**KEAMANAN JARINGAN KOMPUTER**



**Ulan Purnama Sari**

**09011181320003**

**Program Studi Sistem Komputer**

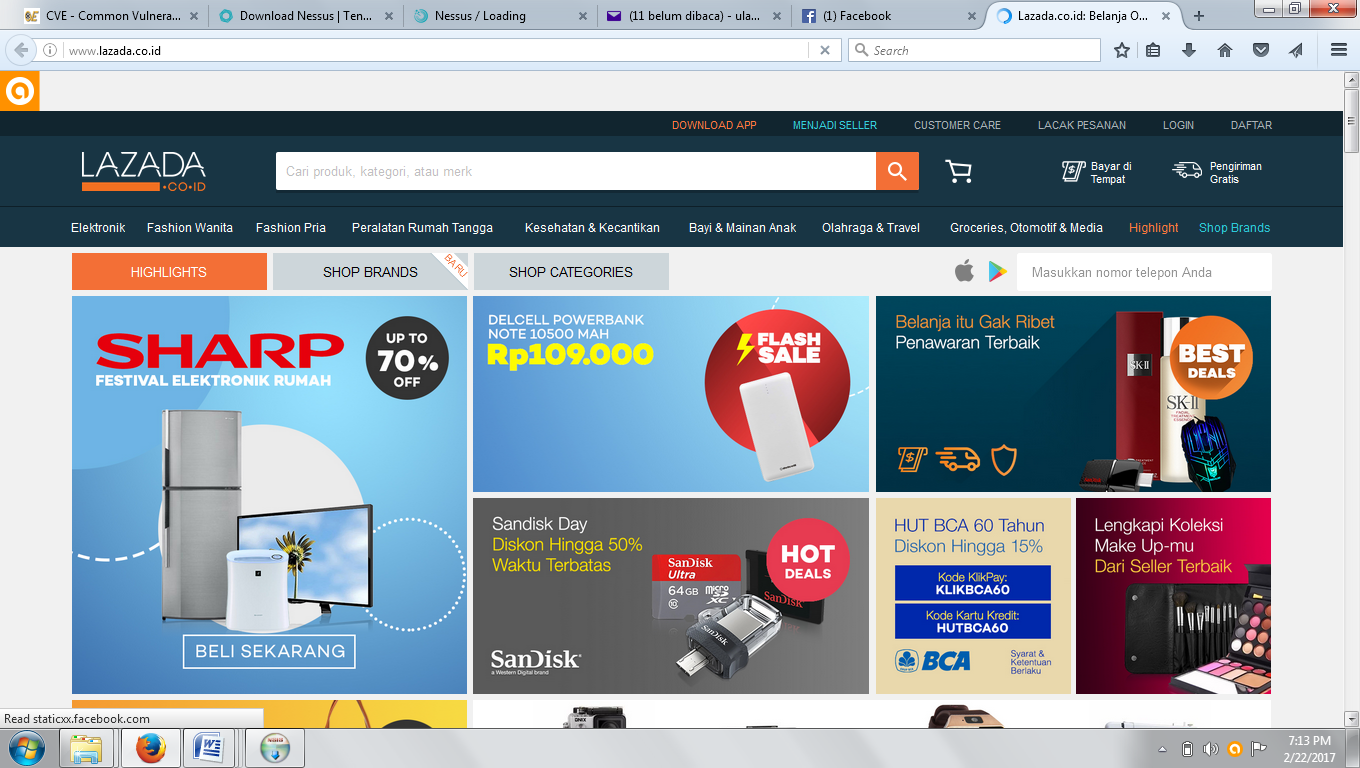
**Fakultas Ilmu Komputer**

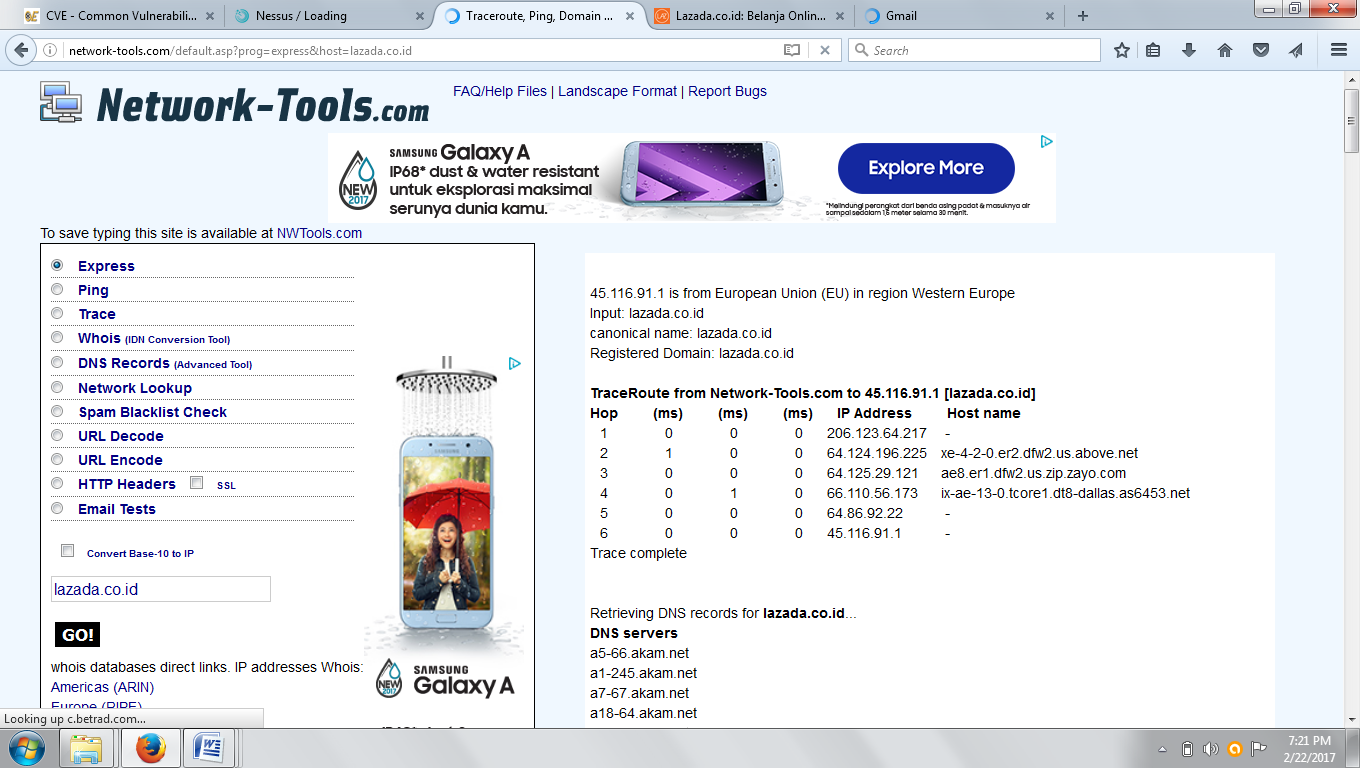
**Universitas Sriwijaya**

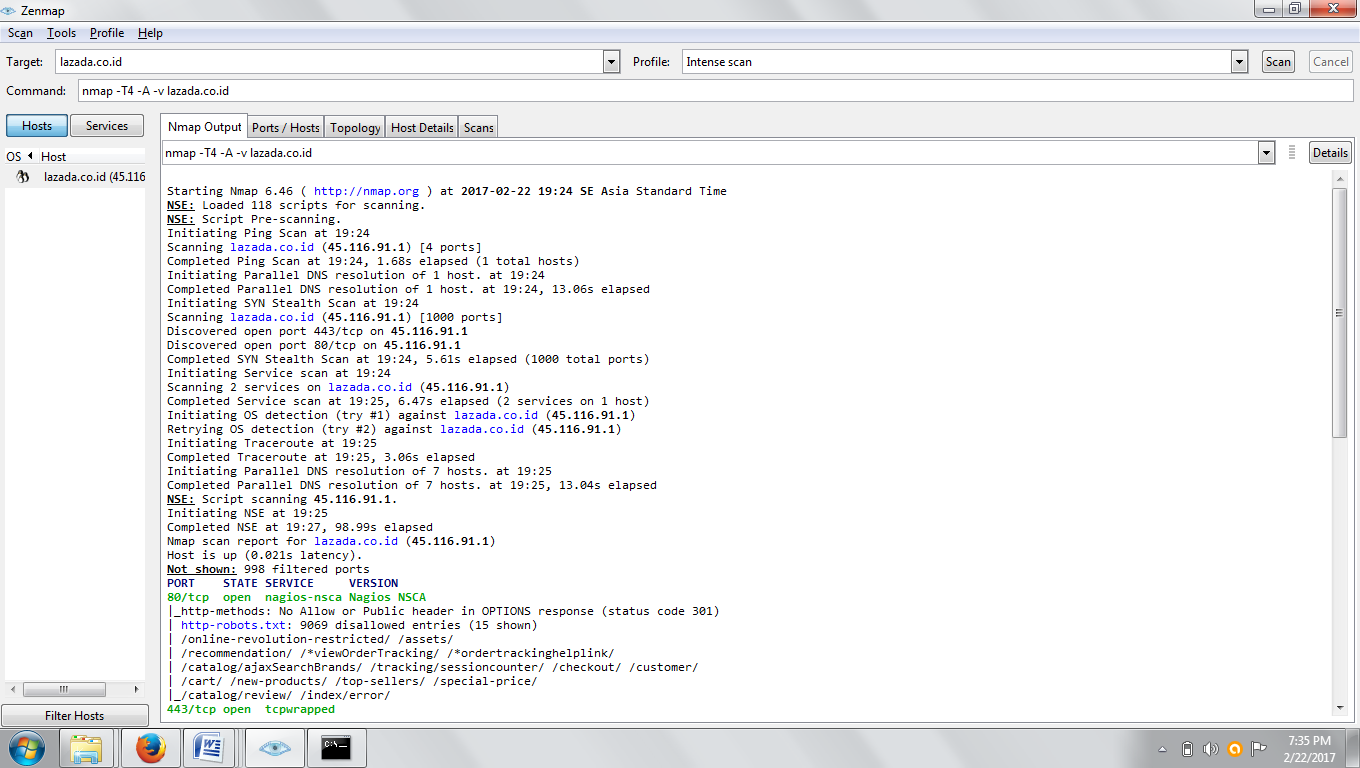
**2017**

**SCANNING**

Lazada.co.id adalah suatu web penjualan dimana web ini berisi berita penjualan pakaian, elektronika, perabotan rumah tangga dll.

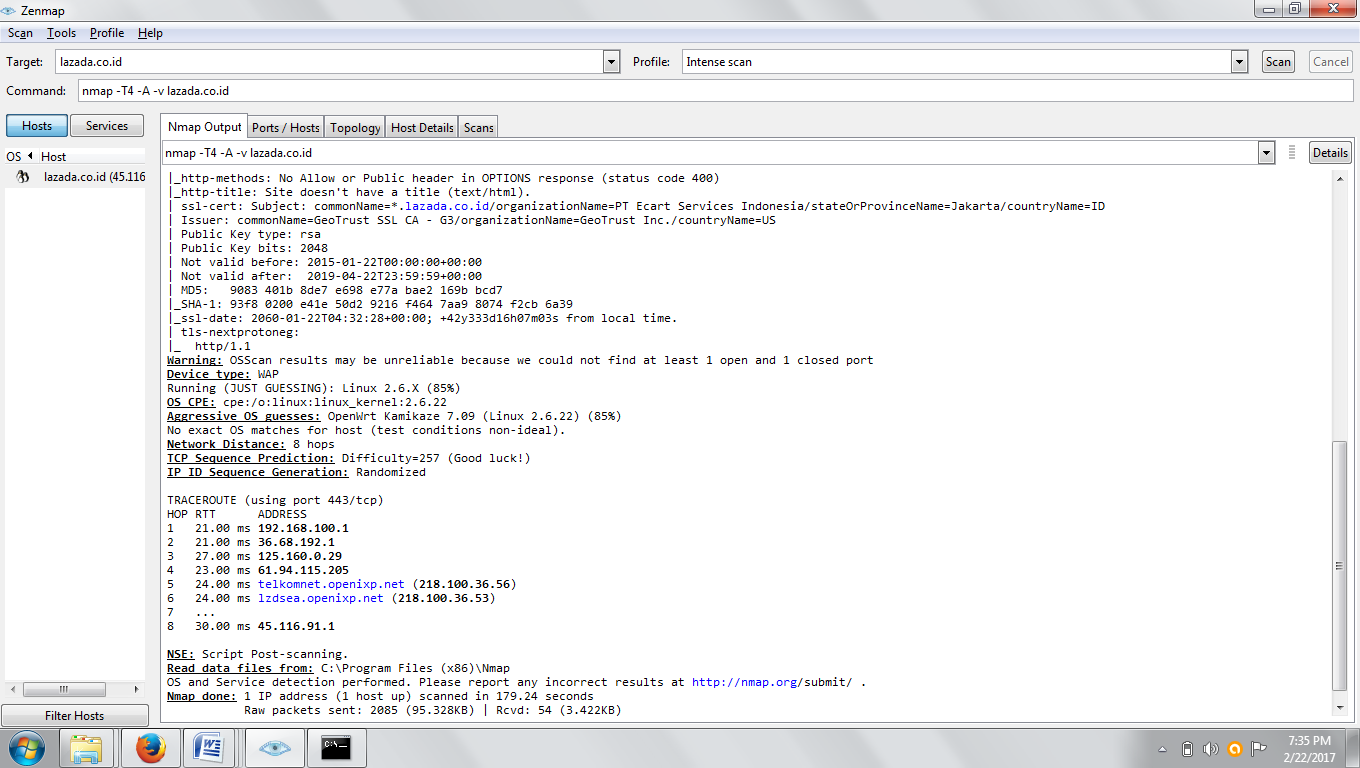


Lazada.co.id memiliki IP 45.116.91.1

Nmap (“Network Mapper”) merupakan sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Ia dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal. Nmap menggunakan paket IP raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, sistem operasi (dan versinya) apa yang digunakan, apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya. Meskipun Nmap umumnya digunakan untuk audit keamanan, namun banyak administrator sistem dan jaringan menganggapnya berguna untuk tugas rutin seperti inventori jaringan, mengelola jadwal upgrade layanan, dan melakukan monitoring uptime host atau layanan.

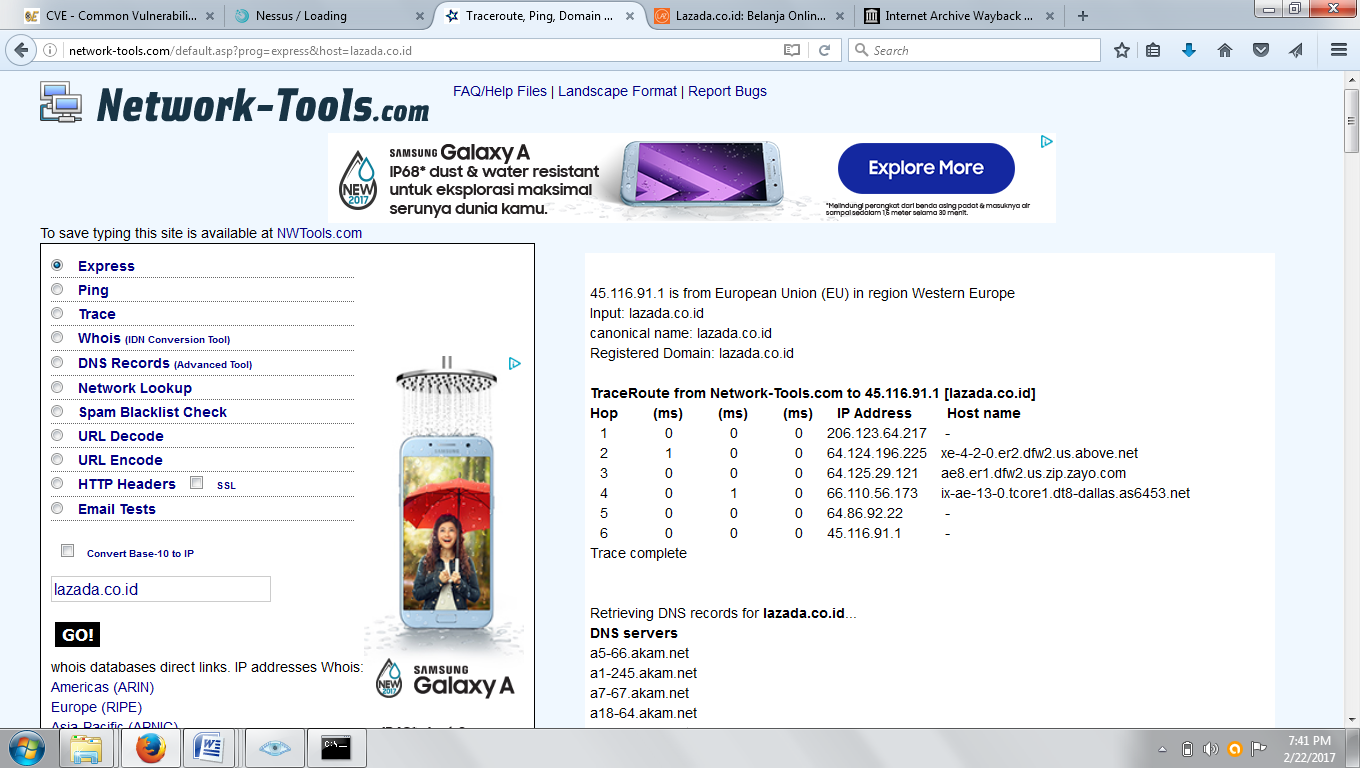
Target Scanning Lazada.co.id

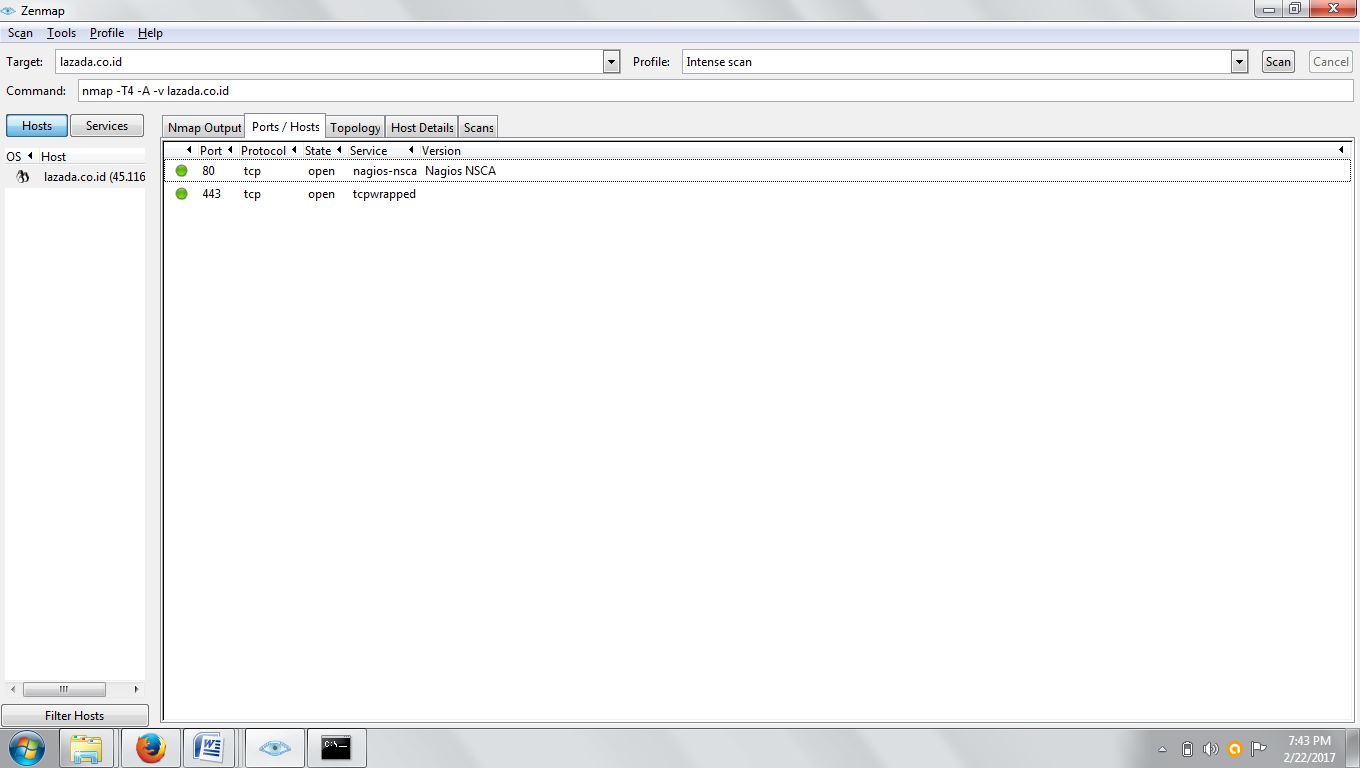
Gambar 1

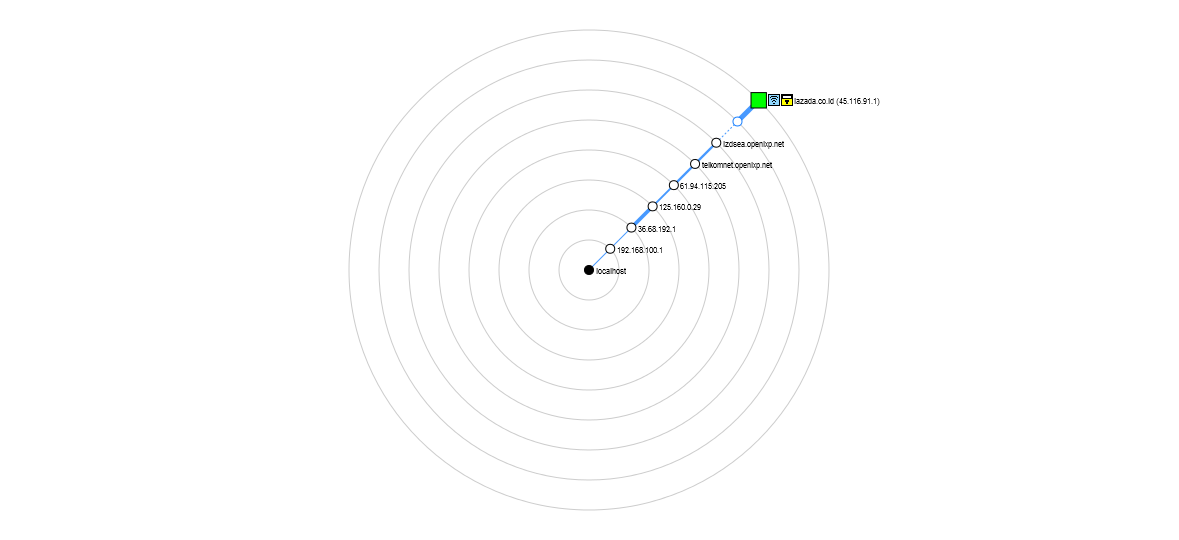


Gambar 2

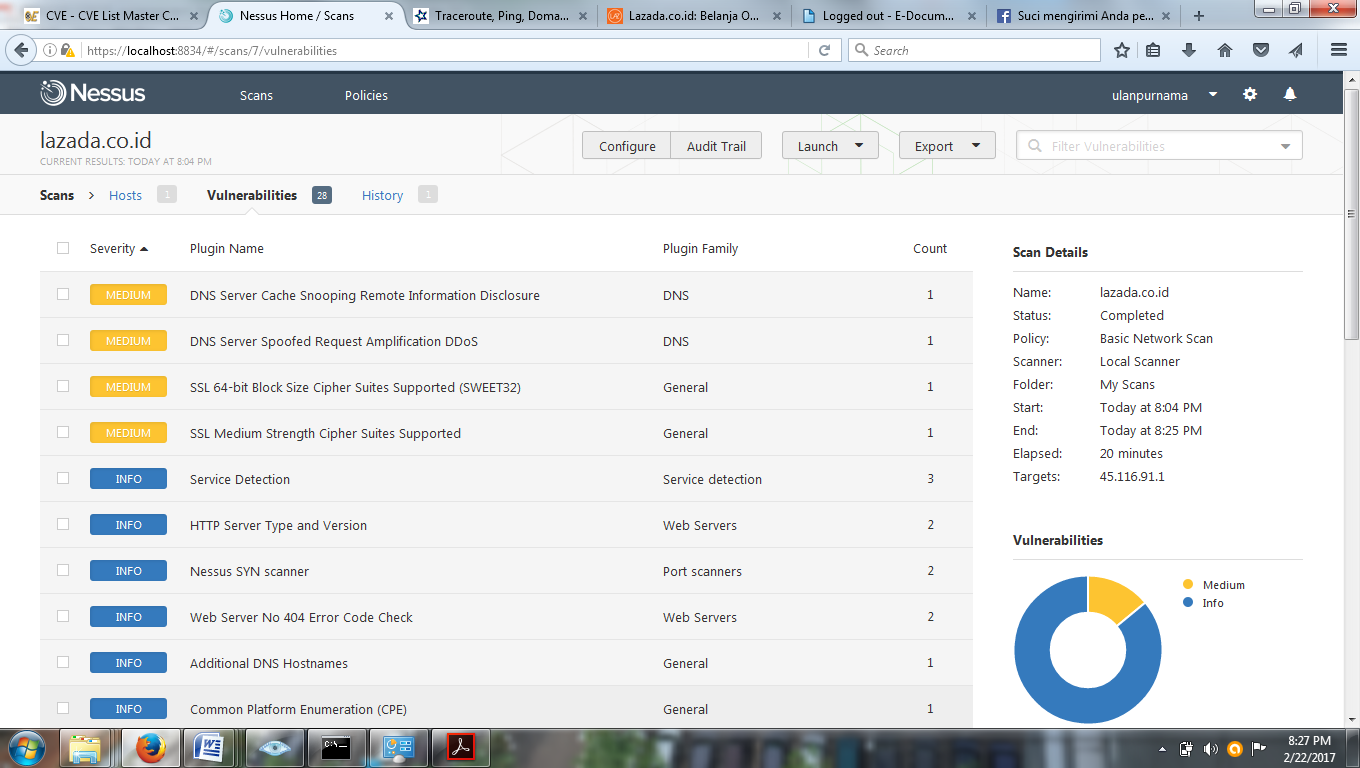
Pada Scanning yang dilakukan dengan software Zenmap dengan target [www.lazada.co.id](http://www.lazada.co.id) (IP Address 45.116.91.1) di dapatkan hasil scanning output yang telah di screenshoot di gambar 1 dan 2.

Port scanning merupakan suatu proses untuk mencari dan membuka port pad asuatu jaringan computer. Dari hasil scanning akan didapat letak kelemahan system tersebut.

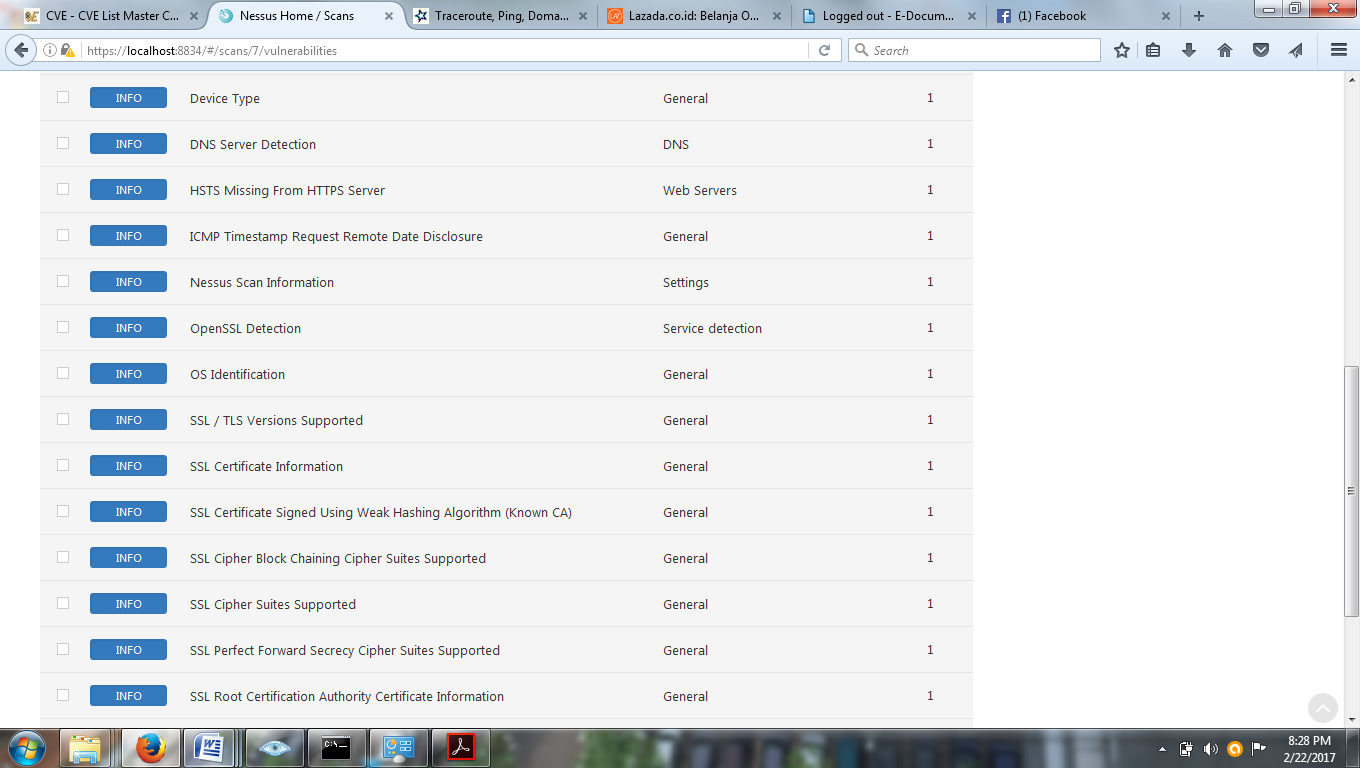
memiliki 6 buah hop pada <http://network-tools.com/>

hanya ada 2 port yang terbuka di situs lazada.co.id yaitu port 80 dan 443 menggunakan protocol TCP.

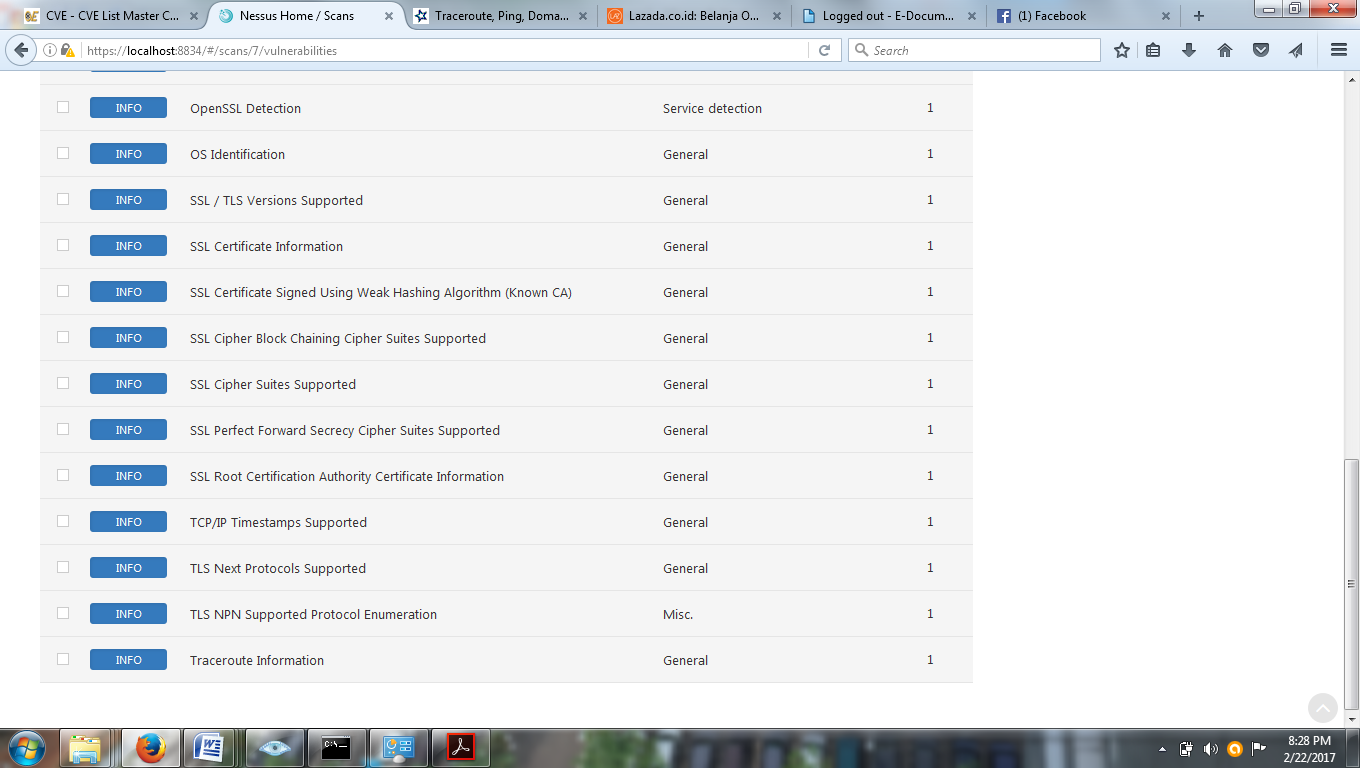
Gambar di atas grafik dari situs lazada.co.id didapatkan dari Nmap.



Gambar 3

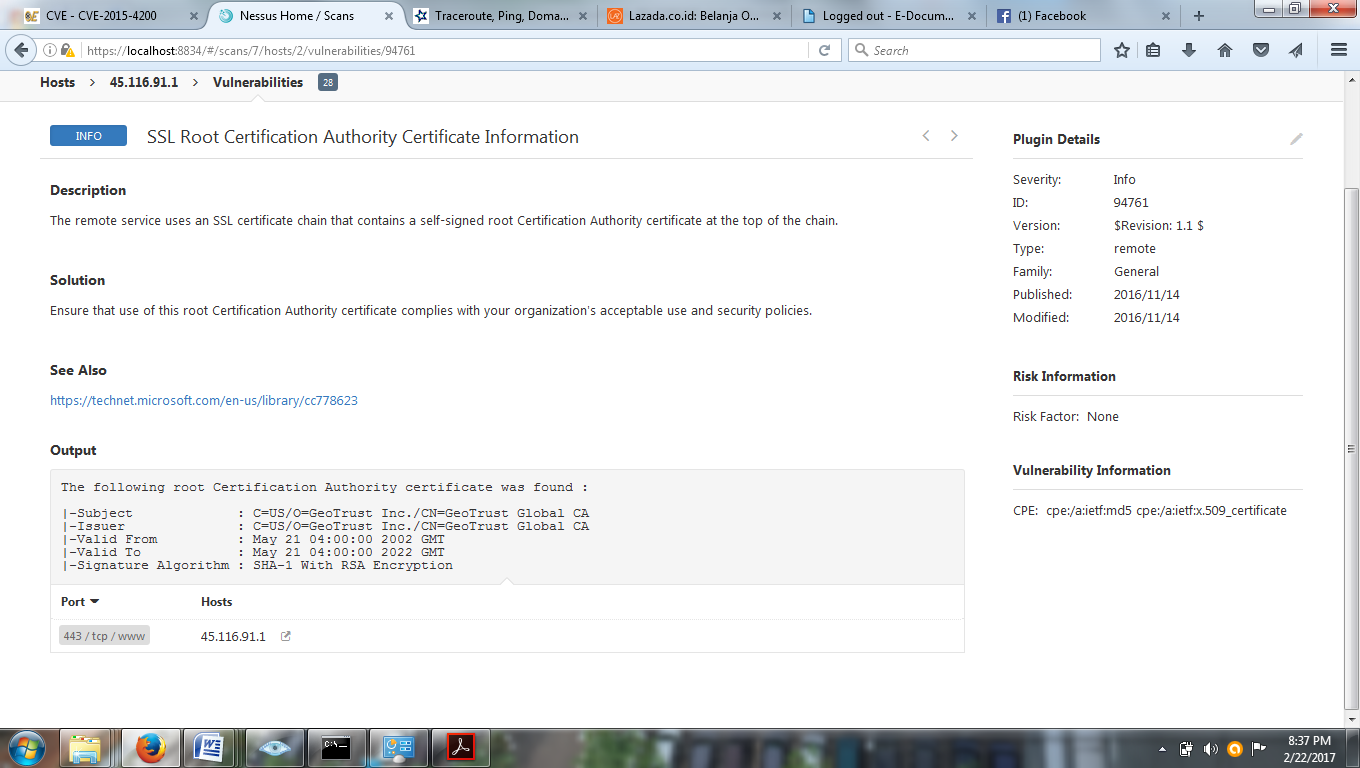


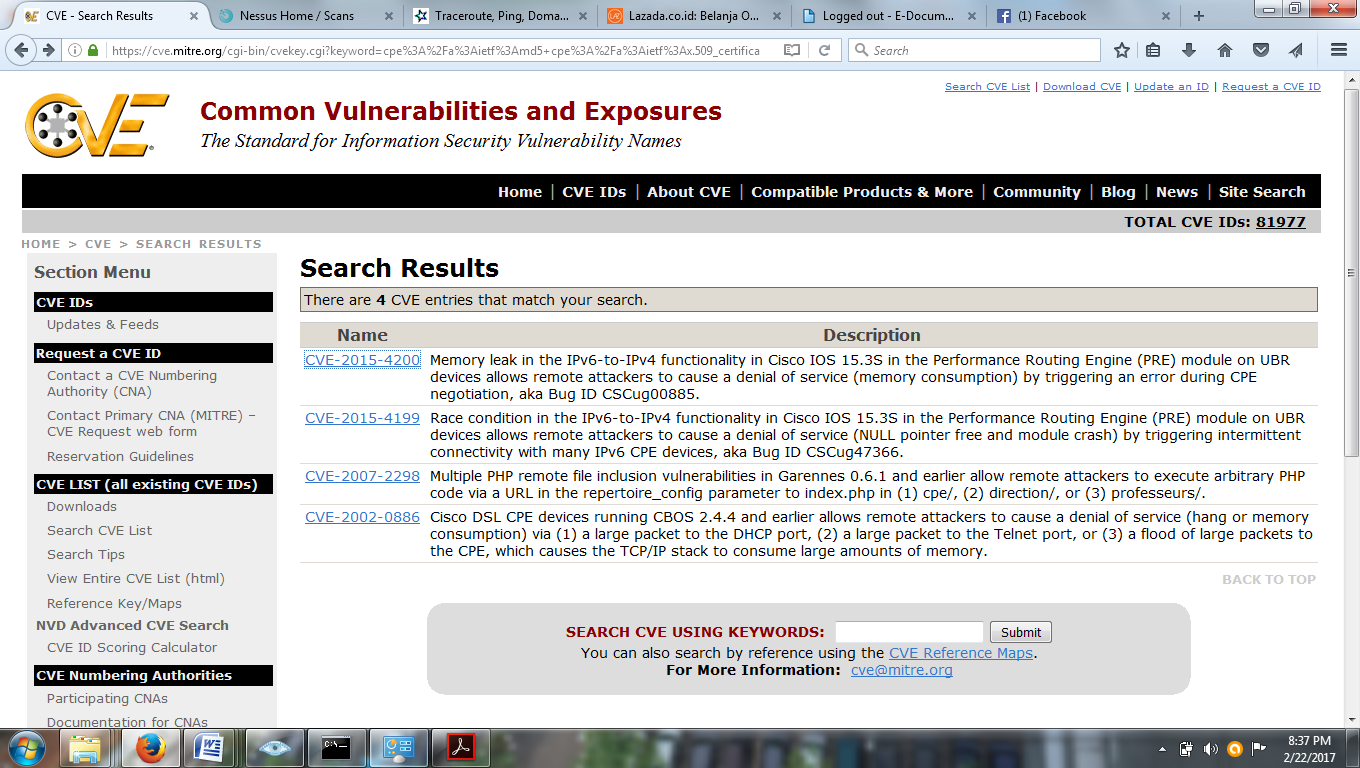
Gambar 4

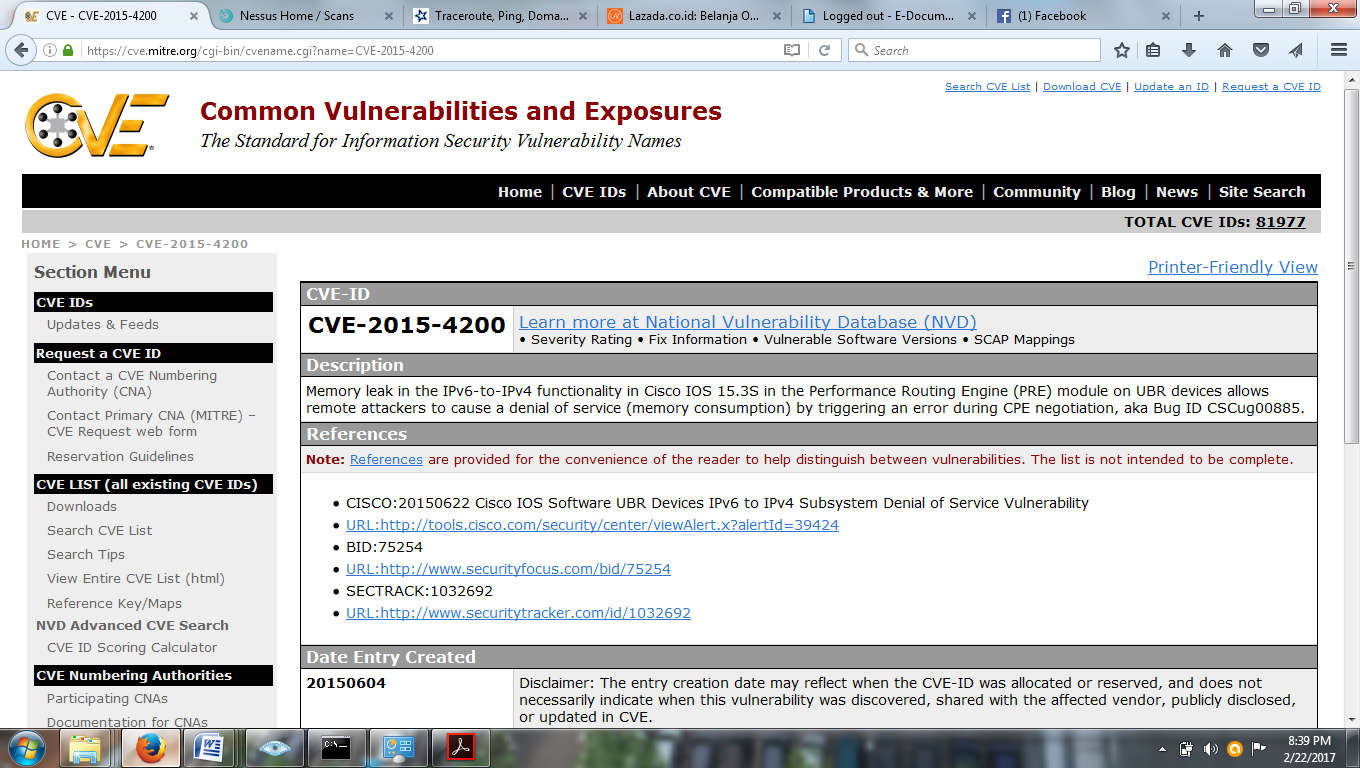


Gambar 5

Pada gambar 3,4 dan 5 hasil dari scanning munggunakan Nessus. Nessus adalah salah satu scanner keamanan jaringan yang harus digunakan oleh administrator system. Nessus merupakan sebuah software scanning, yang dapat digunakan untuk meng-audit kemanan sebuah sistem, seperti vulnerability, misconfiguration, security patch yang belum diaplikasikan, default password, dan denial of service. Nessus berfungsi untuk monitoring lalu-lintas jaringan.







* CISCO: pada tanggal 2015 – 06 - 22
* Cisco IOS Software UBR Devices
* IPv6 to IPv4 Subsystem Denial of Service Vulnerability