TUGAS JARINGAN KOMPUTER



DISUSUN OLEH :

- Nama : Dera Gustina
- Nim : 09011181419003
- Nama dosen : Dr. Deris Stiawan, M.T
- Jurusan : Sistem Komputer
- Fakultas : Ilmu Komputer

Universitas Sriwijaya

Menggunakan software wireshark dan command untuk mengetahui tentang network traffic

PENJELASAN :

Pengertian protokol : Protokol adalah aturan main yang mengatur komunikasi diantara beberapa komputer di dalam sebuah jaringan sehingga komputerkomputer anggota jaringan dan komputer berbeda platform dapat saling berkomunikasi.

Pengertian GET : Get adalah Sebuah permintaan GET mengambil data dari web server dengan menentukan parameter di bagian URL dari permintaan. Jika Anda memeriksa contoh permintaan HTTP bawah ini, kami minta index.html, dan melewati report_id parameter.

Pengertian POST : post adalah Sebuah permintaan HTTP POST memanfaatkan badan pesan untuk mengirim data ke server web.

Pengertian PUT : PUT adalah mirip dengan POST memanfaatkan badan pesan untuk mentransfer data. Namun, ada beberapa perbedaan mendasar antara keduanya. Pertama PUT dianggap idempotent, kedua tindakan seorang PUT ini selalu ditetapkan untuk URI tertentu, akhirnya PUT adalah untuk memuat data untuk sumber daya itu. Dengan kata lain Anda harus tahu lokasi yang tepat dari mana data yang Anda kirimkan akan diambil nanti.

Pengertian HEAD : head adalah HTTP Metode yang digunakan untuk mengambil informasi tentang URL dari web server.

Pengertian DELETE : Menghapus sumber daya tertentu dari web server.

Pengertian TRACE : Metode ini menggemakan kembali permintaan yang diterima sehingga klien HTTP dapat melihat apa server menengah menambahkan atau mengubah permintan.

Pengertian OPTIONS : Metode ini membantu menentukan fungsi server seperti menentukan metode mana yang mendukung web server.

Pengertian CONNECT : Metode connect mengubah Permintaan koneksi ke terowongan TCP / IP transparan. Hal ini membantu memfasilitasi Secure Socket Layer (SSL) berkomunikasi (HTTPS) melalui <u>proxy</u> HTTP yang tidak terenkripsi

Gambar dibawah ini adalah analisis cappture menganalisis traffic websate <u>www.okezone.com</u> menggunakan software wirkshark :

No. Time	Source	Destination	Protocol	Length Onfo	
842 19.166350	192.168.1.5	202.80.220.215	TCP	66 49243-80 [SYN] Seq-0 Win-8192 Len-0 MSS-1460 WS-4 SACK FERM-1	()
844 19,169840	202.80.220.218	192,168,1,5	ICH	62 80-19213 [SYN, ACK] SED 0 ACK 1 W10 4356 LED 0 MSS 1452 SACK FERM 1	
84 5 19, 169910	192.168.1.5	202.80.220.218	TCP	54 49/43 80 [ACK] Seg=1 Ack=1 Win=6:540 Len=0	
646 19.1/0242	102.168.1.5	202.80.220.218	HTTP	368 GET // HTTP/1.1	
849 19,174616	202.80.220.218	192,168,1,5	1CP	54 80-49243 [ACK] seq 1 Ack 316 win 4571 Len 0	
850 19.380433	202.80.220.218	192.168.1.5	IC H	1506 [KH segnent of a reassembled HMI]	
851 149, 681114	202.80.220.218	192.168.1.5	TCP	1506 [TCP segment of a reasonabled PD0]	
852 19.381120	202.80.220.218	192.168.1.5	TCF	251 LTCP segment of a reassembled FDO	
853 19,381152	192.168.1.5	202.80.220.218	ICP.	31 49213-80 [Ack] seq-310 Ack-3102 w1n-05340 Len-0	
8 34 19, 383121	202.80.220.218	192.168.1.5	TCP	1506 [TCP segnent of a reassembled ED0]	
855 19.383896	202.80.220.218	192.168.1.5	TCP	1508 [TCP segment of a reassembled PDU]	
856 19,383933	192.168.1.5	202.80.220.218	15.P	54 49240-80 [Ack] Seg 318 Ack 6006 win 65340 Len 0	
8.57 19, (84052	202.80.220.218	192.168.1.)	TCP	1506 [TCP segment of a reassembled PDN]	-
¥ [F.
R Frame 846: 389	bytes on wine (29	52 bits), 369 bytes	captured	(2952 bits) on interlace 0	
H Ethernet 11, SP	C: Liteonie b6:03	:07 (68:a3:c4:b6:03	:07), USC	:: zte.orpo b8:97:93 (d4:76:ea:b8:97:93)	
Internet Protect	rol Version 4, Sec	: 192.168.1.5. Dat:	202.80.2	20.218	
Transmission Co	antrol Protocol, S	int Port: 40243, Det	PUPL: 80), Seg: 1, Ack: 1, Lun: 315	
H Hypertext Inans	ter Protocol				

0000	d4 76 ea b8 97 93 68 a3	c4 b6 03 07 08 00 45 00	.vhE.	
0010	01 63 66 05 40 00 80 06	Ba b7 c0 a8 01 05 ca 50	. C @ P	100
0020	dc da c0 3b 00 30 8e 33	b4 fa ee 38 cc fa 50 18	[. P. 5 8 P.	
0030	ff 3c Of Gc 00 00 47 45	54 20 2f 20 48 54 54 50	. K.T. GET / HITP	1.3
CH 14()	2f \$1 2e \$1 0d Ha 48 (f	73 74 3a 20 6f 6h 65 7a	/1.1. Ho st: pkez	1
CHI NO	6f 6r 65 2r 58 0f 5d 0d	0a 55 73 65 77 2d 41 67	one.comliser Ag	
0060	65 60 /4 3a 20 4d 6f /a	69 OC 60 01 21 35 20 30	ont: Mpz (11a/5.0	
0070	20 28 57 69 8e 64 61 77	73 20 4c 54 20 36 2c 31	(Window 5 NT 6.1	
0080	3b 20 57 41 57 36 34 3b	20 72 76 3a 34 38 2e 30	: W0W64: rv:45.0	
0090	29 20 47 65 63 6b 6t 2t	32 30 31 30 30 31 30 31) Gecko/ 20100101	
00a0	20 48 69 72 85 66 81 78	2t 34 36 2e 30 0d 0a 41	Firefox /18.0	
00b0	63 63 65 70 74 3a 20 74	65 78 74 2f 68 74 66 6c	ccent: r ext/hrm]	
0000	2c 61 70 70 6c 69 63 61	74 G9 OF Ge 2f 78 G8 74	applica tion/sht	
(Hido)	6d 6c 2b 78 6d 6c 7c 61	70 70 br 69 53 61 74 69	ml xnl.a policati	*

Okezone.com

8472 28.065793 192.168.1.5	202.80.220.218	ICP.	1306 Lick segment of a reassembled HUU
8474 28.065282 182.168.1.5	202.80.220.218	TCP	1 x0E [TCP sequent of a reassembled PDU]
84/4 28.065/09 102.168.1.5	202.80.220.218	TCP	1506 [TCP segment of a reassenbled PDU]
8475 28.065801 192.168.1.5	202.80.220.218	HTTP:	221 POST /ngx pagespeed beacon?orl=http%34%2F%2Fokezone.com%2F HTTP/1.1 (application/x-www-lorm-orlenc
8477 28.071333 202.80.220.218	192.168.1.3	ICP.	31 80-19213 [ALK] seg-139509 ALK-8932 win-13307 Len-0
8478 28.080750 207.80.220.218	192.168.1.5	TCP	54 80549743 [ACK] Segel39509 Ack=11856 Win=16711 Len=0
\$479 28.081222 202.80.220.218	102.168.1.5	TCP	54 80-49243 [ACK] Seg-139569 Ack-12023 Win-16378 Len=0
8485 28,153328 202,80,220,218	192,168,1,5	III I P	364 III (P/1, 1 204 No Content
8493 78.351945 197.168.1.5	202.80.220.218	ICH.	51 19213-60 [At K] Seq-12023 Ack-139879 win-55310 Len-0
*KRIX 48.157449 197.168.1.5	202.80.220.218	TCP	55 [TCP keep Alive] 49243 80 [ACK] Seg=12022 Adl=139829 Win=55340 Line=[Reasonably minus, protocol TCP
9009 38.160229 202.80.220.218	192.165.1.5		54 [TCP Keep-Alive ACK] 80-49243 [ACK] Seq-139879 Ack-12023 Wim-16378 Len-0
9270 48.154734 192.168.1.5	202,80,220,216	JICH:	55 [ICF Keep-Alfve] 45240-80 [ACK] Sep 12022 Ack 139879 win 65040 Len 1[Keassembly error, protocol ICF
9271 48.155907 202.80.220.218	192.108.1.5	TCP	54 [TCP Reep Alive ACR] 88 49/43 [ACR] Seg-1498/9 Ack-12023 Win-163/8 Len=0
(1) ···			11

Okezone.com

Sueam Content	
<pre>GET / HTTP/1.1 Host: okezone.com User-Agent: Mozilla/5.0 (windows NT 6.1; wow64; rv:48.0) Gecko/20100101 Firefox/48. Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;g=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Upgrade-Insecure-Requests: 1</pre>	0
HTTP/1.1 200 OK Server: OKZ-LB-SRVCS Date: Mon, 19 Sep 2016 11:45:14 GMT Content-Type: text/html; charset=UTF-8 Vary: Accept-Encoding Pragma: no-cache X-Page-Speed: 1.11.33.0-0 Cache-Control: max-age=0, no-cache, no-store X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Link: <http: okezone.com=""></http:> ; rel="canonical" Connection: Keep-Alive Set-Cookie: ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A% 2246e7c6cd9c1a72d838808c3fa42c0480%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A13%3A% 22192.168.3.199%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A72%3A%22Mozilla%2F.0+%28windd +NT+6.1%3B+W0%64%3B+rv%3A48.0%294Gecko%2F20100101+Firefox%2F48.0%22%3Bs%3A13%3A% 221ast_activity%22%3Bi%3A1474285514%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3Bs% 705923865ea2c494eca649041ccfc7397c; expires=Mon, 19-Sep-2016 13:45:14 GMT; Max- Age=7200; path=; domain=.okezone.com Set_Cookie: PHPSE5STD=vv&rb09ab3kcl3ieiminn?vcv3: path=/	ws
٠ <u> </u>	•
Entire conversation (189877 bytes)	1
	aw
Find Save As Print O ASCII O EBCDIC O Hex Dump O C Arrays @ F	

Sotware Wireshark memiliki kemampuan untuk menangkap lalu lalang kegiatan yang terjadi pada jaringan milik kita. Selain itu juga bisa mem-filter protokol lain selain ICMP, seperti HTTP dan lain-lain.

Panel pertama merupakan daftar dari data packet yang telah dicapture. Biasanya diurutkan berdasarkan waktu. Panel ini berisi no packet, waktu saat packet di capture, tujuan dan sumber dari packet, protocol yang digunakan dan panjangnya. Hasil yang difilter merupakan hasil dari filter dari packet yang berisi method 'GET'.

Panel ini berisi detail data dari packet yang dipilih di daftar packet. Di baris pertama terdapat frame 93 yang pada umumnya berisi data dari waktu dan panjang paket. Baris Kedua yang terdapat tulisan Ethernet II berisi informasi hardware dari pengirim dan penerima paket. Baris Ketiga berisi versi Internet Protocol. Dari screenshot diatas terlihat IP yang digunakan IPv4 dan jug terlihat IP pengirim dan penerima. Baris Keempat berisi Transmission Control Protocol, ini berisi daftar port pengirim dan port penerima dan flag yang diset untuk paket yang menandakan apakah paket itu sekuensial atau request acknowledgment. Baris Kelima berisi Hyper Text Transfer Protocol yaitu packet tersebut menggunakan protocol HTTP.

Panel ketiga merupakan Bytes dari paket. Panel ini berisi data yang diterima atau dikirim dalam bentuk hexadecimal. Karena kita tidak bisa membaca hexadecimal secara langsung maka dibagian kanan dari data hexadcimal terdapat 'terjemahan'nya.

Ip yang ada pada komputer saya adalah 192.168.1.5 dan ip destination adalah 202.80.220.218 . Terlihat bahwa respon server terhadap Method GET tersebut adalah OK dan pada bagian bawahnya berisi element website tersebut dengan bahasa html, Namun tidak ditemukan Methode POST maupun RESPONS. Pada method POST sendiri, Permintaan POST digunakan untuk mengirim data ke server, misalnya, informasi pelanggan, file upload, dll menggunakan bentuk HTML sedangkan dalam kasus ini hanya ditugaskan untuk mengunjungi sebuah situs kemudian dicapture dan method POST tidak terbaca karena kita tidak melakukan login,search pada website maupun login ke website tersebut. Sedangkan untuk method RESPONS dapat dilihat pada bagian GET yang didalamnya merupakan respon dari server yang dituju dalam kasus ini jika website berhasil dikunjungi maka akan menghasilkan RESPONS OK.

Selain menggunakan software wirshark analisis yang saya gunakan juga menggunakan commad promnt dimana hasilnya adalah sebagai berikut :

es. Admini	strator: C:\Windows\system32\ci	md.exe		
Microsof	ft Windows [Version 6.	1.76001		
Copyrig	ht (c) 2009 Microsoft	Corporation. All rights	reserved.	
C:\User:	s\user>netstat −a			
Active (Connections			
Proto	Local Address	Foreign Address	State	-
TCP	0.0.0.0:135	user-PC:0	LISTENING	
TCP	0.0.0.0:445	user-PC:0	LISTENING	
TCP	0.0.0.0:554	user-PC:0	LISTENING	
TCP	0.0.0.0:2869	user-PC:0	LISTENING	
TCP	0.0.0.0:10243	user-PC:0	LISTENING	
TCP	0.0.0.0:49152	user-PC:0	LISTENING	
TCP	0.0.0.0:49153	user-PC:0	LISTENING	
TCP	0.0.0.0:49154	user-PC:0	LISTENING	
TCP	0.0.0.0:49155	user-PC:0	LISTENING	
TCP	0.0.0.0:49156	user-PC:0	LISTENING	
TCP	0.0.0.0:49161	user-PC:0	LISTENING	
TCP	127.0.0.1:5354	user-PC:0	LISTENING	
TCP	127.0.0.1:5354	user-PC:49157	ESTABLISHED	
TCP	127.0.0.1:5354	user-PC:49159	ESTABLISHED	
TCP	127.0.0.1:6543	user-PC:0	LISTENING	
TCP	127.0.0.1:27015	user-PC:0	LISTENING	
TCP	127.0.0.1:27015	user-PC:49158	ESTABLISHED	
TCP	127.0.0.1:49157	user-PC:5354	ESTABLISHED	
TCP	127.0.0.1:49158	user-PC:27015	ESTABLISHED	
TCP	127.0.0.1:49159	user-PC:5354	ESTABLISHED	
TCP	169.254.100.44:139	user-PC:0	LISTENING	
TCP	192.168.1.5:139	user-PC:0	LISTENING	
TCP	192.168.1.5:49160	ip-203-124-98-19:http	ESTABLISHED	
TCP	192.168.1.5:49166	29:http	TIME WAIT	
TCP	192.168.1.5:49167	ec2-52-24-117-193:http	D TIME WAIT	
TCP	192.168.1.5:49168	112:http	TIME WAIT	
TCP	192.168.1.5:49170	ocsp:http	TIME WAIT	
TCP	192.168.1.5:49171	sa-in-f93:https	TIME WAIT	
TCP	192.168.1.5:49172	sa-in-f101:http	TIME WAIT	
TCP	192.168.1.5:49173	sin04s09-in-f14:https	TIME WAIT	
TCP	192.168.1.5:49175	server-54-230-159-210:	https TIME WAL	IT
TCP	192.168.1.5:49181	kul06s14-in-f4:https	TIME WAIT	
TCP	192.168.1.5:49183	20:https	TIME WAIT	
TCP	192.168.1.5:49184	a23-15-155-27:http	TIME WAIT	
TCP	192.168.1.5:49185	a23-15-155-27:http	TIME WAIT	
TCP	192.168.1.5:49186	20:https	TIME WAIT	
TCP	192.168.1.5:49187	server-54-230-159-112:	https TIME WAL	IT
TCP	192.168.1.5:49190	sb-in-f100:http	TIME WAIT	
TCP	192.168.1.5:49191	kul01s11-in-f3:http	TIME WAIT	
TCP	192.168.1.5:49192	kul01s11-in-f3:https	TIME WAIT	
TCP	192.168.1.5:49193	sa-in-f132:https	TIME WAIT	
TCP	192.168.1.5:49194	sb-in-f94:https	TIME_WAIT	
TCP	192.168.1.5:49195	sa-in-f94:https	TIME WAIT	
TCP	192.168.1.5:49196	sb-in-f102:https	TIME WAIT	
TCP	192.168.1.5:49197	sa-in-f100:https	TIME WAIT	
TCP	192.168.1.5:49198	sin04s05-in-f174:https	S TIME WAIT	
TCP	192.168.1.5:49201	104.25.11.6:https	CLOSE WAIT	
TCP	192.168.1.5:49202	10:http	ESTABLISHED	
TCP	192.168.1.5:49203	114:http	TIME_WAIT	*

C:4.	Administ	rator: C:\Windows\system32\cmd.e	exe	These regula	r sale		
	Administ ICP ICP ICP ICP ICP ICP ICP ICP ICP ICP	ator: C:\Windows\system32\cmd. 192.168.1.5:49201 192.168.1.5:49203 192.168.1.5:49203 192.168.1.5:49205 192.168.1.5:49206 192.168.1.5:49207 192.168.1.5:49207 192.168.1.5:49210 192.168.1.5:49211 192.168.1.5:49213 [::]:48.1.5:49213 [::]:445 [::]:554 [::]:2869 [::]:49153 [::]:49154 [::]:49155 [::]:49154 [::]:49155 [::]:49156 [::]:49156 [::]:49156 [::]:49157 0.0.0.0:500 0.0.0.0:500 0.0.0.0:5005 0.	Xe 104.25.11.6:http 114:http 114:http 114:http 36.86.63.180:htt 106:http 114:http 106:http 114:http 104.16.90.188:ht user-PC:0 user-PC:0 user-PC:0 user-PC:0 user-PC:0 user-PC:0 user-PC:0 user-PC:0 user-PC:0 user-PC:0 user-PC:0 user-PC:0 user-PC:0 user-PC:0 user-PC:0 user-PC:0 user-PC:0 user-PC:0 user-PC:1 user-PC:0 user-PC:1 user	ps ty ttp	CLOSE_WAIT ESTABLISHED TIME_WAIT ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED ESTABLISHED LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING LISTENING STABLISHED ESTABLISHED ESTABLISHED		
	IDP IDP IDP IDP	[::]:56138 [::]:61561 [::]:62342	*:*			+	
	IDP IDP IDP IDP IDP IDP IDP IDP IDP IDP	[::]:500 [::]:4500 [::]:5004 [::]:5355 [::]:5355 [::]:53162 [::]:6138 [::]:61561 [::]:62342 [::]:65431 [::1]:1900 [::1]:56945 [fe80::282f:bc60:98fd: [fe80::943a:b5d8:a476:	*:* *:* *:* *:* *:* *:* *:* *:* *:* *:*	***********			
::\	:\Users\user>						

Pada hasil capture diatas command yang dugunakan yaitu "netstat –a" dan muncul tampilan seperti diatas. Cara membaca hasil capture menggunakan

command netstat –a adalah melihat Local Address yang merupakan IP Address komputer kita sendiri atau merupakan source dan untuk Destination dapat dilihat pada bagian Foreign Address. Sedangkan untuk state merupakan keadaan dari proses lalu lintas data tersebut misalkan listening dapat diartikan menunggu respon user, time wait merupakan proses menunggu respon dari destination.

```
Administrator: C:\Windows\system32\cmd.exe
                                                                                                Windows IP Configuration
Ethernet adapter Bluetooth Network Connection 4:
   Media State . . . . . . . . . . Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wireless Network Connection 2:
   Media State . . . . . . . . . . Media disconnected
Connection-specific DNS Suffix . :
Vireless LAN adapter Wireless Network Connection:
   fe80::943a:b5d8:a476:1648%12
192.168.1.5
255.255.255.0
fe80::1%12
192.168.1.1
                                                  -
Ethernet adapter Local Area Connection:
    Media State .
                                                   : Media disconnected
   Ethernet adapter VirtualBox Host-Only Network:
   Connection-specific DNS Suffix .:
Link-local IPv6 Address . . . . : fe80::282f:bc60:98fd:642c%16
Autoconfiguration IPv4 Address. . : 169.254.100.44
Subnet Mask . . . . . . . . . : 255.255.0.0
Default Gateway . . . . . . . . :
Tunnel adapter isatap.{7C1DB121-1DE9-459E-8592-7BF93B15D4FE}:
   Media State . . . . . . . . . . Media disconnected
Connection-specific DNS Suffix . :
Tunnel adapter isatap.{4F02C20E-C80F-4948-A38C-23C2431F3672}:
                                                  : Media disconnected
    Media State .
   Media State .
Connection-specific DNS Suffix .
Tunnel adapter isatap.{FBB06F33-B825-440F-AF31-E5C4ABC8E2EC}:
   Media State . . . . . . . . . . Media disconnected
Connection-specific DNS Suffix . :
Tunnel adapter Teredo Tunneling Pseudo-Interface:
   Connection-specific DNS Suffix . :
IPv6 Address. . . . . . . . . . : 2001:0:2456:3fb4:1031:3f80:3f57:fefa
Link-local IPv6 Address . . . . : fe80::1031:3f80:3f57:fefa%21
Default Gateway . . . . . . . : ::
```

Gambar diatas adalah gambar ip yang ada pada komputer yang saya gunakan