Tp sécurité

Objectif

L’objectif de ce tp est de réaliser une attaque heartbleed sur un serveur distant.

1) (0,5pts) Connectez-vous via ssh sur le serveur ‘5.196.95.15’ avec le user : ‘hacker’ et le mdp : ‘azerty’. Prouver que la connection est réussie avec un screenshot.

2) (1pts) Ce serveur est vulnérable à heartbleed et il se trouve qu’une application est ouverte sur l’un des ports du serveur.

La commande `netstat -lnptu` vous permettra de trouver le port à cibler. Quel est ce port ?

3) (3,5pts) Pour réaliser notre attaque nous allons utiliser metasploit, pour ce faire une image docker est disponible sur le serveur.

Lancer `docker run -i -t heartbleed:1.0 /bin/bash` pour run une image de kali linux avec metasploit d’installé et de prêt.

Puis `msfconsole` pour ouvrir metasploit (ça prend du temps).

`use auxiliary/scanner/ssl/openssl_heartbleed` vous permettra de charger le module faisant l’attaque.

Voici quelques commandes utiles :

`set verbose true` => permet d’activer le mode verbose (nécessaire pour voir les données leak)
`info` => permet de voir tous les settings du module
`set %settingName%` => permet de modifier la valeur du settings avec %settingName% le nom du paramètre récupéré avec `info`

Paramétrer le module et lancer le avec `run`.

Vous devriez voir le résultat dans la section « Printable info leaked »

Regarder ces données et dites-nous si vous avez trouvé des informations intéressantes et pourquoi ces informations sont pertinentes. Vous pouvez retrouver de nouvelles informations en relançant la commande ou en effectuant des actions sur le serveur (essayer de vous connecter avec firefox sur le serveur, par exemple)