut privasi telah diketahui oleh orang lain tanpa mendapat izin sebelumnya. Aktivitas Spyware terasa sangat berbahaya karena rentan terhadap pencurian password. Dari kegiatan ini juga akhirnya lahir istilah Adware yang merupakan iklan yang mampu muncul secara tiba-tiba di komputer korban hasil dari mempelajari aktivitas korban dalam kegiatan berkomputer. Spam yang muncul secara tak terduga di komputer juga merupakan salah satu dampak aktivitas Spyware yang dirasa sangat menjengkelkan [22].

4. Virtual Box

Virtualbox adalah perangkat lunak virtualisasi untuk menginstal sistem operasi “Operating System”. Kata virtuallilsasi yaitu mengubah atau mengkonversi sesuatu menjadi bentuk simulasi dari bentuk real atau nyata. Misalnya, jika seseorang telah menginstal sistem operasi Windows di komputer

mereka, orang ini juga dapat menjalankan sistem operasi lain yang diinginkan dalam sistem operasi Windows. Bagi Anda yang ingin mencoba berlatih menginstal sistem operasi, Anda tidak perlu menginstal ulang PC / laptop Anda. Anda hanya memerlukan perangkat lunak Virtualbox ini untuk mencoba atau belajar menginstal sistem operasi. Jadi Anda bisa menginstal Linux di dalam Windows secara mudah hanya dengan menggunakan aplikasi VirtualBox ini.

5. Iso Kali Linux

Kali Linux adalah sebuah sistem operasi (OS) open-source yang digunakan untuk tujuan hacking dan pengujian penetrasi pada jaringan komputer. Kali Linux pertama kali dirilis pada tahun 2013 oleh Offensive Security dan merupakan turunan dari Debian Linux. OS ini dikembangkan khusus untuk keperluan keamanan jaringan dan telah menjadi standar industri untuk pengujian penetrasi dan forensik digital. Kali Linux dilengkapi dengan berbagai alat hacking dan pentesting, seperti nmap, metasploit, aircrack-ng, dan banyak lagi. OS ini memiliki fokus pada keamanan dan privasi, serta dapat digunakan sebagai sistem operasi utama atau sebagai OS live pada USB atau CD.

6. Iso Ubuntu Server

Ubuntu Server adalah salah satu distribusi Linux yang dikembangkan oleh Canonical Ltd, perusahaan di belakang Ubuntu. Ubuntu Server ditujukan untuk digunakan sebagai sistem operasi server dan dapat digunakan untuk berbagai tujuan seperti server web, aplikasi, database, virtualisasi, dan banyaklagi.

BAB III
METODOLOGI PENELITIAN

3.1 Metode Penelitian

Metode Penelitian yang akan digunakan untuk penelitian pada Laboratarium Multifungsi menggunakan metode *action research* sebagai berikut :

action research adalah metode penelitian yang digunakan untuk menguji, mengembangkan.

1. *Diagnosis*. Pada tahap ini dilaksanakan analisa kebutuhan, analisa permasalahan yang muncul analisa keinginan *user* dan analisa topologi yang sedang berjalan. Untuk dapat melakukan proses analisa sebelumnya dilakukan proses pengumpulan data yang berupa wawancara dengan Kepala Lab agar mendapatkan gambaran sebenarnya dari lokasi penelitian untuk mempermudah proses perancangan sistem keamanan jaringan.
2. *Action Planing*. Pada tahapan ini dari peneliti memahami masalah dan akan melakukan penerapan konfigurasi *snort* dan *honeypot* menggunakan sistem operasi linux ubuntu untuk menyelesaikan masalah keamanan jaringan pada Laboratarium Multifungsi. Pada tahap ini penulis melakukan persiapan kebutuhan perangkat keras (*hardware*) dan perangkat lunak (*software)* yang diperlukan dan akan melakukan uji coba serangan dengan system yang telah di terapkan.
3. *Intervention*. Pada tahapan peneliti melakukan implementasi *snort* dan *honeypot* menggunakan sistem operasi linux ubuntu sebagai sistem

keamanan jaringan pada Laboratarium Multifungsi setelah itu dilakukan uji coba dari sistem yang dibangun.

4. *Reflection*. Tahap terakhir yang dilakukan penulis yaitu dengan melakukan review dan evaluasi dari tahap-tahap yang telah dilakukan sebelumnya. [23].

3.2 Tempat dan Waktu Penelitian

3.2.1 Tempat penelitian

Penelitian ini dilakukan di Laboratorium Multifungsi UIN Ar-Raniry Jl. Lingkar Kampus, Rukoh, Kec. Syiah Kuala, Kota Banda Aceh.

3.2.2 Waktu Penelitian

Waktu penelitian dilakukan kurang lebih memerlukan 1-5 bulan yaitu pada bulan Februari 2023 – juni 2023. Dimana dalam waktu lima bulan penelitian melakukan observasi lapangan dan wawancara kepada kepala Lab dan staf operator untuk melakukan analisis data dan sampai penyusunan laporan dari hasil penelitian.

3.3 Teknik Pengumpulan Data

Untuk memperoleh data yang diperlukan sebagai landasan penelitian maka peneliti melakukan pengumpulan data menggunakan 3 metode, yaitu :

3.3.1 Penelitian Pustaka (Library Research) : Penelitian ini dilakukan pengumpulan data dengan studi pustaka yakni mencari referensi-referensi di perpustakaan,toko buku, dan internet. Referensi tersebut berupa buku, jurnal, dan peneliti sejenis, yang membahas Keamanan jaringan menggunakan Snort dan Honeypot. Untuk mencari data, mengumpulkan data dan mempelajari data dari buku-buku serta literatur-literatur yang berhubungan dengan permasalahan yang dibahas dalam penelitian.

3.3.2 Studi *Literatur* : Merupakan sumber data sekunder dalam penelitian. Studi literatur dilakukan dengan pengumpulan teori-teori yang berkaitan dengan penelitian riset sebagai bahan untuk melengkapi penelitian. Sumber teori berasal dari buku referensi, hasil penelitian (jurnal dan skripsi), dan artikel terkait.

3.3.3 *Observasi* (Pengamatan)

Menurut Risanty (2017:2), Observasi yaitu teknik pengumpulan data dengan cara mengamati langsung operasi maupun prosedur yang berlaku pada objek penelitian. Dalam penelitian ini penulis melakukan observasi dilingkungan Leb Multifungsi, untuk mengamati dan mencatat serangan apa saja yang ada pada komputer.

3.3.4 Interview (Wawancara)

Menurut Moh Nazir (2014:170), Wawancara adalah proses memperoleh keterangan untuk tujuan penelitian dengan cara tanya jawab, sambil bertatap muka antara si penanya atau pewawancara dengan si penjawab atau responden dengan menggunakan alat yang dinamakan interview guide (panduan wawancara).

3.4 Metode Pengembangan Sistem

Metode pengembangan sistem yang akan digunakan penulis untuk penelitian pada Laboratarium Multifungsi menggunakan metode *action research* sebagai berikut :

5. *Diagnosis*. Pada tahap ini dilaksanakan analisa kebutuhan, analisa permasalahan yang muncul analisa keinginan *user* dan analisa topologi yang sedang berjalan. Untuk dapat melakukan proses analisa sebelumnya dilakukan proses pengumpulan data yang berupa wawancara dengan Kepala Lab agar mendapatkan gambaran sebenarnya dari lokasi penelitian untuk mempermudah proses perancangan sistem keamanan jaringan.
6. *Action Planing*. Pada tahapan ini dari peneliti memahami masalah dan akan melakukan penerapan konfigurasi *snort* dan *honeypot* menggunakan sistem operasi linux ubuntu untuk menyelesaikan masalah keamanan jaringan pada Laboratarium Multifungsi. Pada tahap ini penulis melakukan persiapan kebutuhan perangkat keras *(hardware*) dan perangkat lunak (*software)* yang diperlukan dan akan melakukan uji coba serangan dengan system yang telah di terapkan.

7. *Intervention.* Pada tahapan peneliti melakukan *implementasi snort* dan honeypot menggunakan sistem operasi *linux ubuntu* sebagai sistem keamanan jaringan pada Laboratarium Multifungsi setelah itu dilakukan uji coba dari sistem yang dibangun.
8. *Reflection.* Tahap terakhir yang dilakukan penulis yaitu dengan melakukan review dan evaluasi dari tahap-tahap yang telah dilakukan sebelumnya.

3.5 Alat Dan Bahan Penelitian yang Digunakan

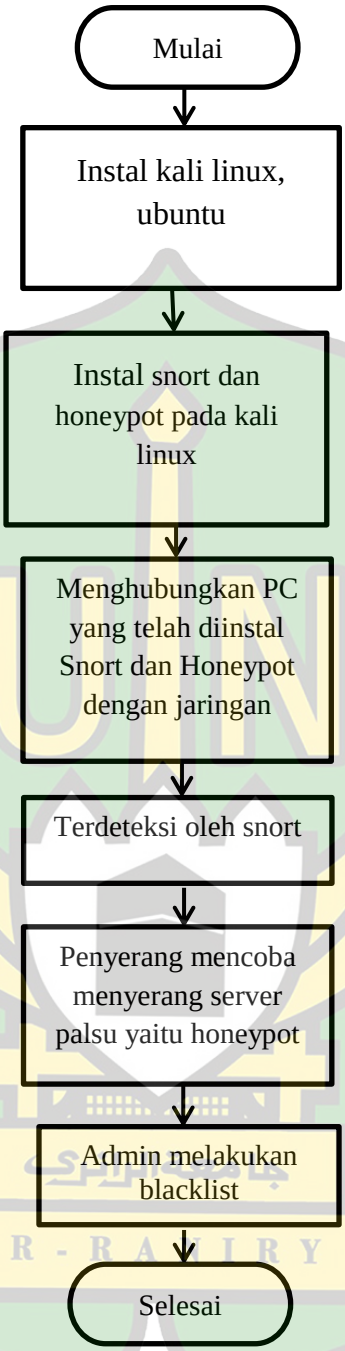
Adapun alat dan bahan yang digunakan pada penelitian ini sebagai berikut.

3.5.1 Perangkat Lunak (*Software)*

a. Snort versi 6. 1. 0-kali9-amd64
b. Honeypot
c. Kali Linux 6. 1. 0-kali9-amd64
d. Virtualbox

3.5.2 Perangkat Keras (*Hardware*)

a. Lebtob Lenovo



Gambar 2.5 : Flowchart Implementasi *Snort* dan *Honeypot*

No	Bentuk Kegiatan	MINGGU PELAKSANAAN																													
		Feb 2023				Mar 2023				Apr 2023				Mei 2023				Jun 2023				Jul 2023				Agu 2023				Sept 2023				Okt 2023			
1	Pengajuan dan Pengesahan Judul																														
2	Observasi																														
3	Penyusunan BAB I dan Revisi																														
4	Penyusunan BAB II dan revisi																														
5	Penyusunan BAB III dan revisi																														
6	Seminar proposal dan Revisi																														
7	Penelitian																														
8	Sidang dan Revisi																														

BAB IV
HASIL DAN PEMBAHASAN

4.1 Hasil Penelitian

4.1.2 Persiapan *Software*

a. Instalasi *Snort*

Snort adalah sebuah softwere atau aplikasi atau juga sebuah too *security* yang berfungsi mendeteksi intruksi-intruksi jaringan, mendeteksi penyusupan yang memasuki jaringan. Snort merupakan sistem pencegahan dan deteksi intrusi jaringan bersifat *open source* dengan berbasis aturan *(rule-driven*) yang digunakan untuk memantau lalu lintas jaringan secara pasif dan memberikan peringatan saat ada ancaman terdeteksi. Snort memiliki kemampuan yang sangat fleksibel dan dapat dikonfigurasi sesuai kebutuhan. Ia juga mendukung integrasi dengan alat-alat keamanan lainnya dan dapat berkolaborasi dengan sistem manajemen keamanan (*security management systems*) yang lebih luas.

Langkah-langkah yang harus dilakukan untuk penginstalan Snort adalah sebagai berikut:

1. Persiapkan Sistem:
    a. Pastikan sistem operasi yang digunakan mendukung Snort. Snort dapat diinstal pada berbagai sistem operasi seperti kali linux versi 6. 1. 0-kali9-amd64
    b. Pastikan juga bahwa sistem terhubung ke internet, karena akan membutuhkan paket-paket yang akan diunduh saat menginstal Snort. Ubuntu versi 18

2. Unduh Snort:

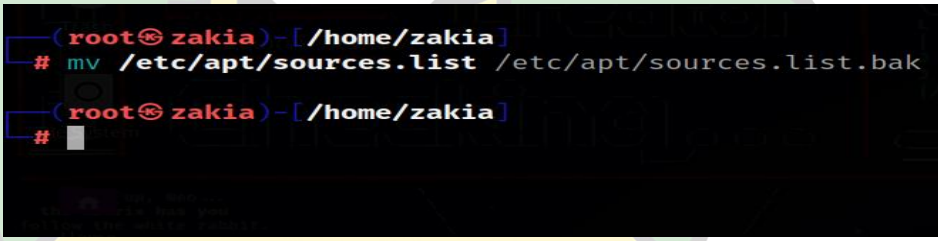
   a. Kunjungi situs resmi Snort di https://www.snort.org/downloads.

   b. Pada penlitian ini sistem Snort yang digunakan adalah versi 2.9.7.0.

   c. Sebelum melakukan installasi sistem snort ada beberapa perintah yang harus dijalankan untuk meng-*install packet-packet* pendukung sistem snort, sebelum melakukan installasi paket juga perlu mempersiapkan beberapa alat bantu lainnya. Berikut perintah untuk melakukan installasi sistem snort:

      1) Back*up sources.list*

         Pada langkah awal perlu dilakukan *backup* dari sources.list sistem kali linux yang digunakan, untuk melakukan backup sources.list harus menggunakan super user agar dapat mengakses file sources.list, setelah masuk ke super user gunakan perintah ***"mv /etc/apt/sources.list /etc/apt/sources.list.bak.***



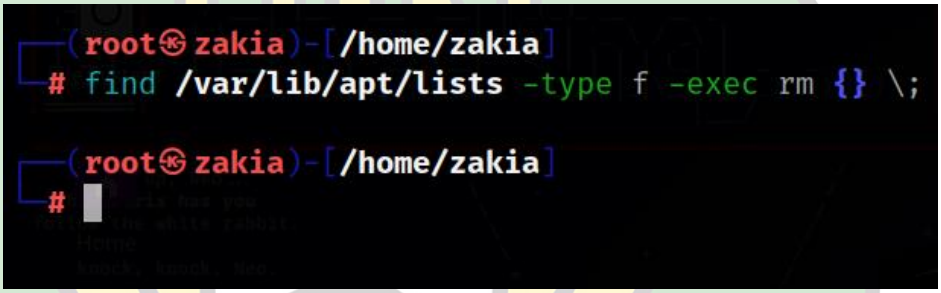
Gambar 4.1 *backup sources.list*

Fungsi backup *sources.list* adalah untuk mencadangkan berkas "sources.list" yang berisi konfigurasi sumber paket perangkat lunak pada sistem linux. Dengan mengganti namanya menjadi *"sources.list.bak",* dengan begitu dapat dengan aman mengedit atau mengganti berkas *"sources.list*" asli tampa kehilangan konfigurasi

yang ada, dan jika terjadi masalah, kita dapat dengan mudah mengembalikan berkas aslinya dari salinan cadangan ini.

2) *Remove update*

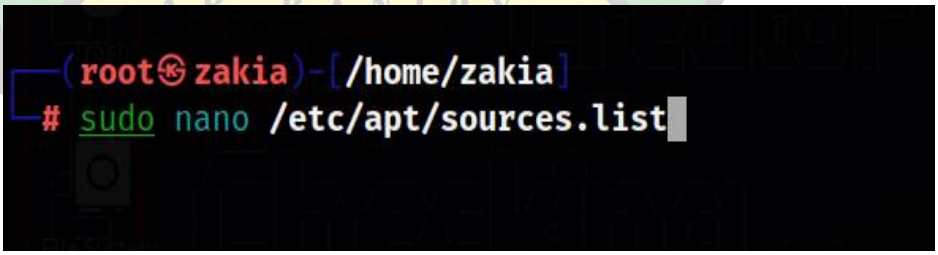
Selanjutnya perintah ini akan mencari semua file di dalam direktori /var/lib/apt/lists dan subdirektori-subdirektorinya, lalu menghapusnya satu per satu. Ini dapat digunakan untuk membersihkan file-file yang sudah tidak diperlukan dalam sistem, misalnya file-file cache dari manajer paket apt pada distribusi linux berbasis debian.



Gambar 4.2 *Remove update*

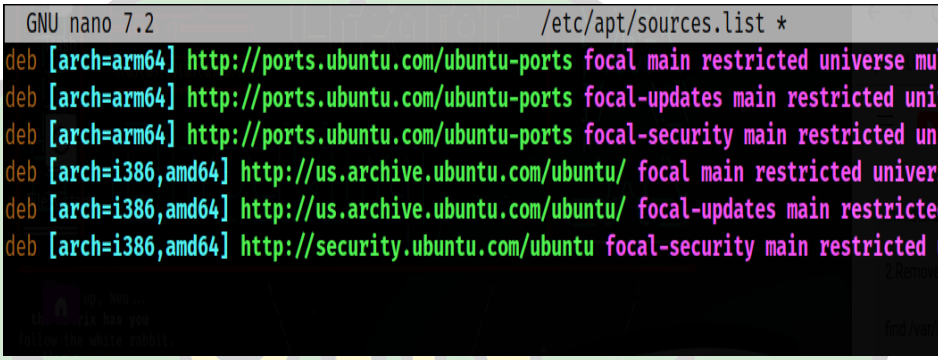
3) *Change sources.list*

Pada tahap ini dilakukan perubahan data dalam *file* sources list, untuk mengubah data dalam file sources.list menggunakan perintah **"sudo nano /etc/apt/sources.list"** seperti perintah pada Gambar 4.3.



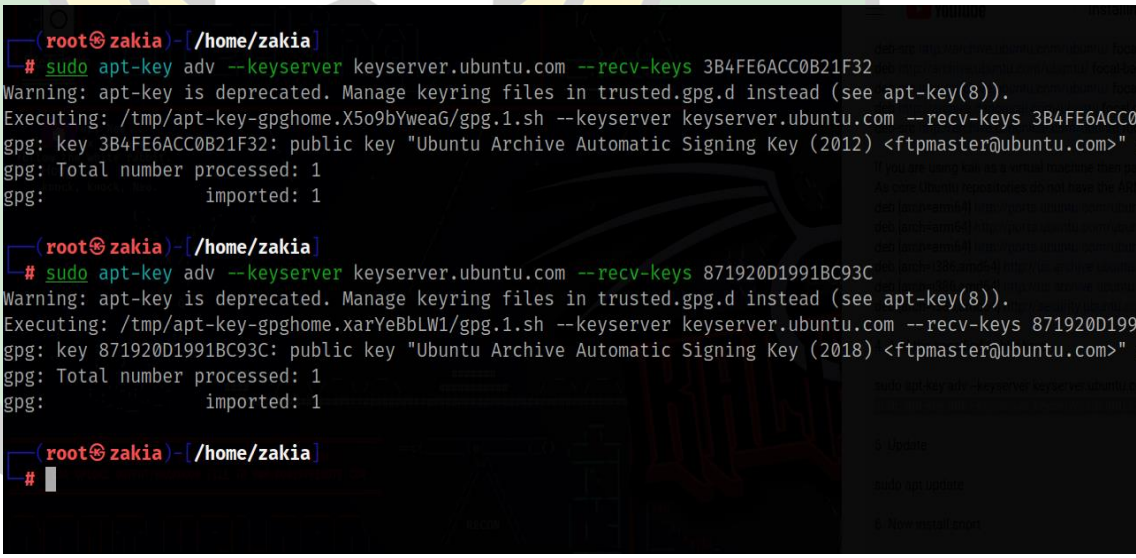
Gambar 4.3 masuk ke dalam *file sources.list*

Setelah menjalankan perintah ini, sistem akan masuk ke dalam file sources.list, setelah masuk ke dalam file sources.list selanjutnya memasukkan beberapa daftar *repository* yang dibutuhkan sistem untuk melakukan installasi, daftar *repository* digunakan pada penelitian ini dapat dilihat pada Gambar 4.4 di bawah ini.



Gambar 4.4 *daftar list Sources.list setelah diubah*

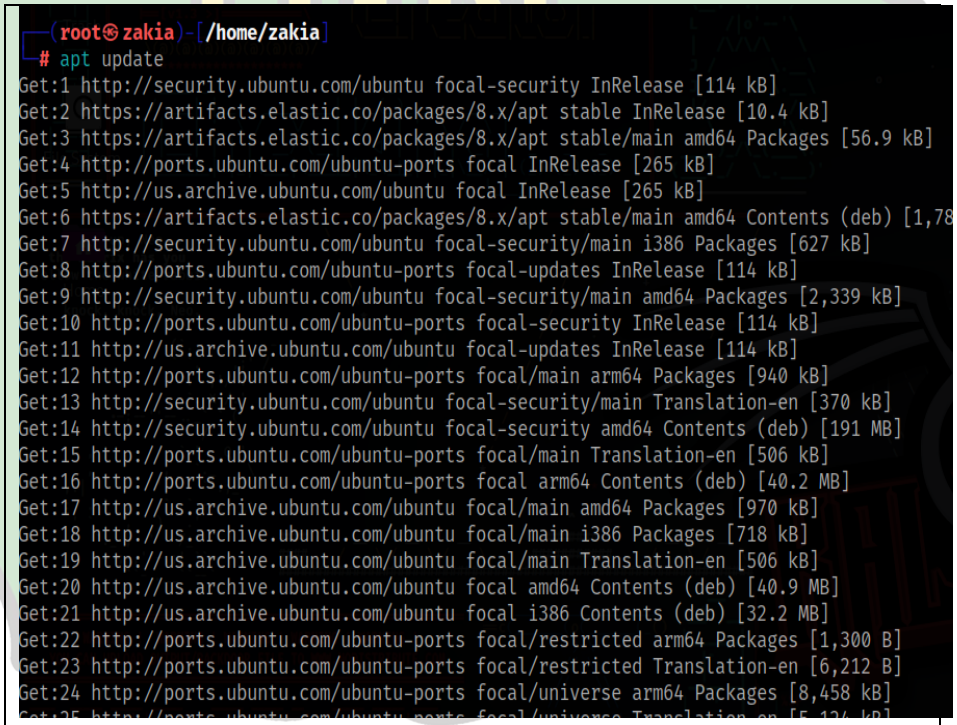
4) Menambahkan spesifik *public key*



Gambar 4.5 perintah menambahkan *public key*

5) Melakukan Update Sistem

Sebelum melakukan installasi sistem snort dibutuhkan untuk melakukan update pada sistem kali linux yang digunkan, karena pada perintah sebelumnya telah dilakukan pembaharuan pada sources.list terdahulu, dengan ini perlu dilakukan update packet dalam sistem kali linux untuk menunjang installasi packet-packet yang dibutuhkan selanjutnya seperti installasi snort. Untuk melakukan update sistem kali linux ini dengan menggunakan perintah **"apt update** atau **sudo apt update"**, perintah yang dijalankan dapat dilihat pada Gambar 4.6.

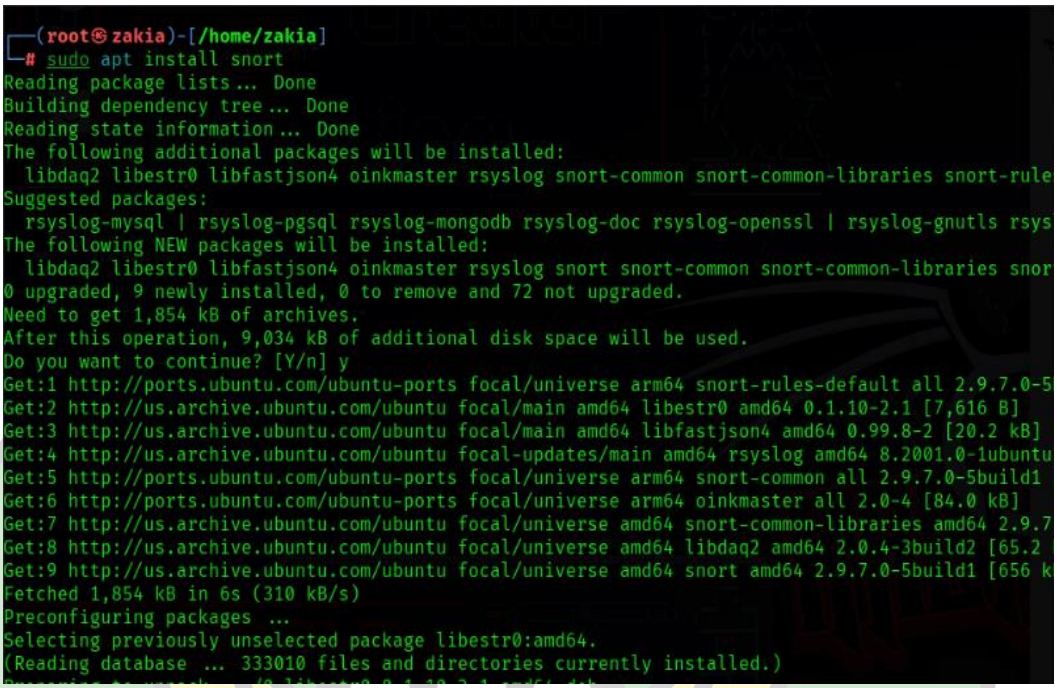


Gambar 4.6 *Update* sistem

6) Installasi *Snort*

langkah selanjutnya adalah melakukan installasi snort pada sistem kali linux, snort yang digunakan pada sistem ini ada snort versi 2.9.7.0. perintah untuk melakukan installasi snort dengan memasukkan

perintah “apt install snort/ sudo apt install snort” perintah dapat dilihat pada gambar 4.7.

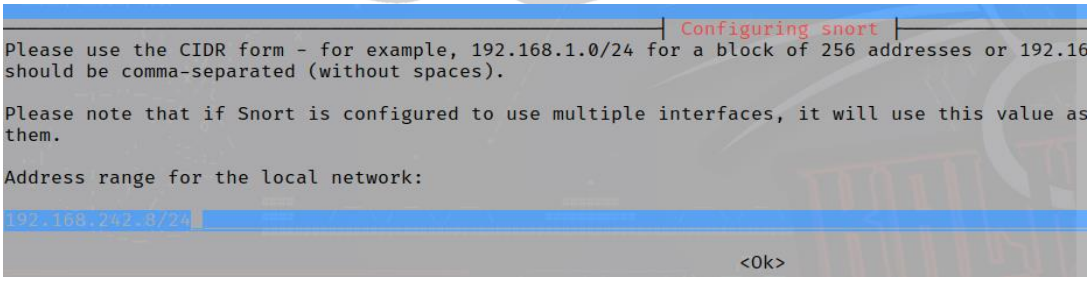


Gambar 4.7 *installasi snort*

Dalam pemerosesan installasi pada sistem snort akan meminta untuk memasukkan alamat ip address untuk dipakai pada sistem snort yang dijalankan, gambar input ip address untuk sistem snort terdapat pada gambar 4.8 di bawah ini.

7) Konfigurasi Snort:

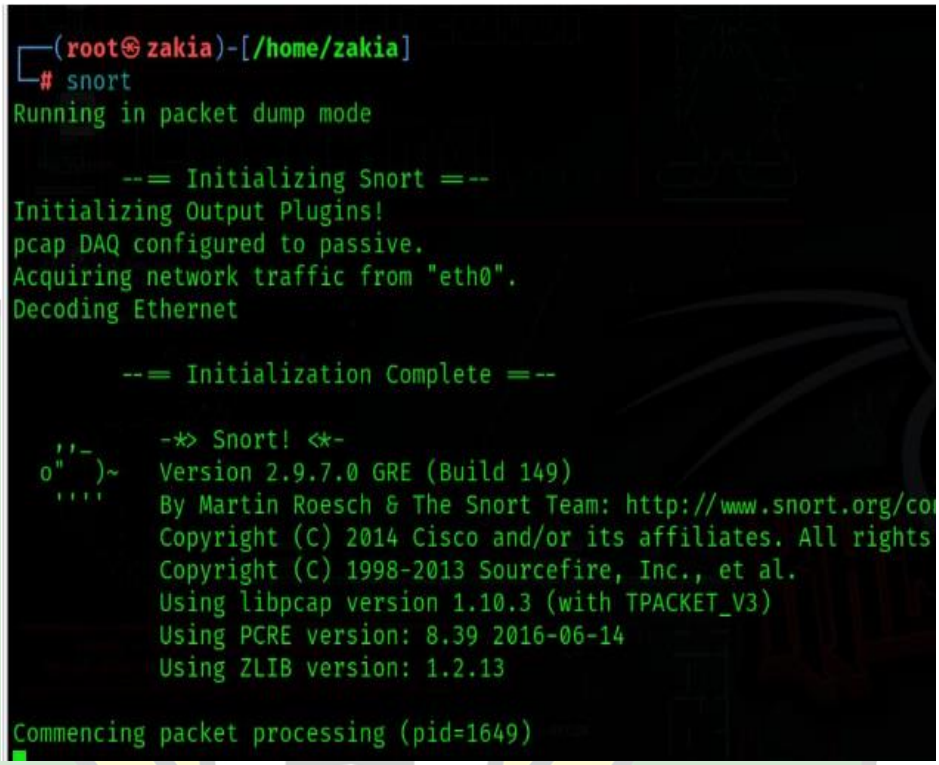
Setelah menginstal Snort, perlu melakukan konfigurasi Ip 192.168.242.0/24 .



Gambar 4.8 *alamat ip address snort*

8) Menjalankan *Snort*

Perintah menjalankan snort dapat dilihat pada Gambar 4.9 dibawah ini.



Gambar 4.9 Menjalankan *Snort*

setelah snort berhasil di install pada sistem kali linux, selanjutnya snort akan dijalankan sebagai Intrution Detection *System* (*IDS*) untuk memperoleh informasi yang terjadi pada sistem *honeypot* secara *realtime*. Perintah untuk mejankan snort dengan memasukan perintah "snort" pada terminal kali linux, dengan begitu sistem snort secara otomatis akan akti

b. Instalasi *Honeypot*

1. Persiapkan Sistem:

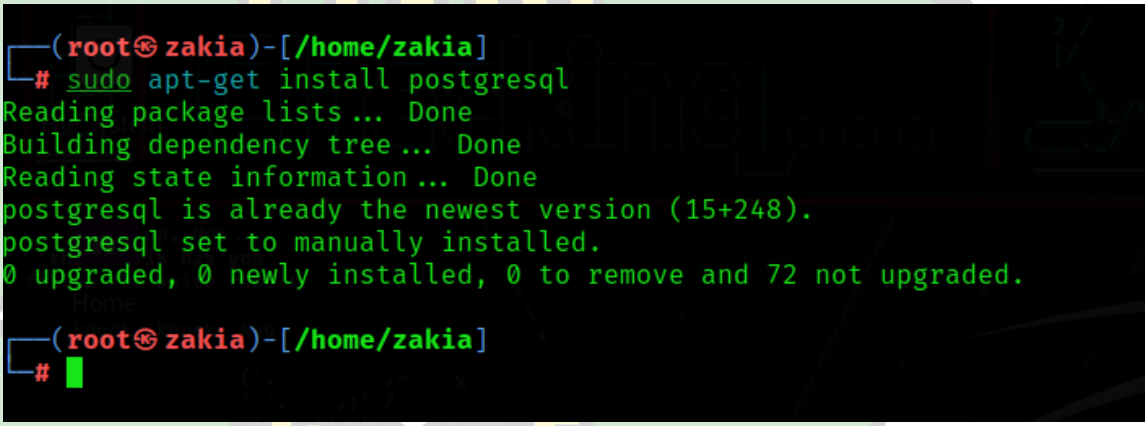
Pastikan sistem operasi dan platform yang di pilih telah terinstal dan dikonfigurasi dengan benar. Pastikan juga sistem terhubung ke internet, karena honeypot membutuhkan koneksi untuk menarik serangan.

2. Unduh dan Instal Honeypot Software:

Sebelum melakukan proses installasi *honeypot* perlu dipersiapkan terlebih dahulu paket pendukung agar pada saat melakukan installasi tidak terjadi *error* karena adanya paket yang dibutuhkan oleh honeypot tidak terinstall.

a. Install postgresql

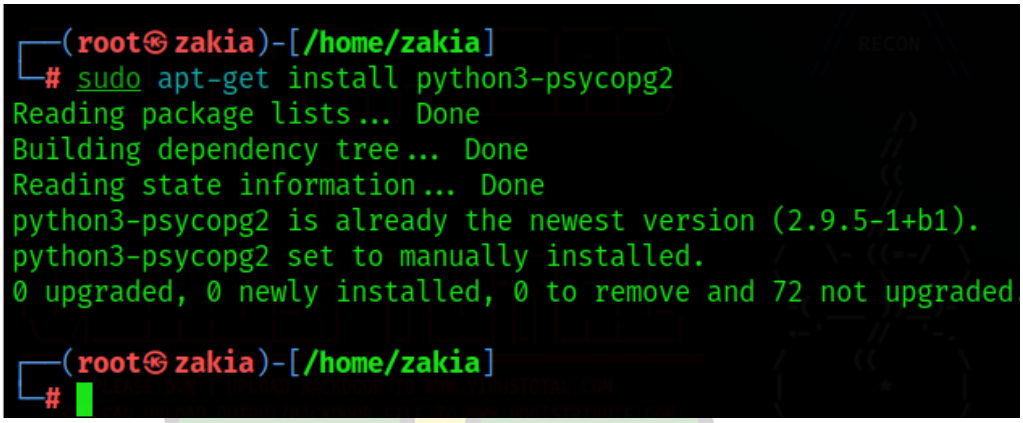
Dalam proses installasi honeypot diperlukan tool postgresql, tool ini adalah salah satu paket dalam proses installasi honeypot, perintah untuk melakukan installasi tool ini dengan perintah **"sudo apt-get install postgresql"** proses installasi dapat diliat pada Gambar 4.9 dibawah ini.



Gambar 4.9 installasi postgresql

b. *Install python3-psycopg2*

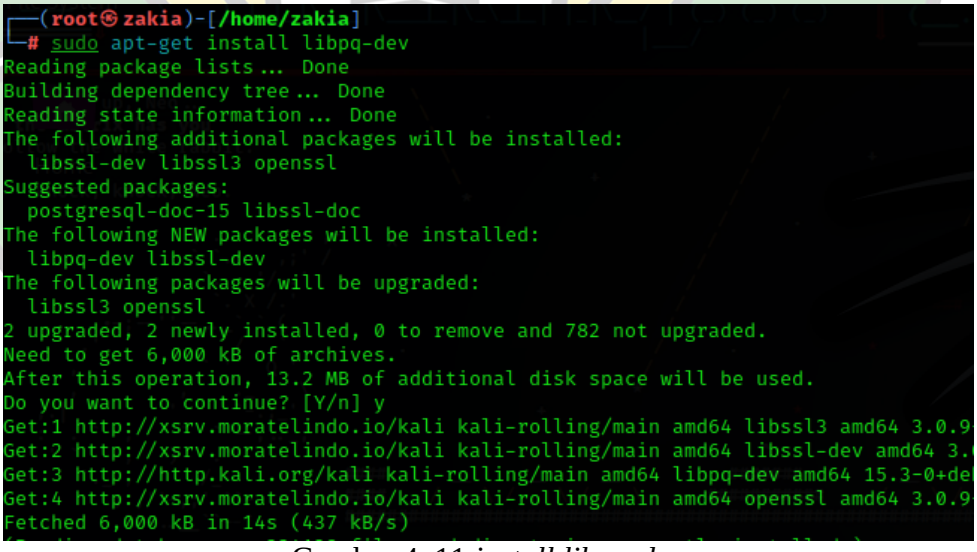
Pada proses berikutnya dilakukann installasi tool *python3-psycopg2* yang berguna untuk mengakses *query SQL* di *postgreSQL* perlu diperhatikan bahwa installasi *psycopg2* membutuhkan python versi 3.9, sebelumnya melakukan installasi *psycopg2* terlebih dahulu melakukan installasi *python3* dengan perintah **"sudo apt-install python3"**, untuk installasi psycopg2 menggunakan perintah **"sudo apt-get install python3-psycopg2"** perintah installasi dapat dilihat pada gambar 4.10 dibawah ini.



Gambar 10 *installation python3-psycopg2*

c. Installasi libpq-dev

Tahapan selanjutnya adalah melakukan installasi *libpq-dev* tool ingin berguna menyalurkan query ke server backend postgreSQL dan menerima hasil query tersebut. Untuk melakukan installasinya menggunakan perintah **"sudo apt-get install libpq-dev"** perintah tersebut dapat dilihat pada Gambar 4.11 di bawah ini.

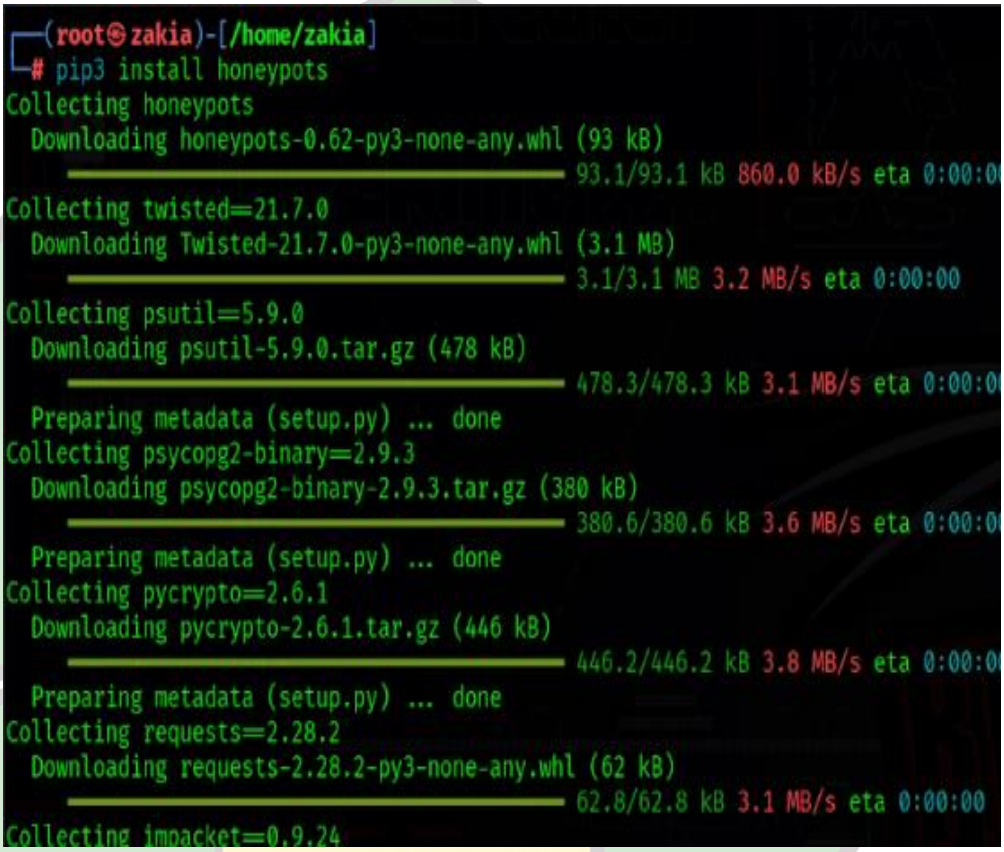


Gambar 4. 11 *install libpq-dev*

d. Installasi honeypot

Setalah selesai melakukan installasi tool sebelumnya, selanjutkan melakukan installasi tool utama yaitu honeypot, sebelum melakukan

installasi *honeypot* perlu dilakukan installasi pip3 dengan perintah **"apt-get install python3-pip"**. Setelah selasai install *pip* selanjutnya install honeypot dengan perintah **"pip3 install honeypot"**, perintah dapat dilihat pada Gambar 4.12 dibawah ini.



Gambar 4.12 *install honeypot*

e. Konfigurasi Honeypot

Pada tahapan selanjutnya sebelum menjalankan tool honeypot, dilakukan konfigurasi pada sistem hoenypot seperti membuat service dari mesin honeypot, memasukan IP Address honeypot, memasukkan username serta password, untuk mengelabui hacker supaya sistme honeypot terlihat seperti mesin asli. Dalam sistem honeypot ini dipersiapkan beberapa service

seperti: FTP,SSH,TELNET,HTTP,HTTPS, dan POP3, konfigurasi honeypot dapat dilihat pada Gambar 4.13 dibawah ini.

Gambar 4.13 Konfigurasi sistem *honeypot*

4.2 Pembahasan

4.2.1 Rancangan Pengujian

Pengujian dilakukan untuk mengetahui seberapa suskes sistem dapat mendeteksi beberapa serangan yang dilakukan. Pada penelitian ini simulasi pengujian penyerangan dilakukan menggunakan *Snort* dan *Honeypot* selesai diimplementasikan. Berikut dibawah ini adalah skema gambaran alur skenario sistem pengujian.

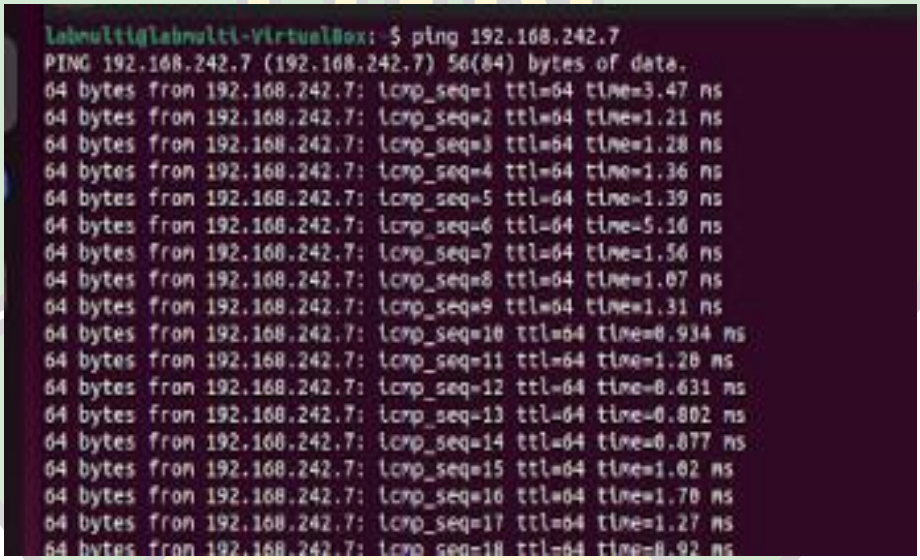
Gambar 4.12 *Flowchart* Sistem Pengujian

4.2.2 Data Uji coba

Skenario Fase *Operate* (Operasional) pengujian untuk Tugas Akhir "Simulasi Sistem Keamanan Jaringan Komputer Berbasis Snort dan Honeypot" adalah sebagai berikut:

a. Uji coba jaringan

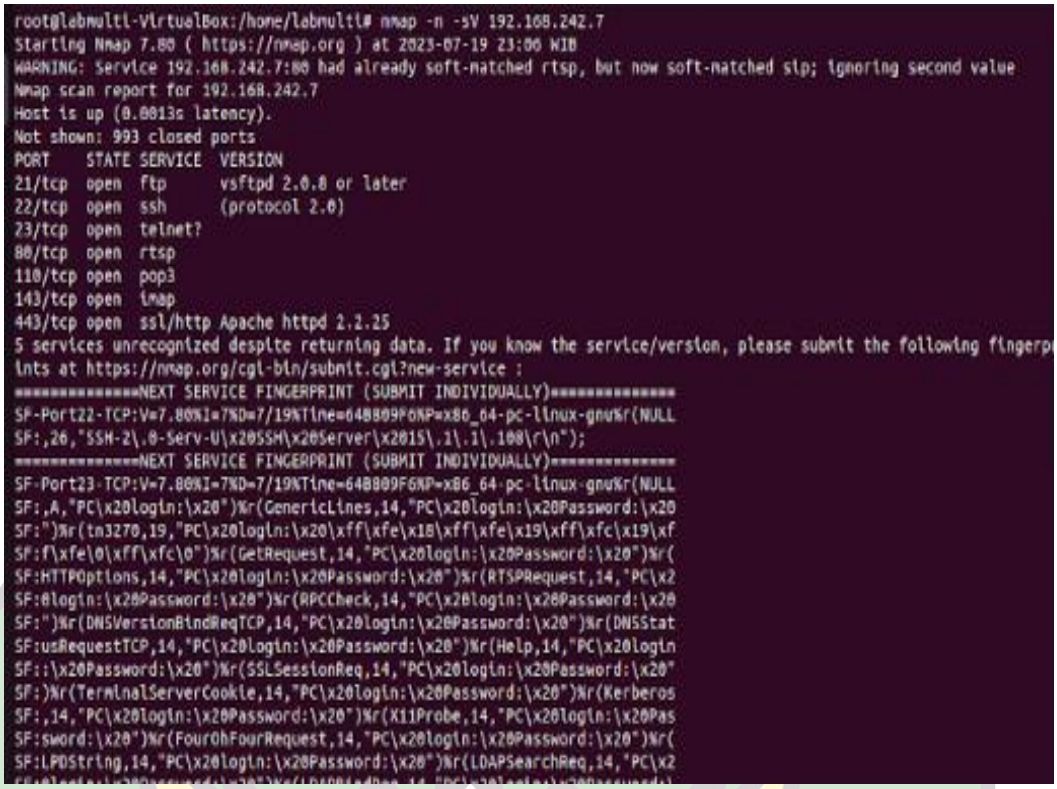
Dalam proses uji coba ini, tahapan pertama melakukan uji coba jaringan dari honeypot apakah sistem honeypot telah terkoneksi dengan perangkat penyerang dengan melakuka ping pada perangkat penyerang, hasil ping dapat lihat pada Gambar 4.14 dibawah ini.



Gambar 4.14 hasil ping sistem honeypot

b. Port Scanning

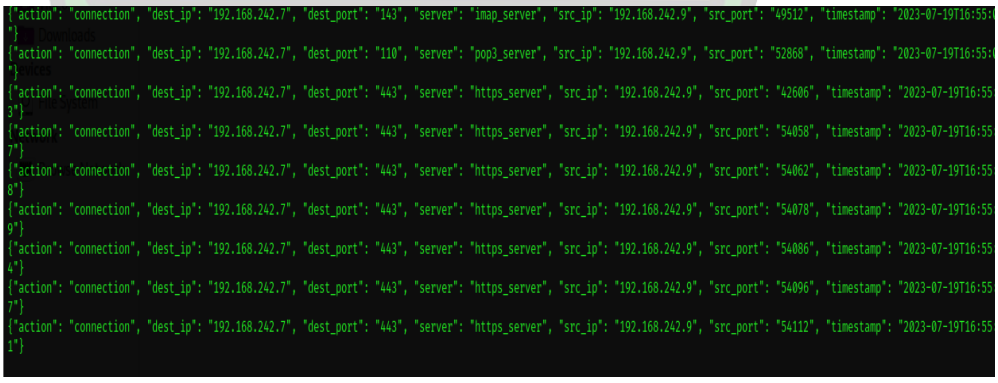
Pada tahapan ini akan dilakukan post scanning yang berguna untuk melihat port-port yang tersedia pada sistem honeypot yang telah dikonfigurasikan sebelumnya dengan menggunakan tool NMAP. Hasil post scanning dapat dilihat pada Gambar 4.15 dibawah ini.



Gambar4. 15 *hasil post scanning*

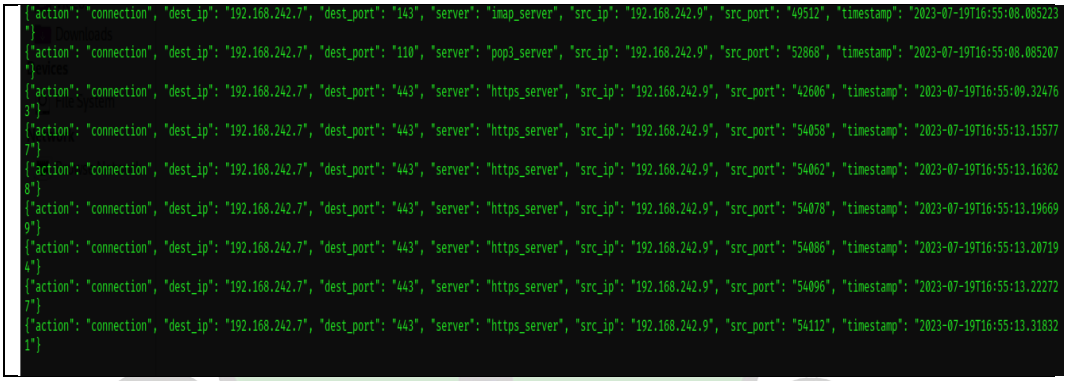
Dengan melakukan port scanning dengan tool nmap ini, diperoleh beberapa port yang terbuka pada sistem honeypot, dan juga memberikan informasi lainnya seperti versi dari port yang digunakan, jenis service, dan status dari port tersbut. Berikut ini adalah hasil IDS dari sistem honeypot dan juga snort terhadap serangan port scanning yang dilakukan.

1. Hasil dari honeypot



Gambar 4.16 *hasil IDS honeypot*

2. Hasil dari snort

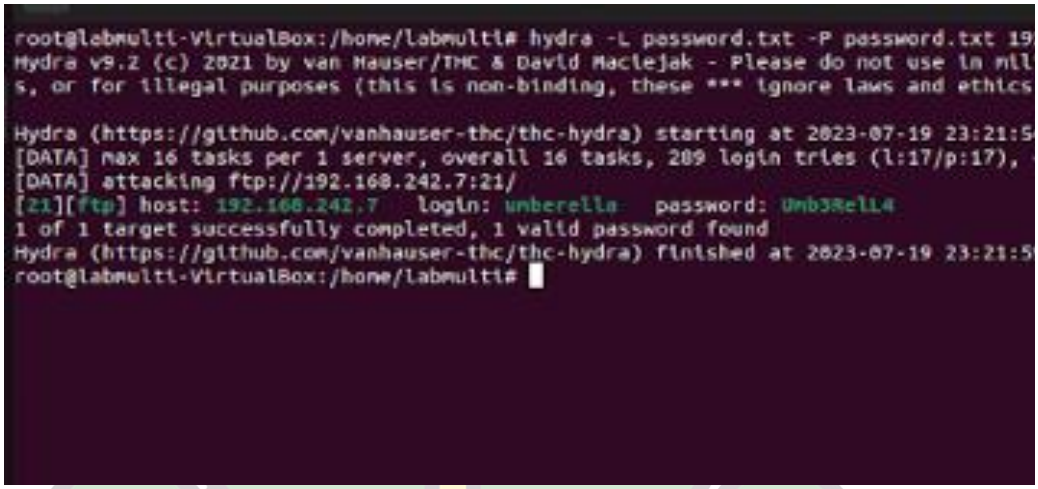


Gambar 4.17 *Hasil IDS snort*

Telihat pada gambar 4.17 IP penyerang yaitu 192.168.242.7 yang tertulis pada baris Source address mencoba melakukan koneksi ke server dengan IP 192.168.10.5 yang tertulis pada baris Dest. Address snort lansung merespon allert tersebut kemudian menampilkan di base snort. Pada proses melakukan port scanning menggunakan tool Nmap ditemukan beberapa port terbuka pada sistem Honeypot, dimana port tersebut telah dikonfigurasi sebelumnya pada sistem honeypot yang bertujuan untuk mengelabui penyerang dan mengira ini adalah sistem yang rentah. Sehingga disaat yang proses proses scanning berjalan, sistem Snort dari Honeypots dan snort mengcapture informasi yang terjadi pada server.

c. Hydra Attack

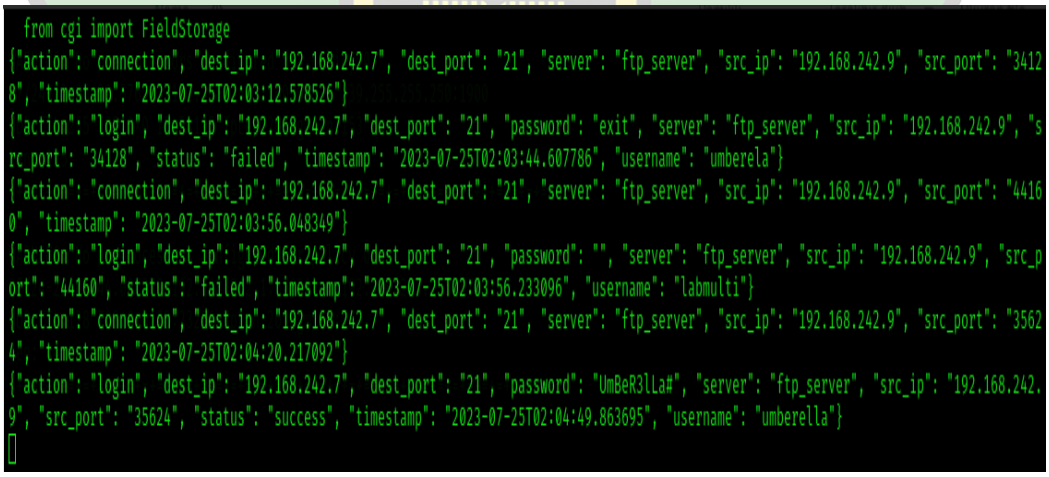
Tahapan serangan selanjutnya dengan melakukan serang hydra attack, hydra attack adalah tool sejenis brute force yang digunakan untuk menemukan username dan password dari sistem honeypot. Hasil serangan hydra attack dapat dilihat pada Gambar 4.18 dibawah in.



Gambar 4.18 *Hydra Attack*

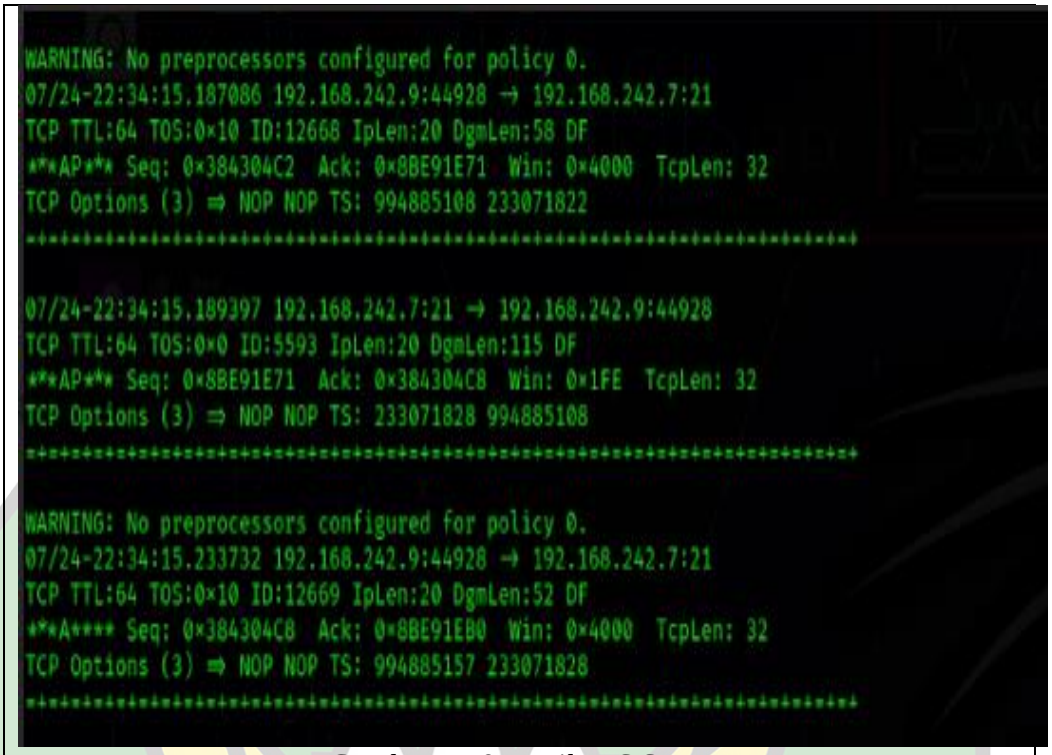
Dengan menggunakan tool hydra ini, perangkat penyerang berhasil menemukan username dan password dari port FTP:21 pada sistem honeypot yang bisa dimanfaatkan untuk melakukan login pada sistem. Tool hydra mendapatkan username “imberella” dan password “Umb3RelL4” pada sistem honeypot, hasil serangan ini terekam pada sistem IDS honeypot dan Snort, hasil IDS yang diperoleh dapat dilihat di bawah ini:

d. Hasil IDS Honeypot



Gambar 4.19 *Hasil IDS Honeypot*

e. Hasil IDS Snort

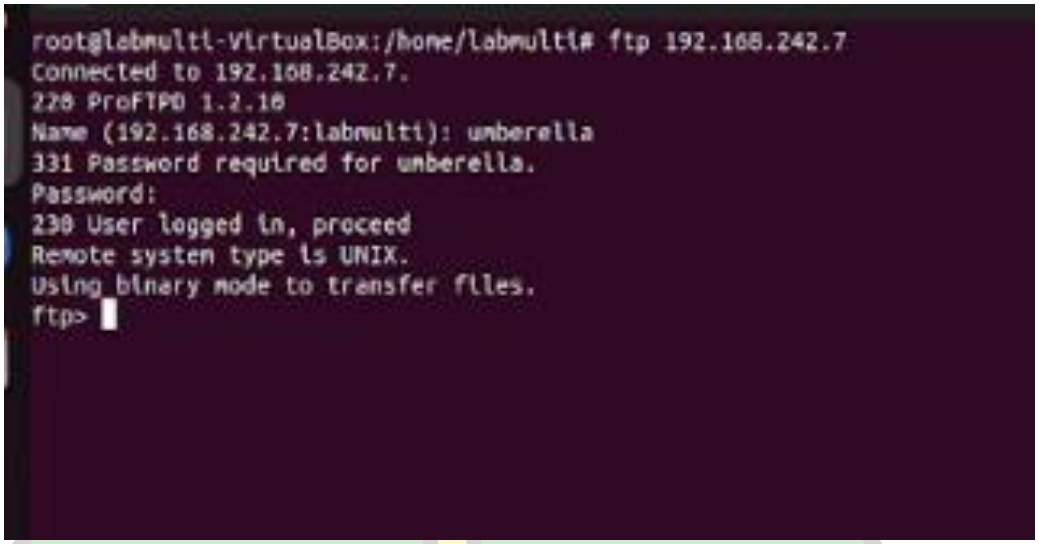


Gambar 4.20 *Hasil IDS Snort*

Dari hasil IDS honeypot dan snort didapatkan informasi dari penyerang berupa alamat IP address yang digunakan penyerang, tanggal dan waktu penyerangan dilakukan, dan juga port yang di tuju oleh penyerang. Dalam IDS ini penyerang melakukan serangan pada port FTP/21, pada Gambar 4.19 terdapat informasi bahwa pernyerang berhasil menemukan username dan password yang terdapat pada sistem honeypot.

f. Akses Port FTP

Pada tahapan ini dilakukan aktifitas login pada ke sistem honeypot pada port ftp/21, hal ini dilakukan untuk memastikan bahwa username dan password yang didapat dari serangan hydra attack adalah benar. Hasil akses login ke port FTP dapat dilihat pada Gambar 4.21 dibawah ini.



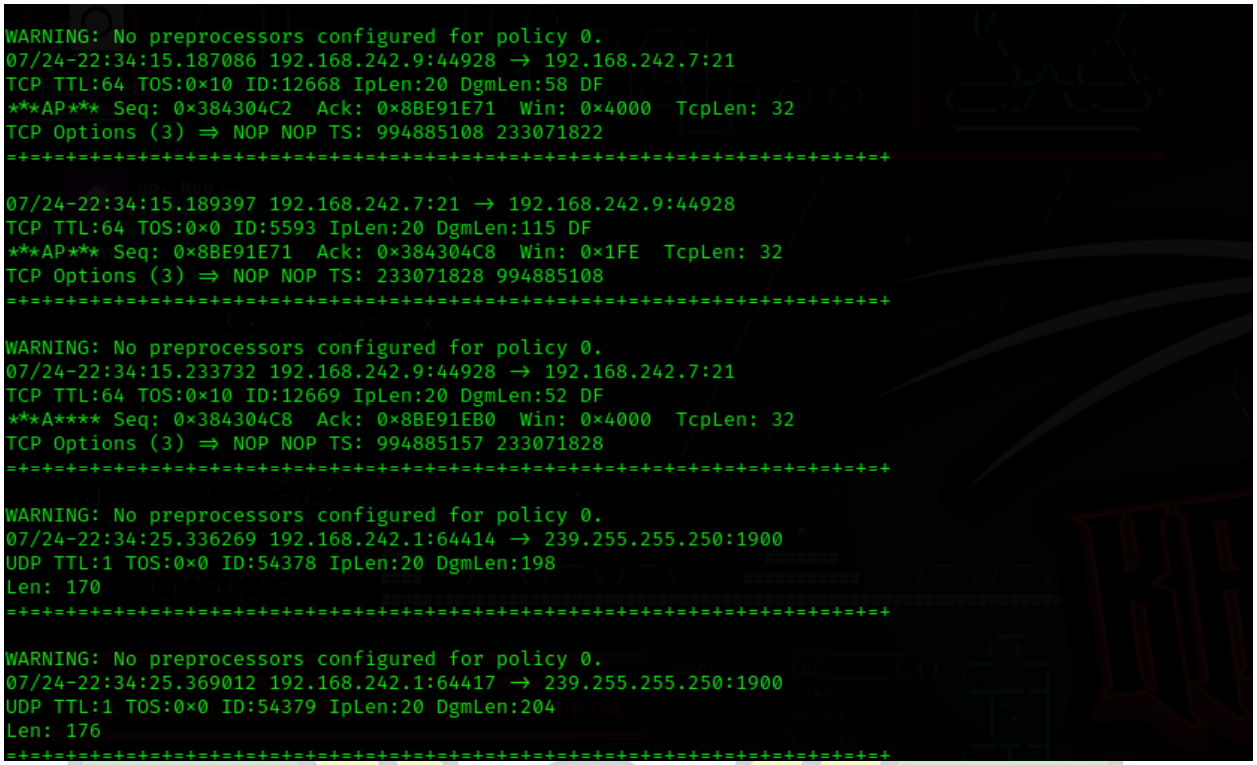
Gambar 4.21 *akses port ftp*

Dari hasil Gambar 4.21 penyerang berhasil melakukan login pada port FTP/21 di sistem honeypot dengan menggunakan username dan password yang telah didapatkan dengan menggunakan tool hydra attack. Namun upaya yang dilakukan penyerang ini tidak berarti apa-apa, karena sistem honeypot ini tidak memiliki file apapun di dalamnya yang bisa dimanfaatkan oleh penyerang. Hasil akses login penyerang ke port FTP/21 ini terengkap oleh sistem IDS honeypot dan snort, hasil IDS dapat dilihat Gambar dibawah ini.

g. Hasil IDS Honeypot

Gambar 4.22 Hasil IDS Honeypot

h. Hasil IDS Snort



Dari hasil IDS sistem honeypot dan snort ini memberikan informasi bahwa penyerang berhasil melakukan login ke dalam port ftp/21 menggunakan usernama dan password dari serangan hydra. Alamat ip address dan waktu serangan yang dilakukan penyerang juga tercatat pada sistem IDS honeypot dan snort.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian diatas maka kesimpulannya adalah:

1. Dengan adanya penelitian ini dimungkinkan untuk mengatasi ekstraksi informasi yang relevan dari log yang dihasilkan oleh honeypots dan Snorts. Melalui informasi yang diperoleh, tingkat ancaman dihasilkan untuk mengklasifikasikan sesi penyerang berdasarkan sekumpulan informasi penyerangan. Sistem yang disajikan melengkapi sebuah IDS snort yang berguna untuk mendapatkan informasi yang terjadi pada sistem ketika adanya penyerangan yang terjadi.
2. Dengan adanya sistem ini mampu mendeteksi ancaman yang sebelumnya tidak diketahui, sekaligus memberikan tingkat keamanan yang lebih tinggi. Dengan sistem honeypots dan snort dapat bekerja sama dalam menahan insiden yang terjadi sehingga penyerang tidak dapat masuk dengan mudah karena penyerang masuk ke dalam perangkap honeypots yang telah dibuat, sehingga server dapat bekerja dengan aman, dan honeypots berhasil mendeteksi aktivitas yang mencurigakan yang dilakuakn hacker, serta menangkap ip address penyerang beserta informasi penyerangan tersimpan pada sistem honeypot dan snort.

5.2 Saran

Setelah melakukan penelitian ini, terdapat beberapa masukan atau saran-saran yang peneliti kemukakan, di antaranya adalah:

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

Daftar Pustaka

[1] Dafiudin, Rahmat. Mengganyang Hacker dengan Snort. Andi Offset. Surabaya,2010.

[2] Akhriana A. 2019. Web App Pendeteksi Jenis Serangan Jaringan Komputer dengan Memanfaatkan Snort Dan Log Honeypot. Makasar: STMIK

[3] P. L. Restanti, "Analisis Kolaborasi IDS Snort dan Honeypot," pp. 1–27, 2014.

[4] T. A. Cahyanto, H. Oktavianto, and A. W. Royan, "Analisis Dan Implementasi Honeypot Menggunakan Dionaea Sebagai Penunjang Keamanan Jaringan," J. Sist. Teknol. Inf. Indones., vol. 1, pp. 86–92, 2016.

[5] A. S. Nugroho, "Analisis Dan Implementasi Honeypot Menggunakan Honeyd Sebagai Alat Bantu Pengumpulan Informasi Aktivitas Serangan Pada Jaringan," Inst. Sains Teknol. AKPRIND, 2013.

[6] Kusnadi. 2018. Analisa Penerapan Intrusion Prevention System (IPS) Berbasis Snort Sebagai Pengaman Server Internet Yang Terintegrasi Dengan Telegram. Jurnal Bite: Bumigora Information And Technology, 1(2).

[7] Laksana. 2017. Implementasi Honeypot Sebagai Pemantau Parameter pada HTTP Request Untuk Mengetahui Tujuan Serangan. Jurnal CITEE.

[8] Laksana. 2017. Implementasi Honeypot Sebagai Pemantau Parameter pada HTTP Request Untuk Mengetahui Tujuan Serangan. Jurnal CITEE.

[9] Nugroho, Ardianto Setyo. 2013. Analisis Dan Implementasi Honeypot Menggunakan Honeyd Sebagai Alat Bantu Pengumpulan Informasi Aktivitas Serangan Pada Jaringan.Institut Sains & Teknologi. Yogyakarta:

AKPRIND.

[10] Arief, Rudiyanto M. 2005. “Penggunaan sistem IDS untuk pengamanan jaringan dan computer”. Yogyakarta: STMIK Amikom.

[11] Husnan, S. (2013). Implementasi Honeypot untuk Meningkatkan Sistem Keamanan Server dari Aktivitas Serangan (Doctoral dissertation, Universitas Muhammadiyah Surakarta).

[12] Leoresta, Arya Ervan,(2014),"Implementasi honeypot sebagai pendeteksi malware pada layanan cloud computing." Program Studi Teknik Informatika Fakultas Sains dan Teknologi. Yogyakarta: Universitas Islam Negeri Sultan Kalijaga.

[13] Mustofa, M. M.,Aribowo, E. (2013). Penerapan Sistem Keamanan Honeypot dan IDS pada Jaringan Nirkabel (Hotspot). Jurnal SarjanaTeknik Informatika.

[14] Putra, Fuadielah Danok Eka (2014) Analisa Perbandingan PerformaIntrusion Detection System Snort, Low Interaction Honeypot Dan High Interaction Honeypot. Skripsi thesis, Universitas Muhammadiyah Surakarta.

[15] T. A. Cahyanto, H. Oktavianto, and A. W. Royan, “Analisis Dan Implementasi Honeypot Menggunakan Dionaea Sebagai Penunjang Keamanan Jaringan,” J. Sist. Teknol. Inf. Indones., vol. 1, pp. 86–92, 2016.

[16] Rafiudin, R. 2012. Mengganyang Hacker Dengan Snort. Yogyakarta: Penerbit Andi.

[17] Pandu Pratama Putra, (2016). Pengembangan Sistem Keamanan Jaringan Menggunakan Rumusan Snort Rule (Hids) untuk Mendeteksi Serangan Nmap.

[18] N. Fitriana dan F. N. Khasanah, "Honeypot Menggunakan Honeyd Sebagai Solusi Keamanan Jaringan Dari Aktivitas Serangan," BINA Insani. ICT J., vol. 5, 2018.

[19] Hatika, L. K., Budiyono, A., & Almaarif, A. (2019). Analisis Ketepatan Deteksi Malware Pada Software Antivirus Menggunakan Metode Analisis Statis. eProceedings of Engineering, 6(2).

[20] Wibisono, R., Budiyono, A., & Almaarif, A. (2019). Analisis Malware Pada Sistem Operasi Android Menggunakan Memory Forensics Berdasarkan Api. eProceedings of Engineering, 6(2).

[21] Febrianto, A. F., Budiyono, A., & Almaarif, A. (2019). Analisis Malware Pada Sistem Operasi Android Menggunakan Metode Network Traffic Analysis. eProceedings of Engineering.

[22] Hatika, L. K., Budiyono, A., & Almaarif, A. (2019). Analisis Ketepatan Deteksi Malware Pada Software Antivirus Menggunakan Metode Analisis Statis. eProceedings of Engineering.

[23] Palcomtech.(2013,23 Desember). Metode Perancangan Jaringan dengan ModelPPDIOO.Diperoleh2Desember2018,darihttp://www.news.palcomtech.com/metode perancangan jaringandengan-model-ppdioo/

DAFTAR RIWAYAT HIDUP

1. Nama : ZAKIA FUADA
2. Nim : 190212006
3. Tempat Tgl Lahir : Aceh Besar, 23 Agustus 2023
4. Jenis Kelamin : Perempuan
5. Alamat : Lam Ue
6. Status : Mahasiswa
7. E- Mail Institusi : 190212006@student.ar-raniry.ac.id
8. Nama Orang Tua :
    a. Ayah : Adnan
    b. Ibu : Dra. Akbari
    c. Pekerjaan Ayah : Petani
    d. Pekerjaan Ibu : Guru
9. Alamat Orang Tua : Lam Ue
10. Pendidikan :
    a. SD/Min : Min Lamjampok
    b. SMP : SMPN 1 Ingin Jaya
    c. SMA : SMAN 1 Ingin Jaya
    d. Perguruan Tinggi : UIN Ar- Raniry Banda Aceh

Banda Aceh 31 Agustus 2023

Zakia Fuada

190212006