TUGAS

KEAMANAN JARINNGAN KOMPUTER

“INTRUSION DETECTION SYSTEM USING SNORT”

DISUSUN OLEH :

MEILINDA EKA SURYANI (09011181320033)

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

INTRUSION DETECTION SYSTEM USING SNORT

Intrusion Detetion System (IDS) adalah suatu perangkat (hardware/software) yang dapat mendeteksi aktivitas yang mencurigakan (tidak normal) yang terjadi pada jaringan komputer, melakukan inspeksi terhadap lalu lintas jaringan (in/out), melakukan analisis dan mencari bukti atas terjadinya penyusupan.

Fungsi IDS:

- Pemantauan pengguna dan aktivitas sistem.
- Audit konfigurasi sistem untuk mengecek kerentanan konfigurasi dan mengecek kesalahan konfigurasi.
- Menilai integritas sistem kritis dan data files.
- Menyadari pola serangan yang dikenal dalam aktivitas sistem.
- Mengidentifikasi aktivitas abnormal melalui analisis statistik.
- Mengelola audit dan menyoroti pengguna yang melanggar kebijakan atau aktivitas normal.
- Mengoreksi kesalahan pada konfigurasi sistem.
- Instalasi dan operasi perangkap untuk merekam informasi tentang penyusup.

Keterbatasan IDS

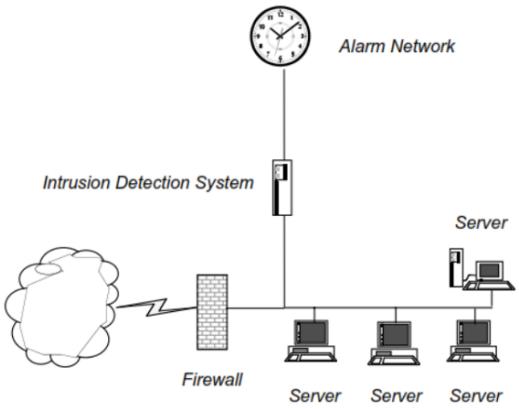
Secara umum, IDS adalah tambahan yang sangat baik untuk keamanan jaringan. Bisa melakukan pendeteksian terhadap lalulintas jaringan yang tidak seharusnya terjadi (abnormal), memberikan informasi tentang penyusupan yang terjadi, tetapi IDS tidak bisa melakukan blocking atau melakukan protect terhadap serangan ataupun adanya lalulintas yang bisa merusak jaringan atau host.

Dalam hal ini, saya menggunakan shopee.co.id dengan IP 103.223.1.38 sebagai target.

Tools yang digunakan:

- NMAP (Windows)
- WIRESHARK (Windows)

- SNORT (Linux)
- MS. EXCEL (Windows)



Gambar 1. Topology IDS

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

1. Berukuran kecil – *Source code* dan *rules* untuk rilis 2.1.1 hanya 2256k.
2. *Portable* untuk banyak OS – Telah diporting ke Linux, Windows, OSX, Solaris, BSD,dll.
3. Cepat – Snort mampu mendeteksi serangan pada network 100Mbps.
4. Free – Kita tidak perlu membayar sepeser pun untuk menggunakan snort. Snort bersifat open source dan menggunakan lisensi gpl
5. Mudah dikonfigurasi – Snort sangat mudah dikonfigurasi sesuai dengan kebutuhan network kita. Bahkan kita juga dapat membuat *rule* sendiri untuk mendeteksi adanya serangan baru.

Snort merupakan *packet sniffing* yang sangat ringan. *Snifing interface* yang digunakan berbasis libpcap (pada Unix tersedia dengan tcpdump, www.tcpdump.org). Pembuat snort sangat fokus pada *engine* yang digunakan untuk mendeteksi serangan dan memanfaatkan tools tcpdump untuk mengambil paket network. Salah satu keunggulan snort adalah bahwa snort memiliki *plugin* sistem yang sangat fleksibel untuk dimodifikasi.

Snort memiliki beberapa komponen yang tiap komponennya mempunyai tugas masing-masing. Pada saat ada paket network yang melewati Ethernet di tempat snort dipasang, maka ada beberapa hal yang dilalui:

- *Packet capture library (libpcap).*

Packet capture library – akan memisahkan paket data yang melalui ethernet card untuk selanjutnya digunakan oleh snort.

- *Packet decoder*.

Packet decoder – mengambil data di layer 2 yang dikirim dari *packet capture library*(proses 1). Pertama ia akan memisahkan Data link (seperti ethernet, TokenRing, 802.11) kemudian protokol IP, dan selanjutnya paket TCP dan UDP. Setelah pemisahan data selesai, snort telah mempunyai informasi protokol yang dapat diproses lebih lanjut.

- *Preprocessor*.

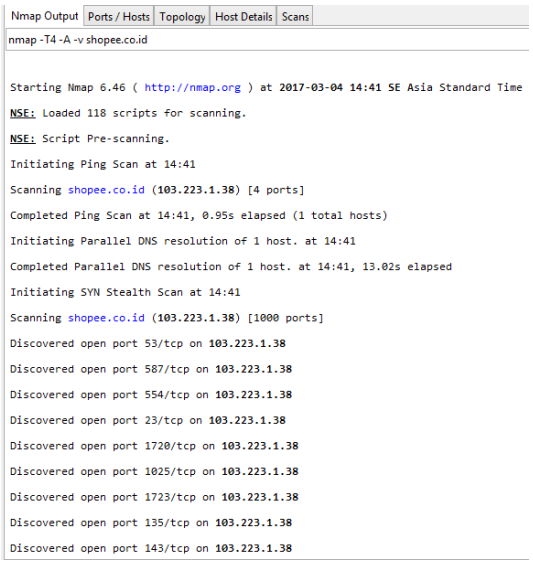
Selanjutnya dilakukan analisis (*preprocessor*) atau manipulasi terhadap paket sebelum dikirim ke *detection engine*. Manipulasi paket dapat berupa ditandai, dikelompokan atau malah dihentikan.

- *Detection Engine*.

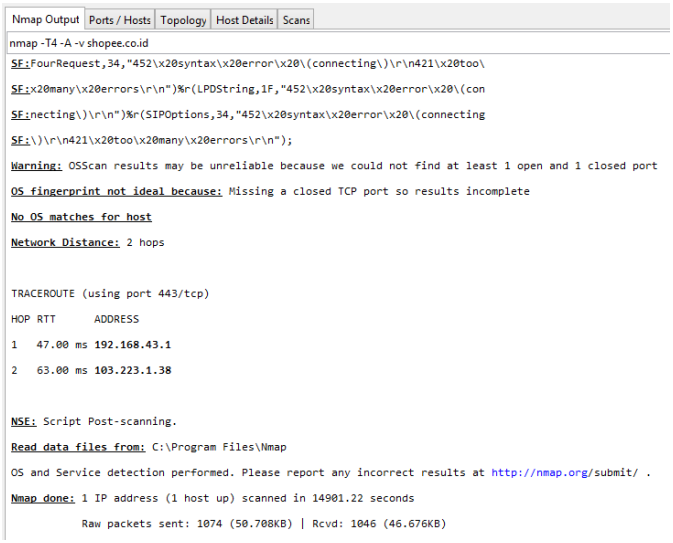
Inilah jantung dari snort. Paket yang datang dari *packet decoder* akan ditest dan dibandingkan dengan *rule* yang telah ditetapkan sebelumnya. *Rule* berisi tanda-tanda (*signature*) yang termasuk serangan.

- *Output*.

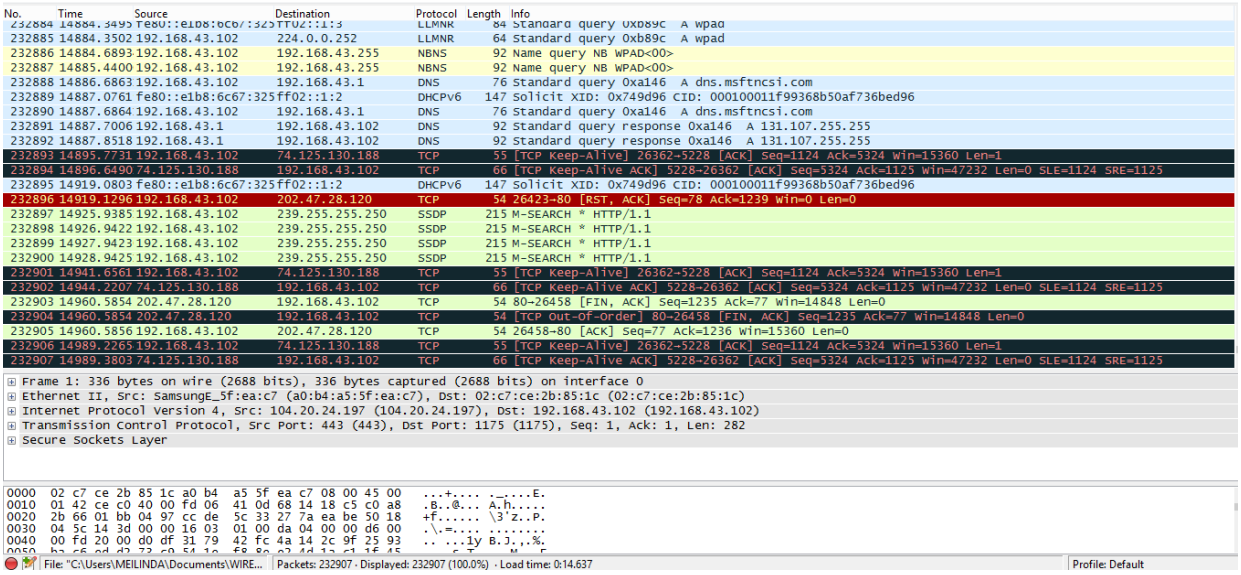
Output yang dihasilkan berupa report dan alert. Ada banyak variasi output yang dihasilkan snort, seperti teks (ASCII), XML, syslog, tcpdump, binary format, atau Database (MySQL, MsSQL, PostgreSQL, dan sebagainya).



Gambar 2. Proses scanning target pada NMAP



Gambar 3. Proses scanning target pada NMAP selesai

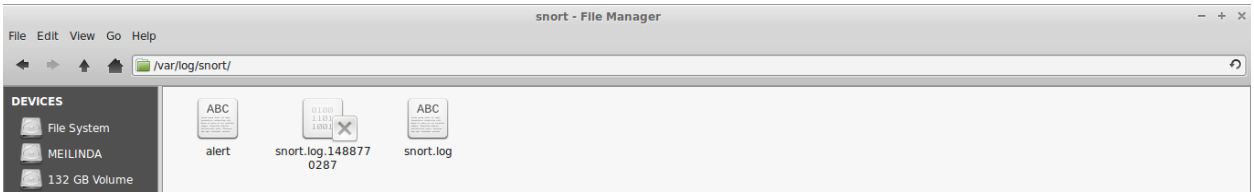


Gambar 4. Paket yang tertangkap oleh Wireshark

Setelah dilakukan peng-capture-an paket menggunakan Wireshark selama proses scan, hasil capture tersebut diolah menggunakan Snort untuk mengetahui alert yang didapat dari hasil scan ke target. Sebelumnya install terlebih dahulu tool Snort menggunakan perintah apt-get install snort. Selanjutnya jalankan Snort dengan perintah

snort –A fast –c /etc/snort/snort.conf –r /home/linda/Documents/WIRESHARK\SHOPEE.pcapng –l /var/log/snort

Dimana /home/linda/Documents/WIRESHARK\SHOPEE.pcapng adalah letak file hasil capture menggunakan Wireshark, dan /var/log/snort adalah lokasi untuk menyimpan file alert dari snort. Dalam direktori tersebut akan terdapat 3 buah file, dalam hal ini saya menggunakan file alert untuk mengetahui jenis alert dan jumlahnya.



Gambar 5. File dalam folder /var/log/snort

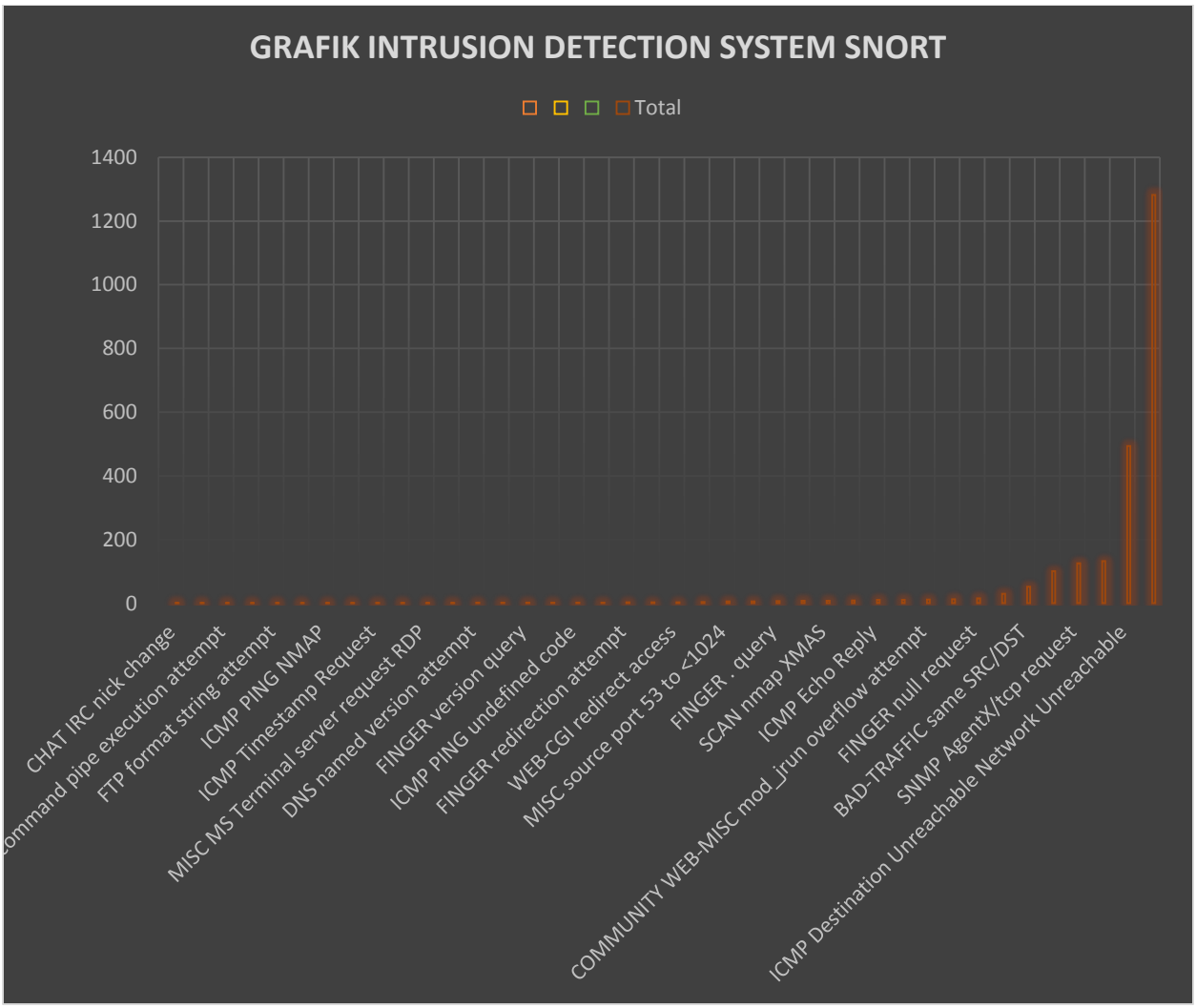
Dalam file alert, terdapat 40 jenis alert dengan total 2362 alert. 2362 alert tersebut dikelompokkan berdasarkan jenisnya sepertii pada table di bawah ini untuk mengetahui alert yang paling sedikit dam paling banyak, juga untuk mempermudah pembuatan grafik.

Tabel Alert

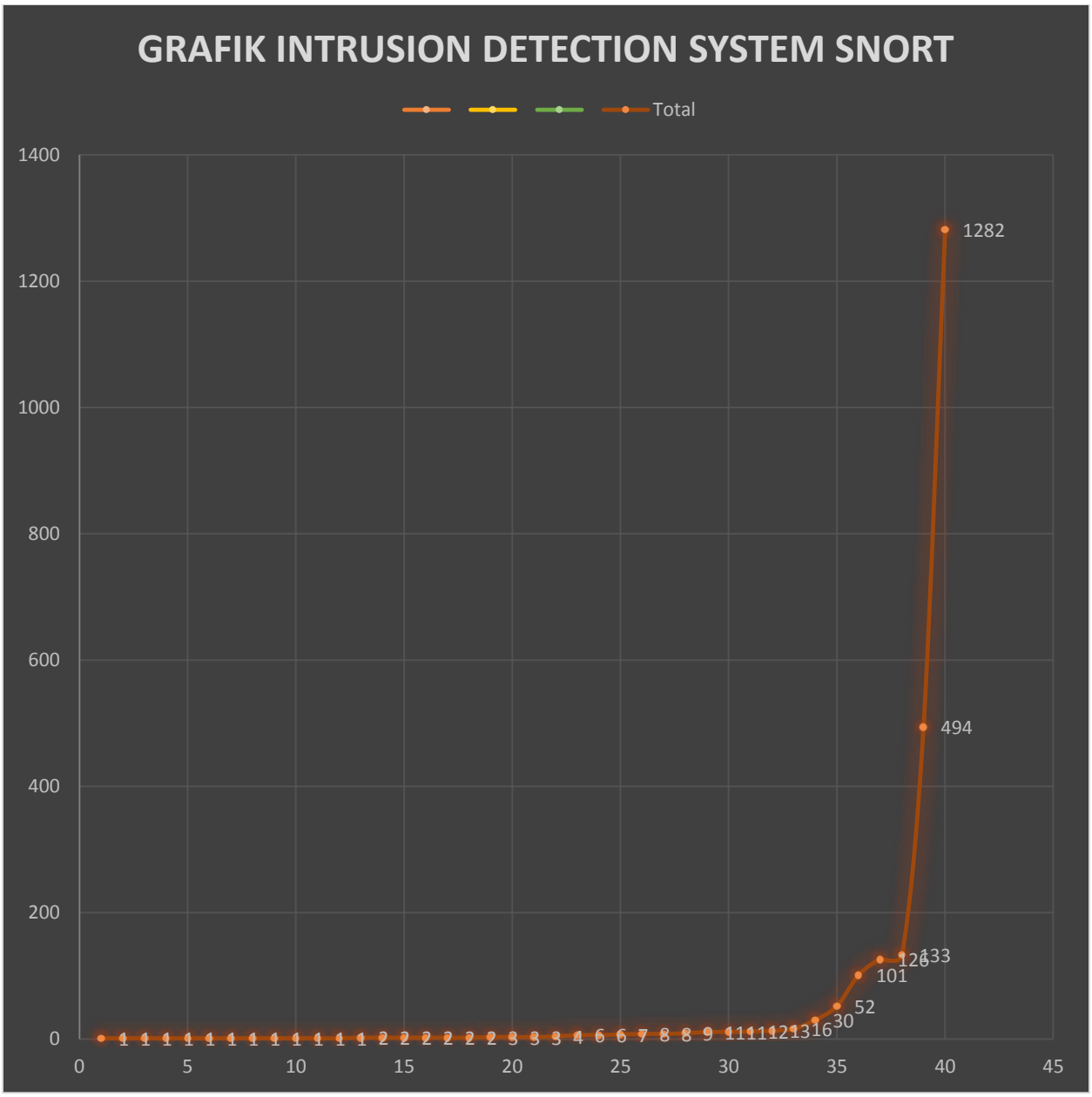
NO	Alert	Total
1	CHAT IRC nick change	1
2	EXPLOIT WINS name query overflow attempt TCP	1
3	FINGER remote command pipe execution attempt	1
4	FINGER root query	1
5	FTP format string attempt	1
6	FTP wu-ftp bad file completion attempt {	1
7	ICMP PING NMAP	1
8	ICMP Time-To-Live Exceeded in Transit	1
9	ICMP Timestamp Request	1
10	MISC MS Terminal server request	1
11	MISC MS Terminal server request RDP	1
12	X11 xopen	1
13	DNS named version attempt	2
14	FINGER remote command execution attempt	2
15	FINGER version query	2
16	ICMP Echo Reply undefined code	2
17	ICMP PING undefined code	2
18	MISC rsyncd overflow attempt	2
19	FINGER redirection attempt	3
20	MISC Source Port 20 to <1024	3
21	WEB-CGI redirect access	3
22	FTP command overflow attempt	4
23	MISC source port 53 to <1024	6

24	RSERVICES rexec password overflow attempt	6
25	FINGER . query	7
26	CMP L3retriever Ping	8
27	SCAN nmap XMAS	8
28	FINGER 0 query	9
29	ICMP Echo Reply	11
30	ICMP PING	11
31	COMMUNITY WEB-MISC mod_jrun overflow attempt	12
32	RSERVICES rexec username overflow attempt	13
33	FINGER null request	16
34	INFO web bug 0x0 gif attempt	30
35	BAD-TRAFFIC same SRC/DST	52
36	SNMP request tcp	101
37	SNMP AgentX/tcp request	126
38	MISC UPnP malformed advertisement	133
39	ICMP Destination Unreachable Network Unreachable	494
40	SCAN UPnP service discover attempt	1282

Setelah hasil alert dikelompokkan berdasarkan jenisnya seperti yang ditampilkan pada table di atas, diketahui bahwa alert CHAT IRC nick change, EXPLOIT WINS name query overflow attempt TCP, FINGER remote command pipe execution attempt, FINGER root query, FTP format string attempt, FTP wu-ftp bad file completion attempt {, ICMP PING NMAP, ICMP Time-To-Live Exceeded in Transit, ICMP Timestamp Request, MISC MS Terminal server request, MISC MS Terminal server request RDP, dan X11 xopen adalah yang paling sedikit menghasilkan alert, yaitu masing masing menghasilkan 1 alert. Sedangkan SCAN UPnP serveice discover attempt adalah yang paling banyak menghasilkan alert, yaitu sebanyak 1282. Berikut adalah grafik IDS menggunakan Snort yang telah dilakukan sebelumnya.

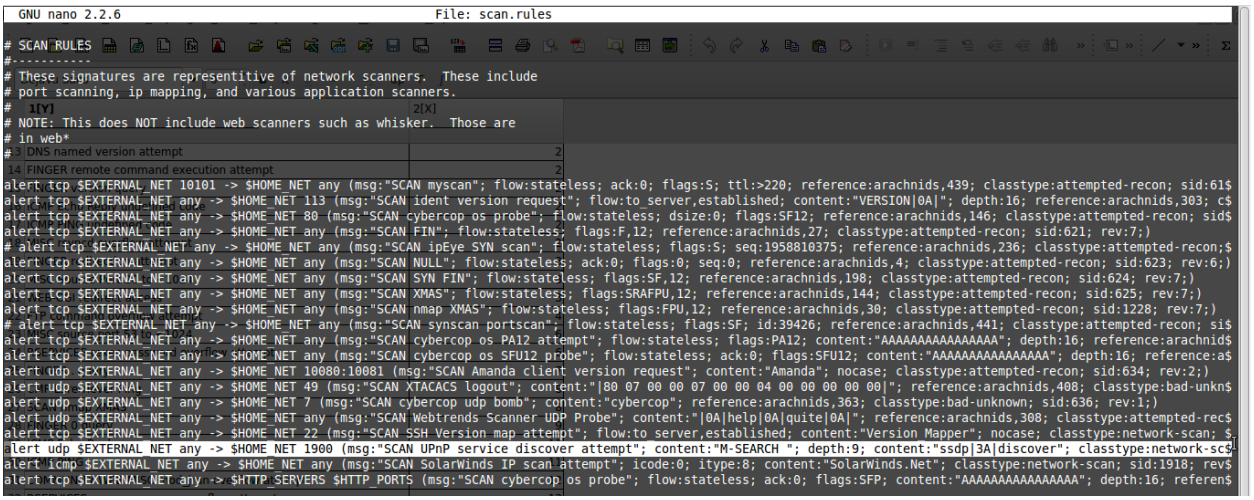


Gambar 6. Grafik IDS SNORT shopee.co.id



Gambar 7. Grafik IDS SNORT shopee.co.id

Dari 40 jenis serangan yang menimbulkan alert di atas, saya mengambil salah satu jenis serangan untuk dilihat rules-nya. Disini saya mengambil SCAN UPnP service discover attempt, yang memiliki total alert paling banyak sebagi sample. SCAN UPnP service discover attempt termasuk dalam serangan scan, yang terdapat pada file scan.rules pada Snort. Dalam file tersebut terdapat banyak serangan berjenis Scan, yang mana salah satunya adalah SCAN UPnP service discover attempt, seperti yang terlihat pada gambar berikut.



Gambar 8. Isi file scan.rules

Daftar Pustaka:

https://alfredoeblog.wordpress.com/2012/11/22/pengeertian-dan-cara-kerja-software-snort/

http://berbagicatatan.web.id/pengertian-ids-intrusion-detection-system/