TUGAS

“KEAMANAN JARINGAN KOMPUTER”

Disusun Oleh :

Nama : Nova Dyati Pradista

Nim : 09011181320005

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

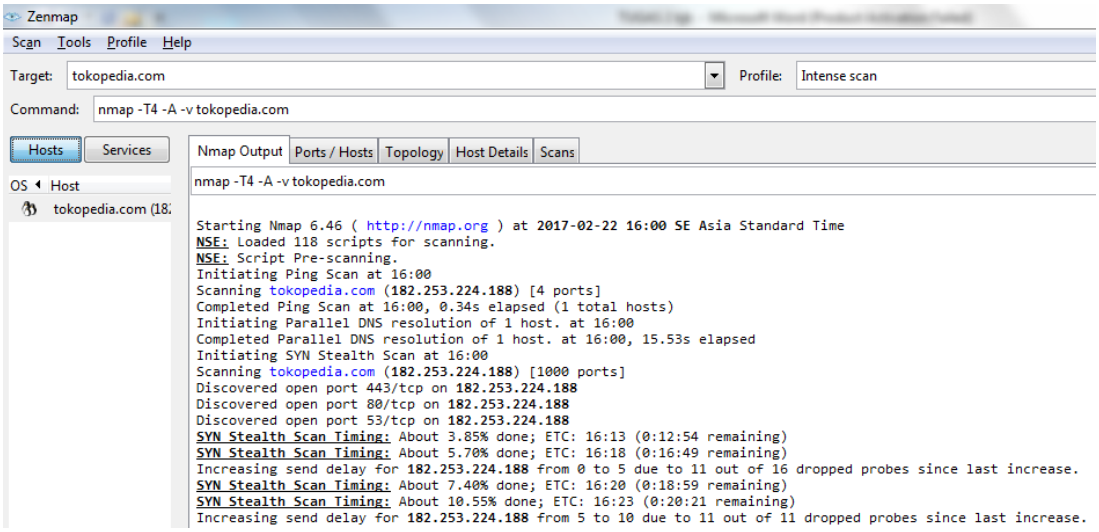
UNIVERSITAS SRIWIJAYA

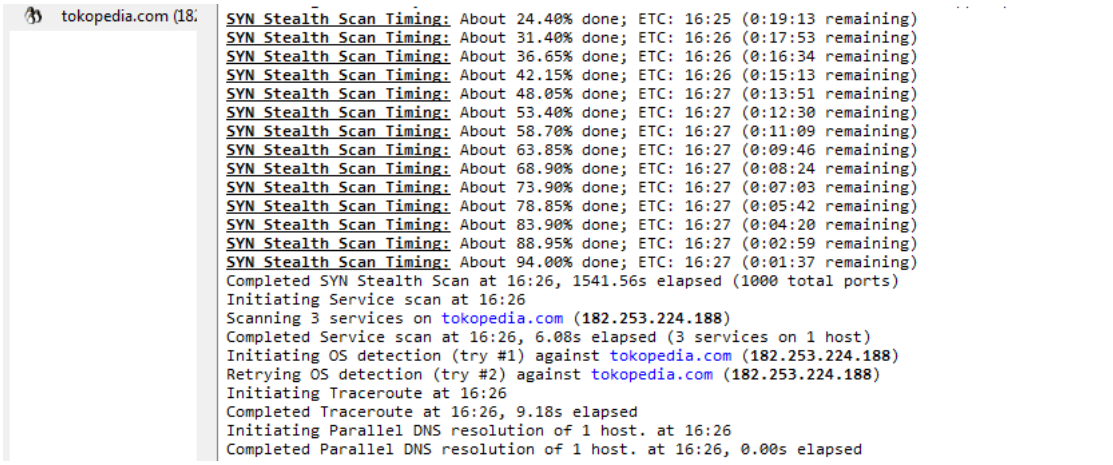
2017

TUGAS 2 : SCANNING

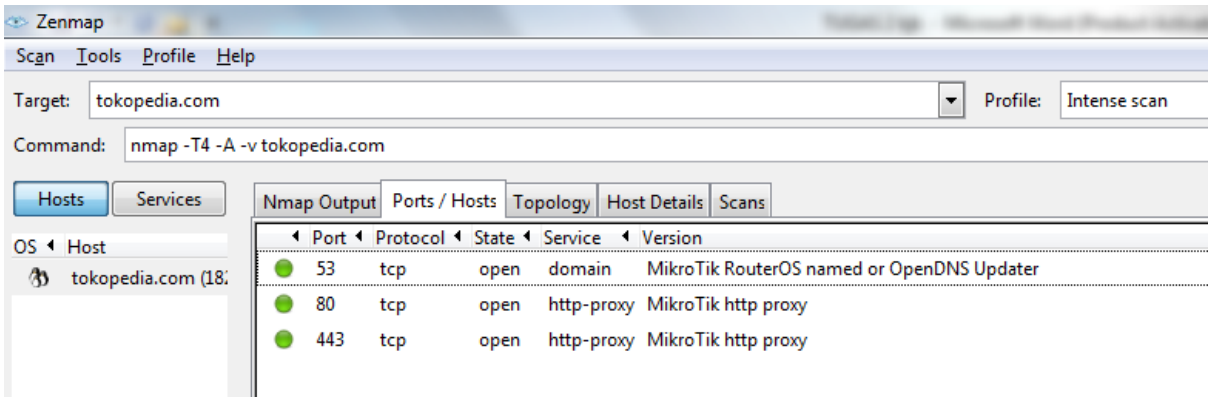
Berikut ditampilkan hasil dari scanning dengan domain www.tokopedia.com menggunakan Nmap:

Nmap output



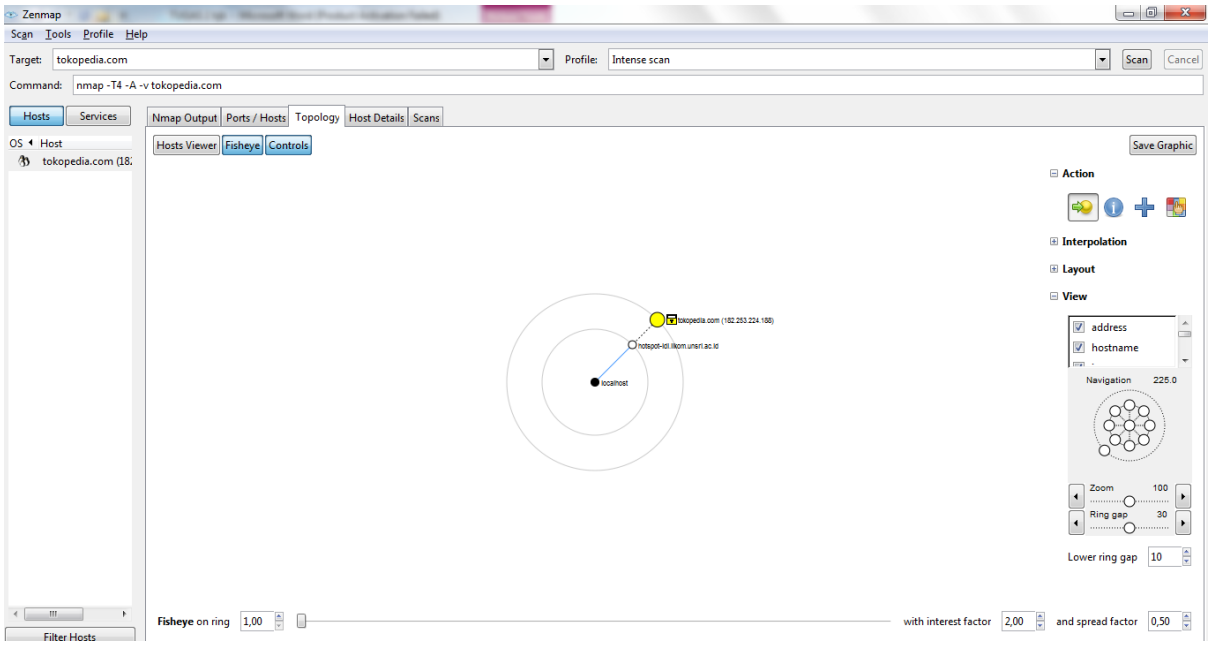


Ports / Hosts



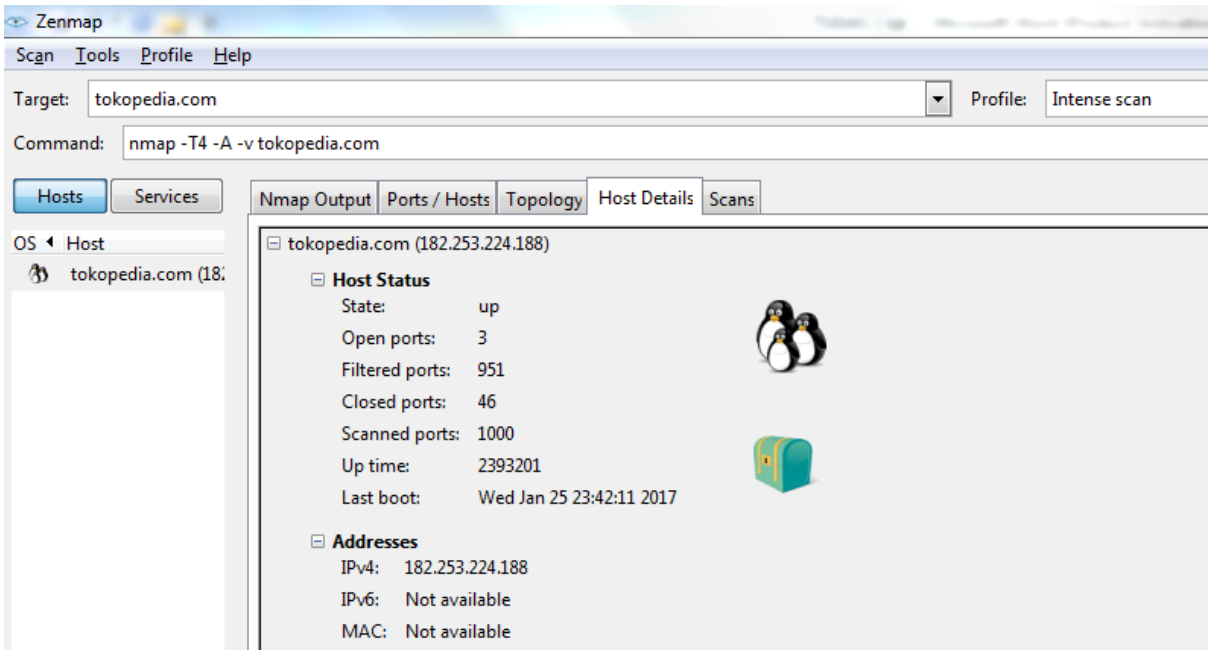
Gambar diatas menunjukkan port / host dari alamat domain www.tokoprdia.com yang memiliki 3 layanan service yaitu domain Mikrotik RouterOS named or OpenDNS Updater dengan port 53, http-proxy MikroTik http proxy dengan port 80, http-proxy MikroTik http proxy dengan port 443 yang masing – masing menggunakan protocol tcp dengan state open.

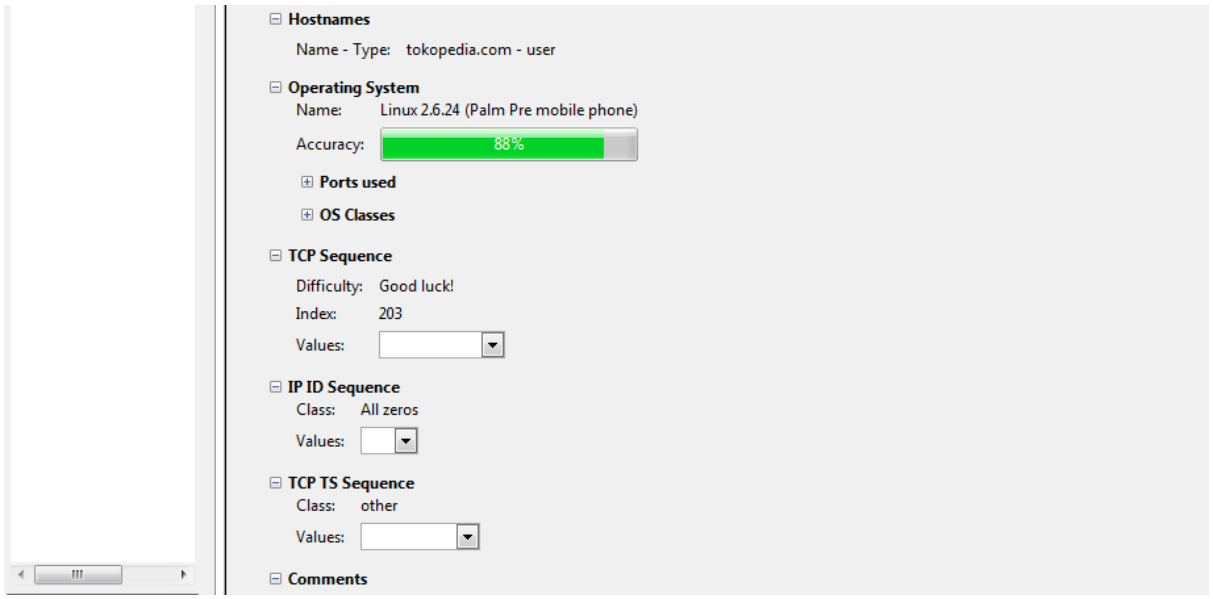
Topology



Gambar diatas menunjukkan topology dari alamat domain www.tokopedia.com 182.253.224.188 yang terhubung melalui localhost dari hotspot-idl-ilkom.unsri.ac.id

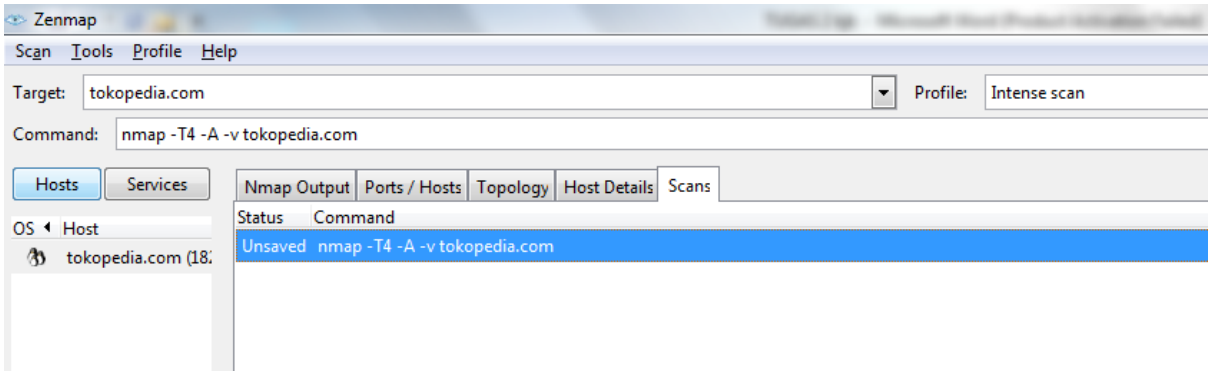
Host details





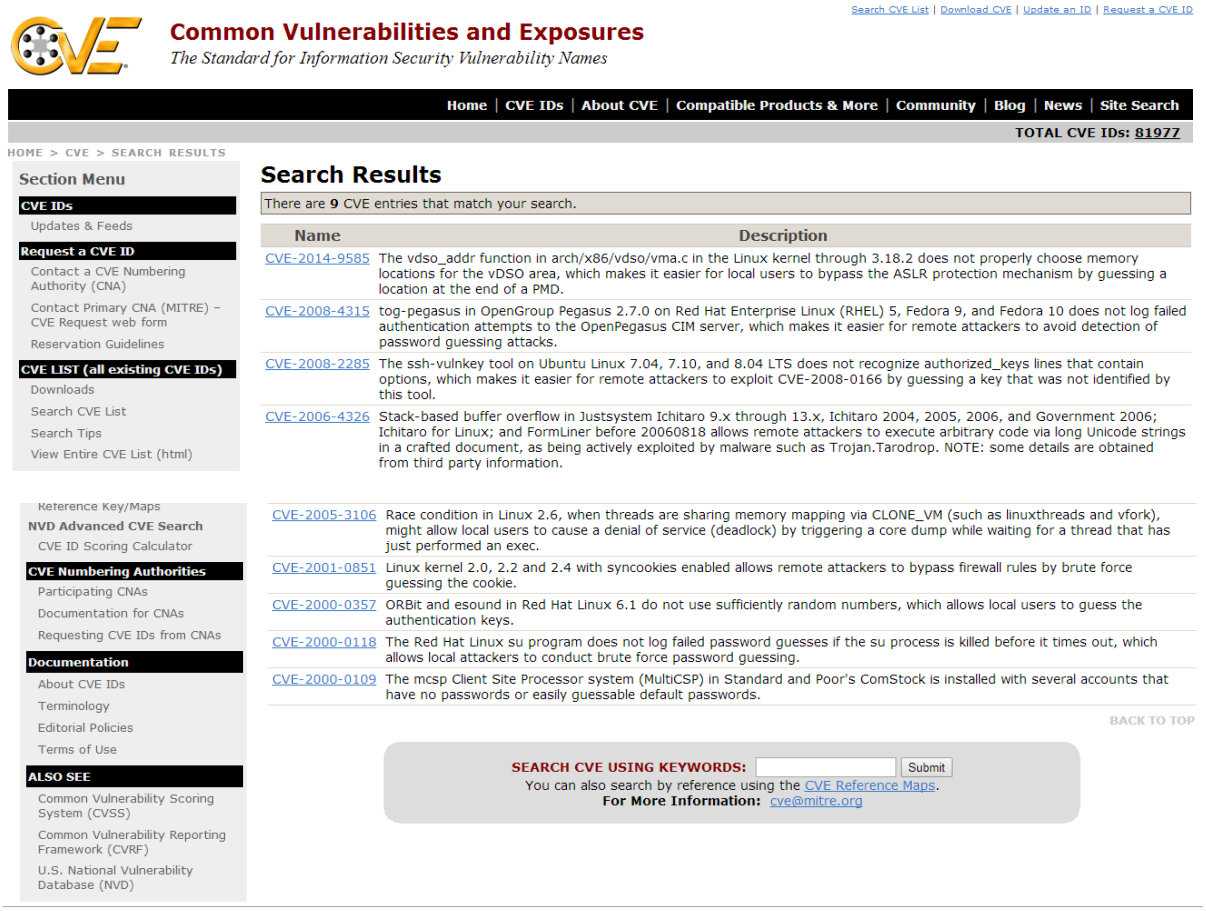
Gambar diatas menunjukkan host details dengan alamat domain www.tokopedia.com 182.253.224.188 yang menampilkan masing – masing berupa host status, addresses, hostname, operating system, port used, os classes, tcp sequence, IP ID sequence, TCP TS sequence dan comments

Scans



Gambar diatas menunjukkan scans dari alamat domain www.tokopedia.com yang menunjukkan berupa status command unsave nmap-T4-v tokopedia.com

Hasil dari CVE www.tokopedia.com



Kesimpulan :

Scanning merupakan kegiatan probe dalam jumlah yang besar dengan menggunakan tool secara otomatis. Tool tersebut secara otomatis dapat mengetahui port – port pada saat host lokal maupun host remote, ip address yang aktif, bahkan bisa untuk mengetahui sistem operasi yang digunakan pada host yang dituju. Tool scanner yang saya gunakan adalah Nmap.

Scanning dapat dibedakan menjadi 3 yaitu :

- Port scanning, dilakukan untuk mengetahui service apa yang dijalankan oleh target berdasarkan well known ports.
- Network scanning, dilakukan untuk mengetahui aktifmya satu host dan ip address dari host tersebut.
- Vulnerability scanning, dilakukan untuk mengetahui sistem operasi, versi sistem operasi, maupun service pack yang digunakan.

Umumnya port scanning tools akan melakukan probe ke host target yang mudah di deteksi oleh IDS. Network scanning maupun vulnerability scanning juga mudah di deteksi oleh IDS, karena tetap melakukan interaksi dengan target.