Jurnal Pendidikan Teknologi Informasi (JUKANTI)
Volume (6) No (1) April 2023–eISSN : 2621-1467

IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) UNTUK MENDETEKSI SERANGAN METASPLOIT EXPLOIT MENGGUNAKAN SNORT DAN WIRESHARK

Julian Lirama Junior Pandari[a], Wiwin Sulistyo[b]

[a,b]Program Studi Teknik Informatika, Fakultas Teknologi Informasi,
Universitas Kristen Satya Wacana, Salatiga
[a]672018100@student.uksw.edu, [b]wiwin.sulistyo@uksw.edu

Abstrak

Keamanan jaringan pada saat ini memang sangat diperlukan. Seiring dengan perkembangannya serangan siber, banyak kejahatan siber yang bekerja melalui jaringan dan mengeksploitasi celah keamanan tanpa adanya akses terlebih dahulu seperti serangan Remote Exploit. Serangan Remote Exploit ini dilakukan dengan cara memanfaatkan celah pada port dan protokol yang terbuka sehingga dapat mengexploitasi sistem operasi komputer target secara jarak jauh dan dapat mencuri data-data pada komputer target. Untuk melakukan Remote Exploit membutuhkan tools Metasploit Framework dengan menggunakan exploit/multi/handler dan menggunakan payload linux/x64/meterpreter/reverse_tcp sehingga dapat mengakses sistem operasi komputer target. IDS (Intrusion Detection System) Snort adalah sebuah sistem yang digunakan untuk memantau trafik jaringan dan mendeteksi intrusi mencurigakan kemudian akan melaporkannya dalam bentuk peringatan atau alert. Dengan menggunakan Intrusion Detection System Snort bertujuan agar dapat melakukan scaning terhadap setiap serangan yang masuk ke dalam jaringan komputer dan sangat membantu dalam minimalisir kerusakan sistem yang dilakukan oleh penyerang. untuk menganalisis lalu lintas jaringan dari paket Remote Exploit digunakan Wireshark sebagai pendeteksi serangan, dan dilakukan pembuktian apakah paket tersebut merupakan virus atau bukan dengan menggunakan Virus Total.

Kata kunci : *Intrusion Detection System*, Snort, Wireshark, Metasploit *Exploit*

Abstract

Network security at this time is indeed indispensable. As cyberattacks evolve, many cyberattacks work through networks and exploit security loopholes without prior access such as Remote Exploit attacks. This Remote Exploit attack is carried out by taking advantage of loopholes in open ports so that it can exploit the targer computer operating system remotely and can steal data on the target computer. To do Remote Exploit requires Metasploit Framework tools using exploit/multi/handler and using linux/x64/meterpreter/reverse_tcp payload so that it can access the target computer's operating system. IDS (Intrusion Detection System) Snort is a system used to monitor network traffic and detect suspicious intrusions and then report it in the form of alerts. By using the Intrusion Detection System Snort aims to be able to scan every attack that enters the computer network and is very helpful in minimizing system damage done by attackers. to multiply network traffic from Remote Exploit packets, Wireshark is used as an attack detector, and proof is carried out whether the packet is a virus or not by using Virus Total.

Keywords : *Intrusion Detection System, Snort, Wireshark, Metasploit Exploit*

1. PENDAHULUAN

Pada masa kini, perkembangan teknologi semakin berkembang dan menjadi kebutuhan dalam kehidupan manusia untuk mengakses informasi apapun. Perkembangan teknologi juga dapat memudahkan pekerjaan manusia dalam kehidupan sehari-hari. Namun dibalik sisi positif tersebut terdapat masalah yang saat ini sering terjadi yaitu ancaman serangan siber yang bisa menembus sistem keamanan jaringan seperti serangan *Remote Exploit*. Serangan *Remote Exploit* adalah serangan yang dilakukan dengan cara memanfaatkan celah *Port* dan *Protokol* yang terbuka sehingga *attacker* dapat mengexploitasi sistem operasi komputer targer secara jarak jauh dan dapat mencuri data-data pada komputer target. *Remot Exploit* memanfaatkan tools *Metasploit Framework* untuk membuat *backdoor* dengan menggunakan *exploit/multi/handler* dan menggunakan *payload linux/x64/meterpreter/reverse_tcp* untuk mengontrol sistem operasi komputer target. Permasalahn ini sangat membutuhkan sistem yang mumpuni dalam mendeteksi serangan siber seperti *Remot Exploit*, harus diperlukan sistem pendeteksi dan peningkatan dalam keamanan jaringan. *IDS (Intrusion Detection System*) adalah sebuah sistem yang digunakan memantau trafik jaringan untuk mendeteksi intrusi mencurigakan dan akan melaporkannya dalam bentuk peringatan atau alert. *IDS* dapat melakukan monitoring terhadap seluruh aktifitas pada jaringan, *IDS* akan langsung melakukan mendeteksi dan memberikan peringatan terhadap gangguan-gangguan atau intrusion pada sistem jaringan.

Salah satu aplikasi *IDS* yang banyak dipakai yaitu *Snort. IDS* (*Intrusion Detection System) Snort* merupakan perangkat yang dapat digunakan untuk mengawasi aktifitas pada sebuah jaringan. dengan kelebihan *snort* yaitu bisa membuat rules sendiri maka dimanfaatkan untuk menerapkan *signature based* detection *IDS* yang dimana *Snort IDS* bertujuan untuk mendeteksi adanya serangan melalui *Port* kemudian menggunakan tambahan *wireshark* untuk melakukan analisis dan memonitoring pada jaringan komputer.

Berdasarkan latar belakang yang ada maka dilakukan penelitian yang bertujuan menerapkan sistem keamanan jaringan berbasis *IDS* (*Intrusion Detection System)* menggunakan *Snort* dan *Wireshark,* yang digunakan untuk membantu administrator jaringan dalam mengamankan sistem jaringan yang ada dari ancaman pencurian dan perusakan data.

Penulisan jurnal tugas akhir ini tentu menggunakan beberapa sumber jurnal di internet. Penulis menemukan beberapa jurnal dengan *benefit* masing-masing dalam membantu penulisan Tugas Akhir ini. Tulisan yang *pertama*, pada penelitian yang berjudul "Analisis Celah Keamanan Jaringan Dan Server Menggunakan Snort Intrusion Detection System" membahas bagaimana penggunaan Snort IDS dalam mendeteksi celah keamanan *website* dari serangan serangan *hacker* yang menggunakan *Backdoor* **.***Kedua,* Menurut penelitian yang berjudul "Analisis Keamanan Jaringan pada Fasilitas Internet (*wifi*) Terhadap Serangan Packet Sniffing" pada penelitian ini membahas tentang pengujian jaringan wifi menggunakan serangan Packet Sniffing yang bisa menangkap atau

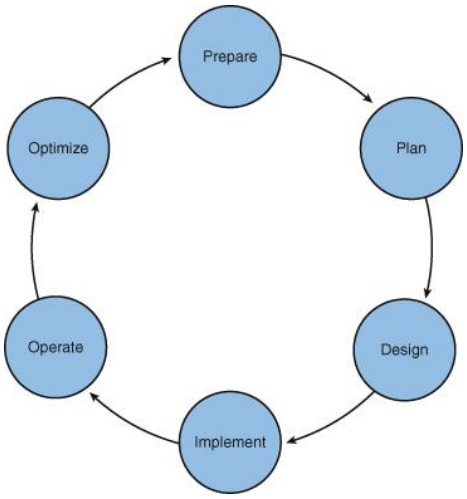
melihat *username* dan *password* dengan penggunaan *tools* Ettercap.

Tulisan yang *ketiga*, penelitian yang berjudul "Deteksi Malware Dridex Menggunakan Signature-based Snort". Penelitian ini menganalisis tentang serangan Malware Dridex pada lalu lintas jaringan dan mengembangkan rules snort untuk mendeteksi keberadaan signiture Dridex. *Keempat,* pada penelitian yang berjudul "Monitoring Jaringan Wireless Terhadap Serangan Packet sniffing Dengan Menggunakan IDS". Penelitian ini membahas tentang proses *sniffing* menggunakan Ettercap dengan indikasi *arp spoof* menggunakan *tools* Ettercap dan melakukan pendeteksian serangan tersebut menggunakan Snort IDS. *Kelima*, pada penelitian yang berjudul "Penerapan Keamanan Jaringan Menggunakan Sistem Snort dan Honeypot Sebagai Pendeteksi dan Pencegah Malware" membahas tentang bagaimana mendeteksi dan mencegah adanya Malware pada jaringan Universitas Udayana menggunakan Snort dan Honeypot. *Keenam*, pada penelitian yang berjudul "Implementasi Intrusion Dection System (IDS) Menggunakan Snort Untuk Mendeteksi Serangan Pada Server" membahas tentang pendeteksian serangan Ddos dengan *Tools* Loic dan Dns Spoof dengan *tools* Ettercap menggunakan Snort IDS yang akan memberikan laporan secara real time.

Adapun sumber-sumebr lai yang menjadi acuan penulis dalam menyelesaikan tugas akhir ini. *Pertama*, pada penelitian "Keamanan FTP Server Berbasiskan IDS dan IPS menggunakan Sistem Operasi Linux Ubuntu" mambahas bagaimana membangun sebuah sistem keamanan pada komputer FTP server dengan menerapkan IDS dan juga IPS sebagai sistem keamana pada komputer server. *Kedua,* pada penelitian "Analisis Keamana Jaringan Pada Web Dari Serangan Sniffing Dengan Metode Eksperimen" penelitian ini membahas tentang pengujian pada salah satu web yang ada di Universitas Kristen Satya Wacana menggunakan *tools* Bettercap, yang dimana sudah memiliki keamanan HTTPS namun tetap bisa terkena serangan *sniffing* sehingga *username* dan *password* dari *user* yang menggunakan website tersebut berhasil terlihat. *Ketiga,* pada penelitian "Pedeteksian Dan Pencegahan Serangan Pada Jaringan Menggunakan Snort Pada Linux Ubuntu" membahas bagaimana penggunaan Snort pada Ubuntu untuk membantu dalalm memproteksi adanya gangguan serangan terhadap jaringan. *Yang terakhir,* dalam penelitian "Deteksi Penyusup Pada Server Menggunakan Metode Intrusion Detection System (IDS) Berbasis Snort" membahas tentang bagaimana mengamankan jaringan pada server warnet dari serangan seperti *ping of death* dan beberapa serangan lain, untuk mengatasi permalahan yang ada maka akan dilakukan penerapan menggunakan Snort IDS, Snort IDS dapat mengetahui apa yang terjadi pada jaringan sesuai dengan yang dihasilkan pada *alert*. Sehingga dalam penulisan tugas akhir ini, total 10 jurnal yang menjadi bahan acuan penulis dalam meninjau tugas akhir ini,

2. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah model *PPDIOO (Prepare, Plan, Design, Implement, Operate, and Optimize).*



Gambar 1. Metode PPDIOO*(Sumber: http://cisco.com).*

Tahapan penelitian pada metode *PPDIOO* dapat dijelaskan sebagai berikut (Cisco: 2011,p13) :

1. *Prepare*
   Pada tahap awal ini proses yang dilakukan adalah mempersiapkan segala sesuatu agar penelitian dapat berjalan dengan baik. Dimulai dengan mengumpulkan data dan informasi untuk bisa membangun sistem keamanan, agar dapat melakukan konfigurasi sehingga bisa dioprasikan dan dapat mengidentifikasi masalah yang ada.
2. *Plan*
   Dalam tahap ini, yang dilakukan adalah perancangan dan menentukan *hardware* dan *software* yang akan digunakan dalam penelitian ini.
3. *Design*
   Dalam tahap desain ini dilakukan sebuah desain topologi jaringan yang sesuai dengan perancangan penelitian.
4. *Implement*
   Dalam tahap ini, dilakukan implementasi sesuai dengan perencanaan yang sudah dibuat.
5. *Operate*
   Merupakan tahap untuk melakukan pengujian pada sistem yang sudah dibuat.
6. Optimize
   Tahap optimisasi ini dilakukan dengan manganalisis dan evaluasi yang bertujuan untuk meningkatkan kinerja sistem agar labih baik.

Pada tahapan *Prepare* akan dilakukan secara bersamaan dengan tahap *plan*, dikarenakan antara perancangan dan persiapan saling berhubungan satu dengan yang lain. Sehinggah pada tahap selanjutnya akan menjadi lebih terarah.

Tabel 1 dan 2 persiapan kebutuhan perangkat pendukung *software* dan *hardware* yang yang digunakan untuk melakukan simulasi serangan *Remot Exploit* seperti sebagai berikut :

Tabel 1. Table Perangkat Lunak

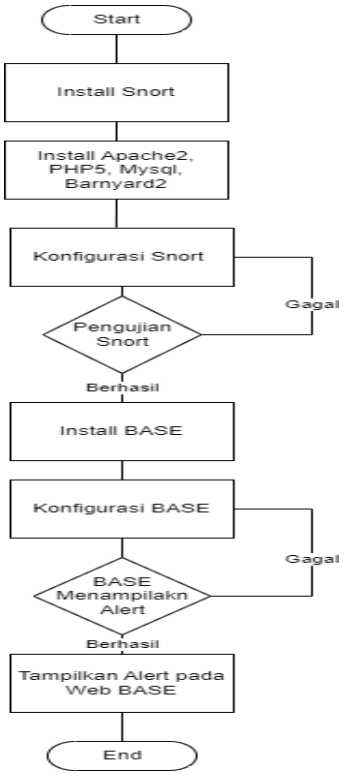
NO	Komponen	versi	Keterangan
1	Ubuntu Dekstop	20.04	Sebagai server OS
2	Snort	2.9.20	Digunakan Untuk mengkap serangan yang masuk ke server
3	Base	1.4.5	Menyimpan alert ke dalam Web Base

4	Wireshark	3.2.3	Menganalisi jaringan komputer
5	Kali Linux	6.0	Sebagai Attacker
6	Metasploit		Aplikasi yang digunakan untuk melakukan serangan remot exploit ke komputer target
7	Virtual Box	7.0	Aplikasi virtual mesin untuk menjalankan OS

Table 2. Tabel Perangkat Keras

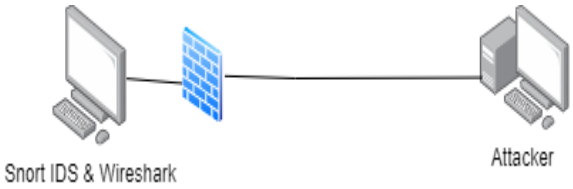
No	Perangkat	IP address
1	Server	192.168.1.29/24
2	Penyerang	192.168.1.11/24

Setelah selesai melakukan persiapan *hardware* dan *software*, maka dilanjutkan dengan *design.* Dalam tahap desain ini dilakukan sebuah desain topologi jaringan yang sesuai dengan perancangan penelitian.



Gambar 2. Diagram Alir Installasi dan Konfigurasi Snort IDS.

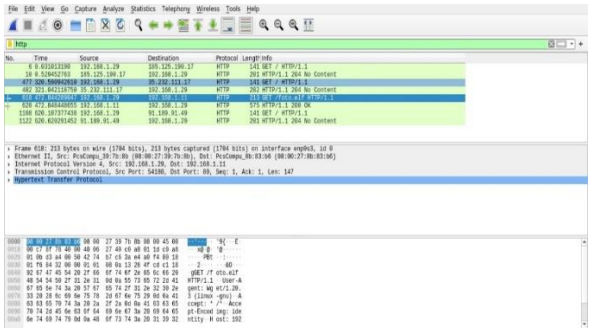
Gambar 2 menunjukan Alir installasi dan konfigurasi Snort IDS. Dimulai dengan melakukan penginstallan Snort sekaligus akan di konfigurasi dan menambahkan Rules-rules *Snort*, kemudian melakukan penginstallan paket Apache2, Mysql server, Barnyard2. selanjutnya melakukan konfigurasi Snort dengan paket-paket yang sudah di instal dan akan melakukan pengujian jika konfigurasi gagal maka akan di ulang dan jika berhasil *Snort* akan dilanjutkan dengan installasi dan konfigurasi *Web BASE*. Jika konfigurasi berhasil maka alert akan ditampilan pada *Web BASE* jika gagal ulangi dari konfigurasi *BASE*.



Gambar 3. Topologi Penelitian.

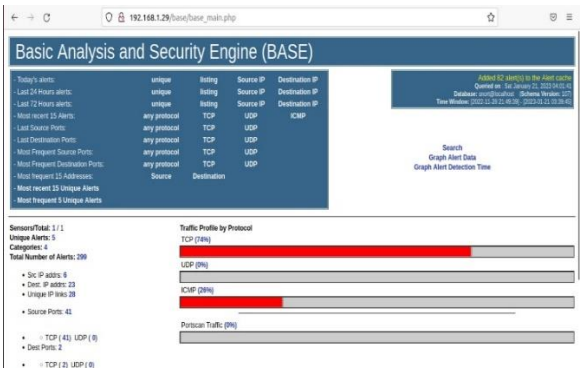
Pada gambar 3 *Design* merupakan tahapan perancangan topologi jaringan yang digunakan. Pada gambar 3 dijelaskan setelah melakukan konfigurasi pada *Snort IDS* peneliti akan melakukan serangan *Remote Exploit* menggunakan *tools Metasploit* untuk mengakses komputer target. Komputer target menjalankan *Snort IDS* sebagai alat untuk mendeteksi serangan dan menggunakan *Wireshark* untuk menganalisi serangan tersebut.

Fase *Implement* "Implementasi *Intrusion Detection System (IDS)* untuk Mendeteksi serangan Metasploit Exploit Menggunakan *Snort IDS* dan *Wireshark"* dibagi menjadi dua bagian yaitu implementasi installasi sistem keamanan *Snort IDS* dan analisi setip paket yang melewati jaringan server.



Gambar 4. pendeteksian remot exploit.

Gambar 4 merupakan tampilan aplikasi *Wireshark* yang digunakan untuk melakukan penganalisis paket data pada jaringan server.

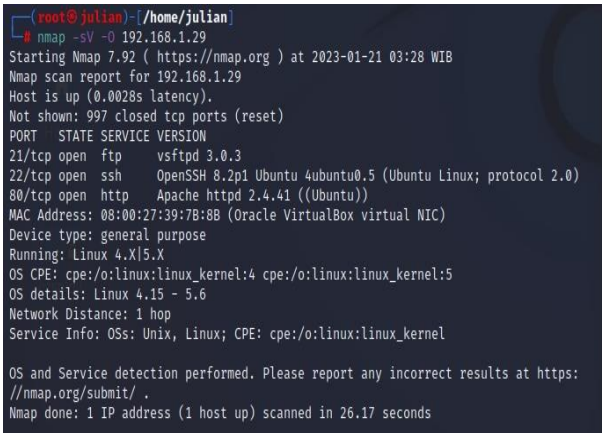


Gambar 5. Tampilan *Base* pada *Snort IDS.*

Tampilan gambar 5 merupakan hasil dari installasi *Snort BASE* yang bisa dilihat dari baris *Traffic Profile by Protocol* menunjukan statistik serangan apa saja yang masuk ke *Server.*

3. HASIL DAN PEMBAHASAN

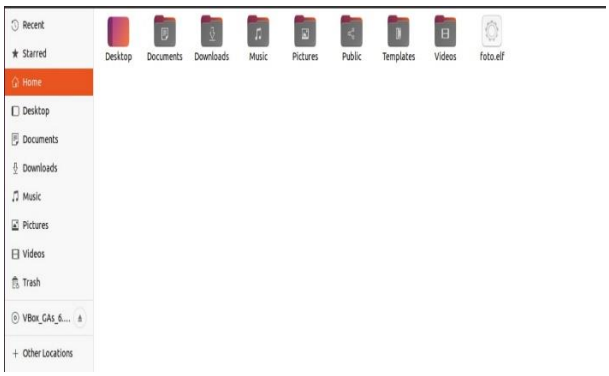
Skenario fase *Operate*, pengujian ini dilakukan dengan menggunakan 1 PC dan 1 laptop sebagai *attacker* dan sebagai *server*. Pengujian ini dilakukan bertujuan untuk membuktikan bahwa administrator *server* dapat menerima pesan notifikasi dari serangan yang dilakukan oleh *attacker.*



Gambar 6. Nmap Scan.

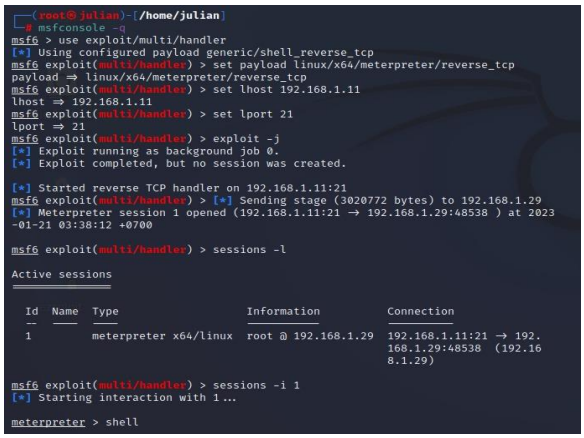
Pada gambar 6 melakukan percobaan Scasnning menggunakan alat bantu *Nmap*, penyerang menggunakan IP

target atau server untuk melakukan mendeteksi host dan port-port yang terbuka pada server.



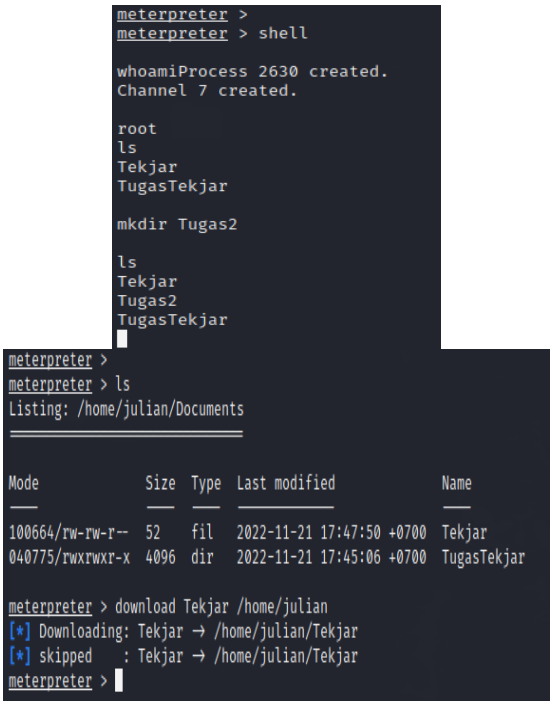
Gambar 7. Target Menjalankan File Elf.

Pada gambar 7 target menjalankan file *Remote Exploit* yang sudah diintall, dimana file tersebut akan membuat attacker langsung tersambung dengan komputer target dan attacker bisa mengontrol komputer target dari jarak jauh. Seperti pada gambar 8 secara otomatis program yang sudah dijalankan akan langsung terkoneksi dengan komputer target.



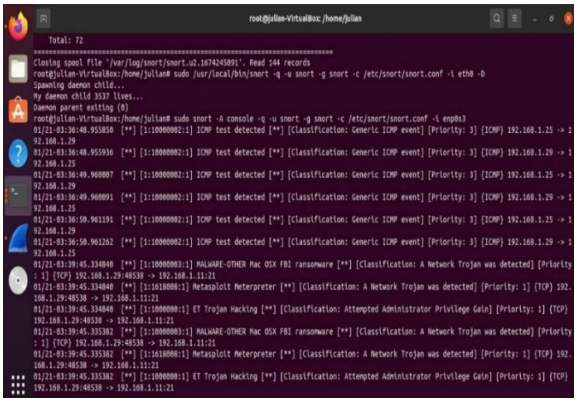
Gambar 8. Proses menjalankan *Payload.*

Hasil dari gambar 8 serangan *Remot Exploit* dengan menggunakan perintah "*use /exploit/multi/handler"* dan melakukan control terhadap komputer target yang sudah menjalankan file yang dikirim *attacker* sebelumnya.



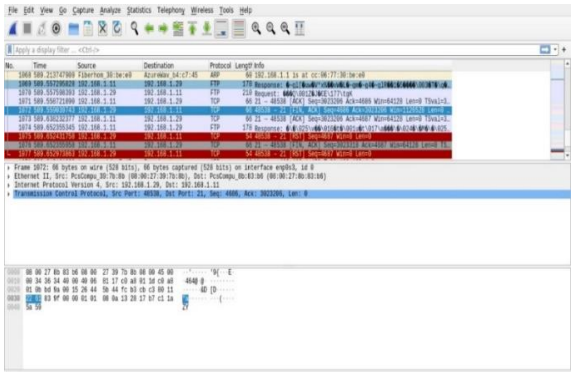
Gambar 9. Attacker melakukan *Remote Exploit* dengan cara membuat file dan mencuri file.

Ketika attacker sudah berhasil masuk maka attacker dengan bebas mengexploitasi komputer target. Seperti pada gambar 9 attacker dengan gampang masuk sebagai root dan bisa membuat file sesuai dengan keinginan attacker dan bahkan bisa juga mencuri file-file penting yang disimpan pada komputer.



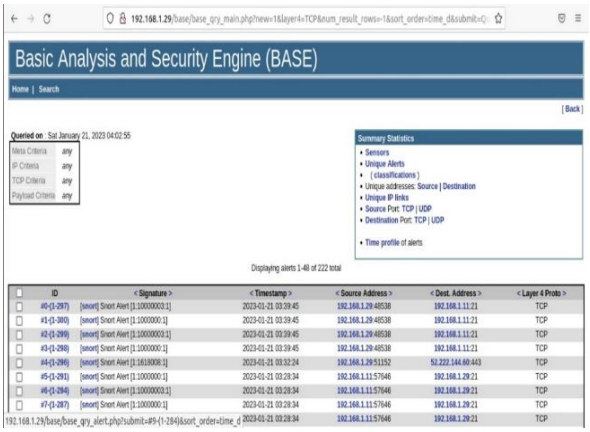
Gambar 10. Tampilan Alert yang Berhasil Mengkap Serangan.

Pada gambar 10 merupakan hasil dari tampilan alert yang sudah di setting pada *Snort* sebelumnya. Yang dimana menunjukan adanya deteksi serangan pada jaringan server dengan peringatan Metasploit Meterpreter dan pesan pada alert tersebut yaitu *Network Trojan* yang bererati ada sebuah jaringan *Virus Trojan* yang masuk ke jaringan server.



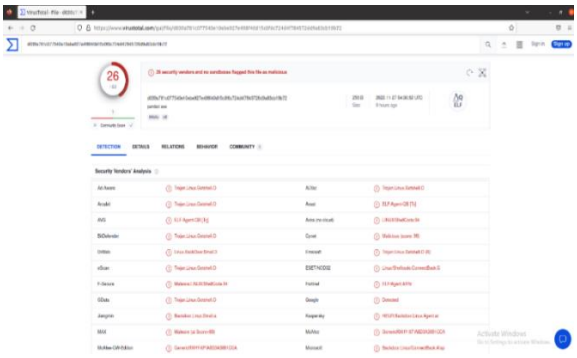
Gambar 11. Aktivitas Tidak Normal pada Jaringan Server.

Proses analisi jaringan pada server dengan menggunakan *tools Wireshark* yang bertujuan untuk menangkap data atau informasi mengenai log activiti dan IP address penyerang. Berdasarkan pada gambar 11 menunjukan ada yang telah mengirimkan file Malware dengan melalui protokol HTTP.



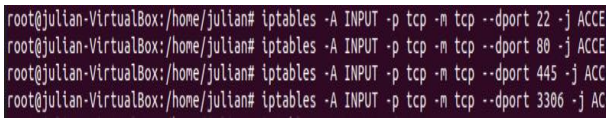
Gambar 12. Tampilan Alert pada Web Base.

Gambar 12 merupakan hasil dari *Snort Base* yang menangkap adanya aktifitas yang melewati *protokol* dan *port* dan bisa dilihat alert yang menunjukan adanya serangan melewati *port* 21 dan 443, alert tersebut akan tersimpan pada *Web Base Snort* dan bisa digunakan untuk melakukan pencegahan pada sistem jaringan.



Gambar 13. Pembuktian Hasil Menggunakan Virus Total.

Pada gambar 13 yaitu tahap akhir, peneliti menganalisis file yang di temukan wireshark menggunakan *Virus Total*. Pada *Virus Total* menunjukan hasil dari 63 security vendors mendeteksi 26 *malicious file* yang menyatakan bahwa file tersbut adalah *Virus* atau *Malware*.



Gambar 14 *Filtering Firewall*.

Gambar 14 merupakan *filtering firewall* yang memperbolehkan untuk di akses yaitu *port* 22, 80, 445, 3306, selain dari port tersebut, lalu lintas yang melewati port lain maka akan di drop.

Fase *Optimalisasi*, untuk mengoptimalkan sistem keamanan jaringan yang telah dibuat maka dilakukan update pada *Snort* jika ada pembaharuan, melakukan upgrade pada rules *Snort* agar dapat mendeteksi lebih banyak lagi serangan *Remote Exploit* yang semakin berkembang. Meningkatkan sistem keamanan agar dapat melakukan otomatis drop pada *port* yang tidak diberi akses pada Firewell yang sudah terpasang. Dan melakukan update pada Sistem Operasi yang digunakan ketiga ada pembaharuan.

Tabel 3. Kelebihan dan Kekurangan

Kelebihan	Kekurangan
Rules Snort yang sudah ditambahkan berkerja dengan baik dan dapat mendeteksi serangan Remote Exploit dengan tepat.	Perlu adanya update rules snort agar dapat mendeteksi serangan Remote Exploit yang semakin bervariasi dari waktu ke waktu.
Web Base yang sudah dikonfigurasi dapat mendeteksi dan menyimpan semua alert yang masuk pada Snort.	Web Base yang dikonfigurasi tidak memunculkan pesan alert yang sama dengan snort.
Melakukan filtering farewall dan memberikan akses pada port yang diinginkan.	

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, "Implementasi *Intrusion Detection System (IDS)* untuk Mendeteksi serangan *Metasploit Exploit* Menggunakan Snort dan Wireshark". Dapat disimpulkan bahwa *IDS Snort* dan *Wireshark* yang di terpkan dapat berjalan dengan baik dengan berhasil menangkap dan mendeteksi serangan *Remote Exploit* sehinggah dapat memberikan *alert* pada server. Dan server bisa melakukan pencegahan dengan cara memblocking alamt IP atau *Port* yang sudah terdeteksi.

DAFTAR PUSTAKA

[1] A,. Hafiz, T. Kurniaawan, N. A. Sivi, F. K. Ikhsan, P. A. Pratomo, 2020, "Analisis Celah Keamanan Jaringan Dan Server Menggunakan Snort Intrusion Detection System," Jurnal Informasi dan Komputer., Vol. 8, No. 2,

[2] Nugroho, Bayu Arie, 2012, "Analisis Keamanan Jaringan pada Fasilitas Internet (wifi) Terhadap Serangan Packet Sniffing," Skripsi.

Surakarta : Universitas Muhammadiyah Surakarta.

[3] Nugraha, Adhitya, 2021, "Deteksi Malware Dridex Menggunakan Signature-based snort", Indonesia Journal Of Computer Science. Vol. 10, No. 1,.

[4] Fauzi, Achmad Rizal dan Suartana, I Made,2017, "Monitoring jaringan Wireless Terhadap Serangan Packet Sniffing Dengan menggunakan Ids," Jurnal Management Informatika., Vol 8 2:11-17,.

[5] R. G. Agus, P. S. Nyoman, M. W. Dewa, 2021 "Penerapan Keamanan Jaringan Menggunakan Sistem Snort dan Honeypot Sebagai Pendeteksi dan Pencegah Malware" Majalah Ilmiah Teknologi Elektro., Vol. 20, No. 1,.

[6] A. Farhan, L. A. S. I. Akbar, dan A. A. Rachman, 2019, "Implementasi Intrusion Dection System (IDS) Menggunakan Snort Untuk Mendeteksi Serangan Pada Server,"

[7] K. Shah, D. P. Yuni, A. Enggar, 2021, "Keamanan FTP Server Berbasis IDS dan IPS Menggunakan Sistem Operasi Linux Ubuntu"., Vol. 6, No. 1,.

[8] Y. Hae, W. Sulistyo, 2021, "Analisis Keamanan Jaringan Pada Web Dari Serangan Sniffing Dengan Metode Eksperimen," Jurnal Teknik Informatika dan Sistem Informasi., Vol. 8, No. 4, Hal. 2095-2105.

[9] R. Razak, 2018, "Pendeteksian Dan Pencegahan Serangan Pada Jaringan menggunaakn Snort Pada Linux Ubuntu," Skripsi. Batusangkar : Institut Agama Islam Negeri Batusangkar.

[10] Syaifuddin, D. R. Akbi, A. G. Tammami, 2021, "Analisis Address Resolution Protocol Poisoning Attack Pada Router Wlan Menggunakan Metode Live Forensics," Jurnal Komputer Terapan., Vol. 7, No. 1, pp. 62 – 73,.

[11] B. Wijaya, A. Pratama, 2020, "Deteksi Penyusup Pada Server Menggunakan Metode Intrusion Detection System (IDS) Berbasis Snort," Jurnal SISFOKOM (Sistem Informasi dan Komputer)., Vol. 09, No. 01, pp. 97 – 101,.

[12] W. W. Purba, R. Efendi, 2021, "Perancangan dan Analisis Sistem Keamanan Jaringan Komputer Menggunakan Snort," AITI (Jurnal Teknologi Informasi)., Vol. 17, No. 2, pp. 143 – 158,.