Université de Caen Normandie

Sécurité Avancée

Master 1 Informatique
Parcours:
CyberSécurité

RAPPORT SUR ATTAQUE DDOS ETUDE ET SIMULATION

Réalisé par :

BOUIMEDJ Sylia 22011983
MAZOUAK Ayoub 21913331
MVUKULU Robin 21813788

Encadrement : KHOUKHI LYES

Résumé du projet:

Notre travail était d'étudier et de simuler un ensemble d'attaques sur des machines virtuelles via l'utilisation de VirtualBox et de Kali Linux dans des contextes différents selon le type d'attaque. Les attaques choisies utilisent des méthodes diverses et sont toutes des attaques DDoS (Déni de service distribué).

Qu'est ce qu'une attaque DDoS ?

Une attaque DDOS (Distributed Denial of Service) est une attaque informatique dans laquelle un grand nombre d'ordinateurs ou de périphériques connectés à Internet inondent un serveur cible avec un grand nombre de requêtes, le rendant ainsi inaccessible aux utilisateurs légitimes. Ces attaques sont souvent menées dans le but de causer des perturbations, de la confusion ou des dommages à l'entreprise ou à l'organisation ciblée.

Quelles sont les cibles principales d'une attaque DDoS ?

- Les serveurs qui hébergent les sites d'achats
- Les entreprises ou les organisations qui dépendent de la fourniture de services en ligne

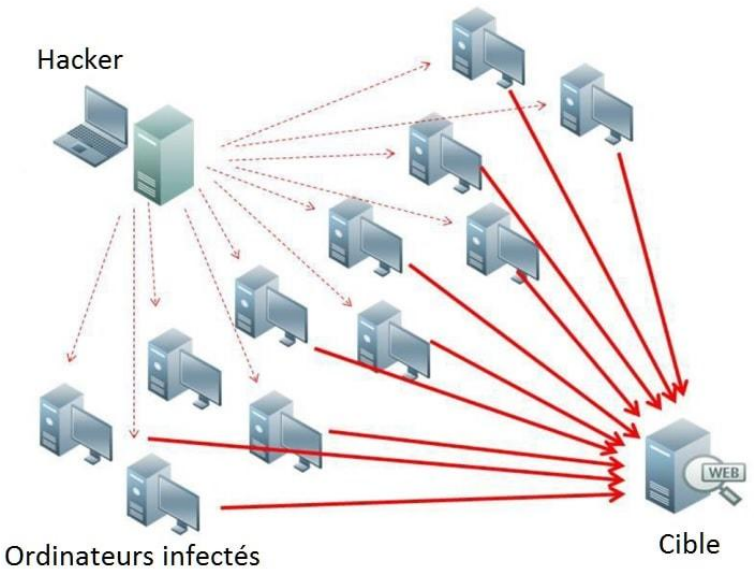


Figure 1: Fonctionnement d'une attaque DDoS

Comment fonctionnent les attaques DDoS ?

Les attaques DDoS consistent à submerger un site web ou un serveur de requêtes pour le rendre indisponible. Les attaquants utilisent souvent un grand nombre d'ordinateurs zombies, également connus sous le nom de botnets, pour envoyer simultanément des demandes de connexion à la cible. Cette surcharge de trafic peut entraîner une baisse des performances ou encore une interruption complète du service. *(Figure 1)*

Quel est le but d'une attaque DDoS ?

Le but de l'attaquant est la prévention totale du fonctionnement normal de la ressource Web. L'attaquant peut également demander un paiement pour arrêter l'attaque. Dans certains cas, une attaque DDoS peut même être une tentative de discréditer ou de nuire à l'entreprise d'un concurrent.
Ce but est atteint grâce à l'une de ces trois stratégies choisie en fonction de l'attaque:

- Surcharge de la bande passante.
- Surcharge des ressources.
- Exploitation d'erreurs système et des lacunes de sécurité.

Quels sont les types d'attaques DDoS ?

Il existe plusieurs types d'attaques DDoS, chacun ayant ses propres caractéristiques et objectifs:

- Attaque d'amplification: Consiste à envoyer des paquets de données à la cible, qui répondra en envoyant une quantité beaucoup plus importante de données en retour, amplifiant ainsi l'attaque. *(Exemple: Attaque par rebond et amplification NTP).*
- Attaque de saturation: Consiste à submerger une cible avec un grand nombre de requêtes pour épuiser ses ressources réseau et la rendre indisponible. *(Exemple: Attaque SYN Flood).*

- Attaque de fragmentation: Consiste à envoyer des paquets illégitimes qui surchargent les ressources de la cible. *(Exemple: Attaque Teardrop)*
- Attaque d'application: Consiste à exploiter les vulnérabilités des applications web ou des serveurs pour les rendre indisponibles. *(Exemple: Attaque HTTP Flood)*

Les attaques présentés dans ce rapport:

Les méthodes d'attaque que nous avons choisies pour simuler les attaques DDoS sont les suivantes:

- Attaque Slowloris
- Attaque par rebond et amplification NTP
- Attaque SYN Flood

Attaque DDoS Slowloris

Explication du principe de l'attaque:

Cette attaque est une attaque de type attaque de saturation qui consiste à exploiter les limites du serveur en envoyant un grand nombre de requêtes HTTP "incomplètes mais légitimes", ce qui maintient la connexion HTTP ouverte pendant une durée maximale. Cela épuise les ressources du serveur ce qui va donc entraîner une surcharge des ressources et rendre le serveur indisponible pour les utilisateurs.

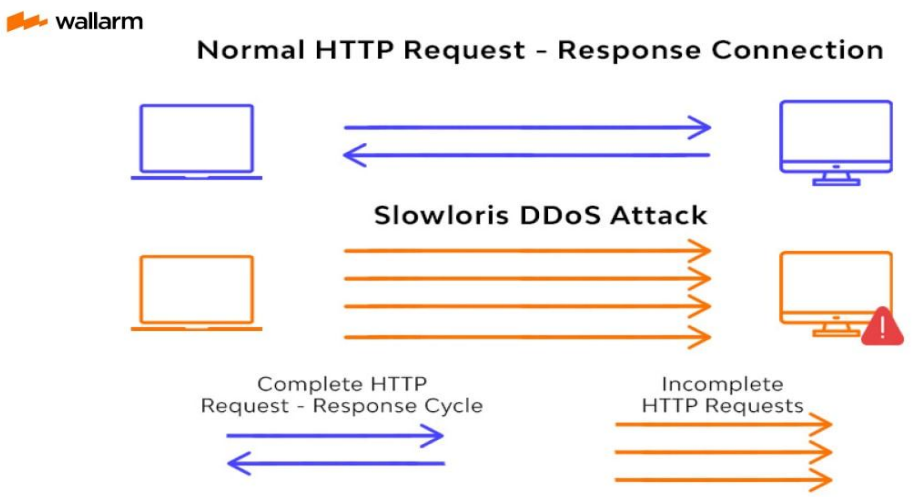


Figure 2: Fonctionnement d'une attaque DDoS Slowloris
source: Wallarm.com

Fonctionnement de l’attaque:

1. L’attaquant envoie une requête HTTP incomplète au serveur cible.
2. Comme la requête est incomplète, le serveur conserve la connexion en attendant de nouvelles données.
3. L’attaquant envoie ensuite de nombreuses requêtes HTTP incomplètes simultanément, ce qui maintient la connexion HTTP ouverte pendant une durée maximale.
4. Les connexions HTTP ouvertes vont consommer toutes les ressources du serveur (Mémoire et processeur).
5. Le serveur finit par être surchargé et ne peut plus traiter les demandes des utilisateurs.

Simulation de l’attaque:

Nous avons utilisé plusieurs machines virtuelle sous VirtualBox:

- Une machine serveur apache (10.0.2.15).
- Une machine client (10.0.2.6).
- Une machine attaquant (10.0.2.7).
-

Nous avons configuré la machine serveur pour qu’elle puisse héberger un serveur apache en utilisant *apache2*. Voici la page de base lors de la connexion au serveur:

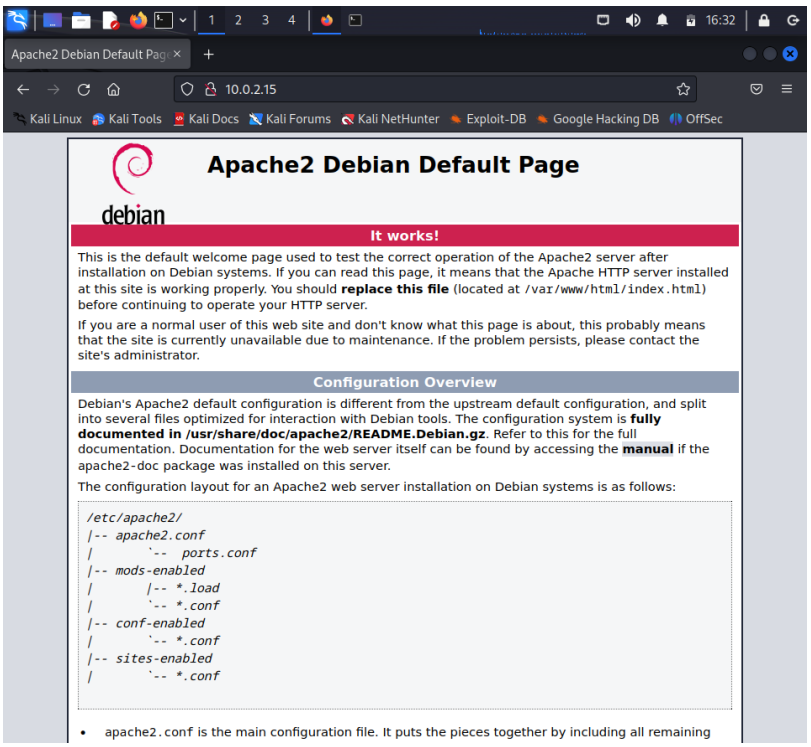


Figure 4: Page avant l'attaque

Ensuite on lance le script de l'attaque slowloris sur la machine attaquant:

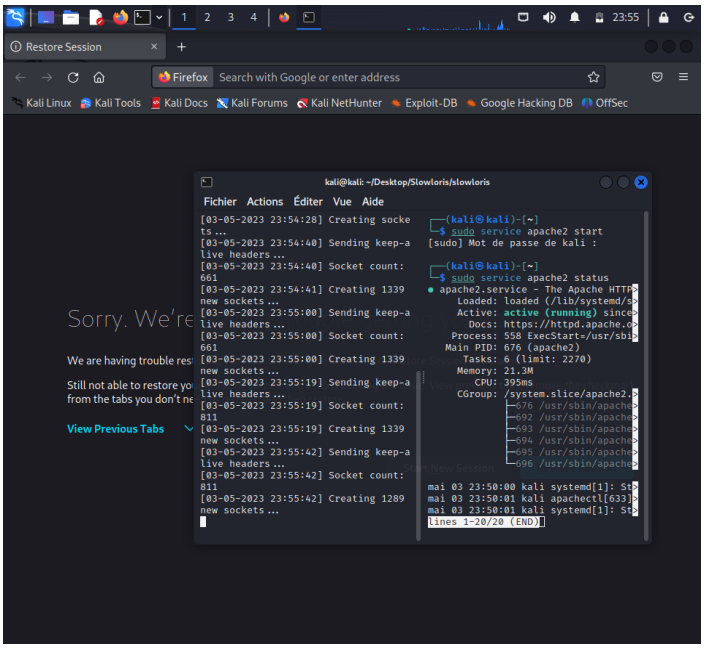


Figure 5: Utilisation du script de l'attaque Slowloris

On remarque les paquets envoyés côté serveur avec Wireshark:

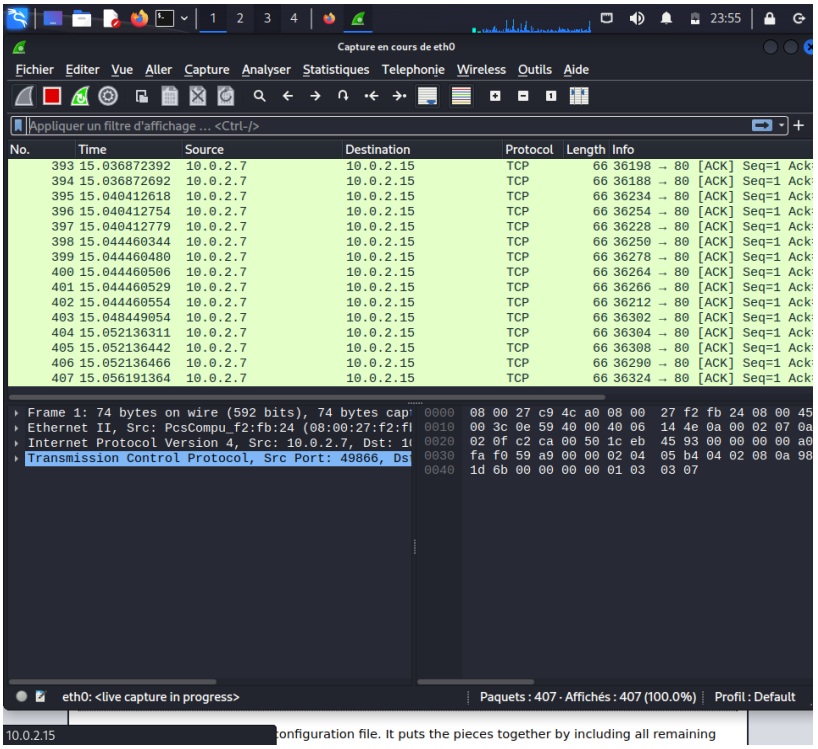


Figure 6: Wireshark des échanges entre l'attaquant et le serveur pendant l'attaque

Par la suite lorsque l'on recharge la page elle charge en boucle:

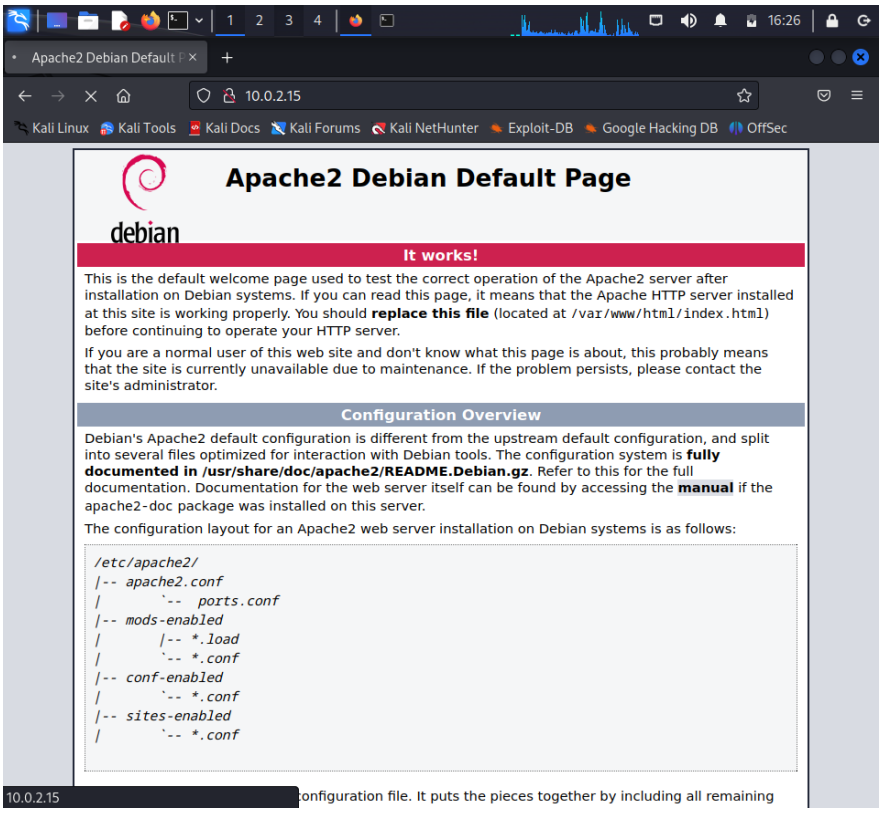


Figure 7: Page web pendant l'attaque

Comment se protéger contre cette attaque ?

- Limiter le nombre de connexions avec le serveur qu'une adresse IP peut ouvrir.
- Augmenter la vitesse de transfert minimale autorisée pour n'importe quelle connexion.
- Limiter la durée pendant laquelle un client est autorisé à rester connecté.

Attaque DDoS par amplification et rebond NTP

Explication du principe de l'attaque:

Cette attaque est une attaque de type attaque d'amplification qui consiste à exploiter les serveurs NTP mal configurés pour amplifier le trafic réseau vers une cible, ce qui va surcharger la bande passante ainsi que les ressources réseau.
L'une de ces requêtes, "monlist", consiste à demander au serveur NTP d'indiquer la liste des derniers utilisateurs avec qui il a eu des échanges. La requête ne nécessitait pas d'authentification et pouvait donc être utilisée pour amplifier le trafic vers une cible en générant des réponses NTP bien plus volumineuses que la requête initiale. Cette méthode était tellement efficace qu'elle a entraîné une mise à jour des serveurs NTP pour supprimer la commande "monlist".

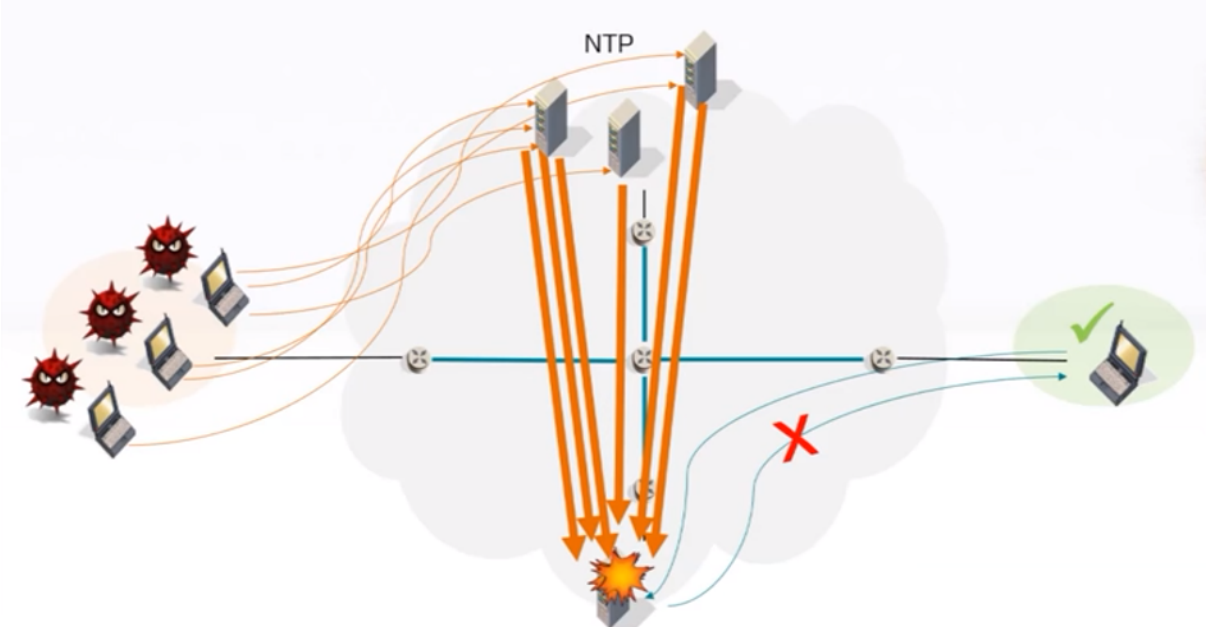


Figure 8: Principe de l'attaque DDoS par amplification et rebond NTP
source: Youtube 6cure

Fonctionnement de l'attaque:

1. L'attaquant envoie des requêtes NTP en se faisant passer pour un des clients des serveurs NTP mal configurés en utilisant l'adresse IP de sa cible comme adresse source.
2. Les serveurs NTP envoient donc des réponses au client puisqu'ils pensent que c'est lui qui a envoyé les requêtes.
3. Comme les réponses sont plus grandes que les requêtes (Exemple avec monlist) le client finit par être submergé de trafic réseau.

Démonstration de l'attaque:

Nous avons utilisé plusieurs machines virtuelle sous VirtualBox:

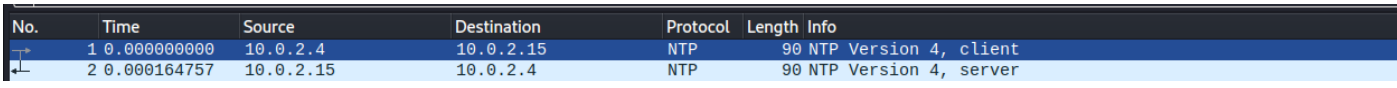
- Une machine serveur NTP (10.0.2.15)
- Une machine client (10.0.2.4)
- Une machine attaquant (10.0.2.5)

Nous avons configuré la machine client pour qu'elle ne reçoive l'heure que grâce au serveur NTP:

```
┌──(kali㉿kali)-[~]
└─$ sudo ntpdate 10.0.2.15
2023-04-29 14:51:37.572718 (+0200) +7.040771 +/- 0.000300 10.0.2.15 s2 no-leap
CLOCK: time stepped by 7.040771
```

Figure 9: Récupération de l'heure via le serveur NTP

Et voici l'échange entre le client et le serveur NTP.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.4	10.0.2.15	NTP	90	NTP Version 4, client
2	0.000164757	10.0.2.15	10.0.2.4	NTP	90	NTP Version 4, server

Figure 10: Visualisation de l'échange via Wireshark

Puis à l'aide d'un script nous avons envoyé des requêtes NTP à partir de la machine attaquant en se faisant passer pour la machine cliente.

Voici le Wireshark côté serveur pendant l'attaque:

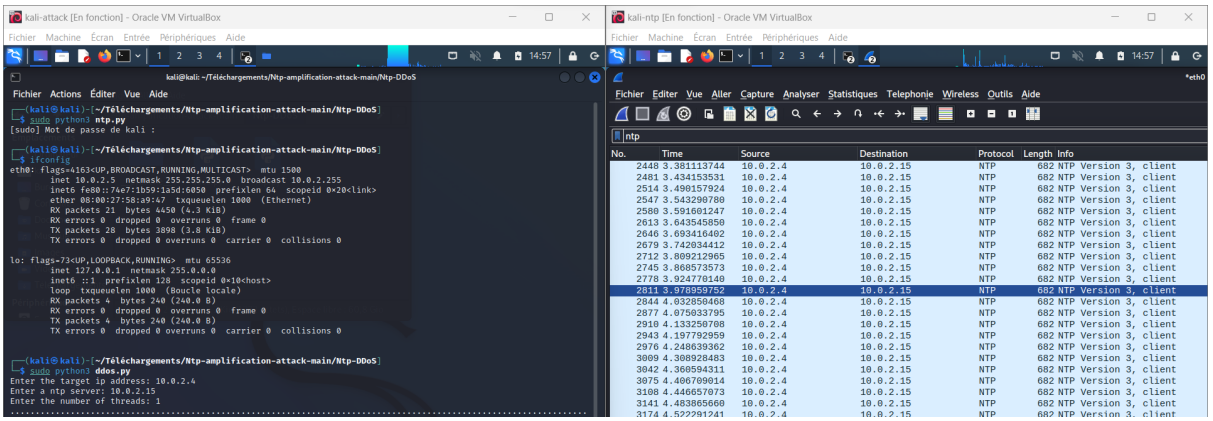


Figure 11: Visualisation des échanges lors de l'attaque NTP par amplification et rebond NTP

Cela indique que le serveur NTP reçoit bien les requêtes NTP. Cependant il n'y répond pas, il est possible que la raison soit que la version des paquets NTP ne soit pas la même version ou que la requête ne soit plus existante.
Cela n'empêche pas non plus le client de faire une requête NTP pour recevoir l'heure actuelle pendant l'attaque. Donc l'attaque a échoué.

Comment se protéger contre cette attaque ?

- Black listing (Pare-feu): Une liste de blocage d'adresse IP ou de domaines pour bloquer le trafic malveillant.
- Blackholing (Routeur): Un mécanisme de routage qui redirige le trafic vers une destination poubelle.
- Blocage de requêtes redondantes: Un mécanisme qui bloque les requêtes redondantes venant de la même adresse IP.
- Blocage de contributeurs inhabituellement volumineux: Un mécanisme qui bloque les adresses IP qui contribuent de manière inhabituelle à une charge de trafic.

Attaque DDoS SYN Flood

Explication du principe de l'attaque:

Cette attaque est une attaque de type attaque de saturation qui consiste à inonder un serveur cible avec une quantité massive de requêtes de connexion SYN. Le but étant de saturer les ressources du serveur et donc d'empêcher les autres utilisateurs de faire des demandes de connexion SYN.

Cette attaque exploite le protocole de communication TCP/IP pour générer de fausses requêtes de connexion SYN mais sans les terminer ce qui fait que le serveur reste dans un état de demande de connexion en attente pour chacune des requêtes et cela mène à l'épuisement des ressources du serveur.

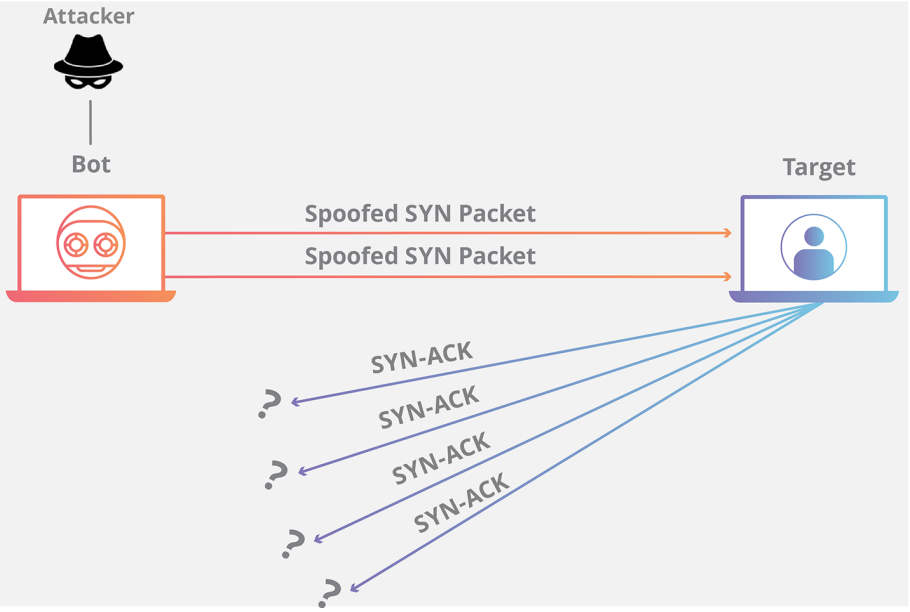


Figure 12: Principe de l'attaque DDoS SYN Flood
source: cloudflare.com

Fonctionnement de l'attaque:

1. L'attaquant envoie une série de demandes de connexion SYN au serveur cible en se faisant passer pour des IP aléatoires ou usurpées en utilisant l'IP spoofing. *(Attaque par usurpation d'identité)*
2. Le serveur répond à chaque demande de connexion SYN en envoyant un paquet SYN-ACK à l'adresse IP source, sauf que cette adresse n'existe pas réellement
3. L'attaquant ne répond donc pas à ces paquets SYN-ACK et continue d'envoyer de nouvelles demandes de connexion SYN afin d'inonder le serveur de demande SYN en suspens.
4. Le serveur se retrouve progressivement saturé de demande, ces ressources étant épuisées il ne peut plus répondre aux clients.

Précision: Il est également possible que l'attaquant utilise sa véritable adresse et empêche sa machine de répondre aux SYN-ACK du serveur. On parle dans ce cas *d'attaque directe*.

Démonstration de l'attaque:

Nous avons utilisé plusieurs machines virtuelle sous VirtualBox:

- Une machine serveur apache (10.0.2.15)
- Une machine client (10.0.2.6)
- Une machine attaquant (10.0.2.7)

En utilisant *htop* on a pu observer l'état du serveur avant:

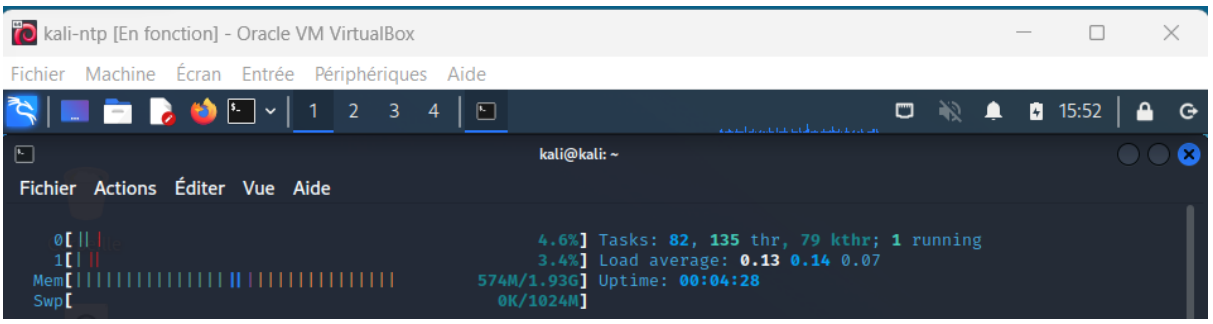


Figure 13: Performance du serveur avant l'attaque SYN Flood

Puis avec l'utilisation *hping3* et la commande *hping3 -S –flood @IPserveur nous avons demandé des requêtes*

Lorsque l'on utilise l'option –flood cela va ignorer les réponses SYN-ACK.

Après quelques minutes voici les performances du serveur:

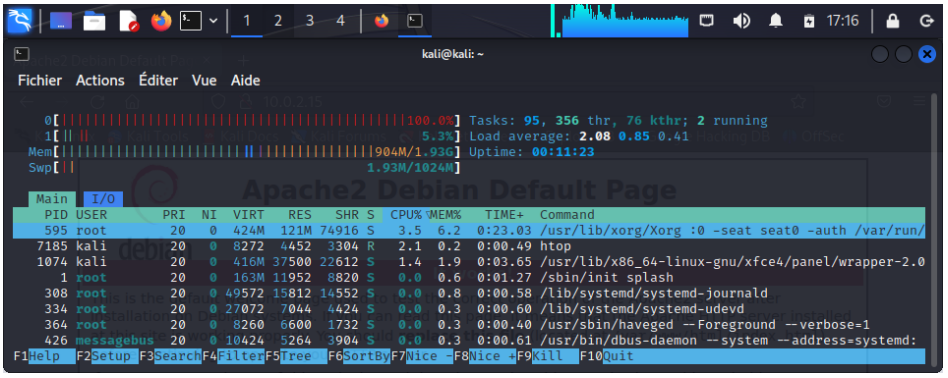


Figure 14: Performance du serveur pendant l'attaque SYN Flood

Et voici le wireshark côté serveur, on remarque que l'on a bien la réception des requêtes SYN et les réponses à ces requêtes SYN ACK, cependant on ne reçoit pas l'ACK qui indique l'accusé de réception de l'attaquant.

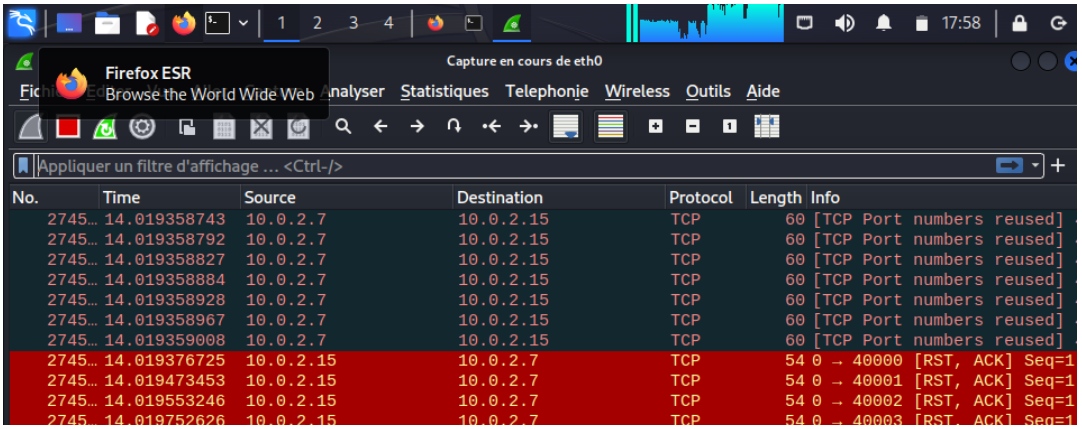


Figure 15: Échanges lors de l'attaque SYN Flood

Et après cela nous avons sur la machine client l'incapacité d'accéder au serveur apache:

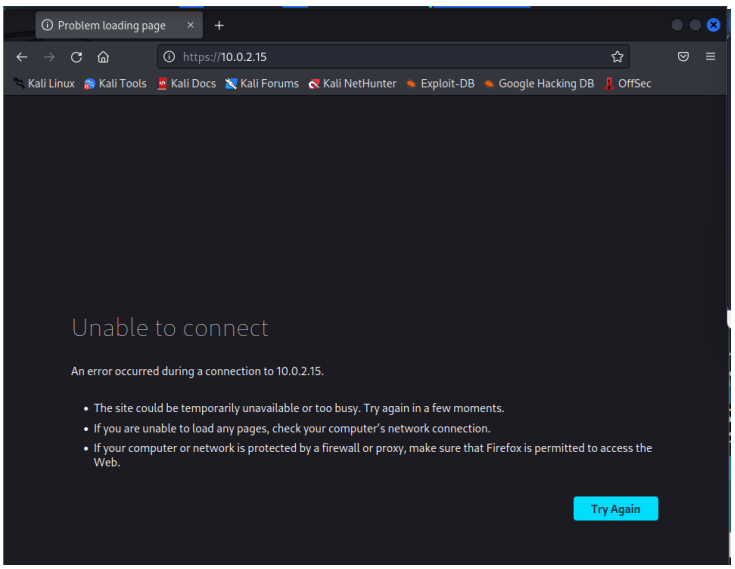


Figure 16: Page inaccessible après l'attaque SYN Flood

Comment se protéger contre cette attaque ?

- Augmenter la file d'attente du backlog: Permettra donc de traiter plus de requêtes SYN.
- Recycler la connexion TCP semi-ouverte: On écrase la connexion la plus ancienne.
- Utiliser des cookies SYN: Après avoir répondu à la demande SYN par un paquet SYN-ACK il peut supprimer la demande SYN du backlog puisqu'il a créé un cookie pour ne pas perdre la connexion.

Conclusion:

Les attaques DDoS visent toutes à perturber un service en ligne en le surchargeant par un nombre conséquent de demandes.

- L'attaque Slowloris va cibler la couche applicative du serveur
- L'attaque par amplification et rebond NTP exploite les faiblesses du protocole pour amplifier le volume du trafic vers sa cible.
- L'attaque SYN Flood va cibler la couche de transport TCP/IP

Ces attaques ont toutes des moyens d'être contrés cependant des serveurs mal configurés peuvent toujours être sensibles à ces attaques.