Tapping Login Website Menggunakan Wireshark Tugas 3 Keamanan Jaringan Komputer



Oleh : Muhammad Fikri Rabbani 09011181621013 Kelas : SK8P Indralaya Dosen pengampu : Deris Stiawan, M.T., Ph.D.

> Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya

1. Tapping Website

a. Website Http (unsecured)

a. Contoh wesite yang tidak menggunakan http

← → ♂ ŵ	🛈 🔏 aavtrain.com/index.asp
Aavirain	Testing Center
Main Menu	
cogni roge	Test Login
	That User Name/Password combination is not in our database. Please try again.
Visit us at the Pilot's Toolbox for flight training and aviation tools	This test center is only for students who have been given access by CFI's using the <u>CFI Toolbox ground school system</u> .
	Username: Password: Submit Submit First Time Students Register Here Contact your instructor if you have forgotten your password.

b. Input data ke dalam kolom username dan password (tidak masalah data valid atau tidak).

Test Login												
That User Name/Password combination is not in our database. Please try again.												
This test center is only by CFI's using th	y for students who have been given access e <u>CFI Toolbox ground school system</u> .											
Username:	First Time Students Register Here											
Password:												
Submit	Contact your instructor if you have forgotten your password.											

- c. Jalankan Capture Wireshark terlebih dahulu sebelum menekan "submit"
- d. Lalu hentikan capture wireshark.
- e. Lakukan analisis terhadap packet yang telah di capture. Pertama filter packet http menggunakan "http.request.method==post".

h	http.request.method == POST														
No. Time		Time	Source	Destination	Protocol	I									
+	127	14.563433	192.168.10	192.185.11.183	HTTP										

f. Pada bagian info akan terdapat tulisan .login atau /login. Atau dalan kasus ini /index.asp. Kemudian klik kanan pada packet tersebut lalu follow > tcp stream.

Protocol	Le	ngth				Info		
HTTP					665	POST	/index.as	sp HT1
	<u>M</u> ark/Unma	irk Packet						
	lgnore/Unig	nore Packet						
	Set/Unset T	ime Reference						
	Time Shift							
	Packet Com	iment						
	Edit Resolve	d Name						
	Apply as Filt	ter	۲					
	Prepare a Fi	lter	•					
	Conversatio	n Filter	•					
	Colorize Co	nversation	•					
	SCTP		۰.					
	Follow		•	٦	TCP Str	eam		
	Conv		•	l	UDP St	ream		
	сору			1	TLS Str	eam		
	Protocol Pre	eferences	•	I	нттр s	tream		
	Decode <u>A</u> s							
	Show Packe	t in New <u>W</u> indow	,					

g. Selanjutnya akan muncul window sebagai berikut. Username dan password akan tampil dengan jelas dalam text tersebut.



b. Website Https (secured)

a. Tampilan TCP stream ketika melakukan login ke website yang terenkripsi.



Gambar 1 Data capture yang ditampilkan hanya akan nampak seperti susunan karakter yang acak, sehingga tidak dapat dibaca oleh attacker.

2. Akses Web Melalui Tor

a. Jalankan Tor Browser dan pastikan sambungan berhasil.



- b. Mulai capture packet menggunakan Wireshark.
- c. Pergi ke web yang diinginkan, misalnya facebook atau google.
 - facebook.com [157.240.25.35]
 - google.com [216.239.38.120]
 - komputer lokal [192.168.100.14]

	Facebook - Lo	g In or Sign Up 🛛 🗙	G Google	× +			- 0	×
٥	↔ ↔ ♥	🛈 🔒 https://ww	w.google.com				··· ☆ S	≡
						Gmail Bilder	Anmelden	
				Goo	gle			
			1					
				Google-Suche	Auf gut Glück!			
	Österreich							
,	Werbeprogramme	Unternehmen	Über Google		Datenschutzerklärung	Nutzungsbedingungen	Einstellunger	ı
Meł	Cookies helfen uns nr erfahren ок	bei der Bereitstellu	ng unserer Dienste	e. Durch die Nutzung unsere	er Dienste erklärst du dich damit einv	rerstanden, dass wir Cook	ties setzen.	

d. Analisis hasil capture.

_

Fil	ter "ip.	src == 192	2.168.100.14	&& ip.dst	== 157.24	40.25.35"							
4	*Wi-Fi						-		×				
File	Edit View	Go Capture Anal	yze Statistics Telephony	Wireless Tools He	lp								
		S 🕅 🔀 🖾 🔍 🧉		0,0,0,1									
Implicit Implicit													
No.	Time	Source	Destination	Protocol	Length	Info							
<									>				
•	wireshark_	Wi-Fi_20190311201130_	a07776.pcapng		Packets: 24	39 · Displayed: 0 (0.0%) · I	Dropped: 0 (0.0%)	Profile: Def	ault				

Gambar 2 Tidak ada packet dari komputer lokal yang dikirimkan langsung ke IP facebook

- Filter "ip.src == 192.168.100.14 && ip.dst == 216.239.38.120"

🚄 *Wi-Fi – 🗆	
	\times
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help	
🗸 🔳 🗷 🐵 📘 🐘 🕱 🖻 🔍 👳 🗠 🕾 🗿 🖳 🧮 🔍 🔍 🗮	
📕 jp.src == 192.168.100.14 & (p.dst == 216.239.38.120)	n +
No. Time Source Destination Protocol Length Info	
<	>
Wireshark_Wi-Fi_20190311201130_a07776.pcapng Profile: [efault 🔡

Gambar 3 Begitu pula sambungan ke IP google

- e. Perbandingan menggunakan browser biasa.
 - Filter "ip.src == 192.168.100.14 && ip.dst == 157.240.25.35"

_																			_
	*Wi-Fi															-		×	
Fil	e Edit	View G	io Captu	re Analyze	e Statis	stics	Telephony	Wirel	ess Too	ls Help	,								
		0	🔝 🗙 🖸	9.0	2 چ			⊕ (a a T	ī .									
	0.src == 192.168.100.148 & in det == 157.240.25.35															+			
-	prore	102/100/10	ion i n didriph		10120100	4					_			1					_
No.	Т	Time	Source			Destin	ation		Protoco		Len	ngth		Info					^
	935 1	L2.609769	192.1	58.100.14		157.3	240.25.3	5	TCP				66	36171 → 443	[SYN]	Seq=0	Win=6553	15	
	943 1	12.638992	192.1	58.100.14		157.	240.25.3	5	TCP				54	36171 → 443	[ACK]	Seq=1	Ack=1 W	.r	
	944 1	12.639067	192.1	58.100.14		157.3	240.25.3	5	TLSv1	2			259	Client Hell	0				
	954 1	L2.655503	192.1	58.100.14		157.3	240.25.3	5	TCP				66	36173 → 443	[SYN]	Seq=0	Win=6553		
	963 1	12.664113	192.1	58.100.14		157.3	240.25.3	5	TCP				66	36177 → 443	[SYN]	Seq=0	Win=6553		
	970 1	12.668712	192.1	58.100.14		157.3	240.25.3	5	TCP				54	36171 → 443	[ACK]	Seq=20	6 Ack=14	11	
	974 1	12.670912	192.1	58.100.14		157.3	240.25.3	5	TCP				54	36171 → 443	[ACK]	Seq=20	6 Ack=28	12	
	976 1	12.671205	192.1	58.100.14		157.3	240.25.3	5	TCP				54	36171 → 443	[ACK]	Seq=20	6 Ack=3	95	
	989 1	12.684162	192.1	58.100.14		157.3	240.25.3	5	TCP				54	36173 → 443	[ACK]	Seq=1	Ack=1 W	r	
	992 1	12.684904	192.1	58.100.14		157.3	240.25.3	5	TLSv1	2			255	Client Hell	0				
	1002 1	12.690391	192.1	58.100.14		157.3	240.25.3	5	TLSv1	2			180	Client Key	Exchan	ge, Cha	nge Cip	ie	
	1003 1	12.690886	192.1	58.100.14		157.3	240.25.3	5	TLSv1	2			141	Application	Data	-			
	1004 1	12.691089	192.1	58.100.14		157.3	240.25.3	5	TLSv1	2			413	Application	Data				
	1006 1	12.693591	192.1	58.100.14		157.3	240.25.3	5	TCP				54	 36177 → 443	[ACK]	Seg=1	Ack=1 W	lr .	
	1008 1	12.694298	192.1	58.100.14		157.3	240.25.3	5	TLSv1	2			252	Client Hell	0				
	1028 1	2.719613	192.1	58.100.14		157.	240.25.3	5	TCP				54	36173 → 443	ГАСК1	Sea=20	2 Ack=14	1	
	1030 1	2.719842	192.1	58.100.14		157.	240.25.3	5	TCP				54	36173 → 443	[ACK]	Sea=20	2 Ack=28	2	~
<																	3	•	
>	Frame	935: 66 b	ovtes on	wire (528	bits)	, 66	bytes ca	ptured	(528 b	ts) on	inter	face 0							^
>	Ethern	et II, Sr	c: Liteo	nTe 9d:ce	:e9 (5	8:00:	e3:9d:c6	:e9), I	Ost: Hua	weiTe 0	02:ad:	95 (c0:70:09:0	2:ad	:95)					
>	Intern	et Protoc	col Versi	on 4, Sro	: 192.	168.1	.00.14, D	st: 15	7.240.25	.35									¥
00	00 c0	70 09 02	ad 95 5	800 e3	9d c6 e	e9 08	00 45 0	0 · p·	· · · x · ·	· · · · E ·									^
00	10 00	34 5e 76	40 00 8	006 c0	83 c0 a	a8 64	0e 9d f	0 .4	v@····	· · · d · · ·									
00	20 19	23 8d 4b	01 bb c	8 f8 97	b3 00 (00 00	00 80 0	2 •#•	к	• • • • • • •									¥
C) 🝸 w	/ireshark_Wi	-Fi_2019031	1202110_a2	0616.pca	png						Packets: 2011 · Disp	blayed	d: 147 (7.3%) · D	ropped: () (0.0%)	Profile: D	efault	

Gambar 4 Capture packet saat mengakses facebook melalui Microsoft Edge

- Filter "ip.src == 192.168.100.14 && ip.dst == 216.239.38.120"

_																			
	(*	Wi-Fi															-		×
F	ile	Edit	View	Go	Capture	Analyze	Statist	ics Te	elephony	Wireles	s Tools	Help							
		đ	0	010		۹ 👄 🖨) 🖭 (î 4		Θ.Θ	Q. 🎹								
			102,100	100.1	4 0 0 in dat	- 216 220												vorcesion	
Ľ	(Jip.	.src ==	192, 100.	. 100. 1	H aa ip.ust	== 210,239	.38.120											xpression	
N	0.	т	me		Source		0	Destinat	ion		Protocol		Length		Info				^
		402 2	.98334	8	192.168	.100.14	2	216.23	9.38.12	0	TCP			54	36151 → 443	[ACK]	Seq=1740	Ack=71	_
		403 2	.98343	0	192.168	.100.14	2	216.23	9.38.12	0	TLSv1.2			100	Application	Data			
		405 3	.15398	5	192.168	.100.14	2	216.23	9.38.12	0	TLSv1.2			184	Application	Data			
		408 3	.18789	4	192.168	.100.14	2	216.23	9.38.12	0	TCP			54	36151 → 443	[ACK]	Seq=1916	Ack=71	
		410 3	.18800	4	192.168	.100.14	2	216.23	9.38.12	0	TCP			54	36151 → 443	[ACK]	Seq=1916	Ack=71	
		412 3	.18855	4	192.168	.100.14	2	216.23	9.38.12	0	тср			54	36151 → 443	[ACK]	Seq=1916	Ack=71	
		413 3	.18875	8	192.168	.100.14	2	216.23	9.38.12	0	TLSv1.2			100	Application	Data			
		415 3	.43582	4	192.168	.100.14	2	216.23	9.38.12	0	TLSv1.2			323	Application	Data			
		418 3	.468814	4	192.168	.100.14	2	216.23	9.38.12	0	TCP			54	36151 → 443	[ACK]	Seq=2231	Ack=71	
		420 3	.46938	3	192.168	.100.14	2	216.23	9.38.12	0	TCP			54	36151 → 443	[ACK]	Seq=2231	Ack=71	
		422 3	.46964	0	192.168	.100.14	2	216.23	9.38.12	0	TCP			54	36151 → 443	[ACK]	Seq=2231	Ack=71	_
		423 3	.46970	5	192.168	.100.14	2	216.23	9.38.12	0	TLSv1.2			100	Application	Data			
		424 3	.52458	8	192.168	.100.14	2	216.23	9.38.12	0	TLSv1.2			595	Application	Data			
		428 3	.55489	7	192.168	.100.14	2	216.23	9.38.12	0	TCP			54	36151 → 443	[ACK]	Seq=2818	Ack=71	
		430 3	.55501	7	192.168	.100.14	2	216.23	9.38.12	0	TCP			54	36151 → 443	[ACK]	Seq=2818	Ack=72	
		432 3	. 55547	2	192.168	.100.14	2	216.23	9.38.12	0	TCP			54	36151 → 443	[ACK]	Seq=2818	Ack=72	
		433 3	.55654	2	192.168	.100.14	2	216.23	9.38.12	0	TLSv1.2			100	Application	Data			~
<																		>	
)	Fr	rame 4	33: 10	00 by	tes on w	/ire (800	bits)	, 100	bytes d	aptured	(800 b	its) on	interface	0					^
>	E	therne	t II,	Src:	LiteonT	e 9d:c6:e	9 (58	:00:e3	3:9d:c6:	e9), Ds	t: Huaw	i⊺e 02	:ad:95 (c0:	70:09:02:ad	:95)				
>	I	nterne	t Prot	ocol	Version	4, Src:	192.1	68.100	0.14, Ds	t: 216.	239.38.	120							¥
6	0000) c0	70 09	02 a	d 95 58	00 e3 9d	c6 e9	9 08 0	0 45 00	· p· ·	· · X · · · ·	•••E•							^
0	0010	00	56 5d	24 4	0 00 80	06 79 5f	c0 at	8 64 0	e d8 ef	·v]\$	@··· y_	٠d٠٠٠							
6	9020	26	78 8d	37 0	1 bb 97	22 ba 2e	52 73	2 0d 6	50 18	&x∙7	····	ln•o <mark>P</mark> •							~
(0	7 w	ireshark_	Wi-Fi_	201903112	02110_a206	16.pcap	ng					Packets: 2	2011 · Displayed:	202 (10.0%) · Dr	opped: 0	(0.0%)	Profile: De	fault 🔡

Gambar 5 Capture packet dengan mengakses google menggunakan browser yang sama, terlihat bahwa packet akan dikirimkan langsung dari komputer lokal ke google