Module : Applications client/serveur

Classe: 2LT

Commandes TCP/IP et analyse de la suite protocolaire TCP/IP sur Wireshark

Objectif

Le but de cette partie du TP est d'analyser des trames Ethernet en vue de comprendre le fonctionnement de quelques protocoles standard de la pile TCP/IP. Les analyseurs de trames Wireshark

Ce TP fera l'objet d'un compte rendu comportant la démarche suivie à chaque étape, les résultats obtenus et leurs interprétations de façon claire et précise.

1. Présentation de l'analyseur de trafic Wireshark

Ethereal est un analyseur de trafic réseau ou "packet sniffer", utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation, etc. C'est un analyseur multi-plateformes, fonctionnel sous Windows, Mac OS X, Linux, Solaris, ainsi que sous FreeBSD. Une récente version d'Ethereal portant le nom de Wireshrak bien d'apparaître. Pour des raisons de compatibilité avec le système Linux installé sur les machines, nous nous contentons d'utiliser Ethereal. Le travail demandé dans ce TP pourra être réalisé de la même façon en utilisant l'analyseur Wireshark.

Ethereal permet d'examiner les données qui transitent sur un réseau ou capturées dans un fichier sur un disque. Il est possible de visualiser le contenu des paquets transmis en direct et en détail. Il permet également le filtrage pour n'afficher que des paquets venant d'une destination ou un protocole par exemple. Plusieurs protocoles sont supportés par Ethereal tels que HTTP, TCP, DNS, FTP, MSN(P), IRC, AIM, ICQ, et POP, qu'il peut visualiser et décoder à partir des paquets capturés.

2. Capture de paquet avec Wireshark

Pour lancer une capture, il faut aller dans le menu Capture / Interface (ou cliquer sur le bouton correspondant). Une nouvelle fenêtre comportant la liste des interfaces réseaux disponibles va apparaître. Il est possible de configurer certaines options de la capture en choisissant le bouton «Options» de l'interface en question. Ces options permettent le filtrage de capture affin de ne capturer que les paquets correspondant aux choix réalisés.

Le filtre de capture dois être spécifié dans le champ "Capture Filter" ou bien cliquez sur le bouton "Capture Filter" pour choisir un des filtres existants ou définir votre filtre et pouvoir le réutiliser pour des captures ultérieures. Ethereal utilise la librairie Libpcap ou Winpcap pour la capture. La syntaxe de filtre de capture utilisé est la même utilisée par ces librairies et est identique à celle de la commande TCPdump.

Inte	el(R)		/10	n ve	Not	harmen	k Cr	nne	ction	OM	icro	eoft'	e Da	rket	Set	uhar	ler) ·	Cani	uring	. Wir	eshark	2				X
Eila I	Edit	View	Go		antur		nalu		Haticti	(141)	Help	3011	310			icuu		cap	uning		Jun					
	Laic La B	<u>v</u> iew	go	- <u>-</u>	apcore		a laiya		i 🖂	1 6	S	12) (res		10	0	0 5		5.24	520	-	
	6 4 G		件 垣	4			~~~	ins		<u> (</u>	~	-	~	-	T	2			Æ	Q	Q E	1	-			>>
Eilter:																•	Expre	ession.	<u>⊂</u> lea	ar <u>App</u> i	y					
No	1	Time			15	Sourc	e					Ð	Desti	natior	1				Proto	ocol	Info					^
	1	1.9	996	30	1	192.	168	3.1.	120				192	.168	3.1.	.1			ICM	P	Ech	0 (ping) 16	eque	5
	8	2.0	002	13	1	L92.	168	3.1.	1			-	192	.168	3.1.	.120)		ICM	P	Ech	o (ping) re	eply	1
	. 9	3.0	009	89	1	L92.	168	3.1.	120			-	192	.168	3.1.	.1			ICM	P	Ech	οÇ	ping) re	eque	s
	10	3.0	015	99	-	L92.	168	3.1.	1				192	.168	3.1.	.120	1		ICM	P	Ech	0 (ping) re	eply	
	11	4.9	972	69		net	ie	in_c	1:10	1:4	y	_	IOSI	nipa	1-24	0:03	:10		ARP		who	na	5 19	2.10	58.T	
	12	4.9	610	576	1	rock	nib.	1_30	.03	16			ne	ada		JT : T	.a.4	2	ARP		192	. 10	c. 10	2 14	15 1	a
	14	28	607	168		rost	hiba	56	.03	16			Bro	adca	ast				ARP		who	ha	\$ 19	2.10	58 1	
	15	41.	004	890	8 4	rost	niba	56	:03	16		-	Bro	adca	ast				ARP		who	ha	5 19	2.10	58.1	
	16	47.	058	783	1	192.	168	3.1.	120				192	.168	3.1.	.1			TCP		476	6 >	htt	p [s	SYNT	
	17	47.	059	727	1	L92.	168	3.1.	1				192	.168	3.1.	.120	1		TCP		htt	p >	476	6 [9	SYN,	
	18	47.	059	766	e 1	L92.	168	3.1.	120			-	192	.168	3.1.	.1			TCP		476	6 >	htt	рĒИ	ACK]	
	19	47.	063	437	2	L92.	.168	3.1.	120				192	.168	3.1.	. 1			HTT	P	GET	1	HTTP	/1.1	1. 1000	
	20	47.	064	181	1	192.	168	3.1.	1			-	192	.168	3.1.	120)		TCP		http	p >	476	6 [A	ACK]	
	21	47.	223	394	1	L92.	168	3.1.	1			_	192	.168	3.1.	.120			TCP		LTC	P S	egme	nt d	of a	
	22	47.	238	LU4		192.	160	5.1.	120				192	1.60	5. <u>1</u> .	120			TCP		LICI	PS	egme	ητ α	от а	6
	23	47.	238	571	6 - 1	192.	100	5.1.	120				192	. 100	5.1.	.±			TCP		476	6 >	ntt	рυ	ACK]	
<u> </u>									.101																13	
0000	00	08	a1	b1	1a	49	00	0e	7b	56	03	1b	08	00	45	00	22	1	C {	v	Ε.					1A
0010	01	bd	2f	86	40	00	80	06	45	eb	<0	a8	01	78	⊂0	a8		1.0.	Ê)	<					
0020	01	01	12	9e	00	50	e4	d7	54	13	e1	8e	0d	dQ	50	18	202	F	Р Т		Р.					-
0030		71	280	21	00	00	4/	45	54	20	21	20	48	54	54	50	1		GE T	/ H	TP					
0040	21	36	28	20	21	20	21	0d	0.2	55	72	65	77	29	41	67	16	8 1	1 5	User.	-00					-
0060	65	6e	74	3a	20	4d	6f	7a	69	6c	60	61	2F	35	Ze	30	er	nt: M	Aoz i	11a/	. ð					
0070	20	28	57	69	6e	64	6f	77	73	3b	20	55	3b	20	57	69	(Wind	dow s	; U;	wi					
0080	6e	64	6f	77	73	20	4e	54	20	35	Ze	31	3b	20	65	6e	no	lows	NT	5.1;	en					
0090	2d	55	53	3b	20	72	76	3a	31	2e	38	2e	31	2e	31	32	-L	JS; [v: 1	.8.1.	12					
oobo	29	20	47	72	65	66	6F	2T 78	32 2E	30	30	30	50	32	30 20	51 21		Geck	CO/ 2	2 0 0	1 1					~
Intel/P		/100.5	/E Ma	r Z	k Con	nech	01	7 O	2 Pa	ckot	2.8	Dicol	2 E	. 46.0	2 E	- L C		- ii ei	Drofi	2. U. C	off.					Caller
meel(R	I FRO	100 0	UL NE	CAMOLI	N ~ 011	netti	on (P	icrU.	. Pa	CUBC:	s, 40	Dishi	ayeu	101	nar Ne	u. u			PTUN	ie, Dela	unc					

Il est aussi possible de filtrer les paquets après capture en utilisant le filtre d'affichage.

Après le choix de l'interface et la définition du filtre s'il existe, lancez la capture des paquets en cliquant sur Start.

3. Analyse de la capture

Après capture, la liste des paquets capturés à travers le filtre peuvent être consultée à partir de la fenêtre principale. Pour analyser le contenu de l'un de ces paquets, il faut d'abord le sélectionner dans la liste des paquets. Les informations intéressantes sont disponibles dans la fenêtre des détails. Cette fenêtre affiche une ligne (extensible) par couche réseau. La capture d'un traffic http de retrouver les couches suivantes:

- couche 2 (Ethernet MAC)
- couche 3 (Internet Protocol IP)
- couche 4 (Transmission control protocol TCP)
- couche 7 (HyperText Transfert Protocol HTTP)

Il suffit de cliquer sur la ligne en question pour avoir plus de détail.

4. Filtrage après capture

Il est aussi possible de capturer la totalité d'un flux, puis, par la suite, effectuer un filtrage pour n'avoir qu'une partie précise. Voire annexe pour la syntaxe de filtrage.

Eilter:	•	Expression	⊆lear	Apply	
---------	---	------------	-------	-------	--

5. Travail demandé :

A. **Questions théoriques**

- 1) Expliquer le principe de capture de trames dans un réseau Ethernet.
- 2) Que peut-on dire sur la sécurité d'un réseau Ethernet.
- 3) Etant donné le réseau auquel vous êtes connecté. En utilisant le logiciel de capture de trame sur une machine A, est ce que vous êtes capable d'observer une conversation entre deux machines B et C ?
- 4) Dans quelles conditions votre machine sera capable de visualiser le trafic émanant d'une autre machine sur le même réseau.

B. Analyse de trafic ARP

- 1) Expliquez dans quelle condition votre machine génère t'elle une trame ARP ?
- 2) Choisir une adresse IP destination et faire en sorte que votre machine émettra une requête ARP dès lors qu'elle commencera à communiquer avec cette dernière.
- 3) Créer un filtre de façon à ce que votre analyseur de trames ne captera que les datagrammes ARP.
- 4) Démarrer la capture, lancer la commande « ping » vers l'adresse IP choisie, puis arrêter la capture.
- 5) Vérifier que vous avez capturé les bonnes trames (la requête ARP émise/reçue depuis/vers votre machine). Expliquer votre démarche.
- 6) Expliquer comment votre analyseur arrive à détecter que les trames capturées encapsulent des datagrammes ARP (indiquer le champ utilisé et sa valeur).
- 7) Déterminer l'adresse Ethernet de votre machine à partir des trames capturées.
- 8) Vers quelle adresse Ethernet la requête ARP a été envoyée. Interpréter cette valeur.
- 9) Analyser le datagramme ARP de réponse et expliquer comment votre machine arrive à déterminer l'adresse MAC relative à votre correspondant.
- 10) Lancer de nouveau l'analyseur de paquets pour qu'il n'affiche que les paquets ARP.
- 11) Choisir une autre machine et changer son adresse IP avec la même adresse IP que celle attribué à votre machine. Utiliser la commande « arping » pour envoyer des paquets ARP reply (avec les adresses IP source et destination la même adresse utilisé par les deux machines). Observer les paquets capturés et expliquer.

C. Analyse de trafic ICMP et HTTP

- 1) Créer un filtre de façon à ce que votre analyseur de trames ne capte que les datagrammes ICMP.
- 2) Démarrer la capture, lancer la commande « ping » vers une adresse IP choisie. Arrêter la capture.
- 3) Retrouver dans le buffer de capture les trames générées par la commande « ping ».
- 4) Quel type de message ICMP (en émission et en réception) a été généré par la commande ping ? Indiquer les champs spécifiques qui vous ont permis de déduire cette valeur.
- 5) En combien de paquets IP a été décomposée la requête émise ? Conclure.
- 6) Quel est le nombre de trames générées par la commande « ping » ? Montrer qu'il est cohérent avec ce qui a été affiché lors de l'exécution de la commande.
- 7) Expliquer comment votre analyseur arrive à détecter qu'il s'agit d'un message ICMP encapsulé dans un paquet IP, qui est lui aussi encapsulé dans une trame Ethernet.
- 8) Interpréter les valeurs des champs IP suivants: FLAG, Offset, et identification relatives aux requêtes ICMP.
- 9) Quelle est la valeur TTL des paquets relatifs aux requêtes ICMP ? Conclure.