Approfondissement des télécommunications et des réseaux
420-531-SF
TP2-CTF (20%)

Contexte

Votre équipe participera à un « capture the flag » (CTF). Un concours de sécurité ou il faut « briser » la sécurité des systèmes pour obtenir des flags. Les flags sont des indicateurs qu'on a obtenu (ou on est en position d'obtenir) de l'information sensible d'un usager.

Le CTF se déroule en deux parties : passive et active.

Les flags auront toujours la forme FLAG-xxxxxxxxxx (où xxxxxxxx est une séquence d'entiers de longueur variable). Dans certains cas (il y aura une mention à cet effet) vous aurez à ajouter le préfixe « FLAG- » à la séquence d'entiers trouvée.

Passive [8 pts]

La partie passive contient 16 flags (0.5 point par flag) dans 5 épreuves. Pour chaque épreuve, vous recevez une (ou des) trace de trafic que vous devrez analyser manuellement avec Wireshark afin d'extraire de l'information. Chaque épreuve est décrite ci-dessous[1] :

1.A Débutant

C'est un warm-up. Vous n'avez pas d'indice, il y a quatre flags à trouver.

1.B Intermédiaire

C'est moins facile (et plus réaliste), mais encore trop facile pour un indice. Il y a deux flags ici.

1.C Crypto hard

Il faut briser la crypto. 1 flag. Bonne chance !

1.D HTTPS

Un flag caché dans du HTTPS, deux autres flags sur le chemin pour s'y rendre. À faire en ordre.

1.E Wireless

Il faut s'introduire sur le sans-fil encrypté. 1 flag.

[1] Sauf A et B, l'ordre n'est pas un bon indicateur du niveau de difficulté.

1.F ???

Pas d'indices, 1 flag.

1.G Crypto easy[2]

A=1, Z=26, 1 flag

1.H Code

On s'éloigne de Wireshark un instant pour faire place à de la programmation. 2 fichiers, 3 flags. 1 dans le fichier .class, 2 dans le fichier .apk. 1 des trois flags ne contient pas le caractère '-'. 2 Indices : « Manifestons pour Certifier ».

1.I Hashing

Deux fichiers pour retrouver un flag.

Active [12 pts]

La partie active contient 6 flags (2 points par flag) dans 6 épreuves. Un environnement réseau isolé (sans connexion externe) est mis à votre disposition dans la classe durant les heures du cours. L'environnement ne peut supporter qu'une équipe à la fois, il faudra donc respecter l'horaire établi et profiter pleinement du temps alloué à votre équipe. Lorsque vous brancher votre machine dans le réseau du CTF, celle-ci doit avoir une IP statique (pas de DHCP) particulière. Vous pouvez utiliser les IP 192.168.1.200 et 192.168.1.201 (la deuxième est si vous voulez une VM[3]) avec le mask /24.

L'environnement réseau comporte une machine physique et quelques machines virtuelles. Pour obtenir des flags, vous devez interagir avec ces machines. Toutes les interactions doivent se faire avec des scripts Python ou Scapy (sauf si c'est clairement indiquer de faire autrement). Vous devrez remettre vos scripts valides (ou ce qui est demandé) pour obtenir les points des flags correspondants.

Pour la majorité des épreuves, les flags se trouvent très facilement dans Wireshark (pas d'encryption).

1.A One script to ping them all[4]

Un premier script python (pas nécessairement scapy) pour pigner toutes les IPs du subnet (192.168.1.0/24).
À partir de la trace de trafic enregistrée lors des pings, faire un second script (scapy cette fois) pour établir la liste des IPs qui répondent au Ping.

---

[2] Avé !
[3] Linux est fortement suggéré ici.
[4] Vous ne devez pas considérer les deux IPs suivantes pour cette épreuve : 192.168.1.200 et 192.168.1.201

À partir de cette liste (le travail peut être fait à la main[5]) d'IPs sous la forme 192.168.1.X, prendre seulement le X de chaque IP, les mettre en ordre croissant et les concaténer pour obtenir votre flag (ajoutez le préfixe « FLAG- » manuellement).
Par example, si les IPs qui répondent au Ping sont : 192.169.1.6, 192.168.1.119, 192.168.1.244, les X sont 6, 119 et 244, le flag serait donc : FLAG-6119244.

1.B Who are you looking for

192.168.1.69 semble constamment chercher quelqu'un sans jamais le trouver. Dès qu'il va le trouver*, il va lui envoyer de l'information sensible (un flag).

1.C Resolving a mystery

192.168.1.111 cherche aussi quequ'un. Une fois trouvé* il va lui demander de résoudre quelquechose. Une fois la résolution faite*, il va envoyer de l'information sensible à la destination.

1.D Discovery in the making

Quelqu'un tente de faire une découverte. Lorsque cette découverte sera faite* le flag sera dans une requête mal sécurisée de couche 7[6].

1.E Recon[7]

Similaire à la question A, mais on veut la liste de toute les machines ayant une IP sur le réseau. À la question A, on ne s'intéressait qu'à celles qui répondent aux Ping, mais certaines machines peuvent être là sans répondre aux Ping (e.g., firewall interne).
Vous devez donc faire une script pour interagir avec chaque IP du subnet afin de les amener à générer une réponse, même pour les IPs qui ne répondent pas aux Ping.
Après avoir roulé ce script et sauvegardé la trace de trafic, faites un second script qui va extraire la liste des IPs qui ont répondu.
À partir de cette liste, prendre le dernier décimal de chaque IP en ordre croissant pour construire le flag (vous devrez ajouter le préfixe « FLAG- » vous-même).

1.F Plain Text MitM

192.168.1.5 tente de faire une requête HTML qui contiendra de l'information sensible. Vous êtes des experts maintenant, pas d'indice[8] (et scapy seulement) !

*Avec votre aide !!!

Remise

[5] Quoique rendu là c'est probablement moins long de faire un script (avec des tests) que de le faire à la main une fois.
[6] Ça ne semble pas dire grand-chose puisque pas mal tout se passe à la couche 7, mais ça dit au moins que ce n'est pas à la couche 2-3.
[7] Vous ne devez pas considérer les deux IPs suivantes pour cette épreuve : 192.168.1.200 et 192.168.1.201
[8] OK, juste un petit… Attention, l'OS de votre VM d'attaque pourrait vous nuire un peu.

Vous devez remettre une archive zip contenant :

- 1 document PDF qui contient :
  - le nom des membres de l'équipe
  - deux tableaux (un pour chaque partie : passive vs active) contenant les flags avec les numéros d'épreuves correspondant (voir l'exemple ci-dessous) et la justification de votre solution.
- Un répertoire pour chaque épreuve de la partie active nécessitant l'utilisation d'un script, avec dans ce répertoire votre (vos) script python/scapy utilisé pour réaliser cette épreuve.

Attention! Pour chaque flag trouvé, <u>une justification complète</u> est nécessaire, afin d'indiquer comment vous avez trouvé le flag.

Voici un exemple de justification complète (Endroit où se trouve le flag, méthode pour le trouver) :

Épreuve	Flags	Justification
1 Intermédiaire (2B)	FLAG-1234567890	Dans la trace B, au paquet 58, dans la couche TCP du paquet, le champ contient le flag. Trouvé avec la commande 'Find Flag in CTF' (Menu Options > CTF) dans Wireshark.

Conclusion

Le but de ce travail est de vous faire apprendre tout en s'amusant (c'est possible). If you're not having fun, you're doing wrong !

Format

Partie Passive		
Épreuve	**Flags**	**Justification**
1	FLAG-???	Blablabla…
1	FLAG-??????	
1	FLAG-???????	
2	…	
2	…	
3	…	
…	…	

Ressources

Voici quelques ressources qui vous seront utiles pour trouver certains flags.

- http://superuser.com/questions/576786/is-it-possible-pattern-ping-in-windows
- https://www.youtube.com/watch?v=EffHJKckgGg&spfreload=10
- http://support.citrix.com/article/CTX116557
- http://mrncciew.com/2014/08/16/decrypt-wpa2-psk-using-wireshark/