BAB 1
PENDAHULUAN

1. 1 Latar Belakang

Dalam era digital yang semakin maju, keamanan jaringan menjadi aspek yang sangat krusial bagi berbagai institusi, termasuk perusahaan besar, kampus, dan organisasi lainnya. Keamanan jaringan merujuk pada proses melindungi jaringan komputer dari akses yang tidak sah, serangan, atau pencurian data. Salah satu pendekatan yang digunakan untuk memastikan tingkat keamanan jaringan adalah dengan melakukan pengujian penetrasi, yang sering dikenal sebagai penetration testing.

Meskipun banyak individu yang telah menguasai bidang teknologi informasi, kenyataannya, di tengah maraknya aktivitas peretasan, keamanan jaringan komputer sering kali belum diuji secara menyeluruh. Hal ini menciptakan celah yang bisa dimanfaatkan oleh para peretas, terutama pada jaringan nirkabel yang dianggap lebih rentan dibandingkan jaringan kabel (Sabdho, 2018). Oleh karena itu, diperlukan tindakan untuk menguji keamanan jaringan komputer saat ini menggunakan metode yang efektif, yaitu Penetration Testing (Ismail, 2020).

Penetration Testing adalah metode yang digunakan untuk mengevaluasi keamanan sistem dan jaringan komputer dengan mensimulasikan serangan pada sistem tersebut (Bayu, 2017). Pengujian ini bertujuan untuk menemukan dan memperbaiki kelemahan dalam sistem sebelum dimanfaatkan oleh penyerang yang dapat menyebabkan kerugian, baik data pribadi maupun data perusahaan (Sanjaya, 2020). Individu yang melaksanakan metode ini dikenal sebagai Pentester (Haeruddin, 2021).

Pengujian penetrasi ini harus dilakukan dengan persetujuan dari pemilik sistem, karena tanpa persetujuan, tindakan tersebut dapat dianggap sebagai aktivitas ilegal atau hacking (Kurniawan, 2021). Hasil dari pengujian ini sangat penting sebagai umpan balik bagi administrator sistem dan jaringan untuk meningkatkan tingkat keamanan di institusi tersebut.

Penetration Testing tidak hanya memberikan gambaran tentang bagaimana suatu sistem dapat diserang, tetapi juga membantu dalam mengidentifikasi kelemahan yang perlu diperbaiki. Sebagai contoh, pengujian DDoS digunakan untuk mengevaluasi sejauh mana sistem dapat menahan serangan dari pihak luar yang berbahaya. Dengan demikian, pengujian ini berperan penting dalam memastikan bahwa sistem telah cukup kuat untuk menangkal serangan nyata.

1. 2 Tujuan Penelitian

Penelitian ini bertujuan untuk menguji dan menganalisis tingkat keamanan jaringan dengan fokus pada layanan Server Message Block (SMB) yang berjalan pada port 445. Analisis yang dilakukan mencakup evaluasi lalu lintas jaringan, pemindaian terhadap jaringan, dan identifikasi kerentanan guna mengungkap potensi celah keamanan. Selain itu, penelitian ini juga menguji efektivitas serangan Distributed Denial of Service (DDoS) menggunakan aplikasi LOIC, dengan tujuan mengevaluasi dampak serangan terhadap ketersediaan dan kinerja layanan SMB. Penelitian ini diharapkan dapat memberikan wawasan mendalam tentang mekanisme gangguan terhadap layanan SMB oleh serangan DDoS, menghambat akses pengguna terhadap sumber daya jaringan, serta merumuskan langkah-langkah mitigasi yang efektif untuk meningkatkan keamanan jaringan secara keseluruhan.

1. 3 Rumusan Masalah

1. Bagaimana melakukan pengujian keamanan jaringan menggunakan metodepenetrasi testing?
2. Apa saja langkah-langkah yang perlu diikuti dalam pengujian keamanan jaringan menggunakan Nmap, Wireshark, dan Loic di Kali Linux?
3. Bagaimana mengidentifikasi kerentanan keamanan jaringan menggunakan Nmap, Wireshark,di Kali Linux?
4. Bagaimana melakukan serangan menggunakan alat-alat yang di sebutkan di atas dan
5. bagaimana mengatasi kerentanan keamanan yang ditemukan selama pengujian dan juga akan memberikan cara bagaimana meningkatkan keamanan keamanan jaringan?

1. 4 Batasan Masalah

1. Pengujian keamanan jaringan dibatasi pada penggunaan serangan DDoS sebagai contoh serangan yang umum dilakukan oleh penjahat dunia maya.
2. Penelitian ini akan menggunakan alat Nmap, Wireshark, dan LOIC dalam pelaksanaan metode penetrasi testing.
3. Fokus utama adalah pada serangan DDoS, sehingga serangan jaringan lainnya tidak akan dibahas dalam penelitian ini.
4. Penelitian ini tidak mencakup alat atau metode penetrasi testing selain Nmap, Wireshark, dan LOIC.