Jurnal ICT Vol V, No. 9, Nov 2014 , 16-23

AKADEMI TELKOM SANDHY PUTRA JAKARTA

FORENSIK JARINGAN PADA LALU LINTAS DATA DALAM JARINGAN HONEYNET DI INDONESIA SECURITY INCIDENT RESPONE TEAM ON INTERNET INFRASTRUCTURE/COORDINATION CENTER

Suyatno Budiharjo[1], Faisal Riyadi[2]
[1,2]Akademi Teknik Telekomunikasi Sandhy Putra Jakarta
[1]suyatno_budihardjo@yahoo.co.id, [2]faisalriyadi93@gmail.com

ABSTRAK

Seiring bertumbuhnya populasi internet yang sangat besar dan signifikan membuat hamper sebagian besar kegiatan dilakukan secara *online*. Berbagai macam kemudahan yang diberikan serta besarnya *sharing data* dalam dunia maya dapat digunakan untuk melakukan transaksi digital dalam kehidupan sehari-hari. Namun seiring perkembangannya yang pesat dalam dunia maya terdapat hal yang perlu di perhatikan yaitu Kejahatan dunia maya (*cybercrime*). *Cybercrime* istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan.

Network forensics berhubungan dengan keamanan, melibatkan pemantauan jaringan untuk lalu lintas anomali dan mengidentifikasi gangguan *network-based* sebagai bukti digital. *Network forensics* juga digunakan untuk melakukan penegakan hukum di dunia maya.

Pada penelitian ini akan dibahas mengenai forensic jaringan untuk memahami proses *network forensics* dan melakukan analisis pada paket data jaringan. Forensik jaringan ini juga berfungsi untuk mengetahui permasalahan yang terjadi pada suatu jaringan agar dapat menegakan hukum di dunia maya serta melakukan pencegahan terhadap *cybercrime*.

Kata Kunci: Internet, Cybercrime, Forensik Jaringan, Jaringan Komputer

ABSTRACT

Internet population grew along with a very large and significant makes almost most of the activity is done online. A wide range of conveniences provided as well as the amount of data sharing in virtual worlds can be used to perform digital transactions in daily life. But along with the rapid development in the virtual world there are things to note that cyber space Crimes (cybercrime). Cybercrime term that refers to the activity of the crime with a computer or network of computers become a tool, target, or the scene of the crime.

Network forensics-related security, involving the monitoring of network traffic for anomalies and identify impaired network-based digital as evidence. Network forensics is also used to conduct law enforcement in cyberspace.

In this research will be discussed regarding the forensic network to understand the process of network forensics and do an analysis on a data packet network. Network forensics is also working to find out the problems that occur on a network in order to uphold the law in cyberspaces as well as perform prevention of cybercrime.

Key Word: Internet, Cybercrime, Network Forensics, Computer Network

1. Pendahuluan

1.1 Latar Belakang

Pada awal mula lahirnya dan dimanfaatkannya internet, dikenal suatu istilah semacam *virtual world* atau *cyber world* untuk menggambarkannya. Dunia maya ini dianggap sebagai sebuah arena interaksi antara mereka yang memiliki "hak eksklusif" penggunaan sistem komputer yang terhubung dalam sebuah jejaring raksasa. Peristiwa historis tersebut secara tidak langsung mewarnai pola pikir manusia di masa-masa awal perkembangan internet, yang mendikotomikan antara dunia nyata dengan dunia maya.

Kemudahan yang disediakan oleh dunia maya semakin tinggi, maka tingkat kriminal yang dapat dilakukan melalui dunia maya. Oleh karena itu dibutuhkan keamanan dalam di dunia maya yang dapat mencari tahu berbagai macam aktifitas yang berhubungan dengan teknologi dunia maya. Dalam ilmu kriminal dikenal istilah forensik, untuk membantu pengungkapan suatu kejahatan melalui pengungkapan bukti-bukti yang sah menurut undang-undang dan peraturan yang berlaku. Seiring dengan kemajuan jaman, berbagai tindakan kejahatan dan kriminal modern dewasa ini melibatkan secara langsung maupun tidak langsung teknologi informasi dan komunikasi. Pemanfaatan komputer, telepon genggam, *email*, internet, *website*, dan lain-lain secara luas dan masif telah mengundang berbagai pihak jahat untuk melakukan kejahatan berbasis teknologi elektronik dan digital. Oleh karena itulah maka belakangan ini dikenal adanya ilmu *digital forensics* yang memdalami kegiatan *forensic* di media elektronikatau digital, *digital forensics* kerap dibutuhkan dan digunakan para penegak hukum dalam usahanya untuk mengungkapkan peristiwa kejahatan melalui pengungkapan bukti-bukti berbasis entitas atau piranti digital dan elektronik.

1.2 Maksud dan Tujuan

Adapun maksud dan tujuan penulisan penelitian ini adalah :

1. Memahami analisa dan proses network forensics.
2. Investigasi packet data jaringan honeynet Id-SIRTII/CC.
3. Menganalisa packet pcap yang terdapat dari jaringan honeynet Id-SIRTII/CC.

1.3 Rumusan Masalah

Dengan memperhatikan identifikasi masalah diatas, maka permasalahan yang akan dipecahkan dalam penulisan penelitian ini adalah :

1. Apa yang dimaksud dengan *Digital Forensics* ?
2. Pengertian dari *Network Forensics*
3. Pengertian *Honeypot* dan *Honeynet*
4. Apa itu wireshark dan konfigurasinya.

1.4 Pembatasan Masalah

Ruang lingkup permasalahan dalam laporan penelitian ini hanya terbatas pada masalah-masalah sebagai berikut:

1. Membahas identifikasi paket data yang di dapat pada jaringan *honeynet* Id-SIRTII/CC.
2. Mengidentifikasi parameter paket data protokol jaringan.
3. Mengidentifikasi parameter serangan pada saat pengambilan lalu lintas data jaringan honeynet Id-SIRTII/CC.
4. Membahas analisis packet data yang di dapat pada jaringan honeynet Id-SIRTII/CC.

2. Dasar Teori

2.1 Digital Forensics

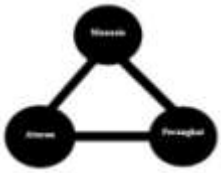
2.1.1 Sejarah *Digital Forensics*

Istilah *digital forensics* awalnya digunakan sebagai sinonim untuk komputer forensik tetapi telah diperluas untuk mencakup penyelidikan dari semua perangkat yang mampu menyimpan digital data.Dengan akar dalam revolusi komputasi pribadi 1970-an dan awal 1980-an, disiplin berkembang secara serampangan selama 1990-an, dan itu tidak sampai awal abad ke-21 bahwa kebijakan nasional muncul.[1] [2]

Selain menemukan bukti langsung dari kejahatan, digital forensik dapat digunakan untuk atribut bukti tersangka tertentu, mengkonfirmasi alibi atau pernyataan, menentukan niat, mengidentifikasi sumber-sumber (misalnya, dalam kasus hak cipta), atau mengotentikasi dokumen.[3] Penyelidikan jauh lebih luas dalam lingkup dari area lain dari analisis forensik (dimana biasa tujuannya adalah untuk memberikan jawaban atas serangkaian pertanyaan sederhana) sering melibatkan waktu-baris kompleks atau hipotesis.[4]

2.1.2 Komponen *Digital Forensics*

Komponen pada digital forensik pada umumnya hampir sama dengan bidang yang lain. Komponen ini mencakup manusia *(people)*, perangkat/peralatan *(equipment)*dan aturan *(protocol)* yang dirangkai, dikelola dan diberdayakan sedemikian rupa dalam upaya mencapai tujuan akhir dengan segala kelayakan dan kualitas sebagaimana bisa dilihat pada gambar berikut: [8]



(Sumber Sulianta Feri. 2008)
Gambar 2.1 Komponen *Digital Forensics*

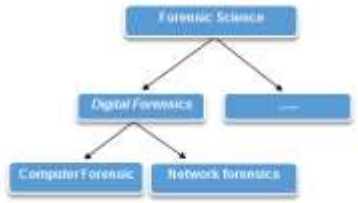
2.1.3 Tahapan pada *Digital Forensics*

Ada berbagai tahapan pada proses implementasi digital forensik. Namun menurut Kemmish [9],secara garis besar dapat diklasifikasikan kepada empat tahapan, yaitu:

1. Identifikasi bukti digital
2. Penyimpanan bukti digital
3. Analisa bukti digital
4. Presentasi

2.2 *Network Forensics*

Network forensics adalah cabang dari *Digital forensics* berkaitan dengan monitoring dan analisis lalu lintas jaringan komputer untuk tujuan pengumpulan informasi, bukti hukum atau deteksi instruksi. [10] Istilah *network forensics* memang di ambil dari terminology yang berhubungan dengan kriminologi. *Network forensics* merupakan kegiatan untuk melakukan pencarian data yang berhubungan dengan kejahatan di lingkungan jaringan komputer.



(Sumber Kurniawan Agus, 2012)
Gambar 2.3 Kedudukan *Network forensics* dalam ilmu *Forensic Science*

2.2.1 Mengapa Perlu *Network forensics*?

Seiring bertumbuhnya populasi internet yang sangat besar dan signifikan membuat hamper sebagian besar kegiatan dilakukan secara *online*. Baik dalam *media social, e-mail, e-banking, mobile banking* dll. Gambaran tersebut menunjukan bahwa teknologi internet menjadi pilar utama dalam operasional hampir seluruh aspek kegiatan sehari-hari.

Dengan bertambahnya kebutuhan yang besar atas jaringan internet, maka kegiatan-kegiatan yang bertujuan jahat seperti *deface, hijacking/cracking, spying, phising, carding,* dsb. Semakin meningkat dengan memanfaatkan jalur jaringan komputer. Mereka merupakan orang-orang yang tidak bertanggung jawab melakukan pencurian data

atau perusakan system dengan *tools* tertentu. Secara teori, walaupun orang-orang ini sudah menghapus jejaknya, baik *log data* maupun log lainnya, kita tetap dapat menganalisis beberapa data yang ditinggalkan system jaringan lainnya. Pada data-data itu selanjutnya dilakukan *forensic analyse*. Kita dapat melakukan *forensic analyse* pada data-data yang ditinggalkan. Pengetahuan tentang data komunikasi beberapa *protocol* jaringan akan menambah kemudahan dalam *forensic analyse* tersebut. [11]

2.2.2 Mengenal Model *Open System Interconnection* (OSI)

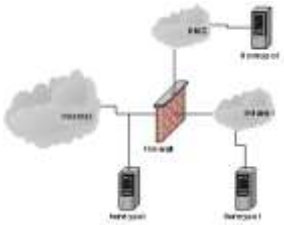
Model *Open System Interconnection* (OSI) telah dikembangkan oleh *International Organization for Standardization* (ISO) sebagai model dari arsitektur komunikasi komputer dan sebagai kerangka kerja untuk pengembangan standar protocol.

2.2.3 Mengenal Arsitektur *TCP/IP*

TCP/IP (singkatan dari *Transmission Control Protocol/Internet Protocol*) adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar- menukar data dari satu komputer ke komputer lain di dalam jaringan Internet. Protokol ini tidaklah dapat berdiri sendiri, karena memang berupa kumpulan protokol (*protocol suite*). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini. Data tersebut diimplementasikan dalam bentuk perangkat lunak (*software*) di sistem operasi. Istilah yang diberikan kepada perangkat lunak ini adalah *TCP/IP stack*. [17]

2.3 Honeynet

Konsep honeynet pertama kali dimulai pada tahun 1999 ketika Lance Spitzner, pendiri Honeynet proyek, menerbitkan karya "*To Build a Honeypot*". Ada beberapa definisi *honeypot* yang disampaikan oleh beberapa peneliti *honeypot* pada jurnal sistem kemanan yang mereka buat maupun dari halaman web. Menurut Lance Spitzner, seorang arsitek sistem keamanan Sun Microsystems,"*A honeypot is security resource whose value lies in being probed, attacked, or compromised*." [20] Definisi ini menjadi acuan beberapa makalah lainnya. Dari definisi itu dapat diambil kesimpulan bahwa *honeypot baru dikatakan suatu sistem keamanan jika honeypot tersebut disusupi, diserang, atau dikendalikan oleh penyerang*. [21]



(Sumber Lance Splitzner, 2002)
Gambar 2.6 Penempatan Honeynet

2.3.1 Tipe dan Kriteria *Honeypots*

Honeypot dibagi menjadi dua tipe dasar, yaitu *production honeypot* dan *research honeypot*. [20]

Penggunaan Honeypot dibedakan dalam 2 (dua) tipe:
1. *Research Honeypots*
2. *Production Honeypots*

Berdasarkan kriteria *honeypot* dapat diklasifikasikan berdasarkan pada tingkat interaksi yang dimilikinya. Tingkat interaksi dapat didefinisikan sebagai tingkat aktivitas *Attacker*/ atau *intruder* di dalam sistem yang diperbolehkan maka semakin tinggi pula tingkat interaksi *honeypot*. [21]

Berikut ini pembagian tingkat interaksi pada penggunaan honeypot:

1. *LOW INTERACTION HONEYPOT*
2. *MEDIUM INTERACTIONHONEYPOT*
3. *HIGH INTERACTIONHONEYPOT*

3. Pembahasan

3.1 Persiapan Dan Pelaksanaan *Network Forensics*

3.1.1 Diagram *Network Forensics*

Pelaksanaan riset *network forensics* yang penulis lakukan di Id-SIRTII/CC. Pelaksanaan riset penulis sebagai *network analyst/investigator* melakukan pengumpulan data dengan metode *reconnaissance*. Selanjutnya melakukan identifikasi data yang diperoleh dan diteruskan dengan melakukan analisa data yang telah di identifikasi yang akan menghasilkan barang bukti berupa data yang di dapatkan setelah melalui beberapa tahap suatu proses agar dapat di presentasikan berbasis digital. Berikut ini merupakan proses pelaksanaan riset *network forensics* yang penulis lakukan di Id-SIRTII/CC

Gambar 3.1 Diagram *Network Forensics*

3.1.2 BaganPelaksanaan Riset *Network Forensics*

Pada proses pelaksanaan riset *network forensics* penulis akan memperlihatkan proses pelaksanaan secara menyeluruh yang penulis gunakan di Id-SIRTII/CC.Berikut proses pelaksanaan secara singkat:

1. Melakukan konfigurasi serta instalasi pada perangkat yang akan digunakan dalam pelaksanaan riset.
2. Mengumpulkan paket data jaringan yang didapatkan dari jaringan honetnet Id-SIRTII/CC.
3. Melakukan analisa terhadap paket yang di dapat, dan.
4. Mempresentasikan hasil analisa yang terjadi selama penelitian

3.2 *Raspberry pi*

3.2.1 Pengenalan *Raspberry PI*

Raspberry Pi (juga dikenal sebagai *RasPi*) adalah sebuah *SBC (Single Board Computer)* seukuran kartu kredit yang dikembangkan oleh *Raspberry PI Foundation* di Inggris (UK) dengan maksud untuk memicu pengajaran ilmu komputer dasar di sekolah-sekolah.

Raspberry Pi menggunakan *system on a chip (SoC)* dari *Broadcom BCM2835*, juga sudah termasuk prosesor *ARM1176JZF-S 700 MHz, GPU VideoCore IV* dan *RAM* sebesar *256 MB* (untuk Rev. B).[24]

3.2.2 Instalasi dan Konfigurasi *Raspberry PI*

Pada penjelasan berikut ini penulis akan menjelaskan tentang cara instalasi *Raspbian OS* dan konfigurasinya pada *raspberry*. *Raspbian* atau lebih dikenal *Debian Wheezy* sendiri merupakan *operating systemlinux arm based* project dari *linux debian*. Penulis menggunakan perangkat *Raspberry PI* karena salah satu syarat yang di izinkan oleh Id-SIRTII/CC dalam pengambilan lalu lintas data di server mereka. Berikut ini gambar *raspberry* yang penulis gunakan dalam riset pengambilan data jaringan *honeynet* Id-SIRTII/CC.

Setelah semua kebutuhan alat riset telah tersedia, hal selanjutnya adalah melakukan instalasi *raspbian os*. Pada saat melakukan riset penulis menggunakan Memory SDHC berukuran 8GB sebagai tempat pengimpanan serta

boot operating system. Berikut ini langkah-langkah dalam melakukan instalasi dan konfigurasinya:

1. Siapkan Memory SDHC minimal berukuran 4GB. Penulis menggunakan 8GB.
2. Download operating system yang dibutuhkan di http://www.raspberrypi.org/downloads/. Penulis menggunakan Debian Wheezy.
3. Download software Win32DiskImager untuk membuat usb boot raspbian. https://launchpad.net/win32-image-writer/+download
4. Ekstrak file *debian wheezy.zip* makan akan mendapatkan file *debian wheezy.img*. Hubungkan *Micro SDHC* ke laptop.
5. Buka aplikasi Win32DiskImager lalu cari *Debian Wheezy.img* yang telah di ekstrak lalu tentukan lokasi *Micro SDHC* dan pilih write dan tunggu hingga proses selesai maka *Micro SDHC* telah terinstal *Raspbian OS* dan siap digunakan.

3.3 Pentest kit installer

3.3.1 Raspberry Pwn

Raspberry Pwn merupakan *package installer* dari pwnie express yang berguna untuk menambah tools keamanan jaringan pada *debian wheezy* dengan basis open source berikut ini tools yang terdapat pada raspberry pwn seperti SET, Fasttrack, kismet, aircrack-ng, nmap, dsniff, netcat, nikto, xprobe, scapy, wireshark, tcpdump, ettercap, hping3, medusa, macchanger, nbtscan, john, ptunnel, p0f, ngrep, tcpflow, openvpn, iodine, httptunnel, cryptcat, sipsak, yersinia, smbclient, sslsniff, tcptraceroute, pbnj, netdiscover, netmask, udptunnel, dnstracer, sslscan, medusa, ipcalc, dnswalk, socat, onesixtyone, tinyproxy, dmitry, fcrackzip, ssldump, fping, ike-scan, gpsd, darkstat, swaks, arping, tcpreplay, sipcrack, proxychains, proxytunnel, siege, sqlmap, wapiti, skipfish, and w3af. [25]

Penulis menggunakan *raspberry pwn* karena lebih mudah untuk menginstall tools keamanan jaringan dan sekaligus wireshark yang akan di pakai sebagai software riset di Id-SIRTII/CC.Berikut ini langkah-langkah instalasi *raspberry pwn* yang penulis lakukan pada saat riset:

1. Buka terminal sebagai root
2. Install git Pwnie Express Github Repository
   pi@raspberry~# apt-get install git
3. Download Raspberry Pwn Installer dari Pwnie Express Github Repository
   pi@raspberry~#git clone https://github.com/pwnieexpress/Raspberry-pwn.git
4. Setelah selesai download buka folder direktori *Raspberry Pwn* dan jalankan *installer script*
   pi@raspberry~#./*INSTALL_raspberry_pwn.sh*
5. Selanjutnya akan muncul konfirmasi untuk melakukan update dan tekan enter untuk melanjutkat proses instalasi dan melakukan update repository.
6. Packet – packet yang akan di install
7. Jika proses install telah selesai maka *raspberry pi* akan melakukan *restart*

3.4 Wireshark

3.4.1 Apa itu Wireshark?

Wireshark adalah sebuah *Network Packet Analyzer* akan mencoba "menangkap" paket paket jaringan dan berusaha untuk menampilkan semua informasi di paket tersebut sedetail mungkin.Kita bi sa mengumpamakan sebuah *Network Packet Analyzer* seba gai alat untuk memeriksa apa yang sebenarnya sedang terjadi di dalam kabel jaringan,Du lunya, tool-tool semacam ini sangatlah mahal harganya atau berbayar. Namun wireshark bisa digunakan secara gratis karena berbasis *open source*. Selain gratis wiresharkdapat berjalan di banyak platform seperti linux, windows, dan Mac OS.

3.4.2 Fitur pada Wireshark

Wireshark dapat dikatakan sebagai *tools* analisis paket data jaringan yang paling sering digunakan dan juga termasuk dalam *tools* yang berguna dalam kegiatan *network forensics*. Berikut ini adalah sebagian fitur pada wireshark:

1. Tersedia dalam platform Unix, Linux, Windows, dan Mac.
2. Dapat melakukan capture packet data jaringan secara real-time.
3. Dapat menampilkan informasi protokol secara lengkap.
4. Packet data dapat disimpan dalam bentuk file dan nantinya dapat dibuka kembali.
5. Pemfilteran packet data jaringan

Daftar yang lebih lengkap tentang fitur interface yang didukung oleh wireshark dapat dilihati di http://wiki.wireshark.org/CaptureSetup/NetworkMedia.

3.4.3 Konfigurasi *Wireshark* pada *Raspberry PI*

Setelah penulis melakukan instalasi wireshark melalu *pentest kit*, selanjutnya penulis akan melakukan sedikit konfigurasi pada wireshark sebelum digunakan untuk melakukan *sniffing* lalu lintas data. Berikut ini langkah-langkah dalam melakukan konfigurasi pada debian wheezy:

1. Buka terminal dan gunakan superuser untuk melakukan konfigurasi pada wireshark.
   pi@raspberry~$ sudo –i
2. Lakukan konfigurasi ulang agar wireshark dapat bekerja dengan baik pada debia wheezy.
   pi@raspberry~# dpkg-reconfigure wireshark-common
3. Langkah berikutnya konfigurasi wireshark agar dapat digunakan oleh mode user
   pi@raspberry~# usermod –a –G wireshark pi
4. Menjalankan wireshark pada *debian wheezy* untuk melakukan sniffing
   pi@raspberry~# wireshark

3.5 Dionaea

3.5.1 Pengenalan *dionaea*

Dionaea adalah salah satu tools honeypot yang mungkin paling terkenal diantara yang lain. Secara garis besar, honeypot dibagi menjadi 3 macam, yaitu *low interaction, medium* dan *high interaction*. *Low interaction* adalah honeypot yang berpura-pura membuka layanan (*service*) komputer seperti *HTTP, FTP, SSH*, dll (contohnya adalah *dionaea, kippo, glastopf*). Sedangkan *high interactionhoneypot* merupakan sebuah sistem operasi sungguhan yang sengaja dibiarkan mempunyai celah keamanan untuk dihack supaya pemilik *honeypot* tahu apa saja yang dieksploitasi oleh para hacker (contoh *high interaction honeypot* adalah HiHat).

3.5.2 Instalasi dan konfigurasi *Dionaea* pada *Raspberry PI*

Berikut ini merupakan langkah-langkah yang dilakukan penulis dalam melakukan instalasi dan konfigurasi dionaea:

1. Buka terminal dan tambahkan source repository
   pi@raspberry~# echo "deb http://packages.s7t.de/raspbian wheezy main" >> /etc/apt/sources.list
2. Langkah berikutnya lakukan update repository
   pi@raspberry~# apt-get update
3. Instal packet yang diperlukan
   pi@raspberry~# apt-get install libglib2.0-dev libssl-dev libcurl4-openssl-dev libreadline-dev libsqlite3-dev libtool automake autoconf build-essential subversion git-core flex bison pkg-config libnl-3-dev libnl-genl-3-dev libnl-nf-3-dev libnl-route-3-dev liblcfg libemu libev dionaea-python dionaea-cython libpcap udns dionaea

4. Melakukan konfigurasi standar pada dionaea
   pi@raspberry~# cp /opt/dionaea/etc/dionaea/dionaea.conf.dist /opt/dionaea/etc/dionaea/dionaea.confchown nobody:nogroup /opt/dionaea/var/dionaea -R
5. Setelah semua langkah selesai jalankan dionaea
   pi@raspberry~#export PATH=$PATH:/opt/dionaea/bin
   dionaea -u nobody -g nogroup -r /opt/dionaea -w /opt/dionaea -p /opt/dionaea/var/dionaea.pid

3.6 Teknik Tapping

3.6.1 Tapping Server

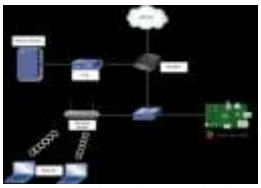
Teknik tapping merupakan salah satu metode yang penulis gunakan dalam melakukan sniffing secara efektif sehingga dapat memperoleh informasi lalu lintas data yang cukup luas di Id-SIRTII/CC. Berikut ini gambar penggunaan teknik tapping pada saat melakukan riset di Id-SIRTII/CC:

Gambar 3.26 Proses Tapping

Gambar 3.26 menunjukan proses tapping yang dilakukan di jaringan honeynet Id-SIRTII/CC dengan menggunakan *raspberry*. Topologi umum honeynet yang digunakan dapat dilihati pada gambar 3.27:

Gambar 3.27 Topologi Umum honeynet Id-SIRTII/CC

Penulis juga menggunakan jaringan *wired-network* dikampus sebagai data pembanding. Berikut ini merupakan topologi yang digunakan pada jaringan *wired-network* Akademi Telkom Jakarta:



Gambar 3.28 Topologi Jaringan Akademi Telkom Jakarta

3.7 *Packet Data* Protokol Jaringan

Protokol jaringan merupakan sebuah aturan atau standart yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih komputer dalam sebuah jaringan. Sedangkan *packet data* merupakan sebuah informasi data yang dibawa pada suatu jaringan. *Packet data* protokol jaringan merupakan salah satu parameter pada pembahasan penulis, berikut ini beberapa protokol jaringan yang ada:

1. *Address Resolution Protocol* (ARP)
2. *Internet Control Message Protokol* (ICMP) *Dynamic Host Configuration Protocol* (DHCP) adalah standar protokol jaringan yang digunakan oleh internet protokol untuk mempermudah pengalokasian alamat *IP* dalam suatu jaringan. [29]
3. *Domain Name System* (DNS
4. *Internet Protocol* (IP)

Pada penjelasan *packet data* protokol jaringan memiliki fungsi kegunaan yang berbeda-beda namun dapat saling berhubungan satu sama lain. Untuk lebih jelasnya mengenai protokol jaringan yang ada dapat digunakan sebagai referensi tambahan dapat dilihat melalui http://en.wikipedia.org/wiki/Internet_protocol_suite.

3.8 Mengenal Jenis-jenis Serangan pada Jaringan

Seiring besarnya perkembangan dunia maya dengan kemudahan dalam mengakses dan berbagi sumber data. Maka berkembang pula kejahatan yang ada dalam dunia maya tersebut. Berikut ini sedikit pengenalana tentang jenis-jenis serangan/gangguan pada suatu jaringan yang penulis gunakan sebagai parameter suatu kejadian:

1. *Denial Of Service* (DOS) dan *Distributed Denial Of Service* (DDoS)
2. *ARP spoofing* (*Poisoning*)
3. *DNS redirection*
4. *Ping Flood*
5. *Man In The Middle Attack*

Pada penjelasan mengenal tentang jenis-jenis serangan yang terjadi pada suatu jaringan dapat di ketahui bahwa banyak juga kekurangan yang ada pada perkembangan dunia maya. Dari beberapa parameter serangan ini yang nantinya akan penulis bahas pada bab berikutnya. Untuk lebih jelasnya lagi tentang banyaknya jenis-jenis serangan dapat dilihat pada http://en.wikipedia.org/portal:Computer_Security.

3.9 Parameter-parameter analisis jaringan honeynet

Pada pelaksaaan analisis lalu lintas data dalam jaringan honeynet di Id-SIRTII/CC penulis menggunakan parameter-parameter berikut sebagai batasan masalah:

1. Melakukan klasifikasi dan analisis paket data protocol jaringan yang di dapat.
2. Parameter pengukuruan jumlah serangan yang terjadi pada saat pengambilan lalu lintas data dalam jaringan honeynet.
3. Melakukan identifikasi jenis-jenis serangan yang terjadi pada saat pengambilan lalu lintas data dalam jaringan honeynet.
4. Melakukan identifikasi efek yang terjadi terhadap lalu lintas data tersebut.

4. Analisis Lalu Lintas Data Dalam Jaringan Honeynet

4.1 Analisa Paket Data Protokol Jaringan

Setelah melihat data yang didapatkan penulis baik dari lalu lintas data dalam jaringan *honeynet* di Id-SIRITII//CC dan jaringan *wired-network* Akademi Telkom Jakarta penulis mendapatkan beberapa jenis serangan paket data protokol jaringan yang paling banyak menjadi serangan pada jaringan. Berikut ini analisa serangan paket data protokol jaringan:

1. Serangan *Ping flood*

4.1 Serangan *Ping Flood* melalui protokol jaringan *ICMP*

Serangan di atas menunjukan bahwa penyerang berulang kali melakukan *ICMP Echo Request* kepada jaringan honeynet dalam jumlah serangan tertentu. Serangan pertama memiliki panjang data sebanyak 300 kali dengan besar paket data 800 bytes dan pada serangan kedua sebanyak 320 kali dengan besar paket data 6500 bytes. Sebuah *ICMP Echo Request* memiliki normal paket data 32 bytes sesuai dengan *RFC 792, Internet Control Message Protocol*.

2. Serangan *TCP Flood*

4.4 Serangan *TCP Flood* melalui protokol jaringan *TCP*

Pada *traffic* gambar 4.4 dapat dilihat telah terjadi permintaan paket *syn* dikirimkan oleh komputer penyerang secara berulang-ulang melalui port yang berbeda mencoba untuk melakukan koneksi dengan jaringan *honeynet* di Id-SIRTII/CC dengan jumlah data *window size value* 8192. Namun saat jaringan honeynet ingin melakukan balasan dengan *syn ack* tidak dapat melakukan balasan tersebut sehingga membuat *window size value* menjadi 0. Seharusnya *window size value* bertambah sesuai dengan balasan data dari jaringan honeynet. Aturan ini sudah baku dan di atur dalam *RFC 813,Windows and Acknowledge Strategy in TCP*.

3. Serangan *UDP Flood*

4.7 Serangan *UDP Flood* melalui protokol jaringan *UDP*

Pada *traffic* serangan gambar 4.7 penyerang melakukan pengiriman secara terus menerus ke dalam jaringan *honeynet* melalui *source port* yang berbeda-beda dengan paket data sebesar 29 bytes menuju *destination port* 80. Paket data tersebut berisikan signature dari penyerang tersebut kalimat berupa "*Bring it down – stress tester"*. Serangan ini teridentifikasi berjumlah 19751 kali pada lalu lintas data dalam jaringan honeynet di Id-SIRTII/CC 2.

4.2 Jumlah Paket Data Dalam Jaringan *Honeynet*

Berikut ini data hasil riset pada lalu lintas data protokol jaringan honeynet di Id-SIRTII/CC yang penulis dapatkan selama pengambilan riset data. Data ini berupa keluaran hasil sniffing lalu lintas data jaringan honeynet di Id-SIRTII/CC pada tanggal 25-04-2014 yang di ambil menggunakan raspberry pi dengan *tools wireshark* 1.8.2 saat pengambilan data berlangsung dan menghasilkan format data dalam bentuk pcap yang merupakan salah satu format keluaran dari *tools wireshark*. Penulis mendapatkan dua paket data jaringan honeynet Id-SIRTII/CC dalam bentuk pcap. Berikut ini paket data jaringan yang penulis dapatkan:

4.11 Grafik lalu lintas data jaringan *honeynet* di Id-SIRTII 1

Pada gambar 4.11 merupakan grafik dari lalu lintas data jaringan honeynet di Id-SIRTII/CC dari hasil sniffing menggunakan raspberry pi. Data yang pertama di ambil pada tanggal 25-04-2014 selama 10 menit pukul 15.10 - 15.20 sore. Grafik tersebut menunjukan banyaknya lalu lintas data yang terjadi pada saat proses sniffing pertama dengan penjelasan berdasarkan banyaknya paket data protokol jaringan yang didapatkan sesuai dengan lamanya waktu pengambilan data selama 10 menit sedangkan kode warna pada grafik tersebut merupakan data protokol jaringan yang ada. Berikut ini penjelasan mengenai kode warna pada gambar 4.10:

1. Hitam adalah protokol jaringan *ARP*
2. Merah adalah protokol jaringan *HTTP*
3. Hijau adalah protokol jaringan *ICMP*
4. Biru adalah protokol jaringan *TCP*
5. Ungu adalah protokol jaringan *UDP*

4.1 Jumlah paket data jaringan honeynet di Id-SIRTII 1

Lalu lintas data honeynet 1	
Protokol	Paket data
ARP	32
DNS	14
HTTP	2329
ICMP	345
ICMPV6	1
IPV6	50
NTP	3
SIP	6
SNMP	24
TCP	5508
UDP	7083
JUMLAH	15395

Pada table 4.1 dapat dilihat pada proses pengambilan lalu lintas data yang pertama dalam jaringan honeynet di Id-SIRTII/CC selama 10 menit penulis mendapatkan 15392 paket data protokol jaringan. Pada proses sniffing selanjutnya penulis mendapatkan grafik lalu lintas data yang lebih padat karena proses waktu sniffing yang lebih lama 25 menit selama pengambilan data yang kedua dalam jaringan honeynet di Id-SIRTII/CC.

4.12 Grafik lalu lintas data jaringan honeynet di Id-SIRTII 2

Pada gambar 4.12 dapat terlihat jelas meningkatnya paket data protokol jaringan yang

didapatkan pada lalu lintas data yang di ambil pada tanggal tanggal 25-04-2014 selama 25 menit pukul 15.25 - 15.50 sore. Grafik pada gambar 4.5 memiliki kode warna yang sama dengan sebelumnya karena protokol jaringan yang paling aktif pada proses pengambilan data tersebut masih sama namun mengalami peningkatan yang sangat besar.

4.2 Jumlah paket data jaringan honeynet di Id-SIRTII 2

Lalu lintas data honeynet 2	
Protokol	Paket data
ARP	224
CDP	12
HTTP	2803
ICMP	545
ICMPV6	8
IPV6	380
MNDP	12
SIP	29
SNMP	265
TCP	39293
UDP	86287
JUMLAH	129858

Pada table 4.2 dapat dilihat pada proses pengambilan lalu lintas data yang kedua dalam jaringan honeynet di Id-SIRTII/CC selama 25 menit penulis mendapatkan 15392 paket data protokol jaringan.

Kesimpulan dari dua data riset lalu lintas data jaringan honeynet di Id-SIRTII/CC dapat di lihat perbedaan yang signifikan dari lama waktu pengambilan data dan banyaknya data yang didapatkan pada Jumlah paket data jaringan honeynet di Id-SIRTII 1 sebanyak 15395 paket data selama 10 menit dan Jumlah paket data jaringan honeynet di Id-SIRTII 2 sebanyak 129858 paket data selama 25 menit.

4.13 Grafik lalu lintas data jaringan Akademi Telkom Jakarta

Pada gambar 4.12 merupakan grafik *traffic* dari lalu lintas data jaringan *wired-network* dengan kode warna yang sama pada *traffic* dari lalu lintas data jaringan honeynet di Id-SIRTII namun paket data protokol jaringan yang di peroleh sangat jauh berbeda. Berikut ini jumlah paket data protokol jaringan yang penulis dapat dari jaringan *wired-network* Akademi Telkom Jakarta:

4.3 Jumlah paket data jaringan Akademi Telkom Jakarta

Lalu lintas data kampus	
Protokol	Paket data
ARP	14
ICMP	541
TCP	9653
UDP	1835
JUMLAH	12043

4.3 Jumlah Serangan Pada Lalu Lintas Data Dalam Jaringan Honeynet

Proses ini merupakan salah satu parameter pengukuran jumlah serangan yang terjadi selama pengambilan lalu lintas data dalam jaringan honeynet di Id-SIRTII/CC. Hasil dari pengukuran ini berupa grafik kolom jumlah serangan pada waktu pengambilan lalu lintas data jaringan *honeynet*. Berikut ini grafik serangan yang terjadi selama pengambilan lalu lintas data dalam jaringan honeynet berdasarkan berapa banyaknya kejadian serangan yang terjadi pada lalu lintas data tersebut:

4.14 Jumlah serangan lalu lintas data dalam jaringan honeynet di Id-SIRTII 1

Sedangkan pada proses pengambilan data yang kedua terjadi peningkatan yang sangat besar ini dikarenakan lebih lamanya pengambilan data pada jaringan aktif selama 25 menit. Berikut ini grafik serangan yang terjadi selama pengambilan lalu lintas data dalam jaringan honeynet berdasarkan berapa banyaknya kejadian serangan yang terjadi pada lalu lintas data yang kedua:

4.15 Jumlah serangan lalu lintas data dalam jaringan honeynet di Id-SIRTII 2

Dari kedua data jumlah serangan pada pengambilan data yang pertama dan kedua dalam jaringan honeynet di Id-SIRTII/CC dapat terlihat perbedaan jumlah serangan yang didapatkan. Jenis serangan tersebut dapat diidentifikasikan dari kedua data selama pengambilan data berlangsung yaitu:

5 *HTTP flood* melalui paket data protokol jaringan *HTTP*.
6 *Ping flood* melalui paket data protokol jaringan *ICMP*.
7 *SYN flood* melalui paket data protokol jaringan *TCP*.
8 *UDP flood* melalui paket data protokol jaringan *UDP*.

Kesimpulan dari kedua data riset lalu lintas data jaringan honeynet di Id-SIRTII dapat dilihat dari golongan atau tipe honeynet yang termasuk dalam *production honeypot* karena tipe ini digunakan oleh suatu institusi baik pemerintah atau swasta sebagai bagian dari infrastruktur keamanan untuk mengukur tingkat keamanan suatu institusi. [20]

4.16 Jumlah serangan lalu lintas data jaringan Akademi Telkom Jakarta

Pada gambar 4.16 dapat dilihat hasil simulasi serangan yang penulis lakukan terhadap jaringan Akademi Telkom Jakarta. Karena keterbatasan jaringan serangan paket data protokol jaringan yang penulis dapatkan sesuai dengan ketahanan jaringan tersebut. Berikut ini serangan yang teridentifikasi pada simulasi serangan yang penulis lakukan pada jaringan *wired-network* Akademi Telkom Jakarta:

1. Serangan melalui paket data protokol jaringan *ICMP* sebanyak 116 kali.
2. Serangan melalui paket data protokol jaringan *TCP* sebanyak 9208 kali.
3. Serangan melalui paket data protokol jaringan *UDP* sebanyak 1771 kali.

5. Penutup

5.1 Kesimpulan

Kesimpulan yang dapat penulis ambil dari forensik jaringan pada lalu lintas data dalam jaringan*honeynet* di Id-SIRTII adalah sebagai berikut:

1. *Network forensics* diperlukan untuk mengungkapkan kejadian yang berlangsung dalam lalu lintas jaringan komputer baik *traffic* yang normal maupun *traffic* serangan pada jaringan tersebut.
2. Serangan yang didapatkan pada lalu lintas data dalam jaringan *honeynet* di Id-SIRTII/CC yang pertama sebanyak 2100 paket data. Pada serangan yang kedua sebanyak 26371 paket data. Dan data simulasi serangan pada jaringan *wired-network* Akademi Telkom Jakarta sebanyak 9324. Perbedaan ini dapat terjadi karena lamanya waktu pengambilan data, ketahanan dari jaringan tersebut, dan banyaknya traffic serangan yang berlangsung pada jaringan tersebut.
3. Saat terjadi serangan dalam jaringan honeynet di Id-SIRTII/CC tidak mempengaruhi jaringan sebenarnya karena honeynet merupakan sistem tiruan yang disiapkan untuk mengumpulkan log dari penyerang. Sedangkan pada simulasi yang dilakukan dengan *wired-network* Akademi Telkom Jakarta perangkat langsung terkena dampak dari serangan tersebut karena tidak memiliki pertahanan pendukung untuk menangkal serangan tersebut.
4. *Honeynet* di Id-SIRTII/CC termasuk dalam golongan *production honeypot* karena tipe ini digunakan oleh suatu institusi baik pemerintah atau swasta sebagai bagian dari infrastruktur keamanan untuk mengukur tingkat keamanan suatu institusi.
5. Serangan yang teridentifikasi pada lalu lintas data dalam jaringan honeynet di Id-SIRTII/CC melalui paket data protokol jaringan adalah
   1) Lalu lintas data pertama *ICMP* sebanyak 300 kali dan *TCP* sebanyak 1800 kali.
   2) Lalu lintas data kedua *HTTP* sebanyak 288 kali, *ICMP* sebanyak 320 kali, *TCP* sebanyak 6072 kali, dan *UDP* sebanyak 19751 kali.
   3) Data hasil simulasi serangan di Akademi Telkom Jakarta sebanyak *ICMP* sebanyak 116 kali, *TCP* sebanyak 9208 kali, *UDP* sebanyak 1771 kali.
6. Serangan – serangan tersebut adalah *ping flood, tcp flood, http flood* dan *udp flood*. Keempatnya termasuk dalam kategori serangan *DoS attack* (*Denial of Service*) merupakan serangan yang membuat korban baik *server* atau *client* menjadi sangat sibuk melayani permintaan dari penyerang sehingga *resource* yang dimilliki oleh *sever* atau *client* tersebut habis.
7. Pencegahan terhadap serangan – serangan tersebut dapat dilakukan dengan cara Mengalihkan serangan dengan menggunakan sistem *honeypot*.
8. Membangun *IDS (Instrusion Detection System)* untuk mendeteksi aktifitas jaringan yang tidak normal.
9. Selalu mengupdate sistem keamanan serta sistem operasi yang digunakan dan menggunakan hardware yang mendukung keamanan jaringan computer.
10. Selalu menggunakan aplikasi dan sistem operasi yang legal bukan bajakan.
11. Menggunakan keamanan jaringan tambahan secara online untuk pertahanan keamanan yang lebih baik dengan biaya tertentu.
12. Bekerja sama dengan ISP untuk mencegah paket dari IP yang dicurigai serta menggunakan layanan tambahan proteksi dari *ddos attack* sebelum masuk ke jaringan pelangganya.

5.2 Saran

Saran-saran dari penulis mengenai forensik jaringan pada lalu lintas data dalam jaringan honeynet di Id-SIRTII/CC adalah sebagai berikut:

1. Dalam melakukan pengumpulan lalu lintas data jaringan dapat melakukan dengan 2 metode yaitu tapping dan port mirroring.
2. Pengumpulan lalu lintas data jaringan harus dilakukan secara legal dengan izin yang telah diberikan.
3. Penggunaan perangkat pengumpulan data juga harus mendapatkan izin dan merupakan perangkat yang legal.
4. *Software* serta aplikasi pengumpulan data merupakan aplikasi yang legal bukan merupakan aplikasi bajakan.

DAFTAR PUSTAKA

[1] M Reith, C Carr, G Gunsch (2002). *"An examination of digital forensic models".International Journal of Digital Evidence*. Retrieved 2 August 2010.

[2] Carrier, B (2001). *"Defining digital forensic examination and analysis tools". Digital Research Workshop II*. Retrieved 2 August 2010.

[3] Various (2009). Eoghan Casey, ed. *Handbook of Digital Forensics and Investigation*. Academic Press. p. 567. ISBN 0-12-374267-6. Retrieved 27 August 2010.

[4] Carrier, Brian D (7 June 2006). *"Basic Digital Forensic Investigation Concepts"*

[5] Undang-undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Bab III Informasi Dokumen dan Tanda Tangan Elektronik pasal 5 ayat 1. 2009. Yogyakarta: Pustaka Yustisia.

[6] Marcella, A. J. & Greenfiled, R. S. 2002. *"Cyber Forensics a field manual for collecting, examining, and preserving evidence of computer crimes"*, Florida: CRC Press LLC.

[7] Digital Forensics. (https://en.wikipedia.org/wiki/Digital_forensics) di akses 28 April 2014

[8] Sulianta, Feri (2008). Komputer Forensic. Elex Media Komputindo

[9] Kemmish, R. M. *What is forensic computer*, Australian institute of Criminology, Canberra (http://:www.aic.gov.au/publications/tandi/ti118.pdf).

[10] Gary Palmer, *A Road Map for Digital Forensic Research*, *Report from DFRWS* 2001, *First Digital Forensic Research Workshop*, Utica, New York, August 7 – 8, 2001, Page(s) 27–30