



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS BRAWIJAYA**

---

BAB : AUDIT DAN MONITORING  
NAMA : DANI ADRIAN  
NIM : 225150201111009  
TANGGAL : 28/03/2024  
ASISTEN : Bernas Cakra Sakti Harisna  
Mohammad Seto Aji Pamungkas

---

**Instalasi Persiapan Lingkungan Praktikum**

**Instruksi instalasi snort versi 2.xx di kali linux**

1. Buat file bernama "bullseye.list" di dalam direktori /etc/apt/sources.list.d/misal:

```
nano /etc/apt/sources.list.d/bullseye.list
```

```
(user@kali)-[~]  
$ sudo nano /etc/apt/sources.list.d/bullseye.list
```

1 Nama : Dani Adrian  
2 NIM : 225150201111009  
3

```
sudo nano /etc/apt/sources.list.d/bullseye.list
```

2. Tambahkan baris berikut ke dalam file tersebut:

```
deb http://deb.debian.org/debian bullseye main contrib non-  
free
```



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS BRAWIJAYA**

BAB : AUDIT DAN MONITORING  
NAMA : DANI ADRIAN  
NIM : 225150201111009  
TANGGAL : 28/03/2024  
ASISTEN : Bernas Cakra Sakti Harisna  
Mohammad Seto Aji Pamungkas

The screenshot shows a Kali Linux desktop environment. In the foreground, a terminal window is open at the prompt `(user@kali)-[/etc/apt/sources.list.d]`. The user has run `ls`, showing `bullseye.list`. The terminal output is as follows:

```
(user@kali)-[/etc/apt/sources.list.d]
$ ls
bullseye.list
(user@kali)-[/etc/apt/sources.list.d]
$
```

In the background, a mousepad window titled `~/Desktop/documentnama - Mousepad` is open, displaying the following text:

```
1 Nama : Dani Adrian
2 NIM : 225150201111009
3
```

The terminal window also shows the content of `bullseye.list` being edited in nano 7.2:

```
GNU nano 7.2 bullseye.list *
deb http://deb.debian.org/debian bullseye main contrib non-free
```

3. Jalankan:

```
sudo apt update
sudo apt install -t bullseye snort
```



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS BRAWIJAYA**

BAB : AUDIT DAN MONITORING  
NAMA : DANI ADRIAN  
NIM : 225150201111009  
TANGGAL : 28/03/2024  
ASISTEN : Bernas Cakra Sakti Harisna  
Mohammad Seto Aji Pamungkas

sudo apt update

```
(user@kali)~[/etc/apt/sources.list.d]
$ sudo apt update
Get:1 http://deb.debian.org/debian bullseye InRelease [116 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 Packages [8068 kB]
Get:3 http://kali.cs.nycu.edu.tw/kali kali-rolling InRelease [41.5 kB]
Get:4 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 Packages [19.5 MB]
Get:5 http://deb.debian.org/debian bullseye/main Translation-en [6236 kB]
Get:6 http://deb.debian.org/debian bullseye/main amd64 Contents (deb) [10.3 MB]
Get:7 http://deb.debian.org/debian bullseye/main all Contents (deb) [31.1 MB]
Get:8 http://deb.debian.org/debian bullseye/contrib amd64 Packages [50.4 kB]
Get:9 http://deb.debian.org/debian bullseye/contrib Translation-en [46.9 kB]
Get:10 http://deb.debian.org/debian bullseye/contrib amd64 Contents (deb) [54.7 kB]
Get:11 http://deb.debian.org/debian bullseye/contrib all Contents (deb) [57.3 kB]
Get:12 http://deb.debian.org/debian bullseye/non-free amd64 Packages [96.3 kB]
Get:13 http://deb.debian.org/debian bullseye/non-free Translation-en [92.2 kB]
Get:14 http://deb.debian.org/debian bullseye/non-free amd64 Contents (deb) [79.9 kB]
Get:15 http://deb.debian.org/debian bullseye/non-free all Contents (deb) [888 kB]
Get:16 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 Contents (deb) [45.9 MB]
Get:17 http://kali.cs.nycu.edu.tw/kali kali-rolling/contrib amd64 Packages [116 kB]
Get:18 http://kali.cs.nycu.edu.tw/kali kali-rolling/contrib amd64 Contents (deb) [247 kB]
Get:19 http://kali.cs.nycu.edu.tw/kali kali-rolling/non-free amd64 Packages [194 kB]
Get:20 http://kali.cs.nycu.edu.tw/kali kali-rolling/non-free amd64 Contents (deb) [884 kB]
Fetched 124 MB in 2min 34s (806 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
90 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

sudo apt install -t bullseye snort

```
(user@kali)~[/etc/apt/sources.list.d]
$ sudo apt install -t bullseye snort
[sudo] password for user:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libadwaita-1-0 libappstream5 libatk-adaptor libboost-dev libboost1.83-dev libopenblas-dev
  libopenblas-pthread-dev libopenblas0 libpython3-all-dev libpython3.12 libpython3.12-dev
  libstemmer0d libxmlb2 libxsimd-dev python3-all-dev python3-beniget python3-gast
  python3-pyatspi python3-pythrane python3.12-dev xtl-dev zenity zenity-common
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libdaq2 libestr0 libfastjson4 liblognorm5 libssl1.1 oinkmaster rsyslog snort-common
  snort-common-libraries snort-rules-default
Suggested packages:
  rsyslog-mysql | rsyslog-pgsql rsyslog-mongodb rsyslog-doc rsyslog-openssl | rsyslog-gnutls
  rsyslog-gssapi rsyslog-relp snort-doc
The following NEW packages will be installed:
  libdaq2 libestr0 libfastjson4 liblognorm5 libssl1.1 oinkmaster rsyslog snort snort-common
  snort-common-libraries snort-rules-default
0 upgraded, 11 newly installed, 0 to remove and 89 not upgraded.
Need to get 0 B/5161 kB of archives.
After this operation, 16.9 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS BRAWIJAYA**

BAB : AUDIT DAN MONITORING  
NAMA : DANI ADRIAN  
NIM : 225150201111009  
TANGGAL : 28/03/2024  
ASISTEN : Bernas Cakra Sakti Harisna  
Mohammad Seto Aji Pamungkas





**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS BRAWIJAYA**

BAB : AUDIT DAN MONITORING  
NAMA : DANI ADRIAN  
NIM : 225150201111009  
TANGGAL : 28/03/2024  
ASISTEN : Bernas Cakra Sakti Harisna  
Mohammad Seto Aji Pamungkas







**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS BRAWIJAYA**

BAB : AUDIT DAN MONITORING  
NAMA : DANI ADRIAN  
NIM : 225150201111009  
TANGGAL : 28/03/2024  
ASISTEN : Bernas Cakra Sakti Harisna  
Mohammad Seto Aji Pamungkas

Package configuration

Configuring snort

Interface(s) which Snort should listen on:

eth0 br-6997956cef8a docker0 br-8017fe66e14

<Ok>

\*~/Desktop/documentnama - Mousepad

File Edit Search View Document Help

1 Nama : Dani Adrian  
2 NIM : 225150201111009

user@kali: /etc/apt/sources.list.d

File Actions Edit View Help

Device "veth2c4031a@if8" does not exist.  
Snort configuration: WARNING: The interfaces configured are not valid  
Device "veth2c4031a@if8" does not exist.  
Snort configuration: WARN: One of the interfaces is not UP in the system, raising question pri  
ority  
Device "veth2c4031a@if8" does not exist.  
Snort configuration: WARNING: The interfaces configured are not valid  
update-rc.d: We have no instructions for the snort init script.  
update-rc.d: It looks like a network service, we disable it.  
Processing triggers for man-db (2.12.0-3) ...  
Processing triggers for kali-menu (2023.4.7) ...  
Processing triggers for libc-bin (2.37-12) ...  
Scanning processes...  
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.  
W: Operation was interrupted before it could finish

\*~/Desktop/documentnama - Mousepad

File Edit Search View Document Help

1 Nama : Dani Adrian  
2 NIM : 225150201111009



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS BRAWIJAYA**

---

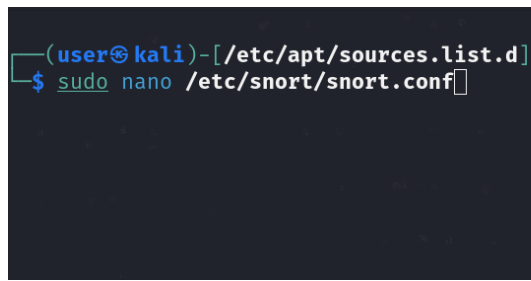
BAB : AUDIT DAN MONITORING  
NAMA : DANI ADRIAN  
NIM : 225150201111009  
TANGGAL : 28/03/2024  
ASISTEN : Bernas Cakra Sakti Harisna  
Mohammad Seto Aji Pamungkas

---

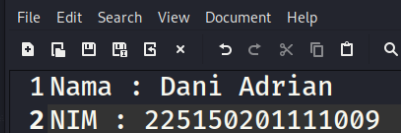
### **Praktik Penggunaan Snort**

Berikut merupakan langkah-langkah yang perlu dilakukan dalam menyelesaikan praktikum:

1. Bukalah file pada `/etc/snort/snort.conf` dengan text editor favoritmu dan perhatikan konfigurasi tersebut serta jelaskan bagian rule dan network:



```
(user@kali)-[/etc/apt/sources.list.d]  
$ sudo nano /etc/snort/snort.conf
```



```
1 Nama : Dani Adrian  
2 NIM : 225150201111009
```

Rule



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS BRAWIJAYA**

BAB : AUDIT DAN MONITORING  
NAMA : DANI ADRIAN  
NIM : 225150201111009  
TANGGAL : 28/03/2024  
ASISTEN : Bernas Cakra Sakti Harisna  
Mohammad Seto Aji Pamungkas

```
user@kali: /etc/apt/sources.list.d
File Actions Edit View Help
GNU nano 7.2 /etc/snort/snort.conf
# sure you re-enable them again:

#include $RULE_PATH/app-detect.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/bad-traffic.rules
#include $RULE_PATH/blacklist.rules
#include $RULE_PATH/botnet-cnc.rules
#include $RULE_PATH/browser-chrome.rules
#include $RULE_PATH/browser-firefox.rules
#include $RULE_PATH/browser-ie.rules
#include $RULE_PATH/browser-other.rules
#include $RULE_PATH/browser-plugins.rules
#include $RULE_PATH/browser-webkit.rules
include $RULE_PATH/chat.rules
#include $RULE_PATH/content-replace.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/experimental.rules
#include $RULE_PATH/exploit-kit.rules
include $RULE_PATH/exploit.rules
#include $RULE_PATH/file-executable.rules
#include $RULE_PATH/file-flash.rules
#include $RULE_PATH/file-identify.rules

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

1 Nama : Dani Adrian  
2 NIM : 225150201111009

Network





**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS BRAWIJAYA**

BAB : AUDIT DAN MONITORING  
NAMA : DANI ADRIAN  
NIM : 225150201111009  
TANGGAL : 28/03/2024  
ASISTEN : Bernas Cakra Sakti Harisna  
Mohammad Seto Aji Pamungkas

```
GNU nano 7.2 /etc/snort/snort.conf
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET

# List of telnet servers on your network
ipvar TELNET_SERVERS $HOME_NET

# List of ssh servers on your network
ipvar SSH_SERVERS $HOME_NET

# List of ftp servers on your network
ipvar FTP_SERVERS $HOME_NET

# List of sip servers on your network
ipvar SIP_SERVERS $HOME_NET
```

**Network:** Ini adalah bagian yang mendefinisikan konfigurasi jaringan yang terkait dengan operasi Snort. Ini mencakup informasi seperti antarmuka jaringan yang digunakan untuk mendengarkan lalu lintas jaringan, subnet yang diawasi, dan konfigurasi alamat IP serta port untuk memfilter dan memantau.

**Rule:** Ini adalah bagian yang mendefinisikan aturan deteksi yang digunakan oleh Snort. Setiap aturan terdiri dari serangkaian kondisi atau pola yang jika terpenuhi, akan menghasilkan tindakan yang telah ditentukan. Aturan ini digunakan untuk mendeteksi aktivitas jaringan yang mencurigakan atau berpotensi berbahaya. Contoh aturan bisa berupa pola-pola spesifik dalam paket jaringan, seperti string yang muncul, alamat IP sumber atau tujuan, port, dan sebagainya.

Dalam konfigurasi snort.conf, kedua bagian ini akan menentukan bagaimana Snort akan memonitor dan merespons lalu lintas jaringan yang masuk. Hal ini memungkinkan Snort untuk berfungsi sebagai sistem deteksi intrusi (IDS) atau



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS BRAWIJAYA**

BAB : AUDIT DAN MONITORING  
NAMA : DANI ADRIAN  
NIM : 225150201111009  
TANGGAL : 28/03/2024  
ASISTEN : Bernas Cakra Sakti Harisna  
Mohammad Seto Aji Pamungkas

sebagai pencegah intrusi (IPS), tergantung pada konfigurasi dan pengaturan yang telah ditentukan.

2. Kembali ke terminal dan jalankan command berikut untuk sniffing menggunakan snort:

```
sudo snort -v -d -e -i <network card yang ingin di cek>
```

Setelah itu, jalankan nmap untuk melakukan scanning pada ip address Anda

```
File Actions Edit View Help
(user@kali)-[/etc/apt/sources.list.d]
$ ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever

2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:14:67:d1 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 83456sec preferred_lft 83456sec
    inet6 fe80::a00:27ff:fe14:67d1/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

3: br-6997956cef8a: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:6e:a0:de:b8 brd ff:ff:ff:ff:ff:ff
    inet 172.19.0.1/16 brd 172.19.255.255 scope global br-6997956cef8a
        valid_lft forever preferred_lft forever
    inet6 fe80::42:6eff:fea0:deb8/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever

4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:f9:47:8a:cb brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever

5: br-8017fe66e144: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:a8:e7:5d:f3 brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.1/16 brd 172.18.255.255 scope global br-8017fe66e144
        valid_lft forever preferred_lft forever
    inet6 fe80::42:a8ff:fee7:5df3/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
```

1 Nama : Dani Adrian  
2 NIM : 225150201111009



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS BRAWIJAYA**

BAB : AUDIT DAN MONITORING  
NAMA : DANI ADRIAN  
NIM : 225150201111009  
TANGGAL : 28/03/2024  
ASISTEN : Bernas Cakra Sakti Harisna  
Mohammad Seto Aji Pamungkas

The screenshot shows two terminal windows. The left window displays the output of the command `sudo snort -v -d -e -i eth0`, showing the initialization of Snort 2.9.15.1, including loading plugins and configuring the network interface. The right window shows the output of the command `nmap 10.0.2.15`, which reports that the host is up and lists open ports: 80/tcp (http), 81/tcp (hosts2-ns), and 82/tcp (xfer). Below the terminal windows, there is a small window titled "1Nama : Dani Adrian" and "2NIM : 225150201111009".

- -v: Opsi ini mengaktifkan mode verbose atau rinci. Ini akan menampilkan lebih banyak informasi selama eksekusi, seperti aturan yang dipicu, statistik lalu lintas, dan lainnya.
- -d: Opsi ini mengaktifkan mode deteksi. Ini akan membuat Snort memproses dan mendeteksi lalu lintas jaringan yang diterima dari antarmuka yang ditentukan.
- -e: Opsi ini memaksa Snort untuk menampilkan konten data paket jaringan dalam outputnya. Ini berguna untuk melihat isi paket secara langsung, yang dapat membantu dalam analisis deteksi.
- -i <network card>: Opsi ini menentukan antarmuka jaringan yang akan digunakan oleh Snort untuk menangkap lalu lintas. Kita harus menentukan nama antarmuka jaringan (misalnya, eth0 untuk Ethernet) yang ingin gunakan untuk memantau lalu lintas.

Setelah menjalankan perintah Snort diatas, ketika menjalankan nmap untuk melakukan pemindaian pada alamat IP , Snort akan memulai pemantauan dan mendeteksi lalu lintas jaringan yang masuk sesuai dengan aturan yang dikonfigurasi



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS BRAWIJAYA**

BAB : AUDIT DAN MONITORING  
NAMA : DANI ADRIAN  
NIM : 225150201111009  
TANGGAL : 28/03/2024  
ASISTEN : Bernas Cakra Sakti Harisna  
Mohammad Seto Aji Pamungkas

Outputnya akan berisi informasi tentang paket yang ditangkap, aturan yang dipicu, dan detail-detail lainnya sesuai dengan opsi yang digunakan (termasuk mode verbose dan mode deteksi). Selain itu, karena menggunakan opsi -e, juga akan menampilkan konten data dari paket jaringan dalam outputnya.

3. Hentikan snort dan jalankan command snort dibawah ini untuk mode packet logger:

```
sudo snort -dev -l ./log -b -i <network card yang ingin dicek>
```

Setelah itu, jalankan nmap untuk melakukan scanning pada ip address

The screenshot shows a terminal window on a Kali Linux system. The user has created a 'log' directory and run 'ls' showing various files. Then, they executed 'sudo snort -dev -l ./log -b -i eth0'. The terminal output shows Snort initializing in packet logging mode. To the right, the nmap output for 10.0.2.15 is displayed, showing open ports 80, 81, and 82. In the bottom right corner, a small window titled 'Moussad' displays the user's name 'Dani Adrian' and NIM '225150201111009'.

```
(user@kali)-[~]
$ mkdir log
$ ls
Desktop  Music  Public  ki-pentesting  sqlmap-part1
Documents  OSINT-Cheat-sheet  Templates  ki-xss  sqlmap-part2
Downloads  Pictures  Videos  log
(user@kali)-[~]
$ sudo snort -dev -l ./log -b -i eth0
[sudo] password for user:
Running in packet logging mode

--== Initializing Snort ==--
Initializing Output Plugins!
Log directory = ./log
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Decoding Ethernet

--== Initialization Complete ==--

--> Snort! <-
o''-~ Version 2.9.15.1 GRE (Build 15125)
.... By Martin Roesch & The Snort Team: http://www.snort.org/cont
act#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rig
hts reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.

(user@kali)-[~]
$ nmap 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 04:58 WIB
Nmap scan report for 10.0.2.15
Host is up (0.000037s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
81/tcp    open  hosts2-ns
82/tcp    open  xfer
Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
(user@kali)-[~]
$
```



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS BRAWIJAYA**

BAB : AUDIT DAN MONITORING  
NAMA : DANI ADRIAN  
NIM : 225150201111009  
TANGGAL : 28/03/2024  
ASISTEN : Bernas Cakra Sakti Harisna  
Mohammad Seto Aji Pamungkas

```
File Actions Edit View Help
(user@kali)-[~]
$ sudo snort -dev -l ./log -b -i eth0
Running in packet logging mode

--== Initializing Snort ==--
Initializing Output Plugins!
Log directory = ./log
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Decoding Ethernet

--== Initialization Complete ==--

--> Snort! <--
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.4 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.3

Commencing packet processing (pid=607132)
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.

File Actions Edit View Help
(user@kali)-[~]
$ nmap 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 04:58 WIB
Nmap scan report for 10.0.2.15
Host is up (0.000037s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
81/tcp    open  hosts2-ns
82/tcp    open  xfer

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds

File Actions Edit View Help
-DesktopDocumentName - Moussapad
File Edit Search View Document Help
1 Nama : Dani Adrian
2 NIM : 225150201111009
3

File Actions Edit View Help
(user@kali)-[~]
$ sudo snort -dev -l ./log -b -i eth0
Running in packet logging mode

--== Initializing Snort ==--
Initializing Output Plugins!
Log directory = ./log
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Decoding Ethernet

--== Initialization Complete ==--

--> Snort! <--
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.4 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.3

Commencing packet processing (pid=687808)
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.

File Actions Edit View Help
(user@kali)-[~/log]
$ cat snort.log.1712188245

f9g*! CCRT'gE5*?o?
@d*d*5!0C'g*RT5*?@*y*+d
fXQ!*:+++backendq*
**RT'g*

f*Q
'g*
'g*
'g*
f*CCRT'gE5*?75D
f*~C'g*RT5*?@*x*+e+d
f*~h**RT'g*backend*

f*~i<'g*RR75
'g*
f/*CCRT'gE5*?7y*
fs*~g*RT5*?@*x*+e+d
5*~l*++++backend*>@a

root-serversnetstld
verisign-grscomx*g* :*Q***

f*~<'g*RR75
'g*
f*~5CCRT'gE5*?7*
f*~C'g*RT5*?@*x*+e+d
f*~**RT'g*ackend*

File Actions Edit View Help
-DesktopDocumentName - Moussapad
File Edit Search View Document Help
1 Nama : Dani Adrian
2 NIM : 225150201111009
3
```

4. Jalankan command berikut untuk menjalankan snort dengan IDS mode:

```
ubuntu@ubuntu-VirtualBox:~$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i enp0s8
10/16-17:24:17.903023 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68
-> 255.255.255.255:67
10/16-17:25:15.460358 [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168
.56.1:35196 -> 192.168.56.10:705
10/16-17:25:15.463030 [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.56.1:4
7476 -> 192.168.56.10:161
```





**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS BRAWIJAYA**

BAB : AUDIT DAN MONITORING  
NAMA : DANI ADRIAN  
NIM : 225150201111009  
TANGGAL : 28/03/2024  
ASISTEN : Bernas Cakra Sakti Harisna  
Mohammad Seto Aji Pamungkas

```
sudo snort -A console -q -u snort -g snort -c  
/etc/snort/snort.conf -i <network yang ingin dicek>
```

Setelah itu, jalankan nmap untuk melakukan scanning pada ip address Anda

The image shows two screenshots. The left screenshot is a terminal window with the command `sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf` and its output, which includes several log entries for ICMP PING, SNMP request, and attempted information leaks. The right screenshot shows a terminal window with the command `sudo nmap -sS 192.168.1.1` and its output, which indicates that the host is up and shows open ports 21/tcp (ftp) and 1723/tcp (pptp).

-A console: Menetapkan output log ke konsol, sehingga pesan log dan peringatan ditampilkan langsung di terminal tempat Anda menjalankan Snort.

-q: Mode diam atau quiet. Ini mengurangi output yang dihasilkan oleh Snort, sehingga hanya pesan penting yang ditampilkan.

-u snort: Menetapkan pengguna yang akan dijalankan oleh Snort. Di sini, Snort akan dijalankan sebagai pengguna "snort".

-g snort: Menetapkan grup yang akan dijalankan oleh Snort. Dalam hal ini, Snort akan dijalankan dalam grup "snort".

-c /etc/snort/snort.conf: Menetapkan lokasi dan nama file konfigurasi Snort yang akan digunakan oleh Snort. Dalam kasus ini, konfigurasi Snort ditempatkan di /etc/snort/snort.conf.





**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS BRAWIJAYA**

---

BAB : AUDIT DAN MONITORING  
NAMA : DANI ADRIAN  
NIM : 225150201111009  
TANGGAL : 28/03/2024  
ASISTEN : Bernas Cakra Sakti Harisna  
Mohammad Seto Aji Pamungkas

---

-i <network yang ingin dicek>: Menetapkan antarmuka jaringan yang akan digunakan oleh Snort untuk mendengarkan lalu lintas jaringan. Anda harus menentukan nama antarmuka jaringan yang ingin Anda gunakan untuk memantau lalu lintas.

Sementara itu, perintah `sudo nmap -sS <ip>` menggunakan Nmap dengan opsi `-sS` untuk melakukan TCP SYN scan terhadap alamat IP yang ditentukan. Munculnya pesan "Attempted Information Leak" bisa disebabkan oleh hasil Nmap yang dianggap sebagai upaya untuk mencoba mendapatkan informasi rahasia atau sensitif. Dalam konteks keamanan, beberapa alat pemindaian seperti Nmap bisa dianggap sebagai alat potensial untuk mencoba mencari lubang keamanan atau mengumpulkan informasi tentang jaringan target.

### **Kesimpulan**

Pada bagian ini, tuliskan kesimpulan apa saja yang didapat dari hasil melaksanakan kegiatan-kegiatan pada bab ini.

File `snort.conf` digunakan untuk menentukan konfigurasi Snort seperti bagian "network" dan bagian "rule".

Bagian "network" mendefinisikan konfigurasi jaringan yang terkait dengan operasi Snort. Ini mencakup informasi seperti antarmuka jaringan yang digunakan untuk mendengarkan lalu lintas jaringan, subnet yang diawasi, dan konfigurasi alamat IP serta port untuk memfilter dan memantau.

Sementara itu, bagian "rule" mendefinisikan aturan deteksi yang digunakan oleh Snort. Setiap aturan terdiri dari serangkaian kondisi atau pola yang, jika terpenuhi, akan menghasilkan tindakan yang telah ditentukan. Aturan ini digunakan untuk mendeteksi aktivitas jaringan yang mencurigakan atau berpotensi berbahaya.

Kedua bagian ini menentukan bagaimana Snort akan memonitor dan merespons lalu lintas jaringan yang masuk. Ini memungkinkan Snort untuk berfungsi sebagai sistem



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS BRAWIJAYA**

---

BAB : AUDIT DAN MONITORING  
NAMA : DANI ADRIAN  
NIM : 225150201111009  
TANGGAL : 28/03/2024  
ASISTEN : Bernas Cakra Sakti Harisna  
Mohammad Seto Aji Pamungkas

---

deteksi intrusi (IDS) atau sebagai pencegah intrusi (IPS), tergantung pada konfigurasi dan pengaturan yang telah ditentukan.

Ketika menjalankan perintah Snort dengan opsi -v -d -e -i, Snort akan memulai pemantauan dan mendeteksi lalu lintas jaringan sesuai dengan aturan yang dikonfigurasi. Outputnya akan menampilkan informasi tentang paket yang ditangkap, aturan yang dipicu, dan konten data paket jaringan. Ketika nmap dijalankan untuk melakukan pemindaian pada alamat IP, Snort akan bereaksi sesuai dengan aturan yang telah ditetapkan, dan pesan log dan peringatan akan ditampilkan di terminal.

Selain itu, perintah Snort dengan opsi -A console -q -u snort -g snort -c /etc/snort/snort.conf -i <network> mengaktifkan mode IDS Snort dengan mengkonfigurasi output log ke konsol. Hal ini memungkinkan pesan log dan peringatan ditampilkan langsung di terminal. Opsi lainnya seperti mode diam (-q), pengguna (-u), grup (-g), lokasi file konfigurasi (-c), dan antarmuka jaringan (-i) juga ditetapkan. Ketika nmap dijalankan untuk melakukan pemindaian pada alamat IP, Snort akan memonitor dan mendeteksi lalu lintas jaringan sesuai dengan aturan yang dikonfigurasi, dan pesan log dan peringatan akan ditampilkan sesuai dengan opsi yang telah ditetapkan.

### **Evaluasi**

1. Apa perbedaan dan batasan-batasan antara IDS, IPS, dan Firewall?

Perbedaan dan batasan antara IDS, IPS, dan Firewall adalah sebagai berikut:

Firewall:

- Perbedaan: Bertindak sebagai penghalang antara jaringan internal dan eksternal, melakukan filtering terhadap lalu lintas berdasarkan aturan yang ditetapkan.



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS BRAWIJAYA**

---

BAB : AUDIT DAN MONITORING  
NAMA : DANI ADRIAN  
NIM : 225150201111009  
TANGGAL : 28/03/2024  
ASISTEN : Bernas Cakra Sakti Harisna  
Mohammad Seto Aji Pamungkas

---

- Batasan: Cenderung bersifat statis dan terbatas dalam mendeteksi serangan yang kompleks atau intrusi yang terjadi di dalam jaringan.

IDS (Intrusion Detection System):

- Perbedaan: Digunakan untuk mendeteksi dan memberi peringatan tentang aktivitas jaringan yang mencurigakan atau berpotensi berbahaya.
- Batasan: Hanya memberikan peringatan tentang serangan yang terdeteksi, tetapi tidak mengambil tindakan langsung untuk mencegahnya.

IPS (Intrusion Prevention System):

- Perbedaan: Memperluas fungsionalitas IDS dengan tidak hanya mendeteksi serangan, tetapi juga mengambil tindakan preventif untuk mencegah serangan mencapai target.
- Batasan: Implementasi yang tidak hati-hati dapat menyebabkan false positive atau false negative yang dapat mengganggu kinerja jaringan atau melewatkan serangan yang sebenarnya.

2. Buatlah konfigurasi Snort IPS menggunakan DAQ AFPacket. Salah satu contoh konfigurasi snort IPS bisa dilihat di dokumentasi resmi berikut:

<https://snort.org/documents/snort-ips-using-daq-afpacket>

Ubah config Snort:

```
## Under Step #2: add the following line config  
policy_mode:inline
```



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS BRAWIJAYA**

BAB : AUDIT DAN MONITORING  
NAMA : DANI ADRIAN  
NIM : 225150201111009  
TANGGAL : 28/03/2024  
ASISTEN : Bernas Cakra Sakti Harisna  
Mohammad Seto Aji Pamungkas

```
## Configure DAQ variables for AFPacket config daq: config
daq: afpacket config

daq_mode: inline

config daq_var: buffer_size_mb=1024
```

```
GNU nano 7.2 /etc/snort/snort.conf
# Configure maximum number of flowbit references. For more information
# config flowbits_size: 64

# Configure ports to ignore
# config ignore_ports: tcp 21 6667:6671 1356
# config ignore_ports: udp 1:17 53

# Configure active response for non inline operation. For more information
# config response: eth0 attempts 2

# Configure DAQ related options for inline operation. For more information
#
config daq: afpacket
config daq_mode: inline
config daq_var: buffer_size_mb=1024

# config daq: <type>
# config daq_dir: <dir>
# config daq_mode: <mode>
# config daq_var: <var>

# <type> ::= pcap | afpacket | dump | nfq | ipq | ipfw
# <mode> ::= read-file | passive | inline
# <var> ::= arbitrary <name>=<value passed to DAQ
# <dir> ::= path as to where to look for DAQ module so's

# Configure specific UID and GID to run snort as after dropping privs

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute
^X Exit      ^R Read File ^N Replace   ^U Paste     ^J Justify
```

```
user@kali: ~
$ snort --daq-list
Available DAQ modules:
pcap(v3): readback live multi unpriv
nfq(v7): live inline multi
ipfw(v3): live inline multi unpriv
dump(v3): readback live inline multi unpriv
afpacket(v5): live inline multi unpriv

(user@kali)-[~]
$
```

```
-/Desktop/documentname - Mousepad
File Edit Search View Document Help
1 Nama : Dani Adrian
2 NIM : 225150201111009
3
```

