INTRODUCTION A LA SECURITE DES PROTOCOLES RESEAUX
Travaux pratiques : lab n°1 – 2h

Manipulation des protocoles réseaux à l'aide d'outils de sécurité
Captures de trames et création de paquets – découverte de scapy

---

1 Aperçu du lab :

A travers ce TP vous allez approfondir vos connaissances sur le comportement des piles TCP/IP de différents OS. Pour cela vous visualiserez les trames qui circulent sur le réseau, les analyserez, et forgerez vos propres paquets. A partir de là vous pourrez comprendre les réponses qui vous seront envoyées, et avec l'expérience, vous serez à même de les prédire.

Vous travaillerez sur vos deux postes de travail dans un premier temps. L'un sera « l'attaquant » et l'autre la « victime » (ou l'un sera Alice et l'autre Bob ;)). Vous pourrez alternerer les victimes avec des postes de la salle qui disposent d'un OS différent pour pouvoir observer les différences de comportement qui peuvent se produire.

Vous travaillerez de façon totalement autonome, vous devrez donc consulter toute la documentation officielle à votre disposition pour comprendre les options que vous utiliserez et les décrire. Pour pouvoir travailler correctement vous aurez besoin d'un support vous décrivant les en-têtes des paquets de la plupart des protocoles, qui vous sera donc fourni avec le sujet.

Normalement vous avez largement le temps de faire toutes les manipulations dans le temps imparti.

2 Objectifs du lab :

Ce TP n'a pas pour objectif de faire de vous des pirates, il faudrait faire de nombreuses heures d'essais sur des systèmes très différents. Le but est de vous faire prendre conscience de ce que l'on peut voir et faire au niveau des couches basses (2, 3 et 4). Vous comprendrez alors tout l'intérêt des dispositifs de sécurité, et vous serez à même de faire les choix nécessaires.
Vous comprendrez alors concrètement pourquoi on met en place des VLANs, du filtrage de paquet Statefull, …

3 Les consignes :

3.1 Utilisation d'un « sniffer » de trames :

Tout au long du lab vous aurez besoin de capturer le trafic entre vos deux postes. Vous utiliserez l'outil wireshark[1].

3.2 Rappels théoriques sur TCP/IP :

- Expliquez en détail le fonctionnement d'une connexion sur un port UDP. Illustrez vos propos en capturant les trames émises lors d'une requête DNS. Vous pourrez par exemple utiliser la commande `nslookup`.

- Expliquer en détail le fonctionnement d'une connexion sur un port TCP. Illustrez vos propos en capturant les trames émises lors d'une requête HTTP sur un site de votre choix. Pour cela vous ne devrez **pas passer** par votre navigateur Web. Donnez le détail de la(es) commande(s) que vous avez utilisé pour cette requête.

3.3 Étude des approfondie du fonctionnement du réseau avec scapy :

3.3.1 Utilisation de scapy[2] :

Scapy est un utilitaire créé en python vous permettant de forger vous même les paquets que vous allez faire transiter sur le réseau.

a. Découverte de l'outil :
   1. Suivez le tutoriel offciel pour prendre en main l'outil. Concentrez vous uniquement sur les paragraphes suivants de la partie *usage*[3] , tout le paragraphe *Interactive tutorial* jusqu'à *Send and receive in a loop* inclu. Pour tester, forgez quelques paquets, capturez les trames et observez le résultat. Décrivez vos manipulations.

b. Techniques avancées :
   1. Réalisation d'une connexion TCP :
      1. Vous forgerez des trames TCP afin de réaliser de bout en bout une connexion 3 Way handshake. Pour cela vous pourrez capturer une connexion TCP pour visualiser en détail comment se positionnent les options.

   2. ARP cache poisonning :
      1. Forgez quelques trames ARP avec scapy.
      2. Expliquer la technique de ARP cache poisonning.
      3. Tentez de monter cette attaque contre une de vos machines. Pour cela vous forgerez vous même les trames ARP, et n'utiliserez pas les fonctions automatiques intégrées à Scapy. Expliquez en détail comment vous avez fait.

4 Les livrables :

A l'issue du TP, vous devrez me remettre un rapport détaillé de votre travail. Ce rapport devra être correctement rédigé.
Vous indiquerez les systèmes d'exploitation des différents postes sur lesquels vous avez travaillé ainsi que leurs adresses IP respectives. (attaquants et victimes)
Pour chacun des points à traiter vous fournirez l'explication détaillée des manipulations que vous avez

1 https://www.wireshark.org/
2 http://www.secdev.org/projects/scapy/
3 http://www.secdev.org/projects/scapy/doc/usage.html

effectuées (commandes et résultats). Vous joindrez les résultats que vous avez obtenus, votre interprétation, ainsi que vos éventuelles remarques et constats. N'hésitez pas également à indiquer vos interrogations sur des résultats.

Pour finir, la note tiendra compte de votre analyse, de la qualité de la rédaction, de votre organisation et du travail en équipe.