The Indonesian Journal of Computer Science
www.ijcs.net
Volume 13, Issue 5, October 2024
https://doi.org/10.33022/ijcs.v13i5.4391

Audit Keamanan Jaringan Komputer Server dari Serangan DDoS Menggunakan Snort Intrusion Detection System

M.Iqbal[1], Yuhandri[2], Syafri Arlis[3]
iqbalcp33@gmail.com[1], yuhandri.yunus@gmail.com[2], syafri_arlis@upiyptk.ac.id[3]
[1,2,3] Fakultas Ilmu Komputer, Universitas Putra Indonesia YPTK Padang, 25221, Indonesia

Informasi Artikel

Diterima : 4 Sep 2024
Direvisi : 29 Sep 2024
Disetujui : 29 Okt 2024

Kata Kunci

Audit, Keamanan Jaringan, DDoS, Snort, IDS

Abstrak

Keamanan jaringan komputer adalah aspek krusial bagi institusi pendidikan yang bergantung pada teknologi informasi untuk kegiatan operasional, termasuk proses belajar mengajar. SMKS YPPI Tualang, sebuah sekolah swasta di Riau yang merupakan bagian dari program CSR PT Indah Kiat Pulp and Paper Tbk, menghadapi ancaman serius dari serangan *Distributed Denial of Service* (DDoS), yang dapat menyebabkan gangguan signifikan pada layanan jaringan. DDoS adalah serangan yang dilakukan oleh beberapa sistem komputer untuk membanjiri server dengan lalu lintas berlebihan, sehingga menyebabkan gangguan layanan. Penelitian ini bertujuan untuk meningkatkan keamanan jaringan di SMKS YPPI Tualang melalui audit keamanan yang mendalam dan implementasi *Snort*, sebuah *Intrusion Detection System* (IDS) yang efektif dalam mendeteksi dan mencegah serangan DDoS. Dengan melakukan analisis terhadap potensi celah keamanan dan kerentanan, penelitian ini diharapkan dapat memberikan kontribusi dalam memitigasi risiko serangan DDoS, sehingga menjaga kelangsungan operasional sekolah. Hasil dari penelitian ini menunjukkan bahwa implementasi *Snort* mampu meningkatkan deteksi dini terhadap ancaman dan memperkuat keamanan jaringan sekolah.

Keywords

Audit, Network Security, DDoS, Snort, IDS

Abstract

Network security is a crucial aspect for educational institutions that rely on information technology for operational activities, including teaching and learning processes. SMKS YPPI Tualang, a private school in Riau that is part of PT Indah Kiat Pulp and Paper Tbk's CSR program, faces serious threats from Distributed Denial of Service (DDoS) attacks, which can cause significant disruptions to network services. DDoS attacks involve multiple computer systems overwhelming a server with excessive traffic, leading to service disruptions. This study aims to enhance network security at SMKS YPPI Tualang through a comprehensive security audit and the implementation of Snort, an Intrusion Detection System (IDS) effective in detecting and preventing DDoS attacks. By analyzing potential security gaps and vulnerabilities, this study is expected to contribute to mitigating the risk of DDoS attacks, thereby ensuring the continuity of the school's operations. The results of this study indicate that the implementation of Snort can improve early threat detection and strengthen the school's network security.

A. Pendahuluan

Jaringan komputer merupakan sebuah sistem yang terdiri dari komputer-komputer yang didesain untuk dapat berbagi sumber daya [1]. Jaringan komputer menjadi komponen penting dalam mendukung aktivitas operasional, terutama di institusi pendidikan yang bergantung pada infrastruktur teknologi informasi untuk proses belajar mengajar. Keamanan jaringan komputer tentunya menjadi masalah yang harus dihadapi ketika memutuskan memulai akses informasi secara *online*, terlebih jika berhubungan dengan data sensitif yang dapat mempengaruhi kinerja dan reputasi [1], tujuannya yaitu untuk mengantisipasi resiko jaringan komputer yang berup ancaman fisik maupun logik baik langsung ataupun tidak langsung mengganggu aktifitas dalam jaringan komputer [2].

SMKS YPPI Tualang, sebuah sekolah swasta di Kecamatan Tualang, Provinsi Riau, yang merupakan bagian dari program *Corporate Social Responsibility* (CSR) PT Indah Kiat *Pulp and Paper Tbk*, menghadapi tantangan serius dalam menjaga keamanan jaringan komputer mereka. Salah satu tindak kejahatan pada jaringan komputer adalah serangan *Distributed Deniel of Service* (DDoS) [3]. DDoS merupakan sebuah percobaan penyerangan dari beberapa sistem komputer yang menargetkan sebuah server agar jumlah *traffic* menjadi terlalu tinggi sampai server tidak bisa menghendel *request* [4]. Berbagai macam serangan DDoS diantaranya *ICMP flooding (ping of death)*, *TCP flooding* dan *UDP flooding* [5]. DDoS yang paling sering digunakan adalah *ping of deadth*, dimana penyerang memanfaatkan komunikasi ICMP untuk dibanjiri oleh paket data yang diminta, sehingga membuat sistem server menjadi lambat [3]. Serangan DDoS saat ini menargetkan layanan yang spesifik, sehingga target akan menjadi *down* [6]. Serangan DDoS mempengaruhi korban dalam bentuk menemukan *bug* atau kelemahan untuk mengganggu layanan atau menghabiskan semua *bandwidth* sumber daya dari sistem korban [7]. Ancaman seperti serangan *Distributed Denial of Service* (DDoS) dapat mengakibatkan gangguan signifikan pada operasional sekolah, termasuk proses belajar mengajar, yang berdampak pada kerugian waktu dan biaya.

Untuk melindungi infrastruktur teknologi informasi SMKS YPPI Tualang, diperlukan audit keamanan jaringan yang bertujuan untuk mendeteksi celah keamanan dan kerentanan pada jaringan. Audit keamanan merupakan proses pengumpulan bukti untuk mengevaluasi keamanan sistem secara keseluruhan termasuk kebijakan, prosedur, kontrol, dan infrastruktur teknologi informasi [8]. Audit ini bertujuan untuk memastikan bahwa sistem memenuhi kebutuhan keamanan organisasi dan meminimalkan resiko keamanan sistem informasi [8]. Salah satu solusi yang dapat digunakan adalah dengan mengimplementasikan *Snort*, sebuah *Intrusion Detection System* (IDS) yang efektif dalam mendeteksi dan mencegah serangan DDoS. Snort merupakan sebuah aplikasi keamanan jaringan yang berfungsi dalam mendeteksi adanya ancaman dalam jaringan komputer, seperti penyusup, pemidaian, maupun penyerangan [5]. *Snort* merupakan *tools* yang berbasis *Intrusion Detection System* (IDS) yang dapat memonitor jaringan yang berdampak serangan dan menyimpan serangan pada log [3]. *Intrusion Detection System* (IDS) merupakan sistem yang mendeteksi dan mencegah tindakan yang dilakukan dengan tujuan merusak komputer dan jaringan komputer [9]. Dalam mengamankan jaringan komputer, metode IDS dapat mengoptimalkan

tingkat keamanan jaringan komputer untuk mendeteksi adanya serangan sehingga administrator segera melakukan tindakan pencegahan [10]. IDS mampu mendeteksi serangan sesusai dengan *rule* yang dibuat dan memberikan penanganan serangan sesuai dengan aksi yang dilakukan oleh administrator [11].

Melalui penelitian ini, diharapkan dapat diidentifikasi potensi celah keamanan serta kerentanan pada jaringan komputer yang dapat dimanfaatkan oleh penyerang. Hasil penelitian ini juga diharapkan dapat memberikan kontribusi yang signifikan dalam meningkatkan keamanan jaringan komputer di SMKS YPPI Tualang, sehingga dapat mencegah terjadinya serangan DDoS dan menjaga kelangsungan operasional sekolah.

B. Metode Penelitian

Penelitian ini dilakukan dalam bentuk tahapan-tahapan yang terstruktur dimana setiap tahapannya harus dilakukan dengan metode yang kritis, dan mampu mengarahkan proses dengan tepat. Metode-metode ini juga harus bersifat logis dan objektif sehingga dapat menjadi rujukan bagi penelitian lainnya. Metode penelitian ini merupakan teknik-teknik yang dipakai dalam merumuskan, menganalisa, mengumpulkan data sampai dengan proses implementasi dan pengujian hasil penelitian.

Tujuan dari penelitian ini adalah melakukan audit keamanan jaringan komputer server pada SMKS YPPI Tualang dengan menerapkan *Intrusion Detection System* (IDS) dengan *tools Snort* untuk mendeteksi celah keamanan dan kerentanan yang terjadi pada jaringan untuk meningkatkan perlindungan terhadap insfrastruktur teknologi informasi yang digunakan dan menganalisa potensi celah keamanan serta kerentanan yang dapat dimanfaatkan oleh penyerang untuk melancarkan serangan DDoS. Penelitian ini dilakukan dengan metode pembentukan kerangka kerja dimana kerangka kerja ini perlu dirancang agar penelitian bisa dilakukan dengan terstruktur dan terarah sesuai tujuan yang diharapkan. Kerangka kerja merupakan tahapan-tahapan proses penelitian yang terurut berdasarkan langkah-langkah yang saling berkaitan. Langkah-langkah tersebut dimulai dari identifikasi masalah, studi literatur, perencanaan audit, pengumpulan data dan informasi, implementasi IDS, pengumpulan data jaringan, pelaksanaan audit, dan pelaporan hasil audit (*reporting*). Kerangka penelitian ini dapat digambarkan sebagai berikut.

Gambar 1. Diagram Alir Penelitian

C. Hasil dan Pembahasan

1. Pengaturan dan Konfigurasi Snort

Snort adalah salah satu sistem deteksi intrusi (*Intrusion Detection System* atau IDS) yang populer dan digunakan untuk mendeteksi serangan terhadap jaringan komputer. Berikut langkah-langkah pengaturan dan konfigurasi *Snort* pada server.

1. Lakukan Instalasi *Snort* pada server
2. Setelah melakukan instalasi Snort pada server, tahap selanjutnya adalah melakukan konfigurasi pada *file snort.conf* yang terletak pada direktori c:\snort\etc\
3. Lakukan konfigurasi jaringan pada *file snort.conf* dengan memasukkan alamat ip yang akan di monitoring atau diaudit. Berikut gambar konfigurasi ip pada *Snort*

```
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.80.1
```

Gambar 2. Konfigurasi *IP Snort*

4. Lakukan konfigurasi *rule snort* pada *file snort.conf* dengan menginputkan alamat *directory rule* yang akan dipakai. Berikut gambar konfigurasi *rule* pada *Snort*

```
# site specific rules
include C:\Snort\rules\local.rules
```

Gambar 3. Konfigurasi *Rule Snort*

5. Konfigurasi aturan *rule* pada *snort* dengan mengakses *file local.rules* yang terdapat pada *folder rules*.
6. Selah aturan *rule* pada *Snort* selesai, *Snort* sudah dapat digunakan untuk analisis dan audit jaringan komputer server dengan mengakses pada *commend prompt*. Berikut tampilan *snort* setelah selesai dilakukan instalasi.

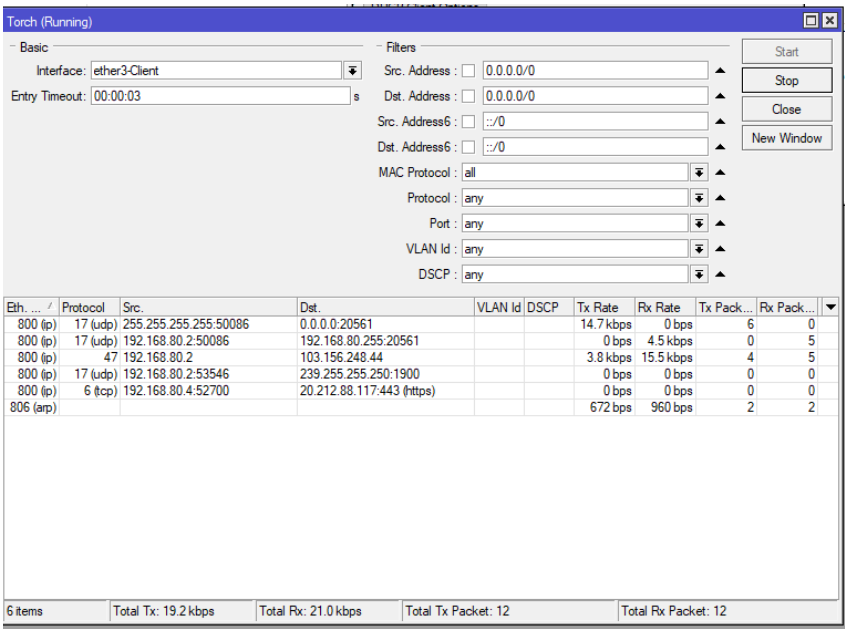
```
C:\Snort\bin>snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11
```

Gambar 4. Tampilan *Snort*

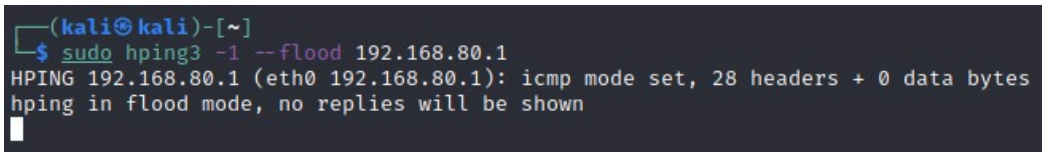
2. Implementasi Audit Server Dengan Metode Intrusion Detection System

Proses awal untuk analisis dan audit apakah router masih dalam keadaan normal atau sudah ada serangan DDoS, dapat dilakukan pengecekan melalui aplikasi WinBox, yaitu melalui *Tourch Running* dan *Resource* untuk melihat beban CPU pada server. Setelah dilakukan pengecekan diketahui belum ada serangan yang masuk , hal ini dapat dilihat dari lalu lintas *destination*, *Tx Rate* dan *Rx Rate*. Tampilan *Tourch* sebelum serangan terjadi dapat dilihat pada gambar 5.



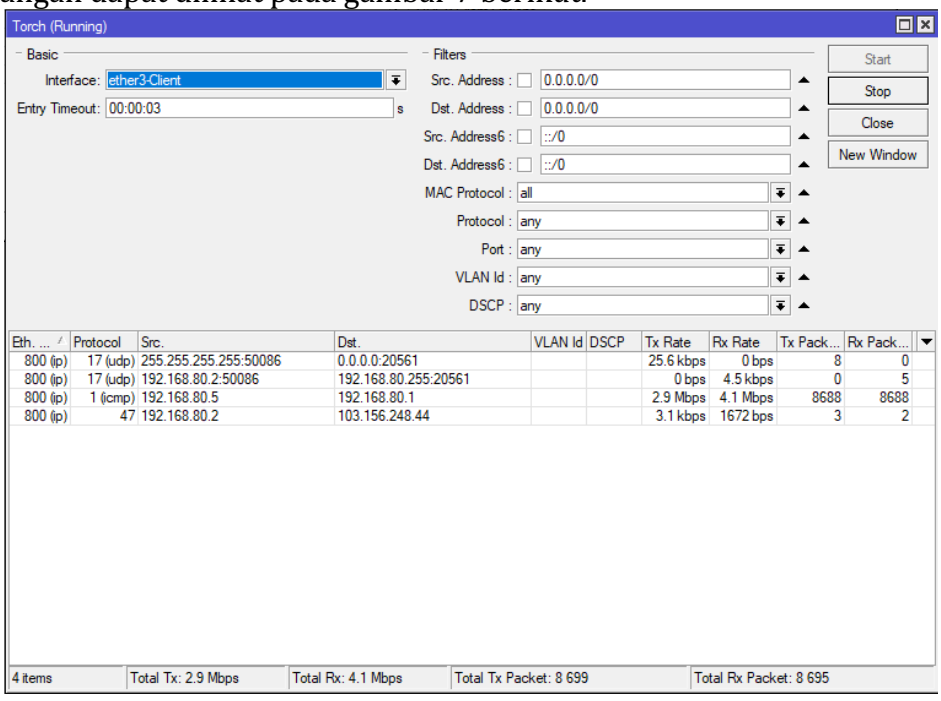
Gambar 5. Tampilan *Tourch* Sebelum Serangan DDoS

Berdasarkan Gambar 5.6, terlihat nilai *Tx Rate* 19.6 kbps dan *Rx rate* 21.0 kbps masih dalam keadaan normal dan *Tx Packet* 12 dan *Rx Packet* 12 dalam keadaan normal. Hal ini dapat disimpulkan belum ada serangan yang masuk dan mengganggu lalu lintas jaringan pada router server. Hal ini dapat dilihat pada kolom *source* dan *destination* terdapat ip dari masing-masing komputer dalam melakukan komunikasi antara satu dengan lainya secara normal. Tahapan selanjutnya adalah mulai melakukan simulasi serangan DDoS pada router menggunakan serangan *ping of deadth* atau *flooding* (Hping3) untuk mengetahui apakah serangan DDoS yang diluncurkan berhasil menembus jaringan router. Pada kondisi ini juga akan dilakukan audit dan analisis serangan DDoS pada router server menggunakan aplikasi *snort*, untuk mengetahui apakah *snort* mampu mendeteksi serangan. Untuk melakukan serangan terhadap perangkat jaringan router atau server yang dituju dengan perintah hping3 -1 –flood 192.168.80.1, yang mana 192.168.80.1 merupakan ip perangkat router server yang merupakan target serangan yang akan dilakukan audit. Simulasi Serangan dapat dilihat pada gambar 6 berikut.



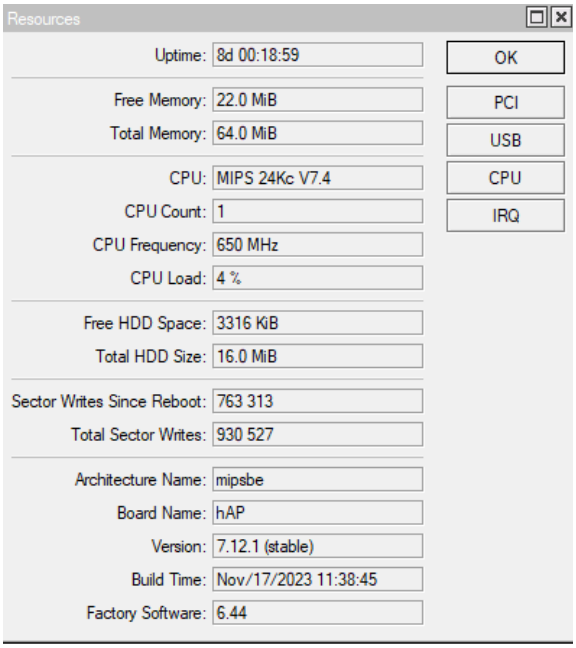
Gambar 6. Pengujian Serangan Pada Server

Ketika penyerangan berlangsung terjadi peningkatan nilai *Tx Rate* yaitu dari keadaan normal 19.6 kbps menjadi 2,9Mbps dan *Rx rate* dari keadaan normal 21.0 kbps menjadi 4,1Mbps, dan *Tx Packet* dari keadaan normal 12 menjadi 8699 dan *Rx Packet* dari keadaan normal 12 menjadi 8695 yang dapat dilihat pada tampilan tourch pada jaringan router server. Tampilan *tourch* ketika terjadi penyerangan dapat dilihat pada gambar 7 berikut.



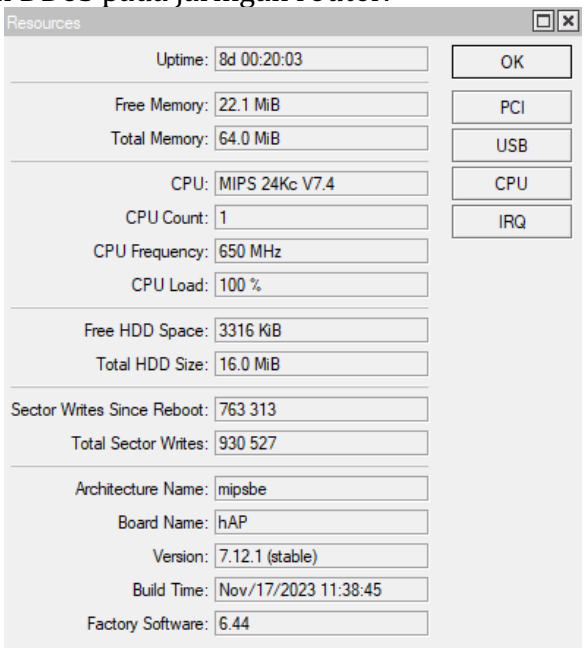
Gambar 7. Tampilan *Tourch* Ketika Terjadi Serangan

Berdasarkan hasil analisis pada *traffic* monitor sistem sebelum terjadi serangan DDoS, diketahui bahwa keadaan *traffic system* sebelum terjadi serangan menunjukkan presentasi *CPU load* adalah 4% dan *free memory* 22,0 MiB belum bergerak secara signifikan karna belum terjadi transaksi serangan DDoS yang dapat mempengaruhi kinerja atau *load* pada jaringan router. Hal ini dapat dilihat pada Gambar 8 berikut ini.



Gambar 8. Kondisi *Resource* Sebelum Terjadi Serangan

Setelah adanya serangan DDoS, CPU dan *memory* mengalami kenaikan akses secara signifikan dan bertahap yang menyebabkan kinerja atau *load* dari *packet* data pada router menjadi *down*. Berikut tampilan *traffic* monitoring system CPU dan memori setelah ada serangan DDoS pada jaringan router.



Gambar 9. Kondisi Setelah Serangan

Gambar 9 menunjukkan setelah ada serangan DDoS yang masuk pada jaringan router, *Load CPU* dan penggunaan *memory* meningkat. Berdasarkan hasil *traffic* monitor *system* setelah terjadi serangan DDoS diketahui *traffic system* monitor *packet* data *CPU load* meningkat menjadi 100 % dan menyebabkan jaringan server menjadi *down*.

3. Penerapan *Snort* Dalam Deteksi Serangan

Setelah tahap simulasi serangan DDoS tahap selanjutnya yaitu penerapan *Snort* pada server untuk mendeteksi serangan yang disimulasikan. Langkah-langkah penerapan *Snort* adalah sebagai berikut.

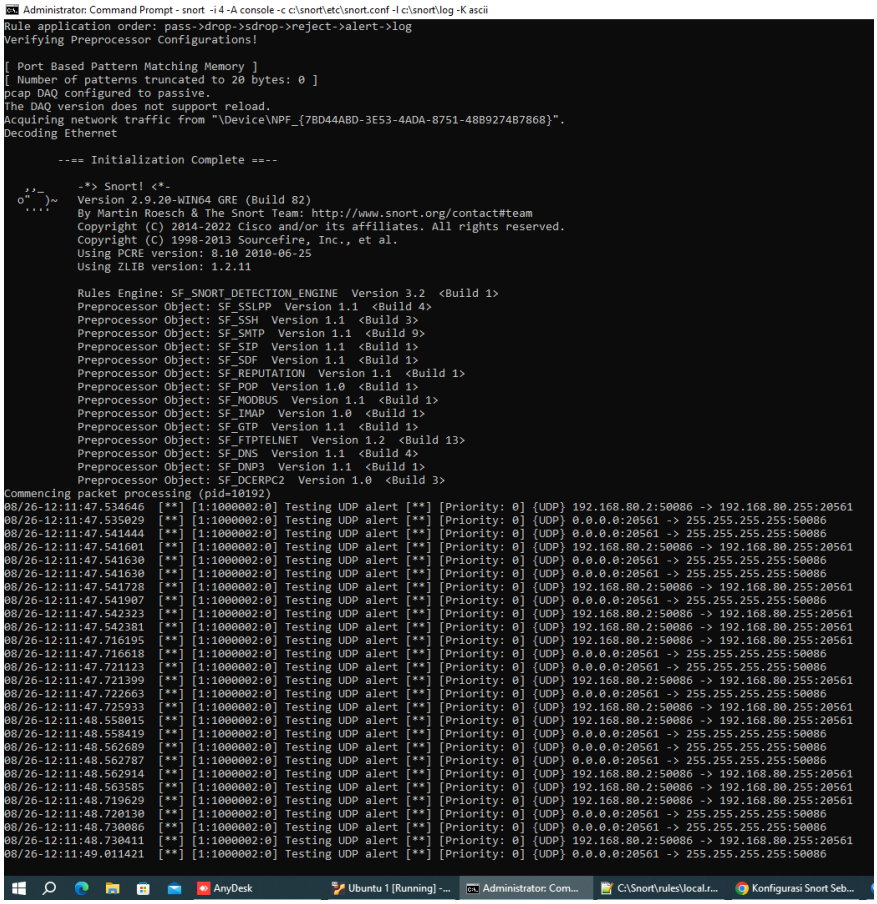
1. Pengaktifan *Snort* pada Server

Snort diaktifkan pada server dengan menggunakan *file* konfigurasi *snort.conf* yang telah disiapkan sebelumnya dengan menggunakan cmd dengan mengetikkan perintah snort -i 4 -A console -c c:\snort\etc\snort.conf -1 c:\snort\log -K ascii yang dapat dilihat pada gambar berikut:

```
C:\Snort\bin>snort -i 4 -A console -c c:\snort\etc\snort.conf -l c:\snort\log -k ascii
```

Gambar 10. Perintah Menjalankan *Snort*

Setelah memasukkan perintah snort -i 4 -A console -c c:\snort\etc\snort.conf -1 c:\snort\log -K ascii, *Snort* akan melakukan monitoring jaringan server dengan menampilkan aktifitas lalu lintas jaringan pada server. Berikut gambar monitoring jaringan pada server menggunakan *Snort* dapat dilihat pada gambar 11.



Gambar 11. Monitoring Jaringan Komputer Server Menggunakan *Snort*

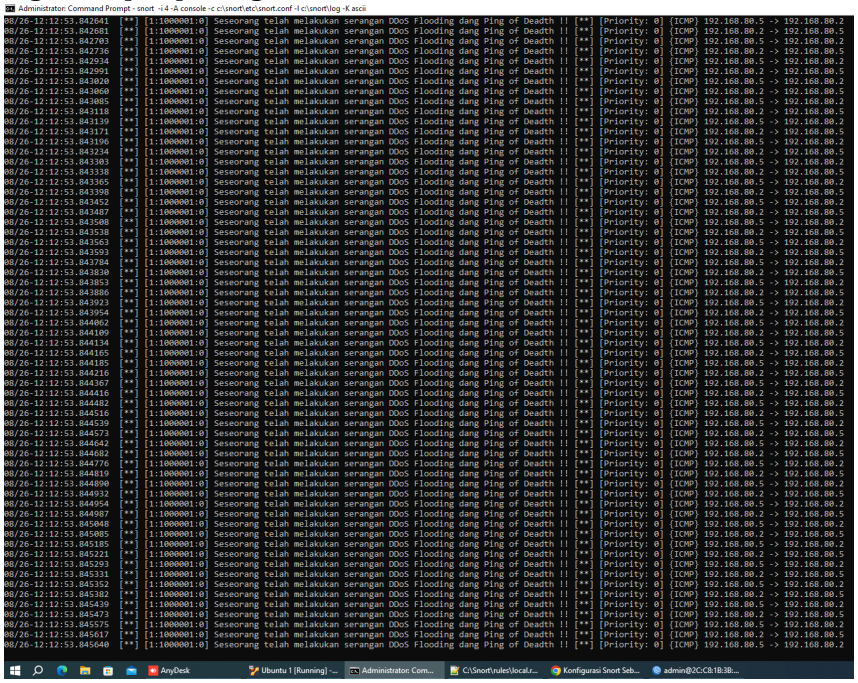
2. Melakukan serangan terhadap server menggunakan *tools* hping3

Serangan terhadap server dilakukan menggunakan *tools* hping3 pada sistem operasi kali linux dengan perintah sudo hping3 -1 –flood 192.168.80.2 yang dapat dilihat pada gambar 12 berikut.

```
└─$ sudo hping3 -1 --flood 192.168.80.2
HPING 192.168.80.2 (eth0 192.168.80.2): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

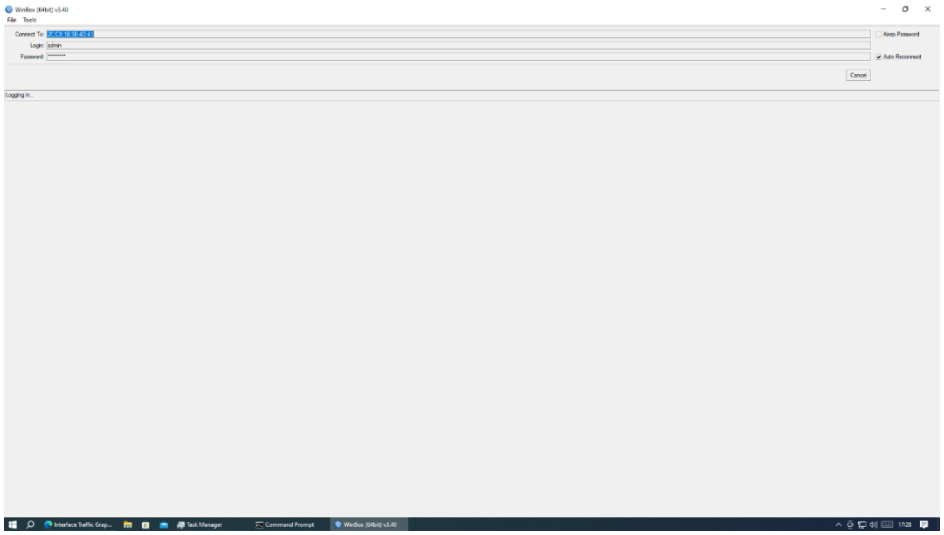
Gambar 12. Perintah Serangan Terhadap Komputer Server

Setelah dilakukan serangan menggunakan perintah pada gambar 12 maka sistem akan mengirimkan paket dengan *traffic* yang besar kepada server sehingga server mendapatkan *packet* dengan beban yang tinggi sehingga membuat server menjadi *down*. Berikut gambar monitoring server menggunakan *Snort* yang menangkap adanya serangan DDoS dengan jenis serangan *ping of deadth* dan *flooding* yang terdapat pada gambar 13 berikut.



Gambar 13. Monitoring Jaringan Server Ketika Terjadi Serangan

Pada gambar 13 terlihat kondisi server yang terkena serangan DDoS dengan jenis serangan *ping of deadth* dan *flooding* yang mana server mendapatkan *packet* dengan protokol icmp yang dikirim oleh *attacker* dengan ip 192.168.80.5 sehingga membuat jaringan server menjadi *down* yang dapat dilihat pada gambar 14



Gambar 14. Kondisi Server Setelah Mengalami Serangan DDoS

Pada gambar 14 menunjukkan keadaan server yang *down* ketika serangan DDoS berlangsung, yang mengakibatkan peningkatan *CPU load* dan penggunaan *memory*. Perbandingan penggunaan *memory* dan *CPU Load* sebelum dan saat terjadi serangan dapat dilihat pada tabel 1 berikut

Tabel 1. Penggunaan *CPU load* dan *memory* sebelum dan saat terjadi serangan

Kondisi	TX Rate	RX Rate	TX Packet	RX Packet	CPU Load	Memory
Normal	19,2kbps	21,0kbps	12	12	4%	22,0MiB
Diserang	2,9Mbps	4,1Mbps	8699	8695	100%	22,1MiB

4. Analisis Log dan Allert

Setelah implementasi *Snort* dalam jaringan, tahap berikutnya adalah melakukan analisis terhadap *log* dan *alert* yang dihasilkan. *Log* dan *alert* ini merupakan hasil dari proses deteksi yang dilakukan oleh *Snort* terhadap berbagai aktivitas yang mencurigakan atau berpotensi sebagai ancaman, seperti serangan DDoS. *Log* yang dihasilkan oleh *Snort* mencakup informasi penting seperti alamat IP sumber dan tujuan, *timestamp*, jenis protokol yang digunakan, serta tanda-tanda khusus dari aktivitas yang terdeteksi sebagai serangan.

Gambar 15. Hasil *Log* Serangan *Attacker*

Pada gambar 15 menunjukkan terjadi serangan pada jaringan komputer server dengan ip 192.168.80.2 pada tanggal 26 Agustus 2024 pukul 11.52 dengan jenis serangan *ping of deadth* dan *flooding* dengan besar paket yang dikirim 660.971 yang dilakukan oleh penyerang dengan ip 192.168.80.5.

5. Evaluasi Audit dan Hasil Analisis

Evaluasi Audit merupakan tahapan yang bertujuan untuk menilai efektivitas *Snort* dalam mendeteksi serangan, terutama serangan *Distributed Denial of Service* (DDoS), serta untuk mengukur kinerja sistem infrastruktur jaringan server. Salah satu tujuan utama dari implementasi Snort adalah untuk mendeteksi berbagai jenis serangan siber secara *real-time*, termasuk serangan DDoS. Dalam evaluasi ini, berbagai jenis serangan DDoS seperti *ping of deadth*, *HTTP Flood*, dan *ICMP Flood* telah diuji untuk menilai respons Snort terhadap ancaman tersebut. Hasil evaluasi Audit dapat dirangkum pada pada tabel 2 berikut.

Tabel 2. Hasil Evaluasi Audit

No	Jenis Serangan	Keterangan
1	*Ping of Deadth*	Snort berhasil mendeteksi serangan *ping of deadth* yaitu serangan dengan mengirimkan *packet ping* yang besar kepada server sehingga membuat server menjadi *down* dengan *alert* yang menunjukkan alamat ip penyerang dengan ip 192.168.80.5 dengan besar *packet ping* yang dikirim sebesar 8699.

2	*ICMP Flood*	Snort berhasil mendeteksi serangan *ICMP Flood* yaitu jenis serangan yang mengirim permintaan paket ping yang besar melalui protokol IMCP dengan *alert* yang menunjukkan ip sumber atau penyerang dengan ip 192.168.80.5 dengan paket yang dikirim sebesar 660.971 terjadi pada tanggal 26 Agustus 2024 pada pukul 11.52
3	*HTTP Flood*	Snort berhasil mendeteksi pola trafik yang tidak normal dengan cepat, menghasilkan *alert* yang menunjukkan adanya lonjakan permintaan HTTP dari alamat IP 10.10.10.1 yang terdeteksi.

Tabel 2 menunjukkan bahwasanya Snort memiliki kemampuan yang baik dalam mendeteksi serangan DDoS, dengan tingkat keberhasilan deteksi yang baik. Berdsarkan hasil audit keamanan jaringan menggunakan metode *Intrusion Detection System* (IDS) dari serangan DDoS yaitu dengan jenis serangan *ping of deadth* dan *flooding* maka dapat disajikan hasil penelitian sebagai laporan jaringan berdasarkan proses audit dan analisis jaringan dari serangan DDoS untuk peningkatan keamanan pada jaringan server yang meliputi perangkat jaringan dan server yang telah peneliti lakukan. Hasil audit dan analisis tersebut dapat dirangkum pada tabel 3 berikut.

Tabel 3. Hasil Audit dan Analisa Serangan Pada Jaringan Server

NO	Analisis	Keterangan
1	Serangan DDoS pada server menggunakan aplikasi Hping3 menggunakan kali linux	Berhasil melakukan serangan pada jaringan komputer server secara terus-menerus dengan *traffic* yang besar sehingga jaringan server menjadi *down*
2	Snort berhasil menangkap aktivitas lalu lintas jaringan yang mencurigakan.	Snort berhasil mendeteksi serangan DDoS yaitu dengan jenis serang *flooding* dan *ping of deadth* dan memperoleh informasi mengenai waktu terjadinya serangan, jenis serangan, besar *packet* yang dikirim dan ip penyerang.
3	*Protocol* serangan yang berhasil di tembus	*Protocol* jaringan yang berhasil ditembus yaitu *protocol* ICMP, UDP, and HTTP.
4	Kondisi CPU dan *memory* perangkat jaringan sebelum diserang	*CPU Load* 4% *Memory* 22,0 MiB
5	Kondisi CPU dan *memory* perangkat jaringan ketika diserang	*CPU Load* 100% *Memory* 22,1 MiB
6	Kondisi CPU dan *memory* perangkat jaringan setelah diserang	*CPU Load* 5% *Memory* 22,1 MiB
7	*Log Activity*	Gagal melakukan login pada perangkat jaringan server ketika terjadi penyerangan
8	a. *IP Address* Penyerang b. IP Router c. IP Komputer Server d. IP Router to ISP (*Internet Service Provider*)	a. 192.168.80.5 b. 192.168.80.1 c. 192.168.80.2 d. 192.168.100.2

Hasil Audit dan analisis menunjukkan bahwasanya *snort* dengan metode *Intrusion Detection System* mampu mendeteksi serangan DDoS yaitu dengan jenis serangan

flooding dan *ping of dedth* dan menunjukkan keamanan jaringan server SMKS YPPI Tualang masih rentan terhadap serangan DDoS dan perlu dilakukan peningkatan keamanan dengan melakukan konfigurasi pada perangkat jaringan dengan melakukan konfigurasi *firewall filter*, *firewall raw* dan memblokir ip yang terdeteksi melakukan penyerangan untuk meningkatkan keamanan jaringan komputer server dari berbagai macam serangan terkhusus serangan DDoS.

6. Rekomendasi Hasil Audit

Berdasarkan hasil audit keamanan yang telah dilakukan sebelum dan sesudah implementasi *Snort* sebagai *Intrusion Detection System* (IDS), terdapat sejumlah rekomendasi yang dapat diambil untuk lebih meningkatkan keamanan jaringan. Rekomendasi ini didasarkan pada temuan-temuan audit yang menyoroti area yang memerlukan perbaikan serta peluang untuk meningkatkan efektivitas sistem keamanan secara keseluruhan. Temuan yang perlu dilakukan peningkatan berdasarkan hasil audit pada keamanan jaringan dapat dilihat pada tabel 4.

No	Temuan	Rekomendasi
1	Serangan DDoS dengan jenis serangan *ping of deadth* dan *flooding* mampu menyerang jaringan komputer server dan membuat perangkat jaringan menjadi *down*	Lakukan peningkatan keamanan pada insfratruktur jaringan komputer server dengan mengkonfigurasi *firewall filter* dan *firewall raw* dengan melakukan bloking ip yang terdeteksi melakukan penyerangan
2	IP penyerang, waktu serangan, jenis serangan dan besar *packet* yang dikirim berhasil terdeteksi menggunakan *tools snort* dengan metode *Intrusion Detection System.*	Lakukan *bloking* pada ip penyerang, dan membatasi besar packet yang dapat diterima oleh jaringan komputer server dengan mengkonfigurasi *firewall* pada *address list*, sehingga *attacker* tidak dapat melakukan serangan kembali.

D. Simpulan

Berdasarkan hasil penelitian penerapan *tools snort* pada server dengan metode *Intrusion Detection System* dalam melakukan Audit keamanan jaringan komputer server, *tools snort* mampu mendeteksi adanya serangan pada jaringan komputer server dengan jenis serangan *ping of deadth* dan *flooding* dengan hasil deteksi berupa waktu terjadinya serangan, jenis serangan, besar packet yang diterima oleh server dan ip penyerang. Serangan yang dikirim mampu membanjiri server dengan packet yang besar sehingga membuat server menjadi *down*. Serangan DDoS sangat berpengaruh terhadap layanan dan kinerja komputer server SMKS YPPI Tualang, hal ini dibuktikan dari serangan yang dilakukan oleh *attecker* dapat membuat perangkat jaringan komputer server dan server menjadi down dan mengganggu aktifitas layanan dan kinerja komputer server. Dari hasil audit keamanan jaringan

yang dilakukan ditemukan celah keamanan pada jaringan sever SMKS YPPI Tualang terhadap serangan DDoS, oleh sebab itu perlu dilakukan peningkatan keamanan pada jaringan server SMKS YPPI Tualang, baik pada insfrastruktur jaringan, perangkat jaringan ataupun dari sisi server itu sendiri agar keamanan jaringan komputer server SMKS YPPI Tualang meningkat dan terhidar dari berbagai serangangan terutama serangan DDoS.

E. Referensi

[1] D. Sudirman and Akma Nurul Yaqin, "Network Penetration dan Security Audit Menggunakan Nmap," *SATIN - Sains dan Teknologi Informasi*, vol. 7, no. 1, pp. 32–44, Jun. 2021, doi: 10.33372/stn.v7i1.702.

[2] H. Yanto, "Intruder Detection Monitoring System in Computer Networks Using Snort Based Sms Alert (Sistem Monitoring Deteksi Penyusup Dalam Jaringan Komputer Menggunakan Snort Berbasis Sms Alert)," *Jurnal KomtekInfo*, vol. 7, no. 2, 2020, doi: 10.35134/komtekinfo.v7i2.

[3] L. Feronika Nainggolan, N. F. Saragih, F. G. N. Larosa, and H. Artikel, "Monitoring Keamanan Jaringan Pada Server Ubuntu Dari Serangan DDoS Menggunakan Snort IDS," 2022. [Online]. Available: http://ojs.fikom-methodist.net/index.php/METHOTIKA

[4] D. Santoso, A. Noertjahyana, and J. Andjarwirawan, "Implementasi dan Analisa Snort dan Suricata Sebagai IDS dan IPS Untuk Mencegah Serangan DOS dan DDOS," 2021.

[5] W. W. Purba and R. Efendi, "Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT," *AITI: Jurnal Teknologi Informasi*, vol. 17, no. Agustus, pp. 143–158, 2020.

[6] F. Nisa and S. Ramadona, "Jurnal Sistim Informasi dan Teknologi https://jsisfotek.org/index.php Sistem Pencegahan Serangan Distributed Denial Of Service Pada Jaringan SDN," vol. 5, no. 3, 2023, doi: 10.60083/jsisfotek.v5i3.269.

[7] R. Nurbahri and G. Widi Nurcahyo, "Jurnal Sistim Informasi dan Teknologi https://jsisfotek.org/index.php Analisis Penggunaan Metode Port Knocking pada Sistem Keamanan Jaringan Komputer (Studi Kasus di Universitas Baiturrahmah)," vol. 5, no. 1, 2023, doi: 10.37034/jsisfotek.v5i1.211.

[8] M. A. Algiffary, M. Izman Herdiansyah, and Y. N. Kunang, "Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Dengan Framework COBIT 2019 Pada RSUD Palembang BARI," *Journal Of Applied Computer Science And Technology (JACOST)*, vol. 4, no. 1, pp. 2723–1453, 2023, doi: 10.52158/jacost.505.

[9] M. Polatgil, "Investigation of The Effect of Data Normalization on Classification and Feature Selection in Intrusion Detection System," *Indonesian Journal of Computer Science*, vol. 11, pp. 13–22, 2022.

[10] M. Pitriyanti, N. Khairani Daulay, and M. Agus Syamsul Arifin, "KLIK: Kajian Ilmiah Informatika dan Komputer Prototype Sistem Deteksi Serangan Pada Server Samsat Menggunakan Intrusion Detection System (IDS) Berbasis Snort," *Media Online*, vol. 3, no. 4, pp. 323–329, 2023, [Online]. Available: https://djournals.com/klik

[11] R. Suwanto, R. Ikhwan, and M. Diponegoro, "Implementasi Intrusion Prevention System (Ips) Menggunakan Snort Dan Iptable Pada Monitoring Jaringan Lokal Berbasis Website," *Jurnal Komputer dan Aplikasi*, vol. 7, pp. 97–107, 2019.