BAB 1
USULAN GAGASAN DAN PEMILIHAN TOPIK

1.1. Latar Belakang Masalah

Di era digital, di mana konektivitas tanpa batas dan pertukaran data terjadi secara masif, keamanan jaringan telah menjadi masalah penting yang tidak dapat disepelekan. Ironisnya, kemajuan teknologi yang menghubungkan dunia juga membuka pintu bagi ancaman siber yang semakin merajalela. Serangan *malware*, serangan *denial-of-service*, dan serangan lainnya terus berevolusi dengan kecanggihan yang semakin meningkat, menargetkan individu, organisasi, dan bahkan infrastruktur nasional penting yang menjadi tulang punggung negara. Sebagai contoh, 282 data pemerintah disandera dan diminta tebusan, sebuah pengingat nyata tentang betapa rentannya sistem keamanan siber [1]. Insiden tersebut tidak hanya menyebabkan kerugian finansial yang signifikan, tetapi juga mengguncang kepercayaan publik dan mengancam stabilitas nasional, seperti yang dilaporkan oleh Satwika, Sudiarsa, dan Swari dalam [2], yang menyatakan bahwa "kebutuhan akan sistem keamanan jaringan yang handal dan terjangkau semakin meningkat, terutama di perguruan tinggi dan UKM."

Namun, penting untuk ditekankan bahwa sistem deteksi intrusi yang dikembangkan dalam proyek ini tidak dimaksudkan untuk mencegah serangan siber berskala besar seperti yang menimpa PDNS. Fokus dari proyek ini adalah menyediakan solusi keamanan jaringan yang terjangkau dan mudah diterapkan untuk pengguna usaha atau organisasi kecil, sehingga mereka dapat mengembangkan kesadaran dan kebiasaan untuk menangani keamanan siber dengan serius. Dengan demikian, diharapkan dapat menciptakan lapisan pertahanan awal yang kuat untuk memerangi ancaman siber yang semakin hari semakin ganas.

Pemilihan isu ini didasarkan pada keprihatinan mendalam terhadap ancaman siber yang terus meningkat di Indonesia, yang diperparah dengan keterbatasan sistem keamanan tradisional. *Firewall* dan antivirus selama ini menjadi andalan untuk melindungi jaringan, tetapi sering kali gagal memblokir serangan yang canggih. Mereka juga mengandalkan deteksi berbasis tanda tangan, sehingga sulit untuk merespons evolusi ancaman yang dinamis. Sementara itu, solusi keamanan modern yang lebih canggih, seperti *Intrusion Detection System* (IDS) dan *Security Information and Event Management* (SIEM), seringkali terkendala oleh biaya penerapan yang tinggi dan kompleksitas manajemen.

Kompleksitas masalah keamanan jaringan ini semakin diperparah oleh berbagai faktor yang saling terkait keragaman teknologi yang digunakan dalam jaringan modern, mulai dari perangkat IoT hingga server berbasis *cloud*, menciptakan banyak potensi eksploitasi bagi para

penyerang. Faktor manusia seperti kurangnya kesadaran dan perilaku pengguna yang ceroboh juga berkontribusi pada peningkatan kerentanan sistem.

Pengembangan sistem deteksi intrusi keamanan jaringan menggunakan Raspberry Pi menawarkan opsi yang menjanjikan untuk memerangi ancaman dunia maya yang semakin intens. Dengan memanfaatkan kekuatan pemrosesan yang ditingkatkan dari Raspberry Pi 5 dan fleksibilitasnya dalam berbagai konfigurasi, sistem ini memiliki potensi untuk menjadi solusi keamanan siber yang komprehensif dan dapat menjangkau berbagai kalangan, termasuk mereka yang terkendala oleh sumber daya yang terbatas. Seperti yang disampaikan oleh Priyo Atmojo dalam [3], Raspberry Pi sepenuhnya mampu menjalankan aplikasi IDS seperti Snort dan Bro, serta berkinerja sangat baik dalam mendeteksi berbagai jenis serangan.

Penelitian sebelumnya juga menunjukkan kemampuan Raspberry Pi sebagai platform IDS yang efektif. Atmojo menemukan bahwa Raspberry Pi mampu menjalankan aplikasi IDS seperti Snort dan Bro, dengan kinerja yang sangat baik dalam mendeteksi berbagai jenis serangan [3]. Satwika et al. dalam [2] mendemonstrasikan kemampuan Raspberry Pi 3 dalam mendeteksi serangan jaringan seperti serangan PING, *port scan*, dan serangan DOS/DDoS menggunakan Snort. Saskara et al. juga menemukan bahwa Raspberry Pi mampu mendeteksi serangan pada jaringan nirkabel, khususnya *WPA2 handshake cracking* menggunakan Kismet [4]. Hasil ini menegaskan bahwa Raspberry Pi dapat menjadi solusi keamanan yang kuat dan efisien dengan konfigurasi dan aplikasi IDS yang tepat.

1.2. Informasi Pendukung Masalah

Keamanan jaringan adalah salah satu komponen penting dalam manajemen infrastruktur teknologi informasi, terutama dalam menghadapi ancaman serangan siber yang terus berkembang, termasuk serangan *malware* dan ancaman terhadap perangkat *Internet of Things* (IoT). Serangan siber seperti *Distributed Denial of Service* (DDoS), serangan ping, *port scanning*, dan serangan *malware* kini menjadi ancaman nyata bagi banyak organisasi dan perusahaan yang sangat bergantung pada jaringan untuk beroperasi.

1.2.1. Serangan Malware Terhadap Jaringan dan IoT

Dengan semakin berkembangnya teknologi *Internet of Things* (IoT), keamanan jaringan menjadi semakin penting karena perangkat IoT seringkali memiliki kerentanan keamanan yang tinggi. *Malware* pada perangkat IoT dapat menginfeksi jaringan, menciptakan celah keamanan yang memungkinkan penyerang untuk mencuri data sensitif atau bahkan mengambil alih kontrol perangkat IoT [5]. Serangan ini dapat

digunakan untuk membuat *botnet*, seperti *Mirai*, yang memanfaatkan perangkat IoT yang terinfeksi untuk melakukan serangan DDoS skala besar, mematikan infrastruktur jaringan yang penting.

Malware yang menyerang perangkat IoT dan jaringan dapat memiliki berbagai bentuk, termasuk *ransomware*, *spyware*, *adware*, dan *botnet*. Semua jenis *malware* ini memiliki potensi merusak jaringan dan infrastruktur IoT dengan menyusup melalui perangkat-perangkat yang sering kali tidak memiliki perlindungan yang memadai.

1.2.2. *Intrusion Detection System* (IDS) dengan Raspberry Pi

Intrusion Detection System (IDS) memainkan peran penting dalam mendeteksi serangan-serangan ini secara *real-time*, termasuk *malware* yang menyerang jaringan IoT. IDS yang dibangun menggunakan Raspberry Pi 5 menjadi solusi yang efektif karena Raspberry Pi merupakan platform dengan biaya rendah namun mampu menjalankan perangkat lunak *open-source* seperti Snort dan Suricata. Kedua perangkat lunak ini dirancang untuk mendeteksi ancaman siber seperti serangan *malware*, *DDoS, port scanning,* dan *ping attack* [6]. Selain itu, Snort dan Suricata mampu mendeteksi berbagai jenis malware dan memberikan peringatan dini kepada administrator jaringan ketika lalu lintas mencurigakan terdeteksi, seperti lalu lintas data abnormal yang diakibatkan oleh *malware* IoT [7]. Deteksi ini memungkinkan administrator untuk segera mengambil tindakan sebelum serangan menyebabkan kerusakan lebih lanjut.

1.2.3. Integrasi Sistem Notifikasi *Real-Time*

Untuk meningkatkan respons terhadap ancaman yang terdeteksi, IDS berbasis Raspberry Pi 5 dapat diintegrasikan dengan sistem notifikasi *real-time* menggunakan aplikasi seperti Telegram. Telegram bot dapat dikonfigurasi untuk mengirimkan notifikasi langsung ke perangkat administrator saat IDS mendeteksi aktivitas mencurigakan, termasuk *malware* yang mencoba menginfeksi perangkat IoT. Dengan sistem ini, administrator dapat dengan cepat mengambil tindakan untuk memitigasi serangan, mengurangi risiko kerusakan lebih lanjut pada jaringan dan perangkat IoT.

1.2.4. Pemilihan Raspberry Pi 5 Sebagai Platform IDS

Dalam proyek pengembangan Sistem Deteksi Intrusi Keamanan Jaringan ini, Raspberry Pi 5 dipilih sebagai *platform* utama. Keputusan ini diambil setelah mempertimbangkan berbagai faktor yang membuatnya lebih unggul dibandingkan

dengan *Single Board Computer* (SBC) lain seperti Raspberry Pi 4B, Orange Pi 5 Pro, dan Nvidia Jetson Nano.

Beberapa hal yang menjadi pertimbangan adalah sebagai berikut :

1. **Performa**

   Raspberry Pi 5 menawarkan peningkatan performa yang signifikan dibandingkan dengan pendahulunya, Raspberry Pi 4B [13]. Prosesor quad-core Arm Cortex-A76 64-*bit* yang beroperasi pada 2.4 GHz pada Raspberry Pi 5 memberikan kemampuan pemrosesan data *real-time* yang lebih baik, krusial untuk menjalankan aplikasi IDS seperti Snort dan Suricata. Meskipun Orange Pi 5 Pro memiliki jumlah *core* prosesor yang lebih banyak (*octa-core*), Raspberry Pi 5 menunjukkan performa *single-thread* yang lebih unggul, sebuah aspek penting untuk aplikasi IDS [14]. Sementara itu, Nvidia Jetson Nano, meskipun memiliki GPU yang lebih powerful untuk pemrosesan AI, namun harganya relatif lebih mahal dan performanya untuk tugas-tugas umum tidak lebih baik dari Raspberry Pi 5 [15].

2. **Konektivitas**

   Raspberry Pi 5 dilengkapi dengan *dual-band wireless* 2.4GHz dan 5GHz, serta Bluetooth 5.0, yang memungkinkan konektivitas jaringan yang lebih cepat dan stabil [13]. Hal ini sangat penting untuk memonitor lalu lintas jaringan secara efektif dan mengirimkan peringatan secara *real-time*. Raspberry Pi 4B memiliki keterbatasan pada *single-band wireless*, sementara Orange Pi 5 Pro, meskipun memiliki *dual-band wireless*, namun kualitas dan stabilitas koneksinya masih dipertanyakan [16].

3. **Efisiensi Daya**

   Raspberry Pi 5 dirancang dengan konsumsi daya yang rendah, sehingga cocok untuk diimplementasikan sebagai sistem yang aktif secara terus-menerus tanpa membebani tagihan listrik. Meskipun Nvidia Jetson Nano menawarkan mode daya rendah, namun konsumsi dayanya secara keseluruhan masih lebih tinggi dibandingkan Raspberry Pi 5 [18].

4. **Harga**

   Dibandingkan dengan SBC lain yang memiliki spesifikasi serupa, Raspberry Pi 5 menawarkan harga yang relatif terjangkau. Hal ini menjadikannya pilihan yang ideal untuk pengembangan sistem IDS yang ekonomis, terutama jika dibandingkan dengan Nvidia Jetson Nano yang memiliki harga lebih tinggi.

5. **Kemudahan Pengembangan**

   Raspberry Pi 5 memiliki komunitas pengguna dan pengembang yang sangat

besar, sehingga tersedia banyak sumber daya, tutorial, dan dukungan untuk memudahkan pengembangan dan implementasi sistem IDS [17]. Ekosistem Raspberry Pi yang luas ini memberikan keunggulan dibandingkan SBC lain yang memiliki komunitas yang lebih kecil, termasuk Orange Pi 5 Pro dan Nvidia Jetson Nano.

1.3. Analisis Umum

Aspek analisis yang berkaitan dengan implementasi *Network Security Intrusion Detection System* (IDS) menggunakan Raspberry Pi mencakup beberapa aspek yaitu :

1.3.1. Aspek Teknis

Network security IDS menggunakan Raspberry Pi menawarkan solusi yang terjangkau untuk mendeteksi aktivitas mencurigakan dalam jaringan. Dengan performa dari Raspberry Pi, seperti prosesor yang cepat dan memori yang lebih besar, sistem ini mampu memproses lalu lintas jaringan secara *real-time* pada sekala lingkungan kecil ke menengah dengan 25 hingga 50 perangkat IoT. Implementasi IDS pada perangkat ini memanfaatkan protokol keamanan dan perangkat lunak *open-source* yaitu snort dan suricata, yang memungkinkan deteksi serangan yang efisien dan pemantauan lalu lintas jaringan secara terus-menerus.

1.3.2. Aspek Ekonomi

Penggunaan *platform* IDS memungkinkan mengurangi maupun memitigasi dampak yang ditimbulkan dari serangan *cyber* yang akan merugikan sebuah usaha atau organisasi. IDS dengan Raspberry Pi memberi keuntungan biaya pengadaan dan pemeliharaan perangkat relatif murah, sehingga cocok untuk digunakan oleh usaha dan organisasi kecil dan menengah yang memiliki anggaran terbatas.Dibandingkan dengan perangkat IDPS dari Cisco yang memerlukan biaya 10 juta hingga 40 juta rupiah untuk skala kecil ke menengah solusi ini jauh lebih terjangkau. Selain itu, dengan menggunakan perangkat lunak *open-source*, biaya lisensi dapat ditekan sehingga memungkinkan lebih banyak organisasi untuk meningkatkan keamanan jaringan mereka tanpa biaya yang mahal.

1.3.3. Aspek Hukum dan Regulasi

Dalam implementasi sistem ini membantu memenuhi standar seperti GDPR (*General Data Protection Regulation*) dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam mengatur perlindungan data pribadi . Pengumpulan dan analisis data jaringan dilakukan dengan transparansi penuh untuk memastikan bahwa tidak ada terjadi pelanggaran terhadap hak privasi usaha dan organisasi.

1.3.4. Aspek Keberlanjutan

Penggunaan Raspberry Pi memberikan keuntungan dari segi keberlanjutan karena konsumsi daya perangkat ini sangat rendah dibandingkan dengan perangkat keras IDS lainnya. Selain hemat energi, Raspberry Pi juga dapat digunakan kembali untuk tujuan lain setelah siklus hidup IDS berakhir, yang dapat mengurangi limbah elektronik.

1.3.5. Aspek Lingkungan

Raspberry Pi yang menggunakan *processor* ARM memberikan dampak lingkungan yang lebih rendah. Sistem ARM32 lebih hemat energi daripada CPU x86 dan ARM64 untuk semua metode yang di-*benchmark*, CPU ARM64 lebih hemat energi daripada CPU x86 untuk jumlah inti dan ukuran molekulnya[12]. Konsumsi daya yang rendah dan efisiensi yang tinggi pada *processor* berarti jejak karbon perangkat ini lebih kecil. Selain itu, keberadaan perangkat ini mendorong pemanfaatan energi secara lebih efisien dalam ekosistem keamanan jaringan, yang selaras dengan upaya global untuk mengurangi dampak lingkungan dari teknologi informasi dan komunikasi.

1.4. Kebutuhan yang Harus Dipenuhi

Berdasarkan wawancara dengan user didapatkan beberapa kebutuhan yang harus dipenuhi dalam pembuatan perangkat IoT *Network Security* IDS yaitu menginginkan sebuah sistem yang mampu memantau dan memberi peringatan dini saat terdapat serangan, jika memungkinkan, langsung memblokir serangan seketika saat terjadi serangan terhadap lingkungan jaringan IoT.

Fitur yang Diharapkan:

1. **Pemantauan, deteksi dan *alert* (peringatan) Serangan *Real time*:**

Perangkat mampu melakukan pemantauan ancaman dan deteksi jika terjadi serangan pada lingkup jaringan perangkat IoT dan langsung memberikan *alert* secara *real-time* . Lalu sistem bisa mengetahui berbagai macam logika serangan yang terjadi seperti Dos/DDoS, syn flood, brute force, spoofing, dan malware sehingga responsif saat terjadi serangan yang sesuai.

2. **Penggunaan Hardware Terjangkau, Efisiensi Daya Tinggi dan Daya Tahan Extra:**

   Sistem menggunakan SBC (Single board computer) untuk basis komputer IDS yang memiliki daya komputasi yang cukup dan memiliki efisiensi yang tinggi sehingga cocok untuk menangani jaringan skala kecil lingkup IoT, memiliki harga terjangkau sehingga disarankan menggunakan Raspberry pi 5. Perangkat juga diharapkan memiliki daya tahan extra karena harus bisa ditempatkan dimana dekat dengan pusat jaringan lingkup IoT yang dilindungi, seperti di gudang jaringan maupun ruang server.

3. **Notifikasi Real-Time:**

   Sistem memiliki fitur notifikasi secara langsung kepada administrator menggunakan jaringan jika terdeteksi adanya serangan, sehingga bisa mengambil tindakan lanjutan untuk mitigasi. Sistem notifikasi diharapkan bisa sampai instan dan bisa dikonfigurasi sesuai dengan serangan yang terjadi.

4. **Biaya Terjangkau dan Efisien :**

   Perangkat diharapkan memiliki harga cukup terjangkau dengan anggaran 2 hingga 3 juta rupiah dibandingkan dengan perangkat idps tersendiri yang rentan harga diatas 10 juta rupiah. Dengan menekan biaya dari penggunaan software yang bersifat open source dan konfigurasi hardware yang cukup baik dengan memilih spesifikasi sesuai dengan kebutuhan tidak perlu memilih yang terlalu mahal seperti penggunaan SD Card dibanding SSD sehingga dengan ini, sistem IDS dapat dibuat dengan biaya yang efisien, dan cocok untuk kebutuhan jaringan IoT skala kecil.

1.5. Solusi Sistem yang Diusulkan

1.5.1. Karakteristik Produk

Produk *Intrusion Detection System* (IDS) yang diusulkan memiliki fitur-fitur utama sebagai berikut:

- Deteksi Serangan *Real-time*: IDS mampu mendeteksi ancaman jaringan seperti *malware*, *DDoS*, *port scanning*, dan *password attack* secara *real-time*.

- Peringatan Otomatis: Sistem mengirimkan *alert* kepada administrator ketika mendeteksi aktivitas mencurigakan, sehingga memungkinkan tindakan cepat untuk mengatasi ancaman.
- Kompatibilitas dengan Raspberry Pi: Sistem berjalan pada Raspberry Pi 5, yang merupakan *platform* berbiaya rendah namun mendukung perangkat lunak *open-source* seperti Snort dan Suricata.
- Fleksibilitas pembaruan untuk *Rules*: Sistem mendukung pembaruan *rule*s deteksi ancaman untuk memastikan IDS dapat menyesuaikan kebutuhan dan bisa selalu *up-to-date* dengan ancaman terbaru.

1.5.2. Analisa Solusi yang Ada

- **Solusi *Single Board Computer (SBC)* yang Ada**

  Dalam pemilihan solusi Single Board Computer (SBC) yang ada, perbandingan antara Raspberry Pi 4 Model B, Raspberry Pi 5, Orange Pi 5 Pro, dan Nvidia Jetson Nano dapat membantu dalam menentukan pilihan terbaik sesuai kebutuhan. Raspberry Pi 4 Model B hadir dengan performa yang andal untuk proyek pemula hingga menengah berkat prosesor quad-core dan RAM hingga 8GB, sedangkan Raspberry Pi 5 membawa peningkatan signifikan sebesar 2x-3x pada prosesor dan GPU yang lebih cepat, memberikan kemampuan yang lebih baik untuk proyek yang memerlukan pemrosesan intensif. Di sisi lain, Orange Pi 5 Pro menonjol dengan spesifikasi CPU yang sangat kuat, namun dengan harga yang lebih kompetitif, menawarkan pilihan menarik bagi mereka yang mencari performa tinggi dengan anggaran lebih. Sementara itu, Nvidia Jetson Nano, meskipun relatif lebih mahal, dirancang khusus untuk pengembangan AI dan aplikasi pembelajaran mesin, menjadikannya pilihan unggul untuk proyek yang membutuhkan komputasi yang berat dan pemrosesan grafis yang tinggi. Berikut dibawah tabel 1.1 untuk perbandingan berbagai macam solusi SBC :

Tabel 1.1 Perbandingan SBC

Spesifikasi	**Raspberry Pi 4 Model B**	**Raspberry Pi 5**	**Orange Pi 5 Pro**	**Nvidia Jetson Nano**
Prosesor	✕ Quad-core Cortex-A72, 1.5	✕ Quad-core Cortex-A76, 2.4	✓ Rockchip RK3588S, 8-	✕ Quad-core ARM Cortex-

	GHz	GHz	core (4x Cortex-A76, 4x Cortex-A55)	A57, 1.43 GHz
GPU	✕ VideoCore VI	✕ VideoCore VII	✕ ARM Mali-G610	✓ 128-core NVIDIA Maxwell GPU
RAM	✕ 2 GB, 4 GB, 8 GB LPDDR4	✕ 4 GB atau 8 GB LPDDR4x	✓ 8 GB,16 GB atau 16 GB LPDDR4x	✕ 2 GB atau 4 GB LPDDR4
Penyimpanan	✕ microSD	✓ microSD, M.2 slot	✕ eMMC (opsional), microSD	✕ microSD
Port USB	✕ 2x USB 3.0, 2x USB 2.0	✕ 2x USB 3.0, 2x USB 2.0	✕ 2x USB 3.0, 2x USB 2.0, USB-C (OTG)	✓ 4x USB 3.0
Ethernet	✕ Gigabit Ethernet	✓ Gigabit Ethernet, PCIe untuk LAN tambahan	✕ 2.5G Ethernet	✕ Gigabit Ethernet
Wi-Fi & Bluetooth	✕ Wi-Fi 802.11ac, Bluetooth 5.0	✓ Wi-Fi 6E, Bluetooth 5.2	✕ Wi-Fi 6, Bluetooth 5.0	✕ Wi-Fi 802.11ac, Bluetooth 4.2
Konektivitas Display	✓ 2x micro HDMI (4K @60Hz)	✓ 2x HDMI (4K @60Hz)	✕ HDMI 2.1, DisplayPort via USB-C	✕ Wi-Fi 802.11ac, Bluetooth 4.2
Konsumsi Daya	✕ 5V/3A	✓ 5V/5A	✕ 5V/4A	✕ 5V/4A
Keunggulan Utama	✕ Murah,	✕ Kinerja lebih	✓ Prosesor lebih	✓ GPU lebih kuat,

	komunitas besar	cepat, Wi-Fi 6E	kuat, dukungan eMMC	ideal untuk AI/ML
Harga (perkiraan)	✓ $35 - $75	✕ $60 - $100	✕ $85 - $150	✕ $99 - $129

- **Solusi Perangkat Lunak IDS yang Ada**

Terdapat beberapa pilihan perangkat lunak IDS yang dapat digunakan dan dibandingkan untuk menentukan pilihan terbaik dalam penggunaan ids, yaitu Snort, Suricata dan zeek. Berikut adalah perbandingannya :

1) Solusi 1: Snort

Gambar 1.1. Logo Snort

Gambar 1.1 diatas adalah logo Snort yang merupakan perangkat lunak yang akan memberikan peringatan ketika terjadi penyusupan ke dalam sistem komputer. Snort dapat meminimalisir serangan-serangan yang terjadi di dalam sistem jaringan komputer dengan cara memberikan *alert* atau peringatan kepada administrator jika ada kegiatan yang mencurigakan[8].

Snort adalah sebuah aplikasi yang memiliki fungsi dapat mencegah intrusi dan serangan jaringan. Snort adalah penggabungan dari *system analysis protocol* dan sistem pendeteksi penyusupan, hal ini sangatlah bermanfaat untuk mendeteksi serangan terhadap host dalam jaringan serta trafik-trafik dan *logging* paket-paket secara *real time* dalam jaringan berbasis TCP/IP[9].

- **Karakteristik :**

1. *Single-threaded*, lebih ringan dan cocok untuk jaringan skala kecil hingga menengah;
2. Mendukung berbagai jenis deteksi serangan, namun terbatas pada satu inti CPU;

3. Memiliki komunitas besar dan didukung oleh Cisco;
4. kurang optimal pada jaringan yang lebih besar atau padat.

2) Solusi 2: Suricata

Gambar 1.2. Logo Suricata

Suricata merupakan IDS, IPS, dan alat monitoring keamanan jaringan yang berbasis open-source. Memiliki logo seperti gambar 1.2 diatas, Suricata adalah sebuah tool keamanan jaringan dengan performa tinggi yang memiliki kemampuan *multi-threaded*. Suricata mampu mendeteksi gangguan secara *realtime*, pencegahan intrusi *inline*, pemantauan keamanan jaringan, dan pemrosesan PCAP *offline*. Suricata memerikas *traffic* jaringan menggunakan *rules* dan *signature* yang kuat dan *Lua scripting* untuk mendukung pendeteksianan serangan yang kompleks[10].

- **Karakteristik :**

1. *Multi-threaded*, mampu menggunakan beberapa inti CPU, sehingga lebih cocok untuk jaringan besar atau padat;
2. Suricata memiliki kemampuan lebih dalam inspeksi lebih mendalam dengan dukungan skrip;
3. Dikembangkan oleh *Open Information Security Foundation (OISF)*, namun komunitasnya lebih kecil dibandingkan Snort;
4. Memerlukan lebih banyak sumber daya komputasi, sehingga mungkin kurang cocok untuk platform seperti Raspberry Pi dalam pengaturan kecil.

3) Solusi 3: Zeek (Bro):

Gambar 1.3. Logo Zeek

Zeek (sebelumnya dikenal sebagai Bro) seperti gambar 1.3 dimana logonya sudah berubah tidak lagi bro, adalah program pemantauan jaringan dan deteksi intrusi. bekerja menangkap dan mengurai lalu lintas jaringan pada intinya dan menyediakan bahasa skrip yang kuat untuk menganalisis lalu lintas lebih lanjut dengan skrip khusus, berdasarkan hal ini, Zeek mengekspos dirinya sebagai platform dengan kemampuan untuk mengkorelasikan berbagai informasi baik dari host dan peristiwa jaringan [11].

- **Karakteristik :**

1. **L**ebih berfokus pada analisis protokol jaringan daripada deteksi serangan secara *real-time* seperti Snort atau Suricata;
2. Zeek menggunakan pendekatan berbasis *event-driven* dan mampu mengolah data jaringan secara mendalam dengan kinerja yang relatif baik pada jaringan besar.
3. Zeek tidak hanya mendeteksi serangan, tetapi juga mengumpulkan dan menganalisis metadata jaringan.
4. Dikembangkan oleh komunitas akademik dan perusahaan keamanan besar.
5. Zeek lebih boros dalam hal penggunaan sumber daya, dan cenderung lebih kompleks untuk dikonfigurasi dibandingkan Snort atau Suricata.
6. Meskipun mampu menangani jaringan besar, Zeek kurang ideal untuk deteksi serangan *real-time* dan lebih berfokus pada pemantauan aktivitas dan pencatatan data jaringan.

Berikut adalah perbandingan dari usulan solusi software IDS pada tabel 1.2 :

Tabel 1.2. Perbandingan Usulan Solusi

Fitur	Snort	Suricata	Zeek (Bro)
Kinerja di Raspberry Pi	✓ (Dapat berjalan dengan baik pada Raspberry Pi, lebih ringan)	✕ (Lebih berat karena *multi-threading*)	✕ (Lebih berat dan memerlukan lebih banyak sumber daya)
Kompatibilitas Sistem Operasi	✓ (Kompatibel dengan	✓ (Kompatibel, namun	✓ (Kompatibel, tapi

	banyak distribusi Linux termasuk Raspberry Pi OS)	lebih kompleks untuk diatur)	pengaturannya memerlukan lebih banyak perhatian)
Penggunaan Sumber Daya CPU	✓ (Lebih ringan pada CPU, cocok untuk Raspberry Pi)	✕ (Menggunakan lebih banyak CPU)	✕ (Lebih berat di CPU karena analisis protokol mendalam)
Penggunaan Memori	✓ (Memori yang lebih efisien pada perangkat berdaya rendah)	✕ (Membutuhkan lebih banyak RAM)	✕ (Memerlukan RAM yang lebih besar untuk proses analisis)
Konfigurasi dan Dokumentasi	✓ (Dokumentasi dan komunitas luas, lebih mudah diatur untuk pemula)	✓ (Dokumentasi baik, namun lebih rumit untuk pengaturan)	✓ (Dokumentasi lengkap, tapi lebih rumit dibandingkan Snort)
Kemampuan Deteksi *Real-time*	✓ (Sangat baik dalam mendeteksi serangan berbasis *signature*)	✓ (Bisa lebih cepat, terutama dengan *multi-threading*)	✕ (Fokus lebih pada pengumpulan data protokol daripada deteksi serangan langsung)
Kemudahan Pengaturan di Raspberry Pi	✓ (Pengaturan relatif mudah, didukung oleh komunitas Raspberry Pi)	✕ (Pengaturan lebih kompleks)	✕ (Pengaturan cukup kompleks dan memerlukan konfigurasi lanjutan)

Dukungan untuk Perangkat Kecil dan Berdaya Rendah	✓ (Sangat sesuai untuk perangkat kecil seperti Raspberry Pi)	✕ (Tidak dioptimalkan untuk perangkat kecil)	✕ (Kurang ideal untuk perangkat berdaya rendah)
Ekosistem Dukungan dan Pengembangan	✓ (Didukung oleh Cisco, komunitas luas, banyak tutorial)	✓ (Dikembangkan oleh OISF, komunitas juga baik tapi lebih fokus pada *enterprise*)	✓ (Dikembangkan oleh OISF, komunitas juga baik tapi lebih fokus pada *enterprise*)
Fleksibilitas dalam *Rule Writing*	✓ (Lebih banyak rule tersedia di komunitas)	✓ (Fleksibel, namun lebih kompleks)	✓ (Sangat fleksibel, karena analisis berbasis skrip)
Kemampuan Deteksi *Malware*	✓ (Dapat mendeteksi *malware* dengan *signature-based detection*, namun butuh aturan khusus)	✓ (Lebih baik dalam deteksi *malware* dengan dukungan *deep packet inspection*)	✓ (Memiliki kemampuan analisis berbasis kejadian, yang bisa mendeteksi perilaku mencurigakan)
Kemampuan Menahan Serangan *Malware*	✕ (Fokus utama pada deteksi, tidak dapat menahan atau memblokir serangan secara langsung)	✓ (Dapat dikonfigurasi untuk mencegah serangan jika diintegrasikan dengan sistem *firewall*)	✕ (Lebih bersifat pasif, mendeteksi dan menganalisis serangan, tidak untuk pencegahan langsung)

1.6. Kesimpulan

Saat ini terjadi peningkatan ancaman siber yang menargetkan berbagai perangkat digital sehingga kebutuhan akan solusi keamanan jaringan yang efektif dan terjangkau menjadi sangat mendesak. Solusi tradisional sering gagal menangani serangan canggih, yang membuka peluang bagi penggunaan IDS berbasis *open-source software* seperti Snort, Suricata dan Zeek pada platform Raspberry Pi 5. Penelitian ini menekankan kompleksitas masalah keamanan jaringan yang dihadapi, terutama kerentanan pada perangkat IoT dan tantangan dalam menghadapi serangan yang terus berkembang. IDS berbasis Raspberry Pi dipilih karena fleksibilitasnya, biaya rendah, dan kemampuannya dalam mendeteksi ancaman secara real-time, meskipun ada beberapa keterbatasan terkait performa dan sumber daya yang perlu dioptimalkan. Penelitian ini juga mengidentifikasi kebutuhan penting dalam sistem deteksi intrusi seperti kemampuan deteksi serangan secara real-time, fleksibilitas dalam konfigurasi, serta integrasi dengan menggunakan sistem notifikasi yang efektif. Secara keseluruhan, pengembangan IDS menggunakan Raspberry Pi 5 menawarkan solusi yang menjanjikan untuk meningkatkan keamanan jaringan IoT dengan pendekatan yang ekonomis dan praktis yang cocok untuk usaha atau organisasi dengan skala kecil hingga menengah.