Keamanan Jaringan Komputer

Disusun Oleh

Nama : Kusuma Dwi Indriani

NIM : 09011181320017

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

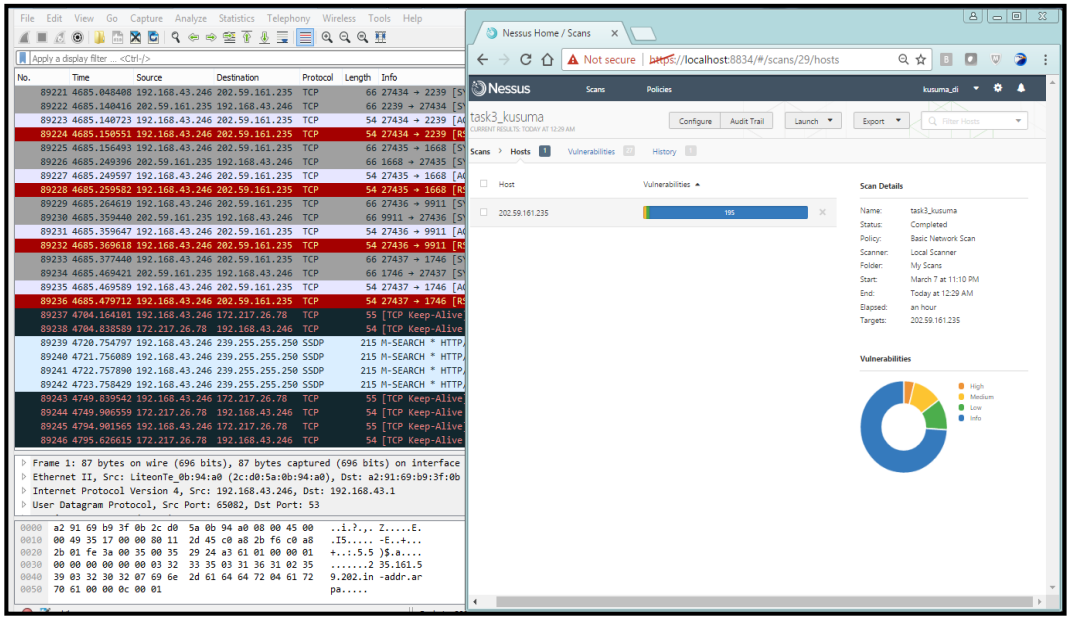
2017

INSTRUCTION DETECTION SYSTEM (IDS) USING SNORT

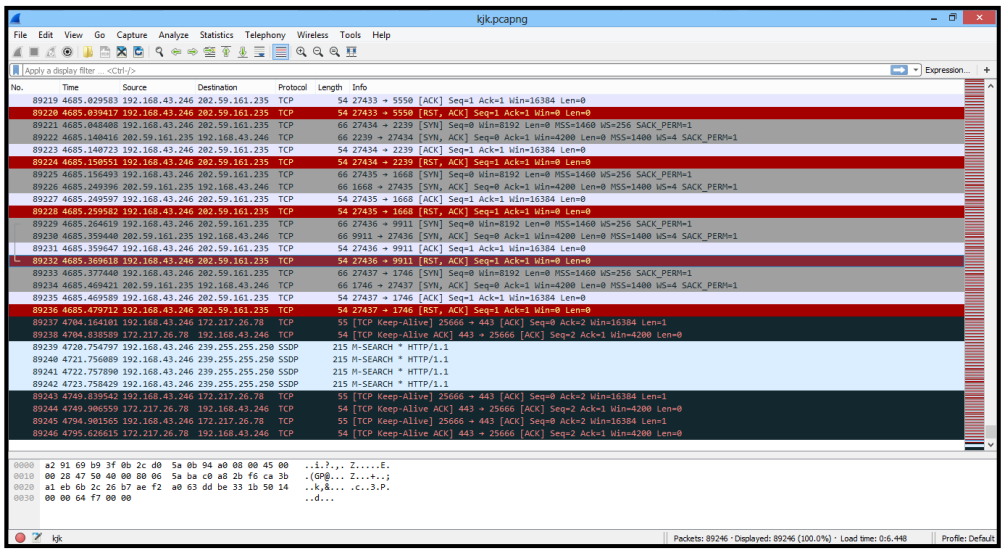
Taget : **www.21cineplex.com (202.59.161.235)**
Waktu Scanning : **7 Maret 2017 pukul 11:10 PM-00:29 AM**
Tools yang digunakan : **-Nessus**
-Wireshark
-Snort

Tahapan-tahapannya adalah sebagai berikut :

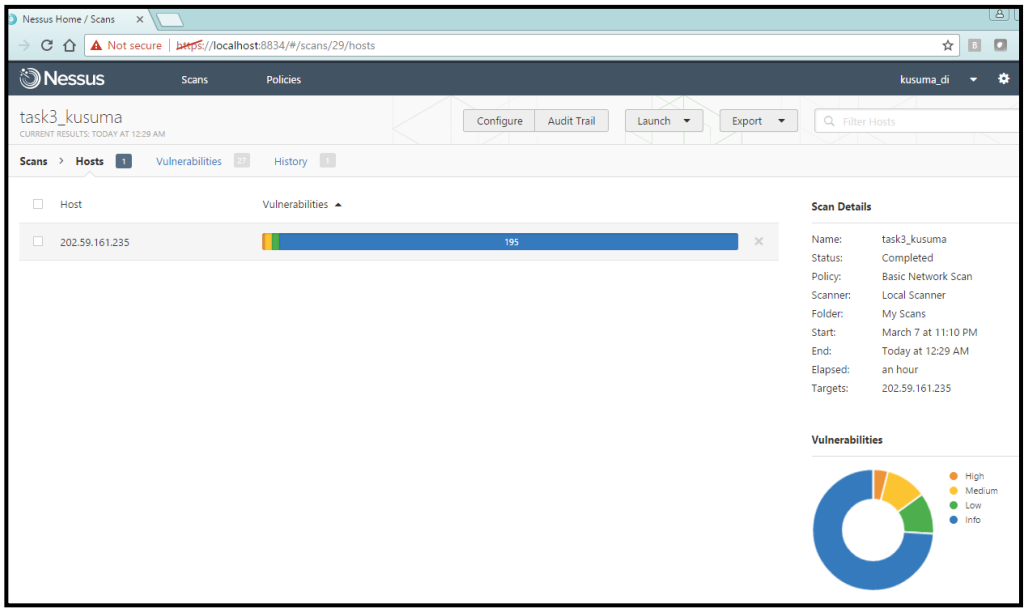
1. Scanning menggunakan Nessus dan buka aplikasi Wireshark secara bersamaan. Tunggu proses Scanning pada Nessus hingga selesai, seperti pada gambar 1.



Gambar 1. Proses scanning selesai



Gambar 2. Hasil pcap aplikasi Wireshark saat memantau proses scanning



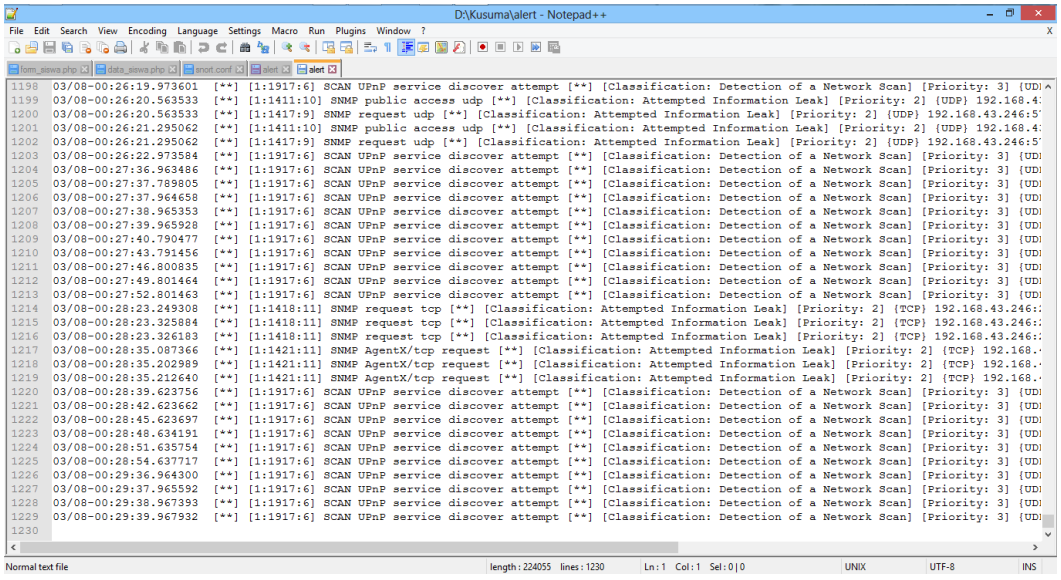
Gambar 3. Hasil scanning pada aplikasi Nessus

Saat melakukan proses scanning aplikasi wireshark menangkap paket-paket yang didapat saat melakukan scanning pada Nessus. Paket yang ditangkap saat proses scanning telah selesai sebanyak 89.246. protokol yang didapat diantaranya DNS, ARP, ICMP, TCP, HTTP, SNMP, DCERPC, SMB dan SSDP.

2. File pcap yang telah disimpan kemudian buka menggunakan aplikasi snort di linux dengan perintah :

Snort –A fast –c /etc/snort/snort.conf –r /home/linda/documents/kjk.pcapng –l /var/log/snort

Hasil yang akan didapatkan dari hasil snort adalah seperti gambar 4. Pada gambar hasil yang ditunjukkan, hampir terlihat seperti file pcap pada wireshark akan tetapi jumlah paket yang ada pada hasil *compile* file tidak sama dengan file pcap. Jumlahnya adalah 1229. Jauh lebih sedikit jika dibandingkan dengan jumlah paket ada pada file pcap wireshark.



Gambar 4. Hasil Alert dari file pcap yang di *compile* dengan snort

Hal tersebut dikarenakan wireshark mengolah paket yang masuk satu demi satu sedangkan snort mengklasifikasikan dalam beberapa jenis beserta prioritasnnya.

3. Dibutuhkan suatu aplikasi yang dapat menglompokkan hasil alert yang ada agar lebih mudah dibaca dan dianalisa maka digunakan phyton. Hasil tersebut dapat dilihat pada tabel 1.

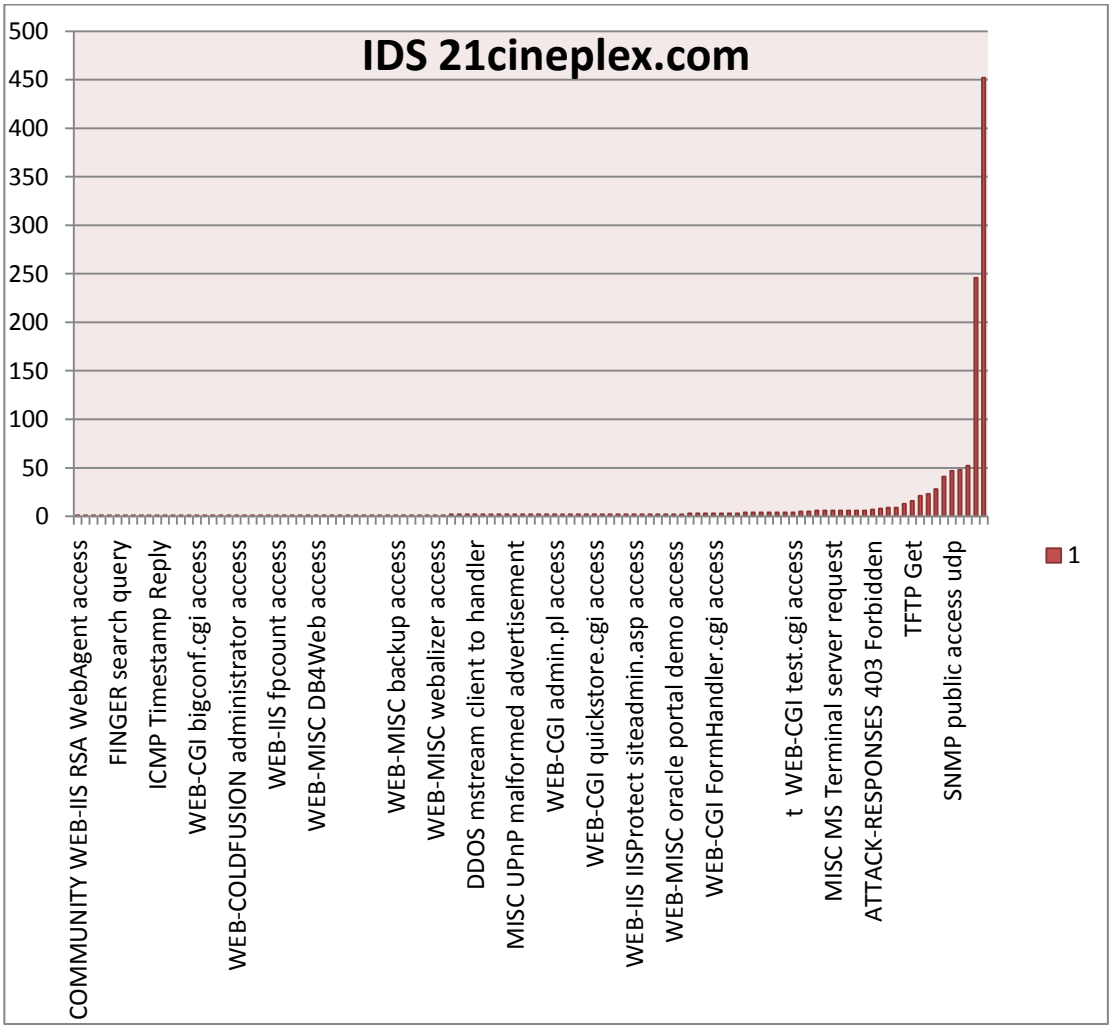
Tabel 1. Rincian Alert dari situs 21cineplex.com

NO	Alert	Jumlah
1	CHAT Yahoo IM message	1
2	COMMUNITY WEB-IIS RSA WebAgent access	1
3	DNS zone transfer TCP	1
4	FINGER . query	1
5	FINGER account enumeration attempt	1
6	FINGER root query	1
7	FINGER search query	1
8	FINGER version query	1
9	FTP CWD ~ attempt	1
10	ICMP Echo Reply	1
11	ICMP Time-To-Live Exceeded in Transit	1
12	ICMP Timestamp Reply	1
13	INFO FTP no password	1
14	POLICY PPTP Start Control Request attempt	1
15	POLICY VNC server response	1
16	WEB-CGI FormHandler.cgi external site redirection attempt	1
17	WEB-CGI bigconf.cgi access	1
18	WEB-CGI faqmanager.cgi arbitrary file access attempt	1
19	WEB-CGI perl command attempt	1
20	WEB-CGI perl.exe access	1
21	WEB-CGI perl.exe command attempt	1
22	WEB-COLDFUSION administrator access	1
23	WEB-FRONTPAGE _vti_rpc access	1
24	WEB-FRONTPAGE shtml.dll access	1
25	WEB-IIS /iisadmpwd/aexp2.htr access	1
26	WEB-IIS ISAPI .ida access	1
27	WEB-IIS fpcount access	1
28	WEB-IIS trace.axd access	1
29	WEB-MISC .DS_Store access	1
30	WEB-MISC /CVS/Entries access	1
31	WEB-MISC /~nobody access	1
32	WEB-MISC DB4Web access	1
33	WEB-MISC Domino names.nsf access	1
34	WEB-MISC ServletManager access	1
35	WEB-MISC TRACE attempt	1
36	WEB-MISC Tomcat SnoopServlet servlet access	1
37	WEB-MISC Tomcat servlet mapping cross site scripting	1

	attempt	
38	WEB-MISC VirusWall FtpSave access	1
39	WEB-MISC WebDAV search access	1
40	WEB-MISC WebLogic ConsoleHelp view source attempt	1
41	WEB-MISC active.log access	1
42	WEB-MISC backup access	1
43	WEB-MISC iPlanet Search directory traversal attempt	1
44	WEB-MISC mod_gzip_status access	1
45	WEB-MISC perl post attempt	1
46	WEB-MISC viewcode access	1
47	WEB-MISC webalizer access	1
48	X11 xopen	1
49	CHAT IRC nick change	2
50	COMMUNITY WEB-MISC JBoss JMXInvokerServlet access	2
51	COMMUNITY WEB-PHP XSS attempt	2
52	DDOS mstream client to handler	2
53	FINGER / execution attempt	2
54	ICMP PING	2
55	ICMP PING NMAP	2
56	ICMP Timestamp Request	2
57	MISC UPnP malformed advertisement	2
58	P2P GNUTella client request	2
59	P2P Outbound GNUTella client request	2
60	SNMP private access udp	2
61	SNMP trap tcp	2
62	WEB-CGI admin.pl access	2
63	WEB-CGI book.cgi access	2
64	WEB-CGI formmail access	2
65	WEB-CGI guestbook.cgi access	2
66	WEB-CGI mailit.pl access	2
67	WEB-CGI quickstore.cgi access	2
68	WEB-CGI test-cgi access	2
69	WEB-CGI upload.cgi access	2
70	WEB-FRONTPAGE /_vti_bin/ access	2
71	WEB-IIS IISProtect access	2
72	WEB-IIS IISProtect siteadmin.asp access	2
73	WEB-IIS ISAPI .idq access	2
74	WEB-IIS ISAPI .idq attempt	2
75	WEB-IIS global.asa access	2
76	WEB-MISC WEB-INF access	2
77	WEB-MISC oracle portal demo access	2

78	WEB-MISC robots.txt access	2
79	MISC rsyncd module list access	3
80	MISC xdmcp info query	3
81	MS-SQL ping attempt	3
82	WEB-CGI FormHandler.cgi access	3
83	WEB-CGI faqmanager.cgi access	3
84	WEB-CGI printenv access	3
85	WEB-MISC source.jsp access	3
86	BAD-TRAFFIC tcp port 0 traffic	4
87	COMMUNITY WEB-MISC JBoss web-console access	4
88	COMMUNITY WEB-MISC Test Script Access	4
89	POP3 SSLv3 invalid timestamp attempt	4
90	WEB-CGI count.cgi access	4
91	WEB-CGI search.cgi access	4
92	t WEB-CGI test.cgi access	4
93	WEB-FRONTPAGE .... request	5
94	WEB-MISC /.... access	5
95	ICMP Address Mask Request	6
96	MISC AFS access	6
97	MISC MS Terminal server request	6
98	SCAN Amanda client version request	6
99	WEB-IIS .htr access	6
100	WEB-IIS iisadmpwd attempt	6
101	WEB-MISC login.htm access	6
102	ATTACK-RESPONSES 403 Forbidden	7
103	WEB-MISC .htaccess access	8
104	SNMP AgentX/tcp request	9
105	SNMP request tcp	9
106	WEB-IIS Directory transversal attempt	13
107	TFTP Get	16
108	POLICY FTP anonymous login attempt	21
109	WEB-MISC /etc/passwd	23
110	WEB-MISC cross site scripting attempt	28
111	INFO FTP Bad login	41
112	SNMP public access udp	47
113	WEB-MISC http directory traversal	48
114	SNMP request udp	52
115	ICMP Destination Unreachable Port Unreachable	246
116	SCAN UPnP service discover attempt	452

Dari tabel diatas, untuk lebih mudah mengamati alert yang paling rendah hingga yang tertinggi maka data disajikan dalam bentuk grafik 1.



Dikarenakan jumlah alert yang banyak (116) maka keterangan dari gambar grafk tidak dapat ditapilkan semua. Akan tetapi dapat disimpulkan bahwa alert dengan prioritas paling banyak yaitu mengenai SCAN UPnP service discover attempt.