BAB 1
PENDAHULUAN

1.1. Latar Belakang

Dalam sebuah jaringan komputer, setiap data di komputer yang terhubung ke internet tidak aman. Artinya data tersebut harus dilindungi agar komputer lain tidak dapat mengaksesnya. Setiap situs *web* dibuat dengan seperangkat kode yang memungkinkannya menampilkan informasi publik dan dapat dilihat oleh siapa saja. Di komputer *server,* tempat situs *web* disimpan, biasanya ada informasi pribadi atau rahasia yang tidak dapat dilihat oleh publik[1]. Sebagian besar serangan yang ada saat ini adalah hasil dari penyalahgunaan *open port*. *Vulnerability exploitation* adalah metode intrusi lain yang lazim. Penyerang akan memindai PC untuk menemukan kerentanan[2].Sehingga, situs web perlu diuji keamanannya melalui penilaian kerentanan dan pengujian penetrasi.

Institut Teknologi Telkom Purwokerto merupakan salah satu lembaga yang memanfaatkan teknologi dalam kegiatan akademik. *Repository web online* merupakan salah satu aset utama Institut Teknologi Telkom Purwokerto yang belum memiliki dokumentasi yang menangani penilaian kerentanan. Kurangnya evaluasi kerentanan yang terdokumentasi menimbulkan kekhawatiran bagi Institut karena penyerang dapat memanfaatkan kelemahan untuk mendapatkan informasi dari suatu aset. Penetapan aset ini mengacu pada penelitian yang sebelumnya menganalisis daftar aset penting IT Telkom Purwokerto. *Repository* memiliki resiko bahaya yang tinggi karena situs menyimpan informasi pribadi yang sensitif. Situs web ini juga diduga melakukan beberapa upaya serangan seperti peretasan dan pelanggaran data, dan data dihapus atau hilang oleh pihak yang tidak bertanggung jawab karena proses keamanan yang lemah[3].

Penilaian kerentanan / *Vulnerability Assessment* merupakan cara untuk mengetahui di mana keamanan situs web mungkin lemah. Sangat penting untuk mengambil tindakan segera untuk mempertahankan situs web dan jika diabaikan maka situs web yang dipegang oleh suatu organisasi, baik yang dikendalikan oleh pemerintah, pribadi, atau individu dapat mengalami kerusakan atau kehilangan yang disebabkan oleh penyerang[4]. Penelitian Riadi I., dkk[5]. Pada tahun 2019

membuktikan dengan menggunakan metode *Vulnerability Assessment* berhasil dalam mengidentifikasi celah keamanan pada *website open journal system (OJS)*.. Penelitian itu menggunakan alat *Open Web Application Security Project* (OWASP). Untuk pengembangan penelitian Riadi I., dkk dengan menggunakan spesifikasi hardware yang lebih high end dan alat yang berbeda yaitu menggunakan alat seperti Zenmap dan Nessus. Alat Zenmap dapat menentukan *port* mana yang terbuka dan host mana yang aktif di jaringan. Pada saat yang sama, alat Nessus mengaudit keamanan sistem dan menghasilkan *output* dalam bentuk kerentanan.

Penelitian ini berupaya mengkaji kerentanan keamanan pada *web server repository* IT Telkom Purwokerto, memantau *port server,* melakukan serangkaian pengujian, dan membuat rekomendasi terkait keamanan jaringan dan layanan *server* repositori untuk menjaga keamanan jaringan dan layanan.

1.2. Perumusan Masalah

Dari latar belakang yang telah diuraikan, maka dapat dirumuskan permasalahan, yaitu:

1. Bagaimana menganalisis hasil monitoring pada *port* server website *repository* IT Telkom Purwokerto ?
2. Bagaimana hasil analisis kerentanan keamanan *server web repository* IT Telkom Purwokerto ?
3. Bagaimana cara memperoleh rekomendasi berdasarkan sistem kerentanan keamanan pada *server repository* IT Telkom Purwokerto?

1.3. Tujuan Penelitian

Tujuan dari penelitian ini antara lain:

1. Mendapatkan hasil monitoring pada *port* server *repository* IT Telkom Purwokerto,
2. Menganalisis hasil kerentanan keamanan pada server *repository* IT Telkom Purwokerto,
3. Memberikan rekomendasi keamanan dalam meningkatkan keamanan dan fungsionalitas *server repository* IT Telkom Purwokerto.

1.4. Ruang Lingkup dan Batasan Masalah

Ruang lingkup dan batasan masalah antara lain :

1. Hanya dilakukan untuk mencari kerentanan kemudian memberikan solusi atas kerentanan tersebut,
2. Subjek yang dijadikan *sampel* penelitian adalah situs web http://repository.ittelkom-pwt.ac.id/,
3. Dilakukan secara *remote* melalui *Tools* Zenmap(Nmap) dan Nessus,
4. Metodologi untuk *Vulnerability Assessment* yang digunakan yaitu *Vulnerabilities scan*.
5. Penelitian ini dilakukan pada rentang bulan Mei - Juli 2022.

1.5. Manfaat Penelitian

Manfaat dari penelitian ini adalah :

1. Referensi untuk menguji kerentanan situs web dan langkah-langkah untuk memperbaiki kerentanan,
2. Bagi sebuah perusahaan atau instansi, dengan dilakukannya penelitian ini diharapkan agar tidak terjadinya serangan dan eksploitasi terhadap server sistem jaringan terutama dari *port* yang terbuka,
3. Manfaat bagi penulis yaitu meningkatkan pengetahuan keamanan jaringan yang dapat diimplementasikan di tempat kerja.

1.6. Sistematika Penulisan

Penelitian ini terbagi menjadi beberapa bab sebagai berikut :

BAB I PENDAHULUAN

Bab ini meliputi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisi tinjauan pustaka yang digunakan sebagai acuan dalam tugas akhir ini dan berisi landasan teori beserta materi pendukung lainnya seperti materi *Vulnerability Assessment*.

BAB III METODE PENELITIAN

Bab ini menjelaskan metodologi penelitian yang menjelaskan alur penelitian, bagaimana mengembangkan dan menguji sistem, dan alat yang digunakan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menguraikan operasi pengumpulan data untuk menetapkan metode pengujian sebelum menjalankan pengujian kerentanan keamanan di situs web target. Proses pengujian menggunakan PC virtual yang menjalankan sistem Kali Linux. Analisis ini mencoba mengidentifikasi kelemahan keamanan pada web server.

BAB V KESIMPULAN DAN SARAN

Bab ini menyampaikan temuan-temuan dari hasil penelitian yang telah dilakukan dan ide-ide untuk penelitian selanjutnya