



**UJI KERENTANAN PENERAPAN *INTERNET OF THINGS*  
(*IOT*) PADA JARINGAN *SMARTHOME* MENGGUNAKAN  
CISCO PACKET TRACER DENGAN METODE *SQUARE***

**LAPORAN SKRIPSI**

**JULIUS DANES NUGROHO**

**4817050199**

**KONSENTRASI KEAMANAN SISTEM INFORMASI  
PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN  
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER  
POLITEKNIK NEGERI JAKARTA**

**2022**



© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta



# UJI KERENTANAN PENERAPAN *INTERNET OF THINGS* (*IOT*) PADA JARINGAN *SMARTHOME* MENGGUNAKAN CISCO PACKET TRACER DENGAN METODE *SQUARE*

## LAPORAN SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan  
untuk Memperoleh Diploma Empat Politeknik

**JULIUS DANES NUGROHO**

4817050199

**POLITEKNIK  
NEGERI  
JAKARTA**

**KONSENTRASI KEAMANAN SISTEM INFORMASI**

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN**

**JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER**

**POLITEKNIK NEGERI JAKARTA**

2022

### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



## LEMBAR PERNYATAAN ORISINALITAS

**Skripsi ini adalah hasil karya saya sendiri,  
dan semua sumber baik yang dikutip maupun dirujuk  
telah saya nyatakan dengan benar.**

**Nama : Julius Danes Nugroho**

**NIM : 4817050199**

**Tanggal : 5 Juli 2022**

**Tanda Tangan :**

**POLITEKNIK  
NEGERI  
JAKARTA**

- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
    - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
    - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
  2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta







## LEMBAR PENGESAHAN

Skripsi ini diajukan oleh:

Nama : Julius Danes Nugroho  
NIM : 4817050199  
Program Studi : Teknik Multimedia dan Jaringan  
Judul Skripsi : Uji Kerentanan Penerapan *Internet of Things (IoT)* Pada Jaringan *Smarthome* Menggunakan Cisco Packet Tracer Dengan Metode *SQUARE*

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Selasa, Tanggal 5, Bulan Juli, Tahun 2022, dan dinyatakan **LULUS**.

Disahkan oleh

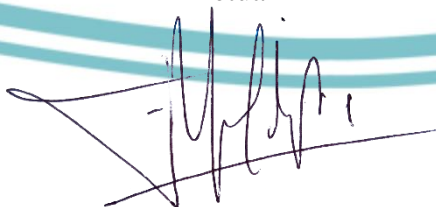
Pembimbing : Dr. Prihatin Oktivasari, S.Si., M.Si. (  )  
Penguji I : Maria Agustin, S.Kom., M.Kom. (  )  
Penguji II : Indra Hermawan, S.Kom., M.Kom. (  )  
Penguji III : Asep Kurniawan, S.Pd., M.Kom. (  )



Mengetahui,

Jurusan Teknik Informatika dan Komputer

Ketua



Mauldy Laya S.Kom., M.Kom.,

NIP. 197802112009121003

**Hak Cipta :**  
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :  
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan satu masalah.  
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta  
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta


## KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan laporan skripsi ini. Penulisan laporan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Diploma Empat Politeknik Negeri Jakarta. Penulis menyadari bahwa tanpa bantuan, bimbingan, dan saran dari berbagai pihak, penulis sangatlah sulit bagi penulis untuk dapat menyelesaikan laporan skripsi ini dengan baik. Oleh karena itu, pada kesempatan ini penulis mengucapkan terima kasih kepada:

1. Orang tua dan keluarga penulis yang telah memberikan bantuan dukungan materil dan moral selama kegiatan penelitian skripsi.
2. Ibu Dr. Prihatin Oktivasari, S.Si., M.Si. selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penelitian dan kegiatan penyusunan laporan skripsi.
3. Bapak Mauldy Laya, S.Kom., M.Kom. selaku Kepala Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta.
4. Seluruh jajaran Dosen dan Staf Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta.

Akhir kata, penulis berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga laporan Skripsi ini membawa manfaat bagi pengembangan ilmu pengetahuan khususnya di bidang teknologi.

Depok, Juni 2022

  
Julius Danes Nugroho

### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta





## HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Julius Danes Nugroho  
NIM : 4817050199  
Program Studi : Teknik Multimedia dan Jaringan  
Jurusan : Teknik Informatika dan Komputer  
Jenis karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty- Free Right*)** atas karya ilmiah saya yang berjudul:

### **Uji Kerentanan Penerapan *Internet of Things (IoT)* Pada Jaringan *Smart*home Menggunakan Cisco Packet Tracer Dengan Metode *SQUARE***

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Politeknik Negeri Jakarta berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di Depok Pada tanggal: 5 Juli 2022

Yang menyatakan

  
Julius Danes Nugroho

- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
    - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
    - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
  2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



## Uji Kerentanan Penerapan *Internet of Things (IoT)* Pada Jaringan *Smarthome* Menggunakan Cisco Packet Tracer Dengan Metode *SQUARE*

### ABSTRAK

*Internet* memungkinkan orang untuk berinteraksi satu sama lain dan dengan objek. Salah satu perkembangan teknologi saat ini yang semakin populer adalah *Internet of Things (IoT)*. Berdasarkan survei IEEE, terjadi tren peningkatan dari tahun 2016 hingga 2017 seperti di bidang automasi industri, *smarthome/cities*, dan keamanan *IoT*. Meningkatnya penggunaan internet menghadirkan tantangan bagi semua kalangan mengenai kebutuhan keamanan jaringan yang digunakan. Penulis membahas tentang keamanan jaringan pada bidang *Smarthome Internet of Things*. Penelitian ini dilakukan untuk menemukan dan mengurangi kerentanan keamanan pada infrastruktur *Smarthome-Home Server* dan *Smarthome-Remote Server*, serta untuk meningkatkan prioritas kebutuhan keamanan yang dibutuhkan. Studi ini dilakukan untuk mengidentifikasi dan mengurangi kerentanan keamanan di infrastruktur *Smarthome-Home Server* dan *Smarthome-Remote Server*, dan untuk meningkatkan prioritas persyaratan keamanan yang diperlukan. Penelitian ini menggunakan metode *SQUARE* untuk menggabungkan beberapa metode penilaian risiko untuk menghasilkan persyaratan keamanan untuk lima skenario ancaman jaringan yang berbeda. Skenario ancaman jaringan diantaranya *reveal SSID*, *rogue access point*, *data sniffing*, *MAC address spoofing*, dan *denial of service (DoS)*. Hasil penelitian ini menunjukkan bahwa ada beberapa persyaratan keamanan yang harus ditempatkan pada *Smarthome-Home Server* dan *Smarthome-Remote Server*.

**Kata Kunci:** *Internet of Things*, Keamanan Jaringan, Metode *SQUARE*, *Smarthome*.

#### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritis atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

## DAFTAR ISI

LEMBAR PERNYATAAN ORISINALITAS .....	ii
LEMBAR PENGESAHAN .....	iii
KATA PENGANTAR.....	iv
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS .....	v
ABSTRAK.....	vi
DAFTAR ISI.....	vii
DAFTAR TABEL .....	ix
DAFTAR GAMBAR.....	x
DAFTAR LAMPIRAN .....	xii
<b>BAB 1 PENDAHULUAN .....</b>	<b>1</b>
1.1. Latar Belakang Masalah.....	1
1.2. Perumusan Masalah .....	6
1.3. Batasan Masalah.....	7
1.4. Tujuan dan Manfaat .....	8
1.5. Sistematika Penulisan.....	9
<b>BAB 2 TINJAUAN PUSTAKA.....</b>	<b>10</b>
2.1. Penelitian Sejenis .....	10
2.2. Keamanan Jaringan .....	16
2.3. Aspek-Aspek Keamanan Jaringan .....	17
2.4. Internet of Things (IoT) .....	18
2.5. <i>Smarthome Network</i> (Jaringan Rumah Cerdas) .....	20
2.6. <i>Smarthome-Home Server</i> dan <i>Smarthome-Remote Server</i> .....	21
2.7. <i>Software as a Service Model (SaaS)</i> .....	21
2.8. <i>Dynamic Host Configuration Protocol (DHCP)</i> .....	22
2.9. <i>Domain Name System (DNS)</i> .....	22
2.10. <i>Service Set Identifier (SSID)</i> .....	22
2.11. <i>MAC Address</i> .....	22
2.12. <i>Internet of Things (IoT) Security Attack Models</i> .....	22





**Hak Cipta :**

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritis atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

2.13.	<i>Internet of Things (IoT) Security Threat Types</i> .....	23
2.14.	Penyalahgunaan Sistem/Ancaman ( <i>Misusecase</i> ) .....	26
2.15.	Penyerang ( <i>Attacker</i> ).....	27
2.16.	<i>Protocol Data Unit (PDU)</i> .....	28
2.17.	<i>Internet Service Provider (ISP)</i> .....	28
2.18.	IPv4/IPv6.....	28
2.19.	<i>Penetration Testing</i> .....	28
2.20.	<i>Vulnerability Assessment</i> .....	29
2.21.	Cisco Packet Tracer.....	29
2.22.	Metode <i>SQUARE (Security Quality Requirements Engineering)</i> .....	31
<b>BAB 3 PERENCANAAN DAN REALISASI .....</b>		<b>32</b>
3.1.	Tahapan Simulasi .....	32
3.2.	Mengidentifikasi Tujuan Keamanan .....	33
3.3.	Pemodelan Sistem Jaringan <i>IoT</i> .....	34
3.4.	Tahapan Pengujian .....	44
3.5.	Tahapan Analisis .....	47
<b>BAB 4 PEMBAHASAN .....</b>		<b>52</b>
4.1.	Hasil Pengujian .....	52
4.2.	Hasil Analisis .....	74
<b>BAB 5 PENUTUP.....</b>		<b>80</b>
5.1.	Kesimpulan .....	80
5.2.	Saran.....	81
<b>DAFTAR PUSTAKA .....</b>		<b>82</b>
<b>LAMPIRAN.....</b>		<b>85</b>



**UJI KERENTANAN PENERAPAN *INTERNET OF THINGS*  
(*IOT*) PADA JARINGAN *SMARTHOME* MENGGUNAKAN  
CISCO PACKET TRACER DENGAN METODE *SQUARE***

**LAPORAN SKRIPSI**

**JULIUS DANES NUGROHO**

**4817050199**

**KONSENTRASI KEAMANAN SISTEM INFORMASI  
PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN  
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER  
POLITEKNIK NEGERI JAKARTA**

**2022**



© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta



# UJI KERENTANAN PENERAPAN *INTERNET OF THINGS* (*IOT*) PADA JARINGAN *SMARTHOME* MENGGUNAKAN CISCO PACKET TRACER DENGAN METODE *SQUARE*

## LAPORAN SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan  
untuk Memperoleh Diploma Empat Politeknik

**JULIUS DANES NUGROHO**

4817050199

**POLITEKNIK  
NEGERI  
JAKARTA**

**KONSENTRASI KEAMANAN SISTEM INFORMASI**

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN**

**JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER**

**POLITEKNIK NEGERI JAKARTA**

2022

### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



## LEMBAR PERNYATAAN ORISINALITAS

**Skripsi ini adalah hasil karya saya sendiri,  
dan semua sumber baik yang dikutip maupun dirujuk  
telah saya nyatakan dengan benar.**

**Nama : Julius Danes Nugroho**

**NIM : 4817050199**

**Tanggal : 5 Juli 2022**

**Tanda Tangan :**

**POLITEKNIK  
NEGERI  
JAKARTA**

- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
    - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
    - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
  2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan satu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta





## LEMBAR PENGESAHAN

Skripsi ini diajukan oleh:

Nama : Julius Danes Nugroho  
NIM : 4817050199  
Program Studi : Teknik Multimedia dan Jaringan  
Judul Skripsi : Uji Kerentanan Penerapan *Internet of Things (IoT)* Pada Jaringan *Smarthome* Menggunakan Cisco Packet Tracer Dengan Metode *SQUARE*

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Selasa, Tanggal 5, Bulan Juli, Tahun 2022, dan dinyatakan **LULUS**.

Disahkan oleh

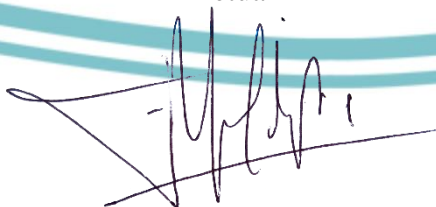
Pembimbing : Dr. Prihatin Oktivasari, S.Si., M.Si. (  )  
Penguji I : Maria Agustin, S.Kom., M.Kom. (  )  
Penguji II : Indra Hermawan, S.Kom., M.Kom. (  )  
Penguji III : Asep Kurniawan, S.Pd., M.Kom. (  )

POLITEKNIK  
NEGERI  
JAKARTA

Mengetahui,

Jurusan Teknik Informatika dan Komputer

Ketua



Mauldy Laya S.Kom., M.Kom.,

NIP. 197802112009121003


## KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan laporan skripsi ini. Penulisan laporan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Diploma Empat Politeknik Negeri Jakarta. Penulis menyadari bahwa tanpa bantuan, bimbingan, dan saran dari berbagai pihak, penulis sangatlah sulit bagi penulis untuk dapat menyelesaikan laporan skripsi ini dengan baik. Oleh karena itu, pada kesempatan ini penulis mengucapkan terima kasih kepada:

1. Orang tua dan keluarga penulis yang telah memberikan bantuan dukungan materil dan moral selama kegiatan penelitian skripsi.
2. Ibu Dr. Prihatin Oktivasari, S.Si., M.Si. selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penelitian dan kegiatan penyusunan laporan skripsi.
3. Bapak Mauldy Laya, S.Kom., M.Kom. selaku Kepala Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta.
4. Seluruh jajaran Dosen dan Staf Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta.

Akhir kata, penulis berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga laporan Skripsi ini membawa manfaat bagi pengembangan ilmu pengetahuan khususnya di bidang teknologi.

Depok, Juni 2022

  
Julius Danes Nugroho

### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta





## HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Julius Danes Nugroho  
NIM : 4817050199  
Program Studi : Teknik Multimedia dan Jaringan  
Jurusan : Teknik Informatika dan Komputer  
Jenis karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty- Free Right*)** atas karya ilmiah saya yang berjudul:

### **Uji Kerentanan Penerapan *Internet of Things (IoT)* Pada Jaringan *Smarthome* Menggunakan Cisco Packet Tracer Dengan Metode *SQUARE***

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Politeknik Negeri Jakarta berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di Depok Pada tanggal: 5 Juli 2022

Yang menyatakan

  
Julius Danes Nugroho

- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
    - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
    - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
  2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



## Uji Kerentanan Penerapan *Internet of Things (IoT)* Pada Jaringan *Smarthome* Menggunakan Cisco Packet Tracer Dengan Metode *SQUARE*

### ABSTRAK

*Internet* memungkinkan orang untuk berinteraksi satu sama lain dan dengan objek. Salah satu perkembangan teknologi saat ini yang semakin populer adalah *Internet of Things (IoT)*. Berdasarkan survei IEEE, terjadi tren peningkatan dari tahun 2016 hingga 2017 seperti di bidang automasi industri, *smarthome/cities*, dan keamanan *IoT*. Meningkatnya penggunaan internet menghadirkan tantangan bagi semua kalangan mengenai kebutuhan keamanan jaringan yang digunakan. Penulis membahas tentang keamanan jaringan pada bidang *Smarthome Internet of Things*. Penelitian ini dilakukan untuk menemukan dan mengurangi kerentanan keamanan pada infrastruktur *Smarthome-Home Server* dan *Smarthome-Remote Server*, serta untuk meningkatkan prioritas kebutuhan keamanan yang dibutuhkan. Studi ini dilakukan untuk mengidentifikasi dan mengurangi kerentanan keamanan di infrastruktur *Smarthome-Home Server* dan *Smarthome-Remote Server*, dan untuk meningkatkan prioritas persyaratan keamanan yang diperlukan. Penelitian ini menggunakan metode *SQUARE* untuk menggabungkan beberapa metode penilaian risiko untuk menghasilkan persyaratan keamanan untuk lima skenario ancaman jaringan yang berbeda. Skenario ancaman jaringan diantaranya *reveal SSID*, *rogue access point*, *data sniffing*, *MAC address spoofing*, dan *denial of service (DoS)*. Hasil penelitian ini menunjukkan bahwa ada beberapa persyaratan keamanan yang harus ditempatkan pada *Smarthome-Home Server* dan *Smarthome-Remote Server*.

**Kata Kunci:** *Internet of Things*, Keamanan Jaringan, Metode *SQUARE*, *Smarthome*.

#### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritis atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

## DAFTAR ISI

LEMBAR PERNYATAAN ORISINALITAS .....	ii
LEMBAR PENGESAHAN .....	iii
KATA PENGANTAR.....	iv
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS .....	v
ABSTRAK.....	vi
DAFTAR ISI.....	vii
DAFTAR TABEL .....	ix
DAFTAR GAMBAR.....	x
DAFTAR LAMPIRAN .....	xii
<b>BAB 1 PENDAHULUAN .....</b>	<b>1</b>
1.1. Latar Belakang Masalah.....	1
1.2. Perumusan Masalah .....	6
1.3. Batasan Masalah.....	7
1.4. Tujuan dan Manfaat .....	8
1.5. Sistematika Penulisan.....	9
<b>BAB 2 TINJAUAN PUSTAKA.....</b>	<b>10</b>
2.1. Penelitian Sejenis .....	10
2.2. Keamanan Jaringan .....	16
2.3. Aspek-Aspek Keamanan Jaringan .....	17
2.4. Internet of Things (IoT) .....	18
2.5. <i>Smarthome Network</i> (Jaringan Rumah Cerdas) .....	20
2.6. <i>Smarthome-Home Server</i> dan <i>Smarthome-Remote Server</i> .....	21
2.7. <i>Software as a Service Model (SaaS)</i> .....	21
2.8. <i>Dynamic Host Configuration Protocol (DHCP)</i> .....	22
2.9. <i>Domain Name System (DNS)</i> .....	22
2.10. <i>Service Set Identifier (SSID)</i> .....	22
2.11. <i>MAC Address</i> .....	22
2.12. <i>Internet of Things (IoT) Security Attack Models</i> .....	22



**Hak Cipta :**

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritis atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

2.13.	<i>Internet of Things (IoT) Security Threat Types</i> .....	23
2.14.	Penyalahgunaan Sistem/Ancaman ( <i>Misusecase</i> ) .....	26
2.15.	Penyerang ( <i>Attacker</i> ).....	27
2.16.	<i>Protocol Data Unit (PDU)</i> .....	28
2.17.	<i>Internet Service Provider (ISP)</i> .....	28
2.18.	IPv4/IPv6.....	28
2.19.	<i>Penetration Testing</i> .....	28
2.20.	<i>Vulnerability Assessment</i> .....	29
2.21.	Cisco Packet Tracer.....	29
2.22.	Metode <i>SQUARE (Security Quality Requirements Engineering)</i> .....	31
<b>BAB 3 PERENCANAAN DAN REALISASI .....</b>		<b>32</b>
3.1.	Tahapan Simulasi .....	32
3.2.	Mengidentifikasi Tujuan Keamanan .....	33
3.3.	Pemodelan Sistem Jaringan <i>IoT</i> .....	34
3.4.	Tahapan Pengujian .....	44
3.5.	Tahapan Analisis .....	47
<b>BAB 4 PEMBAHASAN .....</b>		<b>52</b>
4.1.	Hasil Pengujian .....	52
4.2.	Hasil Analisis .....	74
<b>BAB 5 PENUTUP.....</b>		<b>80</b>
5.1.	Kesimpulan .....	80
5.2.	Saran.....	81
<b>DAFTAR PUSTAKA .....</b>		<b>82</b>
<b>LAMPIRAN.....</b>		<b>85</b>



## DAFTAR TABEL

Tabel 2.1 Perbandingan Literatur Sejenis Dengan Penulis .....	10
Tabel 2.2 Kelebihan dan Kekurangan Literatur Sejenis Dengan Penulis .....	14
Tabel 3.1 Arsitektur Simulasi Pencarian dan Analisa Keamanan Sistem Jaringan .....	32
Tabel 3.2 Tujuan Bisnis Sistem Jaringan <i>Smarthome Internet of Things</i> .....	33
Tabel 3.3 Tujuan Kemanan Sistem Jaringan <i>Smarthome Internet of Things</i> .....	34
Tabel 3.4 Simulasi Perangkat yang Digunakan Dalam <i>Smarthome-Home Server</i>	38
Tabel 3.5 Simulasi Perangkat yang Digunakan Dalam <i>Smarthome-Remote Server</i> .....	41
Tabel 3.6 Aktivitas <i>Misusecase (MC)</i> yang Mungkin Terjadi Dalam <i>Smarthome-Home Server</i> dan <i>Smarthome-Remote Server</i> .....	46
Tabel 3.7 Metode Penilaian Risiko .....	47
Tabel 3.8 Nilai Perbandingan Teknik <i>Risk Assessment</i> .....	48
Tabel 3.9 Nilai Perbandingan Teknik Elisitasi Kriteria <i>Risk Assessment</i> .....	49
Tabel 3.10 Hasil Tingkat Penilaian Risiko Model <i>NIST</i> dan <i>Haimes</i> .....	50
Tabel 4.1 Simulasi Perangkat Penyerang yang Digunakan Dalam <i>Reveal SSID (MC-1)</i> .....	55
Tabel 4.2 Simulasi Perangkat Penyerang yang Digunakan Dalam <i>Rogue Access Point (MC-2)</i> .....	61
Tabel 4.3 Simulasi Perangkat Penyerang yang Digunakan Dalam <i>Data Sniffing (MC-3)</i> .....	64
Tabel 4.4 Simulasi Perangkat Penyerang yang Digunakan Dalam <i>MAC Address Spoofing (MC-4)</i> .....	69
Tabel 4.5 Simulasi Perangkat Penyerang yang Digunakan Dalam <i>Distributed Denial of Service (MC-5)</i> .....	73
Tabel 4.6 Kategori Tingkat Ancaman Serangan Pada Jaringan <i>Smarthome 1 Home Server</i> .....	74
Tabel 4.7 Kategori Tingkat Ancaman Serangan Pada Jaringan <i>Smarthome 2 Remote Server</i> .....	75
Tabel 4.8 Elisitasi Persyaratan Keamanan .....	76
Tabel 4.9 Kategori Persyaratan Keamanan .....	78
Tabel 4.10 Prioritas Persyaratan Keamanan .....	79

### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritis atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



## DAFTAR GAMBAR

Gambar 1.1	Indonesia Peringkat ke-6 Dunia Dalam Pertumbuhan Pengguna Internet Berdasarkan Survei <i>e-Marketer</i> .....	1
Gambar 1.2	Pertumbuhan Pengguna Internet di Indonesia Berdasarkan Survei APJII .....	2
Gambar 1.3	Statistik Perbandingan Konektivitas <i>IoT</i> Sepanjang Tahun 2015 Hingga 2017 .....	3
Gambar 1.4	Statistik Tren <i>IoT</i> Sepanjang Tahun 2016 Hingga 2017 .....	4
Gambar 3.1	Ilustrasi Alur Simulasi Pencarian dan Analisa Keamanan Sistem Jaringan .....	32
Gambar 3.2	Topologi Jaringan <i>Smarthome 1 Home Server</i> .....	35
Gambar 3.3	Topologi Jaringan <i>Smarthome 2 Cloud Server (SaaS)</i> .....	36
Gambar 3.4	Arsitektur <i>Smarthome 1 Home Server</i> .....	37
Gambar 3.5	Perangkat <i>IoT</i> Telah Terhubung ke <i>Smarthome 1 Home Server</i> .....	39
Gambar 3.6	Program <i>SBC Garage Door</i> Jaringan <i>Smarthome 1 Home Server</i> ....	40
Gambar 3.7	Arsitektur <i>Smarthome 2 (SaaS) Remote Server</i> .....	41
Gambar 3.8	Perangkat <i>IoT</i> Telah Terhubung ke <i>Smarthome 2 Remote Server</i> ....	43
Gambar 3.9	<i>Use Case</i> Diagram Aktivitas Dalam Sistem Jaringan <i>Smarthome</i> ....	44
Gambar 3.10	Skenario Pohon Serangan Dalam Sistem Jaringan <i>Smarthome</i> .....	45
Gambar 4.1	Konfigurasi <i>SSID Broadcast Router Smarthome 1 Home Server</i> ....	52
Gambar 4.2	<i>Available SSID Network Smarthome 1</i> di <i>Laptop Attacker</i> .....	53
Gambar 4.3	Konfigurasi <i>SSID Broadcast Router Smarthome 2 Remote Server</i> ...	54
Gambar 4.4	<i>Available SSID Network Smarthome 2</i> di <i>Laptop Attacker</i> .....	54
Gambar 4.5	<i>Rogue Access Point SSID Network Smarthome 1</i> di <i>Laptop Attacker</i> .....	55
Gambar 4.6	<i>Beacon Frame Rogue Access Point Smarthome 1</i> di <i>Laptop Attacker</i> .....	56
Gambar 4.7	Perangkat Sah Terkoneksi ke <i>Rogue Access Point Smarthome 1</i> di <i>Laptop Attacker</i> .....	57
Gambar 4.8	Perangkat Sah Melakukan Koneksi ke <i>Home Server Address</i> Melalui <i>Rogue Access Point Smarthome 1</i> di <i>Laptop Attacker</i> .....	57
Gambar 4.9	Perangkat Penyerang Menerima <i>Packet Broadcast</i> dari <i>Rogue Access Point Smarthome 1</i> di <i>Laptop Attacker</i> .....	58
Gambar 4.10	<i>Rogue Access Point SSID Network Smarthome 2</i> di <i>Laptop Attacker</i> .....	59
Gambar 4.11	Perangkat Sah Terkoneksi ke <i>Rogue Access Point Smarthome 2</i> di <i>Laptop Attacker</i> .....	60
Gambar 4.12	Perangkat Sah Melakukan Koneksi ke <i>Remote Server Address</i> Melalui <i>Rogue Access Point Smarthome 2</i> di <i>Laptop Attacker</i> .....	60

### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



## Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritis atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

Gambar 4.13 Perangkat Penyerang Menerima <i>Packet Broadcast</i> dari <i>Rogue Access Point Smarthome 2</i> di <i>Laptop Attacker</i> .....	61
Gambar 4.14 Perangkat Penyerang Melakukan <i>Data Sniffing</i> ke <i>Home Server</i> Dalam Jaringan .....	62
Gambar 4.15 Pengguna Sah Mengakses <i>FTP IoT Server</i> .....	62
Gambar 4.16 Lalu Lintas <i>Packet</i> yang <i>Ter-capture</i> Melalui Perangkat <i>Sniffer</i> Penyerang.....	63
Gambar 4.17 Perangkat <i>Sniffer</i> Penyerang Melakukan <i>Packet Capturing</i> Jaringan <i>Smarthome-Remote Server</i> .....	64
Gambar 4.18 Perangkat Penyerang Melakukan <i>Packet Flooding</i> ke Perangkat-Perangkat Sah Dalam Jaringan <i>Smarthome-Home Server</i> .....	65
Gambar 4.19 Trafik Data Perangkat Penyerang Melakukan <i>Packet Flooding</i> ke Perangkat-Perangkat Sah Dalam Jaringan .....	65
Gambar 4.20 Perangkat <i>Switch</i> Penyerang Mengumpulkan <i>MAC Address Table</i> Perangkat Sah Dalam Jaringan.....	66
Gambar 4.21 Perangkat Penyerang Mengubah <i>MAC Address</i> Perangkat Menjadi Salah Satu <i>MAC Address</i> Perangkat Sah .....	66
Gambar 4.22 Perangkat Penyerang Melakukan <i>Packet Flooding</i> ke Perangkat-Perangkat Sah Dalam Jaringan <i>Smarthome-Remote Server</i> .....	67
Gambar 4.23 Perangkat <i>Switch</i> Penyerang Mengumpulkan <i>MAC Address Table</i> Perangkat Sah Dalam Jaringan <i>Smarthome 2</i> .....	68
Gambar 4.24 Perangkat Penyerang Mengubah <i>MAC Address</i> Perangkat Menjadi Salah Satu <i>MAC Address</i> Perangkat Sah .....	68
Gambar 4.25 Perangkat Penyerang Melakukan <i>DDoS</i> pada Jaringan <i>Smarthome-Home Server</i> .....	69
Gambar 4.26 Koneksi Perangkat <i>IoT</i> Terputus Dikarenakan Serangan <i>DDoS</i> ke <i>Home Server</i> .....	70
Gambar 4.27 Paket yang Dikirimkan Penyerang pada Jaringan <i>Home Server</i> .....	70
Gambar 4.28 Perangkat Penyerang Melakukan <i>DDoS</i> pada Jaringan <i>Smarthome-Remote Server</i> .....	71
Gambar 4.29 Paket yang Dikirimkan Penyerang pada Jaringan <i>Remote Server</i> ..	71
Gambar 4.30 Paket yang Dikirimkan Penyerang Membebani <i>Home Router</i> .....	72
Gambar 4.31 Layanan <i>IoT Server</i> Lambat dan Tidak Dapat Diakses.....	72

## DAFTAR LAMPIRAN

Lampiran 1 - Daftar Riwayat Hidup .....	85
---	----



© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

# BAB 1

## PENDAHULUAN

### 1.1. Latar Belakang Masalah

Pertumbuhan jumlah pengguna internet di dunia saat ini terus bertambah. Penggunaan internet juga meningkat untuk keperluan bisnis/organisasi, hiburan, jejaring sosial dan pendidikan. Meningkatnya jumlah pengguna internet di seluruh dunia menjadi tantangan bagi semua kalangan mengenai kebutuhan keamanan jaringan yang digunakan. Indonesia merupakan salah satu negara yang jumlah pengguna internetnya terus meningkat dan terus bertambah. Menurut lembaga riset pasar *e-Marketer*, gambar 1.1, penduduk Indonesia yang terkoneksi internet mencapai 83,7 juta pada tahun 2014 dan diperkirakan akan terus tumbuh hingga 2018, mencapai 123 juta. Hal ini menjadikan Indonesia sebagai negara ke-6 di dunia dalam hal pertumbuhan pengguna internet setelah Jepang.

	2013	2014	2015	2016	2017	2018
1. China*	620.7	643.6	669.8	700.1	736.2	777.0
2. US**	246.0	252.9	259.3	264.9	269.7	274.1
3. India	167.2	215.6	252.3	283.8	313.8	346.3
4. Brazil	99.2	107.7	113.7	119.8	123.3	125.9
5. Japan	100.0	102.1	103.6	104.5	105.0	105.4
6. Indonesia	72.8	83.7	93.4	102.8	112.6	123.0
7. Russia	77.5	82.9	87.3	91.4	94.3	96.6
8. Germany	59.5	61.6	62.2	62.5	62.7	62.7
9. Mexico	53.1	59.4	65.1	70.7	75.7	80.4
10. Nigeria	51.8	57.7	63.2	69.1	76.2	84.3
11. UK**	48.8	50.1	51.3	52.4	53.4	54.3
12. France	48.8	49.7	50.5	51.2	51.9	52.5
13. Philippines	42.3	48.0	53.7	59.1	64.5	69.3
14. Turkey	36.6	41.0	44.7	47.7	50.7	53.5
15. Vietnam	36.6	40.5	44.4	48.2	52.1	55.8
16. South Korea	40.1	40.4	40.6	40.7	40.9	41.0
17. Egypt	34.1	36.0	38.3	40.9	43.9	47.4
18. Italy	34.5	35.8	36.2	37.2	37.5	37.7
19. Spain	30.5	31.6	32.3	33.0	33.5	33.9
20. Canada	27.7	28.3	28.8	29.4	29.9	30.4
21. Argentina	25.0	27.1	29.0	29.8	30.5	31.1
22. Colombia	24.2	26.5	28.6	29.4	30.5	31.3
23. Thailand	22.7	24.3	26.0	27.6	29.1	30.6
24. Poland	22.6	22.9	23.3	23.7	24.0	24.3
25. South Africa	20.1	22.7	25.0	27.2	29.2	30.9
<b>Worldwide***</b>	<b>2,692.9</b>	<b>2,892.7</b>	<b>3,072.6</b>	<b>3,246.3</b>	<b>3,419.9</b>	<b>3,600.2</b>

Note: Individuals of any age who use the internet from any location via any device at least once per month; \*excludes Hong Kong; \*\*forecast from Aug 2014; \*\*\*includes countries not listed  
Source: eMarketer, Nov 2014

Gambar 1.1 Indonesia Peringkat ke-6 Dunia Dalam Pertumbuhan Pengguna Internet Berdasarkan Survei *e-Marketer*

Sumber: Kominfo, 2018

Hasil survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet (APJII), gambar 1.2, juga menunjukkan bahwa lebih dari separuh penduduk Indonesia kini sudah terkoneksi dengan Internet. Dalam survei yang dilakukan oleh APJII pada tahun 2011, terdapat 88 juta pengguna internet. Hal ini diikuti oleh survei yang dilakukan sepanjang tahun 2016, yang menunjukkan bahwa jumlah pengguna

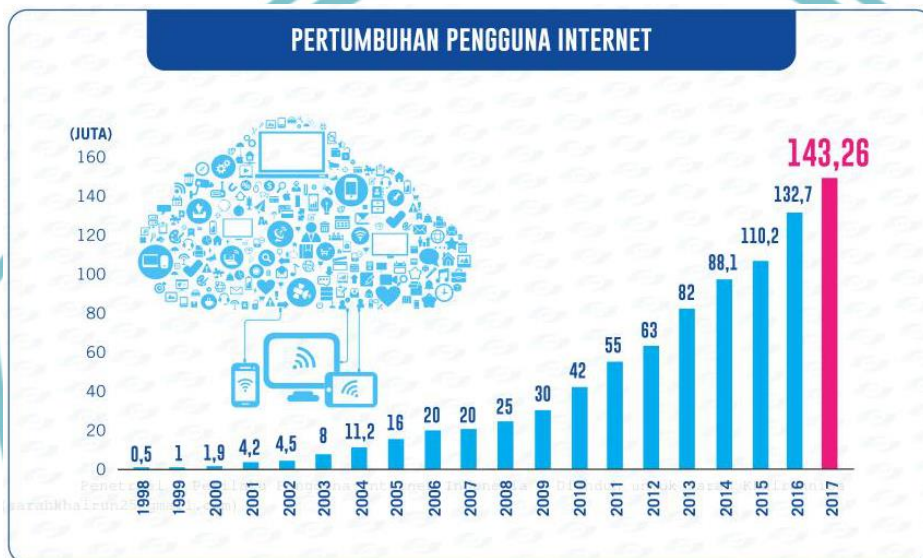


## © Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

internet meningkat 51,8% dibandingkan pengguna internet pada tahun 2011. Pada tahun 2016, 132,7 juta orang Indonesia terhubung ke Internet, anak-anak Jumlah ini berlanjut ke tahun 2017. Pada tahun 2017, 3,26 juta orang Indonesia terhubung ke Internet, setengah dari total penduduk Indonesia sekitar 256,2 juta. Menurut Presiden APJII Jamalul Izza, penyebab pertumbuhan pengguna internet di Indonesia adalah karena perkembangan infrastruktur dan kemudahan memperoleh *smartphone* atau perangkat *mobile*.



Gambar 1.2 Pertumbuhan Pengguna Internet di Indonesia Berdasarkan Survei APJII

Sumber: Technasia, 2018

Produk *Internet of Things* yang paling terkenal adalah *smartcity* dan *smarthomes*. *Internet of Things* merupakan teknologi yang menghubungkan dunia nyata dan dunia maya, yang menjadikan teknologi tersebut menarik dalam membuat dunia menjadi lebih pintar (IEEE Journal 2016). Konsep *Internet of Things* adalah integrasi dari banyak teknologi yang berbeda. *Internet of Things* didukung oleh pengembangan *RFID*, sensor pintar, teknologi komunikasi, dan protokol Internet. Dalam evolusinya, Internet, *smartphone*, dan teknologi *machine-to-machine (M2M)* merupakan tahap pertama dari *Internet of Things*. Di tahun depan, *Internet of Things* diharapkan menjadi salah satu penghubung utama antara teknologi yang





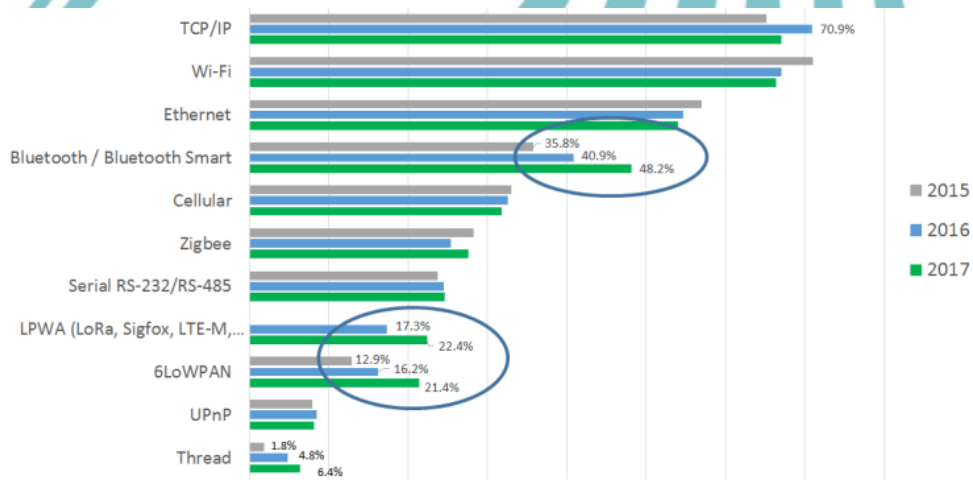
## © Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

berbeda dengan menghubungkan objek fisik cerdas bersama-sama dan memungkinkan aplikasi yang berbeda untuk mendukung *smart decision making*.

Teknologi perangkat elektronik saat ini yang biasa ditemui dan tergabung dalam *Internet of Things* adalah *smartphone*, tablet, komputer, *router*, dan *CCTV*, serta jenis perangkat elektronik berkemampuan jaringan lainnya yang dapat berkabel atau nirkabel untuk berbagi data atau *remote control*. Implementasi *Internet of Things* didukung dengan perkembangan teknologi jaringan dan internet seperti IPv6, 4G dan Wimax, dimana penulis menitikberatkan pada konektivitas protokol internet dari penggunaan internet dari Hal. Penggunaan teknologi jaringan dan internet merupakan hasil survei, gambar 1.3, dengan tingkat pertumbuhan tren *IoT* tertinggi selama 2016 hingga 2017 yang dilakukan oleh IEEE.



Gambar 1.3 Statistik Perbandingan Konektivitas *IoT* Sepanjang Tahun 2015 Hingga 2017

Sumber: IEEE, 2018

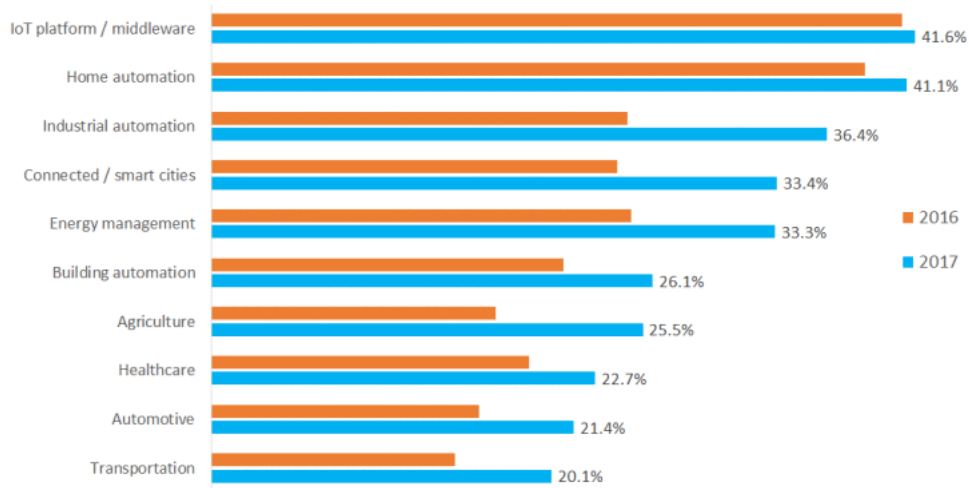
Internet kini telah menjadi kebutuhan esensial dalam kehidupan masyarakat di berbagai bidang seperti bisnis/organisasi, hiburan, media sosial dan pendidikan. Pertumbuhan pengguna Internet di Indonesia menyisakan banyak ruang bagi Indonesia untuk mengadopsi teknologi seperti *Internet of Things*. Hal ini membuat Internet dan *Internet of Things* penting dan diperlukan untuk perkembangannya. Kehadiran *Internet of Things* dalam Perkembangannya Berdasarkan survei pada Gambar 1.4, yang dilakukan oleh IEEE, terdapat tren peningkatan dari tahun 2016



**Hak Cipta :**

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

hingga 2017, seperti di bidang industri automasi, *smarthome/city* dan keamanan *IoT*. Dalam bidang ini, penulis berfokus pada area keamanan jaringan di *Internet of Things Smarthome*.



Gambar 1.4 Statistik Tren *IoT* Sepanjang Tahun 2016 Hingga 2017

Sumber: IEEE, 2018

Pertumbuhan jumlah pengguna internet di Indonesia terus meningkat karena perkembangan infrastruktur dan kemudahan perangkat elektronik portabel. Hal ini menjadi nilai positif dalam industri *networking* di Indonesia. Namun, meningkatnya jumlah pengguna Internet di seluruh dunia menimbulkan tantangan bagi semua kelompok dalam hal keamanan jaringan yang digunakan. Kekhawatiran tentang keamanan dan privasi Internet semakin meluas di komunitas global. Pada tahun 2014, survei Pew Research Center menemukan bahwa sekitar 80 responden di Amerika Serikat mengatakan mereka "setuju" atau "sangat setuju" bahwa orang Amerika harus peduli dengan pengawasan pemerintah, panggilan telepon, dan koneksi internet. Di Indonesia, kekhawatiran tentang keamanan siber dan privasi Internet telah berubah menjadi kekhawatiran dengan munculnya beberapa kasus peretasan yang terjadi pada tahun 2016 dan 2017. Dua di antaranya adalah kasus peretasan yang diserang oleh organisasi peretas situs web komersial terhadap PT. Global Network yang mengoperasikan Tiket.com ini mengalami kerugian hingga Rp 1,9 miliar berdasarkan keterangan polisi yang dilansir kantor berita CNN Indonesia. Tiket.com adalah situs perdagangan yang menawarkan jual beli tiket



## © Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

pesawat, hotel dan kereta api secara *online*. Belakangan, peretasan juga dialami oleh situs salah satu operator telekomunikasi seluler di Indonesia, PT. Telekomunikasi Seluler (Telkomsel). Kasus peretasan bisa sangat merugikan korban peretasan, terutama dari segi reputasi/moral dan kerugian materi. Pelaku penyerangan *website* tersebut diidentifikasi sebagai kelompok *hacker website* komersial yang anggotanya masih pelajar berdasarkan keterangan polisi yang dilansir CNN Indonesia. Hal ini menimbulkan kesadaran masyarakat akan pentingnya keamanan internet, dalam hal ini *Internet of Things* yang akan penulis bahas.

Kondisi jaringan komunikasi rumah yang aman tentu menjadi hal yang sangat penting, hal ini tentunya akan membuat rasa nyaman dan meningkatnya produktifitas penghuni rumah. Adanya perkembangan tersebut maka hal-hal yang berkaitan dengan sarana dan prasarananya menjadi hal utama yang harus dikaji dan dipersiapkan agar proses komunikasi/informasi tetap terjaga dengan baik dan aman (*secure*). Sistem *smarthome IoT* ini menggunakan kombinasi beberapa sistem pintar seperti *smart garage doors*, *smart alarm detection*, *smart renewable energy* dan lain-lain dengan menggunakan beberapa perangkat diantaranya seperti *SBC (Single Board Computer)*, *IoT server*, *home tablet*, *home router*, *smartphone*, *motion sensor*, *smoke detector*, *smart lamp*, *security camera*, *siren*, *AC*, dan *solar panel-battery*. Kondisi ini yang terimplementasi secara riil tentu saja jika akan ada perubahan dan atau lainnya maka akan berpengaruh terhadap kondisi *smarthome* yang ada tersebut. Sehingga untuk menjaga keamanan *smarthome* ini maka perlu adanya upaya untuk melakukan terobosan secara simulasi sehingga biaya dan lainnya dapat dihemat. Salah satu metode yang dapat digunakan untuk melakukan uji atas simulasi kerentanan pada *smarthome* ini dapat menggunakan metode *SQUARE (Security Quality Requirements Engineering)* yang menyediakan identifikasi dan analisis kebutuhan dengan pendekatan masalah non-fungsional ke fungsional dan memberikan hasil keluaran berupa kategori dan prioritas keamanan.

Dalam penelitian ini menggunakan model proses metodologi *SQUARE (Security Quality Requirements Engineering)* yang dikembangkan oleh Nancy R. Mead, Eric D. Hough, dan Theodore R. Stehney di *Carnegie Mellon University*. Dasar

**Jurusan Teknik Informatika dan Komputer – Politeknik Negeri Jakarta**

### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



**Hak Cipta :**

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

pemilihan metodologi tersebut karena proses ini akan menghasilkan kategorisasi dan memprioritaskan kebutuhan keamanan untuk sistem. Fokus dari metodologi ini adalah untuk membangun konsep keamanan dalam tahapan awal dari siklus rekayasa sistem. Model ini juga dapat digunakan untuk mendokumentasikan dan menganalisis aspek keamanan sistem dalam hal perbaikan maupun improvisasi dan modifikasi sistem dimasa depan.

Beberapa penelitian telah dilakukan oleh Isa Shemsi (Shemsi, 2018) yang menerapkan Infrastruktur dan Arsitektur *Smarthome IoT* menggunakan Cisco Packet Tracer Simulator, Andrea Finardi (Finardi, 2018) yang menerapkan Infrastruktur dan Arsitektur *IoT* menggunakan Cisco Packet Tracer Simulator, Zainab Alansari et al (Alansari et al., 2018) mengkaji infrastruktur, arsitektur, keamanan dan privasi, Ernita Dwi Meutia (E. D. Meutia, J. Teknik, E. Universitas, 2015) yang mengkaji keamanan dan privasi *IoT*. Yopi Hidayatul (Yopi, 2015) yang mengevaluasi keamanan jaringan *wireless hotspot* menggunakan metode *SQUARE*, dan Airin (Airin & Nurul, 2021) yang mengkaji uji kerentanan pada *smarthome IoT* untuk mendukung *smart campus*.

Berdasarkan masalah yang telah disebutkan, maka tujuan yang ingin dicapai dari penelitian ini adalah menemukan kerentanan, memberikan kategori dan prioritas keamanan dalam jaringan *Smarthome* baik di *Home Server* dan *Remote Server* dalam penerapan *Internet of Things (IoT)* dengan menggunakan metode *SQUARE (Security Quality Requirements Engineering)*.

### 1.2. Perumusan Masalah

Berdasarkan permasalahan yang muncul, penulis mengajukan rumusan permasalahan dalam penelitian ini, yaitu bagaimana menguji kerentanan penerapan *Internet of Things (IoT)* pada jaringan *smarthome* menggunakan Cisco Packet Tracer dengan metode *SQUARE (Security Quality Requirements Engineering)* untuk memindai kerentanan dan memberikan kategori dan prioritas keamanan di jaringan *Smarthome-Home Server* dan *Smarthome-Remote Server*?



**Hak Cipta :**

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

### 1.3. Batasan Masalah

Berdasarkan permasalahan yang ada, maka penulis membatasi masalah dalam penelitian ini, yaitu:

#### 1.3.1 Metode

1. Metode yang digunakan adalah metode *SQUARE (Security Quality Requirements Engineering)* dengan teknik *Vulnerability Assessment*.
2. Metode pengumpulan data yang digunakan adalah studi literatur, survei, dan simulasi.

#### 1.3.2 Tools

1. Simulasi menggunakan Cisco Packet Tracer ver.8.1.1 yang mendukung lebih banyak perangkat *IoT*.
2. Perangkat virtual jaringan komputer pada simulator Cisco Packet Tracer ver 8.1.1 dalam ruang lingkup *IoT Smarthome*
3. Sistem operasi Windows 11 *Home Single Language*.
4. Laptop ASUS A442UR Processor Intel Core i5-8250U, CPU @ 1.60GHz, Memory 12 GB RAM, Disk Drive HDD 1TB

#### 1.3.3 Proses

1. Konektivitas yang dianalisis adalah IPv4 dan *MAC Address*.
2. Menggunakan dua skenario infrastruktur yakni, *Smarthome-Home Server* dan *Smarthome-Remote Server*.
3. Jaringan *Smarthome Internet of Things (IoT)* yang dianalisis merupakan referensi dari jurnal.
4. Skenario serangan yang disimulasikan dalam ruang lingkup *Smarthome* dan *endpoint/perangkat Smarthome*.
5. Skenario serangan yang disimulasikan sebanyak 5 *misusecase*, yakni *Reveal SSID, Rogue Access Point, Data Sniffing, MAC Address Spoofing*, dan *DDoS*.
6. Skenario serangan yang disimulasikan ditentukan kesimpulan tingkat ancaman serangan berdasarkan dampak yang terjadi dan parameter yang terpenuhi.



## © Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

7. Output penelitian ini berupa hasil analisis berupa kategori (*privacy, integrity, authentication, availability, access control, dan non-repudiation*) dan prioritas keamanan yang dihasilkan dengan metode *SQUARE (Security Quality Requirements Engineering)* dalam *Smarthome-Home Server* dan *Smarthome-Remote Server* dan saran.

### 1.4. Tujuan dan Manfaat

#### 1.4.1 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk menguji kerentanan penerapan *Internet of Things (IoT)* pada jaringan *smarthome* menggunakan Cisco Packet Tracer dengan metode *SQUARE* yang dianggap dapat mencari kerentanan dan memberikan kategori dan prioritas keamanan pada jaringan *Smarthome-Home Server* dan *Smarthome-Remote Server*.

#### 1.4.2 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah:

##### 1.4.2.1 Bagi Masyarakat

- a. Dapat mengetahui pentingnya uji kerentanan jaringan.
- b. Diharapkan hasil analisis penelitian penulis dapat menjadi bahan evaluasi dalam perkembangan *internet of things* di Indonesia khususnya dalam bidang *IoT security*.
- c. Dapat dijadikan referensi dalam melakukan uji kerentanan jaringan untuk keperluan akademik.

##### 1.4.2.2 Bagi Penulis

Keamanan siber saat ini dapat dialami untuk perkembangannya di Indonesia, khususnya di *Internet of Things*. Indonesia adalah negara dengan potensi pengguna internet yang terus meningkat, dalam hal ini merupakan suatu kehormatan untuk terlibat dalam upaya keamanan siber.

##### 1.4.2.3 Bagi Institusi Pendidikan

- a. Mengetahui kemampuan mahasiswa dalam menerapkan ilmunya dan sebagai bahan evaluasi.



**Hak Cipta :**

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

- b. Menambah referensi kepustakaan Politeknik Negeri Jakarta.

### 1.5. Sistematika Penulisan

Dalam penyusunan skripsi ini, pembahasan penulis sajikan dalam beberapa pokok bahasan, diantaranya adalah:

#### I. BAB I PENDAHULUAN

Pada bab ini, menerangkan latar belakang penelitian, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metode penelitian dan sistematika penulisan.

#### II. BAB II TINJAUAN PUSTAKA

Pada bab ini membahas tentang konsep dan teori yang mendasari permasalahan yang digunakan dalam penyusunan penelitian ini. Literatur yang digunakan merupakan buku ataupun penelitian sejenis yang mendukung.

#### III. BAB III PERENCAAN DAN REALISASI

Pada bab ini berisi penjelasan analisa keamanan jaringan dalam *Smarthome Internet of Things (IoT)* menggunakan simulator Cisco Packet Tracer dengan metode *SQUARE* berdasarkan landasan teori yang telah diuraikan sebelumnya. Skenario serangan yang dibuat menerapkan teknik *penetration test* dan *vulnerability assessment*.

#### IV. BAB IV PEMBAHASAN

Pada bab ini berisi hasil dan pembahasan yang didapat dari penelitian yang dilakukan penulis.

#### V. BAB V PENUTUP

Pada bab ini berisi kesimpulan dari hasil penelitian yang telah dilakukan penulis dan saran untuk pengembangan penelitian selanjutnya.



## BAB 5 PENUTUP

### 5.1. Kesimpulan

1. Berdasarkan rumusan masalah dan hasil dari tahapan-tahapan metode *SQUARE* yang telah dilakukan, proses analisis, pencarian dan mitigasi *misusecase* jaringan pada *Smarthome-Home Server* dan *Smarthome-Remote Server* dengan kriteria *security goals* yang disimulasikan dengan Cisco Packet Tracer Simulator dapat disimpulkan bahwa konfigurasi awal pada jaringan tidak sepenuhnya aman. Konfigurasi awal pada jaringan terbukti memiliki kerentanan terhadap 5 skenario *misusecase* jaringan yang telah dilakukan pengujian pada penelitian ini.
2. Berdasarkan hasil semua skenario analisis, pencarian dan mitigasi *misusecase* jaringan menunjukkan tingkat kerentanan ancaman serangan yang beragam untuk setiap skenario pada kedua jaringan *smarthome*. Namun demikian hasil penilaian risiko, pada tabel 4.6 dan 4.7, menunjukkan *Smarthome-Home Server* dan *Smarthome-Remote Server* memiliki tingkat risiko kerentanan yang sama untuk setiap skenario *misusecase*. Adapun *misusecase* dengan tingkat kerentanan tertinggi untuk dua skenario *smarthome* yakni *Data Sniffing* dan *Distributed Denial of Service (DDoS)*.
3. Dampak dari kondisi skenario *misusecase* jaringan yang ditemukan terbukti tidak memenuhi kriteria *security goals* yakni *Privacy, Integrity, Authentication, Availability, Access Control*. Sehingga dimunculkan suatu kategori persyaratan keamanan jaringan dari skenario *misusecase* berdasarkan tingkat risiko *misusecase* pada tabel 4.9 yang dibagi menjadi 4 kategori grup dan memberikan solusi teknis dalam rangka penerapan *IoT* dalam jaringan *smarhome*.
4. Berdasarkan tabel 4.8 elisitasi persyaratan keamanan dan tabel 4.9 kategori persyaratan keamanan dikelompokkan prioritas persyaratan keamanan pada tabel 4.10 yang diajukan untuk jaringan *Smarthome-Home Server* dan

#### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta





*Smarthome-Remote Server* yang diprioritaskan ke dalam 3 kriteria keamanan yakni *Privacy, Authentication, dan Availability*. Rekomendasi yang diajukan berupa penerapan protokol enkripsi manajemen jaringan, *firewall filtering*, dan rutin memperbarui identifikasi akun yang diperlukan sebagai mitigasi dari risiko yang telah disimulasikan.

## 5.2. Saran

Penulis menyadari bahwa Uji Kerentanan Penerapan *Internet of Things (IoT)* Pada Jaringan *Smarthome* ini masih memiliki beberapa kekurangan dan keterbatasan. Oleh karena itu, penulis menyarankan untuk melakukan pengembangan selanjutnya agar menjadi lebih baik. Berikut beberapa pertimbangan untuk penelitian selanjutnya, diantaranya:

1. Melakukan penelitian pencarian dan mitigasi lebih lanjut pada *Smarthome-Home Server* dan *Smarthome-Remote Server* maupun infrastruktur *internet of things (IoT)* lainnya untuk menemukan ancaman dan prioritas keamanan yang belum berhasil ditemukan oleh penulis dalam protokol dan infrastruktur *internet of things (IoT)* lainnya.
2. Menggunakan infrastruktur *smarthome internet of things (IoT)* sebenarnya ataupun penggunaan aplikasi simulator lainnya untuk melakukan analisis dan mitigasi ancaman keamanan.

### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



## DAFTAR PUSTAKA

Akbar, Y. H., 2015. Evaluasi Keamanan Jaringan Wireless Hotspot Menggunakan Metode SQUARE (Studi Kasus Warnet Medianet Sumedang).

Alansari, Z. et al., 2018. *Internet of Things: Infrastructure, Architecture, Security, and Privacy*. Southend, United Kingdom, University of Essex.

Anon., n.d. *Internet of Things Guide*. [Online]  
Available at: <https://internetofthingswiki.com/internet-of-things-securityguide/1112>  
[Accessed 25 April 2022].

Cisco, 2017. *What Is Network Security*. Retrieved from CISCO. [Online]  
Available at: <https://www.cisco.com/c/en/us/products/security/what-is-networksecurity.html>

Finardi, A., 2018. IoT Simulations with Cisco Packet Tracer.

IEEE, 2018. *IoT Towards Definition Internet of Things Issue*. [Online]  
Available at: [https://iot.ieee.org/images/files/pdf\\_IEEE\\_IoT\\_Towards\\_Definition\\_Internet\\_of\\_Things\\_Issuel\\_14MAY15.pdf](https://iot.ieee.org/images/files/pdf_IEEE_IoT_Towards_Definition_Internet_of_Things_Issuel_14MAY15.pdf)

King, N., 2003. *SMART HOME – A DEFINITION*. [Online]  
Available at: [https://www.housinglin.org.uk/\\_assets/Resources/Housing/Housing\\_advice/Smart\\_Home - A definition September 2003.pdf](https://www.housinglin.org.uk/_assets/Resources/Housing/Housing_advice/Smart_Home_-_A_definition_September_2003.pdf)  
[Accessed July 2022].

Kominfo, n.d. *Pengguna Internet Indonesia Nomor Enam Dunia*. [Online]  
Available at: [https://kominfo.go.id/content/detail/4286/pengguna-internet-indonesia-nomor-enam-dunia/0/sorotan\\_media](https://kominfo.go.id/content/detail/4286/pengguna-internet-indonesia-nomor-enam-dunia/0/sorotan_media)

### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



**Hak Cipta :**

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

Kompas Gramedia, 2017. *Pengguna Internet Indonesia Capai 132 Juta*. [Online] Available at:

<https://tekno.kompas.com/read/2016/10/24/15064727/2016.pengguna.internet.di.idonesia.capai.132.juta>

Manuaba, I. B. V. H., Hidayat, R. & Kusumawardani, S. S., 2012. Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus: Kantor Pusat Fakultas Teknik Universitas Gadjah Mada).

McClelland, C., 2018. *IoT Explained – How Does an IoT*. [Online] Available at: <https://www.iotforall.com/iot-explained-how-does-an-iot-systemactually->

Mead, N. R., Hough, E. D., Stehney II & Theodore R, 2005. *Security Quality Requirements Engineering (SQUARE) Methodology*. s.l.:s.n.

Meutia, E. D., 2015. *Internet of Things – Keamanan dan Privasi*. s.l.:s.n.

Netacad Cisco, n.d. *About Packet Tracer*. [Online] Available at: <https://www.netacad.com/courses/packet-tracer>

Rouse, M., 2018. *What is the Internet of Things*. [Online] Available at: <https://internetofthingsagenda.techtarget.com/definition/Internet-of->

Shemsi, I., 2018. Implementing Smart Home Using Cisco Packet Tracer. *International Journal of Engineering Science Invention*, JANUARY.Vol. IV(Issue VII, JANUARY 2018).

Sihombing, O., 2018. Smart Home Design for Electronic Devices. *Journal of Physics: Conf. Series 1007 (2018) 012021*.

Stallings, W., 1995. *Network And Internetwork Security: Principles And Practice*. Prentice Hall. s.l.:s.n.

Techinasia, 2021. *Hampir Setengah Penduduk Indonesia*. [Online] Available at: <https://id.techinasia.com/jumlah-pengguna-internet-indonesia-2014->



## © Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

2018

[Accessed April 2022].

TelecomAcadmey, 2018. *What is IPv6.* [Online]

Available at: <http://telecomacadmey.com/what-isi-pv6>

YourDictionary, 2018. *Network Security.* [Online]

Available at: <http://www.yourdictionary.com/network-security>



### Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



**Hak Cipta :**

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
  - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

## DAFTAR RIWAYAT HIDUP

### LAMPIRAN



Julius Danes Nugroho

Lahir di Jakarta, 24 Juni 1999

Pendidikan yang telah penulis tempuh yaitu SD Santo Markus I Jakarta Timur lulus pada tahun 2011, SMP Santo Markus I Jakarta Timur lulus pada tahun 2014, dan SMA Negeri 14 Jakarta Timur lulus pada tahun 2017. Saat ini sedang menempuh pendidikan Diploma IV Program Studi Teknik Informatika Jurusan Teknik Informatika dan Komputer di Politeknik Negeri Jakarta.

POLITEKNIK  
NEGERI  
JAKARTA