ii

**HALAMAN PENGESAHAN DOSEN PEMBIMBING**

# SIMULASI DAN ANALISIS *ENCRYPTION BASED RANSOMWARE* UNTUK MEMETAKAN EVOLUSI *RANSOMWARE*

**TUGAS AKHIR**

Disusun Oleh:


N a m a : Budi Ibnu Darmawan

NIM : 13523064


Yogyakarta, 11 November 2019

Pembimbing,

( Fietyata Yudha, S.Kom, M.Kom )

iii

**HALAMAN PENGESAHAN DOSEN PENGUJI**

# SIMULASI DAN ANALISIS *ENCRYPTION BASED RANSOMWARE* UNTUK MEMETAKAN EVOLUSI *RANSOMWARE*

## TUGAS AKHIR

Telah dipertahankan di depan sidang penguji sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer dari Program Studi Teknik Informatika di Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 11 November 2019

Tim Penguji

Fietyata Yudha, S.Kom., M.Kom.

**Anggota 1**

Ari Sujarwo, S.Kom., M.I.T.

**Anggota 2**

Kholid Haryono, S.T., M.Kom.

Mengetahui,

Ketua Program Studi Teknik Informatika – Program Sarjana

Fakultas Teknologi Industri

Universitas Islam Indonesia

( Dr. Raden Teduh Dirgahayu, S.T., M.Sc. )

iv

## HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama : Budi Ibnu Darmawan

NIM : 13523064

Tugas akhir dengan judul:

**SIMULASI DAN ANALISIS *ENCRYPTION BASED RANSOMWARE* UNTUK MEMETAKAN EVOLUSI *RANSOMWARE***

Menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila dikemudian hari terbukti ada beberapa bagian dari karya ini adalah bukan hasil karya sendiri, tugas akhir yang diajukan sebagai hasil karya sendiri ini siap ditarik kembali dan siap menanggung resiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 11 oktober 2019


( Budi Ibnu Darmawan)

# HALAMAN PERSEMBAHAN

Segala puji bagi Allah Subhanahu Wa Ta'ala, atas limpahan rahmat dan karunia yang tiada hentinya kepada saya, sehingga saya masih dapat merasakan nikmat Iman, Islam, Rezeki serta Kesehatan setiap harinya tanpa kurang suatu apapun.

Shalawat serta salam senantiasa tercurahkan untuk junjungan kita Nabi Muhammad Shalallahu "Alaihi Wasalam yang telah membawa kita dari zaman yang gelap menuju kepada zaman yang terang benderang. Semoga kita termasuk orang-orang yang mendapat syafaat dari Nabi Muhammad Shalallahu 'Alaihi Wasalam kelak pada hari akhir. Tugas Akhir ini saya persembahkan kepada:

1. Orang Tua saya, Bapak Kasna serta Ibu Baiq Wersih yang selalu memberikan dukungan serta doa untuk saya.
2. Kepada Adik saya, Muhammad Arif Gunawan serta keluarga besar yang selalu ada dan memberikan nasihat serta dukungan untuk saya.
3. Kepada Sahabat dan Teman-Teman yang ada disaat suka maupun duka selama masa perkuliahan saya.
4. Bapak Fietyata Yudha selaku pembimbing Tugas Akhir saya

Penulis menyadari bahwa skripsi ini masih jauh dari kata sempurna, oleh karena itu penulis mengharapkan saran agar skripsi ini menjadi lebih baik lagi.

## HALAMAN MOTO

Masalah akan terasa ringan dengan bersabar dan berlapang dada

***

Pendidikan bukan hanya untuk yang muda tapi untuk segala umur

# KATA PENGANTAR

*Assalamu'alaikum Warahmatullahi Wabarakatuh*

Alhamdulillahirobbilalamin, puji syukur kami panjatkan kehadirat Allah SWT atas limpahan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan Tugas Akhir yang berjudul "Simulasi dan Analisis Encryption Based *Ransomware* Untuk Memetakan Evolusi *Ransomware*". Laporan Tugas Akhir ini dibuat sebagai syarat untuk memperoleh gelar sarjana Teknik Informatika, Universitas Islam Indonesia. Penulis menyadari bahwa dalam pelaksanaan Tugas Akhir dan penyusunan laporan ini tidak dapat lepas dari bimbingan, dukungan dan bantuan dari berbagai pihak. Oleh karena itu perkenankanlah penulis untuk mengucapkan terima kasih dan penghargaan setinggi-tingginya kepada:

1. Allah SWT karena atas karunia-Nya, sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan baik dan semoga Tugas Akhir ini dapat memberikan manfaat di kemudian hari.
2. Orang Tua dan keluarga penulis atas segala doa dan dukungan selama penulis melaksanakan Tugas Akhir.
3. Bapak Fathul Wahid, selaku Rektor Universitas Islam Indonesia
4. Bapak R. Teduh Dirgahayu, selaku Ketua Jurusan Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia
5. Bapak Hendrik, selaku Dosen Pembimbing Akademik di Jurusan Teknik Informatika Fakultas, Teknologi Industri, Universitas Islam Indonesia
6. Bapak Fietyata Yudha, selaku Dosen Pembimbing Tugas Akhir di Jurusan Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia.
7. Sahabat-sahabat yang tergabung dalam grup KONTRAKAN NETIJEN, terima kasih untuk kebersamaan serta motivasi yang telah diberikan selama ini.
8. Sahabat-sahabat selama kuliah yang tergabung dalam grup CYBERDOTA, FPS KOK GAK KELIATAN, KOS SRI MULYONO yang tidak bisa disebutkan satu per satu. Terima kasih untuk kebersamaan dan keceriaan yang telah dilewati bersama.
9. Teman-teman angkatan 2013 (ETERNITY) di Jurusan Teknik Informatika, Universitas Islam Indonesia yang telah memberikan kenangan indah selama kuliah.
10. Semua pihak yang telah banyak membantu dalam pelaksanaan Tugas Akhir yang tidak dapat penulis sebutkan satu per satu.

Penulis menyadari bahwa laporan Tugas Akhir ini masih belum sempurna. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun agar Tugas Akhir ini menjadi lebih baik. Akhir kata, semoga laporan ini dapat bermanfaat dan atas segala bantuan yang telah diberikan semoga mendapat imbalan yang setimpal dari Allah SWT, Amin. Wassalamu'alaikum Warahmatullahi Wabarakatuh

Yogyakarta, 11 Oktober 2019

( Budi Ibnu Darmawan )

# SARI

Institusi yang memliki banyak pengguna internet pasti mempunyai beberapa masalah yang dihadapi oleh pengelola jaringan. Salah satunya adalah penyerangan dari orang yang memiliki niat jahat. Mereka yang melakukan itu untuk kepentingan dia sendiri seperti mengunci data privasi target, melakukan perusakan data atau file. Biasanya pelaku tersebut menyisipkan program yang telah dirancang untuk kepentingannya sendiri kedalam suatu jaringan atau bisa juga melalui aplikasi dan file program itu disebut dengan istilah *Malicious Software (*malware).

Pada penelitian menggunakan tools Cuckoo Sandbox ini, langkah pertama yang harus dilakukan adalah membangun lingkungan penelitian. Lingkungan penelitian ini menggunakan mesin linux yaitu Ubuntu 16.04. agar simulasi dan analisis dapat dilakukan, mesin Linux harus diatur agar dapat menjalankan simulasi dengan cara memasang Virtualbox pada mesin Linux tempat simulasi dan analisis yang akan dijalankan. Virtualbox adalah software virtualisasi untuk memasang sebuah sistem operasi, dimana Virtualbox akan diinstal sistem operasi Ubuntu 16.04

Setelah melakukan penelitan menggunakan tools Cuckoo Sandbox dengan objek *Ransomware* Wannacry, Petya, NotPetya dan Badrabbit penguji menarik kesimpulan bahwa penulis berhasil membangun lingkungan penelitian menggunakan sistem operasi Ubuntu 16.04 LTS. Cuckoo Sandbox dapat diinstal dengan dan dapat terintegrasi dengan baik kepada mesin Virtualbox sebagai wadah eksekusi dan analisis sampel *Ransomware* Wannacry, Petya, NotPetya dan Badrabbit. Kemudian penulis berhasil mengimplementasikan sampel *Ransomware* pada perangkat Windows melalui virtualbox. Dan menganalisis hasil dari tiap *Ransomware* dengan menggunakan Cuckoo Sandbox.

# GLOSARIUM

| | |
|---|---|
| Sandbox | : mekanisme keamanan untuk memisahkan program yang sedang berjalan |
| *Ransomware* | : sebuah software yang dapat menyusup ke sistem operasi sehingga dapat merusak sistem, juga dapat mencuri file-file penting yang ada pada sistem dan mengunci. |
| Plugin | : fungsi atau fitur tambahan yang digabungkan ke sebuah sistem untuk menambah kemampuan dan kinerja sistem tersebut. |
| Cuckcoo Sandbox | : tool yang digunakan untuk mengolah sampel malware |
| RSA | : merupakan salah satu algoritma public key yang populer dipakai dan bahkan masih dipakai hingga saat ini |
| AES | : merupakan algoritma yang menggunakan kunci enkripsi dan kunci dekripsi yang sama |
| CAT | : kategori tingkat bahanya Ransomware |