Sécurité : les 4 piliers de la sécurité : DICP

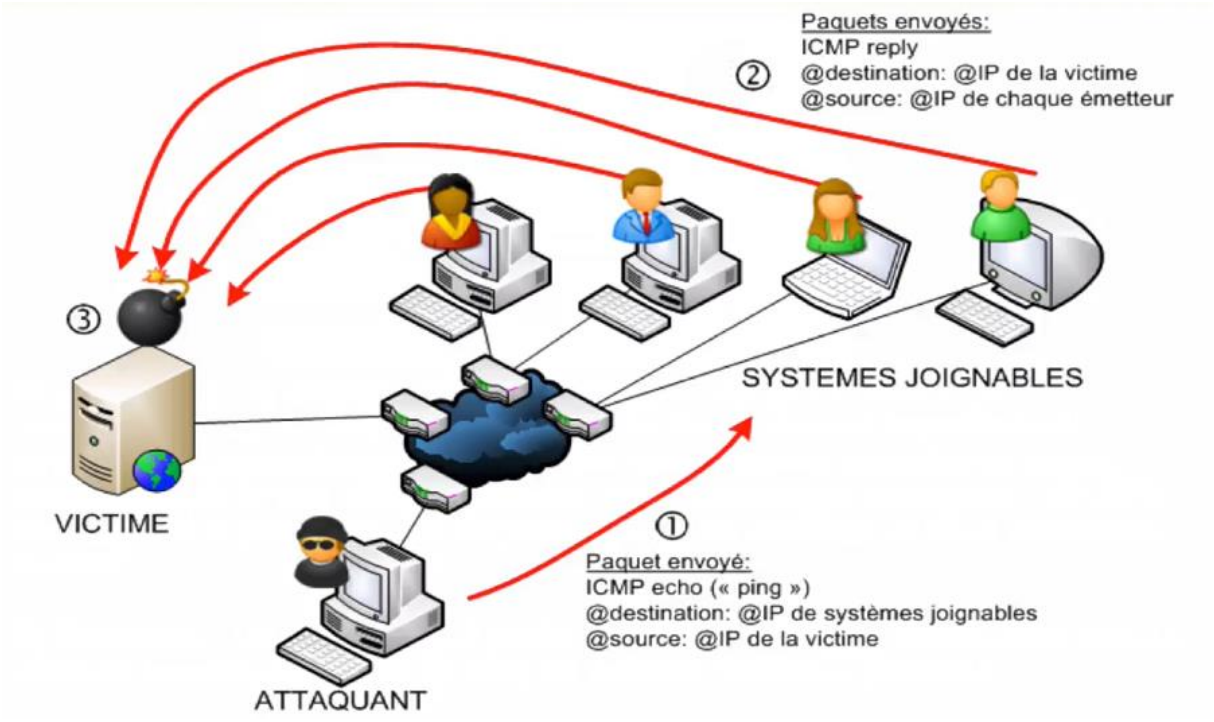
Les 4 piliers de la sécurité sont :

- **La Disponibilité**
- **L'Intégrité**
- **La Confidentialité**
- **Et la Preuve**

1. La Disponibilité

La disponibilité d'un système est une mesure de performance que l'on obtient en divisant la durée durant laquelle le système est opérationnel par la durée totale durant on aurait souhaité qu'il le soit. Elle se mesure en pourcentage (99,99% correspond à une perte de disponibilité de 52 minutes et 34 secondes sur une année)

Les principales menaces de la disponibilité sont les pannes, le déni de service (DOS) ou encore le déni de service distribué



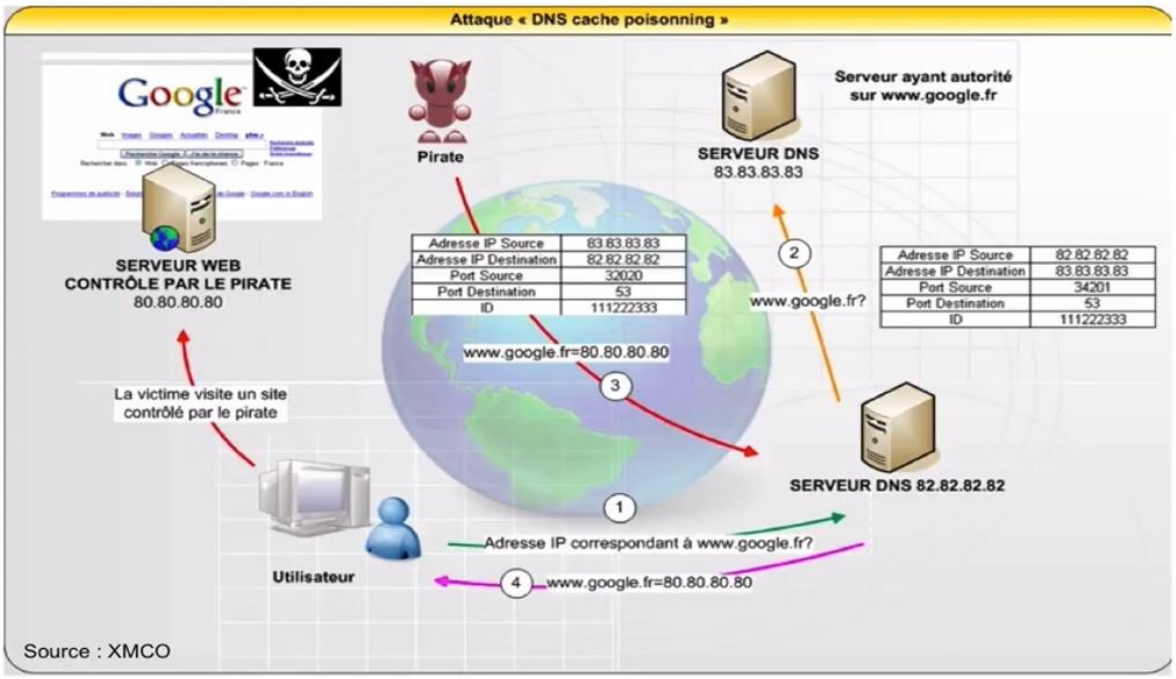
Lors d'une attaque DDOS, l'attaquant envoie un paquet à de multiples destinataires en modifiant l'adresse source, afin que ces derniers répondent simultanément à la victime. Bien sûr ceci s'effectue avec plusieurs centaines, milliers, millions d'intermédiaires au travers d'un malware par exemple. La victime va recevoir des millions de requêtes simultanée et se mettre en déni de service.

2. L'Intégrité

L'intégrité désigne l'état des données qui, lors de leur traitement, de leur conservation ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle

Les erreurs de saisie font partie des principales menaces ainsi que tout ce qui concerne les accès non autorisés aux données suite à des erreurs d'habilitation ou à des actes malveillants.

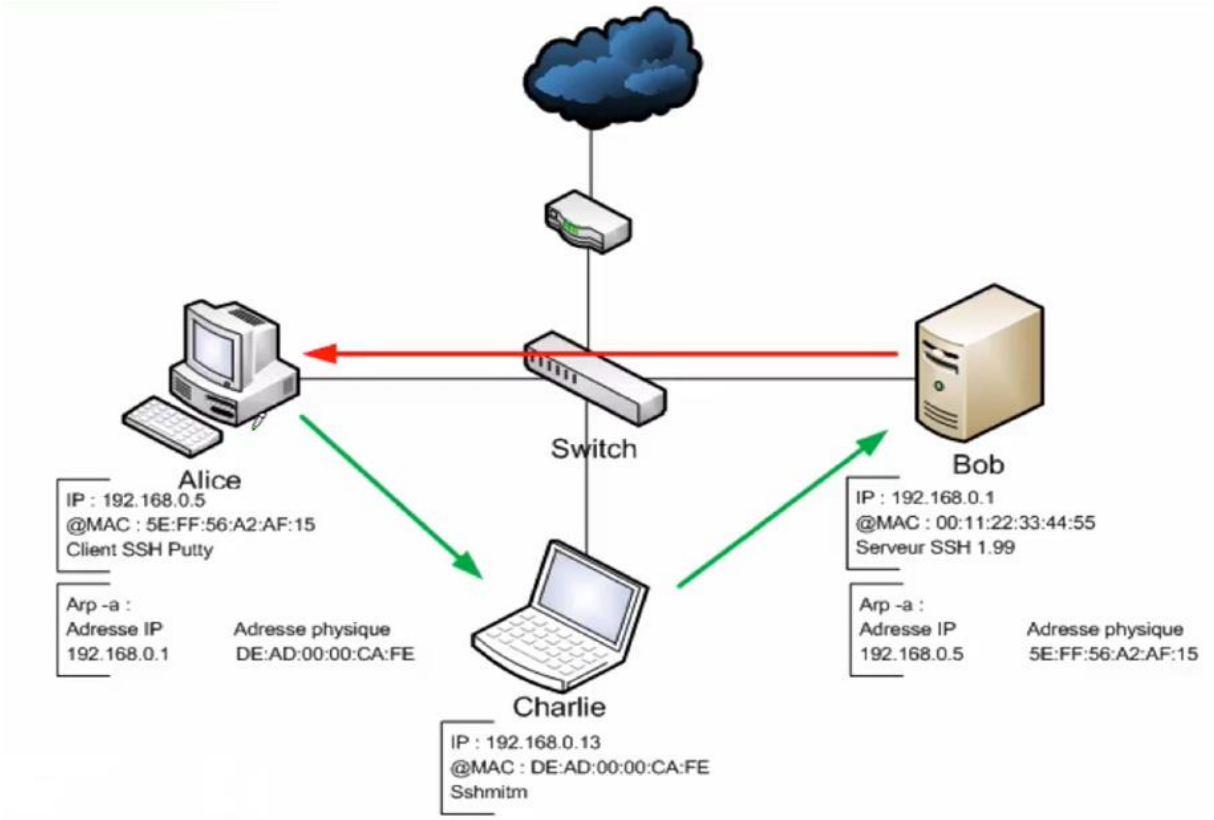
Par exemple un DNS Poisonning :



3. La Confidentialité

La confidentialité est le fait de s'assurer que l'information n'est seulement accessible qu'à ceux dont l'accès est autorisé. Le principe de base est donc qu'une donnée ne doit être accessible que par les personnes qui ont des droits sur cette donnée. C'est le principe du moindre privilège

La négligence humaine (vol ou perte d'un smartphone ou d'un PC portable) est l'une des principales menaces sur la confidentialité au même titre que l'interception des données.



4. La Preuve

La preuve, ou imputabilité ou traçabilité, est le fait d'avoir la possibilité de remonter jusqu'à l'origine d'un évènement et cela de manière sûre et fiable. Cela inclut également la non répudiation : un utilisateur ne peut nier avoir effectué une action ou reçu une information

L'absence de journalisation est l'une des principales menaces ainsi que l'usurpation d'identité ou encore l'utilisation de réseaux et/ou de proxy permettant un certain anonymat. En entreprise, toute connexion internet doit être tracée (quel site, quelle heure, qui, …)

5. Les autres piliers

- L'authentification

L'objectif de l'authentification est de vérifier l'identité d'une entité, et ceci par un identifiant suivi d'un ou plusieurs facteurs d'authentifications

Parmi ces facteurs d'authentification, nous en trouvons 3 :

- Ce que nous savons (ex : mot de passe)
- Ce que nous avons (ex : une carte à puce)
- Ce que nous sommes (ex : une empreinte digitale)

Une authentification est classée forte lorsqu'au moins 2 facteurs parmi les 3 sont exigés

Un paiement par carte bancaire est une authentification forte car la carte est ce que nous avons, et le code est ce que nous savons.

- **Habilitation**

L'habilitation est le fait de vérifier si une entité demandant d'accéder à une ressource a les droits pour le faire. Les actions de l'entité doivent ensuite être encadrés.

3 mécanismes doivent être mis en œuvre :

- L'authentification (vue au paragraphe précédent)
- Des autorisations (qui a accès à quoi)
- La traçabilité (tout doit être journalisé)