JEPIN
(Jurnal Edukasi dan Penelitian Informatika)
ISSN(e): 2548-9364 / ISSN(p) : 2460-0741

Vol. 8
No. 2
Agustus
2022

Analisis *Rules Intrusion Detection Prevention System* (IDPS) Suricata untuk Mendeteksi dan Menangkal Aktivitas *Crypto Mining* pada Jaringan

Fadhil Raditya[#1], Jeckson Sidabutar[#2]

[#]*Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara*
Bogor, Indonesia

[1]fadhil.raditya@student.poltekssn.ac.id

[2]jeckson.sidabutar@poltekssn.ac.id

Abstrak— **Perkembangan teknologi informasi sangat pesat khususnya perkembangan pada sektor finansial dalam hal ini adalah mata uang kripto. Salah satu cara untuk mendapatkan aset mata uang kripto adalah dengan melakukan penambangan mata uang kripto. Hal tersebut dapat memicu penyerang untuk membuat suatu aplikasi berbahaya yang disisipkan pada server perusahaan atau instansi, dan membuat aplikasi tersebut melakukan aktivitas penambangan mata uang kripto. Oleh karena itu sistem keamanan jaringan pada suatu instansi atau perusahaan harus menerapkan pengamanan tambahan dalam hal ini adalah *Intrusion Detection Prevention System* (IDPS) yang digunakan sebagai sistem pendeteksi serta penangkalan aktivitas berbahaya pada jaringan, salah satunya adalah penambangan mata uang kripto. Adapun aplikasi IDPS yang dapat diimplementasikan pada jaringan instansi atau perusahaan adalah Suricata. Penelitian ini melakukan analisis rules IDPS Suricata dalam mendeteksi dan menangkal aktivitas penambangan mata uang kripto pada jaringan. Terdapat 2 jenis simulasi yang dilakukan yaitu dengan membandingkan default rules dengan custom rules yang dibuat untuk mendeteksi dan menangkal aktivitas penambangan 10 jenis mata uang kripto diantaranya Ethereum (ETH), Conflux (CFX), Bitcoin Gold (BTG), Ethereum Classic (ETC), Monero (XMR), TON, AION, Zcash (ZEC), FLUX dan Raven (RVN). Analisis yang dilakukan meliputi perhitungan nilai *accuracy*, *precision*, *recall*, dan *f-measure*. Hasil yang didapat menunjukkan bahwa custom rules yang dibuat dan diimplementasikan untuk mendeteksi dan menangkal aktivitas penambangan mata uang kripto memiliki peningkatan nilai *accuracy* sebesar 0,2%, nilai *recall* sebesar 48,94%, dan nilai *f-measure* sebesar 32,39% dari default rules Suricata.**

Kata kunci— **IDPS, Suricata, *Crypto Mining*, *Rules*, Analisis Efektivitas**

I. PENDAHULUAN

Beberapa tahun terakhir perkembangan teknologi informasi khususnya dibidang mata uang kripto berkembang sangat pesat, mata uang kripto merupakan salah satu terobosan baru yang digunakan sebagai investasi di dunia [1]. Di Indonesia, nilai transaksi mata uang kripto mencapai Rp 478,5 trilliun dan pengguna yang sudah mencapai 7,4 juta orang per Juli 2021 [2]. Hal tersebut memikat para investor maupun pengguna untuk mendapatkan aset mata uang kripto dengan berbagai cara, salah satunya adalah dengan melakukan *mining* mata uang kripto [3].

Cara kerja dari *mining* adalah menyamakan nilai *hash* yang ada pada *pool mining* dan dijadikan *proof-of-work* agar mendapat aset mata uang kripto tersebut [4]. Aplikasi yang digunakan untuk melakukan *Crypto Mining* diantaranya XMRig, Bminer, GMiner, serta lolMiner. Keempat aplikasi tersebut memiliki performa yang cukup baik serta efisien dalam melakukan *Crypto Mining* [5]. *Crypto Mining* bekerja menggunakan *Central Processing Unit* (CPU) dan GPU (Graphic *Processing Unit*) untuk melakukan *mining* dalam mendapatkan *block hash* [6]. Adanya sistem *mining* pada mata uang kripto membuat banyak ancaman di bidang keamanan siber, salah satu contohnya adalah serangan *malware Crypto Miner*. Serangan ini bekerja dengan cara melakukan *mining* pada perangkat yang telah terinfeksi, kemudian akan mengirimkan hasilnya kepada wallet mata uang kripto penyerang [7]. Selain itu terdapat beberapa pihak yang menggunakan jaringan publik untuk melakukan *mining crypto*currency, sehingga dapat menimbulkan kerusakan pada sumber daya pada jaringan. Pada tahun 2018 terdapat kerugian mencapai 53 juta dolar amerika yang dihasilkan oleh serangan WannaMine, yaitu serangan yang menggunakan teknik eksploit EternalBlue seperti WannaCry kepada server ataupun pusat data di seluruh dunia [8]. Proses *Crypto Mining* akan membuat temperatur pada GPU atau perangkat yang digunakan mengalami kenaikan yang signifikan dikisaran 80 hingga 90 derajat celcius [9]. Nilai temperatur yang tinggi dari GPU dan CPU merupakan salah satu faktor penyebab kerusakan dan memperpendek umur perangkat tersebut [10]. Penggunaan CPU dalam *Crypto Mining* juga mempengaruhi kinerja dari

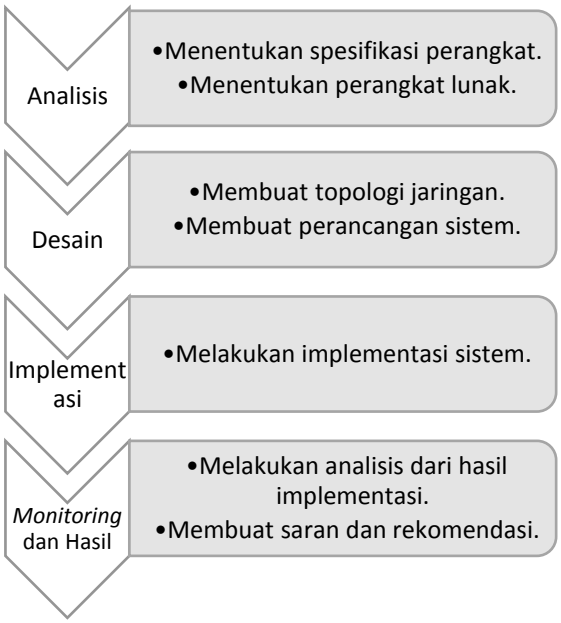
server yang ditumpangi, sehingga dapat berdampak terhadap layanan yang berada pada server tersebut [9].

Berkaitan dengan hal tersebut, diperlukan adanya sistem pendeteksi serta penangkalan *Crypto Mining* yang berjalan pada jaringan internet. Suricata adalah salah satu aplikasi *open-source* yang mengkombinasikan *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS), serta *Network Security Monitoring* (NSM) sehingga Suricata dapat digunakan untuk mendeteksi serta menangkal aktivitas *Crypto Mining* [11]. Pada penelitian yang dilakukan oleh A. D. Ralianto dan S. Cahyono [12], didapati bahwa tingkat akurasi Suricata dalam mendeteksi serangan 30% lebih tinggi dibandingkan dengan Snort. Aturan/*rules* untuk IDPS Snort dalam mendeteksi serta menangkal aktivitas penambangan mata uang kripto Monero juga dikembangkan pada penelitian [7]. Penelitian [13] membuat sebuah sistem deteksi serta mendeteksi 5 mata uang kripto yang ditambang yaitu Bitcoin, Bitcoin-Cash, DogeCoin, LiteCoin, dan Monero. Selanjutnya pada penelitian [14] dihasilkan perbandingan antara tingkat pendeteksian VirusTotal dengan sistem *Mining Detection* and *Prevention System* (MDPS) yang dibuat terhadap *malware* penambang (*Crypto Miner Malware*) yang diuji dari sistem browser. Dari ketiga penelitian terkait tersebut akan dilakukan pengembangan berupa pembuatan *rules* IDPS Suricata untuk mendeteksi dan menangkal aktivitas *crypto mining*. Adapun *rules* yang dibuat pada penelitian ini digunakan untuk mendeteksi 10 mata uang kripto yang ditambang yaitu Ethereum (ETH), Conflux (CFX), Bitcoin Gold (BTG), Ethereum Classic (ETC), Monero (XMR), TON, AION, Zcash (ZEC), FLUX dan Raven (RVN).

Penelitian ini akan melakukan pembuatan *custom rules* serta analisis tingkat efektivitas *custom rules* IDPS Suricata dalam mendeteksi serta menangkal aktivitas *crypto mining* pada jaringan. Tingkat efektivitas yang diuji adalah nilai *accuracy*, *precision*, *recall*, *dan f-measure* dimana nilai tersebut merupakan suatu tolak ukur untuk bisa menganalisis *rules* suricata yang dibuat untuk mendeteksi dan menangkal aktivitas *crypto mining* pada jaringan [13]. Kemudian hasil analisis tersebut akan dijadikan sebagai saran dan masukan untuk pengembangan *rules* IDPS Suricata selanjutnya.

II. METODE PENELITIAN

Metode yang digunakan dalam melakukan implementasi IDPS adalah metodologi *Network Development Life Cycle* (NDLC). NDLC dipilih karena dapat digunakan dalam melakukan implementasi topologi jaringan dalam hal ini adalah implementasi IDPS pada jaringan. Pada NDLC terdapat beberapa proses yang dilakukan yaitu *analysis*, *design*, *simulation prototyping*, *implementation*, *monitoring*, dan *management* yang dilakukan secara bertahap [15].



Gambar 1. Metodologi penelitian

A. Analisis

Tahap Analisis dilakukan untuk menentukan spesifikasi perangkat yang akan digunakan dalam penelitian. Selain itu juga, mempersiapkan tools yang akan digunakan dalam penelitian. Analisis kebutuhan sangat penting dilakukan agar sistem yang dibangun dapat berjalan sesuai dengan yang diharapkan. Analisis kebutuhan sistem pada penelitian ini berdasarkan literatur yang berkaitan mengenai Suricata, IDPS, *Cryptocurrency Mining*, Perangkat *Crypto Mining*, dan Aplikasi *Crypto Mining*.

B. Desain

Tahap ini dilakukan perancangan sistem yang akan dibangun agar sesuai dengan kebutuhan dan tujuan yang diinginkan. Perancangan penelitian ini disajikan dalam bentuk gambar yang berisi proses alur pengujian yang akan dilakukan dan arsitektur rancangan penelitian. Rancangan penelitian yang dibuat bertujuan untuk menggambarkan proses simulasi yang akan dilakukan pada penelitian ini. Simulasi akan dilakukan dengan cara menjalankan proses penambangan mata uang kripto pada jaringan. Simulasi tersebut dilakukan sebanyak 48 kali (berdasarkan *mining pool*) dengan jenis mata uang kripto yang berbeda-beda.

C. Implementasi

Implementasi sistem bertujuan untuk membuat lingkungan (environtment) yang akan digunakan untuk melakukan simulasi pengujian sistem. Pembuatan lingkungan simulasi menggunakan perangkat yang dibutuhkan sesuai analisis kebutuhan sebelumnya, dengan menggunakan sistem operasi Ubuntu 20.04 LTS yang akan dilakukan instalasi tools IDPS Suricata, serta perangkat penambangan yang akan diinstalasi tools XMRig, Bminer, GMiner, dan lolMiner.

D. Monitoring dan Hasil

Pada tahap ini, peneliti melakukan perhitungan tingkat efektivitas IDPS Suricata dalam menangkal dan mendeteksi aktivitas penambangan mata uang kripto. Nilai efektivitas yang digunakan yaitu *accuracy*, *precision*, *recall*, dan *f-measure*. Penilaian dilakukan dengan cara menghitung jumlah *True Positive* (TP), *False Positive* (FP), *True Negative* (TN), dan *False Negative* (FN). Dengan rumus perhitungan yang berbeda-beda setiap nilai yang disajikan dalam bentuk tabel dan grafik untuk mempermudah analisis. Kemudian dilakukan analisis terhadap hasil perhitungan yang didapatkan untuk dijadikan sebagai saran dan masukan untuk pengembangan rules IDPS Suricata selanjutnya.

III. HASIL PENELITIAN DAN PEMBAHASAN

A. Analisis Kebutuhan Sistem

Dalam membuat suatu rancangan dan melakukan implementasi sebuah sistem, diperlukan analisis terhadap skema dan perangkat apa saja yang dibutuhkan dalam melakukan penelitian. Pada tahap ini spesifikasi perangkat keras dan perangkat lunak yang akan digunakan diidentifikasi.

1) Kebutuhan dan Spesifikasi Perangkat Keras: Spesifikasi minimum yang dibutuhkan untuk melakukan implementasi IDPS Suricata adalah sebuah computer dengan RAM minimal 4 GB, dan prosesor *dual-core* [16]. Pada penelitian ini akan diimplementasikan IDPS Suricata pada sebuah server computer dengan spesifikasi yang dilihat pada Tabel 2. Sementara spesifikasi minimum yang dibutuhkan untuk melakukan *Crypto Miining* adalah memiliki CPU intel Core i3, RAM sebesar 4 GB, dengan sistem operasi Winodws 10, dan GPU Nvidia GTX 460 [17]. Pada penelitian ini akan menggunakan spesifikas perangkat *Crypto Mining* diatas spesifikasi minimum agar simulasi *Crypto Mining* dapat berjalan sebagaimana mestinya, untuk spesifikasi perangkat *Crypto Mining* dapat dilihat pada Tabel 2. Dalam tabel tersebut terdapat spesifikasi perangkat keras yang akan digunakan, meliputi sistem operasi, prosesor, RAM, dan lain sebagainya.

TABEL I
SPESIFIKASI SERVER IDPS

Spesifikasi	Keterangan
Sistem Operasi	Ubuntu 20.04 LTS
Prosesor	Intel Xeon E3-1240 v6 3.7Ghz
Kartu Grafis	Nvidia Quadro P600 2 GB
RAM	32 GB
Kapasitas Penyimpanan	2 TB
Peran	Server IDPS

TABEL III
SPESIFIKASI PERANGKAT *CRYPTO MINER*

Spesifikasi	Keterangan
Sistem Operasi	Windows 10
Prosesor	AMD Ryzen 7 2700 3.2GHz
Kartu Grafis	Nvidia GeForce GTX 1650 4 GB
RAM	16 GB
Kapasitas Penyimpanan	1 TB
Peran	*Crypto Miner*

2) Kebutuhan Perangkat Lunak: Berikut merupakan perangkat lunak yang dibutuhkan untuk menjalankan sistem dan akan diimplementasikan sesuai dengan perancangan yang dibuat. Dimana perangkat lunak IDPS yang digunakan pada penelitian ini adalah Suricata, karena memiliki nilai akurasi yang lebih tinggi jika dibandingkan dengan perangkat lunak IDPS lainnya [12]. Sementara itu perangkat lunak untuk *Crypto Mining* yang dapat digunakan untuk menambang 10 jenis mata uang kripto pada penelitian ini adalah XMRig, Bminer, GMiner, dan lolMiner. Adapun spesifikasi perangkat lunak yang digunakan untuk IDPS dapat dilihat pada Tabel 3 dan spesifikasi perangkat lunak yang digunakan untuk *Crypto Mining* dapat dilihat pada Tabel 4.

TABEL IIIII
SPESIFIKASI PERANGKAT LUNAK PADA SERVER IDPS

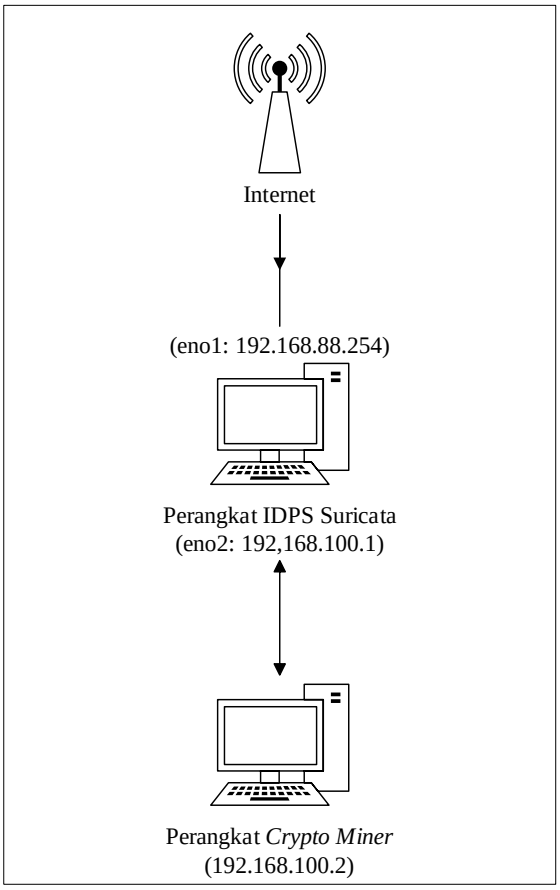
Perangkat Lunak	Deskripsi	Versi
Suricata	Perangkat lunak yang digunakan sebagai *Intrusion Detection Prevention System* (IDPS) dalam melakukan implementasi sistem.	6.0.4

TABEL IVV
SPESIFIKASI PERANGKAT LUNAK PADA *CRYPTO MINER*

Perangkat Lunak	Deskripsi	Versi
XMRig	Perangkat lunak yang digunakan untuk melakukan penambangan mata uang kripto XMR.	6.16.4
Bminer	Perangkat lunak yang digunakan untuk melakukan penambangan mata uang kripto ETH, RVN, ZEC, dan CFX.	16.4.10
GMiner	Perangkat lunak yang digunakan untuk melakukan penambangan mata uang kripto ETH, BTG, ETC, TON, AION, RVN, dan FLUX.	2.91
lolMiner	Perangkat lunak yang digunakan untuk melakukan penambangan mata uang kripto ETH, BTG, ETC, TON, AION, ZEC, dan FLUX.	1.48.0

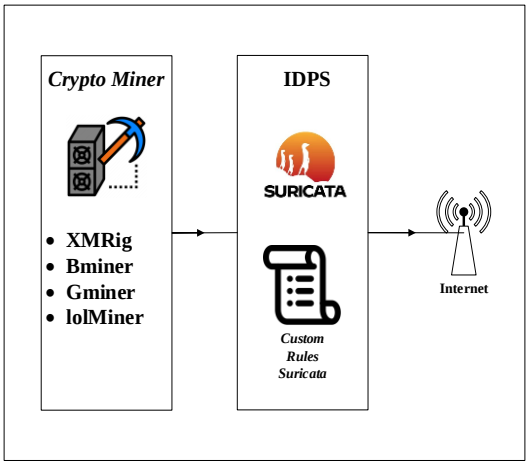
B. Desain

1) Topologi Sistem: Pada topologi sistem ini akan dijelaskan terkait sistem yang akan diimplementasikan pada jaringan. Sistem IDPS dan *Crypto Mining* akan diimplementasikan pada topologi yang bisa dilihat pada Gambar 2. Pada penelitian ini akan diimplementasikan IDPS Suricata pada perangkat ASUS Workstation TS100-E9-PI4 sebagai sensor pendeteksi serta prevensi terhadap aktivitas penambangan mata uang kripto pada jaringan. Selanjutnya terdapat perangkat ASUS ROG GL10DH yang akan diimplementasikan sebagai *Cryptocurrency Miner*. Perangkat *Cryptocurrency Miner* nantinya tidak terhubung langsung ke internet, melainkan terhubung terlebih dahulu melalui IDPS Suricata yang tersambung ke jaringan internet.



Gambar 2. Topologi jaringan

2) Gambaran Umum Sistem: Skema pada Gambar 3 merupakan gambaran umum bagaimana sistem yang akan diimplementasikan pada penelitian ini. Terdapat dua buah perangkat yang terdiri dari perangkat untuk *mining crypto* dan juga perangkat IDPS Suricata.



Gambar 3. Gambaran umum sistem

Gambar 3 merupakan gambaran umum sistem yang akan diimplementasikan pada penelitian ini. Terdapat dua perangkat utama yaitu perangkat IDPS Suricata yang akan diimplementasikan dengan *Custom Rules* serta perangkat *Crypto Miner* yang digunakan untuk melakukan simulasi *Crypto Mining*. Perangkat *Crypto Miner* terhubung langsung dengan perangkat IDPS Suricata yang terhubung ke jaringan.

C. Konfigurasi Rules IDPS Suricata

Pada tahap ini dilakukan instalasi dan konfigurasi IDPS Suricata pada perangkat ASUS Workstatiton TS100-E9-PI4. Terdapat beberapa proses yang akan dilakukan diantaranya adalah melakukan instalasi dan konfigurasi Suricata menjadi mode IPS, serta pembuatan dan penambahan rules Crypto Mining. Dalam penambahan rules Crypto Mining, terdapat kriteria Rule Suricata yang akan diuji pada penelitian ini dan dapat dilihat pada Tabel 5.

TABEL V
KRITERIA *RULE* SURICATA

Nama *Rule* Suricata	**Kriteria *Rule* Suricata**				
	Action	***Protocol***	***Source / Destination***	***Port***	***Rule Options***
Default rule	alert	tcp	$EXTERNAL_NET / $HOME_NET	Any	flow:established,to_client; content:" |22|mining.notify|22|";classtype:coin-mining;
Custom Rule Alert	alert	tcp	$HOME_NET / any	Any	dns_query; content:"alamat DNS *mining*"; classtype:coin-mining;
Custom Rule Drop	drop	tcp	Any / IP Address	Any	classtype:coin-mining;

Tabel 5 memuat kriteria *Rule* Suricata yang akan diuji pada penelitian ini. Penelitian ini akan menggunakan 3 buah rule yaitu *Default Rule, Custom Rule Alert*, dan *Custom Rule Drop*. Adapun struktur dan fungsi dari setiap *rule* berbeda, *Default Rule* memiliki aksi untuk melakukan *alert* atau notifikasi apabila adanya aktivitas *Crypto Mining* pada jaringan. *Default Rule* juga berisikan konten "|22|mining.notify|22|" yang berarti setiap paket yang melewati Suricata dan berisi konten tersebut akan dianggap sebagai aktivitas *Crypto Mining*. Selanjutnya *Custom Rule Alert* berfungsi sebagai pendeteksi adanya aktivitas *Crypto Mining* pada jaringan. Perbedaan dengan *Default Rule* ialah tipe yang digunakan pada konten tersebut berisikan "alamat DNS *mining*", sehingga setiap kali ada aktivitas percobaan koneksi ke alamat *mining pool*, maka akan langsung dianggap sebagai aktivitas *Crypto Mining* pada jaringan. Rule terakhir yaitu *Custom Rule Drop* yang berfungsi sebagai penangkal aktivitas *Crypto Mining* pada jaringan. Dengan menggunakan aksi drop, maka setiap percobaan koneksi yang menuju ke alamat IP dari *mining pool* yang dijalankan akan diblokir sehingga koneksi tidak dapat dilakukan. Adapun struktur dari *Custom Rules* yang dibuat bisa dilihat pada Tabel 6.

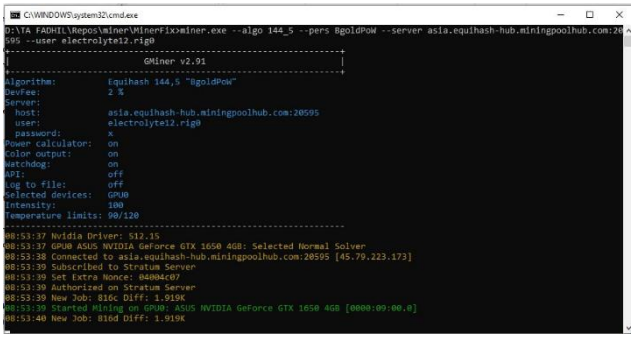
TABEL VI
STRUKTUR *CUSTOM RULES*

No	Nama *Rule*	Struktur *Custom Rules*
1.	***Rule Alert***	`alert dns $HOME_NET any -> any any (msg:"Terdapat percobaan Mining XMR yang mengarah ke (xmr.2miners.com)"; dns_query; content:"xmr.2miners.com"; nocase; isdataat:!1,relative; classtype:coin-mining; sid:1001; rev:1;)`
2.	***Rule Drop***	`drop tcp any any -> 51.89.96.41 any (msg:"Percobaan Mining Crypto yang mengarah ke (51.89.96.41) telah di blokir"; classtype:coin-mining; sid:2001; rev:1;)`

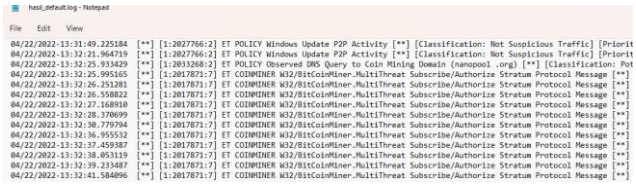
Cara kerja dari *custom rules* tersebut adalah dengan membaca *request* dari DNS dan alamat IP yang dituju dari lalu lintas jaringan yang berjalan. Apabila terdapat DNS ataupun alamat IP yang teridentifikasi sebagai alamat untuk melakukan *Crypto Mining*, maka suricata akan mencatat pada *log* dan memblokir alamat IP tersebut sehingga perangkat *mining* tidak dapat melakukan koneksi. Sementara apabila tidak terdapat DNS maupun alamat IP yang teridentifikasi sebagai alamat untuk melakukan *Crypto Mining*, maka lalu lintas jaringan akan diteruskan sehingga tetap bisa berjalan sebagai mana mestinya (tidak dilakukan blokir koneksi dan diidentifikasi sebagai lalu lintas jaringan yang normal).

D. Simulasi Crypto Mining pada Jaringan

Pada bagian ini akan diperlihatkan beberapa contoh simulasi *Crypto Mining* serta bagaimana IDPS Suricata mendeteksi maupun menangkal aktivitas *Crypto Mining* pada jaringan.

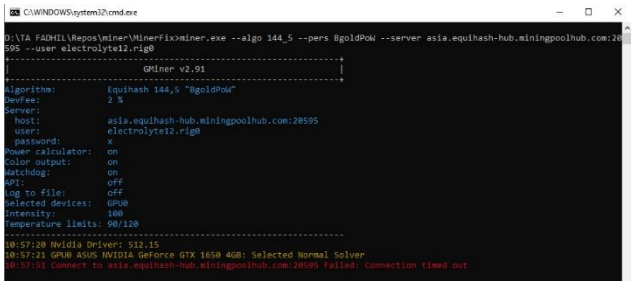


Gambar 4. *Crypto mining* dengan *rule default* pada IDPS Suricata



Gambar 5. Hasil deteksi *rule default* IDPS Suricata

Pada Gambar 4 dan 5 didapati percobaan simulasi *Crypto Mining* dengan menggunakan *rule default* pada IDPS Suricata. Dimana *rule default* sudah dapat mendeteksi adanya aktivitas *Crypto Mining* pada jaringan, namun simulasi *Crypto Mining* tetap berjalan dan tidak terblokir oleh *rule default* tersebut.



Gambar 6. Simulasi *Crypto Mining* dengan *Custom Rule* IDPS Suricata

Gambar 7. Hasil deteksi *rule custom* IDPS Suricata

Pada Gambar 6 dan 7 merupakan percobaan simulasi *Crypto Mining* menggunakan *Custom Rule* pada IDPS Suricata. Dimana *rule custom* dapat mendeteksi dan menangkal aktivitas *Crypto Mining* yang berjalan pada jaringan.

E. Hasil Pengujian Simulasi Crypto Mining

Berikut merupakan hasil pengujian dari simulasi *Crypto Mining* yang kemudian dilakukan pendeteksian dan penangkalan oleh IDPS Suricata. Terdapat dua simulasi yaitu dengan menggunakan *default rules* pada IDPS Suricata serta menggunakan *custom rules* pada IDPS Suricata. Tabel 7 merupakan hasil simulasi menggunakan *default rules* IDPS Suricata, dan Tabel 8 merupakan hasil simulasi menggunakan *custom rules* IDPS Suricata.

TABEL VII
CONFUSION MATRIX DEFAULT RULES

Mining Cryptocurrency		**Keadaan Seharusnya**	
		***Crypto Mining* Berjalan**	**Tidak ada aktivitas *Crypto Mining***
Hasil Deteksi	***Crypto Mining* Berjalan**	192	0
	Tidak ada aktivitas *Crypto Mining*	184	93436

Berdasarkan Tabel 7, dapat dilakukan perhitungan dan analisis dari hasil pengujian menggunakan *rules default* Suricata, yaitu:

$$Accuracy = \frac{(192+93436)}{(192+93436+0+184)} * 100\% = 99{,}8\% \quad (1)$$

$$Precision = \frac{(192)}{(192+0)} * 100\% = 100\% \quad (2)$$

$$Recall = \frac{192}{(192+184)} * 100\% = 51{,}06\% \quad (3)$$

$$F\text{-}measure = 2 \times \frac{(1\times 0.5106)}{(1+0.5106)} * 100\% = 67{,}61\% \quad (4)$$

Berdasarkan hasil perhitungan tersebut dapat diketahui bahwa *rules default* pada Suricata memiliki nilai *accuracy* sebesar 99,8%, yang berarti *rules default* pada Suricata dapat mendeteksi 998 dari 1000 paket *crypto mining* yang berjalan pada jaringan. Sementara itu didapatkan nilai *precision* sebesar 100% yang berarti tidak terdapat paket bernilai *false positive* pada penggunaan *rules default*. Selanjutnya nilai *recall* yang didapat yaitu sebesar 51,06% yang berarti *rules default* dari Suricata belum bisa mendeteksi semua paket yang seharusnya bisa diklasifikasikan sebagai paket *crypto mining*. Sehingga nilai *f-measure* yang didapatkan adalah sebesar 67,61% yang berarti performa atau tingkat efektivitas *rules default* Suricata bernilai 6,76 dari 10.

TABEL VIII
CONFUSION MATRIX CUSTOM RULES

Mining Cryptocurrency		**Keadaan Seharusnya**	
		***Crypto Mining* Berjalan**	**Tidak ada aktivitas *Crypto Mining***
Hasil Deteksi	***Crypto Mining* Berjalan**	387	0
	Tidak ada aktivitas *Crypto Mining*	0	15708

$$Accuracy = \frac{(387+15708)}{(387+15708+0+0)} * 100\% = 100\% \quad (1)$$

$$Precision = \frac{(387)}{(387+0)} * 100\% = 100\% \quad (2)$$

$$Recall = \frac{387}{(387+0)} * 100\% = 100\% \quad (3)$$

$$F\text{-}measure = 2 \times \frac{(1X1)}{(1+1)} * 100\% = 100\% \quad (4)$$

Berdasarkan hasil perhitungan tersebut dapat diketahui bahwa *rules custom* yang diimplementasikan pada Suricata saat melakukan *crypto mining* memiliki nilai *accuracy* sebesar 100%, yang berarti *rules custom* yang diimplementasikan pada Suricata dapat mendeteksi 100 dari 100 paket *crypto mining* yang berjalan pada jaringan. Sementara itu didapatkan nilai *precision* sebesar 100% yang berarti tidak terdapat paket bernilai *false positive* pada penggunaan *rules custom*. Selanjutnya nilai *recall* yang didapat yaitu sebesar 100% yang berarti *rules custom* yang diimplementasikan pada Suricata sudah mendeteksi semua paket yang seharusnya diklasifikasikan sebagai *crypto mining* sehingga tidak terdapat nilai *true negative*. Sehingga nilai *f-measure* yang didapatkan adalah sebesar 100% yang berarti performa atau tingkat efektivitas *rules custom* Suricata saat melakukan pendeteksian terhadap aktivitas *crypto mining* bernilai 10 dari 10. Untuk melihat perbandingan nilai signifikan pada hasil akhir dari kedua pengujian antara *rule default* dengan *rule custom*, peneliti menggunakan *One Sample Test* dan didapati hasil seperti pada Gambar 8.

One-Sample Test

Test Value = 90

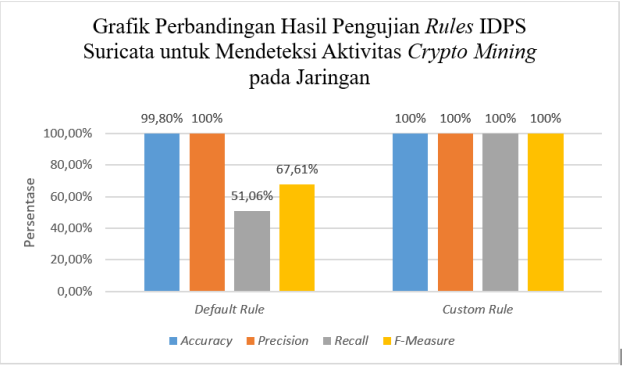
	t	df	Significance One-Sided p	Significance Two-Sided p
Accuracy	99.000	1	.003	.006
Recall	-.591	1	.330	.660
F_Measure	-.383	1	.384	.767

Gambar 8. *One-sample test*

Pada hasil pengujian *One-Sample Test* dengan nilai uji 90, didapati bahwa hasil *Accuracy* pada kedua pengujian tidak memiliki nilai yang signifikan dengan nilai signifikansinya hanya 0.003, namun yang membuat

perbedaan pada pengujian ini terdapat pada nilai *Recall* dan *F-Measure* yang diuji pada kedua *rule*, dimana terdapat nilai yang cukup signifikan diantara keduanya.

F. Analisis Hasil Pengujian Rules IDPS Suricata



Gambar 9. Grafik perbandingan *rules* IDPS Suricata

Dari grafik yang disajikan pada Gambar 9, terlihat bahwa terdapat peningkatan pada nilai *accuracy* sebesar 0,2%, nilai *recall* sebesar 48,94%, dan nilai *f-measure* sebesar 32,39%. Dari hasil tersebut dapat dilihat bahwa performa atau tingkat efektivitas Adapun faktor yang mempengaruhi bertambahnya tingkat efektivitas *Rule* Suricata dalam mendeteksi aktivitas *Crypto Mining* adalah *Custom Rule* yang dibuat untuk mendeteksi aktivitas *Crypto Mining* berbasis *signature-based detection*, dimana tanda yang digunakan pada pendeteksian aktivitas *Crypto Mining* pada penelitian ini adalah *Domain Name System* (DNS) dari setiap *mining pool* yang diakses sehingga hasil dari tingkat efektivitas *rule* suricata dalam mendeteksi aktivitas *Crypto Mining* meningkat. Selanjutnya pada Tabel 9 terdapat hasil *rule suricata* dalam menangkal aktivitas *Crypto Mining* pada jaringan.

TABEL IX
PERBANDINGAN KAPABILITAS *RULE* SURICATA

Rule Suricata	Aplikasi *Crypto Mining*			
	XMRig	Bminer	GMiner	lolMiner
Default Rule	X	X	X	X
Custom Rule	✓	✓	✓	✓

Dapat dilihat pada Tabel 9 bahwa *Custom Rule* pada Suricata bekerja dengan sangat baik, dimana *rule* tersebut dapat menangkal aktivitas *Crypto Mining* pada jaringan dari setiap aplikasi yang digunakan. Sementara itu *Default Rule* Suricata tidak dapat menangkal aktivitas *Crypto Mining* pada jaringan, dan hanya bisa melakukan pendeteksian adanya aktivitas *Crypto Mining* pada jaringan tersebut. Adapun hal yang membuat *Custom Rule* dapat menangkal aktivitas *Crypto Mining* pada jaringan adalah dengan adanya aksi *drop* pada setiap *rules*-nya. Sehingga setiap paket yang teridentifikasi sebagai aktivitas *Crypto Mining* akan langsung ditangkal dan tidak dapat lanjut. Sementara hal tersebut tidak terdapat *Default Rule*, yang hanya menyediakan aksi *alert* pada setiap pendeteksian aktivitas *Crypto Mining*.

IV. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan penelitian analisis rules *Intrusion Detection Prevention System* Suricata dalam mendeteksi dan menangkal aktivitas *Crypto Mining* pada jaringan yang dilakukan, kesimpulan untuk menjawab rumusan masalah dalam penelitian ini adalah sebagai berikut.

1. Kriteria rules IDPS Suricata yang diimplementasikan untuk mendeteksi dan menangkal aktivitas *Crypto Mining* pada jaringan adalah sebagai berikut :
   a. Rule memiliki aksi alert untuk mencatat segala aktivitas *Crypto Mining* yang terdeteksi pada jaringan..
   b. Rule memiliki aksi drop untuk menangkal atau memblokir aktivitas *Crypto Mining* yang terdeteksi pada jaringan, pada rule drop akan dilakukan pemblokiran melalui alamat IP yang berkaitan dengan aktivitas *Crypto Mining*.
   c. Setiap rule memiliki konten DNS Query serta alamat IP yang berkaitan dengan aktivitas *Crypto Mining*.
   d. Rule yang diimplementasikan berbasis *Signature-based detection*, sehingga harus mengetahui
2. Tingkat efektivitas *custom rules* IDPS Suricata yang diimplementasikan pada untuk mendeteksi dan menangkal aktivitas *Crypto Mining* pada jaringan bernilai 100% dengan rincian tingkat *accuracy* 100%, *precision* 100%, *recall* 100% dan *f-measure* bernilai 100%. Nilai tersebut berarti custom rules IDPS Suricata yang diimplementasikan dapat berjalan sesuai dengan tujuannya yaitu mendeteksi segala aktivitas *Crypto Mining* pada jaringan sesuai dengan *mining pool* yang digunakan untuk *Crypto Mining* serta dapat memblokir aktivitas *Crypto Mining* pada jaringan sehingga perangkat *mining* tidak dapat melakukan koneksi ke *mining pool*. Custom Rules IDPS Suricata juga memiliki peningkatan efektivitas jika dibandingkan dengan Default Rule IDPS Suricata. Dimana terdapat peningkatan pada nilai *accuracy* sebesar 0,2%, nilai *recall* sebesar 48,94%, dan nilai *f-measure* sebesar 32,39%. Sehingga dapat disimpulkan bahwa custom rules IDPS Suricata yang dibuat untuk menangkal dan mendeteksi aktivitas *Crypto Mining* dalam hal ini penambangan mata uang kripto ETH, CFX, BTG, ETC, XMR, TON, AION, ZEC, FLUX dan RVN dapat berjalan sesuai dengan yang diharapkan. Yaitu dapat mendeteksi adanya aktivitas penambangan, serta menangkal aktivitas tersebut dengan aksi drop pada *Custom Rules* yang dibuat.

B. Saran

Adapun beberapa saran yang dapat dijadikan sebagai pengembangan untuk penelitian selanjutnya adalah sebagai berikut.

1. Menambahkan dataset pengujian dari *pool* dan jenis mata uang kripto yang ditambang untuk meningkatkan kapabilitas rules dalam mendeteksi dan menangkal aktivitas *Crypto Mining* pada jaringan.
2. Menggunakan metode machine-learning based dalam proses pendeteksian dan penangkalan aktivitas *Crypto Mining* untuk menambah tingkat akurasi dan presisi serta dapat mengikuti perkembangan mata uang kripto tanpa harus dilakukan pembaruan terhadap rules-nya.
3. Menambahkan fungsi notifikasi pada media social seperti Whatsapp atau Telegram pada sistem IDPS Suricata sehingga pengguna mendapatkan informasi lebih cepat ketika terdapat aktivitas *Crypto Mining* pada jaringan.
4. Menambahkan berbagai skenario tambahan dalam penelitian untuk mengetahui threat atau ancaman apa saja yang mungkin bisa menjadikan IDPS uricata menjadi tidak bisa mendeteksi ataupun menangkal aktivitas *Crypto Mining* pada jaringan.

REFERENSI

[1] F. Steinmetz, M. von Meduna, L. Ante, and I. Fiedler, "Ownership, uses and perceptions of cryptocurrency: Results from a population survey," *Technol. Forecast. Soc. Change*, vol. 173, no. August, p. 121073, 2021, doi: 10.1016/j.techfore.2021.121073.

[2] "Tren Adopsi Uang Kripto di Dunia, Bagaimana Indonesia? - Analisis Data Katadata." https://katadata.co.id/ariayudhistira/analisisdata/613b6c1d8a22d/tren-adopsi-uang-kripto-di-dunia-bagaimana-indonesia (accessed Oct. 12, 2021).

[3] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Cryptocurrency*, Nov. 2008, doi: 10.1162/ARTL_a_00247.

[4] J. Beccuti and C. Jaag, "The Bitcoin Mining Game: On the Optimality of Honesty in Proof-of-work Consensus Mechanism," *Tech. Rep.*, vol. 41, no. 0, pp. 0–20, 2017, [Online]. Available: www.swiss-economics.ch

[5] G. S. Ubhi and J. K. Sahiwal, "A Review on Software Mining: Current Trends and Methodologies," *Int. J. Eng. Res. Appl.*, vol. 07, no. 04, pp. 40–45, 2017, doi: 10.9790/9622-0704054045.

[6] K. Sigler, "Crypto-jacking: how cyber-criminals are exploiting the crypto-currency boom," *Comput. Fraud Secur.*, vol. 2018, no. 9, pp. 12–14, 2018, doi: 10.1016/S1361-3723(18)30086-1.

[7] P. W. Tsai, "Design and Development of Multi-Pattern Matching Rules for Detecting Cryptocurrency Mining in Packet Inspection," *Commun. CCISA*, pp. 41–51, 2021, [Online]. Available: https://cccisa.ccisa.org.tw/article/view/2480

[8] V. Kalgutkar, R. Kaur, H. Gonzalez, N. Stakhanova, and A. Matyukhina, "Code authorship attribution: Methods and challenges," *ACM Comput. Surv.*, vol. 52, no. 1, 2019, doi: 10.1145/3292577.

[9] "Can mining damage my GPU or a PC? | NiceHash." https://www.nicehash.com/blog/post/can-mining-damage-my-gpu-or-a-pc (accessed Nov. 03, 2021).

[10] E. Zuberi and A. Wool, "Characterizing GPU Overclocking Faults," in *Computer Security -- ESORICS 2021*, 2021, pp. 110–130.

[11] "What is Suricata — Suricata 7.0.0-dev documentation." https://suricata.readthedocs.io/en/latest/what-is-suricata.html (accessed Oct. 13, 2021).

[12] A. D. Ralianto and S. Cahyono, "Perbandingan Nilai Akurasi Snort dan Suricata dalam Mendeteksi Intrusi Lalu Lintas di Jaringan," no. 1, 2018.

[13] J. Z. I. Muñoz, "Detection of Bitcoin miners from network measurements," no. April, 2019.

[14] A. Swedan, A. N. Khuffash, M. M. Othman Othman, and A. Awad, "Detection and Prevention of Malicious Cryptocurrency Mining on Internet-Connected Devices," *ACM Int. Conf. Proceeding Ser.*, 2018, doi: 10.1145/3231053.3231076.

[15] J. E. Goldman and P. T. Rawles, *Applied data communications: a business-oriented approach*. Wiley New York, 2004.

[16] C. Garcia, "Suricata IDS: An overview of threading capabilities | AT&T Cybersecurity," 2019. https://cybersecurity.att.com/blogs/security-essentials/suricata-ids-threading-capabilities-overview (accessed Aug. 18, 2022).

[17] "Crypto Mining Simulator system requirements | Can I Run Crypto Mining Simulator." https://www.systemrequirementslab.com/cyri/requirements/crypto-mining-simulator/20845 (accessed Aug. 18, 2022).