MEMBANGUN *PORTABLE WIRELESS INTRUSION DETECTION SYSTEM (IDS)* DENGAN *EMBEDDED SYSTEM* BERBASIS *OPEN SOURCE* (STUDI KASUS: PT NETKRIDA TUAH CAKRAWALA)

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Komputer pada
Program Studi Sistem Informasi

Oleh:

AZWIR IRVANNANDA
11353102055

UIN SUSKA RIAU

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PEKANBARU
2021

LEMBAR PERSETUJUAN

MEMBANGUN *PORTABLE WIRELESS INTRUSION DETECTION SYSTEM (IDS)* DENGAN *EMBEDDED SYSTEM* BERBASIS *OPEN SOURCE* (STUDI KASUS: PT NETKRIDA TUAH CAKRAWALA)

TUGAS AKHIR

Oleh:

AZWIR IRVANNANDA
11353102055

Telah diperiksa dan disetujui sebagai laporan tugas akhir
di Pekanbaru, pada tanggal 21 Februari 2021

Ketua Program Studi	Pembimbing
Idria Maita, S.Kom., M.Sc.	**Eki Saputra, S.Kom., M.Kom.**
NIP. 197905132007102005	**NIP. 198307162011011008**

LEMBAR PENGESAHAN

MEMBANGUN *PORTABLE WIRELESS INTRUSION DETECTION SYSTEM (IDS)* DENGAN *EMBEDDED SYSTEM* BERBASIS *OPEN SOURCE* (STUDI KASUS: PT NETKRIDA TUAH CAKRAWALA)

TUGAS AKHIR

Oleh:

AZWIR IRVANNANDA
11353102055

Telah dipertahankan di depan sidang dewan penguji
sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer
Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau
di Pekanbaru, pada tanggal 19 Februari 2021

Pekanbaru, 19 Februari 2021
Mengesahkan,

Dekan	Ketua Program Studi
Dr. Drs. Ahmad Darmawi, M.Ag.	Idria Maita, S.Kom., M.Sc.
NIP. 196606041992031004	NIP. 197905132007102005

DEWAN PENGUJI:

Ketua : **Idria Maita, S.Kom., M.Sc.**

Sekretaris : **Eki Saputra, S.Kom., M.Kom.**

Anggota 1 : **Inggih Permana, S.T., M.Kom.**

Anggota 2 : **Muhammad Luthfi Hamzah, B.IT., M.Kom.**

LEMBAR HAK ATAS KEKAYAAN INTELEKTUAL

Tugas Akhir yang tidak diterbitkan ini terdaftar dan tersedia di Perpustakaan Universitas Islam Negeri Sultan Syarif Kasim Riau adalah terbuka untuk umum, dengan ketentuan bahwa hak cipta ada pada penulis. Referensi kepustakaan diperkenankan dicatat, tetapi pengutipan atau ringkasan hanya dapat dilakukan atas izin penulis dan harus dilakukan mengikuti kaedah dan kebiasaan ilmiah serta menyebutkan sumbernya.

Penggandaan atau penerbitan sebagian atau seluruh Tugas Akhir ini harus memperoleh izin tertulis dari Dekan Fakultas Sains dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim Riau. Perpustakaan dapat meminjamkan Tugas Akhir ini untuk anggotanya dengan mengisi nama, tanda peminjaman dan tanggal pinjam pada *form* peminjaman.

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Pekanbaru, 19 Februari 2021

Yang membuat pernyataan,

AZWIR IRVANNANDA

NIM. 11353102055

LEMBAR PERSEMBAHAN

Alhamdulillahirabbil'alamin. Puji syukur selalu tersandarkan kepada Allah Azza wa Jalla yang senantiasa Ia melimpahkan karunia ilmu pengetahuan untuk kita agar kita menjadi orang yang bertaqwa. Allahumma salli 'ala sayyidina Muhammad wa 'ala ali sayyidina Muhammad. Salawat dan salam selalu tercurahkan kepada Sayyidina Muhammad Rasulullah beserta para sahabat dan orang-orang yang mengikuti beliau. Semoga kita tergolong orang-orang yang selalu menjalankan dan menjaga Sunnah beliau.

Tugas akhir ini, studi ini saya selesaikan, dan saya persembahkan untuk membahagiakan dan menyampaikan salah satu cita-cita dan harapan kedua orang tua tercinta, yaitu Almarhum Ayahanda Adnan (Sutan Chaniago) bin Ruslan (Datuak Rajo Basa Nan Kuniang) dan Ibunda Zulfarni Binti Abdul Gafar. Serta saya perembahkan untuk 5 orang adik-adikku tersayang yang semoga menjadi generasi yang bermanfaat bagi bangsa dan agama. Kemudian dipersembahkan kepada seluruh keluarga besar yang selalu mendukung saya untuk menyelesaikan studi.

Semoga kelak, Allah meridhoi saya untuk dapat menjadi insan yang alim, adil, dan ihsan, sehingga dapat memberikan manfaat bagi orang banyak dari apa-apa yang Allah titipkan kepada saya.

KATA PENGANTAR

Alhamdulillahirabbil'alamin. Puji syukur selalu tersandarkan kepada Allah Azza wa Jalla yang senantiasa Ia melimpahkan karunia ilmu pengetahuan untuk kita agar kita menjadi orang yang bertaqwa. Allahumma salli 'ala sayyidina Muhammad wa 'ala ali sayyidina Muhammad. Salawat dan salam selalu tercurahkan kepada Sayyidina Muhammad Rasulullah beserta para sahabat dan orang-orang yang mengikuti beliau. Semoga kita tergolong orang-orang yang selalu menjalankan dan menjaga Sunnah beliau.

Pada bagian ini penulis ingin mengucapkan terima kasih banyak kepada seluruh pihak yang telah membantu dan turut mendukung terselesaikannya tugas akhir ini.

Semoga Allah meridhoi tugas akhir ini dan segala bentuk pengetahuan dan informasi yang ada di dalamnya dapat menjadi manfaat bagi kita semua. Terutama dalam perkembangan keamanan teknologi informasi dan komunikasi serta dalam perkembangan FOSS (*Free Open Source Software*), khususnya di Bumi Lancang Kuning Provinsi Riau ini.

Banyak sekali pihak yang telah membantu penulis dalam penelitian dan penyusunan tugas akhir ini, baik secara moril maupun materil. Untuk itu pada kesempatan ini penulis mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. H. Akhmad Mujahidin, S.Ag., M.Ag., sebagai Rektor Universitas Islam Negeri Sultan Syarif Kasim Riau.
2. Bapak Dr. Drs. Ahmad Darmawi, M.Ag., sebagai Dekan Fakultas Sains dan Teknologi.
3. Ibu Idria Maita, S.Kom., M.Sc., sebagai Ketua Program Studi Sistem Informasi.
4. Bapak Eki Saputra, S.Kom., M.Kom., sebagai dosen pembimbing tugas akhir ini.
5. Bapak Inggih Permana, S.T., M.Kom., Bapak Muhammad Luthfi Hamzah, B.IT., M.Kom., dan Ibu Megawati, S.Kom., M.T., sebagai dosen penguji.
6. NETKRIDA (PT NETKRIDA TUAH CAKRAWALA) yang telah memberikan izin, kesempatan, dan fasilitas dalam melakukan penelitian tugas akhir ini.
7. Teristimewa untuk jasa Almarhum Ayahanda, Adnan (Sutan Chaniago) bin Ruslan (Datuak Rajo Basa Nan Kuniang) yang telah mendidik dan mengajarkan prinsip berjiwa besar dan mental pejuang serta inti sari kepemimpinan sebagai anak laki-laki yang berlandaskan ilmu pengetahuan, ilmu

agama, dan menjunjung budaya. Dan teruntuk Ibunda tercinta Zulfarni Binti Abdul Gafar yang selalu sabar, selalu menyayangi, dan menjadi penasehat yang baik, sebagai penyemimbang semangat muda dalam diri yang penuh ambisi. Serta 5 orang adik-adikku tersayang yang semoga menjadi generasi yang bermanfaat bagi bangsa dan agama. Kemudian kepada Nenek di Banda dan seluruh keluarga besar yang selalu mendukung saya untuk menyelesaikan studi.

8. Nasya R Idris, yang telah banyak mendukung secara moril serta membantu dalam penyusunan redaksi tugas akhir ini.
9. Kepada guru-guru, orang-orang yang mengajarkanku ilmu yang bermanfaat, teman-teman terbaikku, adik-adik perjuanganku, Aulia Rahman, dan seluruh teman-teman yang walaupun tidak penulis sebutkan satu persatu secara tekstual, namun secara kontekstual nyatanya telah membantu dalam setiap perjalan penulis hingga selesainya tugas akhir ini.
10. Kepada "rumahku" UXER dan kini telah melebur menjadi Asosiasi Teknologi Informasi dan Open Source (ATIOS), beserta seluruh keluargaku di dalamnya, tempat penulis bernaung, berkarya, dan belajar berbagi manfaat dalam dunia teknologi informasi dan komunikasi.
11. Civitas Akademika Universitas Islam Negeri Sultan Syarif Kasim Riau, terkhusus seluruh Keluarga Besar Mahasiswa Sistem Informasi Fakultas Sains dan Teknologi. "Tetaplah BERSATU dan teruslah MAJU, kebanggaanku!"

Dan terima kasih sekali lagi kepada seluruh pihak yang penulis mungkin tidak menuliskan semuanya di dalam kata pengantar ini. Semoga Allah Azza wa Jalla membalaskan kebaikan tuan dan puan seluruhnya. Dalam penulisan tugas akhir ini, tentunya terdapat kekurangan-kekurangan. Untuk itu penulis sangat mengharapkan kritik dan saran yang membangun untuk pengembangan penelitian ini menjadi lebih baik lagi. Akhir kata penulis berharap semoga tugas akhir ini dapat bermanfaat, dan semoga Allah meridhoi segala ilmu dan perbuatan kita.

Pekanbaru, 21 Februari 2021

Penulis,

AZWIR IRVANNANDA

NIM. 11353102055

MEMBANGUN *PORTABLE WIRELESS INTRUSION DETECTION SYSTEM (IDS)* DENGAN *EMBEDDED SYSTEM* BERBASIS *OPEN SOURCE* (STUDI KASUS: PT NETKRIDA TUAH CAKRAWALA)

AZWIR IRVANNANDA
NIM: 11353102055

Tanggal Sidang: 19 Februari 2021
Periode Wisuda:

Program Studi Sistem Informasi
Fakultas Sains dan Teknologi
Universitas Islam Negeri Sultan Syarif Kasim Riau
Jl. Soebrantas, No. 155, Pekanbaru

ABSTRAK

Menurut hasil riset, survey, dan berbagai penelitian menunjukkan jumlah serangan pada teknologi informasi dan komunikasi terus meningkat secara signifikan, baik secara kualitas mapun kuantitas. NETKRIDA, adalah perusahaan Layanan IT Konsultan Indonesia yang berlokasi di Pekanbaru, Riau berbadan hukum perusahaan dengan nama PT NETKRIDA TUAH CAKRAWALA. Salah satu layanan dari NETKRIDA adalah layanan keamanan jaringan, khususnya jaringan *wireless*. Untuk memastikan tingkat keamanan jaringan komunikasi dan infromasi khususnya jaringan *wireless* yang lebih cenderung rentan karena dapat digunakan langsung oleh siapa saja yang dapat menjangkau area konektifitasnya (*hotspot*). Maka, perlu dibangun sebuah aplikasi pendukung keamanan jaringan sebagai upaya dalam melakukan pencegahan dan mengurangi potensi eksploitasi lebih jauh terhadap kerentanan. Aplikasi pendukung keamanan jaringan tersebut dapat berupa]*Portable Wireless* IDS (*Intrusion Detection System*), yaitu perangkat yang dibangun untuk dapat melakukan monitoring dan pendeteksian dini terhadap aktifitas-aktifitas di dalam jaringan yang dapat menyebabkan security incident, guna melindungi asset-aset informasi dan komunikasi. IDS ini dibangun dengan menggunakan pemanfaatan dan pengembangan sistem operasi Linux dan berbagai aplikasi FOSS (*Free Open Source Software*).

Kata Kunci: *Portable Wireless IDS, Intrusion Detection System, Free Open Source Software, keamanan infromasi, jaringan wireless.*

BUILDING A PORTABLE WIRELESS INTRUSION DETECTION SYSTEM (IDS) WITH EMBEDED SYSTEM BASED ON OPEN SOURCE (CASE STUDY: PT NETKRIDA TUAH CAKRAWALA)

AZWIR IRVANNANDA
NIM: 11353102055

Date of Final Exam: February 19th 2021
Graduation Period:

Department of Information System
Faculty of Science and Technology
State Islamic University of Sultan Syarif Kasim Riau
Soebrantas Street, No. 155, Pekanbaru

ABSTRACT

According to the results of research, surveys, and various studies, it shows that the number of attacks on information and communication technology continues to increase significantly, both in quality and quantity. NETKRIDA, is an Indonesian IT Consultant Services company located in Pekanbaru, Riau, which is a company under the name PT NETKRIDA TUAH CAKRAWALA. One of the services from NETKRIDA is network security services, especially wireless networks. To ensure the security level of communication networks and information, especially wireless networks that are more likely to be vulnerable because it can be used directly by anyone who can reach the area konekitasnya (hotspot). Therefore, it is necessary to build a network security support application as an effort to prevent and reduce the potential for further exploitation of vulnerability. Such network security support applications can be Portable Wireless IDS (Intrusion Detection System), a device built to monitor and detect early activities on the network that can cause security incident, to protect information and communication assets. IDS is built using the use and development of Linux operating system and various applications FOSS (Free Open Source Software).

Keywords: *Portable Wireless IDS, Intrusion Detection System, Free Open Source Software, information security, wireless network*

DAFTAR ISI

LEMBAR PERSETUJUAN ii

LEMBAR PENGESAHAN iii

LEMBAR HAK ATAS KEKAYAAN INTELEKTUAL iv

LEMBAR PERNYATAAN v

LEMBAR PERSEMBAHAN vi

KATA PENGANTAR vii

ABSTRAK ix

ABSTRACT x

DAFTAR ISI xi

DAFTAR GAMBAR xiv

DAFTAR TABEL xvi

DAFTAR SINGKATAN xvii

1 PENDAHULUAN 1

1.1 Latar Belakang 1

1.2 Perumusan Masalah 3

1.3 Batasan Masalah 3

1.4 Tujuan Penelitian 3

1.5 Manfaat Penelitian 4

1.6 Sistematika Penulisan 4

2 LANDASAN TEORI 6

2.1 Aspek Keamanan Informasi 6

2.2 Jaringan *Wireless* 7

2.3 Kelemahan Jaringan *Wireless* 8

2.3.1 Kelemahan pada *Physical Layer* 8

2.3.2 Kelemahan pada *Network Layer* 9

2.4 Landasan Pentingnya Keamanan Data Elektronik 10

2.5 Linux dan *Free Open Source Software* (FOSS) 10
2.6 *(Intrusion Detection System)* 11
2.6.1 Klasifikasi IDS (*Intrusion Detection System*) 11
2.6.2 Metode Deteksi pada IDS (*Intrusion Detection System*) . . 12
2.6.3 Komponen pada IDS (*Intrusion Detection System*) 13
2.7 *Raspberry* Pi 13
2.8 *Embedded System dan Internet of Things* 14
2.9 Profil Instansi 15

3 METODOLOGI PENELITIAN 16
3.1 Metodologi Penelitian Tugas Akhir 16
3.2 Tahap Perencanaan 17
3.3 Tahap Pengumpulan Data 17
3.4 Tahap Analisa dan Perancangan 17
3.5 Tahap Pembuatan dan Implementasi 17
3.6 Tahap Pengujian Aplikasi 17

4 ANALISA DAN PERANCANGAN 18
4.1 Analisis 18
4.1.1 Model dan Kemampuan IDS 18
4.1.2 Spesifikasi Kebutuhan IDS (*System Requirements*) 19
4.1.3 Spesifikasi Jaringan *Wireless* untuk Simulasi Pengujian . . 21
4.1.4 Spesifikasi Perangkat Penguji Coba (*Attacker*) 21
4.2 Perancangan 21
4.2.1 Rancangan *Portable Wireless* IDS 21
4.2.2 Rancangan Jenis Pengujian Serangan 22
4.2.3 Rancangan Jaringan Simulasi Pengujian *Portable Wireless IDS* 23

5 IMPLEMENTASI DAN PENGUJIAN 24
5.1 Hasil Implementasi 24
5.1.1 Perakitan Hardware *Raspberry Pi* 24
5.1.2 Instalasi *Raspberry Pi OS* 27
5.1.3 Instalasi IDS Pada *Raspberry Pi OS* 28
5.2 Hasil Penguji 31
5.2.1 Menyiapkan Simulasi Jaringan Wireless 31
5.2.2 Pengujian Serangan (*Wireless Attack*) 32
5.3 Aktivasi Mode Otomatis 38

6 PENUTUP **39**
6.1 Kesimpulan 39
6.2 Saran 39

DAFTAR PUSTAKA

LAMPIRAN A HASIL WAWANCARA **A - 1**

LAMPIRAN B HASIL PRESENTASI **B - 1**

LAMPIRAN C PROSES PERAKITAN **C - 1**

LAMPIRAN D HASIL PENGUJIAN **D - 1**

DAFTAR GAMBAR

2.1 NIDS dan HIPS 11

3.1 *Flowchart* metodologi penelitian 16

4.1 Tangkapan Layar Properties Jaringan *Wireless* untuk Simulasi. . . . 21
4.2 Kebutuhan Hardware untuk *Wireless* IDS. 22
4.3 Rancangan Topologi Simulasi Pengujian *Wireless* IDS. 23

5.1 Board *Raspberry Pi* dan *acrylic case* 24
5.2 *Lithium Battery* pada *acrylic case* 25
5.3 *Touch screen 3,5 inch* (tampak depan) 25
5.4 *Touch screen 3,5 inch* (tampak belakang) 25
5.5 *Touch screen 3,5 inch* terpasang pada *Raspberry Pi* 26
5.6 Air Live X.USB-3 *Wireless Card Adapter* 26
5.7 *Wireless Card Adapter* terpasang di slot USB *Raspberry Pi* 26
5.8 *Wireless Card Adapter* terpasang di slot USB *Raspberry Pi*(2) . . . 27
5.9 *Flashing Raspberry Pi OS* 27
5.10 Tampilan *Raspberry Pi* OS saat pertama kali *booting* 28
5.11 Tampilan *Desktop Raspberry Pi OS* 28
5.12 *Instalasi Aircrack-NG Suite* 29
5.13 *Instalasi tshark, xterm, wireshark, dan tcpdump* 29
5.14 *Download script Wireless IDS* 29
5.15 *Download script Wireless IDS* 30
5.16 Install *Script Wireless IDS* 30
5.17 Instalasi *Firmware Air Live* X.USB-3 *Wireless Card Adapter* 30
5.18 *Wireless IDS* berhasil berjalan di Raspberry Pi OS 31
5.19 Rancangan Topologi Simulasi Pengujian *Wireless IDS*. 31
5.20 Menjalankan *airmon-ng* dan *airodump-ng*. 32
5.21 Informasi sejumlah AP yang terjangkau oleh *wireless card adapter "Attacker"* 33
5.22 Menjalankan Airreplay-NG 34
5.23 Pengiriman *packet* untuk memutuskan jaringan 34
5.24 Sebuah client terputus dan tidak bisa terhubung dengan AP "NETKRIDA" 35
5.25 Wireless IDS mendeteksi adanya serangan *deauthentication* 35
5.26 Membuat daftar nama AP 36

5.27 Menggunakan mdk3 untuk membuat banyak AP *cloning* ”NETKRIDA” 36
5.28 Menggunakan mdk3 untuk membuat banyak AP *cloning* ”NETKRIDA” 37
5.29 *Wireless IDS* berhasil mendeteksi keanehan banyaknya AP” 37
5.30 *Brute Force WPS* PIN dengan Reaver 38
5.31 IDS dapat mendeteksi kejanggalan *Brute Force WPS* PIN dengan Reaver 38

A.1 Wawancara Pembimbing Sekaligus Sekretaris Prodi Sistem Informasi A - 1
A.2 Wawancara dan Pengumpulan Data Dengan PT NETKRIDA . . . . A - 2

B.1 Presentasi Dengan PT NETKRIDA . . . . . B - 1

C.1 Proses Perakitan . . . . . C - 1
C.2 Proses Perakitan . . . . . C - 1
C.3 Proses Perakitan . . . . . C - 2

D.1 Hasil Produk . . . . . D - 1
D.2 Proses Pengujian . . . . . D - 1
D.3 Proses Pengujian . . . . . D - 2
D.4 Proses Pengujian . . . . . D - 2

DAFTAR TABEL

DAFTAR SINGKATAN

AGC	:	*Apollo Guidance Computer*
AP	:	*Access Point*
CM	:	*Command Module*
FOSS	:	*Free Open Source Software*
HIDS	:	*Host-based Intrusion Detection System*
IDS	:	*Intrusion Detection System*
NIDS	:	*Network Intrusion Detection System*
SBC	:	*Single-Board Circuit*
SSID	:	*Service Set Identifier*

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Sebelumnya internet adalah sebuah jejaring komunikasi antara lembaga riset di perguruan tinggi Amerika Serikat, kini telah menjadi sebuah dunia tersendiri, tempat orang-orang berjejaring dan berkumpul secara global dan mendunia. Oleh karena internet merupakan wanaha tempat berkumpul "dari, oleh, dan untuk" semua orang di dunia maya, maka keamanan informasi menjadi satu isu utama, baik dari segi konten, infrastuktur, dan interaksi. Sejalan dengan semakin demokratisnya dunia internet, makan berbanding lurus dengan meningkatnya resiko insiden keamanan informasi, baik yang terjadi secara sengaja maupun tidak disengaja (Indrajit, 2012)

Seiring perkembangan teknologi komunikasi membuat infrastuktur jaringan beralih ke jaringan wireless. Dikarenakan karena sifat mobilitasnya, yang tentunya fleksibel dan mudah dalam perancangannya (Gast, 2005). Seluruh pengguna jaringan wireless dapat bergerak bebas selagi terhubung dalam sinyal yang ditangkap oleh *wireless adapter*. Karena sifat penyebaran jaringan *text* yang transmisinya ke segala arah, membuat setiap node nya memiliki kerentanan terhadap serangan, yang sekaligus menjadi kelemahan pada jaringan wireless itu sendiri.

Oleh karena akses menuju layanan internet hari ini didominasi dengan penggunaan konektifitas *wireless network* (jaringan nirkabel), maka banyak *hotspot* untuk akses internet melalui *wireless network*, baik di instansi pemerintahan, pertahanan, layanan publik, korporasi hingga untuk kebutuhan di cakupan rumah tangga, yang kemudian berpotensi menjadi target serangan. Serangan pada jaringan pada dasarnya dapat dikelompokkan menjadi dua buah, yaitu serangan pasif dan serangan aktif. Serangan pasif adalah serangan yang melakukan pemantauan secara diam-diam tanpa terdeteksi, dan menunggu data-data yang didapatkan dari pemantauan tersebut. Pada serangan aktif penyerangan lebih dilakukan secara agresif, selain melakukan pemantauan juga melakukan perubahan atau manipulasi aliran data. Begitu banyak model serangan yang dilakukan dan dapat mengeksploitasi kelemahan menjadi sesuatu yang lebih berakibat fatal, maka diperlukannya sebuah sistem keamanan yang dapat mendeteksi masalah-masalah keamanan ini (Sharma, Sharma, dan Singh, 2012). Upaya yang dilakukan untuk menghadapi permasalahan keamanan pada jaringan *wireless* salah satunya adalah dengan penggunaan *Intrusion Detection System* (IDS) (Gómez, Gil, Padilla, Baños, dan Jiménez, 2009).

Kerentanan pada jarigan wireless terhadap serangan-serangan, diperlukan sebuah alat yang mampu mendeteksi (*Intrusion Detection System*) secara dini serangan-serangan terhadap jaringan *wireless* tersebut. Namun, kebanyakan alat atau tools yang ada saat ini berbayar dan harganya relatif mahal, sementara itu pengembangan alternatif *free open source software* yang sudah ada dan dengan teknologi yang mumpuni dapat dilakukan, dan dapat dikembangkan lebih jauh sehingga memiliki nilai mobilitas yang seirama dengan sifat jaringan *wireless* itu sendiri.NETKRIDA, adalah sebuah perusahaan jasa layanan konsultansi teknologi informasi yang berdomisili di kota Pekanbaru, Provinsi Riau. NETKRIDA berbadan hukum usaha perseroan terbatas dengan nama PT NETKRIDA TUAH CAKRAWALA NETKRIDA. Dengan berbagai layanan jasa teknologi informasi mulai dari pengembangan aplikasi berbasis mobile dan web, jaringan komputer, keamanan data, dan juga pelatihan teknologi informasi.

Salah satu layanan dari NETKRIDA adalah layanan keamanan jaringan, khususnya jaringan *wireless*. Untuk memastikan tingkat keamanan jaringan komunikasi dan infromasi khususnya jaringan *wireless* yang lebih cenderung rentan karena dapat digunakan langsung oleh siapa saja yang dapat menjangkau area konektifitasnya (*hotspot*). Maka, perlu dibangun sebuah perangkat pendukung sebagai bentuk produk atau layanan keamanan jaringan dalam upaya melakukan pencegahan dan mengurangi potensi eksploitasi terhadap kerentanan pada Lampiran A. Perangkat pendukung keamanan jaringan tersebut dapat berupa IDS (*Intrusion Detection System*), yaitu perangkat yang dibangun untuk dapat melakukan monitoring dan pendeteksian dini terhadap aktifitas-aktifitas di dalam jaringan yang dapat menyebabkan *security incident*,melakukan presentasi guna melindungi asset-aset informasi dan komunikasi dapat dilihat pada Lampiran B.

Perangkat IDS (*Intrusion Detection System*) tersebut juga harus dapat digunakan secara portable, artinya dapat dengan mudah digunakan kapan saja, dan dimana saja degan mudah, sehingga dapat digunakan langsung oleh level end-user. Maka dari itu, penulis membangun perangkat IDS dengan menggunakan *embedded system* berbasis *open source software* dan *hardware mini komputer board Raspberry Pi* yang juga berlisensi]*open source*. Berdasarkan latar belakang tersebut, maka penulis menjadikan topik ini sebagai penelitian tugas akhir dengan judul: MEMBANGUN *PORTABLE WIRELESS IDS (INTRUSION DETECTION SYSTEM) DENGAN EMBEDED SYSTEM BERBASIS OPEN SOURCE*.

1.2 Perumusan Masalah

Berdasarkan latar belakang tersebut, maka dapat dirumuskan beberapa permasalahan yaitu:

1. Bagaimana merancang dan membangun suatu *embedded system* sebagai IDS (*Intrusion Detection System*) *portable* dengan pemanfaatan *open source*, sehingga menjadi alternatif perangkat yang mumpuni dan efisien.
2. Bagaimana melakukan *setup* atau *implementasi portable* IDS pada jaringan *wireless*.
3. Bagaimana menguji kinerja dan kehandalan IDS dengan melakukan simulasi serangan pada jaringan *wireless*.

1.3 Batasan Masalah

Batasan masalah tugas akhir ini adalah:

1. Pengujian dan IDS dilakukan pada jaringan wireless yang telah ditentukan khusus, di kantor PT NETKRIDA TUAH CAKRAWALA.
2. IDS digunakan untuk jaringan *wireless* mode insfrastruktur yang menggunakan AP (*Access Point*).
3. Pembangunan IDS dan pengujiannya menggunakan Linux dan *Open Source*.
4. Pengujian dilakukan pada jaringan WiFi (*Wireless Fidelity*) yang memiliki *Dynamic Host Control Protocol* (DHCP) *Server*.
5. IDS yang dikembangkan berjenis NIDS (*Network based IDS*).
6. *Hardware* yang digunakan untuk membangun *portable* IDS adalah *Raspberry Pi model B*.

1.4 Tujuan Penelitian

Dalam Tugas Akhir ini terdapat dua tujuan, yaitu:

1. Tujuan Umum

   Adapun tujuan dari penelitian ini adalah membangun sebuah produk portable IDS sebagai security tool alternatif dengan pemanfaatan open source. Sehingga dapat dengan mudah digunakan oleh end-user sebagai pendeteksi dini upaya serangan terhadap jaringan wireless.
2. Tujuan Khusus

   Adapun tujuan khusus dalam Tugas Akhir ini adalah:
   (a) Membuat inovasi sebuah produk *tool security* alternatif yang efisien dan efektif untuk PT NETKRIDA
   (b) Mengembangkan dan meningkatkan popularitas pemanfaatan *Open Source* dalam dunia IT khususnya dalam bidang keamanan jaringan

wireless.

(c) Meningkatkan kesadaran masyarakat tentang sangat pentingnya segi keamanan komunikasi dan infromasi.

(d) Meningkatkan kesadaran dan penerapan standarisasi keamanan jaringan *wireless* pada *public access*.

(e) Menekan biaya untuk sumber daya teknologi dalam bisnis dengan pemakaian perangkat-perangkat dan aplikasi-aplikasi yang berbasis *Open Source*.

1.5 Manfaat Penelitian

Adapun manfaat dari peletian ini adalah sebagai berikut:

1. Dapat menghasilkan suatu *portable device* yang dapat menjadi alat keamanan jaringan *wireless* berupa IDS yang relatif murah, namun mumpuni, serta mudah untuk dibawa.
2. *Portable* IDS dapat digunakan oleh korporasi maupun perorangan. Sehingga dapat diperbanyak nantinya untuk diproduksi dalam jumlah yang masive untuk kepentingan komersil.
3. Menjadi solusi alternatif IDS yang jauh lebih praktis untuk dipakai tidak hanya pada satu jaringan wireless saja.
4. Dapat memudahkan praktisi/profesional/pelaku IT, seperti NETKRIDA untuk saat melakukan layanan uji coba keamanan jaringan, menemukan pelaku MITM (*Man in The Middle*) yang biasa melakukan tindakan illegal pada jaringan wireless, karena tercatat dalam *logs*-nya *portable wireless* IDS ini. Atau saat melakukan demonstrasi produk yang menggunakan jaringan, IDS dapat mendeteksi jika ada penyusup (*intruder*) yang mengganggu atau ingin menggagalkan operasi.

1.6 Sistematika Penulisan

Sistematika penulisan ini disusun agar dalam penulisan laporan lebih teratur serta sesuai dengan tujuan yang diharapkan, berikut sistematika penulisan penelitian tugas akhir ini adalah:

BAB 1. PENDAHULUAN

Pada bab ini berisi tentang latar belakang pemilihan judul, rumusan masalah, batasan masalah, tujuan, manfaat tugas akhir dan sistematika penulisan.

BAB 2. LANDASAN TEORI

Pada bab ini berisi penjelasan tentang teori-teori yang berasal dari jurnal, buku serta studi kepustakaan yang digunakan sebagai landasan teori dalam pembuatan tugas akhir ini.

BAB 3. METODOLOGI PENELITIAN

Pada bab ini membahas tentang tahapan-tahapan serta metode penelitian yang akan digunakan dalam penelitian tugas akhir ini. Baik metodologi pengembangan sistem, analisa, perancangan, hingga *testing*.

BAB 4. ANALISA DAN PERANCANGAN

Pada Bab ini berisi tentang analisa dan perancangan *portable wireless* IDS (*intrusion detection system*) dengan embeded system berbasis *open source*.

BAB 5. IMPLEMENTASI DAN PENGUJIAN

Pada Bab ini berisi tentang pengimplementasian hasil dari analisa dan perancangan menjadi sebuah produk jadi, *portable wireless IDS*, yang siap diterapkan dan dilakukan uji coba terhadap kinerjanya.

BAB 6. PENUTUP

Pada Bab Penutup ini akan dipaparkan kesimpulan dari hasil penelitian ini serta saran dan hal-hal terkait untuk pengembangan selanjutnya.

BAB 2
LANDASAN TEORI

2.1 Aspek Keamanan Informasi

Pada keamanan informasi diperlukan hal-hal pokok yang dikenal dengan CIA, yaitu *Confidentiality, Integrity, dan Availability* (Chad, 2012). Berdasarkan ISO27000, definisi dari ketiga hal tersebut adalah sebagai berikut:

1. *Confidentiality Confidentiality* adalah karakteristik yang dikenakan kepada informasi. Untuk melindungi informasi dan memelihara Confidentiality dari informasi maka harus dijamin bahwa informasi tersebut tidak tersedia atau tertutup untuk entitas yang tidak berwenang meliputi individual dan proses.
2. *Integrity Integrity* dapat diartikan sebagai keaslian, akurasi, dan kelengkapan dari informasi.
3. *Availability Availability* menyangkut tentang akses dan kegunaan saat entitas yang berwenang membutuhkan akses. Seiring berkembangnya teknologi informasi dan security, aspek keamanan berkembang dari CIA ke beberapa aspek lain diantaranya:
4. *Authentication*

   Authentication adalah proses untuk membuktikan klaim dari karakter atau identitas suatu entitas. Biasanya, *Authentication* diimplementasikan berupa multi-factor *Authentication* yang meliputi *"what you have"* seperti magnetic swipe card, kartu atm, dan lain-lain; *"what you know"* seperti PIN, password, dan lain-lain; dan what you are seperti sidik jari, retina mata, suara, dan lain-lain.
5. *Access Control*

   Access Control meliputi authorization dan pembatasan akses pengguna terhadap resource yang ada.
6. *Non repudiation*

   Non repudiation merupakan prinsip ketidakterbantahkan suatu transaksi sebagai bukti bahwa suatu event terjadi atau suatu aksi benar-benar dilakukan dengan entitas dan asal yang jelas sehingga pengguna tidak dapat mengelak terhadap kejadian atau aksi yang telah dilakukan.
7. *Accountability*

   Accountability adalah aspek yang membahas tentang tanggung jawab entitas terhadap tugas dan respon yang diharapkan.

2.2 Jaringan *Wireless*

Jaringan *Wireless* adalah jaringan tanpa kabel atau biasa disebut dengan istilah nirkabel, yang menggunakan frekuensi radio untuk komunikasi antara perangkat yang terhubung. Jaringan *wireless* bekerja pada *bandwith* dengan gelombang 2,4GHz (802.11b, 802.11g) atau 5GHz (802.11a). Pada umumnya perangkatnya memiliki kualifikasi Wi-Fi,IEEE 802.11b atau akomodasi IEEE 802.11g, dan memiliki beberapa proteksi keamanan seperti *Wired Equivalent Privacy* (WEP) dan *Wireless Protected Access* (WPA) (Wong, 2003). Jaringan *wireless* menghubungkan perangkat-perangkat komputer satu dengan lainnya menggunakan sinyal dengan media udara sebagai media jalur lintasannya. Perbedaan jaringan wireless dengan jaringan LAN adalah medianya, jaringan LAN menggunakan media kabel untuk terhubung, sedangan *wireless* menggunakan sinyal di udara sebagai media lalu lintas datanya.

Adapun jenis-jenis jaringan wireless adalah sebagai berikut:

1. *Wireless Wide Area Networks* (WWAN)

   Wireless Wide Area Networks (WWAN) adalah jaringan tanpa kabel yang memungkinkan pengguna terhubung secara public maupun privat. Luas konektivitas WWAN mencakup suatu daerah yang sangat luas, seperti kota atau sebuah negara, yang terhubung melalui antenna pemancar bahkan sistem satelit oleh penyelenggara jasa telekomunikasi. Teknologi WWAN dikenal popular sekarang pada teknologi komunikasi seluler. Hingga saat ini teknologi 4G sudah digunakan, dan akan beralih ke teknologi 5G yang sudah ditemukan.

2. *Wireless Metropolitan Area Networks* (WMAN)

   WMAN adalah jaringan tanpa kabel yang menghubungkan jaringan nirkabel di beberapa lokasi dalam suatu area metropolitan, contohnya menghubungkan koneksi antara jaringan beberapa kampus atau beberapa rumah sakit dalam suatu kota, dan bisa dicapai dengan biaya yang relatif murah dibandingkan dengan penggunaan *fiber optic* ataupun kabel tembaga. WMAN biasa juga digunakan sebagai cadangan (backup) jaringan yang berbasis kabel, dan dapat diaktifkan ketika jaringan berbasis kabel mengalamai gangguan.

3. *Wireless Local Area Networks* (WLAN).

   WLAN merupakan jaringan tanpa kabel yang areanya bersifat local, contohnya dalam area Gedung sebuah perusahaan, area cafe, perpustakaan, dan pada area public yang cakupannya lokal. Pemanfaatan WLAN diarea *public outdoor* seperti taman sangatlah efektif karena tidak diperlukan instalasi

kabel yang rumit dan beresiko terkena korsleting.

4. *Wireless Personal Area Networks* (WPAN).

   WPAN adalah suatu jaringan nirkabel ad hoc. WPAN biasa digunakan dalam ruang operasi personal. WPAN biasanya digunakan untuk kepentingan pribadi, seperti teknologi bluetooth dan infrared.

2.3 Kelemahan Jaringan *Wireless*

Secara umum, celah keamanan pada jaringan *wireless* terdapat empat lapisan (*layer*) yang mana layer-layer tersebut terlibat dalam proses terjadinya komunikasi data pada jaringan *wireless*, diantaranya adalah *Physical layer, Network Layer, User Layer,* dan *Application Layer*. Dengan kata lain, pada setiap layer proses komunikasi jaringan *wireless* terdapat potensi celah-celah keamanan. Maka dari itu, keamanan jaringan *wireless* menjadi sangat rentan dan serius dan perlu menjadi perhatian khusus dalam penggunaannya. Setidaknya di dalam penelitian ini penulis fokus menyajikan kelemahan pada dua buah lapisan layer yang sudah pasti tidak terlepaskan dengan jaringan *wireless* itu sendiri, yaitu *Physical layer* dan *Network Layer*, berikut pemaparannya:

2.3.1 Kelemahan pada *Physical Layer*

Kelemahan pada *Physical Layer* (layer fisik) akan berhubungan dengan proses komunikasi data, tepatnya dengan media pembawa komunikasi data itu sendiri, yaitu udara bebas. Di hamparan udara bebas tersebut lalu-lintas data-data berwujud sinyal radio dalam frekuensi tertentu. Bebasnya lalu-lintas data berbentuk sinyal radio tersebut yang sangat dapat berpotensi dijangkau oleh semua orang. Berikut adalah celah keamanan umum pada lapisan *Physical layer*:

1. *Bleeding Coverage Area*

   Bleeding Coverage Area merupakan kelemahan yang berasal dari sifat jaringan *wireless* itu sendiri. Sinyal jaringan *wireless* yang dipancarkan oleh *Access Point* (AP) memiliki panjang, lebar, dan tinggi jangkauan. Oleh karena itu sinyal *wireless* sulit untuk diketahui dan diperhitungkan dengan tepat area jangkauannya. Dalam hal ini, sangat memungkin sebuah jaringan *wireless* terpancara melebihi jangkauan area yang ditentukan untuknya. Misalnya, sebuah AP di sebuah ruangan kantor NETKRIDA di pasang hanya untuk meng-cover ruangan kantor NETKRIDA itu saja, namun kenyataannya kantor tetangga atau rumah orang lain yang berada disekitar dapat menjangkau atau menggunkan jaringan *wireless* ini. Hal inilah yang disebut dengan *bleeding coverage area*. Dengan adanya *coverage area* ini, akan sangat berpotensi untuk dieksploitasi lebih jauh oleh orang-orang

yang tidak mempunyai hak di luar.Aktifitas mencari *bleeding coverage area* untuk dieksploitasi biasa disebut dengan istilah *war driving* .

2. *External Access Point*

Merupakan potensi celah keamanan jaringan wireless dari sisi *physical*, contohnhya, pada kantor NETKRIDA terdapat beberapa client atau pengguna sebuah *access point* resmi dari kantor NETKRIDA, namun dengan sengaja seorang yang ingin melakukan tindakan illegal memasang sebuah *access point* "fisik" secara illegal yang mana jangkauan sinyalnya sampai ke dalam lingkungan kantor NETKRIDA dan dapat dijangkau oleh perangkat-perangkat pengguna di kantor tersebut.

Misalnya, *access point* tersebut juga tidak diberikan password SSID-nya, bagi perangkat yang membuat settingan *auto-connect* ke *wireless* akan sangat mudah terjebak masuk ke dalam jaringan *wireless* yang dibuat oleh *external access point* ini yang notabene tidak memakai password atau autentikasi untuk terhubung dan bahkan jika sinyalnya lebih kuat dari *access point* resmi kantor NETKRIDA itu sendiri.

2.3.2 Kelemahan pada *Network Layer*

1. *Rogue Access Point*

Rogue Access Point merupakan AP (*access point*) illegal yang tidak dibuat oleh administrator jaringan pada sebuah kantor atau area tersebut secara resmi. Merupakan Teknik serangan eksploitasi lebih jauh dari kelemahan *External Access Point (physical)* yang mana pada *Rogue Access Point* hanya memerlukan sebuah alat yang dapat membuat jaringan *wireless* atau *Service set Identifier* (SSID) jaringan wireless secara banyak atau berapapun yang diinginkan dan melakukan broadcast sehingga perangkat mana pun bisa menggunakannya atau terhubung ke jaringan melalui SSID yang dibuat. Misalnya pada sebuah gedung instansi pemerintah atau tempat publik, café misalnya dibuatlah SSID-SSID palsu yang mana setiap orang yang sudah terhubung bisa berpotensi dieksploitasi lebih jauh.

2. *Evil Twin Access Point* Tidak jauh berberda konsepnya dengan *Rogue Access Point* kelemahan dengan memanfaatkan teknik *Evil Twin Access Point* ini adalah dengan membuat *access point* palsu yang relative sama persis dengan *access point target* yang ada dalam lokasi atau sebuah area. Dengan kata lain melakukan tiruan atau *cloning*. Nama SSID dan tampilan login (jika ada) dibuat sama persis untuk mencuri data seperti password dan sebagainya.

2.4 Landasan Pentingnya Keamanan Data Elektronik

Landasan pentingnya keamanan data elektronik dalam aktifitas komputer/jaringan secara umum diatur menurut:

1. Regulasi
   UU – ITE (Undang-Undang – Informasi dan Transaksi Elektronik)
2. Standarisai
   SNI ISO 27001:2009 – Sistem Manajemen Keamanan Informasi

2.5 Linux dan *Free Open Source Software* (FOSS)

Free and Open Source Software (Perangkat lunak Bebas dan Sumber Terbuka) merupakan perangkat lunak yang bersifat bebas sekaligus memberikan kode sumber terbuka (open source). FOSS merupakan kebalikan dari perangkat lunak proprietary, merupakan perangkat lunak yang hanya dapat digunakan dengan lisensi yang sangat ketat serta kode sumbernya tidak terbuka. FOSS dapat menjadi solusi alternatif dalam mengembangkan sebuah perangkat komputer, karena banyaknya dukungan dari developer yang bisa berkontribusi dengan bebas, FOSS saat ini berkembang begitu cepat dan maju (Crowston dan Howison, 2005).

Kata "Free" di sini tidak mutlak berarti gratis, melainkan berarti "bebas" (freedom), siapa saja diberikan kebebasan untuk menggunakan, mengembangkan, dan membagikan FOSS tersebut. Hingga saat ini project FOSS telah memegang pasar dunia, contohnya Android, sistem operasi mobile berbasis kernel Linux (Lakhani dan Von Hippel, 2004).

Linux awalnya merupakan sebuah sistem operasi komputer bertipe Unix. Peralatan sistem dan pustakanya umumnya berasal dari sistem operasi GNU, yang publikasikan pada 1983 oleh Richard Stallman, sehingga muncul nama alternatif yang dikenal dengan GNU/Linux. Pada awalnya Linux merupakan proyek pribadi Linus Torvalds yang merupakan nama sang penciptanya, nama Linux sendiri diperkenalkan pada 1991 yang berasal dari mana pembuatnya tersebut. Kemudian Linux akhirnya menjadi proyek open source yang dikembangkan secara komunitas, siapa saja dapat berkontribusi di dalam proyek pengembangan Linux, sehingga kode sumber Linux dapat dimodifikasi, digunakan dan didistribusikan kembali secara bebas oleh siapa saja (Stallman dan Manual, 1986).

Linux awalnya lebih dikenal dalam dunia server, dengan didukung pula oleh perusahaan-perusahaan komputer ternama seperti Intel, Dell, Hewlett-Packard, IBM, Novell, Oracle Corporation, Red Hat, dan Sun Microsystems. Sekarang Linux sudah menjadi sistem operasi di berbagai perangkat, mulai dari komputer, handphone, video game, router, hingga sistem smart home, serta super car. Ke-

suksesan Linux sendiri untuk berkembang adalah ketidaktergantungannya kepada vendor, serta faktor keamanan dan stabilannya yang tinggi.

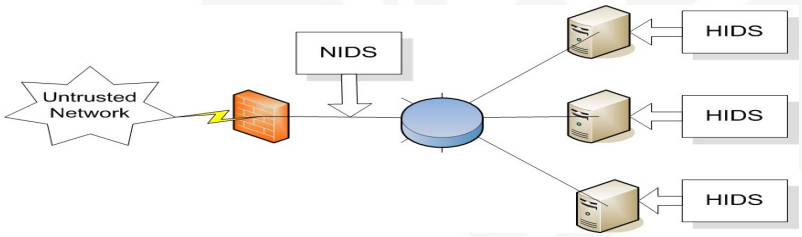
2.6 *(Intrusion Detection System)*

Penyerangan terhadap jaringan *wireless* menjadi sangat mudah dilakukan oleh siapa saja dikarenakan jaringan *wireless* yang menggunakan sinyal dalam lalu-lintas datanya mudah dijangkau bahkan diakses untuk dilakukan penyerangan atau eksploitasi lebih lanjut. Maka dari itu perlu adanya Tindakan pencegahan dini berupa pemantauan terhadap keaman jaringan wireless tersebut, salah satunya dengan membangun sistem pemantau berupa *Wireless* Intrusion Detection System (IDS).

IDS adalah alat atau aplikasi yang dapat mendeteksi aktivitas-aktivitas yang mencurigakan dalam sebuah jaringan, wireless IDS dibuat khusus untuk melakukan pemantauan keamanan pada jaringan *wireless*. *Wireless* IDS bekerja dengan melakukan kegiatan traffic sniffing pada sinyal untuk memantau paket-paket data yang berlalu-lintas dan melaporkan jika ada terjadi lalu-lintas yang mencurigakan. IDS adalah perangkat yang dibangun untuk dapat melakukan monitoring dan pendeteksian dini terhadap aktifitas-aktifitas di dalam jaringan yang dapat menyebabkan security incident, guna melindungi asset-aset informasi dan komunikasi.

2.6.1 Klasifikasi IDS (*Intrusion Detection System*)

Ilustrasi perbedaan NIDS dan HIDS dapat dilihat pada Gambar 2.1



Gambar 2.1. NIDS dan HIPS

IDS pada dasarnya diklasifikasikan menjadi 2 jenis:

1. *Network Intrusion Detection System* (NIDS)

   NIDS bekerja pada jaringan, menggunakan sensor yang diletakkan di jaringan. NIDS memonitor dan menganalisa keseluruhan lalu-lintas jaringan, dan membuat analisis laporan yang diteruskan ke *console* sehingga dapat diketahui hasil dari kinerjanya. NIDS baisanya bekerja dengan menggunakan atau mengkombinasikan metode deteksi *signature analysis, anomaly analysis,* dan *application/protocol analysis*. (Bace dan Mell, 2001)

2. *Host-based Intrusion Detection System* (HIDS)

   HIDS berkeja dengan agent yang diletakkan pada setiap host dalam sebuah jaringan, HIDS memonitor dan menganalisa lalu-lintas yang berasal dan keluar dari masing-masing host dimana HIDS itu ditempatkan. HIDS hanya memonitor spesifik host yang ditempatinya berbeda dengan NIDS yang memonitor keseluruhan jaringan. Namun, karena memonitor lebih spesifik setiap host, HIDS dapat lebih detail melihat aktifitas yang ada pada host.

2.6.2 Metode Deteksi pada IDS (*Intrusion Detection System*)

IDS melakukan metode deteksi berdasarkan dua metode, yaitu signature based dan anomaly based (Jyothsna, Prasad, dan Prasad, 2011), yaitu sebagai berikut:

1. *Signature-based (Knowledge-based) Detection*

   Suatau aktifitas, termasuk serangan memiliki karakteristik, pola atau memiliki ciri jejak yang disebut *footprint* yang berbeda dari satu dan lainnya. *Footprint* tersebut dapat juga diistilahkan dengan *signature*, beberapa *signature* kemudian dikumpulkan menjadi sebuah *signature database*. Berdasarkan *signature database* inilah IDS melakukan pendeteksian atau analisa terhadap suatu serangan, dengan mencocokkan aktifitas dengan data yang terkumpul di *signature database*.

   (a) Kelebihan:
      i. Sederhanan pengimplementasiannya karena sudah ada *signature database* sebagai pedoman.
      ii. Relatif lebih cepat untuk mendeteksi serangan yang sama dan menghasilkan deteksi *true positive* yang banyak.
      iii. Relatif sedikit menghasilkan *deteksi false positive*.

   (b) Kekurangan:
      i. Sulit mendeteksi serangan *zero day attack* atau serangan jenis baru, karena tidak dapat mendeteksi tiep serangan yang tidak ada di *signature database*. Sehingga diperlukannya untuk selalu memperbarui *signature database* yang dimiliki.
      ii. Melakukan *packet analysis* dengan size yang besar dan banyak, memerlukan *resource* yang besar.

2. *Anomaly-Based (Behavior-based) Detection* Adalah cara deteksi dengan kemampuan untuk mengetahui atau memperlajari *behavior* atau kebiasaan sistem atau jaringan terlebih dahulu. Kemudian setelah dipelajari dan

direkam sebagai sebuah *behavior* IDS akan mendeteksi segala bentuk aktivitas, yang bukan dikenal sebagai behavior maka itu disebut dengan *anomaly*, dan ditangkap sebagai serangan terhadap sistem atau jaringan.

(a) Kelebihan:
   i. Dengan melakukan *baselining* pada sistem terlebih dahulu, maka metode *aanomaly based* akan relatif lebih dapat mendeteksi serangan jenis baru yang menyerang dibandingkan dengan *signature based*.

(b) Kekurangan:
   i. Cukup membutkan waktu untuk melakukan pembelajaran atau *baselining* pada sebuah sistem atau jaringan.
   ii. Relatif lebih sulit untuk diterapkan dengan cepat dan dikonfigurasi daripada *signature based*.
   iii. Relatif lebih banyak menghasilkan deteksi *false positive*.

2.6.3 Komponen pada IDS (*Intrusion Detection System*)

Ada beberapa tipe komponen pada IDS seperti yang dijelaskan berikut ini:

1. *Sensor* atau *Agent*
   Sensor atau *Agent* berfungsi sebagai yang bertugas menganalisa kegiatan lalu-lintas data. *Sensor* biasanya digunakan untuk memantau di jaringan biasa dipakai pada NIDS. Sedangkan agent biasa dipakai pada HIDS.
2. *Management Server*
   ]*Management Server* berfungsi menerima dan mengelola informasi yang dikirimkan oleh *sensor* atau *agen*.
3. *Database Server*
4. *Database Server* berfungsi sebagai tempat menyimpan data yang dicatat oleh *sensor, agent,* atau *management sever*.
5. *Console*
   Console berfungsi sebagai *interface* yang memberikan informasi kepada pengguna atau administrator IDS.

2.7 *Raspberry* Pi

Raspberry Pi, disingkat dengan Raspi, adalah sebuah *single-board circuit (SBC)* atau komputer berpapan tunggal. Ukuran Raspi kurang lebih seukuran luas kartu kredit. Sama halnya dengan komputer biasa, Raspi dapat digunakan untuk mengerjakan program perkantoran, game, pemutar video dan musik, dan melakukan aktifitas lainnya layaknya komputer pada umumnya. Raspi dikem-

bangkan oleh Rasberry Pi Foundation bersama beberapa pengembang dan ahli komputer dari Universitas Cambridge di Inggris (Robinson dan Cook, 2013)

Inisiasi awal dibalik pembuatan Raspi berasal dari ide Eben Upton, Rob Mullins, Jack Lang, dan Alan Mycroft, dari Laboratorium Komputer Universitas Cambridge untuk membuat sebuah inovasi baru dalam pemrogramman komputer, karena kekhawatiran mereka pada menurunnya keahlian dan jumlah siswa yang berminat dengan ilmu komputer saat itu. Mereka kemudian mendirikan *Rasberry Pi Foundation* bersama dengan dua teman lainnya, yaitu Pete Lomas dan David Braben pada tahun 2009.

Pada tahun 2012 *Rasberry Pi* Model B pertama kalinya memasuki produksi massal. Dalam peluncurannya pada akhir Febuari tahun 2012, hanya dalam beberapa jam saja sudah terjual 100.000 unit *Rasberry Pi*. Kemudian pada bulan Februari 2016, *Rasberry Pi Fundation* mengumumkan bahwa mereka telah melakukan penjualan hingga 8 juta perangkat *Rasberry Pi*, sehingga menjadikan *Rasberry Pi* sebagai perangkat komputer paling laris di Inggris saat itu.

2.8 *Embedded System dan Internet of Things*

Embedded system atau sistem tertanam merupakan sistem komputer khusus yang dirancang untuk menjalankan tugas tertentu dan biasanya sistem tersebut tertanam dalam satu kesatuan sistem. Sistem ini menjadi bagian dari keseluruhan sistem yang terdiri atas mekanik dan perangkat keras lainnya.

Sistem embedded modern yang pertama dikenali adalah Apollo Guidance Computer, dikembangkan oleh Charles Stark Draper di MIT Instrumentasi Laboratorium, awal 1960-an. Apollo Guidance Computer (AGC) adalah on-board digital computer (papan komputer digital), diinstall di setiap acecraft program Apollo, baik Command Module (CM) dan Lunar Module (LM). Disediakan onboard computation untuk mendukung spacecraft guidance, navigasi dan kontrol. Apollo flight computer adalah yang pertama menggunakan Integrated Circuit (IC). Software AGC ditulis dalam bahasa assembly AGC (Mostafa dan Frear, 2015)

Bidang embedded system mencakup penguasaan perangkat keras (hardware). Sistem embedded merupakan sebuah sistem (rangkaian elektronika) digital yang merupakan bagian dari sebuah sistem yang lebih besar, yang biasanya bukan berupa sistem elektronika. Kata embedded menunjukkan bagian yang tidak dapat berdiri sendiri. Berbeda dengan sistem digital yang didesain untuk general purpose. Embedded system biasanya diimplementasikan dengan menggunakan mikrokontroler, sistem embedded dapat memberikan respon yang sifatnya real time dan banyak digunakan pada peralatan digital, seperti jam tangan.

Embedded system adalah sistem dengan ciri-ciri sebagai berikut:

1. Mempunyai *computing power*. Dengan kata lain dilengkapi dengan sebuah *processor*.
2. Bekerja di lingkungan luar ruangan IT. Jadi kemungkinan besar tidak dilengkapi dengan AC dan menghadapi gangguan dari luar seperti getaran dan debu.
3. Memiliki tugas yang spesifik. Beda dengan PC atau Server yang relatif lebih *multi purpose.*

Internet of things (IoT) merupakan sebuah konsep komputasi yang membuat mesin-mesin memiliki kemampuan untuk saling berinteraksi sehingga dapat menghasilkan sesuatu yang bermanfaat bagi manusia. *Embedded system* dan *internet of things*, keduanya tidak bisa dipisahkan, karena *embedded system* tidak akan berkembang jika tidak ditanamkan teknologi seperti IoT, begitu pula IoT tidak akan berarti apa-apa jika tidak ditanamkan ke *embedded system*. *Internet of things* (IoT) membutuhkan *sensor*, dan *sensor* tersebut adalah *embedded system*.

2.9 Profil Instansi

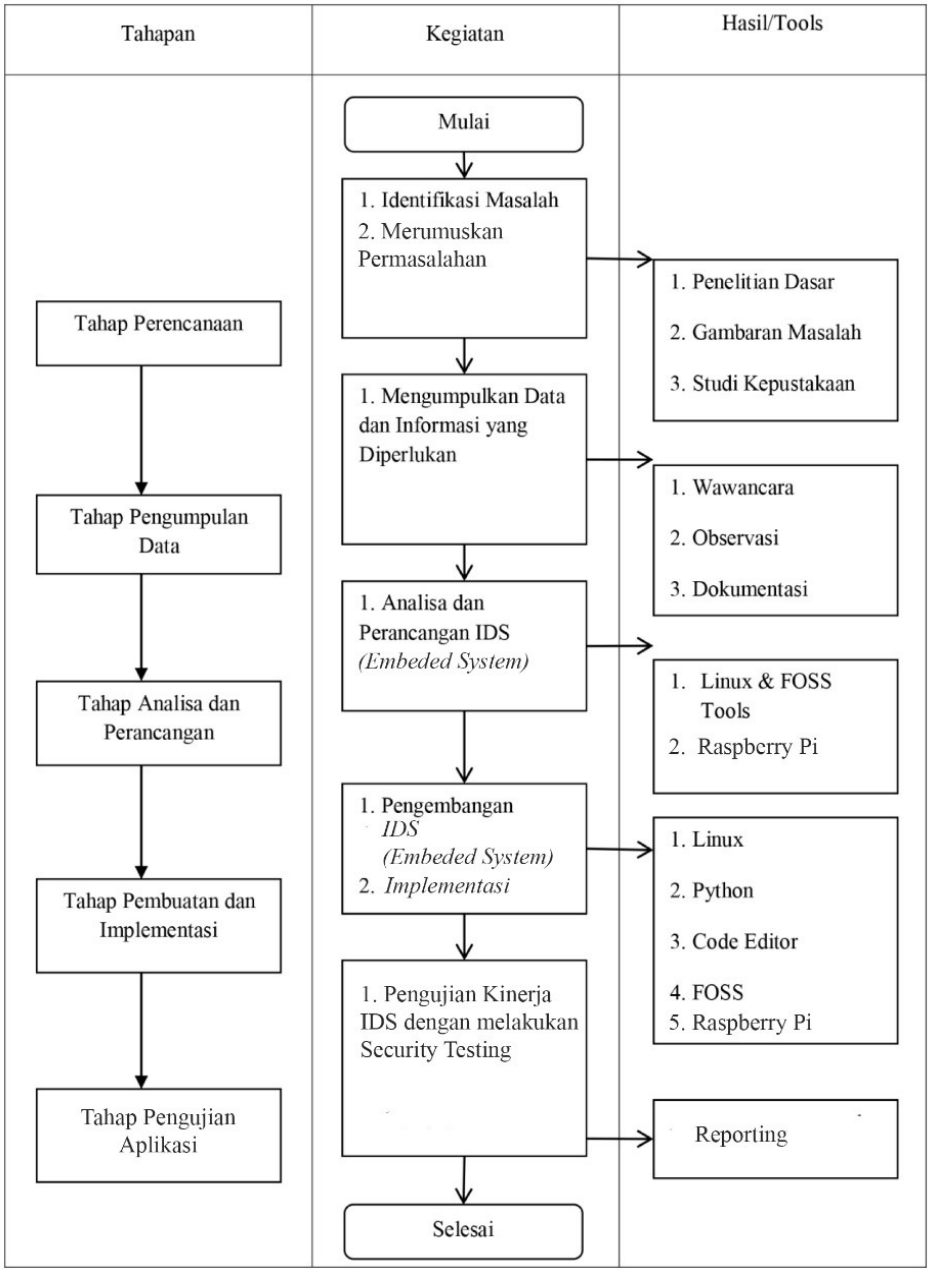
NETKRIDA, adalah perusahaan Layanan IT Konsultan Indonesia yang berlokasi di Pekanbaru, Riau berbadan hukum perusahaan dengan nama PT NETKRIDA TUAH CAKRAWALA. NETKRIDA melayani jasa pembuatan dan pegembangan website, desktop aplikasi, desain grafis, jaringan/networking, komunikasi multimedia, keamanan sistem dan jaringan, sistem terintegrasi, monitoring/audit sistem maupun jaringan, dan berbagai solusi IT lainnya.

Dalam situs webnya (netkrida.co.id) NETKRIDA mengatakan, "NETKRIDA menjadi solusi terbaik untuk segala permasalahan dan keinginan di bidang Teknologi Informasi dan Komunikasi. Dengan berkomitmen memberikan pelayanan terbaik yang profesional dan kualitas produk dan layanan yang selalu up-to-date, Anda akan mendapakan solusi IT yang sesuai dengan harapan dan kebutuhan Anda".

BAB 3
METODOLOGI PENELITIAN

3.1 Metodologi Penelitian Tugas Akhir

Dalam penelitian ini ada beberapa tahap-tahap yang peneliti lakukan. Adapun metodologi penelitian yang penulis lakukan dapat dijabarkan secara garis besar pada Gambar 3.1



Gambar 3.1. *Flowchart* metodologi penelitian

3.2 Tahap Perencanaan

Tahap perencanaan adalah tahap perencanaan penelitian dengan melakukan penelitian dasar. Penelitian dasar dilakukan dengan menanyakan kepada instansi beberapa masalah yang sedang dihadapi sehingga terbentuk latar belakang masalah, tujuan penelitian dan batasan masalahnya. Setelah itu, mencari referensi (studi kepustakaan) dengan membaca jurnal mengenai penelitian sejenis dan literatur yang berhubungan dengan masalah.

3.3 Tahap Pengumpulan Data

Pada tahap ini, peneliti melakukan penelitian lebih lanjut terhadap masalah yang telah ditentukan. Penulis melakukan wawancara dan observasi kepada pembimbing penelitian di kantor NETKRIDA dan beberapa orang teknisi mengenai informasi jaringan *wireless* yang akan di lakukan sebagai objek penelitian kerja praktek. Penulis mengumpulkan dokumentasi informasi yang diperlukan sebagai referensi dalam pembuatan aplikasi.

3.4 Tahap Analisa dan Perancangan

Setelah selesai mengumpulkan data yang diperlukan, penulis melakukan analisa informasi jaringan *wireless* dan IDS yang akan dibangun menggunakan *tools Free and Open Source Software* yang telah dipersiapkan. Setelah analisa selesai, penulis menentukan model rancangan sistem kemanan jaringan berupa *Portable Wireless* IDS (*Intrusion Detection System*) sebagai sistem pendeteksi serangan keamanan pada jaringan wireless.

3.5 Tahap Pembuatan dan Implementasi

Pada tahap ini, rancangan yang telah ditentukan (*Portable IDS berbasis Open Source Software*) dikembangkan (*development*) untuk dapat disesuaikan dan diterapkan pada jaringan *wireless* yang telah ditentukan untuk uji coba implementasi. Penulis menggunakan bahasa pemrograman Python dengan pengembangan di atas platform sistem Operasi Linux pada *Raspberry Pi*.

3.6 Tahap Pengujian Aplikasi

Setelah aplikasi IDS selesai dibangun, maka dilakukanlah uji coba kinerja IDS pada jaringan *wireless*, dengan melakukan simulasi serangan (*security testing*) terhadap jaringan *wireless* yang telah dipasang IDS.

BAB 6
PENUTUP

6.1 Kesimpulan

Serangan terhadap jaringan wireless dapat terjadi kapan dan dimana saja. Oleh karena itu diperlukan sebuah proses monitoring agar potensi dan aktifitas serangan dapat diketahui secara dini sehingga dapat dicegah dan dilakukan tindakan. IDS berbasis *Open Source Software* dapat menjadi alternatif yang jauh lebih murah dengan kinerja dan tujuan yang sama dalam bidang security.

Portable Wireless IDS yang penulsi bangun bekerja dengan baik dan efektif dan memiliki mobilitas yang tinggi, bisa dibawa kemana-mana dengan mudah dan juga tentunya mumpuni untuk mendeteksi tipe-tipe serangan *wireless attack* saat ini. *text* ini sangat berguna bagi perusahaan jasa security seperti PT NETKRIDA TUAH CAKRAWALA sebagai kelengkapan dalam melakukan operasi pekerjaan. Dan dapat menjadi alat yang dipasang untuk *network security forensic* merekam aktifitas user-user atau *client* yang dicurigai melakukan aktifitas illegal dalam lingkungan sebuah *wireless network*.

6.2 Saran

Dalam penelitian ini penulis menarik beberapa pengamatan yang dapat dijaikan saran dalam pengembangan kedepan untuk *Portables Wireless IDS* ini, yaitu sebagai berikut:

1. Perlu adanya pengembangan atau penambahan kamus jenis serangan yang dapat dideteksi oleh *Portables Wireless IDS* ini.
2. Perlu pengembangan antar muka yang lebih *user-friendly* agar orang awam lebih mudah membaca tampilan monitoring IDS.
3. Perlu adanya desain *hardware-case* yang lebih menarik untuk *wireless IDS*ini.

DAFTAR PUSTAKA

Bace, R. G., dan Mell, P. (2001). *Intrusion detection systems.* US Department of Commerce, Technology Administration, National Institute of ....

Chad, P. (2012). The cia triad and engineering principles for information technology security. *Retrieved*.

Crowston, K., dan Howison, J. (2005). The social structure of free and open source software development. *First Monday*.

Gast, M. (2005). *802.11 wireless networks: the definitive guide*. " O'Reilly Media, Inc.".

Gómez, J., Gil, C., Padilla, N., Baños, R., dan Jiménez, C. (2009). Design of a snort-based hybrid intrusion detection system. Dalam *International work-conference on artificial neural networks* (hal. 515–522).

Indrajit, R. E. (2012). Cert. csirt. id-sirtii. tim pengawas keamanan internet. *MANAJEMEN KEAMANAN INFORMASI DAN INTERNET*, *20*(2), 20–36.

Jyothsna, V., Prasad, R., dan Prasad, K. M. (2011). A review of anomaly based intrusion detection systems. *International Journal of Computer Applications*, *28*(7), 26–35.

Lakhani, K. R., dan Von Hippel, E. (2004). How open source software works:"free" user-to-user assistance. Dalam *Produktentwicklung mit virtuellen communities* (hal. 303–339). Springer.

Mostafa, A. K., dan Frear, M. (2015). Running page: Benefits of embedded systems.

Robinson, A., dan Cook, M. (2013). *Raspberry pi projects*. John Wiley & Sons.

Sharma, P., Sharma, N., dan Singh, R. (2012). A secure intrusion detection system against ddos attack in wireless mobile ad-hoc network. *International Journal of Computer Applications*, *41*(21).

Stallman, R. M., dan Manual, G. E. (1986). Free software foundation. *El proyecto GNU–Fundación para el software libre*.

Wong, S. (2003). The evolution of wireless security in 802.11 networks: Wep, wpa and 802.11 standards. *SANS Institute*, 1–9.

LAMPIRAN A
HASIL WAWANCARA

Adapun hasil wawancara pada penelitian ini dapat dilihat pada Gambar A.1, Gambar A.2.

Gambar A.1. Wawancara Pembimbing Sekaligus Sekretaris Prodi Sistem Informasi

Gambar A.2. Wawancara dan Pengumpulan Data Dengan PT NETKRIDA

LAMPIRAN B
HASIL PRESENTASI

Adapun hasil presentasi penelitian dengan PT NETKRIDA dapat dilihat pada Gambar B.1.

Gambar B.1. Presentasi Dengan PT NETKRIDA

LAMPIRAN C
PROSES PERAKITAN

Adapun proses perakita pada penelitian ini dapat dilihat pada Gambar C.1, Gambar C.2, Gambar C.3.

Gambar C.1. Proses Perakitan

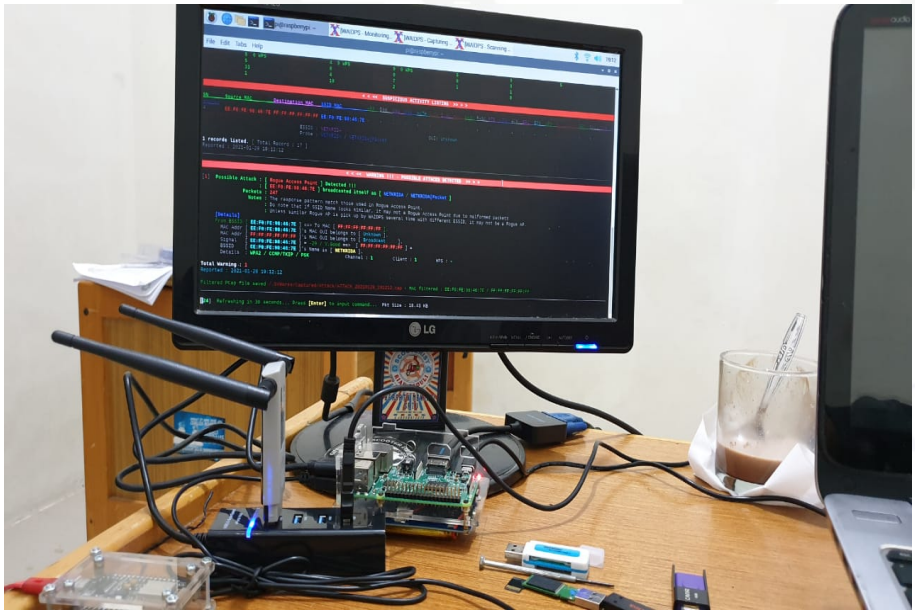
Gambar C.2. Proses Perakitan

Gambar C.3. Proses Perakitan

LAMPIRAN D
HASIL PENGUJIAN

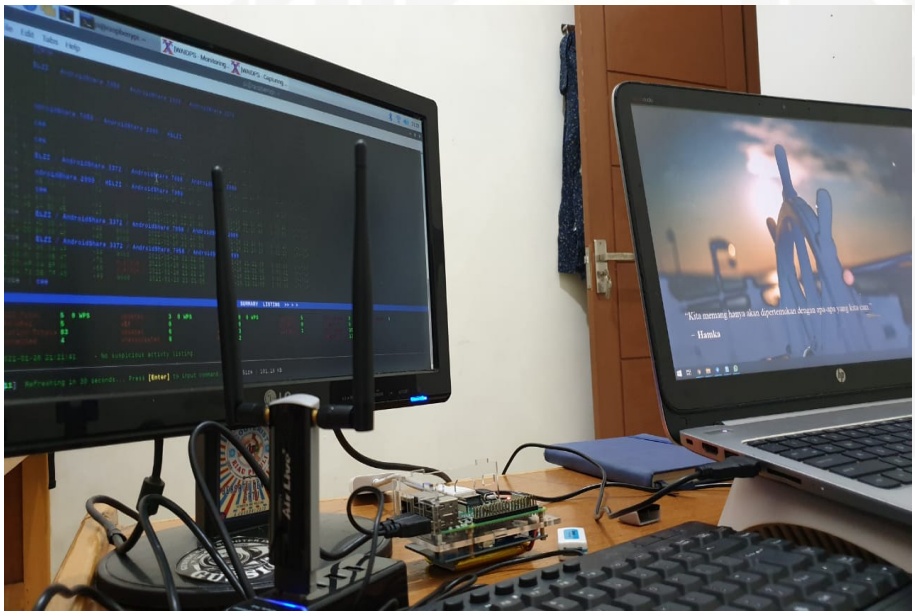
Adapun hasil dari penelitian ini dapat di lihat pada Gambar D.1, Gambar D.2, Gambar D.3, Gambar D.4.

Gambar D.1. Hasil Produk



Gambar D.2. Proses Pengujian

Gambar D.3. Proses Pengujian



Gambar D.4. Proses Pengujian

DAFTAR RIWAYAT HIDUP

Azwir Irvannanda, lahir di kota Pekanbaru, Provinsi Riau pada hari Rabu 22 Februari 1995 M bertepatan dengan 22 Ramadhan 1415 H. Anak pertama dari enam bersaudara dari pasangan Ayah Adnan (Sutan Chaniago) bin Ruslan (Datuak Rajo Basa Nan Kuniang) dan Ibu Zulfarni Binti Abdul Gafar. Penulis menyelesaikan pendidikan sekolah dasar di SD Negeri 016 kecamatan Tampan, kota Pekanbaru pada tahun 2007. Pada tahun yang sama penulis melanjutkan sekolah ke SMP Negeri 23 kota Pekanbaru dan lulus pada tahun 2010, kemudian melanjutkan ke sekolah kejuruan di SMK Negeri 2 kota Pekanbaru, dengan mengambil Jurusan Teknik Komputer dan Jaringan, penulis lulus SMK pada tahun 2013. Pada tahun 2013 penulis melanjutkan pendidikan ke tingkat perguruan tinggi di Universitas Islam Negeri Sultan Syarif Kasim (UIN SUSKA) Riau, Fakultas Sains dan Teknologi, Program Studi Sistem Infromasi. Penulis menyelesaikan studi strata satu (S1) di UIN SUSKA pada tahun 2021 dengan meraih gelar Sarjana Komputer (S.Kom.).