BAB 4
HASIL PENELITIAN

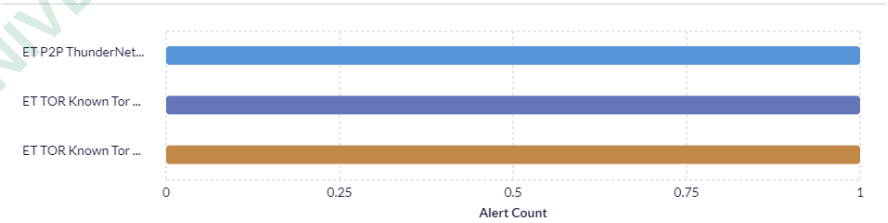
4.1 RINGKASAN HASIL PENELITIAN

Penelitian ini memanfaatkan DynamiteLab untuk menganalisis trafik jaringan di Kampus 1 UNJAYA. Hasilnya mengungkapkan pola trafik dan anomali mencurigakan, seperti aktivitas yang terkait dengan protokol P2P *ThunderNetwork* dan jaringan Tor. Sebagian besar peringatan dipicu oleh protokol TCP, sedangkan UDP menyumbang sisanya. Kategori peringatan utama meliputi *Misc Attack* dan *Potential Corporate Privacy Violation*, yang menunjukkan adanya ancaman dan risiko pelanggaran privasi. Host internal (172.16.11.32) dan eksternal (108.137.182.98) menjadi titik fokus, dengan host internal menghasilkan peringatan terbanyak. Protokol TCP dan UDP adalah sumber utama peringatan, yang mengindikasikan perlunya perhatian lebih lanjut terhadap ancaman potensial.

4.2 ANALISIS POLA TRAFIK DAN ANOMALI

Berdasarkan analisis yang dilakukan menggunakan DynamiteLab, diperoleh hasil berupa pola trafik dan deteksi anomali pada jaringan yang sedang dianalisis.

4.2.1 Distribusi Peringatan Berdasarkan Jumlah



Rule	Count
ET P2P ThunderNetwork UDP Traffic	1
ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 861	1
ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 432	1

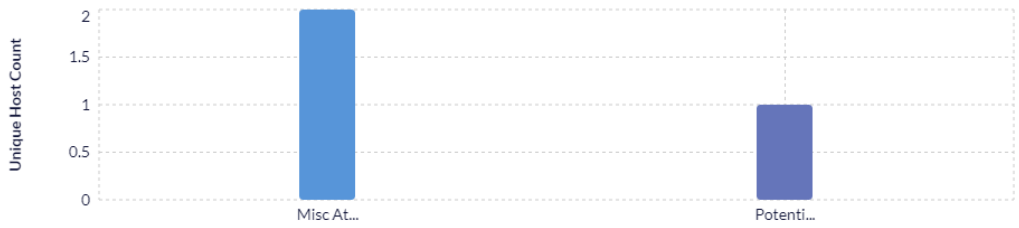
Gambar 4.1 *Top Rules by Alert Count*

Pada Gambar 4. 1 menampilkan hasil analisis lalu lintas jaringan dan menampilkan aturan teratas berdasarkan jumlah peringatan. Berikut adalah penjelasan detailnya:

1. Grafik Bar
    a. *ET P2P ThunderNetwork UDP Traffic*: Lalu lintas UDP yang terkait dengan jaringan P2P *ThunderNetwork*.
    b. *ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 861*: Lalu lintas yang terkait dengan *node relay/router Tor* yang dikenal, bukan *exit node*, dalam grup 861.
    c. *ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 432*: Lalu lintas yang terkait dengan *node relay/router Tor* yang dikenal, bukan exit node, dalam grup 432.
2. Interpretasi
    a. *ET P2P ThunderNetwork UDP Traffic* adalah aturan yang mendeteksi lalu lintas dari protokol P2P yang menggunakan ThunderNetwork, yang mungkin dianggap sebagai aktivitas mencurigakan dalam konteks tertentu.
    b. *ET TOR Known Tor Relay/Router (Not Exit) Node Traffic* menunjukkan adanya lalu lintas melalui jaringan Tor yang dikenal, tetapi melalui node relay atau router yang bukan exit node, yang dapat menandakan penggunaan Tor untuk menyembunyikan asal atau tujuan dari lalu lintas tersebut.

DynamiteLab mendeteksi adanya aktivitas jaringan yang terkait dengan protokol P2P dan jaringan Tor, yang menunjukkan aktivitas mencurigakan atau penyalahgunaan jaringan di UNJAYA.

4.2.2 Kategori Peringatan Teratas



Category	Count
Misc Attack	2
Potential Corporate Privacy Violation	1

Gambar 4.2 *Top Alert Categories by Alert Count*

Gambar 4.2 menunjukkan hasil analisis dari DynamiteLab yang menyoroti kategori peringatan teratas berdasarkan jumlah peringatan yang muncul. Berikut adalah penjelasan lebih detail mengenai gambar tersebut:

1. Grafik batang horizontal menunjukkan kategori peringatan *(alert categories)* yang paling sering muncul, dihitung berdasarkan jumlah host unik yang terhubung dengan kategori tersebut. Ada dua kategori utama yang diidentifikasi:
   a. *Misc Attack*: Kategori ini terkait dengan 2 unique host count, yang berarti dua host telah memicu peringatan di bawah kategori ini.
   b. *Potential Corporate Privacy Violation*: Kategori ini terkait dengan 1 unique host count, yang menunjukkan satu host yang terlibat dalam potensi pelanggaran privasi perusahaan.
2. Interpretasi
   a. *Misc Attack*: Kategori ini kemungkinan mencakup berbagai serangan atau aktivitas mencurigakan yang tidak secara spesifik diklasifikasikan. Dengan dua host unik yang terlibat, hal ini bisa menunjukkan adanya aktivitas serangan umum di jaringan.
   b. *Potential Corporate Privacy Violation*: Kategori ini mengindikasikan potensi pelanggaran privasi yang bisa merugikan perusahaan, seperti akses atau penyebaran data sensitif. Fakta bahwa

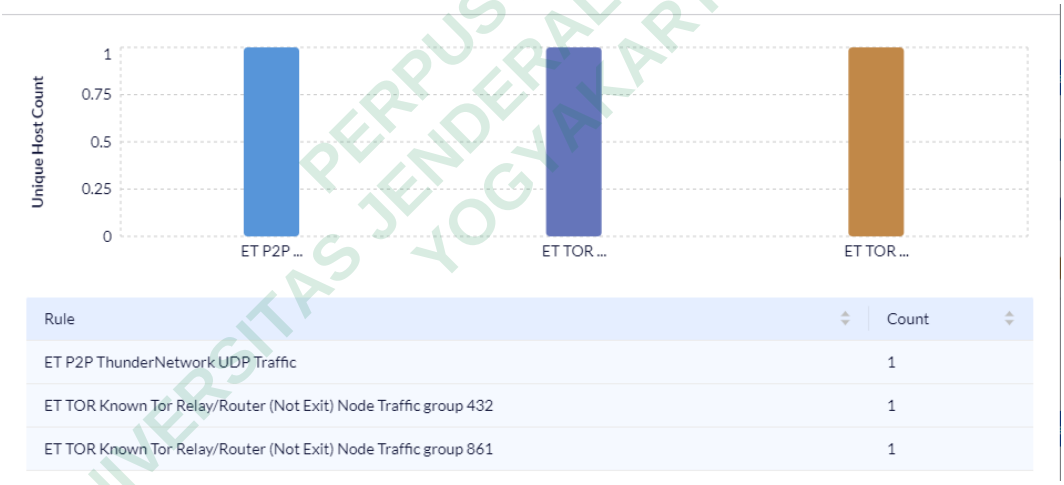
ada satu host unik yang terlibat menunjukkan adanya risiko keamanan yang signifikan.

DynamiteLab mengidentifikasi dua kategori ancaman penting: satu terkait dengan serangan umum dan yang lainnya dengan potensi pelanggaran privasi. Organisasi perlu segera mengambil langkah untuk menilai dan menangani host yang terlibat dalam aktivitas ini guna mencegah risiko lebih lanjut terhadap keamanan jaringan dan privasi data perusahaan di UNJAYA.

4.3 DETEKSI AKTIVITAS MENCURIGAKAN

Dalam upaya mendeteksi aktivitas mencurigakan pada jaringan, salah satu cara yang efektif adalah dengan menganalisis aturan peringatan yang diterapkan serta mengidentifikasi host yang paling sering menghasilkan peringatan.

4.3.1 Peringatan Berdasarkan Jumlah Host Unik



Rule	Count
ET P2P ThunderNetwork UDP Traffic	1
ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 432	1
ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 861	1

Gambar 4.3 *Top Rules by Unique Host Count*

Gambar 4.3 merupakan hasil analisis dari DynamiteLab yang menampilkan aturan teratas berdasarkan jumlah host unik yang memicu peringatan. Berikut penjelasan rinci mengenai gambar tersebut:

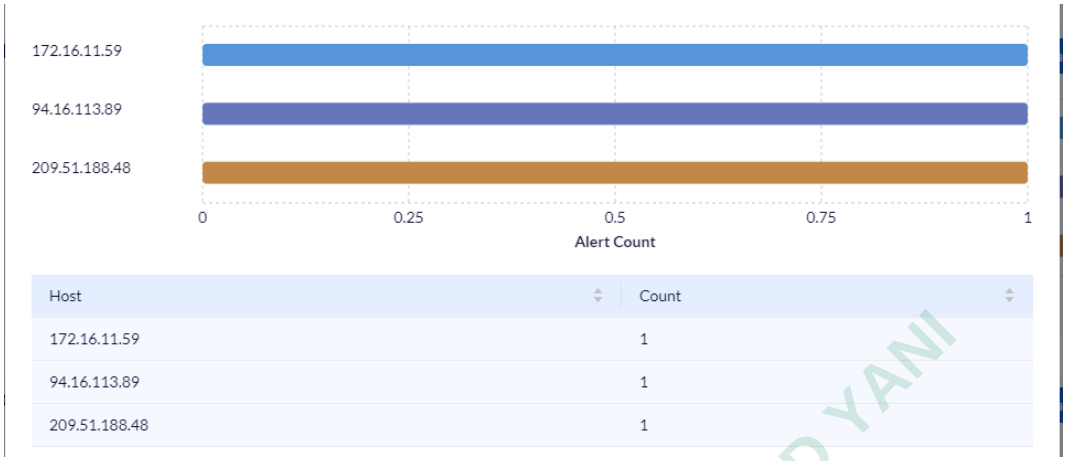
1. Grafik ini menampilkan tiga aturan (rules) yang paling sering memicu peringatan, dihitung berdasarkan jumlah host unik yang terhubung dengan aturan tersebut. Masing-masing aturan dipicu oleh satu host unik. Ketiga aturan tersebut adalah:

a. *ET P2P ThunderNetwork UDP Traffic*: Lalu lintas UDP yang terkait dengan jaringan *P2P ThunderNetwork*.
b. *ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 432:* Lalu lintas yang terkait dengan *node relay/router Tor* yang dikenal, namun bukan *exit node*, dalam grup 432.
c. *ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group* 861: Lalu lintas yang terkait dengan node *relay/router Tor* yang dikenal, namun bukan *exit node*, dalam grup 861.

2. Interpretasi:
   a. *ET P2P ThunderNetwork UDP Traffic:* Deteksi lalu lintas ini mengindikasikan penggunaan protokol P2P ThunderNetwork, yang mungkin dianggap mencurigakan atau ilegal tergantung pada kebijakan keamanan.
   b. *ET TOR Known Tor Relay/Router (Not Exit) Node Traffic*: Lalu lintas yang melalui node *relay/router Tor* yang dikenal, namun bukan exit node, menunjukkan penggunaan jaringan Tor, yang sering digunakan untuk menyembunyikan asal atau tujuan lalu lintas, sehingga bisa menjadi tanda adanya upaya untuk menyamarkan identitas atau tujuan sebenarnya.

DynamiteLab mengidentifikasi tiga aturan utama yang terkait dengan aktivitas jaringan, masing-masing dipicu oleh satu host unik. Ini menunjukkan adanya aktivitas yang melibatkan jaringan P2P dan Tor di UNJAYA, yang mungkin memerlukan perhatian lebih lanjut untuk memastikan tidak ada penyalahgunaan atau risiko keamanan yang signifikan.

4.3.2 Host yang Paling Sering Memicu Peringatan



Host	Count
172.16.11.59	1
94.16.113.89	1
209.51.188.48	1

Gambar 4.4 *Top Alert-Generating Hosts*

Gambar 4.4 menampilkan hasil analisis menggunakan DynamiteLab pada kategori "*Top Alert-Generating Hosts.*" Grafik batang horizontal dan tabel menunjukkan host atau alamat IP di jaringan yang paling banyak memicu alert.

1. Host 172.16.11.59, 94.16.113.89, dan 209.51.188.48: Masing-masing host ini menghasilkan satu alert, yang berarti bahwa ketiganya terlibat dalam aktivitas jaringan yang dianggap mencurigakan atau berpotensi berbahaya.
2. Interpretasi : Meskipun tidak ada satu host yang secara dominan memicu banyak alert, setiap host yang memicu alert tetap memerlukan investigasi lebih lanjut. Hal ini penting untuk memastikan apakah aktivitas tersebut mengindikasikan potensi ancaman keamanan yang lebih besar atau hanya anomali yang tidak berbahaya.

Secara keseluruhan, DynamiteLab memberikan indikasi bahwa setiap host yang memicu alert memerlukan pemeriksaan lebih lanjut untuk menentukan apakah ada potensi risiko keamanan yang perlu ditindaklanjuti.

4.4 Evaluasi dan Analisis Ancaman

Pada bagian ini, akan dilakukan evaluasi terhadap protokol serta host yang terlibat dalam memicu dan menerima peringatan keamanan, berdasarkan data yang tersedia.

4.4.1 Protokol yang Paling Sering Memicu Peringatan

TCP 66.67%
UDP 33.33%

Protocol	Count
TCP	2
UDP	1

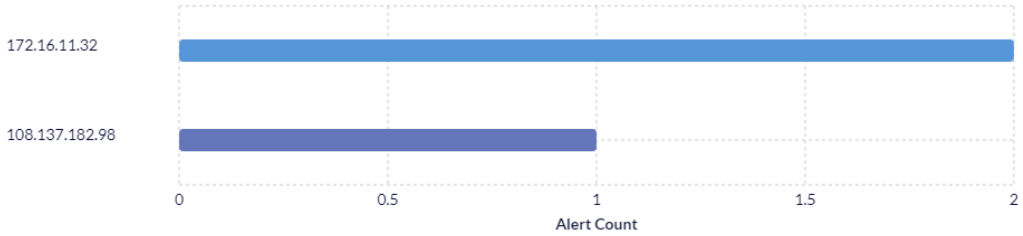
Gambar 4.5 *Top Alert Generating Protocols*

Gambar 4.5 memperlihatkan protokol-protokol jaringan yang paling banyak memicu peringatan berdasarkan analisis file PCAP. Dalam gambar ini, ada dua protokol utama yang menjadi sumber alert:

1. *TCP (Transmission Control Protocol):*
   a. Menyumbang 66,67% dari total peringatan yang terdeteksi.
   b. Protokol TCP menghasilkan 2 peringatan.
2. UDP *(User Datagram Protocol):*
   a. Menyumbang 33,33% dari total peringatan yang terdeteksi.
   b. Protokol UDP menghasilkan 1 peringatan.

Dari data ini, dapat disimpulkan bahwa mayoritas aktivitas mencurigakan atau anomali yang terdeteksi di jaringan melibatkan protokol TCP, diikuti oleh UDP. Analisis lebih mendalam terhadap lalu lintas yang menggunakan kedua protokol ini dapat membantu mengidentifikasi potensi ancaman atau masalah keamanan pada jaringan yang dianalisis.

4.4.2 Host yang Paling Sering Menerima Peringatan



Host	Count
172.16.11.32	2
108.137.182.98	1

Gambar 4.6 *Top Alert-Receiving Hosts*

Gambar 4.6 menampilkan hasil analisis yang mengidentifikasi host (alamat IP) dalam jaringan yang menerima peringatan terbanyak. Berikut rincian hasil dari grafik dan tabel yang ditampilkan:

1. Host 172.16.11.32:
   a. Menerima 2 peringatan.
   b. Host ini adalah yang paling banyak menerima peringatan di antara host yang dianalisis.
2. Host 108.137.182.98:
   a. Menerima 1 peringatan.
   b. Meskipun menerima lebih sedikit peringatan dibandingkan host pertama, host ini tetap menjadi salah satu dari dua host dengan jumlah peringatan terbanyak.

Analisis ini menunjukkan bahwa host dengan IP 172.16.11.32 lebih rentan atau lebih terlibat dalam aktivitas yang memicu peringatan keamanan dibandingkan host lainnya. Ini bisa menjadi tanda adanya potensi ancaman atau aktivitas mencurigakan yang perlu diperiksa lebih lanjut dalam analisis keamanan jaringan.

4.5 PEMBAHASAN

Bagian ini membahas hasil deteksi ancaman dan anomali yang ditemukan selama penelitian, serta mengevaluasi relevansi dan keterbatasan penelitian dalam konteks keamanan jaringan. Selain itu, rekomendasi pengembangan sistem juga diberikan untuk meningkatkan efektivitas deteksi ancaman dan mitigasi risiko di masa mendatang.

4.5.1 Analisis Hasil Deteksi Ancaman dan Anomali

Berikut tabel 4.1 menunjukkan hasil analisis parameter dan alert dari deteksi ancaman dan anomali jaringan.

Tabel 4.1 Hasil Analisis Parameter dan Alert Jaringan

Parameter	**Alert**		
Timestamp	7/26/2024 10:07:09 AM	7/26/2024 10:07:09 AM	7/26/2024 10:07:13 AM
Source IP	172.16.11.59	94.16.113.89	209.51.188.48
Destination IP	108.137.182.98	172.16.11.32	172.16.11.32
Source Port	44527	9003	443
Transport Protocol	UDP	TCP	TCP
Signature Name	ET P2P ThunderNetwork UDP Traffic	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 861	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 432
Alert Description	Potential Corporate Privacy Violation	Misc Attack	Misc Attack
Severity	High	Medium	Medium

Parameter	Alert		
Signature ID	2009099	2522860	2522431

Dari tabel 4.1 menunjukan hasil penelitian bahwa protokol TCP dan UDP menjadi sumber utama peringatan pada jaringan yang dianalisis. Hal ini menegaskan bahwa meskipun TCP merupakan protokol yang andal untuk komunikasi jaringan, sifatnya yang kompleks membuatnya lebih rentan terhadap eksploitasi, terutama dalam bentuk serangan berbasis koneksi seperti DoS. Sedangkan UDP, yang digunakan untuk komunikasi tanpa koneksi, berkontribusi terhadap sisa peringatan, menunjukkan potensi ancaman dari transfer data yang lebih cepat namun kurang terlindungi.

Selain itu, analisis terhadap host yang terlibat menunjukkan bahwa host internal (172.16.11.32) dan host yang terpapar internet (108.137.182.98) menerima peringatan yang signifikan. Ini mengindikasikan adanya potensi serangan dari luar serta perlunya penguatan keamanan internal. Host internal ini kemungkinan besar merupakan target penting dalam jaringan yang harus dilindungi dengan langkah-langkah keamanan yang lebih kuat, seperti firewall dan segmentasi jaringan.

Penemuan utama:

1. Protokol TCP: Terlibat dalam sebagian besar peringatan dan membutuhkan peningkatan pengawasan serta penanganan terhadap potensi serangan berbasis koneksi.
2. Protokol UDP: Meskipun tidak dominan, tetap harus diperhatikan karena karakteristiknya yang rentan terhadap serangan seperti *UDP flood*, terutama karena adanya alert dengan tingkat keparahan tinggi.
3. Host Internal dan Eksternal: Menjadi sasaran utama, membutuhkan audit keamanan yang lebih mendalam dan mitigasi terhadap potensi ancaman dari luar dan dalam jaringan.

4.5.2 Relevansi dan Keterbatasan Penelitian

Penelitian ini memiliki relevansi penting dalam evaluasi keamanan jaringan, terutama dalam mendeteksi anomali dan ancaman melalui analisis file PCAP. Temuan dari penelitian ini memberikan wawasan tentang potensi ancaman yang mungkin dihadapi oleh jaringan Kampus 1 UNJAYA, serta langkah-langkah pencegahan yang perlu diambil untuk meningkatkan keamanan jaringan. Penelitian ini berhasil mengidentifikasi ancaman-ancaman kunci yang dapat merusak keamanan jaringan, serta menggunakan DynamiteLab untuk melakukan analisis mendalam terhadap aktivitas mencurigakan, yang memberikan informasi berharga untuk perbaikan keamanan.

Namun, terdapat beberapa keterbatasan dalam penelitian ini. Hasilnya sangat bergantung pada file PCAP yang digunakan, dan jika dataset yang dianalisis tidak mencakup seluruh aktivitas jaringan, maka hasilnya mungkin tidak sepenuhnya representatif. Selain itu, penggunaan satu alat analisis seperti DynamiteLab dapat membatasi sudut pandang dalam memahami ancaman secara komprehensif. Oleh karena itu, penggunaan beberapa alat deteksi ancaman yang lebih beragam agar dapat memberikan hasil yang lebih akurat dan menyeluruh.