

**SIMULASI PERCOBAAN HONEYPOT BERBASIS MODERN HONEY
NETWORK SEBAGAI IDENTIFIKASI SERANGAN PADA
INDUSTRIAL CONTROL SYSTEM (ICS)**

SKRIPSI



disusun oleh

Hendriawan

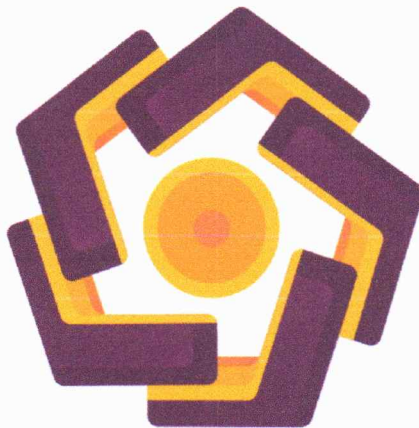
14.11.8064

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2018**

**SIMULASI PERCOBAAN HONEYPOT BERBASIS MODERN HONEY
NETWORK SEBAGAI IDENTIFIKASI SERANGAN PADA
INDUSTRIAL CONTROL SYSTEM (ICS)**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Hendriawan

14.11.8064

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2018**



PERSETUJUAN

SKRIPSI

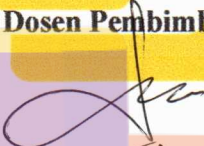
**SIMULASI PERCOBAAN HONEYPOT BERBASIS MODERN HONEY
NETWORK SEBAGAI IDENTIFIKASI SERANGAN PADA
INDUSTRIAL CONTROL SYSTEM (ICS)**

yang dipersiapkan dan disusun oleh

Hendriawan
14.11.8064

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 26 September 2017

Dosen Pembimbing


Sudarmawan, S.T., M.T
NIK. 190302035

PENGESAHAN

SKRIPSI

SIMULASI PERCOBAAN HONEYPOT BERBASIS MODERN HONEY NETWORK SEBAGAI IDENTIFIKASI SERANGAN PADA INDUSTRIAL CONTROL SYSTEM (ICS)

yang dipersiapkan dan disusun oleh

Hendriawan
14.11.8064

telah dipertahankan di depan Dewan Penguji
pada tanggal 17 Juli 2018

Susunan Dewan Penguji

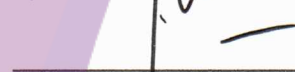
Nama Penguji

Melwin Syafrizal, S.Kom., M.Eng.
NIK. 190302105

Hastari Utama, M.Cs.
NIK. 190302230

Yudi Susanto, M.Kom.
NIK. 190302039

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 20 Juli 2018

DEKAN FAKULTAS ILMU KOMPUTER


Krisnawati, S.Si, M.T.
NIK. 190302038



PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

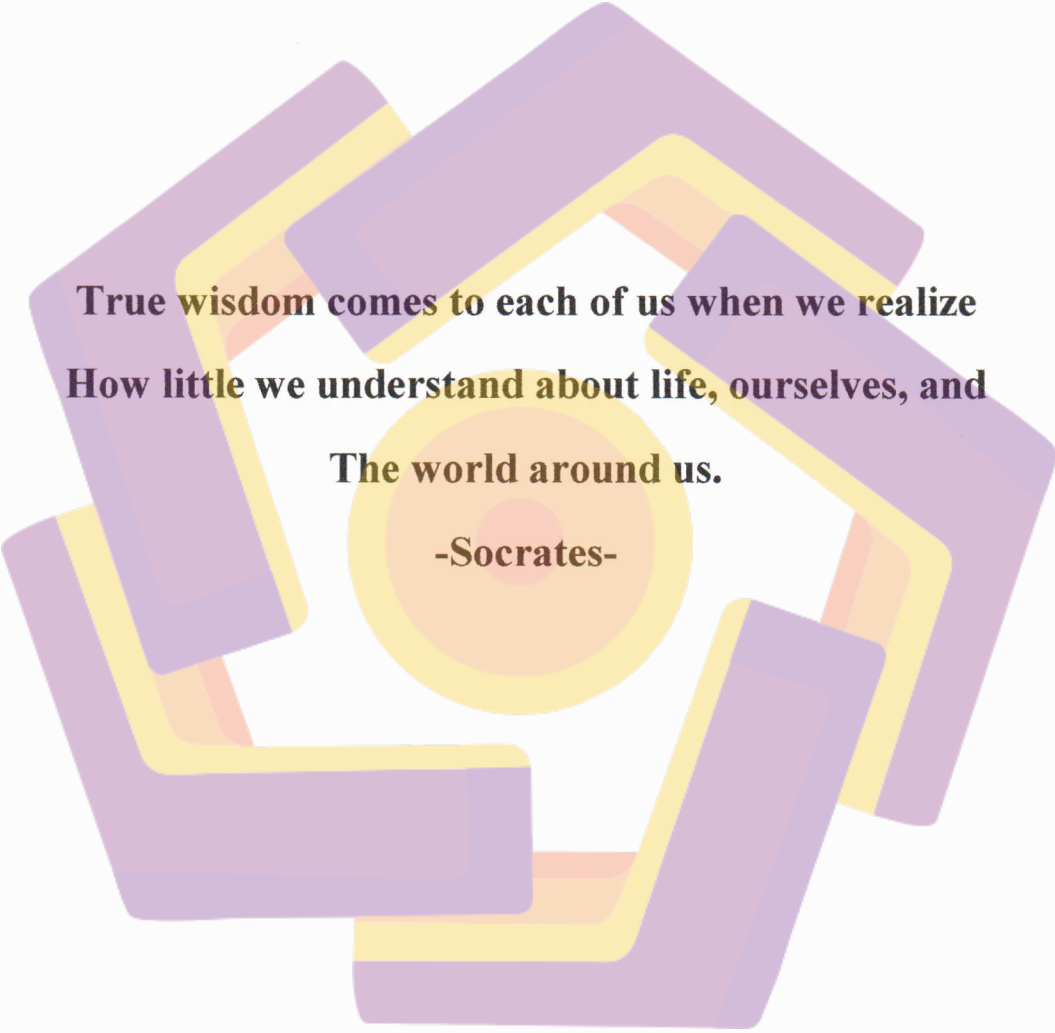
Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 20 Juli 2018



Hendriawan
NIM. 14.11.8064

MOTTO



**True wisdom comes to each of us when we realize
How little we understand about life, ourselves, and
The world around us.**

-Socrates-

PERSEMBAHAN



Teruntuk Ibu, Ayah . . .

Dan perempuan yang selalu dalam pelukan . . .

KATA PENGANTAR

Alhamdulillah, segala puji syukur kehadiran Allah SWT Sang Maha Segalanya, sehingga skripsi dengan judul “**SIMULASI PERCOBAAN HONEYPOT BERBASIS MODERN HONEY NETWORK SEBAGAI IDENTIFIKASI SERANGAN PADA INDUSTRIAL CONTROL SYSTEM (ICS)**” dapat selesai dengan baik. Sebuah perjuangan dalam meraih gelar S. Kom yang tentunya tidak dapat lepas dari segala bentuk dukungan materiil maupun non materiil dari berbagai pihak, untuk itu penulis ucapkan terimakasih kepada :

- Ayah Ibu tercinta, tersayang dan terkasih. Terimakasih atas segala dukungan, restu, dan doa tulus yang selalu Ayah Ibu panjatkan. Bangga dan bahagia sekali rasanya memiliki Ayah Ibu dalam hidup ini.
- Kekasihku Annisa Pramahadi, terima kasih atas dorongan semangat selama pengerjaan skripsi ini. Caramu dalam menyemangatiku memberi andil besar hingga aku berada pada titik sekarang ini.
- Bapak Sudarmawan, S.T., M.T. selaku pembimbing yang selalu memberikan saran dan masukan dalam menyelesaikan skripsi ini.
- Segenap teman-teman kelas S1 TI-08 angkatan 2014 yang sudah banyak memberikan cerita, support dan masukan dalam jangka masuk kuliah sampai sekarang
- Septyo Ade Setiawan, sebagai sahabat saya yang selalu bercerita dan memberikan masukan sekaligus menemani saya sehingga selalu dapat memberikan motivasi.
- Dan segenap pihak yang tidak dapat penulis sebutkan semua. Terimakasih atas segalanya. Semoga Allah SWT memberikan balasan yang lebih baik.

Yogyakarta, 18 Juli 2018

Hendriawan

DAFTAR ISI

JUDUL	2
LEMBAR PERSETUJUAN.....	3
LEMBAR PENGESAHAN	iv
PERNYATAAN.....	v
MOTTO	vi
PERSEMBAHAN	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	ix
DAFTAR TABEL	xiii
DAFTAR GAMBAR.....	xiv
INTISARI	xix
ABSTRACT.....	xx
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian	4
1.6 Metode Penelitian.....	5
1.6.1 Metode Pengumpulan Data	5
1.6.1.1 Studi Kepustakaan	5
1.6.1.2 Metode Observasi	5
1.6.2 Metode Pengembangan Sistem.....	5
1.6.2.1 Planning	5
1.6.2.2 Analisis	5
1.6.2.3 Perancangan.....	6

1.6.2.4	Implementasi	6
1.6.2.5	Testing	6
1.7	Sistematika Penelitian	6
BAB II LANDASAN TEORI		8
2.1	Tinjauan Pustaka	8
2.2	Dasar Teori.....	12
2.2.1	Jaringan Komputer	12
2.2.2	Tipe-Tipe Jaringan Komputer.....	13
2.2.2.1	Local Area Network (LAN)	13
2.2.2.2	Wide Area Network (WAN).....	13
2.2.2.3	Metropolitan Area Network (MAN).....	14
2.2.3	Keamanan Jaringan	14
2.2.3.1	Firewall.....	15
2.2.3.2	IDS	16
2.2.3.3	IPS.....	16
2.2.4	VPS	17
2.2.5	Linux.....	17
2.2.5.1	Ubuntu	18
2.2.6	Honeypot.....	19
2.2.6.1	Sejarah Honeypot	19
2.2.6.2	Pengertian Honeypot	20
2.2.6.3	Manfaat Honeypot	23
2.2.6.4	Jenis-jenis Honeypot.....	23
2.2.6.5	Modern Honey Network	27
2.2.6.6	MongoDB	27
2.2.10.7	Hpfeeds & Hpfeeds-logger.....	28
2.2.6.8	Snort.....	28
2.2.6.9	Kippo	29
2.2.6.10	Cowrie	29
2.2.6.11	Dionaea.....	29
2.2.6.12	ConPot	30
2.2.6.13	Splunk.....	30

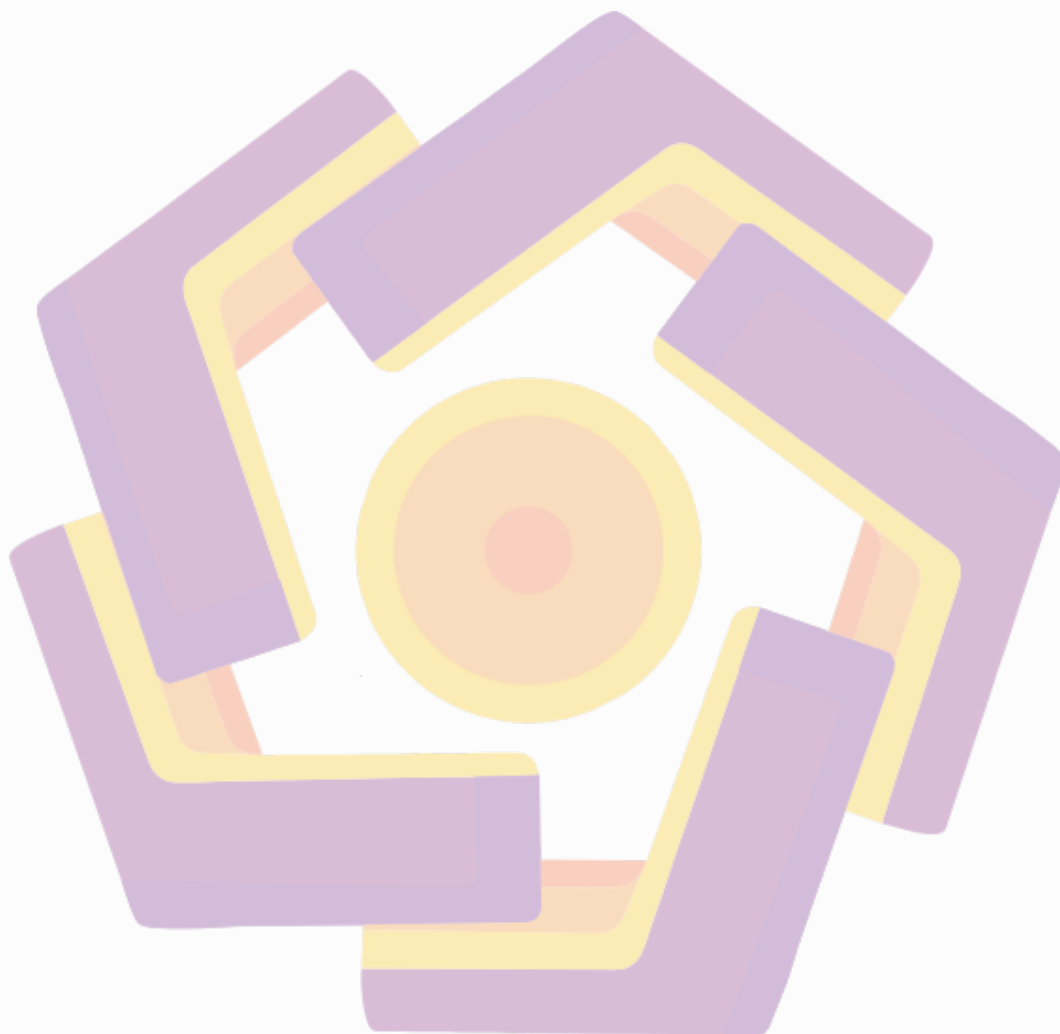
2.2.7	Industrial Control System.....	31
2.2.7.1	ICS.....	31
2.2.7.2	Sistem SCADA.....	33
2.2.7.3	Distributed Control Systems (DCS).....	35
2.2.7.4	Topologi Dasar Programmable Logic Controller (PLC).....	37
2.2.7.5	Perbedaan ICS dan Sistem Sekuritas Teknologi Informasi.....	39
BAB III METODE PENELITIAN.....		45
3.1	Gambaran Penelitian.....	45
3.2	Topologi.....	46
3.2.1	Rancangan A.....	46
3.2.2	Rancangan B.....	47
3.3	Alat dan Bahan.....	48
3.4	Langkah-Langkah Penelitian.....	49
3.4.1	Konfigurasi dan Instalasi Server <i>Modern Honey Network</i>	49
3.4.2	Konfigurasi dan instalasi <i>Modern Honey Network</i>	51
3.4.3	Konfigurasi dan instalasi sensor <i>Honeypot</i>	57
3.4.3.1	Instalasi <i>Honeypot ConPot</i>	57
3.4.3.2	Instalasi <i>Honeypot Snort & Cowrie</i>	60
3.4.3.3	Instalasi <i>Honeypot Dionaea</i>	62
3.4.4	Konfigurasi dan instalasi Splunk.....	63
3.4.5	Pengujian.....	75
3.4.5.1	Pengujian <i>DoS Attack</i>	75
3.4.5.2	Pengujian Port Scanning.....	83
3.4.5.3	Pengujian <i>ICS/SCADA Attack</i>	89
3.4.5.4	Pengujian Dictionary Attack.....	97
BAB IV HASIL DAN PEMBAHASAN.....		107
4.1	Hasil Pengujian <i>DoS Attack</i>	107
4.2	Hasil Pengujian <i>Port Scanning</i>	108
4.3	Hasil Pengujian <i>ICS/SCADA Attack</i>	109
4.4	Hasil Pengujian Dictionary Attack.....	110
4.5	Hasil Data MHN.....	111
4.6	Hasil Data Splunk.....	114

BAB V PENUTUP.....115

5.1 Kesimpulan115

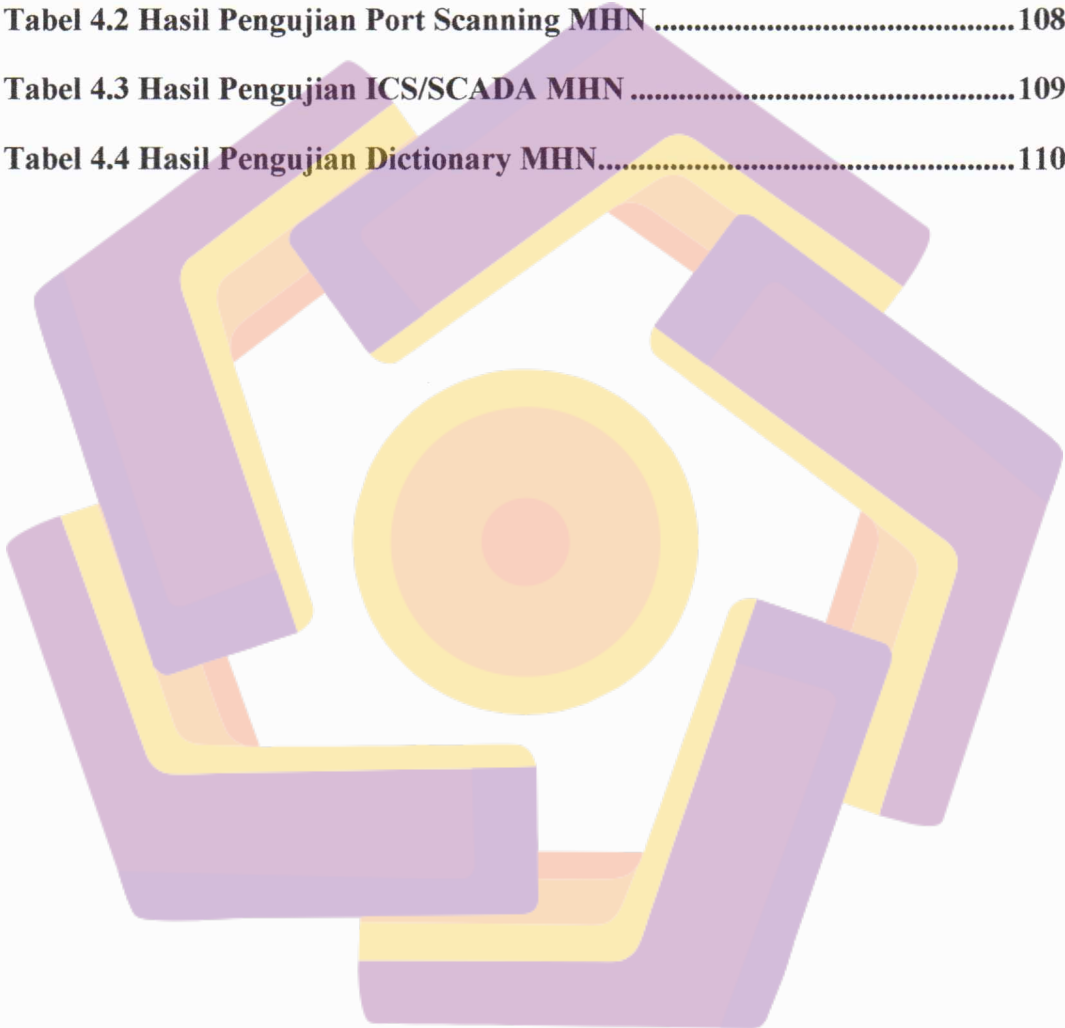
5.2 Saran116

DAFTAR PUSTAKA.....117



DAFTAR TABEL

Tabel 2.1 Perbedaan Referensi dan Penelitian.....	10
Tabel 4.1 Hasil Pengujian DoS Attack MHN.....	107
Tabel 4.2 Hasil Pengujian Port Scanning MHN	108
Tabel 4.3 Hasil Pengujian ICS/SCADA MHN	109
Tabel 4.4 Hasil Pengujian Dictionary MHN.....	110



DAFTAR GAMBAR

Gambar 2.1 MHN Server Architecture	31
Gambar 2.2 Operasi Dasar ICS.....	32
Gambar 2.3 SCADA System General Layout	34
Gambar 2.4 Contoh Implementasi DCS	36
Gambar 2.5 Implementasi Sistem Kontrol PLC.....	38
Gambar 3.1 Topologi Rancangan A.....	46
Gambar 3.2 Topologi Rancangan B.....	47
Gambar 3.3 IP Address Server.....	50
Gambar 3.4 Gambar Topologi Server Rancangan B	51
Gambar 3.5 Upgrade dan Update Ubuntu	52
Gambar 3.6 Install Git.....	52
Gambar 3.7 Clone MHN	52
Gambar 3.8 Install Package MHN	53
Gambar 3.9 Cek Status package/Daemon MHN	53
Gambar 3.10 Install MHN Server	54
Gambar 3.11 Input Email & Password MHN.....	54
Gambar 3.12 Konfigurasi MHN-Celery Worker.....	55
Gambar 3.13 Login page MHN	56
Gambar 3.14 Index MHN.....	56
Gambar 3.15 Deploy Command Script.....	58
Gambar 3.16 Deploy Command Conpot	58
Gambar 3.17 Script Command.....	59

Gambar 3.18 Deploy Command Conpot Pada Server	59
Gambar 3.19 Sensor Conpot pada Rancangan A	60
Gambar 3.20 Sensor Conpot pada Rancangan B	60
Gambar 3.21 Sensor Snort & Cowrie pada Rancangan A.....	61
Gambar 3.22 Sensor Snort & Cowrie pada Rancangan B.....	61
Gambar 3.23 Sensor Dionaea pada Rancangan A.....	62
Gambar 3.24 Sensor Dionaea pada Rancangan B	62
Gambar 3.25 Install HPFeed-logger untuk Splunk.....	63
Gambar 3.26 Download Splunk for Linux	64
Gambar 3.27 Download Splunk pada Server.....	64
Gambar 3.28 Membuka Package Splunk	65
Gambar 3.29 Instalasi Splunk	65
Gambar 3.30 Agreement dan Pengisian password Splunk.....	65
Gambar 3.31 Login Page Splunk.....	66
Gambar 3.32 Halaman utama Splunk	66
Gambar 3.33 Aplikasi Integrasi MHN dan Splunk.....	67
Gambar 3.34 Install App from File.....	68
Gambar 3.35 Upload File Integrasi MHN	68
Gambar 3.36 Aplikasi MHN pada Splunk	69
Gambar 3.37 MHN for Splunk.....	69
Gambar 3.38 Data Input	70
Gambar 3.39 File & Directories	70
Gambar 3.40 Memasukkan Direktori Log MHN-Splunk.....	71
Gambar 3.41 Splunk yang Berhasil Terintegrasi	71
Gambar 3.42 Splunk yang Berhasil Terintegrasi	72

Gambar 3.43 Date Server UTC 0	72
Gambar 3.44 Date Splunk Tidak Sinkron.....	73
Gambar 3.45 Account Setting.....	73
Gambar 3.46 Penggantian TimeZone	74
Gambar 3.47 Timezone Terkonfigurasi.....	74
Gambar 3.48 IP Public Client Penguji.....	75
Gambar 3.49 Pengujian DoS Attack Rancangan A.....	77
Gambar 3.50 Pengujian DoS Attack Rancangan B.....	77
Gambar 3.51 Hasil DoS Port 22 Rancangan A	77
Gambar 3.52 Hasil DoS Port 22 Rancangan B.....	78
Gambar 3.53 Pengujian Dos Attack Rancangan A port 8080	78
Gambar 3.54 Pengujian DoS Attack Rancangan B port 8080.....	78
Gambar 3.55 Hasil Pengujian DoS Attack Rancangan A port 8080.....	79
Gambar 3.56 Hasil Pengujian DoS Attack Rancangan B port 8080.....	80
Gambar 3.57 Pengujian DoS Attack Rancangan A port 80.....	80
Gambar 3.58 Pengujian DoS Attack Rancangan B port 80.....	81
Gambar 3.59 Hasil Pengujian DoS Attack Rancangan A port 80.....	81
Gambar 3.60 Hasil Pengujian DoS Attack Rancangan B port 80.....	82
Gambar 3.61 Port Scanning Rancangan A.....	83
Gambar 3.62 Port Scanning Rancangan B.....	83
Gambar 3.63 Port Scanning Server Conpot Rancangan B.....	84
Gambar 3.64 Hasil Port Scanning Rancangan A.....	85
Gambar 3.65 Hasil Port Scanning Rancangan B.....	85
Gambar 3.66 Scanning port 102 Rancangan A.....	86
Gambar 3.67 Hasil Scan Port 102 Rancangan A	87

Gambar 3.68 Scanning Port 102 Rancangan B.....	87
Gambar 3.69 Hasil Scan port 102 Rancangan B.....	88
Gambar 3.70 Pengujian port 502 rancangan A	89
Gambar 3.71 Pengujian port 502 rancangan B.....	89
Gambar 3.72 Hasil Port Scanning Port 502 Rancangan B	90
Gambar 3.73 Metasploit Modbus rancangan A.....	91
Gambar 3.74 Metasploit Modbus rancangan B.....	91
Gambar 3.75 Hasil Metasploit Modbus rancangan B.....	91
Gambar 3.76 Menjalankan Diagslave Rancangan A.....	92
Gambar 3.77 Menjalankan Diagslave Rancangan B.....	92
Gambar 3.78 Stop Conpot Rancangan A	93
Gambar 3.79 Stop Conpot Rancangan B.....	93
Gambar 3.80 Diagslave pada Rancangan A.....	93
Gambar 3.81 Diagslave pada Rancangan B.....	94
Gambar 3.82 Hasil Metasploit Rancangan A.....	94
Gambar 3.83 Hasil Metasploit Rancangan B.....	94
Gambar 3.84 Koneksi Diagslave Rancangan A	95
Gambar 3.85 Koneksi Diagslave Rancangan B.....	95
Gambar 3.86 Hasil Serangan Rancangan B.....	96
Gambar 3.87 Conpot Analytics Rancangan A	96
Gambar 3.88 Conpot Analytics Rancangan B	97
Gambar 3.89 Password List.....	98
Gambar 3.90 Pengujian Hydra Rancangan A	98
Gambar 3.91 Pengujian Hydra Rancangan B.....	99
Gambar 3.92 Hasil Pengujian Rancangan A.....	99

Gambar 3.93 Hasil Pengujian Rancangan B.....	100
Gambar 3.94 Pengujian Dengan username hendri R-A.....	100
Gambar 3.95 Pengujian Dengan username hendri R-B.....	101
Gambar 3.96 Hasil Pengujian Cowrie Pada Splunk R-A	101
Gambar 3.97 Hasil Pengujian Cowrie pada Splunk R-B.....	102
Gambar 3.98 Koneksi Port 22 Rancangan A	103
Gambar 3.99 Koneksi Port 22 Rancangan B.....	104
Gambar 3.100 Login pada server palsu R-A.....	105
Gambar 3.101 Login pada Server Palsu R-B.....	105
Gambar 3.102 Direktori opt server palsu.....	106
Gambar 3.103 Direktori opt server asli.....	106
Gambar 4.1 Sensor MHN Rancangan A	111
Gambar 4.2 Sensor MHN Rancangan B	111
Gambar 4.3 Grafik Perbandingan Conpot Cowrie	112
Gambar 4.4 Grafik Perbandingan Conpot Cowrie	113
Gambar 4.5 Overview Splunk Rancangan A	114
Gambar 4.6 Overview Splunk Rancangan B	114

INTISARI

Pada tahun 2010, terdapat berita besar ketika worm *Stuxnet* menyerang *Programmable Logic Controller* (PLC) pada fasilitas pengayaan nuklir di negara Iran. Secara halus memanipulasi data umpan balik pada unit sentrifugal yang dipercaya sebagai serangan pertama yang dilancarkan oleh sebuah negara sehingga fasilitas nuklir tersebut mengalami mati total.

Pada skripsi ini, peneliti mencoba untuk membuat dan membandingkan rancangan dari permasalahan yang ada dan mencoba memberikan informasi kepada admin sebuah jaringan untuk dapat menganalisa dan mendeteksi serangan yang tertuju pada sebuah sistem atau server. Dengan menggunakan *Modern Honey Network* sebagai pusat kendali untuk berbagai *honeypot*, dan dengan integrasi aplikasi Splunk yang dapat menampilkan data serangan secara grafik.

Aplikasi yang dibuat dalam penelitian ini mampu mendeteksi serangan yang tertuju pada server yang di tangkap oleh sensor *honeypot* yang akan di laporkan ke *Modern Honey Network* sebagai pusat untuk informasi dari setiap serangan dan juga Splunk yang dapat menampilkan data serangan tersebut ke dalam grafik dan juga info asal serangan dalam peta dunia.

Kata Kunci: *PLC, Modern Honey Network, Honeypot, Splunk, ICS, SCADA, Dionaea, Snort, Cowrie, Conpot*

ABSTRACT

In 2010, there was great news when the Stuxnet worm attacked the Programmable Logic Controller (PLC) at a nuclear enrichment facility in Iran. It subtly manipulates the feedback data on the centrifugal unit believed to be the first attack launched by a country so that the nuclear facility is totally dead.

In this thesis, researchers try to make and compare the design of the existing problems and try to provide information to the admin of a network to be able to analyze and detect attacks directed on a system or server. By using Modern Honey Network as the control center for various honeypot, and with Splunk application integration that can display graphical attack data.

The applications created in this study are able to detect attacks directed at the server captured by the sensor honeypot that will be reported to the Modern Honey Network as the center for information of each attack and also Splunk that can display the attack data into the graph and also the original info attack in the world map.

Keyword: *PLC, Modern Honey Network, Honeypot, Splunk, ICS, SCADA, Dionaea, Snort, Cowrie, Conpot*