Project 17: NetWitness (15 pts.)

Kebutuhan Project

Komputer Windows. Pada tutorial ini menggunakan Windows 7 virtual machine.

Menginstal NetWitness

- 1. Buka browser dan arahkan ke http://www.emc.com/security/rsa-netwitness.htm#!freeware
 - a. Click "Download NetWitness Investigator Freeware"
 - b. Isi form dan click **Submit**. Bisa di download juga di elearning
 - c. Download file NwInvestigatorSetup.exe dengan ukuran (131 MB).
 - d. Install software dengan default options.
 - e. Buka desktop, double-click icon "NetWitness Investigator 9.6".
 - f. Jendela "NetWitness Investigator 9" terbuka. Kotak pop up, berisi pesan "Revocation information for the security certificate for this site is not available...".
 - g. Click Yes untuk mem-bypass pesan.
 - h. Isi form registrasi.
 - i. Check email untuk product activation code. Ikuti instruksi di email untuk mengaktifkan NetWitness.
 - j. NetWitness sekarang sudah aktif, seperti berikut:



k. Tutup tab Register.

Menginstal Wireshark

- 2. Jika di komputer belum ada Wireshark, bisa di download di http://www.wireshark.org/
- 3. Jalankan Wireshark. Pilih network adapter yang terkoneksi ke Internet

Mengumpulkan Evidence

4. Open a Web browser and do these things:

- a. Go to <u>http://id.wikipedia.org/</u> and log in with the user name **Fccf** and a password of **foresec**
- b. Pada Wikipedia, masuk ke Portal Sumatera dan loading halaman mengenai portal Sumatera.
- C. Buka halaman: <u>http://elearning.binadarma.ac.id.</u>
- d. Stop packet capture. Simpan file packet capture dengan nama **YOURNAME** dan jenis file gunakan "**Wireshark/tcpdump**/ ... -libpcap (*.pcap)", seperti berikut:



Mengimport Evidence ke NetWitness

- 5. Di NetWitness, dari menu bar, click Collection, "New Local Collection".
 - a. Masukkan Collection Name berupa **YOURNAME** (gunakan nama masing-masing, seperti berikut:

New Local Col	lection	×
Local Collection		
Collection Name	YOURNAME	
	Override Default Location	
	$C: \label{eq:c:Vers} to the the the the the the the the the the$	•••
	Lock Collection	
	Auto Connect	
	ОК Сан	ncel

- b. Click OK
- C. Pada panel kiri NetWitness, double-click YOURNAME seperti berikut:

NetWitness Investigator 9								
: <u>C</u> ollection <u>E</u> dit <u>V</u> iew	<u>B</u> ookmarks <u>H</u> istory	y <u>H</u> elp						
All Data		NetWitness Investigator						
Collection	-	🕶 🕂 🗙 🎨 Welcome 💽						
Name	Status							
Demo Collection	-	Getting Started						
YOURNAME	-	Getting Started Simply double elisibility						
		Broadcast Yourself						

- d. Status harus memperlihatkan "Connecting", dan setelah beberapa detik, berubah menjadi "Ready".
- e. Di NetWitness, dari menu bar, click Collection, "Import Packets".
- f. Arahkan ke file YOURNAME.pcap dan double-click it.
- g. Status field memperlihatkan progress--, 1%, kemudian 99%, kemudian Done.

Menganalisis Evidence

- 6. Pada Collections pane NetWitness, double-click kembali YOURNAME.
 - a. Report muncul, memperlihatkan daftar jenis trafik, seperti berikut.



- b. Items memperlihatkan shown below:
 - Tab Collections Tab
 - Tombol Toggle Timeline memperlihatkan grafik data
 - **Drill Path** memperlihatkan filters yang digunakan untuk menghilangkan data yang tidak penting—data yang akan kita cari pada YOURNAME collection.
 - Pada Report, pasangan entries muncul: Value diikuti dengan nomor Sessions di parentheses, missal DHCP (2).

	Drill Path	
Toggle Tim	leline	
Collections Tab	NetWitness Investigator 9	
	<u>Collection</u> Edit <u>View</u> Bookmarks <u>H</u> istory elp	Value
	All Data YOURNAME	Value
	🐻 🚧 Welcome 💿 🧶 YOURNAME 😱	
	<u>9</u> < 2013-04-17 09:25	
	Service Type (6 items) DNS (236) - HTTP (59) - OTHER (46) - SSL (3) - NETBIOS (2) - DHCP (2)	
	Hostname Aliases (20 of 107+ items) wikipedia-lb.eqiad.wikimedia.org (28) - upload.wikimedia.org (12) - bits.wikimedi ytimg.l.google.com (2) - www3.l.google.com (2) - www.gstatic.com (2) - wikidata- e5903.g.akamaiedge.net (2) - clients.l.google.com (2) - cdn.syndication.twimg.co	Sessions

- C. Click tombol Toggle Timeline memperlihatkan Timeline, seperti berikut.
- d. Timeline memperlihatkan traffic dalam bentuk grafik, dan bisa digunakan untuk meperlihatkan dalam interval waktu tertentu. Dalam project ini toggle timeline tidak digunakan, jadi click tombol **Toggle Timeline** lagi untuk menyembunyikannya.

😧 NetWitness Investigator 9 📃 📼 🗶								
: <u>⊂</u> ollec	tion	Edit View Bookmarks History Help						
All Data		YOURNAME	00	2				
6	isi Wel			4 Þ ×				
	22	🗉 123 abc 1 👪 🧰 🖳 🖓 🏹 🍋 拱 拱 🤿 🖒 🔗						
tion T	ime C	Graph of Session Traffic		a 🔽 📭				
		7.5						
ž	2							
sinr		5						
ě	1	2.5						
	< 201	0 3-05-08 00:07		2013-05-08 00:08 >				
Į	Service Type (4 items) HTTP (14) - SSL (2) - DNS (2) - OTHER (2)							
c	Hostname Aliases (6 items) elearning.binadarma.ac.id (7) - upload.wikimedia.org (6) - microsoft secure server authority (2) - urs.microsoft.com.nsatc.net (1) - meta.wikimedia.org (1) - id.wikipedia.org (1)							
	Source IP Address (3 items) 10.0.2.15 (18) - 208.80.154.225 (1) - 208.80.154.224 (1)							
ŗ	-ll-	Dectination IP address (7 items)		×				
Click to q	juery fo	or all sessions that have this meta		CAP .::				

Mencari Wikipedia Login

- 7. Pada bagian Report, pada bagian atas berjudul "Service Type", click link biru HTTP.
 - a. Filter ini mengeluarkan semua non-HTTP traffic. Perhatikan Drill Path berubah menjadi "YOURNAME > HTTP", seperti berikut:



- b. Setengah bagian jendela sebelah kanan memperlihatkan Log panel yang kosong. Jika kita memiliki log files di dalam collection, hal ini akan sangat membantu, akan tetapi dalam kasus ini data hanya berisi file PCAP tanpa logs, jadi panel ini tidak membantu.
- **C.** Pada bagian Report, pada bagian judul kedua "Hostname Aliases", click link biru **id.wikipedia.org**.
- d. Filter ini membuang semua trafik ke hosts lain. Perhatikan Drill Path berubah menjadi "YOURNAME > HTTP > id.wikipedia.org", seperti berikut:



- e. Sekarang click angka biru dalam kurung di sebelah kanan id.wikipedia.org dalam contoh "1". Angka yang ditunjukkan bisa jadi berbeda.
- f. Bagian ini memperlihatkan sessions dengan banyak details, seperti terlihat di bawah. Panel og di sebelah kanan hanya menghabiskan tempat – tutup dengan meng-click tombol X.

Project 17: NetWitness

🛐 Ne	tWitness Investigato	r9					×
∶ <u>c</u> ol	lection <u>E</u> dit <u>V</u> iew	v <u>B</u> ookm	arks <u>H</u> is	story	Help		
All Da	ita			1	YOURNAME > HTTP > id.wikip > Sessions > title=ls > Sessions 🙆 🔞		~
			_				
	Kai Welcome 🖂	W YOUR	NAME 🔛			4	×
	Page 1 of 1	0	0				
Ction		Time	Service	Gine	Eventr Dis	playing 1 = 1 of 1	~
		2012		40.29		piaying 1 of 1	
		May-08	TCP /	KB KB	08.00.27.48.0F.05 -> 52.54.00.12.35.02		
		00:07:4	в нттр		1184 > 20 (http)		
					navland: (FEER		
					madium: Ethernet		
					ten flags: 25		
	View				treams: 2		
					/2 packets: 90		
					12 lifetime: 37		
					action: get		
					directory: /w/		
					filename: index.php		
					Lot extension: php		
					n query: title=Istimewa:Masuk_log&returnto=Portal%3ASumatera		
					🧑 referer: http://id.wikipedia.org/w/index.php?title=Istimewa:Keluar_log&returnto=Portal%3ASumater	ra	
					Client: Mozilla/4.0		
					🗼 alias.ip: 208.80.154.225		
					🗼 alias.host: id.wikipedia.org		
					laction: put		~
						CAR	2

g. Scroll down dan cari "Password=foresec", sperti berikut:

	💽 NetWitness Investiga	ator 9	_ = X
	Collection Edit V	iew <u>B</u> ookmarks <u>H</u> istory <u>H</u> elp	
	All Data	YOURNAME > HTTP > id.wikipedia.org > Sessions for "	
	🕞 😻 Welcome 🖂	W YOURNAME	d ⊳ ×
	Collection Page 1 of 1		~
		Autorio cui forma pontori gi	
		filename: index.php	
		bt extension.ppp Perferer: http://id.wikipedia.org/w/index.php?title=Istimewa.Masuk_log&returnto=Portal%3ASumatera	
-		C client: MoZillar 4.0 ★ alias.ip: 208.80.154.225	=
		Alias.nost. Id.wikipedia.org 7 query:	
		title=Istimewa:Masuk_log&action=submitlogin&type=login&returnto=Portal:Sumatera&wpName=Fcct&wpPassword=foresec&wpLo	ginAttempt=Masi
		filename: Portal textension: <none></none>	
		query: Sumatera preferer: http://id.wikipedia.org/w/index.php?title=Istimewa:Masuk_log&returnto=Portal%3ASumatera	
		Client: Mozilla/4.0	
		klias.host: id.wikipedia.org	
	<	ger action: get	>
			CAP

Simpan Screen Image

- 8. Pastikan "Password=foresec" terlihat.
- 9. Tekan PrintScrn. Simpan keseluruhan gambar desktop dengan nama "NamaKamu_Proj17a".

Menampilkan Rekonstruksi

10. Pada bagian atas tengah jendela NetWitness, pada Drill Path, click HTTP.

- a. Pada bagian "Hostname Aliases", click elearning.binadarma.ac.id
- b. Pada bagian "Hostname Aliases", click angka di sebelah kanan "elearning.binadarma.ac.id "-dalam contoh, angka 6
- C. Sekali lagi, Logs panel --ditutup.
- d. HTTP sessions dengan server elearning.binadarma.ac.id tampil, seperti berikut:

💽 Nel	Witness Investigator 9	Poolmarks History Hola				_ = X
All Da	a		OURNAME > HTTP > elearni	ng.bina > Sessions for "		
6	🔯 Welcome 💿 👩	YOURNAME				4 Þ X
Collect	Page 1 of 1			• 📕 🤿 🗅 🔗		
9		Time	Service	Size Eve	ents	Displaying 1 - 6 of 6
	Long Unents its Des	2013-May-08 00:08	523 IP/TCP/HT	TP 58.27 K8	08:00:27:A8:0F:05 -> 52:54:00:12:35:0 10.0.2.15 -> 10.237.2.9 1204 -> 80 (http) payload: 53193 medium: Ethernet tcp.flags: 26 streams: 2 packets: 119 lifetime: 1 action: get directory: / filename: <none> extension: <none> extension: <none> client: Mozilla/4.0 alias.ip: 10.237.2.9 alias.host: elearning.binadarma.ac.id action: get directory: /theme/standard/ filename: styles.php</none></none></none>	2
	<					
_						CAP .

- e. Pada sisi kiri Report untuk tiap session, terdapat icon yang memperlihatkan bagaimana tampilan halaman Web, dengan tombol **View** berwarna abu-abu.
- f. Click tombol View.
- g. Maka akan terlihat "NetWitness Reconstruction" halaman dari packets, sperti berikut:

NetWitness Investigator 9 Collection Edit View Al Data	Bookmarks History He	IP YOURNAME > HTTI	P > elearning.bina	> elearning.bina	> Sessions for "	YOURNAME Loos	-	
Page 1 of 1					174	Page 0 of 0	00 * * >	
edion	Time	Service	Size Events		Displaying 1 - 6 of 6	Time	Displaying 0 - 0 c	ro 🛆
	2013-May-08 00:08:23	IP / TCP / HTTP	58.27 KB 📒 08:0 🗼 10.0	0:27:A8:0F:05 -> 5; .2.15 -> 10.237.2.9	2:54:00:12:35:02	6		~
YOURNAME Content	- Session 12							• 4 ×
	🔲 🗹 🖭 hex	8 🛛 🔍 🔎	🔕 🗈 🄗 📕					
NetWitness Record Time 5/08/2013 0:0 Protocol 2048/6/80	struction for session 8:23 to 5/08/2013 0:08: Flags Keep Assembled	ID: 12 (Source 1 24 Packet Size 59,6 AppMeta NetworkMe	0.0.2.15 : 1204, 69 bytes Payload	Target 10.237.2. Size 53,193 bytes 19				
R E Q U E S T								•
e-Learning l	Jniversitas Bin	a Darma					You are not logged in. (Log English (en) 💌 G	n) 0
Main Menu Site news Ruang Ngobro						X ubd	onal Standard	

Simpan Screen Image

11. Pastikan header "e-learning Universitas Bina Darma " terlihat.

- a. Tekan PrintScrn key. Simpan keselurhan desktop image dengan nama "NamaKamu_Proj17b".
- b. Tutup panel "NetWitness Reconstruction" dengan meng- click tombol X.

Pencarian

12. Pada bagian atas jendela NetWitness, pada Drill Path, click tulisan biru YOURNAME.

a. Pada sebelah kanan jendela, di baris yang sama dengan "YOURNAME", click icon kaca pembesar di sudut kanan atas, seperti berikut:

Project 17: NetWitness

15 point



13. Pada kotak pencarian, ketikkan Sumatera seperti berikut. Click tombol Search.



14. Maka akan tampil report, memperlihatkan hasil pencarian, dengan thumbnails halaman di sisi kiri seperti berikut:



- 15. Tekan tombol prinscreen untuk mengkopi seluruh desktop. Simpan dengan nama "NamaKamu_Project17c".
- 16. Click thumbnails untuk melihat Reconstruction halaman.

Mengumpulkan Project

17. Kirim melalui elearning.

Last modified 5-8-13