TP1

SNIFFING DU TRAFIC AVEC WIRESHARK

Objectifs :

- Savoir manipuler / monter un réseau virtuel.
- Savoir filtrer les données dans Wireshark.
- Découvrir les vulnérabilités des services Telnet et HTTP.

Introduction

La technique de Sniffing permet de capturer les données transitant sur un réseau. Les pirates informatiques utilisent cette technique afin de récupérer à travers des utilisateurs et des administrateurs réseaux des informations sensibles et confidentielles qui traversent les réseaux telles que les couples : identifiants/mots de passe.

I. Préparation de l'environnement de virtualisation

1. Télécharger et installer la version finale du logiciel *VirtualBox*.
2. Télécharger et installer *Oracle VM VirtualBox Extension Pack*.

II. Préparation des machines virtuelles

1. Depuis votre session sur le site https://foad.ensicaen.fr/ télécharger les deux machines virtuelles « **Student.ova** et **MyServer.ova** ».
2. Importer ces deux machines virtuelles dans VirtualBox.
3. Discuter avec votre enseignant sur la façon de réaliser un réseau virtuel.
4. Lancer la VM « **Student** » et utiliser le compte « student | student » pour se connecter.
5. Lancer la VM « **MyServer** » et utiliser le compte « student | ensicaen » pour se connecter.
6. Attribuer une adresse IP à chaque machine virtuelle.
7. Vérifier la connectivité entre les deux VMs.

   i.e : La machine virtuelle MyServer ne doit pas se connecter au réseau Internet.

III. Capture de mot de passe de Telnet

1. Dans la machine « **Student** » lancer le terminal et taper la commande « *whoami* ».
2. Lancer Wireshark dans la machine « Student » et spécifier l'interface de capture de trafic.
3. Lancer la capture de trafic.
4. Ouvrir un terminal, taper la commande **telnet** suivie de **l'adresse IP** de la machine « **MyServer** »
5. Authentifiez-vous avec le compte de « MyServer »
6. Taper la commande *whoami*. Expliquer le résultat obtenu.
7. Arrêter la capture de trafic dans Wireshark.
8. Analyser le trafic capturé et appliquer un filtrage des données pour le service Telnet.
9. Identifier et extraire le login et le mot de passe échangés lors de la communication.
10. Taper « *quit* » pour sortie de la session telnet.
11. Quelle solution envisagée pour que le données d'authentification soient sécurisés.

IV. Capture des données du protocole HTTP

1. Lancer une nouvelle capture avec Wireshark.
2. Ouvrir le navigateur Firefox.
3. Dans la barre d'adresse URL, taper l'adresse suivante : http://@IP de la machine MyServer
4. Cliquer sur le lien « *DVWA* »
5. Dans la page d'authentification, saisir « admin | password »
6. Une fois authentifié, arrêter la capture des données.
7. Analyser le trafic capturé et appliquer un filtrage des données pour le service HTTP.
8. Quelle solution envisagée pour que le données d'authentification soient sécurisés.

En cas d'erreur de ce genre, utiliser cette solution

Erreur	Solution
E: Could not get lock /var/lib/dpkg/lock-frontend - open (11: Resource temporarily unavailable) **E:** Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), is another process using it?	sudo rm /var/lib/apt/lists/lock sudo rm /var/cache/apt/archives/lock sudo rm /var/lib/dpkg/lock* sudo dpkg --configure –a sudo apt update