Etude et simulation d'attaque DDoS sur machines virtuelles

21802468 Brian Longuet, 22005759 Mathis Roptin, 22000558 Matéo Delerue-Houard

15 avril 2024

Table des matières

1 Introduction

1.1 Qu'est-ce qu'une attaque DDoS ?

De nos jours, la sécurité est devenue une préoccupation majeure au sein des organisations. Parmi toutes les menaces auxquelles elles sont confrontées, les attaques DDoS (Distributed Denial of Service) se distinguent par leur capacité à paralyser les services en ligne en les submergeant de trafic malveillant. Les conséquences de telles attaques peuvent être dévastatrices, allant de pertes financières à la réputation de l'organisme.

1.2 L'objectif de notre projet

Comprendre les mécanismes mis en place pour faire tomber un réseau, en simulant une attaque DDoS sur une machine virtuelle.

Il est important de noter que l'utilisation de tels procédés est contraire à l'éthique et peut entraîner des poursuites judiciaires.

2 Fondements théoriques

2.1 Les différents types d'attaques DDoS

Attaques par saturation de bande passante :

- **UDP Flood** : Envoyer un grand nombre de paquets UDP (User Datagram Protocol) à la cible pour saturer sa bande passante.
- **ICMP Flood** : Inonder la cible avec un grand nombre de paquets ICMP (Internet Control Message Protocol), souvent en utilisant des requêtes ping, pour la submerger.
- **SYN Flood** : Envoyer un grand nombre de requêtes SYN (Synchronize) à la cible dans le but de saturer ses connexions TCP (Transmission Control Protocol), empêchant ainsi les nouvelles connexions légitimes.
- **HTTP Flood** : Envoyer un grand nombre de requêtes HTTP (Hypertext Transfer Protocol) à la cible, souvent en utilisant des bots web, pour surcharger ses serveurs web.

Attaques par épuisement des ressources :

- **Slowloris** : Ouvrir un grand nombre de connexions HTTP incomplètes et les maintiennent ouvertes, épuisant ainsi les ressources du serveur.
- **RUDY** (R-U-Dead-Yet) : Similaire à Slowloris, RUDY utilise des requêtes HTTP POST lentes et complètes pour épuiser les ressources du serveur.
- **Attaques d'épuisement de la couche applicative** : Cibler les ressources applicatives spécifiques, telles que les sessions, les caches ou les bases de données, pour épuiser les ressources de la cible.

Attaques de réflexion ou amplification :

— **UDP Reflection ou Amplification** : Envoyer des requêtes UDP avec l'adresse IP de la cible falsifiée à des serveurs mal configurés qui renvoient des réponses plus volumineuses à la cible, amplifiant ainsi l'attaque.

— **DNS Amplification** : Envoyer de petites requêtes DNS (Domain Name System) à des serveurs DNS ouverts avec l'adresse IP de la cible falsifiée, qui renvoient des réponses plus volumineuses, amplifiant ainsi l'attaque.

2.2 Comment fonctionne une attaque DDoS ?

Étape 1 : Les cybercriminels recrute le plus grand nombre de PC zombies (botnets) pour effectuer leurs attaques groupées. Ces PC ont été infectés par des logiciels malveillants et sont contrôlés à distance. Souvent, ce sont des utilisateurs de vieux systèmes d'exploitation non mis à jour, ou éventuellement l'utilisation de logiciels non certifiés qui sont les plus touchés.

Étape 2 : Les attaquants coordonnent les botnets pour envoyer simultanément du trafic vers la cible.

Étape 3 : Les attaquants déclenchent l'attaque en envoyant des requêtes malveillantes à leur cible.

Étape 4 : Vérifiez si l'infrastructure ciblée est indisponible pour déterminer si l'attaque a fonctionné. L'objectif de cette attaque est de saturer la capacité de traitement du serveur, ainsi que la bande passante, etc ... pendant quelques minutes voire plus.

En résumé, une attaque DDoS exploite la force combinée de multiples dispositifs infectés pour submerger les ressources d'une cible, rendant ainsi ses services inaccessibles aux utilisateurs légitimes. La complexité et la diversité des attaques DDoS exigent des mesures de sécurité robustes pour protéger les infrastructures contre cette menace persistante. Les attaquants doivent également utiliser de nombreux subterfuges pour éviter la détection et l'arrêt de l'attaque, comme la modification des adresses IP sources, etc ...

2.3 Les outils utilisés pour effectuer ces attaques

1. **Hping3 :** est un outil de test de réseau polyvalent et flexible, conçu pour générer et manipuler des paquets réseau. Il est couramment utilisé pour lancer des attaques de type ICMP ou SYN Flood, etc... Il permet également de tester les règles d'un pare-feu, de scanner les ports de manière avancée, et bien d'autres fonctionnalités. En outre, il constitue un outil didactique précieux pour l'apprentissage de TCP/IP, et on pourrait le comparer à un couteau suisse du domaine des réseaux.

2. **Slowloris :** Bien que Slowloris soit plus une technique qu'un outil spécifique, il existe des implémentations logicielles de Slowloris disponibles, notamment en Perl et en Python. Ces implémentations peuvent être utilisées pour mener des attaques Slowloris contre des serveurs web.

3. **Slowhttptest :** est un outil de test qui permet de simuler des attaques Slowloris et d'évaluer la résilience des serveurs web face à ce type d'attaque.

4. **LOIC (Low Orbit Ion Cannon), XerXes, etc ...**

2.4 Quelles sont les motivations derrière ces attaques ?

En général, les cybercriminels le font pour des raisons pécuniaires, dans le but d'extorquer de l'argent aux victimes (comme avec le cheval de Troie ZeuS (ransomware) en 2007). Dans le cas des attaques DDoS, les motivations sont plus ciblées ; elles proviennent de la concurrence, de hackers cherchant à se faire une notoriété, à camoufler d'autres attaques ou simplement par plaisanterie.

3 Comment contrer ce type d'attaque ?

3.1 Firewalls

L'utiliser telle quelle, sans modification, n'est malheureusement pas suffisant. Cependant, nous pouvons l'améliorer pour que rien ne puisse passer.

— Effectuer un filtrage basé sur l'adresse IP ;

— Limiter le traffic utilisant des protocoles spécifiques (ICMP, UDP, HTTP) ;

— Limiter les connexions simultanées ;

— Mise en place de whitelists ;

— Limiter le débit ou le nombre de requêtes par source ;

— Déploiement de CDN (Content Delivery Network), ce sont des réseaux de serveurs dispersés géographiquement qui optimisent la distribution du contenu web. En répartissant les requêtes HTTP sur plusieurs serveurs, ils atténuent les attaques DDoS en absorbant une partie du trafic malveillant. Certains CDN proposent également des outils de filtrage pour bloquer les requêtes malveillantes, renforçant ainsi la résilience de l'infrastructure contre ces attaques.

3.2 Système de détection d'intrusion (IDS)

Ce logiciel est conçu pour détecter les activités suspectes ou malveillantes sur les réseaux informatiques. Ses fonctions sont :

— La surveillance en permanence du traffic réseau ;

— L'analyse des événements, recherche de schémas ou de comportement anormaux ;

— Utilisation de bases de données de signatures connues pour détecter des activités malveillantes ;

— Détection d'instructions basée sur des règles (tentatives de connexion SSH) ;

— Prendre des mesures automatiquement ou fournir aux administrateurs les données nécessaires pour qu'ils puissent arrêter l'attaque.

4 Simulation d'attaque DDoS

4.1 Mise en place

Pour mener à bien ce test, vous aurez besoin d'une machine virtuelle destinée à être la cible, ainsi que d'une autre machine qui effectuera l'attaque.

4.2 Lancement de la démo

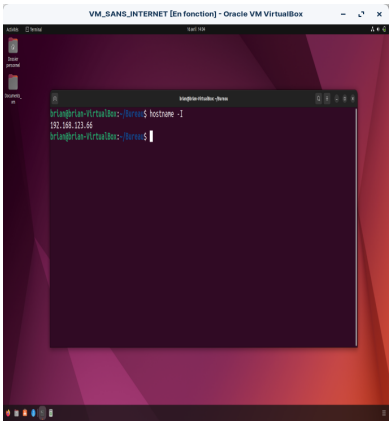

Figure 1 – Avant de commencer, nous devons connaître l'adresse IP de la machine cible. Pour cela, nous utiliserons la commande "**hostname -I**", qui nous donne "**192.168.123.66**".

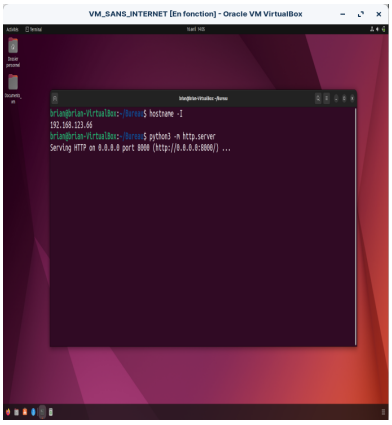

Figure 2 – Ensuite, nous lancerons le serveur Python avec la commande "**python3 -m http.server**".

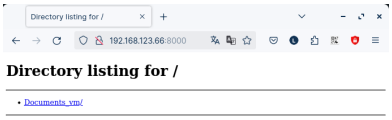

Figure 3 – Pour accéder au serveur de la machine virtuelle via son navigateur sur la machine hôte, nous utilisons cette adresse : "**192.168.123.66 :8000**".

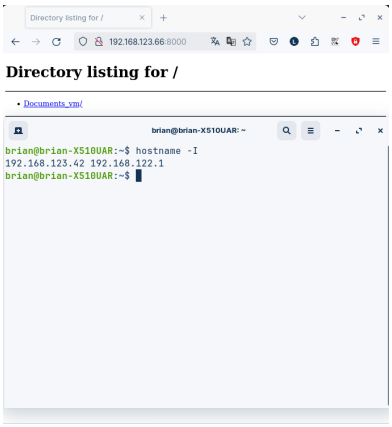

Figure 4 – On vérifie que le serveur fonctionne correctement et on en profite pour afficher l'adresse IP de la machine hôte, afin de démontrer que nous ne sommes pas dans l'environnement de la machine virtuelle.

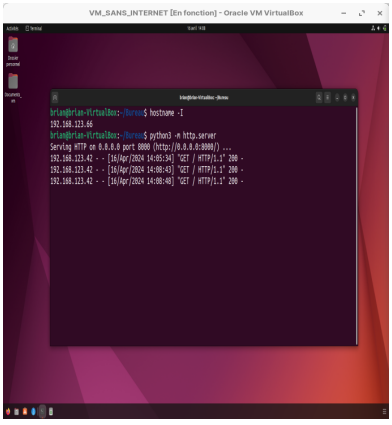

Figure 5 – Cette image illustre les appels GET que nous effectuons pour nous connecter au serveur.

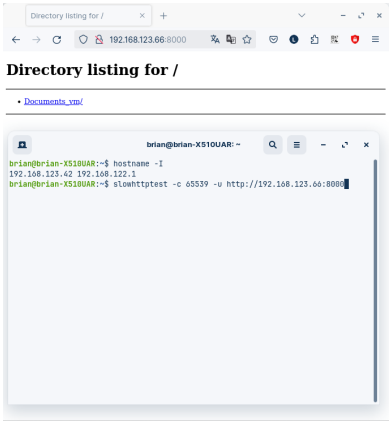

Figure 6 – Enfin, pour lancer l'attaque DDoS, nous utilisons la commande "**slowhttptest -c 65539 -u http ://192.168.123.66 :8000**".

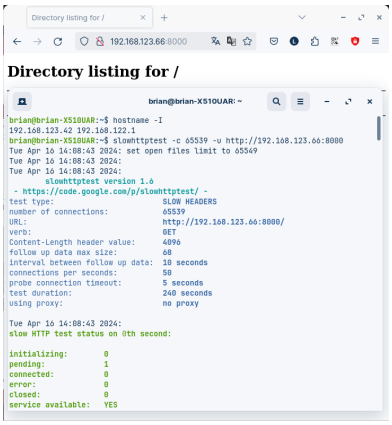

Figure 7 – Les données au debut du test.

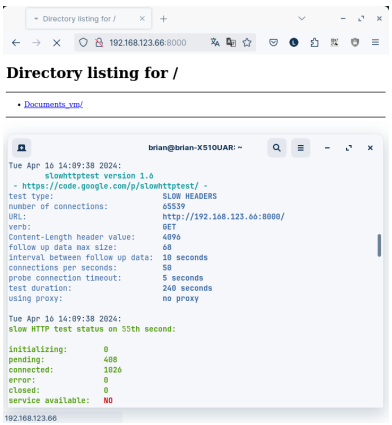

Figure 8 – Les données à la fin du test, on peut également remarquer que les serveur est down.

5 Analyse

5.1 Résultats de la démo

Préambule : Pour commencer, nous avons paramétré le test de la manière suivante : le type d'attaque utilisé est le "SLOW HEADERS", qui vise à saturer le serveur en envoyant lentement des en-têtes HTTP. Nous avons opté pour la méthode GET. Avec un nombre de connexions établies de 65 539 et un total de 50 connexions par seconde, le test a duré environ 240 secondes.

Évolution du test :

— Le test commence par un état où seules quelques connexions sont en attente ou en cours d'établissement (pending).

— Au fur et à mesure que le temps avance, le nombre de connexions établies (connected) augmente progressivement.

— À un certain point, le serveur semble être saturé, comme indiqué par l'augmentation du nombre de connexions en attente et aucune nouvelle connexion n'est établie (service available : NO).

Analyse :

— Le test indique que le serveur a réussi à gérer un certain nombre de connexions simultanées jusqu'à un certain point, mais il atteint ensuite sa limite de capacité.

— L'augmentation du nombre de connexions en attente indique que le serveur n'est plus en mesure de répondre aux nouvelles demandes, ce qui peut être interprété comme une saturation des ressources serveur.

— Ces signes suggèrent que le serveur est vulnérable à une attaque DDoS, où un grand nombre de requêtes simultanées peuvent entraîner une interruption de service pour les utilisateurs légitimes.

Conclusion :
Ce test met en évidence la nécessité pour le propriétaire du serveur de renforcer sa capacité à résister aux attaques DDoS en mettant en place des mesures de sécurité appropriées telles que des pare-feu, des services de mitigation des attaques DDoS et une optimisation des performances du serveur.

6 Conclusion

Les attaques DDoS demeurent une menace sérieuse pour les infrastructures modernes, comme l'ont révélé notre étude et simulation. En explorant les mécanismes des attaques DDoS et en examinant les outils utilisés pour les exécuter, nous avons mieux compris les risques auxquels sont confrontées les organisations.

Les simulations ont mis en lumière la vulnérabilité des machines virtuelles face à ces attaques, soulignant ainsi l'importance cruciale de mesures de protection adaptées. En étudiant des solutions telles que les pare-feu, les systèmes de détection d'intrusion et les CDN, nous avons identifié des stratégies efficaces pour renforcer la résilience des infrastructures.

Il est essentiel pour les organisations de maintenir leur vigilance et de mettre en place des pratiques de sécurité solides pour se protéger contre les attaques DDoS. Cela nécessite non seulement l'utilisation de technologies avancées, mais également la sensibilisation et la formation du personnel.

En résumé, notre rapport souligne l'importance cruciale de la sécurité informatique dans un monde connecté, où les attaques DDoS représentent une menace constante. En adoptant une approche proactive et en investissant dans des solutions de sécurité robustes, les organisations peuvent mieux se protéger et assurer la disponibilité de leurs services en ligne pour leurs utilisateurs.

7 Sources

— https ://www.hostinger.fr/tutoriels/cdn
— https ://datadome.co/fr/learning-center/comment-mettre-fin-a-une-attaque-ddos-4-mesures-a-prendre-des-maintenant/
— https ://github.com/shekyan/slowhttptest ?tab=readme-ov-file
— https ://github.com/gkbrk/slowloris
— https ://github.com/Samsar4/Ethical-Hacking-Labs/blob/master/2-Scanning-Networks/1-hping3.md
— etc ...