BAB I
PENDAHULUAN

1.1 Latar Belakang

Meningkatnya ketergantungan terhadap jaringan komputer dan layanan digital di bidang pendidikan, pemerintahan, serta dunia usaha telah menempatkan stabilitas dan keamanan jaringan sebagai prioritas utama. Menurut Yoachimik et al., data dari laporan keamanan internasional menunjukkan bahwa terjadi lebih dari 6,6 juta serangan DDoS selama tahun 2024, dengan jumlah kejadian yang naik dari 274.000 kasus pada awal 2023 menjadi 512.000 kasus pada akhir 2024, yang mengindikasikan peningkatan ancaman yang berkelanjutan [1]. Kenaikan ini menyoroti pentingnya adanya sistem pengawasan jaringan yang dapat mengidentifikasi penyimpangan lalu lintas secara langsung, meneliti pola serangan, serta memberikan data yang tepat kepada pengelola untuk menghindari gangguan layanan atau hambatan operasional.

Di lingkungan kampus, beban lalu lintas jaringan mengalami peningkatan seiring dengan bertambahnya jumlah perangkat dan layanan berbasis internet, seperti Sistem Manajemen Pembelajaran (LMS), aplikasi administrasi, serta sistem akademik. Penelitian kasus yang dilakukan di Gedung GKB Fakultas Ekonomi dan Bisnis UPN "Veteran" Jawa Timur menunjukkan adanya peningkatan latensi dan penurunan throughput pada saat jam sibuk, yang pada akhirnya mengganggu kegiatan akademik dan administrasi [2]. Penerapan PRTG Network Monitor dalam penelitian tersebut memungkinkan identifikasi titik kemacetan, sedangkan analisis dengan menggunakan Wireshark mengungkap paket anomali serta kesalahan konfigurasi yang tidak terdeteksi pada dasbor monitoring. Keadaan ini memerlukan pentingnya penggunaan instrumen monitoring yang sesuai untuk mendukung proses pendeteksian dan analisis lalu lintas jaringan sesuai dengan kebutuhan operasional [3].

Namun demikian, kebanyakan penelitian terdahulu hanya mengkaji PRTG dan Wireshark secara terpisah. Misalnya, penelitian tentang PRTG menitikberatkan

pada indikator keseluruhan seperti latency, throughput, packet loss, serta efektivitas pengawasan dalam situasi normal atau puncak beban [2], sedangkan penelitian terkait Wireshark diterapkan untuk paket, pemeriksaan protokol, serta identifikasi sniffing atau penyimpangan data [4]. Penelitian perbandingan langsung di antara keduanya masih sangat sedikit; Hanya ada beberapa kajian seperti "*A Comparative Study Between Wireshark and Paessler Router Traffic Grapher (PRTG) in Network Monitoring and Analysis*" yang bertujuan menilai perbedaan kemampuan monitoring dan analisis masing-masing alat [3]. Ketiadaan data empiris kuantitatif pada berbagai kondisi lalu lintas baik normal, padat, maupun yang melibatkan pola serangan menjadikan penelitian perbandingan yang semakin krusial untuk memberikan panduan yang objektif kepada pengelola jaringan.

Penelitian berjudul *"Analisis Perbandingan Performa PRTG Network Monitor dan Wireshark dalam Deteksi dan Analisis Trafik Jaringan"* ini disusun untuk menjawab kesenjangan penelitian yang ada dengan melakukan evaluasi komparatif antara kedua alat berdasarkan sejumlah parameter teknis, seperti *throughput, latency* atau *response time, packet loss*, efektivitas pendeteksian anomali maupun serangan, kemampuan filtering trafik, serta tingkat kedalaman analisis paket. Kajian ini diharapkan mampu menghasilkan rekomendasi berbasis data empiris mengenai kondisi penggunaan yang paling tepat untuk masing-masing alat, sekaligus menjelaskan bagaimana keduanya dapat saling melengkapi dalam penerapan strategi monitoring dan keamanan jaringan yang lebih adaptif. Seiring meningkatnya kompleksitas arsitektur jaringan dan tingginya risiko serangan siber pada berbagai sektor, temuan dari penelitian ini menjadi sangat penting untuk mendukung praktik pengelolaan jaringan modern. Oleh karena itu, penelitian lebih lanjut diperlukan guna memperluas cakupan skenario, memperdalam analisis, dan memperkaya pemahaman mengenai efektivitas berbagai perangkat monitoring dalam menghadapi dinamika trafik jaringan yang terus berkembang.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalah dalam penelitian ini sebagai berikut :

1. Parameter teknis apa saja yang digunakan untuk mengukur efektivitas PRTG Network Monitor dan Wireshark dalam deteksi dan analisis trafik jaringan, khususnya terkait *throughput*, *latency/response* time, *packet loss*, efektivitas deteksi anomali atau serangan, kemampuan *filtering*, serta kedalaman analisis paket?
2. Bagaimana perbandingan kinerja PRTG Network Monitor dan Wireshark berdasarkan parameter *throughput*, *latency/response time*, *packet loss*, efektivitas deteksi anomali atau serangan, kemampuan *filtering*, dan kedalaman analisis paket pada kondisi trafik normal, trafik padat (bottleneck), dan trafik yang mengandung pola serangan DDoS skala uji?
3. Pada setiap skenario lalu lintas jaringan, baik dalam kondisi normal, padat, maupun yang mengandung pola serangan, perlu dilakukan analisis komparatif terhadap alat yang digunakan untuk menentukan kemampuan deteksi dini serta tingkat akurasi analisis anomali dan serangan jaringan. Selain itu, penelitian ini juga bertujuan untuk mengidentifikasi sejauh mana kedua alat tersebut dapat saling melengkapi dalam meningkatkan efektivitas strategi pemantauan dan penguatan keamanan jaringan di lingkungan institusi pendidikan maupun organisasi perusahaan?

1.3 Batasan Masalah

Penelitian ini memiliki beberapa batasan agar pembahasan tetap terarah dan tidak melebar ke luar ruang lingkup yang ditetapkan. Batasan masalah dalam penelitian ini adalah sebagai berikut :

1. Batasan Ruang Lingkup Penelitian

   Penelitian ini dibatasi pada lingkungan jaringan lokal (LAN) yang dibangun dalam bentuk simulasi, sehingga seluruh proses pengujian dilakukan pada skenario yang terkontrol dan tidak melibatkan jaringan

operasional berskala besar. Fokus penelitian tidak mencakup jaringan produksi (*real environment*), jaringan perusahaan dengan arsitektur kompleks, maupun infrastruktur berbasis cloud. Dengan demikian, hasil analisis yang diperoleh terutama menggambarkan performa perangkat monitoring pada kondisi LAN dasar yang umum digunakan di lingkungan kampus atau organisasi kecil.

2. Batasan pada Penggunaan PRTG Network Monitor

Pada penelitian ini, penggunaan PRTG Network Monitor dibatasi hanya pada konfigurasi sensor berbasis SNMP dan Flow seperti NetFlow atau *sFlow* sebagai mekanisme utama dalam proses pemantauan jaringan. Parameter yang diamati melalui PRTG difokuskan pada tiga indikator teknis, yaitu *throughput*, *latency/response time*, serta *packet loss*, sehingga analisis performa yang dilakukan tetap berada dalam ruang lingkup monitoring dasar yang relevan dengan tujuan penelitian. Penelitian ini tidak mencakup pengujian fitur PRTG lainnya, seperti integrasi multi-WAN, kemampuan clustering, integrasi cloud, maupun manajemen pengguna tingkat lanjut, karena fitur tersebut dianggap berada di luar fokus penelitian dan tidak memberikan pengaruh signifikan terhadap perbandingan yang dilakukan.

3. Batasan pada Penggunaan Wireshark

Penggunaan Wireshark dalam penelitian ini dibatasi hanya pada fungsi dasar penangkapan dan analisis paket yang mencakup proses *packet sniffing*, penyaringan paket (*filtering*), pembacaan protokol, serta analisis statistik sederhana. Penelitian tidak mencakup penggunaan fitur lanjutan seperti integrasi dengan sistem *network forensics*, analisis lalu lintas terenkripsi secara mendalam, otomatisasi deteksi serangan, maupun penggunaan plugin eksternal. Selain itu, proses analisis paket difokuskan pada data yang diperoleh dari jaringan LAN simulasi tanpa melibatkan perangkat atau sistem yang berada di luar lingkungan pengujian tersebut.

4. Lingkup Skenario Pengujian

Skenario pengujian yang digunakan dibatasi pada kondisi jaringan

lokal yang disimulasikan dengan jumlah perangkat yang terbatas, seperti beberapa klien, satu server, serta perangkat jaringan pendukung. Pengujian tidak mencakup arsitektur jaringan yang kompleks atau berskala besar seperti topologi multi-site, jaringan backbone, ataupun jaringan dengan segmentasi VLAN tingkat lanjut. Trafik yang diuji juga hanya meliputi protokol umum seperti HTTP, DNS, dan ICMP sebagai representasi layanan web, layanan nama domain, dan kontrol jaringan. Beban trafik dibangkitkan dalam rentang tertentu yang masih sesuai dengan kapasitas lingkungan simulasi, sehingga tidak digunakan skenario dengan trafik berintensitas tinggi yang biasanya ditemukan dalam jaringan operasional berskala besar.

5. Batasan pada Jenis Trafik dan Ruang Lingkup Analisis

   Penelitian tidak menganalisis trafik yang dienkripsi menggunakan protokol keamanan canggih seperti TLS versi terbaru, sehingga proses inspeksi paket terbatas pada trafik yang tidak terenkripsi. Selain itu, penelitian tidak membahas integrasi kedua alat dengan layanan berbasis cloud, sistem deteksi intrusi (IDS/IPS), atau platform keamanan terpadu lainnya. Analisis hanya difokuskan pada parameter teknis seperti *throughput*, *latency*, *packet loss*, ketepatan deteksi anomali, dan kemampuan filtering paket. Dengan demikian, hasil penelitian terutama relevan untuk evaluasi performa alat monitoring pada lingkungan LAN standar di kampus atau perusahaan, bukan untuk analisis skala enterprise atau jaringan cloud modern

1.4 Tujuan Penelitian

Tujuan penelitian yang ingin dicapai dari penelitian ini sebagai berikut :

1. Mengetahui dan mengukur efektivitas PRTG Network Monitor dalam mendeteksi trafik jaringan serta menyajikan informasi performa jaringan (seperti *throughput, latency/response time, dan packet loss*) melalui mekanisme monitoring berbasis sensor.
2. Menganalisis dan mengukur kemampuan Wireshark dalam

melakukan penangkapan paket (*packet capture*) dan memberikan analisis mendalam terhadap struktur paket, termasuk identifikasi anomali dan kesalahan konfigurasi, untuk mendukung proses troubleshooting jaringan.

3. Membandingkan efektivitas PRTG Network Monitor dan Wireshark berdasarkan parameter kuantitatif yang relevan, seperti tingkat akurasi deteksi trafik, kecepatan *respon/alert*, kemampuan filtering, dan kedalaman analisis paket, sehingga diperoleh evaluasi terukur mengenai keunggulan dan keterbatasan masing-masing alat dalam proses monitoring dan analisis jaringan.
4. Penelitian ini bertujuan untuk melakukan kajian komparatif terhadap PRTG Network Monitor dan Wireshark guna menilai perbedaan kapabilitas keduanya dalam aktivitas monitoring dan analisis trafik jaringan, sehingga dapat diperoleh rekomendasi pemilihan alat yang paling sesuai untuk kebutuhan evaluasi performa jaringan.

1.5 Manfaat Penelitian

Penelitian ini dilakukan dengan harapan dapat memberikan manfaat bagi pembaca baik dari segi teoritis maupun praktis.

1.5.1 Manfaat Teoritis

Penelitian ini diharapkan memberikan kontribusi dalam pengembangan ilmu jaringan komputer, terutama pada kajian mengenai metode monitoring dan analisis trafik jaringan. Pemahaman mengenai efektivitas PRTG Network Monitor dan Wireshark dapat memperkaya literatur terkait perbedaan pendekatan antara monitoring berbasis sensor dan analisis paket secara mendalam. Temuan penelitian ini juga dapat memperkuat teori mengenai performa jaringan, teknik deteksi anomali, serta kerangka evaluasi perangkat monitoring yang dapat dijadikan referensi ilmiah bagi mahasiswa, akademisi, maupun peneliti yang melakukan studi lanjutan pada topik serupa.

1.5.2 Manfaat Praktis

Dari sisi praktis, penelitian ini diharapkan memberikan manfaat langsung bagi berbagai pihak yang berhubungan dengan pengelolaan jaringan. Bagi mahasiswa dan peneliti, penelitian ini dapat membantu dalam memahami teknik pengukuran performa jaringan, penggunaan alat monitoring, serta penentuan parameter teknis yang relevan dalam sebuah pengujian. Bagi administrator jaringan, hasil penelitian dapat menjadi dasar dalam memilih alat monitoring yang paling sesuai dengan karakteristik trafik dan kebutuhan operasional, serta membantu menentukan kapan PRTG atau Wireshark lebih efisien digunakan dalam deteksi masalah maupun troubleshooting. Sementara itu, bagi institusi pendidikan dan perusahaan, hasil penelitian ini dapat menjadi rujukan dalam merancang strategi monitoring yang lebih efektif, menentukan kebijakan pemantauan jaringan, serta meningkatkan keandalan layanan digital melalui pemilihan tools yang tepat berdasarkan kompleksitas arsitektur jaringan masing-masing.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini disusun agar pembahasan tersusun secara runtut dan mudah dipahami. Adapun struktur penulisan skripsi ini adalah sebagai berikut :

BAB I PENDAHULUAN

Berisikan tentang Latar Belakang Masalah, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, dan Manfaat Penelitian. Bab ini memberikan gambaran awal mengenai alasan dilakukannya penelitian, ruang lingkup penelitian, serta arah dan kontribusi yang ingin dicapai.

BAB II TINJAUAN PUSTAKA

Berisi dasar teori yang relevan dengan penelitian serta penelitian terdahulu yang mendukung landasan konseptual. Bab ini memuat teori jaringan komputer, monitoring jaringan, parameter trafik (*latency, throughput, packet loss*), prinsip kerja PRTG Network Monitor, prinsip kerja Wireshark, teori keamanan jaringan, serta kerangka pemikiran sebagai pijakan dalam penelitian.

BAB III METODE PENELITIAN

Bab ini berisi tentang penjelasan mengenai metode yang digunakan, mencakup jenis penelitian, objek penelitian, lokasi dan waktu penelitian, metode pengumpulan data, instrumen penelitian, serta skenario pengujian. Bab ini juga memuat rancangan eksperimen untuk menguji perbandingan PRTG dan Wireshark berdasarkan parameter tertentu serta teknik analisis data.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini akan membahas tentang pemaparan hasil pengujian pada berbagai kondisi trafik (normal, padat, dan mengandung serangan), analisis performa kedua alat, serta perbandingan efektivitas PRTG dan Wireshark. Bab ini juga menjelaskan interpretasi hasil uji, visualisasi output, evaluasi kelebihan–kekurangan masing-masing tools, dan keterkaitannya dengan teori serta penelitian sebelumnya.

BAB V PENUTUP

Berisi kesimpulan yang menjawab rumusan masalah serta saran untuk penelitian berikutnya maupun rekomendasi penggunaan alat monitoring bagi administrator jaringan dan institusi terkait.