ANALYSE DE FICHIERS PCAP

Vue d'ensemble

Ce laboratoire initie à l'analyse de fichiers PCAP à l'aide de l'outil Tshark. Vous analyserez un fichier PCAP existant, à la recherche d'une tentative de connexion invalide spécifique. PCAP signifie "packet capture" (capture de paquet), et c'est un format de fichier standard pour stocker le trafic enregistré à partir d'un réseau.

PCAP (Packet CAPture) est un format de fichier utilisé pour enregistrer les paquets de données qui transitent sur un réseau. Les fichiers PCAP sont utilisés par des outils d'analyse de réseau comme Wireshark, tcpdump, et Tshark pour capturer et enregistrer le trafic réseau pour une analyse ultérieure.

Réalisation du laboratoire

Le laboratoire est lancé depuis le répertoire de travail de labtainer sur votre hôte Linux, par exemple, une machine virtuelle Linux. À partir de là, lancez la commande :

```
labtainer pcapanalysis
```

Le terminal virtuel résultant est connecté à un ordinateur qui contient le fichier PCAP intéressant.

Tâches

1. Exécutez tshark pour effectuer l'analyse PCAP

A) Pour voir les différentes options disponibles pour tshark, faites :

```
man tshark
```

B) Exemple de commande Tshark pour afficher des champs spécifiques :

```
tshark -T fields -e frame.number -e frame.time -e telnet.data -r telnet.pcap
```

2. Affichez le paquet contenant le mot de passe "admin" invalide

Localisez le paquet contenant le mot de passe fourni lorsque l'utilisateur a tenté de se connecter en tant qu'utilisateur "admin".

Avec Tshark, pour afficher uniquement une trame réseau, utilisez l'option `-Y frame.number==N`.

N est le numéro de la trame.

Stop the labtainer

Lorsque le laboratoire est terminé, ou si vous souhaitez arrêter de travailler pendant un moment, exécutez

stoplab

depuis le répertoire de travail du labtainer hôte. Vous pouvez toujours redémarrer le labtainer pour continuer votre travail. Lorsque le labtainer est arrêté, un fichier zip est créé et copié à un emplacement affiché par la commande stoplab. Lorsque le laboratoire est terminé, envoyez ce fichier zip à l'instructeur.