# 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 | Tanda Tangan |
|---|---|
| **Melwin Syafrizal, S.Kom., M.Eng.**<br>**NIK. 190302105** | |
| **Hastari Utama, M.Cs.**<br>**NIK. 190302230** | |
| **Yudi Susanto, M.Kom.**<br>**NIK. 190302039** | |

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

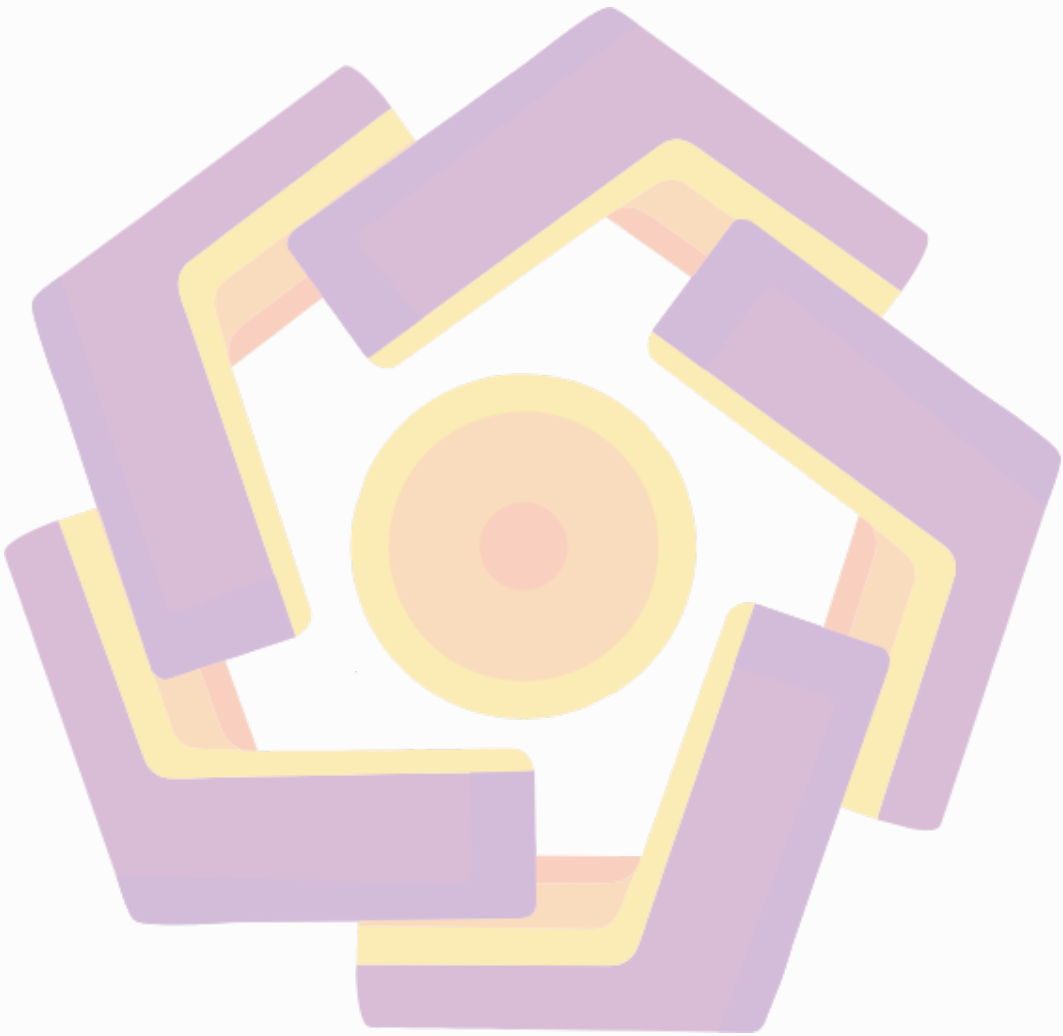
Alhamdulillah, segala puji syukur kehadirat Allah SWT Sang Maha Segalanya, sehingga skripsi dengan judul "**SIMULASI PERCOBAAN HONEYPOT BERBASIS MODERN HONEY NETWORK SEBAGAI IDENTIFIKASI SERANGAN PADA INDUSTRIAL CONTROL SYSTEM (ICS)**" dapat selesai dengan baik. Sebuah perjuangan dalam meraih gelar S. 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



# DAFTAR TABEL

# DAFTAR GAMBAR

# 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*