SAE11 – TP “Jean Boomer”

Prérequis

Travail à faire avec une machine physique Windows sur le réseau de l’IUT, authentifiée en 802.1x.

Importer sur VirtualBox le fichier de VM présentes sur le NAS :
\\172.16.0.8\TP\SAE11\vm_sae11

Double-cliquer directement, faire importer, soyez patients pendant 5min.Vous obtiendrez 2 VM :
- SAE11-Windows10-JeanBoomer (machine de la victime)
- SAE11-Kali-Linux (machine de l’attaquant ; logs : kali/kali, attention au qwerty)

Vérifier la configuration : chaque VM doit avoir une carte réseau en “NAT” et une en “Réseau privé hôte” ; si besoin, créer un réseau privé hôte dans le menu :
Fichier > Outils > Network Manager > Créer.

Mise en garde

Ce TP est à but pédagogique et est réalisé dans un cadre de jeu, sur des machines virtuelles et des faux comptes. Cela ne veut pas dire qu’il faut tout prendre à la légère et s’imaginer devenir un hacker après coup... Réfléchissez aux conséquences de vos actions sur les réseaux publics : il y a des textes de Loi sur le scan de ports, les attaques par force brute, l’usurpation d’identité, etc.

Merci de ne pas modifier les mots de passe ou ne pas polluer les comptes “fake” du TP.
Cela prends du temps de mettre en place de genre de TP donc respectez le travail des enseignants !

Introduction

Ce TP a pour but de vous faire découvrir les conséquences désastreuses d’une mauvaise application des recommandations de l’ANSSI en ce qui concerne la politique de gestion des mots de passe.

Ça y est, votre vieil oncle Jean Boomer (c’est son vrai nom !) s’est enfin mis à l’informatique. Il a suivi des cours du 3ème age et a une superbe machine Windows 10 avec un compte à son nom. Il a aussi créé des profils sur différents réseaux sociaux… Vous avez un accès physique à ce PC.

Vous êtes dans la peau d’un jeune ethical hacker, et votre but est de découvrir le maximum d’informations sur votre oncle. Vous allez donc réaliser différentes étapes pour prendre le contrôle de ses comptes, pour enfin lui faire la morale et lui préconiser de meilleures pratiques.

Recherche d’informations

1) Accéder à la machine Windows comme vous pouvez… Il doit bien y avoir un moyen de se connecter sur un compte quelconque ! Une fois fait, relever l’adresse IP de la machine.

2) Sur votre machine Kali, vous disposez de l'outil **sherlock** : il s'agit d'un programme d'aide à l'ingénierie sociale qui permet de scanner un grand nombre de sites à la recherche d'un nom d'utilisateur. Utiliser sherlock pour chercher sur quels sites l'utilisateur jeanboomer1964 est référencé.

NB : si besoin, installer ou réinstaller les outils avec la commande apt ; j'ai l'impression que sherlock est un peu capricieux s'il n'est pas à jour.

3) A l'aide de la liste de sites retrouvés, cherchez des informations publiques sur Jean Boomer : centres d'intérêt, famille, date de naissance, … et notez les dans un coin ! Faites attention, il y a beaucoup de faux positifs sur sherlock.

4) L'outil **cupp** (Common User Password Profiler) permet de générer une liste de mots de passes probables à partir de données connues d'un utilisateur. Utilisez-le pour générer une liste pour Jean Boomer.

NB : vu que c'est un TP de découverte, on va éviter de donner trop d'infos à cupp sinon on va se retrouver avec une liste de 100 000 mots de passe potentiels, ce qui prendrait des heures pour l'attaque. Contentez-vous du strict miminum, vous devriez obtenir environ 2300 mots de passe.

5) Lister les services actifs sur la machine de Jean avec **nmap**. Lesquels peuvent être exploités ? Utiliser de la documentation en ligne si vous ne connaissez pas tous les services.

Attaque et contrôle distant

6) Réaliser une attaque par dictionnaire du service exploitable avec l'outil **hydra**
Soyez patients, cela peut prendre une dizaine de minutes…

7) Se connecter à distance sur le compte utilisateur de Jean Boomer avec l'outil **xfreerdp** de Kali

NB : en cas de soucis avec rdp, vous pouvez vous connecter directement sur le profil de Jean Boomer sur la VM !

8) Consulter l'historique de navigation de Jean.
Y-a-t-il un moyen de récupérer d'autres mots de passes ?

9) A partir de ces informations, tentez de récupérer l'accès à la boite mail de Jean Boomer.
Allez donc espionner ses mails !

Durcissement

Essayez de lister le nombre d'erreurs que votre vieil oncle Jean Boomer a réalisé.
Proposez des solutions pour éviter que ce genre de scénario se répète !