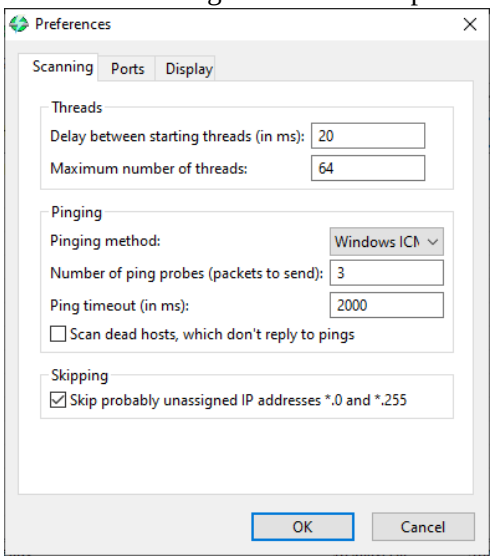
Nama : Tidhar Katon Birowo
NIM : L200170187
Kelas : A

PRAKTIKUM KEAMANAN JARINGAN KOMPUTER
MODUL 2

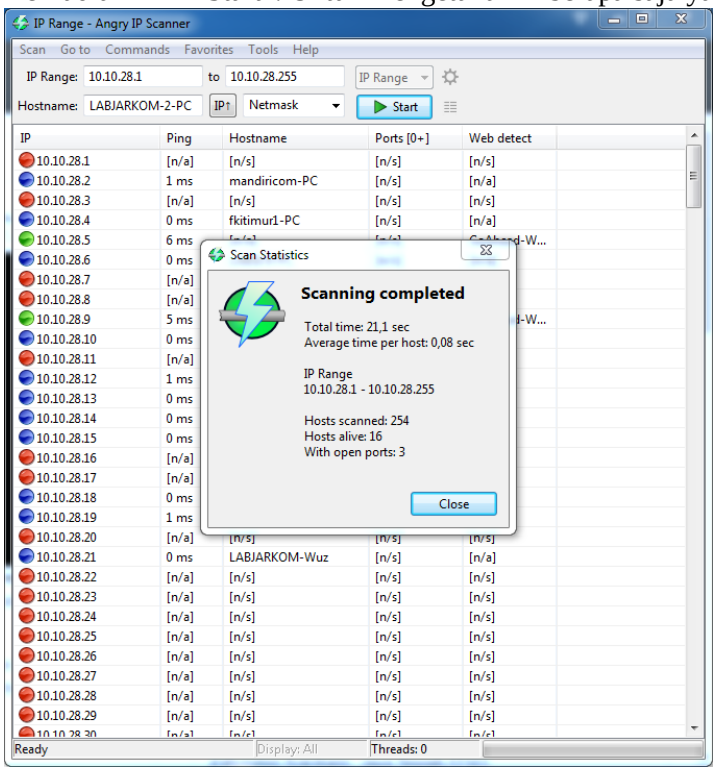
Percobaan & Tugas 1

Mencari Komputer yang hidup/aktif dengan program Angry IP Scanner.

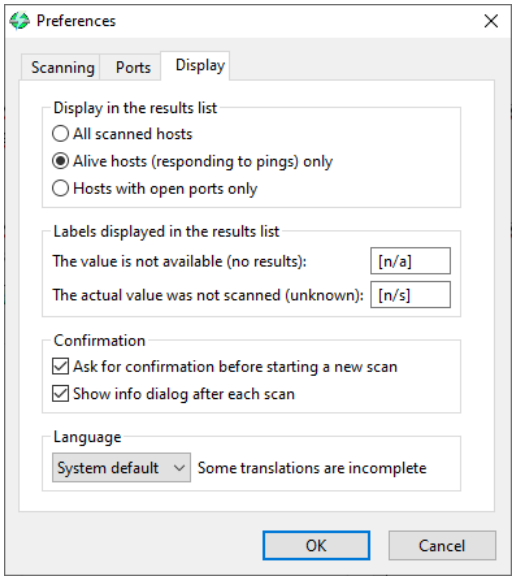
Melakukan setting di dalam menu preferences



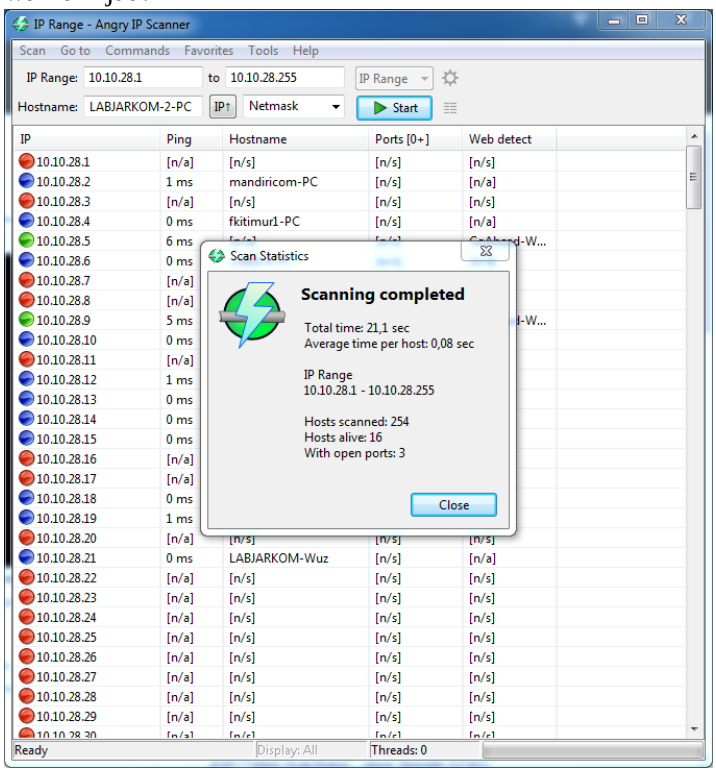
Memasukkan Alamat IP Local UMS (10.10.28.1 to 10.10.255) terhadap aplikasi Angry IP Scanner, Kemudian Klik “Start”. Untuk mengetahui IP berapa saja yang aktif



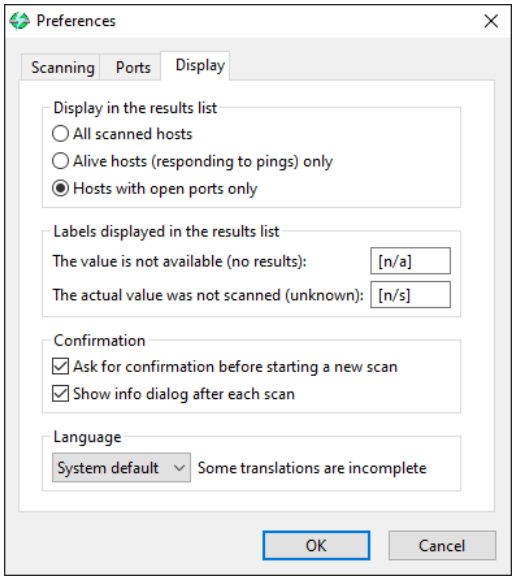
Melakukkan Setting agar aplikasi Angry IP Scanner hanya dapat Men-scan Komputer yang hidup saja.



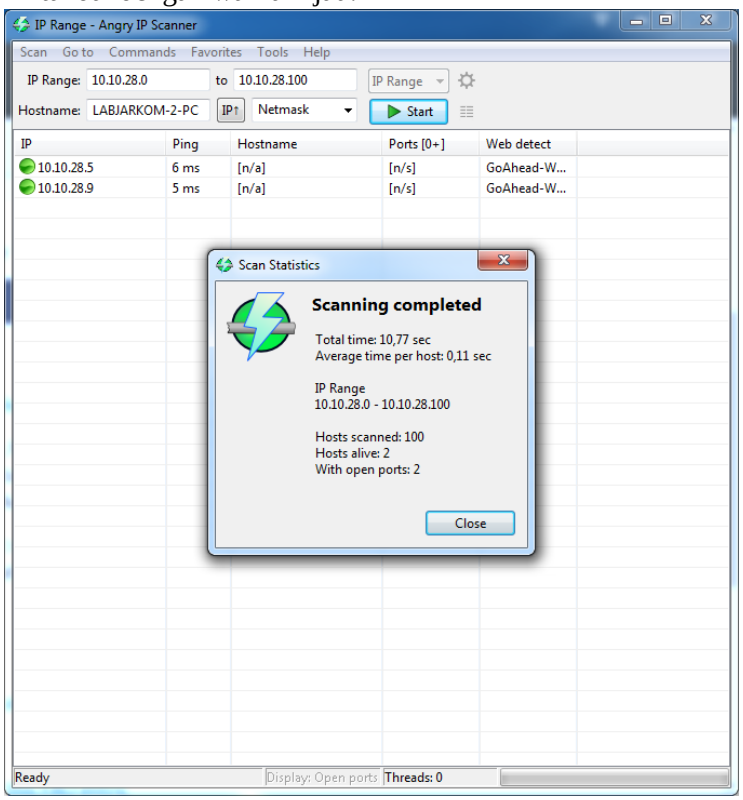
Hasil dari Scan Ulang untuk mengetahui komputer mana saja yang sedang aktif. Di tandai dengan warna hijau.



Melakukkan Setting agar aplikasi Angry IP Scanner hanya dapat Men-scan Komputer yang hidup saja dan port nya terbuka. Kemudian melakukan scan ulang



Hasil dari Scan Ulang untuk mengetahui komputer mana saja yang sedang aktif dan port nya terbuka. Di tandai dengan warna hijau.



Percobaan & Tugas 2

Mencari Port yang terbuka dengan Nmap

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.18362.657]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\tidha>nmap -h
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
```

Melakukan Scanning dengan menggunakkan (nmap -sS 10.10.28.10) IP Address yang aktif

```
C:\Users\LABJARKOM-2>nmap -sS 10.10.28.10
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-03 11:23 SE Asia Standard Tim
e
Nmap scan report for 10.10.28.10
Host is up (0.0058s latency).
All 1000 scanned ports on 10.10.28.10 are filtered (532) or closed (468)
MAC Address: 00:E0:4C:68:07:56 (Realtek Semiconductor)

Nmap done: 1 IP address (1 host up) scanned in 3.14 seconds
```

Melakukan Scanning dengan menggunakkan (nmap -sT 10.10.28.15)IP Address yang aktif

```
C:\Users\LABJARKOM-2>nmap -sT 10.10.28.15
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-03 11:25 SE Asia Standard Tim
e
Nmap scan report for 10.10.28.15
Host is up (0.0010s 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: 38:60:77:73:39:7A (Pegatron)

Nmap done: 1 IP address (1 host up) scanned in 41.80 seconds
```

Melakukan Scanning port lebih dari satu target Komputer (nmap -sS 10.10.28.1-100)

```
C:\WINDOWS\system32\cmd.exe
C:\Users\tidha>nmap 10.10.28.1-100
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-09 20:53 SE Asia Standard Time
Nmap scan report for 10.10.28.1
Host is up (0.020s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 10.10.28.2
Host is up (0.020s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 10.10.28.3
Host is up (0.021s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 10.10.28.4
Host is up (0.018s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
```

Melakukan Scanning Port dengan menggunakkan nmap minimal 3 website memakai Teknik -sS dan -sT

- Website www.bagas31.com

```
C:\Users\LABJARKOM-2>nmap -sS www.bagas31.com
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-03 11:47 SE Asia Standard Tim
e
Nmap scan report for www.bagas31.com (104.27.157.29)
Host is up (0.023s latency).
Other addresses for www.bagas31.com (not scanned): 104.27.156.29
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy
8443/tcp  open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 5.33 seconds

C:\Users\LABJARKOM-2>nmap -sT www.bagas31.com
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-03 11:48 SE Asia Standard Tim
e
Nmap scan report for www.bagas31.com (104.27.157.29)
Host is up (0.019s latency).
Other addresses for www.bagas31.com (not scanned): 104.27.156.29
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy
8443/tcp  open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 41.89 seconds
```

- Website www.visitklaten.com

```
C:\Users\LABJARKOM-2>nmap -sS www.visitklaten.com
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-03 11:30 SE Asia Standard Tim
e
Nmap scan report for www.visitklaten.com (139.162.11.19)
Host is up (0.041s latency).
rDNS record for 139.162.11.19: glaceon.rapidplex.com
Not shown: 986 filtered ports
PORT      STATE  SERVICE
20/tcp    closed ftp-data
21/tcp    open   ftp
22/tcp    closed ssh
25/tcp    open   smtp
53/tcp    closed domain
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
465/tcp   open   smtps
587/tcp   open   submission
993/tcp   open   imaps
995/tcp   open   pop3s
21571/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 5.38 seconds

C:\Users\LABJARKOM-2>nmap -sT www.visitklaten.com
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-03 11:41 SE Asia Standard Tim
e
Nmap scan report for www.visitklaten.com (139.162.11.19)
Host is up (0.028s latency).
rDNS record for 139.162.11.19: glaceon.rapidplex.com
Not shown: 990 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
443/tcp open  https
465/tcp open  smtps
587/tcp open  submission
993/tcp open  imaps
995/tcp open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 41.74 seconds
```

- Website www.youtube.com

```
C:\WINDOWS\system32\cmd.exe

C:\Users\tidha>nmap -sS www.youtube.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-09 21:02 SE Asia Standard Time
Nmap scan report for www.youtube.com (74.125.130.190)
Host is up (0.023s latency).
Other addresses for www.youtube.com (not scanned): 172.253.118.91 142.250.4.93 74.125.24.93 74.125.24.136 74.125.24.91 7
4.125.24.190 172.217.194.136 172.217.194.190 172.217.194.93 172.217.194.91 74.125.130.136
rDNS record for 74.125.130.190: sb-in-f190.1e100.net
Not shown: 997 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 8.52 seconds

C:\Users\tidha>nmap -sT www.youtube.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-09 21:03 SE Asia Standard Time
Nmap scan report for www.youtube.com (74.125.130.190)
Host is up (0.0037s latency).
Other addresses for www.youtube.com (not scanned): 172.253.118.91 142.250.4.93 74.125.24.93 74.125.24.136 74.125.24.91 7
4.125.24.190 172.217.194.136 172.217.194.190 172.217.194.93 172.217.194.91 74.125.130.136
rDNS record for 74.125.130.190: sb-in-f190.1e100.net
Not shown: 997 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 63.23 seconds
```

Teknik – Teknik scan yang dapat di lakukan oleh nmap antara lain :

- Ping Scan

Teknik ini merupakan teknik yang paling cepat. Dikarenakan teknik ini tidak melakukan port scanning, melainkan hanya digunakan untuk mengidentifikasi dan menemukan host yang aktif(online) pada suatu jaringan.

- TCP Full Open

Teknik ini digunakan untuk memastikan adanya port dengan status open dan terdapat listener di sistem. Cara kerja dari teknik ini adalah dengan three-way-handshake. Jadi teknik ini akan berhasil ketika antara sisi A (scanner) dengan sisi B (sistem) dapat terbentuk three-way-handshake. Dan apabila tidak ada balasan sampai terbangunnya three-way-handshake maka teknik ini gagal.

- TCP Half Open (SYN Scan)

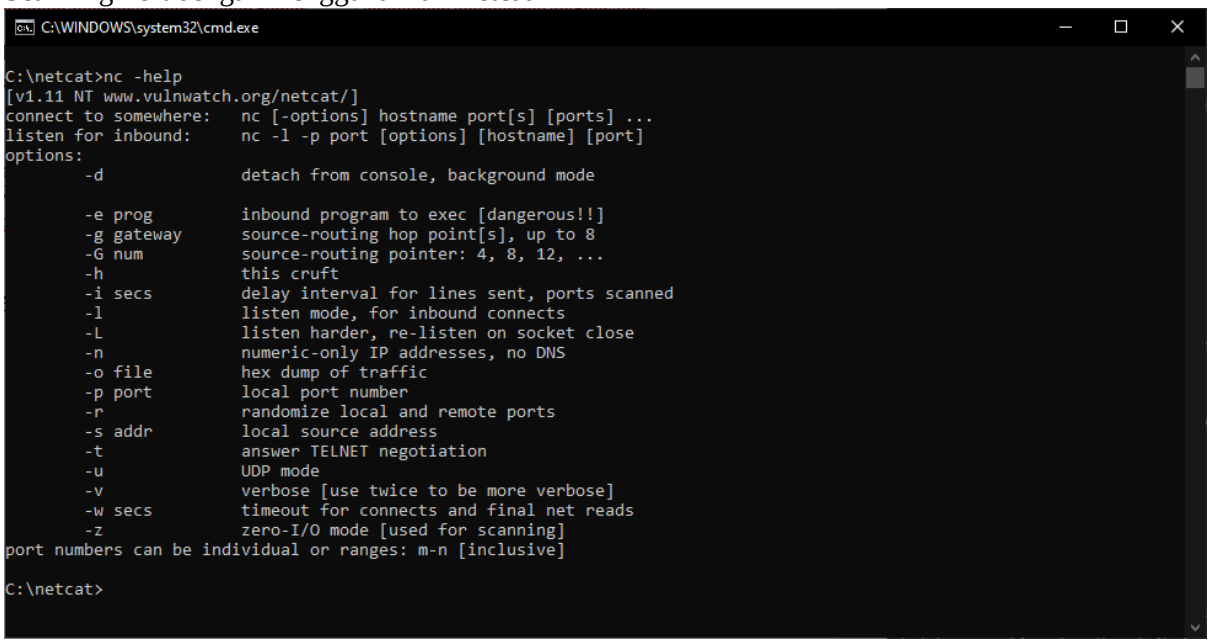
Teknik ini merupakan teknik yang umum digunakan pertama kali. Teknik ini dapat melakukan scanning port dengan cepat. Selain itu juga teknik ini dapat membedakan status port Open, Closed, dan Filtered. Sistem kerjanya dengan mengirimkan paket SYN, kemudian menunggu respon dari sistem target. Apabila mendapatkan balikan SYN/ACK maka port tersebut Open, kemudian apabila mendapatkan balikan RST maka port tersebut Closed, dan apabila tidak mendapatkan balasan setelah beberapa saat, maka port tersebut Filtered.

- UDP Scan

Teknik ini digunakan untuk mengidentifikasi port UDP. Adapun layanan yang menggunakan UDP, seperti DNS, SNMP, DHCP, dan lain sebagainya. Teknik ini sering diabaikan oleh auditor keamanan, dikarenakan akan lebih lambat daripada scanning pada port TCP.

Percobaan & Tugas 3

Scanning Port dengan menggunakkan Netcat



```
C:\WINDOWS\system32\cmd.exe

C:\netcat>nc -help
[v1.11 NT www.vulnwatch.org/netcat/]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, background mode

        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]

C:\netcat>
```

Melakukan Scanning Port TCP dan UDP mulai dari port 1-150

(nc -v -z -w2 10.10.28.0 1-150) & (nc -u -v -z -w2 10.10.28.0 1-150)

```
C:\Users\LABJARKOM-2\Downloads\netcat-1.11>nc -v -z -w2 10.10.28.0 1-150
10.10.28.0: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [10.10.28.0] 150 (sql-net): TIMEDOUT
(UNKNOWN) [10.10.28.0] 149 (?): TIMEDOUT
(UNKNOWN) [10.10.28.0] 148 (?): TIMEDOUT
(UNKNOWN) [10.10.28.0] 147 (?): TIMEDOUT
(UNKNOWN) [10.10.28.0] 146 (?): TIMEDOUT
(UNKNOWN) [10.10.28.0] 145 (?): TIMEDOUT
(UNKNOWN) [10.10.28.0] 144 (?): TIMEDOUT
(UNKNOWN) [10.10.28.0] 143 (imap): TIMEDOUT
(UNKNOWN) [10.10.28.0] 142 (?): TIMEDOUT
(UNKNOWN) [10.10.28.0] 141 (?): TIMEDOUT
(UNKNOWN) [10.10.28.0] 140 (?): TIMEDOUT
(UNKNOWN) [10.10.28.0] 139 (netbios-ssn): TIMEDOUT
(UNKNOWN) [10.10.28.0] 138 (?): TIMEDOUT
(UNKNOWN) [10.10.28.0] 137 (netbios-ns): TIMEDOUT
(UNKNOWN) [10.10.28.0] 136 (?): TIMEDOUT
(UNKNOWN) [10.10.28.0] 135 (epmap): TIMEDOUT
(UNKNOWN) [10.10.28.0] 134 (?): TIMEDOUT
(UNKNOWN) [10.10.28.0] 133 (?): TIMEDOUT
(UNKNOWN) [10.10.28.0] 132 (?): TIMEDOUT
^C
C:\Users\LABJARKOM-2\Downloads\netcat-1.11>nc -u -v -z -w2 10.10.28.0 1-150
10.10.28.0: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [10.10.28.0] 150 (?) open
(UNKNOWN) [10.10.28.0] 149 (?) open
(UNKNOWN) [10.10.28.0] 148 (?) open
(UNKNOWN) [10.10.28.0] 147 (?) open
(UNKNOWN) [10.10.28.0] 146 (?) open
(UNKNOWN) [10.10.28.0] 145 (?) open
(UNKNOWN) [10.10.28.0] 144 (?) open
(UNKNOWN) [10.10.28.0] 143 (?) open
(UNKNOWN) [10.10.28.0] 142 (?) open
(UNKNOWN) [10.10.28.0] 141 (?) open
(UNKNOWN) [10.10.28.0] 140 (?) open
(UNKNOWN) [10.10.28.0] 139 (?) open
(UNKNOWN) [10.10.28.0] 138 (netbios-dgm) open
(UNKNOWN) [10.10.28.0] 137 (netbios-ns) open
(UNKNOWN) [10.10.28.0] 136 (?) open
(UNKNOWN) [10.10.28.0] 135 (epmap) open
(UNKNOWN) [10.10.28.0] 134 (?) open
(UNKNOWN) [10.10.28.0] 133 (?) open
(UNKNOWN) [10.10.28.0] 132 (?) open
(UNKNOWN) [10.10.28.0] 131 (?) open
(UNKNOWN) [10.10.28.0] 130 (?) open
(UNKNOWN) [10.10.28.0] 129 (?) open
(UNKNOWN) [10.10.28.0] 128 (?) open
(UNKNOWN) [10.10.28.0] 127 (?) open
(UNKNOWN) [10.10.28.0] 126 (?) open
(UNKNOWN) [10.10.28.0] 125 (?) open
(UNKNOWN) [10.10.28.0] 124 (?) open
(UNKNOWN) [10.10.28.0] 123 (ntp) open
(UNKNOWN) [10.10.28.0] 122 (?) open
(UNKNOWN) [10.10.28.0] 121 (?) open
(UNKNOWN) [10.10.28.0] 120 (?) open
```

Melakukan Scanning Port mulai dari port 1-500 dengan menggunakkan netcat (3 website)

- Website www.bagas31.com

```
C:\WINDOWS\system32\cmd.exe
C:\netcat>nc -u -v -z -w2 www.bagas31.com 1-500
DNS fwd/rev mismatch: www.bagas31.com != 29.156.27.104.in-addr.arpa
DNS fwd/rev mismatch: www.bagas31.com != 29.157.27.104.in-addr.arpa
www.bagas31.com [104.27.156.29] 500 (isakmp) open
www.bagas31.com [104.27.156.29] 499 (?) open
www.bagas31.com [104.27.156.29] 498 (?) open
www.bagas31.com [104.27.156.29] 497 (?) open
www.bagas31.com [104.27.156.29] 496 (?) open
www.bagas31.com [104.27.156.29] 495 (?) open
www.bagas31.com [104.27.156.29] 494 (?) open
www.bagas31.com [104.27.156.29] 493 (?) open
www.bagas31.com [104.27.156.29] 492 (?) open
www.bagas31.com [104.27.156.29] 491 (?) open
www.bagas31.com [104.27.156.29] 490 (?) open
www.bagas31.com [104.27.156.29] 489 (?) open
www.bagas31.com [104.27.156.29] 488 (?) open
www.bagas31.com [104.27.156.29] 487 (?) open
www.bagas31.com [104.27.156.29] 486 (?) open
www.bagas31.com [104.27.156.29] 485 (?) open
www.bagas31.com [104.27.156.29] 484 (?) open
www.bagas31.com [104.27.156.29] 483 (?) open
www.bagas31.com [104.27.156.29] 482 (?) open
www.bagas31.com [104.27.156.29] 481 (?) open
www.bagas31.com [104.27.156.29] 480 (?) open
www.bagas31.com [104.27.156.29] 479 (?) open
www.bagas31.com [104.27.156.29] 478 (?) open
www.bagas31.com [104.27.156.29] 477 (?) open
www.bagas31.com [104.27.156.29] 476 (?) open
www.bagas31.com [104.27.156.29] 475 (?) open
www.bagas31.com [104.27.156.29] 474 (?) open
```

- Website www.visitklaten.com

```
C:\WINDOWS\system32\cmd.exe
C:\netcat>nc -u -v -z -w2 www.visitklaten.com 1-500
DNS fwd/rev mismatch: visitklaten.com != glaceon.rapidplex.com
visitklaten.com [139.162.11.19] 500 (isakmp) open
visitklaten.com [139.162.11.19] 499 (?) open
visitklaten.com [139.162.11.19] 498 (?) open
visitklaten.com [139.162.11.19] 497 (?) open
visitklaten.com [139.162.11.19] 496 (?) open
visitklaten.com [139.162.11.19] 495 (?) open
visitklaten.com [139.162.11.19] 494 (?) open
visitklaten.com [139.162.11.19] 493 (?) open
visitklaten.com [139.162.11.19] 492 (?) open
visitklaten.com [139.162.11.19] 491 (?) open
visitklaten.com [139.162.11.19] 490 (?) open
visitklaten.com [139.162.11.19] 489 (?) open
visitklaten.com [139.162.11.19] 488 (?) open
visitklaten.com [139.162.11.19] 487 (?) open
visitklaten.com [139.162.11.19] 486 (?) open
visitklaten.com [139.162.11.19] 485 (?) open
visitklaten.com [139.162.11.19] 484 (?) open
visitklaten.com [139.162.11.19] 483 (?) open
visitklaten.com [139.162.11.19] 482 (?) open
visitklaten.com [139.162.11.19] 481 (?) open
visitklaten.com [139.162.11.19] 480 (?) open
visitklaten.com [139.162.11.19] 479 (?) open
visitklaten.com [139.162.11.19] 478 (?) open
visitklaten.com [139.162.11.19] 477 (?) open
visitklaten.com [139.162.11.19] 476 (?) open
visitklaten.com [139.162.11.19] 475 (?) open
visitklaten.com [139.162.11.19] 474 (?) open
visitklaten.com [139.162.11.19] 473 (?) open
```

- Website www.ign.com

```
C:\WINDOWS\system32\cmd.exe
C:\netcat>nc -u -v -z -w2 www.ign.com 1-500
DNS fwd/rev mismatch: ign.map.fastly.net != 135.9.101.151.in-addr.arpa
ign.map.fastly.net [151.101.9.135] 500 (isakmp) open
ign.map.fastly.net [151.101.9.135] 499 (?) open
ign.map.fastly.net [151.101.9.135] 498 (?) open
ign.map.fastly.net [151.101.9.135] 497 (?) open
ign.map.fastly.net [151.101.9.135] 496 (?) open
ign.map.fastly.net [151.101.9.135] 495 (?) open
ign.map.fastly.net [151.101.9.135] 494 (?) open
ign.map.fastly.net [151.101.9.135] 493 (?) open
ign.map.fastly.net [151.101.9.135] 492 (?) open
ign.map.fastly.net [151.101.9.135] 491 (?) open
ign.map.fastly.net [151.101.9.135] 490 (?) open
ign.map.fastly.net [151.101.9.135] 489 (?) open
ign.map.fastly.net [151.101.9.135] 488 (?) open
ign.map.fastly.net [151.101.9.135] 487 (?) open
ign.map.fastly.net [151.101.9.135] 486 (?) open
ign.map.fastly.net [151.101.9.135] 485 (?) open
ign.map.fastly.net [151.101.9.135] 484 (?) open
ign.map.fastly.net [151.101.9.135] 483 (?) open
ign.map.fastly.net [151.101.9.135] 482 (?) open
ign.map.fastly.net [151.101.9.135] 481 (?) open
ign.map.fastly.net [151.101.9.135] 480 (?) open
ign.map.fastly.net [151.101.9.135] 479 (?) open
ign.map.fastly.net [151.101.9.135] 478 (?) open
ign.map.fastly.net [151.101.9.135] 477 (?) open
ign.map.fastly.net [151.101.9.135] 476 (?) open
ign.map.fastly.net [151.101.9.135] 475 (?) open
ign.map.fastly.net [151.101.9.135] 474 (?) open
ign.map.fastly.net [151.101.9.135] 473 (?) open
```

Percobaan & Tugas 4

Mendeteksi Sistem Operasi Target dengan Nmap

- Nmap -O 10.10.28.15

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.18362.657]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\tidha>nmap -O 10.10.28.15
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-09 21:40 SE Asia Standard Time
Nmap scan report for 10.10.28.15
Host is up (0.016s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Apple TV 5.2.1 or 5.3 (89%), Crestron XPanel control system (89%), OpenBSD 4.3 (88%), Vodavi XTS-
IP PBX (87%), Asus RT-AC66U router (Linux 2.6) (86%), Asus RT-N10 router or AXIS 211A Network Camera (Linux 2.6) (86%),
Linux 2.6.18 (86%), Linux 2.6.24 (86%), Asus RT-N16 WAP (Linux 2.6) (86%), Asus RT-N66U WAP (Linux 2.6) (86%)
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 25.67 seconds
```

- Nmap -p80 -O 10.10.28.15

```
C:\WINDOWS\system32\cmd.exe

C:\Users\tidha>nmap -O 10.10.28.15
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-09 21:40 SE Asia Standard Time
Nmap scan report for 10.10.28.15
Host is up (0.016s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Apple TV 5.2.1 or 5.3 (89%), Crestron XPanel control system (89%), OpenBSD 4.3 (88%), Vodavi XTS-
IP PBX (87%), Asus RT-AC66U router (Linux 2.6) (86%), Asus RT-N10 router or AXIS 211A Network Camera (Linux 2.6) (86%),
Linux 2.6.18 (86%), Linux 2.6.24 (86%), Asus RT-N16 WAP (Linux 2.6) (86%), Asus RT-N66U WAP (Linux 2.6) (86%)
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 25.67 seconds

C:\Users\tidha>nmap -p80 -O 10.10.28.15
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-09 21:42 SE Asia Standard Time
Nmap scan report for 10.10.28.15
Host is up (0.0025s latency).

PORT   STATE SERVICE
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Apple TV 5.2.1 or 5.3 (98%), Crestron XPanel control system (98%), Vodavi XTS-IP PBX (97%), Ninte
ndo Wii game console (94%), Sony Bravia V5500-series TV (93%), Sony Bravia W5500-series TV (93%), Brother MFC-7820N prin
ter (93%), Microsoft Xbox game console (modified, running XboxMediaCenter) (93%), NEC UNIVERGE SV8100 PBX (93%), 3Com Su
perStack 3 Switch 3870 (92%)
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 21.46 seconds
```

Melakukan langkah di atas dengan menggunakkan IP Publik website tertentu (3 Website)

- Website www.kuyhaa-me.com (Nmap -O www.kuyhaa-me.com)

```
C:\WINDOWS\system32\cmd.exe

C:\Users\tidha>nmap -O www.kuyhaa-me.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-09 21:45 SE Asia Standard Time
Nmap scan report for www.kuyhaa-me.com (164.68.102.83)
Host is up (0.15s latency).
rDNS record for 164.68.102.83: vmi279619.contaboserver.net
Not shown: 994 closed ports
PORT     STATE    SERVICE
25/tcp   filtered smtp
53/tcp   open     domain
80/tcp   open     http
443/tcp  open     https
3306/tcp open     mysql
8080/tcp open     http-proxy
Device type: printer|broadband router|WAP|general purpose|webcam
Running (JUST GUESSING): Lexmark embedded (90%), Asus embedded (90%), Linux 2.6.X|2.4.X (90%), AXIS embedded (87%)
OS CPE: cpe:/h:lexmark:x644e cpe:/h:asus:rt-ac66u cpe:/o:linux:linux_kernel:2.6 cpe:/h:asus:rt-n16 cpe:/o:linux:linux_ke
rnel:2.4 cpe:/h:axis:211_network_camera cpe:/o:linux:linux_kernel:2.6.20 cpe:/o:linux:linux_kernel:2.4.26
Aggressive OS guesses: Lexmark X644e printer (90%), Asus RT-AC66U router (Linux 2.6) (90%), Asus RT-N16 WAP (Linux 2.6)
(90%), Asus RT-N66U WAP (Linux 2.6) (90%), Tomato 1.28 (Linux 2.6.22) (90%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (89%),
 Linux 2.6.18 - 2.6.22 (89%), Linux 2.6.24 (89%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russia
n 0.9 (Linux 2.4.30) (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.71 seconds
```

- Website www.kuyhaa-me.com (Nmap -p80 -O www.kuyhaa-me.com)

```
C:\WINDOWS\system32\cmd.exe

C:\Users\tidha>Nmap -p80 -O www.kuyhaa-me.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-09 21:49 SE Asia Standard Time
Nmap scan report for www.kuyhaa-me.com (164.68.102.83)
Host is up (0.0048s latency).
rDNS record for 164.68.102.83: vmi279619.contaboserver.net

PORT   STATE SERVICE
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 2.4.26 (Slackware 10.0.0) (93%), Linux 2.6.18 - 2.6.22 (93%), OpenWrt 0.9 - 7.09 (Linux 2.4
.30 - 2.4.34) (93%), OpenWrt White Russian 0.9 (Linux 2.4.30) (93%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (93%), Vodavi
XTS-IP PBX (91%), Crestron XPanel control system (91%), Tomato 1.27 - 1.28 (Linux 2.4.20) (91%), Linux 3.2.0 (91%), Mikr
oTik RouterOS 6.15 (Linux 3.3.5) (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.06 seconds
```

- Website www.skype.com (Nmap -O www.skype.com)

```
C:\WINDOWS\system32\cmd.exe

C:\Users\tidha>nmap -O www.kuyhaa-me.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-09 21:45 SE Asia Standard Time
Nmap scan report for www.kuyhaa-me.com (164.68.102.83)
Host is up (0.15s latency).
rDNS record for 164.68.102.83: vmi279619.contaboserver.net
Not shown: 994 closed ports
PORT     STATE    SERVICE
25/tcp   filtered smtp
53/tcp   open     domain
80/tcp   open     http
443/tcp  open     https
3306/tcp open     mysql
8080/tcp open     http-proxy
Device type: printer|broadband router|WAP|general purpose|webcam
Running (JUST GUESSING): Lexmark embedded (90%), Asus embedded (90%), Linux 2.6.X|2.4.X (90%), AXIS embedded (87%)
OS CPE: cpe:/h:lexmark:x644e cpe:/h:asus:rt-ac66u cpe:/o:linux:linux_kernel:2.6 cpe:/h:asus:rt-n16 cpe:/o:linux:linux_ke
rnel:2.4 cpe:/h:axis:211_network_camera cpe:/o:linux:linux_kernel:2.6.20 cpe:/o:linux:linux_kernel:2.4.26
Aggressive OS guesses: Lexmark X644e printer (90%), Asus RT-AC66U router (Linux 2.6) (90%), Asus RT-N16 WAP (Linux 2.6)
(90%), Asus RT-N66U WAP (Linux 2.6) (90%), Tomato 1.28 (Linux 2.6.22) (90%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (89%),
 Linux 2.6.18 - 2.6.22 (89%), Linux 2.6.24 (89%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russia
n 0.9 (Linux 2.4.30) (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.71 seconds
```

- Website www.skype.com (Nmap -p80 -O www.skype.com)

```
Select C:\WINDOWS\system32\cmd.exe

C:\Users\tidha>Nmap -p80 -O www.skype.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-09 21:52 SE Asia Standard Time
Nmap scan report for www.skype.com (52.113.194.133)
Host is up (0.0041s latency).

PORT   STATE SERVICE
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Apple TV 5.2.1 or 5.3 (98%), Crestron XPanel control system (98%), Vodavi XTS-IP PBX (97%), Ninte
ndo Wii game console (94%), Sony Bravia V5500-series TV (93%), Sony Bravia W5500-series TV (93%), Brother MFC-7820N prin
ter (93%), Microsoft Xbox game console (modified, running XboxMediaCenter) (93%), NEC UNIVERGE SV8100 PBX (93%), 3Com Su
perStack 3 Switch 3870 (92%)
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 21.30 seconds
```

- Website www.twitter.com (Nmap -O www.twitter.com)

```
C:\WINDOWS\system32\cmd.exe
C:\Users\tidha>Nmap -O www.twitter.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-09 22:03 SE Asia Standard Time
Nmap scan report for www.twitter.com (104.244.42.1)
Host is up (0.026s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
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: PBX|firewall|router
Running (JUST GUESSING): Vodavi embedded (87%), Juniper embedded (85%), Juniper JUNOS 13.X (85%)
OS CPE: cpe:/h:vodavi:xts-ip cpe:/h:juniper:srx100 cpe:/o:juniper:junos:13.3r8
Aggressive OS guesses: Vodavi XTS-IP PBX (87%), Juniper SRX100 firewall (85%), Juniper JUNOS 13.3R8 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 8 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.92 seconds
```

- Website www.twitter,com (Nmap -p80 -O www.twitter.com)

```
C:\WINDOWS\system32\cmd.exe
C:\Users\tidha>Nmap -O www.twitter.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-09 22:03 SE Asia Standard Time
Nmap scan report for www.twitter.com (104.244.42.1)
Host is up (0.026s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
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: PBX|firewall|router
Running (JUST GUESSING): Vodavi embedded (87%), Juniper embedded (85%), Juniper JUNOS 13.X (85%)
OS CPE: cpe:/h:vodavi:xts-ip cpe:/h:juniper:srx100 cpe:/o:juniper:junos:13.3r8
Aggressive OS guesses: Vodavi XTS-IP PBX (87%), Juniper SRX100 firewall (85%), Juniper JUNOS 13.3R8 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 8 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.92 seconds
```