SHELLSHOCK

MEMBRE :

- BAGHDADI Radhouane RT3
- GAMMOUDI Ibtissem RT4
- RAHMOUNI Mohamed RT3
- BERGAOUI Halima RT4
- JAAFAR Ali RT3
- CHEBBI Sana RT4

Table de matière

1. Présentation de l'atelier

Termes à connaitre :

1.1. Le SHELL

C'est un interpréteur de commandes il représente une interface entre l'utilisateur et le système d'exploitation. Il peut être utilisé comme un simple interpréteur de commande, mais il est aussi possible de l'utiliser comme langage de programmation interprété (scripts). On peut citer quelques un :

- sh: « Bourne Shell ». L'ancêtre de tous les shells.
- bash: « Bourne Again Shell » : Une amélioration du Bourne Shell, disponible par défaut sous Linux et Mac OS X.

1.2. Les variables d'environnement

Elles permettant de paramétrer le fonctionnement du système (langue utilisé, chemins vers les fichiers, exécutables, chemin vers les librairies, etc)

1.3. Les Protocoles de communication

Ils sont des règles pour un type de communication particulier. Cette faille exploite plusieurs machines donc avant de démarrer une attaque il faut avoir une connaissance sur le protocole de connexion. Dans nos démonstrations nous allons utiliser les Protocoles : TCP/IP, HTTP, ICMP.

1.4. Un serveur

C'est un dispositif informatique matériel ou logiciel qui offre des services, à différents clients. Il existe plusieurs types de serveur : DHCP, TELNET, WEB …

2. Présentation des outils utilisés

On a besoin aux outils suivants dans notre atelier :

- ❖ Deux machines ayant Un système d'exploitation utilisant comme le sh ou bash comme un interpréteur de commande

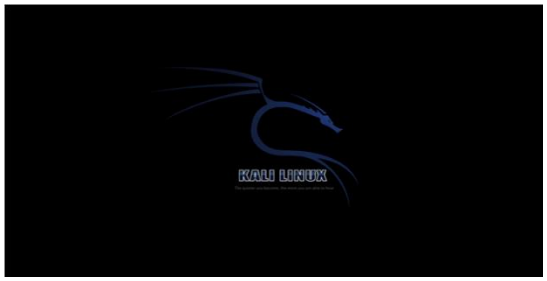
Par exemple : Ubuntu qui est un système libre et gratuit.

- ✓ La première machine sera un serveur. Elle va jouer le rôle de la machine cible.
- ✓ La deuxième sera la machine du Hacker.

D'autres systèmes peuvent être utilisés :

Versions payées :

Version gratuit :



❖ Le logiciel libre *Apache* HTTP *Server* (*Apache*) est un serveur HTTP créé et maintenu au sein de la fondation *Apache*.
Installé et configuré sur la première machine Ubuntu (la machine victime).

❖ Vmware workstation un logiciel qui permet la création des machines virtuelles.

3. Architecture/Topologie du réseau

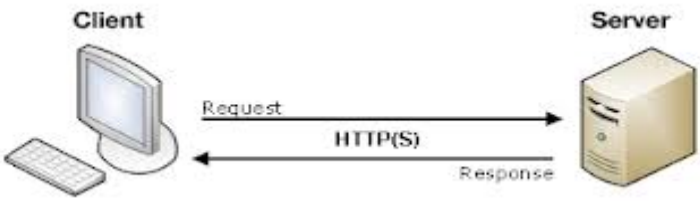
❖ Architecture réseau

L'architecture utilisée est une architecture client-serveur:

- Le serveur apache est un serveur HTTP qui héberge une application web qui à son tour traite les requêtes http du client et lui renvoie une réponse.

Le serveur utilise une version bash vulnérable, il représente alors la victime

- Le client est une machine linux qui envoie des requêtes http au serveur apache et récupère les résultats



❖ Architecture de l'application web

- La formulaire.html: c'est une page web représentant un formulaire qui se compose de deux champs nom et mot de passe

- scripte.cgi: c'est scripte cgi qui traite les données entrée et renvoie «bonjour nom_du_client qui a déjà saisi dans le formulaire »

4. Configuration des outils

« SHELLSHOCK : la fin du monde ?? » c'était le titre d'un article en BBC le 26 septembre derniers la date ou elle est rendue publique, oui cette faille existait à la base du système d'exploitation libre et gratuit GNU/Linux, c'est-à-dire dès La première version de Bash fut créée vers 1988.
Ca découverte était par un Français, Stéphane Chazelas, qui travaille comme responsable informatique dans une société de robotique écossaise. Il n'est pas chercheur en sécurité, mais c'est une fine connaisseuse d'Unix, GNU Linux et des logiciels libres en général !!!
Aucune configuration n'est nécessaire.

Réaction des hackers Professionnels

Pourquoi la faille est-elle très dangereuse ?

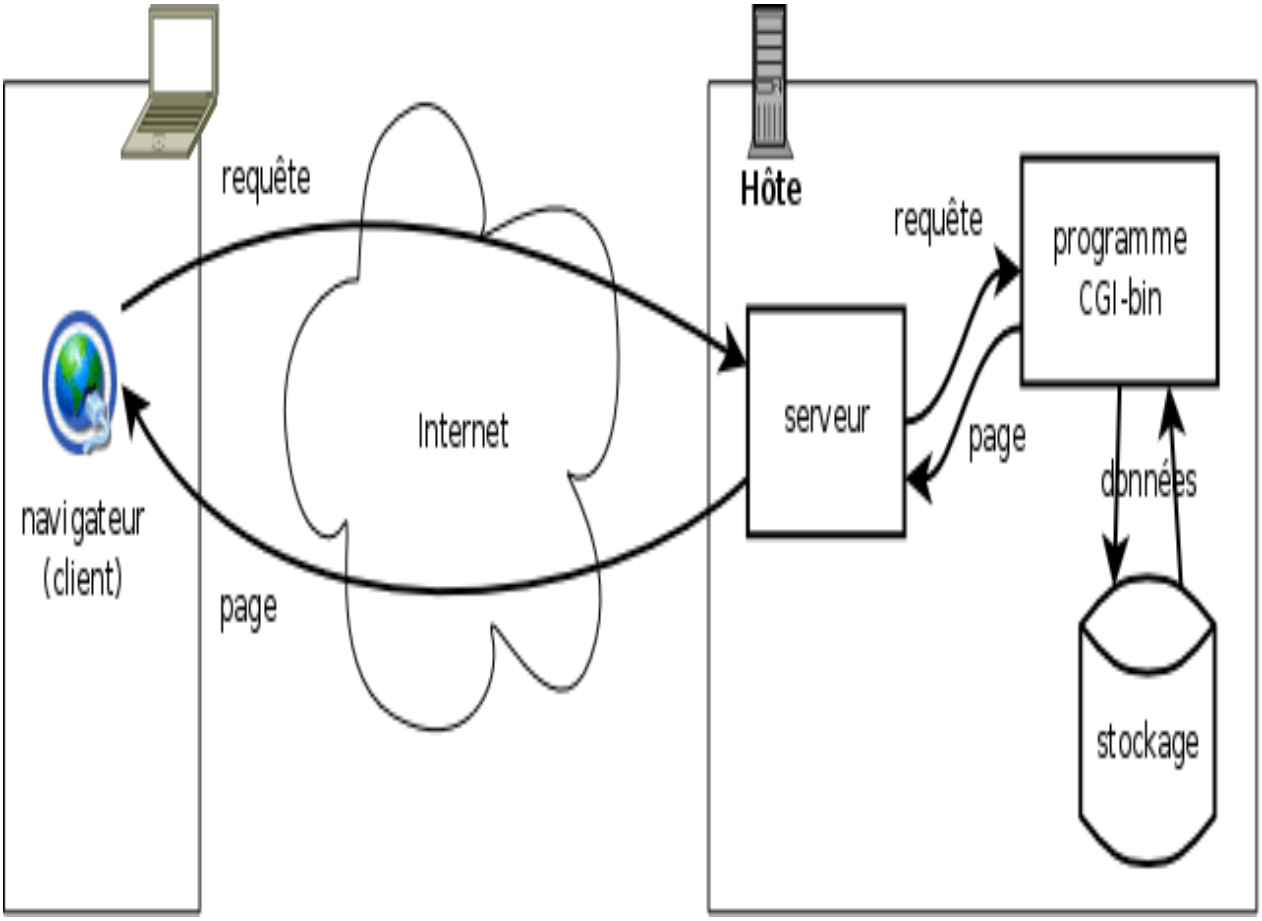
- Sa sera possible d'exécuter n'importe quelle commande sur le Shell, vous serais juste limité par les droits d'accès.

- Très facile à l'exploiter : Elle ne demande pas une grande connaissance pour exécuter des simples commandes mais si vous êtes un professionnel vous pourrez tout faire.

Un exemple d'attaque :

Machine victime : un serveur HTTP → On va se profiter des requêtes et script CGI.

Principe d'attaque :



Nom de l'en-tête	Description
Accept	Type de contenu accepté par le browser (par exemple *text/html*). Voir types MIME
Accept-Charset	Jeu de caractères attendu par le browser
Accept-Encoding	Codage de données accepté par le browser
Accept-Language	Langage attendu par le browser (anglais par défaut)
Authorization	Identification du browser auprès du serveur
Content-Encoding	Type de codage du corps de la requête
Content-Language	Type de langage du corps de la requête
Content-Length	Longueur du corps de la requête
Content-Type	Type de contenu du corps de la requête (par exemple *text/html*). Voir types MIME
Date	Date de début de transfert des données
Forwarded	Utilisé par les machines intermédiaires entre le browser et le serveur
From	Permet de spécifier l'adresse e-mail du client
From	Permet de spécifier que le document doit être envoyé s'il a été modifié depuis une certaine date
Link	Relation entre deux URL
Orig-URL	URL d'origine de la requête
Referer	URL du lien à partir duquel la requête a été effectuée
User-Agent	Chaîne donnant des informations sur le client, comme le nom et la version du navigateur, du système d'exploitation

5. Un scénario de test

Attachez vos ceintures sa prend du temps et de concentration pour l'expliquer :

Utilisation de variables d'environnement spécialement conçues pour injecter des commandes Shell (CVE-2014-6271 & CVE-2014-7169).

☠env x='() { :;}; echo vulnerable CMD1' bash -c CMD2

Création d'une variable d'environnement

la commande n'est pas supposée être ici : racine de la faille

commande à exécuter après la création de la variable

1er étape :

- injecter la commande CMD1 dans un entête de paquet HTTP et diffuser cette paquet : on doit choisir la commande qui nous sert à détecter les machines vulnérables, par exemple
  - ☠ Ping –c5 @IP_de_ma_machine.

Cela oblige les machines cible de lancer un Ping vers ma machine et donc avoir une information sur ma cible.

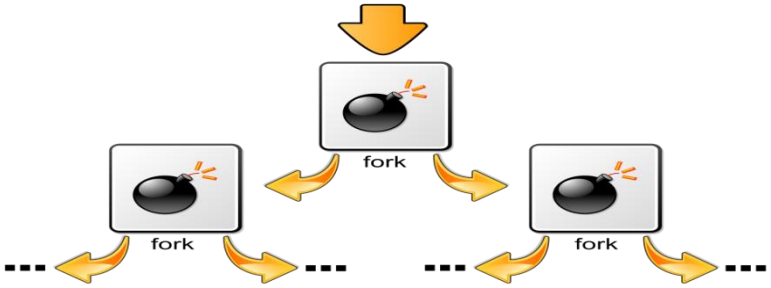
2eme étape :

- Le problème Shellshock est un exemple d'une exécution de code arbitraire(ACE). Dans cette étape on peut Controller la machine victime. Ejecter son lecteur cd par exemple 3:) .
  - ☠ curl -H "User-Agent: () { :; }; /bin/eject" http://example.com/chemin_du_fichier.cgi

BINGO!!!! C'était difficile n'est-ce pas??

D'autre commande qui peuvent remplacer usr/bin/eject :

FORKBOMB : La fork bomb est une forme d'attaque par déni de service contre un système informatique utilisant la fonction fork. Elle est basée sur la supposition que le nombre de programmes et de processus pouvant être exécutés simultanément sur un ordinateur est limité.



- Le code:(){ :|:&};:
- Reverse Shell : la commande nc « netcat » permet d'ouvrir un port d'écoute. Donc la possibilité d'ouvrir un Shell et envoyer des commandes qui s'exécute directement sur la machine victime.
- Buffer over-flow : attaque très avancé. Pour plus d'information consulter le site suivant http://securityxploded.com/remote-buffer-overflow-exploits.php

6. Conclusion

Plusieurs sociétés de sécurité européennes et américaines remarquent que des pirates se sont précipités pour l'exploiter avant que les administrateurs de serveurs n'aient eu le temps d'installer le correctif. Les experts affirment avoir déjà détecté une série d'attaques utilisant spécifiquement la faille Shellshock :

- scannage des réseaux du département de la défense américain pour repérer des serveurs vulnérables
- apparition d'un nouveau *worm* (« ver », soit un virus capable de s'autopropager)
- création de *botnets* (réseaux clandestins d'ordinateurs contrôlés à distance à l'insu de leurs propriétaires) destinés à diffuser du spam
- tentative de blocage des serveurs du distributeur Akamai

La société de sécurité russe Kaspersky affirme que le danger de piratage ne se limite pas au Web : *« Les pires problèmes ne pourront pas être réparés – notamment sur les appareils de l'Internet des objets, dont les logiciels sont installés une fois pour toutes, sans possibilité de mises à jour ni d'introduction de patchs.* » Même chose pour les appareils de connexion intégrés au réseau, par exemple les routeurs wifi domestiques.