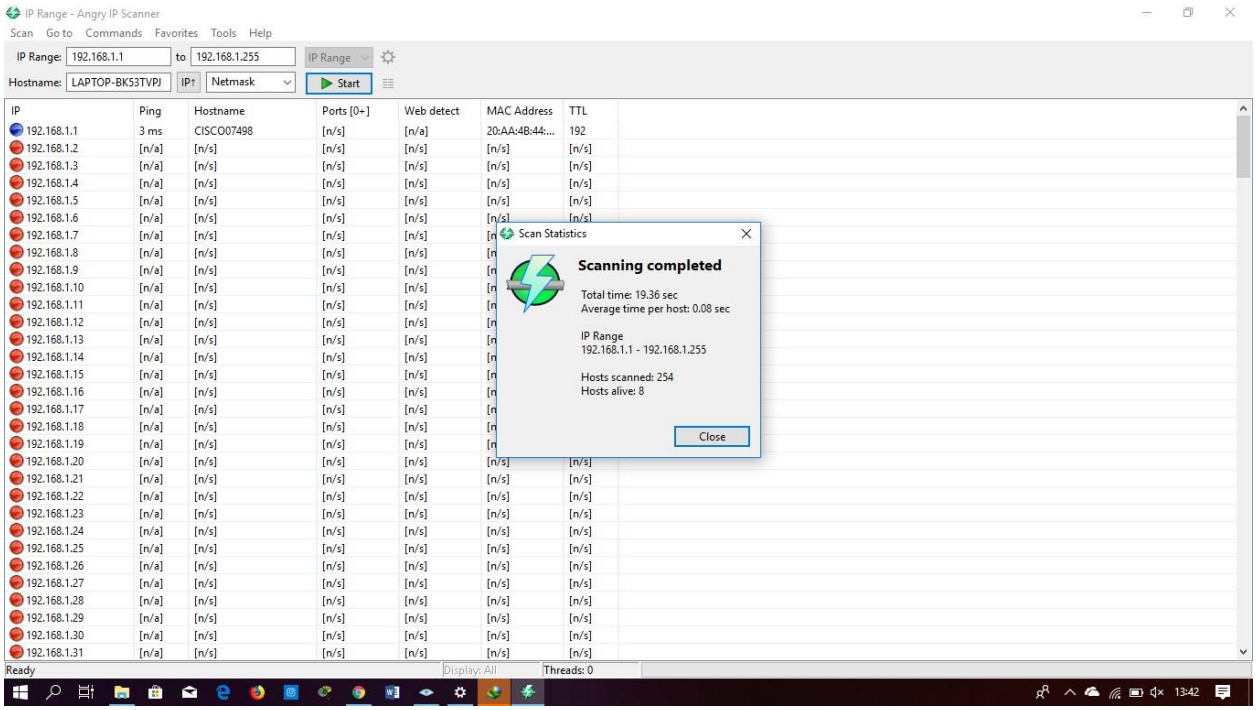
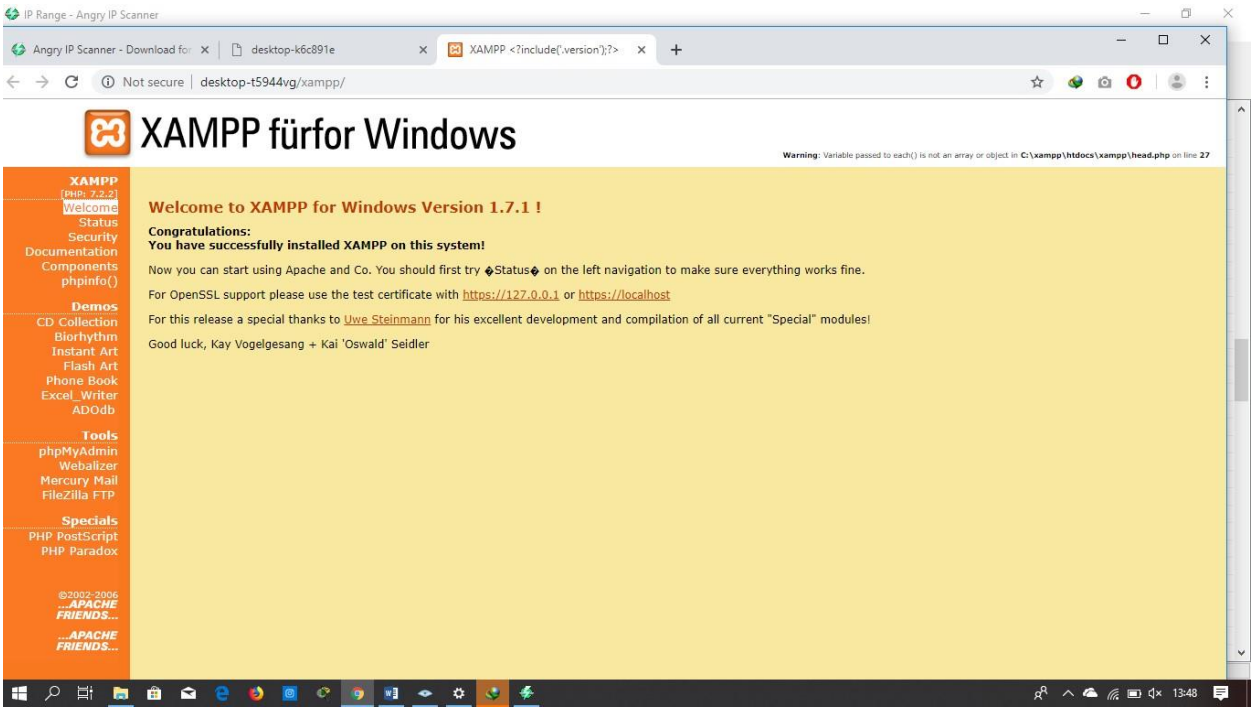
Nama : Ahmad Faisal

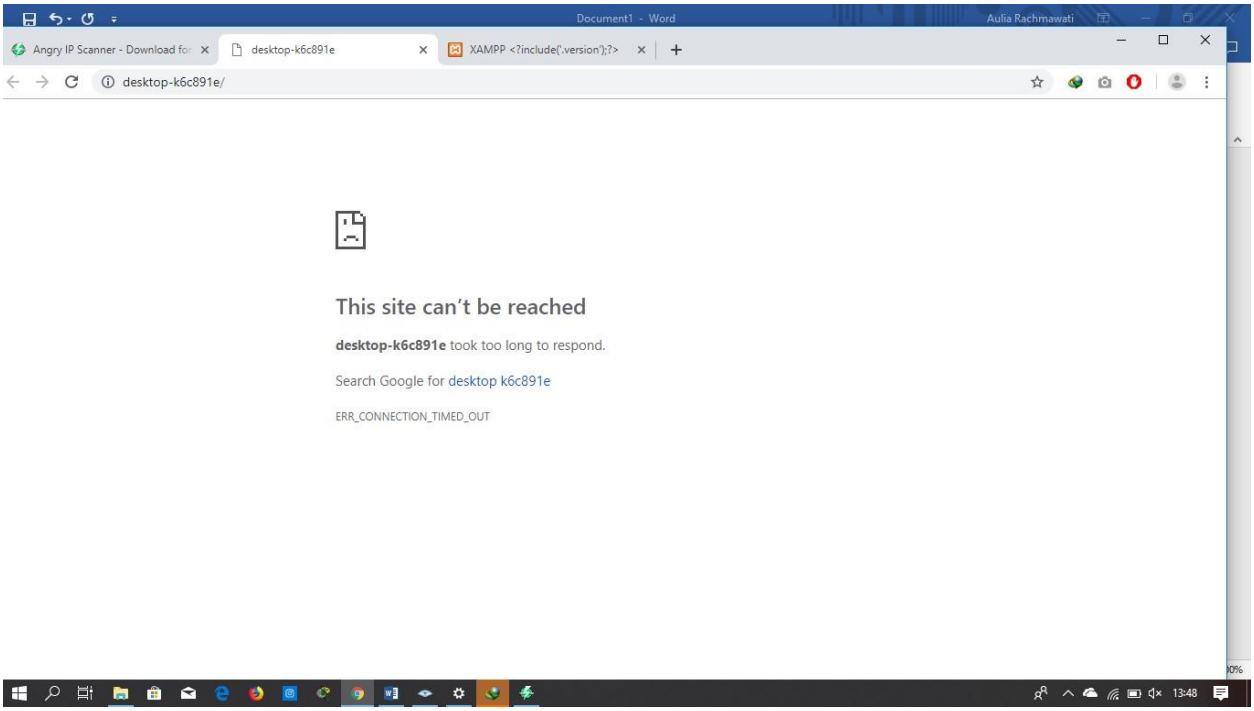
Nim : L200160117

Modul 2

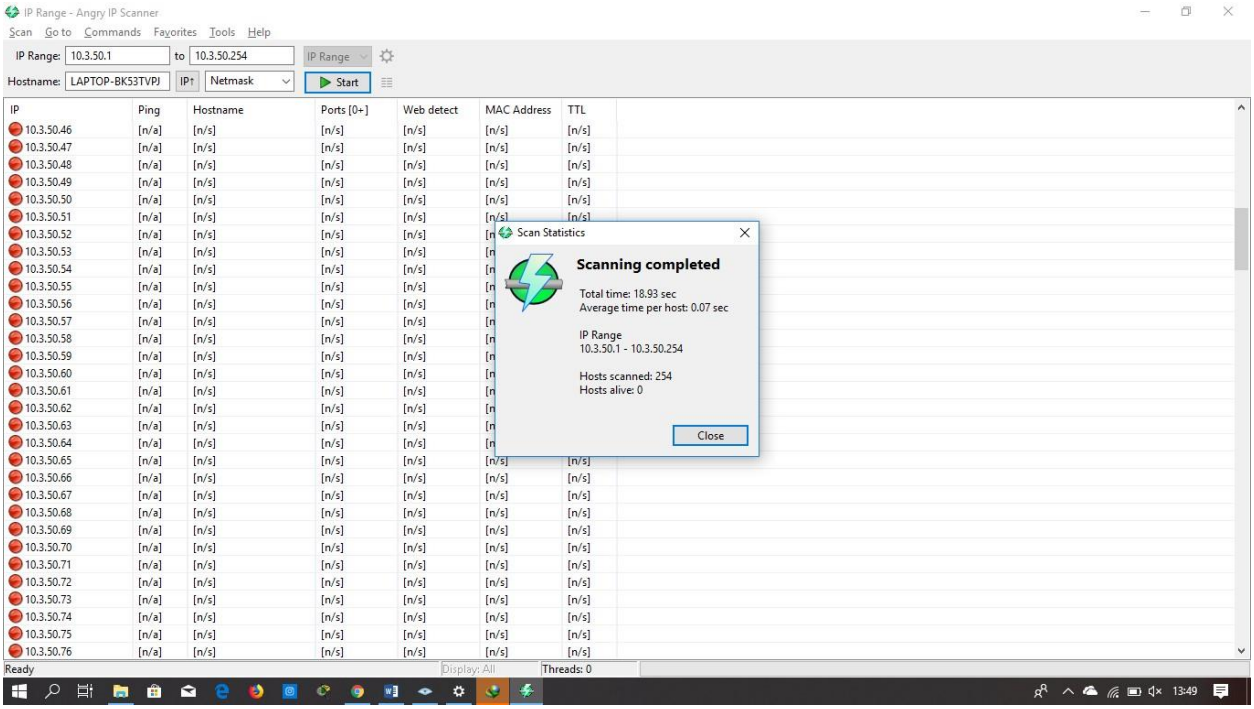
1. Percobaan 1




IP Range - Angry IP Scanner
Angry IP Scanner - Download fo
desktop-k6c891e
XAMPP <?include('.version');?>
Not secure
desktop-t5944vg/xampp/
XAMPP fürfor Windows
Warning: Variable passed to each() is not an array or object in C:\xampp\htdocs\xampp\head.php on line 27
XAMPP
[PHP: 7.2.2]
Welcome
Status
Security
Documentation
Components
phpinfo()
Demos
CD Collection
Biorhythm
Instant Art
Flash Art
Phone Book
Excel_Writer
ADOdb
Tools
phpMyAdmin
Webalizer
Mercury Mail
FileZilla FTP
Specials
PHP PostScript
PHP Paradox
©2002-2006
...APACHE FRIENDS...
...APACHE FRIENDS...
Welcome to XAMPP for Windows Version 1.7.1 !
Congratulations:
You have successfully installed XAMPP on this system!
Now you can start using Apache and Co. You should first try Status on the left navigation to make sure everything works fine.
For OpenSSL support please use the test certificate with https://127.0.0.1 or https://localhost
For this release a special thanks to Uwe Steinmann for his excellent development and compilation of all current "Special" modules!
Good luck, Kay Vogelgesang + Kai 'Oswald' Seidler
13:48


Document1 - Word
Aulia Rachmawati
Angry IP Scanner - Download fo
desktop-k6c891e
XAMPP <?include('.version');?>
desktop-k6c891e/
This site can't be reached
desktop-k6c891e took too long to respond.
Search Google for desktop k6c891e
ERR_CONNECTION_TIMED_OUT
13:48

Tugas Percobaan 1



2. Percobaan 2

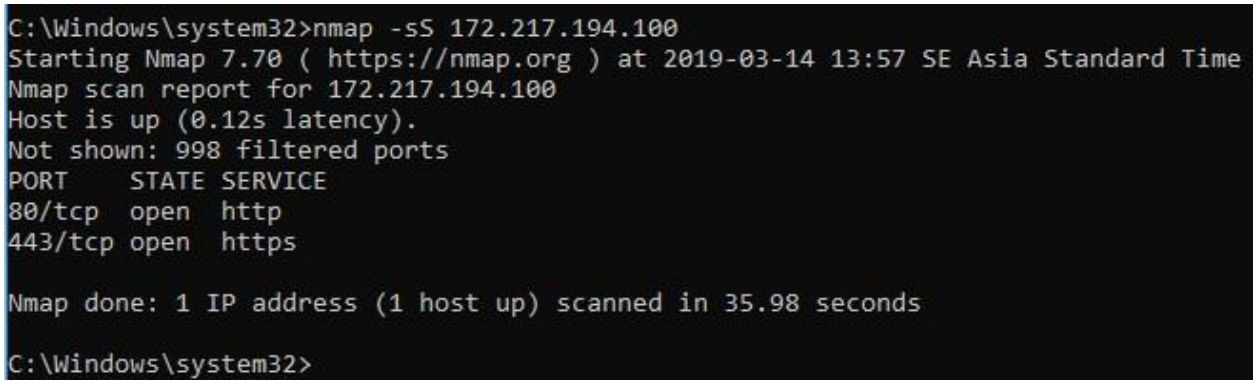
```
C:\Windows\system32>nmap -sS 192.168.1.129
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 13:53 SE Asia Standard Time
Nmap scan report for 192.168.1.129
Host is up (0.17s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 74:C6:3B:CE:9C:E3 (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 44.37 seconds

C:\Windows\system32>
```

```
C:\Windows\system32>nmap -sT 192.168.1.129
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 13:54 SE Asia Standard Time
Nmap scan report for 192.168.1.129
Host is up (0.032s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 74:C6:3B:CE:9C:E3 (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 59.55 seconds

C:\Windows\system32>
```

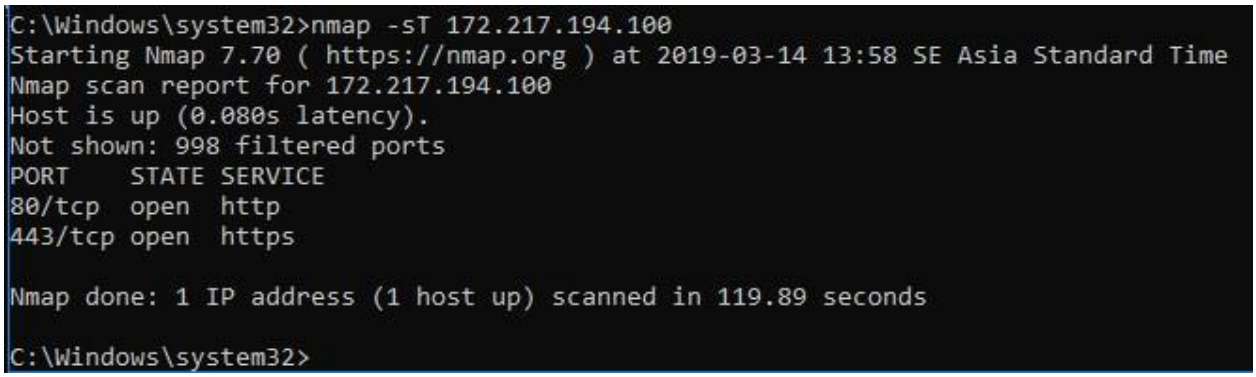
Tugas percobaaan 2

Google

- Teknik -sS

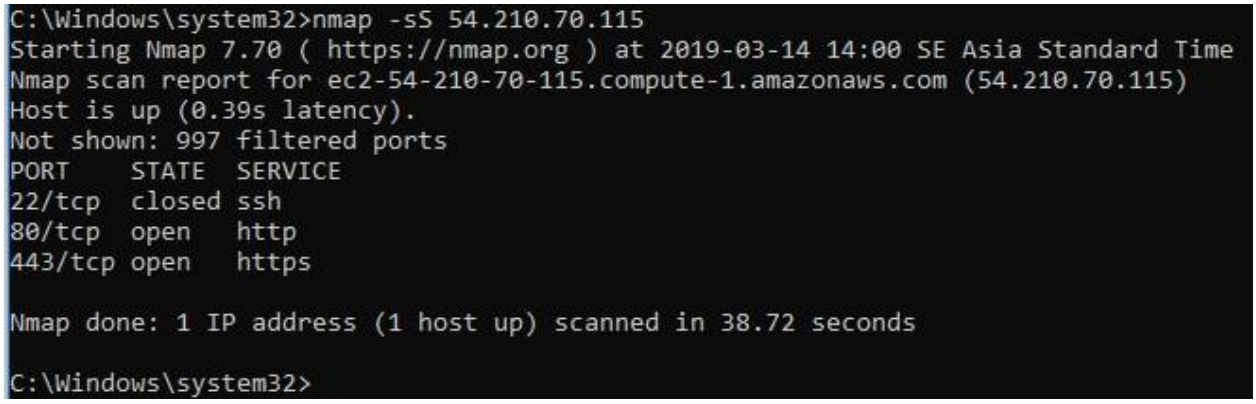


- Teknik -sT



Instagram

- Teknik -sS



- Teknik -sT

```
C:\Windows\system32>nmap -sT 54.210.70.115
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 14:02 SE Asia Standard Time
Nmap scan report for ec2-54-210-70-115.compute-1.amazonaws.com (54.210.70.115)
Host is up (0.31s latency).
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 236.75 seconds

C:\Windows\system32>
```

Ums

- Teknik -sS

```
C:\Windows\system32>nmap -sS 103.226.174.210
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 14:03 SE Asia Standard Time
Nmap scan report for 103.226.174.210
Host is up (0.11s latency).
Not shown: 993 filtered ports
PORT     STATE  SERVICE
22/tcp   closed ssh
80/tcp   open   http
443/tcp  closed https
465/tcp  closed smtps
587/tcp  closed submission
2222/tcp open   EtherNetIP-1
3306/tcp closed mysql

Nmap done: 1 IP address (1 host up) scanned in 24.67 seconds

C:\Windows\system32>
```

- Teknik -sT

```
C:\Windows\system32>nmap -sT 103.226.174.210
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 14:04 SE Asia Standard Time
Nmap scan report for 103.226.174.210
Host is up (0.055s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
2222/tcp open  EtherNetIP-1

Nmap done: 1 IP address (1 host up) scanned in 88.29 seconds

C:\Windows\system32>
```

Teknik – Teknik scan yang bias dilakukan oleh nmap :

TCP SYN Scan (-sS)
Teknik ini merupakan teknik scanning pada Nmap yang populer. Teknik dapat melakukan scanning port dengan cepat. Teknik ini dapat membedakan status port Open, closed dan filtered. Cara kerjanya adalah dengan mengirimkan sebuah paket SYN, kemudian

menunggu jawaban dari sistem target. Bila kita mendapat jawaban paket SYN/ACK berarti port tersebut open, bila kita mendapat paket RST berarti port closed. Bila kita tidak mendapat jawaban seteah beberapa saat, maka port ditandai filtered.

TCP connect() Scan (-sT)
Scanning ini digunakan bila kita tidak memiliki privilege (admin/root). Scanning ini menggunakan fungsi system call connect pada OS. Metode ini membutuhkan waktu lebih lama dan umumnya dapat terbaca oleh IDS.

UDP Scan -sU
Metode ini digunakan untuk mengidentifikasi port UDP. Layanan DNS, SNMP dan DHCP adalah beberapa layanan yang menggunakan paket UDP.

FIN Scan (-sF), Xmas Tree Scan (-sX) dan Null Scan (-sN)
Teknik ini sering disebut teknik stealth. Banyak digunakan pada jaringan yang dilindungi Firewall. Teknik ini tidak dapat digunakan pada komputer dengan OS Windows. Selain itu hasil scan akan sulit membedakan status open dan filtered

Ping Scan (-sP)
Teknik ini merupakan teknik scanning yang paling cepat. Teknik ini tidak melakukan port scanning, umumya digunakan untuk menemukan host yang hidup pada suatu jaringan.

Version Detection (-sV)
Teknik ini dapat digunakan untuk mengetahui versi dari aplikasi yang digunakan pada komputer target.

Scan IP Protocol (-sO)
Teknik ini dapat menemukan protokol IP pada komputer target, misalnya ICMP, TCP, dan UDP

Scan ACK (-sA)
Teknik ini tidak dapat digunakan untuk menemukan port yang terbuka, tapi berguna pada jaringan yang dilindungi firewall maupun packet filter. Hasil scanning bisa digunakan untuk menentukan tipe firewal yang digunakan apakah statefull atau tidak serta port mana yang difilter.

RPC Scan (-sR)
Teknik ini digunakan untuk menemukan aplikasi yang menggunakan remote call procedure pada target.

Idlescan (-sI)
Teknik ini digunakan bila kita tidak memiliki akses langsung ke komputer target. Biasanya karena target dilindungi firewall.

3. Percobaan 3
   - SCANNING PORT TCP (192.168.1.115)

```
C:\Users\ASUS\Desktop\netcat>nc -v -z -w2 192.168.1.115 80-85
PARROT [192.168.1.115] 80 (http) open

C:\Users\ASUS\Desktop\netcat>
```

- SCANNING PORT UDP (192.168.1.115)

```
C:\Users\ASUS\Desktop\netcat>nc -u -v -z -w2 192.168.1.115 80-85
PARROT [192.168.1.115] 85 (?) open
PARROT [192.168.1.115] 84 (?) open
PARROT [192.168.1.115] 83 (?) open
PARROT [192.168.1.115] 82 (?) open
PARROT [192.168.1.115] 81 (hosts2-ns) open
PARROT [192.168.1.115] 80 (?) open

C:\Users\ASUS\Desktop\netcat>
```

Tugas percobaan 3

Ums

```
C:\Users\ASUS\Desktop\netcat>nc -v -z -w2 103.226.174.220 80-85
ums.ac.id [103.226.174.220] 85 (?): TIMEDOUT
ums.ac.id [103.226.174.220] 84 (?): TIMEDOUT
ums.ac.id [103.226.174.220] 83 (?): TIMEDOUT
ums.ac.id [103.226.174.220] 82 (?): TIMEDOUT
ums.ac.id [103.226.174.220] 81 (hosts2-ns): TIMEDOUT
ums.ac.id [103.226.174.220] 80 (http) open

C:\Users\ASUS\Desktop\netcat>
```

Google

```
C:\Users\ASUS\Desktop\netcat>nc -v -z -w2  216.239.38.120 80-85
www.google.co.id [216.239.38.120] 85 (?): TIMEDOUT
www.google.co.id [216.239.38.120] 84 (?): TIMEDOUT
www.google.co.id [216.239.38.120] 83 (?): TIMEDOUT
www.google.co.id [216.239.38.120] 82 (?): TIMEDOUT
www.google.co.id [216.239.38.120] 81 (hosts2-ns): TIMEDOUT
www.google.co.id [216.239.38.120] 80 (http) open

C:\Users\ASUS\Desktop\netcat>
```

Yahoo

```
C:\Users\ASUS\Desktop\netcat>nc -v -z -w2 106.10.250.11 80-85
media-router-fp2.prod1.media.vip.sg3.yahoo.com [106.10.250.11] 85 (?): TIMEDOUT
media-router-fp2.prod1.media.vip.sg3.yahoo.com [106.10.250.11] 84 (?): TIMEDOUT
media-router-fp2.prod1.media.vip.sg3.yahoo.com [106.10.250.11] 83 (?): TIMEDOUT
media-router-fp2.prod1.media.vip.sg3.yahoo.com [106.10.250.11] 82 (?): TIMEDOUT
media-router-fp2.prod1.media.vip.sg3.yahoo.com [106.10.250.11] 81 (hosts2-ns): TIMEDOUT
media-router-fp2.prod1.media.vip.sg3.yahoo.com [106.10.250.11] 80 (http) open

C:\Users\ASUS\Desktop\netcat>
```

4. Percobaan 4

IP 10.201.31.123

```
C:\Users\ASUS>nmap -O 10.201.31.123
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-18 09:23 SE Asia Standard Time
Nmap scan report for 10.201.31.123
Host is up (0.091s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 38:59:F9:2F:4A:7C (Hon Hai Precision Ind.)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1
cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.26 seconds
```

Tugas Percobaan 4

ums

```
C:\Users\ASUS>nmap -O 103.226.174.220
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-18 09:11 SE Asia Standard Time
Nmap scan report for 103.226.174.220
Host is up (0.11s latency).
Not shown: 983 filtered ports
PORT      STATE  SERVICE
20/tcp    closed ftp-data
21/tcp    open   ftp
22/tcp    open   ssh
53/tcp    open   domain
80/tcp    open   http
161/tcp   closed snmp
443/tcp   open   https
465/tcp   closed smtps
587/tcp   closed submission
3306/tcp  open   mysql
8080/tcp  closed http-proxy
8081/tcp  closed blackice-icecap
50000/tcp closed ibm-db2
50001/tcp closed unknown
50002/tcp closed iiimsf
50003/tcp closed unknown
50006/tcp closed unknown
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.06 seconds
```

Google

```
C:\Users\ASUS>nmap -O 74.125.130.147
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-18 09:09 SE Asia Standard Time
Nmap scan report for sb-in-f147.1e100.net (74.125.130.147)
Host is up (0.031s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): OpenBSD 4.X (89%)
OS CPE: cpe:/o:openbsd:openbsd:4.3
Aggressive OS guesses: OpenBSD 4.3 (89%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.41 seconds
```

Uny

```
C:\Users\ASUS>nmap -O 185.53.177.30
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-18 09:40 SE Asia Standard Time
Nmap scan report for 185.53.177.30
Host is up (0.66s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): FreeBSD 11.X|12.X|8.X (91%), Apple iOS 11.X (85%), Crestron 2-Series (85%)
OS CPE: cpe:/o:freebsd:freebsd:11.0 cpe:/o:freebsd:freebsd:12 cpe:/o:apple:iphone_os:11.0 cpe:/o:freebsd:freebsd:8.2 cpe
:/o:crestron:2_series
Aggressive OS guesses: FreeBSD 11.0-STABLE (91%), FreeBSD 11.0-RELEASE (90%), FreeBSD 11.0-RELEASE - 12.0-CURRENT (87%),
 Apple iOS 11.0 (85%), FreeBSD 8.2-STABLE (85%), Crestron XPanel control system (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 177.62 seconds
```