Jurusan Teknologi Informasi Politeknik Negeri Malang

Jobsheet : Penyerangan Keamanan Jaringan

Pengampu: Tim Ajar Keamanan Sistem dan Jaringan Komputer

September 2021

Topik

Penyerangan Keamanan Jaringan: Praktek scanning dengan nmap dan Praktek Footprinting

Tujuan

Mahasiswa diharapkan dapat:

1. memahami jenis-jenis serangan, konsep footprinting & scanning, melakukan traceroute untuk mengetahui hop router yang dilewati, menggunakan aplikasi spiderfoot, web data extractor, portscan dan Foot printing.

Praktikum: Praktek scanning dengan nmap

Nmap merupakan alat bantu yang sangat berguna dalam melakukan scanning. Terdapat banyak teknik scanning Nmap. Masing-masing teknik memiliki kelebihan dan kekurangan sendiri. Beberapa diantaranya adalah:

TCP SYN Scan (-sS)

Teknik ini merupakan teknik scanning pada Nmap yang populer. Teknik dapat melakukan scanning port dengan cepat. Teknik ini dapat membedakan status port Open, closed dan filtered. Cara kerjanya adalah dengan mengirimkan sebuah paket SYN, kemudian menunggu jawaban dari sistem target. Bila kita mendapat jawaban paket SYN/ACK berarti port tersebut open, bila kita mendapat paket RST berarti port closed. Bila kita tidak mendapat jawaban seteah beberapa saat, maka port ditandai filtered.

TCP connect() Scan (-sT)

Scanning ini digunakan bila kita tidak memiliki privilege (admin/root). Scanning ini menggunakan fungsi system call connect pada OS. Metode ini membutuhkan waktu lebih lama dan umumnya dapat terbaca oleh IDS.

UDP Scan -sU

Metode ini digunakan untuk mengidentifikasi port UDP. Layanan DNS, SNMP dan DHCP adalah beberapa layanan yang menggunakan paket UDP.

FIN Scan (-sF), Xmas Tree Scan (-sX) dan Null Scan (-sN)

Teknik ini sering disebut teknik stealth. Banyak digunakan pada jaringan yang dilindungi Firewall. Teknik ini tidak dapat digunakan pada komputer dengan OS Windows. Selain itu hasil scan akan sulit membedakan status open dan filtered

Ping Scan (-sP)
Teknik ini merupakan teknik scanning yang paling cepat. Teknik ini tidak melakukan port scanning, umumya digunakan untuk menemukan host yang hidup pada suatu jaringan.

Version Detection (-sV)
Teknik ini dapat digunakan untuk mengetahui versi dari aplikasi yang digunakan pada komputer target.

Scan IP Protocol (-sO)
Teknik ini dapat menemukan protokol IP pada komputer target, misalnya ICMP, TCP, dan UDP

Scan ACK (-sA)
Teknik ini tidak dapat digunakan untuk menemukan port yang terbuka, tapi berguna pada jaringan yang dilindungi firewall maupun packet filter. Hasil scanning bisa digunakan untuk menentukan tipe firewal yang digunakan apakah statefull atau tidak serta port mana yang difilter.

RPC Scan (-sR)
Teknik ini digunakan untuk menemukan aplikasi yang menggunakan remote call procedure pada target.

Idlescan (-sI)
Teknik ini digunakan bila kita tidak memiliki akses langsung ke komputer target. Biasanya karena target dilindungi firewall

Langkah	Keterangan
1	Unduh Nmap dari www.nmap.org! Install Nmap!
2	Konek ke Access Point yang digunakan pada praktikum!
3	Catat dan laporkan IP anda!
4	Jalankan perintah berikut: nmap -sP (alamat IP subnet)/24
5	Jalankan perintah berikut: nmap -sP -PT80 (IP subnet)/24
6	Pilih sebuah komputer target dan lakukan Scanning metode TCP Connect dengan menjalankan perintah berikut: nmap -sT (alamat IP target)
7	Lakukan Scanning metode Stealth Scan dengan menjalankan perintah berikut: nmap -sS (IP target)

8	Lakukan Scanning metoda FIN Scan dengan menjalankan perintah berikut: nmap -sF (IP target)
9	Lakukan Scanning metoda Xmas Tree Scan dengan menjalankan perintah berikut: nmap -sX (IP target)
10	Lakukan Scanning metoda Null Scan dengan menjalankan perintah berikut: nmap -sN (IP target)
11	Lakukan Scanning metoda UDP Scan dengan menjalankan perintah berikut: nmap -sS -O (IP Target)

Laporan Praktikum:

No	**Pertanyaan/Perintah**
1	Laporkan layanan dan port apa saja yang aktif pada komputer target!
2	Laporkan Operating System apa yang digunakan komputer target!
3	Jelaskan apa perbedaan dari scanning yang anda lakukan pada latihan praktek no 4 dan no 5!
4	Jelaskan apa perbedaan dari teknik scan TCP Connect dan Stealth Scan!
5	Jelaskan apa kegunaan dari teknik FIN scan, Xmas Scan dan Null Scan!
6	Pada hasil scan menggunakan Nmap terdapat 6 macam status port yaitu open, closed, filtered, unfiltered, open|filtered dan closed|filtered. Jelaskan apa perbedaan dari masing-masing status tersebut!
7	Jelaskan apa kegunaan dari UDP Scan!
8	Dari hasil scanning, jelaskan bagaimana caranya untuk mengetahui bahwa komputer target dilindungi oleh Firewall!

Referensi :

- https://nmap.org/book/man-port-scanning-techniques.html
- https://github.com/scipag/vulscan
- https://blog.rootshell.be/2010/06/03/vulnerability-scanner-within-nmap/
- https://nmap.org/book/nse.html
- Nmap Cheat Sheet: From Discovery to Exploits – Part 1: Introduction to Nmap

- Nmap Cheat Sheet: From Discovery to Exploits, Part 2: Advance Port Scanning with Nmap And Custom Idle Scan

- https://www.cyberciti.biz/networking/nmap-command-examples-tutorials/

-- *Selamat Mengerjakan* --