PARTICIPATION CHALLENGES CTF RENNES

Présentation

J'ai eu l'opportunité de participer à un CTF organisé par l'école IMIE sur Rennes ou j'ai pu rencontrer des personnes désireuses de partager leurs connaissances avec tous ceux voulant évoluer dans le domaine de la **sécurité informatique**.

Présentation du CTF

Voici les noms des différentes équipes participantes à l'événement :

- Team J'Hack (nous)
- Team Flan
- Team Jesus
- Team PaInternet
- Un serveur WINDOWS 2012

Chaque équipe avait à sa disposition 4 VMs :

- Un serveur Sambda
- Une debian 8 avec un Wordpress
- Une debian 8 avec un FTP
- Un Windows serveur 2012

Des sondes étaient disponibles sur chacune de nos machines, l'intérêt de ces sondes est simplement d'envoyer un ping toutes les minutes sur les machines cibles, si la machine cible ne répondait pas alors on perdait des points (10 points) sinon on continuait à en gagner (5 points).

Il existait aussi un autre moyen plus efficace pour gagner des points à savoir les **exploits** ! Selon le type de **failles** et leurs conséquences sur l'adversaire il était possible de gagner très rapidement des points (par exemple un accès **root** sur une machine distante rapportait 12 000 points).

Le CTF a duré une semaine, les deux premiers jours il était interdit de protéger ses VMs en installant des patches, le but étant de découvrir le maximum de failles à exploiter sur nos adversaires, c'était aussi le moment de gagner un maximum de points ! Sur 3 les derniers jours on était autorisé à protéger nos machines, il était alors plus difficile de trouver des failles dues à cette protection.

Démarche de notre équipe

En ce qui concerne notre équipe, nous avions décidé de diviser notre troupe en 2, d'un côté une sous-équipe d'attaques et une sous-équipe de défense.

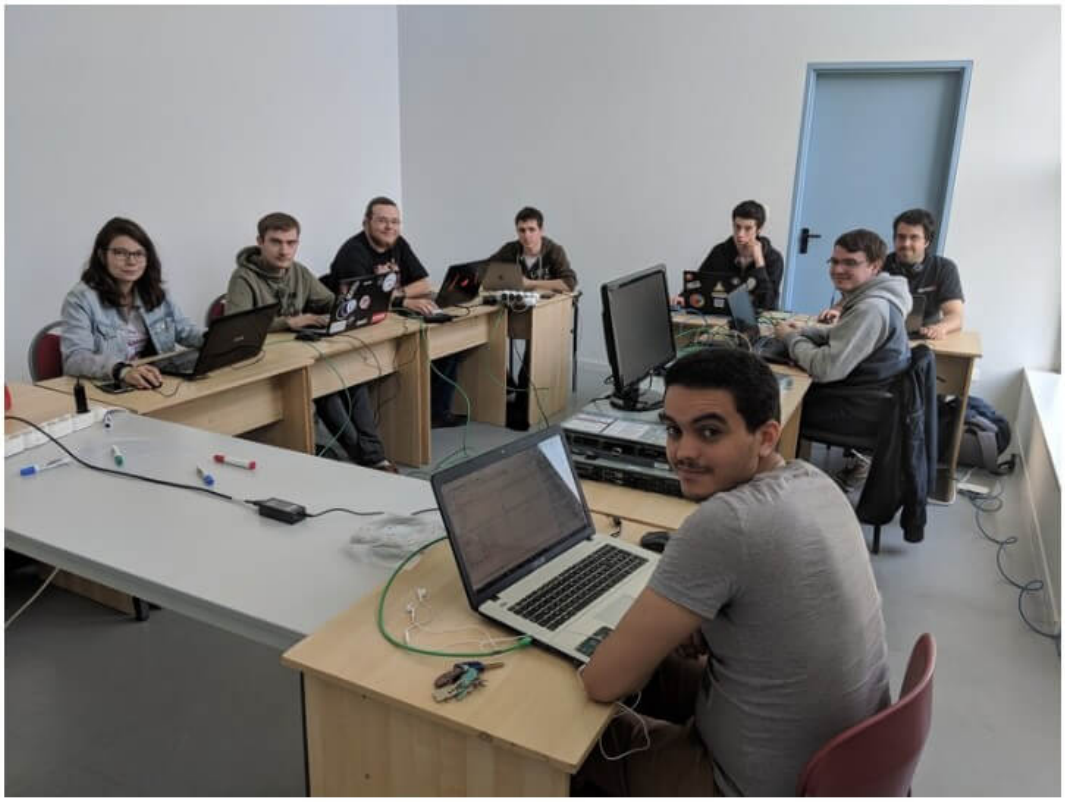
Je faisais partie de l'équipe de défense. Mon rôle dans l'équipe était de me documenter et de trouver le maximum de patches pour nos serveurs.

Comme sur les deux premiers jours nous n'étions pas autorisés à installer des patches, j'en ai profité pour créer des scripts de sécurité et de préparer des patches pour nos serveurs et de tout mettre en place à partir du troisième jour du CTF tout en continuant à protéger nos serveurs les jours suivants. Comme je découvrais et je me documentais sur des patches j'en profitais pour partager avec l'équipe

d'attaques les **vulnérabilités** que je corrigeais pour qu'ils les exploitent sur nos adversaires.

Photos

Notre équipe est sortie **victorieuse** de ce CTF, voici ci-dessous quelques photos de cet événement.

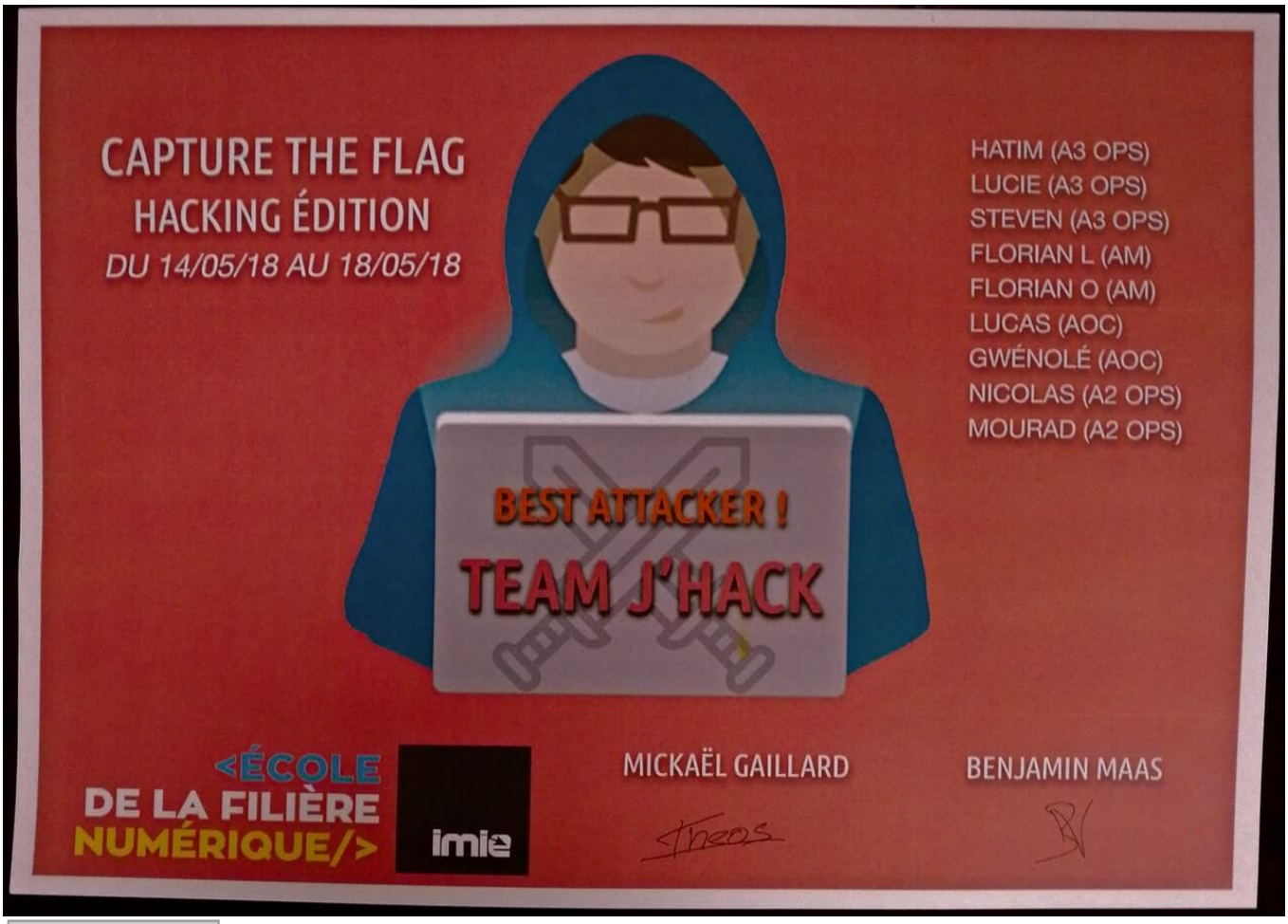


Team J'Hack

- Hatim (A3 OPS)
- Lucie (A3 OPS)

Teams list

NAME	SCORE
Team J'Hack	176150
Team Flan	163600
Team Jesus	148730
Team Painternet	125040
Team Kalinous Reborn !	45470



Plus de photos