UNIVERSITÉ
CAEN
NORMANDIE

SMINF2F7 : Sécurité avancée

Etudes et simulations d'attaques DDoS sur machines virtuelles

Membres du projet :

Nathan FRANCLET, Alex SUMAQIE, Gaëtan COULOMBIER

Encadré par : Lyes KHOUKHI

Avril 2024

Table des matières

1 Contexte **2**
1.1 L'attaque DDoS 2
1.2 Statistiques des attaques 2
1.3 Les objectifs 3

2 Simulation d'attaques DDoS **5**
2.1 BGP Flowspec et sFlow 5
2.2 Topologie du réseau et fonctionnement 6
2.3 Attaques et réponses 6

3 Conclusion **8**

Contexte

1.1 L'attaque DDoS

Une attaque par déni de service vise à rendre indisponible un ou plusieurs services. Un déni de service peut consister à exploiter, par exemple, une vulnérabilité logicielle ou matérielle. L'interruption de service peut également s'effectuer en empêchant l'accès à ce service, par exemple en saturant la bande passante du réseau : on parle alors d'attaques volumétriques. Par ailleurs, une attaque peut solliciter, jusqu'à épuisement, une ou plusieurs ressources d'un service. Il peut s'agir, par exemple, de l'ouverture d'un grand nombre de nouvelles sessions TCP dans un intervalle de temps très court, ou encore d'un nombre trop important de traitements concurrents effectués par une base de données. On parle de « déni de service distribué » (de l'anglais Distributed Denial of Service ou DDoS) lorsque l'attaque fait intervenir un réseau de machines (souvent compromises) afin d'interrompre le ou les services visés.[1]

Les attaques DDoS peuvent varier en termes de complexité, de durée et de taille, mais l'objectif principal reste toujours le même : saturer les ressources de la cible pour la rendre inaccessible aux utilisateurs légitimes.

1.2 Statistiques des attaques

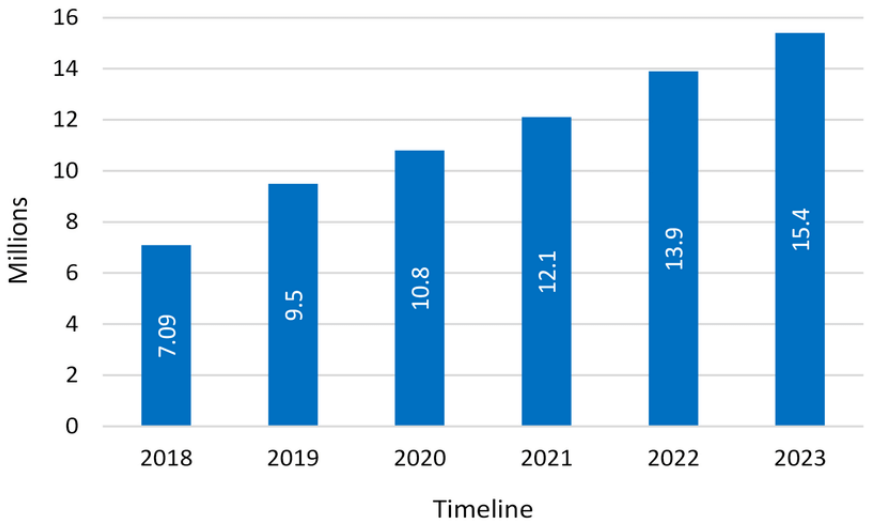

FIGURE 1.1 – Tendances globales des attaques DDoS entre 2018 et 2023 [3]

La tendance à la hausse du nombre d'attaques DDoS illustrée par la Figure 1.1 souligne l'ampleur croissante de cette menace dans le paysage numérique mondial. Cette augmentation constante réaffirme que les attaques DDoS restent un outil efficace et relativement accessible pour les cybercriminels, qu'ils soient motivés par des gains financiers, des conflits idéologiques ou d'autres motifs.[3]

Face à cette réalité, il devient impératif pour les entreprises et les organisations de toutes tailles de mettre en place des mesures de protection robustes pour assurer la disponibilité de leurs services en ligne

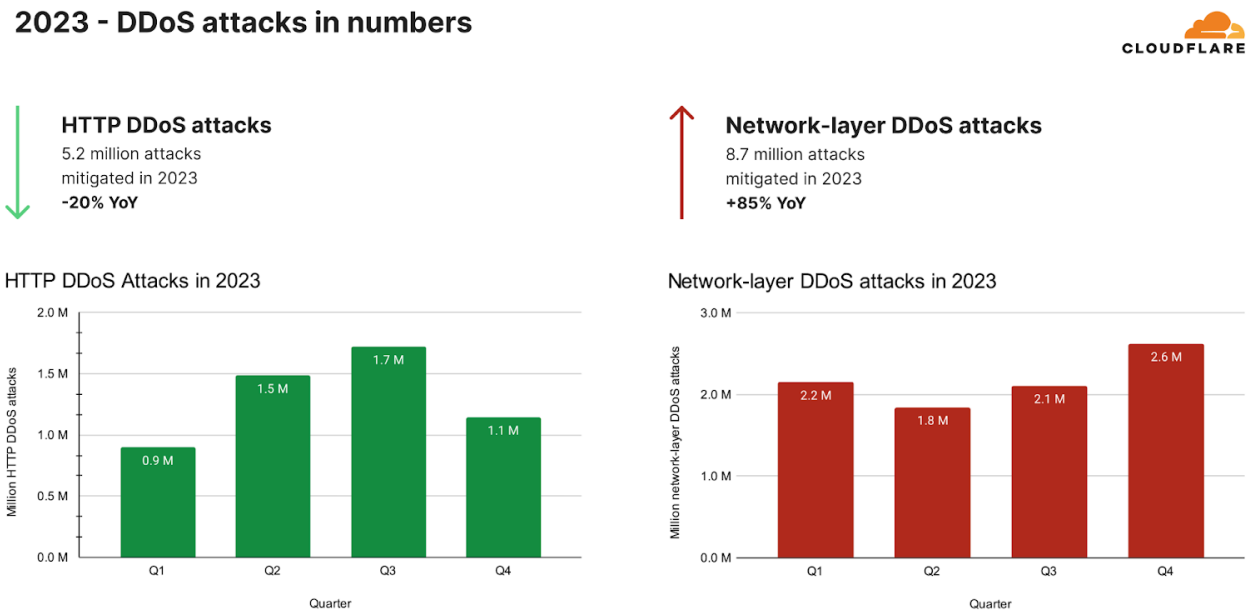

FIGURE 1.2 – Attaques DDoS utilisant HTTP et la couche réseau par trismestre [5]

La Figure 1.2 met en lumière une tendance intéressante : les attaques DDoS évoluent vers l'utilisation de la couche réseau plutôt que de se limiter au protocole HTTP. Cela signifie que les attaquants exploitent des vulnérabilités au niveau de l'infrastructure sous-jacente, ce qui rend ces attaques potentiellement plus sophistiquées et difficiles à contrer. En se concentrant sur la couche réseau, les attaquants peuvent contourner les mesures de sécurité applicatives et cibler directement les ressources sous-jacentes, augmentant ainsi l'impact et la complexité des attaques DDoS.[5] Cette évolution souligne l'importance pour les entreprises et les organisations de renforcer leur sécurité à tous les niveaux du réseau pour se protéger efficacement contre ces attaques en constante évolution.

1.3 Les objectifs

Notre projet, visant à étudier et simuler des attaques DDoS, permet d'aborder les points suivants :

— Compréhension des menaces émergentes : Étudier les attaques DDoS permet de mieux comprendre les tendances et les évolutions dans le domaine de la cybercriminalité. En analysant les méthodes utilisées par les attaquants, les chercheurs et les professionnels de la sécurité peuvent anticiper les nouvelles techniques et renforcer leurs défenses.

— Formation et sensibilisation : La simulation d'attaques DDoS offre une opportunité précieuse de former le personnel à réagir de manière adéquate en cas d'attaque réelle. En simulant des scénarios réalistes, les équipes de sécurité peuvent améliorer leur temps de réponse, leur coordination et leur capacité à atténuer les effets néfastes d'une attaque.

— Validation des politiques de sécurité : Tester les politiques et les procédures de sécurité à travers des simulations d'attaques permet de vérifier leur efficacité et leur applicabilité dans des situations critiques. Cela aide les organisations à identifier les lacunes dans leurs politiques de sécurité et à les ajuster en conséquence pour garantir une protection maximale contre les attaques DDoS.

En somme, l'étude et la simulation des attaques DDoS sont essentielles pour renforcer la résilience des organisations face à cette menace persistante et en constante évolution, en leur permettant d'anticiper, de se préparer et de se défendre efficacement contre de telles attaques.

Simulation d'attaques DDoS

2.1 BGP Flowspec et sFlow

La sécurisation des réseaux est une préoccupation majeure pour les entreprises et les fournisseurs de services. Deux technologies, BGP Flowspec et sFlow, jouent un rôle crucial dans la détection et l'atténuation de ces menaces, offrant des approches complémentaires pour renforcer la sécurité du réseau.

BGP Flowspec, ou Border Gateway Protocol Flowspec, étend les capacités du protocole BGP en permettant la distribution de règles de filtrage précises pour spécifier le trafic à accepter, rejeter ou rediriger. Contrairement à la configuration manuelle des règles de filtrage sur chaque routeur, BGP Flowspec permet aux opérateurs de définir des politiques de filtrage de manière centralisée et de les distribuer dynamiquement à travers le réseau.[9][4][2]

L'utilisation de BGP Flowspec permet une réaction rapide aux menaces en déployant des règles de filtrage spécifiques pour bloquer le trafic malveillant. Par exemple, lorsqu'une attaque DDoS est détectée, des règles Flowspec peuvent être propagées pour filtrer le trafic en fonction de ses caractéristiques, telles que l'adresse source, la destination, ou les protocoles utilisés. Cette approche permet d'atténuer l'impact de l'attaque en bloquant le trafic nuisible au niveau du réseau, avant qu'il n'atteigne les infrastructures critiques.[9][4][2]

sFlow est une technologie de surveillance du trafic réseau qui permet de collecter des échantillons du trafic en temps réel, offrant ainsi une visibilité approfondie sur le comportement du réseau. Contrairement à d'autres méthodes de surveillance qui peuvent être intensives en termes de ressources, sFlow utilise un échantillonnage basé sur une méthode probabiliste pour collecter des données sur le trafic, ce qui réduit la charge sur les dispositifs de surveillance.[8]

En collectant des échantillons du trafic à des intervalles réguliers, sFlow fournit des informations précieuses sur les modèles de trafic, les tendances d'utilisation et les anomalies potentielles. Cette visibilité accrue permet aux administrateurs réseau de détecter rapidement les comportements suspects, tels que des flux de trafic anormaux associés à des attaques DDoS ou à des intrusions.[8]

Dans le cadre de notre projet, nous avons combiné BGP Flowspec pour la réaction rapide aux menaces au niveau du réseau et sFlow pour la surveillance approfondie du trafic afin d'évaluer leur efficacité dans notre simulation.

2.2 Topologie du réseau et fonctionnement

Afin d'être le plus proche d'une situation réelle lors de notre simulation, nous avons utilisé ce projet : `https://github.com/sflow-rt/containerlab/`.

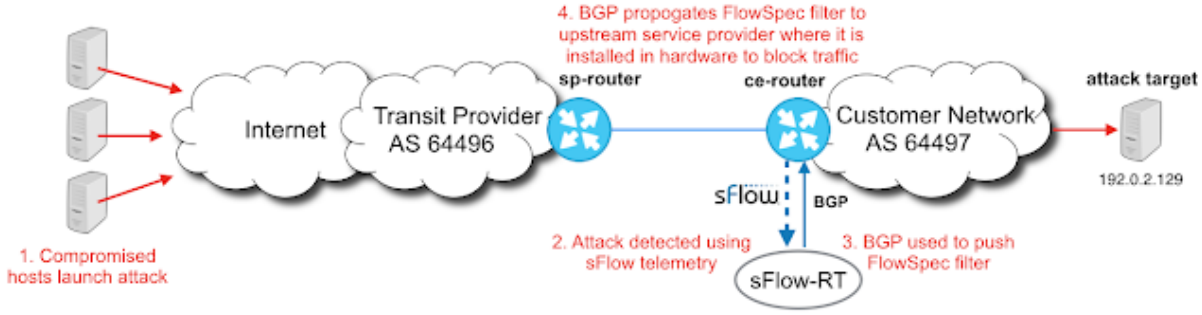

FIGURE 2.1 – Schéma de la topologie réseau du projet [6]

Comme le montre la Figure 2.1, le réseau comporte 3 composantes clés : le routeur du client (ce-router), une machine sFlow-RT et le routeur du fournisseur (sp-router). Le routeur du côté client collecte les données de télémétrie sFlow du réseau, incluant des informations sur les flux de trafic. Ces données sFlow sont ensuite transmises à la machine sFlow-RT pour une analyse en temps réel. Notre simulation va permettre de lancer une attaque DDoS depuis un réseau extérieur (Internet ici) qui a pour cible la machine du côté client (192.0.2.129). Avec cette topologie, on montre que si la machine sFlow-RT identifie des caractéristiques spécifiques d'une attaque, alors une règle BGP Flowspec est générée et envoyée au routeur du client (ce-router) afin de propager la règle à tous les routeurs du réseau pour contrer l'attaque.[6]

2.3 Attaques et réponses

Les types d'attaques implémentés dans notre simulation sont les suivants [7] :

— IP flood : L'inondation IP est un type d'attaque volumétrique qui consiste à envoyer un grand nombre de paquets IP à une adresse et à un protocole ciblés. Cette attaque vise à consommer la bande passante de la cible, ce qui provoque une congestion du réseau et peut entraîner une interruption du service.

— IP fragmentation : Les attaques par fragmentation IP consistent à envoyer un grand nombre de paquets IP fragmentés à une adresse et à un protocole cibles. Ces paquets fragmentés peuvent épuiser les ressources de l'hôte car ils doivent être réassemblés, ce qui entraîne un déni de service.

— UDP flood : Une inondation UDP est un type d'attaque DDoS dans lequel un attaquant envoie un grand nombre de paquets UDP (User Datagram Protocol) à un serveur ciblé, dans le but de le submerger. Le serveur tente de traiter chaque paquet entrant, mais en raison du volume de paquets, il finit par être submergé et ne peut plus fournir le service

prévu.

— ICMP flood : Une inondation ICMP, également connue sous le nom d'inondation Ping, est un type d'attaque DDoS qui envoie un grand nombre de paquets de demande d'écho ICMP (communément appelés "pings") à un serveur ciblé. Le serveur est alors submergé en essayant de répondre à toutes les demandes d'écho, ce qui entraîne un déni de service.

— SYN flood : Une attaque SYN Flood est un type d'attaque DDoS qui exploite le processus d'échange TCP. L'attaquant envoie un grand nombre de paquets TCP/SYN avec des adresses IP source usurpées à un serveur cible. Le serveur répond à chaque demande et attend ensuite la dernière étape de la poignée de main, qui n'arrive jamais. Cela laisse un grand nombre de connexions semi-ouvertes, ce qui consomme des ressources et peut conduire à un déni de service.

Pendant notre simulation, des règles ont été créées et propagées automatiquement aux routeurs lors des attaques citées ci-dessus grâce à des seuils définis en amont dans sFlow-RT (Figure 2.1). On peut retrouver ces règles comme réponses aux attaques [7] :

— Dans le cas d'une attaque par inondation IP, une règle BGP Flowspec peut être créée pour bloquer tout le trafic du protocole IP 47 (GRE) vers l'adresse ciblée. Cette règle atténue efficacement l'attaque en empêchant l'inondation de paquets d'atteindre la cible.

— Pour les attaques par fragmentation IP, une règle BGP Flowspec peut être définie pour bloquer les paquets fragmentés afin qu'ils n'atteignent pas l'adresse et le protocole ciblés. Cette règle atténue rapidement l'attaque en empêchant les paquets fragmentés d'épuiser les ressources de la cible.

— Dans le cas d'une inondation UDP, une règle peut être définie pour bloquer tout le trafic UDP provenant des adresses IP attaquantes. De même, pour les inondations ICMP et SYN, des règles peuvent être définies pour bloquer toutes les demandes d'écho ICMP et tous les paquets TCP/SYN provenant des adresses IP attaquantes, respectivement.

Conclusion

En conclusion, en réponse de l'impact des attaques DDoS sur les infrastructures réseau, des solutions telles que BGP Flowspec et sFlow ont vu le jour pour atténuer ces menaces. L'analyse du contexte a révélé la nature persistante et préoccupante des attaques DDoS, mettant en évidence la nécessité d'adopter des mesures proactives pour renforcer la sécurité du réseau.

En intégrant BGP Flowspec et sFlow, les organisations peuvent améliorer leur capacité à détecter, analyser et atténuer les attaques DDoS. BGP Flowspec permet une réaction rapide en déployant des règles de filtrage dynamiques pour bloquer le trafic malveillant, tandis que sFlow fournit une surveillance approfondie du trafic en temps réel, facilitant la détection précoce des anomalies.

De plus, la simulation d'attaques DDoS a été réalisée pour mettre en évidence l'efficacité de ces solutions dans un environnement contrôlé. Cette simulation a permis de mieux comprendre les mécanismes de défense contre les attaques DDoS et d'évaluer la pertinence des stratégies de réponse.

En définitive, l'application conjointe de BGP Flowspec et de sFlow offre une approche presque complète pour atténuer les attaques DDoS et renforcer la sécurité des réseaux. Cependant, il est important de noter que cette solution n'est pas généraliste et concerne seulement les attaques DDoS. En effet, la sécurité du réseau est un processus continu qui nécessite une vigilance constante et une adaptation aux nouvelles menaces émergentes, autres que les attaques DDoS.

Bibliographie

[1] ANSSI. Comprendre et anticiper les attaques ddos. https://cyber.gouv.fr/sites/default/files/2015/03/NP_Guide_DDoS.pdf, 2015.

[2] C. Loibl, S. Hares, R. Raszuk, D. McPherson, M. Bacher. Rfc 8955 : Dissemination of flow specification rules. https://www.rfc-editor.org/rfc/rfc8955, 2020.

[3] Faisal Hussain,Syed Ghazanfar Abbas, Muhammad Husnain,Ubaid U. Fayyaz, Farrukh Shahzad,Ghalib A. Shah. Iot dos and ddos attack detection using resnet. https://www.researchgate.net/publication/348639527_IoT_DoS_and_DDoS_Attack_Detection_using_ResNet, 2020.

[4] Justin Ryburn. Deploying bgp flowspec. https://www.juniper.net/documentation/en_US/day-one-books/DO_BGP_FLowspec.pdf, 2015.

[5] Omer Yoachimik, Jorge Pacheco. Ddos threat report for 2023 q4. https://blog.cloudflare.com/ddos-threat-report-2023-q4, 2024.

[6] Peter. Real-time ddos mitigation using bgp rtbh and flowspec. https://blog.sflow.com/2020/02/real-time-ddos-mitigation-using-bgp.html, 2020.

[7] Peter. Ddos attacks and bgp flowspec responses. https://blog.sflow.com/2022/03/ddos-attacks-and-bgp-flowspec-responses.html, 2022.

[8] sFlow. About sflow. https://sflow.org/about/, 2024.

[9] Xander Thuijs. Understanding bgp flowspec (bgp-fs). https://community.cisco.com/t5/service-providers-knowledge-base/asr9000-xr-understanding-bgp-flowspec-bgp-fs/ta-p/3139916, 2015.