MODUL 2

FOOTPRINTING

2.1 Tujuan Praktikum

1. Dapat mengenal dan memahami konsep Footprinting.
2. Dapat menggunakan alat dari Teknik Footprinting.
3. Mampu menganalisis hasil yang didapat dari Teknik Footprinting.

2.2 Alat dan Bahan

1. Kali Linux
2. VirtualBox
3. Httrack
4. Laptop
5. The Harvest
6. Ngrox

2.3 Dasar Teori

2.3.1 Pengenalan Footprinting

Footprinting adalah proses pengumpulan informasi tentang target tertentu secara sistematis dan terstruktur. Informasi yang dikumpulkan dapat berupa informasi umum seperti alamat fisik, nomor telepon, dan email, hingga informasi teknis seperti sistem operasi, aplikasi yang digunakan, jaringan yang digunakan, dan informasi pengguna.

2.3.2 Tujuan Utama Footprinting

Tujuan dari Footprinting adalah untuk mendapatkan informasi yang cukup tentang target agar dapat mengeksploitasi celah keamanan yang ada dalam sistem target. Informasi yang diperoleh dari Footprinting dapat digunakan untuk merancang serangan seperti *social engineering, phising,* dan *hacking*. Berikut adalah tujuannya:

1. *Know Security Posture*

   Footprinting memungkinkan penyerang mengetahui postur keamanan eksternal dari organisasi target.

2. *Reduce Focus Area*

   Footprinting mengurangi area fokus penyerang pada area tertentu dari alamat IP, jaringan, nama domain, akses jarak jauh, dan lain-lain.

3. *Identify Vulnerabilities*

   Footprinting memungkinkan penyerang untuk mengidentifikasi kerentanan dalam sistem target untuk memilih eksploitasi yang sesuai.

4. *Draw Network Map*

   Footprinting memungkinkan penyerang untuk menggambar peta atau menguraikan infrastruktur jaringan organisasi target untuk mengetahui tentang lingkungan aktual yang akan mereka hancurkan.

2.3.3 Metode Footprinting

Ada beberapa metode yang dapat digunakan dalam proses Footprinting, diantaranya:

1. Pencarian di mesin pencari

   Metode ini melibatkan pencarian informasi melalui mesin pencari seperti Google, Bing, atau Yahoo. Pencarian dilakukan dengan memasukkan kata kunci terkait target. Dari hasil pencarian, dapat ditemukan informasi umum seperti alamat fisik, nomor telepon, email, dan informasi terkait domain.

2. Pencarian di website publik

   Metode ini melibatkan pencarian informasi melalui website publik seperti situs web Perusahaan atau organisasi. Pencarian dilakukan dengan memeriksa halaman web untuk menemukan informasi yang relevan dengan target. Informasi yang dapat ditemukan meliputi struktur situs web, konten, dan infromasi kontak.

3. Pencarian di sosial media

   Metode ini melibatkan pencarian informasi melalui sosial media seperti Facebook, LinkedIn, dan Twitter. Pencarian dilakukan dengan memasukkan nama target ke dalam mesin pencari sosial media. Dari hasil pencarian, dapat ditemukan informasi seperti profil pengguna, konten yang diposting, dan kontak.

4. Pencarian di forum *online*

   Metode ini melibatkan pencarian informasi melalui forum *online* yang terkait dengan target. Pencarian dilakukan dengan memasukkan kata kunci terkait target seperti topik diskusi, pengguna yang terlibat dalam diskusi, dan informasi terkait dengan industri atau bidang target.

5. Pencarian di database publik

   Metode ini melibatkan pencarian informasi melalui database publik. Dari hasil pencarian, dapat ditemukan informasi seperti alamat fisik, nomor telepon, email, dan informasi terkait dengan domain. Pencarian dilakukan dengan memasukkan kata kunci terkait target ke dalam mesin pencari database publik. Dari hasil pencarian, dapat ditemukan informasi seperti alamat fisik, nomor telepon, Email, dan informasi terkait dengan domain.

2.3.4 Jenis-Jenis Teknik Footprinting

Ada beberapa Teknik yang dapat ditemukan dalam proses Footprinting, diantaranya:

1. *Passive Footprinting*

   Teknik yang tidak melibatkan interaksi langsung dengan target. Contohnya, pencarian di mesin pencari atau pencarian di website publik.

2. *Active Footprinting*

   Teknik yang melibatkan interaksi langsung dengan target. Contohnya, melakukan *port scanning* atau mengirimkan Email *phising*.

3. *Inner Footprinting*

   Pencarian informasi terhadap suatu situs di mana sudah berada di dalam jaringan computer tersebut (berada di dalam gedungnya dan menggunakan fasilitas internet gratis).

4. *Outer Footprinting*

   Pencarian informasi terhadap suatu situs di mana tidak berada di dalam jaringan computer target (berada jauh dari computer target).

2.3.5 Reconnaissance

Yang dimaksud dengan "*Reconnaissance*" adalah suatu tahap persiapan di mana *hacker* atau pihak yang akan melakukan "serangan" berusaha mencari

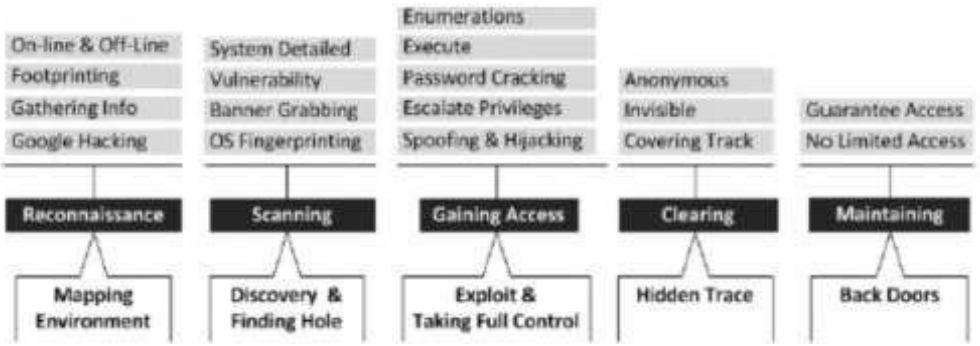
informasi sebanyak-banyaknya mengenai target atau sasaran sistem yang ingin diserang sebelum rangkaian proses penyerangan dilaksanankan.

Reconnaissance adalah istilah militer yang digunakan untuk menyebut metodologi yang digunakan untuk mengurangu ketidakjelasan tentang musuh, lingkungan, dan daerah untuk semua tipe. Teknik *reconnaissance* menyertakan *network scanning* melalui jaringan internal dan eksternal yang dilakukan tanpa memiliki izin dari pemilik server.

Reconnaissance dibagi menjadi 2, yaitu:

- *Active Reconnaissance* adalah pengumpulan data dengan cara bertatap muka langsung atau berhubungan langsung dengan target/sasaran.
- *Passive Reconnaissance* adalah menggunakan media informasi seperti berita, internet, dan lain-lain.

Reconnaissance merupakan tahapan pertama dalam melakukan percobaan untuk menembus atau menyerang (*attack*) sebuah sistem. Ada beberapa Langkah dan Teknik yang umumnya digunakan Ketika mencoba menembus atau menyerang (*attack*) sebuah sistem, seperti terlihat pada gamabar di bawah.



2.3.6 Langkah-Langkah Footprinting

1. Pemindaian Port

   Teknik ini melibatkan penggunaan alat pemindai port untuk mengidentifikasi port mana yang terbuka pada sistem target. Informasi ini dapat digunakan untuk menemukan layanan apa saja yang tersedia pada sistem target.

2. Enumerasi

   Teknik ini digunakan untuk mengumpulkan informasi tentang akun pengguna dan sistem file yang terpasang pada sistem target. Informasi ini daoat digunakan untuk mengidentifikasi celah keamanan pada sistem target.

3. Analisis Jaringan

   Teknik ini melibatkan penggunaan alat dan Teknik untuk mengidentifikasi komponen jaringan seperti router dan switch. Informasi ini dapat digunakan untuk memahami bagaimana data mengalir melalui jaringan dan memperoleh pemahaman yang lebih baik tentang arsitektur jaringan.

4. Pemindaian Rentang IP

   Teknik ini melibatkan penggunaan alat untuk mencari informasi tentang komputer yang terhubung pada jaringan. Informasi ini dapat digunakan untuk mengidentifikasi sistem target yang tidak terlihat secara langsung.

5. Analisis Kerentangan

   Teknik ini melibatkan penggunaan alat untuk mengidentifikasi celah keamanan target. Informasi ini dapat digunakan untuk mengambil Tindakan yang diperlukan untuk memperkuat keamanan sistem target.

2.3.7 Solusi Keamanan Footprinting

Proses Footprinting dapat menyebabkan beberapa dampak negatif, seperti hilangnya data rahasia, pencurian identitas, pencurian data pribadi, dan serangan siber. Oleh karena itu, penting bagi sebuah organisasi atau Perusahaan untuk memperkuat sistem keamanan agar tidak rentan terhadap serangan siber.

Beberapa Langkah yang dapat diambil untuk mencegah serangan yang berasal dari proses Footprinting adalah:

- Mengurangi jumlah informasi yang dapat diakses secara publik.
- Menggunakan teknologi keamanan yang tepat seperti firewall, antivirus, dan enkripsi data.

- Memastikan bahwa perangkat lunak yang digunakan selalu diperbaharui dengan *patch* terbaru.
- Memberikan pelatihan keamanan siber pada karyawan agar mereka dapat mengenali serangan *cyber* dan Tindakan pencegahan yang tepat,