

TUGAS KEAMANAN JARINGAN KOMPUTER

“Scanning”



OLEH : ERICK OKVANTY HARIS

NIM : 09011181320012

SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
INDRALAYA

2016

Nmap

Nmap (Network Mapper) adalah sebuah aplikasi atau tool yang berfungsi untuk melakukan *port scanning*. Nmap dibuat oleh Gordon Lyon, atau lebih dikenal dengan nama Fyodor Vaskovich. Aplikasi ini digunakan untuk meng-audit jaringan yang ada. Sistem Operasi yang digunakan, dan feature-feature scanning lainnya. Pada awalnya, Nmap hanya bisa berjalan di sistem operasi Linux, namun dalam perkembangannya sekarang ini, hampir semua sistem operasi bisa menjalankan Nmap ini. disisi lain Nmap (Network Mapper) adalah sebuah program open source yang berguna untuk mengeksplorasi jaringan. Nmap didesain untuk dapat melakukan scan jaringan yang besar, juga dapat digunakan untuk melakukan scan host tunggal. Nmap menggunakan paket IP untuk menentukan host- host yang aktif dalam suatu jaringan, port-port yang terbuka, sistem operasi yang dipunyai, tipe firewall yang dipakai, dll.

1. Hasil scanning menggunakan Command Prompt dan Zenmap GUI

- Proses Quick Scanning

```
C:\Users\Erick Okvanty Haris>nmap -sU -T4 -F www.blibli.com
Starting Nmap 6.46 < http://nmap.org > at 2017-02-22 19:37 Pacific Standard Time
Nmap scan report for www.blibli.com (202.158.55.137)
Host is up (0.044s latency).
rDNS record for 202.158.55.137: ip55-137.chn.net.id
Not shown: 92 closed ports
PORT      STATE      SERVICE      VERSION
25/tcp    filtered  smtp
80/tcp    open      http         BigIP
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
443/tcp   open      ssl/https?
3128/tcp  filtered  squid-http
8080/tcp  filtered  http-alt
8080/tcp  filtered  http-proxy

Service detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 209.75 seconds
```

- Proses Full Scan

```
C:\Users\Erick Okvanty Haris>nmap -sT www.blibli.com
Starting Nmap 6.46 < http://nmap.org > at 2017-02-22 20:38 Pacific Standard Time
Nmap scan report for www.blibli.com (202.158.55.137)
Host is up (0.0025s latency).
rDNS record for 202.158.55.137: ip55-137.cbn.net.id
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 83.06 seconds
C:\Users\Erick Okvanty Haris>
```

Gambar.1.1 proses scanning menggunakan Nmap pada Command Prompt

Pada gambar 1 ini target yang dipilih yaitu www.blibli.com, menggunakan command line `-sV` (Version Detection Scan) yang berfungsi untuk menghasilkan beberapa output port yang terbuka.

Zenmap GUI:

Scan Tools Profile Help

Target: Profile:

Command:

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

www.blibli.com (20)

nmap -T4 -A -v www.blibli.com

Starting Nmap 6.46 (<http://nmap.org>) at 2017-02-21 21:57 Pacific Standard Time
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 21:57
Scanning www.blibli.com (202.158.55.137) [4 ports]
Completed Ping Scan at 21:57, 0.61s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:57
Completed Parallel DNS resolution of 1 host. at 21:57, 1.38s elapsed
Initiating SYN Stealth Scan at 21:57
Scanning www.blibli.com (202.158.55.137) [1000 ports]
Discovered open port 443/tcp on 202.158.55.137
Discovered open port 80/tcp on 202.158.55.137
Discovered open port 8254/tcp on 202.158.55.137
Completed SYN Stealth Scan at 21:57, 6.53s elapsed (1000 total ports)
Initiating Service scan at 21:57
Scanning 3 services on www.blibli.com (202.158.55.137)
Completed Service scan at 22:00, 152.15s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against www.blibli.com (202.158.55.137)
Retrying OS detection (try #2) against www.blibli.com (202.158.55.137)
Initiating Traceroute at 22:00
Completed Traceroute at 22:00, 0.03s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 22:00
Completed Parallel DNS resolution of 2 hosts. at 22:00, 0.01s elapsed
NSE: Script scanning 202.158.55.137.
Initiating NSE at 22:00
Completed NSE at 22:01, 97.10s elapsed
Nmap scan report for www.blibli.com (202.158.55.137)
Host is up (0.011s latency).
rDNS record for 202.158.55.137: ip55-137.cbn.net.id
Not shown: 989 closed ports
PORT STATE SERVICE VERSION
25/tcp filtered smtp
80/tcp open http BigIP
_http-methods: No Allow or Public header in OPTIONS response (status code 302)
_http-server-header: Software version grabbed from Server header.
_Consider submitting a service fingerprint.
_Run with --script-args http-server-header.skip
_http-title: Did not follow redirect to https://www.blibli.com/

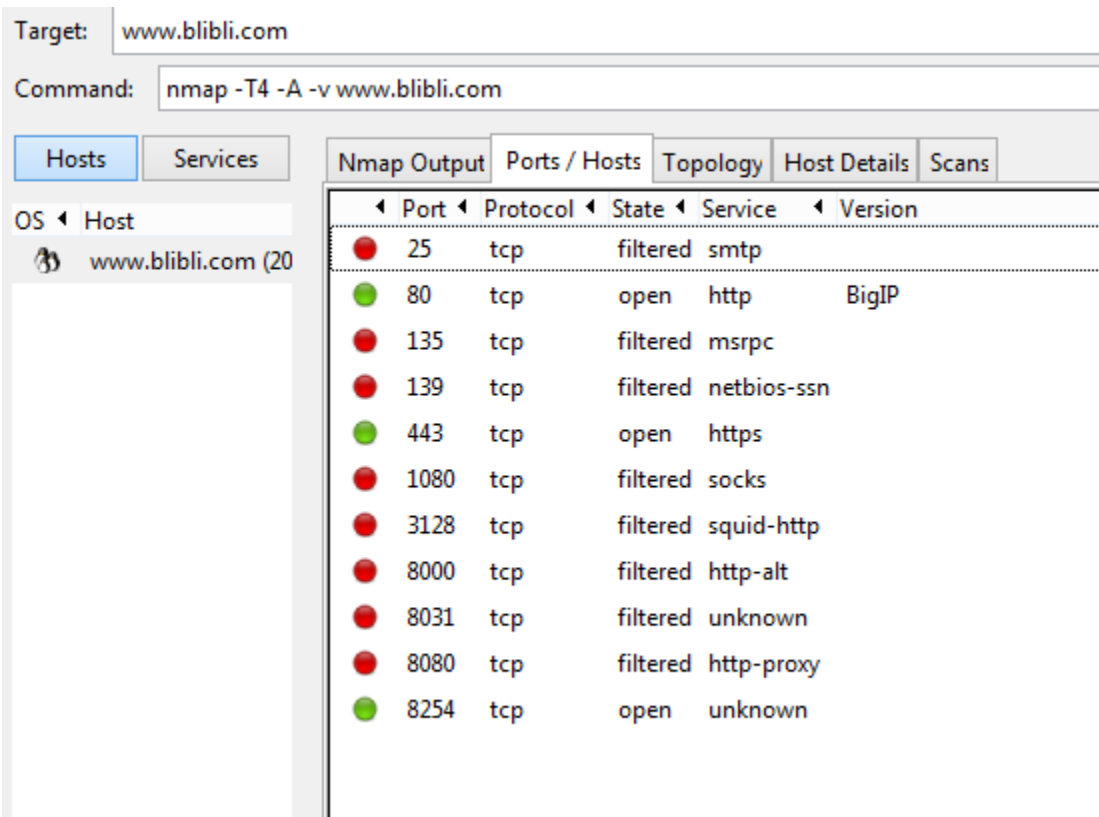
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
443/tcp open ssl/https?
_http-favicon: Unknown favicon MD5: 91DFB2FEF8B43F7BC8C552A838BE232A
_http-methods: GET HEAD POST PUT DELETE TRACE OPTIONS PATCH
_Potentially risky methods: PUT DELETE TRACE PATCH
_See <http://nmap.org/nsedoc/scripts/http-methods.html>
_http-robots.txt: 9 disallowed entries
_/_cgi-bin/_/_wp-admin/_/_wp-includes/_/_wp-content/_/_archives/_/_replytocon/_/_wp-*/_/_author/_/_comments/_/_feed/_
_http-title: Toko Online Blibli.com, Sensasi Belanja Online Shop ala Mall
_ssl-cert: Subject: commonName=www.blibli.com/organizationName=PT GLOBAL DIGITAL NIAGA/stateOrProvinceName=DKI Jakarta/countryName=ID
_Issuer: commonName=Symantec Class 3 EV SSL CA - G3/organizationName=Symantec Corporation/countryName=US
_Public Key type: rsa
_Public Key bits: 2048
_Not valid before: 2015-05-26T23:00:00+00:00
_Not valid after: 2017-07-17T22:59:59+00:00
_MD5: bd41 86c0 1fd2 7988 3177 e0c4 d634 c2ad
_SHA-1: 59e2 c3d5 8e29 c98c ce91 5ed0 6114 33b2 0ca3 cb2c
1080/tcp filtered socks
3128/tcp filtered squid-http
8000/tcp filtered http-alt
8031/tcp filtered unknown
8080/tcp filtered http-proxy
8254/tcp open unknown
Device type: general purpose
Running (JUST GUESSED): Linux 2.6.X (87%)
OS CPE: ope:/o:linux:linux_kernel:2.6
Aggressive OS guesses: Linux 2.6.18 (87%), Linux 2.6.9 - 2.6.27 (87%), Linux 2.6.10 (CentOS 5, x86_64, SMP) (86%), Linux 2.6.15 - 2.6.30 (85%), Linux 2.6.22 (85%), Linux 2.6.8 - 2.6.27 (85%), Linux 2.6.9 - 2.6.18 (85%), Linux 2.6.11 (Auditor) (85%), Linux 2.6.5 (SUSE Enterprise Server 9) (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 11.917 days (since Fri Feb 10 00:01:05 2017)
Network Distance: 2 hops

```

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 1.00 ms 10.94.16.1
2 1.00 ms ip55-137.cbn.net.id (202.158.55.137)

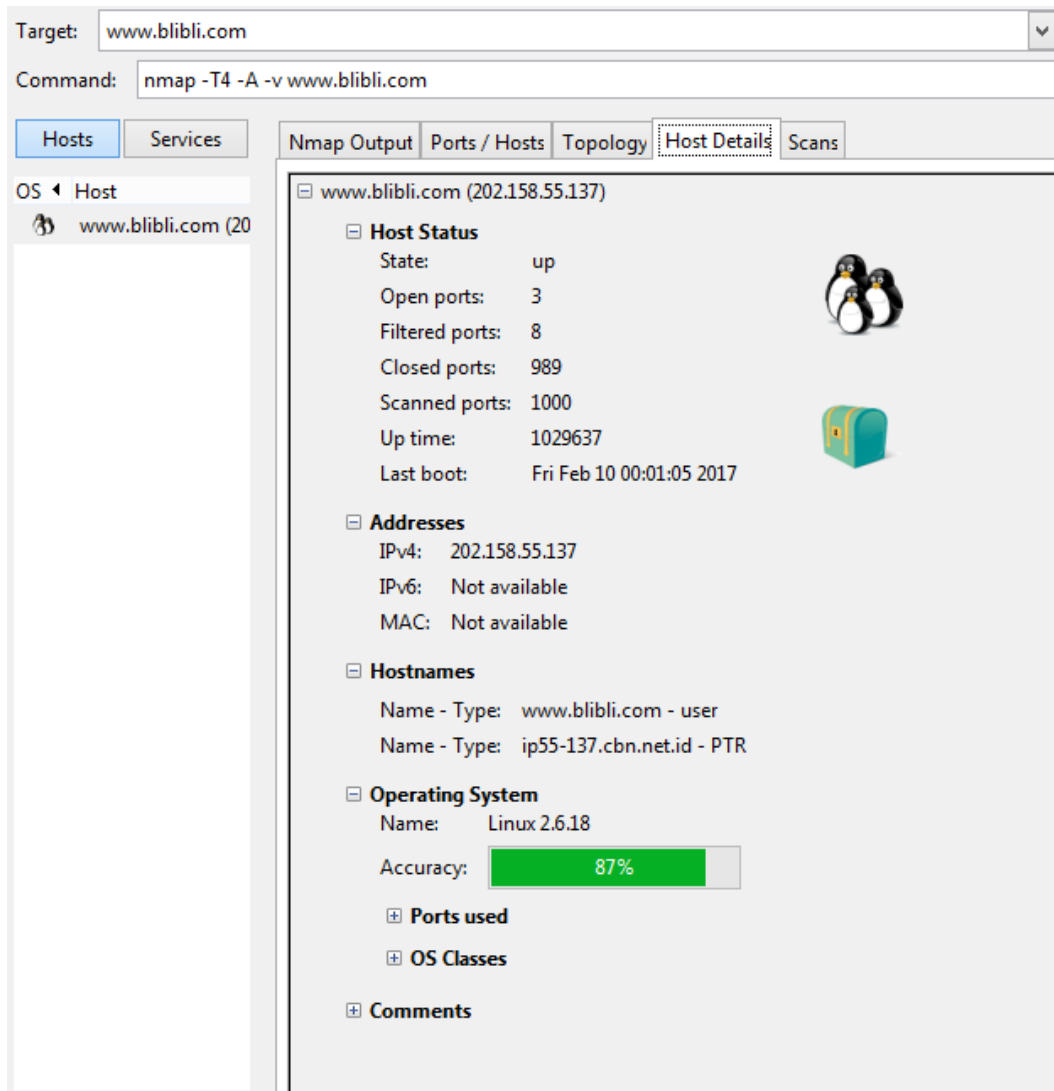
NSE: Script Post-scanning.
Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 272.23 seconds
Raw packets sent: 1126 (51.624KB) | Rcvd: 1046 (43.008KB)

```



Gambar.2 Scanning menggunakan Zenmap GUI

Dari hasil scanning diatas, domain www.blibli.com memiliki tiga buah port yang terbuka, yaitu port 80/tcp , port 443/tcp dan port8254/tcp. Port 80/tcp merupakan port HTTP World Wide Web dari domain itu sendiri dan port 443/tcp adalah protokol yang didefinisikan untuk berkomunikasi tergantung pada aplikasi namun berbeda dengan kedua port tersebut, dikarenakan port tersebut tidak diketahui .



Gambar.3 Informasi mengenai Host Detail

Pada informasi yang kita dapat pada Gambar.3 terdapat informasi mengenai host status, addresses, hostnames, dan operating system. Pada gambar diatas menunjukkan bahwa terdapat 1000 port, diantaranya adalah 3 prt yang terbuka, prt yang terfilterisasi ada 8 port, kemudian 989 port yang tertutup. Kemudian IP pada www.blibli.com menggunakan IPV4 : 202.158.55.137 yang menggunakan OS Linux Versi 2.6.18 Dengan akurasi sebanyak 87%.