Utilisation Avancée de Wireshark

R303

Dans ce TP, nous allons utiliser Wireshark pour étudier différents scénarios d'analyse de trafic dans un contexte de supervision de réseau ou d'études d'attaques. Ce sera aussi l'occasion de manipuler les nombreuses fonctions avancées de Wireshark.

Vous pouvez télécharger le fichier traces.tar.gz depuis
http://www.i3s.unice.fr/~urvoy/docs/M3105/traces.tar.gz
et dezipper/détarer le fichier pour obtenir les traces sur lesquelles nous allons travailler.

Vous devez envoyer votre rapport en fin de séance à l'encadrant·e par mail.

I – Analyse d'une trace vers un serveur Web.

Ouvrez la trace http_espn.pcap avec Wireshark. Il s'agit de trafic lié au téléchargement de la page d'entrée d'un site Web capturé sur la machine de l'utilisateur.

1. Quelle est la composition de la trace en terme de protocoles UDP/TCP d'une part et d'applications au dessus de ces 2 couches transports d'autre part? Utilisez la fonction **protocol hierarchy** du menu **statistics**.
2. Faire un filtre sur le port 80 TCP seulement. Faites à nouveau un **protocol hierarchy**. On veut comprendre pourquoi la fraction de trafic HTTP est si faible alors que le port 80 est le port HTTP. Pour se faire, analysez la connexion sur le port 38433 :
   a) A quoi servent les 3 premiers paquets TCP ?
   b) Combien d'objets sont demandés par le client ?
   c) Analysez le contenu des paquets TCP avec des données (plus de 66 octets), envoyés depuis le serveur vers le client en réponse au GET :
      i. Où se situe le 200 OK dans les données : utilisez la sous-fenêtre d'en bas de Wireshark, pas la fenêtre intermédiaire.
      ii. Quelle trame Wireshark marque comme HTTP (dans la fenêtre intermédiaire) et quelles trames marque-t-il comme TCP ?
      iii. Quelle semble être la logique derrière ce choix ?
3. Combien y a t-il de conversations au niveau IP, TCP et UDP dans cette trace? Utilisez la fonction **conversations** du menu **statistics** .
4. Relier le niveau Ethernet de la fonction **conversations** du menu **statistics, avec l'endroit où la capture a été faite**?
5. Concentrons nous sur le trafic DNS. Créez un filtre pour ne récupérer que les demandes de résolutions DNS. Pour cela, il faut se placer sur un paquet DNS où il y a une requête, puis sur le champ dans l'en-tête applicative où apparaît le code qui indique que c'est une requête et faire un click droit et **Prepare As filtered** puis **Selected**. Combien en trouvez-vous (Wireshark indique le nombre de paquets filtrés dans la barre en bas) ?
6. Passons aux requêtes HTTP. Pour les trouver, nous allons utiliser la fonction **HTTP - Requests** du menu **Statistics** (appuyez sur **Create Stats** quand on vous le demande).
   a) Interprétez les 2 premières colonnes du résultat? **Attention, certaines URL sont**

tellement grandes qu'il faut bien scroller à droite pour voir les deux colonnes.

b) En quoi ce résultat est compatible avec l'analyse DNS faite précédemment?

c) Créez un filtre pour calculer le nombre d'objets effectivement téléchargés (en filtrant sur le bon code réponse HTTP du serveur en utilisant à nouveau le **Prepare As filtered** puis Selected). Combien y en a-t-il?

d) Expliquez la différence de 2 objets entre les questions a) et c) en regardant tous les codes réponses du serveur (pas seulement les 200 OK)

II Dépannage

Un utilisateur de votre réseau (vous avez été promu ingénieur réseau – félicitations!) n'arrive pas à accéder à Internet. Il arrive en revanche à accéder aux ressources internes (serveurs de données, mail, imprimantes, etc.). Vous capturez la trace **nowebaccess1**.pcap sur le commutateur d'attachement de la machine de l'utilisateur.

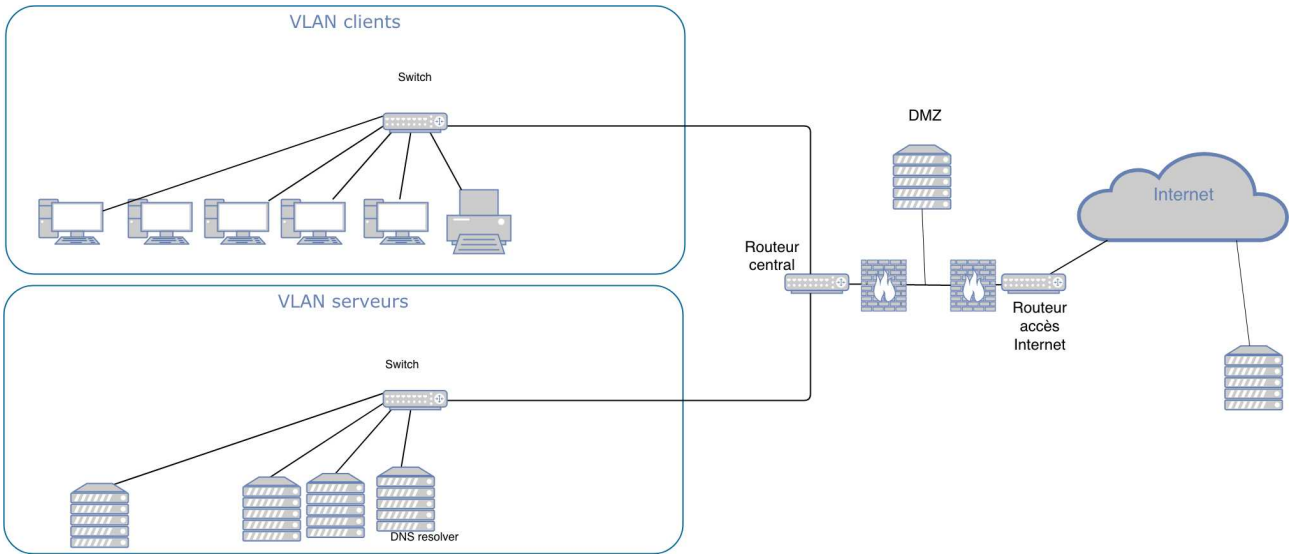
Quelques informations :

- l'adresse IP de la machine de l'utilisateur est 172.16.0.8 et les serveurs DNS configurés sur la machine sont 4.2.2.2 et 4.2.2.1.
- Ne tenez pas compte de « bad internet checksum » au niveau IP (provient vraisemblablement du fait que la capture s'est faite sur une machine où le calcul de la somme de contrôle est déporté sur la carte physique. Wireshark capture avant ce calcule et croit donc à un erreur dans le paquet.)

Il faut penser à la machine comme :

- Appartenant à un VLAN (réseau IP).
- Accédant à un serveur DNS qui est dans un autre VLAN. Ces 2 VLANs sont dans le réseau de l'entreprise.
- L'entreprise accède à Internet via une passerelle (en générale différente de celle entre VLANs internes).

Cela correspond au schéma suivant :



Analysez chaque trame ou groupe de trames pour déterminer ce que fait la machine et poser un

diagnostic de panne.
Il faut être précis. Si par exemple, vous pensez qu'une machine est utilisée comme passerelle, vous devez dire quels éléments vous font penser cela. Pour vous aider à formuler le diagnostic, il faut déterminer :

- Si la machine a une connexion physique qui fonctionne.
- Si la passerelle lui permettant de changer de VLAN dans l'entreprise fonctionne (est bien configurée dans la machine).
- Si la passerelle (routeur) entre l'entreprise et l'Internet semble active.
- Si la configuration DNS de la machine semble correcte.

Notez qu'il y a plusieurs diagnostics possibles et que ce diagnostic peut être partiel car il peut y avoir plusieurs causes possibles à une observation.

III Dépannage bis

Un autre utilisateur se plaint de ne pas pouvoir accéder à certains sites Web (mais pas tous). Vous capturez à nouveau une trace de trafic qui s'appelle nowebaccess3.pcap.

Analysez chaque trame ou groupe de trames pour déterminer ce que fait la machine et poser un diagnostic de panne. Montrer que le problème se situe à l'extérieur du réseau de l'entreprise qui ne comprend que des machines dans la plage d'adresses 172.16/24.

V Processus d'Attaque

Parmi les machines que vous gérez (vous êtes toujours dans le même rôle d'ingénieur réseau), vous en avez une pour laquelle votre système de détection d'intrusions génère beaucoup d'alarmes. Vous capturez du trafic sur le commutateur de rattachement de cette machine. La trace s'appelle attaque1.pcap.

1. Utilisez l'outil **Statistics/Conversation** pour analyser la trace
   a) Combien y-a-t-il de conversations au niveau IP et TCP?
   b) Classez les conversations niveau TCP par nombre de paquets et reportez le résultat dans votre rapport.
   c) Regardez les conversations avec 5 paquets et celles avec 2 et analysez la suite de paquets échangés au niveau TCP: il suffit de partir du menu conversation, de faire un clic droit sur la conversation puis un **Apply as Filter.**
2. Pour comprendre la différence entre les conversations à 2 et à 5 paquets, prenez le cas de votre machine.
   a) Quels sont les services présents sur la machine? (expliquez comment vous avez fait pour les trouver en utilisant la commande netstat (dans le paquet net-tools si netstat n'esgt pas installé)).
   b) Expliquez la différence de comportement au niveau TCP entre les cas où vous faites un telnet (sur l'interface de loopback) sur des ports ouverts ou non et voyez la réaction de la machine au niveau TCP avec wireshark.
   c) Que se passe-t-il pour les cas dans la trace attaque1.pcap où il y a un seul paquet en tout ? (question difficile)