



**ANALISIS KEAMANAN JARINGAN
SCADA *SYSTEM AUTOMATION* PADA PROSES
INDUSTRI**

TESIS
**Diajukan Sebagai Salah Satu Syarat Untuk Menyelesaikan
Program Pascasarjana Program Magister Teknik Elektro**

Oleh
Anas Nangim
55415110012

**PROGRAM PASCASARJANA
UNIVERSITAS MERCU BUANA
JAKARTA
2017**

PENGESAHAN TESIS

Judul : Analisis Keamanan Jaringan SCADA *System Automation*
Pada Proses Industri

Nama : Anas Nangim

Nim : 55415110012

Program : Pascasarjana

Konsentrasi : Securiti ICT

Tanggal :



UNIVERSITAS
MERCU BUANA

Dr. Hamzah Hilal, MS.c

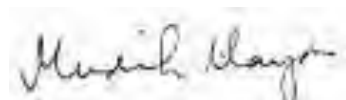
Mengesahkan

Direktur Pascasarjana



Prof. Dr. Didik Junaidi Rachbini

Ketua Program Studi



Prof. Dr.-Ing Mudrik Alaydrus

PERNYATAAN

Saya bertanda tangan di bawah ini menyatakan dengan sebenar-benarnya bahwa seluruh tulisan dan pernyataan tesis ini :

Judul : Analisis Keamanan Jaringan SCADA *System Automation* Pada Proses Industri

Nama : Anas Nangim

NIM : 55415110012

Program : Pascasarjana

Konsentrasi : Securiti ICT

Tanggal :

Merupakan hasil studi literatur, penelitian lapangan dan *penetrasi testing* oleh Penulis dengan bimbingan Pembimbing yang telah ditetapkan dengan surat keputusan Ketua Program Studi Magister Teknik Elektro Universitas Mercu Buana. Tesis ini belum pernah diajukan untuk memperoleh gelar magister pada program sejenis pada perguruan tinggi lain. Semua informasi, data dan hasil pengolahan yang digunakan, telah dinyatakan secara jelas sumber dan dapat diperiksa kebenarannya.

Jakarta, 28 September 2017

A yellow revenue stamp with a scalloped border. The text on the stamp includes "NETERAI TEMPEL" at the top, a Garuda logo on the right, the number "6000" in large bold letters, and "RUPIAH" below it. A unique identification number "T234AEF873412721" is printed in the middle. A black ink signature is written across the bottom of the stamp.

Anas Nangim

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Puji syukur kami panjatkan kehadiran Allah SWT yang telah memberikan karunia nikmat iman, islam, hidayah dan ilmu pengetahuan sehingga Kami dapat menyelesaikan dalam penyusunan tesis dengan judul **Analisis Keamanan Jaringan SCADA System Automation Pada Proses Industri**. Dalam penelitian ini masih terdapat banyak kekurangan, kami mengharapkan masukan, kritik dan saran yang bersifat membangun ke arah perbaikan dan penyempurnaan untuk penelitian selanjutnya.

Ucapan terima kasih Kami sampaikan kepada :

1. Istri tercinta Wahyu Listyorini, Kedua Orang Tua Ayah dan Ibu, Saudara kandung Kakak dan Adik yang selalu memberikan dukungan moral dan spiritual kepada Kami.
2. Dr. Hamzah Hilal, MS.c selaku dosen Pembimbing yang selalu memberikan pengarahan dalam penulisan tesis ini.
3. Prof. Dr.-Ing Mudrik Alaydrus selaku Ketua Program Studi Magister Teknik Elektro Universitas Mercu Buana yang telah memberikan dukungan sehingga dapat menyelesaikan penelitian ini.
4. Teman-teman seperjuangan Magister Teknik Elektro angkatan 17 Universitas Mercu Buana dan semua pihak yang tidak dapat disebutkan satu persatu yang telah memberikan dukungan dan doanya kepada kami.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Jakarta, 28 September 2017

Anas Nangim

DAFTAR ISI

	Halaman
Halaman Judul	1
Abstrak	Error! Bookmark not defined.
Abstract	Error! Bookmark not defined.
Pengesahan Tesis.....	2
Pernyataan	3
Kata Pengantar	4
Daftar Isi.....	5
Daftar Gambar	8
Daftar Tabel.....	9
Daftar Singkatan.....	10
Bab I Pendahuluan.....	Error! Bookmark not defined.
1.1 Latar Belakang	Error! Bookmark not defined.
1.2 Studi Literatur.....	Error! Bookmark not defined.
1.3 Rumusan Masalah	Error! Bookmark not defined.
1.4 Tujuan Penelitian.....	Error! Bookmark not defined.
1.5 Batasan Masalah.....	Error! Bookmark not defined.
1.6 Kontribusi.....	Error! Bookmark not defined.
1.7 Ruang Lingkup	Error! Bookmark not defined.
1.8 Sistematika Penulisan.....	Error! Bookmark not defined.
Bab II SCADA Dan Ancamannya.....	Error! Bookmark not defined.
2.1 SCADA	Error! Bookmark not defined.
2.2 Komponen SCADA.....	Error! Bookmark not defined.
2.2.1 <i>Remote Terminal Unit</i>	Error! Bookmark not defined.
2.2.2 <i>Master Terminal Unit</i>	Error! Bookmark not defined.
2.2.3 <i>Network</i>	Error! Bookmark not defined.
2.2.4 <i>Programmable Logic Controller</i>	Error! Bookmark not defined.
2.3 Ancaman SCADA	Error! Bookmark not defined.
2.3.1 <i>Bot Network Operators</i>	Error! Bookmark not defined.
2.2.2 <i>Criminal Groups</i>	Error! Bookmark not defined.
2.2.3 <i>Foreign Intelligence Services</i>	Error! Bookmark not defined.

2.2.4 Hackers	Error! Bookmark not defined.
2.2.5 Insiders	Error! Bookmark not defined.
2.2.6 Phishers	Error! Bookmark not defined.
2.2.7 Spammers	Error! Bookmark not defined.
2.2.8 Spyware Atau Malware	Error! Bookmark not defined.
2.2.9 Terrorists	Error! Bookmark not defined.
2.3 Serangan Terhadap SCADA.....	Error! Bookmark not defined.
2.3.1 Man-In-The-Middle Attack.....	Error! Bookmark not defined.
2.3.2 Opc/Dcom Attack	Error! Bookmark not defined.
2.4 Serangan Pada PLC	Error! Bookmark not defined.
2.4.1 Cryptographic Attacks.....	Error! Bookmark not defined.
2.4.2 Replay Attacks	Error! Bookmark not defined.
2.4.2 Fragmentation Attacks	Error! Bookmark not defined.
2.4.3 Dos Attacks	Error! Bookmark not defined.
2.5 Serangan Pada HMI.....	Error! Bookmark not defined.
2.5.1 Cryptographic Attacks.....	Error! Bookmark not defined.
2.5.2 Replay Attacks	Error! Bookmark not defined.
2.5.3 Fragmentation Attacks	Error! Bookmark not defined.
2.5.4 Dos Attacks	Error! Bookmark not defined.
2.5.5 Back Door Through Access Point /Internet ...	Error! Bookmark not defined.
defined.	
2.5.6 Sql Injection Attack	Error! Bookmark not defined.
Bab III Metodologi.....	Error! Bookmark not defined.
3.1 Metodologi Penelitian	Error! Bookmark not defined.
3.2 Desain Penelitian	Error! Bookmark not defined.
3.3 Instrumen Penelitian.....	Error! Bookmark not defined.
3.4 Hardware Pendukung Dan Spesifikasi	Error! Bookmark not defined.
3.5 Software Pendukung.....	Error! Bookmark not defined.
3.6 Komunikasi PLC Dengan Komputer ...	Error! Bookmark not defined.
3.7 Pembuatan Program PLC	Error! Bookmark not defined.
3.8 Pembuatan Program SCADA	Error! Bookmark not defined.
3.9 Kali Linux	Error! Bookmark not defined.

3.10 Kelebihan Dan Kekurangan <i>Kali Linux</i>	Error! Bookmark not defined.
A.Kelebihan <i>Kali Linux</i>	Error! Bookmark not defined.
B.Kekurangan <i>Kali Linux</i>	Error! Bookmark not defined.
3.11 Tool <i>Kali Linux</i>	Error! Bookmark not defined.
3.12 Menjalankan Pengukuran Data	Error! Bookmark not defined.
Bab IV Analisis Dan Hasil Pengujian	Error! Bookmark not defined.
4.1 Metode Keamanan SCADA	Error! Bookmark not defined.
4.2 Gambaran Alat Simulasi Serangan.....	Error! Bookmark not defined.
4.3 Penetrasi Testing	Error! Bookmark not defined.
4.4 Cara Mengetahui Sistem SCADA Terdapat Serangan.....	Error! Bookmark not defined.
Bookmark not defined.	
4.5 Visualisasi Penetrasi Testing HMI	Error! Bookmark not defined.
4.6 Langkah-Langkah Meningkatkan Keamanan Sistem SCADA .	Error! Bookmark not defined.
Bookmark not defined.	
4.7 Analisis <i>Traffic</i> Jaringan	Error! Bookmark not defined.
4.7.1 Metode Tanpa Serangan (Normal)	Error! Bookmark not defined.
4.7.2 Metode Dengan Serangan (Tidak Normal)	Error! Bookmark not defined.
defined.	
4.8 Analisis Hasil Pengujian	Error! Bookmark not defined.
Bab V Kesimpulan Dan Saran Kesimpulan Dan Saran ...	Error! Bookmark not defined.
defined.	
5.1 Kesimpulan.....	Error! Bookmark not defined.
5.2 Saran	Error! Bookmark not defined.
Daftar Pustaka	Error! Bookmark not defined.
Lampiran	Error! Bookmark not defined.

DAFTAR GAMBAR

	Halaman
<u>Gambar 1.1 Populasi Penyebaran <i>Worm Struxnet</i></u>	2
<u>Gambar 1.2 Perkembangan <i>Worm Struxnet</i></u>	3
<u>Gambar 2.1 Gambar SCADA</u>	8
<u>Gambar 2.2 Serangan OPC</u>	15
<u>Gambar 2.3 Capture Password Dengan <i>Wireshark</i></u>	15
<u>Gambar 2.4 Serangan <i>Back Door</i></u>	20
<u>Gambar 2.5 SQL Injection</u>	21
<u>Gambar 3.1 Diagram Flow Chat Penelitian</u>	23
<u>Gambar 3.2 Desain Penelitian</u>	24
<u>Gambar 3.3 Seting IP komputer</u>	26
<u>Gambar 3.4 Tes Komunikasi</u>	26
<u>Gambar 3.5 Program PLC <i>Penetrasi Testing</i></u>	27
<u>Gambar 3.6 Flowchart pembuatan SCADA</u>	28
<u>Gambar 3.7 Visualisasi SCADA</u>	29
<u>Gambar 3.8 <i>Kali Linux</i></u>	30
<u>Gambar 4.1 Tes Uji Coba Serangan</u>	34
<u>Gambar 4.2 <i>Scan</i> Dengan <i>Kali Linux</i></u>	35
<u>Gambar 4.3 Hasil <i>Scanning Port</i></u>	36
<u>Gambar 4.4 Serangan Yang Diblok</u>	37
<u>Gambar 4.5 Serangan Yang Terjadi Terus-menerus</u>	38
<u>Gambar 4.6 HMI Diserang Melalui Jaringan</u>	38
<u>Gambar 4.7 SCADA Tidak Menampilkan Kondisi <i>Realnya</i></u>	39
<u>Gambar 4.8 <i>Capture Data</i> Saat Kondisi Normal</u>	41

<u>Gambar 4.9 Capture Saat Kondisi Diserang</u>	43
<u>Gambar 4.10 Captur Disconeting Reques</u>	43
<u>Gambar 4.11 Hasil Penangkapan Penyerang</u>	45
<u>Gambar 4.12 Hasil Analisis Menggunakan Wireshark</u>	46

DAFTAR TABEL

.....	Halaman
<u>Tabel 1.1 Penelitian Terkait</u>	5
<u>Tabel 3.2 Tools Kali Linux</u>	31
<u>Tabel 4.1 Panjang Paket Normal</u>	41
<u>Tabel 4.2 Internet Protokol Normal</u>	41
<u>Tabel 4.3 Load Distribusi Normal</u>	42
<u>Tabel 4.4 Panjang Paket Tidak Normal</u>	44
<u>Tabel 4.5 Internet Protokol Tidak Normal</u>	44
<u>Tabel 4.6 Load Distibusi Tidak Normal</u>	44
<u>Tabel 4.7 Traffic Normal Dan Tidak Normal</u>	46
<u>Tabel 4.8 Rata-Rata Paket Normal Dan Tidak Normal</u>	46

UNIVERSITAS
 MERCU BUANA

DAFTAR SINGKATAN

RTU	: <i>Remote Terminal Unit</i>
SCADA	: <i>Supervisory Control and Data Acquisition</i>
HMI	: <i>Human Machinery Interface</i>
LAN	: <i>Lokal Area Networking</i>
TCP	: <i>Transport Control Protokol</i>
IP	: <i>Internet Protocol</i>
MTU	: <i>Master Terminal Unit</i>
PLC	: <i>Programable Logic Controller</i>
IT	: <i>Informasi Teknologi</i>
MAC Address	: <i>Media Access Control address</i>
DNP3	: <i>Distributed Network Protocol version 3</i>
DCS	: <i>Distributed Control System</i>
Modbus/IP	: <i>System Komunikasi Protokol Berbasis TCP/IP network</i>
FTP	: <i>File Transfer Protokol</i>
Http	: <i>Hypertext Transfer Protocol</i>
Https	: <i>Hypertext Transfer Protocol secure</i>
SSL	: <i>Secure Socket Layer</i>
TSL	: <i>Transport Layer Security</i>
FINS	: <i>Protokol Komunikasi PLC omron</i>
SQL	: <i>Structured Query Language</i>
MITM	: <i>Man in The Middle</i>

BUS	: Media Perpindahan Data dalam Komputer
PC	: <i>Pesonal Computer</i>
ARP	: <i>Address Resolution Protocol</i>
OPC	: <i>Open Platform Communication</i>
EIA	: <i>Eletronic Industries Association</i>
SONET	: <i>Synchronous Optical Network</i>
DEC	: <i>Digital Equipment Corporation</i>
DIX	: DEC Intel dan Xerox
IEEE	: <i>Institute of Electrical and Elektronik Engineers</i>
AP	: <i>Akses Point</i>
URL	: <i>Uniform Resource Locator</i>
BEAST	: <i>Browser Exploit Against</i>
ICS	: <i>Industrial Control system</i>
CMD	: <i>Command</i>



UNIVERSITAS
MERCU BUANA