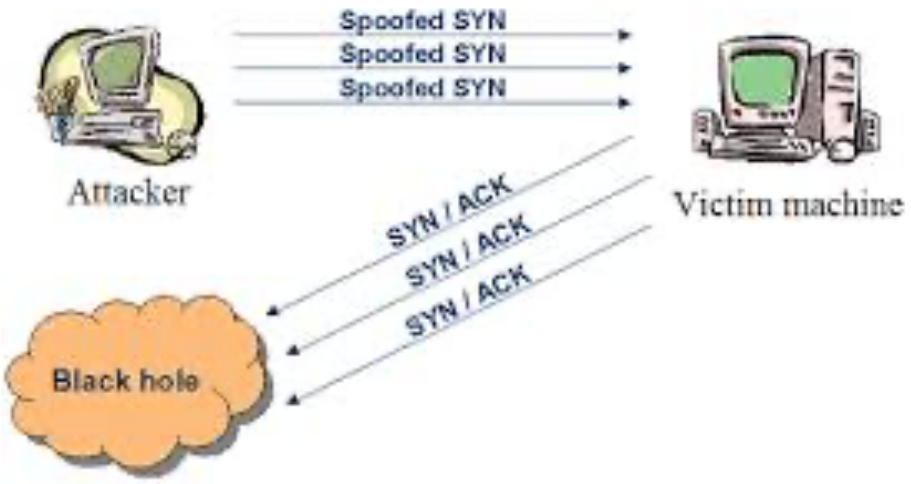
SAE 15 : Analyse

Après le traitement du fichier qu'on devait analyser on a repérer des choses qui ne vont pas bien sur le réseau et qui peuvent mener à le dysfonctionnement de ce réseau . Alors on a trouvé que :

- **l'adresse IP suivante (source) : 190-0-175-100.gba.solunet.com.ar a envoyé plusieurs requêtes HTTP (plus de 2000 dans moins de 45s) et à chaque fois avec un numéro de port différent mais à la même adresse IP :184.107.43.74 (destination) avec un flag [S] =SYN ce qui veut dire : cette adresse IP source a essayé de se synchronisé plus de 1000 fois pour établir sa requête mais elle ne reçoit pas d'accusé de reception (SYN + ACK) de la part de l'adresse de destination . Ce phénomène est considéré parmi les attaques de déni de service et il s'appelle exactement une attaque SYN Flood. Cette attaque consiste à provoquer un déni de service en émettant un nombre important de demandes de synchronisation TCP incomplète avec un serveur .Celui qui pratique cette attaque comme dans notre cas celui ayant l'adresse IP source , il envoie une série de messages SYN, mais laisse les connexions semi-ouvertes. La file d'attente du serveur se remplit et le nouveau client ne peut plus se connecter et par la suite un déni de service DoS .**



Et c'est pour cela notre adresse IP source ne recevait pas d'accusé de reception car notre adresse victime ne savait d'ou venait les SYN vu qu'ils sont spoofed ça veut dire « usurpé » ils portent une fausse identité informatique si on peut dire .

- **Le deuxième phénomène qu'on a remarqué dans la longue succession de trames qu'on a dans le fichier à traiter c'est un énormes de pings envoyés par le même poste d'adresse IP(source): BP-Linux8 (des request ICMP) et qui sont envoyés à la même adresse IP (destination) : 192.168.115.1 . Ceci est aussi parmi les attaques de déni de service et ce type d'attaque s'appelle :Ping 'O**

Death et en français : ping de la mort . Ce type d'attaque consiste à saturer un routeur ou un serveur en envoyant un nombre important de requêtes ICMP request dont les datagrammes dépassent la taille maximum autorisée .

<u>Mais c'est quoi l'attaque par déni de service :</u>

Une attaque par déni de service est une attaque informatique ayant pour but rendre indisponible un service ou d'empêcher les utilisateurs d'utiliser un service dont ils ont droit . Alors , il peut s'agir:

- **L'inondation d'un réseau agi. d'empêcher son fonctionnement ;**
- **La perturbation des connexions entre deux machines, empêchant l'accès à un service**
- **L'obstruction d'accès à un service pour une personne en particulier**