Tugas Mata Kuliah

KEAMANAN JARINGAN KOMPUTER



Nama : Faris Abdul Aziz Nim : 09011181320020

Jurusan Sistem Komputer

Fakultas Ilmu Komputer Universitas Sriwijaya

2016

TUGAS 4

INSTRUCTION DETECTION SYSTEM MENGGUNAKAN SNORT

Instruction Detection System (IDS) adalah sebuah system yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan kegiatan yang mencurigakan didalam sebuah system jaringan. Dimana pada Tugas kali ini saya akan melihat traffic yang ada pada situs www.ptba.co.id dengan menggunakan aplikasi snort. Aplikasi snort sendiri berfungsi sebagai sniffer dan packet logger pada sebuah jaringan selain itu snort dapat digunakan untuk mendeteksi sebuah serangan.

TUGAS : scanning situs target sambil menjalankan wireshark, kemudian compile menggunakan snort, lihat apa yang terjadi? (ketika telah mendapatkan data alert buat table dan grafiknya)

1. TARGET SITUS DAN TOOLS YANG DIGUNAKAN

Pada tugas ke-4 ini saya masih melakukan scanning terhadap perusahaan PT Bukit Asam yang memiliki IP, kemudian saya menggunakan beberapa tools untuk membantu melakukan tugas ini, berikut merupakan toolsnya adalah Wireshark dan Zenmap.

2. LANGKAH-LANGKAH YANG DILAKUKAN

Langkah-langkah pada tugas ini adalah sebagai berikut:

1. Buka Wireshark dan lakukan scanning pada situs yang dituju

 Zenmap 	and the second second					L	- 0	×
Scan Ioo	ls <u>P</u> rofile <u>H</u> e	lp						
Target: w	ww.ptba.co.id		▼ P	rofile:	Intense scan	•	Scan	Cancel
Command:	nmap -T4 -A	-v www.ptba.co.id						
Hosts	Senices							
TIUSIS	Jervices	Intriap Output Ports / Hosts Topology Host Details Scans					_	
OS 4 Host	•	nmap -T4 -A -v www.ptba.co.id					•	Details
		Discovered open port 960/trp on 202,158,49.50 Discovered open port 960/trp on 202,158,49.50 Discovered open port 2021/trp on 202,158,49.50 Discovered open port 2021/trp on 202,158,49.50 Discovered open port 4021/s/trp on 202,158,49.50 Discovered open port 4021/s/trp on 202,158,49.50 Discovered open port 403/s/trp on 202,158,49.50 Discovered open port 6103/trp on 202,158,49.50 Discovered open port 6103/trp on 202,158,49.50 Discovered open port 6103/trp on 202,158,49.50 Discovered open port 6105/trp on 202,158,49.50 Discovered open port 8053/trp on 202,158,49.50 Discovered open port 999/trp on 202,158,49.50 Discovered open port 990/trp on 202,158,49.50 Discovered open port 980/trp on 202,158,49.						
		Discovered open port 5989/tcp on 202.158.49.50 Discovered open port 8009/tcp on 202.158.49.50 Completed SYN Stealth Scan at 20:27, 3.125 elapsed (1000 total Initiating Service scan at 20:27, 3.125 elapsed (1000 total	ports	;)				E
		Intracting Service Scan at 2012/						*

Gambar 2.1 Scanning menggunakan Zenmap

Pada gambar 2.1 melakukan scanning terhadap situs <u>www.ptba.co.id</u> dimana pada saat melakukan scanning pada situs tersebut, dilakukan juga scan wireshark untuk melihat traffic data pada saat scanning tersebut. Dan dapat dilihat pada gambar 2.2 untuk hasil scan wireshark

🖕 faris.pcapng (Wireshark 2.2.1 (v2.2.1-0-ga6fbd27 from master-2.2))						
Eile Edit View Go Capture Analyze Statistics Telephony Iools Internals Help						
• •	ک 🔳 🛦 (🕒 🗎 🗶 🎜	् 🗢 🔿 春 🕹		R. Q. Q. 🖻 👹 🕅 🥵 % 🛄	
Filter:				 Expression 	. Clear Apply Save	
No.	Time	Source	Destination	Protocol Le	Length Info	^
9	2 21.459459	112.215.161.5	1 192.168.43.89	TCP	54 80-1114 [ACK] Seg=2 ACK=2 Win=1013 Len=0	
9	3 21.519195	112.215.161.4	8 192.168.43.89	TCP	66 80-1129 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 WS=32 SACK_PERM=1	
9	4 21.519250	192.168.43.89	112.215.161.48	TCP	54 1129-80 [ACK] Seq=1 Ack=1 win=65800 Len=0	
9	5 21.519379	192.168.43.89	112.215.161.48	HTTP	370 GET /MFEWTZBNMESWSTAJBgUrDgMCGgUABBQ1mI4Ww4R5LZiQ295pj40F%2F44yyAQUyk7dWyc1Kdn27sPlU%2B%2BkwBmWHa8C	C
9	6 21.894485	192.168.43.89	239.255.255.250	SSDP	417 NOTIFY * HTTP/1.1	
9	7 22.128234	192.168.43.89	112.215.161.48	TCP	370 [TCP Retransmission] 1129-80 [PSH, ACK] Seq=1 Ack=1 win=65800 Len=316	
9	08 23.220440	192.168.43.89	239.255.255.250	SSDP	359 NOTIFY * HTTP/1.1	
9	9 23.221343	52.71.191.253	192.168.43.89	TCP	54 443-1112 [ACK] Seq=1 Ack=1401 Win=263 Len=0	
10	0 23.26/314	192.168.43.89	239.255.255.250	SSDP	350 NOTIFY * HTTP/1.1	
10	1 23.314094	192.108.43.89	239.233.235.230	SSDP	402 NOLLEY * HIP/LL	
10	2 23.35/020	102 169 42 90	112 215 161 49	TCP	24 442-TILLZ [ACK] SEGET ACK-ZOOL WITHEZ/4 LEGTED	
10	4 23 501235	192.108.43.89	230 255 255 250	SSDR	3YO [ICP KELT dismission] 1129-80 [PSH, ALK] SEQEL ALKET WITEOSOOD LETESTO 3YO [ICP KELT dismission] 1129-80 [PSH, ALK] SEQEL ALKET WITEOSOOD LETESTO	•
10	5 23 548061	192.168 43.89	239 255 255 250	SSDP	350 NOTEY HTTP/1 1	
10	6 23 688361	192 168 43 89	239 255 255 250	SSDP		
10	7 23 782017	192 168 43 89	239 255 255 250	SSDP	418 NOTIEY * HTTP/1 1	
10	8 23, 837596	52,71,191,253	192,168,43,89	TCP	54 443-1112 [ACK] Seg=1 Ack=3605 Win=285 Len=0	
10	9 23,839336	112,215,161,4	8 192,168,43,89	TCP	54 80-1129 [ACK] Seg=1 Ack=317 win=30272 Len=0	
11	0 23.868495	52.71.191.253	192.168.43.89	TLSV1.2	536 Application Data	
11	1 24.060835	112.215.161.4	8 192.168.43.89	TCP	66 [TCP Dup ACK 109#1] 80-1129 [ACK] Seq=1 Ack=317 win=30272 Len=0 SLE=1 SRE=317	1
11	2 24.078267	192.168.43.89	52.71.191.253	TCP	54 1112-443 [ACK] Seq=3605 Ack=483 win=16450 Len=0	-
11	3 24.342732	112.215.161.4	8 192.168.43.89	тср	66 [TCP Dup ACK 109#2] 80-1129 [ACK] Seq=1 Ack=317 win=30272 Len=0 SLE=1 SRE=317	
11	4 24.368757	112.215.161.4	8 192.168.43.89	тср	1454 [TCP segment of a reassembled PDU]	-
					4 m	
D Era	mo 114 · 1454	hytes on wire	(11632 hits) 1454 h	tes canture	ed (11632 hits) on interface 0	
E Eth	ernet II. Sr	c: Asustekc f2	:f9:e8 (ac:9e:17:f2:f9	e8). Dst: 4	Azureway 17:5d:6f (f0:03:8c:17:5d:6f)	
I Int	ernet Proto	ol Version 4.	Src: 112,215,161,48, 0	st: 192.168.	8.43.89	
. Tra	nsmission Co	ontrol Protocol	, Src Port: 80, Dst Po	ort: 1129, 50	Seg: 1. Ack: 317. Len: 1400	
			,			
0000	f0 03 8c 17	5d 6f ac 9e	17 f2 f9 e8 08 00 45 0	0]o	E.	
0010	05 aU 52 b6	040 00 3b 06	e9 98 /0 d/ a1 30 c0 a	18R.@.;.	;p0.	
0030	03 b2 3d a1	00 00 48 54	54 50 2f 31 2e 31 20 3	2=HT	нт тР/1.1 2	
0040	30 30 20 4f	4b 0d 0a 53	65 72 76 65 72 3a 20 6	е 00 ок	.s erver: n	-
0050	67 60 60 79	0 0 0 0 1 2 6F	60 74 65 60 74 2d 54 7	0 ainv Co		-

Gambar 2.2 Traffic Wireshark

2. Compile data menggunakan snort

Setelah mendapatkan hasil pcap dari wireshark lakukan compile file pcap dengan perintah snort – A fast –c /etc/snort/snort.conf –r (tempat direktori file pcap tersimpan) lalu jika tidak terdapat error lihat apakah data alert berhasil didapatkan. Berikut screenshoot hasil alert yang didapatkan.

40	03/08-16:59:31.458859	[**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.89 -> 202.158.49.50	
41	03/08-16:59:31.480890	[**] [1:453:5] ICMP Timestamp Request [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.89 -> 202.158.49.50	
42	03/08-16:59:31.552459	[**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 202.158.49.50 -> 192.168.43.89	
43	03/08-16:59:31.596932	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5.
44	03/08-16:59:31.630457	[**] [1:451:5] ICMP Timestamp Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 202.158.49.50 -> 192.168.43.89	
45	03/08-16:59:31.690510	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5.
46	03/08-16:59:38.110636	[**] [1:485:4] ICMP Destination Unreachable Communication Administratively Prohibited [**] [Classification: Misc activity] [Priority: 3]	C
47	03/08-16:59:38.688048	[**] [1:485:4] ICMP Destination Unreachable Communication Administratively Prohibited [**] [Classification: Misc activity] [Priority: 3]	£
48	03/08-16:59:39.771419	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5.
49	03/08-16:59:41.222063	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5. =
50	03/08-16:59:41.268976	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5.
51	03/08-16:59:41.315770	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5
52	03/08-16:59:41.502938	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5
53	03/08-16:59:41.549919	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5.
54	03/08-16:59:41.690403	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5
55	03/08-16:59:41.784183	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Friority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5
56	03/08-16:59:48.415742	[**] [1:1418:11] SNMP request top [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.89:33303 -> 202.158.49	-1
57	03/08-16:59:49.833406	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5
58	03/08-16:59:49.864715	[**] [1:1418:11] SNMP request top [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.89:33304 -> 202.158.49	41
59	03/08-16:59:51.330841	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5.
60	03/08-16:59:51.377732	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5.
61	03/08-16:59:51.424679	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5.
62	03/08-16:59:51.611662	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5.
63	03/08-16:59:51.658689	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5.
64	03/08-16:59:51.798863	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5.
65	03/08-16:59:51.892528	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5
66	03/08-16:59:53.119938	[**] [1:485:4] ICMP Destination Unreachable Communication Administratively Prohibited [**] [Classification: Misc activity] [Priority: 3]	€
67	03/08-16:59:55.979604	[**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.89:33303 -> 202	-1
68	03/08-16:59:56.104336	[**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.89:33304 -> 202	-1
69	03/08-16:59:58.115839	[**] [1:485:4] ICMP Destination Unreachable Communication Administratively Prohibited [**] [Classification: Misc activity] [Priority: 3]	£
70	03/08-16:59:59.895177	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5.
71	03/08-17:00:01.439690	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5.
72	03/08-17:00:01.486577	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5.
73	03/08-17:00:01.533361	[**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.25	5.

Gambar 2.3 Data Alert

Pada gambar 2.3 terdapat data alert yang dimana pada Wireshark tidak didapatkan, atau lebih tepatnya diekstrak untuk mendapatkan hasil traffic yang tidak dapat dilihat secara rinci oleh wireshark. Dan untuk melakukan ini digunakan alat bantu yaitu countalert.py yang merupakan tools dengan bahasa pyton.

3. HASIL SAJIAN DATA

Setelah mendapatkan data berikut merupakan tampilan dari hasil sajian data alert berupa table dan grafik.

No	ALERT	JUMLAH
1	Alert ICMP PING NMAP	1
2	Alert ICMP Timestamp Reply	1
3	Alert ICMP Timestamp Request	1
4	Alert SNMP AgentX/tcp request	2
5	Alert SNMP request tcp	2
6	Alert ICMP Echo Reply undefined code	2
7	Alert ICMP PING undefined code	3





Gambar 3.2 Grafik Alert