KEAMANAN JARINGAN KOMPUTER



Eko Pratama

09011181320004

Program Studi Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

2017

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 Krakatausteel.com 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. krakatau steel yang memiliki IP 118.97.204.70, kemudian saya menggunakan beberapa tools untuk membantu melakukan tugas ini, berikut merupakan toolsnya:

- Wireshark : merupakan sebuah tools yang digunakan untuk menganalisa traffic dari sebuah jaringan
- **Nmap :** merupakan sebuah alat bantu untuk melakukan scanning pada target yang dituju

2. LANGKAH-LANGKAH YANG DILAKUKAN

Langkah yang dilakukan untuk tugas kali ini dapat dilihat seperti beberapa gambar dibawah ini:

Buka wireshark sambil melakukan scanning

```
root@Server:/home/server# nmap -0 118.97.204.70
Starting Nmap 7.01 ( https://nmap.org ) at 2017-03-07 01:19 EST
Nmap scan report for 118.97.204.70
Host is up (0.00079s latency).
All 1000 scanned ports on 118.97.204.70 are filtered
Too many fingerprints match this host to give specific OS details
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.17 seconds
root@Server:/home/server# nmap -v -sX 118.97.204.70
Starting Nmap 7.01 ( https://nmap.org ) at 2017-03-07 01:22 EST
Initiating Ping Scan at 01:22
Scanning 118.97.204.70 [4 ports]
Completed Ping Scan at 01:22, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:22, 13.00s elapsed
Initiating 118.97.204.70 figures]
Completed XMAS Scan at 01:22, 1.40s elapsed (1000 total ports)
Nmap scan report for 118.97.204.70
are closed
All 1000 scanned ports on 118.97.204.70 are closed
```

Gambar 2.1 Scanning

Pada gambar 2.1 saya melakukan scanning terhadap situs target <u>www.krakatausteel.com</u> dimana saat melakukan scanning saya menjalankan aplikasi wireshark untuk melihat traffic data yang terjadi saat melakukan scanning. Pada gambar 2.2 dibawah merupakan hasil dari traffic di aplikasi wireshark saat melakukan scanning.

📕 el	(o.pc	apng [Wi	ireshark 2.2.1 (v	2.2.1-0-ga	6fbd27 from m	aster-2.2)]			-	-	-	a	-	Sec. 1						×
<u>F</u> ile	Edi	it <u>V</u> iew	<u>Go</u> Capture	<u>A</u> nalyze	Statistics T	elephony <u>T</u>	ools Intern	als <u>H</u> elp												
0	۲	<u> </u>	🔬 🖻 🛛	X 2	; 🔍 🔶 I	🔹 😜 😨	⊻ 🗉		ର୍ ପ୍ 🖭	i 🏼 🕻	2 鸦	% 😫								
Filte	r:						~ E	xpression	Clear Apply	Save										
No.		Time	Source		Dest	ination	F	Protocol L	ength Info											-
	293	156.0	99014 192.1	.68.43.8	9 118	3.97.204.	70	ТСР	62 27050)→256 [SYN] :	Seq=0 W	in=8192	Len=0	MSS=146	0 SACK_I	PERM=1			
	294	156.0	99254 192.1	.68.43.8	9 118	3.97.204.	70	тср	62 27051	L→1720	[SYN]	Seq=0 N	vin=819	2 Len=0	MSS=14	60 SACK.	_PERM=1			
	295	156.1	02089 192.1	68.43.1	. 192	2.168.43.	89	ICMP	90 Desti	ination	unre	achab1e	(Netwo	rk unre	achable)				
	296	156.1	05667 192.1	.68.43.8	9 118	3.97.204.	70	ТСР	62 27052	2→554 [SYN] :	Seq=0 W	in=8192	Len=0	MSS=146	0 SACK_I	PERM=1			
	297	156.1	06097 192.1	.68.43.8	9 118	3.97.204.	70	тср	62 27053	3→8080	[SYN]	Seq=0 \	vin=819	2 Len=0	MSS=14	60 SACK.	_PERM=1			
	298	156.1	06312 192.1	.68.43.8	9 118	8.97.204.		ТСР	62 27054	+113 [SYN] :	seq=0 W	i n=8192	Len=0	MSS=146	0 SACK_I	PERM=1			
	299	156.1	06455192.1	.68.43.8	9 118	3.97.204.	70	ТСР	62 27055	5→445 [SYN] :	Seq=0 W	in=8192	Len=0	MSS=146	0 SACK_I	PERM=1			
	300	156.1	06578192.1	.68.43.8	9 118	3.97.204.	70	тср	62 27056	5→80 [s	YN S	eq=0 Win	1=8192	Len=0 M	ISS=1460	SACK_P	ERM=1	 		
	301	156.1	06695 192.1	.68.43.8	9 118	3.97.204.	70	ТСР	62 27057	7→23 [s	YN] S	eq=0 Wi	า=8192	Len=0 M	ISS=1460	SACK_PI	ERM=1			
	302	156.1	22065 192.1	.68.43.8	9 118	3.97.204.	70	ТСР	62 27058	3→21 [s	YN] S	eq=0 Wi	า=8192	Len=0 M	ISS=1460	SACK_PI	ERM=1			
	303	156.1	22268 192.1	.68.43.8	9 118	8.97.204.	70	тср	62 27059)→22 [s	YNJ S	eq=0 Wi	n=8192	Len=0 M	ISS=1460	SACK_PI	ERM=1			
	304	156.5	49372 192.1	.68.43.8	9 118	3.97.204.	70	ТСР	62 27060)→995 [SYN] :	seq=0 W	in=8192	Len=0	MSS=146	0 SACK_I	PERM=1			
	305	156.5	49497 192.1	.68.43.8	9 118	3.97.204.	70	ТСР	62 27061	L→443 [SYN] :	Seq=0 W	in=8192	Len=0	MSS=146	0 SACK_I	PERM=1			
	306	156.5	49606 192.1	.68.43.8	9 118	8.97.204.	70	тср	62 27062	2→25 [s	YNJ S	eq=0 Win	า=8192	Len=0 M	ISS=1460	SACK_PI	ERM=1			
	307	156.5	49718 192.1	.68.43.8	9 118	3.97.204.	70	ТСР	62 27063	3→1025	[SYN]	Seq=0 \	vin=819	2 Len=0	MSS=14	60 SACK	_PERM=1			
	308	156.5	49822 192.1	.68.43.8	9 118	3.97.204.	70	ТСР	62 27064	I→111 [SYN] :	Seq=0 W	in=8192	Len=0	MSS=146	0 SACK_I	PERM=1			
	309	156.5	49922 192.1	.68.43.8	9 118	3.97.204.	70	тср	62 27065	5→139 [SYN] :	seq=0 W	in=8192	Len=0	MSS=146	0 SACK_I	PERM=1			
	310	156.5	50027 192.1	.68.43.8	9 118	3.97.204.	70	TCP	62 27066	5+3306	[SYN]	Seq=0 \	vin=819	2 Len=0	MSS=14	60 SACK.	_PERM=1			
	311	156.5	50132 192.1	.68.43.8	9 118	3.97.204.	70	тср	62 27067	7→1723	[SYN]	Seq=0 N	vin=819	2 Len=0	MSS=14	60 SACK,	_PERM=1			
	312	156.5	50229 192.1	.68.43.8	9 118	3.97.204.	70	тср	62 27068	3→5900	[SYN]	Seq=0 \	vin=819	2 Len=0	MSS=14	60 SACK	_PERM=1			
	313	156.6	45568192.1	.68.43.8	9 118	3.97.204.	70	тср	62 27069)→199 [SYN] :	Seq=0 W	in=8192	Len=0	MSS=146	0 SACK_I	PERM=1			
	314	156.6	45794 192.1	.68.43.8	9 118	3.97.204.	70	тср	62 27070)+110 [SYN] :	Seq=0 W	in=8192	Len=0	MSS=146	0 SACK_I	PERM=1			
	315	156.6	45965 192.1	.68.43.8	9 118	3.97.204.	70	тср	62 27071	L→53 [s	YN] S	eq=0 Win	n=8192	Len=0 M	ISS=1460	SACK_PI	ERM=1			
4	216	156 6	46110100 1	60 47 0	110	07 704	70 .	TCD	62 27071	002 [Fog O W	0100	Lon 0	NCC 146	O CACK	1	 	 	•
			62. http://		(LOC HART	co. hum			- Indexes and		0									
	ramo theo	e 298: rnet T	62 Dytes (on wire ureway 1	(496 D1ts) 17:5d:6f (1), 62 Dyt F0:03:8c:	17:5d:6f	red (490). Dst:	Asustekc f	1ntert 2.f9.e	ace u 8 (ac	•9e•17•f		8)						
	nter	rnet P	rotocol Ve	rsion 4	Sec 192	168 43 8	Q Det	118 07 3	204 70	211.510	0 (40			•/						
	ran	smissi	on Control	Protoco	al Src Po	t: 27054	DST PO	rt · 113	Seg: 0 1	en: 0										
					,	2. 27034	,													
0000		ac 9e 1	17 †2 f9 e	B TO 03	8c 17 5d	6T 08 00	45 00	0.10	JOE.											
0020		c 46 4	69 ae 00 7	1 a6 ch	38 0d 00	ao 20 39	70 02	. U. \@	+YVa											
003	ő á	20 00 0	eb 7d 00 0	0 02 04	05 b4 01	01 04 02	10 02		· · · · · · · · · · · · ·											
1																				



• 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

57	[1:401:6] ICMP Destination Unreachable Network Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.1 -> 192.168.43.89	*
58	[1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] (TCP) 192.168.43.89:25485 -> 118.97.204.70:161	
59	[1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] (TCP) 192.168.43.89:25563 -> 118.97.204.70:161	
60	[1:401:6] ICMP Destination Unreachable Network Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.1 -> 192.168.43.89	
61	[1:401:6] ICMP Destination Unreachable Network Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.1 -> 192.168.43.89	
62	[1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.255.250:1900	
63	[1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] (TCP) 192.168.43.89:25065 -> 118.97.204.70:705	
64	[1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] (TCP) 192.168.43.89:25123 -> 118.97.204.70:705	
65	[1:401:6] ICMP Destination Unreachable Network Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.1 -> 192.168.43.89	
66	[1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.43.89:25485 -> 118.97.204.70:161	
67	[1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] (ICMP) 192.168.43.89 -> 118.97.204.70	
68	[1:384:5] ICMP FING [**] [Classification: Misc activity] [Priority: 3] (ICMP) 192.168.43.89 -> 118.97.204.70	
69	[1:1418:11] SNMP request top [**] [Classification: Attempted Information Leak] [Priority: 2] (TCP) 192.168.43.89:25563 -> 118.97.204.70:161	
70	[1:384:5] ICMP FING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.89 -> 118.97.204.70	
71	[1:384:5] ICMP FING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.89 -> 118.97.204.70	
72	[1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.89 -> 118.97.204.70	E
73	[1:384:5] ICMP FING [**] [Classification: Misc activity] [Priority: 3] (ICMP) 192.168.43.89 -> 118.97.204.70	
74	[1:384:5] ICMP FING [**] [Classification: Misc activity] [Priority: 3] (ICMP) 192.168.43.89 -> 118.97.204.70	
75	[1:384:5] ICMP FING [**] [Classification: Misc activity] [Priority: 3] (ICMP) 192.168.43.89 -> 118.97.204.70	
76	[1:401:6] ICMP Destination Unreachable Network Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.1 -> 192.168.43.89	
77	[1:384:5] ICMP FING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.89 -> 118.97.204.70	
78	[1:384:5] ICMP FING [**] [Classification: Misc activity] [Priority: 3] (ICMP) 192.168.43.89 -> 118.97.204.70	
79	[1:384:5] ICMP FING [**] [Classification: Misc activity] [Priority: 3] (ICMP) 192.168.43.89 -> 118.97.204.70	
80	[1:384:5] ICMP FING [**] [Classification: Misc activity] [Priority: 3] (ICMP) 192.168.43.89 -> 118.97.204.70	
81	[1:401:6] ICMP Destination Unreachable Network Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.1 -> 192.168.43.89	
82	[1:384:5] ICMP FING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.89 -> 118.97.204.70	
83	[1:384:5] ICMP FING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.89 -> 118.97.204.70	
84	[1:384:5] ICMP FING [**] [Classification: Misc activity] [Priority: 3] (ICMP) 192.168.43.89 -> 118.97.204.70	
85	[1:384:5] ICMP FING [**] [Classification: Misc activity] [Priority: 3] (ICMP) 192.168.43.89 -> 118.97.204.70	
86	[1:401:6] ICMP Destination Unreachable Network Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.1 -> 192.168.43.89	
87	[1:401:6] ICMP Destination Unreachable Network Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.1 -> 192.168.43.89	
88	[1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.255.250:1900	
89	[1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.255.250:1900	
90	[1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] (UDP) 192.168.43.89:1900 -> 239.255.255.250:1900	
91	[1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] (UDP} 192.168.43.89:1900 -> 239.255.255.250:1900	
92	[1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UDP} 192.168.43.89:1900 -> 239.255.255.250:1900	
93	[1:401:6] ICMP Destination Unreachable Network Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.43.1 -> 192.168.43.89	-

Gambar 2.3 Data Alert

Setelah berhasil mendapatkan alert kita melakukan compile terhadap data alert dengan alat bantu countalert.py yang dimana alat bantu tersebut merupakan tools dengan bahasa python yang berfungsi untuk mengekstrak data alert yang telah didapatkan. Setelah melakukan ekstrak didapatlah hasil dari traffic yang telah kita lakukan dengan wireshark.

3. HASIL SAJIAN DATA

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

NO	ALERT	JUMLAH
1	ICMP PING NMAP	6
2	SCAN UPnP service discover attempt	6
3	SNMP AgentX/tcp request	12
4	SNMP request tcp	12
5	ICMP PING	38
6	ICMP Destination Unreachable Network	115
7	MISC UPnP malformed advertisement	265



Gambar 3.1 Grafik alert