Les méthodes d'attaques

Introduction

Les risques d'atteinte à l'intégrité, à la confidentialité et à la disponibilité des données des entreprises font peser une menace croissante sur la réputation et le fonctionnement de toutes organisations.

L'impact d'une infraction ou d'un manquement à la conformité peut engendrer des coûts financiers élevés, ternir l'image de marque d'une entreprise, et restreindre définitivement son évolution.

L'essentiel pour les organisations réside dans la protection de leurs informations et savoir-faire interne, la confidentialité des données et des méthodes et la continuité de production.

Il est donc primordial de qualifier le risque et de repérer les zones sensibles.

La compréhension des vulnérabilités et des risques d'une entreprise constitue une première phase vers la sécurisation du réseau, la priorisation des investissements en sécurité et la conformité.

La sécurité informatique a pour principaux objectifs :

Critères de sécurité	Définitions
Disponibilité	Propriété d'accessibilité au moment voulu des biens essentiels.
Intégrité	Propriété d'exactitude et de complétude des biens essentiels.
Confidentialité	Propriété des biens essentiels de n'être accessibles qu'aux utilisateurs autorisés.

Prévention d'intrusions

Les menaces sur les systèmes informatiques ne cessent de se multiplier, suivant en cela la complexité et l'ouverture des SI, le rythme d'évolution des technologies… et l'erreur ou la négligence humaines, première source de menace.

Le succès grandissant des « appliances » de sécurité depuis 2004 repose sur un traitement des différents aspects de la sécurité à partir d'une seule et même plateforme mutualisant et homogénéisant les traitements.

> Une « appliance » de sécurité se compose d'éléments matériels et logiciels, qui peuvent être mis en œuvre et administrés à partir d'une console unique et centralisée.

Elle propose les fonctionnalités suivantes :

- Passerelle VPN
- Firewall
- Analyse des flux réseau
- Chiffrement des flux
- Filtrage d'url
- Prévention d'intrusion

- Détection des vulnérabilités
- Authentification des utilisateurs
- Antivirus
- Antispam et antiphishing
- Analyse de logs
- Vol de données

L'atout central des « appliances » est d'éviter l'assemblage de briques technologiques, la simplification des infrastructures de sécurité, l'allègement des charges de mises à jour, du pilotage du système de sécurité et de l'acquisition des compétences.

En contrepartie, on peut noter les risques attachés à ces « appliances », risque de ralentissement du trafic et centralisation des risques de défaillance ou de vulnérabilité.

Les critères de choix d'une « appliance » de sécurité prendront donc en compte plus particulièrement certaines caractéristiques :

- **La couverture fonctionnelle** et les capacités d'intégration ou d'interface avec l'ensemble du SI et de l'infrastructure de gestion de la sécurité.
- **La performance** : La mise à jour continue doit permettre de disposer de versions toujours actualisées garantissant la plus grande efficacité possible. La performance passe par la puissance de traitement mais aussi par les différentes méthodes mise en œuvre et leur combinaison.
- **La simplicité de configuration**, de mise à jour et de reporting, éléments clés de la maîtrise des coûts d'infrastructure.

Enfin, domaine fréquemment sous-estimé, la certification des « appliances » : Des certifications sont éditées, relevant de règles de conformité réglementaire, et recouvrent différents niveaux de sécurité en France ou en Europe.

Les familles

Les programmes malveillants

Les virus

Un virus est un programme qui a pour but de modifier, de bloquer ou de détruire des fichiers sur les ordinateurs.

Il existerait d'après les éditeurs d'antivirus de 15000 à 20000 virus, mais seulement 10 % d'actifs.

Les vers

Un ver est un programme capable de se propager à travers un réseau. Il ne se réplique pas sur un même ordinateur mais sur plusieurs dans le but d'engorger un ou plusieurs réseaux.
Les vers se propagent le plus souvent par l'intermédiaire des messageries.
Le ver arrive dans un mail contenant une pièce jointe, récupère le carnet d'adresses et envoie des copies de lui-même à tous les destinataires.

Les Trojans

Les chevaux de Troie s'installent au cœur de l'ordinateur pour en ouvrir les portes à l'insu de l'utilisateur.
Ils permettent ainsi aux personnes ayant les outils adéquats, de collecter des données de l'utilisateur, de toucher à leur intégrité et de contrôler le système.
Les moyens d'introduction sont variés, failles de sécurité, envoi par mail, utilitaires gratuits.

Les spywares

Ce sont des mouchards qui envoient des informations personnelles (liste des sites visités, applications installées…) à des personnes, organismes ou sociétés.
Le but est essentiellement commercial. Il s'agit de vous classer, de construire votre profil de consommateur pour que l'éditeur du spyware puisse le revendre à des sociétés friandes de ce genre d'information.

Les cookies

Les cookies sont de petits fichiers que les serveurs Web stockent sur votre ordinateur. Ils permettent à des sites, que vous avez déjà visités, de garder une trace de votre passage et de mémoriser ainsi vos préférences voire votre identité.
Ils contiennent rarement des informations de première importance. Cependant, mal gérés ils peuvent permettre la création d'une base de données concernant les internautes.

Les Hoax

Un hoax est en fait un canular. Ce phénomène est apparu il y a quelques années et l'on a accusé les éditeurs d'antivirus de propager de fausses informations concernant la sécurité pour vendre leurs produits.
Ce phénomène a aussi pour but de saturer les réseaux de fausses informations pour créer l'affolement.

Les malwares

Les créateurs de programmes malveillants passent par les modules complémentaires des navigateurs web pour propager les malwares et les applications indésirables. Cette approche s'avère redoutablement efficace pour les cybercriminels, car de nombreux utilisateurs vouent une confiance aveugle dans ces modules ou les considèrent simplement comme inoffensifs.

Les attaques par réseau

Attaque de l'homme du milieu

On parle d'attaque Man in the Middle lorsqu'une entité tiers intercepte les communications entre deux systèmes/utilisateurs. Il peut s'agir de n'importe quelle forme de communication en ligne — e-mail, réseaux sociaux, navigation Internet… Les pirates peuvent non seulement espionner les conversations privées, mais ils peuvent aussi cibler toutes les informations que renferment les appareils et terminaux.

Comment protéger un réseau contre cette attaque ?

Utiliser des certificats d'authentification
Imposer HSTS pour éviter les attaques de détournement de https vers http
Utiliser S/MIME pour les mails

Attaque par rebond (SMURF)

Les « attaques par rebond » constituent une famille d'attaques de systèmes informatiques qui consistent à utiliser un ou des systèmes intermédiaires, participant à leur insu à

l'attaque, et permettant à un assaillant de rester caché. Le but est le plus souvent d'envoyer un gros volume de données à un serveur pour le saturer.

Exemple via le protocole NTP
Le cybercriminel envoie de petites demandes à des serveurs NTP, en falsifiant l'adresse du paquet UDP afin que les demandes semblent provenir du système ciblé par le pirate.
La possibilité d'usurper l'adresse UDP est une composante indispensable des attaques par amplification DNS et NTP.

Les serveurs NTP impliqués dans l'attaque renvoient une réponse conséquente aux petites demandes, renvoyant toutes les informations à la cible. Le serveur se retrouve alors submergé et mis hors ligne.

D'après The Open Resolver Project, les 28 millions de résolveurs ouverts représentent une menace significative.

Comment protéger un réseau contre cette attaque ?

Bloquer le trafic de diffusion dirigé vers le réseau
Configurer les hôtes et les routeurs de sorte qu'ils ne répondent pas aux requêtes ICMP echo request.

Attaque par déni de service

Une « attaque par déni de service » est une attaque ayant pour but de rendre indisponible un service et d'empêcher les utilisateurs légitimes d'y accéder.

L'attaque par déni de service vise à bloquer un serveur de fichiers, un serveur web ou empêcher la distribution de courriel .

Comment protéger un réseau contre cette attaque ?

Configurer le firewall pour filtrer les packets ICMP echo ou les limiter à un pourcentage de la bande passante.
Configurer le routeur pour désactiver le broadcast.

Balayage de port

Le « balayage de port » (port scanning en anglais) est une technique servant à rechercher les ports ouverts sur un serveur de réseau.

1 – Balayage par ping

Permet de connaitre si la cible est accessible. Un balayage par ping est un envoi massif de requêtes echo ICMP à différentes cibles et attendre les réponses.

2 – TCP Half-Open

Cette méthode permet de trouver d'éventuels ports ouverts sur la cible. Le scanner envoie un message SYN et note les réponses SYN-ACK. Le scanner n'établit jamais la communication en envoyant le ACK final , la cible est laissée en attente.

3 – Connexion TCP

Cette méthode est équivalente à la précédente, mais elle va jusqu'au bout, ce qui rend le pirate visible et permet de détecter les attaques plus facilement.

4 – UDP

Cette méthode utilise l'envoie d'un paquet vide pour connaitre l'existence de ports ouverts ou fermés (DHCP, DNS, SNMP…) .

5 – Balayage furtif

Ce balayage s'appuie sur le flag FIN pour lequel vous n'attendez pas de réponse. Si un RST est reçu, c'est que le port est fermé, si rien n'arrive en retour, cela signifie que le port est ouvert.

Comment protéger un réseau contre ces attaques ?

Désactiver la réponse au Ping
Cacher/bloquer les ports
Faire les mises à jour nécessaires
Désactiver les services et applications inutiles

Usurpation d'IP

L'usurpation d'adresse IP est une technique qui consiste à envoyer des paquets IP en utilisant une adresse IP source différente de celle de l'ordinateur qui les émet. L'objectif

est de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès.

Les attaques de système

L'écran bleu de la mort

Cette technique consiste à provoquer des erreurs grave sous Windows.

Comment protéger un système contre cette attaque ?

> Ne télécharger que des applications ou pilotes surs.

Fork Bomb

Cette méthode créée un grand nombre de processus très rapidement afin de saturer l'espace disponible et qu'aucun nouveau programme ne puissent démarrer tant qu'aucun autre ne termine.

Comment protéger un système contre cette attaque ?

> Un moyen simple de protéger son système consiste à fixer des limites au nombre de processus pouvant être instanciés par les utilisateurs.

Les attaques de mots de passe

Attaque par dictionnaire

Cette méthode repose sur le fait que de nombreuses personnes utilisent des mots de passe courants (par exemple : un prénom, une couleur ou le nom d'un animal). C'est pour cette raison qu'il est toujours conseillé de ne pas utiliser de mot de passe comprenant un mot ou un nom.

Attaque par force brute

Il s'agit de tester, une àune, toutes les combinaisons possibles.

En théorie la complexité d'une attaque par force brute est une fonction exponentielle de la longueur du mot de passe, la rendant virtuellement impossible pour des mots de passe de longueur moyenne.

Comment protéger un mot de passe contre cette attaque ?

Utiliser des mots de passe de 8 caractères mini et de forme complexe.
Modifier les mots de passe régulièrement

Force des mots de passe

#	min.	min.+maj.	alphanum.	imprimable
3	10^4	10^5	10^5	10^6
4	10^5	10^6	10^7	10^7
5	10^7	10^8	10^9	10^{10}
6	10^8	10^{10}	10^{10}	10^{11}
7	10^9	10^{12}	10^{12}	10^{13}
8	10^{11}	10^{13}	10^{14}	10^{15}
14	10^{14}	10^{24}	10^{25}	10^{27}
	1 s	10 s	1 min	1 h

Elle consiste à demander à l'utilisateur de fournir lui-même son mot de passe.
C'est une technique qui est très efficace et qui joue sur les relations humaines. On va exploiter le stress ou des conditions particulières qui vont faire que la personne va vous révéler son authentifiant.
Elle se fait au moyen d'une simple communication téléphonique ou par mail.

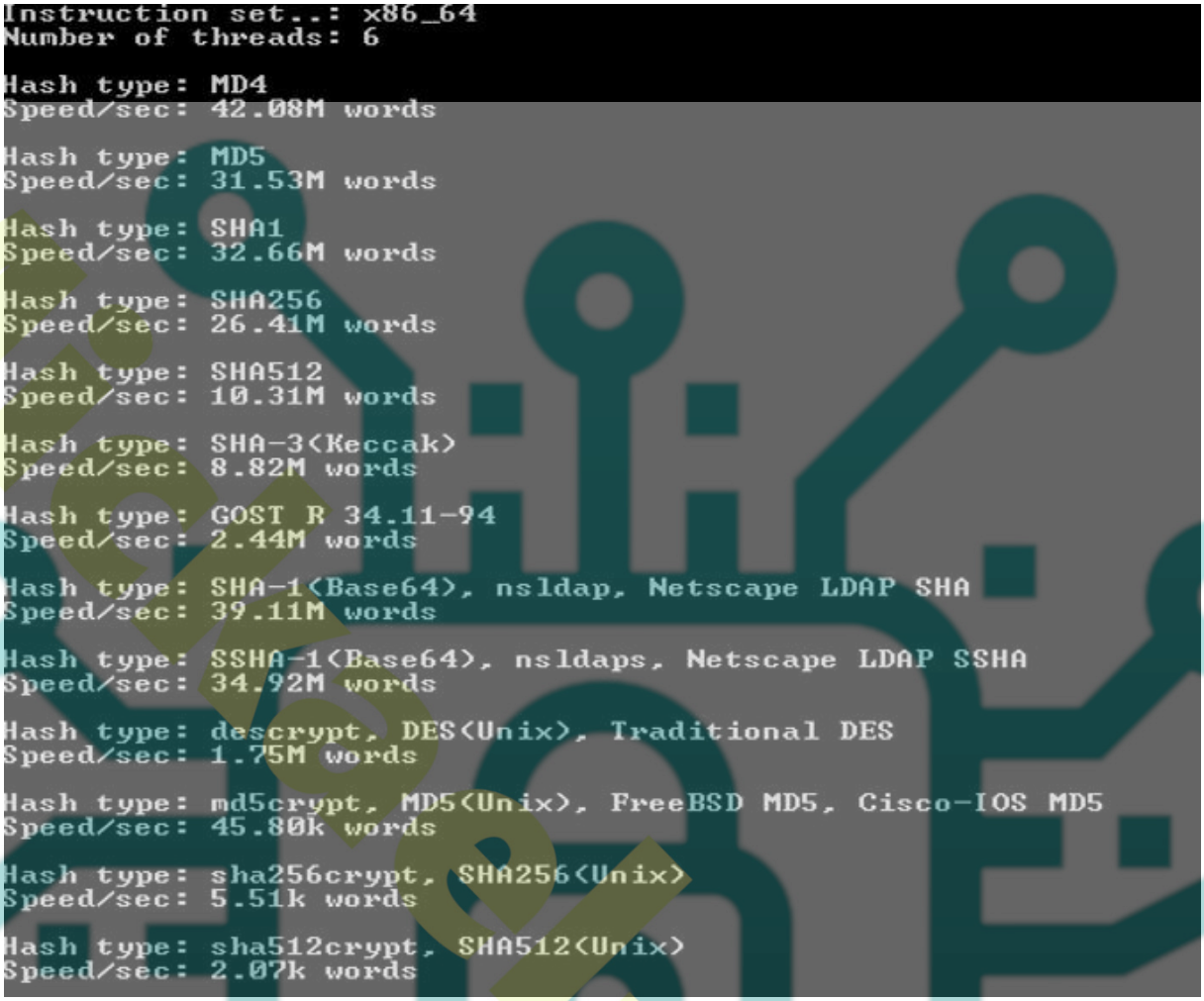
L'attaquant peut utiliser des outils comme John the Ripper ou hashcat.

Liste des mots de passe publiée par RockYou suite au vol de 32 millions de comptes

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Rank	Password	Number of Users with Password (absolute)
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

Hashcat est réputé comme être le logiciel le plus rapide pour cracker des hashs.
Dans la capture ci-dessous avec un processeur à 6 cœurs, on sait combien de mots de passe sont cherchés en une seconde en fonction du type de chiffrement.



Générer un mot de passe solide

Conseil de la CNIL

https://madiba.encs.concordia.ca/software/passwordchecker/

Analyse sur plusieurs sites

Attaque de site web

Modification (defacing)

Désigne la modification non sollicitée de la présentation d'un site web. Les défacements sont provoqués par l'utilisation de failles présentes sur une page Web ou tout simplement une faille du système d'exploitation du serveur web.

Cross-site scripting

Le XSS, est un type de faille de sécurité des sites web permettant d'injecter du contenu dans une page, permettant ainsi de provoquer des actions sur les navigateurs web visitant la page. Les possibilités des XSS sont très larges puisque l'attaquant peut utiliser tous les langages pris en charge par le navigateur (JavaScript, Java, Flash…) Il est par exemple possible de rediriger vers un autre site pour du Hameçonnage ou encore de voler la session en récupérant les cookies.

Comment protéger un site web contre cette attaque ?

Vérifier le code, passer par un langage intermédiaire (autre que HTML) comme XML.
Utiliser les protections des Frameworks tels que Symfony
Utiliser l'échappement unitaire via PHP (strip_tags, htmlspecialchars, htmlentities)
Mettre à jour les versions des logiciels
Utiliser des modules serveurs permettant de gérer les requêtes malicieuses.
Utiliser le header HTTP X-XSS-Protection dans HTML5

Attaque d'applications

Exploit

Un « exploit » est un élément de programme permettant à un individu ou un logiciel malveillant d'exploiter une faille de sécurité informatique dans un système d'exploitation ou dans un logiciel que ce soit à distance ou sur la machine sur laquelle cet exploit est exécuté ; ceci, afin de prendre le contrôle d'un ordinateur ou d'un réseau, de permettre

une augmentation de privilège d'un logiciel ou d'un utilisateur, ou encore d'effectuer une attaque par déni de service.

Comment protéger une application contre cette attaque ?

Vérifier les logiciels utilisés
Utiliser un antivirus
Éviter la navigation sur les sites corrompus

Dépassement de tampon

Un « dépassement de tampon » est un bug par lequel un processus écrit à l'extérieur de l'espace alloué au tampon, écrasant ainsi des informations nécessaires au processus.

Comment protéger une application contre cette attaque ?

Développer des applications à l'aide de langages de programmation évolués, assurant une gestion de la mémoire allouée.
Utiliser des bibliothèques de fonctions sécurisées.
Mettre à jour les logiciels.

Shellcode

Un « shellcode » est une chaîne de caractères qui représente un code binaire exécutable.

Comment protéger une application contre cette attaque ?

Mettre à jour les OS.
Isoler les processus.

Attaque sur le protocole Kerberos

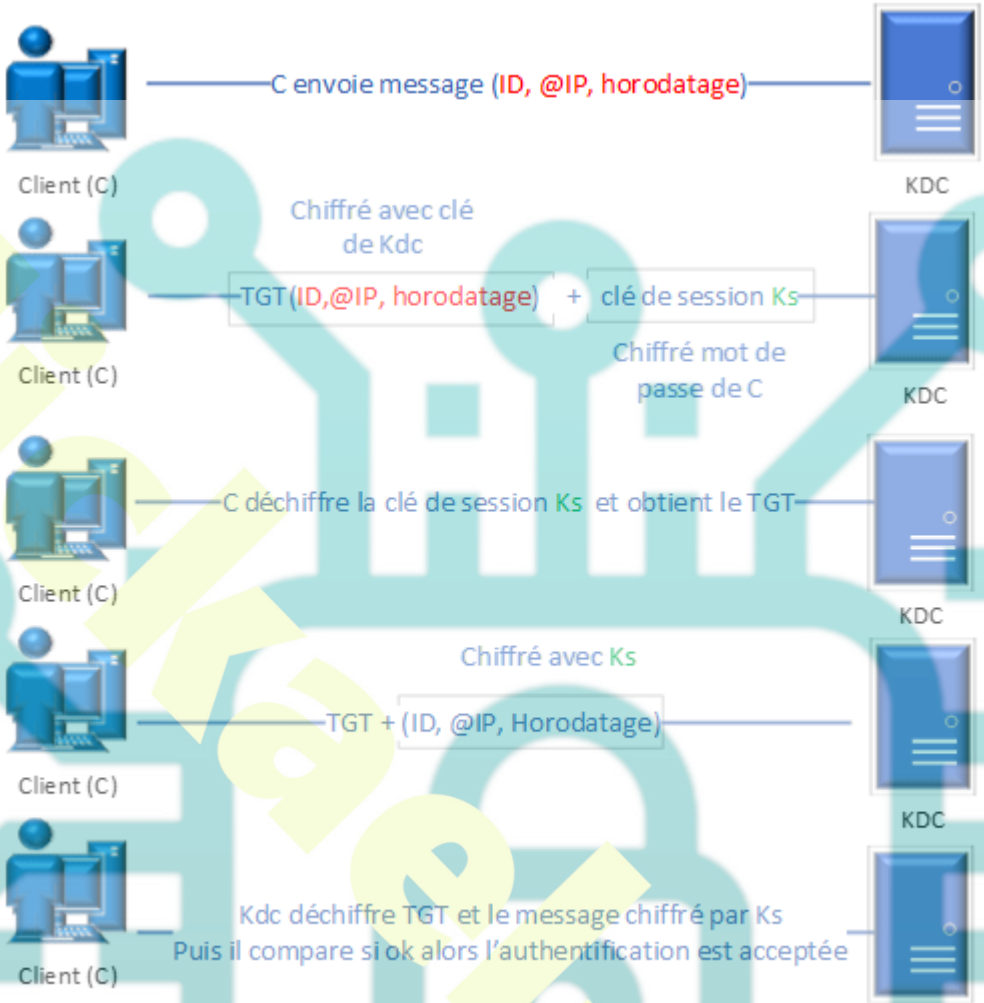
Présentation

Kerberos part d'un principe simple : *le mot de passe ne doit jamais circuler sur le réseau, que ce soit en clair ou sous une forme chiffrée quelconque.*

Le protocole Kerberos repose sur un système de cryptographie à base de clés secrètes. Historiquement, c'était DES qui était utilisé pour chiffrer les données, aujourd'hui le défaut est AES.

Kerberos s'appuie sur deux services pour fonctionner :
Le serveur d'authentification (**AS**) et le service de délivrement de tickets de service (**TGS**)

Ces deux services sont la clé de voûte de tout le système, ce sont eux qui font sa force, mais aussi sa principale faiblesse en cas de panne ou d'attaque. Ces deux rôles complémentaires sont toujours regroupés en une même entité logicielle, appelée Centre de Distribution des Clé (**KDC** – Key Distribution Center)



Présentation Kerberos

Historique des attaques sur Kerberos

KDC Spoofing

Cette attaque se base sur la possibilité d'usurper les réponses du KDC. Certaines applications n'utilisent pas le protocole Kerberos dans son ensemble. De ce fait un utilisateur possédant un accès physique à la machine peut effectuer une authentification avec un mot de passe fixé et bloquer l'envoi de la requête AS_REQ au KDC. En effet,

l'attaquant va répondre lui-même à cette requête en forgeant une requête AS_REQ avec le mot de passe précédemment utilisé.

Comment protéger une application contre cette attaque ?

> Afin de se protéger de cette attaque, il est nécessaire d'effectuer l'étape suivante du protocole, c'est-à-dire réaliser une demande de ticket au TGS.

Replay Attack

Comme évoqué précédemment, le serveur s'assure que le client peut accéder au service en validant uniquement la dernière requête envoyée : Application Server Request (AP_REQ). Cette attaque par rejeu nécessite que l'attaquant mette en place un Man-In-The-Middle entre le client et le serveur. Par la suite, il y a deux possibilités :

- Soit l'attaquant effectue une écoute du réseau et renvoie la requête AP_REQ émise par le client afin d'obtenir un accès au service.
- Soit l'attaquant empêche le client d'envoyer la requête AP_REQ au serveur et l'utilise pour obtenir l'accès au service à la place du client.

Comment protéger une application contre cette attaque ?

> **Timestamp**
> La durée d'utilisation de l'AP_REQ est limitée à un certain temps (en général 5 minutes).
> **Cache**
> Le serveur (V) stocke en mémoire les requêtes (ou plus précisément les authentificateurs) effectuées par le client pendant la durée d'utilisation autorisée. Ainsi, toutes les requêtes en double sont rejetées.
> **Adresse IP**
> Le ticket fourni par le KDC peut contenir la liste des adresses IP autorisées à utiliser ce ticket. Cette information est conservée dans la requête AP_REQ. Ainsi, le serveur est en mesure de vérifier si l'expéditeur de la requête a le droit d'utiliser ce ticket.

Kerberos et le chiffrement

Une autre catégorie d'attaque consiste à exploiter les faiblesses des algorithmes de chiffrement utilisés par Kerberos.
Historiquement, Kerberos utilisait uniquement l'algorithme DES. Le protocole a depuis évolué pour intégrer un mécanisme de négociation de l'algorithme de chiffrement entre le client et le KDC. Cependant, il est possible pour un attaquant de forcer la demande en utilisant un algorithme faible.

Comment protéger une application contre cette attaque ?

Limiter les algorithmes acceptés côté client et serveur.
Sous environnement Windows, les algorithmes faibles sont désactivés à partir de Windows 7 et Windows 2008 R2.

L'attaque Pass the Ticket

Cette attaque permet de s'authentifier localement sur le poste client, et ce même si l'authentification Kerberos est complètement réalisée. Du côté attaquant, cela nécessite le contrôle des flux réseau échangés entre le client et le KDC, ainsi qu'un accès physique sur l'équipement.

L'attaque se déroule en deux phases :

1 – Écoute d'une authentification Kerberos légitime
2 – Rejeu d'un ticket valide

Comment protéger une application contre cette attaque ?

Seule l'implémentation du protocole Kerberos par Microsoft est vulnérable à l'attaque Pass the Ticket.
En revanche, l'implémentation Kerberos fournie par le MIT n'est pas vulnérable en raison du respect des spécifications du protocole. En effet, l'implémentation de Microsoft n'effectue que les deux premiers échanges pour authentifier un utilisateur (AS_REQ/AS_REP et TGS_REQ/TGS_REP), tandis que celle du MIT ajoute l'envoi de la requête AP_REQ.

Les attaques SSL/TLS

Les protocoles TLS (Transport Layer Security) et SSL (Secure Socket Layer) sont d'abord là pour permettre un chiffrement de la connexion entre un client et un serveur. En chiffrant la connexion, on s'assure ainsi qu'aucun tiers ne viendra lire ou modifier son contenu.
Ces protocoles s'appuient le principe de clé publique, SSL/TLS basée sur des certificats.

POODLE

POODLE (Padding Oracle On Downgraded Legacy Encryption) cherche à dégrader l'ensemble des connexions chiffrées vers la version la moins sécurisée. Ainsi, il est possible de déchiffrer simplement les cookies sécurisés envoyés au travers d'une connexion SSL.

Comment protéger une application contre cette attaque ?

Utiliser TLS 1.4
Mettre à jour les navigateurs vers la version la plus récente qui protège contre la dégradation du chiffrement des connexions.

BEAST

BEAST (Browser Exploit Against SSL/TLS) touche SSL 3.0 et TLS 1.0. Un pirate peut déchiffrer les données échangées entre les 2 parties, grâce à une vulnérabilité dans l'implémentation du mode CBC (Cipher Block Chaining) de TLS 1.0. L'attaque se fait côté client grâce à une technique de Man in the Middle qui consiste à injecter des paquets spécialement formatés dans le flux TLS.

Comment protéger une application contre cette attaque ?

Utiliser TLS 1.4

Heartbleed

C'est une vulnérabilité découverte dans l'extension heartbeat d'OpenSSL qui est utilisée pour garder active une connexion. Le client envoie régulièrement des requêtes contenant une certaine quantité d'informations (données + tailles des données) et le serveur doit répondre avec le même « heartbeat » (données + tailles).

Le pirate forme une requête donnée + taille plus grande à laquelle le serveur va répondre en utilisant des données aléatoires contenues dans sa mémoire. On a alors une fuite de données non chiffrée.

Comment protéger une application contre cette attaque ?

> Mettre à jour vers la dernière version d'OpenSSL.

SWEET32

SWEET32 comme BEAST profite d'une faiblesse dans le mode CBC où sont encore utilisé de vieux ciphers comme TripleDES et Blowfish, vulnérable à des attaques par collision. En collectant et analysant au maximum 32 GB de data chiffrée, un attaquant peut trouver la clé privée et déchiffrer le contenu.

DROWN

Cette attaque touche tous les services qui reposent SSLv2. Un pirate peut alors déchiffrer des connexions TLS récentes entre des clients et des serveurs totalement à jour en envoyant des requêtes SSLv2 forgées avec la même clé privée que celle échangée entre des serveurs légitimes.

Comment protéger une application contre cette attaque ?

> Mettre à jour vers la dernière version de TLS et supprimer SSL.

Les applications web

La représentation d'ouverture, de distribution de l'architecture Web et de flexibilité du protocole HTTP, posent des problèmes de sécurité àtous les niveaux du modèle n-tiers, car la richesse de la sémantique des flux métiers, les multiples plateformes de développement, les nombreux langages, rendent très difficile la maitrise du processus de sécurisation des applications Web.

Au niveau des systèmes de défense, la plupart des systèmes de détection d'intrusion et de filtrage applicatif utilisent des règles de sécurité. La majorité de ces règles sont des signatures d'attaques. Le degré de granularité de compréhension de cette signature peut conduire soit àune granularité trop fine qui risque de ne pas correspondre aux attaques polymorphes utilisant des techniques furtives, soit granularité trop large oùla signature est trop générale et risque de générer de fausses alertes ou de bloquer des flux légitimes.

Le problème est que les attaquants ont le temps d'analyser, de se documenter sur les cibles (environnement d'exécution, architecture, vulnérabilités connues, …) et d'essayer d'adapter l'attaque en fonction de l'ensemble des informations collectées en vue trouver un moyen d'échapper aux signatures déployées sur les systèmes de défense.

Injection SQL

La plupart des sites web ne surveillant pas les entrées autres que les noms d'utilisateurs et les mots de passe, un pirate informatique peut utiliser les zones d'entrée pour envoyer ses propres requêtes, c'est-àdire injecter du SQL dans la base de données pour créer, lire, mettre àjour, altérer ou supprimer les données stockées dans la base de données principale.

Exemple de code non sécurisée pour récupérer les comptes

```
$id = $_GET['id']; $getid = "SELECT first_name , last_name FROM users
WHERE user_id = ' $id'";
```

Ce codage permet au pirate d'injecter, via l'entrée de cette application, du code SQL pouvant récupérer tous les utilisateurs inscrits dans la base de données y compris l'administrateur par cette instruction :

```
/* http://www.cible.victime/user/?id=' OR 'toto '='toto
```

Ce qui peut se traduit au niveau de la requête SQL comme suit :

```
SELECT first_name , last_name FROM users WHERE user_id = '' OR
'toto'='toto'
```

Cross Site Scripting XSS

Le code injecté est un script qui a comme but de s'exécuter sur le client Web. Il passe généralement par le bais d'un champ d'un formulaire qui sera stocké dans une base de données du côté serveur et une fois chargé par le client Web, il est exécuté.

Cross Site Request Forgery CSRF

Cette attaque est semblable à l'XSS. La faille se situe toujours dans une entrée non filtrée par l'application Web. Un attaquant peut donc injecter du code malicieux conduisant à son exécution dés que le navigateur se charge.

Un exemple d'une requête obligeant un administrateur à changer son propre mot de passe à son insu :

```
/* <img src="http://cible.victime/?
password_new=mikmak&amp;password_conf=
mikmak&amp;Change=Change" border="0" height="5" width="5">
```

Ce code utilisé par le pirate dans un champ de formulaire non filtré, est chargé par l'administrateur de l'application. La balise <img indique au navigateur d'aller chercher une image de taille 0 à partir du lien indiqué dans scr="".
Le fonctionnement habituel du navigateur est d'aller sur le site pour récupérer l'image , mais en visitant cette ressource, il exécute une action de changement de mot de passe dans la session courante de l'administrateur. Ce qui à pour conséquence, de changer le mot de passe de l'administrateur, ce mot de passe étant connu uniquement par le pirate.

Solutions de filtrage Web

Actuellement, les modèles de sécurité recommandent le déploiement frontal d'un Web Application Firewall (WAF), devant le serveur Web qui héberge ces applications. ModSecurity est un WAF open-source qui se base sur un serveur Web ou un reverse-proxy, pour traiter les requêtes et les réponses HTTP.

Techniques furtives d'évasion aux systèmes de filtrage

Des outils tels que WAFlulz , SqlMap et nmap sont capables de détecter l'empreinte du WAF, ainsi que l'existante d'un système de type HaProxy. Ces outils donnent aux pirates des informations sur la démarche à suivre pour lancer l'attaque.

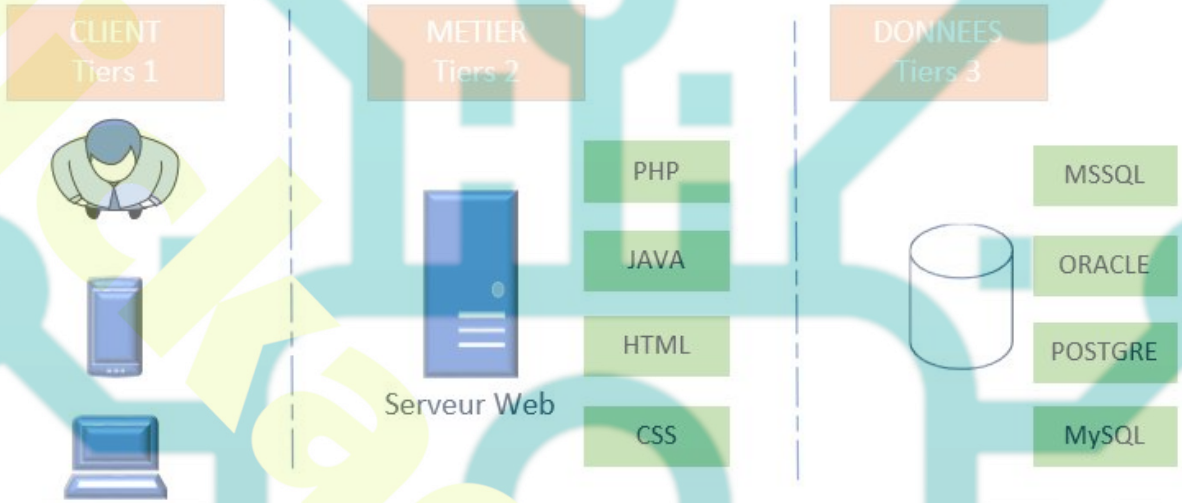
Les astuces qui permettent de troubler le WAF sont par exemple :

La casse – jouer sur les majuscules et minuscules
SeLeCT ou sELEcT
Espacement – jouer sur le caractère de tabulation, le retour charriot, le retour à la ligne.
Concaténation des chaines de caractères – cacher les mots clés via les opérateurs || ou += % [?, 2,3,4]
'DR' || 'OP' <===> DROP
Encapsulation – induire en erreur les filtres basés sur la suppression du AND
AandND , AandandandandND , Aandandandandand ….ND
Commentaires – tout ce qui se trouve en commentaire sera éliminé par l'interpréteur du langage.
'/**/MA/**/BASE/**/SEL/**/ECT/**/password/**/FR/**/OM/**/Users /**/WHE/**/RE/**/username/**/LIKE/**/'admin'-
La chaine SEL/*texte*/ECT est passé a SQL, ce dernier va l'interpréter comme SELECT en fusionnant les les deux parties se trouvant avant et après les /.

Encodage d'URL

Permet d'utiliser les paramètres du Query-string (venant juste après le caractère?) dans l'URL de la requête HTTP. Pour contourner les filtres

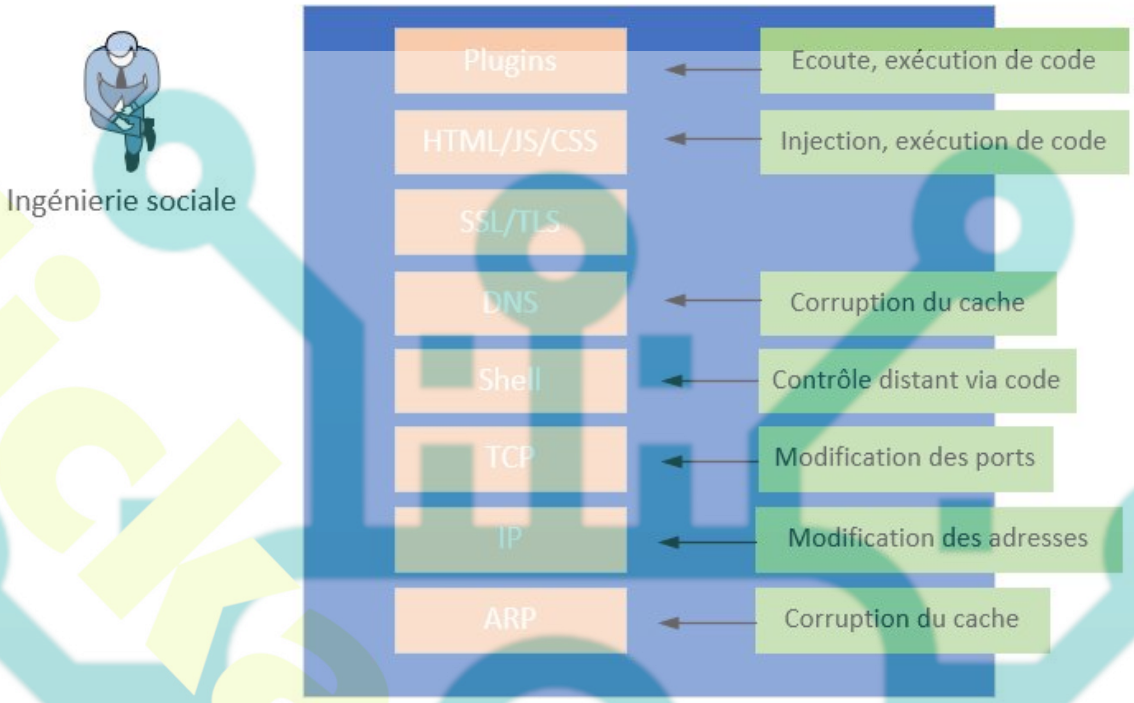
empêchant l'injection des espaces et les caractères de commentaire "/" et "*" on réalise l'injection suivante :
/**/MA/**/BASE/**/SEL/**/ECT/**/password/**/FR/**/OM/**/Users /**/WHE/**/RE/**/username/**/LIKE/**/'admin'-



Une classification orientée entrées des Applications Web

Les attaques du coté client

Un client Web peut être un utilisateur d'un navigateur Web installé sur une machine fixe ou mobile, il peut être aussi un robot logiciel (Bot) qui scrute l'application Web d'une manière autonome ou semi-autonome pour de bonnes ou de mauvaises intentions.



L'ingénierie sociale est l'art de manœuvrer un humain pour lui dérober des informations confidentielles (comptes, données bancaires…). Le vecteur d'attaque est le plus souvent un mail d'hameçonnage ou un appel téléphonique.

Dans un navigateur Web, on peut trouver un Plug-in malveillant, installé via un malware ou un utilisateur, utilisé pour compromettre la confidentialité des échanges. Ce programme permet d'écouter, éventuellement de modifier, les données avant leur chiffrement par le protocole SSL/TLS.

La modification du cache ARP permet à un attaquant d'intercepter et de modifier toutes les requêtes et les réponses des clients.

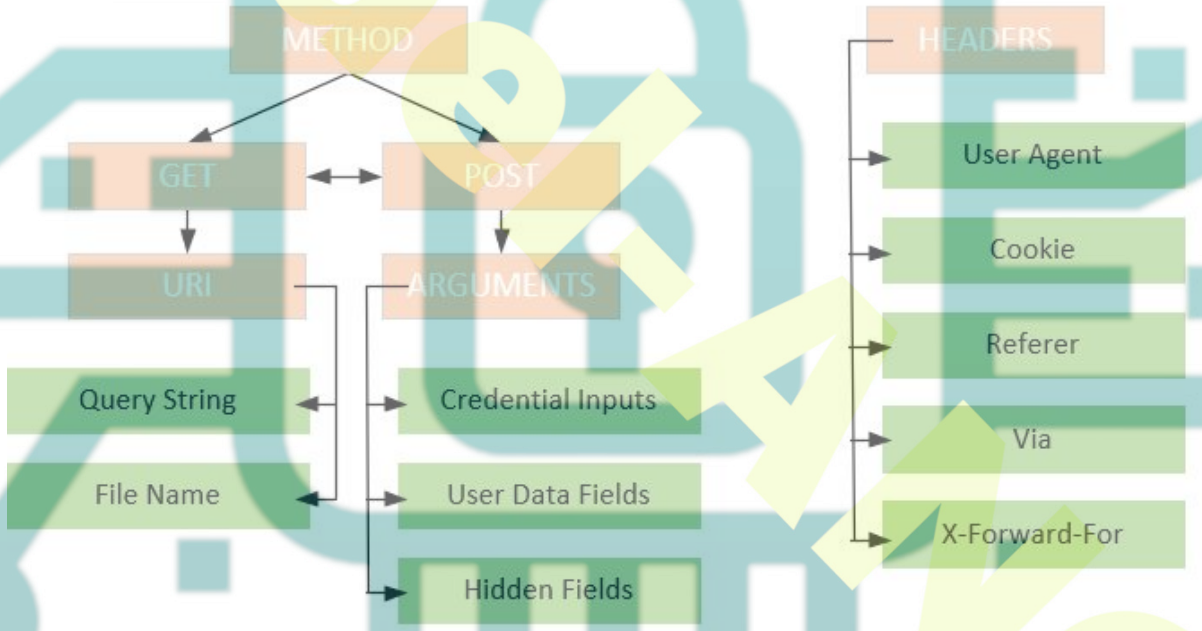
La mémoire cache du DNS est utilisée pour accélérer les résolutions d'adresses IP par l'explorateur. Une fausse association (adresse IP Nom de domaine) conduit à la redirection des requêtes des utilisateurs vers de faux vrais sites contrôlés par un attaquant. L'objectif de ce détournement est généralement le vol des identifiants et des mots de passe des clients.

Le problème avec l'attaque MITM est que l'attaquant peut modifier les données des messages envoyés et reçus par la cible de l'attaque. Cette modification peut concerner les en-têtes TCP/IP, les adresses IP et les ports TCP, pour réaliser des redirections des requêtes et des réponses HTTP vers et depuis des sites de phishing contrôlés par l'attaquant.

L'absence d'un mécanisme de validation des adresses IP et des ports TCP au niveau local peut donc permettre ce genre d'attaques.

Les attaques coté serveur

Pour protéger l'application Web des menaces externes, il convient d'analyser chaque composante du protocole HTTP qui constitue une entrée, car une mauvaise définition de ces entrées peut entrainer le passage d'une attaque vers l'application Web. Le protocole HTTP est un protocole extensible et cette extension peut porter sur un nouvel entête par exemple, qui sera peut être considéré par l'application Web comme étant une variable d'entrée à évaluer et à interpréter.



1 – **Dans l'URI d'une méthode GET, il existe deux entrées possibles :**

- **Le Query-String** : est la chaine de caractères venant derrière le? ou le # dans l'URL d'une requête HTTP. Les attaques par injection SQL, injection de commandes système, injection d'entrées LDAP et le XSS sont des cibles des attaquants utilisant cette entrée.
- **File Name** : les noms de fichiers sont considérés aussi comme un paramètre d'entrée dans une requête de type GET. Pour faciliter le codage, certains développeurs préfèrent manipuler les noms de fichiers sans imposer un contrôle stricte sur ces noms

de fichiers. Des traversées de répertoires dans le système de fichiers pour accéder à des fichiers sensibles non sécurisés peuvent être injectées via ce vecteur.

2 – **Les arguments d'une requête HTTP utilisant la méthode POST sont les variables utilisées par l'application Web sous forme de champs de saisie. Ces champs peuvent être :**

- Des champs contenant des credentials de sécurité tels que les login et les mots de passe (Plain text ou Cipher text)
- Des champs de saisie des données d'utilisateurs généralement en texte claire ASCII.
- Des champs cachés (visuellement) utilisés par les développeurs pour récupérer des données calculées d'un formulaire. Néanmoins, ces champs sont modifiables via un simple outil d'édition de code source.

3 – **Les en-têtes du protocole HTTP peuvent être récupérés pour réaliser des opérations de formatage du contenu ou de débogage.**

- **User Agent** : est l'identité du navigateur Web, il est utilisés par l'application Web pour adapter le redu (HTML/JavaScript/CSS) en fonction de la version du User Agent (Smart Phone, tablette, PC). Cette entrée est vulnérable à des attaques telles que ShellShock qui permet d'insérer du code Shell et affecter les OS sur lequel tourne l'application Web.
- **Cookie** : est utilisé par l'application pour récupérer un cookie de session déjà inscrit dans la base des cookies. Cette entrée est potentiellement vulnérable aux attaques par injection de code SQL.
- **Referer** : est un moyen pour l'application Web de savoir quel est l'initiateur d'une requête relayée par plusieurs systèmes proxy. Le contenu de cet en-tête est une adresse IP , mais un pirate peut falsifier cette adresse en utilisant sa propre adresse IP pour récupérer la réponse de l'application à la place de l'initiateur légitime de la requête.
- **Via** : l'en-tête Via, concatène les informations pour chaque élément traversé dans une réponse ou requête, séparés par des virgules. Lorsqu'un client lance une requête avec un en-tête Via vers un serveur web, le serveur Web d'origine renvoi une réponse avec l'en-tête Via souvent suivant le même chemin.
  Cet en-tête peut donc être modifié par un attaquant pour rediriger les requêtes/réponses. Il suffit d'injecter une étape supplémentaire en intermédiaire ou en finale dans le parcours de la transaction HTTP.
- **X-Forwarded-For** est un en-tête HTTP qui est inséré par des proxies pour identifier l'adresse IP du client. L'adresse IP demandée est toujours une adresse locale et l'adresse IP du client doit être extraite de la requête. Cet en-tête peut donc, contenir

plusieurs adresses IP.
Cet en-entête peut contenir du code malicieux exécutable du côté du serveur et il peut permettre de contourner les restrictions du contrôle d'accès basé sur les adresses IP en insérant une adresse IP locale.

Service DHCP

DHCP Starvation

Le principe est d'utiliser la notion d'adresse réservée utiliser par un serveur DHCP après son OFFER. En effet, en attendant une validation du client via un REQUEST, le ou les serveurs DHCP ayant émis des offres considèrent que l'IP ne peut être prise par une autre machine. Le serveur met l'IP proposée en réserve pour ne pas qu'elle soit de nouveau proposé à une autre machine et ainsi éviter les conflits.

L'attaque consiste donc à créer des demandes en très grand nombre jusqu'à prendre toutes les adresses de l'étendue, un client véritable ne pourra donc pas obtenir d'adresses (DDOS).

DHCP Rogue

Cette attaque peut faire suite au DHCP Starvation, il suffit pour cela d'installer un DHCP pirate qui prend la place du DHCP légitime, permettant ainsi de fournir de faux paramètres et d'attirer les clients vers des sites ou des réseaux litigieux.

Comment protéger contre cette attaque ?

Superviser les baux DHCP libres/attribués avec un logiciel de supervision.
Générer des alertes si les seuils sont dépassés.
Utiliser des IDS réseau pour détecter et protéger le réseau.
Utiliser les possibilités offertes par les switches (Anti DHCP Snooping) pour préciser quels sont les serveurs DHCP autorisés.
Activer le Port Security pour fixer un seuil d'adresses MAC possibles sur un port.
Utiliser IPSEC pour chiffrer et authentifier les messages
Utiliser DHCP Explorer qui permet de faire la liste de tous les serveurs DHCP qui vont répondre à une requête DHCP.

Service DNS

DNS Cache Poisoning and Spoofing

La mise en cache DNS est utilisée dans tout le Web pour accélérer les temps de chargement et réduire les charges sur les serveurs DNS.

Les caches sont présents sur toute la chaine allant des serveurs TDL jusqu'au cache de la machine locale. Une attaque visant les serveurs TDL provoque une répercussion sur toute la chaine.

Le but de l'empoisonnement DNS est d'acheminer les utilisateurs vers un site Web frauduleux.

Comment protéger contre cette attaque ?

Faire des mises à jour régulière du programme.
Réduire le TTL.
Supprimer régulièrement les caches DNS des machines locales et des systèmes réseau.
Mettre en place le DNSSEC afin de signer les zones des noms de domaine sur l'ensemble de la chaine.

Attaque par amplification DNS (de type DDoS)

Ces attaques ne ciblent pas le service DNS mais exploitent la nature ouverte des services DNS pour renforcer la force des attaques de déni de service distribuées (DDoS). Ces attaques ont ciblé notamment la BBC, Microsoft, Sony…

L'attaquant utilise un réseau d'ordinateurs infectés par des logiciels malveillants pour envoyer de grandes quantités de trafic vers une cible, comme un serveur. Le but est de surcharger la cible et de ralentir ou de l'écraser.

Les attaques DDoS peuvent être utilisées aussi contre les serveurs DNS comme ce qui arrivé aux services DNS de Dyn.

Comment protéger contre cette attaque ?

Utiliser des pare-feu contre le DDOS
Utiliser plusieurs serveurs pour absorber une attaque.

Les pare-feux

Il existe différentes catégories de firewall pour pouvoir répondre aux besoins de chaque entreprise.

Le pare-feu sans état (stateless firewall)

C'est le plus vieux dispositif de filtrage réseau introduit sur les routeurs. Il regarde chaque paquet indépendamment des autres et le compare à une liste de règles pré configurées.

Le pare-feu à états (stateful firewall)

Les pare-feu à états vérifient la conformité des paquets à une connexion en cours. C'est-à-dire qu'ils vérifient que chaque paquet d'une connexion est bien la suite du précédent paquet et la réponse à un paquet dans l'autre sens. Ils savent aussi filtrer intelligemment les paquets qui servent à la signalisation des flux IP.

Le pare-feu applicatif

Dernière génération de pare-feu, ils vérifient la complète conformité du paquet à un protocole attendu. Chaque application est gérée par un module différent pour pouvoir les activer ou les désactiver à la demande.

Un pare-feu applicatif va être, par exemple, en mesure d'analyser une connexion HTTP et de n'autoriser les commandes PUT qu'à un nombre restreint de machines.

Le pare-feu identifiant

Ce pare-feu réalise l'identification des connexions passant à travers le filtre IP. L'administrateur peut ainsi définir les règles de filtrage par utilisateur et non plus par adresse IP ou MAC, et ainsi suivre l'activité réseau par utilisateur.

Une autre approche est l'identification connexion par connexion (sans avoir cette association IP = utilisateur et donc sans compromis sur la sécurité) qui permet d'identifier

également sur des machines multi-utilisateurs.

Le pare-feu personnel

Le pare-feu personnel, généralement installé sur une machine de travail, agit comme un pare-feu à états. Bien souvent, il vérifie aussi quel programme est à l'origine des données. Le but est de lutter contre les virus informatiques et les logiciels espions.

Le portail captif

Les portails captifs sont des pare-feu dont le but est d'intercepter les usagers d'un réseau de consultation afin de leur présenter une page web spéciale (par exemple : avertissement, charte d'utilisation, demande d'authentification, etc.) avant de les laisser accéder à Internet. Ils sont utilisés pour assurer la traçabilité des connexions et/ou limiter l'utilisation abusive des moyens d'accès. On les déploie essentiellement dans le cadre de réseaux de consultation Internet mutualisés, filaires ou Wi-Fi.

Choisir son pare feu

Un certain nombre de questions essentielles sont à se poser lors de l'acquisition de son pare feu pour bien cibler ses besoins, telles que :

- le nombre d'utilisateurs et de serveurs d'entreprise sur le réseau local
- le nombre de sites distants et d'utilisateurs nomades à connecter au site d'entreprise
- le type et nombre d'accès internet
- le débit nécessaire pour assurer une qualité de service à l'entreprise
- la nécessité ou non de filtrer l'accès Internet des utilisateurs
- la nécessité ou non de bloquer le téléchargement illégal
- la nécessité ou non d'assurer une continuité de service des accès Internet, VPN et pare-feu

https://www.itcentralstation.com/categories/firewalls

Comparatif Firewall

Les détecteurs d'intrusions

Un système de détection d'intrusions (IDS, Intrusion détection System) peut être assimilé à un renifleur utilisé dans le sens de la protection réseau.

Un IDS ne filtre pas les paquets à la manière d'un pare-feu, mais il les capture et les inscrit dans un fichier. Il est aussi doté de fonctions spéciales, permettant entre autres de :

détecter des activités anormales,
rechercher d'éventuelles faiblesses
détecter des changements dans le système de fichiers.

Mais le système de détection d'intrusions sert avant tout à relever les tentatives de sondage ou de connexion au système.

Une utilité des IDS est de savoir ce que filtre réellement le pare-feu. Pour cela il suffit d'en installer un avant et un autre après le dispositif et de comparer les résultats de sortie.

Les IPS (Systèmes de prévention d'intrusion) tentent quant à eux de bloquer l'attaque en cours mais ils sont difficiles à paramétrer.

Les familles de systèmes de détection d'intrusion

Les **NIDS** (Network Based Intrusion Detection System) , qui surveillent l'état de la sécurité au niveau du réseau.
Les **HIDS** (HostBased Intrusion Detection System) , qui surveillent l'état de la sécurité au niveau des hôtes.

NIDS (IDS réseau)

Un NIDS se découpe en trois grandes parties : la capture, les signatures et les alertes.

1. Capture

La capture sert à la récupération de trafic réseau principalement en temps réel.
La capture doit refragmenter les paquets reçus pour être capable de détecter les attaques cachées dans des paquets découpés. La capture doit être capable également de détecter des commandes illégales (ex : http://localhost\windows, file://c:\perso)

2. Signatures

Les bibliothèques de signatures sont similaires à celle des antivirus en s'appuyant sur des

signatures d'attaques.

3. Alertes

Les alertes sont stockées dans les journaux du système.

HIDS (IDS machine)

Les HIDS, "système de détection d'intrusion machine" sont des IDS dédiés à un matériel ou un système d'exploitation.

Ils surveillent :
1. l'activité de la machine : processus, ressources consommées…
2. l'activité de l'utilisateur : connexions, commandes utilisées, messages envoyés, programmes activés, dépassement du périmètre défini…
3. l'activité malicieuse d'un ver, virus ou cheval de Troie

APPROCHE PAR SCÉNARIO

Les systèmes à base de signatures recherchent dans l'activité de l'élément surveillé les signatures (empreintes) d'attaques connues.

Ce principe de détection peut être contourné par des pirates maquillant leurs attaques en modifiant la signature connue par les IDS et de ce fait l'attaque devient invisible par l'IDS.

APPROCHE COMPORTEMENTALE

Les systèmes à approche comportementale détectent les différentes anomalies sur le réseau. C'est l'administrateur qui définit le fonctionnement "légitime" et cela peut demander une phase d'apprentissage assez longue pour fixer ce niveau. Par la suite l'IDS sera en mesure de signaler à l'administrateur toute situation qui s'éloigne du niveau de fonctionnement de référence.

Cependant, ce fonctionnement engendre un certain nombre de faux positifs et des ajustements sont nécessaires.

IPS

Un système de prévention d'intrusion (Intrusion Prevention System) est un outil similaire aux IDS, qui permet de prendre des mesures pour diminuer les impacts d'une attaque

comme bloquer des ports automatiquement.

Les IPS peuvent parer les attaques connues et inconnues. Comme les IDS, ils ne sont pas fiables à 100 % et risquent même en cas de faux positif de bloquer du trafic légitime.

RÉPONSE ACTIVE

Les réponses actives permettent d'interrompre le flux intrusif en envoyant une requête d'arrêt de connexion à l'émetteur, mais elles peuvent présenter des inconvénients.

1. En analysant la valeur situées dans les trames de réponse, il est quelquefois possible de déduire quel est l'IDS qui les a émit.
2. Si l'attaquant utilise le spoofing, l'IPS peut bloquer une adresse valide et du coup, nous empêcher de communiquer avec (FAI, DNS…). il faut alors utiliser une liste blanche de ce qu'il ne faut absolument pas bloquer.

La liste blanche bloque le paquet suspect mais ne coupe pas définitivement la communication vers cette adresse.

RÉPONSE PASSIVE

Cette technique consiste à bloquer les flux intrusif sans en informer la source. Le pirate n'est pas au coutant de l'existence d'un IPS. Cependant, on retombe malheureusement sur un des problèmes vu ci-dessus, l'authenticité de la source de l'attaque.

IDS / IPS : schéma

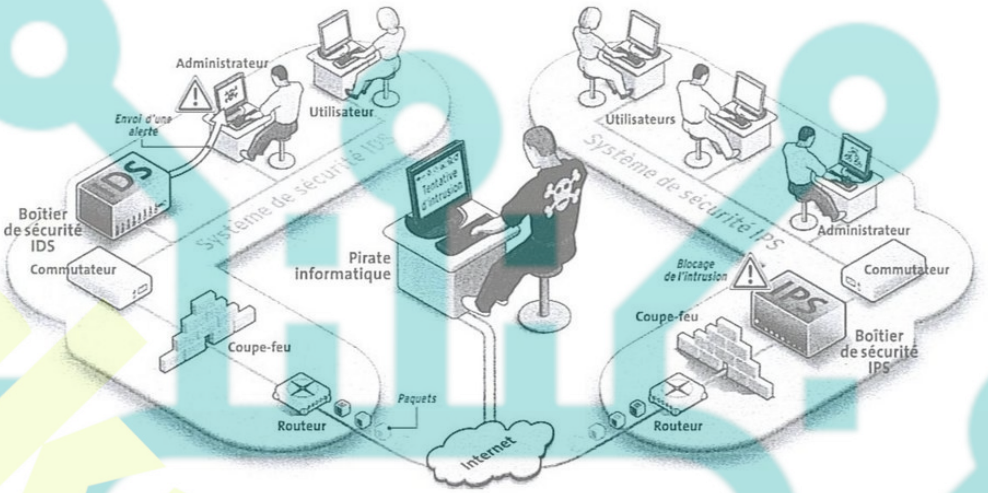


Schéma IPS et IDS

Quelques produits

Security Onion

Security Onion est une distribution Linux basée sur Ubuntu utilisée pour la surveillance du réseau et la détection des intrusions. cet IDS peut surveiller plusieurs VLAN et sous-réseaux et fonctionne correctement dans les environnements virtuels. Cette configuration ne peut être utilisée que comme IDS. Actuellement, il n'est pas supporté pour être exécuté en tant qu'IPS. L'assistant de configuration convivial permet de créer en quelques minutes un groupe de nombreux capteurs distribués pour les entreprises.

OSSEC

OSSEC est un système de détection d'intrusion d'hôte à source ouverte (HIDS) qui offre plusieurs modules supplémentaires pouvant être utilisés avec les fonctionnalités de base d'IDS. En plus de la détection d'intrusion, OSSEC peut effectuer la surveillance de l'intégrité des fichiers et la détection de rootkit avec des alertes en temps réel, qui sont toutes gérées de manière centralisée avec la possibilité de créer différentes stratégies, en fonction des besoins de l'entreprise. OSSEC est multi-plateformes

OpenWIPS-NG

OpenWIPS-NG est un système IDS / IPS sans fil qui repose sur un serveur, des capteurs et des interfaces et disponible librement. Développé par l'auteur de Aircrack-NG, ce système dispose de nombreuses fonctionnalités et services déjà conçus pour la numérisation, la détection et la prévention des intrusions. OpenWIPS-NG est modulaire et permet à un administrateur de télécharger des plug-ins pour des fonctionnalités supplémentaires. Il fournit également une installation pour effectuer WIPS avec un budget serré.

Suricata

Contrairement aux autres systèmes IDS / IPS, Suricata est le plus directement en concurrence avec Snort. Ce système a une architecture similaire à Snort qui repose sur des signatures et peut même utiliser des règles Snort.

Bro IDS

Bro IDS resemble à Security Onion, cependant, il utilise plus que les règles IDS pour savoir d'où viennent les attaques. Il utilise une large gamme de modules d'analyse de protocole pour contrôler le trafic et prendre des décisions concernant sa conformité à diverses normes. C'est un complément très puissant à Snort.

https://dbprog.developpez.com/securite/ids/

Détection d'intrusions

Tests d'intrusion

Metasploit

Metasploit vérifie plus de 1 300 programmes et vous aide à déterminer comment les hackers peuvent vous pirater.
https://www.metasploit.com/ < http://snip.ly/dn9nl

Scanner de réseau Nmap

Nmap crée une carte détaillée du réseau et de ses ressources. Le logiciel fournit un certain nombre de fonctionnalités pour les tests des réseaux informatiques.
https://nmap.org/book/nmap-overview-and-demos.html
https://nmap.org/book/nmap-overview-and-demos.html

Portswigger Burp Suite

Burp Suite fournit une plateforme intuitive pour effectuer des tests de pénétration afin d'évaluer la sécurité des applications web.
https://portswigger.net/burp/ < https://portswigger.net/burp/

SQLmap

Sqlmap est un outil de test d'intrusion qui permet l'automatisation de la détection des défauts d'injection SQL.
http://sqlmap.org/ < http://snip.ly/vctmi

Kali Linux

Récemment mis au point, Kali Linux est un **outil de test d'intrusion populaire** créé par Black Hat.
https://www.kali.org/ < https://www.kali.org/
https://www.offensive-security.com/community-projects/
https://www.offensive-security.com/community-projects/
https://www.vpnmentor.com/blog/kali-linux-a-guide-to-ethical-hacking/ https://www.vpnmentor.com/blog/kali-linux-a-guide-to-ethical-hacking/