Université de Caen Normandie
UFR des Sciences
Département Informatique

Master 1 : Informatique

Rapport de projet
Simulation des attaques DDOS

Stanislas Fouche (22007315)
Mahamat Ahmat Ahmat (21912949)
Aref Elaggoun (21910171)
Ahmed Zakaria Memar (22211764)
Tuteur : M. Lyes Khoukhi

2023 - 2024

Table des matières

1 Introduction

Dans un monde où la technologie occupe une place majeure, son rôle dans les entreprises,les gouvernements et même dans nos vies quotidiennes est indéniable. Avec cette omniprésence technologique émerge également un besoin crucial de sécurité informatique.

Au fil des années, de nombreuses attaques visant à voler des données sensibles, à pirater des systèmes et à menacer la stabilité de certaines infrastructures ont pu voir le jour. Ces attaques continueront d'évoluer, de s'adapter et de poser des défis croissants à la sécurité.

Dans cette optique, cette étude se concentre sur un aspect spécifique de la sécurité informatique : la lutte contre les attaques par déni de service distribué (DDoS). En explorant les différentes formes de ces attaques et en examinant les solutions disponibles pour les contrer, nous cherchons à mieux comprendre les défis posés par ces menaces et à proposer des recommandations pour renforcer la résilience des infrastructures numériques face à de telles attaques.

Pour ce faire, nous simulerons ces attaques sur des conteneurs Docker, permettant ainsi une analyse approfondie de leurs mécanismes et de leurs effets.

2 DDoS

2.1 Principe

Avant d'attaquer DDoS, comprenons tout d'abord le DoS ou attaque par déni de service. Une attaque par déni de service (DoS) consiste à rendre un appareil numérique indisponible en saturant ses capacités de traitement avec des requêtes excessives, provoquant ainsi un déni de service pour les utilisateurs légitimes. Elle est généralement lancée depuis un seul ordinateur. En revanche, une attaque par déni de service distribué (DDoS) implique plusieurs sources, souvent coordonnées via un réseau de machines infectées, ou botnet, augmentant significativement son ampleur et son impact.

DDoS : Distributed Denial of Service

L'attaque DDoS est l'une des attaques les plus connues dans le monde de la sécurité informatique. Comme son nom l'indique, elle permet de viser un service en ligne afin de le rendre indisponible ou d'au moins ralentir grandement son fonctionnement en saturant ses ressources telles que la capacité de traitement ou la bande passante.

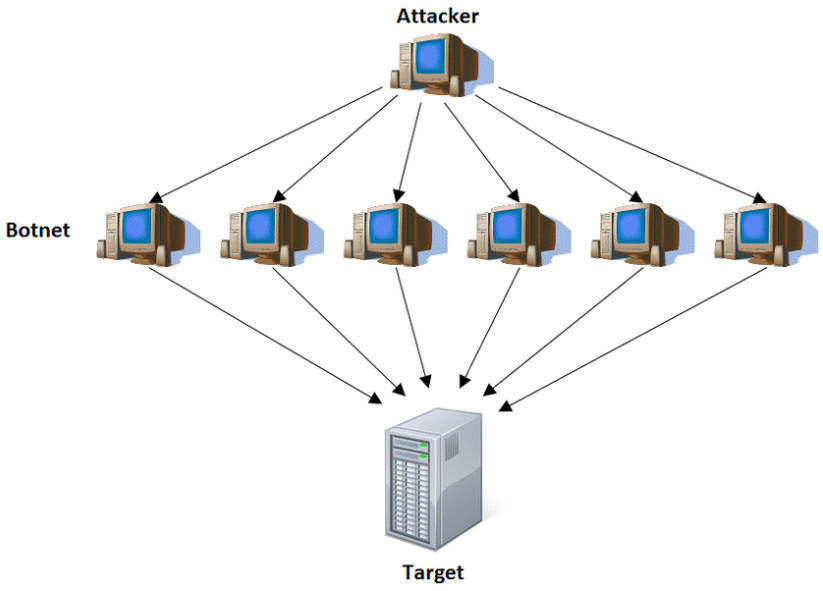

FIGURE 2.1 – Botnet [3]

2.2 Types d'attaques choisi

Il existe plusieurs types d'attaques DDoS, on va s'intéresser ici surtout à des attaques Protocoles et Volumétrique.

On pourra tenter de combiner plusieurs types d'attaques DDoS pour maximiser leur impact (Attaque Hybrid)

2.2.1 ACK Flood Attack

Les attaques de type ACK flood ciblent la couche transport, ou couche 4, dans le cadre de cyberattaques DDoS. Cette technique consiste à submerger un système avec un flux excessif de paquets TCP (Transmission Control Protocol), spécifiquement des accusés de réception (ACK), qui jouent un rôle clé dans le mécanisme de connexion TCP, illustré par un échange de signaux entre deux appareils. En saturant le serveur avec ces paquets, sa bande passante est gravement perturbée. L'objectif principal de cette attaque est de consommer les ressources du serveur en le forçant à gérer un grand nombre de connexions simultanées et à utiliser intensivement sa bande passante, ce qui peut finalement interrompre le service pour les utilisateurs légitimes.

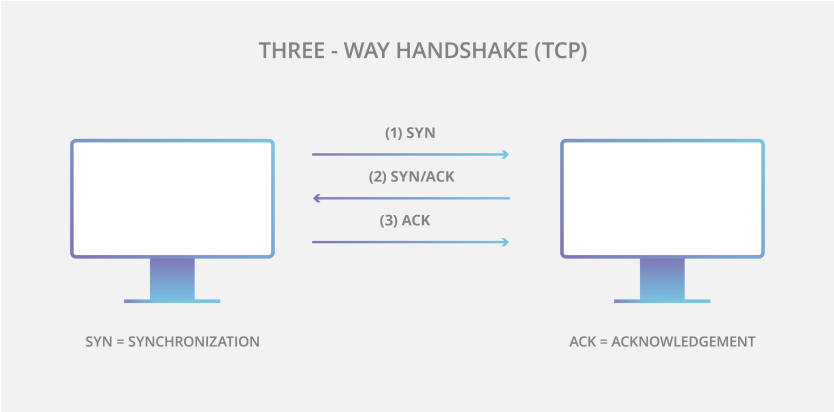

FIGURE 2.2 – TCP attack [6]

2.2.2 SYN Flood Attack

Les attaques SYN flood exploitent la phase d'initialisation de la connexion TCP, où chaque connexion débute par un échange appelé "handshake". Lors d'une attaque SYN flood, l'attaquant envoie rapidement une multitude de demandes de connexion SYN vers la cible sans finaliser le processus de "handshake". Cela remplit la file d'attente des connexions semi-ouvertes du serveur, le bloquant ainsi et empêchant les nouvelles connexions légitimes. L'objectif est de consommer les ressources disponibles pour le traitement des connexions, causant une dégradation ou un arrêt complet des services de la cible

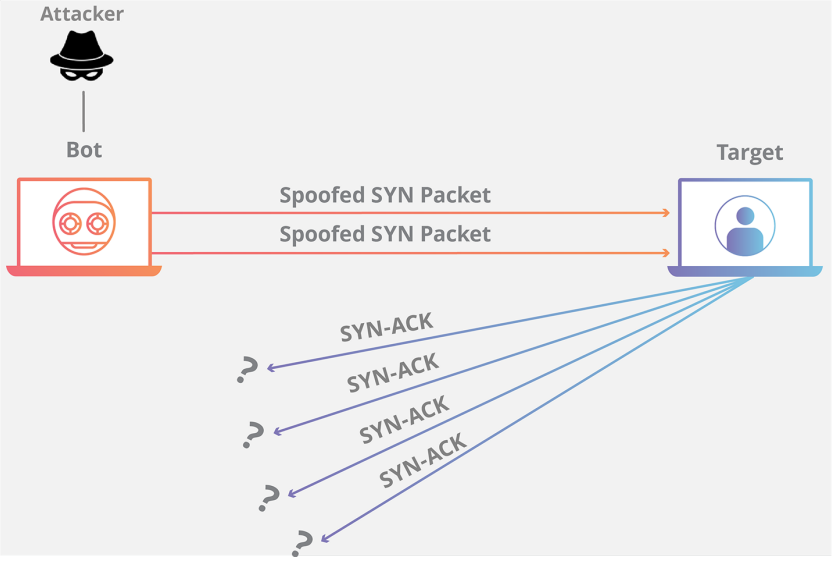

FIGURE 2.3 – SYN Flood Attack [7]

2.2.3 HTTP Flood Attack

L'attaque DDoS Slowloris est une stratégie de cyber-attaque ciblant la couche 7 (couche application) du modèle OSI. Cette méthode vise à saturer un serveur, une base de données ou une API en établissant de multiples connexions TCP simultanées tout en envoyant un volume réduit mais constant de requêtes HTTP. Slowloris est conçu pour maintenir ces connexions actives le plus longtemps possible, en soumettant des requêtes HTTP qui, bien que paraissant légitimes, sont anormalement lentes. En dispersant ces requêtes sur diverses adresses IP et en exploitant les connexions TCP multithreads, Slowloris épuise les ressources du serveur ciblé, résultant en un déni de service. Les attaques de type HTTP Flood, notamment les attaques HTTP GET et POST, sont particulièrement redoutables car elles peuvent envoyer un grand nombre de demandes simultanées qui, en plus de saturer les capacités du serveur, compliquent la distinction entre trafic légitime et malveillant, rendant leur mitigation difficile

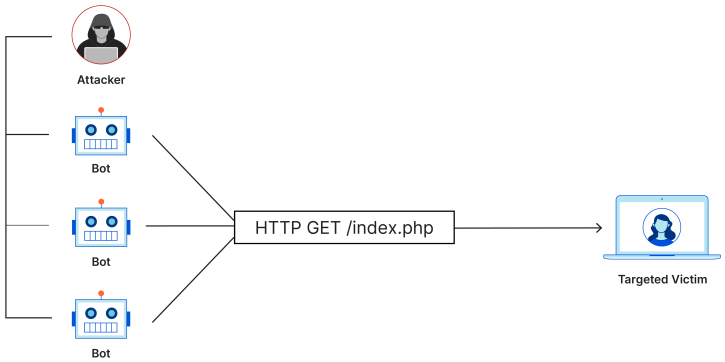

FIGURE 2.4 – HTTP Flood Attack [8]

3 Implémentation

3.1 Docker Container

Pour l'implémentation des attaques, nous avons adopté Docker Container, un outil de conteneurisation qui nous permet de simuler des environnements contrôlés et sécurisés. Grâce à cette technologie, nous pouvons créer des environnements isolés et reproduire les tests de manière cohérente, garantissant ainsi la fiabilité et la sécurité de nos expérimentations. Cette méthode nous permet de créer des environnements isolés et répétables pour nos tests, assurant ainsi la reproductibilité et la sécurité de nos expérimentations.Nous avons configuré trois types de conteneurs Docker distincts pour mener à bien notre simulation :

- **Conteneurs Cibles** : Un conteneur pour le serveur web Apache et un autre pour le serveur Nginx. Ces serveurs sont configurés pour répondre aux requêtes HTTP et sont les cibles de nos attaques simulées.
- **Conteneur Attaquant** : Ce conteneur contient les scripts d'attaque, notamment hping3 pour les attaques de type ACK et SYN flood, et slowloris pour simuler une attaque par saturation de connexions HTTP. Ce conteneur joue le rôle de l'attaquant dans nos simulations.
- **API** utilisé pour les serveurs [5]

4 Les Solutions

La mitigation efficace des attaques DDoS repose sur l'implémentation de stratégies de contrôle de trafic au niveau du réseau. Ces mécanismes sont essentiels pour prévenir et réduire l'impact des attaques en saturant les ressources réseau.

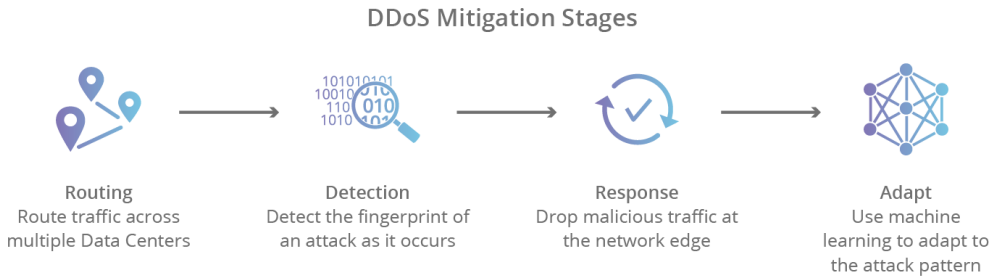

FIGURE 4.1 – Mitigation stages [9]

L'atténuation d'une attaque DDoS à l'aide d'un fournisseur basé sur le cloud se décompose en 4 étapes :

1. **Détection** : pour arrêter une attaque distribuée, un site web doit être capable de distinguer une attaque d'un volume élevé de trafic normal. Si un site Web est submergé de nouveaux visiteurs légitimes en raison du lancement d'un produit ou d'une annonce, il est indispensable qu'il évite de les ralentir ou les empêche de visualiser le contenu du site web. La réputation IP, les modèles d'attaques fréquents et les données antérieures permettent d'effectuer une bonne détection.
2. **Réponse** : durant cette étape, le réseau de protection DDoS répond à une menace entrante identifiée en éliminant intelligemment le trafic de bots malveillants et en absorbant le reste du trafic. En utilisant les règles de page WAF pour les attaques de la couche application (L7), ou un autre processus de filtrage pour traiter les attaques de niveau inférieur (L3/L4) telles que le memcached ou l'amplification NTP, un réseau est capable d'atténuer la tentative de perturbation.
3. **Routage** : En routant intelligemment le trafic, une solution d'atténuation DDoS efficace divisera le trafic restant en fragments maîtrisables pour empêcher le déni de service.
4. **Adaptation** : Un bon réseau analyse le trafic à la recherche de modèles tels que la répétition de blocs IP incriminés, d'attaques particulières en provenance de certains pays ou de protocoles particuliers mal utilisés. En s'adaptant aux modèles d'attaque, un service de protection peut se renforcer contre les attaques futures.

5 Conclusion

— **Menace sur la stabilité d'Interne**t : Les attaques par déni de service distribué (DDoS) constituent une menace majeure pour la sécurité et la stabilité d'Internet. Il est impératif que les organisations se préparent à se défendre efficacement contre ces attaques pour protéger leurs infrastructures.

— **Impact organisationne**l : Les attaques DDoS peuvent infliger de sérieux dommages aux organisations, se traduisant par des pertes financières importantes, une détérioration de la réputation, et diverses conséquences juridiques.

— **Défense multicouche** : Pour contrer ces menaces, les organisations doivent déployer une stratégie de défense multicouche. Cette approche inclut la surveillance du réseau, la mise en place de contrôles d'accès, l'utilisation de pare-feu et de systèmes de détection d'intrusions, ainsi que l'exploitation de réseaux de diffusion de contenu, de services de protection DDoS spécialisés, et une planification soignée des réponses aux incidents.

— **Implications légales** : Il est crucial de rappeler que les attaques DDoS sont des actes illégaux pouvant entraîner des poursuites criminelles, des responsabilités civiles, et des sanctions sévères telles que des amendes ou des peines d'emprisonnement pour les auteurs.

Bibliographie

[1] DDoS - DDos documentation

[2] Botnet - DDos Botnet documentation

[3] Botnet - DDos Botnet publication

[4] Comment se protéger - bouyguestelecom - Protection DDoS

[5] Page web images - CatAPI

[6] ACK - ACK Attack documentation

[7] SYN - SYN Attack documentation

[8] HTTP FLOOD - HTTP Flood Attack

[9] Solution - Solution Mitigation