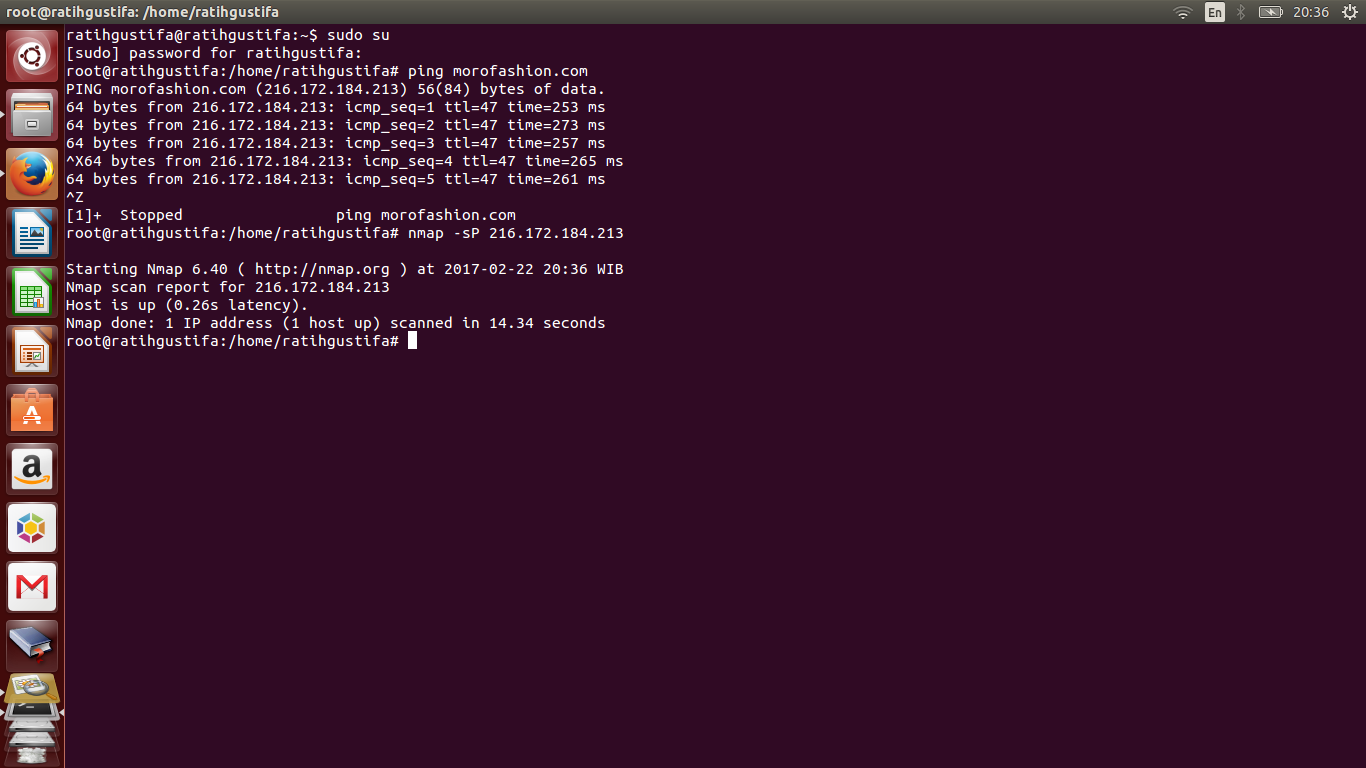
Analisa proses Scanning pada website menggunakan NMAP

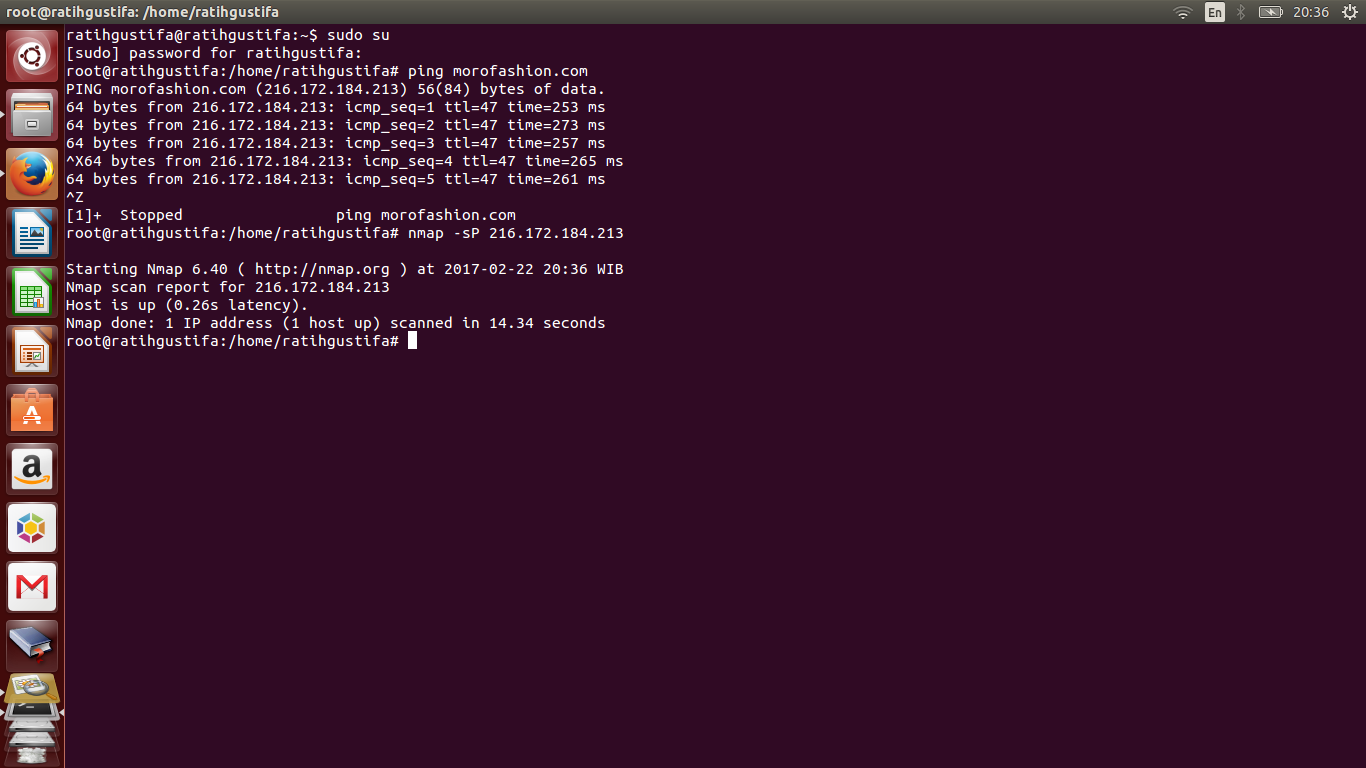
Scanning merupakan Proses yang mana penyerang memiliki gambaran mengenai mesin-mmengenai mesin-mesin jaringan , sistem operasi, lalu administrator dari sistemnya, semua diskusi yang dikirim ke milis , lokasi kantor dan lain lain, pada titik ini seorang penyerang mengetahui bahwa yang akan di lakukannya kemudian mungkin tercatat disistem. Penyerang juga memiliki peta jaringan , perangkat dan tools serta kesiapan untuk mengidentifikasi layanan yang ada untuk membuka port.  
  
Pada proses Scanning kali ini akan di lakukan penyerangan dengan menggunakan tools NMAP , yang mana target yang akan di coba kali ini yaitu sebuah website yaitu www. Morofashion.com. NMAP ini merupakan tools yang bersifat gratis. Scanning kali ini akan di lakukan beberapa tahapan yaitu :

1. mengetahui IP address target   
pada proses ini akan dilakukan proses ping yang mana dengan proses ping ini akan diketahui IP adress yang digunakan target   
pada proses ini menggunakan sintaks sbg berikut :  
$ ping [target]



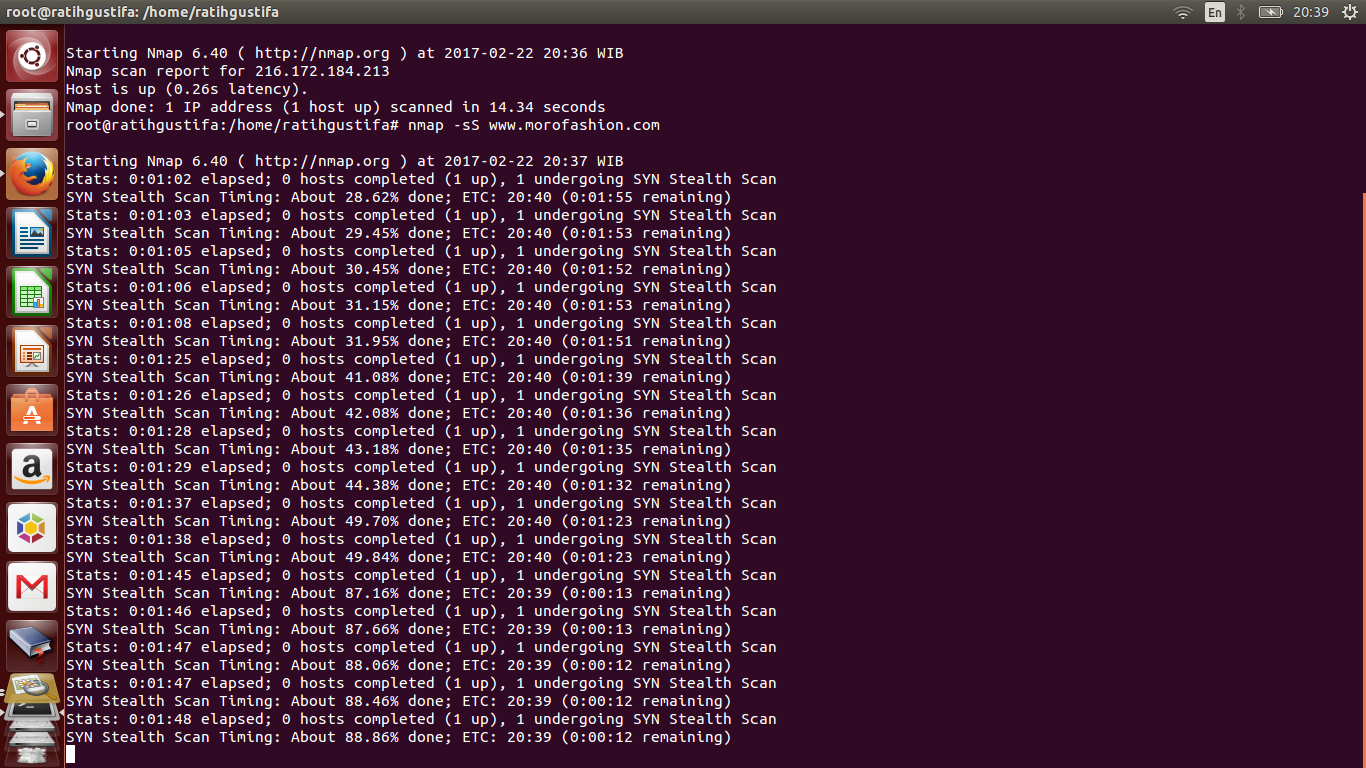
2. Identifying active machine

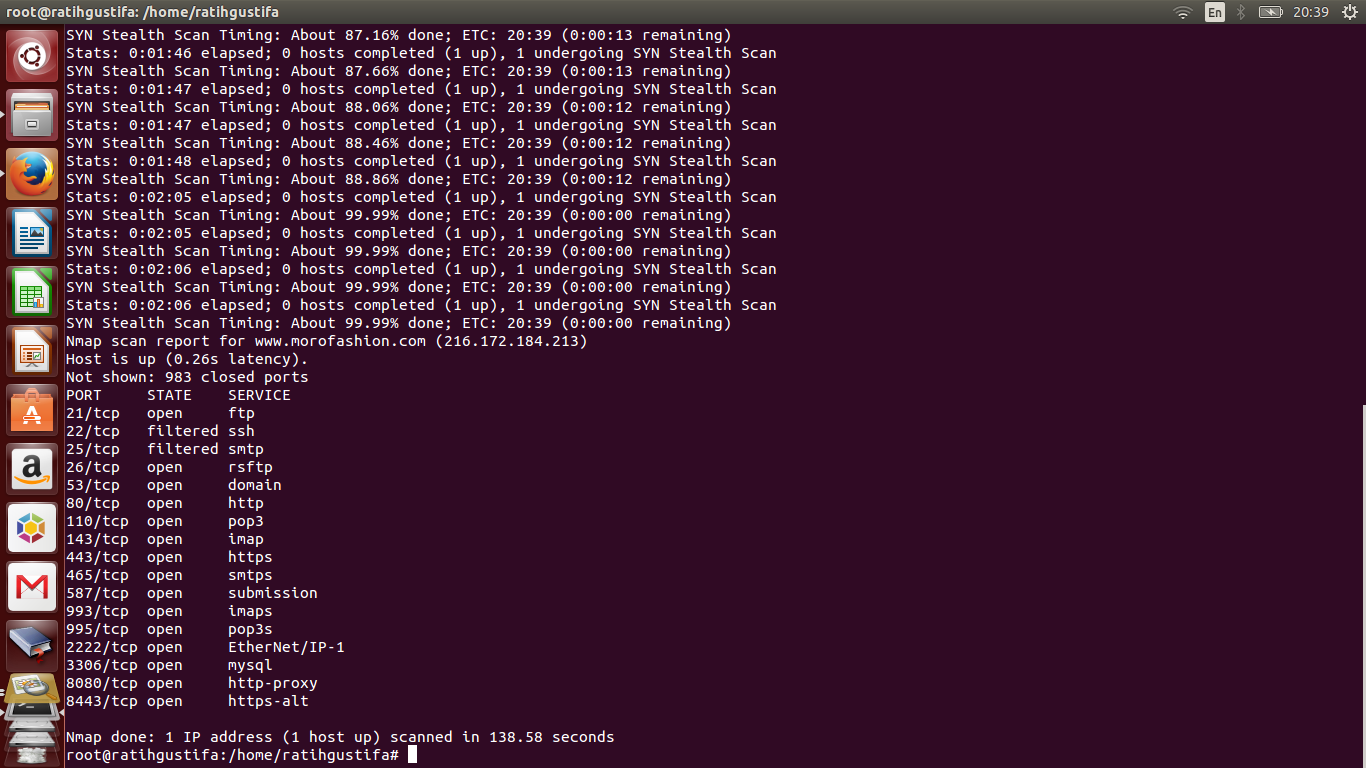
Tahap pertama yang dilakukan adalah mengidentifikasi mesin yang aktif pada range network yang dijadikan target . untuk itu kita menggunakan perintah –sV



3. Finding open ports

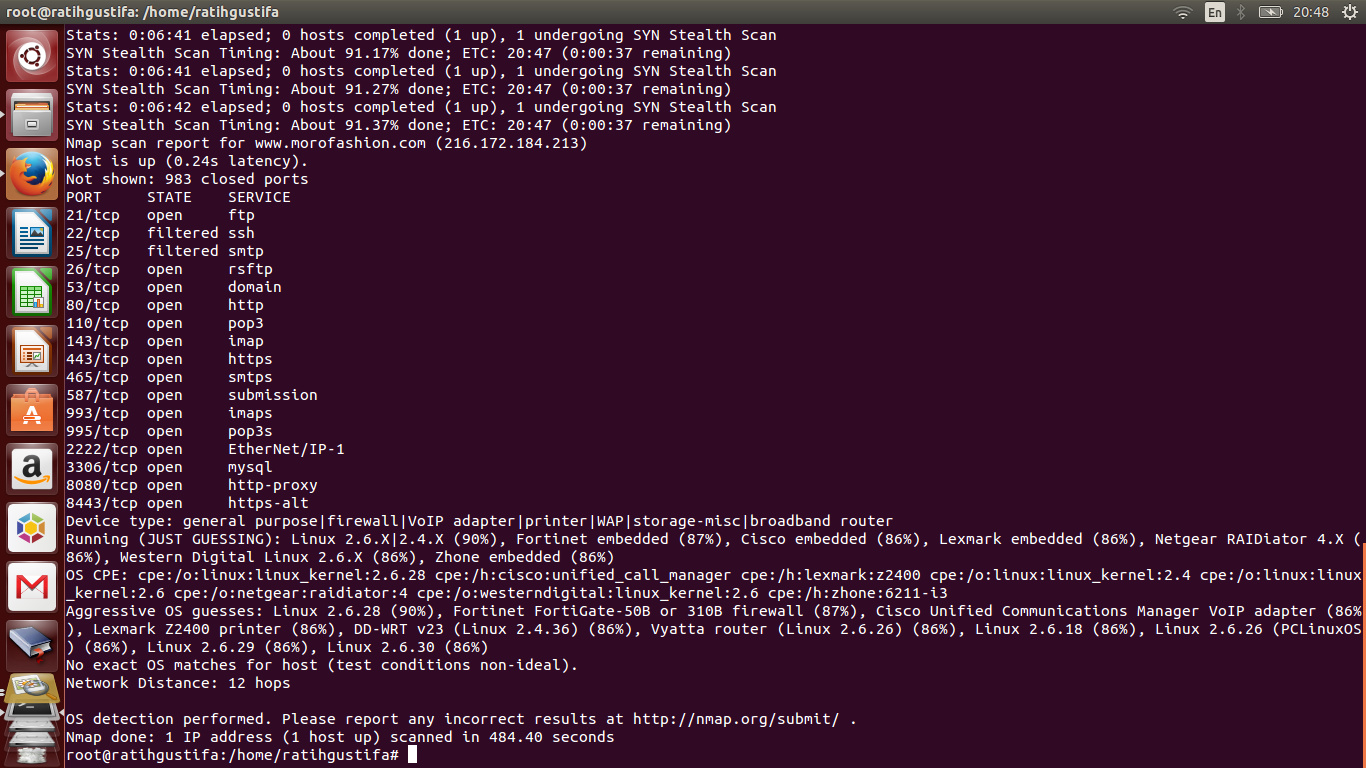
Dengan informasi range network target dan mesin yang aktif, proses selanjutnya adalah scanning port pada mesin yang aktif untuk melihat port yang terbuka. Pada step ini saya menggunakan option "-sS" dan option "-p", dan pilih salah satu ip/mesin yang aktif untuk di-scan





4. OS Fingerprint

Pada bagian proses pengumpulan informasi ini, adalah menentukan sistem operasi apa yang berjalan pada mesin yang aktif untuk mengetahui tipe sistem yang sedang ditest security nya. Kita akan menggunakan option "-O" untuk mendeteksi OS yang berjalan.



Ketika Nmap tidak dapat mendeteksi OS secara tepat, ia terkadang memberikan kemungkinan terdekat. Tebakan yang cocok akan dilakukan oleh Nmap. Dengan option ini membuat Nmap menduga dengan lebih agresif. Nmap tetap akan memberitahu anda ketika kecocokan tidak sempurna, dicetak dan menampilkan tingkat kepercayaan (persentase) untuk setiap dugaan.

4. Service fingerprinting

Setelah port yang open diketahui dengan menggunakan salah satu metode scan diatas, hal selanjutnya adalah deteksi versi dari service yang sedang berjalan. Nmap akan berusaha menentukan nama protokol layanan serta versi dari layananan tersebut. Dan untuk mendeteksi versi dari service tersebut kita menggunakan option "-sV".

