Nama: Limas Baginta

NPM: 1306368690

Jurusan: Teknik Komputer

Praktikum: Keamanan Jaringan Komputer

Tugas Tambahan Modul 7

1. Langkah-langkah konfigurasi snort hingga dapat berfungsi sebagai IDS

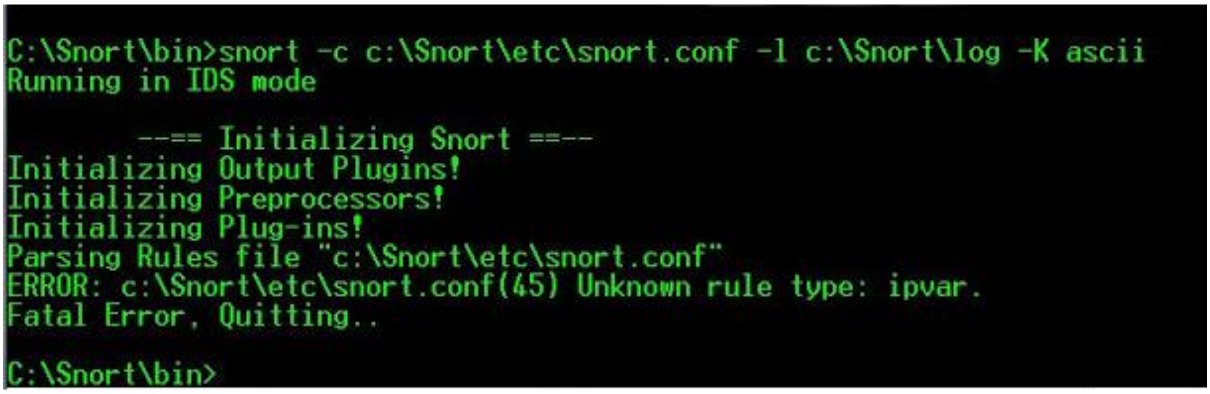
a. Pertama Download Snort installer dari www.snort.org
Install **Snort** and **Winpcap**
dan explor in C:\snort Folder
Kembali menuju www.snort.org
Login snort dan download **RULES** dari www.snort.org.
Unrar rule.zip menuju c:\snort [overwrite]

b. Ketik cmd dalam pencarian windows, dan pilih RUN AS ADMINISTRATOR lalu ketik
C:\snort\bin>snort -c c:\snort\etc\snort.conf -l c:\snort\log -K ascii

Yang mana:

-c = Test file konfigurasi
-l = Direktori log
-K = Logging mode [pcap (default), ascii, none]

Eror-1:



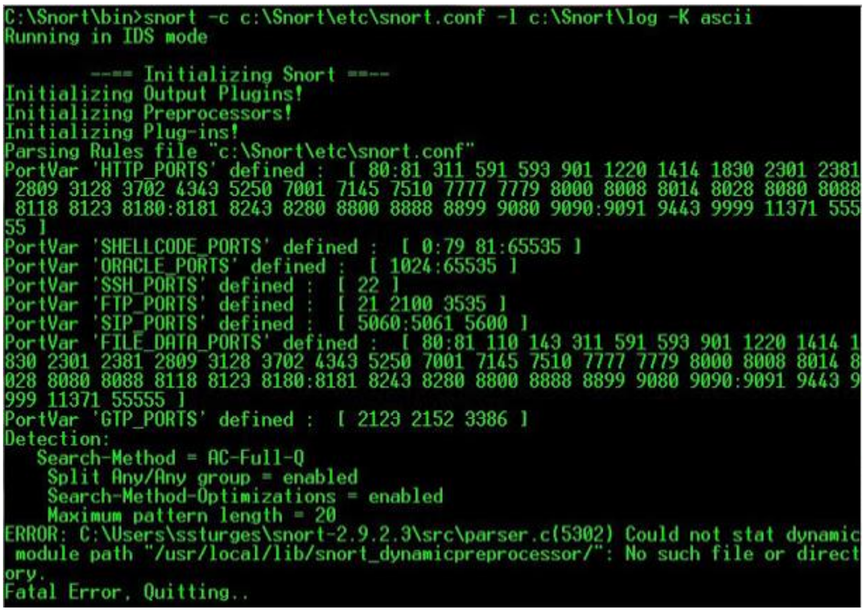
```
C:\Snort\bin>snort -c c:\Snort\etc\snort.conf -l c:\Snort\log -K ascii
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\Snort\etc\snort.conf"
ERROR: c:\Snort\etc\snort.conf(45) Unknown rule type: ipvar.
Fatal Error, Quitting..

C:\Snort\bin>
```

Berlokasi dalam c:\snort\etc\
Pada line 45, replace kata

"Ipvar to var" (replace all)

Run command lagi pada CMD:
C:\snort\bin>snort -c c:\snort\etc\snort.conf -l c:\snort\log -K ascii

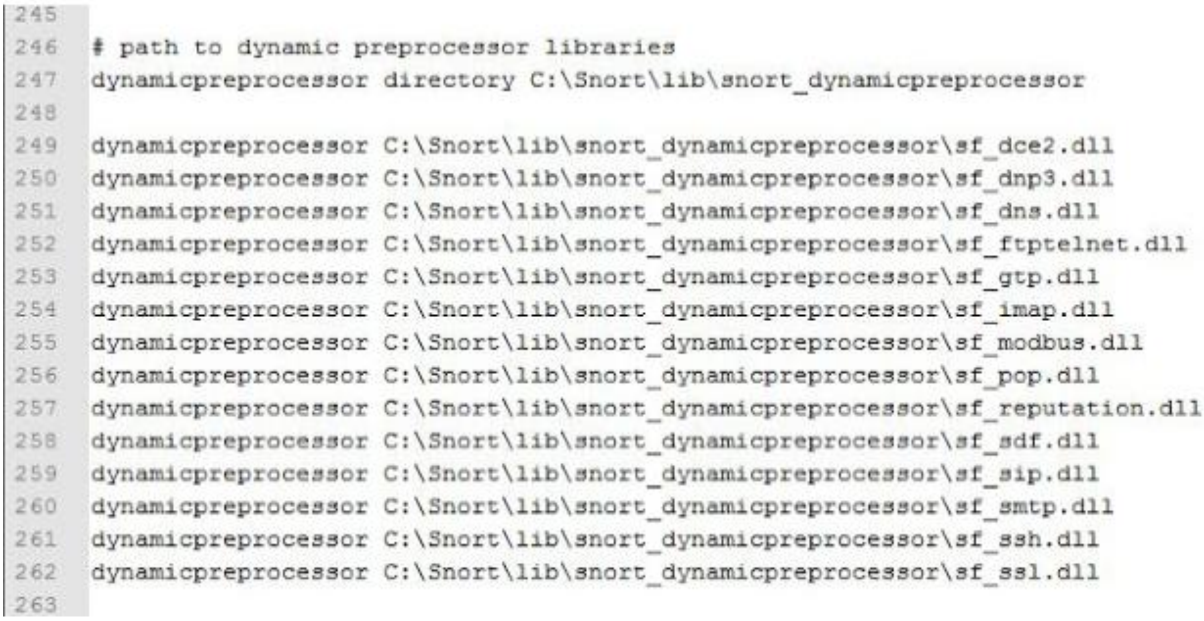
Eror-2:



```
C:\Snort\bin>snort -c c:\Snort\etc\snort.conf -l c:\Snort\log -K ascii
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\Snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 591 593 901 1220 1414 1830 2301 2381
 2809 3128 3702 4343 5250 7001 7145 7510 7777 7779 8000 8008 8014 8028 8080 8088
 8118 8123 8180:8181 8243 8280 8800 8888 8899 9080 9090:9091 9443 9999 11371 555
55 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 591 593 901 1220 1414 1
830 2301 2381 2809 3128 3702 4343 5250 7001 7145 7510 7777 7779 8000 8008 8014 8
028 8080 8088 8118 8123 8180:8181 8243 8280 8800 8888 8899 9080 9090:9091 9443 9
999 11371 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
ERROR: C:\Users\ssturges\snort-2.9.2.3\src\parser.c(5302) Could not stat dynamic
 module path "/usr/local/lib/snort_dynamicpreprocessor/": No such file or direct
ory.
Fatal Error, Quitting..
```

Ganti path menjadi C:\snort\lib\snort_dynamicpreprocessor\

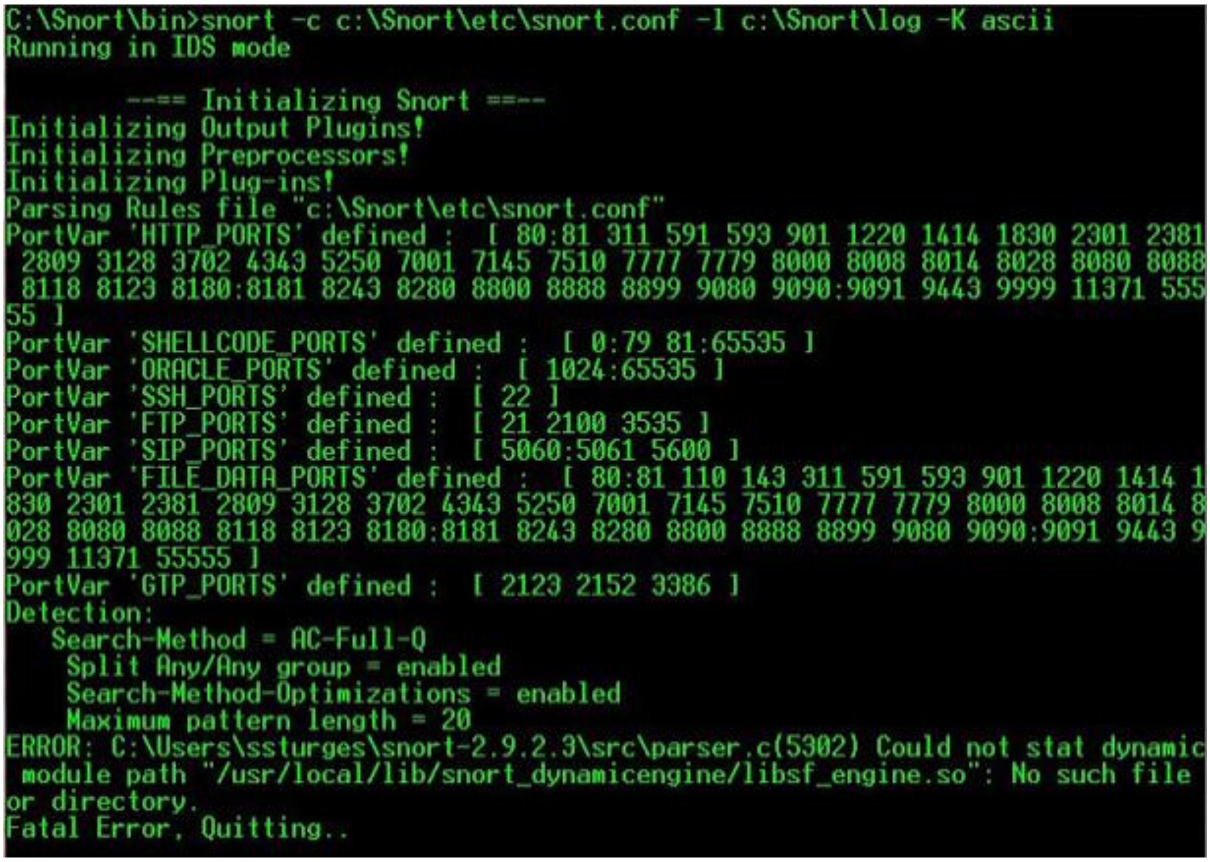
Lalu copy semua data dalam folder tersebut dan paste pada file konfigurasi pada line 249



```
245
246  # path to dynamic preprocessor libraries
247  dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor
248
249  dynamicpreprocessor C:\Snort\lib\snort_dynamicpreprocessor\sf_dce2.dll
250  dynamicpreprocessor C:\Snort\lib\snort_dynamicpreprocessor\sf_dnp3.dll
251  dynamicpreprocessor C:\Snort\lib\snort_dynamicpreprocessor\sf_dns.dll
252  dynamicpreprocessor C:\Snort\lib\snort_dynamicpreprocessor\sf_ftptelnet.dll
253  dynamicpreprocessor C:\Snort\lib\snort_dynamicpreprocessor\sf_gtp.dll
254  dynamicpreprocessor C:\Snort\lib\snort_dynamicpreprocessor\sf_imap.dll
255  dynamicpreprocessor C:\Snort\lib\snort_dynamicpreprocessor\sf_modbus.dll
256  dynamicpreprocessor C:\Snort\lib\snort_dynamicpreprocessor\sf_pop.dll
257  dynamicpreprocessor C:\Snort\lib\snort_dynamicpreprocessor\sf_reputation.dll
258  dynamicpreprocessor C:\Snort\lib\snort_dynamicpreprocessor\sf_sdf.dll
259  dynamicpreprocessor C:\Snort\lib\snort_dynamicpreprocessor\sf_sip.dll
260  dynamicpreprocessor C:\Snort\lib\snort_dynamicpreprocessor\sf_smtp.dll
261  dynamicpreprocessor C:\Snort\lib\snort_dynamicpreprocessor\sf_ssh.dll
262  dynamicpreprocessor C:\Snort\lib\snort_dynamicpreprocessor\sf_ssl.dll
263
```

Lakukan lagi: C:\snort\bin>snort -c c:\snort\etc\snort.conf -l c:\snort\log -K ascii

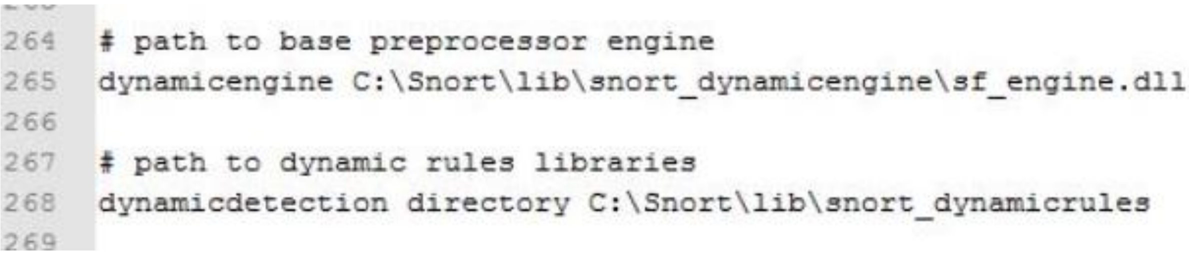
Eror-3:



```
C:\Snort\bin>snort -c c:\Snort\etc\snort.conf -l c:\Snort\log -K ascii
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\Snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 591 593 901 1220 1414 1830 2301 2381
 2809 3128 3702 4343 5250 7001 7145 7510 7777 7779 8000 8008 8014 8028 8080 8088
 8118 8123 8180:8181 8243 8280 8800 8888 8899 9080 9090:9091 9443 9999 11371 555
55 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 591 593 901 1220 1414 1
830 2301 2381 2809 3128 3702 4343 5250 7001 7145 7510 7777 7779 8000 8008 8014 8
028 8080 8088 8118 8123 8180:8181 8243 8280 8800 8888 8899 9080 9090:9091 9443 9
999 11371 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
ERROR: C:\Users\ssturges\snort-2.9.2.3\src\parser.c(5302) Could not stat dynamic
 module path "/usr/local/lib/snort_dynamicengine/libsf_engine.so": No such file
or directory.
Fatal Error, Quitting..
```

Ganti path untuk dynamicengine and dynamicrulesmenjadi

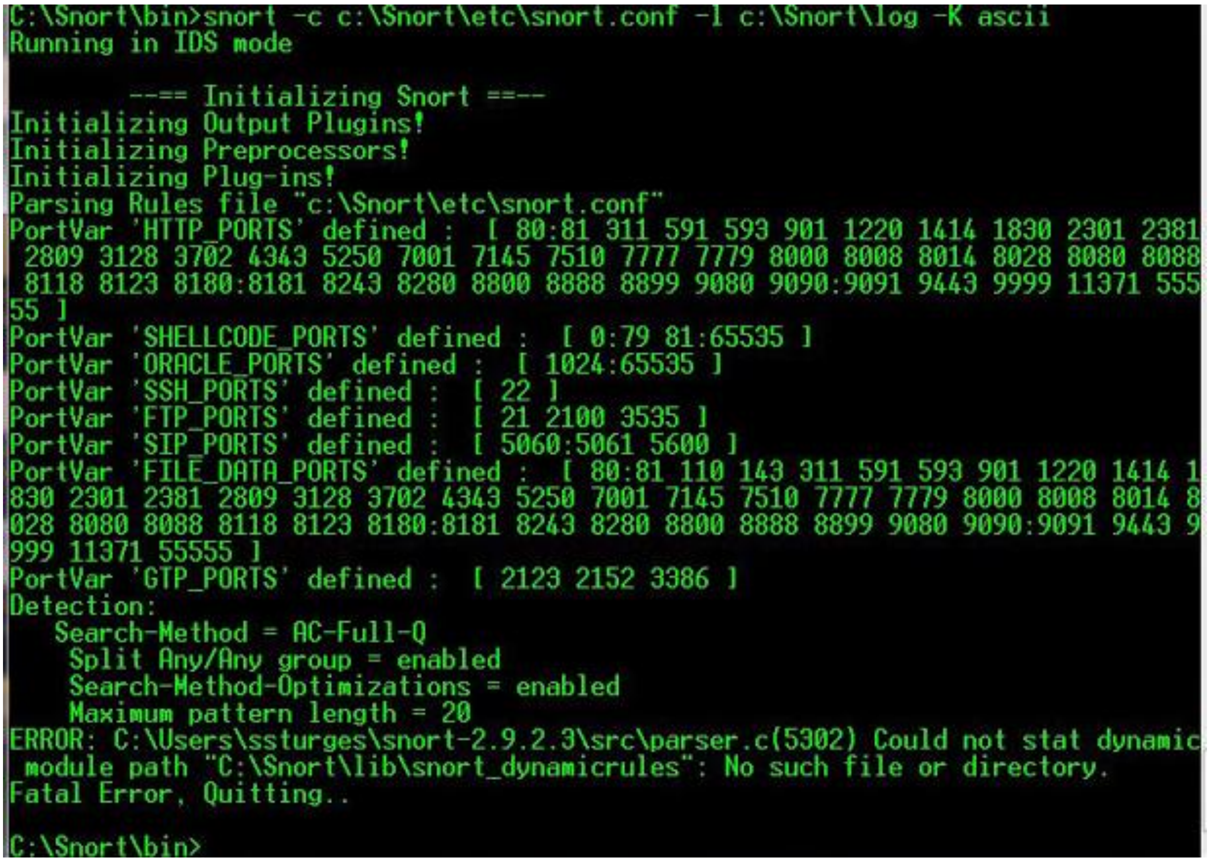
c:\snort\lib and change the ".SO" extension to ".dll"



```
# path to base preprocessor engine
dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll

# path to dynamic rules libraries
dynamicdetection directory C:\Snort\lib\snort_dynamicrules
```

Run kembali: C:\snort\bin>snort -c c:\snort\etc\snort.conf -l c:\snort\log -K ascii

Eror-4:

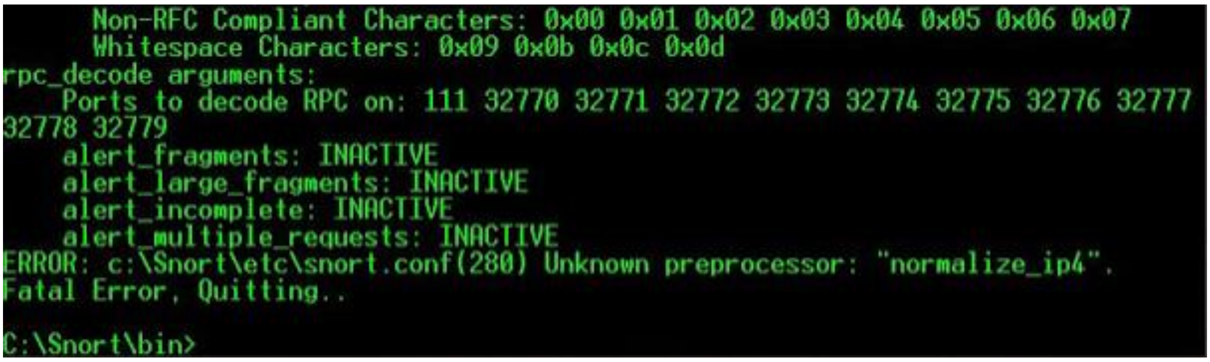


```
C:\Snort\bin>snort -c c:\Snort\etc\snort.conf -l c:\Snort\log -K ascii
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\Snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 591 593 901 1220 1414 1830 2301 2381
 2809 3128 3702 4343 5250 7001 7145 7510 7777 7779 8000 8008 8014 8028 8080 8088
 8118 8123 8180:8181 8243 8280 8800 8888 8899 9080 9090:9091 9443 9999 11371 555
55 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 591 593 901 1220 1414 1
830 2301 2381 2809 3128 3702 4343 5250 7001 7145 7510 7777 7779 8000 8008 8014 8
028 8080 8088 8118 8123 8180:8181 8243 8280 8800 8888 8899 9080 9090:9091 9443 9
999 11371 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
ERROR: C:\Users\ssturges\snort-2.9.2.3\src\parser.c(5302) Could not stat dynamic
 module path "C:\Snort\lib\snort_dynamicrules": No such file or directory.
Fatal Error, Quitting..

C:\Snort\bin>
```

buat folder dengan nama snort_dynamicrules dalam C:\snort\lib\

Run lagi: C:\snort\bin>snort -c c:\snort\etc\snort.conf -l c:\snort\log -K ascii

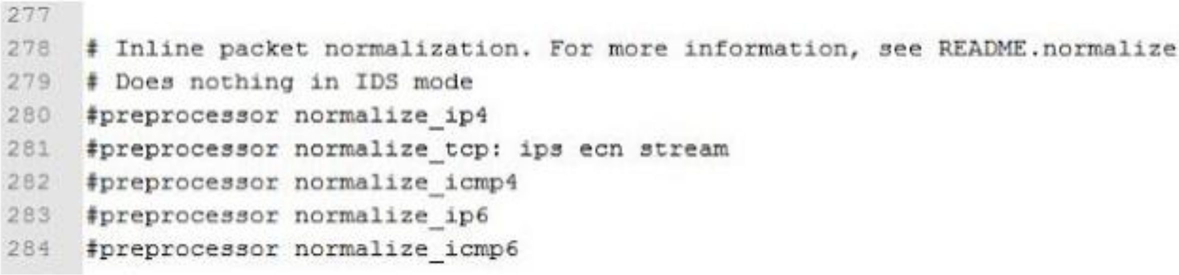
Eror-5:



```
      Non-RFC Compliant Characters: 0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07
      Whitespace Characters: 0x09 0x0b 0x0c 0x0d
rpc_decode arguments:
    Ports to decode RPC on: 111 32770 32771 32772 32773 32774 32775 32776 32777
32778 32779
    alert_fragments: INACTIVE
    alert_large_fragments: INACTIVE
    alert_incomplete: INACTIVE
    alert_multiple_requests: INACTIVE
ERROR: c:\Snort\etc\snort.conf(280) Unknown preprocessor: "normalize_ip4".
Fatal Error, Quitting..

C:\Snort\bin>
```

Pada line 278 sampai 284

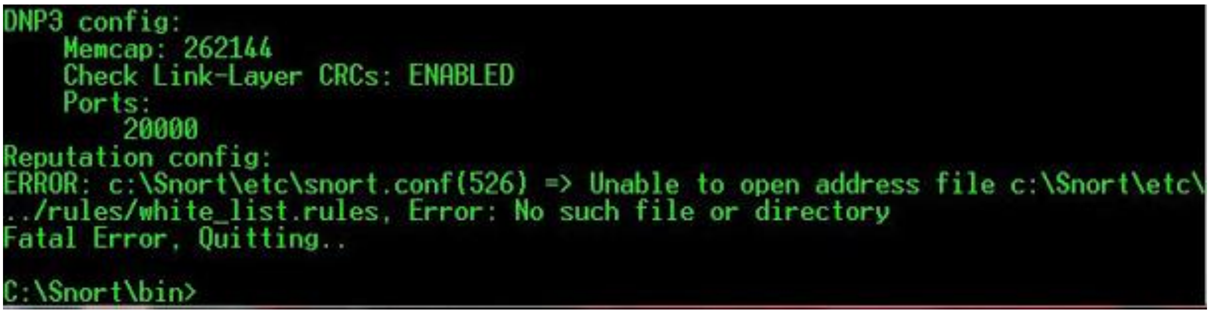
Lalu beri komentar pada semua preprocessor normalize(menggunakan #)



```
277
278  # Inline packet normalization. For more information, see README.normalize
279  # Does nothing in IDS mode
280  #preprocessor normalize_ip4
281  #preprocessor normalize_tcp: ips ecn stream
282  #preprocessor normalize_icmp4
283  #preprocessor normalize_ip6
284  #preprocessor normalize_icmp6
```

Run lagi: C:\snort\bin>snort -c c:\snort\etc\snort.conf -l c:\snort\log -K ascii

Eror-6:

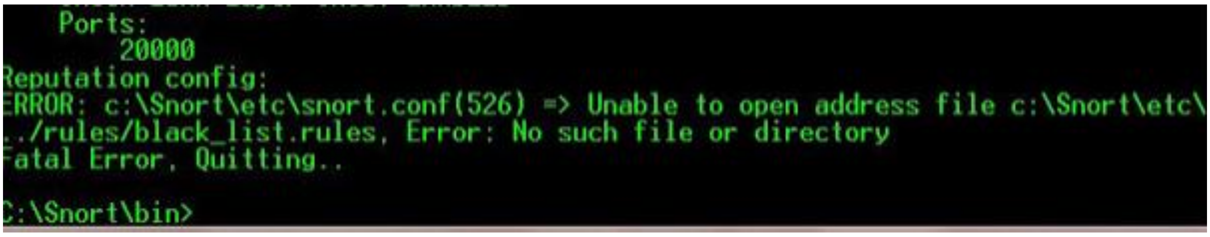


```
DNP3 config:
    Memcap: 262144
    Check Link-Layer CRCs: ENABLED
    Ports:
        20000
Reputation config:
ERROR: c:\Snort\etc\snort.conf(526) => Unable to open address file c:\Snort\etc\
../rules/white_list.rules, Error: No such file or directory
Fatal Error, Quitting..

C:\Snort\bin>
```

Kemudian buat dokumen text dalam c:\snort\rules\ dengan nama “white_list.rules”

Run lagi: C:\snort\bin>snort -c c:\snort\etc\snort.conf -l c:\snort\log -K ascii

Eror-7:



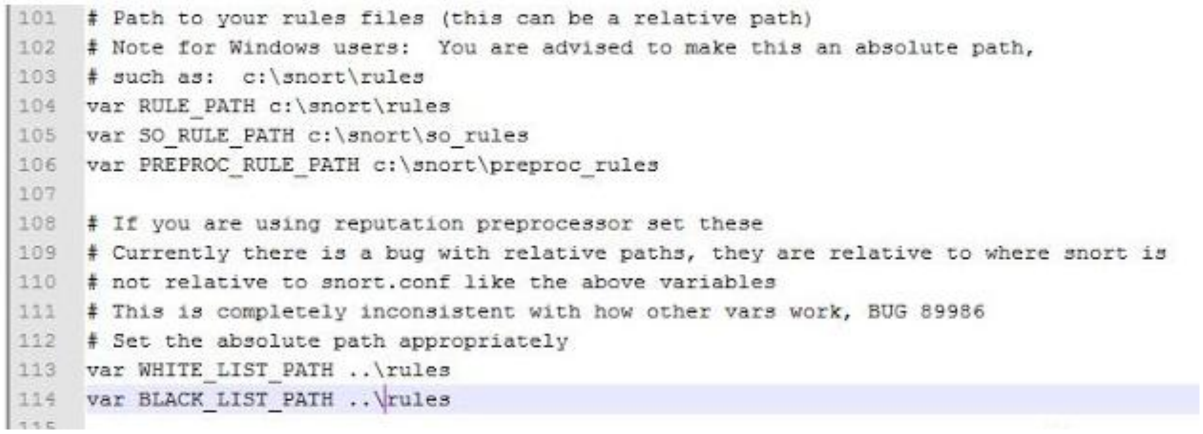
```
    Ports:
        20000
eputation config:
RROR: c:\Snort\etc\snort.conf(526) => Unable to open address file c:\Snort\etc\
./rules/black_list.rules, Error: No such file or directory
atal Error, Quitting..

:\Snort\bin>
```

Lalu buat dokumen text dalam   c:\snort\rules\ dengan nama “Black_list.rules”

Buka **snort.conf**

Line 104 ubah path dari var RULE_PATH

sama seperti line no. 105 and 106



```
101 # Path to your rules files (this can be a relative path)
102 # Note for Windows users:  You are advised to make this an absolute path,
103 # such as:  c:\snort\rules
104 var RULE_PATH c:\snort\rules
105 var SO_RULE_PATH c:\snort\so_rules
106 var PREPROC_RULE_PATH c:\snort\preproc_rules
107
108 # If you are using reputation preprocessor set these
109 # Currently there is a bug with relative paths, they are relative to where snort is
110 # not relative to snort.conf like the above variables
111 # This is completely inconsistent with how other vars work, BUG 89986
112 # Set the absolute path appropriately
113 var WHITE_LIST_PATH ..\rules
114 var BLACK_LIST_PATH ..\rules
```

Sekarang pada line 113 dan 114, yakni

var WHITE_LIST_PATH ../rules

var BLACK_LIST_PATH ../rules

ubah tanda ‘/ ’ menjadi ‘ \ ’

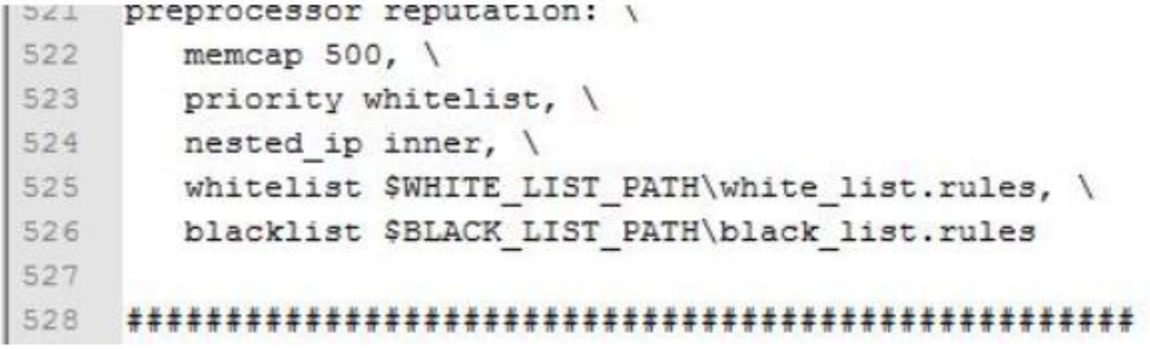
Pada line 525 dan 526

Cari line:

**whitelist $WHITE_LIST_PATH/white_list.rules, **

blacklist $BLACK_LIST_PATH/black_list.rules

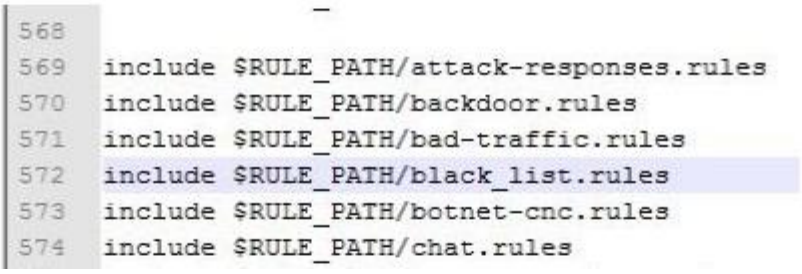
dan ubah tanda ‘/’ menjadi ‘\’



```
521  preprocessor reputation: \
522     memcap 500, \
523     priority whitelist, \
524     nested_ip inner, \
525     whitelist $WHITE_LIST_PATH\white_list.rules, \
526     blacklist $BLACK_LIST_PATH\black_list.rules
527
528  ####################################################
```

Pada line 572 include $RULE_PATH/blacklist.rules

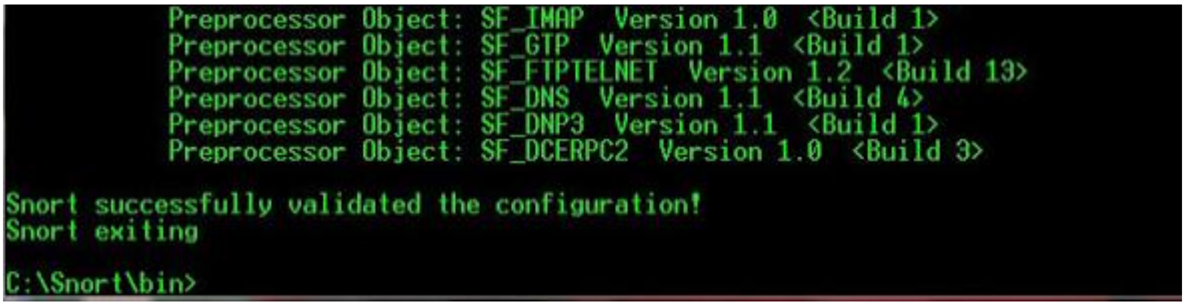
Ubah nama blacklist menjadi black_list



```
568
569  include $RULE_PATH/attack-responses.rules
570  include $RULE_PATH/backdoor.rules
571  include $RULE_PATH/bad-traffic.rules
572  include $RULE_PATH/black_list.rules
573  include $RULE_PATH/botnet-cnc.rules
574  include $RULE_PATH/chat.rules
```

Akhirnya run:

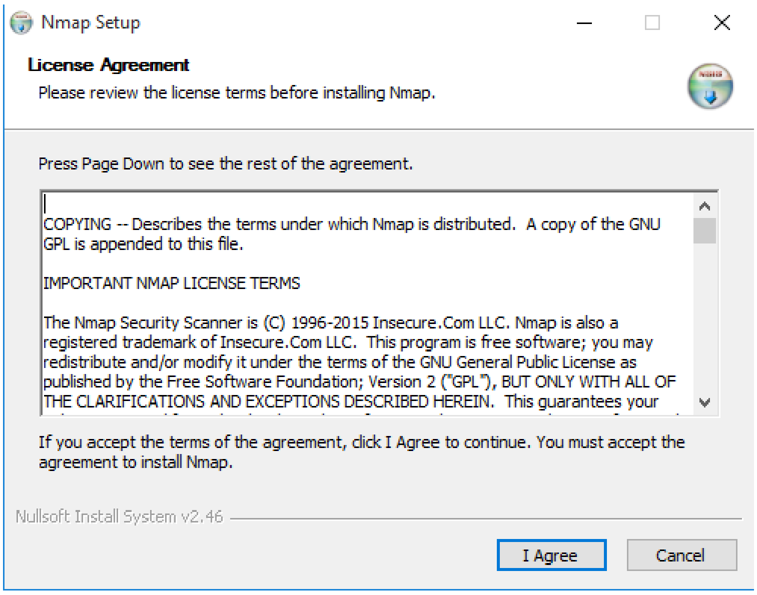
C:\snort\bin>snort -i 1 -l c:\snort\log -c c:\snort\etc\snort.conf -T



```
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>

Snort successfully validated the configuration!
Snort exiting

C:\Snort\bin>
```

2. Langkah-langkah instalasi nmap

a.



Nmap Setup

License Agreement

Please review the license terms before installing Nmap.

Press Page Down to see the rest of the agreement.

COPYING -- Describes the terms under which Nmap is distributed. A copy of the GNU GPL is appended to this file.

IMPORTANT NMAP LICENSE TERMS

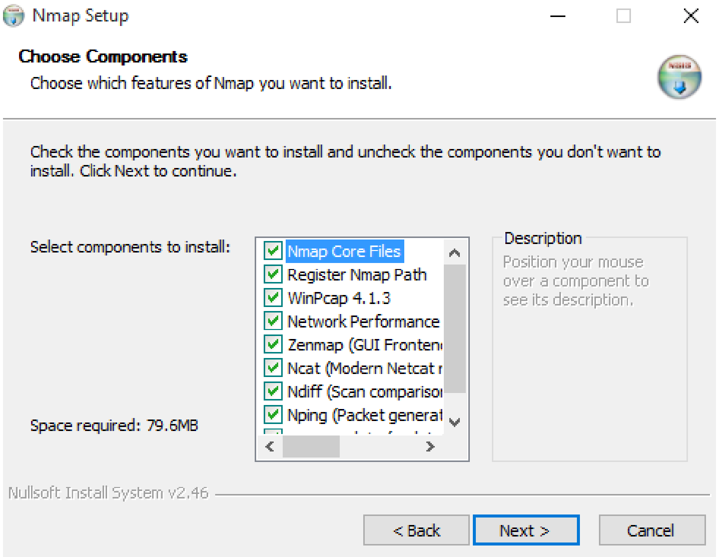
The Nmap Security Scanner is (C) 1996-2015 Insecure.Com LLC. Nmap is also a registered trademark of Insecure.Com LLC. This program is free software; you may redistribute and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; Version 2 ("GPL"), BUT ONLY WITH ALL OF THE CLARIFICATIONS AND EXCEPTIONS DESCRIBED HEREIN. This guarantees your

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Nmap.

Nullsoft Install System v2.46

Klik “I Agree”

b.



Nmap Setup

Choose Components

Choose which features of Nmap you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

- ☑ Nmap Core Files
- ☑ Register Nmap Path
- ☑ WinPcap 4.1.3
- ☑ Network Performance
- ☑ Zenmap (GUI Fronten
- ☑ Ncat (Modern Netcat r
- ☑ Ndiff (Scan compariso
- ☑ Nping (Packet generat

Space required: 79.6MB

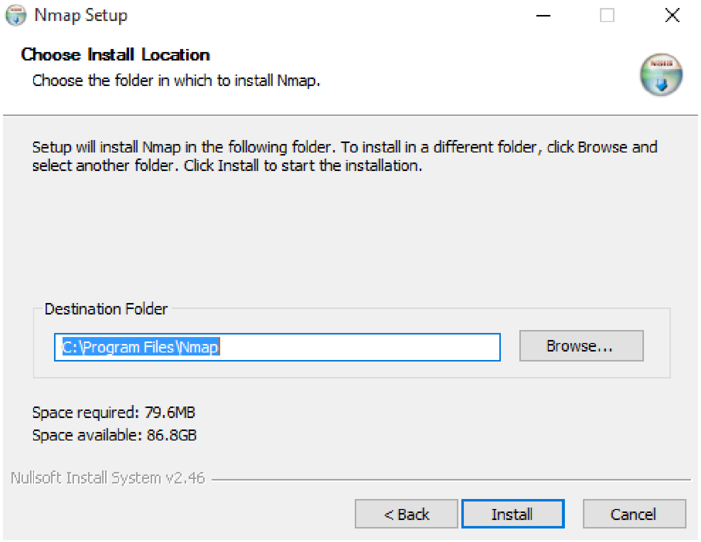
Description

Position your mouse over a component to see its description.

Nullsoft Install System v2.46

Klik “Next”

c.



Nmap Setup

Choose Install Location

Choose the folder in which to install Nmap.

Setup will install Nmap in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder

C:\Program Files\Nmap

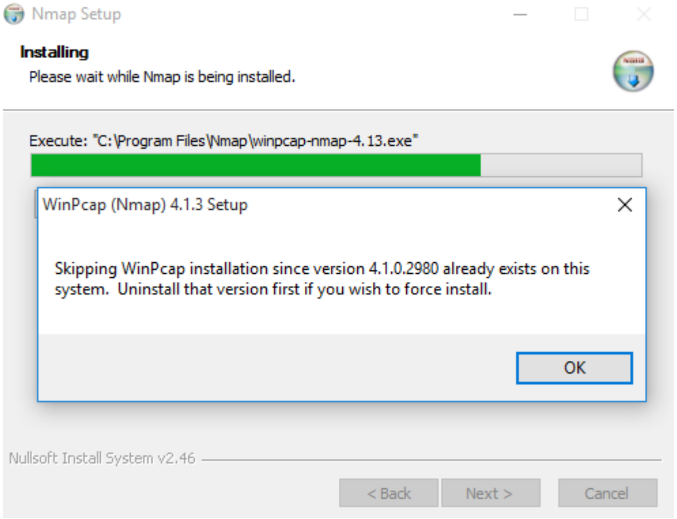
Space required: 79.6MB

Space available: 86.8GB

Nullsoft Install System v2.46

Pilih destinasi folder lalu klik “Install”

d.



Nmap Setup

Installing

Please wait while Nmap is being installed.

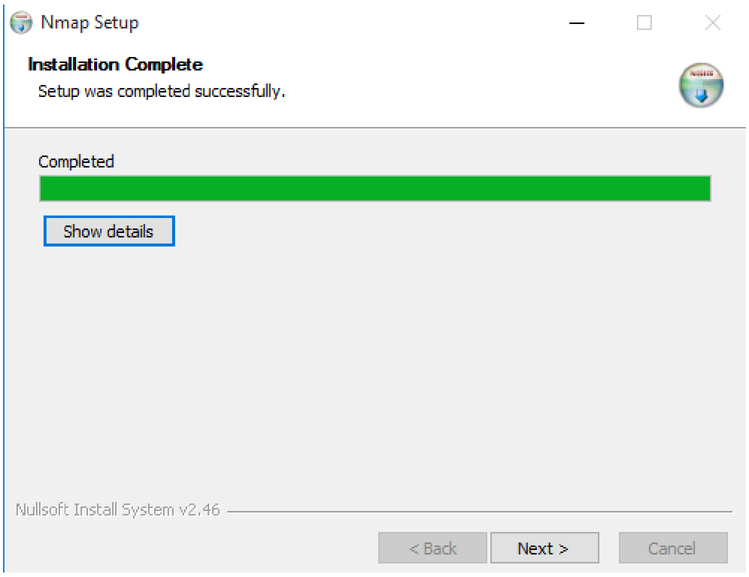
Execute: "C:\Program Files\Nmap\winpcap-nmap-4.13.exe"

WinPcap (Nmap) 4.1.3 Setup

Skipping WinPcap installation since version 4.1.0.2980 already exists on this system. Uninstall that version first if you wish to force install.

Nullsoft Install System v2.46

Apabila Winpcap telah terinstal klik “OK” e.



Nmap Setup

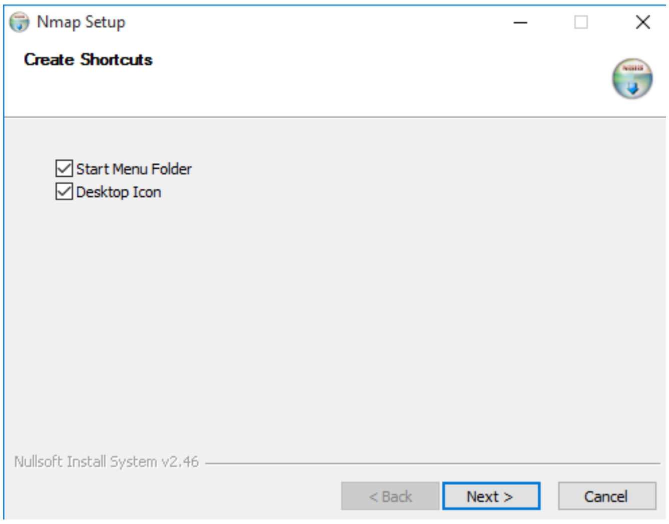
Installation Complete

Setup was completed successfully.

Completed

Klik “Next”

f.



Nmap Setup

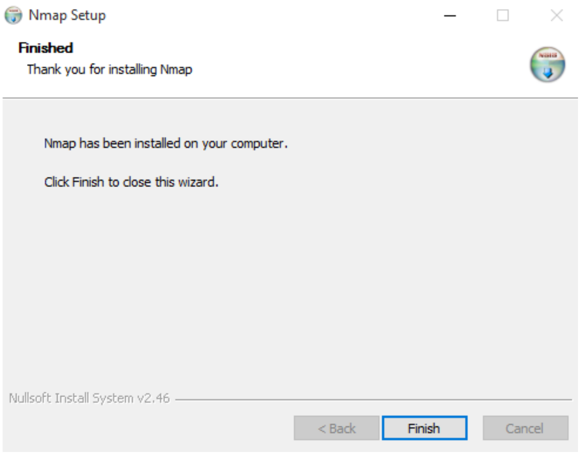
Create Shortcuts

☑ Start Menu Folder

☑ Desktop Icon

Klik “Next”

g.



Finished

Thank you for installing Nmap

Nmap has been installed on your computer.

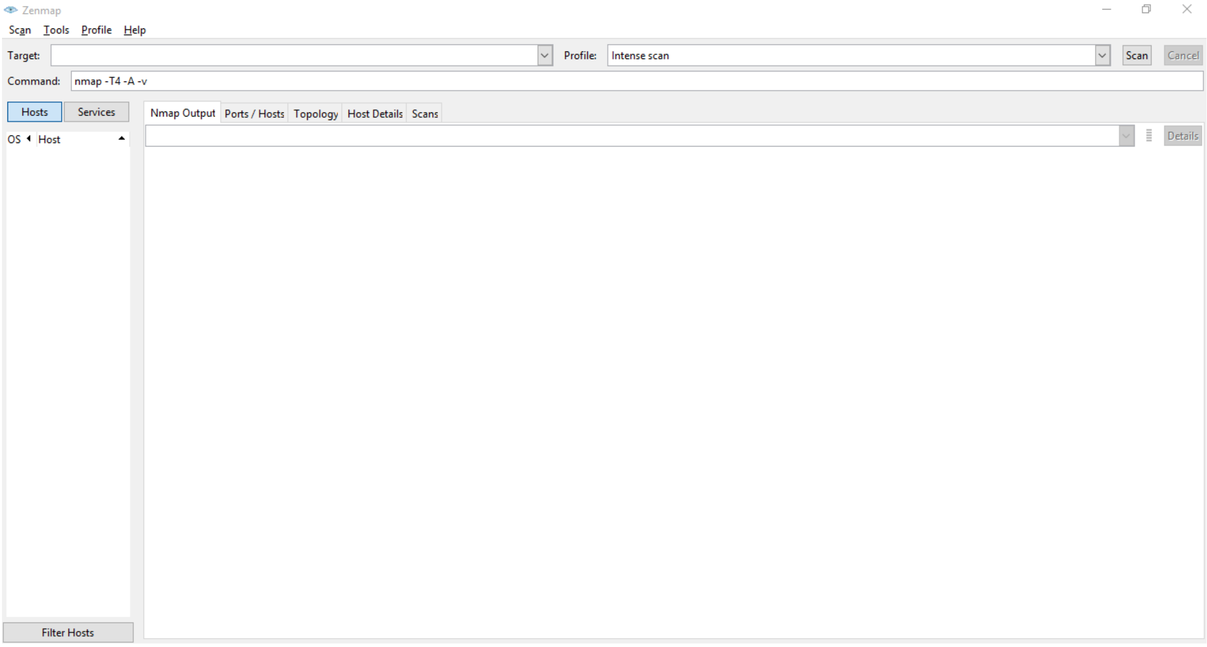
Click Finish to close this wizard.

Klik “Finish”

Penggunaan aplikasi simulasi serangan:

1. Buka zenmap

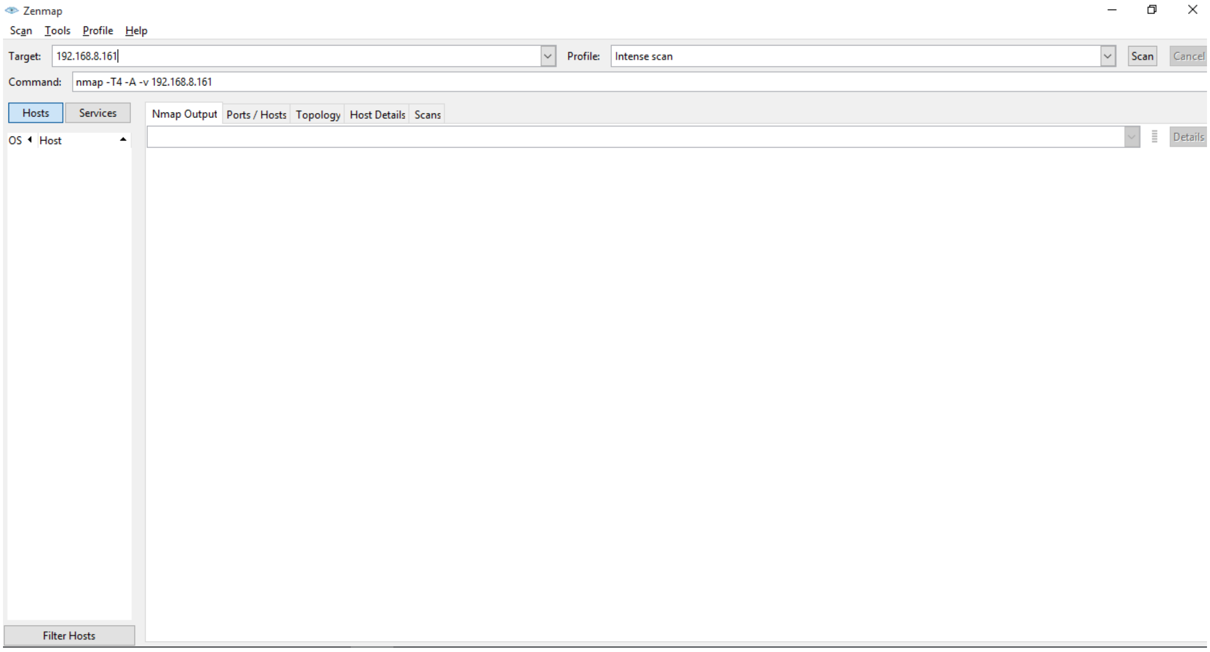
Lalu ketikkan IP Target lalu klik “Scan”



Profile: Intense scan

Command: nmap -T4 -A -v

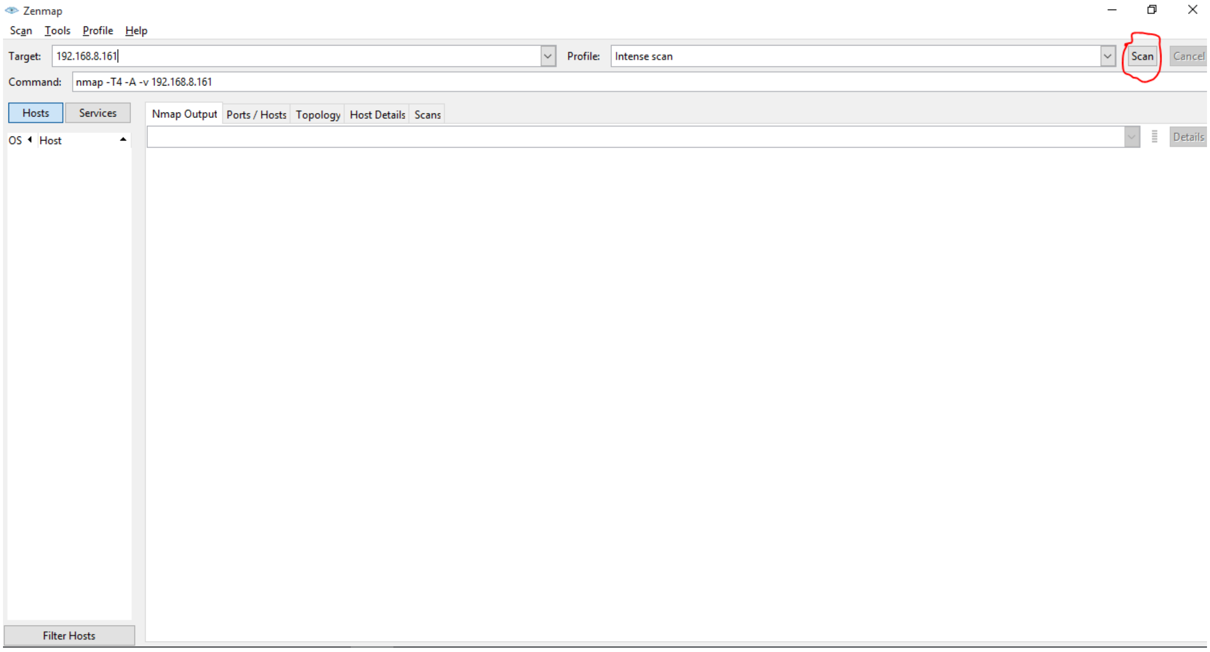
2. Isi IP target


Target: 192.168.8.161

Profile: Intense scan

Command:
```
nmap -T4 -A -v 192.168.8.161
```

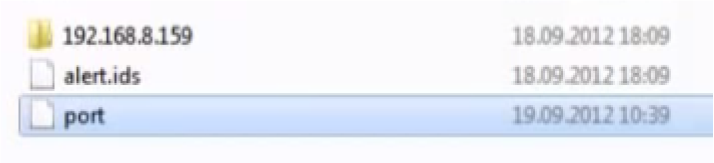
3. Lalu klik “Scan”


Target: 192.168.8.161

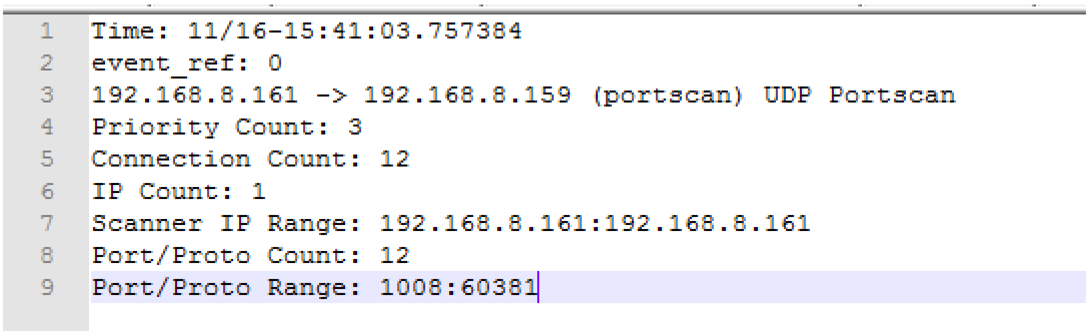
Profile: Intense scan

Command:
```
nmap -T4 -A -v 192.168.8.161
```

3.Screenshot laporan serangan (langkah 4)



192.168.8.159	18.09.2012 18:09
alert.ids	18.09.2012 18:09
port	19.09.2012 10:39



```
Time: 11/16-15:41:03.757384
event_ref: 0
192.168.8.161 -> 192.168.8.159 (portscan) UDP Portscan
Priority Count: 3
Connection Count: 12
IP Count: 1
Scanner IP Range: 192.168.8.161:192.168.8.161
Port/Proto Count: 12
Port/Proto Range: 1008:60381
```

4. Penjelasan dari screenshot laporan serangan tersebut

Dari hasil port.log

Terlihat bahwa IP penyerang adalah 192.168.8.161

dan IP yang diserang adalah 192.168.8.159

Kejadian ini berlangsung dengan menyeleksi (scanning) 12 IP dan akhirnya penyerang berhasil menyerang IP 192.168.8.159

Jenis Port yang dilakukan scan adalah UDP Port yang mana UDP menyediakan cheksum untuk data integrity dan port number dari source menuju destination suatu datagram.