KEAMANAN JARINGAN KOMPUTER

Eko Pratama

09011181320004

Program Studi Sistem Komputer

Fakultas Ilmu Komputer

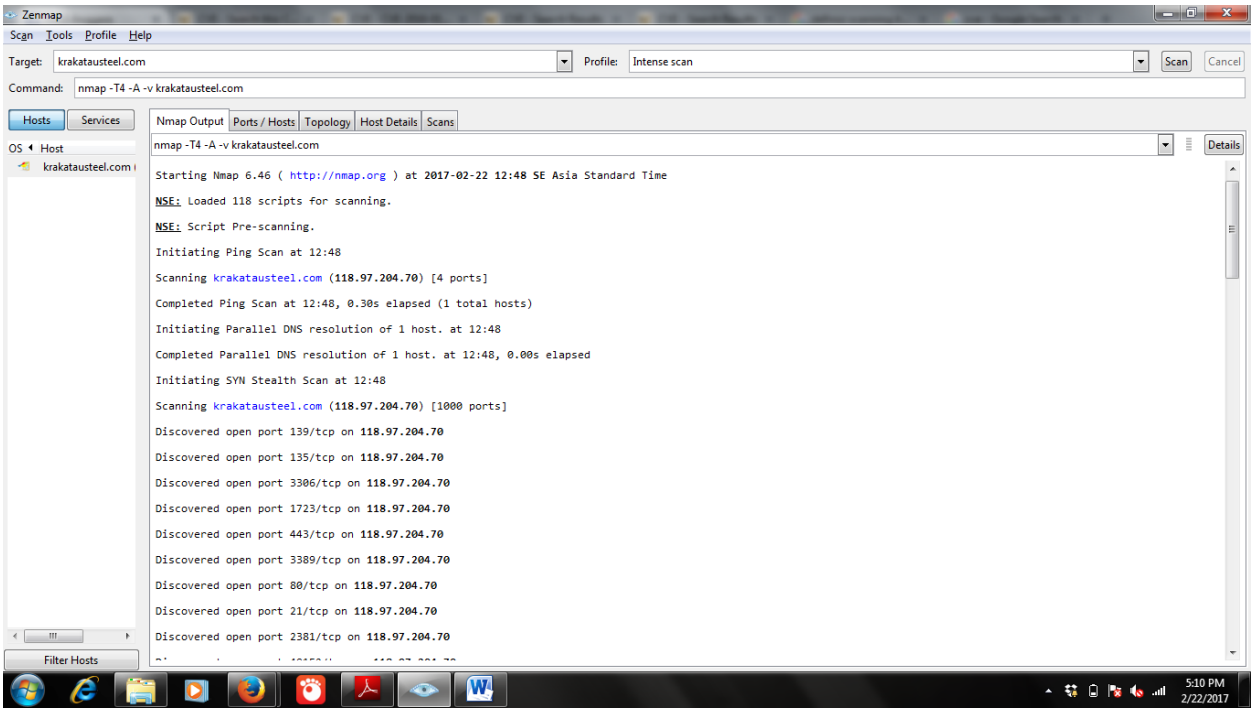
Universitas Sriwijaya

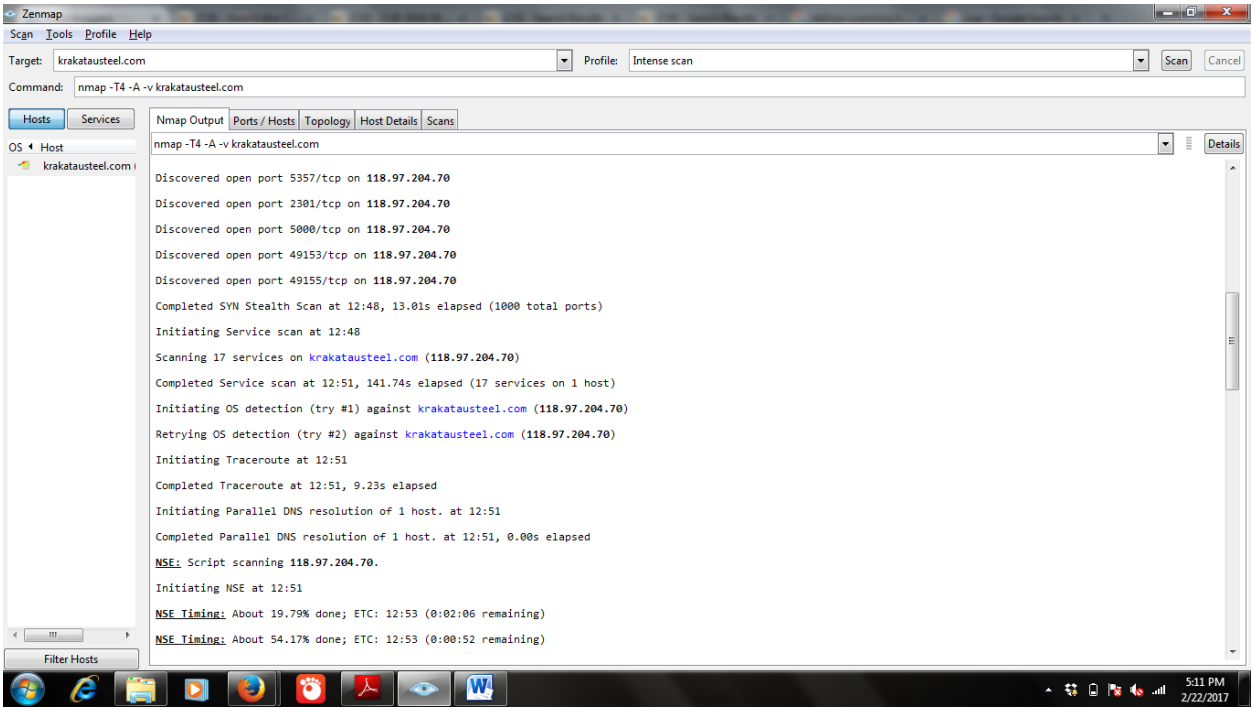
2017

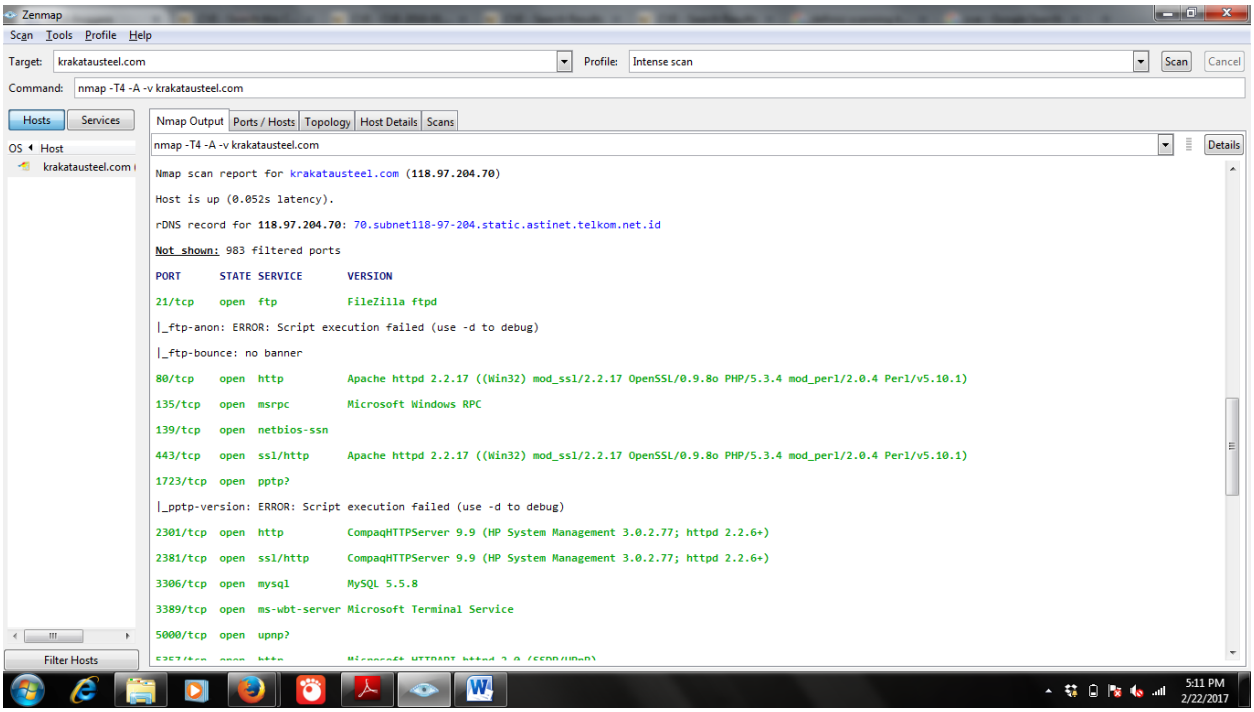
SCANNING

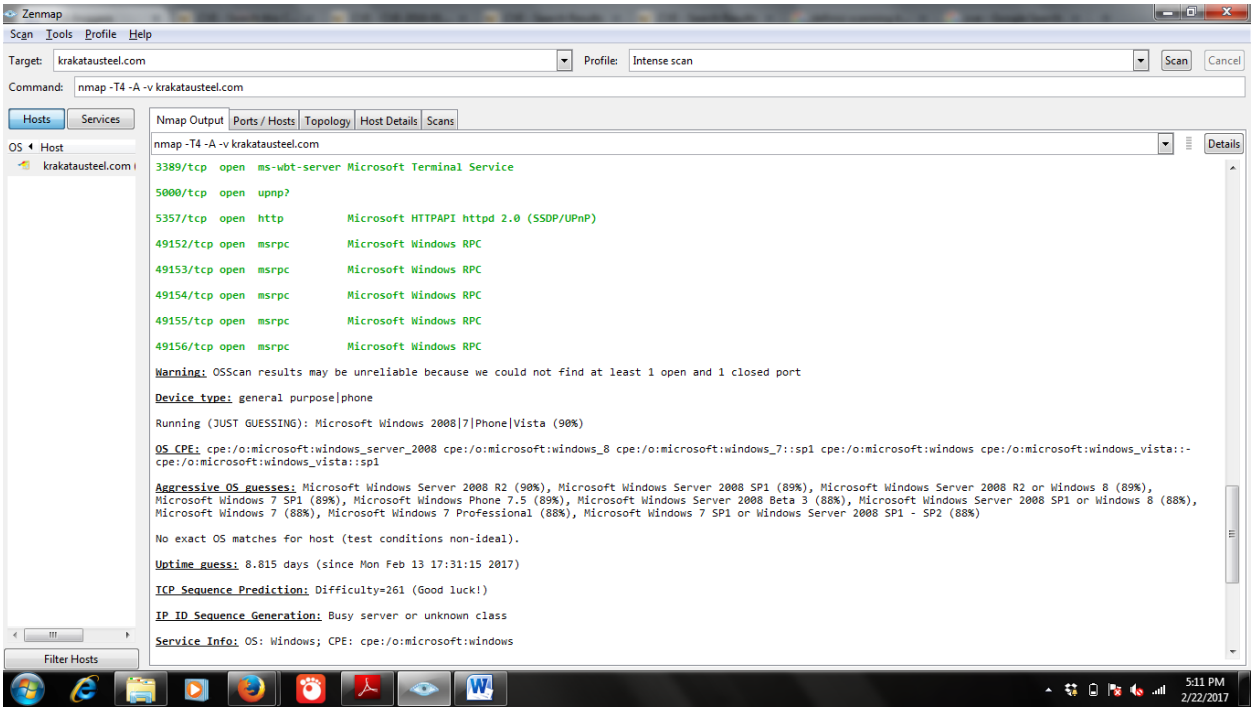
Scanning adalah metode yang digunakan untuk mengetahui keberadaan sebuah user apakah dalam keadaan aktif atau off. Untuk itu diperlukaan sebuah software yang dapat memastikan keberadaan dari user-user yang ada dalam jaringan.

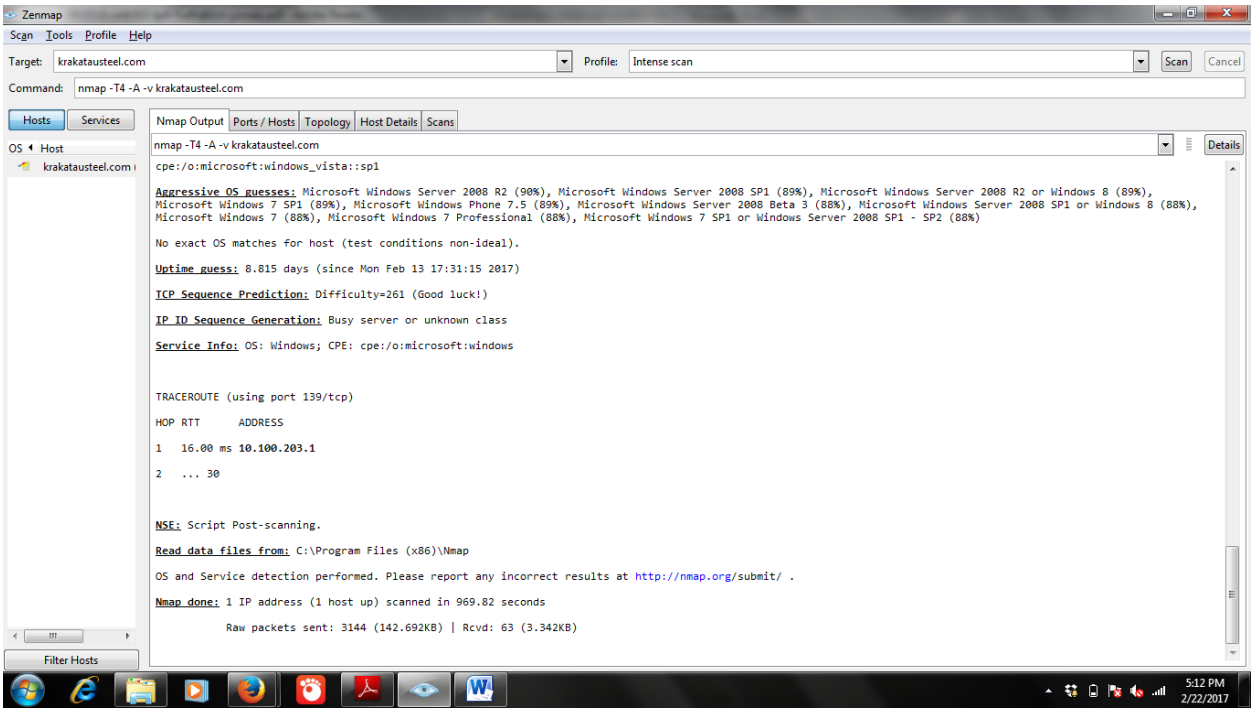
Pada Scanning yang dilakukan dengan software Zenmap dengan target www.krakatausteel.com (IP Address 118.97.204.70) didapatkan hasil scanning output yang telah di screenshoot dibawah:



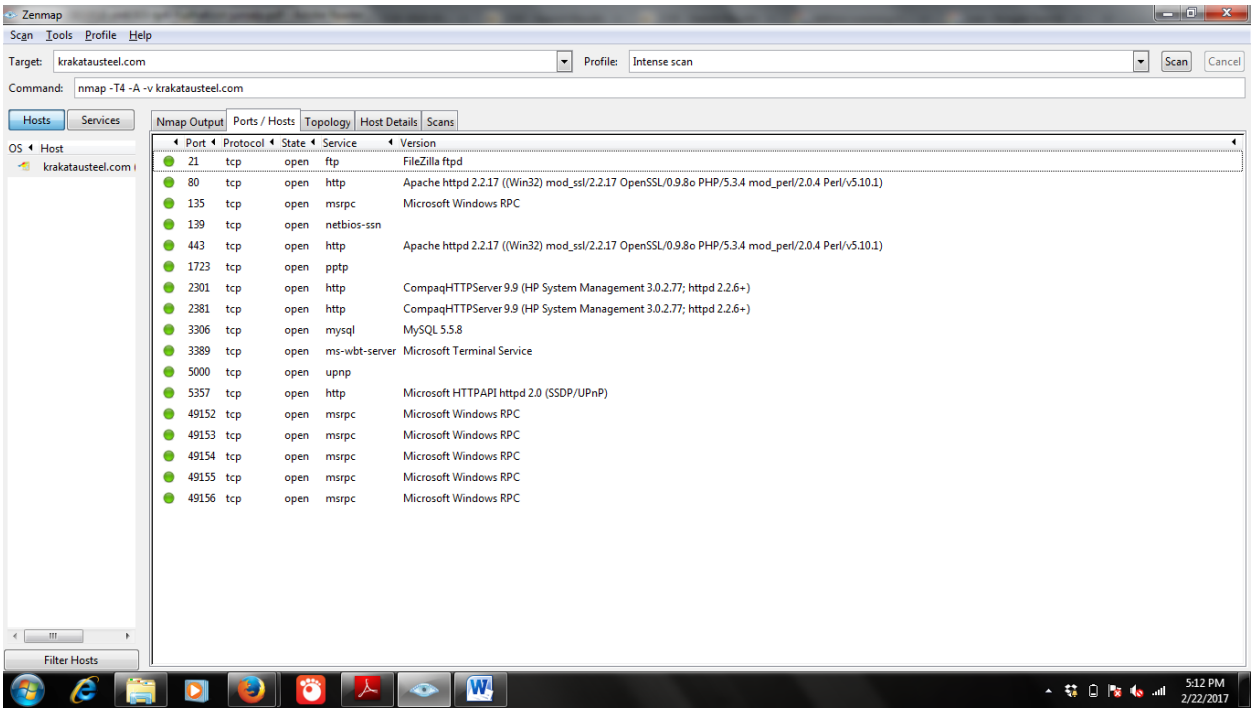

Zenmap
Scan Tools Profile Help
Target: krakatausteel.com
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v krakatausteel.com
Hosts
Services
OS Host
krakatausteel.com
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v krakatausteel.com
Details
Discovered open port 5357/tcp on 118.97.204.70
Discovered open port 2301/tcp on 118.97.204.70
Discovered open port 5000/tcp on 118.97.204.70
Discovered open port 49153/tcp on 118.97.204.70
Discovered open port 49155/tcp on 118.97.204.70
Completed SYN Stealth Scan at 12:48, 13.01s elapsed (1000 total ports)
Initiating Service scan at 12:48
Scanning 17 services on krakatausteel.com (118.97.204.70)
Completed Service scan at 12:51, 141.74s elapsed (17 services on 1 host)
Initiating OS detection (try #1) against krakatausteel.com (118.97.204.70)
Retrying OS detection (try #2) against krakatausteel.com (118.97.204.70)
Initiating Traceroute at 12:51
Completed Traceroute at 12:51, 9.23s elapsed
Initiating Parallel DNS resolution of 1 host. at 12:51
Completed Parallel DNS resolution of 1 host. at 12:51, 0.00s elapsed
NSE: Script scanning 118.97.204.70.
Initiating NSE at 12:51
NSE Timing: About 19.79% done; ETC: 12:53 (0:02:06 remaining)
NSE Timing: About 54.17% done; ETC: 12:53 (0:00:52 remaining)
5:11 PM
2/22/2017


Zenmap
Scan Tools Profile Help
Target: krakatausteel.com
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v krakatausteel.com
Hosts
Services
OS Host
krakatausteel.com
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v krakatausteel.com
Details
Nmap scan report for krakatausteel.com (118.97.204.70)
Host is up (0.052s latency).
rDNS record for 118.97.204.70: 70.subnet118-97-204.static.astinet.telkom.net.id
Not shown: 983 filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp FileZilla ftpd
|_ftp-anon: ERROR: Script execution failed (use -d to debug)
|_ftp-bounce: no banner
80/tcp open http Apache httpd 2.2.17 ((Win32) mod_ssl/2.2.17 OpenSSL/0.9.8o PHP/5.3.4 mod_perl/2.0.4 Perl/v5.10.1)
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn
443/tcp open ssl/http Apache httpd 2.2.17 ((Win32) mod_ssl/2.2.17 OpenSSL/0.9.8o PHP/5.3.4 mod_perl/2.0.4 Perl/v5.10.1)
1723/tcp open pptp?
|_pptp-version: ERROR: Script execution failed (use -d to debug)
2301/tcp open http CompaqHTTPServer 9.9 (HP System Management 3.0.2.77; httpd 2.2.6+)
2381/tcp open ssl/http CompaqHTTPServer 9.9 (HP System Management 3.0.2.77; httpd 2.2.6+)
3306/tcp open mysql MySQL 5.5.8
3389/tcp open ms-wbt-server Microsoft Terminal Service
5000/tcp open upnp?
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5:11 PM
2/22/2017

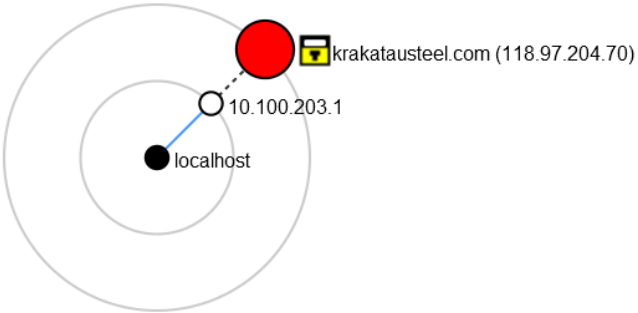

Zenmap
Scan Tools Profile Help
Target: krakatausteel.com
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v krakatausteel.com
Hosts
Services
OS Host
krakatausteel.com
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v krakatausteel.com
Details
3389/tcp open ms-wbt-server Microsoft Terminal Service
5000/tcp open upnp?
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open msrpc Microsoft Windows RPC
49153/tcp open msrpc Microsoft Windows RPC
49154/tcp open msrpc Microsoft Windows RPC
49155/tcp open msrpc Microsoft Windows RPC
49156/tcp open msrpc Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running (JUST GUESSING): Microsoft Windows 2008|7|Phone|Vista (90%)
OS CPE: cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows Server 2008 R2 (90%), Microsoft Windows Server 2008 SP1 (89%), Microsoft Windows Server 2008 R2 or Windows 8 (89%), Microsoft Windows 7 SP1 (89%), Microsoft Windows Phone 7.5 (89%), Microsoft Windows Server 2008 Beta 3 (88%), Microsoft Windows Server 2008 SP1 or Windows 8 (88%), Microsoft Windows 7 (88%), Microsoft Windows 7 Professional (88%), Microsoft Windows 7 SP1 or Windows Server 2008 SP1 - SP2 (88%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 8.815 days (since Mon Feb 13 17:31:15 2017)
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Filter Hosts
5:11 PM
2/22/2017


Zenmap
Scan Tools Profile Help
Target: krakatausteel.com
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v krakatausteel.com
Hosts
Services
OS Host
krakatausteel.com
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v krakatausteel.com
Details
cpe:/o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows Server 2008 R2 (90%), Microsoft Windows Server 2008 SP1 (89%), Microsoft Windows Server 2008 R2 or Windows 8 (89%), Microsoft Windows 7 SP1 (89%), Microsoft Windows Phone 7.5 (89%), Microsoft Windows Server 2008 Beta 3 (88%), Microsoft Windows Server 2008 SP1 or Windows 8 (88%), Microsoft Windows 7 (88%), Microsoft Windows 7 Professional (88%), Microsoft Windows 7 SP1 or Windows Server 2008 SP1 - SP2 (88%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 8.815 days (since Mon Feb 13 17:31:15 2017)
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
TRACEROUTE (using port 139/tcp)
HOP RTT ADDRESS
1 16.00 ms 10.100.203.1
2 ... 30
NSE: Script Post-scanning.
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 969.82 seconds
Raw packets sent: 3144 (142.692KB) | Rcvd: 63 (3.342KB)
Filter Hosts
5:12 PM
2/22/2017

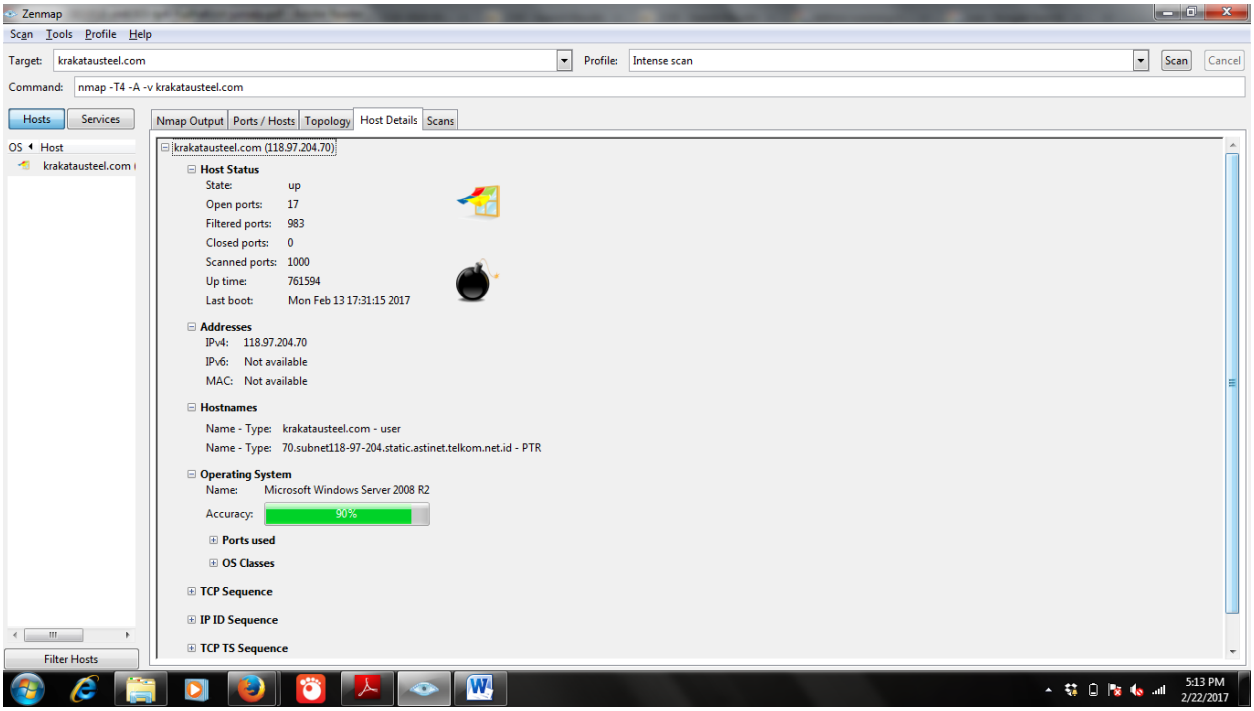
Port scanning merupakan suatu proses untuk mencari dan membuka port pada suatu jaringan computer. Dari hasil scanning akan didapat letak kelemahan sistem tersebut. Hasil screenshoot dibawah merupakan beberapa port yang terbuka untuk memulai serangan.



Dapat dilihat dari Gambar diatas bahwa terdapat 17 Port yang terbuka yang biasa digunakan penyerang untuk masuk melakukan serangan disalah satu port tersebut. Seperti diantaranya port 21, 80 , 135, 139, dll. Dari screenshoot diatas terlihat bahwa seluruh port yang terbuka menggunakan protocol TCP.



Dari gambar dibawah dapat dilihat hasil hop dari localhost menuju ke PT.Krakatau Steel dimana terjadi 2 hop. Hop pertama menuju ke IP 10.100.203.1 sebelum akhirnya sampai ke IP 118.97.204.70 milik KrakatauSteel.com



Screenshoot diatas menggambarkan tentang detail dari hosts yang dimana terdapat beberapa status dari host itu sendiri seperti yang terjadi ketika selesai melakukan scanning didapatkan StateUP, Port yang terbuka 17, port yang terfilter 983, port yang tertutup tidak ada, Port yang terscan 1000 dan Operating System yang digunakan target adalah Microsoft Windows Server 2008 R2.