

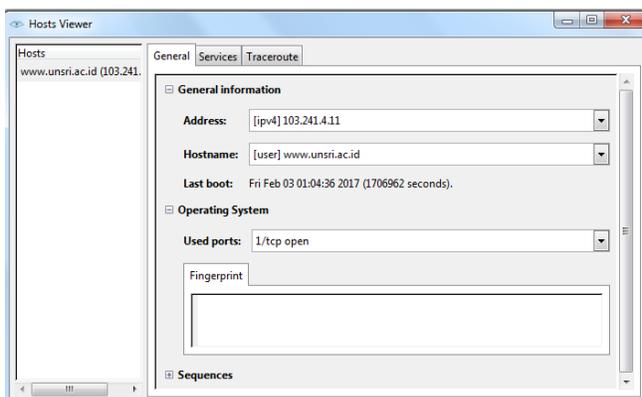
NAMA : DWI KURNIA PUTRA
NIM : 09011181320019
MK : KEAMANAN JARINGAN KOMPUTER

NETWORK SCANNING

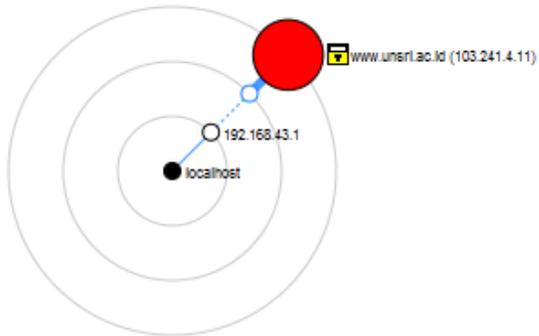
Merupakan tahapan didalam proses hacking yang mana hacker atau yang melakukan “serangan” menggunakan berbagai alat dan tools untuk berusaha mencari celah masuk atau lokasi tempat serangan yang akan dilakukan. Dalam scanning, biasanya yang akan di-scan yaitu port dalam sistem computer(port scanning), pemetaan jaringan(network mapping), pencarian kerawanan/kerapuhan(vulnerability scanning) dan lain sebagainya.

Tool yang saya gunakan yaitu **Zenmap** yang merupakan aplikasi multi platform sebagai interface sederhana untuk apikasi nmap. Nmap (Network Mapper) sendiri adalah sebuah aplikasi open source untuk explorasi network dan audit keamanannya. Nmap bekerja dengan melakukan scan terhadap komputer (host) stand alone ataupun host yang terhubung dalam sebuah jaringan, menentukan host-host yang aktif dalam suatu jaringan, menentukan informasi sistem operasi, port-port yang terbuka dan jenis firewall yang digunakan. Fungsi Zenmap adalah untuk eksplorasi dan audit keamann jaringan dan untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal.

Berikut merupakan ujicoba “Scanning” yang saya lakukan ke situs www.unsri.ac.id



Topologi dari www.unsri.ac.id



Hasil dari scanning website www.unsri.ac.id

The screenshot shows the Nmap interface with the following details:

- Target: www.unsri.ac.id
- Command: `nmap -T4 -A -v www.unsri.ac.id`
- Hosts: www.unsri.ac.id (103.241.4.11)
- Host Status:
 - State: up
 - Open ports: 980
 - Filtered ports: 20
 - Closed ports: 0
 - Scanned ports: 1000
 - Up time: 1706962
 - Last boot: Fri Feb 03 01:04:36 2017
- Addresses:
 - IPv4: 103.241.4.11
 - IPv6: Not available
 - MAC: Not available
- Hostnames:
 - Name - Type: www.unsri.ac.id - user
- TCP Sequence:
 - Difficulty: Good luck!
 - Index: 261
 - Values:
- IP ID Sequence:
 - Class: Randomized
 - Values:
- TCP TS Sequence:
 - Class: 1000HZ
 - Values: