NAMA : SUCI ANGGRAENI

NIM : 09011181320030

KEAMANAN JARINGAN KOMPUTER

INSTRUCTION DETECTION SYSTEM USING SNORT

IDS (*Intrusion Detection System*) adalah sebuah sistem yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan. IDS sendiri muncul dengan beberapa jenis dan pendekatan yang berbeda yang intinya berfungsi untuk mendeteksi traffic yang mencurigakan didalam sebuah jaringan.

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 merupakan *packet sniffing* yang sangat ringan. *Snifing interface* yang digunakan berbasis libpcap (pada Unix tersedia dengan tcpdump dan wireshark). 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.

Target : www.bukalapak.com

IP target : 182.253.238.102

Tools yang digunakan:

- NMAP (linux)
- WIRESHARK (linux)
- SNORT (Linux)
- MS. EXCEL (Windows)

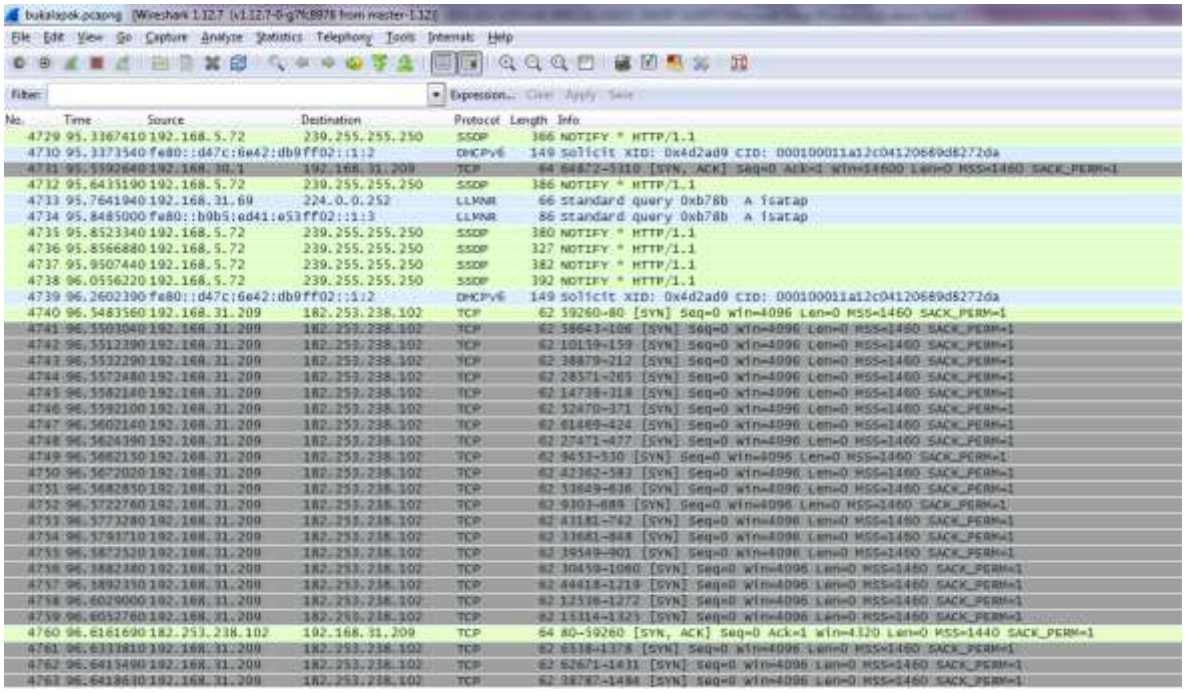
Sebelim melakukan sniffer pada snort lakukan dulu scaning pada nmap dan buka bersamaan wireshark pada saat melakukan scanning target. Berikut tampilan hasil scanning dan peng-capture-an paket menggunakan Wireshark.

NAMA : SUCI ANGGRAENI

NIM : 09011181320030

KEAMANAN JARINGAN KOMPUTER

Gambar 1. Tampilan scanning pada nmap



Gambar 2. Tampilan capture pada sniffing 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

NAMA : SUCI ANGGRAENI

NIM : 09011181320030

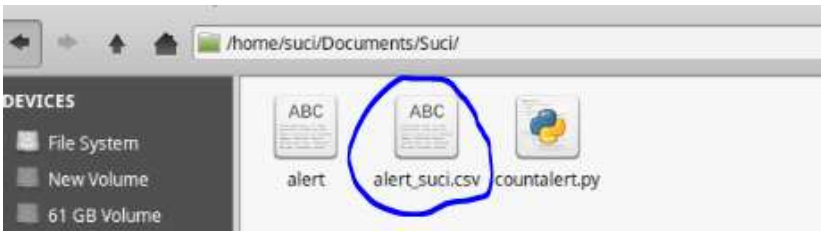
KEAMANAN JARINGAN KOMPUTER

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

kemudian setelah menjalankan perintah diatas maka akan menghasilkan sebuah file alert. Untuk membaca dan mengetahui berapa banyak alert yang di dapat, file alert tersebut di compile menggunakan python sehingga akan menghasilkan sebuah file yang berformat csv. Dengan menjalankan perintah berikut :

python countalert.py alert alert_suci.csv

Dapat dilihat pada gambar di bawah ini.



Gambar 3. Hasil compile file alert menjadi alert_suci.csv

Dalam file alert, terdapat 135 jenis alert dengan total 9589 alert. Untuk mengetahui alert yang paling banyak dan yang paling sedikit dan juga untuk mempersentasikan nya dalam bentuk grafik maka data dari file alert tersebut disajikan dalam sebuah table. Berikut table alert.

No	Total	Alert
1	1	**CHAT IRC nick change**
2	1	**COMMUNITY WEB-IIS RSA WebAgent access**
3	1	**DDOS mstream client to handler**
4	1	**DNS named authors attempt**
5	1	**EXPLOIT WINS name query overflow attempt TCP**
6	1	**FINGER remote command pipe execution attempt**
7	1	**FINGER root query**
8	1	**FTP format string attempt**

NAMA : SUCI ANGGRAENI

NIM : 09011181320030

KEAMANAN JARINGAN KOMPUTER

9	1	**FTP wu-ftp bad file completion attempt {**
10	1	**ICMP Timestamp Reply**
11	1	**MISC MS Terminal server request**
12	1	**MISC MS Terminal server request RDP**
13	1	**RPC portmap listing TCP 111**
14	1	**RPC portmap rusers request TCP**
15	1	**SNMP trap tcp**
16	1	**WEB-CGI FormHandler.cgi external site redirection attempt**
17	1	**WEB-CGI bigconf.cgi access**
18	1	**WEB-CGI perl command attempt**
19	1	**WEB-CGI perl.exe access**
20	1	**WEB-CGI perl.exe command attempt**
21	1	**WEB-CGI swc access**
22	1	**WEB-CGI wrap access**
23	1	**WEB-COLDFUSION administrator access**
24	1	**WEB-FRONTPAGE _vti_rpc access**
25	1	**WEB-FRONTPAGE shtml.dll access**
26	1	**WEB-IIS /iisadmpwd/aexp2.htr access**
27	1	**WEB-IIS ISAPI .ida access**
28	1	**WEB-IIS fpcount access**
29	1	**WEB-IIS trace.axd access**
30	1	**WEB-MISC .DS_Store access**
31	1	**WEB-MISC /CVS/Entries access**
32	1	**WEB-MISC /~nobody access**
33	1	**WEB-MISC DB4Web access**
34	1	**WEB-MISC ServletManager access**
35	1	**WEB-MISC TRACE attempt**
36	1	**WEB-MISC Tomcat SnoopServlet servlet access**
37	1	**WEB-MISC Tomcat servlet mapping cross site scripting**

NAMA : SUCI ANGGRAENI

NIM : 09011181320030

KEAMANAN JARINGAN KOMPUTER

		attempt
38	1	**WEB-MISC VirusWall FtpSave access**
39	1	**WEB-MISC WebDAV search access**
40	1	**WEB-MISC WebLogic ConsoleHelp view source attempt**
41	1	**WEB-MISC active.log access**
42	1	**WEB-MISC backup access**
43	1	**WEB-MISC iPlanet Search directory traversal attempt**
44	1	**WEB-MISC mod_gzip_status access**
45	1	**WEB-MISC perl post attempt**
46	1	**WEB-MISC viewcode access**
47	1	**WEB-MISC webalizer access**
48	1	**X11 xopen**
49	2	**BAD-TRAFFIC tcp port 0 traffic**
50	2	**COMMUNITY WEB-MISC JBoss web-console access**
51	2	**FINGER remote command execution attempt**
52	2	**FINGER version query**
53	2	**ICMP Destination Unreachable Communication Administratively Prohibited**
54	2	**ICMP Echo Reply undefined code**
55	2	**ICMP PING undefined code**
56	2	**ICMP Timestamp Request**
57	2	**MISC rsyncd overflow attempt**
58	2	**RPC portmap cachefsd request TCP**
59	2	**RPC portmap mountd request TCP**
60	2	**RPC portmap rstatd request TCP**
61	2	**RPC portmap ypserv request TCP**
62	2	**WEB-CGI admin.pl access**
63	2	**WEB-CGI book.cgi access**
64	2	**WEB-CGI faqmanager.cgi access**

NAMA : SUCI ANGGRAENI

NIM : 09011181320030

KEAMANAN JARINGAN KOMPUTER

65	2	**WEB-CGI formmail access**
66	2	**WEB-CGI guestbook.cgi access**
67	2	**WEB-CGI mailit.pl access**
68	2	**WEB-CGI quickstore.cgi access**
69	2	**WEB-CGI test-cgi access**
70	2	**WEB-CGI upload.cgi access**
71	2	**WEB-FRONTPAGE /_vti_bin/ access**
72	2	**WEB-IIS IISProtect access**
73	2	**WEB-IIS IISProtect siteadmin.asp access**
74	2	**WEB-IIS ISAPI .idq access**
75	2	**WEB-IIS ISAPI .idq attempt**
76	2	**WEB-IIS global.asa access**
77	2	**WEB-MISC WEB-INF access**
78	2	**WEB-MISC oracle portal demo access**
79	2	**WEB-MISC robots.txt access**
80	3	**DNS zone transfer TCP**
81	3	**FINGER redirection attempt**
82	3	**ICMP Address Mask Request**
83	3	**ICMP PING NMAP**
84	3	**MISC AFS access**
85	3	**MISC Source Port 20 to <1024**
86	3	**MISC xdmcp info query**
87	3	**MS-SQL ping attempt**
88	3	**RPC portmap bootparam request TCP**
89	3	**WEB-CGI FormHandler.cgi access**
90	3	**WEB-CGI redirect access**
91	3	**WEB-MISC source.jsp access**
92	4	**COMMUNITY WEB-MISC Test Script Access**
93	4	**FTP command overflow attempt**

NAMA : SUCI ANGGRAENI

NIM : 09011181320030

KEAMANAN JARINGAN KOMPUTER

94	4	**P2P GNUTella client request**
95	4	**P2P Outbound GNUTella client request**
96	4	**SNMP private access udp**
97	4	**WEB-CGI count.cgi access**
98	4	**WEB-CGI search.cgi access**
99	4	**WEB-CGI test.cgi access**
100	5	**SCAN Amanda client version request**
101	5	**WEB-CGI printenv access**
102	5	**WEB-FRONTPAGE .... request**
103	5	**WEB-MISC /.... access**
104	6	**COMMUNITY WEB-PHP XSS attempt**
105	6	**DNS named version attempt**
106	6	**MISC source port 53 to <1024**
107	6	**RSERVICES rexec password overflow attempt**
108	6	**WEB-IIS .htr access**
109	6	**WEB-IIS iisadmpwd attempt**
110	7	**FINGER . query**
111	7	**SNMP public access udp**
112	7	**WEB-MISC login.htm access**
113	8	**ICMP L3retriever Ping**
114	8	**ICMP Time-To-Live Exceeded in Transit**
115	8	**SCAN nmap XMAS**
116	9	**FINGER 0 query**
117	12	**ICMP Echo Reply**
118	13	**ICMP PING**
119	13	**RSERVICES rexec username overflow attempt**
120	14	**BAD-TRAFFIC Unassigned/Reserved IP protocol**
121	16	**COMMUNITY WEB-MISC mod_jrun overflow attempt**
122	16	**FINGER null request**

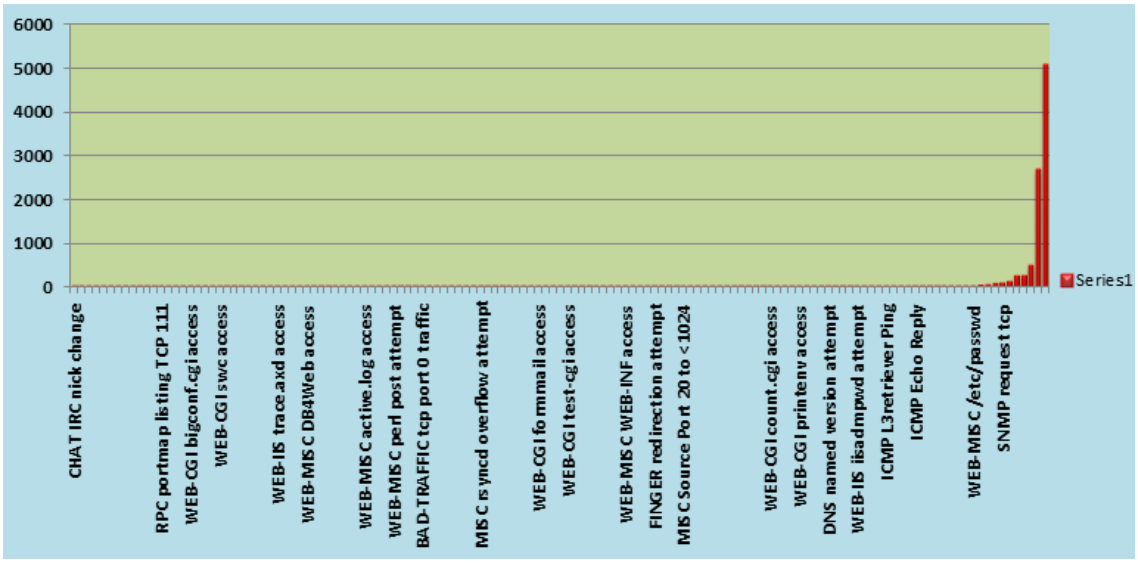
NAMA : SUCI ANGGRAENI

NIM : 09011181320030

KEAMANAN JARINGAN KOMPUTER

123	16	**SNMP request udp**
124	17	**WEB-IIS Directory transversal attempt**
125	26	**WEB-MISC /etc/passwd**
126	37	**INFO web bug 0x0 gif attempt**
127	59	**WEB-MISC http directory traversal**
128	73	**WEB-MISC cross site scripting attempt**
129	102	**SNMP request tcp**
130	127	**SNMP AgentX/tcp request**
131	238	**ICMP Destination Unreachable Port Unreachable**
132	252	**BAD-TRAFFIC same SRC/DST**
133	494	**ICMP Destination Unreachable Network Unreachable**
134	2682	**SCAN UPnP service discover attempt**
135	5093	**MISC UPnP malformed advertisement**

Setelah disajikan dalam bentuk table dapat dilihat bahwa alert yang paling banyak itu adalah **MISC UPnP malformed advertisement** dengan total aleret sebanyak **5039** alert.



Gambar 4. Tampilan grafik file alert