```
#! /usr/bin/env python
>./start.py
              >Johan Wahyudi
              >09011281320031
```

THREAT PACKET ANALYSIS USING SNORT

1. Introduction

Dalam sebuah jaringan komputer, keamanan menjadi salah satu bagian yang terpenting dan harus di perhatikan untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi para pengguna. Sistem harus di lindungi dari segala macam serangan dan ancaman oleh pihak pihak yang tidak bertanggung jawab.

Implementasi *Intrusion Detection System* (IDS) adalah salah satu upaya untuk mengindentifikasi adanya serangan maupun ancaman dari pihak yang tidak bertanggung jawab, misalnya penyusup yang tidak mempunyai otoritas (*cracker*) ataupun seorang user yang sah tetapi menyalahgunakan *privilege* sumber daya sistem.

IDS akan melakukan pemberitahuan saat mendeteksi sesuatu yang dianggap mencurigakan atau tindakan ilegal. IDS tidak melakukan pencegahan terjadinya penyusupan. Selain analisa secara realtime, IDS bisa juga melakukan analisa terhadap data hasil *capture* sebuah jaringan untuk di analisa apakah telah terjadi serangan atau tidak.

2. Scope of Problem

- *Intrusion Detection System* (IDS) yang di gunakan pada percobaan ini adalah *Snort* versi 2.9.6.0 GRE (Build 47)
- alamat IP sistem yang di uji 103.241.4.11 (http://unsri.ac.id), hanya untuk pembelajaran, di luar itu menyalahi aturan dan akan di proses sesuai undang-undang yang berlaku.
- IDS *Snort* di gunakan untuk deteksi serangan tidak secara realtime, melainkan dari sebuah file pcap hasil *Capture Malicious Traffic.*
- hanya melakukan aktivitas scanning port yang terbuka dan service remote yang aktif pada sistem.

3. Network Scanning.

Network Scanning adalah sebuah teknik yang digunakan untuk melakukan scanning pada sebuah jaringan. Teknik ini digunakan untuk mendapatkan data seperti IP, Port, File data yang keluar masuk melalui jaringan serta merekam aktivitas internet browsing.

4. What is Intrusion Detection ?

Dikutip dari Wikipedia [1] *Intrusion Detection System* (disingkat IDS) adalah sebuah metode yang dapat digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas *inbound* dan *outbound* dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan).

A. *Network Based* (Network IDS)

Semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. NIDS umumnya terletak di dalam segmen jaringan penting di mana server berada atau terdapat pada "pintu masuk" jaringan. Kelemahan NIDS adalah bahwa NIDS agak rumit diimplementasikan dalam sebuah jaringan yang menggunakan switch Ethernet, meskipun beberapa vendor switch Ethernet sekarang telah mendukung penerapan fungsi IDS di dalam switch buatannya untuk memonitor port atau koneksi.

B. *Host Based* (HIDS)

Aktivitas sebuah host jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak. HIDS seringnya diletakkan pada server-server kritis di jaringan, seperti halnya firewall, web server, atau server yang terkoneksi ke Internet.

C. Implementasi dan cara kerja

Ada beberapa cara bagaimana IDS bekerja. Cara yang paling populer adalah dengan menggunakan pendeteksian berbasis *signature* (seperti halnya yang dilakukan oleh beberapa antivirus), yang melibatkan pencocokan lalu lintas jaringan dengan basis data yang berisi cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Sama seperti halnya antivirus, jenis ini membutuhkan pembaruan terhadap basis data *signature IDS* yang bersangkutan.

Metode selanjutnya adalah dengan mendeteksi adanya anomali, yang disebut sebagai *Anomaly-based IDS*. Jenis ini melibatkan pola lalu lintas yang mungkin merupakan sebuah serangan yang sedang dilakukan oleh penyerang. Umumnya, dilakukan dengan menggunakan teknik statistik untuk membandingkan lalu lintas yang sedang dipantau dengan lalu lintas normal yang biasa terjadi. Metode ini menawarkan kelebihan dibandingkan *signature-based IDS*, yakni ia dapat mendeteksi bentuk serangan yang baru dan belum terdapat di dalam basis data *signature IDS*. Kelemahannya, adalah jenis ini sering mengeluarkan pesan *false positive*. Sehingga tugas administrator menjadi lebih rumit, dengan harus memilah-milah mana yang merupakan serangan yang sebenarnya dari banyaknya laporan *false positive* yang muncul.

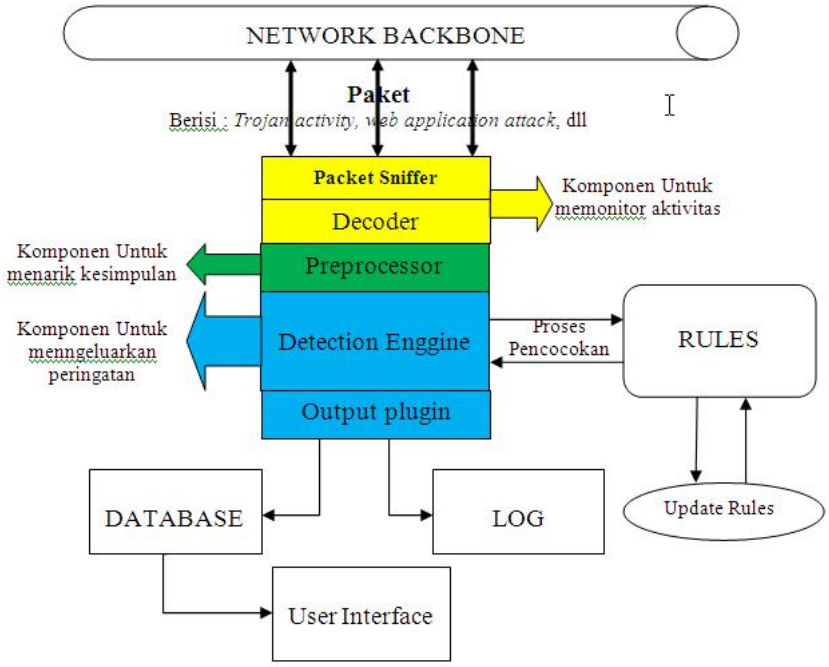
5. Snort

Snort adalah NIDS yang bekerja dengan menggunakan *signature detection,* berfungsi juga sebagai sniffer dan packet logger [2]. Snort pertama kali di buat dan dikembangkan oleh Marti Roesh, lalu menjadi sebuah opensource project.

Tiga (3) buah mode mengoperasikan snort, yaitu :
1. Sniffer mode, untuk melihat paket yang lewat di jaringan.
2. Packet logger mode, untuk mencatat semua paket yang lewat di jaringan untuk di analisa di kemudian hari.
3. Intrusion Detection mode, pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer. Untuk menggunakan mode IDS ini diperlukan setup dari berbagai rules / aturan yang akan membedakan sebuah paket normal dengan paket yang membawa serangan.

a) Cara Kerja Snort

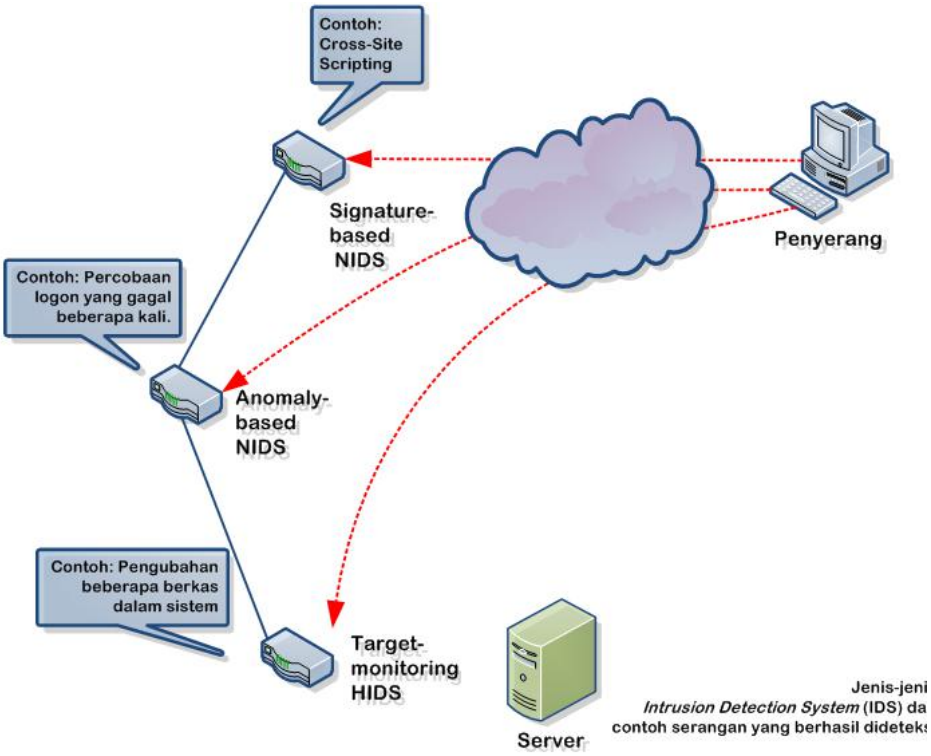
Ada beberapa cara bagaimana IDS bekerja. Cara yang paling populer adalah dengan menggunakan pendeteksian berbasis signature (seperti halnya yang dilakukan oleh beberapa antivirus), yang melibatkan pencocokan lalu lintas jaringan dengan basis data yang berisi cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Sama seperti halnya antivirus, jenis ini membutuhkan pembaruan terhadap basis data signature IDS yang bersangkutan.



(*gambar : cara kerja snort)*

```
#! /usr/bin/env python
>./start.py
              >Johan Wahyudi
              >09011281320031
```

Metode selanjutnya adalah dengan mendeteksi adanya anomali, yang disebut sebagai Anomaly-based IDS, Teknik lainnya yang digunakan adalah dengan memantau berkas-berkas sistem operasi, yakni dengan cara melihat apakah ada percobaan untuk mengubah beberapa berkas sistem operasi, utamanya berkas log. Teknik ini seringnya diimplementasikan di dalam HIDS, selain tentunya melakukan pemindaian terhadap log sistem untuk memantau apakah terjadi kejadian yang tidak biasa.



(gambar : Implementasi dan cara kerja)

6. Scan Port and Service Remote Attack.

Port Scaning adalah aktivitas yang dilakukan untuk memeriksa status port TCP dan UDP pada sebuah sistem, ada beberapa option yang di gunakan pada saat melakukan scanning, diantaranya :

Command & Option	Keterangan
Nmap -sV <ip address>	Deteksi *remote service*
Nmap -O <ip address>	Deteksi *remote Opeting sistem*
Nmap -PA <ip address>	*Scan using TCP ACK*
Nmap -PS <ip address>	*Scan using TCP Syn*
Nmap -PO <ip address>	*Scan using IP Protocol ping*
Nmap -PU <ip address>	*Scan using UDP ping*
Nmap -sU <ip address>	*Scan using UDP services*

```
#! /usr/bin/env python
>./start.py
              >Johan Wahyudi
              >09011281320031
```

7. Spoofing TCP/IP stack OS Fingerprinting attack.

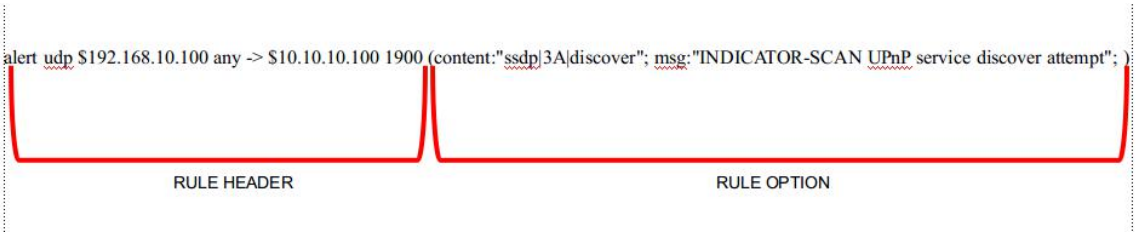
OS Fingerprint adalah aktifitas yang di lakukan untuk mengetahui sistem operasi yang di gunakan oleh server target, pada percobaan disini menggunakan *tools nmap dan xprobe2* di linux.

Command and Options	Keterangan
Nmap -O <ip address>	Deteksi *remote Opeting sistem*
Xprobe2 <ip address>	Deteksi *remote Opeting sistem*

8. Structure Rules Snort

Untuk bisa mendektesi sebuah serangan dan *malicious traffic,* snort membutuhkan rules yang mempunyai format penulisan, di bawah ini contoh rules basic untuk deteksi aktifitas *scanning port* di jaringan

Struktur rule untuk deteksi *aktifitas scanning port*



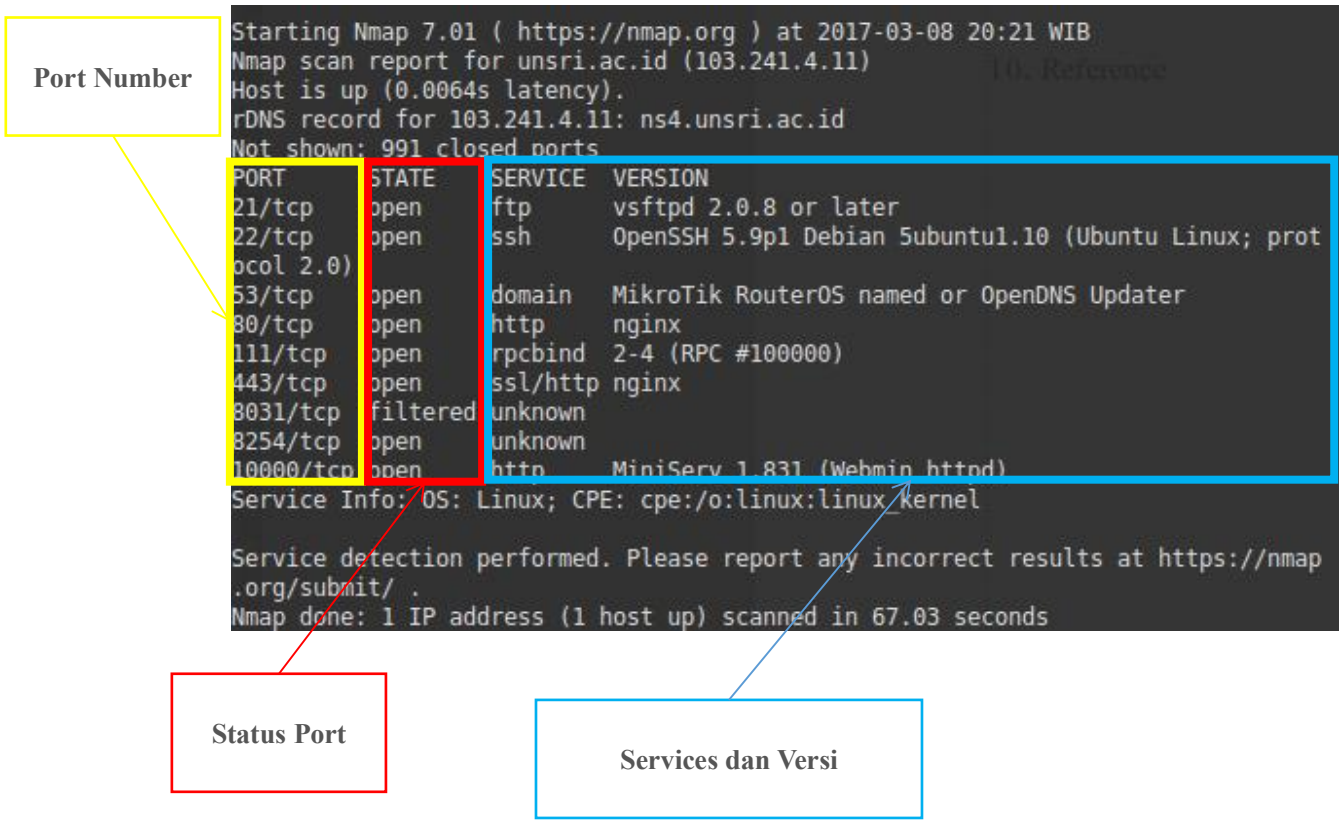
Penjelasan format :

Rules Header	Rules Option
Alert (Rule Action)	content:"ssdp|3A|discover" (Keyword)
Udp (Protocol)	msg:"INDICATOR-SCAN UPnP service discover attempt"; (Message Alert)
$192.168.10.100 (Source Address)	
Any (Source Port)	
-> (Drection)	
$10.10.10.100 (Destination Address)	
1900 (Destination Port)	

```
#! /usr/bin/env python
>./start.py
              >Johan Wahyudi
              >09011281320031
```

9. Assessment Results

a) Hasil Scan menggunakan tools nmap option -sV

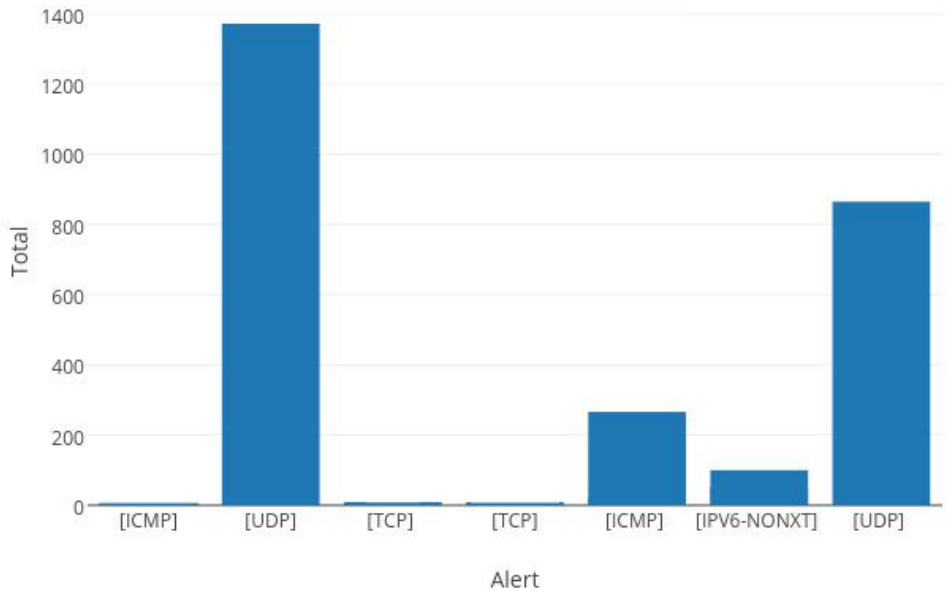


b) Data *alert attack* dari snort

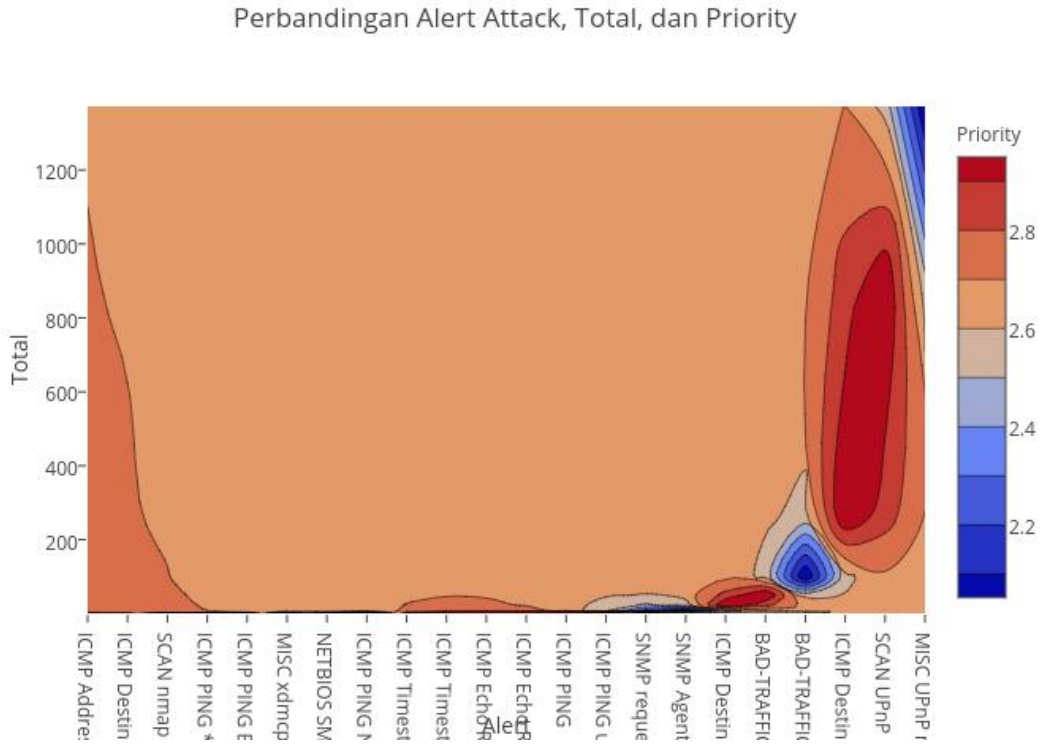
	Total	Priority	Alert	Classification Attack	Protocol
0	1	3	ICMP Address Mask Request	Misc activity	[ICMP
1	1	3	ICMP Destination Unreachable Protocol Unreachable	Misc activity	[ICMP
2	1	2	SCAN nmap XMAS	Misc activity	[ICMP
3	2	3	ICMP PING *NIX	Misc activity	[ICMP
4	2	3	ICMP PING BSDtype	Misc activity	[ICMP
5	2	2	MISC xdmcp info query	Attempted Information Leak	[UDP
6	2	3	NETBIOS SMB IPC$ unicode share access	Generic Protocol Command Decode	[TCP
7	3	2	ICMP PING NMAP	Misc activity	[ICMP
8	3	3	ICMP Timestamp Reply	Misc activity	[ICMP
9	3	3	ICMP Timestamp Request	Misc activity	[ICMP
10	5	3	ICMP Echo Reply	Misc activity	[ICMP
11	5	3	ICMP Echo Reply undefined code	Misc activity	[ICMP
12	5	3	ICMP PING	Misc activity	[ICMP
13	5	3	ICMP PING undefined code	Misc activity	[ICMP
14	7	2	SNMP request tcp	Attempted Information Leak	[TCP
15	8	2	SNMP AgentX/tcp request	Attempted Information Leak	[TCP
16	23	3	ICMP Destination Unreachable Host Unreachable	Misc activity	[ICMP
17	50	3	BAD-TRAFFIC 0 ttl	Misc activity	[IPV6-NONXT
18	100	2	BAD-TRAFFIC same SRC/DST	Potentially Bad Traffic	[IPV6-NONXT
19	266	3	ICMP Destination Unreachable Port Unreachable	Misc activity	[ICMP
20	865	3	SCAN UPnP service discover attempt	Detection of a Network Scan	[UDP
21	1372	2	MISC UPnP malformed advertisement	Misc activity	[UDP

```
#! /usr/bin/env python
>./start.py
            >Johan Wahyudi
            >09011281320031
```

c) Grafik perbandingan antara Protokol yang di gunakan dan Total Serangan

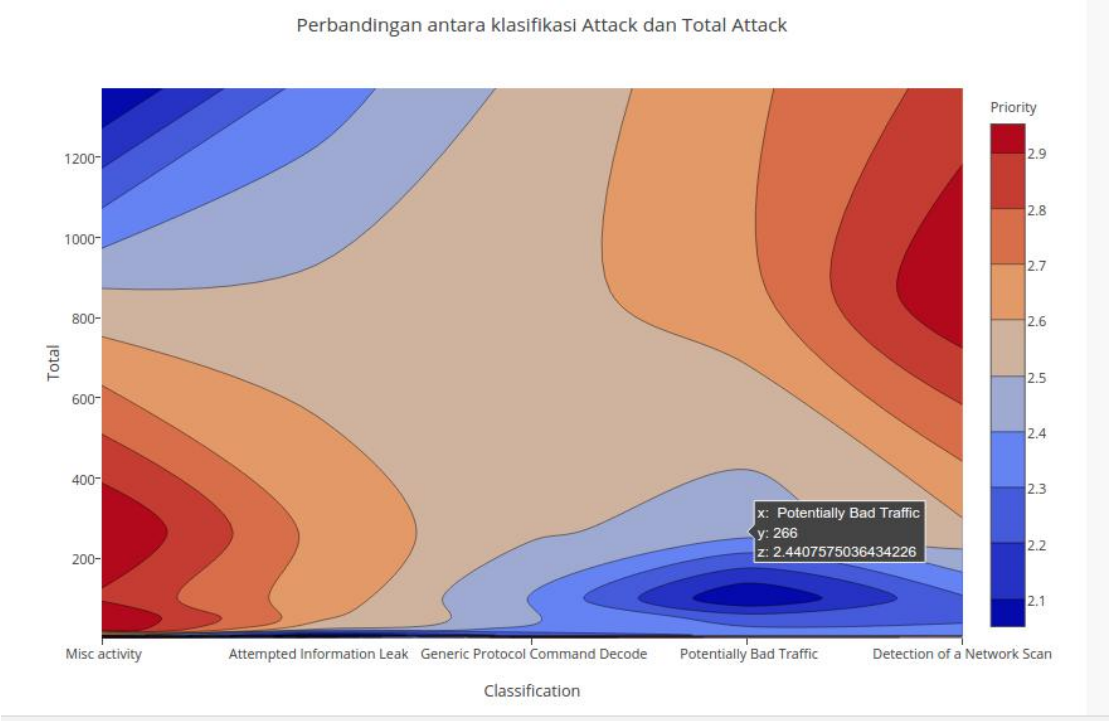


d) Grafik perbandingan antara Alert Attack, Total Serangan dan Tingkat Prioritas Serangan.



```
#! /usr/bin/env python
>./start.py
              >Johan Wahyudi
              >09011281320031
```

e) Grafik perbandingan antara Klasifikasi Attack dan Total Attack



10. Reference

[1]"Intrusion detection system", En.wikipedia.org, 2017. [Online]. Available: https://en.wikipedia.org/wiki/Intrusion_detection_system. [Accessed: 04- Mar- 2017].

[2] T. Cook, G. Conti, and D. Raymond, "*When Good Ninjas Turn bad: Preventing Your Students from becoming the Threat,"Proc. 16th Colloquium for Information System Security Education, 2012, pp. 61-67.*

[3] CommView tool, *http://www.tamos.com/*