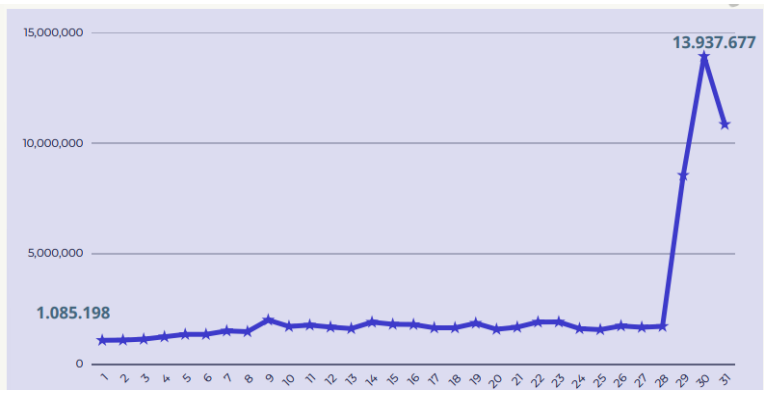
BAB I
PENDAHULUAN

1.1. Latar Belakang Penelitian

Pada saat ini dunia berada dalam era informasi, yang merupakan kelanjutan dari era prasejarah dan lainnya. Di era informasi ini, keberadaan informasi mempunyai arti dan peranan yang sangat penting bagi seluruh aspek kehidupan dan merupakan salah satu kebutuhan hidup semua orang, baik individu maupun organisasi. Di dukung dengan perkembangan ilmu pengetahuan dan teknologi, informasi semakin mudah untuk diakses oleh semua orang dalam bentuk informasi digital. Dari hasil survei penetrasi internet Indonesia tahun 2024 yang dirilis Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), maka tingkat penetrasi internet Indonesia menyentuh 79,5%. Dibandingkan dengan sebelumnya maka peningkatan 1,4%, kemajuan teknologi informasi merupakan salah satu pertimgbangan masyarakat untuk memenuhi kebutuhan berkomunikasi (Amir & Jhon, 2024). Perkembangan ini tentunya membawa perubahan positif yaitu digitalisasi pada setiap sektor seperti pendidikan, kesehatan, dan lainnya. Di sisi lain perkembangan pada era teknologi informasi tentunya membawa dampak negatif yang ditimbulkan seperti kejahatan siber.

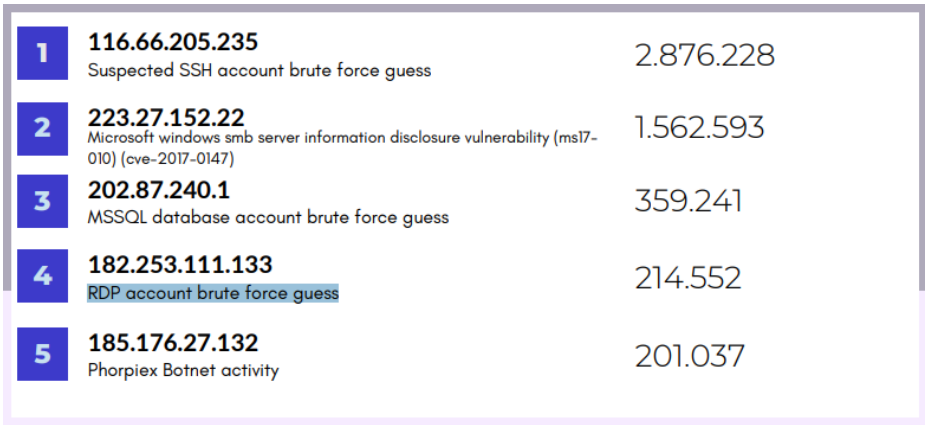
Dengan meningkatnya konektivitas dan pertukaran informasi secara daring, organisasi, perusahaan, dan individu semakin rentan terhadap serangan siber yang terus berkembang (Angraeni & Maulani, 2023). Dalam penelitian (Chandra & Snowe, 2020) menjelaskan bahwa kejahatan siber merupakan istilah untuk segala aktivitas kriminal yang dilakukan dengan menggunakan teknologi komputer. Dalam Undang-Undang Nomor 19 Tahun 2016 tentang informasi dan transaksi elektronik (UU ITE) terdapat tujuh jenis yang diklasifikasikan sebagai kejahatan siber diantaranya yaitu meretas *(hacking),* intersepsi illegal, mengotori *(defacing),* pencurian elektronik, *interferance,* memfasilitasi tindak pidana terlarang, pencurian identitas. Kejahatan siber ini semakin marak di terjadi di Indonesia, seperti salah satu contoh kejahatan siber yang terjadi di sektor perbankan pada salah satu bank ternama di Indonesa, pada mei 2023 salah satu server Bank Syariah dikabarkan lumpuh selama 5 hari. Menyebabkan para nasabahnya tidak dapat mengakses

aplikasi *mobile banking* mereka. Grup *hacker* asal Rusia, *Lockbit*, mengaku bertanggung jawab atas lumpuhnya server bank tersebut. Mereka telah mencuri data sebesar 1,5 byte, termasuk di dalamnya data pribadi konsumen dan pegawai. Mereka pun mengancam pihak bank untuk membayar sejumlah uang agar data tersebut dapat dijanjikan, jika tidak maka data-data tersebut akan dijual ke dark web. Kasus *cybercrime* ini masuk ke dalam jenis serangan *Ransomeware* terbesar di Indonesia (Intan *et al.*, 2024). Masalah-masalah semacam ini menunjukan bahwa Indonesia masih kurang serius mengenai ancaman kejahatan siber.



Gambar 1. 1 Grafik Trafik Anomali di Indonesia tahun 2023
(Sumber: Badan Siber dan Sandi Negara (BSSN, 2023)

Menurut data hasil dari monitoring Badan Pusat Statistik (BPS), Indonesia mencatatkan jumlah anomali trafik yang signifikan pada tahun 2023, dengan total 78. 464. 385 kejadian dengan angka tertinggi sebesar 13.937.677. Angka ini menunjukan peningkatan yang mencolok dan menyoroti tantangan besar yang dihadapi dalam mengelola keamanan jaringan yang semakin kompleks. Masih dalam laporan data dari BPS dalam tahun yang sama, menemukan top 5 sumber utama anomali trafik yang signifikan. Sumber-sumber ini meliputi:



Gambar 1. 2 Top 5 Sumber Anomali
(Sumber: Badan Siber dan Sandi Negara (BSSN, 2023)

Anomali trafik dari sumber-sumber ini menyoroti risiko yang tinggi terhadap keamanan jaringan di berbagai sektor. *Suspected SSH Account Brute Force Guess* merupakan salah satu jenis serangan yang sering kali tercatat memiliki angka anomali tertinggi dari 5 top sumber anomali traffik tahun 2023 di Indoensia. Kejahatan siber merupakan bentuk kriminalitas yang kompleks karena semua orang dapat menjadi korban, termasuk teknologi itu sendiri. Menurut Sudarmadi & Runturambi (2019) keamanan siber mempunyai kedudukan berarti dalam melindungi data sebab jadi perihal yang krusial untuk melindungi informasi dalam media penyimpanan serta menjamin data yang dikirim dalam kondisi nyaman dan proteksi sistem data terhadap ancaman siber.

Pengembangan lingkungan sistem keamanan siber yang baik dimulai dari pengembangan sistem keamanan jaringan. Menurut (Santoso *et al.*, 2022) dalam (Cahya *et al.*, 2023) jaringan komputer tidak akan dapat berfungsi tanpa adanya keamanan jaringan. Dijelaskan juga oleh Islami (2018) keamanan siber dapat dikonseptualisasikan sebagai serangkaian kebijakan, pedoman, prosedur, dan tindakan yang diperlukan untuk meminimalkan risiko pelangaran, instrusi, atau pencurian dalam pelaksanaan transaksi elektronik. Dalam penelitian (Febyola, Indah, dan Nurul, 2022) keamanan siber memiliki beberapa unsur pokok yang terkandung dalam keaman siber diantaranya: Kebijakan Keamanan Dokumen, Infrastruktur Informasi, Pertahanan Perimeter, Sistem Pemantauan Jaringan, Sistem Informasi dan Manajemen Acara, Penilaian Keamanan Jaringan, Ketersedian

Sumber Daya Manusia. Terkait dengan kondisi keamanan siber di Indonesia perlu adanya perbaikan mengenai pengembangan sistem keamanan siber dan sumber daya manusia dalam bidang keamanan siber.

Minimnya sumber daya yang memiliki kompetensi pada keamanan jaringan merupakan salah satu penyebab masih maraknya kasus kejahatan siber yang terjadi di Indonesia. Menurut (Van Solms & Van Niekerk, 2013) dalam Sri Cahaya (2020) salah satu aspek penting dalam sistem keamanan siber adalah faktor sumber daya manusia. Dalam konteks ini, faktor manusia sangat berhungan dengan peran yang dimainkan dalam proses keamanan dan dapat memberikan dampak positif maupun negatif terhadap keamanan siber. Pengembangan submer daya manusia dalam bidang keamanan siber tidak akan mudah perlu adanya sebuah sistem dan standar penilaian yang sesuai, oleh karena itu perlu adanya kerjasama dengan sektor pendidikan dalam membangun sumber daya manusia yang berkompeten dalam bidang keamanan jaringan. Menurut laporan dari CNBC Indonesia, ahli keamanan siber atau *Network Security Analyst* masuk dalam daftar 10 pekerjaan paling dicari di tahun 2024. Data ini diungkapkan oleh Kementerian Ketenagakerjaan (Kemnaker) yang menempatkan profesi ini di peringkat ke-4, mencerminkan tingginya kebutuhan akan profesional yang mampu melindungi infrastruktur digital dari ancaman siber yang semakin meningkat (Linda, 2024). Hal ini tentunya menjadi sebuah tantangan untuk semakin mengembangkan sumber daya manusia di Indonesia dalam bidang keamanan siber. Hal ini tentunya menjadi sebuah keharusan dalam mengembangkan sumber daya manusia di bidang keamanan siber dengan cara berkolaborasi secara komprehensif antar sektor pemerintah, pendidikan dan Dunia Usaha dan Dunia Industri.

Dalam beradapatasi diri dengan percapatan tranformasi masyarakat kerah budaya digital, Menteri Ketenagakerjaan Republik Indonesia telah menetapkan Standar Kompetensi Kerja Nasional Indonesia (KKNI) kategori informasi yang berkaitan dengan keamanan informasi. Hal ini dilakukan untuk mengajarkan setiap orang yang bekerja dalam keamanan informasi untuk memiliki kemampuan yang kompeten untuk memerangi kejahatan siber. Menurut Standar Kompetensi Kerja

Nasional Indonesia (SKKNI) No. 55 Tahun 2015, SKKNI adalah rumusan mengenai kemampuan kerja yang meliputi pengetahuan, keterampilan, dan atau keahlian, serta sikap kerja yang berkaitan dengan pelaksanaan tugas dan persyaratan pekerjaan yang diatur sesuai dengan peraturan perundang-undangan yang berlaku. *Network Security Analyst* (NSA) adalah tenaga ahli yang menagani desain, pelaksanaan, pengawasan, dan pengembangan setiap langkah keamanan untuk melindungi jaringan komputer perusahaan (Exaplan Training, 2022). Berdasarkan pendekatan KKNI, lulusan S1 berada pada jenjang kualifikasi Tingkat VI dengan kompetensi NSA yang diharapkan adalah 12 unit kompetensi SKKNI. Sejalan dalam dunia pelatihan, pendidikan, dan sertifikasi, terdapat 12 indikator inti *Network Security Analyst* yang terbagi menjadi dua ranah utama: Administrasi dan Teknis. Menurut LSP Digital Indonesia, "*Network Security Analyst* bertanggung jawab untuk mengelola sistem pertahanan dan perlindungan keamanan informasi" (LSP Digital Indonesia, 2024). Unit kompetensi NSA disajikan kedalam Tabel 1.1.

Tabel 1. 1 Daftar Unit Kompetensi NSA

No	Ranah	Kode Unit	Unit Kompetensi
1	**Administrasi**	J.62090.005	Menyusun Dokumen Kebijakan Keamanan Informasi
		J.62090.006	Melaksanakan Kebijakan Keamanan Informasi
		J.62090.026	Menyediakan Dukungan Keamanan bagi Pengguna
		J.62090.043	Mengimplementasikan Manajemen Perbaikan/Respon terkait Keamanan Informasi
2	**Teknis**	J.62090.025	Mengelola Sistem Pertahanan dan Perlindungan Keamanan Informasi
		J.62090.029	Mengelola Perimeter Keamanan
		J.62090.032	Menerapkan Kontrol Akses Berdasarkan Konsep/Metodologi yang Telah Ditetapkan

No	Ranah	Kode Unit	Unit Kompetensi
		J.62090.035	Mengkaji Efektivitas Penerapan Kontrol Akses
		J.62090.036	Melaksanakan Uji Coba Sistem Pertahanan Keamanan Informasi
		J.62090.037	Mendeteksi Kerentanan (Vulnerabilitas) Keamanan dan Potensi Pelanggaran
		J.62090.038	Melaksanakan Evaluasi Kelemahan (Vulnerabilitas) Keamanan

Penurunan setiap unit kompetensi dari SKKNI untuk *Network Security Analyst* (NSA) dilakukan secara sistematis untuk memastikan bahwa setiap aspek kompetensi terukur dengan jelass dan dapat di implementasikan kedalam pendidikan, pelatihan dengan lebih baik. Ranah teknis dalam SKKNI untuk *Network Security Analyst* mencakup berbagai konfigurasi penting untuk keamanan jaringan, termasuk konfigurasi sistem pertahanan dan perlindungan keamanan informasi, pengelolaan perimeter keamanan, serta penerapan dan evaluasi kontrol akses berdasarkan metodologi yang telah ditetapkan. Selain itu, konfigurasi yang berfokus pada pencegahan serangan *brute force* dan *port scanning* termasuk kedalam pengelolaan siklus pemberian akses, pengujian sistem pertahanan keamanan, deteksi kerentanan, dan evaluasi kelemahan keamanan untuk memastikan perlindungan jaringan yang komprehensif.

Pentingnya evaluasi pembelajaran dalam pendidikan dan pelatihan untuk *Network Security Analyst* (NSA) tidak dapat diabaikan. Menurut Simanjuntak (2024), evaluasi pembalajaran sangat penting untuk meningkatkan kualitas pengajaran, memberikan umpan balik, dan menilai kemajuan siswa. Evaluasi pembelajaran bertujuan untuk memastikan bahwa hasil belajar peserta didik selaras dengan standar kompetensi yang telah ditetapkan, dalam hal ini SKKNI. Melalui evaluasi yang tepat, kemampuan teknis dan pengetahuan peserta didik dapat diukur secara objektif. Watson (2024), berpendapat bahwa penilaian kinerja melibatkan mengevaluasi hasil pekerjaan tertentu berdasarkan standar yang telah ditetapkan.

Performance assessment berbasis KKNI menjadi krusial dalam konteks ini karena tidak hanya menilai pengetahuan teoretis, tetapi juga mengukur kemampuan praktis dalam menerapkan konfigurasi keamanan jaringan yang kompleks. Penggunaan *Performance Assessment* memberikan gambaran yang lebih akurat tentang kesiapan peserta didik dalam menghadapi tantangan nyata di lapangan, terutama dalam mengelola dan melindungi jaringan dari ancaman keamanan yang terus berkembang. Urgensi ini semakin meningkat seiring dengan kebutuhan akan tenaga kerja yang kompeten dan siap menghadapi berbagai skenario serangan siber.

Peneliti menyimpulkan bahwa semakin tinggi masalah keamanan jaringan yang terjadi di Indonesia membuat terbuka peluang tenaga kerja keamanan jaringan terutama *Network Security Analyst*. Maka peneliti melakukan penelitian kolaborasi dengan peneliti lain untuk merancang sebuah website media pembelajaran berisi kompetensi jaringan komputer dengan menggunakan pendekatan KKNI dan sudah diintegrasikan dengan SKKNI. Penelitian ini berfokus pada pengembangan *Performance Assessment* berbasis KKNI yang terintegrasi dengan SKKNI untuk meningkatkan akurasi penilaian kompetensi keamanan siber. Penelitian ini berjudul "**Pengembangan *Performance Assessment* Berbasis KKNI untuk Memperkuat Akurasi Penilaian Kompetensi Keamanan Siber**" dan diharapkan dapat meningkatkan kualitas penilaian dalam bidang keamanan jaringan.

1.2. Rumusan Masalah

Berdasarkan penjelasan latar belekang masalah sebelumnya, maka rumusan masalah dari penelitian ini:

1) Bagaimana perancangan *Performance Assessment* bidang keahlian teknis *network security analyst*?
2) Bagaimana validitas jobsheet dalam mencapai kompetensi mahasiswa dalam mata kuliah Jaringan Komputer?
3) Bagaimana reliabilitas *Performance Assessment* dalam *jobsheet* untuk mengukur kompetensi mahasiswa dalam praktik mata kuliah Jaringan Komputer?

4) Bagaimana hasil belajar terhadap *Performance Assessment* yang telah dikembangkan?

1.3. Batasan Masalah

Kompetensi keamanan jaringan yang terdapat di Standar Kompetensi Nasional Indonesia (SKKNI) sangat banyak, dalam penelitian ini peneliti menggunakan SKKNI *Network Secutiy Analyst* (NSA). Berdasarkan pendekatan KKNI, lulusan S1 berada pada jenjang kualifikasi Tingkat VI dengan kompetensi NSA yang diharapkan adalah 12 unit kompetensi SKKNI. Pada penelitian ini kompetensi teknik hanya mencakup 5 unit kompetensi dari 12 unit kompetensi SKKNI NSA diantaranya :

1) J.62090.006 (Melaksanakan Kebijakan Keamanan Informasi)
2) J.62090.025 (Mengelola Sistem Pertahanan dan Perlindungan Keamanan Informasi)
3) J.62090.026 (Menyediakan Dukungan Keamanan)
4) J.62090.029 (Mengelola Perimeter Keamanan)
5) J.62090.036 (Melaksanakan uji coba sistem pertahanan keamanan informasi)

Dengan merujuk pada Kriteria Unjuk Kerja (KUK) pada SKKNI Nomor 55 Tahun 2015 tentang Penetapan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Kegiatan Pemrograman, Konsultasi Komputer dan Kegiatan YBDI Bidang keamanan Informasi. Sehingga dari turunan KUK dari 5 unit tersebut dikembangkan sebuah *Performance Assessment* 2 konfigurasi yaitu konfigurasi *Brute Force* dan *Port Scanning* sebagai materi praktik yang akan digunakan.

1.4. Tujuan Penelitian

Berdasarkan rumusan masalah yang dipaparkan diatas, maka penelitian ini terdapat beberapa tujuan yaitu:

1) Mengembangkan *Performance Assessment* berbasis KKNI untuk meningkatkan akurasi penilaian kompetensi keamanan siber,

2) Menghasilkan *jobsheet* sebagai konten pada *website* "JobSheetKu" yang akan digunakan sebagai media praktik dalam peningkatan kompetensi *Network Security Analyst*.

1.5. Manfaat Penelitian

Berdasarkan latar belakang, penelitian ini memiliki manfaat secara teoritis dan idealis diantaranya sebagai berikut:

1.5.1. Manfaat Teoritis

Penelitian ini diharapkan dapat memberikan wawasan dan pengetahuan mengenai pengembangan Performance Assessment, KKNI, dan SKKNI dalam keamanan jaringan.

1.5.2. Manfaat Praktis

Adapun manfaat praktis dari penelitian ini yaitu:

1) Hasil penelitian ini diharapkan dapat membantu dunia pendidikan, pelatihan sertifikasi dalam meningkatkan akurasi penilaian kompetensi keamanan siber dalam mengevaluasi yang efektif dan relevan untuk mempersiapkan peserta didikan yang kompeten.
2) Penggunaan *Performance Assessment* ini akan meningkatkan akurasi penilaian kompetensi sesuai dengan SKKNI dan membantu mempersiapkan tenaga kerja yang lebih terampil di bidang keamanan siber.

1.6. Struktur Organisasi Skripsi

Sesuai dengan pedoman karya tulis ilmiah UPI Tahun 2021 terdapat organisasi dari penulisan skripsi yang berjudul "Pengembangan *Performance Assessment* Berbasis KKNI untuk Memperkuat Akurasi Penilaian Kompetensi Keamanan Siber" terdiri dari 5 bab secara berurutan, yaitu:

1) BAB I Pendahuluan

   Pada BAB I ini berisikan pemaparan tentang latar belakang, penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, dan struktur organisasi skripsi.
2) BAB II Kajian Teori

Pada BAB II dalam penelitian ini berisikan pemaparan terkait topik penelitian dan teori-teori dasar ayng dapat dijadikan acuan, seperti *Performance assessment*, KKNI, Kompetensi Teknik, dan SKKNI Network Security Analyst.

3) BAB III: Metode Penelitian

   Bab ini berisi tentang jenis penelitian, pengumpulan data, prosedur penelitian, serta analisis data.

4) BAB IV: Temuan dan Pembahasan

   Bab ini berisi tentang hasil dan pembahasan mengenai penelitian yang dilakukan

5) BAB V: Simpulan, Implikasi, serta Rekomendasi

   Bab ini berisi simpulan, implikasi, dan rekomendasi yang didasarkan pada hasil penelitian yang diperoleh.