TP : Étude de la faille Heartbleed

DUREE 4H

EPISEN - ITS
Université Paris-Est Créteil

Le bogue Heartbleed est une faille de sécurité dans OpenSSL qui a affecté et continue d'affecter des millions de personnes dans le monde. Le cryptage SSL et TLS utilisé pour sécuriser les informations sur le web est exploité par des cyberattaquants pour obtenir des informations précieuses sur les utilisateurs, telles que des mots de passe, des informations de facturation et d'autres informations d'identification précieuses.

En envoyant un paquet forgé un client peut récupérer des bribes de la mémoire, jusqu'à 64K de la RAM du serveur web exécutant SSL. Les clients peuvent tenter des reconnexions dans l'espoir de garder une connexion SSL active et obtenir de nombreuses informations. Cela peut être des variables stockées en mémoire et éventuellement les clés/certificats. En cause, une fonction de copie de mémoire qui copie davantage de mémoire qu'elle ne devrait avant de renvoyer le tout au client....

Heartbleed

1. Objectifs pédagogiques :

Sécurisé un système d'information est sans conteste une tâche ardue et il est inenvisageable de penser en faire le tour en une série de TP. Cette série de TP est donc conçue comme une série de challenges qui répondent, chacun, à un objectif différent. Le but espéré est de vous pousser à la réflexion et à approfondir les sujets étudiés.

L'étude de ces failles informatiques est uniquement à but pédagogique et ne vise pas à pousser à l'illégalité. L'objectif pédagogique de cette activité est de sensibiliser les étudiants aux vulnérabilités des failles informatiques les plus classiques.

2. Prérequis :

Avant de commencer le TP nous recommandons fortement de lire et comprendre le cours relatif à la vulnérabilité étudiée. En plus de comprendre le fonctionnement de la faille, ses risques et ses enjeux ceci vous permettra d'acquérir de la facilité dans la réalisation du TP.
Après la réalisation de ce TP, nous vous encourageons à tester vos connaissances via le QCM présent sur la plateforme.

3. TP :

Le but de ce TP est d'apprendre à faire un test d'identification OpenssL sans attaque et par la suite réaliser un test d'identification avec attaque.

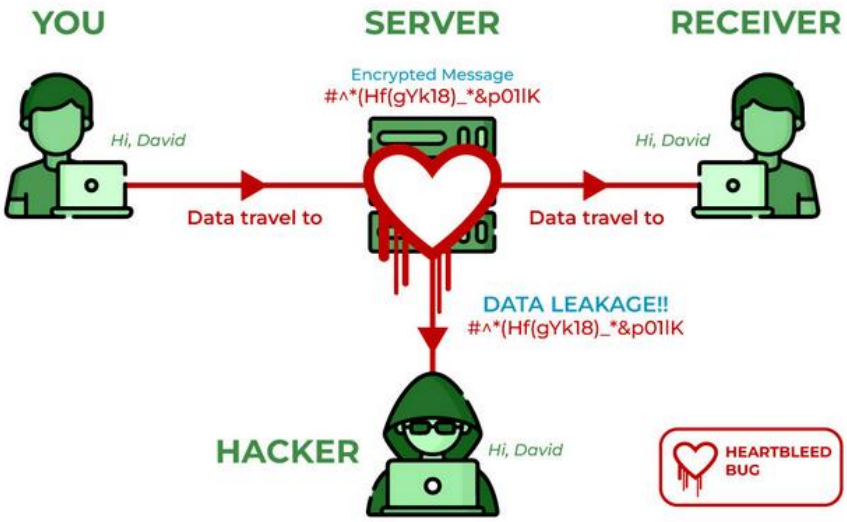
Partie1

Prérequis :

- Une machine virtuelle Ubuntu (machine victime version 12.04.5)
- Une machine virtuelle Kali-linux (machine attaquant version 2020.4)

Configurez les deux VM en mode réseau privé.

1) Rappelez le principe de la faille Heartbleed



2) Donnez le plan d'adresse et lancez un PING depuis la machine Kali pour voir la communication des deux machines.

3) Pour toutes les commandes ci-dessous, faites des captures d'écran.

Sur la machine attaquante :

nmap -sV –script = ssl-heartbleed @IP_machine_victime.

Expliquez ce qu'elle fait.

Tapez la commande et expliquez son résultat :

nmap scan report for @machine_victime.

4) Metasploit est un outil pour le développement et l'exécution d'exploits contre une machine à distance, il permet d'automatiser, d'industrialiser et surtout de faciliter l'exploitation de failles.

Vous allez dès présent prendre main sur la console de métasploit :
Tapez la commande **msfconsole** sur la machine kali-linux, vous devrez voir apparaitre une interface comme sur la capture suivante :

5) Effectuez la recherche des différents modules openssl concernant la faille heartbleed en tapant la commande : **search openssl_heartbleed.**
Utilisez par la suite la commande :
use auxiliary/scanner/ssl/openssl_heartbleed et dites ce qu'elle renvoie.

Consultez les options nécessaires en exécutant la commande : show options. Cette commande devrait vous renvoyer cet environnement :

6) Exécutez la commande set **rhost @machine_victime** ;

En exécutant la commande show info, énumérez les actions possibles disponible dans métasploit. Exploitez ces trois actions et expliquez ce qu'elles renvoient. N'oubliez pas de run après l'exécution de chaque action.

Placez-vous dans le répertoire **.msf4/loot** pour exécuter la dernière action énumérez (celle qui apparait en dernier sur la liste des actions disponibles). Expliquez le résultat.
Sur la VM kali-linux, allez sur le navigateur présent récupérer le fichier attack.py https://seedsecuritylabs.org/Labs_16.04/Networking/Heartbleed/ .
Attribuez à ce fichier des droits : 775 et exécutez le script suivant :
python ./attack.py @machine_victime -p 443 et expliquez le résultat.

Partie2 :
Prérequis : 2 machines virtuelles Debian dont l'une sera victime et l'autre la machine attaquante.
Paquets à installer : apache2
But : configurer la machine victime pour qu'elle soit à mesure d'utiliser la version vulnérable d'openssl ; installer un serveur web sur la victime afin qu'il soit attaqué en utilisant un script python qui exploite le bug heartbleed dans openssl.

Une fois les paquets installés, configurez les vm en mode réseau privé.

1) Sur la machine victime :

Exécutez les commandes qui vont suivre :

a) pour activer le module ssl : **sudo a2enmod ssl**
b) Pour activer le site web: **sudo a2ensite default-ssl**
c) Pour redémarrer le serveur web : **sudo /etc/init.d/ apache2 restart**

Pour vous assurer que votre serveur web fonctionne correctement, faites communiquer les deux VM entre elles.
Maintenant, essayez d'ouvrir serveur web sur la machine attaquant.

2) Sur la machine attaquant :

Exécutez la commande: **openss s_client -connect @machine_victime:443** et expliquez le résultat.
Par la suite il faudra configurer un script python qui enverra un message malveillant composé d'un simple message « hello », la taille de la charge utile sera 64 Ko, ce qui entraînera une saturation de la mémoire de la victime.

Le script heartbleed.py en l'exécutant grâce à la commande python heartbleed.py @machine_victime vous pourrez voir la mémoire de la victime sur le serveur, le message « hello » généré par le script.

Dans le dossier **/var/www/html** de votre machine victime, modifier le fichier le code pour le remplacer par un code de connexion avec identification html.
Essayez de vous connecter au serveur web cette fois-ci ! Dites ce que vous remarquez.
Relancez le script et expliquer le résultat. Pourquoi les identifications de connexion du serveur web sur la machine victime sont-ils visibles et facilement accessible par l'attaquant ?

4. Approfondir la réflexion :

Dans ce TP nous avons utilisé des outils disponibles sur la distribution Debian et via CLI. Néanmoins, nous vous recommandons d'approfondir vos connaissances avec la distribution Kali Linux qui permet de mettre à votre disposition de nombreux outils simples à utiliser et performants pour le domaine de la cybersécurité.

Pourquoi OpenSSL 1.0.1 fait un dump mémoire avec cette attaque ?
https://blogmotion.fr/internet/securite/exploit-ssl-11140