DOCUMENT DE CADRAGE DE LA SA11 :

SE SENSIBILISER A L'HYGIENE INFORMATIQUE ET A LA CYBERSECURITE : CHALLENGE FTP

Introduction

Un CTF « Capture The Flag » est une suite de challenges de cybersécurité à enchainer pour récupérer des informations (un fichier, un mot de passe, un accès à une machine, …) que l'on appelle le drapeau.

Deux des plus importantes CTF d'attaques/défenses ont lieu chaque année à la **DEF CON**, la plus grande conférence de hackers et le **NYU-CSAW** (Cyber Security Awareness Week), le plus grand concours de cybersécurité étudiant. Plusieurs IUT R&T en France ou écoles d'ingénieurs organisent aussi des CTF et nous vous indiquerons les dates de ces CTF pour que vous puissiez y participer pendant votre formation.

Les challenges et CTF sont de très bons exercices pour un des métiers dans le domaine de la cybersécurité : pentester. Le pentester réalise des tests d'intrusion c'est-à-dire des évaluations techniques de la sécurité d'environnements informatiques. Il identifie les vulnérabilités et propose des actions de remédiation. Ce métier nécessite des connaissances solides dans différents domaines comme :

- le réseau
- la sécurité informatique (cryptographie, systèmes de codage, audit de sécurité réseau et web)
- le développement logiciel et systèmes informatiques (systèmes embarqués / industriels / …)

On vous propose donc dans cette SAE de réaliser un premier CTF débutant orienté sur le réseau et les cours que vous avez pu avoir pendant ce premier semestre de formation avec l'utilisation de Python et Scapy.

Il existe de nombreuses plateformes proposant ce type d'entrainement. Pour les débutants, certaines plateformes proposent des « challenges » pour vous entrainer avant de passer aux CTF. La plus connue est **Root-Me** : https://www.root-me.org/. **Nous utiliserons cette plateforme pendant la formation et vous devez donc vous y inscrire en utilisant un identifiant comportant les 4 premières lettres de votre prénom suivies des 4 premières lettres de votre nom**. A la fin de la première année il est fortement conseillé d'avoir fait au moins une dizaine de challenges (en réseaux prioritairement mais vous pouvez commencer à explorer d'autres domaines notamment App-systèmes).

Ensuite, vous pourrez faire des CTF sur des plateformes hébergeant des machines à attaquer comme **HackTheBox** : https://www.hackthebox.eu/. Il existe également la possibilité de récupérer les machines sous la forme de machine virtuelle par exemple sur **VulnHub** : https://www.vulnhub.com/.

LE CTF à réaliser

Salut jeune Padawan, les Sith préparent une attaque contre une planète localisée dans la bordure médiane. Heureusement le maître Jedi Guillemin a intercepté la communication chiffrée envoyée par Dark Plageuis à Dark Sidious qui indique la planète qui sera détruite et la date de l'attaque. Il est parti en mission sur Tatouine et te confie la mission de décoder ce message. Fais vite énormément de vies en dépendent ! La communication a été enregistrée dans un fichier nommé McDiarmid.pcapng.

Planning prévisionnel : le planning prévisionnel du travail qui sera réalisé pour cette SAE ainsi que les ressources qui vous aideront à réaliser ce travail sont indiqués ci-dessous :

<table>
<tr><th>Jour</th><th>Volume horaire</th><th>Travail à réaliser en séance</th><th>Encadrant</th></tr>
<tr><td rowspan="2">Lundi 18 décembre matin</td><td>CM 1h</td><td>Présentation de la SAE, Introduction à Scapy</td><td>AyM</td></tr>
<tr><td>Projet 1h</td><td>Analyse de la capture Wireshark et installation du client et serveur FTP</td><td>AyM</td></tr>
<tr><td rowspan="2">Lundi 18 décembre matin – Mardi 19 décembre</td><td rowspan="2">3h encadrée
Projet 5h</td><td rowspan="2">Récupération automatique du login et du mot de passe
Récupération du fichier transmis à partir du numéro de port TCP et décodage du message chiffré</td><td>AyM</td></tr>
<tr><td>Aucun</td></tr>
<tr><td rowspan="3">Mercredi 20 décembre - Jeudi 21 décembre</td><td rowspan="3">3h encadrée et 6h de projet</td><td>Récupération automatique du numéro de port TCP négocié pour le transfert et du fichier</td><td>Aucun</td></tr>
<tr><td rowspan="2">Finalisation et récupération en temps réel du login, mot de passe et du fichier lors d'une connexion à un serveur FTP</td><td>AyM, LB, WG</td></tr>
<tr><td>Aucun</td></tr>
<tr><td>Vendredi 22 décembre</td><td>Soutenances 08h-12h</td><td>Soutenances</td><td>AyM, WG</td></tr>
</table>

Planning prévisionnel de la SAE11

Rendus : pour cette SAE vous devrez réaliser un notebook Jupyter avec les programmes et explications sur la résolution du CTF. Le notebook doit être rendu sur Moodle avant jeudi 21 décembre 20h30 sous la forme d'une archive avec le notebook et un répertoire avec les images de votre notebook.

Nombre d'étudiants par groupe de SAE : 3 étudiants

Enseignants responsables : Ayoub MAMRI (AyB : ayoub.mamri@uvsq.fr),
Willy Guillemin (WG : willy.guillemin@iut-velizy.uvsq.fr),
Lotfi BENACHOUR (LB : lotfi.benachour@uvsq.fr)

Ressources concernées :

- R101 : initiation aux réseaux informatiques
- R102 : architecture des réseaux
- R103 : réseaux locaux et équipement actifs
- Notebook 1 : Introduction à Scapy SAE11
- Notebook 2 : Les fichiers avec Python

Détails du travail à réaliser en séances de projet

Première séance:

Analyse du protocole de transfert de fichier

Tout le travail réalisé ci-dessous devra être dans votre notebook.

1. Ouvre le fichier McDiarmid.pcapng dans Wireshark et mettre une image de cette capture dans ton notebook avec le détail du 2ème paquet.
2. Les informations vitales recherchées ont été transférées dans un fichier codé. En regardant la capture, précise quel protocole applicatif a été utilisé pour l'envoi de ce fichier. Pour la suite tu pourras t'aider de Wikipédia.
3. Quel est l'adresse IP du client et du serveur.
4. Quel protocole de transport est utilisé par ce protocole applicatif et quel est le numéro de ports TCP utilisés par ce protocole (hors transfert de données).
5. Quel est la « banner » message de bienvenue de ce site ?
6. Ces insouciants ne connaissent visiblement tes talents de hacker, ils ont utilisé un protocole transmettant le login et le mot de passe en clair ! Quels sont-ils et dans quels messages sont-ils transmis ?
7. Une seconde connexion TCP est utilisée pour l'envoi des données. Quel message est utilisé pour préciser sur quelle adresse IP et quel numéro de port envoyer les données et comment l'adresse IP et le numéro de port sont indiqués ?
8. Il existe 2 modes de fonctionnement pour ce protocole : passif et actif. Quel mode est utilisé ici ?
9. Combien de transfert de données sont utilisées dans la capture, avec quelles commandes sont-elles initiées et pour quelles données transférées.
10. Quel est le nom du fichier transmis, combien de bytes contient ce fichier à transférer et combien de paquets vont être transmis et avec quelle taille (pourquoi cette taille) ?
11. Quel message marque la fin du téléchargement ?

Installation de FileZilla

1. Installer le client et le serveur FTP respectivement sur vos 2 PC : https://filezilla-project.org.
2. Créer un utilisateur, stocker un fichier et faire un test de téléchargement.

Finaliser votre notebook puis commencer à étudier le fonctionnement de Scapy en regardant le notebook d'Introduction à Scapy.

Deuxième séance:

Récupération automatique du login et du mot de passe

Dans votre notebook :

1. Charger la capture Wireshark dans votre notebook et trouver les paquets avec le login et mot de passe de l'utilisateur.
2. Créer pas à pas les commandes pour récupérer le login et mot de passe de l'utilisateur.
3. Écrire un script pour récupérer automatiquement le login et mot de passe de l'utilisateur.

Récupération du fichier transmis à partir du numéro de port TCP et décodage du message chiffré

1. Comment identifier le plus simplement le paquet transportant les données du fichier transféré (et seulement ces paquets) ?
2. Crée un programme qui récupère toutes les données transférées dans la capture Wireshark et stocke les dans un fichier nommé SW2.pdf.
3. Ouvre le fichier SW2.pdf.
4. Visiblement Dark_Sidious est chargé de tuer un Jedi. Le reconnais-tu sur la photo ?

Les Sith ont utilisés un chiffrement par substitution pour chiffrer le texte (une lettre du message est remplacée par une autre dans le message chiffré). Heureusement une personne infiltrée nous a fourni, au prix de sa vie, la correspondance de la substitution :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
W	S	E	R	D	X	C	F	T	Y	G	V	B	H	U	N	J	I	O	K	L	M	P	A	Z	Q

La première ligne correspond aux lettres du message, et la seconde ligne aux lettres du message chiffré. Par exemple le A est remplacé par W. La ponctuation et les espaces n'ont pas été modifiés.

5. Écrit un programme pour décoder le message. Ton maître Jedi t'indique que tu peux utiliser dans ton programme :
   - la méthode find sur une chaîne de caractères : chaîne.find(caractère) qui renvoie la position du caractère dans la chaîne
   - que si le caractère n'est pas présent, cette méthode renvoie -1
6. Envoie vite (on regardera l'heure d'envoi) à ton maître Jedi la date et la planète qui va être attaquée (sur Moodle dans un fichier txt).

<u>Troisième séance:</u>

Récupération automatique du numéro de port TCP négocié pour le transfert et du fichier

Bravo , tu as fait la partie la plus importante et tu as sauvé beaucoup de vies! Maintenant pour aller encore plus vite la prochaine fois, ton maître Jedi te demande d'automatiser ce travail.

1. Créer pas à pas les commandes pour récupérer le numéro de port négocié pour le transfert de données ainsi que le nom du fichier à transférer.

2. Écrire un script pour récupérer automatiquement le numéro de port négocié pour le transfert, le nom du fichier et le fichier.

Quatrième séance :

Pour éviter d'avoir à te transmettre les fichiers qui nous subtilisons à l'ennemi il est souhaitable que nous puissions récupérer le login/mot de passe et les fichiers en temps réel lorsque nous interceptons les communications des Siths avec nos attaques MITM.

1. Dans un fichier texte (et pas dans ton notebook), écrit un script Python qui :

    a. Sniff les paquets FTP
    b. Récupère le login et mot de passe de l'utilisateur
    c. Identifie le numéro de port négocié pour un transfert de fichier ainsi que le nom du fichier et la fin de transfert
    d. Enregistrer le fichier avec le nom de fichier utilisé pour le transfert

2. Vérifie le fonctionnement de ton script Python en le testant lors d'un transfert de fichier entre le client et le serveur FTP FileZilla. (tu copieras le script dans ton notebook).

3. Explique ce qu'est une attaque MITM.

Rappel : tu as jusqu'à 20h30 pour déposer ton notebook sur Moodle/E-campus/Mail.

PS : qui est ce McDiarmid ?

FICHE D'EVALUATION

Membres du binôme :

……

Le binôme a-t-il réalisé toutes les tâches demandées sur cette SAE ?

☐ non ☐ 0 à 20% ☐ 20 à 40% ☐ 40 à 60% ☐ 60 à 80% ☐ 80 à 100%

Maîtrise de la partie réseau (protocole FTP, structuration en couches, ports TCP, Scapy …). Niveau 1 : faible, Niveau 5 : très bon.

☐ 0 à 20% ☐ 20 à 40% ☐ 40 à 60% ☐ 60 à 80% ☐ 80 à 100%

Maîtrise de la partie programmation. Niveau 1 : mauvais, Niveau 5 : très bon.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Pas évaluable

Qualité du notebook et des explications sur les programmes réalisés. Niveau 1 : mauvais, Niveau 5 : très bon.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Pas évaluable

Note proposée et commentaires :

- **0 < note < 5** : Aucun ou pratiquement aucun travail
- **5 < note < 8** : travail insuffisant
- **8 < note < 11** : travail correcte mais l'étudiant à des difficultés (difficultés à structurer ses explications, difficulté à partir du général vers le plus détaillé, difficulté en programmation, …)
- **11 < note < 14** : travail correcte et niveau attendu atteint
- **14 < note < 20** : Bon à très bon travail avec maitrise des différents objectifs d'une présentation et de la programmation.

____
20