Laboratoire http (90 min)

	Objectifs	sudo ./c 2

Prérequis Avoir étudié avant la séance de labo

- http://www.tdeig.ch/publication/tutorial_http.pdf
- https://developer.chrome.com/devtools/docs/network#resource-network-timing

Les buts de ce labo sont d'illustrer :

• Les principaux mécanismes du protocole http	**20 min**
• Le rôle du cache client et des *cookies*	**20 min**
• L'authentification http basic	**10 min**
• L'utilité de Google Development Tool	**20 min**
• L'exploitation du serveur à partir des logs	**10 min**

Session Ouvrir une **session Windows 7** administrateur : compte=**albert** username=**admin**

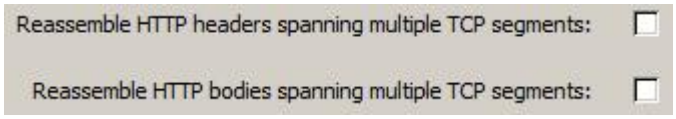
Cadre Ce labo s'effectue individuellement avec un PC Windows 7 situé dans l'intranet
Voir http://www.tdeig.ch/Schema_Reseau.pdf

Action Copier sur le bureau le dossier partagé **`\\10.2.1.1\doclabo\RPI\3_http`** contenant les fichiers utiles

1	Analyse du protocole http	20'

Objectif Etudier les principaux éléments du protocole http à partir de l'acquisition **IE_cache_vide,** qui a été produite en lançant IE avec http://www.td.unige.ch/ comme page par défaut après avoir vidé le cache (*Alt - Tools – Internet Options – Delete… - Delete all…*)

Action Cliquer sur **IE_cache_vide**
Décocher l'option Name resolution afin d'afficher les valeurs numériques
Dans Wireshark, Edit – Preferences – Protocols – HTTP,
désactiver



Q1a Qu'apprenez-vous dans la vue Wireshark : Statistics – Conversations onglet TCP ?

Q1b Compléter le tableau suivant :

No	←→	Port 1683	Port 1684	Commentaire
1	→	Yes		Demande d'établissement du client
3				
4				http GET (host=www.td.unige.ch, connection=keep alive)
5				
6				html
8				
9				
10				
12				
13				
15				
16				
17				
18				
36				
37				

Remarque Le paquet 4 contient un élément de persistance avec le champ ***keep-alive.***

2	**Cache client**	10’

Objectif Comprendre le rôle exact des raccourcis F5 et CTRL F5 du navigateur **Internet Explorer**

Action Lancer Wireshark (raccourci bureau)

Q2a Comment procédez-vous pour sélectionner la bonne interface Ethernet ?

Action Lancer IE
Choisir le FQDN www.unige.ch
Observer le nombre de trames (paquets) vues par Wireshark

Q2b Quel est le volume échangé ?

Action Typer F5

Q2c Quel est le volume échangé ?

Action Typer CTRL F5

Q2d Quel est le volume échangé ?

Action Vider le cache : Alt – Tools – Internet Options – Delete… – Delete all…

Q2e Quel est l’effet ?

Action Effacer l’historique : CTRL H – Clic-droit sur Today – Delete

Q2f Quel est l’effet ?

3	***Cookie***	10’

Objectif Comprendre le fonctionnement des *cookies* à partir de l’acquisition **http-cookie** réalisée avec le site google qui dépose les 2 *cookies (Temporary Internet files de IE)* suivants :
`PREF=ID=a3abbe10bbdcd09a:TM=1170750725:LM=1170750725: ... google.com/`
`PREF=ID=6ff6dc9dfc494a14:TM=1170750725:LM=1170750725: ... google.ch`

Action Activer un filtre d’affichage http

Q3a Combien de paquets contiennent du http ?

Q3b Quel est le FQDN sélectionné dans le paquet 6

Q3c Dans quel paquet le 1er cookie est-il envoyé ?

Q3d S’agit-il d’une opération de lecture ou d’écriture ?

Q3e Dans quel paquet le 2ème cookie est-il envoyé ?

Q3f Quel est le cookie utilisé par le client dans le paquet 20 ?

Remarque Vous pouvez utiliser les filtre http.cookie et http.set_cookie pour retrouver plus facilement les paquets utilisant un cookie

4	Authentification	10’

Objectif Trouver *username* et *password* utilisés dans une session avec **www.td.unige.ch** à partir de l’aquisition **http-auth-basic**

Action Ouvrir cette acquisition pour la comparer avec les explications du §11.1 et du §14 du document http://www.tdeig.ch/publication/tutorial_http.pdf

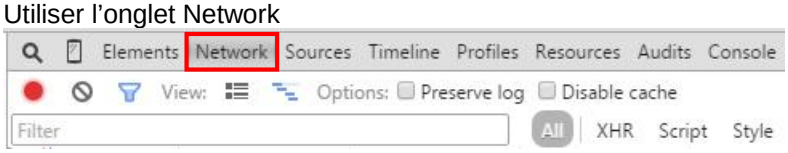
Q4a Dans quel paquet est transmis le mot de passe ?
Expliquer la méthodologie (navigateur et wireshark) pour répondre à la question

Q4b Quelle est la valeur du mot de passe ?

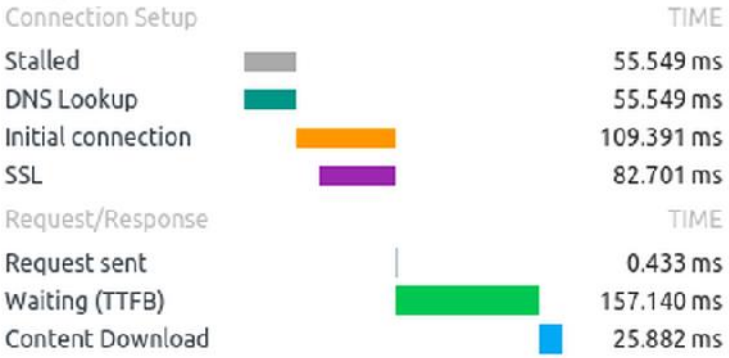
5	Google Development Tool	20’

Objectif Apprentissage de l’outil avec **www.tdeig.ch**

Action Lancer le navigateur Google Chrome
Typer Ctrl maj i ou F12 pour activer l’outil
Utiliser l’onglet Network



Obtenir ce détail du timing



Q5a Quel résultat obtenez-vous ?

Q5b Quels sont les éléments intéressants ?

Action Analyser l’échange avec **www.unige.ch**

Q5c Quel résultat obtenez-vous ? Quels sont les éléments intéressants ?

6	Analyse des logs	10’

Introduction L’analyse des *logs* constitue un moyen de détection des intrusions. Elle exige très vite une méthodologie appropriée face au volume de données reçues quotidiennement.

Les données *(logs)* mises à disposition proviennent du serveur IIS6 du laboratoire utilisé en 2006 accessible depuis www.td.unige.ch

L’architecture IIS6 comprend notamment le module http.sys *(kernel-mode device driver)* qui intercepte les requêtes pour analyse.

Ce module bloque une requête si :

- l'URL ne satisfait pas certains critères (URL malformée)
- le traitement de la requête dépasse certains *time-out* (problème de connexion)

et journalise l'événement dans **httperr.log**

Il peut aussi informer que le service est indisponible

Format de **httperr.log**

Le *log* est un fichier texte composé de 12 champs séparés entre eux par des espaces. Lorsqu'un champ contient une valeur non valable, elle est remplacée par le caractère **(-),** si un champ contient un caractère non imprimable celui-ci est remplacé par **(+)**.
Le format de ces *logs* n'est pas le *W3C Extended log file format.*

Nom des Champs	Description
Date	Date
Time	Heure
Client Ip	Ip du Client
Client Port	Port du Client
Server Ip	Ip du serveur
Server Port	Port du Serveur
Protocol version	Version du protocole http utilisé par le client
Verb	Méthode HTTP utilisée par le client
CookedURL and query	URL + Requête du client
Protocol status	Code status http produit par la requête du client
Site Id	Valeur numérique indiquant le site demandé
Reason phrase	Information sur la raison de l'erreur

Consulter iis6.pdf pour plus de détail

Objectif **Comprendre l'information contenue dans http_err.xls**

Action Utiliser https://sheet.zoho.com/excelviewer pour répondre aux questions

Q6a Déterminer les tentatives d'intrusion relatives aux lignes (paquets) :

512

588

604

613

614

848

Introduction Les requêtes qui traversent avec succès le filtre précédent sont mises dans la file d'attente du *Worker Process* qui est chargé du traitement

Le site du laboratoire ne contient que des pages html statiques

Chaque requête est journalisé dans un fichier au format W3C

W3C Extended Log File Format (IIS 6.0)
The W3C Extended log file format is the default log file format for IIS.

Field prefixes have the following meanings :

- s server action
- c client action
- cs client to server action
- sc server to client action

Field	Appears As	Description

Field	Appears As	Description
Date	date	The date on which the activity occurred.
Time	time	The time, in coordinated universal time (UTC), at which the activity occurred.
Server IP Address	s-ip	The IP address of the server on which the log file entry was generated.
Method	cs-method	The requested action, for example, a GET method.
URI Stem	cs-uri-stem	The target of the action, for example, Default.htm.
User Name	cs-username	The name of the authenticated user who accessed your server. Anonymous users are indicated by a hyphen.
Client IP Address	c-ip	The IP address of the client that made the request.
Protocol Version	cs-version	The protocol version —HTTP or FTP —that the client used.
User Agent	cs(User-Agent)	The browser type that the client used.
Referrer	cs(Referrer)	The site that the user last visited. This site provided a link to the current site.
HTTP Status	sc-status	The HTTP status code.
Win32 Status	sc-win32-status	The Windows status code.
Bytes Sent	sc-bytes	The number of bytes that the server sent.
Bytes Received	cs-bytes	The number of bytes that the server received.
Time Taken	time-taken	The length of time that the action took, in milliseconds.

Not all fields will contain information → a hyphen (-) appears as a placeholder when there is no information.
If a field contains a nonprintable character, it will be replaced with a plus sign (+) to preserve the log file format.

Remarque Vous disposez, dans la fenêtre de partage, du raccourci **IIS Log File Format (IIS 6.0)**

Objectif **Comprendre l'information contenue dans ex040615.xls**

Action Utiliser https://sheet.zoho.com/excelviewer pour répondre aux questions

Q6b Déterminer les tentatives d'intrusion relatives aux lignes (paquets) :

33

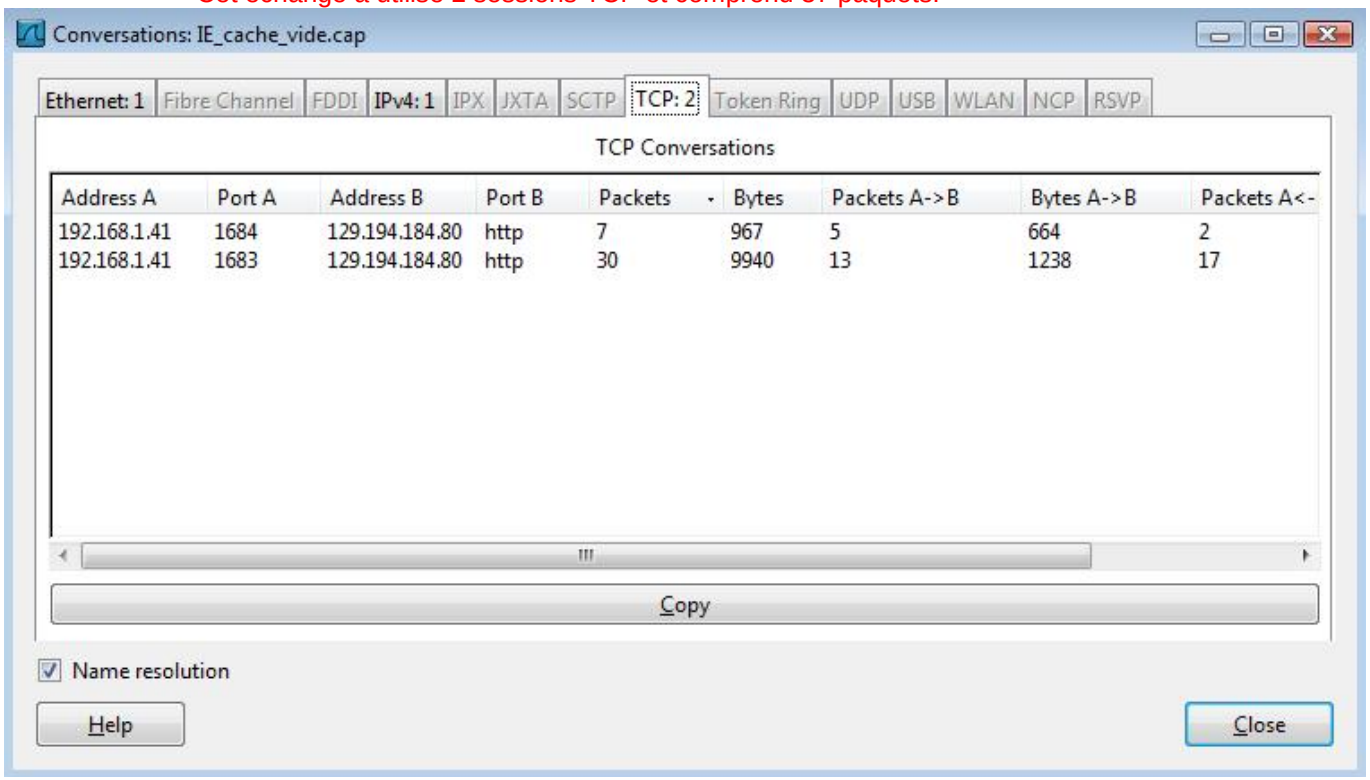
35

36

Labo terminé	**Toutes les unités centrales seront éteintes avec un script** **Tous les écrans seront éteints depuis le tableau électrique**

Corrigé

Q1a Qu'apprenez-vous dans la vue Wireshark : Statistics – Conversations onglet TCP ?
Cet échange a utilisé 2 sessions TCP et comprend 37 paquets.



Q1b Compléter le tableau suivant :

No	←→	Port 1683	Port 1684	Commentaire
1	→	Yes		Demande d'établissement TCP du client sur port 1683
3	→	Y		Session TCP établie
4	→	Y		http GET (host=www.td.unige.ch, connection=keep alive)
5	←	Y		http 200 OK (default.html, server=MS-IIS6.0) voir view source
6				
8	→		Y	Demande d'établissement TCP du client sur port 1684
9	←	Y		Contenu de la page en html
10	←	Y		Contenu de la page en html
12	←	Y		Contenu de la page en html
13				
15	→		Y	Session TCP établie
16				
17	←		Y	http 304 Not Modified
18				
36	→	Y		TCP RST (Reset)
37	→		Y	TCP RST (Reset)