

**IMPLEMENTASI NETWORK INTRUSION DETECTION SYSTEM
SNORT DALAM MENDETEKSI SERANGAN CRYPTOJACKING**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



diajukan oleh

MOH. SESAR ABDUL SYUKUR

18.83.0156

Kepada

PROGRAM SARJANA

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

**IMPLEMENTASI NETWORK INTRUSION DETECTION SYSTEM
SNORT DALAM MENDETEKSI SERANGAN CRYPTOJACKING**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



diajukan oleh

MOH. SESAR ABDUL SYUKUR

18.83.0156

Kepada

PROGRAM SARJANA

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

HALAMAN PERSETUJUAN

SKRIPSI

**IMPLEMENTASI NETWORK INTRUSION DETECTION SYSTEM
SNORT DALAM MENDETEKSI SERANGAN CRYPTOJACKING**

yang disusun dan diajukan oleh

Moh. Sesar Abdul Syukur

18.83.0156

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 03 Oktober 2021

Dosen Pembimbing,

ii

Dony Ariyus M.Kom

NIK. 190302128

HALAMAN PENGESAHAN

SKRIPSI

**IMPLEMENTASI NETWORK INTRUSION DETECTION SYSTEM
SNORT DALAM MENDETEKSI SERANGAN CRYPTOJACKING**

yang disusun dan diajukan oleh

Moh. Sesar Abdul Syukur

18.83.0156

Telah dipertahankan di depan Dewan Penguji
pada tanggal 22 Agustus 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Andika Agus Slameto, M.Kom

NIK. 190302109

Wahyu Sukestastama Putra, S.T., M.Eng

NIK. 190302328

Dony Arivus, M.Kom

NIK. 190302128

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 Agustus 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, S.Kom., M.Kom.

NIK. 19030209

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Moh. Sesar Abdul Syukur
NIM : 18.83.0156

Menyatakan bahwa Skripsi dengan judul berikut:

IMPLEMENTASI NETWORK INTRUSION DETECTION SYSTEM SNORT DALAM MENDETEKSI SERANGAN CRYPTOJACKING

Dosen Pembimbing : Dony Ariyus, M. Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 22 Agustus 2022

Yang Menyatakan,

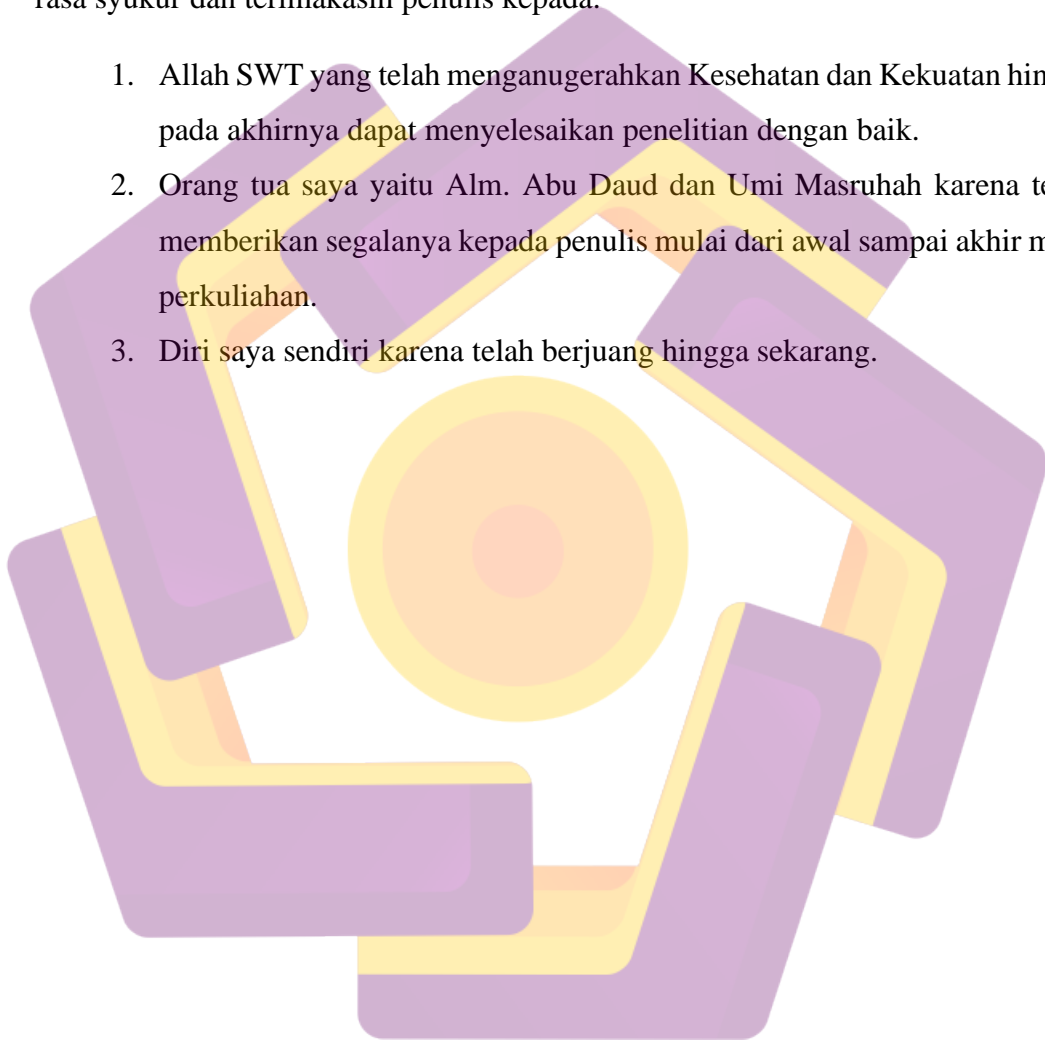


Moh. Sesar Abdul Syukur

HALAMAN PERSEMBAHAN

Dengan segala puji dan syukur kepada Allah SWT dan Rasulullah SAW serta dukungan dan doa dari orang-orang tercinta, akhirnya skripsi ini dapat diselesaikan dengan baik. Oleh karena itu, dengan rasa bangga dan bahagia penulis khaturkan rasa syukur dan terimakasih penulis kepada:

1. Allah SWT yang telah menganugerahkan Kesehatan dan Kekuatan hingga pada akhirnya dapat menyelesaikan penelitian dengan baik.
2. Orang tua saya yaitu Alm. Abu Daud dan Umi Masruhah karena telah memberikan segalanya kepada penulis mulai dari awal sampai akhir masa perkuliahan.
3. Diri saya sendiri karena telah berjuang hingga sekarang.



KATA PENGANTAR

Assalamu'alaikum Wr.Wb.

Puji Syukur saya panjatkan kepada Allah SWT yang telah memberikan berkah dan karunia-Nya , memberikan kekuatan, kemudahan dan ketabahan hati serta mempermudah proses penelitian hingga penulis dapat menyelesaikan tugas akhir yang berjudul **“IMPLEMENTASI NETWORK INTRUSION DETECTION SYSTEM SNORT DALAM MENDETEKSI SERANGAN CRYPTOJACKING”** dengan lancar dan tepat waktu.

Tugas akhir ini merupakan salah satu syarat semua mahasiswa Jurusan Teknik Komputer Universitas Amikom Yogyakarta untuk mendapatkan gelar Sarjana.

Dalam penyusunan Tugas Akhir ini penulis banyak menerima bantuan, bimbingan, arahan, serta motivasi dari berbagai pihak baik secara langsung ataupun tidak langsung, kemudian penulis ingin menyampaikan rasa hormat dan terima kasih kepada :

1. Bapak Prof. Dr. M. Suyanto, MM selaku Rektor Universitas Amikom Yogyakarta dan segenal pimpinan rektoran Universitas Amikom Yogyakarta.
2. Bapak Hanif Al Fatta, S.Kom., M.Kom. selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
3. Bapak Dony Ariyus, M.Kom selaku Kepala Program Studi Teknik Komputer serta Dosen Pembimbing penulis dalam menyelesaikan tugas akhir ini.
4. Seluruh Dosen dan Karyawan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta khususnya Program Studi Teknik Komputer yang telah memberikan bimbingan, ilmu, nasihat kepada semua mahasiswa khususnya kepada penulis.
5. Terima kasih kepada (Alm) Abi, Ummi, Bapak, Kakak-Kakak yang telah memberikan do'a, waktu, motivasi dan semangat hingga penulis dapat menyelesaikan penelitian ini dengan baik.

6. Terima kasih kepada Calon Istri saya Nurul Hidayah yang telah memberikan dukungan, perhatian, kasih sayang hingga akhirnya semua dapat berjalan secara lancar.
7. Terimakasih kepada teman-teman saya Bertha, Bhimo, Atthar, Billa, Elis, Reza, Cholis, Bima, Udin, Lutfi, Ali, Azza, Juju, Faisal dan masih banyak lagi yang tidak bisa saya sebutkan semuanya, saya merasa sangat bersyukur mempunyai teman dan sahabat yang selalu ada dikala senang ataupun susah, tanpa kalian mungkin saya tidak bisa melangkah sejauh ini, sekali lagi terima kasih.

Penulis menyadari bahwa penulisan tugas akhir ini masih jauh dari kata sempurna baik dari penulisan hingga penyajian data, untuk itu segala macam saran dan masukan yang membangun semoga senantiasa diberikan untuk penelitian dimasa depan. Terakhir semoga skripsi ini memberikan manfaat kepada semua pihak dan membuka awal perjalanan kesuksesan penulis dimasa depan.

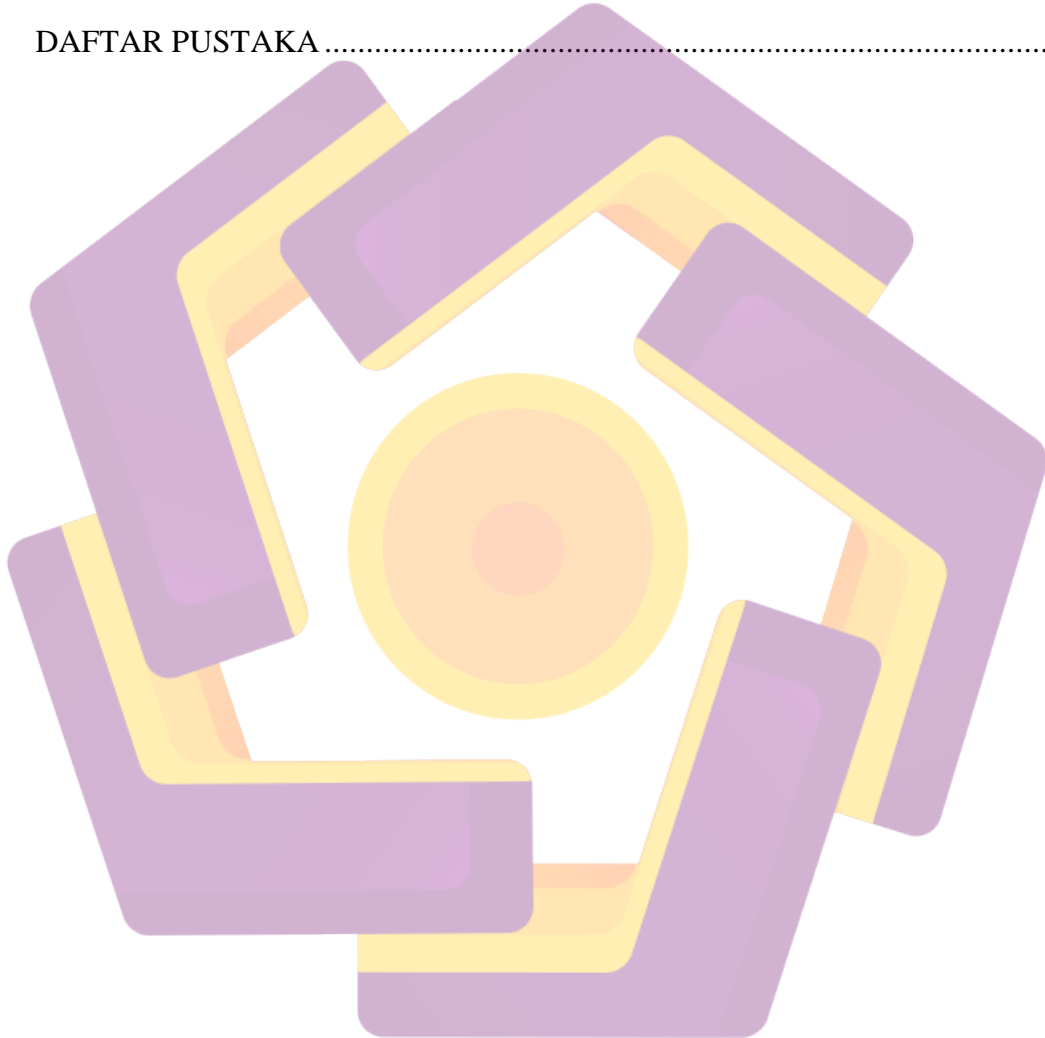
Yogyakarta,
Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN.....	ii
SKRIPSI.....	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI.....	viii
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
INTISARI.....	xiv
Abstract	xv
BAB I Pendahuluan	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan masalah	2
1.4 Maksud dan Tujuan Penelitian	2
1.5 Manfaat Penelitian	2
1.6 Metode Penelitian	3
1.6.1 Metode Pengumpulan Data.....	3
1.6.2 Metode Analisis.....	3
1.6.3 Metode Perancangan.....	3
1.7 Sistematika Penulisan	3
BAB II Landasan Teori.....	5
2.1 Kajian Pustaka	5
2.2 Internet	8
2.2.1 <i>World Wide Web (WWW)</i>	9
2.2.1.1 <i>Web server</i>	10
2.2.1.2 <i>Web browser</i>	10

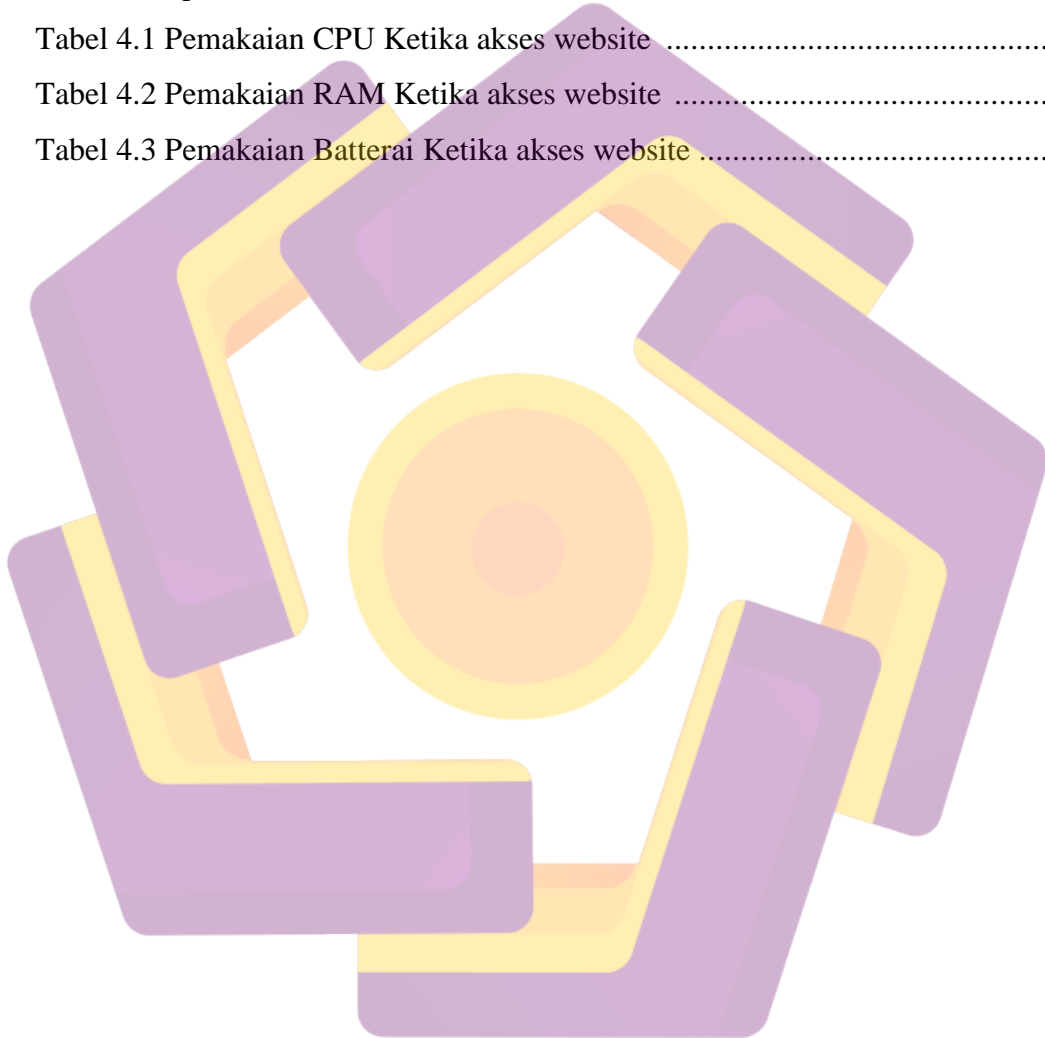
2.2.1.3	<i>Webpage</i>	13
2.2.1.4	<i>Website</i>	13
2.3	<i>Cryptocurrency</i>	14
2.3.1.	Karakteristik <i>Cryptocurrency</i>	15
2.3.2.	Jenis – Jenis <i>Cryptocurrency</i>	16
2.4	<i>Cryptomining</i>	18
2.4.1	Cara kerja <i>Cryptomining</i>	19
2.4.2	Metode <i>Cryptomining</i>	20
2.4.3	Manfaat dan Kerugian dari <i>Cryptomining</i>	24
2.5	<i>Cryptojacking</i>	25
2.5.1.	Cara Kerja <i>Cryptojacking</i>	26
2.5.2.	Cara kerja berdasarkan Teknik	28
2.5.3.	Jenis – Jenis <i>Obfuscation</i> pada <i>Cryptojacking</i>	29
2.6	IDS (<i>Intrusion Detection System</i>)	33
2.6.1.	Cara kerja IDS	33
2.6.2.	Jenis-Jenis <i>Intrusion Detection System</i>	34
2.7	<i>Snort</i>	37
2.7.1.	Jenis penerapan <i>Snort</i>	38
BAB III Metodologi Penelitian		39
3.1.	Alat dan Bahan Penelitian	39
3.1.1.	Perangkat keras (<i>hardware</i>)	39
3.1.2.	Perangkat Lunak (<i>software</i>)	40
3.2.	Langkah Penelitian	40
3.3.	Metode Penelitian	43
3.3.1.	Tahap Persiapan	43
3.3.2.	Pengujian	44
3.3.3.	Analisis Dampak Serangan	44
BAB IV Hasil dan Pembahasan		46
4.1	Hasil Penelitian	46
4.1.1	Instalasi <i>Snort</i>	46
4.1.2	Pengujian <i>Snort</i>	49
4.2	Dampak <i>Cryptojacking</i>	52

4.2.1. Pemakaian CPU.....	52
4.2.2. Pemakaian RAM	53
4.2.3. Pemakaian Batterai	55
BAB V Kesimpulan dan Saran.....	56
5.1 Kesimpulan.....	56
5.2 Saran	56
DAFTAR PUSTAKA.....	59



DAFTAR TABEL

Tabel 2.1 Penelitian yang Berkaitan	7
Tabel 3.1 Spesifikasi Komputer Penelitian	24
Tabel 3.2 Spesifikasi Virtual Komputer	24
Tabel 3.2 Spesifikasi Virtual Korban	25
Tabel 4.1 Pemakaian CPU Ketika akses website	31
Tabel 4.2 Pemakaian RAM Ketika akses website	32
Tabel 4.3 Pemakaian Batterai Ketika akses website	33



DAFTAR GAMBAR

Gambar 2.1 Internet	8
Gambar 2.2 World Wide Web.....	9
Gambar 2.3 Web Server.....	10
Gambar 2.4 Cookie Web	11
Gambar 2.5 Google Chrome	12
Gambar 2.6 Mozilla Firefox	12
Gambar 2.7 Webpage	13
Gambar 2.8 Website	14
Gambar 2.9 Logo Bitcoin	17
Gambar 2.10 Logo Ethereum	17
Gambar 2.11 Logo Litecoin	18
Gambar 2.12 Kegiatan Cryptomining	19
Gambar 2.13 GPU Mining	21
Gambar 2.14 ASIC Mining	22
Gambar 2.15 Cloud Mining	23
Gambar 2.16 CPU Mining	24
Gambar 2.17 Serangan Cryptojacking	25
Gambar 2.18 Serangan Cryptojacking tahun 2017	26
Gambar 2.19 Script pada oceanoffgames.com	28
Gambar 2.20 Script pada anmaxjp.com	29
Gambar 2.21 Script pada musicjinni.com	29
Gambar 2.22 Script pada piratebay.cr	30
Gambar 2.23 Perbandingan kode sebelum dan sesudah di- obfuscate	30
Gambar 2.24 Script CoinHive yang dipanggil dari domain lain	32
Gambar 2.25 Intrusion Detection System	33
Gambar 2.26 Network Intrusion Detection System	34
Gambar 2.27 Host Intrusion Detection System (HIDS)	35
Gambar 2.28 Signature Based Intrusion Detection System	36

Gambar 2.29 Anomaly Based Intrusion Detection System	37
Gambar 2.30 Logo software snort	37
Gambar 3.1 Alur Penelitian	40
Gambar 3.1 Daftar Alir	42
Gambar 4.1 Instalasi snort	45
Gambar 4.2 Isi IP Tujuan	45
Gambar 4.3 Copy file snort_conf	46
Gambar 4.4 Edit file test_snort.conf	46
Gambar 4.5 Hapus rule tidak terpakai pada test_snort.conf	47
Gambar 4.6 Masuk direktori rules dan edit isi rule	47
Gambar 4.7 Isikan rule cryptojacking	48
Gambar 4.8 Website yang dicurigai terdapat cryptojacking	48
Gambar 4.9 System monitor sebelum akses website	49
Gambar 4.10 System monitor ketika akses website	49
Gambar 4.11 Snort sudah terkonfigurasi	50
Gambar 4.12 Akses website dan menjalankan snort	50
Gambar 4.13 Alert yang muncul ketika website diakses	50
Gambar 4.14 Grafik Pemakaian CPU	52
Gambar 4.15 Grafik Pemakaian RAM	53
Gambar 4.16 Grafik Pemakaian Batterai	54

INTISARI

Website diciptakan khusus sebagai wadah dan alat untuk menyebarkan informasi digital. Namun terdapat berbagai ancaman terhadap keamanan *website*, salah satu serangan yang mencuri perhatian khusus adalah *cryptojacking*. Serangan *cryptojacking* dilakukan oleh pelaku yang mengincar sumber daya dari komputer pengguna tanpa diketahui, dampak dari serangan *cryptojacking* tidak terlalu besar namun jika terjadi terus menerus maka perangkat korban akan mengalami kerusakan berat hingga kerusakan total. Serangan *cryptojacking* memanfaatkan *website* sebagai wadah untuk menyisipkan *script* yang akan otomatis berjalan ketika *website* tersebut di akses. Dalam karya tulis ini peneliti memanfaatkan perangkat lunak IDS *Snort* untuk mendeteksi serangan *cryptojacking* yang bertujuan agar pengguna menyadari ketika tanpa sadar mengakses *website* yang mengandung *script cryptojacking*. Peneliti menggunakan metode analisis eksperimen yaitu membuat percobaan langsung pada web yang dicurigai terdapat skrip *cryptojacking*. Dalam tugas akhir ini, penelitian yang dilakukan berhasil mendeteksi *script cryptojacking* yang berada dalam sebuah *website* dengan waktu 2.15 detik, selanjutnya peneliti membuat laporan tentang dampak yang disebabkan oleh serangan *cryptojacking* untuk kemudian di analisis dan dengan harapan dapat mendapatkan gambaran tentang kerusakan apa saja yang dapat disebabkan oleh serangan *cryptojacking*, penulis berharap dengan penelitian ini dapat memberikan dampak positif kepada masyarakat luas tentang keamanan berselancar di *internet* dikemudian hari.

Kata kunci : *Internet*, Intrusion Detection System, *Cryptojacking*, *Snort*, Keamanan siber.

Abstract

The website was created specifically as a place and tool for disseminating digital information. However, there are various threats to web security, one of the attacks that stole particular attention is cryptojacking. Cryptojacking attacks are carried out by perpetrators who target resources from the user's computer without being noticed, the impact of a cryptojacking attack is not too large but if it occurs continuously, the victim's device will suffer severe damage to total damage. Cryptojacking attacks use the website as a place to insert a script that will automatically run when the website is accessed. In this paper, the researcher uses IDS Snort software to detect cryptojacking attacks, which aims to make users aware when they unknowingly access websites that contain cryptojacking scripts. The researcher uses the experimental analysis method, which is to make a direct experiment on a web that is suspected of containing cryptjacking scripts. In this final project, the research carried out succeeded in detecting a cryptojacking script that was on a website with a time of 2.15 seconds, then the researcher made a report about the impact caused by cryptojacking attacks for later analysis and in the hope of getting an idea of what damage can be caused. by cryptojacking attacks, the author hopes that this research can have a positive impact on the wider community about the security of surfing the internet in the future.

Keyword: Website, Intrusion Detection System, Cryptojacking, Snort, Cybersecurity.