



**RANCANG BANGUN IDS DAN IPS MENGGUNAKAN  
BASE SNORT PADA SERANGAN DATA FLOODING  
PADA JARINGAN JURUSAN TIK PNJ**

**LAPORAN SKRIPSI**

**Dita Nurhayati  
4817050111**

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN  
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER  
POLITEKNIK NEGERI JAKARTA  
2021**



## **RANCANG BANGUN KEAMANAN SISTEM SERVER**

### **RANCANG BANGUN IDS DAN IPS MENGGUNAKAN BASE SNORT PADA SERANGAN DATA FLOODING PADA JARINGAN JURUSAN TIK PNJ**

#### **LAPORAN SKRIPSI**

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

**DITA NURHAYATI**

**4817050111**


**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN  
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER  
POLITEKNIK NEGERI JAKARTA**

**2021**



## HALAMAN PERNYATAAN ORISINALITAS

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

Nama : Dita Nurhayati  
NIM : 4817050111  
Tanggal : 30 Juni 2021  
Tanda Tangan : 

### 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 PENGESAHAN

Skripsi diajukan oleh:

Nama : Dita Nurhayati  
NIM : 4817050111  
Program Studi : Teknik Multimedia dan Jaringan  
Judul Skripsi : Rancang Bangun IDS dan IPS Menggunakan Base Snort  
Pada Serangan Data Flooding Pada Jaringan Jurusan TIK  
PNJ

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Rabu, Tanggal 30,  
Bulan Juni Tahun 2021 dan dinyatakan **LULUS**.

Disahkan oleh

Pembimbing I : Fachroni Arbi Murad, S.Kom., M.Kom. (FAM)

Penguji I : Maria Agustin, S.Kom., M.Kom. (Maun)

Penguji II : Muhammad Yusuf Bagus Rasyiidin, S.Kom., M.T.I. (YBR)

Penguji III : Ariawan Andi Suhandana, S.Kom., M.T.I. (AS)

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, pennisan karya ilmiah, pennisan laporan, pennisan kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



## KATA PENGANTAR

Puji Syukur saya panjatkan kepada Tuhan Yang Maha Esa, 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 Sarjana Terapan Politeknik. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan laporan skripsi, sangatlah sulit bagi penulis untuk menyelesaikan skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

- a. Bapak Fachroni Arbi Murad, S.Kom., M.Kom. selaku dosen pembimbing yang telah memberikan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan skripsi ini;
- b. Bapak Defiana Arnaldy, S.Tp., M.Si. selaku kepala program studi serta dosen yang juga telah ikut membantu untuk mengarahkan penulis dalam penyusunan skripsi ini;
- c. Orang tua dan keluarga penulis yang sudah memberikan bantuan dukungan penuh secara moral dan material;
- d. Cahya Mulyadi dan Jahuda Dolf Bacas yang telah memberikan support selama penyusunan skripsi ini;
- e. Suci Rahmadhani, selaku teman satu tim, satu perjuangan dalam penyusunan laporan skripsi ini yang telah memberikan bantuan dukungan secara moral;
- f. Sahabat saya “Paguyuban Memantik” yang terdiri dari Laily Rachmi Tsani, Trisya Talia David, Suci Rahmadhani, Sabrina Annisa Adrienda, dan Refina Julianita yang selalu menemani saya berbulan-bulan dari pagi hingga pagi kembali Menyusun skripsi ini; dan
- g. Teman-teman “Bismillah”, teman kelas satu perjuangan dari awal hingga akhir masa perkuliahan yang tidak pernah putus memberikan semangat.

Akhir kata, penulis berharap Allah SWT. Membalas segala kebaikan semua pihak yang telah membantu. Semoga laporan skripsi ini dapat bermanfaat bagi semua masyarakat.

Bogor, 30 Juni 2021

Penulis

### 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 menggunakan 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 dibawah ini:

Nama : Dita Nurhayati  
NIM : 4817050111  
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:

### **Rancang Bangun IDS dan IPS Menggunakan Base Snort Pada Serangan Data Flooding Pada Jaringan Jurusan TIK PNJ.**

Dengan Hak Bebas Royalti Noneksklusif ini Politeknik Negeri Jakarta berhak menyimpan, mengalih media/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di: Bogor Pada tanggal: 30 Juni 2021

Yang Menyatakan

(Dita Nurhayati)

- 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 menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



## Rancang Bangun IDS dan IPS Menggunakan Base Snort Pada Serangan *Data Flooding* Pada Jaringan Jurusan TIK PNJ.

### ABSTRAK

Saat sebuah perangkat komputer terhubung oleh suatu jaringan, perangkat komputer tersebut memiliki potensi dan rentan untuk diretas atau disusupi. Dengan demikian, dibutuhkan sistem keamanan yang dapat mendeteksi, menganalisis, dan mengambil tindakan pada lalu lintas jaringan yang tidak diinginkan. Maka dari itu dibuatlah sistem keamanan jaringan *Intrusion Detection System (IDS)* yang mendeteksi serangan atau paket tidak diinginkan, *Basic Analysis and Security engineering (BASE)* sebagai sistem monitoring GUI, serta *IPTables* sebagai *Intrusion Prevention System (IPS)* yang mengatur tindakan pada paket-paket mencurigakan. Sistem diuji menggunakan serangan *TCP flooding* menggunakan *SlowLoris* dan *UDP flooding* menggunakan *HPING3*, pengujian menunjukkan serangan *TCP flooding* sebanyak 500 paket membutuhkan waktu 10,77 s dengan rata-rata *response time* 21,54 ms, dan serangan 1000 paket membutuhkan waktu 23,06 s dengan rata-rata 23,06 ms. Sedangkan pada serangan *UDP flooding* sebanyak 500 paket membutuhkan waktu 248,54 s dengan rata-rata 5,9 ms, dan serangan 1000 paket membutuhkan waktu 499,98 s dengan rata-rata 6,3 ms. Serangan 500 dan 1000 paket ini tidak mempengaruhi *load time website* namun mempengaruhi performa server diantaranya CPU dan Memori. Setelah melakukan pengujian dapat disimpulkan bahwa *IPTables* efektif dalam melakukan blocking jaringan penyerang.

**Kata Kunci:** *Basic Analysis Security Engineering (BASE), Data Flooding, Denial of Service (DoS), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Snort.*

#### 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 menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



## DAFTAR ISI

HALAMAN PERNYATAAN ORISINALITAS .....	ii
HALAMAN PENGESAHAN.....	iii
KATA PENGANTAR.....	iv
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS.....	v
ABSTRAK .....	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	x
DAFTAR TABEL .....	xii
BAB I.....	1
PENDAHULUAN .....	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah .....	2
1.3 Batasan Masalah .....	3
1.4 Tujuan dan Manfaat.....	3
1.4.1 Tujuan.....	3
1.4.2 Manfaat.....	4
1.5 Metode Pelaksanaan .....	4
BAB II.....	6
TINJAUAN PUSTAKA.....	6
2.1 Penelitian Sejenis .....	6
2.2 Keamanan Jaringan.....	9
2.3 Data Flooding .....	10
2.4 <i>Intrusion Detection System (IDS)</i> .....	11
2.5 <i>Intrusion Prevention System (IPS)</i> .....	12
2.6 Ubuntu .....	13
2.7 VirtualBox .....	13
2.8 Snort.....	14
2.9 BASE .....	15
2.10 Nmap .....	16
2.11 <i>IP Table</i> .....	16
2.12 <i>Barnyard2</i> .....	16
2.13 <i>Denial of Service</i> .....	17

### 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 menggunakan 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 kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

2.14	SlowLoris .....	17
2.15	HPing.....	18
2.16	Apache2.....	18
2.17	PHP.....	19
2.18	Wordpress.....	19
2.19	Cisco Packet Tracer .....	20
2.20	SSH dan PuTTY.....	20
BAB III.....		21
PERENCANAAN DAN REALISASI.....		21
3.1	Perancangan Sistem.....	21
3.1.1	Deskripsi Sistem .....	21
3.1.2	Alur Pengerjaan .....	21
3.1.3	Desain Topologi Jaringan.....	22
3.1.4	Spesifikasi Perangkat.....	23
3.1.5	Skenario Pengujian .....	24
3.1.6	Diagram Blok .....	25
3.2	Realisasi Sistem .....	26
3.2.1	Pemindaian Server Jurusan TIK.....	26
3.2.2	Pembangunan Server <i>Dummy</i> Jurusan TIK .....	29
3.2.3	Pembangunan Website <i>Dummy</i> .....	31
3.2.4	Implementasi <i>Intrusion Detection System (IDS)</i> .....	36
3.2.5	Implementasi <i>Intrusion Prevention System (IPS)</i> .....	40
BAB IV.....		43
HASIL DAN PEMBAHASAN .....		43
4.1	Pengujian .....	43
4.2	Deskripsi Pengujian .....	43
4.3	Prosedur Pengujian .....	43
4.3.1	Pengujian <i>Intrusion Detection System (IDS)</i> Snort Base Pada Server JTIK PNJ.....	43
4.3.2	Pengujian <i>Intrusion Prevention System (IPS)</i> IPTables Pada Server JTIK PNJ.....	44
4.4	Data Hasil Pengujian .....	44
4.4.1	Pengujian <i>Intrusion Detection System (IDS)</i> Snort Base Pada Server JTIK PNJ.....	44



**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 menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

4.4.2	Pengujian <i>Intrusion Prevention System (IPS)</i> IPTables Pada Server JTIK PNJ.....	49
4.5	Analisis Data dan Evaluasi.....	50
4.5.1	Analisis Data Hasil Pengujian <i>Intrusion Detection System (IDS)</i> .....	51
4.5.2	Analisis Data Hasil Pengujian <i>Intrusion Detection System (IPS)</i> .....	63
BAB V	.....	65
PENUTUP	.....	65
5.1	Kesimpulan.....	65
5.2	Saran .....	65
DAFTAR PUSTAKA	.....	xiii
LAMPIRAN	.....	xvi
DAFTAR RIWAYAT HIDUP	.....	xvi





## DAFTAR GAMBAR

Gambar 1. 1 Metode PPDIIOO.....	4
Gambar 2. 1 Logo Ubuntu.....	13
Gambar 2. 2 Logo Virtual Box.....	13
Gambar 2. 3 Logo Snort.....	15
Gambar 2. 4 Logo NMap.....	16
Gambar 2. 5 Denial Of Service.....	17
Gambar 2. 6 Logo Apache.....	18
Gambar 2. 7 Logo PHP.....	19
Gambar 2. 8 Logo WordPress.....	19
Gambar 2. 9 Logo Putty.....	20
Gambar 3. 1 Alur Pengerjaan.....	21
Gambar 3. 2 Desain Topologi Jaringan.....	22
Gambar 3. 3 Skenario Pengujian.....	24
Gambar 3. 4 Diagram Blok.....	25
Gambar 3. 5 Proses Scanning Menggunakan Nmap.....	27
Gambar 3. 6 Hasil Scanning pada Nmap.....	27
Gambar 3. 7 Hasil Scanning Menggunakan Builtwith.....	28
Gambar 3. 8 Hasil Scanning Menggunakan Builtwith.....	29
Gambar 3. 9 Tampilan Spesifikas Server Dummy.....	30
Gambar 3. 10 Tampilan Akses PuTTY.....	30
Gambar 3. 11 Status OpenSSH Pada Server.....	31
Gambar 3. 12 Status Apache2.....	32
Gambar 3. 13 Tampilan Apache Pada Browser.....	32
Gambar 3. 14 Status menunjukkan versi PHP yang berjalan.....	33
Gambar 3. 15 Konfigurasi PHP Berhasil.....	33
Gambar 3. 16 Akun Wordpress yang Disimpan Pada MySQL.....	34
Gambar 3. 17 Tampilan Default Pada Wordpress.....	34
Gambar 3. 18 Tampilan Website Dummy.....	35
Gambar 3. 19 Tampilan Website Dummy.....	35
Gambar 3. 20 Pengaturan pada Snort.conf.....	36
Gambar 3. 21 Pengaturan Pada File local.rules.....	37
Gambar 3. 22 Konfigurasi Berhasil.....	38
Gambar 3. 23 Barnyard yang Telah Terinstalasi.....	38
Gambar 3. 24 Basis Data Snort.....	39
Gambar 3. 25 Basic Analysis and Security Engine.....	40
Gambar 3. 26 Default Policy yang Digunakan\.....	41
Gambar 4. 1 SlowLoris Mulai Menyerang dengan TCP Flooding.....	45
Gambar 4. 2 BASE Mendeteksi dan Memberikann Alert.....	46
Gambar 4. 3 HPING3 Mulai Menyerang Dengan UDP Flooding.....	47
Gambar 4. 4 BASE Mendeteksi serangan.....	48
Gambar 4. 5 command TCP DROP Pada IPTables.....	49
Gambar 4. 6 command UDP DROP Pada IPTables.....	49
Gambar 4. 7 IPTables Chain.....	49
Gambar 4. 8 SlowLoris Mengirim Request.....	52
Gambar 4. 9 HPING3 Mengirim Request.....	52
Gambar 4. 10 Grafik Average Time/Packet (ms).....	54
Gambar 4. 11 Keadaan Server Sebelum Diserang.....	56

### 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 menggunakan 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

Gambar 4. 12 Keadaan Server Saat Dilakukan Serangan TCP Flooding 500 Paket.....	57
Gambar 4. 13 Keadaan Server Saat Dilakukan Serangan TCP Flooding 1000 Paket.....	57
Gambar 4. 14 Keadaan Server Saat Dilakukan Serangan UDP Flooding 500 Paket .....	58
Gambar 4. 15 Keadaan Server Saat Dilakukan Serangan UDP Flooding 1000 Paket ....	58
Gambar 4. 16 Diagram Kinerja CPU (Angka Tertinggi) .....	59
Gambar 4. 17 Diagram Kinerja Memori (Angka Tertinggi) .....	59



## DAFTAR TABEL

Tabel 2. 1 Penelitian Sejenis .....	6
Tabel 3. 1 Alamat IP .....	23
Tabel 3. 2 Perangkat Keras .....	23
Tabel 3. 3 Perangkat Lunak.....	23
Tabel 3. 4 Ketentuan IPTables .....	41
Tabel 4. 1 Data Hasil Pengujian pada TCP Flood.....	46
Tabel 4. 2 Data Hasil Pengujian pada UDP Flood .....	48
Tabel 4. 3 Data Hasil Pengujian pada IPTables .....	50
Tabel 4. 4 Tabel Analisis Data .....	51
Tabel 4. 5 Respon Time .....	53
Tabel 4. 6 Average Time/Packet .....	53
Tabel 4. 7 Pengaruh Serangan.....	55
Tabel 4. 8 Pengaruh Serangan Pada Server.....	56
Tabel 4. 9 Data Hasil Pengujian IPTable .....	63

© 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 menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta





## BAB I

### PENDAHULUAN

#### 1.1 Latar Belakang

Internet merupakan media yang sangat pesat perkembangannya seiring berjalannya waktu. Semakin pesatnya perkembangan internet, semakin mudah untuk dijangkau oleh masyarakat umum. Segala kalangan mampu menjangkau kehebatan dunia internet, dimana semakin terbukanya dunia internet juga membuat informasi sulit untuk disaring, terlebih lagi banyak informasi krusial yang mudah untuk disalahgunakan seperti halnya informasi mengenai *hacking* dan *cracking* yang didukung oleh *tools* yang sangat mudah didapatkan.

Saat sebuah perangkat komputer terhubung oleh suatu jaringan, otomatis perangkat komputer tersebut memiliki potensi untuk diretas atau disusupi. Berbagai cara untuk meretas sudah semakin banyak, mulai dari jaringan yang tidak memiliki sistem keamanan hingga jaringan yang memiliki sistem keamanan yang tinggi sekalipun masih rentan terhadap ancaman ini. Peretasan merupakan suatu usaha penyusupan sebuah jaringan tanpa izin dengan maksud memantau dan mengambil dan atau tidak mengambil sebuah data.

Hingga saat ini, ancaman keamanan suatu jaringan komputer memiliki beragam macam, seperti *data flooding*, *port scanning*, DoS dan lain-lain. Hal inilah yang nantinya akan menjadi ancaman terbesar sebuah sistem jaringan komputer, dimana data akan mudah didapat dan atau dirusak oleh seorang *hacker*. Oleh karena itu, dibutuhkan *Intrusion Detection Systems (IDS)* yang merupakan sebuah sistem yang berfungsi untuk memonitor lalu lintas jaringan dan dapat mendeteksi ancaman serta serangan yang terjadi pada sebuah jaringan komputer. IDS akan memberikan sebuah peringatan atau tanda jika terdapat suatu ancaman yang ada pada jaringan komputer yang sedang diamati.

Server yang merupakan pusat data disimpan dan diolah dalam satu jaringan, permintaan yang dikirim oleh klien akan diolah oleh server. Kinerja server bergantung terhadap pertukaran data yang dikirim oleh klien pada jaringan. Pada suatu jaringan, administrator merupakan orang yang bertugas untuk memonitoring

#### 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 menggunakan 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 kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

server. Dari monitoring server itulah administrator dapat memantau keamanan jaringan dari server tersebut, dimana serangan/ancaman dapat dideteksi dan melakukan tindakan apabila masuk pada sebuah jaringan. Keamanan merupakan hal yang sangat penting dan dibutuhkan agar suatu jaringan dengan mudah dan aman dalam mengolah data.

Snort sebagai perangkat lunak pendeteksi intrusi berperan penting dalam memonitor lalu lintas jaringan komputer, sebab Snort merupakan sebuah aplikasi atau *tool* sekuriti yang berfungsi untuk mendeteksi intrusi-intrusi jaringan (penyusupan, penyerangan, pemindaian, dan beragam bentuk ancaman lainnya), sekaligus juga melakukan pencegahan. Dalam praktiknya, snort sangat andal untuk membentuk logging paket-paket dan analisis *traffic* secara real-time dalam jaringan berbasis TCP/IP (Ma'sum, dkk., 2017).

Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta (TIK PNJ) memiliki sebuah server sebagai tempat menyimpan data-data seperti repositori jurusan dan lainnya, server ini tersambung dengan jaringan Politeknik Negeri Jakarta, dimana jaringan PNJ merupakan jaringan yang sangat luas dan diakses secara bebas oleh civitas akademika PNJ. Dengan demikian, lalu lintas jaringan PNJ sangat rentan terhadap ancaman keamanan jaringan yaitu salah satunya adalah *data flooding* yang merupakan bagian dari jenis serangan *Denial of Service* (DoS), dimana DoS masih masuk kedalam 10 kategori ancaman keamanan *cyber* teratas.

Penelitian ini dibuat untuk membuat rancang bangun sistem keamanan jaringan server menggunakan Base Snort pada server *dummy* Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta dimana serangan *Data Flooding* dapat dideteksi oleh IDS Snort dimana mode yang digunakan adalah mode *intrusion detection*, serta mampu melakukan block secara otomatis menggunakan IPTables pada penyerang sehingga penyerang tidak bisa mengakses server.

### 1.2 Perumusan Masalah

Perumusan masalah yang terdapat pada penelitian Rancang Bangun IDS dan IPS Menggunakan Base Snort Pada Serangan *Data Flooding* Pada Jaringan Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta adalah:



## © 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

1. Bagaimana membangun sebuah sistem server yang dapat mendeteksi serta mencegah terjadinya *data flooding* dengan cara pemblokiran IP dan Port oleh IPTable?
2. Bagaimana IDS dan IPS bisa diimplementasikan dengan menggunakan Base Snort?
3. Apakah Snort Base mampu mendeteksi serangan *TCP flood* dan *UDP flood*?
4. Apakah serangan *TCP flood* dan *UDP flood* mempengaruhi performa server Jurusan TIK PNJ?
5. Bagaimana IPTables dapat efektif mencegah serangan *TCP flood* dan *UDP flood* agar tidak dapat masuk pada jaringan server JTIK?

### 1.3 Batasan Masalah

Batasan masalah yang ditentukan dalam penelitian Rancang Bangun IDS dan IPS Menggunakan Base Snort Pada Serangan Data Flooding Pada Jaringan Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta adalah sebagai berikut :

1. Sistem keamanan diimplementasikan pada server *dummy* jurusan TIK PNJ menggunakan sistem operasi Ubuntu yang dijalankan dengan VirtualBox.
2. TCP dan *UDP flooding* dideteksi oleh Snort Base sebagai IDS serta dilakukan pencegahan menggunakan IPTables sebagai IPS.
3. Serangan disimulasikan secara *internal network*, dimana penyerang berada dalam satu jaringan internet dengan server.
4. Jenis serangan yang diluncurkan adalah TCP dan *UDP flooding* dimana serangan tersebut termasuk ke dalam *Denial of Service (DoS)*, serangan hanya dijalankan dengan perangkat lunak SlowLoris dan HPing3.
5. Pengujian TCP dan *UDP flooding* berupa serangan pengiriman 500 paket dan 1000 paket pada server.

### 1.4 Tujuan dan Manfaat

#### 1.4.1 Tujuan

Tujuan dari rancang bangun ini adalah mengimplementasikan sistem keamanan server menggunakan Snort Base sebagai IDS dan IPTables sebagai





**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 menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

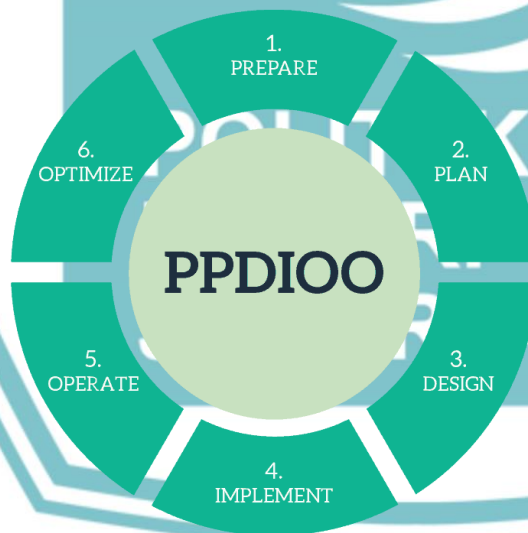
IPS yang akan diuji menggunakan serangan TCP *flooding* dan UDP *flooding* dengan *tools* SlowLoris untuk TCP *flooding* serta HPING3 untuk UDP *flooding* sehingga sistem keamanan server mampu serta efektif dalam mendeteksi dan mencegah serangan *data flooding* pada server JTIK PNJ.

#### 1.4.2 Manfaat

Manfaat dari Rancang Bangun IDS dan IPS Menggunakan Base Snort Pada Serangan *Data Flooding* Pada Jaringan Jurusan TIK PNJ adalah terbentuknya sistem server yang aman dari serangan *data flooding* karena telah diterapkannya snort base dan IPTable untuk mendeteksi serta menanggulangi serangan tersebut.

#### 1.5 Metode Pelaksanaan

Penelitian ini dilakukan dengan pendekatan metode PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize), dimana metode PPDIOO didijelaskan sebagai berikut:



Gambar 1. 1 Metode PPDIOO.

#### 1) Prepare

Pada Langkah ini, penulis melakukan persiapan seperti membaca jurnal dan referensi serta mempersiapkan perangkat lunak dan perangkat keras yang dibutuhkan untuk realisasi sistem yang dibuat.



## © 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 menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

### 2) Plan

Langkah ini dilakukan perencanaan berdasarkan tujuan dan kebutuhan. Peneliti akan mengimplementasikan IDS dan IPS untuk sistem keamanan server, dalam perencanaannya IDS yang digunakan adalah Snort Base serta Iptables sebagai IPS. Terdapat 2 jenis pengujian yaitu TCP *Flooding* dan UDP *Flooding*, dimana penyerangan TCP *Flooding* menggunakan Slowloris dan UDP *Flooding* menggunakan HPING3.

### 3) Design

Pada langkah ini peneliti menggunakan langkah *design* untuk merancang topologi jaringan, alur pengerjaan, alur pengujian, serta skenario pengujian.

### 4) Implementasi

Langkah implementasi digunakan oleh peneliti untuk mengimplementasikan sistem yang sudah direncanakan seperti implementasi IDS dan IPS pada server. Melakukan konfigurasi juga ada pada tahap ini.

### 5) Operate

Pada tahap *operate* pengujian sistem dilakukan, dimana pengujian seperti monitoring serangan, mendeteksi serangan pada Base Snort, pengujian sistem pencegah serangan pada ip tables, melakukan blok akses server terhadap attacker.

### 6) Optimize

Setelah dilakukan pengoperasian sistem, terdapat beberapa kekurangan sehingga dilakukan kembali optimisasi terhadap sistem yang telah dibuat seperti penambahan sumber daya pada server, dan lain-lain.



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 menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

## BAB V PENUTUP

### 5.1 Kesimpulan

Berdasarkan hasil dari penelitian yang berjudul “Implementasi IDS dan IPS Menggunakan Base Snort Pada Serangan Data Flooding Pada Jaringan Jurusan TIK PNJ”, maka dapat ditarik kesimpulan sebagai berikut:

- a. BASE SNORT mampu mendeteksi lalu lintas serangan yang masuk pada sebuah jaringan server
- b. IPTables efektif dalam mencegah intrusi yang masuk ke dalam jaringan server, dimana alamat penyerang tidak akan bisa masuk ke dalam jaringan saat dilakukan aksi *DROP*.
- c. Serangan *UDP flood* dan *TCP Flood* yang terjadi pada jaringan internal dapat mengganggu aktifitas server dan website, sehingga IDS dan IPS sangat dibutuhkan oleh sebuah server yang sedang berjalan.
- d. Serangan *UDP flood* dan *TCP Flood* mampu mempengaruhi performa CPU dan Memori pada server Jurusan TIK PNJ dimana saat terjadinya serangan terdapat perubahan kenaikan angka pada CPU dan Memori.

### 5.2 Saran

Berdasarkan pengimplementasian sistem IDS dan IPS serta beberapa pengujian yang dilakukan, terdapat beberapa saran yang dapat diusulkan pada penelitian ini, diantaranya:

- a. Memahami lebih dalam tentang *snort rules* sehingga *snort rules* bisa dimanfaatkan semaksimal mungkin.
- b. Dalam proses virtualisasi, server yang dibangun harus memiliki *resource* yang besar agar BASE dapat berjalan dengan lancar serta dalam melakukan serangan bisa lebih mendalam.
- c. Menggunakan sistem monitoring yang lebih baru.



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

## DAFTAR PUSTAKA

- Aminanto, A. & Sulisty, W., 2019. Simulasi Sistem Keamanan Jaringan Komputer Berbasis IPS Snort dan HoneyPot.. *AITI: Jurnal Teknologi Informasi*, pp. 135-150.
- Behal, S. & Kumar, K., 2017. Characterization and Comparison of DDoS. *International Journal of Network Security*, Volume 19, pp. 383-393.
- Birajdar, G., 2014. Implementation of Embedded Web Server Based on ARM11 and Linux using Raspberry PI. *International Journal of Recent Technology and Engineering (IJRTE)*, Volume 3, pp. 64-66.
- Cicimov, I., 2014. *Host-based IDS with Snort, Barnyard2 and Snorby in AWS*. [Online]  
Available at: <https://icicimov.github.io/blog/security/HIDS-with-Snort-Barnyard2-and-Snorby/>  
[Accessed 28 5 2021].
- Dar, M. H. & Harahap, S. Z., 2018. Implementasi Snort Intrusion Detection System (IDS) Pada Sistem Jaringan Komputer. *Informatika*, pp. 14-23.
- Fadhilillah1, A. S., DR. Nyoman Bogi A K, S. & Arif Indra Irawan, S., 2019. ANALISIS PERFORMANSI IDS MENGGUNAKAN METODE DETEKSI ANOMALYBASED TERHADAP SERANGAN DOS. *e-Proceeding of Engineering*, Volume 6, pp. 3398-3406.
- GUETARI, R., CHETOUANI, A., TABIA, H. & KHLIFA, N., 2020. Real time emotion recognition in video stream, using B-CNN and F-CNN. *2020 5th International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, Volume 5, pp. 1-6.
- Hassen, O. A. & Ibrahim, H. k., 2017. Preventive Approach against HULK Attacks in Network. *International Journal of Computing and Business Research (IJCBR)*, Volume 7.



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 menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

Ma'sum, M. S., Irwansyah, M. A. & Priyanto, H., 2017. Analisis Perbandingan Sistem Keamanan Jaringan Menggunakan Snort dan Netfilter. *Jurnal Sistem dan Teknologi Informasi*, Volume 5, pp. 56-60.

Ma'sum, M. S., Irwansyah, M. A. & Priyanto, H., 2017. Analisis Perbandingan Sistem Keamanan Jaringan Menggunakan Snort dan Netfilter. *Jurnal Sistem dan Teknologi Informasi (JUSTIN)*, Volume 5, pp. 56-60.

Patel, S. K. & Sonker, A., 2016. Rule-Based Network Intrusion Detection System for Port Scanning with Efficient Port Scan Detection Rules Using Snort. *International Journal of Future Generation Communication and Networking*, Volume 9, pp. 339-350.

Pradipta, Y. W. & Asmunin, 2017. Implementasi Intrusion Prevention System (IPS) Menggunakan Snort dan IP Tables Berbasis Linux. *Jurnal Manajemen Informatika*, Volume 7, pp. 21-28.

Sanfilippo, S., 2006. *HPing*. [Online] Available at: <http://www.hpings.org/> [Accessed 28 05 2021].

Santosa, B., Boedi, D. & Putra, Y. I., 2010. Remastering Distro Ubuntu Untuk Menunjang Pembelajaran Informatika. *Seminar Nasional Informatika 2010 (semnasIF 2010)*, pp. C-56-C-65.

Sutarti, Pancaro, A. P. & Saputra, F. I., 2018. Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal. *Jurnal PROSISKO*, Volume 5, pp. 1-8.

Suwanto, R., Ruslianto, I. & Diponegoro, M., 2019. Implementasi Intrusion Prevention System (IPS) Menggunakan SNORT dan IPTable Pada Monitoring Jaringan Lokal Berbasis Website. *Jurnal Komputer dan Aplikasi*, Volume 7, pp. 97-107.

Tambunan, G. & Mantra, I., 2020. Implementasi Keamanan IDS/IPS Dengan SNORT dan IPTables Pada Server. *SENAMIKA*, pp. 10-16.



## © 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 mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

Triandi, B., 2015. Sistem Keamanan Jaringan Dalam Mencegah Flooding Data Dengan Metode Bloking dan Port. *Seminar Nasional Teknologi Informasi dan Multimedia*, pp. 49-54.



## Lampiran 1 Daftar Riwayat Hidup

# LAMPIRAN DAFTAR RIWAYAT HIDUP

Dita Nurhayati

Lahir di Bogor pada tanggal 30 bulan Januari tahun 1999. Lulus dari SDN Semplak 2 Bogor pada tahun 2011, SMPN 2 Bogor pada tahun 2014, dan SMAN 2 Bogor pada tahun 2017 serta Diploma II program studi *Network Administrator Professional* di CCIT-FTUI pada tahun 2019. Saat ini sedang menempuh Pendidikan Diploma IV Program Studi Teknik Informatika Jurusan Teknik Informatika dan Komputer di Politeknik Negeri Jakarta.



POLITEKNIK  
NEGERI  
JAKARTA

© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

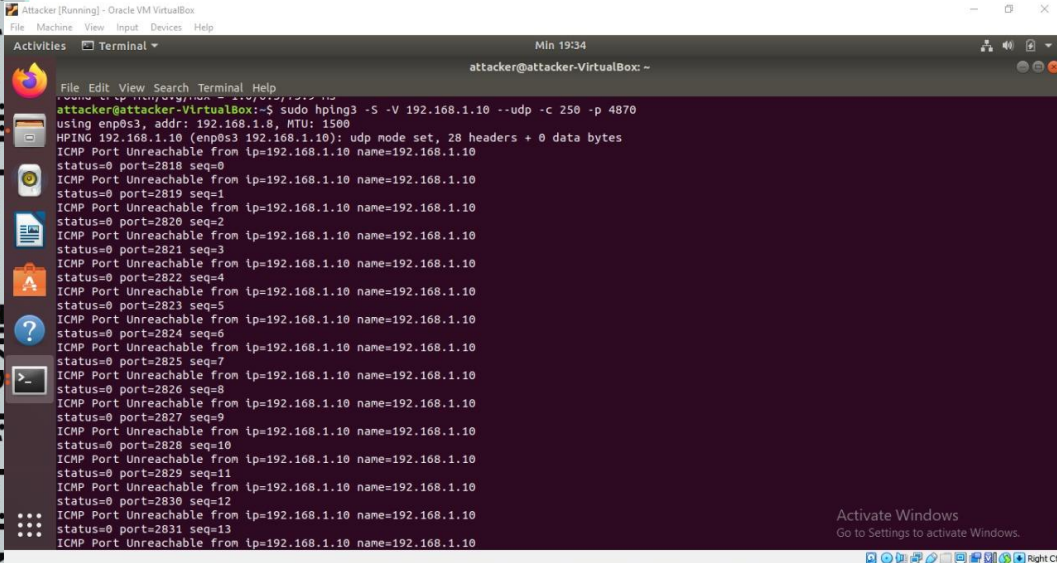
Hak Cipta :

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 kritik atau tinjauan suatu masalah.
  - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

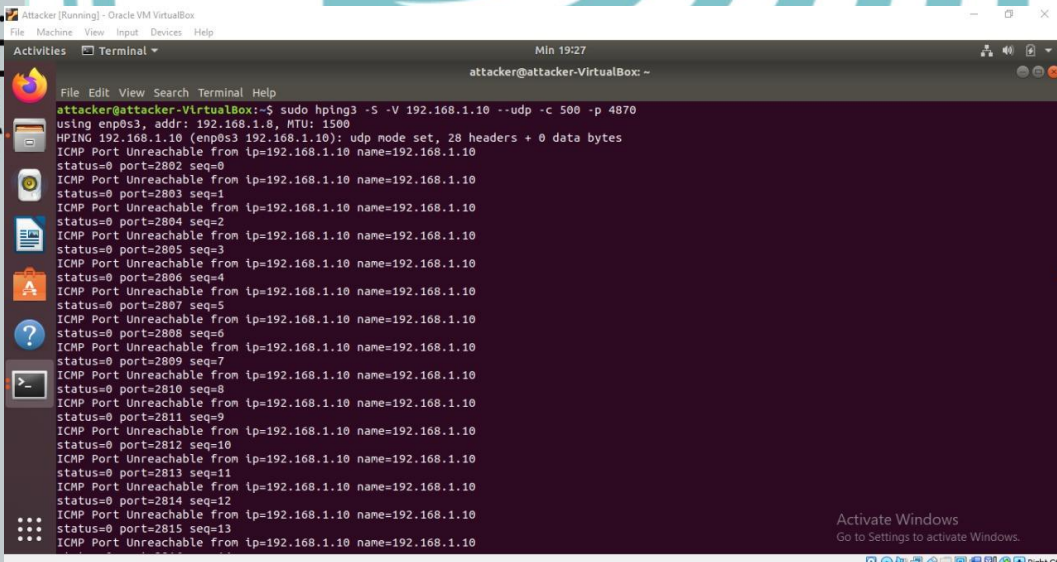


Hak Cipta :

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 menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



Gambar 6 Serangan UDP Flooding 500 Paket



Gambar 7 Serangan UDP Flooding 1000 Paket





## 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 menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

```
attacker@attacker-VirtualBox: ~/Desktop/Slowloris/slowloris
attacker@attacker-VirtualBox:~/Desktop/Slowloris/slowloris$ sudo python3 slowloris.py 192.168.1.10 -p 4870 -v -s 63
[20-06-2021 19:20:15] Attacking 192.168.1.10 with 63 sockets.
[20-06-2021 19:20:15] Creating sockets...
[20-06-2021 19:20:15] Creating socket nr 0
[20-06-2021 19:20:15] Creating socket nr 1
[20-06-2021 19:20:15] Creating socket nr 2
[20-06-2021 19:20:15] Creating socket nr 3
[20-06-2021 19:20:15] Creating socket nr 4
[20-06-2021 19:20:15] Creating socket nr 5
[20-06-2021 19:20:15] Creating socket nr 6
[20-06-2021 19:20:15] Creating socket nr 7
[20-06-2021 19:20:15] Creating socket nr 8
[20-06-2021 19:20:15] Creating socket nr 9
[20-06-2021 19:20:15] Creating socket nr 10
[20-06-2021 19:20:15] Creating socket nr 11
[20-06-2021 19:20:15] Creating socket nr 12
[20-06-2021 19:20:15] Creating socket nr 13
[20-06-2021 19:20:15] Creating socket nr 14
[20-06-2021 19:20:15] Creating socket nr 15
[20-06-2021 19:20:15] Creating socket nr 16
[20-06-2021 19:20:15] Creating socket nr 17
[20-06-2021 19:20:15] Creating socket nr 18
[20-06-2021 19:20:15] Creating socket nr 19
[20-06-2021 19:20:15] Creating socket nr 20
[20-06-2021 19:20:15] Creating socket nr 21
[20-06-2021 19:20:15] Creating socket nr 22
[20-06-2021 19:20:15] Creating socket nr 23
[20-06-2021 19:20:15] Creating socket nr 24
[20-06-2021 19:20:15] Creating socket nr 25
[20-06-2021 19:20:15] Creating socket nr 26
[20-06-2021 19:20:15] Creating socket nr 27
[20-06-2021 19:20:15] Creating socket nr 28
```

Gambar 8 Serangan TCP Flooding 500 Paket

```
attacker@attacker-VirtualBox: ~/Desktop/Slowloris/slowloris
attacker@attacker-VirtualBox:~/Desktop/Slowloris/slowloris$ sudo python3 slowloris.py 192.168.1.10 -p 4870 -v -s 125
[17-06-2021 20:00:05] Attacking 192.168.1.10 with 125 sockets.
[17-06-2021 20:00:05] Creating sockets...
[17-06-2021 20:00:05] Creating socket nr 0
[17-06-2021 20:00:05] Creating socket nr 1
[17-06-2021 20:00:05] Creating socket nr 2
[17-06-2021 20:00:05] Creating socket nr 3
[17-06-2021 20:00:05] Creating socket nr 4
[17-06-2021 20:00:05] Creating socket nr 5
[17-06-2021 20:00:05] Creating socket nr 6
[17-06-2021 20:00:05] Creating socket nr 7
[17-06-2021 20:00:05] Creating socket nr 8
[17-06-2021 20:00:05] Creating socket nr 9
[17-06-2021 20:00:05] Creating socket nr 10
[17-06-2021 20:00:05] Creating socket nr 11
[17-06-2021 20:00:05] Creating socket nr 12
[17-06-2021 20:00:05] Creating socket nr 13
[17-06-2021 20:00:05] Creating socket nr 14
[17-06-2021 20:00:05] Creating socket nr 15
[17-06-2021 20:00:05] Creating socket nr 16
[17-06-2021 20:00:05] Creating socket nr 17
[17-06-2021 20:00:05] Creating socket nr 18
[17-06-2021 20:00:05] Creating socket nr 19
[17-06-2021 20:00:05] Creating socket nr 20
[17-06-2021 20:00:05] Creating socket nr 21
[17-06-2021 20:00:05] Creating socket nr 22
[17-06-2021 20:00:05] Creating socket nr 23
[17-06-2021 20:00:05] Creating socket nr 24
[17-06-2021 20:00:05] Creating socket nr 25
[17-06-2021 20:00:05] Creating socket nr 26
[17-06-2021 20:00:05] Creating socket nr 27
[17-06-2021 20:00:05] Creating socket nr 28
```

Gambar 9 Serangan TCP Flooding 1000 Paket