

Analisis Keamanan Jaringan dari Serangan DoS pada Sistem Inventaris Sanggar Tari Natya Lakshita menggunakan IDS

Zahra Arwananing Tyas, Arizona Firdonsyah, Wulan Ramdhani

* Program Studi Teknologi Informasi, Universitas 'Aisyiyah Yogyakarta

** Program Studi Teknologi Informasi, Universitas 'Aisyiyah Yogyakarta

*** Program Studi Teknologi Informasi, Universitas 'Aisyiyah Yogyakarta

* zahraatyas@unisayogya.ac.id,**arizona@unisayogya.ac.id,*** wulanramdhani047@gmail.com

ABSTRACT

Information technology is advancing very quickly. Currently, there is highly qualified support for internet facilities. A quality internet service has both advantages and disadvantages for its users. An example of the negative impact of the development of internet technology is attacks from irresponsible parties or often called hackers. Sanggar Tari Natya Lakshita's Inventory System is a newly built system, so attack testing is needed because network security is important to maintain data integration in the network. The test is carried out using a DoS attack with the LOIC tool. IDS is the method used in research with the Snort tool that functions as an intruder detector. The study aims to determine the results and effects of attacks on the Inventory System and determine how the IDS framework works with the Snort tool in detecting attacks. carried using 1 computer and 1 laptop. The results of the attack on the inventory system showed that Snort succeeded in detecting an attack sent by LOIC by displaying the attacker's IP and IP target through port 80, then the recommendations were given related to the stages of handling network security based on CSIRT guidelines at Sanggar Tari Natya Lakshita that can be implemented.

Keyword: *IDS, Snort, Denial of Service, LOIC, Inventory System Network Security*

1. Pendahuluan

Perkembangan teknologi informasi sangat pesat. Dukungan fasilitas internet saat ini sangat mumpuni. Fasilitas internet yang mumpuni tentu memiliki dampak positif dan negatif bagi penggunanya. Contoh dampak negatif dari perkembangan teknologi internet adalah serangan dari pihak yang tidak bertanggung jawab atau sering disebut *hacker*, oleh karena itu seorang administrator jaringan harus memastikan bahwa jaringan komputer perusahaan terlindungi dari serangan. Jenis serangan yang dapat dilakukan oleh hacker salah satunya adalah DoS. DoS (*Denial of Service*) merupakan serangan terhadap jaringan komputer yg beroperasi dengan mengirimkan *request* secara terus menerus agar server tetap sibuk dan tidak mampu mengatasi *request* yang diterima sehingga server menjadi rusak [1].

Efek dari serangan DoS menyebabkan jaringan komputer menjadi kurang optimal kinerjanya. Akibat terburuk dari serangan ini adalah penyusup mampu membuat program untuk dirinya sendiri yang bersifat merusak untuk mendapatkan suatu keuntungan [2]. Kerusakan pada jaringan mengakibatkan sehingga menyebabkan jaringan menjadi lambat bahkan merusak sistem jaringan [3].

Sanggar Tari Natya Lakshita merupakan lembaga yang bergerak dibidang pendidikan dan pelatihan, sebelumnya lembaga tari ini berbentuk sanggar sesuai perkembangan pendidikan non formal yang disusun oleh negara kemudian menjadi LPK Tari Natya Lakshita yang dipimpin oleh Didik Hadiprayitno, S.ST (Didik Nini Thowok), yang didirikan pada 2 Februari 1980, pada tahun 1994 Sanggar Tari Natya Lakshita terdaftar sebagai anggota HIPKI (Himpunan Penyelenggaraan Khusus Indonesia) sehingga sekarang dapat disebut sebagai LPK Tari Natya Lakshita [4].

Data yang dicatat pada Sanggar Tari Natya Lakshita masih dilakukan secara manual sehingga dibutuhkan sistem yang mencatat data-data inventaris dari Sanggar Tari Natya Lakshita. Sistem Inventaris yang telah dibuat berisi data-data penting sehingga membutuhkan sistem yang aman. Sistem yang aman diperlukan pengujian serangan guna mengetahui keamanan dari sistem inventaris tersebut.

Penelitian ini berfokus pada pengujian keamanan jaringan pada sistem inventaris yang ada di Sanggar Tari Natya Lakshita yang sistemnya baru dibangun sehingga perlu adanya pengujian keamanan jaringan pada sistem inventaris tersebut. Percobaan penyerangan dilakukan menggunakan jenis serangan DoS (*Denial Of Service*) dengan alat bantu LOIC (*Low Orbit Ion Cannon*). LOIC dapat melumpuhkan *website* dengan cara mengirimkan *packet* sebanyak mungkin melalui *domain* atau ip server komputer target[5].

Framework atau metode yang digunakan pada penelitian ini adalah IDS (*Intrusion Detection System*). IDS merupakan metode yang secara otomatis memantau lalu lintas jaringan yang mencurigakan, selain itu IDS dapat mencegah resiko keamanan sistem jaringan yang meningkat, mendeteksi serangan dan pelanggaran

keamanan sistem jaringan. Alat bantu yang digunakan untuk mendeteksi serangan adalah Snort. Snort adalah perangkat lunak untuk mendeteksi penyusup dan mampu menganalisis lalu lintas secara *real-time*. Snort juga memiliki hubungan dengan IDS dalam menanggapi insiden serangan terhadap host jaringan.

Tujuan dari penelitian ini yaitu mengetahui bagaimana hasil dari serangan DOS (Denial of Service) dengan alat bantu LOIC pada Sistem Inventaris Sanggar Tari Natya Lakshita dan mengetahui cara kerja *framework* IDS dengan tools Snort, jika terjadi serangan pada keamanan jaringan Sistem Inventaris Sanggar Tari Natya Lakshita sehingga dapat dilakukan pendeteksian. Manfaat penelitian untuk mahasiswa mendapatkan pemahaman lebih mendalam mengenai sistem keamanan jaringan yang bisa dikembangkan dalam dunia teknologi, selain itu mahasiswa juga mendapatkan pemahaman mengenai jenis serangan dan jenis pendeteksian serangan yang digunakan pada penelitian, sedangkan manfaat untuk Sanggar Tari Natya Lakshita dapat mengetahui seberapa aman keamanan jaringan pada sistem inventaris jika dilakukan penyerangan dan mendapatkan rekomendasi penanggulangan serangan untuk digunakan memperkuat keamanan jaringan pada sistem inventaris.

2. Metode Penelitian

Metode penelitian yang digunakan adalah studi pustaka dan studi lapangan:

a. Studi Pustaka

Metode ini merupakan metode pengumpulan data melalui buku, jurnal, maupun artikel yang dijadikan acuan analisis penelitian yang akan dilakukan [2].

b. Studi Lapangan

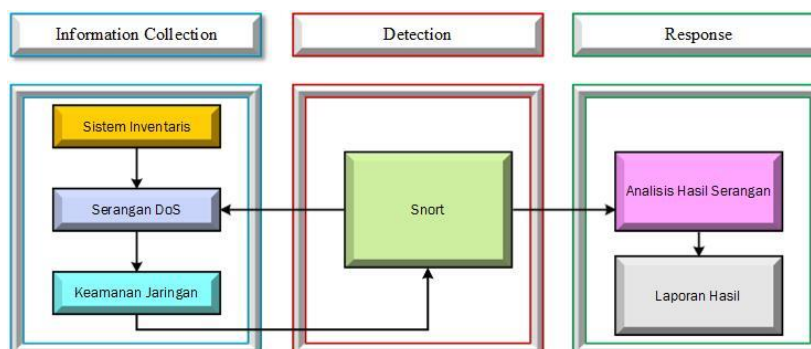
Metode ini merupakan metode pengumpulan data dengan melakukan pengamatan secara langsung pada lokasi penelitian yang bertujuan untuk pengambilan data dan memperoleh informasi [6]. Diagram alir metode penelitian ditunjukkan pada Gambar 1.



Gambar 1 Diagram Alir Metode Penelitian

2.1. Tahapan Kerja IDS

IDS memiliki 3 tahapan kerja yaitu information collection, detection, dan response, dari 3 tahapan tersebut mencakup rencana penelitian yang akan dilakukan [7], skema bagan alir dalam tahapan kerja IDS dapat dilihat pada Gambar 3.



Gambar 3 Tahapan Kerja IDS

Bagan alir dari tahapan kerja IDS pada gambar 1 dijelaskan sebagai berikut.

a. Information collection (Koleksi Informasi)

Information collection, pada tahapan ini terdapat 3 komponen yaitu sistem inventaris, serangan DoS, keamanan jaringan. Proses tahapannya yaitu sistem inventaris diserang menggunakan jenis serangan DoS, dan yang akan diserang adalah keamanan jaringan dari sistem inventaris dengan alat bantu penyerangan LOIC.

b. Detection (Deteksi)

Detection, pada tahapan ini dilakukan pendeteksian serangan menggunakan Snort, lalu dilakukan pengulangan serangan kemudian di deteksi, dari hasil deteksi akan di analisis pada tahap respon.

c. Response (Tanggapan)

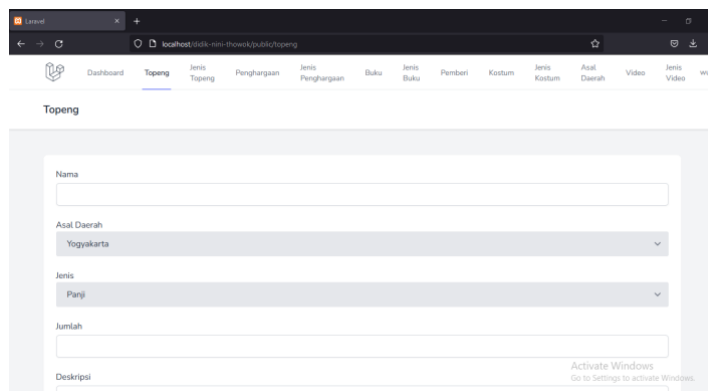
Response, setelah dilakukan serangan dan mendapatkan hasil pendeteksian maka dilakukan analisis hasil serangan, jika serangan DoS berhasil melakukan penyerangan pada sistem inventaris maka akan diberikan rekomendasi penanganan insiden keamanan pada Sanggar Tari Natya Lakshita untuk diimplementasikan, kemudian dari hasil analisis tersebut maka akan dibuat laporan hasil

3. Hasil dan Pembahasan

Hasil dan pembahasan merupakan tahap pemaparan hasil dari serangan pada Sistem Inventaris Sanggar Tari Natya Lakshita. IDS memiliki 3 tahapan kerja yaitu *information collection*, *detection* dan *response* yang dapat dijelaskan sebagai berikut.

3.1. Information Colection

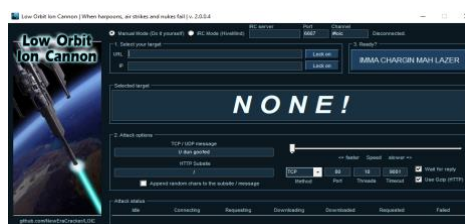
Information collection merupakan tahap awal untuk mengetahui informasi pada Sistem Inventaris Sanggar Tari Natya Lakshita yang menjadi target serangan, sebelumnya dilakukan persiapan Sistem Inventaris Sanggar Tari Natya Lakshita sehingga bisa diakses kemudian dilakukan proses instalasi dan konfigurasi Snort dan LOIC yang digunakan untuk pendeteksian dan penyerangan. Tampilan Sistem Inventaris seperti pada Gambar 3.



Gambar 3 Tampilan Sistem Inventaris

3.1.1. Instalasi dan Konfigurasi LOIC

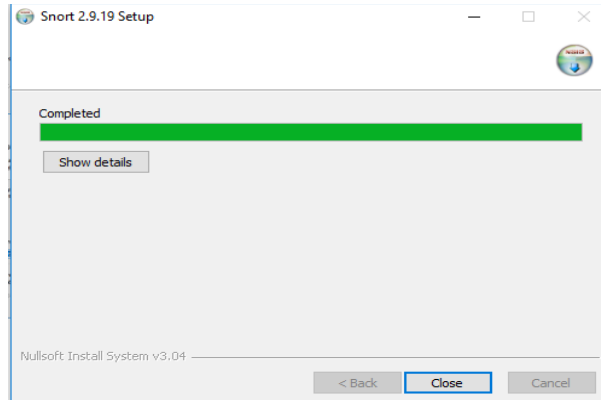
LOIC pada penelitian ini digunakan sebagai alat untuk melakukan serangan pada keamanan jaringan Sistem Inventaris Sanggar Tari Natya Lakshita dengan jenis serangan DoS, LOIC di pasang pada komputer 1 yang berperan sebagai penyerang dengan IP 10.0.221.247. Tampilan LOIC setelah berhasil terpasang ditampilkan pada Gambar 4.



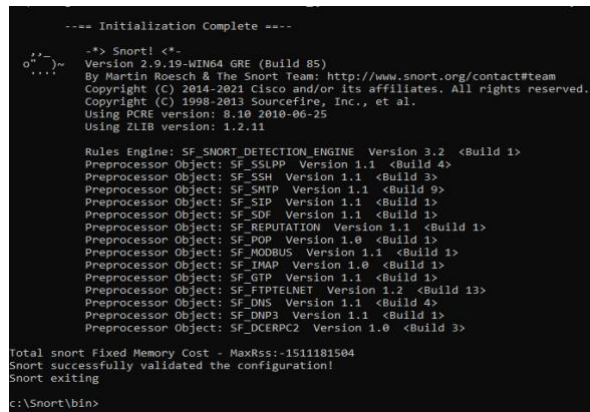
Gambar 4 Tampilan LOIC

3.1.2. Instalasi dan Konfigurasi Snort

Snort merupakan perangkat lunak IDS yang berbasis opensource dan digunakan untuk mengamankan jaringan dari aktifitas yang berbahaya [8]. Penelitian ini menggunakan Snort sebagai alat pendeteksi serangan. Snort di-instal pada laptop 1 yang berperan sebagai pendeteksi dengan IP 10.0.221.1. tampilan Snort setelah berhasil terinstal dan berhasil dikonfigurasi seperti pada Gambar 5 dan Gambar 6.

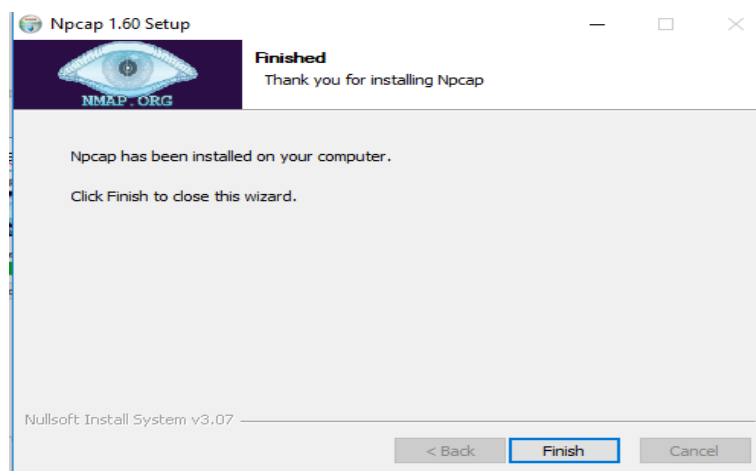


Gambar 5 Snort berhasil di instal



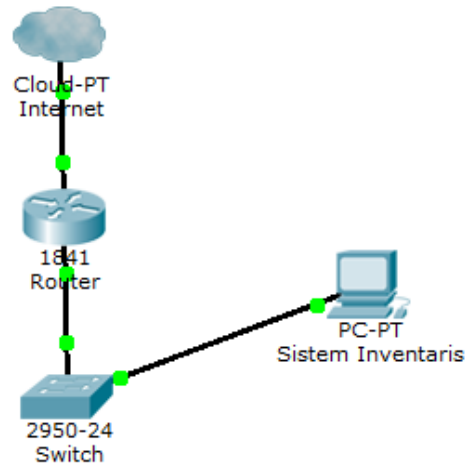
Gambar 6 Snort berhasil di konfigurasi

Gambar 5 dan Gambar 6 diatas merupakan tampilan Snort berhasil terinstal dan terkonfigurasi, setelah Snort berhasil terinstal Snort membutuhkan software pendukung agar Snort bisa digunakan yaitu Npcap. Npcap berfungsi untuk menangkap lalu lintas jaringan dan menganalisis atau membaca tangkapan yang disimpan kemudian menganalisis hasil tangkapan tersebut, tampilan Npcap setelah terinstal seperti pada Gambar 4.7.



Gambar 7 Tampilan Npcap setelah terinstal

Gambar 7 merupakan topologi jaringan komputer pada Sanggar Tari Natya Lakshita, dimana Sistem Inventaris yang menjadi target penyerangan belum terdapat Snort.



Gambar 7 Topologi Jaringan komputer pada Sanggar Tari Natya Lakshita

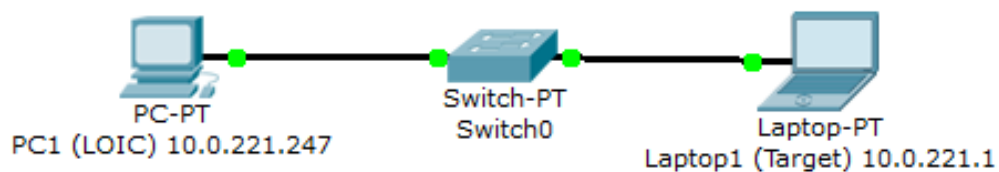
3.1.3. Penyerangan menggunakan 1 Komputer dan 1 Laptop

Proses penyerangan dengan menggunakan 1 komputer dan 1 laptop, dimana komputer 1 berfungsi sebagai penyerang dan laptop 1 berfungsi sebagai target yang terdapat Sistem inventaris dan sudah terpasang Snort. Tabel IP komputer dan laptop yang digunakan ditunjukkan pada Tabel 1.

Tabel 1 IP komputer dan Laptop

Nama komputer/laptop	IP Address komputer/laptop	Subnet mask	Keterangan
UNISA-B-11 (Komputer 1)	10.0.221.247	255.255.255.0	Penyerang
ACER (Laptop 1)	10.0.221.1	255.255.255.0	

Tabel 1 merupakan tabel yang berisi nama komputer, laptop, alamat IP dan subnet mask yang terdapat pada komputer maupun laptop yang digunakan, komputer 1 merupakan penyerang dimana pada komputer 1 terdapat LOIC, sedangkan Laptop 1 merupakan target sekaligus pendeteksi karena pada laptop 1 terdapat Sistem Inventaris yang dijadikan target dalam penyerangan dan pada laptop 1 sudah terpasang Snort yang berperan sebagai pendeteksi serangan, seperti topologi penyerangan pada Gambar 8.



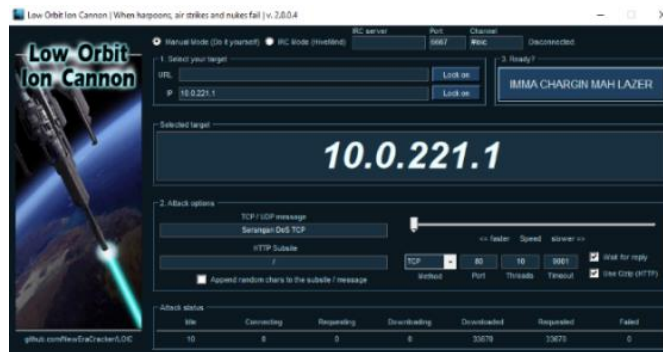
Gambar 8 Topologi Penyerangan 2 Perangkat

Skenario penyerangan menggunakan 2 perangkat dilakukan menggunakan 3 metode serangan yang terdapat pada LOIC yaitu TCP,UDP dan HTTP ditunjukkan pada Tabel 2.

Tabel 2 Skenario Penyerangan 2 Perangkat

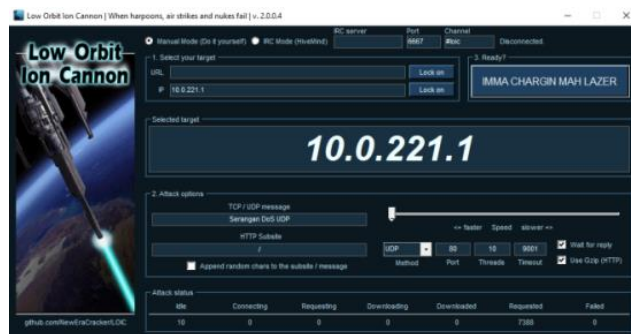
IP penyerang	IP target	Metode	Port	Threads	Timeout
10.0.221.247	10.0.221.1	TCP	80	10	90001
10.0.221.247	10.0.221.1	UDP	80	10	90001
10.0.221.247	10.0.221.1	HTTP	80	10	90001

- a. Penyerangan yang pertama menggunakan metode serangan TCP (*Transmission Control Protocol*) yang terdapat pada LOIC dengan memasukkan IP komputer target, seperti pada Gambar 9.



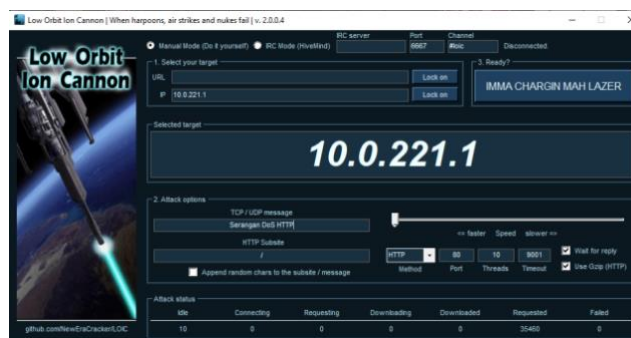
Gambar 9 Metode Serangan TCP

- b. Proses penyerangan selanjutnya menggunakan metode serangan UDP (*User Datagram Protocol*) dengan memasukkan IP target pada kolom IP yang terdapat pada LOIC, seperti pada Gambar 10.



Gambar 10 Metode Serangan UDP

- c. Metode serangan yang ketiga menggunakan metode HTTP dengan memasukkan alamat IP target pada kolom IP yang terdapat pada LOIC, seperti pada Gambar 11.



Gambar 11 Metode Serangan HTTP

3.2. Detection

Detection merupakan tahap kedua pada metode IDS, tahap ini adalah tahap deteksi hasil serangan LOIC pada keamanan jaringan Sistem Inventaris menggunakan tool Snort

- a. Hasil monitoring Snort pada serangan metode TCP (*Transmission Control Protocol*), Snort berhasil mendeteksi adanya serangan yang dikirim oleh LOIC dengan menampilkan hasil IP penyerang menuju IP target melalui port 80, seperti pada Gambar 12 (gambar yang diberi kotak merah).

```
Administrator: Command Prompt - snort -i 5 -c c:\Snort\etc\snort.conf -A console
99/01-14:24:30.705899  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61194 -> 10.0.221.1:80
99/01-14:24:30.720895  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61190 -> 10.0.221.1:80
99/01-14:24:30.720895  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61194 -> 10.0.221.1:80
99/01-14:24:30.720895  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61193 -> 10.0.221.1:80
99/01-14:24:30.720921  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61191 -> 10.0.221.1:80
99/01-14:24:30.720921  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61196 -> 10.0.221.1:80
99/01-14:24:30.720921  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61187 -> 10.0.221.1:80
99/01-14:24:30.720921  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61195 -> 10.0.221.1:80
99/01-14:24:30.721297  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61189 -> 10.0.221.1:80
99/01-14:24:30.721322  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61188 -> 10.0.221.1:80
99/01-14:24:30.721322  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61192 -> 10.0.221.1:80
99/01-14:24:30.736600  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61189 -> 10.0.221.1:80
99/01-14:24:30.736600  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61194 -> 10.0.221.1:80
99/01-14:24:30.736600  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61193 -> 10.0.221.1:80
99/01-14:24:30.736643  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61187 -> 10.0.221.1:80
99/01-14:24:30.736643  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61195 -> 10.0.221.1:80
99/01-14:24:30.736643  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61189 -> 10.0.221.1:80
99/01-14:24:30.736643  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61188 -> 10.0.221.1:80
99/01-14:24:30.736643  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61191 -> 10.0.221.1:80
99/01-14:24:30.736643  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61192 -> 10.0.221.1:80
99/01-14:24:30.737215  ** [1:100001:0] Serangan DoS TCP ** [Priority: 0] {TCP} 10.0.221.247:61190 -> 10.0.221.1:80
```

Gambar 12 Hasil Monitoring Snort Metode TCP

- b. Hasil monitoring Snort terhadap serangan metode UDP (*User Datagram Protocol*) yang terdapat pada LOIC, Snort berhasil mendeteksi adanya serangan yang dikirim oleh LOIC dengan menampilkan IP penyerang menuju IP target melalui port 80, seperti pada Gambar 13 (gambar yang diberikan kotak merah).

```
Administrator: Command Prompt - snort -i 5 -c c:\Snort\etc\snort.conf -A console
99/01-14:30:06.023357  ** [1:100002:0] Serangan DoS UDP ** [Priority: 0] {UDP} 10.0.221.247:53658 -> 10.0.221.1:80
99/01-14:30:06.023357  ** [1:100002:0] Serangan DoS UDP ** [Priority: 0] {UDP} 10.0.221.247:53657 -> 10.0.221.1:80
99/01-14:30:06.023357  ** [1:100002:0] Serangan DoS UDP ** [Priority: 0] {UDP} 10.0.221.247:53655 -> 10.0.221.1:80
99/01-14:30:06.023357  ** [1:100002:0] Serangan DoS UDP ** [Priority: 0] {UDP} 10.0.221.247:53652 -> 10.0.221.1:80
99/01-14:30:06.023357  ** [1:100002:0] Serangan DoS UDP ** [Priority: 0] {UDP} 10.0.221.247:53654 -> 10.0.221.1:80
99/01-14:30:06.023357  ** [1:100002:0] Serangan DoS UDP ** [Priority: 0] {UDP} 10.0.221.247:53656 -> 10.0.221.1:80
99/01-14:30:06.023357  ** [1:100002:0] Serangan DoS UDP ** [Priority: 0] {UDP} 10.0.221.247:53660 -> 10.0.221.1:80
99/01-14:30:06.038998  ** [1:100002:0] Serangan DoS UDP ** [Priority: 0] {UDP} 10.0.221.247:53657 -> 10.0.221.1:80
99/01-14:30:06.038998  ** [1:100002:0] Serangan DoS UDP ** [Priority: 0] {UDP} 10.0.221.247:53656 -> 10.0.221.1:80
99/01-14:30:06.038998  ** [1:100002:0] Serangan DoS UDP ** [Priority: 0] {UDP} 10.0.221.247:53660 -> 10.0.221.1:80
99/01-14:30:06.038998  ** [1:100002:0] Serangan DoS UDP ** [Priority: 0] {UDP} 10.0.221.247:53653 -> 10.0.221.1:80
99/01-14:30:06.038998  ** [1:100002:0] Serangan DoS UDP ** [Priority: 0] {UDP} 10.0.221.247:53654 -> 10.0.221.1:80
99/01-14:30:06.038998  ** [1:100002:0] Serangan DoS UDP ** [Priority: 0] {UDP} 10.0.221.247:53652 -> 10.0.221.1:80
99/01-14:30:06.038998  ** [1:100002:0] Serangan DoS UDP ** [Priority: 0] {UDP} 10.0.221.247:53655 -> 10.0.221.1:80
99/01-14:30:06.038998  ** [1:100002:0] Serangan DoS UDP ** [Priority: 0] {UDP} 10.0.221.247:53651 -> 10.0.221.1:80
99/01-14:30:06.038998  ** [1:100002:0] Serangan DoS UDP ** [Priority: 0] {UDP} 10.0.221.247:53658 -> 10.0.221.1:80
99/01-14:30:06.038998  ** [1:100002:0] Serangan DoS UDP ** [Priority: 0] {UDP} 10.0.221.247:53659 -> 10.0.221.1:80
```

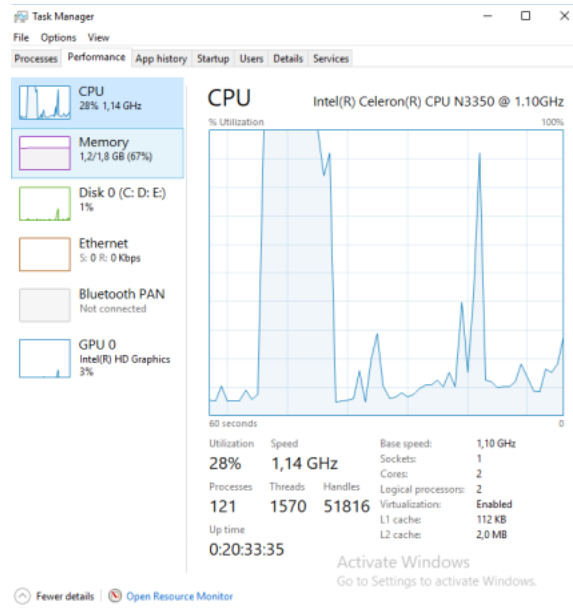
Gambar 13 Hasil Monitoring Snort Metode UDP

- c. Hasil monitoring Snort terhadap serangan yang dikirim oleh metode HTTP, seperti pada Gambar 14.

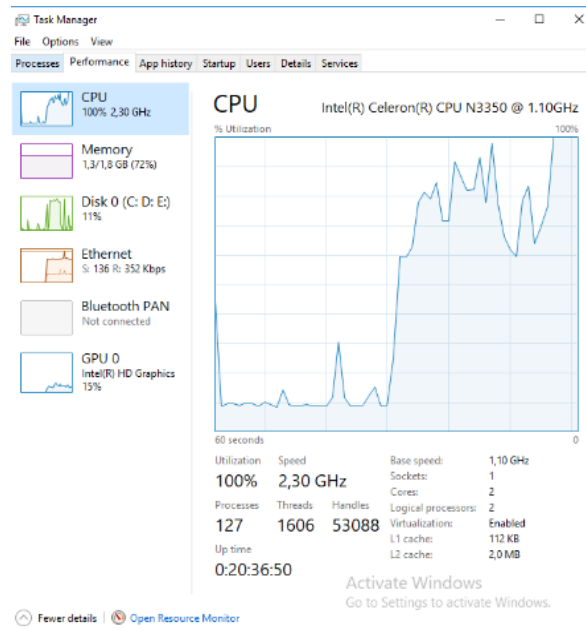
```
221.1:57980
99/01-14:37:57.958274  ** [1:100003:0] Serangan DoS HTTP ** [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:a158:f7e3:9496:9857 -> ff02:0000:0000:0000:0000:0000:0000:0000:0016
99/01-14:37:57.968221  ** [1:100003:0] Serangan DoS HTTP ** [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:a158:f7e3:9496:9857 -> ff02:0000:0000:0000:0000:0000:0000:0000:0016
99/01-14:37:57.968221  ** [1:100003:0] Serangan DoS HTTP ** [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:a158:f7e3:9496:9857 -> ff02:0000:0000:0000:0000:0000:0000:0000:0016
99/01-14:37:57.968221  ** [1:100003:0] Serangan DoS HTTP ** [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:a158:f7e3:9496:9857 -> ff02:0000:0000:0000:0000:0000:0000:0000:0016
99/01-14:37:57.984282  ** [1:100003:0] Serangan DoS HTTP ** [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:a158:f7e3:9496:9857 -> ff02:0000:0000:0000:0000:0000:0000:0000:0016
```

Gambar 14 Hasil Monitoring Snort Metode HTTP

Hasil dari tiga metode serangan yang menunjukkan bahwa serangan yang menggunakan LOIC berhasil dideteksi oleh Snort dengan menampilkan IP penyerang menuju IP target melalui port 80, efek dari serangan mengakibatkan komputer menjadi overload seperti penggunaan CPU pada komputer target mencapai 100% seperti pada gambar 15 dan 16.



Gambar 15 Penggunaan CPU sebelum serang



Gambar 16 Penggunaan CPU setelah diserang

Tabel 3 Hasil Implementasi Skenario Penyerangan 2 Perangkat

IP penyerang	IP target	Metode	Port	Threads	Timeout	Hasil
10.0.221.247	10.0.221.1	TCP	80	10	90001	Terdeteksi
10.0.221.247	10.0.221.1	UDP	80	10	90001	Terdeteksi
10.0.221.247	10.0.221.1	HTTP	80	10	90001	Terdeteksi

3.3. Response

Response merupakan tahap analisis hasil dan laporan hasil serangan yang didapatkan pada penyerangan. Hasil yang di peroleh dari penyerangan yang dilakukan pada Sistem Inventaris Sanggar Tari Natya Lakshita sebanyak tiga kali dengan menggunakan metode penyerangan yang berbeda-beda yaitu TCP, UDP, dan HTTP.

























3.3.1. Analisis hasil serangan

Hasil serangan menggunakan 1 komputer dan 1 laptop menunjukkan Snort berhasil mendeteksi serangan DoS menggunakan tiga metode TCP, UDP dan HTTP pada LOIC. Serangan metode TCP, Snort mendeteksi serangan dengan menampilkan IP Address penyerang yaitu 10.0.221.247 menuju IP komputer target 10.0.221.1 melalui port 80. Hasil serangan menggunakan metode UDP yaitu Snort berhasil mendeteksi serangan dengan menampilkan hasil monitoring IP Address penyerang 10.0.221.247 dan IP Address target 10.0.221.1 melalui port 80, begitu juga dengan hasil monitoring Snort terhadap serangan DoS metode HTTP mendeteksi IP Address penyerang 10.0.221.247 dan IP address target 10.0.221.1 melalui port 80. Efek dari serangan yang dikirim oleh LOIC mengakibatkan komputer menjadi *over load* sehingga penggunaan CPU pada saat dilakukan penyerangan mencapai 100%.

3.3.2. Laporan

Tahap ini merupakan *reporting* atau pelaporan hasil analisis serangan yang dilakukan pada sistem inventaris Sanggar Tari Natya Lakshita. Hasil dari serangan DoS menggunakan *tool* LOIC pada Sistem inventaris berhasil dilakukan penyerangan karena Snort mendeteksi adanya serangan yang dikirim oleh LOIC, dari permasalahan tersebut diberikan rekomendasi penanganan insiden keamanan jaringan berdasarkan panduan CSIRT pada Sanggar Tari Natya Lakshita yang bisa di implementasikan, penanganan insiden keamanan jaringan memiliki enam tahapan antara lain tahap persiapan, tahap identifikasi, tahap penahanan, tahap *eradication*, tahap *recovery* dan tahap *follow up*, tujuan dari tahap-tahap penanganan adalah untuk memastikan manajemen yang efektif dan konsisten dari insiden keamanan jaringan komputer [11].

Tabel 7 Laporan Hasil Analisis Serangan

No	Jenis Informasi Analisis	Keterangan																																								
1	Serangan DoS dengan tiga metode menggunakan LOIC pada keamanan jaringan sistem inventaris menggunakan 1 komputer dan 1 laptop	Snort berhasil mendeteksi serangan dari tiga metode yang dikirim LOIC dengan menampilkan IP Address penyerang dan IP target melalui port 80 sehingga komputer target menjadi <i>over load</i> dan mengakibatkan penggunaan CPU mencapai 100% ketika dilakukan penyerangan.																																								
2	Snort Log	<table border="1"> <tr> <td></td> <td>snort.log.1657768241</td> <td>14/07/2022 10:12</td> <td>1657768241 File</td> <td>86 KB</td> </tr> <tr> <td></td> <td>snort.log</td> <td>14/07/2022 10:37</td> <td>1657769791 File</td> <td>1.336 KB</td> </tr> <tr> <td></td> <td>snort.log.1657803202</td> <td>14/07/2022 19:53</td> <td>1657803202 File</td> <td>80 KB</td> </tr> <tr> <td></td> <td>snort.log.1657806302</td> <td>14/07/2022 20:46</td> <td>1657806302 File</td> <td>45 KB</td> </tr> <tr> <td></td> <td>snort.log.1657806940</td> <td>14/07/2022 20:56</td> <td>1657806940 File</td> <td>649 KB</td> </tr> <tr> <td></td> <td>snort.log.1657808258</td> <td>14/07/2022 21:24</td> <td>1657808258 File</td> <td>8 KB</td> </tr> <tr> <td></td> <td>snort.log.1657847825</td> <td>15/07/2022 8:18</td> <td>1657847825 File</td> <td>195 KB</td> </tr> <tr> <td></td> <td>snort.log.1657848835</td> <td>15/07/2022 8:35</td> <td>1657848835 File</td> <td>29 KB</td> </tr> </table>		snort.log.1657768241	14/07/2022 10:12	1657768241 File	86 KB		snort.log	14/07/2022 10:37	1657769791 File	1.336 KB		snort.log.1657803202	14/07/2022 19:53	1657803202 File	80 KB		snort.log.1657806302	14/07/2022 20:46	1657806302 File	45 KB		snort.log.1657806940	14/07/2022 20:56	1657806940 File	649 KB		snort.log.1657808258	14/07/2022 21:24	1657808258 File	8 KB		snort.log.1657847825	15/07/2022 8:18	1657847825 File	195 KB		snort.log.1657848835	15/07/2022 8:35	1657848835 File	29 KB
	snort.log.1657768241	14/07/2022 10:12	1657768241 File	86 KB																																						
	snort.log	14/07/2022 10:37	1657769791 File	1.336 KB																																						
	snort.log.1657803202	14/07/2022 19:53	1657803202 File	80 KB																																						
	snort.log.1657806302	14/07/2022 20:46	1657806302 File	45 KB																																						
	snort.log.1657806940	14/07/2022 20:56	1657806940 File	649 KB																																						
	snort.log.1657808258	14/07/2022 21:24	1657808258 File	8 KB																																						
	snort.log.1657847825	15/07/2022 8:18	1657847825 File	195 KB																																						
	snort.log.1657848835	15/07/2022 8:35	1657848835 File	29 KB																																						
3	IP Address Penyerang	10.0.221.247																																								
4	IP Address Target	10.0.221.249 10.0.221.1																																								

4. Kesimpulan

Hasil dari serangan DoS dengan menggunakan *tool* LOIC pada Sistem Inventaris Sanggar Tari Natya Lakshita berhasil dilakukan penyerangan karena Snort berhasil mendeteksi adanya serangan dengan menampilkan IP penyerang dan IP target melalui port 80, efek dari serangan juga membuat komputer target menjadi *over load* dan mengakibatkan penggunaan CPU mencapai 100%, kemudian diberikan rekomendasi tahap-tahap penanganan insiden keamanan jaringan berdasarkan panduan CSIRT pada Sanggar Tari Natya Lakshita yang bisa di implementasikan antara lain tahap persiapan, tahap identifikasi, tahap penahanan, tahap *eradication*, tahap *recovery* dan tahap *follow up*.

Cara kerja IDS Snort dalam melakukan pendeteksian serangan memiliki tiga tahapan kerja, tahap pertama yaitu membaca *rule* Snort yang berisi pola-pola serangan, tahap kedua Snort *engine* membaca paket data kemudian membandingkan dengan *rule* Snort, tahap ketiga *alert* dengan mencatat serangan penyusup kemudian Snort *engine* mendeteksi paket data yang lewat berupa serangan lalu Snort *engine* akan mengirimkan *alert* berupa *log* file dan *log* file akan tersimpan di dalam *database*.

Referensi

- [1] W. W. Purba and R. Efendi, "Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT," vol. 17, no. 2, pp. 143–158, 2021.
- [2] P. Panggabean, "Analisis Network Security Snort Metode Intrusion Detection System Untuk Optimasi Keamanan Jaringan Komputer," *Jursima*, vol. 6, no. 1, p. 1, 2018, doi: 10.47024/js.v6i1.107.
- [3] M. Ulfa, "Implementasi Insrusion Detection System (IDS) Di Jaringan Internet Universitas Bina Darma," *J. Imiah MATRIK*, vol. 15, no. 12, pp. 105–118, 2013.
- [4] D. N. Thowok, "Sanggar Tari Natya Lakshita," *didiknikthowok.id*, 2020. .
- [5] A. Y. Suharmanto, A. S. M. Lumenta, and X. B. N. Najoran, "Analisa Keamanan Jaringan Wireless Di Universitas Sam Ratulangi," *J. Tek. Inform.*, vol. 13, no. 3, pp. 1–10, 2018, doi: 10.35793/jti.13.3.2018.28074.
- [6] J. D. Susanto, "SATIN – Sains dan Teknologi Informasi Keamanan Jaringan Menggunakan IDS / IPS Strataguard sebagai Layanan Kemanan Jaringan Terpusat," vol. 3, no. 2, 2017.
- [7] M. Akbar, "PERANCANGAN SOFTWARE IDS SNORT UNTUK PENDETEKSIAN SERANGAN INTERRUPTION (Netcut) PADA JARINGAN WIRELESS," *J. INSTEK (Informatika Sains dan Teknol.*, vol. 3, no. 1, pp. 121–129, 2018, doi: 10.24252/instek.v3i1.5007.
- [8] E. K. Dewi and P. Kasih, "ANALISIS LOG SNORT MENGGUNAKAN NETWORK FORENSIC," vol. 02, 2017.
- [9] M. Anif, S. Hws, and M. D. Huri, "Penerapan Intrusion Detection System (IDS) dengan metode Deteksi Port Scanning pada Jaringan Komputer di Politeknik Negeri Semarang," *J. TELE, Vol. 13 Nomor 1*, vol. 13, no. 1, pp. 25–30, 2015.
- [10] D. Kurnia, "Analisis Forensik Serangan SQL Injection dan DoS Menggunakan Instrution Detection System Pada Server Berbasis Lokal," *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 4, no. 2, pp. 208–212, 2020, [Online]. Available: <https://jurnal.uisu.ac.id/index.php/infotekjar/article/view/2420>.
- [11] Ninla Elmawati Falabiba, "Keamanan Jaringan," pp. 3–15, 2019.