Travaux pratiques 4.5.3 : Examen des protocoles de la couche application et de la couche transport

Schéma de topologie

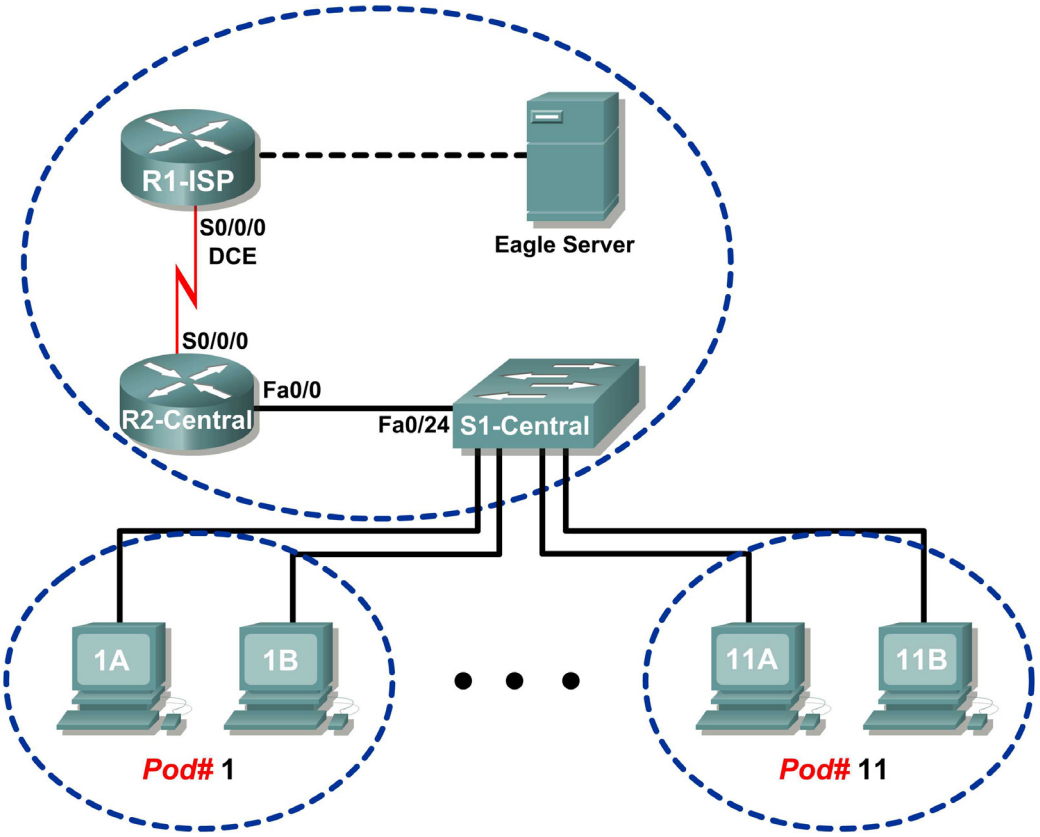


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	S/O
	Fa0/0	192.168.254.253	255.255.255.0	S/O
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	S/O
	Fa0/0	172.16.255.254	255.255.0.0	S/O
Eagle Server	S/O	192.168.254.254	255.255.255.0	192.168.254.253
	S/O	172.31.24.254	255.255.255.0	S/O
host*Pod*#A	S/O	172.16.*Pod*#.1	255.255.0.0	172.16.255.254
host*Pod*#B	S/O	172.16.*Pod*#.2	255.255.0.0	172.16.255.254
S1-Central	S/O	172.16.254.1	255.255.0.0	172.16.255.254

Objectifs pédagogiques

À la fin de ce chapitre, vous saurez :

- configurer l'ordinateur hôte pour capturer les protocoles de la couche application ;
- capturer et analyser la communication HTTP entre l'ordinateur hôte pod et un serveur Web ;
- capturer et analyser la communication FTP entre l'ordinateur hôte pod et un serveur FTP ;
- observer l'établissement et la gestion des canaux de communication par TCP avec les connexions HTTP et FTP.

Contexte

La fonction principale de la couche transport consiste à effectuer le suivi des conversations des applications sur le même hôte. Toutefois, les besoins de données sont différents selon les applications. Par conséquent, divers protocoles de transport ont été développés pour y répondre.
Les protocoles de couche application définissent la communication entre les services réseau, un serveur Web et un client, et un serveur FTP et un client, par exemple. Le client établit la communication avec le serveur approprié et ce dernier lui répond. Pour chaque service réseau, un serveur différent écoute sur un autre port les connexions de clients. Plusieurs serveurs sont susceptibles de figurer sur le même périphérique final. Il est possible qu'un utilisateur ouvre plusieurs applications clientes sur le même serveur. Toutefois, chaque client communique de façon exclusive avec une session établie entre le client et le serveur.

Les protocoles de couche application reposent sur les protocoles TCP/IP de niveau inférieur, tels que TCP ou UDP. Ces travaux pratiques examinent deux protocoles de couche application standard, HTTP et FTP, ainsi que la gestion du canal de communication par les protocoles TCP et UDP de la couche transport. Les requêtes standard du client et les réponses correspondantes du serveur seront également étudiées.

Scénario

Dans ces travaux pratiques, vous utiliserez des applications clientes pour vous connecter aux services réseau d'Eagle Server. Vous surveillerez les communications à l'aide du logiciel Wireshark et analyserez les paquets capturés.

Un navigateur Web, tel qu'Internet Explorer ou Firefox, sera utilisé pour vous connecter au service réseau d'Eagle Server. Ce dernier comprend plusieurs services réseau préconfigurés, tels que HTTP, en attente de répondre aux requêtes du client.

Le navigateur Web sera également utilisé pour examiner le protocole FTP, ainsi que le client de ligne de commande FTP. Cet exercice démontrera que la communication sous-jacente avec le serveur reste identique même si les clients sont différents.

Tâche 1 : configuration de l'ordinateur hôte pod pour capturer les protocoles de couche application.

Les travaux pratiques doivent être configurés comme illustré dans le schéma de topologie et dans la table d'adressage logique. Si ce n'est pas le cas, demandez de l'aide auprès de votre formateur.

Étape 1 : téléchargement et installation de wireshark.

Figure 1. Page de téléchargement de Thunderbird sur FTP

Si Wireshark n'est pas installé sur l'ordinateur hôte pod, vous pouvez le télécharger à l'adresse eagle-server.example.com. Reportez-vous à la figure 1. L'URL de téléchargement est ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter3.

1. Cliquez avec le bouton droit sur le nom de fichier de wireshark, puis enregistrez le fichier dans l'ordinateur hôte pod.
2. Une fois le fichier téléchargé, double-cliquez sur le nom de fichier et installez Wireshark avec les paramètres par défaut.

Étape 2 : démarrage de Wireshark et configuration de l'interface de capture.

1. Démarrez Wireshark à partir de **Démarrer > Tous les programmes > Wireshark > Wireshark**.
2. Lorsque l'écran d'ouverture s'affiche, définissez l'interface de capture appropriée. L'interface avec l'adresse IP de l'ordinateur hôte pod est correcte. Reportez-vous à la figure 2.

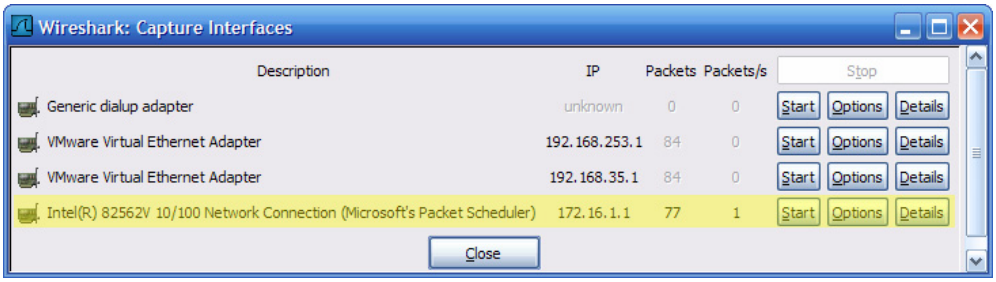


Figure 2. Écran de capture de l'interface Wireshark

Vous pouvez lancer Wireshark en cliquant sur le bouton **Démarrer** de l'interface. Ensuite, cette dernière est utilisée comme celle par défaut et ne nécessite pas de modifications.

Wireshark doit commencer la consignation des données.

3. Arrêtez Wireshark pour le moment. Vous l'utiliserez dans les tâches à venir.

Tâche 2 : capture et analyse de la communication HTTP entre l'ordinateur hôte pod et un serveur Web.

HTTP est un protocole de couche application qui repose sur des protocoles de niveau inférieur comme TCP pour établir et gérer le canal de communication. HTTP version 1.1 est défini dans la RFC 2616 de 1999. Cette partie des travaux pratiques démontre la manière dont les sessions entre plusieurs clients Web et le serveur Web restent distinctes.

Étape 1 : lancement de la capture à l'aide de Wireshark.

Démarrez une capture Wireshark. Les résultats s'affichent par type de paquet.

Étape 2 : démarrage du navigateur Web de l'hôte pod.

1. À l'aide d'un navigateur Web tel qu'Internet Explorer ou Firefox, connectez-vous à l'URL http://eagle-server.example.com. Une page Web semblable à la figure 3 s'affiche. Ne fermez pas ce navigateur Web avant que le système ne vous le demande.

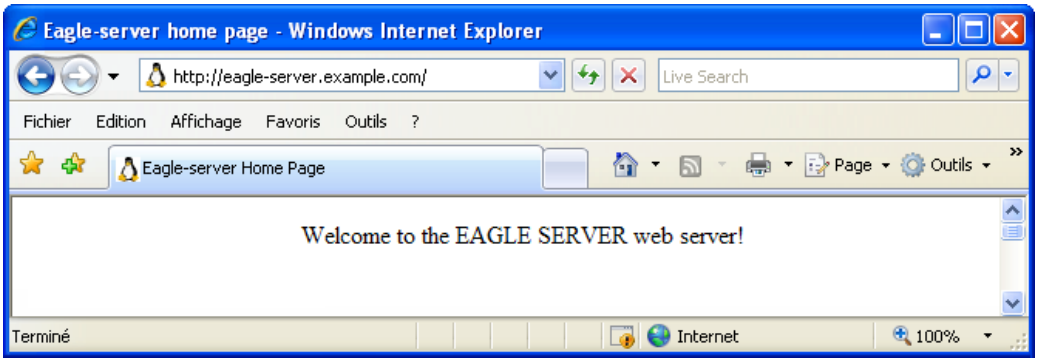


Figure 3. Navigateur Web connecté au serveur Web

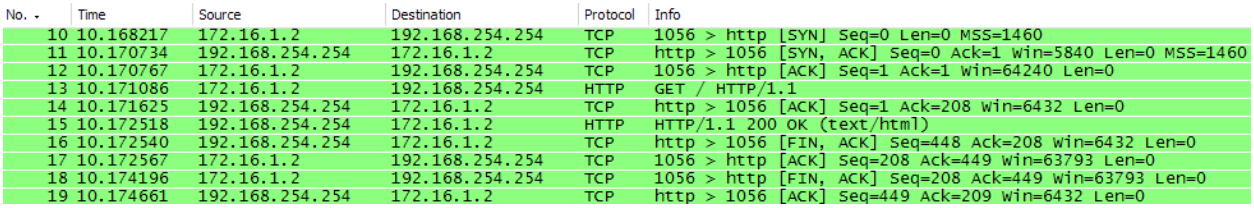
2. Cliquez sur le bouton **Actualiser** du navigateur Web. L'affichage dans le client Web reste le même.
3. Ouvrez un deuxième navigateur Web et connectez-vous à l'URL http://eagle-server.example.com/page2.html. Ceci permet d'afficher une page Web différente.

   Ne fermez aucun des deux navigateurs jusqu'à l'arrêt de la capture Wireshark.

Étape 3 : arrêt des captures Wireshark et analyse des données capturées.

1. Arrêtez les captures Wireshark.
2. Fermez les navigateurs Web.

Les données Wireshark obtenues sont affichées. Au moins trois sessions HTTP ont été créées dans l'étape 2. La première session HTTP a démarré avec une connexion à http://eagle-server.example.com. La deuxième session s'est produite avec une actualisation. La troisième session a eu lieu avec l'accès du deuxième navigateur Web à http://eagle-server.example.com/page2.html.



No.	Time	Source	Destination	Protocol	Info
10	10.168217	172.16.1.2	192.168.254.254	TCP	1056 > http [SYN] Seq=0 Len=0 MSS=1460
11	10.170734	192.168.254.254	172.16.1.2	TCP	http > 1056 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
12	10.170767	172.16.1.2	192.168.254.254	TCP	1056 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
13	10.171086	172.16.1.2	192.168.254.254	HTTP	GET / HTTP/1.1
14	10.171625	192.168.254.254	172.16.1.2	TCP	http > 1056 [ACK] Seq=1 Ack=208 Win=6432 Len=0
15	10.172518	192.168.254.254	172.16.1.2	HTTP	HTTP/1.1 200 OK (text/html)
16	10.172540	192.168.254.254	172.16.1.2	TCP	http > 1056 [FIN, ACK] Seq=448 Ack=208 Win=6432 Len=0
17	10.172567	172.16.1.2	192.168.254.254	TCP	1056 > http [ACK] Seq=208 Ack=449 Win=63793 Len=0
18	10.174196	172.16.1.2	192.168.254.254	TCP	1056 > http [FIN, ACK] Seq=208 Ack=449 Win=63793 Len=0
19	10.174661	192.168.254.254	172.16.1.2	TCP	http > 1056 [ACK] Seq=449 Ack=209 Win=6432 Len=0

Figure 4. Session HTTP capturée

Un exemple de session HTTP capturée est illustré à la figure 4. Avant que HTTP puisse commencer, vous devez créer la session TCP. Ceci est visible dans les trois premières lignes de session, numéros 10,11 et 12. Utilisez la capture ou les données Wireshark semblables pour répondre aux questions suivantes :

3. Renseignez le tableau suivant à partir des informations disponibles dans la session HTTP :

Adresse IP du navigateur Web	
Adresse IP du serveur Web	
Protocole de couche transport (UDP/TCP)	
Numéro de port du navigateur Web	
Numéro de port du serveur Web	

4. Quel ordinateur a lancé la session HTTP, et comment ?

_____

_____

5. Quel ordinateur a signalé au départ une fin de la session HTTP, et comment ?

_____

_____

6. Sélectionnez la première ligne du protocole HTTP, une requête **GET** provenant du navigateur Web. Dans la figure 4 ci-dessus, la requête **GET** s'affiche sur la ligne 13. Allez dans la deuxième fenêtre Wireshark (du milieu) pour examiner les protocoles en couches. Si nécessaire, développez les champs.
7. Quel protocole est intégré (encapsulé) au segment TCP ?

_____

8. Développez le dernier enregistrement de protocole, et tout sous-champ. Il s'agit des informations réelles envoyées au serveur Web. Renseignez le tableau suivant à l'aide des informations provenant du protocole.

Version du protocole	
Méthode de requête	
* URI de requête	
Langue	

* L'URI de requête est le chemin d'accès au document demandé. Dans le premier navigateur, le chemin d'accès est le répertoire racine du serveur Web. Bien qu'aucune page ne soit demandée, certains serveurs Web sont configurés pour afficher un fichier par défaut (si disponible).

Le serveur Web répond avec le paquet HTTP suivant. À la figure 4, ceci s'affiche sur la ligne 15. Une réponse au serveur Web est possible car le serveur Web (1) comprend le type de requête et (2) dispose d'un fichier à retourner. Parfois, les pirates informatiques envoient des requêtes inconnues ou déformées au serveur Web afin d'arrêter le serveur ou d'accéder à la ligne de commande du serveur. En outre, une requête de page Web inconnue entraîne un message d'erreur.

9. Sélectionnez la réponse du serveur Web, puis accédez à la deuxième fenêtre (du milieu). Ouvrez tous les sous-champs réduits de HTTP. Notez les informations renvoyées à partir du serveur. Dans cette réponse, seules quelques lignes de texte figurent (les réponses du serveur web peuvent contenir des milliers ou des millions d'octets). Le navigateur Web comprend et met en forme correctement les données dans la fenêtre du navigateur. .
10. Quelle est la réponse du serveur Web à la requête **GET** du client Web ?

_____

11. Que signifie cette réponse ?

_____

12. Faites défiler la fenêtre supérieure de Wireshark jusqu'à ce que la deuxième session HTTP, actualisation, soit visible. Un exemple de capture est illustré à la figure 5.

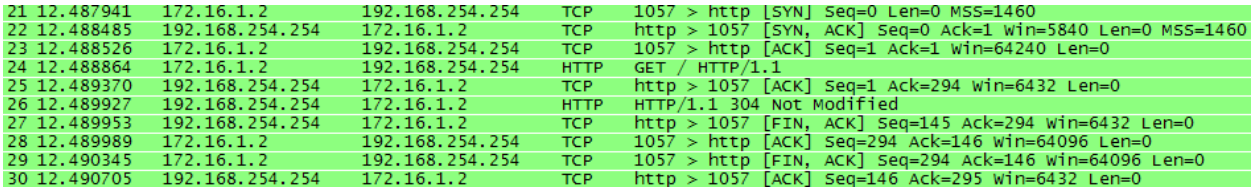


Figure 5. Session HTTP capturée pour l'actualisation

La signification de l'actualisation figure dans la réponse du serveur, `304 Not Modified`. Avec un seul paquet retourné pour la requête **GET** initiale et l'actualisation, la bande passante utilisée est minime. Toutefois, pour une réponse initiale qui contient des millions d'octets, un seul paquet de réponse peut faire gagner une bande passante significative.

Comme cette page Web a été enregistrée dans le cache du client Web, la requête **GET** contenait les instructions supplémentaires suivantes à l'intention du serveur Web :

```
If-modified-since: Fri, 26 Jan 2007 06:19:33 GMT\r\n
If-None-Match: "98072-b8-82da8740"\r\n
```
<- numéro d'étiquette de la page (ETAG)

13. Quelle est la réponse ETAG du serveur Web ?

_____

Tâche 3 : capture et analyse de la communication FTP entre l'ordinateur hôte pod et un serveur Web.

Le protocole FTP de la couche application a subi une révision significative depuis sa première publication dans la RFC 114 de 1971. FTP version 5.1 est défini dans la RFC 959 d'octobre 1985

Vous pouvez utiliser ce navigateur Web standard pour communiquer avec d'autres composants que le serveur HTTP. Dans cette tâche, le navigateur Web et un utilitaire FTP de ligne de commande sont utilisés pour télécharger les données à partir d'un serveur FTP.

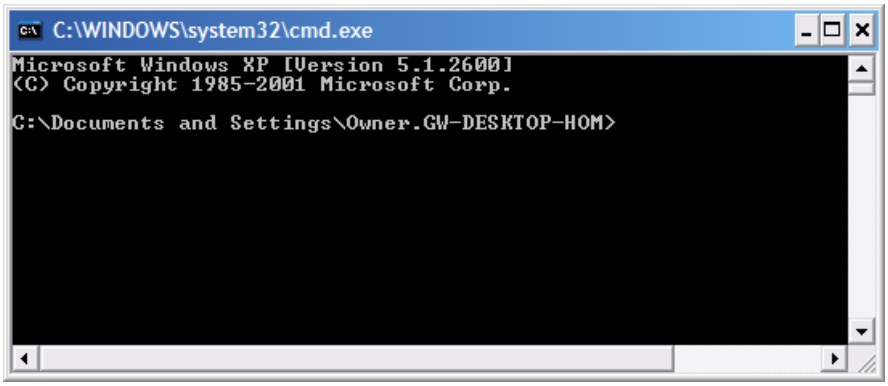


Figure 6. Écran de ligne de commande Windows

En préparation de cette tâche, ouvrez une ligne de commande sur l'ordinateur hôte pod. Pour effectuer ceci, cliquez sur **Démarrer > Exécuter**, tapez **CMD**, puis cliquez sur **OK**. Un écran similaire à la figure 6 apparaît.

Étape 1 : lancement de la capture à l'aide de Wireshark.

Si nécessaire, reportez-vous aux tâches 1 et 2 pour ouvrir Wireshark.

Étape 2 : démarrage du client FTP de la ligne de commande de l'hôte pod.

1. Démarrez une session FTP de l'ordinateur hôte pod avec le serveur FTP, à l'aide de l'utilitaire de client FTP de Windows. Pour l'authentification, utilisez l'ID d'utilisateur **anonyme**. En réponse à l'invite du mot de passe, appuyez sur <**ENTRÉE**>.

```
> ftp eagle-server.example.com
Connected to eagle-server.example.com.
 220 Welcome to the eagle-server FTP service.
User (eagle-server.example.com:(none)): anonymous
331 Please specify the password.
Password: <ENTRÉE>
230 Login successful.
```

2. L'invite du client FTP est `ftp>`. Le client attend donc une commande à envoyer au serveur FTP. Pour afficher une liste de commandes pour le client FTP, tapez **`help <ENTRÉE>`** :

```
ftp> help
Les commandes peuvent être abrégées.  Les commandes sont les suivantes :

!           delete      literal     prompt      send
?           debug       ls          put         status
append      dir         mdelete     pwd         trace
ascii       disconnect  mdir        quit        type
bell        get         mget        quote       user
binary      glob        mkdir       recv        verbose
bye         hash        mls         remotehelp
```

```
cd          help          mput        rename
close       lcd           open        rmdir
```

Malheureusement, la plupart des commandes du client FTP complique l'emploi de l'utilitaire de ligne de commande pour un novice. Nous n'utilisons que quelques commandes pour l'évaluation de Wireshark.

3. Tapez la commande **dir** pour afficher le contenu de répertoire actuel :

```
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Jan 12 04:32 pub
```

Le client FTP figure au répertoire racine du serveur FTP. Il ne s'agit pas du répertoire réel mais du niveau le plus haut auquel l'utilisateur **anonyme** peut accéder. L'utilisateur **anonymous** a été placé dans une prison racine, qui lui interdit l'accès en dehors du répertoire actuel.

4. Les sous-répertoires peuvent être cependant parcourus, et les fichiers transférés vers l'ordinateur hôte pod. Allez dans le répertoire pub/eagle_labs/eagle1/chapter2, téléchargez un fichier, et quittez le répertoire.

```
ftp> cd pub/eagle_labs/eagle1/chapter2
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 0 100     5853 Jan 12 04:26 ftptoeagle-server.pcap
-rw-r--r--  1 0 100     4493 Jan 12 04:27 http to eagle-server.pcap
-rw-r--r--  1 0 100     1486 Jan 12 04:27 ping to 192.168.254.254.pcap
-rw-r--r--  1 0 100 15163750 Jan 12 04:30 wireshark-setup-0.99.4.exe
226 Directory send OK.
ftp: 333 bytes received in 0.04Seconds 8.12Kbytes/sec.
ftp> get "ftptoeagle-server.pcap"
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for ftptoeagle-server.pcap
(5853 bytes).
226 File send OK.
ftp: 5853 bytes received in 0.34Seconds 17.21Kbytes/sec.
ftp> quit
221 Goodbye.
```

5. Fermez la fenêtre de ligne de commande avec la commande exit.
6. Arrêtez les captures Wireshark, et enregistrez-les sous FTP_Command_Line_Client.

Étape 3 : démarrage du navigateur Web de l'hôte pod.

1. Démarrez à nouveau les captures Wireshark.

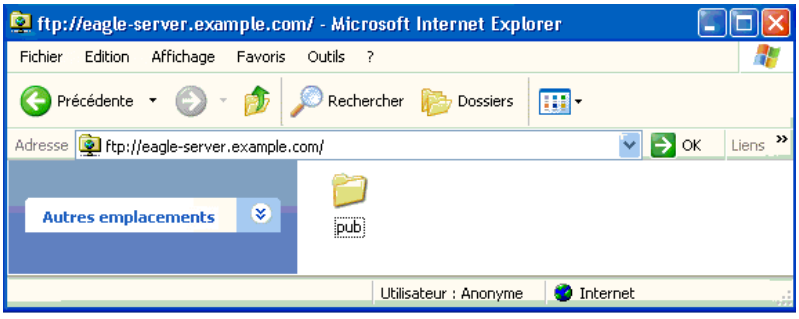


Figure 7. Navigateur Web utilisé comme client FTP

2. Ouvrez un navigateur Web comme illustré à la figure 7, et tapez l'URL `ftp://eagle-server.example.com`. Une fenêtre de navigateur s'ouvre avec le répertoire pub affiché. En outre, le navigateur Web s'est connecté au serveur FTP en tant qu'utilisateur Anonyme, comme illustré au bas de la capture d'écran.
3. À l'aide du navigateur, faites défiler vers le bas la liste de répertoires jusqu'à ce que le chemin d'accès à l'URL soit `pub/eagle-labs/eagle1/chapter2`. Double-cliquez sur le fichier `ftptoeagle-server.pcap` et enregistrez-le.
4. Une fois que vous avez terminé, fermez le navigateur Web.
5. Arrêtez les captures Wireshark, et enregistrez-les sous FTP_Web_Browser_Client.

Étape 4 : arrêt des captures Wireshark et analyse des données capturées.

1. Si ce n'est pas déjà fait, ouvrez la capture Wireshark FTP_Web_Browser_Client.
2. Dans la fenêtre Wireshark supérieure, sélectionnez la capture FTP qui est la première transmission de protocole FTP, Réponse : 220. Il s'agit de la ligne 23 à la figure 8.

No.	Time	Source	Destination	Protocol	Info
12	16.276555	172.16.1.2	192.168.254.254	DNS	Standard query A eagle-server.example.com
13	16.277284	192.168.254.254	172.16.1.2	DNS	Standard query response A 192.168.254.254
14	16.278059	172.16.1.2	192.168.254.254	TCP	1073 > ftp [SYN] Seq=0 Len=0 MSS=1460
15	16.278540	192.168.254.254	172.16.1.2	TCP	ftp > 1073 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
16	16.278575	172.16.1.2	192.168.254.254	TCP	1073 > ftp [ACK] Seq=1 Ack=1 Win=64240 Len=0
23	26.281472	192.168.254.254	172.16.1.2	FTP	Response: 220 Welcome to the eagle-server FTP service.
24	26.281672	172.16.1.2	192.168.254.254	FTP	Request: USER anonymous
25	26.282120	192.168.254.254	172.16.1.2	TCP	ftp > 1073 [ACK] Seq=47 Ack=17 Win=5840 Len=0
26	26.282137	192.168.254.254	172.16.1.2	FTP	Response: 331 Please specify the password.
27	26.282201	172.16.1.2	192.168.254.254	FTP	Request: PASS IEUser@
28	26.283451	192.168.254.254	172.16.1.2	FTP	Response: 230 Login successful.
29	26.313423	172.16.1.2	192.168.254.254	FTP	Request: opts utf8 on
30	26.313959	192.168.254.254	172.16.1.2	FTP	Response: 501 Option not understood.
31	26.314042	172.16.1.2	192.168.254.254	FTP	Request: syst
32	26.314493	192.168.254.254	172.16.1.2	FTP	Response: 215 UNIX Type: L8
33	26.314595	172.16.1.2	192.168.254.254	FTP	Request: site help
34	26.315028	192.168.254.254	172.16.1.2	FTP	Response: 550 Permission denied.
35	26.315113	172.16.1.2	192.168.254.254	FTP	Request: PWD
36	26.315566	192.168.254.254	172.16.1.2	FTP	Response: 257 "/"
37	26.352350	172.16.1.2	192.168.254.254	FTP	Request: noop
38	26.352821	192.168.254.254	172.16.1.2	FTP	Response: 200 NOOP ok.
39	26.482680	172.16.1.2	192.168.254.254	FTP	Request: CWD /
40	26.483243	192.168.254.254	172.16.1.2	FTP	Response: 250 Directory successfully changed.
41	26.484334	172.16.1.2	192.168.254.254	FTP	Request: TYPE A
42	26.484824	192.168.254.254	172.16.1.2	FTP	Response: 200 Switching to ASCII mode.
43	26.485292	172.16.1.2	192.168.254.254	FTP	Request: PORT 172,16,1,2,4,50
44	26.485800	192.168.254.254	172.16.1.2	FTP	Response: 200 PORT command successful. Consider using PASV.
45	26.485892	172.16.1.2	192.168.254.254	FTP	Request: LIST
46	26.486503	192.168.254.254	172.16.1.2	TCP	ftp-data > 1074 [SYN] Seq=0 Len=0 MSS=1460 TSV=12998374 TSER=0 WS=2
47	26.486558	172.16.1.2	192.168.254.254	TCP	1074 > ftp-data [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=0 TSV=0 TSER=
48	26.486948	192.168.254.254	172.16.1.2	TCP	ftp-data > 1074 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=12998375 TSER=0
49	26.487052	192.168.254.254	172.16.1.2	FTP	Response: 150 Here comes the directory listing.
50	26.487252	192.168.254.254	172.16.1.2	FTP-DA	FTP Data: 61 bytes
51	26.487267	192.168.254.254	172.16.1.2	FTP	Response: 226 Directory send OK.

Figure 8. Capture Wireshark d'une session FTP avec un navigateur Web

3. Allez dans la fenêtre Wireshark du milieu et développez le protocole FTP. Ce dernier communique à l'aide de codes, tout comme HTTP.

Qu'est-ce que la réponse 220 du serveur FTP ?

_____

Lorsque le serveur FTP a envoyé une réponse : 331 Spécifiez le mot de passe, quelle a été la réponse du navigateur Web ?

_____

Quel numéro de port le client FTP utilise-t-il pour se connecter au port 21 du serveur FTP ?

_____

Lors du transfert de données ou avec une simple liste de répertoires, un nouveau port est ouvert. Il s'agit du mode de transfert. Ce mode peut être actif ou passif. En mode actif, le serveur ouvre une session TCP à l'intention du client FTP et transfère les données sur ce port précis. Le numéro du port source du serveur FTP est 20. En outre, le numéro du port du client FTP est un numéro supérieur à 1023. Toutefois, le client ouvre un nouveau port à l'intention du serveur pour le transfert des données. Les deux numéros de ports sont supérieurs à 1023.

Quel est le numéro de port FTP-DATA que le serveur FTP utilise ?

_____

4. Ouvrez la capture Wireshark FTP_Web_Browser_Client, et observez la communication FTP. Bien que les clients soient différents, les commandes sont semblables.

Étape 5 : modes de transfert actif et passif de FTP

Les implications entre les deux modes sont très importantes d'un point de vue de la sécurité des informations. Le mode de transfert définit la configuration du port de données.

En mode de transfert actif, un client démarre une session FTP avec le serveur sur le port 21 standard de TCP. Pour le transfert des données, le serveur lance une connexion à partir du port 20 standard de TCP vers le port élevé d'un client, un numéro de port supérieur à 1023. Reportez-vous à la figure 9.

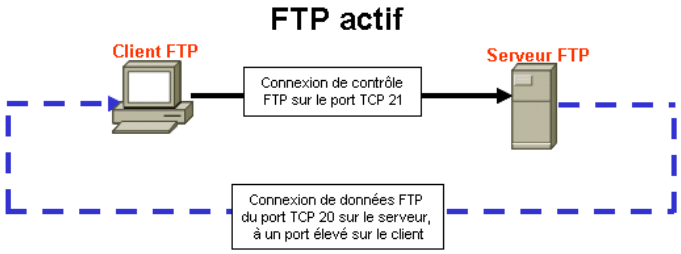


Figure 9.

Sauf si le pare-feu du client FTP est configuré pour autoriser les connexions de l'extérieur, le transfert de données risque d'échouer. Afin d'établir la connectivité pour le transfert des données, le client FTP doit autoriser les connexions FTP (ce qui sous-entend le filtrage dynamique des paquets), ou désactiver le blocage.

En mode de transfert passif, un client démarre une session FTP avec le serveur sur le port 21 standard de TCP. Il s'agit de la même connexion utilisée en mode de transfert actif. Pour le transfert des données, cependant, deux modifications majeures interviennent. Premièrement, le client établit la connexion des données avec le serveur. Deuxièmement, les ports élevés sont utilisés aux deux extrémités de la connexion. Reportez-vous à la figure 10.

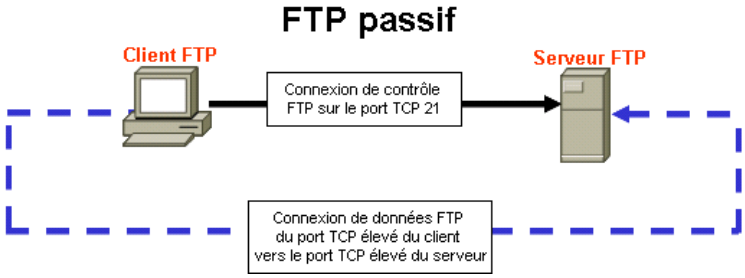


Figure 10.

Sauf si le serveur FTP est configuré pour autoriser une connexion avec un port élevé aléatoire, le transfert des données échoue. Seules quelques applications clientes de FTP acceptent les modifications apportées au mode de transfert.

Tâche 4 : Remarques générales

La communication des protocoles HTTP et FTP repose sur TCP. TCP gère la connexion entre le client et le serveur pour garantir la transmission des datagrammes.

Une application cliente peut être soit un navigateur Web soit un utilitaire de ligne de commande. Toutefois, chacun doit envoyer et recevoir des messages qui peuvent être correctement interprétés. Le protocole de communication est généralement défini dans une RFC.

Le client FTP doit s'authentifier auprès du serveur FTP, même si l'authentification est ouverte à tout le monde. L'utilisateur Anonyme dispose normalement d'un accès restreint au serveur FTP et ne peut donc pas télécharger de fichiers.

Une session HTTP commence lorsqu'une requête est transmise au serveur HTTP et se termine lorsque le client HTTP a accusé réception de la réponse. Une session FTP, cependant, dure jusqu'à ce que le client signale qu'il la quitte avec la commande **`quit`**.

HTTP utilise un protocole unique pour communiquer avec le serveur HTTP. Le serveur écoute les connexions de clients sur le port 80. FTP utilise, cependant, deux protocoles. Le serveur FTP écoute sur le port 21 de TCP, comme la ligne de commande. Selon le mode de transfert, le serveur ou le client peut établir la connexion des données.

Vous pouvez accéder à plusieurs protocoles de la couche application par un simple navigateur Web. Alors que seuls HTTP et FTP ont été examinés, le navigateur peut également prendre en charge Telnet et Gopher. Le navigateur sert de client au serveur. Il envoie des requêtes et traite les réponses.

Tâche 5 : confirmation

Tout en activant la capture Wireshark, utilisez un navigateur Web pour accéder à R2 à l'adresse http://172.16.255.254/level/7/exec ou utilisez un client Telnet pour vous connecter à un périphérique Cisco tel que S1-Central ou R2-Central. Observez le comportement du protocole HTTP ou Telnet. Transmettez les commandes pour observer les résultats.

Dans quelle mesure le protocole Telnet de la couche application est-il semblable à HTTP et FTP ? En quoi TELNET est-il différent ?

_____

_____

Tâche 6 : nettoyage

Si l'installation de Wireshark a eu lieu sur l'ordinateur hôte pod pour ces travaux pratiques, il se peut que le formateur souhaite la suppression de l'application. Pour supprimer Wireshark, cliquez sur **Démarrer > Panneau de configuration > Ajout/Suppression de programmes**. Faites défiler la liste vers le bas, cliquez avec le bouton droit sur **Wireshark**, puis cliquez sur **Supprimer**.

Si vous devez supprimer les fichiers téléchargés de l'ordinateur hôte pod, effacez tous les fichiers récupérés à partir du serveur FTP.

Sauf indication contraire du formateur, mettez les ordinateurs hôtes hors tension. Enlevez le matériel utilisé durant les travaux pratiques, et préparez la salle pour le cours suivant.