



SISTEM MONITORING SERANGAN JARINGAN KOMPUTER BERBASIS *WEB SERVICE* MENGGUNAKAN *HONEYPOT* SEBAGAI *INTRUSION PREVENTION SYSTEM*

Inda Sari¹, Muh Yamin^{*2}, LM. Fid Aksara^{*3}

^{1,*2,*3}Jurusan Teknik Informatika, Fakultas Teknik, Universitas Halu Oleo, Kendari
e-mail : ¹inenginds@gmail.com, ^{*2}muh_yamin@uho.ac.id, ^{*3}fidaksara@uho.ac.id

Abstrak

Keamanan sangat penting terlebih untuk menjaga integritas dari suatu data bagi pengguna layanan internet. Banyak cara untuk melakukan penyusupan jaringan komputer, berawal dari sekedar mencoba-coba hingga berusaha merusak dan mencuri informasi penting pada *server*. Salah satu cara untuk mengatasi permasalahan ini yaitu dengan adanya sebuah sistem pencegah serangan atau biasa disebut dengan metode *Intrusion Prevention System* (IPS) agar suatu serangan yang ada tidak bisa langsung menyentuh data atau *file* yang tidak seharusnya diketahui oleh orang lain.

Honeypot merupakan sistem yang sengaja dikorbankan agar diserang untuk memperoleh informasi dari kegiatan penyerang serta mengetahui metode yang digunakan dalam menyerang suatu sistem. Hasil serangan terhadap sistem tersebut dapat ditampilkan dalam sebuah sistem *monitoring* dan dapat pula ditampilkan melalui *Web Service*. Hasil yang didapatkan dari penelitian ini bahwa pembuatan sistem *monitoring* serangan jaringan komputer berbasis *Web Service* menggunakan *Honeypot* sebagai IPS berhasil diterapkan. Serangan yang masuk melalui *port* TCP adalah sebanyak 33,96%, UDP 33,96%, dan ICMP 32,07%.

Kata Kunci—*Honeypot, Web Service, Intrusion Prevention System*

Abstract

Security is very important especially to maintain the integrity of data for internet service users. There are many ways to infiltrate computer networks, starting from just experimenting to trying to damage and steal important information on the server. One way to overcome this problem is by the existence of an attack prevention system or commonly referred to as the Intrusion Prevention System (IPS) so that an attack can not directly touch the data or files that others should not know.

Honeypot is a system that is deliberately sacrificed in order to be attacked to obtain information from the activities of the attacker and to know the methods used in attacking a system. The results of attacks on the system can be displayed in a monitoring system and can also be displayed through a Web Service. The results obtained from this study that the creation of a Web Service -based computer network attack monitoring system uses a Honeypot as an IPS successfully implemented. Attacks that enter through TCP ports are 33.96%, UDP 33.96%, and ICMP 32.07%.

Keywords— *Honeypot, Web Service, Intrusion Prevention System*

1. PENDAHULUAN

Perkembangan teknologi sangatlah pesat terutama dalam teknologi komunikasi dan informasi. Seiring dengan

perkembangan teknologi informasi tersebut menjadikan keamanan suatu informasi sangatlah penting terlebih lagi pada suatu jaringan yang terkoneksi dengan internet. Di jaman sekarang, jaringan komputer bukanlah



sesuatu yang baru, hampir semua layanan digital menggunakan jaringan komputer [1]. Pada saat jaringan internet sudah digunakan orang di berbagai belahan bumi, selain membawa dampak positif, internet juga mempunyai dampak negatif, yang menimbulkan masalah baru yang sangat mengancam yaitu masalah keamanan jaringan itu sendiri.

Keamanan sangat penting terlebih untuk menjaga integritas dari suatu data bagi pengguna layanan internet. Banyak cara untuk melakukan penyusupan jaringan komputer, berawal dari sekedar mencoba-coba hingga berusaha merusak dan mencuri informasi penting pada *server*. Banyak hal untuk melakukan pengamanan pada jaringan komputer, diantaranya diperlukan perangkat yang mendukung dan juga sumber daya manusia yang mampu menyelesaikan setiap masalah keamanan dari jaringan komputer.

Salah satu cara untuk mengatasi permasalahan ini yaitu dengan adanya sebuah sistem pencegah serangan atau biasa disebut dengan metode *Intrusion Prevention System* (IPS) agar suatu serangan yang ada tidak bisa langsung menyentuh data atau *file* yang tidak seharusnya diketahui oleh orang lain. IPS merupakan pengembangan dari *Intrusion Detection System* (IDS). *Honeypot* dapat diterapkan untuk memperoleh informasi-informasi dari kegiatan penyerang, serta mengetahui metode yang digunakan dalam menyerang suatu sistem sehingga dapat dilakukan tindakan pencegahan terhadap sistem yang dilindungi sebenarnya [2]. Informasi yang diperoleh dari kegiatan peretasan tersebut dapat digunakan sebagai laporan Administrator jaringan dengan ditampilkan pada sebuah *web monitoring*. Selain itu, hasil *log* serangan dapat ditampilkan melalui *Web Service* agar semua orang dapat melihat hasil dari *log* serangan tersebut tanpa mengakses *database* dan *web monitoring* secara langsung.

Berdasarkan permasalahan tersebut, maka Penulis melakukan penelitian yang berjudul “Sistem Monitoring Serangan Jaringan Komputer Berbasis *Web Services* Menggunakan *Honeypot* sebagai *Intrusion Prevention System* (IPS)”.

2. METODE PENELITIAN

2.1 Jaringan Komputer

Menurut Forouzan di dalam bukunya yang berjudul *Computer Network A Top Down Approach*, disebutkan bahwa jaringan komputer adalah hubungan dari sejumlah perangkat yang dapat saling berkomunikasi satu sama lain. Perangkat yang dimaksud pada definisi ini mencakup semua jenis perangkat komputer (komputer desktop, laptop, *smartphone*, PC, *tablet*) dan perangkat penghubung [1].

Selain itu, jaringan komputer adalah interkoneksi antara 2 komputer *autonomous* atau lebih, yang terhubung dengan media transmisi kabel atau tanpa kabel (*wireless*). *Autonomous* adalah apabila sebuah komputer tidak melakukan kontrol terhadap komputer lain dengan akses penuh, sehingga dapat membuat komputer lain, *restart*, *shutdowns*, kehilangan *file* atau kerusakan sistem [3].

2.2 *Intrusion Prevention System* (IPS)

IPS adalah pendekatan yang sering digunakan untuk membangun sistem keamanan komputer dengan mengkombinasikan teknik *firewall* dan metode IDS dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang akan masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket. disaat serangan telah teridentifikasi, IPS akan menolak akses (*block*) dan mencatat (*log*) semua paket data yang teridentifikasi tersebut. Jadi IPS bertindak seperti layaknya *firewall* yang akan melakukan, mengizinkan dan *block* yang dikombinasikan seperti IDS yang dapat mendeteksi paket secara detail. IPS menggunakan *signatures* untuk mendeteksi aktivitas lalu lintas data di jaringan dan terminal, dimana pendeteksian paket yang masuk dan keluar (*inbound-outbound*) dapat dicegah sedini mungkin sebelum merusak atau mendapatkan akses ke dalam jaringan lokal [4].

Secara umum, ada dua jenis IPS, yaitu *Host-Based Intrusion Prevention System* (HIPS) dan *Network-Based Intrusion Prevention System* (NIPS) [5].

1. *Host-Based Intrusion Prevention System (HIPS)*

HIPS adalah sama seperti halnya *Host-Based Intrusion Detection System (HIDS)*. Program agen HIPS dipasang secara langsung di sistem yang diproteksi untuk dimonitor aktivitas sistem internalnya. HIPS juga bisa memantau aliran data dan aktivitas pada aplikasi tertentu.

Sebagai contoh penggunaan HIPS yaitu misalnya untuk mencegah *intrusion* pada *web server*. Dari sisi keamanan mungkin solusi HIPS bisa mencegah datangnya ancaman terhadap *host*. Tetapi dari sisi *performance*, harus diperhatikan apakah HIPS memberikan dampak negatif terhadap *performance host*, karena memasang sistem keamanan HIPS pada sistem operasi mengakibatkan penggunaan sumber daya komputer *host* menjadi semakin besar.

2. *Network-Based Intrusion Prevention System (NIPS)*

NIPS tidak melakukan pantauan secara khusus pada satu *host* saja tetapi melakukan pantauan dan proteksi dalam satu jaringan secara global. NIPS menggabungkan fitur IPS dengan *firewall* dan kadang disebut sebagai *in-line IDS* atau *Gateway Intrusion Detection System (GIDS)*.

Sistem kerja IPS yang populer yaitu pendeteksian berbasis *signature*, pendeteksian berbasis anomali, dan *monitoring* berkas-berkas pada sistem operasi *host*. Sistematis IPS yang berbasis *signature* adalah dengan cara mencocokkan lalu lintas jaringan dengan *signature database* milik IPS yang berisi *attacking rule* atau cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Sistematis IPS yang berbasis anomali adalah dengan cara melibatkan pola-pola lalu lintas jaringan yang pernah terjadi. Umumnya, dilakukan dengan menggunakan teknik statistik. Teknik lain yang digunakan adalah dengan cara melakukan *monitoring* berkas-berkas sistem operasi pada *host*. IPS akan melihat apakah adapercobaan untuk mengubah beberapa berkas sistem operasi, utamanya berkas log.

2.3 *Honeypot*

Honeypot merupakan sebuah sistem atau komputer yang sengaja dijadikan umpan untuk menjadi target serangan dari penyerang (*attacker*). Komputer tersebut melayani

serangan yang dilakukan oleh *attacker* dalam melakukan penetrasi terhadap *server* tersebut. *Honeypot* akan memberikan data palsu apabila ada aktifitas yang tidak biasa yang akan masuk ke dalam sistem atau *server*. Secara teori *Honeypot* tidak akan mencatat *traffic* yang legal, sehingga dapat dilihat bahwa yang berinteraksi dengan *Honeypot* adalah *user* yang menggunakan sumber daya sistem yang digunakan secara ilegal. Jadi *Honeypot* seolah-olah menjadi sistem yang berhasil disusupi oleh *attacker*, padahal penyerang tidak masuk ke sistem sebenarnya, tetapi masuk ke sistem yang palsu [6].

2.4 *Web Service*

Web Service merupakan sebuah sistem perangkat lunak yang didesain untuk mendukung interaksi mesin ke mesin di dalam sebuah jaringan komputer. *Intercafe* suatu *Web Service* diuraikan dalam sebuah format *machine-processible* seperti *Web Service Description Language (WSDL)*. Pada umumnya pesan ini melalui HTTP dan XML yang merupakan salah satu standar dari *web*.

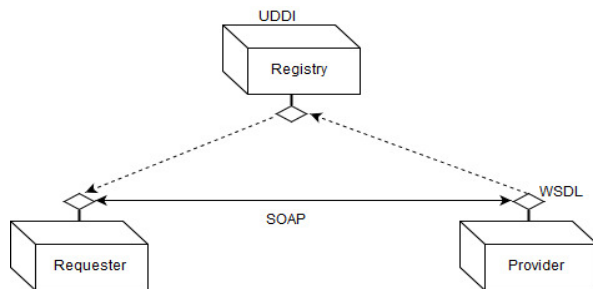
Web Service secara teknis memiliki mekanisme interaksi antar sistem sebagai penunjang interoperabilitas, baik berupa agregasi (pengumpulan) maupun sindikasi (penyatuan). *Web Service* memiliki layanan terbuka untuk kepentingan integrasi data dan kolaborasi informasi yang bisa diakses melalui internet dengan berbagai pihak menggunakan teknologi yang dimiliki oleh masing-masing pengguna. Sekalipun mirip dengan *Application Programming Interface (API)* berbasis *web*, *Web Service* lebih unggul karena dapat dipanggil dari jarak jauh melalui internet. Pemanggilan *Web Service* bisa menggunakan bahasa pemrograman apa saja dan dalam *platform* apa saja, sementara API hanya bisa digunakan dalam *platform* tertentu.

Konsep arsitektur yang mendasari teknologi *Web Service* adalah *Service Oriented Architecture (SOA)*. SOA mendefinisikan 3 peran berbeda yang menunjukkan peran dari masing-masing komponen dalam sistem, yaitu:

1. *Service Provider*, yaitu suatu entitas yang menyediakan *interface* terhadap sistem yang akan menjalankan suatu sekumpulan tugas tertentu.
2. *Service Requestor*, yaitu suatu entitas yang meminta/memperoleh (dan menentukan) *software service* dalam rangka

menyelesaikan tugas dan menyediakan solusi bisnis tertentu.

3. *Service Registry*, yaitu entitas yang bertindak sebagai penyimpan (*repository*) suatu *software service* yang dipublikasikan oleh *service provider*. Arsitektur *Web Service* dapat dilihat pada Gambar 1.



Gambar 1 Arsitektur *Web Service*

2.5 Port Number

Nomor *port* (*port number*) merupakan sejumlah angka biner sepanjang 16-bit yang berfungsi sebagai nomor untuk layanan yang digunakan di dalam jaringan komputer. Nomor *port* pada jaringan komputer diperkenalkan pertama kali oleh pasangan *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP) sebagai dua buah pasangan protokol yang telah ada di dalam jaringan komputer sejak jaringan komputer itu pertama kali diciptakan. Kedua pasangan protokol ini berada pada *Transport Layer*.

Jaringan komputer mengenal tiga jenis klasifikasi atau kelompok utama untuk nomor *port*. Ketiga kelompok untuk penomoran *port* di dalam jaringan komputer tersebut meliputi *Well Known Port*, *Dynamic Port*, dan *Registered Port*.

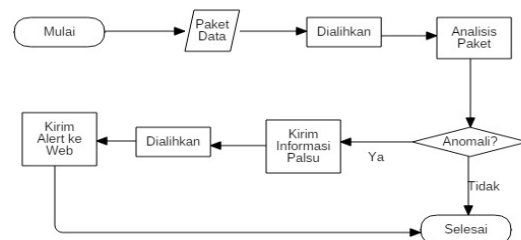
2.6 Protokol Jaringan

Protokol jaringan didefinisikan sebagai aturan dan format standar yang mengatur proses komunikasi, pengiriman dan penerimaan pesan, pembacaan pesan, serta mengkoordinasikan semua komputer yang terhubung di dalamnya. Protokol tidak hanya sebagai sebuah ataupun sekumpulan aturan saja, tetapi sebagai format standar pada jaringan komputer untuk memudahkan di dalam proses komunikasi transfer data, dan koneksi. Oleh karena itu protokol berada di semua *layer* pada permodelan *OSI layer* di dalam jaringan komputer dan memiliki fungsinya masing-masing [1].

Protokol memberikan banyak sekali manfaat di dalam jaringan komputer, baik dalam bentuk layanan, integrasi dengan aplikasi, dan kemudahan bagi pengembang aplikasi. Beberapa protokol pada jaringan komputer diantaranya yaitu *File Transfer Protocol* (FTP), *User Datagram Protocol* (UDP), dan *Internet Control Message Protocol* (ICMP).

2.7 Gambaran Umum Sistem

Gambaran umum sistem merupakan penjelasan umum dari proses sistem yang akan dibangun. Gambar 2 menunjukkan gambaran sistem keamanan yang akan dibangun menggunakan *Honeypot*. Berdasarkan pada Gambar 2, setiap paket data yang ada akan dialihkan ke *server* palsu, karena selama sistem *Honeypot* aktif, maka selama itu pula *IP server* akan disamarkan. Paket yang masuk kemudian dianalisis, jika dianggap sebagai anomali maka akan diberikan respon informasi palsu untuk penyerang lalu dialihkan, lalu sistem memberikan *alert* ke *web* dan selesai. Namun, jika paket tidak dianggap sebagai serangan maka proses langsung selesai.



Gambar 2 Gambaran Umum Sistem

2.8 Rancangan Use Case Diagram Sistem

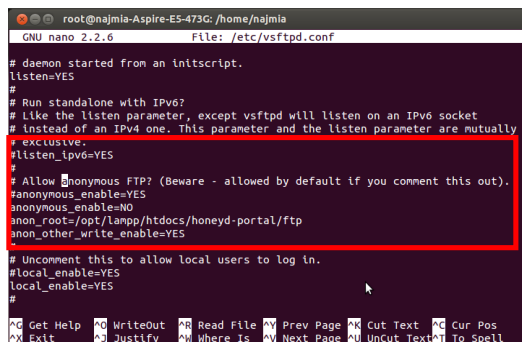
Use Case Diagram digunakan untuk memodelkan fungsionalitas sistem yang dilihat dari pengguna yang ada diluar sistem (aktor). Berikut adalah *Use Case Diagram* untuk sistem *monitoring* yang dibangun. *Use Case Diagram* sistem dapat dilihat pada Gambar 3.

2.9 Topologi Sistem

Topologi yang digunakan pada pengujian sistem ini adalah topologi *Star* seperti yang ada pada Gambar 4, dimana dalam topologi tersebut ada *PC* (*Personal Computer*) yang akan berperan sebagai *attacker* untuk mengirimkan paket-paket berisi anomali terhadap *server*, *router* yang berperan sebagai penghubung, *client* yang akan

akun FTP terlebih dahulu, pastikan aplikasi VSFTPD sudah terpasang pada komputer *server*. Cara membuat akun FTP *Server* adalah sebagai berikut :

1. Mengetikan perintah “*sudo nano /etc/vsftpd.conf*” pada terminal linux, kemudian pada tampilan baru yang muncul ketikkan *Ctrl+W* untuk mencari kata *anonymous*. Buat konfigurasi seperti yang ada pada Gambar 7.



```

root@najmia-Aspire-E5-473G: /home/najmia
GNU nano 2.2.6 File: /etc/vsftpd.conf
# daemon started from an initscript.
listen=YES
#
# Run standalone with IPv6?
# Like the listen parameter, except vsftpd will listen on an IPv6 socket
# instead of an IPv4 one. This parameter and the listen parameter are mutually
# exclusive.
#listen_ipv6=YES
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=YES
anonymous_enable=NO
anon_root=/opt/lamp/htdocs/honeyd-portal/ftp
anon_other_write_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
local_enable=NO
#

```

Gambar 7 Konfigurasi FTP Server

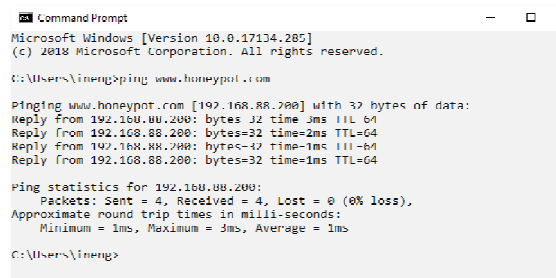
2. Menghapus *user FTP default* dengan mengetikan perintah “*sudo user del FTP*” (*FTP* adalah nama *user*)
3. Membuat *user FTP* baru dengan menuliskan perintah “*useradd -d /opt/lamp/htdocs/honeyd-portal/FTP skripsiinda*”
4. Setelah membuat *user name* kemudian membuat *password* dengan mengetikkan perintah “*passwd kripsiinda*”
5. Me-restart VSFTPD dengan mengetikkan perintah “*/etc/init.d/vsftpd restart*”.

3.3 Pengujian Sistem

Pengujian sistem keamanan menggunakan *Honeypot* sebagai IPS dilakukan dengan menggunakan 3 pengujian, yaitu dengan melakukan perintah *ping*, *scanning port* dan *FTP attack*. Pengujian dengan melakukan perintah *ping* dan *scanning port* dilakukan dalam 2 kondisi, yaitu saat *Honeypot* aktif dan pada saat *Honeypot* tidak aktif agar dapat melihat apakah *Honeypot* berhasil memberikan informasi palsu kepada penyerang dan apakah catatan serangan bisa tampil pada sistem *monitoring* yang dibuat. Sedangkan untuk pengujian *FTP attack* dilakukan untuk mengetahui apakah *server* bisa diakses oleh penyerang dan sistem *monitoring* dapat menampilkan *monitoring* serangan terhadap *server* tersebut.

1. Melakukan Perintah *Ping*

Pengujian dengan melakukan perintah *ping* dilakukan dengan mencoba perintah *ping* ke *domain name* yang sudah ditentukan menggunakan *command prompt*, pengujian ini dilakukan untuk mencoba mendapatkan informasi *IP address* dari *server*. Saat keadaan *server* tidak mengaktifkan sistem *Honeypot*, PC penyerang mampu melakukan *ping* ke *domain name* dan berhasil mendapatkan *IP address server* asli seperti pada Gambar 8.



```

Microsoft Windows [Version 10.0.17134.285]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Vineng>ping www.honeypot.com

Pinging www.honeypot.com [192.168.88.200] with 32 bytes of data:
Reply from 192.168.88.200: bytes=32 time=1ms TTL=64
Reply from 192.168.88.200: bytes=32 time=2ms TTL=64
Reply from 192.168.88.200: bytes=32 time=1ms TTL=64
Reply from 192.168.88.200: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.88.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

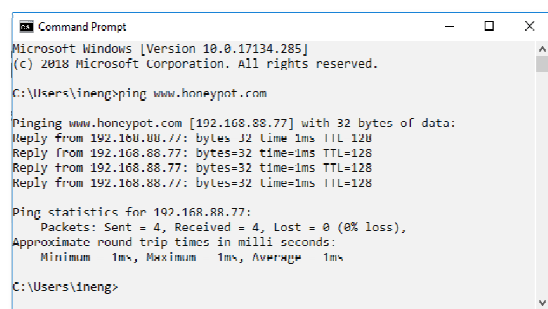
C:\Users\Vineng>

```

Gambar 8 Melakukan *Ping Domain Name* tanpa Mengaktifkan *Honeypot*

Gambar 9 menunjukkan bahwa saat melakukan perintah *ping* ke alamat *www.honeypot.com* saat sistem *Honeypot* tidak diaktifkan, maka akan mendapatkan respon *reply from 192.168.88.200* dimana IP tersebut merupakan *IP address* dari *server* asli. Kemudian, setelah *Honeypot* diaktifkan, saat penyerang melakukan *test ping* maka *IP address* yang akan muncul yaitu *IP address* palsu yang sudah diatur sebelumnya.

Dengan adanya pemalsuan *IP server* asli ini, penyerang akan beranggapan bahwa *IP* yang didapatkannya adalah *IP* yang sesungguhnya dan apabila akan melanjutkan penyerangan pada tingkatan berikutnya akan menggunakan *IP* palsu ini, namun penyerang tidak akan bisa melakukan serangan ditingkat selanjutnya karena *IP* yang dipakai adalah *IP* palsu.



```

Microsoft Windows [Version 10.0.17134.285]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Vineng>ping www.honeypot.com

Pinging www.honeypot.com [192.168.88.77] with 32 bytes of data:
Reply from 192.168.88.77: bytes=32 time=1ms TTL=128
Reply from 192.168.88.77: bytes=32 time=1ms TTL=128
Reply from 192.168.88.77: bytes=32 time=1ms TTL=128
Reply from 192.168.88.77: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.88.77:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli seconds:
        Minimum 1ms, Maximum 1ms, Average 1ms

C:\Users\Vineng>

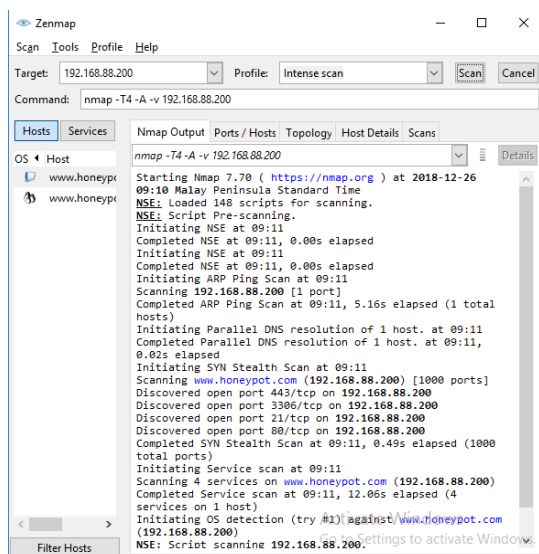
```

Gambar 9 Melakukan *Ping Domain Name* dengan Mengaktifkan *Honeypot*

2. Melakukan *Scanning Port*

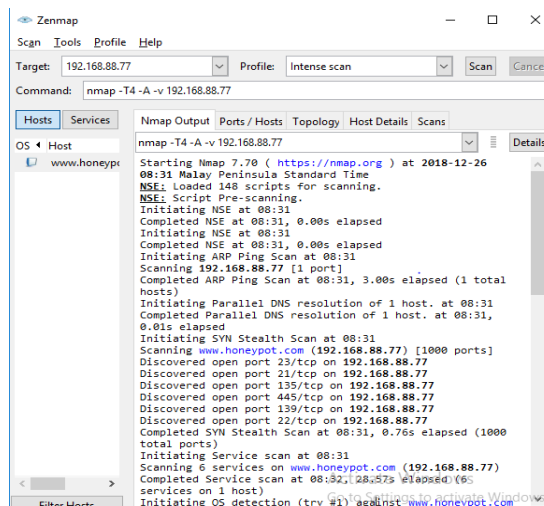
Pengujian tahap berikutnya yaitu dengan melakukan *scanning port* menggunakan aplikasi yang sudah ada, pada penelitian ini digunakan aplikasi *Nmap* untuk mengetahui *port* apa saja yang terbuka. Pengujian dilakukan dengan menargetkan *IP address* yang didapatkan saat melakukan perintah *ping* sebelumnya. Saat menargetkan *IP address* 192.168.88.200 aplikasi *Nmap* akan menampilkan *port* yang sesungguhnya terbuka, namun jika *honeypot* diaktifkan maka *port* yang akan ditampilkan adalah *port* yang sudah dikonfigurasi pada sistem *Honeypot*.

Gambar 10 menunjukkan beberapa *port* yang terbuka merupakan *port* yang sesungguhnya atau bukan *port* yang sengaja dipalsukan sesuai yang sudah dikonfigurasi. Jika penyerang berhasil mengetahui *port* mana saja yang terbuka, maka penyerang akan lebih mudah untuk menentukan akan melakukan serangan melalui jalur mana saja.



Gambar 10 Melakukan *Scanning Port* tanpa Mengaktifkan *Honeypot*

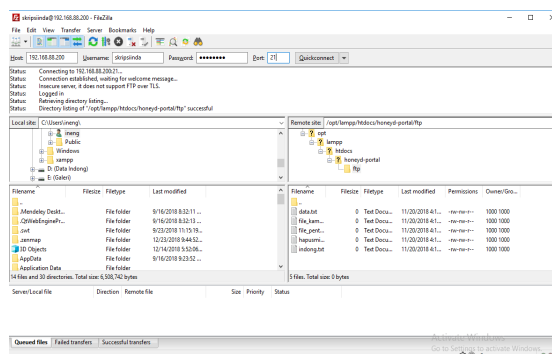
Gambar 11 menunjukkan bahwa aplikasi *scanning port* menerima informasi *scanning port* yang palsu sesuai dengan yang telah diatur sebelumnya. Apabila penyerang mendapatkan informasi palsu mengenai *port* yang terbuka, penyerang akan sulit untuk melakukan serangan tahap berikutnya karena masuk melalui jalur yang sebenarnya tidak ada.



Gambar 11 Melakukan *Scanning Port* dengan Mengaktifkan *Honeypot*

3. FTP Attack

Pengujian FTP *attack* dilakukan dengan menggunakan aplikasi *FileZilla*. *FileZilla* adalah aplikasi FTP *Client* yang digunakan untuk mengakses *file* pada komputer lain karena dengan menggunakan aplikasi FTP *Client* ini sudah mendukung untuk melakukan sistem manajemen seperti *rename* dan *delete*. Pada penelitian ini, untuk mengakses FTP *Server* *IP address* yang digunakan harus menggunakan *IP server* asli seperti pada Gambar 12.



Gambar 12 Tampilan *FileZilla* saat Mengakses FTP *Server*

a. Hasil Pengujian Sistem

Setelah melakukan pengujian menggunakan perintah *ping* dan *scanning port*, hasil pengujian ditampilkan pada Tabel 1.

Tabel 1 Hasil Pengujian Sistem

WAKTU PENYERANGAN	TIPE PORT	IP PENYERANG	PORT SERANGAN
2018-11-26-12:39:44.6153	ICMP	192.168.88.254	8(0)

2018-11-26-12:39:45.6218	ICMP	192.168.88.254	8(0)	2018-11-26-13:27:07.4501	TCP	192.168.88.254	445
2018-11-26-12:39:46.6358	ICMP	192.168.88.254	8(0)	2018-11-26-13:27:07.4510	TCP	192.168.88.254	1720
2018-11-26-12:39:47.6482	ICMP	192.168.88.254	8(0)	2018-11-26-13:27:07.4513	TCP	192.168.88.254	22
2018-11-26-12:39:48.6621	ICMP	192.168.88.254	8(0)	2018-11-26-13:27:07.4516	TCP	192.168.88.254	23
2018-11-26-12:39:49.6900	ICMP	192.168.88.254	8(0)	2018-11-26-13:29:45.1417	UDP	192.168.88.254	41409
2018-11-26-12:39:50.6868	ICMP	192.168.88.254	8(0)	2018-11-26-13:29:49.5006	UDP	192.168.88.254	41409
2018-11-26-12:39:51.6989	ICMP	192.168.88.254	8(0)	2018-11-26-13:29:55.7198	UDP	192.168.88.254	41409
2018-11-26-12:42:54.2285	TCP	192.168.88.254	25	2018-11-26-13:29:56.6771	UDP	192.168.88.254	137
2018-11-26-12:42:54.2288	TCP	192.168.88.254	554	2018-11-26-13:29:56.6773	UDP	192.168.88.254	137
2018-11-26-12:42:54.2292	TCP	192.168.88.254	3389	2018-11-26-13:29:56.6779	UDP	192.168.88.254	1434
2018-11-26-12:42:54.2295	TCP	192.168.88.254	111	2018-11-26-13:29:57.8227	UDP	192.168.88.254	137
2018-11-26-12:42:54.2299	TCP	192.168.88.254	110	2018-11-26-13:29:57.8726	UDP	192.168.88.254	137
2018-11-26-12:42:54.2312	TCP	192.168.88.254	8080	2018-11-26-13:29:58.9646	TCP	192.168.88.254	445
2018-11-26-12:42:54.2318	TCP	192.168.88.254	113	2018-11-26-13:29:58.9652	UDP	192.168.88.254	137
2018-11-26-12:42:54.2323	TCP	192.168.88.254	1025	2018-11-26-13:29:59.0723	UDP	192.168.88.254	137
2018-11-26-12:42:54.2329	TCP	192.168.88.254	199	2018-11-26-13:30:00.1119	UDP	192.168.88.254	137
2018-11-26-12:45:43.5575	UDP	192.168.88.254	137				
2018-11-26-12:45:43.5576	UDP	192.168.88.254	1434				
2018-11-26-12:45:43.5581	UDP	192.168.88.254	137				
2018-11-26-12:45:44.6753	UDP	192.168.88.254	137				
2018-11-26-12:45:46.9647	UDP	192.168.88.254	137				
2018-11-26-12:45:47.1205	UDP	192.168.88.254	137				
2018-11-26-12:45:48.6858	UDP	192.168.88.254	137				
2018-11-26-13:26:43.5982	ICMP	192.168.88.254	8(0)				
2018-11-26-13:26:44.1270	ICMP	192.168.88.254	8(0)				
2018-11-26-13:26:45.1425	ICMP	192.168.88.254	8(0)				
2018-11-26-13:26:46.1623	ICMP	192.168.88.254	8(0)				
2018-11-26-13:26:47.1740	ICMP	192.168.88.254	8(0)				
2018-11-26-13:26:49.2015	ICMP	192.168.88.254	8(0)				
2018-11-26-13:26:50.2112	ICMP	192.168.88.254	8(0)				
2018-11-26-13:26:51.2269	ICMP	192.168.88.254	8(0)				
2018-11-26-13:26:52.2346	ICMP	192.168.88.254	8(0)				
2018-11-26-13:27:07.4491	TCP	192.168.88.254	993				
2018-11-26-13:27:07.4494	TCP	192.168.88.254	3306				
2018-11-26-13:27:07.4497	TCP	192.168.88.254	143				
2018-11-26-13:27:07.4498	TCP	192.168.88.254	587				

Pada Tabel 1, *log* serangan merupakan *log* yang diambil secara acak dari sistem *monitoring*. Berdasarkan Tabel 1 hasil pengujian dapat dibuatkan grafik seperti yang ada pada tampilan *dashboard* dimana masing-masing menggunakan Persamaan (1).

Diketahui :

TCP : 18
 UDP : 18
 ICMP : 17
 Total data : 53

Ditanyakan : a. Persentase TCP
 b. Persentase UDP
 c. Persentase ICMP
 d. Grafik *log* serangan

Penyelesaian :

$$\text{Persentase TCP} = \frac{\text{TCP}}{\text{Total Data}} \times 100\%$$

$$= \frac{18}{53} \times 100\%$$

$$= 33,96 \%$$

$$\text{Persentase UDP} = \frac{\text{UDP}}{\text{Total Data}} \times 100\%$$

$$= \frac{18}{53} \times 100\%$$

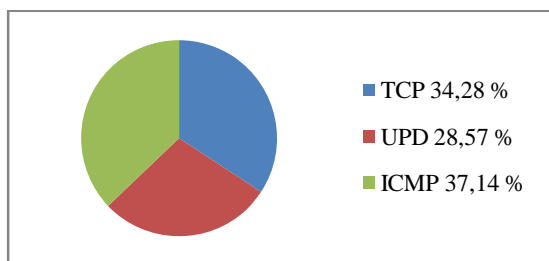
$$= 33,96 \%$$

$$\text{Persentase ICMP} = \frac{\text{ICMP}}{\text{Total Data}} \times 100\%$$

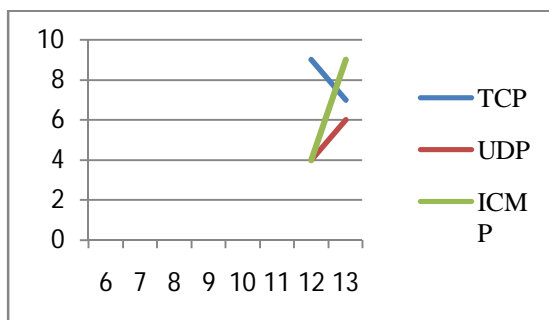
$$= \frac{17}{53} \times 100\%$$

$$= 32,07 \%$$

Dari perhitungan, dapat dibuatkan grafik *log* serangan seperti pada Gambar 13 dan Gambar 14, dimana yang berwarna biru merupakan total serangan yang mengarah pada *port* TCP sebanyak 33,96%, warna biru untuk total serangan yang mengarah pada *port* UDP sebanyak 33,96%, dan yang berwarna hijau untuk serangan yang mengarah pada *port* ICMP sebanyak 32,07%.



Gambar 13 Grafik Log Attack Static



Gambar 14 Grafik Log Serangan dalam 8 Jam

b. Tampilan Hasil *Monitoring* pada *Web Service*

Pada *Web Service* data yang disediakan hanya hasil *log* serangan yang masuk pada sistem *monitoring* dan daftar Admin. Contoh untuk informasi Admin seperti pada Gambar 15 dan hasil *monitoring log* serangan dapat dilihat seperti pada Gambar 16.

Name	Email	Address	Action
indung	indung.sari	Y	TEXT
admin	eke	Y	TEXT

Gambar 15 Informasi Admin pada *Web Service*

Time	Port	Attacker	Victim
2018-11-09-08:11:41.0188	tcp(6)	192.168.88.243	14968192.168.88.7722:70
2018-11-09-08:11:40.8162	tcp(6)	192.168.88.243	14972192.168.88.77139:70
2018-11-09-08:11:40.8161	tcp(6)	192.168.88.243	14970192.168.88.77137:70
2018-11-09-08:11:40.7598	tcp(6)	192.168.88.243	14967192.168.88.7723:600
2018-11-09-08:11:25.3592	tcp(6)	192.168.88.243	166192.168.88.7721:410
2018-11-09-08:11:25.3571	tcp(6)	192.168.88.243	681192.168.88.77145:410
2018-11-09-08:11:25.2577	tcp(6)	192.168.88.243	65192.168.88.7722:440
2018-11-09-08:11:25.2012	tcp(6)	192.168.88.243	918192.168.88.7722:440
2018-11-09-08:11:25.2013	tcp(6)	192.168.88.243	478192.168.88.77139:440
2018-11-09-08:11:25.1988	tcp(6)	192.168.88.243	681192.168.88.77137:410
2018-11-09-08:11:24.1179	tcp(6)	192.168.88.243	681192.168.88.77137[Windows-2008R2]1373
2018-11-09-08:11:24.1178	tcp(6)	192.168.88.243	65192.168.88.77137[Windows-2008R2]1373
2018-11-09-08:11:24.1177	tcp(6)	192.168.88.243	166192.168.88.77137[Windows-2008R2]1373
2018-11-09-08:11:24.1175	tcp(6)	192.168.88.243	218192.168.88.7723[Windows-2008R2]1373
2018-11-09-08:11:24.1174	tcp(6)	192.168.88.243	478192.168.88.77139[Windows-2008R2]1373
2018-11-09-08:11:24.1110	tcp(6)	192.168.88.243	681192.168.88.77137[Windows-2008R2]1373
2018-11-09-08:11:24.0449	tcp(6)	192.168.88.243	13068192.168.88.77145:160
2018-11-09-08:10:23.2272	tcp(6)	192.168.88.243	13068192.168.88.77145:160
2018-11-09-08:10:23.2014	tcp(6)	192.168.88.243	13068192.168.88.77145:160

Gambar 16 Hasil *Monitoring Log* Serangan pada *Web Service*

4. KESIMPULAN

Berdasarkan penelitian dan hasil pengujian yang dilakukan pada penelitian ini, maka dapat disimpulkan:

1. Sistem keamanan jaringan komputer menggunakan *Honeypot* sebagai IPS berhasil mengenali *port* TCP, UDP, ICMP dan anomali terhadap sistem atau *host* dengan mengidentifikasi setiap paket data yang masuk.
2. Pembangunan *web monitoring* dapat menampilkan aktivitas anomali berdasarkan *log* serangan yang masuk pada sistem keamanan.
3. *Log* serangan berhasil ditampilkan pada *Web Service* sesuai dengan *request* dari *user*.
4. Berdasarkan hasil pengujian yang dilakukan, serangan yang masuk melalui *port* TCP adalah sebanyak 33,96%, UDP sebanyak 33,96%, dan ICMP sebanyak 32,07%.

5. SARAN

Adapun saran-saran yang dapat diberikan untuk pengembangan lebih lanjut terhadap penelitian ini adalah untuk penanganan serangan yang lebih aman bisa menggunakan SNORT dan Suricata dan sistem *monitoring* sudah bisa diintegrasikan dengan berbagai *platform* atau sistem operasi manapun.

DAFTAR PUSTAKA

[1] A. E. Pratama, I Putu, *Handbook*

- Jaringan Komputer*, September.
Bandung: Informatika, 2015.
- [2] L. P. Aidin, S. M. Nasution, and F. Azmi, "Implementasi High Interaction Honeypot pada Server," *e-Proceeding Eng.*, Vol. 3, No. 2, pp. 2172–2178, 2016.
- [3] J. Gondohanindijo, "IPS (Intrusion Prevention System) untuk Mencegah Tindak Penyusupan/Intrusi," *Maj. Ilm. Inform.*, Vol. 3, No. 3, pp. 38–59, 2012.
- [4] D. M. Myzda, "Analisa dan Konfigurasi Network Intrusion Prevention System (NIPS) pada Linux Ubuntu 10 . 04 Lts," Universitas Islam Negeri Sultan Syarif Kasim Riau, 2011.
- [5] M. M. Mustofa and E. Aribowo, "Penerapan Sistem Keamanan Honeypot dan IDS pada Jaringan Nirkabel (Hotspot)," *J. Sarj. Tek. Inform.*, Vol. 1, No. 1, pp. 111–118, 2013.
- [6] R. Hidayat and A. Ashari, "Penerapan Teknologi Web Service untuk Integrasi Layanan Puskesmas dan Rumah Sakit," *Berk. MIPA, (23)I*, Vol. 23, No. 1, pp. 64–77, 2013.
- [7] Y. Hanapi, I. P. Ningrum, and R. Ramadhan, "Identifikasi Sidik Jari Menggunakan Discrete Wavelet Transform dan Canberra Distance," *semanTIK*, Vol. 1, No. 1, pp. 1–10, 2015.
-