BAB 2

DASAR TEORI DAN TINJAUAN PUSTAKA

2. 1 Dasar Teori

Keamanan jaringan (network security) adalah elemen krusial dalam menjaga integritas, kerahasiaan, dan ketersediaan data serta sumber daya yang diakses melalui jaringan komputer. Risiko dalam keamanan jaringan mencakup berbagai macam ancaman yang dapat mengakibatkan kerugian signifikan bagi organisasi atau individu. Salah satu risiko utama adalah akses tidak sah ke sistem jaringan, yang dapat digunakan oleh peretas untuk mencuri data sensitif atau mengganggu operasi bisnis. Penyalahgunaan sumber daya jaringan, seperti yang terjadi dalam serangan DDoS (Distributed Denial of Service), merupakan ancaman yang dapat menyebabkan gangguan besar pada layanan online, membuatnya tidak tersedia bagi pengguna sah.

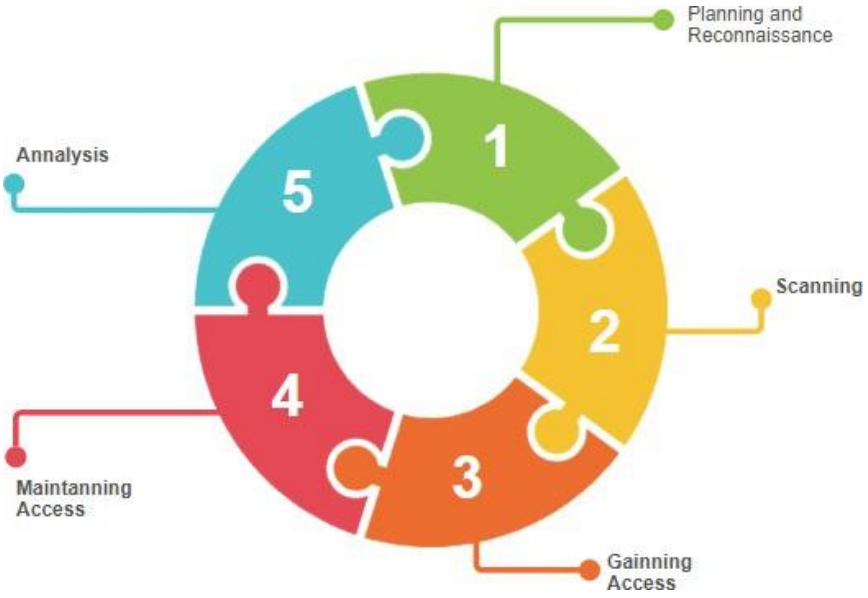
Kali Linux adalah distribusi Linux yang dirancang khusus untuk pengujian penetrasi dan keamanan siber, dilengkapi dengan alat-alat seperti Nmap dan Wireshark. Sedangkan VirtualBox adalah perangkat lunak virtualisasi yang memungkinkan menjalankan beberapa sistem operasi secara bersamaan di satu mesin fisik. Pengujian berupa simulasi di dalam lingkungan virtualisasi memungkinkan simulasi lingkungan uji yang aman dan terisolasi untuk pengujian keamanan jaringan tanpa risiko terhadap sistem utama.

Proses ini melibatkan identifikasi dan eksploitasi kerentanan untuk memahami dampak serangan dan memberikan rekomendasi perbaikan. Alat seperti Nmap digunakan untuk scanning TCP, SYN, dan UDP guna mengidentifikasi host dan layanan di jaringan serta mengungkap kerentanan. Wireshark berfungsi sebagai analyzer paket jaringan, menangkap dan memeriksa lalu lintas secara detail untuk memahami aktivitas jaringan secara mendalam. LOIC digunakan untuk melakukan serangan DDoS, mengirimkan paket TCP, UDP, atau HTTP secara massal ke target untuk membanjiri bandwidth atau sumber daya server.

Penyalahgunaan jaringan komputer mencakup firewall, IDS/IPS, dan praktik keamanan lainnya. Serangan DDoS berupaya membuat layanan online tidak tersedia dengan membanjiri target dengan lalu lintas dari berbagai sumber, menyebabkan gangguan signifikan. Dalam pengujian ini, Wireshark menangkap paket data yang melewati antarmuka jaringan dan memerlukan prosesor kuat untuk analisis data besar. Nmap dijalankan pada mesin dengan akses jaringan, menggunakan berbagai antarmuka untuk scanning. LOIC, yang ditulis dengan C# dan .NET, mengirimkan paket data ke target, memungkinkan penyesuaian intensitas serangan melalui pengaturan thread dan jumlah paket.

2. 2 Metode yang di Gunakan

Pada penelitian ini metode yang akan digunakan. Tahapan investigasi yang merupakan Langkah-langkah yang di lakukan dalam tugas akhir ini adalah sebagai berikut. (Pohan, 2021).



Gambar 2.1 Metode yang di Gandeng

2. 3 Analisis Kebutuhan Sistem

Kebutuhan sistem yang di gunakan di dalam perancangan tugas akhir ini terdiridari perangkat keras, perangkat lunak sehingga dalam penulisan tugas akhir ini agar dapat berjalan dengan baik. Berikut ini adalah daftar perangkat-perangkat yang di gunakan diantara-Nya.

2. 4 Perangkat Keras

Perangkat hardware ini dibutuhkan adalah.

a. Kali Linux.
b. Laptop Windows 10.
c. Router.

2. 5 Perangkat Lunak

Perangkat software yang dibutuhkan adalah.

a. Wireshark.
b. Nmap (Network Mapper).
c. LOIC (Low Orbit Ion Cannon).