Labo 1A : Introduction à internet (60 min)

1 Objectifs

Le but de ce labo est d'illustrer l'architecture d'internet au travers de diverses commandes (ipconfig, ping, tracert, …) et de logiciels gratuits tels que superscan.

2 Configuration du poste de travail 10'

Objectif Ouvrir une session utilisateur Username=**ursula** password=**user**

Remarques Votre PC (Vista Enterprise), désigné par Dx (D1-D16), est situé dans l'intranet

Action *Start – Run…* - **`\\10.1.1.1\FilesTD\Labo409\Labo1`**
S'authentifier sur le serveur Username=**rpi** password=**rpi**
Conserver cette fenêtre de partage

Objectif Déterminer la config. TCP/IP de votre poste (slide 19)

Action Ouvrir l'interface de commande **Command Prompt** situé sur le bureau
Typer **`c:\..>ipconfig /all`**

Question 2a Indiquer la valeur de l'adresse Ethernet
Question 2b Indiquer la valeur de l'adresse IP
Question 2c Indiquer la valeur de l'adresse IP de "mon" serveur DNS (voir slide 10)
Question 2d Indiquer la valeur de l'adresse IP du routeur (slide 19)

Question 2e Compléter la figure ci-contre représentant votre PC avec les valeurs numériques des différentes couches

Remarque Vous pouvez obtenir les mêmes informations depuis Start – Settings – Network Connections en effectuant un clic droit sur Local Area Network puis Status - Details…
Fermer avec Close pour sélectionner Properties (marqué du bouclier)
Vista vous demande une authentification avec droit admin (user = albert pass = admin) pour ouvrir *Local Area Connection Properties* et modifier la configuration.

3 Commande ping 5'

Objectif Utiliser la commande ping qui permet de mesurer le temps aller et retour d'un paquet

Action Dans l'interface de commande, typer **`c:\..>ping www.cern.ch`**

Question 3a Quel est l'adresse IP correspondante ?
A quelle classe d'adresse appartient-elle ? Voir slide 17

Question 3b Pour cette commande ping, pouvez-vous utiliser en argument l'adresse IP à la place de www.cern.ch ?

Remarque Vous pouvez retrouver les commandes précédemment entrés avec la touche curseur ↑

Question 3c Qu'observez-vous pour la commande ping www.microsoft.ch ?
Contrôler que ce site est en fonction avec le navigateur Internet Explorer (IE)
Expliquer la contradiction observée

4 Full Qualified Domain Name (FQDN), adresse IP, résolution DNS 15'

Objectif Comprendre les mécanismes liés au DNS (slides 8, 9, 10)

Action Ouvrir le navigateur IE pour contrôler que FQDN=www.td.unige.ch correspond à IP=129.194.184.80

Question 4a Utiliser la commande ping pour compléter le tableau

FQDN	Adresse IP
www.td.unige.ch	
ftp.td.unige.ch	
s1.tdeig	

Question 4b Qu'y a-t-il de particulier pour FQDN = s1.tdeig ?

Action Typer la commande **`ipconfig /displaydns`** pour afficher le contenu du cache DNS de votre PC.

Remarque Vous pouvez effacer le contenu de ce cache avec la commande **`ipconfig /flushdns`** puis entrer à nouveau les commandes ping précédentes afin de contrôler précisément le contenu de ce cache.

Question 4c Des sites importants comme google.com comprennent actuellement 30 *clusters* de 2000 serveurs. Comment procédez-vous pour connaître 3 adresses IP différentes correspondant à www.google.com ?

Objectif Modifier le fichier **c:\WINDOWS\system32\drivers\etc\hosts** pour rediriger les requêtes destinées à www.company.com sur l'adresse IP = 129.194.184.80

Action Contrôler qu'un utilisateur comme ursula ne peut pas modifier ce fichier
Depuis Start – Programs – Accesories, sélectionner Notepad par un clic droit puis Run as administrator pour lancer Notepad avec les droits administrateur
File – Open…
Se mettre dans le répertoire **c:\WINDOWS\system32\drivers\etc** puis taper **`hosts`** pour ouvrir le fichier, ajouter l'équivalence IP FQDN
Contrôler avec IE que la requête http://www.company.com est redirigée sur cette adresse IP.

Remarque Les mécanismes DNS étant vitaux pour communiquer sur internet, il est important d'en comprendre le fonctionnement pour identifier les risques potentiels.

Client DNS Lors d'une résolution DNS (ping www.cern.ch, http://www.google.com, …), le client DNS de votre poste de travail effectue les opérations suivantes jusqu'à ce qu'il obtienne l'adresse IP correspondante (slide 10) :

1. Lire le fichier c:\WINDOWS\system32\drivers\etc\hosts
2. Lire le cache (résultat identique à ipconfig /displaydns)
3. Demander que "son" serveur DNS (voir §2) lui fournisse la réponse

Durée de vie Les mécanismes DNS font un large usage de mémorisations intermédiaires dans le cache DNS du poste de travail et dans les caches DNS des divers serveurs DNS.

Action Ouvrir le navigateur pour sélectionner divers liens puis observer la durée de vie (commande ipconfig / displaydns - champ Time To Live) de chaque équivalence présente dans votre cache DNS.

5 Commande tracert (traceroute) 5'

Objectif Utiliser la commande tracert qui permet de déterminer le nombre de routeurs traversés (slide 16)

Action Exécuter la commande **`tracert www.luth.se`**

Question 5a Combien y a-t-il de routeurs ?
Question 5b Quelle est l'adresse IP du serveur web = www.luth.se

Remarque Lancer le navigateur sur cet URL puis sélectionner **English** (en haut à droite) pour connaître la position géographique

Remarque Vous pouvez utiliser le site web http://visualroute.bboxbbs.ch/ si le flux ICMP est bloqué dans votre entreprise.

Variante Choisir d'autres destinations au format FQDN ou adresse IP

6	**Port TCP/UDP**	10'

Objectif Comprendre la notion de port (slide 20)

Action Contrôler avec IE que le serveur 129.194.184.80 héberge 2 sites web sur les ports 80 (défaut) et 8080.
Ouvrir IE puis entrer : http://129.194.184.80
http://129.194.184.80 :80
http://129.194.184.80 :8080

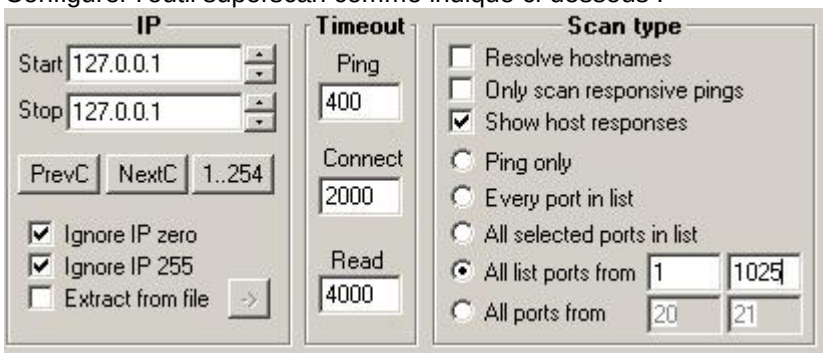
Objectif Utiliser l'outil Superscan qui tente d'établir diverses connexions afin d'aficher la liste des ports Ouverts

Descriptif Produit développé en 2000 par Foundstone
A powerful connect-based TCP port scanner, pinger and hostname resolver.
Multithreaded and asynchronous techniques make this program extremely fast and versatile.
Perform ping scans and port scans using any IP range or specify a text file to extract addresses from.
Scan any port range from a built in list or specified range.
Resolve and reverse-lookup any IP address or range.
Modify the port list and port descriptions using the built in editor.
Connect to any discovered open port using user-specified "helper" applications (e.g. Telnet, Web browser, FTP) and assign a custon helper application to any port.
Save the scan list to a text file.
User friendly interface.

Action Exécuter Superscan (raccourci Bureau)

Objectif Connaître l'empreinte *(fingerprint)* que votre PC transmet à un *hacker*

Action Configurer l'outil superscan comme indiqué ci-dessous :



Remarque L'adresse IP = 127.0.0.1 (présente dans le fichier c:\WINDOWS\system32\drivers\etc\hosts) désigne la machine locale (votre PC)

Question 6a Quels sont les ports ouverts ?
Attendre la fin du *scan*, puis cliquer sur Expand all
Question 6b Sont-ils nécessaires pour un usage stricte en mode client ?
Question 6c Quels sont les ports ouverts pour www.td.unige.ch et 10.1.1.10

Remarque Il est important de comprendre qu'une attaque ne peut s'effectuer que sur un port ouvert et qu'une configuration sécurisée du poste de travail ou d'un serveur doit limiter les risques en fonction des besoins des utilisateurs.
L'excellent site http://www.dshield.org/trends.html vous renseigne en temps réel sur les ports les plus visités par les *scanners* du type superscan, nmap, …
Certains, comme nmap, tentent d'identifier le type du système d'exploitation de la cible distante.

7 Transfert de fichier 5'

Objectif Récupérer le fichier Programme.pdf situé sur ftp.td.unige.ch (slide 13)

Action Ouvrir le navigateur puis entrer ftp://ftp.td.unige.ch/
User Name **oiseau** *Password* **bleu**
Copier ce fichier dans D:\

Remarque L'opération précédente a été effectuée dans une interface graphique *(*GUI = *Graphical User Interface)*
Vous pouvez obtenir le même résultat en ligne de commande *(*CLI = *Command Line Interface)*

Action

```
C:\...>ftp ftp.td.unige.ch
User ...: oiseau
Password: bleu
ftp> cd abc
ftp> get programme.pdf
```

Remarque Le firewall windows envoie un message indiquant qu'il a bloqué le transfert ftp, cependant il est possible d'autoriser le transfert (pour cela, sélectionner Unblock)

Remarque Le fichier sera alors copié dans le dossier utilisateur (ici C:\Users\ursula)

Question 7a Comment s'appelle la valeur affichée en Kbytes/sec ?
Question 7b Quelle est la valeur théorique maximum ?

8 Navigateur 5'

Objectif Contrôler que IE est capable de lire divers formats .txt .jpeg

Action Ouvrir IE et lui glisser divers formats de fichiers
Utiliser ceux présents dans la fenêtre \\10.1.1.1\FilesTD\Labo409\Labo1
Fermer puis ouvrir IE pour chaque nouveau fichier

9 En réserve

Objectif Utiliser l'outil Cyberkit 2.2 : Ping, TraceRoute, … Whois, NS LookUp, …
Recourir au besoin à l'aide

Objectif Utiliser quelques possibilités du site http://www.iptools.com/

Labo 1B : Organismes internet (30 min)

1 Objectifs

Cette partie pratique utilise divers liens pour illustrer la structure de l'ISP *(Internet Service Provider)* Switch, la gouvernance *internet* et le service whois.

2 Structure réseau (Switch, CERN, …) et serveurs *root* DNS 10'

Introduction Cet opérateur *internet (Internet Service Provider)* raccorde les diverses hautes école (EPF-Uni-HES) de Suisse.

Objectif Cette première carte http://www.switch.ch/fr/network/infrastructure/ donne la structure du réseau basée sur des liaisons fibre optique *(dark fiber)* et précise en bas de page les connexions avec *internet*

Remarque La terminologie *dark fiber* signifie que l'utilisateur est libre de placer les équipements (routeurs) de son choix aux extrémités de cette fibre.
Certains opérateurs préfèrent offrir un service avec routeur afin d'utiliser cette fibre à leur guise.

Utiliser le lien CIXP *(CERN Internet eXchange Point)* (http://www.cixp.ch) pour découvrir l'importance du CERN depuis 1989 comme un point d'interconnexion majeur en Europe à *internet*.

Actions Sélectionner :
Members – Telecom Operators
Members – Internet Service Providers
Miscellaneous – Traffic Statistics
Selon http://www.dicodunet.com/definitions/hebergement/mrtg.htm
MRTG est un outil pour surveiller la charge de la circulation des données qui transitent sur un réseau, un sous-réseau ou sur certaines machines.
MRTG produit des pages HTML contenant des images qui fournissent une représentation visuelle du trafic désiré.
MRTG est basé sur les langages Perl et C, il fonctionne sous UNIX et Windows NT.
MRTG est utilisé sur l'ensemble de la toile et est devenu l'un des systèmes d'analyse de monitoring les plus importants.
Miscellaneous – Other Internet Exchanges
Miscellaneous – I.root-servers at CIXP
Une copie du serveur DNS i-root présente à Genève

Remarque Le site http://www.root-servers.org énumère les 13 (A – M) serveurs DNS *root*
Le 21 oct 2002, 7 serveurs étaient indisponibles suite à une attaque de type *Distributed Denial of Service*

Objectif Connaître grâce à http://www.switch.ch/network/stat/weather/weathermap.html le bulletin de santé du réseau Switch

Actions Situer CERN, GE, EPFL, UniLausanne, …
Placer le curseur sur une flèche pour connaître la charge moyenne (30 min.)
Observer la charge dans le sens opposé

3 Noms de domaine 10'

Introduction L'opérateur Switch gère les domaines **.ch** et **.li**

Objectif Recherche d'informations sur des noms de domaine

Action Utiliser le site **www.nic.ch**
Sélectionner (à gauche) **Chercher** pour savoir si un nom de domaine est déjà réservé

Question3a Utiliser http://www.ripe.net/whois pour déterminer la date d'enregistrement et le nom du propriétaire du domaine unige.ch

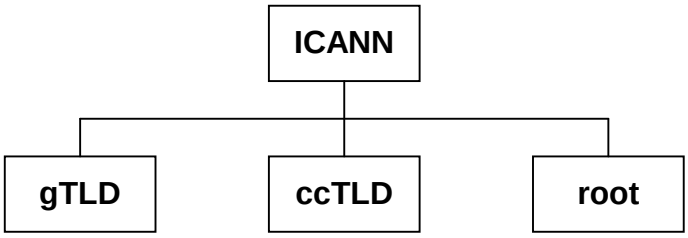
4	**Gouvernance *internet***	5’

Introduction

Le lien http://www.icann.org/faq/ précise les principales missions de *Internet Corporation for Assigned Names and Numbers* (ICANN) créé en novembre 1998.

Selon l’UIT, *ICANN manages the allocation and assignment of IP addresses and autonomous system numbers. IP numbers are allocated or assigned, upon documented requests, in the form of address blocks from the Internet Assigned Numbers Authority (IANA) to Regional Internet Registries. These registries, in turn, assign blocks of addresses to Internet Service Providers (ISP), who then use them to number downstream customer*

Structure



Generic Top Level Domain	(slide 8)	http://www.iana.org/gtld/gtld.htm
Country Code Top Level Domain	(slide 8)	http://www.iana.org/cctld/
Root	(slide 8)	http://www.root-servers.org

5	**Quelques liens en réserve**

http://www.arin.net/	American Registry for Internet Numbers (ARIN)
www.apnic.net	Asia Pacific Network Information Center (APNIC)
http://www.wipo.int/amc/en/index.html	Centre d’arbitrage et de médiation de l’OMPI
http://www.isc.org/ops/ds/reports/2005-07/	Internet Domain Survey, Jul 2005

Number of Hosts advertised in the DNS
Distribution of Top-Level Domain Names by Host Count
Distribution by Top-Level Domain Name by Name
Top 100 Host Names
Top 100 Second-Level Domain Names → bluewin.ch
Host Count Graph
Domain Server Software Distribution