TELECOM Nancy 1A - RS -Réseaux
TP n°1 Modèle en couches et couche Applicative

1 Introduction au Cyber-range de TELECOM Nancy

La plateforme Cyber-range de HNS permet la création de topologies réseau constituées de machines virtuelles (Virtual Machines). Elle est notamment utilisée dans les cours de cybersécurité (scénarios de type "capture the flag"). Pour pouvoir réaliser les TP du module Réseau, chaque élève dispose d'une mini-topologie de réseau d'entreprise constituée de 5 éléments :

- un accès à Internet (Topology Gate)
- une passerelle / pare-feu (pfsense)
- un switch
- deux machines sous linux debian

L'intérêt du cyber-range est double :

1. chaque élève dispose de sa topologie qui persiste d'un TP à l'autre
2. vous avez les privilèges d'administrateur sur toutes les VMs de votre topologie

1.1 Connexion au cyber-range

Un client lourd, appelé "hyneview", est nécessaire pour se connecteur au cyber-range. Il existe pour Windows et Linux et peut être téléchargé à cette adresse : `http://matrix-repository.telecomnancy.univ-lorraine.fr/` [1]. Il peut être exécuté dans toutes les salles de TP de l'école mais également sur vos machines personnelles.
À noter : la connexion au cyber-range n'est possible qu'au sein du réseau de l'école, soit physiquement, soit en utilisant le VPN (voir la page de l'intranet consacrée s'il vous faut le configurer).
Une fois le client hyneview téléchargé et exécuté, vous devez vous connecter au serveur du cyberrange (ci-dessous) avec le couple login/ mot de passe qui vous sera fourni par l'enseignant. Celui-ci est spécifique au cyber-range et vous devez le conserver pour les prochains TPs.

`matrix.telecomnancy.univ-lorraine.fr:4063`

Une fois connecté, il ne vous reste plus qu'à ouvrir votre topologie réseau nommée "Réseaux NOM_DE_FAMILLE".

1.2 Utilisation du cyber-range

Toutes les VMs instanciées dans les topologies partagent les ressources (mémoire, CPU, stockage) des deux serveurs du cyberrange. **Veillez à bien éteindre vos VMs à la fin du TP** (ou plus généralement quand vous avez fini d'utiliser votre topologie) pour libérer les ressources pour les autres utilisateurs.
Pour démarrer une VM il faut faire :

1. Define Entity -> Intelligent (répartit équitablement la charge entre les serveurs)
2. Start Entity

Pour que l'initialisation des interfaces réseau se passent bien il faut démarrer les VMs dans cet ordre : 1)Topology Gate, 2)Switch, 3)Pfsense. Puis attendre que Pfsense soit démarré (environ 1 minute) pour finir par les deux machines terminales. Une fois une VM démarrée un double clic sur son icône ouvre le déport d'écran (Remote Display).
Les identifiants pour se logger sur les VMs sont les suivants :

1. cette page semble poser problème avec certains navigateurs (Chrome) qui force une consultation en https

— sur l'interface web de pfsense (accessible avec un navigateur à l'adresse 192.168.1.1) : admin / pfsense

— sur les systèmes linux debian : hns / hns

Pour arrêter une VM il faut faire :

— *De préférence*, Shutdown (ou bien arrêter la VM via son interface graphique) = arrêt propre via signaux système

— *Ou, en cas de problème*, Stop Entity (revient à couper l'alimentation)

— Undefine Entity

Pour chacun des exercices ci-dessous il vous est demandé de d'observer le trafic réseau correspondant avec l'analyseur de traffic Wireshark (vu en cours) : soit en réalisant la capture depuis le switch, soit directement sur les marchines terminales.

Exercice 1 Vérifier la bonne connectivité de chacune des deux machines de votre réseau :

1. l'interface réseau de votre machine (eth0) est-elle activée et a t-elle reçue une adresse IP locale (192.168.1.X) de la passerelle via DHCP : *ip a* ?
2. pouvez-vous pinger l'interface LAN de la passerelle : *ping 192.168.1.1* ?
3. pouvez-vous pinger pinger une adresse IP à l'extérieur de votre réseau local : *ping 8.8.8.8* ?
4. pouvez-vous faire une résolution DNS : *nslookup www.univ-lorraine.fr* ?

2 DNS

Exercice 2

Configuration DNS locale :

1. Rajouter un second serveur DNS à vos machines, par exemple 1.1.1.1 ou 8.8.8.8. Il faut pour cela rajouter une seconde ligne *nameserver* au fichier /etc/resolv.conf.
2. Dans l'interface web de pfsense, dans Services / DNS Resolver / General Settings, donnez un nom spécifique à chacune de vos deux machines et vérifiez que leur nouveau nom peut être résolu. Il faut pour cela ajouter deux entrées dans la section Host Overrides. Au niveau du domaine demandé, renseignez simplement localdomain.
3. Montrer comment la résolution locale avec le fichier /etc/hosts peut prendre le pas sur le service DNS. Quel en est l'impact en terme de sécurité ? Pour information, l'ordre de consultation des bases de données est défini dans le fichier /etc/nsswitch.conf.

Requêtes DNS diverses :

1. Observer avec Wireshark les requêtes DNS générées lors de la consultation de sites web.
2. dig permet d'envoyer des requêtes DNS et de consulter les réponses. nslookup et host proposent un service similaire mais moins complet. A l'aide de l'outil dig , effectuer différents types de requêtes DNS (directe, inverse, mail exchange, name server, etc.) pour le nom de domaine de votre choix, par exemple *univ-lorraine.fr*. Pour chaque requête, expliquer les éléments de réponses donnés.
3. Interroger l'annuaire avec la commande whois pour obtenir des informations relatives à quelques domaines de votre choix.

3 Web

Exercice 3 HTTP (HyperText Transfer Protocol) est le protocole de transfert d'hypertextes utilisé par les client/serveur WEB. Il est défini dans les RFC rfc2616 pour HTTP/1.1. Nous allons considérer pour cet exercice le site `www.videolan.org` qui propose deux modes d'accès : via HTTP ou HTTPS (et sans rebasculement automatique vers le second comme c'est aujourd'hui l'usage).

1. Dans Firefox, ouvrez les outils de développement web (Ctrl+Shift+I) et allez dans l'onglet "Réseau".

2. Capturer des traces HTTP à partir de `wireshark` en accédant à `http://www.videolan.org/` depuis votre browser.
3. Déterminer la première requête HTTP envoyée au serveur web et analyser l'entête HTTP.
4. Dans wireshark, suivre le flux TCP lié à cette requête et vérifier que le contenu du fichier HTML apparaît en clair.
5. Comparer les traces capturées par wireshark aux objets téléchargés par Firefox. Déterminer le nombre de messages GET nécessaires au chargement de la page.

HTTPS (Hypertext Transfer Protocol Secure)

1. Après avoir vidé le cache ou dans une nouvelle fenêtre de navigation privée, recharger la même page en HTTPS tout en faisant une nouvelle capture avec wireshark : `https://www.videolan.org/`.
2. Observer la pile protocolaire différente du précédent chargement et notamment l'utilisation de TLS.
3. Vérifier que le contenu transitant sur le lien est désormais chiffré.

4 SSH et Rsync

Exercice 4
SSH (Secure SHell) est un utilitaire fondamental qui permet d'ouvrir un terminal à travers une connexion chiffrée TLS sur un hôte distant (voir également son corollaire scp).

1. Lancer le service SSH sur vos machines et tester son bon fonctionnement.
2. Faire un transfert de fichier texte à l'aide de la commande scp entre vos deux machines et capturez le trafic. Vérifier que le contenu du fichier n'est pas visible sur le lien.

Utilisez maintenant la commande rsync pour synchroniser un répertoire entre vos machines.

5 FTP (facultatif)

Exercice 5
FTP (File Transfer Protocol) est le protocole standard de transfert de fichier utilisé dans l'Internet. Il est défini dans le RFC rfc959.
Le but de l'exercice est d'utiliser telnet de façon à dialoguer avec un serveur FTP distant. Les étapes sont les suivantes :

1. Récupérer par `ftp anonymous` le RFC décrivant le protocole FTP sur le site `ftp.ripe.net`. Le fichier `rfc959.txt` se trouve dans le répertoire `rfc`.
2. Rechercher le port de service FTP.
3. Faire un `telnet ftp.ripe.net <ftp_port>` et réaliser les opérations suivantes :
   — Taper HELP
   — Faire afficher le répertoire courant. Vous pouvez vous aider du rfc959 et notamment de la section 4.1 (FTP COMMANDS).
   — Aller dans le répertoire rfc.
   — Passer en mode passif. Noter le numéro de port retourné par le serveur <port_data>.
   — Trouver la commande correspondant à ls.
   — Ouvrir dans un xterm et faire un `telnet ftp.ripe.net <port_data>`. Que constatez-vous ?

6 HTTP à la main (facultatif)

telnet est le protocole d'émulation de terminal normalisé dans le cadre de l'Internet. On déclenche un client de la façon suivante : `telnet <hostname>` Si on ajoute un numéro de port après `<hostname>`, le client telnet se connecte en TCP au serveur associé à ce numéro de port sur la station distante. Il est alors possible de communiquer interactivement avec ce serveur à la condition de respecter son protocole.

Exercice 6

Le but de l'exercice est d'utiliser telnet de façon à dialoguer avec un serveur HTTP distant. Les étapes sont les suivantes :

1. Exécuter la commande : `telnet www.loria.fr <http_port>` avec http_port le port de service de HTTP
2. Dialoguer de manière interactive avec le serveur HTTP de manière à obtenir la page d'accueil en français du site interrogé (commande GET) en version HTTP /1.1 ; c'est–dire l'équivalent de http ://www.loria.fr/fr/
3. Que constatez-vous ?