Network Discovery

(Host Discovery)

By anjik

Latar Belakang

- Alokasi pengalamatan IP yang besar
- Mengetehui port (pintu masuk) pada layanan jaringan. Test dengan Port Scanner
- Banyak teknik yang dapat dilakukan untuk mengetahui akses melalui open port
- Jumlah port TCP dan UDP masing-masing 65535
- Teknik yang dilakukan untuk menjaga akses terhadap open port

Host Discovery

- Host Discovery adalah istilah yang dilakukan untuk mengetahui informasi tentang suatu host dalam serangkaian tahapan dalam *penetration testing*, dengan mengidentifikasi segala kemungkinan suatu host yang dapat diakses pada jaringan.
- Jika terdapat firewall, maka sulit untuk mengetahui berapa jumlah host dibelakang firewall dalam suatu jaringan.
- Tools yang paling mudah didapatkan untuk melakukan host discoery adalah NMAP.

Nmap sebagai Tools dalam Host Discovery

- Nmap / Network Map adalah sebuah aplikasi yang dapat dipakai untuk memonitor jaringan dari berbagai virus dan serangan yang mencurigakan.
- Termasuk untuk mengecek kesalahan konfigurasi jika memang ada.
- Nmap di desain sebagai utilitas gratis untuk penjelajahan jaringan atau audit keamanan.
- Banyak administrator sistem dan jaringan menggunakan untuk beberapa pekerjaan seperti *network inventory*, mengatur *setting* jaringan, penjadwalan upgrade, dan monitoring penyimpanan data.

Fitur NMAP

- **Flexible** mendukung banyak sekali teknik canggih untuk memetakan jaringan dengan menggunakan IP Filters, firewall, router, dan hambatan lainnya. Memiliki beberapa mekanisme port scanning (baik TCP dan UDP), deteksi OS, deteksi versi, ping sweeps, dan lain sebagainya.
- **Powerful** Nmap telah digunakan untuk scanning jaringan yang besar dari ratusan ribu mesin.
- **Portable** kebanyakan system operasi telah di dukung oleh Nmap. Beberapa di antaranya termasuk Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, dan lain lain.
- **Free** Software ini tersedia secara gratis.
- **Desain**, saat ini terdapat nmap versi GUI, yaitu zenmap

PERINTAH SEDERHANA NMAP

Intense SCAN (nmap -T4 -A -v localhost)

```
Starting Nmap 6.25 ( http://nmap.org ) at 2013-03-18 11:22 SE Asia Standard Time
NSE: Loaded 106 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Parallel DNS resolution of 1 host. at 11:22
Completed Parallel DNS resolution of 1 host. at 11:22, 0.00s elapsed
Skipping SYN Stealth Scan against localhost (127.0.0.1) because Windows does not support scanning your own machine
(localhost) this way.
Initiating Service scan at 11:22
Skipping OS Scan against localhost (127.0.0.1) because it doesn't work against your own machine (localhost)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 11:22
Completed NSE at 11:22, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up.
PORT      STATE   SERVICE           VERSION
1/tcp     unknown tcpmux
3/tcp     unknown compressnet
4/tcp     unknown unknown
6/tcp     unknown unknown
21/tcp    unknown ftp
22/tcp    unknown ssh
23/tcp    unknown telnet
24/tcp    unknown priv-mail
25/tcp    unknown smtp
```

Other Command

Intense plus UDP

nmap -sS -sU -T4 -A -v localhost

Intense scan, all TCP ports

nmap -p 1-65535 -T4 -A -v localhost

Intense scan, no ping

nmap -T4 -A -v -Pn localhost

Ping scan

nmap -sn localhost

Other Command

Quick scan

nmap -T4 -F localhost

Quick scan plus

nmap -sV -T4 -O -F --version-light localhost

Quick traceroute

nmap -sn --traceroute localhost

Regular scan

nmap localhost

Slow comprehensive scan

nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script all localhost