heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

iICT

Labo TIB

IP et numéros de port

Objectifs d'apprentissage

1. Connaître les champs les plus importants des en-têtes IP et TCP.
2. Connaître services Internet les plus courants et leurs numéros de port.
3. Savoir scanner les services actifs d'une machine avec nmap.
4. Savoir utiliser l'outil Netcat.

Contenu

Dans ce laboratoire, nous allons étudier comment les données sont transmises entre une application source et une application destinatrice grâce à IP. Nous allons aussi étudier les numéros de port qui permettent communiquer avec plusieurs applications sur la même machine.

1. Analyse des protocoles IP et TCP
2. Analyse des numéros de port
3. Utilisation de nmap pour énumérer les ports ouverts d'une machine.
4. Apprentissage de l'outil Netcat.

Rapport à fournir

Un rapport de 3 pages au maximum avec les éléments suivants :

1. Nom du laboratoire, noms des étudiants, date du laboratoire
2. **Objectif 1 : Analyse des protocoles IP et TCP**
    - Rappel de l'objectif d'apprentissage et du critère de succès.
    - Décrivez les champs les plus importants des paquets IP et TCP. Donnez des exemples de valeurs, selon une capture Wireshark lors de l'accès à une page Web.
3. **Objectif 2 : Identifier les services d'une machine**
    - Rappel de l'objectif d'apprentissage et du critère de succès.
    - Etablissez les listes des services qui tournent sur
        - votre machine Linux
        - votre machine Windows
        - l'équipement 10.192.79.176

      Commentez les services trouvés.
    - Incluez le tableau complété avec les ports les plus courants.
4. **Objectif 3 : Expérimenter avec les connexions**
    - Réponses aux questions de la section « Quelques questions ».
5. Auto-évaluation : est-ce que vous avez atteint les objectifs d'apprentissage de la page 1 ?

Délai

Le fichier PDF du rapport doit être envoyé à l'aide du formulaire
http://iict-space.heig-vd.ch/jer/rendu-labo-tib/
avant le début du prochain laboratoire.

1 Introduction

Dans les laboratoires précédents nous avons observé qu'Internet consiste d'une multitude de réseaux interconnectés. Ces réseaux peuvent utiliser des technologies très différentes. Le réseau d'une entreprise est typiquement basé sur Ethernet. Le réseau d'un opérateur intercontinental consiste de fibres optiques et utilise donc des protocoles et technologies très différentes.

Le langage commun qui permet à tous ces réseaux de communiquer est le protocole IP. IP est donc le protocole qui permet l'interconnexion de réseaux hétérogènes.

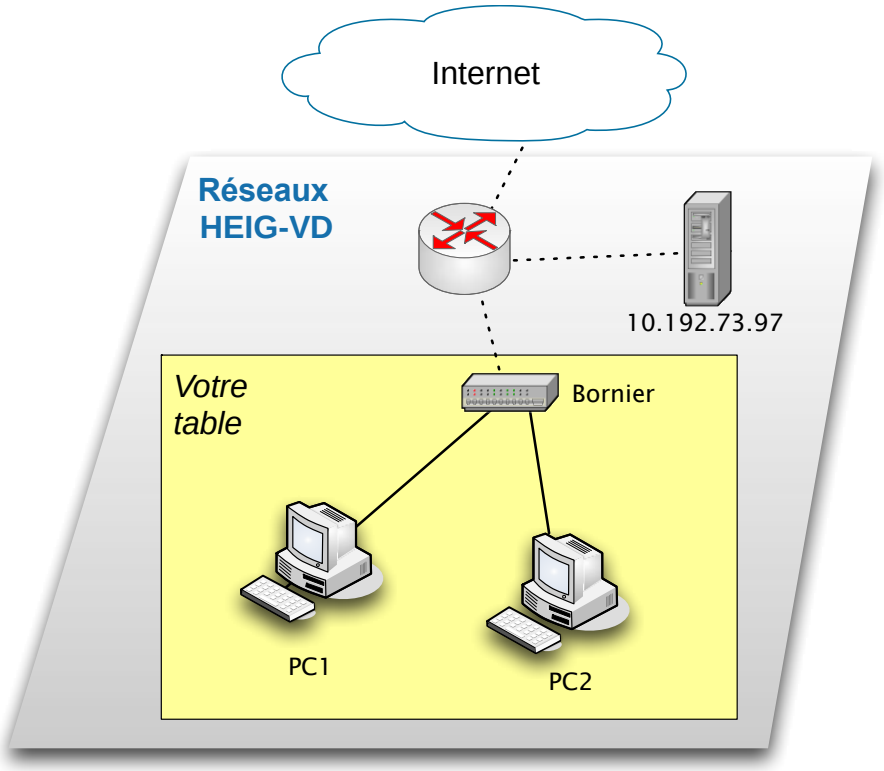
IP définit principalement deux choses :

- les mécanismes et formats de transmission de paquets
- l'adressage des nœuds (adresses IP).

Dans ce laboratoire, nous allons étudier le premier point afin de comprendre comment les données sont transmises entre une application source et une application destinatrice. Nous allons aussi étudier les numéros de port qui permettent communiquer avec plusieurs applications sur la même machine.

2 Matériel

Pour ce laboratoire, nous avons besoin de deux PCs Linux connectés à Internet.



Objectif 1 : Analyse des protocoles IP et TCP

Le premier objectif est d'apprendre le format des paquets IP et TCP.

L'objectif est atteint si vous savez décrire les champs les plus importants des paquets IP et TCP.

Procédez par les étapes suivantes :

1. Lancez Wireshark et utilisez comme filtre d'affiche « http ».
2. Avec le navigateur, connectez-vous sur un site Web.
3. Analysez les paquets IP et TCP.
   Les formats des paquets IP et TCP sont montrés ci-dessous.

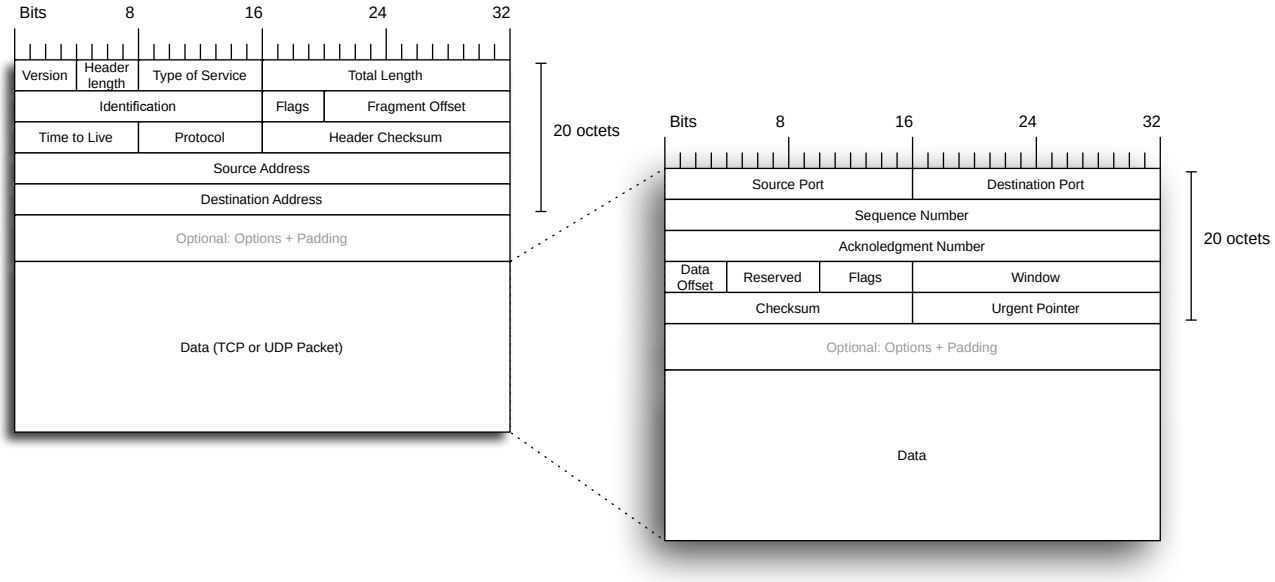


Figure 1: Format des paquets IP et TCP

4. Lisez les spécifications de
   IP (RFC 791, http://www.ietf.org/rfc/rfc791.txt, pages 11-14) et de
   TCP (RFC 793, http://www.ietf.org/rfc/rfc793.txt, pages 15-16)
   et décrivez les champs suivants :
   a. IP : *Version, Time to Live, Protocol, Source Address, Destination Address*
   b. TCP : *Source Port, Destination Port*
5. Indiquez comme exemples les valeurs de ces champs que vous voyez dans la capture Wireshark.

Objectif 2 : Identifier les services d'une machine

Le premier objectif est d'apprendre à identifier les services qui tournent sur une machine.

L'objectif est atteint si vous savez :

- utiliser le logiciel nmap pour énumérer les services actifs sur une machine,
- connaissez les numéros de ports utilisés par les services les plus courants.

ATTENTION

Avant de continuer, voici un mot de précaution. Vous allez apprendre à utiliser l'outil *nmap* pour scanner les ports ouverts d'une machine. Ce logiciel est un outil précieux pour un administrateur de système ou un expert de sécurité afin détecter des failles de sécurité. Mais il est aussi souvent utilisé par des pirates informatiques.

Effectuer un port scan sur une machine qui ne vous appartient pas peut – selon le pays – avoir des conséquences légales.

Afin de garder un comportement éthiquement correct, **ne scannez pas de machines sans autorisation.**

Les numéros de port permettent à plusieurs applications sur la même machine de communiquer avec l'extérieur. Une application peut donc être contactée lorsqu'on connaît son adresse IP et son numéro de port[1].

Les services comme HTTP ou Mail utilisent des ports fixes qui ont été définis dans une norme. Les clients, par exemple le navigateur Web, utilisent des ports aléatoires qui changent pour chaque connexion.

Exercices

- Scannez d'abord votre propre machines Linux avec la commande :

```
sudo nmap -sV 127.0.0.1
```

  nmap a beaucoup de fonctions de balayage de ports. L'option –sV est déjà avancée. Elle ne teste pas seulement si un port est ouvert, mais essaye de confirmer la version du serveur qui travaille sur ce port.
- Analysez les services qui tournent sur la machine Linux. Qu'est-ce que vous en pensez ?

[1] Plus correctement : il faut aussi connaître le protocole de transport : TCP ou UDP.

- Puis, récupérez l'adresse IP de la machine Windows sur laquelle la VM tourne et effectuez un scan. Analysez les services. Qu'est-ce que vous en pensez ?
- Finalement scannez l'équipement 10.192.79.176 avec la commande

```
sudo nmap -sV -p 1-100 10.192.79.176
```

Cette commande ne scanne que les ports 1-100, pour limiter le temps. Un scan complet prend beaucoup de temps.

- Analysez les services qui tournent sur cet équipement. Qu'est-ce que vous en pensez ?
- Afin de mieux connaître les numéros de port les plus courants, cherchez les informations pour compléter le tableau ci-dessous avec les numéros de ports les plus courants.

Numéro de port	**Service**	**Description**
80	Web (HTTP)	Utilisé par les serveurs Web pour les requêtes http://…
20, 21		
22		
25		
53		
443		

Objectif 3 : Expérimenter avec les connexions

L'objectif de cette partie est de s'amuser en explorant l'outil Netcat.

J'espère que l'objectif va être atteint.

Nous allons explorer un autre outil précieux : l'outil Netcat (nc). Netcat est le 'couteau suisse' des outils réseau. Il vous permet de chatter entre deux machines, de transférer des fichiers, de simuler un serveur Web, et beaucoup plus. Mais comme nous allons voir, Netcat est très simple.

Chatter

Essayez le suivant :

- Sur le PC1 Linux, lancez Netcat comme serveur qui écoute le port 7777 :

```
ncat -l –p 7777
```

- Sur l'autre machine, connectez-vous comme client sur ce serveur :

```
ncat adresse_ip 7777
```

- en remplaçant *adresse_ip* par l'adresse IP du PC1.

Ensuite tapez du texte sur les deux consoles. Vous pouvez chatter ! Pour quitter, tapez Ctrl-C.

Transférer un fichier

Pour transférer un ficher avec Netcat, essayez le suivant :

- Sur le PC1, lancez Netcat comme serveur sur le port 7777

```
ncat -l –p 7777 > monFichier
```

  La fin de la ligne '> monFichier' redirige les données reçues dans le ficher monFichier.
- Sur le PC2, créez un fichier quelconque, par exemple avec un document LibreOffice
- Toujours sur le PC2, tapez la commande pour transférer le fichier :

```
ncat adresse_ip 7777 < nom_du_fichier
```

  La dernière partie de la commande '< nom_du_fichier' redirige le contenu du fichier à la commande nc.

Avec ces deux commandes vous avez transféré le fichier entre les deux ordinateurs.

Simuler un serveur Web

Un serveur Web écoute le numéro de port 80. Donc avec Netcat vous pouvez simuler un serveur Web. Il y a déjà un serveur Web qui utilise le port 80, donc nous allons démarrer notre serveur Web simulé sur le port 7000 :

- Sur le PC1, lancez Netcat comme serveur sur le port 7000.
- Sur le PC2, ouvrez le navigateur et tapez http://<adresse IP>:7000, avec l'adresse IP du premier ordinateur.
- Sur le PC1, vous voyez la requête HTTP envoyé par le navigateur.
- Sur le PC1, tapez « Hello », Enter, puis Ctrl-C pour fermer la connexion.
- Dans le navigateur, vous voyez le texte envoyé depuis le PC1.

Simuler un navigateur

Vous pouvez aussi simuler un navigateur, donc un client Web.

- Sur un des PC, tapez

```
ncat www.google.ch 80
```

- Pour vous connecter au server Web Google.
- Puis, dans la console, envoyé une requête HTTP :

```
GET / HTTP/1.1
<ENTER>
<ENTER>
```

- Vous verrez que Google vous envoie la page Web http://www.google.ch

Le serveur Web le plus simple du monde

Pour terminer, vous pouvez construire le server le plus simple du monde avec Netcat.

- Sur PC1, tapez la commande

```
while true; do { echo -e 'HTTP/1.1 200 OK\r\n'; echo Heure à Yverdon;
date; } | sudo ncat -l –p 7000; done
```

- Sur PC2, utilisez le navigateur pour accéder à l'adresse IP et port 7000 du PC. Rafraichissez la page plusieurs fois et regardez l'heure affichée.
- Expliquez comment la commande sur PC1 fonctionne !

Quelques questions

Pour revenir aux choses sérieuses, répondez aux questions suivantes :

- Pourquoi, à votre avis, faut-il exécuter la commande comme administrateur (avec sudo) si l'on veut lancer un serveur sur un port 1 – 1023, mais pas sur les ports supérieurs à 1023 ?
- Est-ce qu'il est possible de lancer deux services qui écoutent le même numéro de port sur la même machine ?
- Et si un utilise TCP (*nc -l -p no_de_port*) et l'autre UDP (*nc -l -u meme_no_de_port*) ?

3 Exercices avancés

***Les exercices de cette section ne sont pas obligatoires**. Ils ne seront pas considérés pour la note.*

Mais si vous avez de l'intérêt et du temps, je vous encourage à les faire, afin d'approfondir vos connaissances et apprendre encore d'avantage sur les technologies des réseaux. Dans ce cas vous pouvez joindre vos réponses aux exercices avancés au rapport de laboratoire.

Approfondir vos connaissances des outils réseau

Netcat et nmap sont des outils précieux et puissants. Si vous avez le temps, pouvez pouvez approfondir vos connaissances de ces deux outils, par exemple avec ces tutoriels :

- Nmap : http://nmap.org/bennieston-tutorial/
- Netcat : http://www.binarytides.com/netcat-tutorial-for-beginners/

D'autres outils vous permettent d'examiner le trafic réseau sur une machine Linux :

- Afficher les connexions ouvertes d'une machine Linux

```
netstat -tlpn
```

- Afficher les activités réseau en continu

```
lsof -i -r
```

- Cette commande montre les connexions établies par une machine Linux. Après l'avoir exécutée, utilisez par exemple votre navigateur. Terminer la commande avec Ctrl-C.

Un autre outil très pratique est wget. Il simule un client Web sans avoir besoin d'un navigateur. Par exemple pour télécharger un fichier dont vous connaissez le lien :

```
wget http://www.heig-vd.ch/docs/pdf-calendriers-
academiques/calendriers-academiques-2012-2013-departement-tin-tic.pdf
```

Et après autant de travail, nous méritons bien un peu de loisir. Utilisez Netcat pour regarder la guerre des étoiles :

```
nc towel.blinkenlights.nl 23
```