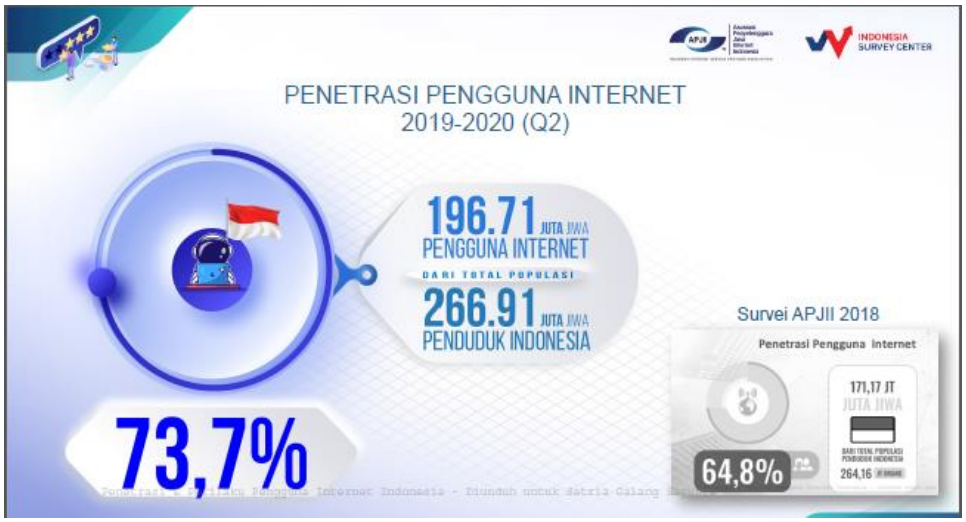
BAB I
PENDAHULUAN

1.1 Latar Belakang

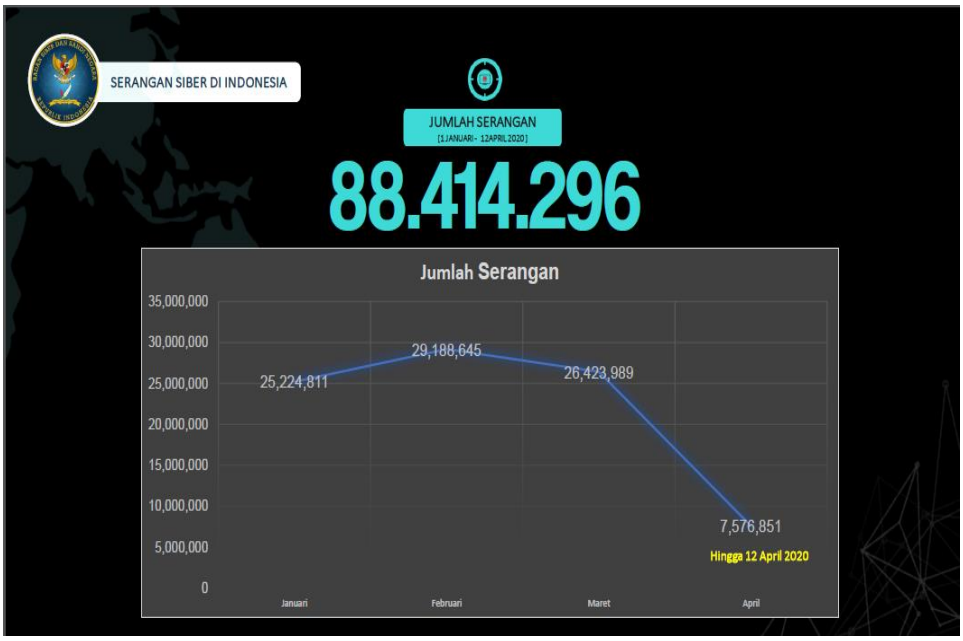
Kemajuan teknologi informasi dan sistem pertahanan siber saat ini berkembang begitu pesat dengan kemajuan teknologi pada bidang siber khususnya pada *webserver* dan *database* dapat menjadi suatu ancaman dalam pencurian data dan informasi sehingga perlu adanya penilaian keamanan untuk menanggulangi terjadinya pencurian data[1]. Keamanan jaringan juga menjadi aspek yang sangat penting seiring dengan peningkatan jumlah pengguna internet dan sistem pertahanan siber. Hasil survei yang dilakukan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) dengan *Indonesia Survey Center* (*ISC*) pada tahun 2019-2020 kuartal ke-2 menyebutkan bahwa jumlah pengguna internet naik menjadi 73,7% , dari total 266.91 juta jiwa penduduk Indonesia sebanyak 196.71 juta jiwa merupakan pengguna internet[2].



Gambar 1. 1 Hasil Survei APJII dengan ISC Tahun 2019-2020 Q2 [2]

Pada gambar 1.1 merupakan ringkasan hasil survei penggunaan internet di Indonesia yang dirilis oleh APJII dengan *ISC* pada kuartal kedua

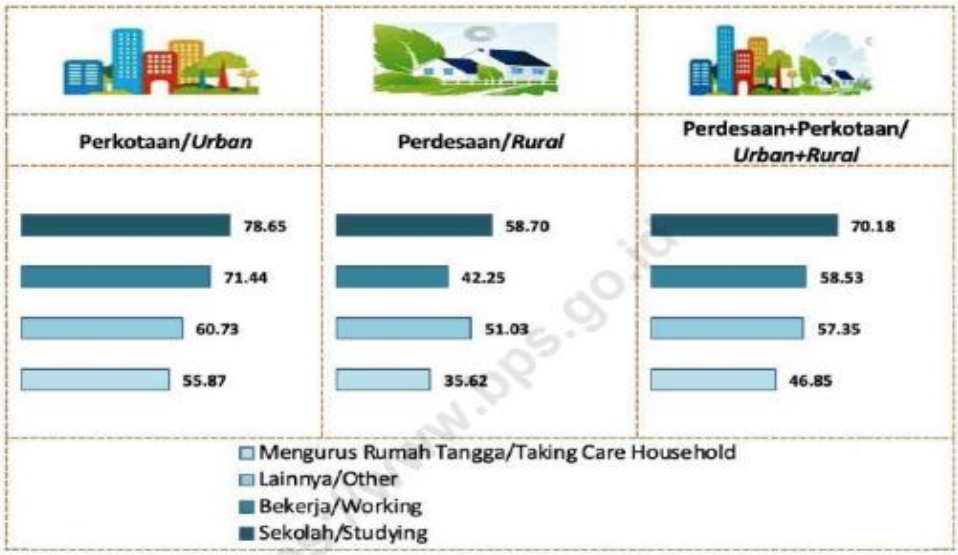
tahun 2019-2020. Dengan tingginya jumlah pengguna internet di Indonesia tentu perlu adanya sebuah pengawasan dan pengamanan pada sistem agar terhindar dari serangan kejahatan siber. Menurut laporan Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) mencatat 88.414.926 serangan siber telah terjadi sejak 1 Januari hingga 12 April 2020, jenis serangan yang paling banyak adalah *trojan activity* sebanyak 56% dan aktivitas *Information gathering* (pengumpulan informasi) sebanyak 43%[3].



Gambar 1. 2 Laporan Serangan Siber 1 april - 12 april 2020[3]

Pada gambar 1.2 menunjukkan informasi jumlah serangan siber di Indonesia yang dikeluarkan oleh Pusat Operasi Keamanan Siber Nasional. Dalam aspek kehidupan hampir semua dipengaruhi oleh internet termasuk dalam lingkup pekerjaan, seperti lembaga pemerintahan internet merupakan sarana yang paling mudah untuk mempercepat pertukaran informasi dengan hanya mengirim *email* pesan sudah sampai di tujuan dengan cepat dan juga mempercepat tersebarnya informasi cukup menggunakan media sosial yang pada akhirnya dapat memberikan pelayanan publik yang lebih baik dari hanya mengandalkan jalur birokrasi konvensional[4].

Menurut laporan Badan Pusat Statistik jumlah pengguna internet di pedesaan dalam lingkup pekerjaan mencatat 51,3 %[5]. Pada gambar 1.3 dibawah ini menunjukan penggunaan internet di berbagai lingkup yang dikeluarkan oleh Badan Pusat Statistik tahun 2020.



Gambar 1. 3 Laporan Pengguna Internet di Indonesia – 2020 [5]

Berdasarkan laporan yang dikeluarkan oleh BPS tersebut internet sudah banyak digunakan dalam berbagai lingkup baik di wilayah perkotaan maupun pedesaan. Seiring dengan banyaknya penggunaan internet tersebut kemampuan sistem keamanan jaringan mutlak menjadi sangat penting untuk menjaga kenyamanan berselancar di internet, sistem keamanan jaringan selayaknya harus selalu diukur dan ditingkatkan untuk mengurangi potensi kejahatan siber yang berdampak pada kerusakan atau terganggunya sistem jaringan komputer yang telah ada. Jaringan komputer merupakan sebuah sistem telekomunikasi yang menghubungkan dua atau lebih komputer untuk saling berkomunkasi dan bertukar data[6]. Layanan *wireless* kini sudah banyak digunakan baik pada lingkungan rumah, kampus, perusahaan, maupun instansi pemerintah sebagai akses internet, hal ini memudahkan para penggunanya dalam menerima informasi. Dengan luasnya jaringan *wireless* dan kemudahan akses tersebut tentu bisa muncul masalah baru yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk

melakukan serangan atau *hacking* yang mengganggu aktivitas komputer yang berada di sebuah jaringan. Keamanan jaringan komputer merupakan proses mencegah dan mengidentifikasi akses penggunaan yang tidak sah serta mengurangi resiko jaringan komputer dari ancaman yang dapat menganggu aktivitas yang sedang berlangsung dalam jaringan komputer[8]. Saat ini sering ditemukan perangkat jaringan *wireless* yang dipasang masih menggunakan konfigurasi *wireless* bawaan *vendor* seperti *SSID*, *IP Address*, *remot*e manajemen, *DHCP enable*, *channel* frekuensi, tanpa *enkripsi* bahkan *user/password* sistem perangkat tersebut masih standar bawaan *vendor*[9].

Kantor Balai Desa Kalisapu merupakan tempat layanan publik yang berada di Kecamatan Slawi Kabupaten Tegal yang saat ini menggunakan teknologi jaringan *Wireless Local Area Network* (*WLAN*) sebagai sarana akses internet untuk berbagai keperluan baik bersifat administrasi, menyimpan data-data warga pada *server* komputer lokal maupun layanan lainnya untuk memenuhi kebutuhan masyarakat yang hanya menggunakan satu *wireless access point* untuk mengakses jaringan internet, yang memiliki konfigurasi keamanan *password wifi WPA2-PSK* yang masih bisa saja di *crack* dengan jenis serangan *cracking the encryption* dengan *tools aircrack-ng*[9] untuk mendapatkan akses gratis, sistem konfigurasi masih bawaan *vendor* yang dapat dimanfaatkan oleh orang yang tidak bertanggung jawab dengan menyerang infrastrukur jaringan dengan jenis serangan *router attack*[10]. Hal ini bisa mengakibatkan trafik jaringan yang tidak stabil dan juga tentu saja konfigurasi seperti ini sangat rentan keamanannya, maka dari itu dibutuhkan pengujian keamanan jaringan untuk mengevaluasi kerentanan pada sistem keamanan jaringan *wireless*.

Salah satu metode yang digunakan untuk pengujian keamanan jaringan ini yaitu *penetration testing* yang merupakan metode untuk melakukan evaluasi dan analisa terhadap keamanan dari sebuah sistem dan jaringan komputer. Dalam pengujian keamanan jaringan ini akan

menggunakan *penetration testing execution standard* (*PTES*) sebagai acuan dalam pelaksanaannya. *PTES* merupakan salah satu standar atau acuan yang digunakan sebagai pedoman uji penetrasi yang memiliki panduan detail terkait metode dan teknik yang digunakan pada setiap tahap pengujian[11]. *PTES* memiliki tujuh tahapan, yaitu tahap pra-interaksi (*pre-engagement*), tahap pengumpulan informasi (*intelligence gathering*), pemodelan ancaman (*threat modelling*), analisis kerentanan (*vulnerability analysis*), eksploitasi (*exploitation*), pasca eksploitasi (*post exploitation*), dan tahap pelaporan (*reporting*)[9]. Berdasarkan uraian diatas, maka penulis tertarik untuk mengambil judul "**Pengujian Keamanan Jaringan *Wireless* Menggunakan Metode *Penetration Testing Execution Standard* (PTES)**", dengan harapan dapat menguji, mengevaluasi, dan memberikan solusi keamanan pada sebuah sistem jaringan.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka dirumuskan permasalahan yang ada pada Kantor Balai Desa Kalisapu Kecamatan Slawi Kabupaten Tegal yaitu bagaimana cara menguji dan mengevaluasi kerentanan sebuah sistem keamanan jaringan *wireless*.

1.3 Batasan Masalah

Berdasarkan identifikasi masalah yang telah diuraikan di atas , maka permasalahan dalam penelitian ini dibatasi pada :

1. Pengujian dilakukan pada jaringan *wireless LAN* di Kantor Balai Desa Kalisapu Kecamatan Slawi Kabupaten Tegal.
2. Pengujian dengan jenis serangan *Cracking The Encryption* untuk menguji keamanan enkripsi *password* dan *Router Attack* untuk menguji tingkat keamanan jaringan *wireless* yang digunakan.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai adalah melakukan pengujian keamanan jaringan *wireless* menggunakan metode *PTES* dengan memakai jaringan *wireless LAN* di Kantor Balai Desa Kalisapu Kecamatan Slawi Kabupaten Tegal.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut :

1. Memberikan solusi keamanan jaringan yang diakibatkan melalui uji coba serangan celah keamanan yang ada.
2. Dapat dijadikan sebagai acuan dalam pengujian keamanan jaringan di tempat yang lain.