الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique

Mémoire de Master

Filière Télécommunication

Spécialité Réseaux et Télécommunication

Présenté par

Aoudia Manel

&

Lahouassa Sahar

Mise en place d'une plateforme pour la détection des attaques DOS

Proposé par : Mehdi Merouane

Année Universitaire 2018-2019

Remerciements

Nous tenons tout d'abord à remercier Dieu le tout puissant, miséricordieux qui nous a donné la force et la patience d'accomplir ce modeste travail.

Nous voudrions aussi présenter nos sincères remerciements à notre encadreur Dr. MEHDI Merouane, et nous voudrions également lui témoigner notre gratitude pour son soutien et ses conseils qui nous ont été très précieux afin de mener notre travail à bon port, Merci.

Nos vifs remerciements vont également au prestigieux membre du jury et à tout le staff du département de Génie Electrique de l'université de Blida 1 très spécialement nos professeurs durant tout ce cycle de 5ans.

Enfin, nous remercions chaleureusement nos chers parents pour leur soutien et leur patience, qui ont étaient toujours là dans les moments difficiles pour nous pousser à l'avant.

Merci.

ملخص:

لضمان أمن أنظمة المعلومات، من الضروري إعداد أنظمة أمنية وتدعيمها بنظام كشف التسلل.

لقد اخترنا تصميم منصة تجريبية للطلاب، والهدف منها اعتراض هجمات الحرمان من الخدمة (DOS)، استنادًا إلى هجمات UDP Flood وICMP Flood وTCP Flood وhttp Flood، من أجل تصميم التواقيع التي تساعدنا في تطبيق قواعد اكتشاف جديدة مطبقة في برنامج Snort مفتوح المصدر باستخدام منهج سيناريو يسمح بتحليل حركة البيانات الواردة ومقارنتها بالتواقيع المصممة. تُظهر عمليات محاكاة مختلفة للهجمات بوضوح فعالية هذه الطريقة في اختبارات الكشف.

كلمات المفاتيح: أمن، سلامة، هجمات، شبكة، هجمات الحرمان، التواقيع، كشف، تسلل، البيانات

Résumé :

Pour assurer la sécurité des systèmes d'informations il est nécessaire de mettre en place des systèmes de sécurité et les compléter avec un système de détection d'intrusion.

Nous avons choisi de concevoir une plateforme expérimentale pour les étudiants, le but est d'intercepter les attaques dénis de service (DOS), basé sur les attaques UDP Flood, ICMP Flood, TCP Flood et http Flood, afin de concevoir des signatures qui vont nous aider à mettre en place des nouvelles règles de détection implémentées dans le logiciel open source Snort suivant une approche par scenario qui permet d'analyser le trafic entrant et le comparer avec les signatures conçues. Different simulations d'attaques montrent clairement l'efficacité de cette méthode lors des tests de detections.

Mots clés : Sécurité ; Détection ; Intrusion ; Attaques ; DOS ; Signatures ; NIDS.

Abstract :

To ensure the security of the information systems, it is necessary to set up a security system and complete it with an intrusion detection system. We have chosen to create this experimental platform for students, the goal of this plateform is to intercept the DOS attacks based on UDP Flood, ICMP Flood, Ping of death, TCP Flood and Http Flood to design signatures that will help us implement new detection rules implemented in the open source software Snort following a scenario approach that allows analyzing the incoming traffic and compare it with the designed signatures. Different simulations of attacks clearly show the effectiveness of this method during detection tests.

Keywords : Security ; Detection ; Intrusion ; Attacks ; DOS ; Signatures ; NIDS.

Listes des acronymes et abréviations

ACK	Acknowledgment.
ADODB	Active DATA Objects DATA Base
ARP	Address Resolution Protocol.
BASE	Basic Analysis and Security Engine.
CPU	Central Processing Unit
DDOS	Distributed Denial of Service.
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server.
DOS	Denial of Service.
FTP	File Transfer Protocol.
HTTP	HyperText Transfer Protocol.
HIDS	Host Intrusion Detection System
ICMP	Internet Control Message Protocol.
IDS	Intrusion Detection System.
IP	Internet Protocol.
IPS	Intrusion Prevention System.
ISO	International Organization for Standardization.
LAN	Local Area Network.
LOIC	Low Orbit Ion Cannon
MAC	Media Access Control.
MAN	Metropolitan Area Network.
NIDS	Network Intrusion Detection System.
OS	Operating System.
OSI	Open Systems Interconnection
PC	Personal Computer
PCAP	Packet Capture
PHP	Personal Home Page.
POP	Post Office Protocol.
PSH	Push
RAM	Random Access memory.
RST	Reset
SGBD	Système de Gestion de Base de Données
SMS	Short Message System
SSH	Secure SHell.
SYN	Synchronize.
SMTP	Simple Mail Transfer Protocol.
TCP	Transmission Control Protocol.
TTL	Time To Live.
UDP	User Datagramme Protocol.
VPN	Virtual Private Network
WAN	Wide area network
WI-FI	Wireless Fidelity
XSS	Crosse Site Scripting

Table des matières

Chapitre 2 : Attaques et sécurité informatique.

Chapitre 3 : Simulation des attaques et conception des signatures.

Liste des figures

Liste des tableaux

Actuellement, les réseaux informatiques et internet sont de plus en plus présents dans les entreprises ainsi que chez les particuliers, ceci a favorisé la communication, le progrès du commerce et l'accès à l'information. L'interconnexion des ordinateurs permet aux utilisateurs malveillants d'exploiter l'ouverture des réseaux dans un but malveillant et d'utiliser les ressources à des fins nuisibles et de lancer des attaques de divers types.

La sécurité des systèmes d'information, repose en premier lieu sur la mise en place d'une politique de sécurité en mettant en place un pare-feu et des anti-virus, et pour compléter cette politique de sécurité la mise en œuvre d'un système de détection d'intrusion est nécessaire.

Pendant notre formation en réseaux et télécommunication nous n'avons pas eu l'opportunité de bien simuler et maitriser les systèmes de détection d'intrusion, pour cela nous avons choisi de mettre en place une plateforme expérimentale destinée aux étudiants pour bénéficier d'une étude qui leur sera utile dans leur formation.

Donc le projet consiste à mettre en place un ensemble d'outils d'attaques reposant sur plusieurs faiblesses au sein même des protocoles TCP, UDP, ICMP et http, ces différents outils font références à une attaque très répondue actuellement c'est l'attaque Denis de Services (DOS). A cet effet nous allons faire des simulations d'attaques à base des logiciels ayant pour but de déduire les signatures d'intrusion de chaque attaque à savoir (UDP Flood, ICMP Flood, Ping of death, TCP Flood et http Flood), puis élaborer tout une solution basée autour du système de détection d'intrusion avec lequel des règles de détections d'attaques vont être conçues. Afin de cerner notre problématique et d'apporter des éléments de réponses à un certain nombre de question posées et surtout aider l'étudiant lors de sa formation à bien assimiler cette partie.

Afin de bien mener notre travail, notre plateforme a été fragmenté en quatre étapes qui se caractérisent sous quatre chapitres dans ce mémoire.

Le premier chapitre intitulé « Généralité sur les réseaux informatiques » est consacré à la présentation de certains concepts fondamentaux relatifs aux protocoles réseau (TCP / IP) dans le but d'obtenir des pré-acquis.

Le second chapitre nommé « Attaques et sécurité informatique » définit les différents techniques et types d'attaques, proposant ainsi une description détaillée des attaques DOS et certaines méthodes de protection.

Le troisième chapitre « Conception des signatures d'attaque » est consacré à la réalisation des attaques DOS avec différents outils, et l'analyse du trafic réseau pour concevoir des signatures afin d'écrire des règles de détection dans le prochain chapitre.

Dans le dernier chapitre « Tests et simulation », nous allons mettre en œuvre Snort, et créer des règles de détection que nous testerons vers la fin pour confirmer leur fiabilité à travers des simulations d'attaques.

Enfin, nous terminons le mémoire par une conclusion générale ou nous révélerons si notre objectif à bien était atteint.

1.1 Introduction

Au cours de cette dernière décennie les réseaux informatiques sont devenus beaucoup plus important et indispensables vu qu'ils ont facilité la gestion et l'infrastructure des entreprises et permettent d'échanger les informations de manière simple entre machines. Toutes ces innovations ont permis de faciliter la vie mais ont aussi contribué au développement de nouveaux risques qui sont les attaques informatiques.

L'objectif principale de ce chapitre est les réseaux informatiques pour cela nous allons définir quelques notions de base ainsi que le modèle OSI et le protocole TCP/IP.

1.2 Définition d'un réseau informatique

Un réseau informatique est un ensemble d'équipements reliés entre eux grâce à des moyens matériels et logiciels pour échanger des informations, partager des ressources et faire circuler des données [1].

1.2.1 Les éléments constitutifs d'un réseau informatique

Un réseau est constitué de périphériques reliés entre eux par un support de transmission.

a Les périphériques finaux

Ces périphériques forment l'interface entre les utilisateurs et le réseau. Un périphérique est une source ou destination d'un message transmit sur le réseau, chaque périphérique final présent sur le réseau est identifié à l'aide d'une adresse, il peut être un ordinateur, un smartphone ou une tablette . . . etc.

b Les périphériques intermédiaires

En plus des périphériques finaux, les réseaux dépendent de périphériques intermédiaires pour fournir la connectivité et l'acheminement des données à l'intérieur de réseau.

Ces périphériques connectent les hôtes individuels au réseau et peuvent connecter plusieurs réseaux individuels afin de former un inter-réseau.

Parmi ces périphériques réseaux intermédiaires y a des périphériques d'accès réseau (commutateur), des périphériques inter-réseau (routeur) et des périphériques de sécurité.

Ces périphériques utilisent l'adresse d'hôte de destination ainsi que les informations concernant les interconnexions pour déterminer le chemin de la donnée sur le réseau.

- **Les supports de transmission**

Afin que les informations circulent au sein d'un réseau, il est nécessaire de relier les différentes unités de communications à l'aide d'un support de transmission.

La transmission de donnée peut s'effectuer via un canal physique (interface filaire) par exemple des câbles coaxiaux, métalliques, par fibre optique, ou à travers des communications non filaires, en utilisant les ondes radio, l'infrarouge (WIFI) ou le laser.

c **Logiciel**

Le logiciel est un composant numérique qui gère le traitement des données par la machine, et ordonne son fonctionnement, on distingue deux types de logiciel : les systèmes d'exploitation et les applications. Les deux sont intimement liés dans le sens qu'une application est habituellement créée pour fonctionner avec un système d'exploitation, qui lui est conçu pour tourner sur une machine en particulier [2].

1.3 Type de réseau informatique

En fonction de la localisation, la distance et le débit, les réseaux sont classés en trois types :

1.3.1 Le réseau LAN (Local Area Network)

Le LAN est un ensemble d'ordinateur connecté les uns proches des autres l'interconnexion sera dans un bâtiment ou à un groupe de bâtiment pas trop éloignés (quelque centaine de mètres).

1.3.2 Le réseau MAN (Métropolitain Area Network)

Un réseau MAN interconnecte plusieurs LAN géographiquement proches (au maximum quelques kilomètres) à des débits importants.

1.3.3 Le réseau WAN (Wide Area Network)

Un réseau WAN interconnecte des réseaux locaux et métropolitains à l'échelle de la planète, d'un pays, d'une région ou d'une ville.

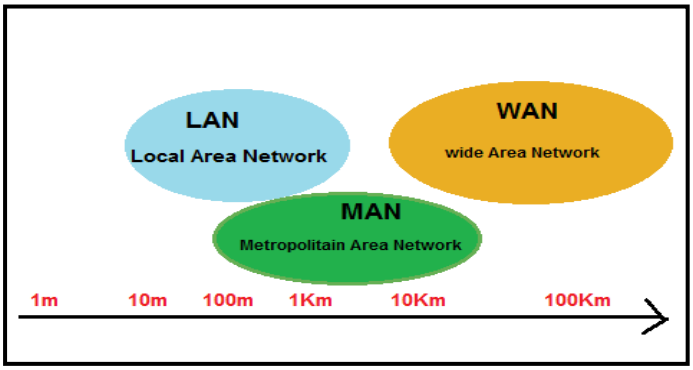


Figure 1-1. Type de réseaux informatiques.

1.4 L'architecture des réseaux informatiques

1.4.1 Réseau Point à point (Peer to Peer)

Un réseau point à point (réseau d'égale à égale) permet l'échange de fichiers, le partage de flux ou d'application sans avoir besoin de tout centraliser sur un serveur, toute machine de ce réseau est à la fois cliente et serveur.

Chaque machine fait partie du réseau point à point est alors considérée comme un nœud qui participe à l'échange d'information. Ce qui permet de décentraliser les services, ce type de réseau est utilisé pour le travail collaboratif, les outils de recherche et l'échange de contenu…etc.

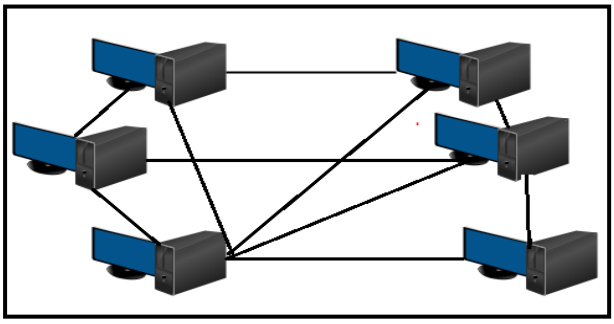


Figure 1-2. Réseau point à point.

1.4.2 Réseau Client/serveur

Un réseau client-serveur est un réseau qui utilise deux types d'ordinateur communiquent via des protocoles, un ordinateur central appelé serveur est un fournisseur de service, généralement très puissant en termes de capacité d'entrée-sortie, et un ordinateur client est un consommateur de services.

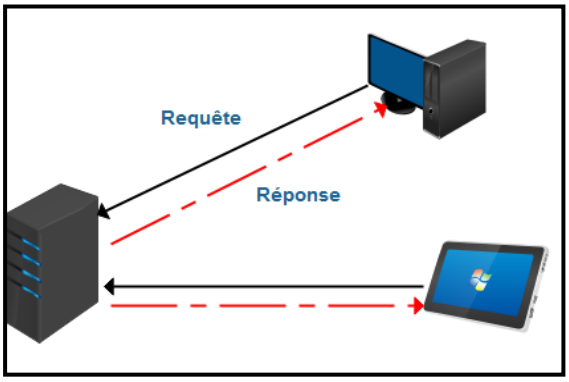


Figure 1-3. Réseau Client/serveur.

1.5 Les topologies utilisées dans un réseau

Pour pouvoir utiliser un réseau, Il faut définir une méthode d'accès entre les ordinateurs, ce qui permet de connaître la manière dont les informations sont échangées. Il existe deux types de topologies :

1.5.1 Topologie physique

La topologie physique décrit la manière dont les périphériques sont reliés, ils peuvent être interconnectés selon les topologies physiques suivantes :

a La topologie en bus

Tous les hôtes sont connectés directement à une liaison.

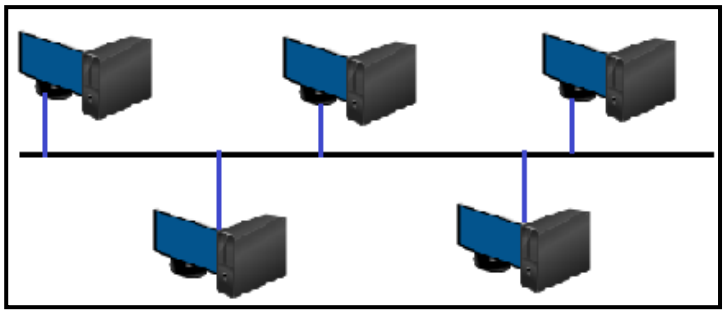


Figure 1-4. Topologie en bus.

b La topologie en anneau

Les périphériques finaux sont connectés à ses voisins en formant un anneau fermé.

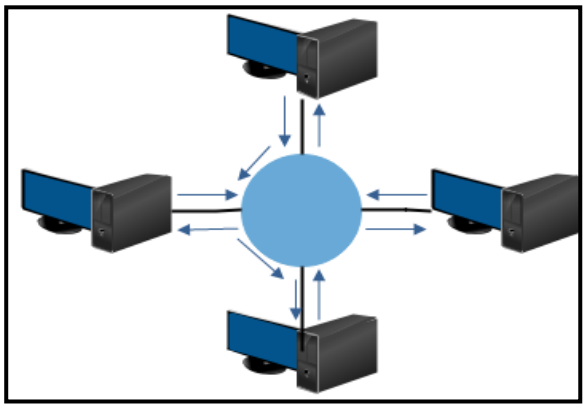


Figure 1-5. Topologie en anneau.

c La topologie en étoile

Les périphériques finaux sont connectés à un nœud central. Par exemple un commutateur.

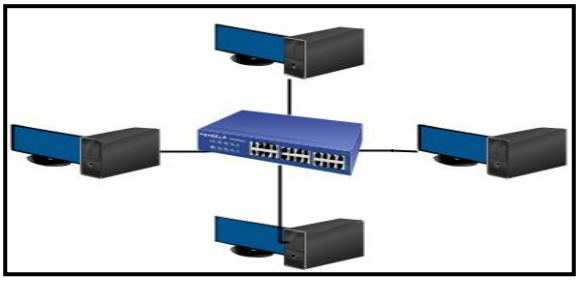


Figure 1-6. *Topologie en étoile.*

1.5.2 Topologie logique

La topologie logique décrit la manière dont les données transitent dans les lignes de communication, les topologies les plus courantes sont Ethernet, Token Ring et FDDI.

1.6 Modèle OSI et TCP/IP

1.6.1 Modèle OSI

Le modèle OSI (Open Systems Interconnection) est une norme établie par l'ISO, afin de permettre aux systèmes ouverts (ordinateur, terminal, réseau, …) d'échanger des informations avec d'autres équipements hétérogènes. Cette norme est constituée de 7 couches, dont 4 premières sont dites couches basses, elles assurent le transfert d'information par les différents services de transport et les 3 couches supérieures font le traitement de l'information par les différents services applicatifs.

1.6.2 Modèle TCP/IP

Le modèle TCP/IP (Transmission Control Protocol/Internet Protocol) appelé aussi modèle Internet par ce qu'il est la source du réseau internet, le modèle TCP/IP est fondé sur quatre couches, chaque couche assure une fonction de maintenance et de service de la communication.

Les services de la couche physique et liaison de donnée du modèle OSI sont intégrés dans une seule couche (accès réseau) du modèle TCP/IP et celles de la couche session et présentation sont réalisés par la couche application.

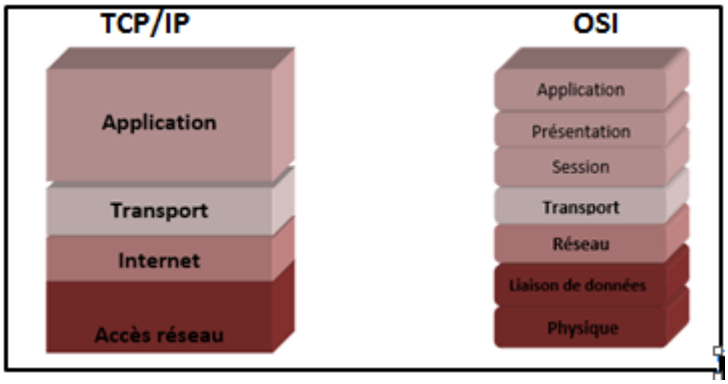


Figure 1-7. Les couche de modèle OSI et TCP/IP.

1.7 Les couches du modèle TCP/IP

1.7.1 Couche Accès réseau

La couche accès réseau du modèle TCP/IP spécifie la forme sous laquelle les données doivent être acheminées sur le réseau.

1.7.2 Couche internet

La couche internet est celle qui s'occupe d'adresser les interfaces, de déterminer le bon chemin à travers les inter-réseau et d'encapsuler les paquets de donnés donc elle remplit une fonction d'adressage logique, du routage et d'encapsulation des données.

a Protocole IPv4

Internet Protocol version 4, est un protocole qui assure la livraison des paquets sans connexion, et s'occupe à identifier les machines sur le réseau par des adresses IP uniques.

b L'adresse ipv4

Une adresse IPv4 est une identification unique pour un hôte sur un réseau IP. Une adresse IP est un nombre d'une valeur de 32 bits représentée par 4 valeurs décimales pointées ; chacune a un poids de 8 bits (1 octet) prenant des valeurs décimales de 0 à 255 séparées par des points [3].

Il y a deux types d'adresse IP :

- **Adresse IP publique** : est une adresse attribuée à un seul appareil par les routeurs des FAI (fournisseur d'accès internet).
- **Adresse IP privée** : est une adresse non routable par internet, généralement utilisée par les entreprises pour attribuer les adresses IPv4 aux hôtes dans leur réseau interne.

Classe	Plage d'adresses privées
A	10.0.0.0 à 10.255.255.255
B	172.16.0.0 à 172.13.255.255
C	192.168.1.0 à 192.168.255.255

Tableau 1-1. Les classes des adresses IP.

c Masque de sous-réseau

Un masque de sous réseau est une suite de 32 bits divisée en 4 octets pointés composée uniquement d'abord d'une suite de 1 et, après d'une suite de 0. Un masque va préciser de manière certaine dans quel réseau se trouve une adresse IP.

Classe	Masque
A	255.0.0.0 ou /8
B	255.255.0.0 ou /16
C	255.255.255.0 ou /24

Tableau 1-2. Masque de sous réseaux.

d En-tête de paquet IPv4

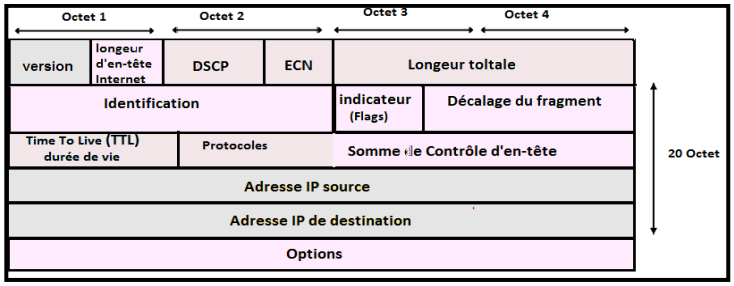


Figure 1-8. En-tête d'IPV4.

Un en-tête IPv4 dispose d'une taille variable de minimum 20 octets et de maximum 60 octets, la taille d'un paquet entier peut aller jusque 65536 octets.

- **Version** : Le champ version indique la version du protocole est égale à 4 pour IPv4.
- **Indicateur (Flags)** : Ce champ permet d'indiquer si un paquet peut être fragmenté ou non.
- **Time To Live TTL (duré de vie)** : Le champ TTL est utilisé pour limiter la durée de vie d'un paquet.
- **Protocol** : Indique le protocole de couche supérieur à utiliser ensuite.
- **Longueur d'en-tête internet** : Représente la somme de contrôle calculée sur l'en-tête du paquet IPv4. Ce champ permet de contrôler l'intégrité de l'entête.
- **Options** : Permet d'ajouter différentes informations optionnelles et rarement utilisées.

1.7.3 Couche transport

La couche transport du modèle TCP/IP effectue le transport des données entre deux applications, les deux principaux protocoles fonctionnant dans cette couche sont le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol).

a Protocole TCP (Transmission Control Protocol)

Le protocole TCP fournit un service de transfert de données fiables, offre des services d'établissement et de fin de dialogue ainsi que des messages de maintenance de la communication en mode fiable et connecté avec des accusés de réception et du séquençage des données.

En-tête TCP :

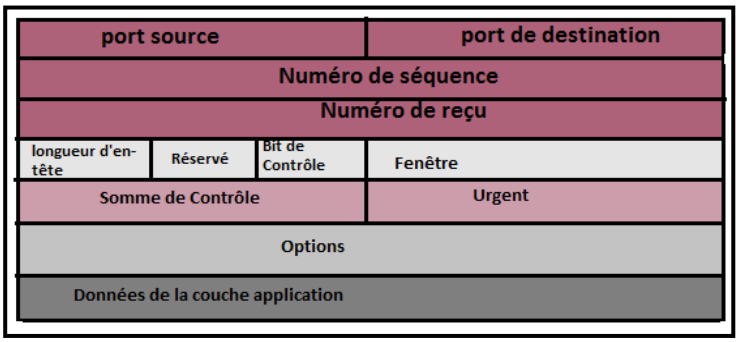


Figure 1-9. En-tête TCP.

- **Port source et port de destination** : c'est le numéro de port logique utilisé par l'application
- **Numéro de séquence** : c'est un nombre qui identifie la position des données à transmettre par rapport au segment original.
- **Numéro de reçu** : c'est un numéro qui identifie les données reçues.
- **Réservé :** Six bits réservés pour le futur usage.
- **Somme de contrôle** : utilisé pour contrôler les erreurs dans l'en-tête et les données du segment.
- **Options** : c'est un paramétrage de TCP, sa présence est détectée dès lors que l'en-tête est supérieur à 5.

Les flags dans l'en-tête TCP :

Les drapeaux TCP(Flags) sont utilisés dans les transferts de paquets TCP pour indiquer un état de connexion particulier ou fournir des informations supplémentaires. Ils peuvent être utilisés à des fins de dépannage ou pour contrôler le traitement d'une connexion particulière. Il existe quelques indicateurs TCP beaucoup plus utilisés que d'autres, tels que « SYN », « ACK » et « FIN » [4].

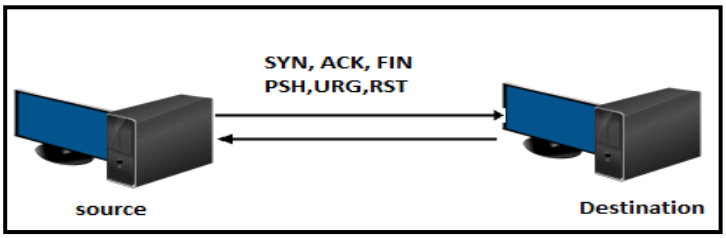


Figure 1-10. TCP flags.

Flag SYN : c'est un indicateur de synchronisation codé sur 1bit, utilisé comme première étape pour établir une connexion à trois voies entre deux machines.

Flag ACK « accusé de réception » : le drapeau ACK est codé sur 1 bit et utilisé pour accuser la réception du paquet.

Flag FIN : ce champ est codé sur 1 bit, utilisé dans le dernier paquet envoyé par le serveur pour indiquer la fin de transmission.

Flag URG : le drapeau URG est utilisé pour informer le destinataire du traitement des paquets urgents avant le traitement de tous les autres paquets [4].

Flag PSH : le champ PSH codé sur 1 bit indique au destinataire de traiter les paquets envoyés et de ne pas attendre le remplissage de mémoire tampons.

Flag RST : le drapeau RST demande la réinitialisation de la connexion.

- **Etablissement d'une connexion :**

L'établissement d'une connexion TCP s'effectue en trois temps, comme le montre le schéma de la figure 1-12.

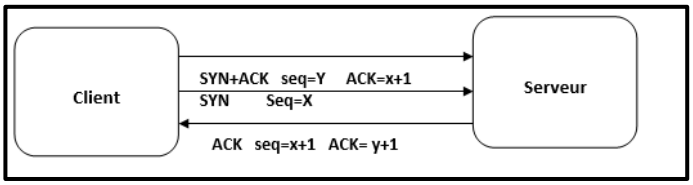


Figure 1-11. Etablissement d'une connexion TCP.

Le client envoie un segment comportant le drapeau SYN, avec sa séquence initiale (Seq = x), le serveur répond avec sa propre séquence (seq=y), mais il doit également acquitter le paquet précédent, ce qu'il fait avec ACK (seq = x + 1). Enfin Le client doit acquitter le deuxième segment avec ACK (seq = y + 1).

b Protocole UDP (User Datagram Protocol)

Le protocole UDP permet aux applications d'accéder directement à un service de transmission de datagramme. Il possède un mécanisme permettant d'identifier les processus d'application à l'aide de numéro de port UDP. Il est orienté datagramme (sans connexion), ce qui évite le problème lié à l'ouverture et à la fermeture des connexions [5].

En-tête UDP :

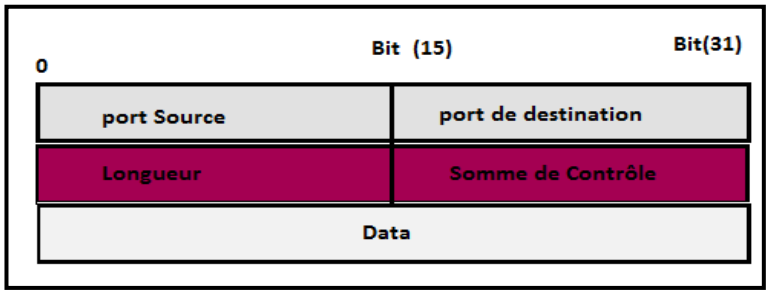


Figure 1-12. En-tête UDP.

- **Les ports :**

Les ports sont des portes d'entrée entre les hôtes terminaux. Ils sont codés sur 16 bits de 0 à 65535. Les hôtes utilisent les ports TCP ou UDP pour identifier les sessions à l'origine (port source) et à la destination.

Numéro du port	Type	Le protocole
21	TCP	FTP
22	TCP	SSH
25	TCP	SMTP
53	UDP	DNS
110	TCP	POP3
80	TCP	Http
546	UDP	DHCP

Tableau 1-3. Liste des ports.

1.7.4 Couche Application

Cette couche permet l'accès aux services réseaux et l'exécution des protocoles au niveau d'utilisateur. Les clients de messageries et les navigateurs web sont des exemples de ces types d'applications.

Les protocoles de couche application les plus utilisés sont :

a ***Protocole HTTP (protocole de transfert HyperText) :*** c'est un protocole de transfert des données sur internet (des pages web écrites en HTML).

b ***Protocole FTP (protocole de transfert de fichier) :*** est un protocole de type client/serveur, utilisé pour transférer des fichiers entre ordinateurs.

c ***Protocole POP (protocole de bureau de poste)*** *:* ce protocole permet de récupérer les E-mail sur le serveur internet.

d ***Protocole SMTP (protocole simple de transfert de courrier)*** **:** est un protocole de transfert des courriers sur un réseau, son principal rôle est de router les emails en utilisant les adresses du destinataire.

e ***Protocole DHCP (protocole dynamique de configuration d'hôte)*** **:** il s'agit d'un protocole qui permet à un ordinateur connecté à un réseau local d'obtenir dynamiquement et automatiquement sa configuration IP, le but principal étant la simplification de l'administration d'un réseau, le DHCP est un distribuant des adresses IP.

1.8 Terminologie de la sécurité informatique

Aujourd'hui, les systèmes informatiques occupent une place importante dans les entreprises, dans les administrations et dans le quotidien des particuliers grâce au développement d'internet. Les internautes peuvent ainsi bénéficier à moindre coût de moyens de communication rapides, partager des ressources de traitement et de stockage de grandes capacités (Cloud Computing), faciliter les échanges commerciaux et financiers (e-Commerce, e-Banking), fournir et utiliser de nombreux services en ligne (e-Administration, e-Health, e-Learning, etc.), participer à des communautés virtuelles et à des réseaux sociaux, se divertir (e-Gaming, e-Television, etc.) et, plus généralement, partager et accéder à l'information.

Toutes ces innovations ont permis de faciliter la vie à tous mais ont aussi contribué au développement de nouveaux risques qui sont les attaques informatiques, les méthodes de piratages sont de plus en plus nombreuses et perfectionnées, elles peuvent se traduire par des vols d'informations confidentielles, des destructions de données numériques, des coupures de services voire même des dégâts matériels.

1.8.1 Objectifs des attaques

- Prouver ses compétences techniques.
- Empêcher l'accès à une ressource (Bombes logiques, DOS), Timothy Lloyd a créé une des plus célèbres bombes logiques afin de venger la société Omega Engineering, cette bombe a 6 lignes de codes et a explosé le 31 Juillet 1996 et a causé des dommages qui coutent plus de 10 millions de dollars [6].
- Prendre le contrôle d'une ressource (BotNets DDOS), Le 27 Avril 2007 l'Estonie a été victime d'une violente attaque en DDOS venant de la Russie à cause d'un différend diplomatique, ce qui a mené au blocage des services bancaires et tous les systèmes des pays, ce qui a empêché la population d'acheter à manger, cette cyberattaque a bloqué tout le pays pendant plusieurs semaines [7].
- Récupérer de l'information sur un système (Espionnage industriel).
- Générer des revenus : (Vol, Extorsion, Publicité), la Citibank a été cassé par Vladimir Levin en 1994 qui a viré plus de 10 millions de dollars vers des d'autres comptes en USA, Finlande, Pays Bas, Israël et l'Allemagne en s'introduisant dans la base de données de la banque [8].

1.8.2 Vulnérabilité

La plupart des systèmes logiciels contiennent des vulnérabilités, c'est-à-dire des fautes de conception ou de configuration. Un attaquant peut alors exploiter ces vulnérabilités comme autant de vecteurs d'attaque pour effectuer différentes actions malveillantes dans un système informatique.

Les vulnérabilités les plus connues sont :

- Le débordement de tampon (Buffer Overflow),
- Injection SQL,
- Cross-site-scripting (XSS).
- Oubli de valider les entrées des utilisateurs.
- Contrôle d'accès inefficace.

- Mauvaise gestion des erreurs.
- Mauvaise utilisation du chiffrement.
- Failles dans l'administration distante.
- Mauvaise configuration du serveur web et des applications.

1.8.3 Menace

La menace désigne l'exploitation d'une faiblesse de sécurité par un attaquant, que ce soit interne ou externe à l'entreprise, on cite :

- Logiciel malveillant (malware).
- Virus, par exemple Stuxnet, découvert en 2010, a perturbé le programme nucléaire iranien et il avait comme cible les centrifugeuses de la centrale de Natanz ou il perturbait son fonctionnement ce qui a mené à la destruction de plusieurs centaines d'entre elles [9].
- Logiciel espion ou cheval de Troie, comme Skygofree un spyware identifié fin 2017, il cible les smartphones Android et il est capable de tracer leur localisation, d'enregistrer des conversations audios et d'intercepter des SMS ainsi que connecter un terminal infecté à un réseau Wi-Fi malveillant [10].
- Pourriel (spam).
- Hameçonnage(phishing).
- Attaque DDOS, un pirate informatique néerlandais a lancé des attaques DDOS contre des sites très médiatisés comme la BBC et Yahoo News, en utilisant un botnet DDOS, construit en utilisant le malware Mirai IoT.

1.8.4 Risque

Les menaces engendrent des risques et des couts humains et financiers : perte de confidentialité des données sensibles, indisponibilité des infrastructures et des données, dommages pour le patrimoine intellectuel et la notoriété :

- Yahoo a subi en 2014 une cyberattaque qui a affectée 500 millions de comptes utilisateurs. Cela constituait le plus gros piratage massif de données individuelles dirigé contre une seule société. Noms, dates de naissance, numéros de téléphone et mots de passe ont été volés [11].
- En décembre 2013, Target, deuxième chaîne de distribution américaine a été victime d'une cyberattaque. Les données de 110 millions de clients ont été récupérées. Les données bancaires de 40 millions de clients ont été volées et les données personnelles de 70 autres millions de clients ont été subtilisées (noms, adresses postales, numéros de téléphones et adresses e-mail) [11].
- En octobre 2013, Adobe annonce le piratage massif de son infrastructure informatique. Les informations personnelles de 2,9 millions de comptes ont été dérobées (identifiants, mots de passe, noms, numéros de cartes bancaires et dates d'expiration) [11].

1.8.5 Intrusion

Opération qui consiste à accéder, sans autorisation, aux données d'un système informatique ou d'un réseau, en contournant ou en désamorçant les dispositifs de sécurité mis en place.

Conclusion

Ce chapitre nous a permis de découvrir et de comprendre les notions et les aspects élémentaires des réseaux informatiques, où nous avons décrit les modèles OSI et TCP/IP, ainsi que les terminologies de la sécurité informatique que nous verrons en détail dans le chapitre qui suit.

La sécurité informatique est un enjeu important et majeur à prendre sérieusement et prioritairement en considération, pour le réaliser il est nécessaire de connaitre ses notions de base et les moyens de le protéger.

2.1 Introduction

Les exigences de la sécurité de l'information au sein des organisations ont conduit à des changements au cours des dernières décennies. Avant la sécurité de l'information était assurée par des moyens physiques ou administratifs, mais avec l'introduction de l'ordinateur, le besoin d'outils automatisés pour protéger les fichiers et les autres informations stockées est devenu évident.

On donne naissance alors à une collection d'outils conçus pour protéger des données et contrecarrer les pirates qu'on nomme sécurité informatique.

Ce chapitre introduit les notions de base de la sécurité informatique : menace, vulnérabilité ainsi que les moyens de se prémunir.

2.2 La sécurité informatique

La sécurité informatique c'est l'ensemble des moyens mis en place pour diminuer la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles en identifiant les exigences fondamentales en sécurité informatique. Elle s'exprime le plus souvent par les objectifs de sécurité suivants :

a **Disponibilité :** Demande que l'information sur le système soit *disponible* aux personnes autorisées.

b **Intégrité :** Demande que l'information sur le système ne puisse être *modifiée* que par les personnes autorisées.

c **Confidentialité :** Demande que l'information sur le système ne puisse être *lue* que par les personnes autorisées [12].

Le but de cette recherche est de donner un aperçu des intentions des pirates et donner une idée de leur façon de procéder afin de contrer leurs attaques et il est nécessaire de connaître les principaux types d'attaques afin de mettre en place des mesures de précaution.

2.3 Le pirate

Est une personne qui trouve et exploite les faiblesses des systèmes informatiques ou des réseaux pour y accéder, en utilisant plusieurs techniques parmi eux :

- L'envoi de chevaux de Troie
- La recherche de trous de sécurité.
- L'usurpation d'identité.
- Changement des droits utilisateurs d'un ordinateur.

2.4 Les attaques

2.4.1 Définition d'une attaque

C'est un acte malveillant envers un système informatique (système d'exploitation, logiciel ou utilisateur) en exploitant sa faille à des fins nuisibles non connues par l'exploitant du système.

2.4.2 Anatomie des attaques

Fréquemment appelés " les 5 P " dans la littérature, ces cinq verbes anglophones constituent le squelette de toute attaque informatique [13] :

a ***Probe*** **:** consiste en la collecte d'informations sur le système cible à l'aide de plusieurs outils.

b ***Penetrate*** **:** utilisation des informations récoltées pour pénétrer un réseau à l'aide de techniques.

c ***Persist :*** création d'un compte avec des droits de super utilisateur pour pouvoir se réinfiltrer ultérieurement.

d ***Propagate :*** cette étape consiste à observer ce qui est accessible et disponible sur le réseau local.

e ***Paralyze :*** cette étape consister à agir et nuire puis effacer les traces.

2.4.3 Type d'attaque

Les hackers utilisent plusieurs techniques d'attaques. Ils sont regroupés en 3 familles :

a Les attaques directes

L'hacker attaque directement la victime à partir de son ordinateur.

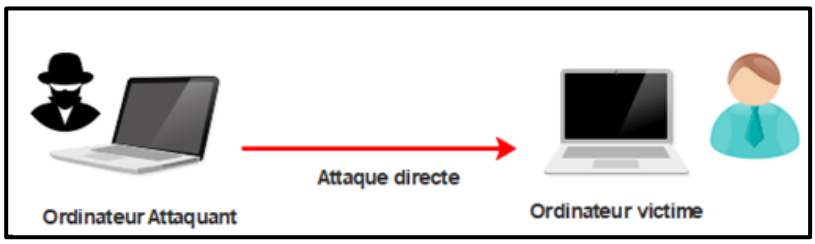


Figure 2-1 : Attaque directe.

b Les attaques indirectes par rebond

L'attaque par rebond consiste à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer ses traces (telle que son adresse IP) et dans le but d'utiliser les ressources de la machine qui sert de rebond.

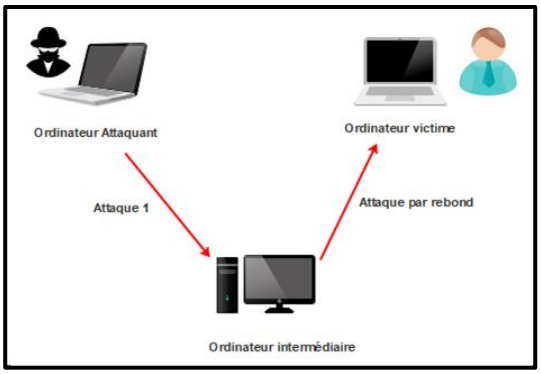


Figure 2-2 : Attaque indirecte par rebond.

c Les attaques indirectes par réponse

L'attaquant envoie une attaque requête à l'ordinateur intermédiaire pour qu'il la répercute et la réponse à la requête est donc envoyée à l'ordinateur victime.

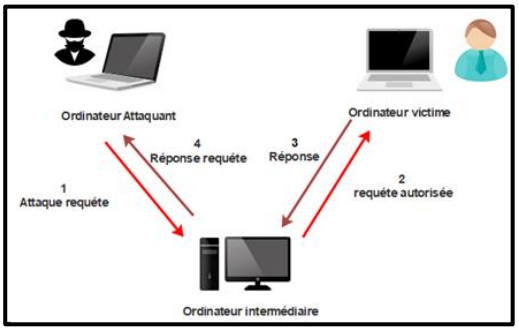


Figure 2-3 : Attaque indirecte par réponse.

2.4.4 Topologie des attaques

a Bombes logiques

Une Bombe logique est une partie d'un programme malveillant qui reste dormante dans le système hôte jusqu'à ce qu'un instant survienne, ou que certaines conditions soient réunies, pour déclencher des effets dévastateurs en son sein [14].

b Cheval de Troie

Un Cheval de Troie est un programme effectuant une fonction illégale en donnant l'apparence d'effectuer une fonction légale. La fonction illégale peut consister en la révélation ou la modification d'informations [14].

c Porte dérobée

Une porte dérobée est un moyen de contourner les mécanismes de contrôle d'accès. C'est donc une fonctionnalité inconnue de l'utilisateur légitime qui donne un accès secret au logiciel [14].

d Virus

Un virus est un élément de programme qui, lorsqu'il s'exécute, se reproduit en s'adjoignant à un autre programme (du système ou d'une application), Il peut ensuite se propager à d'autres ordinateurs (via un réseau) à l'aide du programme légitime sur lequel il s'est inséré [14].

e Ver

Un ver est un programme individuel qui se reproduit et se propage à l'insu des utilisateurs. Contrairement aux virus, un ver n'a pas besoin d'un logiciel hôte pour se dupliquer [14].

2.4.5 Quelques attaques connues

a Attaques de mot de passe

C'est le cassage d'un mot de passe en testant tous les mots de passe possibles ou bien essayer les combinaisons « simplistes », qui sont utilisées par la majorité des utilisateurs [15].

Pour se protéger il faut utiliser un mot de passe difficile à trouver qui comprend au moins 8 caractères, incluant des lettres (majuscules et minuscules), des chiffres et des symboles.

b Attaque man in the middle

Son objectif est de détourner le trafic entre deux machines pour intercepter, modifier ou détruire les données transmises au cours de la communication, ou bien écouter une communication entre deux interlocuteurs et falsifier les échanges afin de se faire passer pour l'une des parties [16].

- **ARP Poisoning**

Consiste à exploiter une faiblesse du protocole ARP en retrouvant l'adresse IP d'une machine à partir de l'adresse physique (adresse MAC) de sa carte réseau. Elle consiste à s'interposer entre deux machines du réseau et de transmettre à chacune un paquet falsifié indiquant que l'adresse MAC de l'autre machine a changé tout en fournissant celle de l'attaquant. Alors à chaque fois que l'une d'elles souhaitera communiquer avec l'autre, les paquets seront envoyés à l'attaquant, qui les transmettra de manière transparente à la machine destinatrice [17].

- **Vol de session TCP (TCP session hijacking)**

Est une technique consistant à intercepter une session TCP initiée entre deux machines afin de la détourner. Dans la mesure où le contrôle d'authentification s'effectue uniquement à l'ouverture de la session, un pirate réussissant cette attaque parvient à prendre possession de la connexion pendant toute la durée de la session [18].

c Phishing

C'est une attaque qui consiste à duper la victime par l'intermédiaire d'un courrier électronique qui ressemble à celui d'une véritable société (commerce en ligne, banque, etc.) et par le biais d'un formulaire factice, les pirates obtiennent des informations personnelles telles que numéro de compte bancaire, numéro client, code confidentiel, mot de passe, pour réaliser des transactions financières frauduleuses et revendent parfois ces informations volées. Pour se protéger il faut vérifier l'adresse du site qui s'affiche dans le navigateur, et ne pas communiquer des informations sensibles par messagerie ou téléphone et éviter les formulaires [19].

d Attaque par cheval de Troie

Cette attaque consiste à pénétrer dans une machine et installer un logiciel (cheval de Troie) qui va permettre à l'attaquant de contrôler la victime et avoir des informations sur la machine. La mesure de protection face à ce type d'attaque est de mettre en service un antivirus et le mettre à jour, un nettoyeur de troyens peut aussi être utile.

e Ingénierie sociale

Consiste à exploiter la naïveté des individus pour obtenir des informations. Un pirate peut ainsi obtenir le mot de passe d'un individu en se faisant passer pour un administrateur du réseau ou bien à l'inverse en demandant de réinitialiser le mot de passe en prétextant un caractère d'urgence. Seule une formation du personnel permet de se protéger de cette attaque [16]

f Mail bombing

Consiste à envoyer un grand nombre d'emails (plusieurs milliers par exemple) à un ou plusieurs destinataires afin de saturer le serveur de mails et la bande passante ainsi que rendre impossible aux destinataires de continuer à utiliser l'adresse électronique. Pour se protéger de cette attaque il ne faut pas communiquer l'adresse personnelles sauf au personnes dignes de confiance [20].

2.5 Les attaques par déni de service (DOS)

Les attaques par déni de services (Denial Of Service en anglais ou DOS) sont des attaques qui ont pour but rendre une machine ou un réseau indisponible durant une certaine période. Elle peut paraitre sans danger si elle vise un réseau ou un ordinateur particulier, mais peut s'avérer redoutable lorsqu'elle vise un serveur ou des ressources matérielles appartenant à une grande société dépendante de son infrastructure réseau [21].

Ces attaques sont très répandues sur les réseaux car elles sont assez simples à réaliser mais malgré ça elles peuvent mener à des conséquences désastreuses. En outre la détection et la prévention de ce genre d'attaques sont très difficiles car elles peuvent prendre plusieurs formes et quasiment tous les systèmes informatiques sont vulnérables.

Le principe général des attaques DOS, implique l'envoie des données ou des paquets de taille ou de contenu inhabituel, ceci a pour but de provoquer des réactions inattendues du réseau ou de la machine cible, pouvant aller jusqu'à l'interruption du service.

2.6 Attaques par déni de service distribué (DDOS)

Une attaque est dite « déni de service distribué » si elle est effectuée au même temps par une multitude de sources, ils trouvent leur origine dans des botnets ou des réseaux vulnérables.

Généralement considérées comme des attaques volumétriques à cause de leur énorme consommation de bande passante et leur ampleur mondiale, leur objectif est de provoquer la saturation des routeurs, pare-feu, serveurs et autres périphériques ou comme arme de diversion pour voler des données ou la propriété intellectuelle [22].

2.6.1 Principe

Son principe consiste à utiliser une grande quantité de postes « Zombies », auparavant infectées par des « backdoors » ou « troyens », dans le but de paralyser la réponse du serveur attaqué. Les maîtres sont eux-mêmes reliés aux postes « daemons ». Le pirate se sert des postes maîtres pour contrôler les postes daemons qui effectueront l'attaque, sans cela, le pirate devrait se connecter lui-même à chaque daemon ce qui serait plus long à mettre en place, et plus facilement repérable. Pour utiliser les masters et daemons.

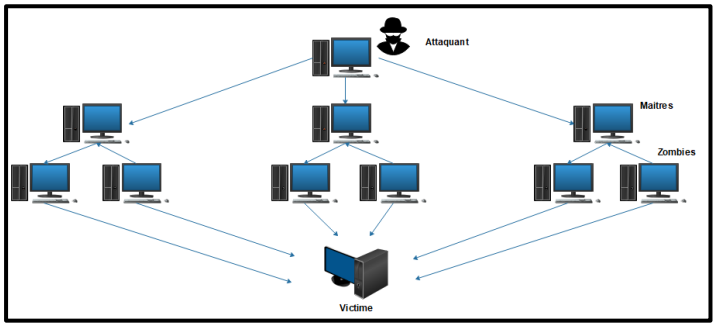


Figure 2-4 : Attaque DDOS.

2.6.2 Types d'attaques DOS

On cite cinq grands types d'attaques utilisant différents protocoles et couches réseaux.

a SYN Flood

Cette attaque utilise des paquets TCP contenant le flag SYN qui signifie à la cible que l'on veut établir une connexion avec elle. Elle consiste à envoyer un grand nombre de demandes de connexions au serveur cible (SYN) à partir de plusieurs machines et ne pas y répondre. Lors d'une demande de connexion, le serveur est en attente et bloque pendant un certain temps une partie de ses ressources pour cette nouvelle connexion. Le but est d'envoyer plus de demandes qu'il ne peut en traiter dans un temps donné. Ainsi, le serveur gaspille toutes ses ressources réseau à répondre à des requêtes qui ne mènent nulle part et il ne pourra plus subvenir aux besoins de vrais clients [21].

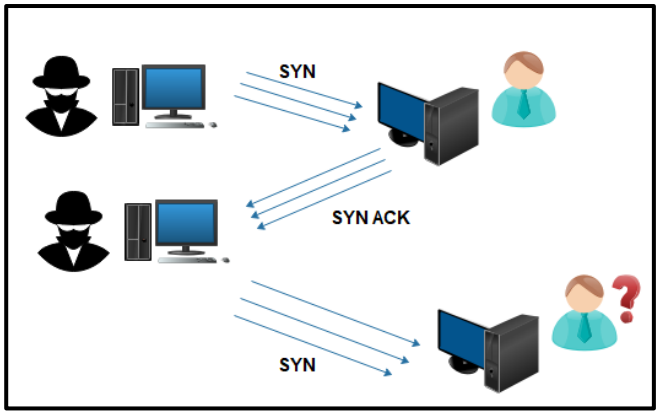


Figure 2-5 : Attaque SYN Flood.

b UDP Flood

Cette attaque exploite le mode non connecté du protocole UDP et consiste à saturer le trafic réseau en envoyant une grande quantité de paquets UDP à une machine.

Cette attaque mène à la congestion du réseau et la saturation des ressources et de la bande passante de la victime ce qui conduit à l'effondrement de la totalité du réseau [23].

c Http Flood

Cette attaque est utilisée par les pirates pour attaquer les serveurs web et les applications, elle consiste à les inonder de requêtes http, Il s'agit d'ensembles de requêtes HTTP GET ou POST légitimes, basés sur des sessions, envoyés à un serveur Web cible. Ces demandes sont spécifiquement conçues pour consommer une quantité importante des ressources du serveur et peuvent donc entraîner une condition de déni de service (sans nécessiter nécessairement un taux élevé de trafic réseau). De telles demandes sont envoyées en masse, augmentant ainsi la puissance globale de l'attaque [24].

d Ping of Death

Les paquets ICMP possèdent généralement un champ data de 56 octets. Certains systèmes deviennent vulnérables en envoyant des PING avec un champ de données plus important. Les systèmes en général ne sont pas prévus pour recevoir des paquets ICMP plus gros que les paquets IP traditionnels (64K), mais les PING peuvent être fragmentées. Cependant, une fois rassemblée, ces paquets causeront une saturation de la mémoire tampon. Cette attaque est de nos jours obsolète car la majorité des systèmes ont été corrigée. Elle touchait tous les systèmes d'exploitation et même les équipements réseaux tels que les routeurs et les imprimantes [22].

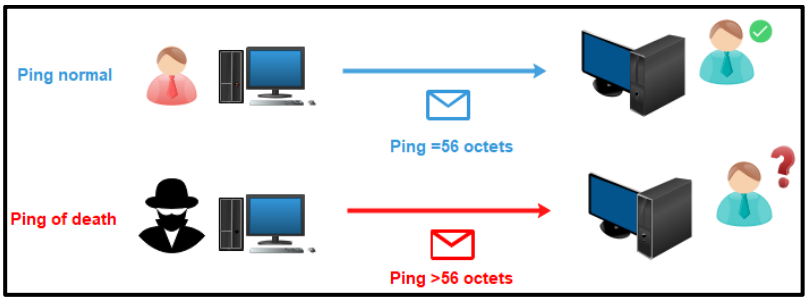


Figure 2-6: Attaque Ping of death.

e ICMP Flood

Les attaques ICMP Flood exploitent le protocole ICMP qui permet aux utilisateurs d'envoyer un paquet d'écho à un hôte distant pour vérifier s'il est toujours actif. Plus précisément, lors d'une attaque par inondation DOS ICMP, l'attaquant envoie de gros volumes de paquets ICMP_ECHO_REQUEST à la victime. Ces paquets demandent une réponse de la victime, ce qui entraîne la saturation de la bande passante de la connexion réseau de la victime. Lors d'une attaque par inondation ICMP, l'adresse IP source peut être usurpée. L'attaquant utilise l'usurpation d'adresse IP pour masquer sa véritable identité [25].

2.6.3 Les outils

Il existe de nombreux outils qui servent à réaliser les attaques par dénis de services selon le système, que l'on soit sous Windows, Linux ou autres systèmes d'exploitation.

a Hping3

Hping3 est un programme puissant qui permet d'envoyer les paquets TCP, UDP et ICMP et permet en plus de modifier certains champs des en-têtes de ces paquets. Il comporte aussi un trace route et des capacités à détecter les systèmes d'exploitation d'une cible. Cet outil peut s'avérer très puissant et peut être utilisé par exemple pour effectuer une attaque SYN Flood, Ping Flood, UDP Flood et Smurf [21].

b LOIC

C'est un programme qui permet de réaliser des attaques de déni de service distribué (**DDOS**) depuis son ordinateur. Ce qui le différencie de la plupart des outils d'attaque de ce type déjà disponibles, c'est sa facilité d'utilisation. LOIC propose trois types d'attaques : le Flood HTTP**,** le Flood TCP et le Flood UDP [26].

c Slowloris

Slowloris est un script perl qui met en œuvre une attaque par dénis de service contre les serveurs Web et il peut être exécuté sur n'importe quel système Unix. L'attaque consiste à initier des requêtes HTTP sans les terminer, la connexion étant maintenue active par l'envoi répétitif d'en-têtes. Une fois l'attaque lancée le serveur cible maintien des connexions ouvertes dans l'état ESTABLISHED.

Après un temps relativement court le serveur n'est plus accessible. Cet état est maintenu pendant toute la durée de l'attaque [27].

d Pyloris

Pyloris est un outil de déni de service HTTP qui permet à l'attaquant de créer ses propres en-têtes de requête HTTP. Il a une interface graphique facile à utiliser.

Son objectif est de maintenir les connexions TCP ouvertes le plus longtemps possible entre l'attaquant et les serveurs victimes. Cela entraîne l'épuisement des ressources de la table de connexion du serveur. Une fois que la table de connexion du serveur est épuisée, il ne sera plus en mesure de gérer les nouvelles connexions d'utilisateurs légitime ce qui entraînera un déni de service [28].

e SYN-Flood Python

Est un script écrit en Python, utilisé pour réaliser l'attaque SYN Flood en envoyant un nombre défini de demande de connexions TCP à la victime qui entrainera l'épuisement du serveur ceci entrainera à un déni de service.

f Xerxes

XerXes est un outil simple utilisé pour attaquer les serveurs web. Lors de son exécution, l'outil lance une inondation de connexion TCP sur sa cible, provoquant ainsi l'épuisement des ressources de la table de session, ce qui provoque une panne du serveur [29].

2.7 Les moyens de se prémunir

Il est très important de se prémunir contre ces attaques faciles à réaliser et pouvant provoquer de graves dégâts Il existe plusieurs moyens, plus ou moins efficace, permettant de détecter et/ou de bloquer ces attaques.

2.7.1 Firewall

Les firewalls sont des équipements réseaux qui permettent de filtrer les paquets entrants et sortants afin de prévenir toutes attaques de l'extérieur. Ils se basent sur un fonctionnement séquentiel et un ensemble de règles pour autoriser seulement les connexions légitimes.

En utilisant un pare-feu puissant, ça peut arrêter l'accès réseau indésirable et rester protégé contre les différents types d'attaques DDOS. Les pares-feux sont la première ligne de défense car ils empêchent tout accès non autorisé.

- **Inconvénient :**

Dans le cadre des attaques DOS, le problème majeur est que les attaquants utilisent des connexions légitimes pour perpétrer leurs attaques. De plus, les firewalls ne peuvent pas efficacement différencier les connexions légitimes et illégitimes.

2.7.2 Cryptographie

La cryptographie est une science qui permet de convertir des informations claires en informations codées. Puis à partir de ces dernières les informations originales sont restituées.

Les mécanismes permettant de la réaliser sont :

a Chiffrement

Pour assurer la sécurité d'un document électronique, on chiffre le document ; et pour cela il existe deux grandes familles d'algorithmes de chiffrements, ceux à clés symétriques et ceux à clés asymétriques.

- **Algorithme de chiffrement symétrique :** Il consiste à utiliser la même clé (clé privée) pour le chiffrement ainsi que pour le déchiffrement.
- **Algorithme de chiffrement asymétrique :** Il consiste à utiliser une paire de clés asymétrique (une clé publique et une clé privée) pour le chiffrement et le déchiffrement [30].

b Signature électronique

La signature électronique est un mécanisme qui permet d'assurer les fonctions d'authentification, d'intégrité et de non répudiation, elle possède plusieurs propriétés rendant son utilisation incontournable :

- Une signature ne peut être falsifiée.
- Une signature donnée n'est pas réutilisable pour un autre document.
- La modification d'un document signé altère la signature de ce document.
- Une signature ne peut être niée [31].

2.7.3 VPN

Un réseau virtuel privé, crée un tunnel crypté pour acheminer tout le trafic internet en masquant l'adresse IP de toute sorte de surveillance. Un attaquant ne pourra voir que l'adresse IP du serveur VPN et ne pourra donc pas inonder le réseau.

2.7.4 Mise à jour du système

La mise à jour est un moyen très simple à mettre en œuvre pour éviter les dénis de services applicatifs, car elle permet souvent de corriger des failles logicielles, qui peuvent être utilisées par des attaquants. Il est donc important de mettre à jour tous les logiciels de son système très régulièrement.

2.8 Système de détection d'intrusion (IDS)

Un IDS est un ensemble de logiciel et/ou de matériel, qui a pour rôle de surveiller tous les paquets qui transitent sur un système, dans le but de détecter toutes tentatives d'intrusions et qui peuvent déclencher différentes alertes en fonction du trafic et de sa configuration. C'est un système qui fonctionne en temps réel, et qui requiert beaucoup de ressources, aussi bien en CPU pour traiter chaque paquet, qu'en bande passante. C'est la raison pour laquelle il est préférable de l'installer sur un système dédié [32].

2.8.1 Principe de détection des intrusions

Il existe plusieurs méthodes permettant de détecter une intrusion :

a L'Approche par scénario ou par signature

Consiste à détecter des signatures d'attaques (ensemble de caractéristiques permettant d'identifier une activité intrusive : une chaîne alphanumérique, une taille de paquet inhabituelle, une trame formatée de manière suspecte, …) Connues dans les paquets circulant sur le réseau.

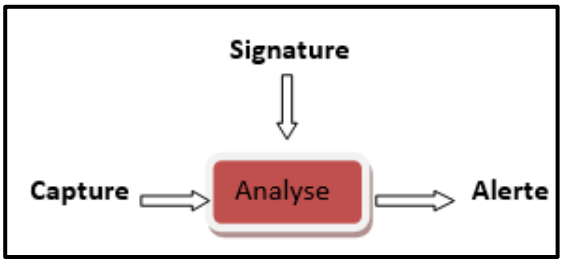


Figure 2-7 : Approche par signature.

b L'Approche comportementale ou par Anomalie

Consiste à détecter une activité suspecte dans le comportement de l'utilisateur en dressant un profil à partir de ses habitudes et déclencher une alerte lorsque des événements hors profil se produisent.

2.8.2 Format d'IDS

Les IDS sont disponibles sous deux formats :

a Les logiciels

Peuvent être installés sur l'OS de n'importe quel administrateur de réseau. Ils sont faciles à installer, configurer et contrôler.

b Les appliances

Sont des « boîtes noires » dédiées, connectées au réseau et implémentées d'un OS propriétaire d'un firewall et des interfaces réseaux requises.

2.8.3 Différents types d'IDS

Il existe plusieurs types d'IDS mais on peut les classer en deux grandes familles :

a Les NIDS

Un NIDS (Network IDS) est un système qui va écouter en temps réel, et de manière passive, tous les flux transitant sur un réseau afin de détecter les intrusions. Un NIDS capture donc tout le trafic réseau, l'analyse, et génère des alertes lorsque des paquets suspects sont détectés.

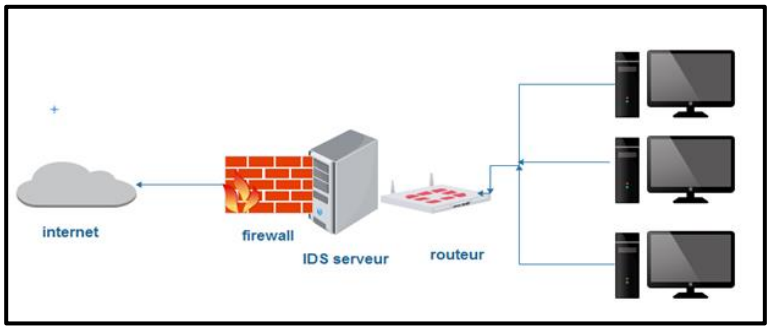


Figure 2-8 : NIDS.

b Les HIDS

Un HIDS (Host IDS) est dédié à une machine en particulier, il analyse seulement le trafic entrant et sortant de cette machine, il récupère les informations qui lui sont données par le matériel ou le système d'exploitation.

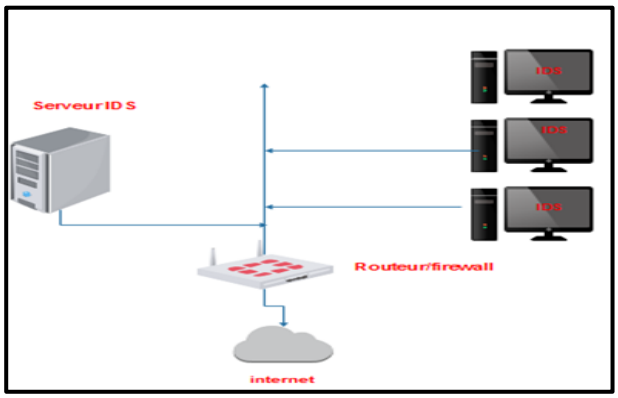


Figure 2-9 : HIDS.

c IPS

Les IPS (Intrusion Prevention System) sont un ensemble de matériel et de logiciel ayant pour but d'empêcher les intrusions ou autres activités suspectes détectées. Les IPS sont donc des outils actifs permettant de stopper toutes activités suspectes, contrairement aux IDS qui ne font que les détecter.

2.9 Travail à faire

A travers notre plateforme expérimentale, nous allons essayer de décrire comment le système de détection d'intrusion open source Snort détecte les attaques DOS en comparant le trafic pendant l'attaque par rapport au trafic normal, ce qui nous oblige donc à décrire aussi le trafic normal.

En raison des différences trouvées dans la comparaison on va obtenir des signatures et proposer une solution pour la détection. Et cela afin de cerner notre problématique et d'apporter des éléments de réponses à un certain nombre de question posées au début de ce travail.

Notre travail est divisé en 2 volets :

2.9.1 Volet 1

- Simulation des attaques: ICMP Flood, Ping of death, UDP Flood, TCP Flood, http Flood avec plusieurs outils.
- Analyse des paquets avec Wireshark.
- Comparaison des paquets des attaques avec les paquets normaux.
- Conception des signatures.

2.9.2 Volet 2

- Création des règles de détection en se basant sur les signatures obtenues en utilisant un IDS open source Snort.
- Tester la fiabilité des règles.

Tout au long de notre recherche on utilise les logiciels suivants :

- Wireshark version 3.0.1 64 bits.
- Snort version 2.9.0.5.
- BASE version 1.4.5.

2.10 Wireshark

Wireshark est un logiciel d'analyse réseau (sniffer) qui permet de visualiser l'ensemble des données transitant sur la machine qui l'exécute, et d'obtenir des informations sur les protocoles applicatifs utilisés. Les octets sont capturés en utilisant la librairie réseau PCAP, puis regroupés en blocs d'informations et analysés par le logiciel [33].

2.10.1 Présentation de l'interface Wireshark

a Capture des paquets

Quand on clique sur une interface et on commence la capture la fenêtre principale s'ouvre et elle est divisée en trois sections :

(1) Affiche l'ensemble des paquets capturés.

(2) Affiche le détail d'un paquet sélectionné.

(3) Reproduit le contenu l'ensemble du paquet sous forme octale et ASCII.

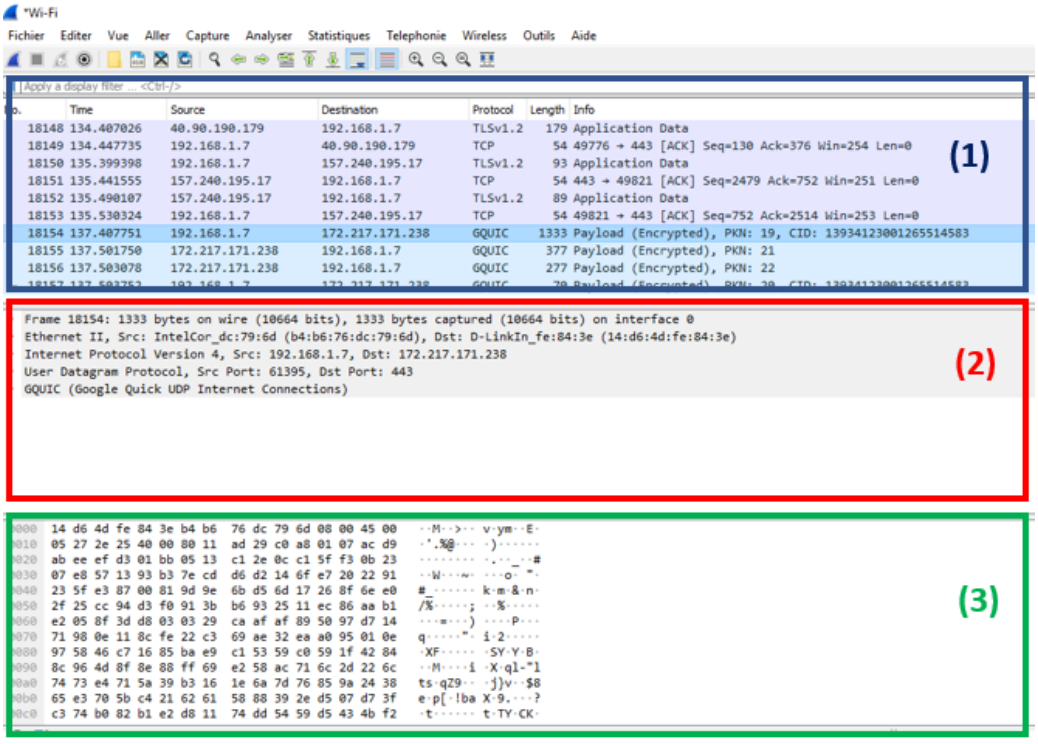


Figure 2-10. Capture du paquet.

b Liste des paquets capturés

L'ensemble des paquets capturés est divisé en 7 zones :

(1) Numéro du paquet.

(2) Temps.

(3) Adresse IP source.

(4) Adresse IP destination.

(5) Protocole.

(6) Longueur du paquet.

(7) Information sur le paquet.

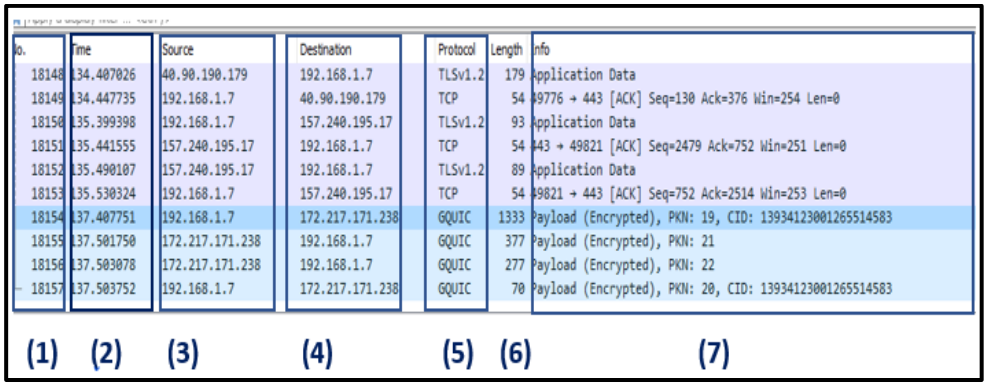


Figure 2-11 : Liste des paquets capturés.

2.11 IDS Snort

2.11.1 Présentation de Snort

C'est un système de détection d'intrusion réseau (NIDS) Open source, publié sous licence GPL, fonctionne sur les systèmes d'exploitation Windows et linux, à l'origine écrit par Martin Roesch.

Snort est l'un des NIDS les plus performants, il est capable d'effectuer la journalisation des paquets et l'analyse de paquet afin de faire la correspondance de contenu et détecter les attaques, nous avons travaillé avec la version 2.9.0.5.

2.11.2 Fonctionnement de Snort

Snort peut être configuré pour fonctionner en trois modes :

a Le mode sniffer

Il lit les paquets circulant sur le réseau et les affiche d'une façon continue sur l'écran.

b Le mode « packet logger »

Il journalise le trafic réseau dans des répertoires sur le disque.

c Le mode détecteur d'intrusions réseau (NIDS)

Il analyse le trafic du réseau, compare ce trafic à des règles déjà définies par l'utilisateur et établi des actions à exécuter.

2.11.3 Les règles Snort

Snort permet d'écrire des règles personnelles et utilise un langage de description simple et léger.

Ces règles sont devisées en deux sections logiques, l'entête et les options de la règle :

a L'entête de la règle

Contient l'action de la règle, le protocole, les adresses IP source et destination ainsi que les ports source et destination.

b Option de la règle

Contient les messages d'alertes et les informations sur les parties du paquet qui doivent être inspectées pour déterminer si l'action de la règle doit être acceptée.

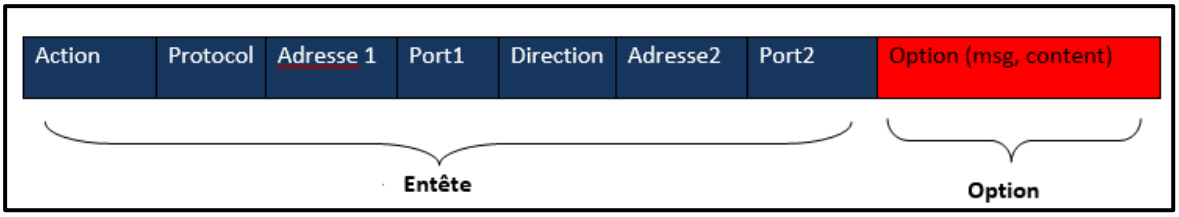


Figure 2-12 : Format de la règle Snort.

c Description de format de signature

- **Le champ « action » :** contient les actions menées par Snort qui permet de générer ou ignorer ou faire enter le paquet ainsi qu'activer ou définir les règles dynamiques ; Il y a cinq principales actions : alert, pass, log, activate, dynamic.
- **Le champ « protocole** » : décrit le protocole utilisé pour la communication, Snort supporte les protocoles TCP, UDP, ICMP et IP.
- **Les champs « Direction » :** gèrent la direction des échanges réseau (->, <-, <->) sur Snort.
- **Les champs « Adress/Port » :** décrivent les adresses IP et les ports des machines qui échangent des données sur le réseau.
- **Les options de règle :** spécifient entre parenthèse contient les principes de détection d'intrusion, toutes les options de la règle sont séparées les unes des autres par un caractère point-virgule « ; ».

Pour chaque option le format est nom option : valeur1 [, valeur2…] ci-dessous les options utilisées dans la création des règles :

- msg : affiche un message dans les alertes et journalise les paquets.
- dsize : teste la taille de la charge du paquet contre une valeur .
- flags : teste les drapeaux TCP pour certaines valeurs .
- content : recherche un motif dans la charge d'un paquet.

d Exemple d'une règle

Cette règle génère une alerte quand l'adresse 192.168.20.54 reçoit un ping de la part de n'importe quelle adresse en affichant le message « Ping test ».

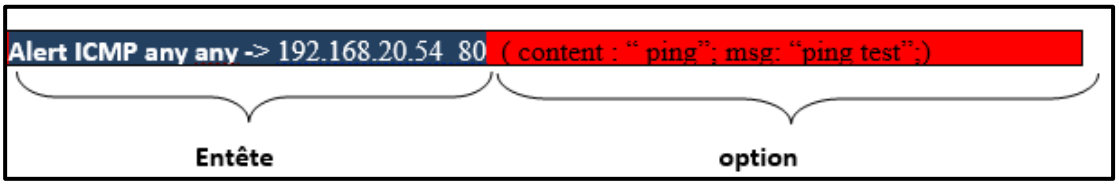


Figure 2-13 : Exemple d'une règle.

2.12 La console BASE

Par défaut, les alertes de Snort sont enregistrées dans un simple fichier texte qui son analyse n'est pas facile, d'où la nécessité d'une interface graphique, la plus utilisée est la console BASE (Basic Analysis Security Engine) une application Web écrite en PHP qui interface la base de données dans laquelle Snort stocke ses alertes. Pour fonctionner, BASE a besoin d'un certain nombre de dépendances :

- Un SGBD installé : MySQL.
- Un serveur http : Apache.
- Module PHP.
- La bibliothèque ADODB.

Pour cela nous avons travaillé avec Wamp Server version 2.2 (Apache 2.2.22, MySQL 5.5.24, PHP 5.3.4).

Conclusion

Dans ce chapitre nous avons vu l'impact des attaques sur le réseau informatique ainsi que les mesures qu'il faut prendre pour assurer sa protection.

Aujourd'hui, les attaques envers les systèmes informatiques sont devenues nombreuses et fréquentes, et les outils d'attaques sont de plus en plus disponibles et exploitables d'où la nécessité d'un système de détection d'intrusion, c'est une technologie qui a le concept de détecter ce type d'attaques.

3.1 Introduction

Les attaques DOS sont aujourd'hui fréquentes, notamment du fait de la relative simplicité de leur mise en œuvre, l'objectif principal de ce chapitre est de simuler ces attaques avec plusieurs outils et d'extraire leurs signatures.

Tout d'abord nous discutons de l'environnement utilisé, après nous verrons la simulation des attaques et l'analyse du flux de données pour le comparer à celui des paquets normaux et extraire les signatures de ces attaques.

3.2 Environnement

3.2.1 Hacker

La majorité des outils d'attaque sont conçus pour Linux, alors pour avoir de bons résultats nous avons préféré de travailler dans un environnement Linux, plus précisément : **Kali linux**, car il nous fournit un espace de travail unique et nous assure une fiabilité de résultats incomparable.

Kali Linux est une distribution gratuite GNU/Linux basée sur Debian sortie le 13 mars 2013 développé, fondé et maintenu par Offensive Security. Son objectif est de fournir une distribution regroupant l'ensemble des outils nécessaires aux tests de sécurité d'un système d'information.

3.2.2 Victime

Nous avons choisi de travailler sous Windows 7, car c'est un système d'exploitation moins sécurisé et vulnérable et peux contenir des failles de sécurité. Microsoft Windows 7 (Microsoft Windows NT 6.1) est commercialisé le 22 Octobre 2009. [34]

Fiche technique	Hacker	Victime
Fonction		
Marque de PC	HP	HP
Processeur	Intel ® Core™ i3-3110M CPU@ 2.40 GHz 2.40 GHz	Intel ® Core™ i3-3217U CPU@ 1.80 GHz 1.80 GHz
RAM	4,00Go	4,00Go
Type du système	Système d'exploitation 64 bits	Système d'exploitation 64 bits
Système d'exploitation	Kali Linux+ Windows 10	Windows 7
Carte réseau local	Ethernet Controller	Realtek PCIe FE Family Controller

Tableau 3-1. Caractéristiques des équipements.

3.3 Simulation

3.3.1 Schéma de travail

Pour faire la simulation nous avons travaillé dans un réseau LAN en utilisant 4 PC reliés avec des câbles RJ45.

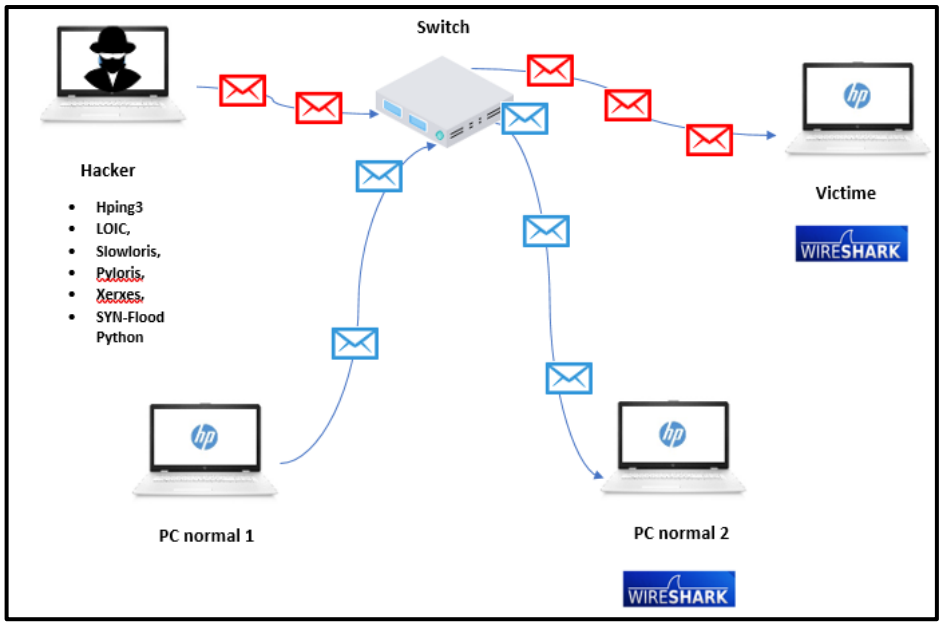


Figure 3-1. Schéma de travail.

- Adresse IP Hacker sous Kali Linux : 192.168.43.78.
- Adresse IP Hacker sous Windows 10: 192.168.43.19.
- Adresse IP victime : 192.168.43.239.

a Ping

On a effectué un ping (une commande qui permet de tester l'accessibilité d'une autre machine à travers un réseau IP) à partir du hacker pour vérifier l'existence de la machine victime sur le réseau**.**

- Formule utilisée : **#ping 192.168.43.239.**

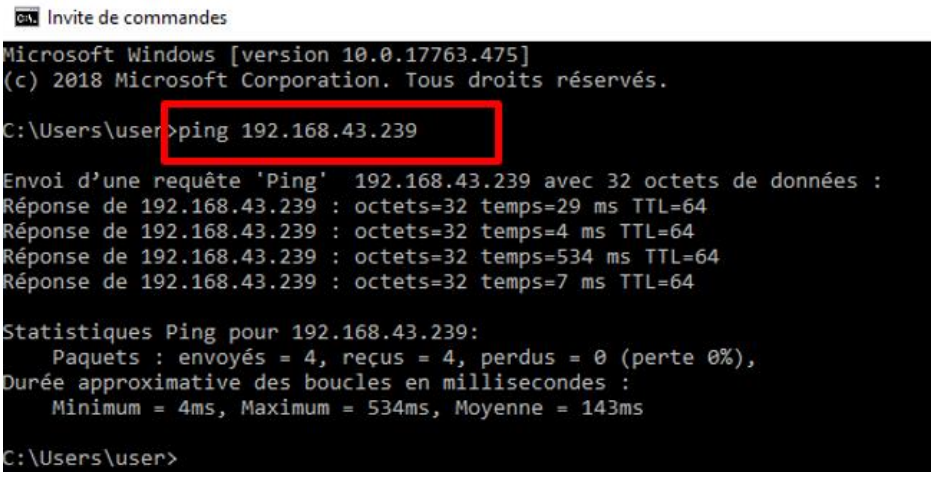


Figure 3-2. *Ping*

Après avoir fait le ping , on va simuler les attaques avec différents outils.

3.4 Attaque UDP Flood

On a réalisé l'attaque UDP en utilisant les outils Hping3 et LOIC.

3.4.1 Hping3

- Adresse IP de l'hacker usurpée : 192.168.43.48
- Formule utilisée : **#hping3 -2 -i u10000 -a 192.168.43.48 192.168.43.239**

-2 : définit le protocole UDP.

-i : définit l'intervalle de temps entre chaque attaque, (u) pour microsecondes.

-a : définit l'adresse source (l'adresse usurpée).

- Nombre de paquets envoyés : 3956 paquets.

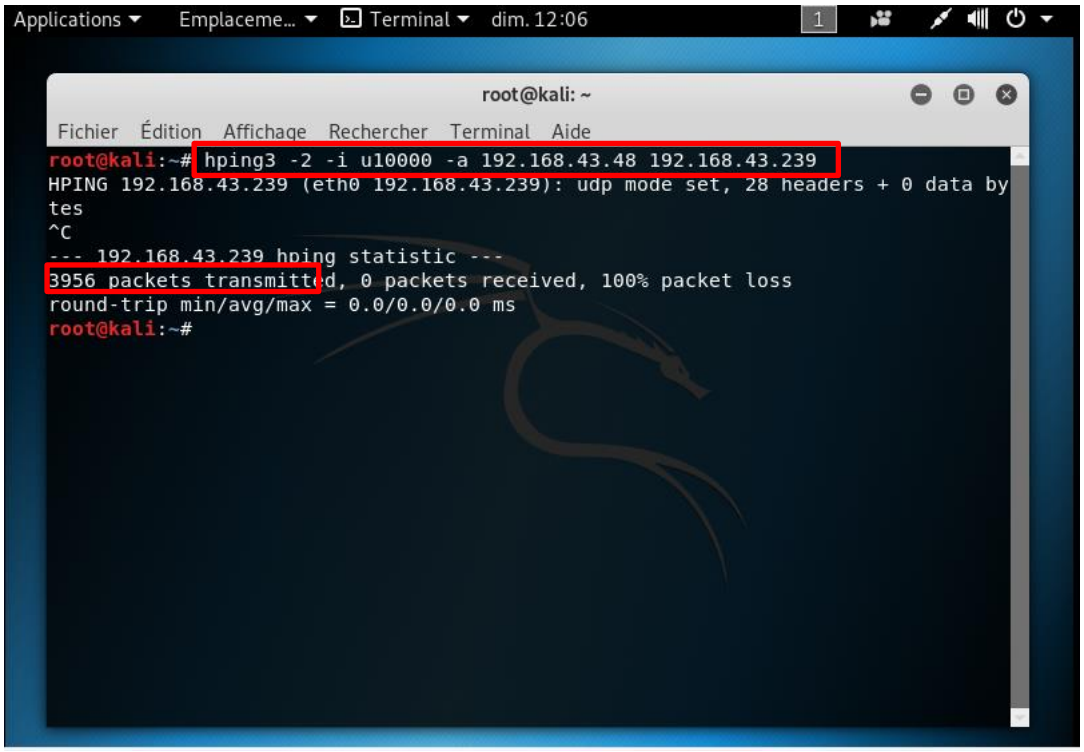


***Figure 3-3**. Attaque UDP Flood Hping3.*

Pendant que l'attaque est en cours, on analyse les paquets dans la machine victime, et on remarque la réception d'un grand nombre de paquets UDP sans arrêt pendant l'attaque à partir de l'adresse 192.168.43.48 (attaquant).

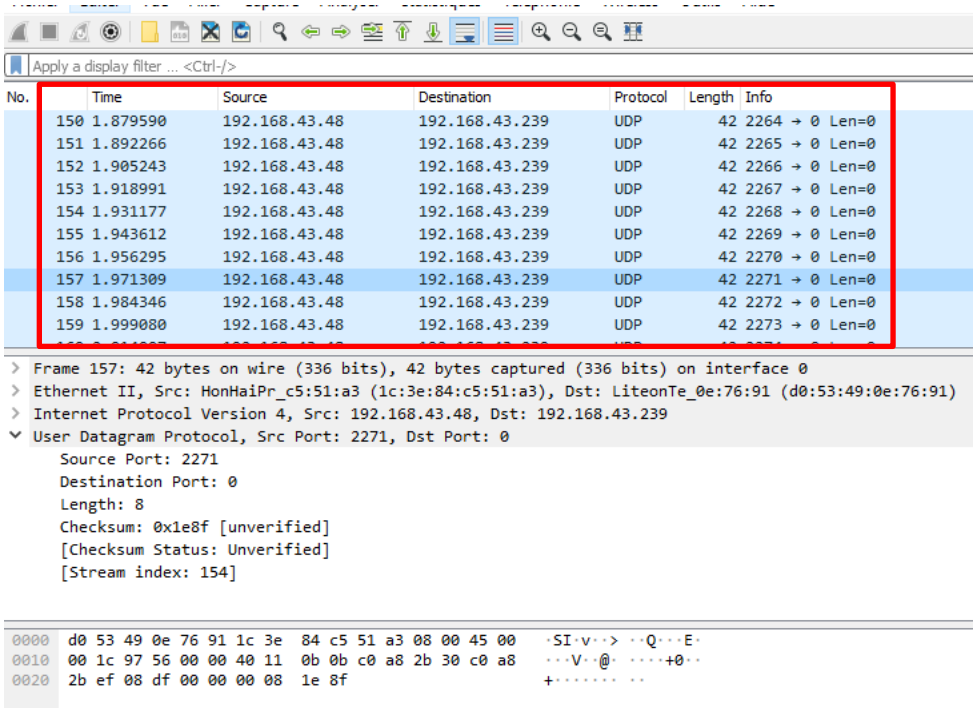


Figure 3-4. Analyse de paquets Attaque UDP Flood Hping3

On trace le graphe qui affiche le nombre de paquets/S pendant 36 secondes, on choisit de tracer les paquets UDP, et on remarque que sa valeur est très élevée pendant l'attaque et la valeur maximale est égale à 9000, elle commence à diminuer après 6 secondes (la fin de l'attaque).

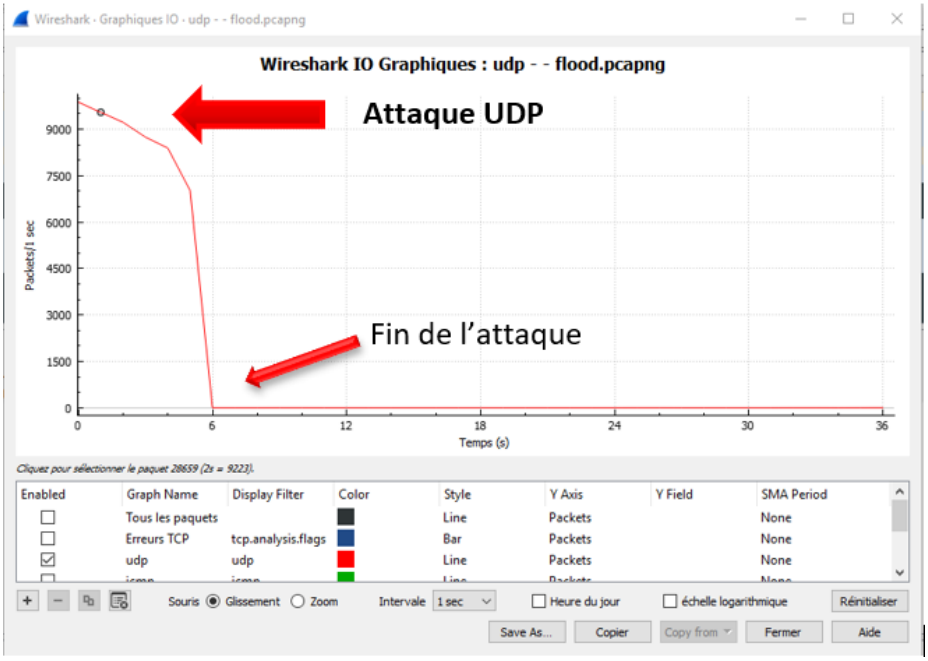


Figure 3-5. Nombre de paquet/S UDP Flood Hping3.

3.4.2 LOIC

Cet outil a été utilisé sous Windows 10 car on a eu des difficultés à l'installer sous Kali Linux.

a Fonctionnement de l'outil

Comme le montre la figure suivante :

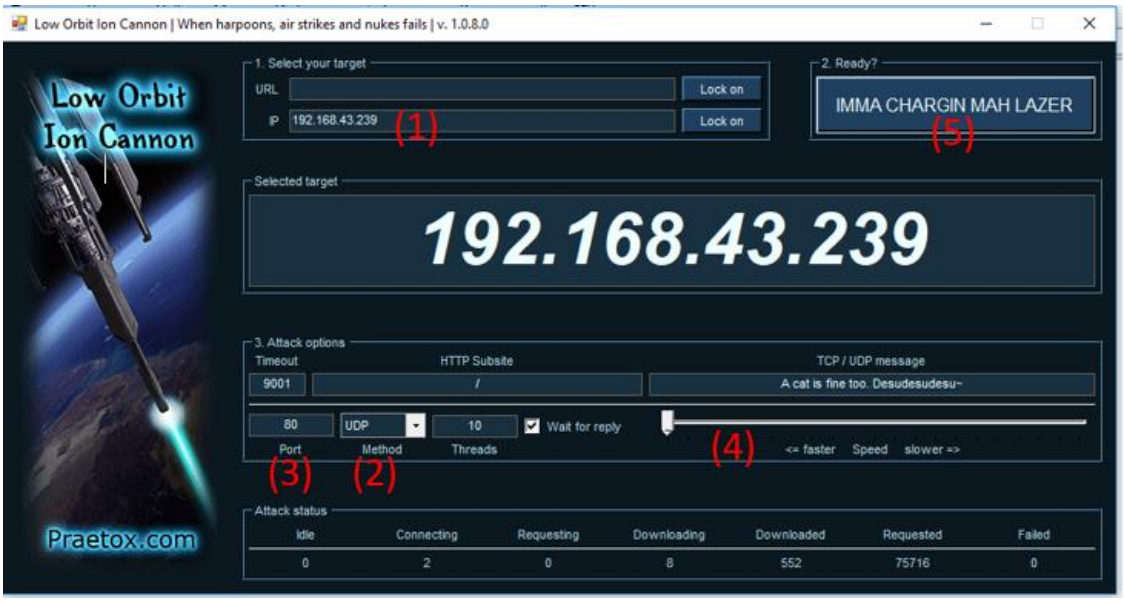


Figure 3-6. Fonctionnement LOIC.

(1) Adresse IP de la victime. (192.168.43.239) et on clique sur Lock On.

(2) Type d'attaque (UDP).

(3) Le port (80).

(4) Vitesse de l'attaque (maximum).

(5) Lancement de l'attaque.

On analyse les paquets dans la machine victime et on remarque la réception d'une quantité importante de paquets UDP à partir de l'adresse 192.168.43.19 et de plusieurs ports vers le port 80, la réception des paquets s'arrête dès la fin de l'attaque.

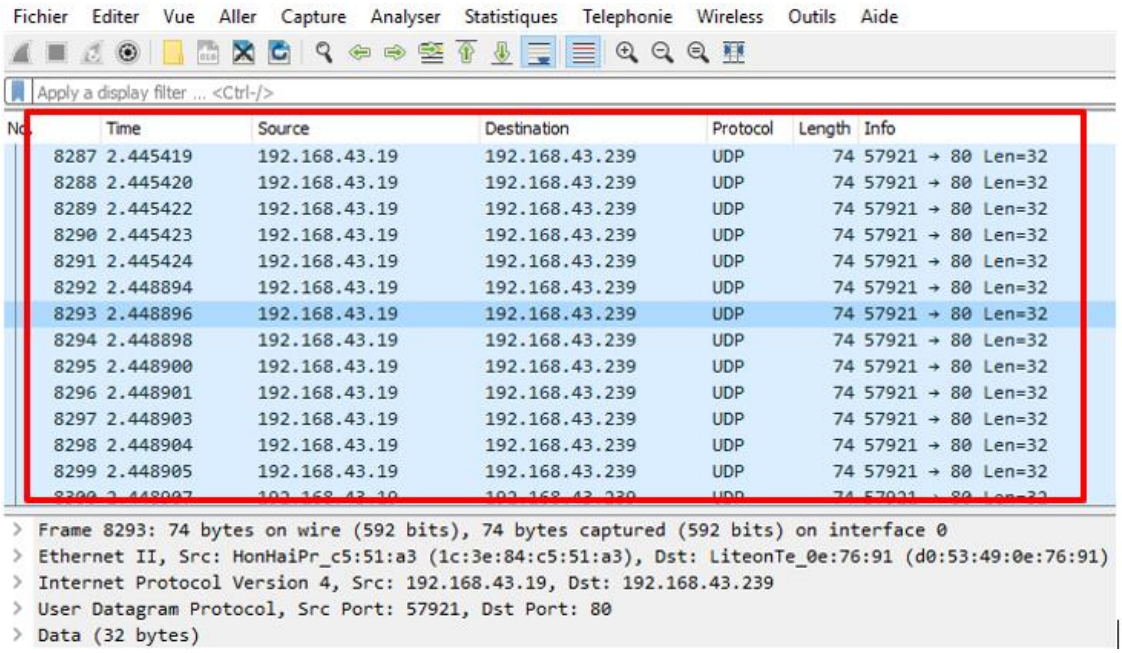


Figure 3-7. Analyse de paquets UDP Flood LOIC.

On peut tirer du graphe que le nombre de paquets UDP/S pendant 5 est très élevés et sa valeur maximale est 3600, elle commence à diminuer vers la fin de l'attaque.

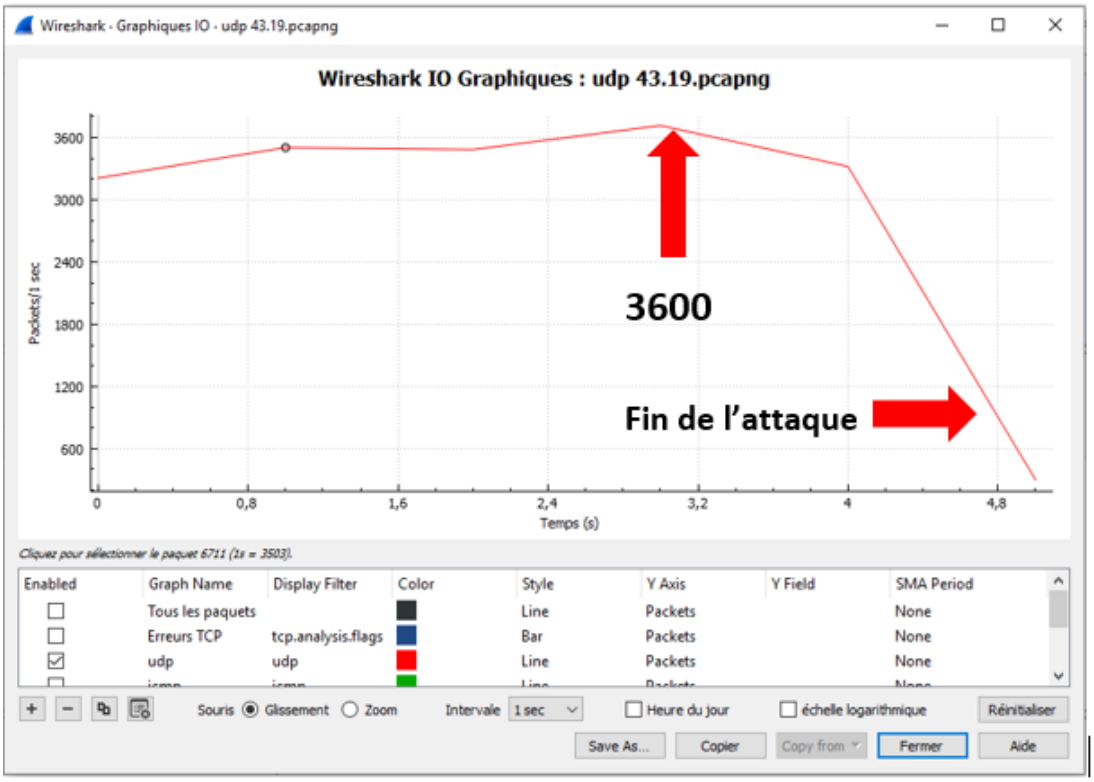


Figure 3-8. Nombre de paquets/S UDP Flood LOIC.

3.5 UDP

On analyse les paquets qui circulent entre les 2 PC normaux, et quand on trace le graphe qui affiche le nombre de paquets UDP/S pendant 1 minute on remarque que la valeur maximale est 235 et elle est presque stable et égale à 10.

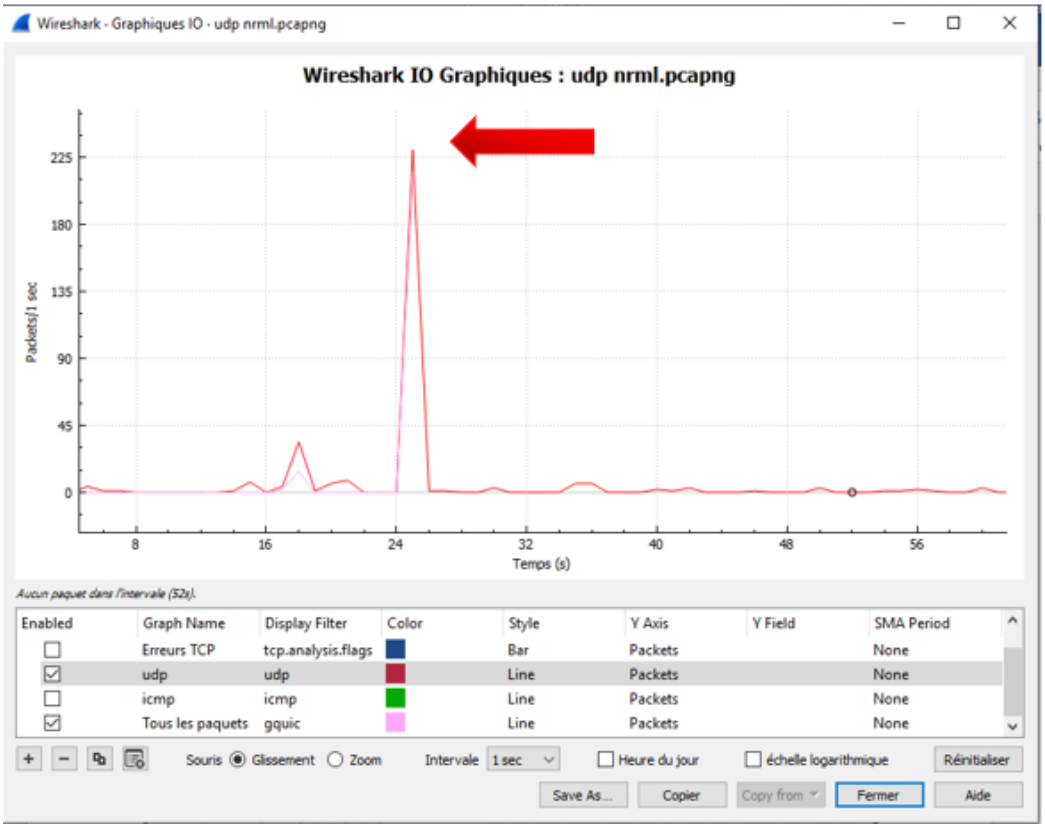


Figure 3-9. Nombre de paquets/S UDP.

Quand on analyse les paquets on les filtre en écrivant UDP, on remarque la réception d'une grande quantité de paquets du protocole GQUIC, ce protocole permet l'envoi rapide de paquets simples via le protocole UDP sans connexion**.**

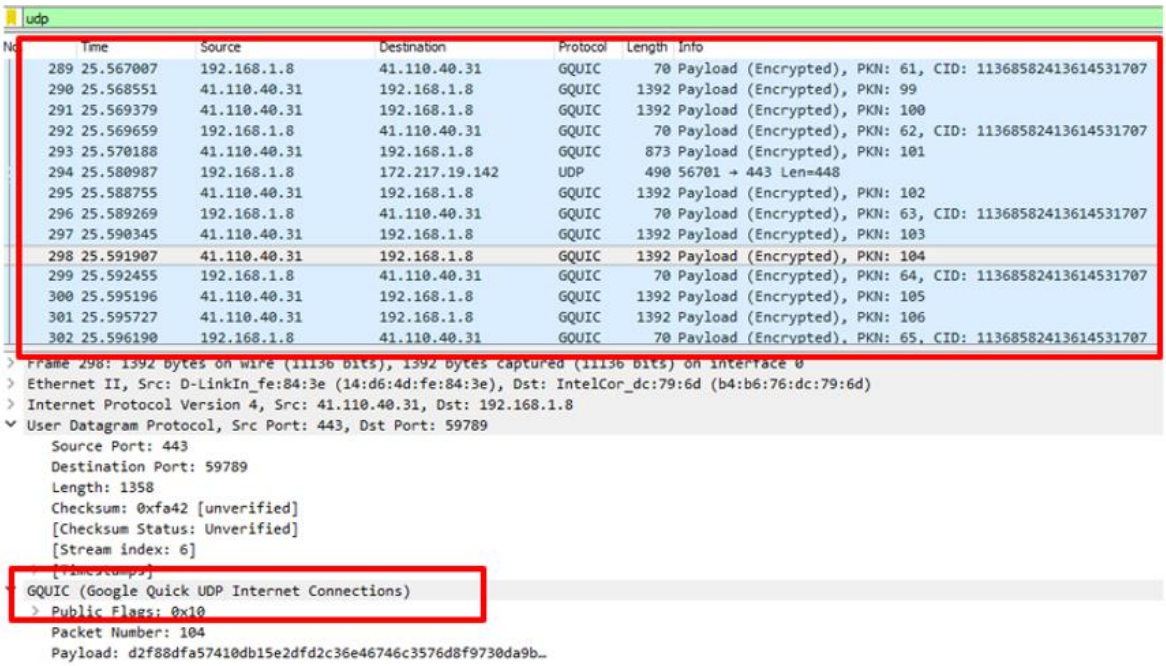


Figure 3-10. Analyse de paquets UDP.

3.5.1 Signature UDP

	Paquet normal	Attaque UDP	Différence
Nombre de paquets/S	Ne dépasse pas 235 paquets/S.	>9000 paquets/s pour Hping3. >3600 paquets/s pour LOIC.	L'attaque UDP dépasse le nombre de paquets normal

Tableau 3-2. Signature UDP.

3.6 Attaque ICMP

Nous avons utilisé Hping3 pour l'attaque ICMP Flood, et un ping pour réaliser l'attaque ping of death.

3.6.1 ICMP Flood :

- Adresse IP de l'hacker usurpée : 192.168.43.48
- Formule utilisée : **#hping3 -1 -i u10000 -a 192.168.43.48 192.168.43.239**

-1 : définit le protocole ICMP.

-i : définit l'intervalle de temps entre chaque attaque, (u) pour microsecondes.

-a : définit l'adresse source (l'adresse usurpée).

- Nombre de paquets envoyés : 3234 paquets.

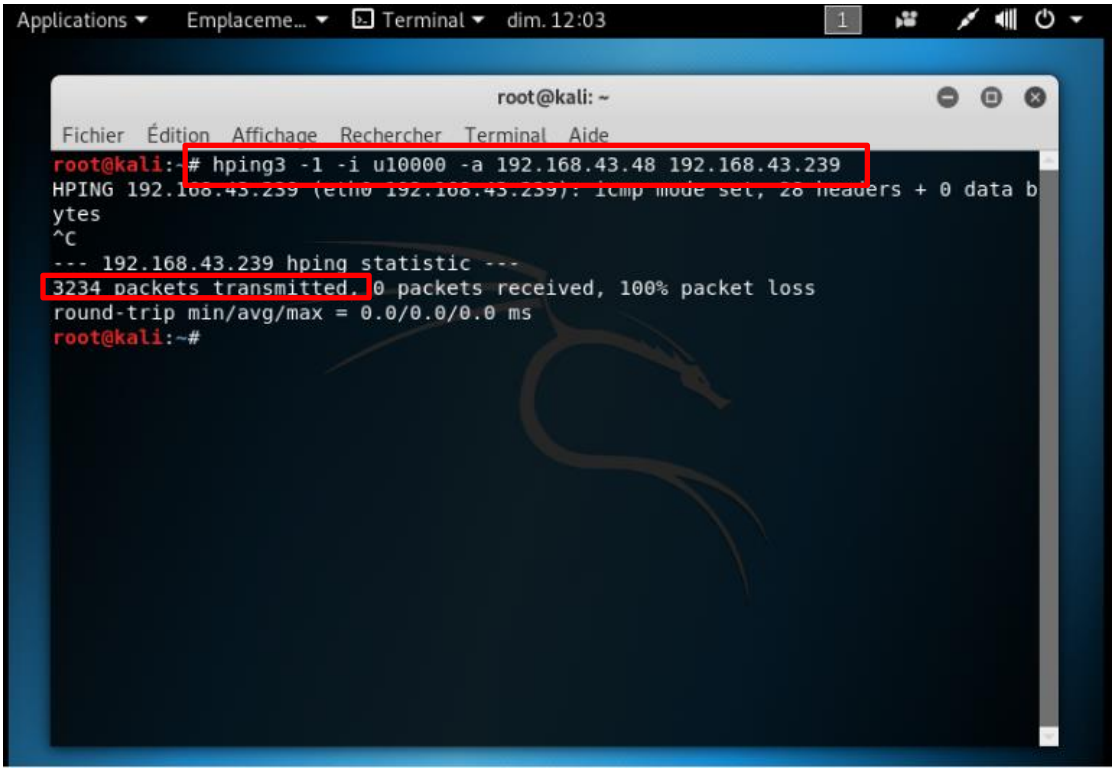


Figure 3-11. Attaque ICMP Flood.

a Analyse du paquet

Pendant l'attaque on remarque la réception d'un grand nombre de requêtes ICMP request (ping) sans arrêt à partir de l'adresse 192.168.43.48 (attaquant) sans aucune réponse de la victime (reply), la réception de paquets s'arrête vers la fin de l'attaque.

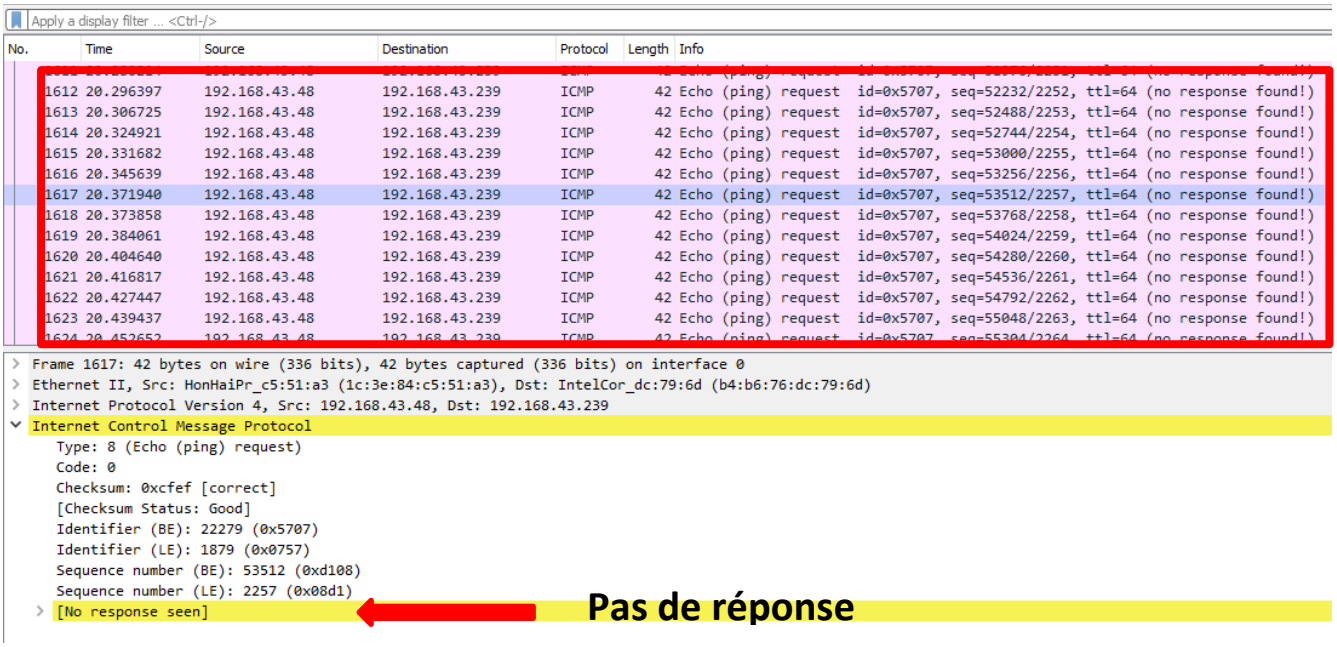


Figure 3-12. Analyse de paquets ICMP Flood.

Quand on trace le nombre de paquets ICMP/S pendant 36 secondes on remarque que sa valeur est presque stable et est égale à 84paquets/s puis elle diminue et s'annule (fin de l'attaque).

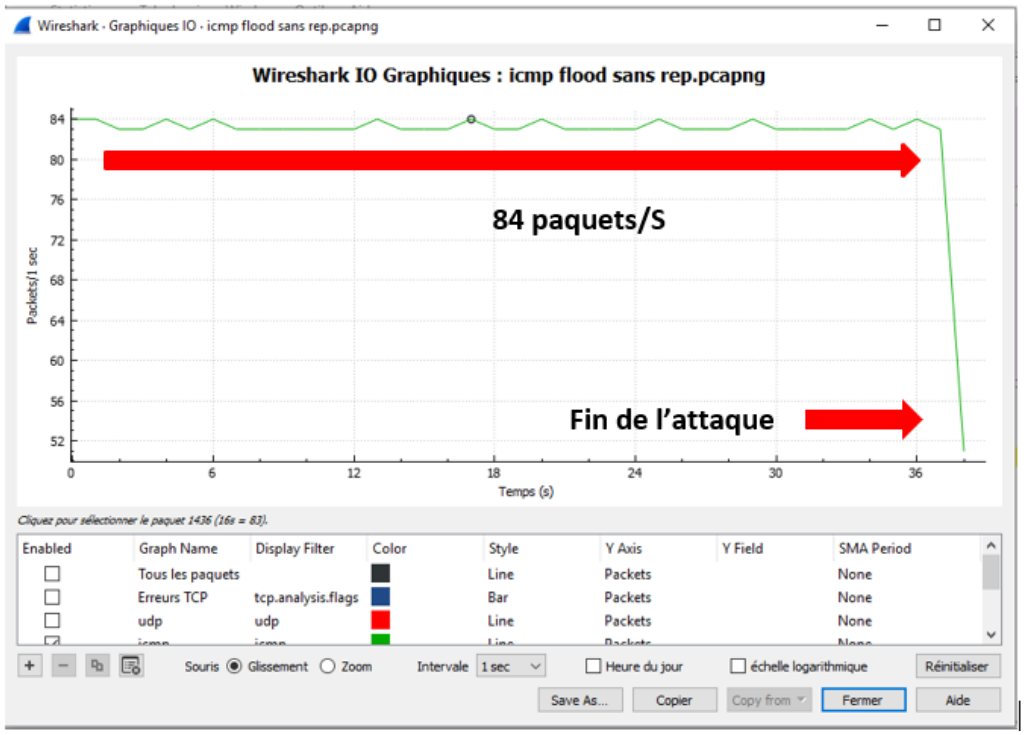


Figure 3-13. Nombre de paquets/S ICMP Flood.

3.6.2 Attaque Ping of death

Cette attaque est lancée sous Windows 10 en utilisant l'invite de commande on envoie un Ping d'une taille de 65500 octets en utilisant la commande suivante :

#ping 192.168.43.239 -t -l 65500

- Ping : pour envoyer une requête Ping.
- -t : pour effectuer un test ping.
- -l : identifie la taille du ping.

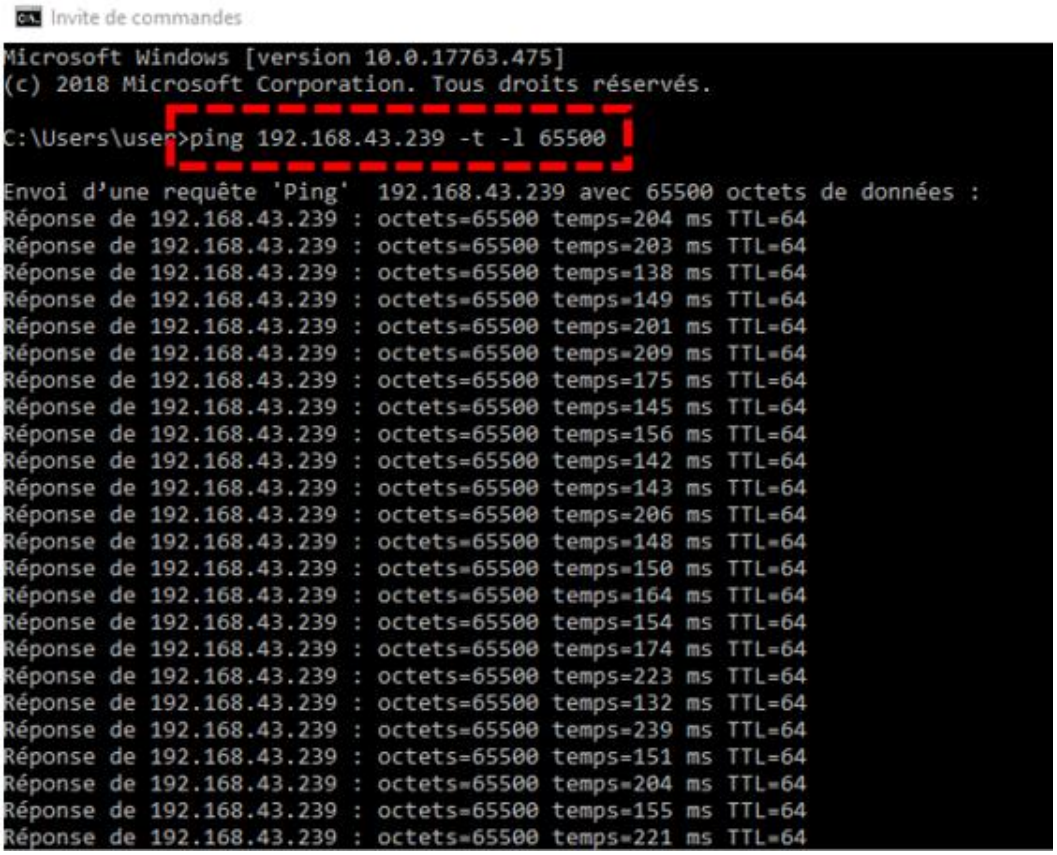


Figure 3-14. Attaque Ping of death.

a Analyse du paquet

Pendant que l'attaque est en cours, on analyse les paquets et on remarque la réception de plusieurs paquets ICMP request à partir de 192.168.43.78 avec une taille de 65500 octets.

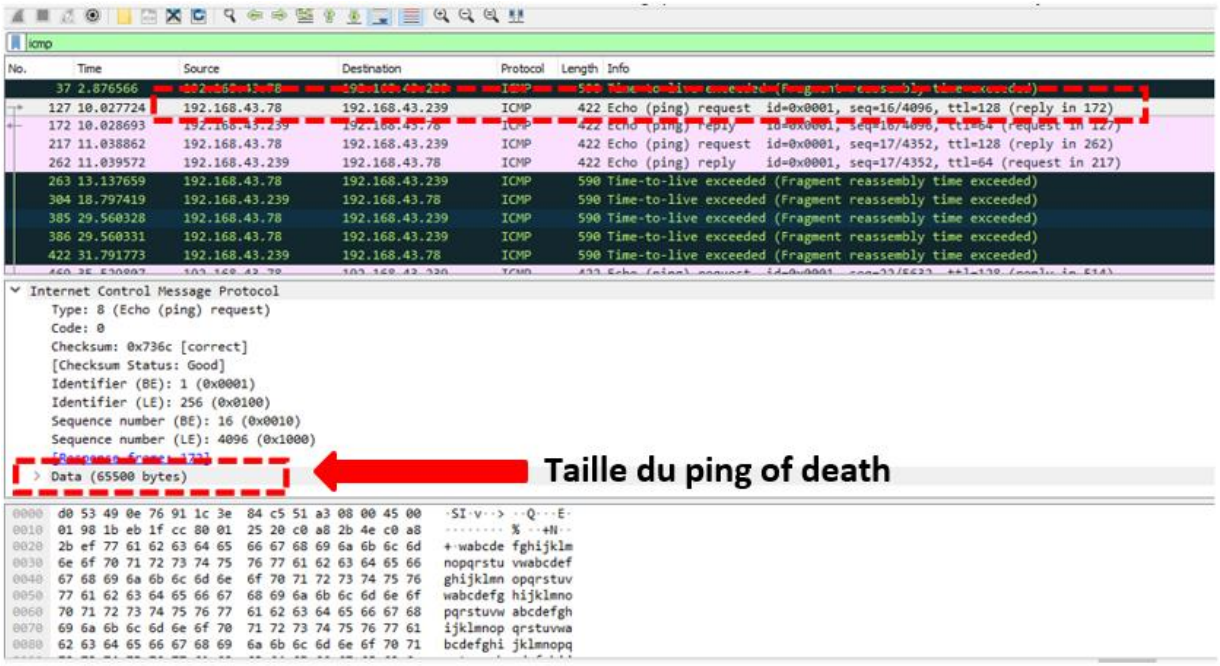


Figure 3-15. Taille ping of death.

3.7 ICMP

On envoie une requête ping du PC 1 vers le PC 2 puis on analyse les paquets, on remarque alors que la taille des paquets ICMP request reçus est 32 octets.

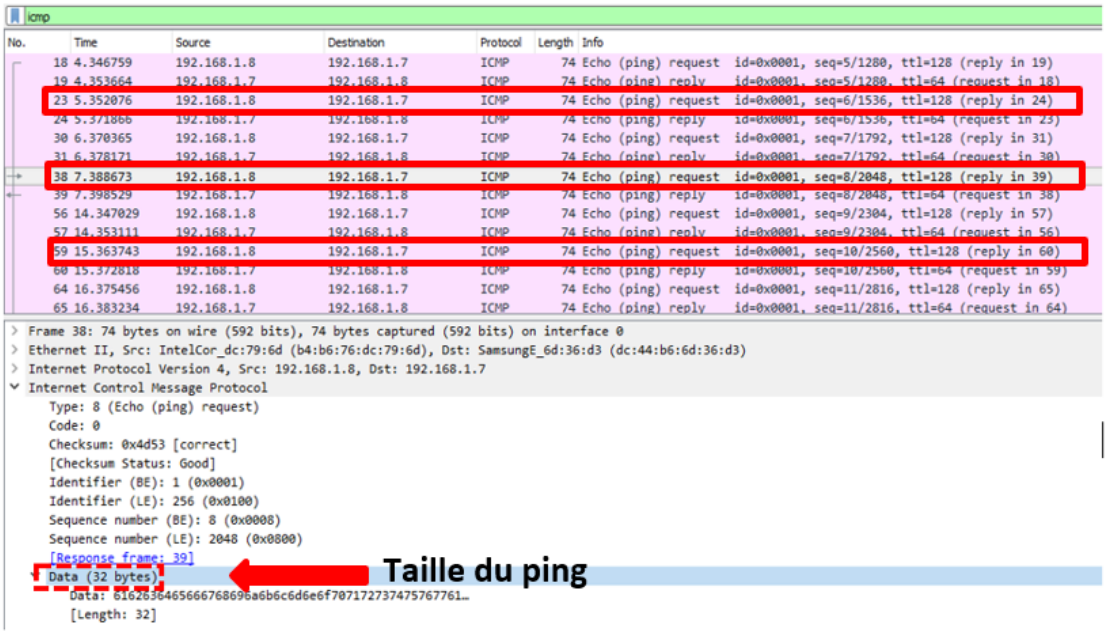


Figure 3-16. Taille ping normal.

Après avoir tracé le graphe qui affiche le nombre de paquets ICMP/S pendant 15 secondes dans le cas d'un ping normal on remarque que la valeur maximale est 2.

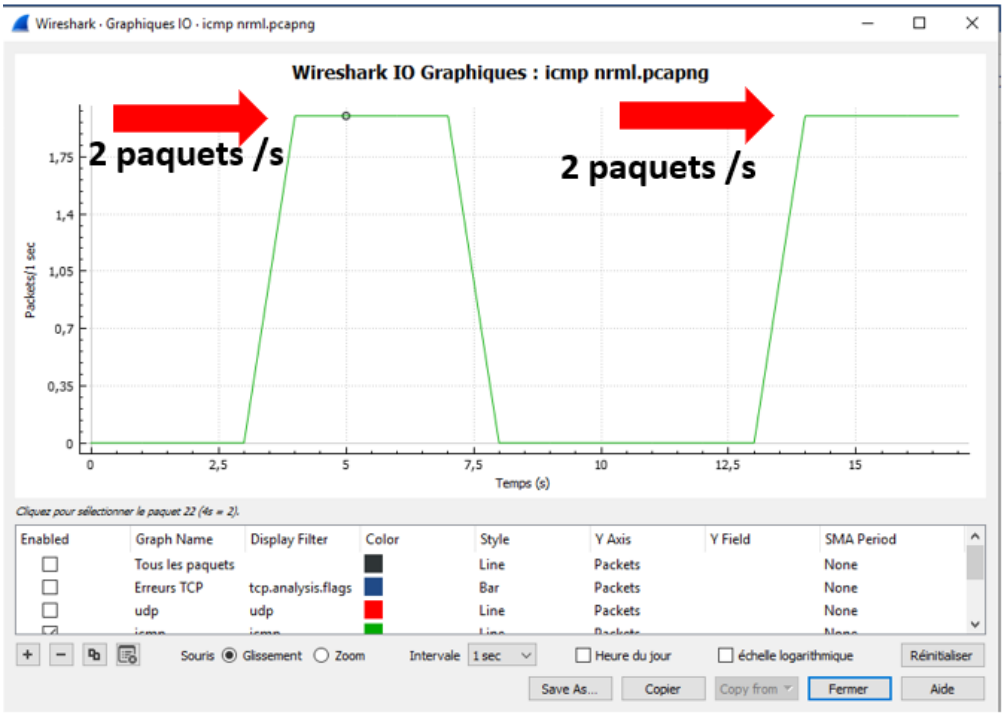


Figure 3-17. Nombre de paquets/S ICMP.

3.7.1 Signature ICMP

	ICMP normal	Attaque ICMP	Différence
Taille du paquet	Ping normal :32 Octets	Ping of death : 65500 octets	Taille du ping of death>ping normal
Nombre de paquets/S	2 paquets/S	ICMP Flood : Presque 84 paquets/S	Nombre de paquets/S dans l'attaque ICMP>paquet ICMP normal

Tableau 3-3. Signature ICMP.

3.8 Attaque TCP Flood

On va utiliser les outils suivants : Hping3, SYN-Flood Python, Xerxes, Slowloris,Pyloris et LOIC.

3.8.1 Hping3

L'avantage de Hping3 dans l'attaque TCP Flood c'est qu'il nous permet d'envoyer à la victime plusieurs flags, nous allons simuler les flags FIN et PSH.

a PSH

- Adresse IP de l'hacker usurpée : 192.168.43.48
- Formule utilisée : **#hping3 -P -i u10000 -a 192.168.43.48 192.168.43.239**

-P : définit le flag Push.

-i : définit l'intervalle de temps entre chaque attaque, (u) pour microsecondes.

-a : définit l'adresse source (l'adresse usurpée).

- Nombre de paquets envoyés : 3918.

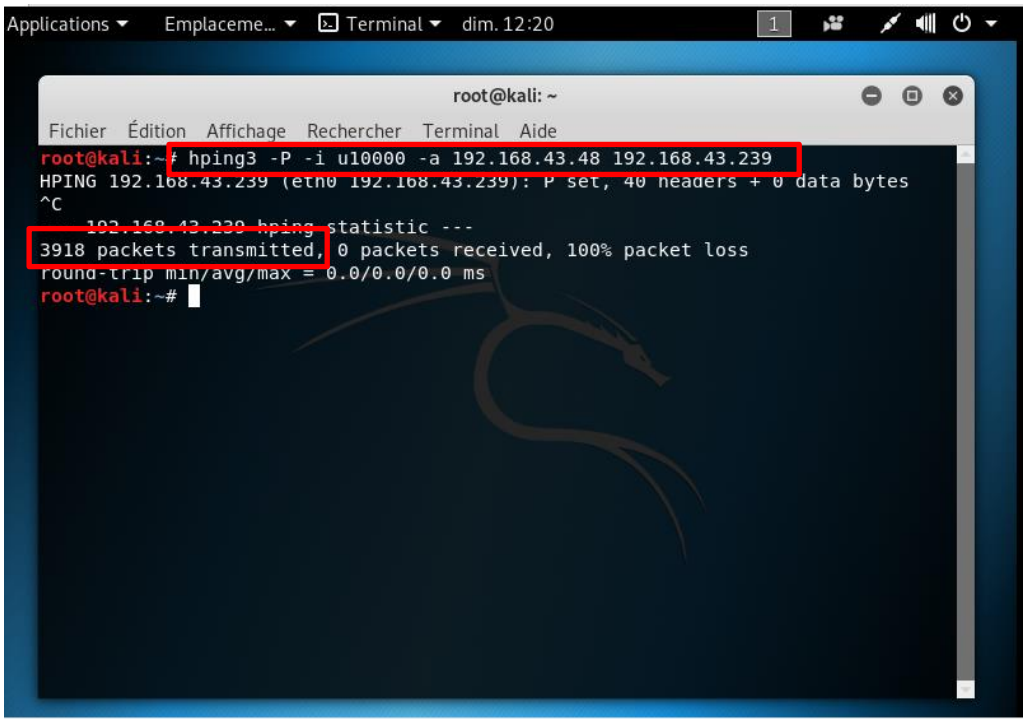


Figure 3-18. Attaque TCP Flood flag PSH

- **Analyse du paquet :**

Pendant que l'attaque est en cours on analyse les paquets et on remarque qu'il y'a un grand nombre de paquets TCP qui portent le flag PSH (PSH=1) et les autres flags = 0, à partir de l'adresse 192.168.43.48 (attaquant).

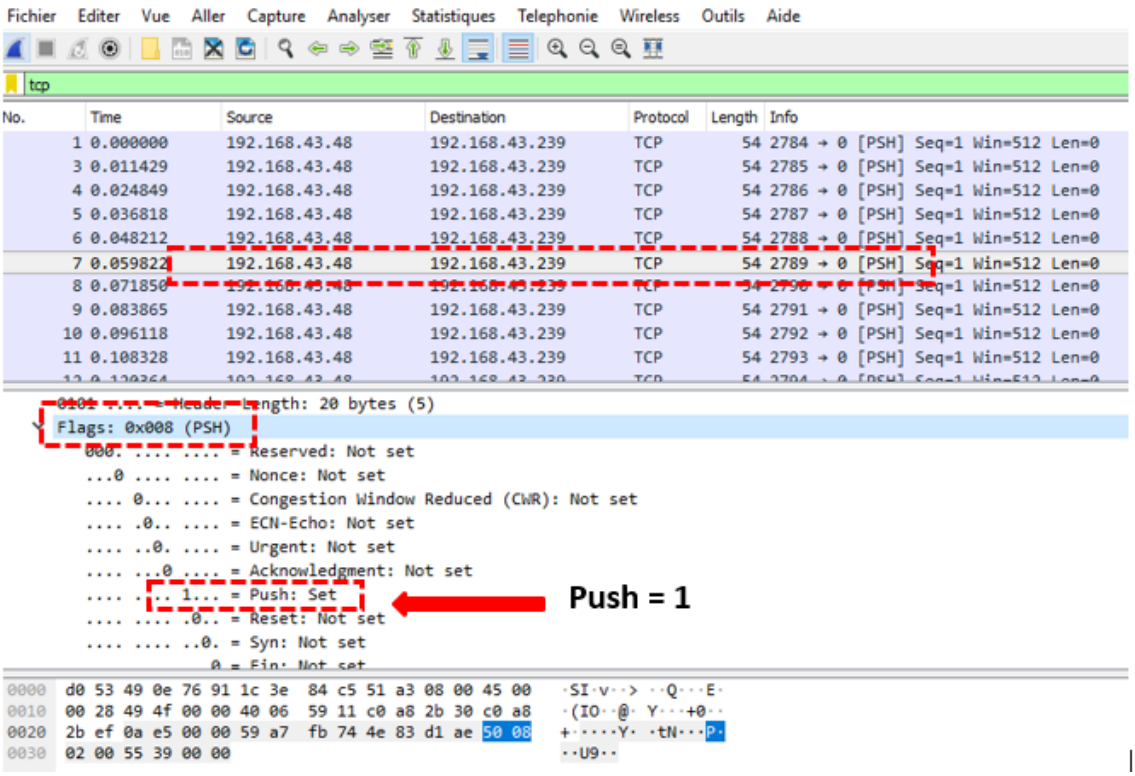


Figure 3-19. Analyse de paquets TCP Flood flag PSH.

b FIN

- Formule utilisée : **#hping3 -F -i u10000 -a 192.168.43.48 192.168.43.239**

-F : définit le flag FIN.

- Nombre de paquets envoyés : 4751 paquets.

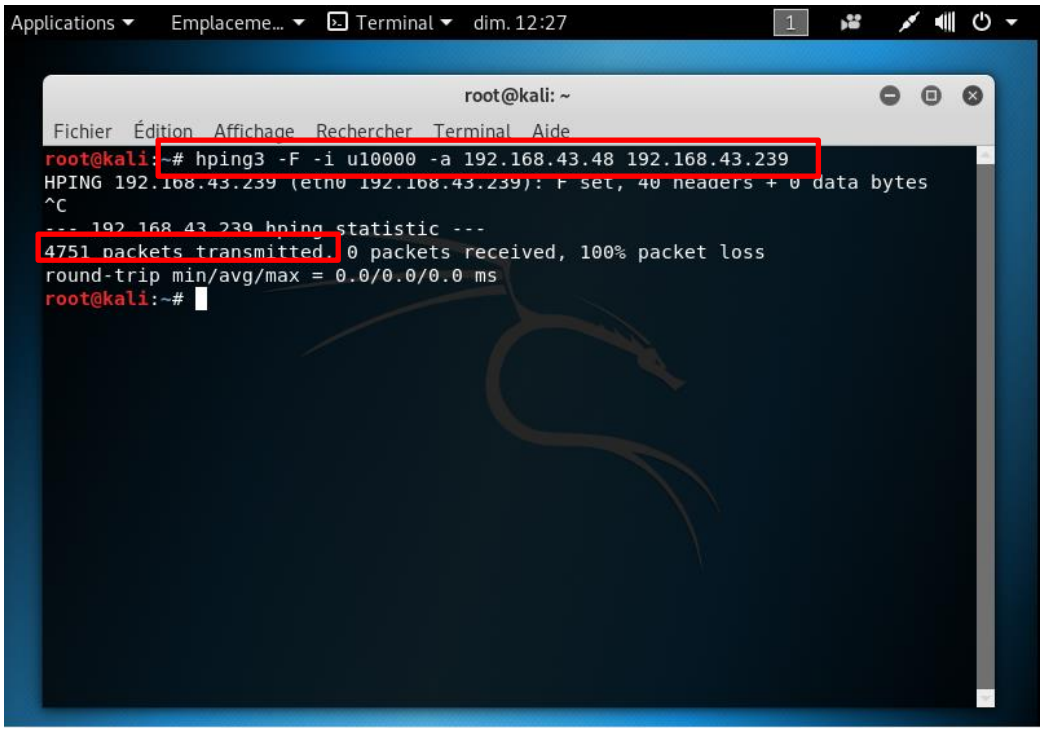


Figure 3-20. Attaque TCP Flood Flag FIN.

- **Analyse du paquet :**

Pendant l'analyse des paquets on remarque un grand nombre de paquets TCP avec le flag FIN (FIN=1) qui demande d'arrêter la connexion TCP alors qu'il n'y a pas une.

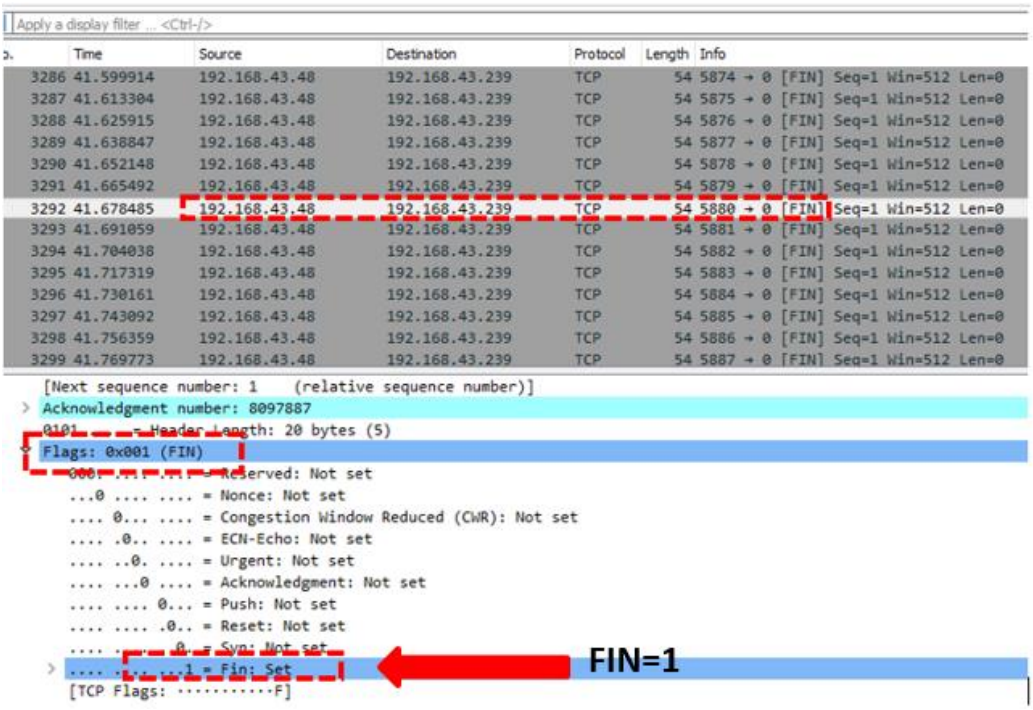


Figure 3-21. Analyse de paquets TCP Flood flag FIN

3.8.2 SYN-Flood Python

Pour lancer SYN-Flood Python on tape dans le terminal :

#python SYN-Flood

Après cela on nous demande d'introduire l'adresse IP de la victime, le port et le nombre de paquets qu'on veut envoyer.

(1) IP victime : 192.168.43.239

(2) Port :80.

(3) Nombre de paquets : 200.

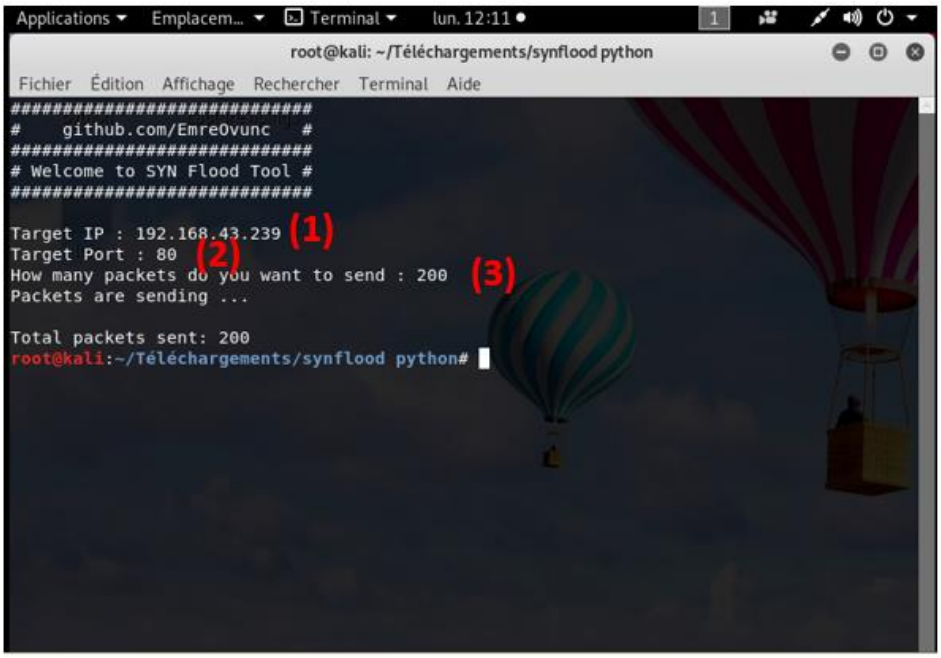


Figure 3-22. Attaque TCP Flood SYN-Flood Python.

- **Analyse du paquet :**

On remarque pendant l'analyse des paquets qu'il y'a plusieurs demandes de connexion TCP (flag SYN=1) provenant de plusieurs adresses IP, dans ce cas nous avons conclu que cet outil utilise l'usurpation des adresses IP.

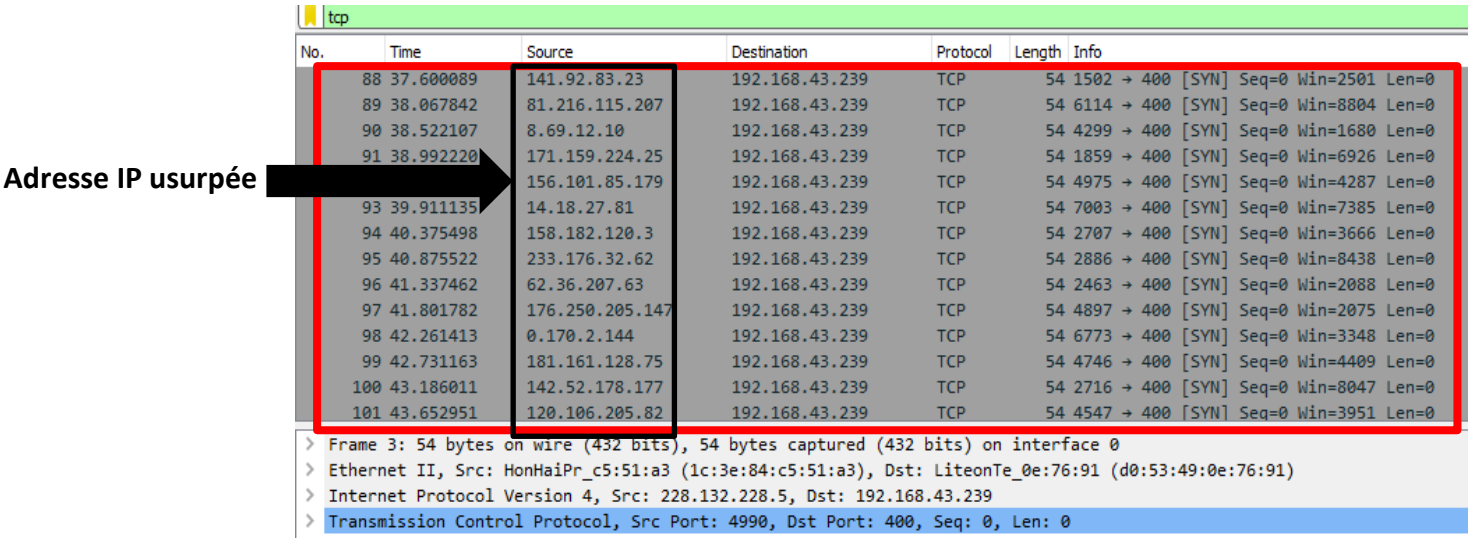


Figure 3-23. Analyse de paquets TCP Flood SYN-Flood Python.

Dans le graphe qui affiche le nombre de paquets TCP/S pendant 15 secondes on remarque que la valeur maximale est égale à 6 et que cette valeur alterne, ensuite elle diminue jusqu'à 2 et augmente à 6.

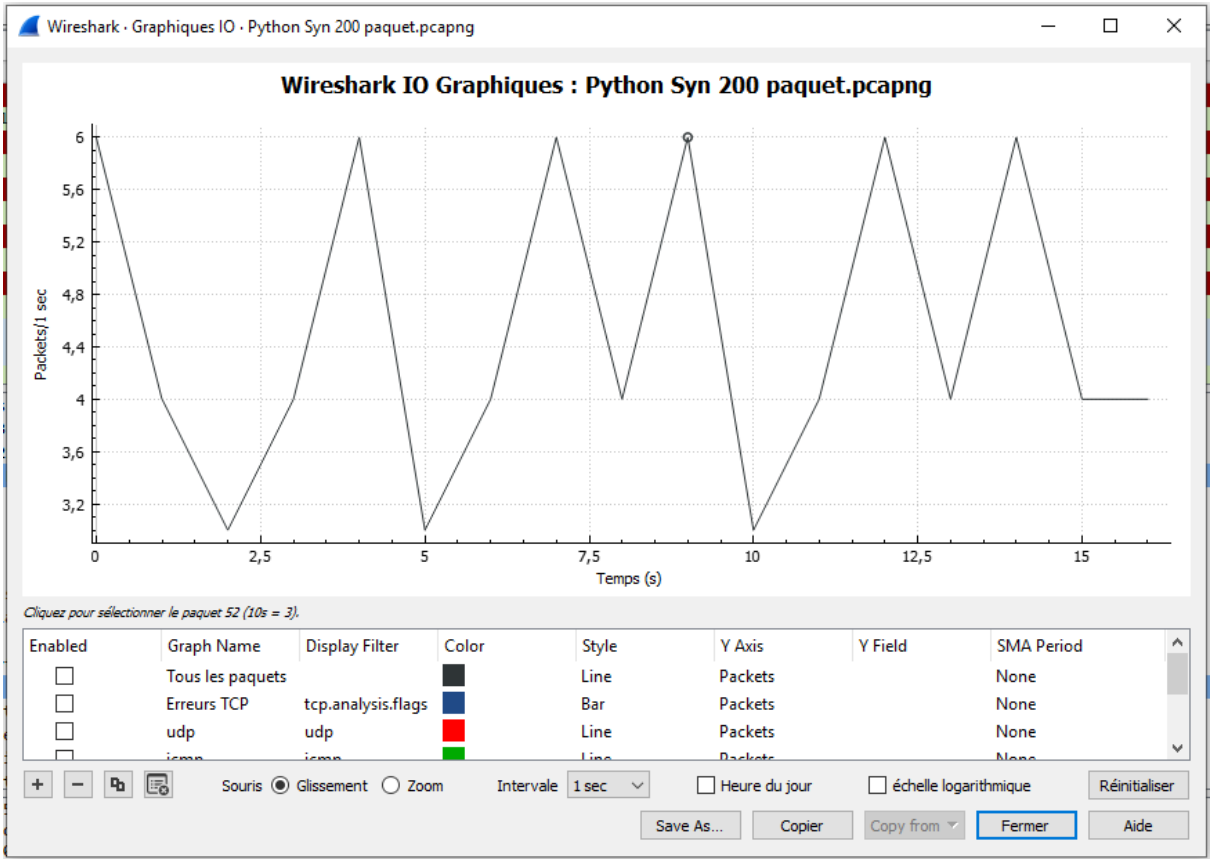


Figure 3-24. Nombre de paquets/S TCP Flood SYN-Flood Python.

3.8.3 LOIC

- Adresse IP victime : 192.168.43.239.
- Port : 80
- Protocole : TCP.

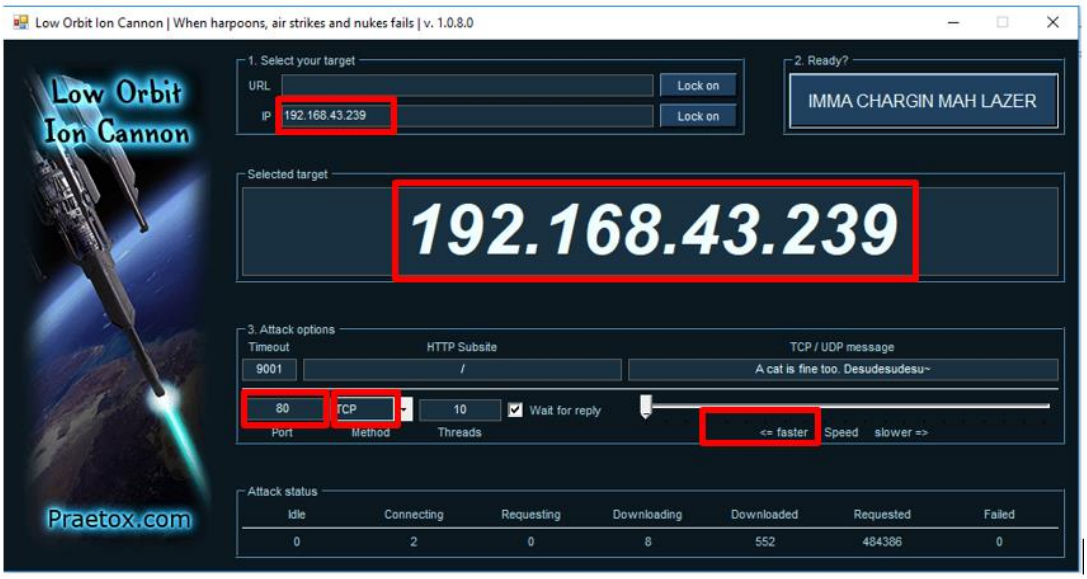


Figure 3-25. Attaque TCP Flood LOIC.

- **Analyse du paquet :**

On remarque pendant l'analyse qu'il y'a beaucoup de paquets TCP qui portent les deux flags PSH (PSH=1) qui indique à la victime de traiter les paquets envoyés et de ne pas attendre le remplissage de mémoire tampons et ACK (ACK=1) qui lui indique l'accusés de réception, ces paquets proviennent de l'adresse IP 192.168.43.19 (attaquant).

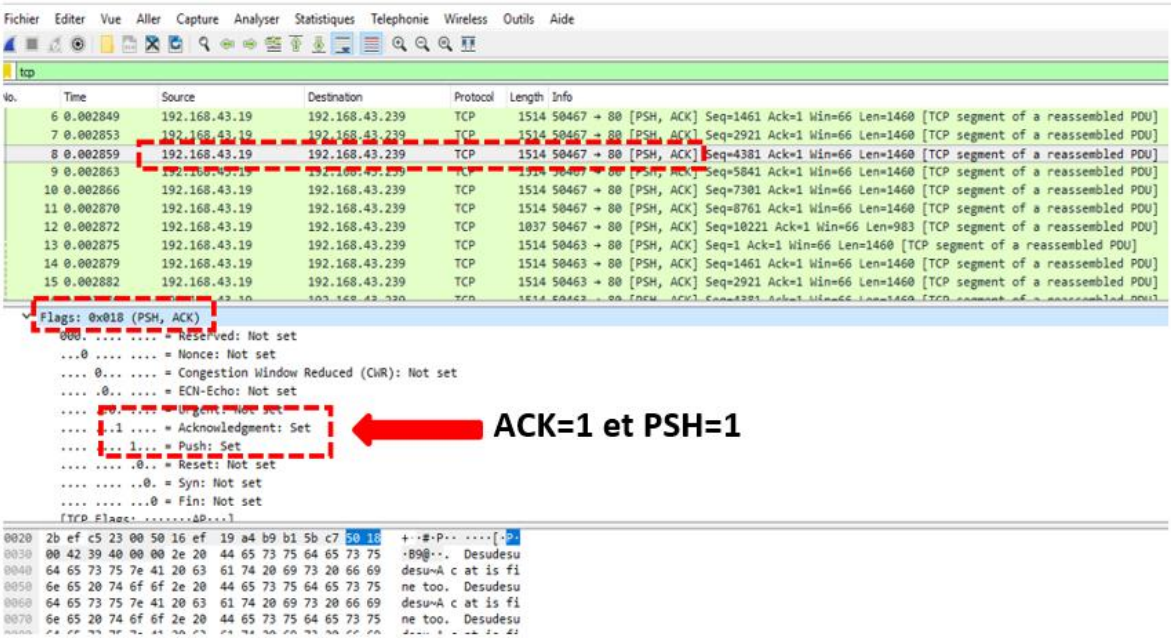


Figure 3-26. Analyse de paquets TCP Flood LOIC.

3.8.4 Slowloris

- Formule utilisée : **#perl Slowloris.pl -dns 192.168.43.239 -options**

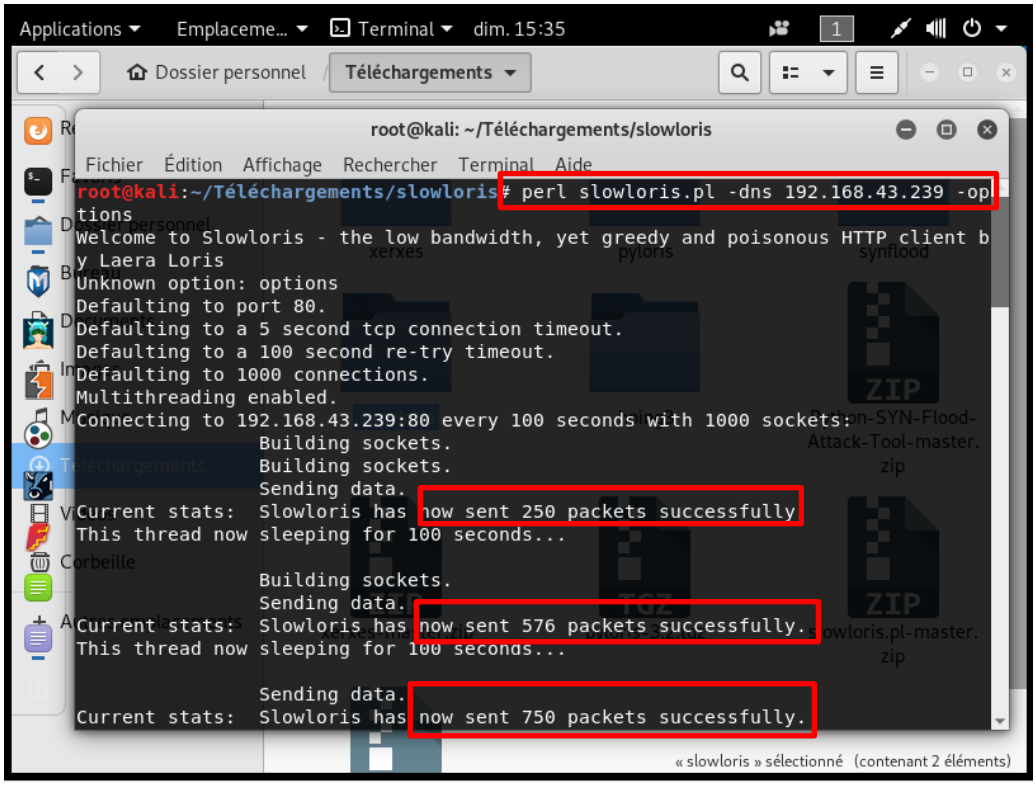


Figure 3-27. Attaque TCP Flood Slowloris.

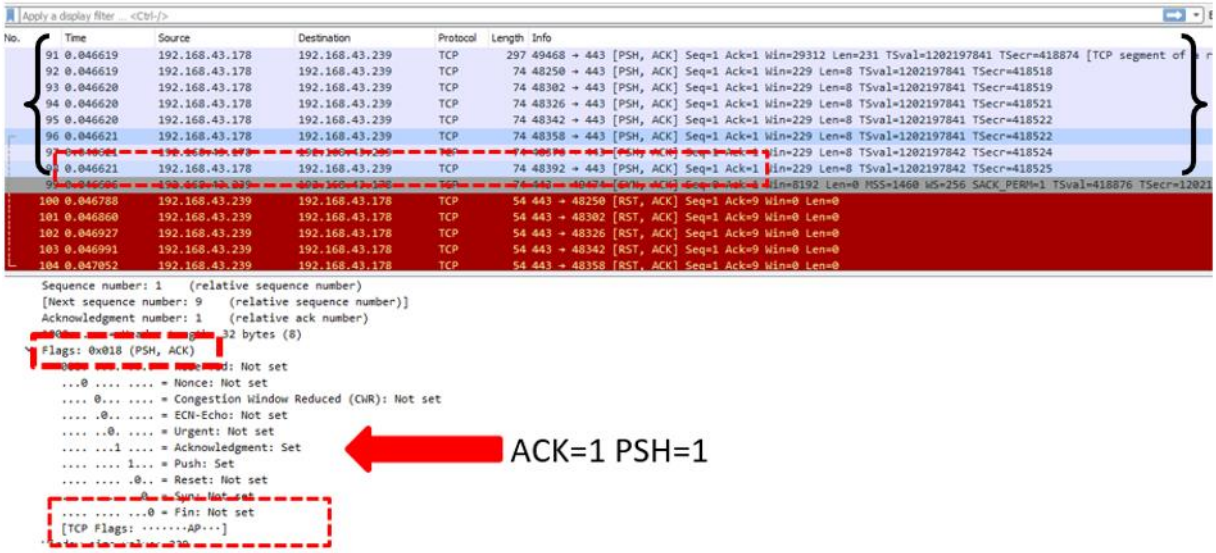


Figure 3-28. Analyse de paquets 1 TCP Flood Slowloris.

- **Analyse du paquet :**

Pendant l'analyse on remarque la réception d'une quantité importante de paquets TCP qui portent les flags ACK(ACK=1) qui signifie une réponse à SYN=1 alors qu'il n'y a pas eu de connexion avant, et d'autres paquets avec les flags PSK et ACK (ACK=1+PSH=1) à partir de l'adresse 192.168.43.78 (attaquant), la réception des paquets s'arrête dès que l'attaque est terminée.

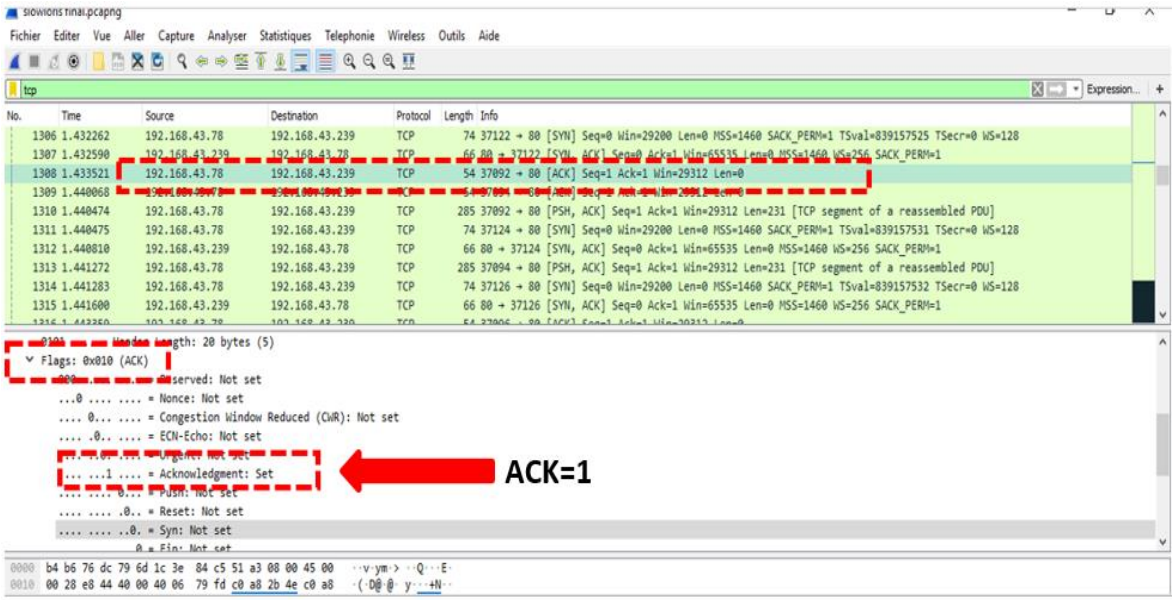


Figure 3-29. Analyse de paquets 2 TCP Flood Slowloris.

3.8.5 Pyloris

Pour lancer l'outil Pyloris on tape la commande suivante dans le terminal :

#python Pyloris.py

Après cela la fenêtre suivante s'ouvre :

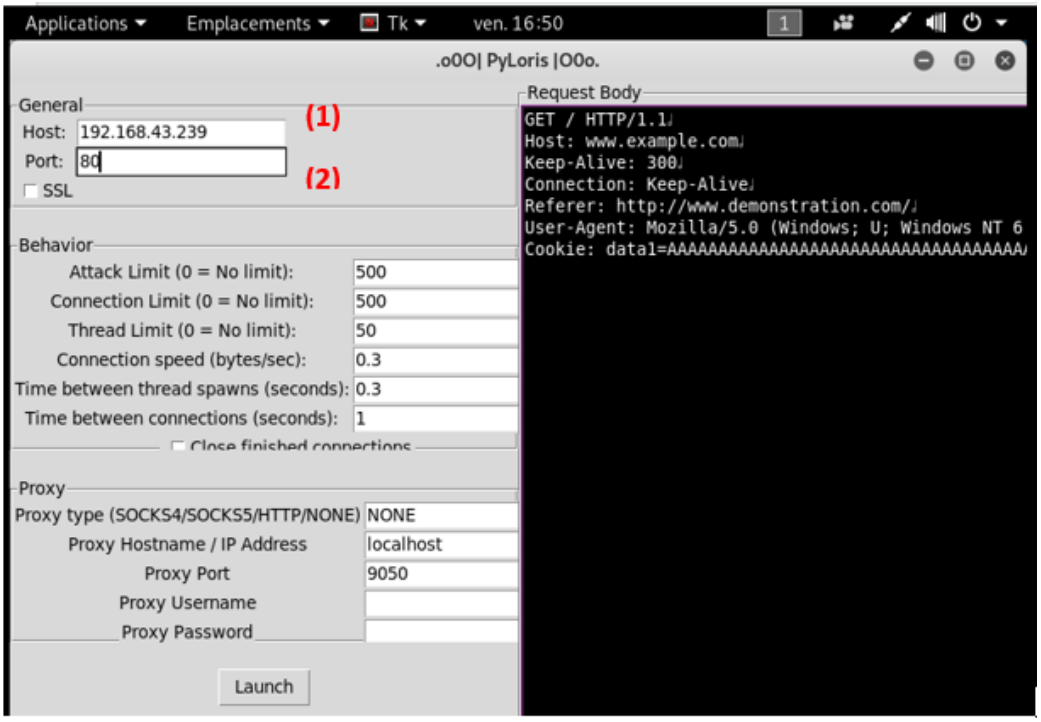


Figure 3-30. Démarrage Pyloris.

(1) Adresse IP victime : 192.168.43.239

(2) Port : 80.

On introduit l'adresse IP de la victime dans la case 1 et le port dans la case 2 ensuite on clique sur Launch.

Ensuite pour arrêter l'attaque on clique sur « Stop Attack ».

- Nombre d'attaques lancées : 79.

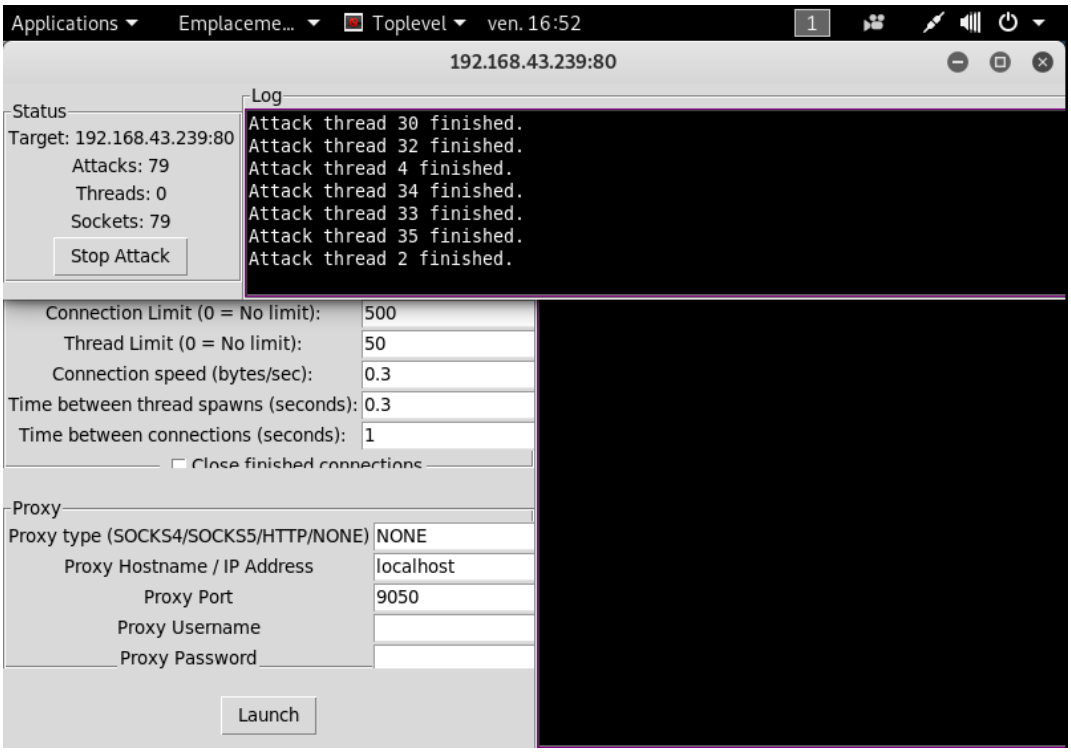


Figure 3-31. Attaque TCP Flood Pyloris.

- **Analyse du paquet :**

Pendant l'attaque on remarque la réception d'une quantité importante de paquets TCP, il y'a ceux qui portent le flag SYN (SYN=1) pour faire une demande connexion, ces paquets proviennent de l'adresse 192.168.43.78 (attaquant).

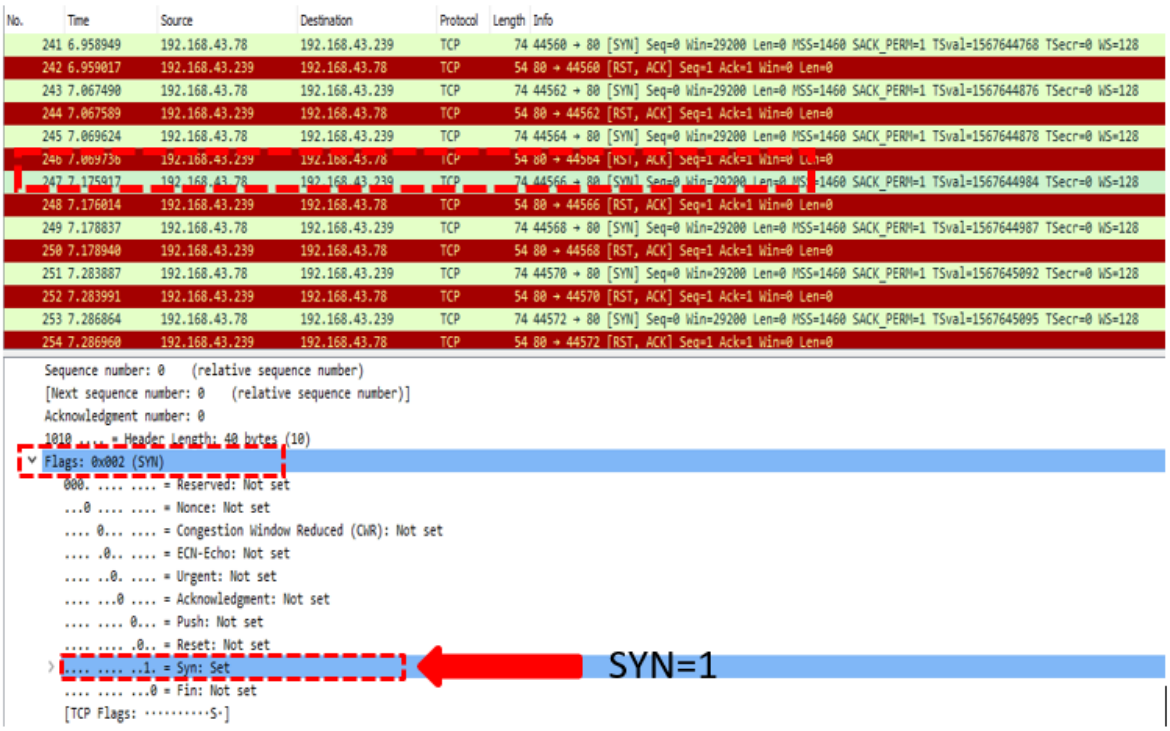


Figure 3-32. *Analyse de paquets TCP Flood Pyloris.*

3.8.6 Xerxès

- Commande démarrage : **#gcc xerxes.c -o xerxes.**
- Formule utilisée **: # ./xerxes 192.168.43.239 80**

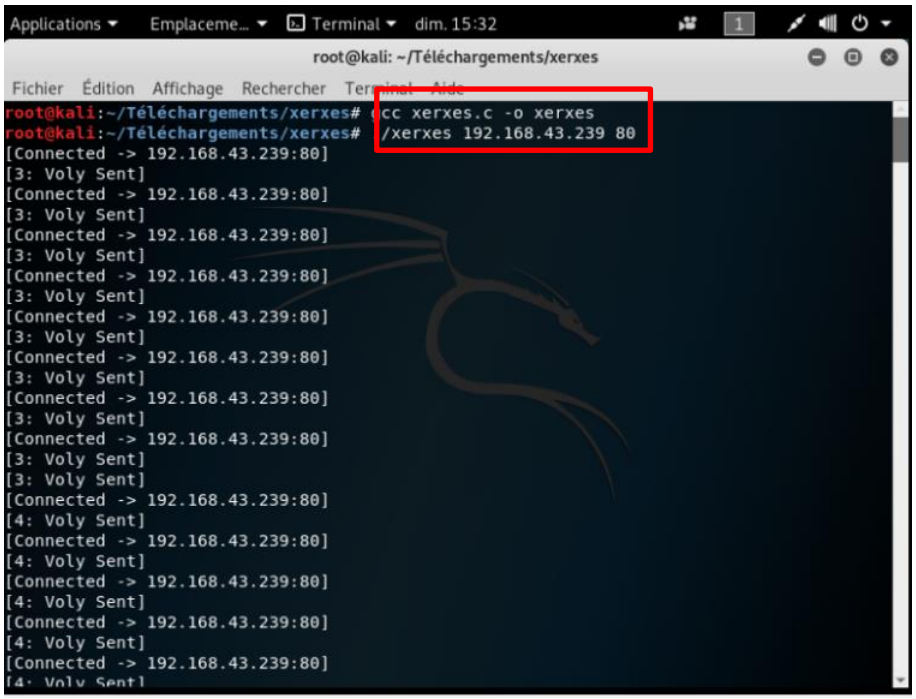


Figure 3-33. Attaque TCP Flood Xerxes.

- **Analyse du paquet :**

Pendant l'attaque on analyse les paquets et on remarque la réception de beaucoup de paquets TCP qui portent les flags ACK et PSH (ACK=1+PSH=1) à partir de l'adresse 192.168.43.78 pour indique à la victime de traiter les paquets envoyés et de ne pas attendre le remplissage de mémoire tampons ainsi qu'un accusé de réception d'une connexion qui n'a pas eu lieu au paravent.

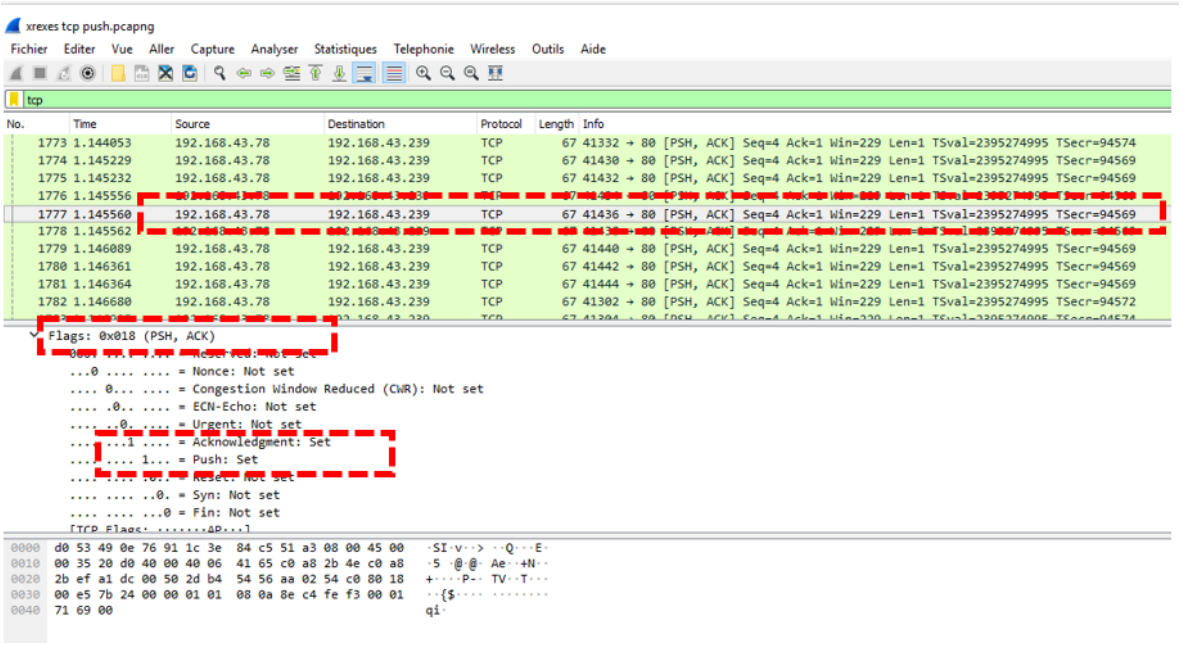


Figure 3-34. Analyse de paquets TCP Flood Xerxes

3.9 TCP

On analyse les paquets TCP qui transitent entre le PC1 et le PC2 et on remarque que ces paquets portent le flag ACK (ACK=1), et les autres flags sont égale à 0, SYN=0, PSH=0, FIN=0.

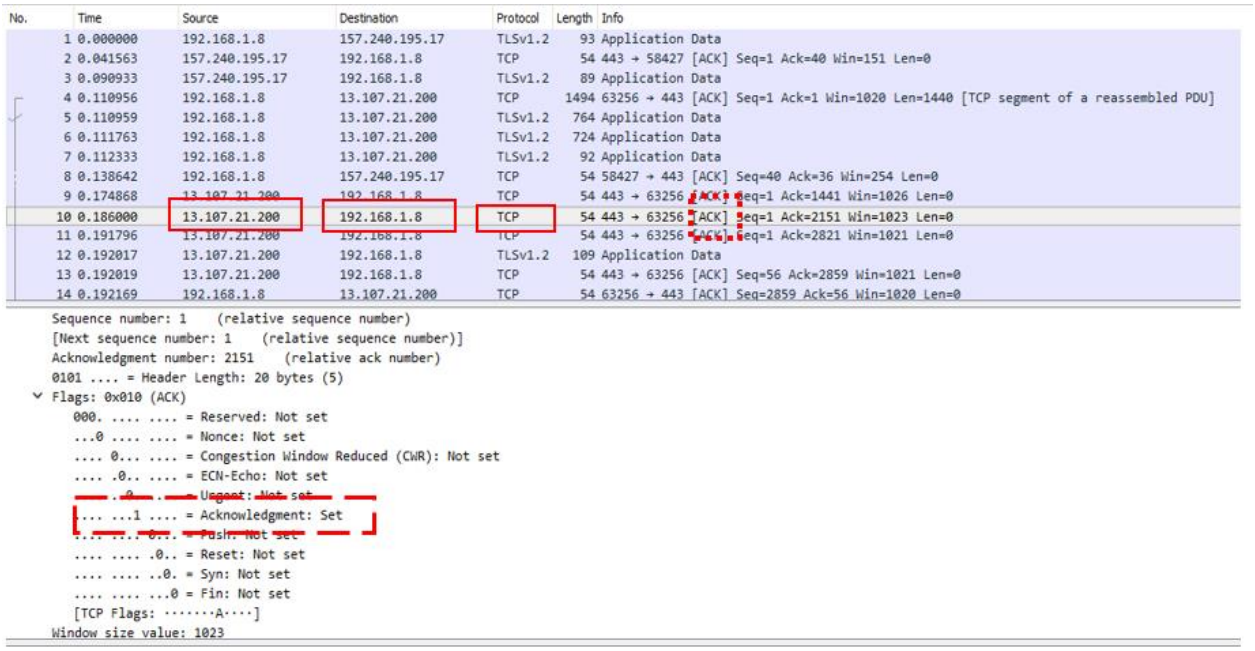


Figure 3-35. Analyse de paquets TCP.

Dans le graphe qui affiche le nombre de paquets TCP/S qui transitent dans le réseau pendant 1 minute on remarque que la valeur varie de 10 à 60 et peut atteindre les 100 paquets/S.

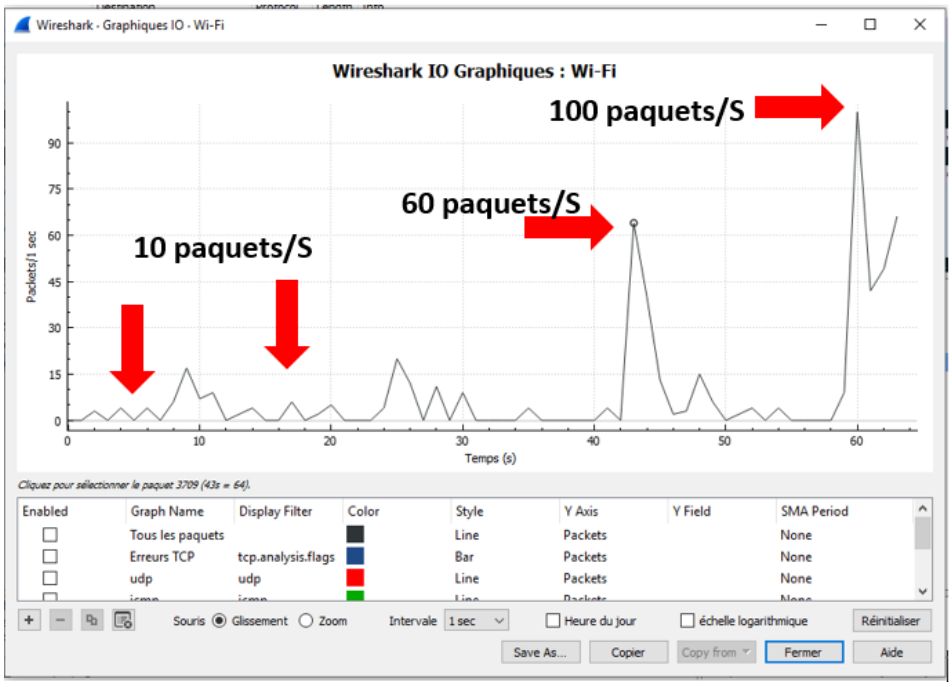


Figure 3-36. Nombre de paquets/S TCP.

3.9.1 Signature TCP

	Paquet normal	Attaque TCP	Différence
Nombre de paquets/S	Ne dépasse pas 100 paquets/S pendant 1 min.	>9000 paquets/s pour Hping3. 4000 paquets/s pour LOIC.	L'attaque TCP peut atteindre une valeur > 9000 paquets/S dans une courte durée alors que dans le cas d'un paquet TCP normal la valeur maximale pendant 1 min est 100.
Les flags	Flag PSH=0 Flag FIN=0 Flag SYN=0 Flag ACK=1	• PSH=1 et ACK=1 pour LOIC, Xerxes et Slowloris. • Hping3 selon la formule. • SYN=1 pour SYN-Flood Python et Pyloris.	Les flag Push et ACK sont positionnées (PSH=1+CK=1). Le Flag SYN est positionné (SYN=1).

Tableau 3-4. Signature TCP.

3.10 Attaque http Flood

On va simuler cette attaque avec l'outil LOIC.

- Adresse IP victime : 192.168.43.239.
- Port :80.
- Protocole : http.

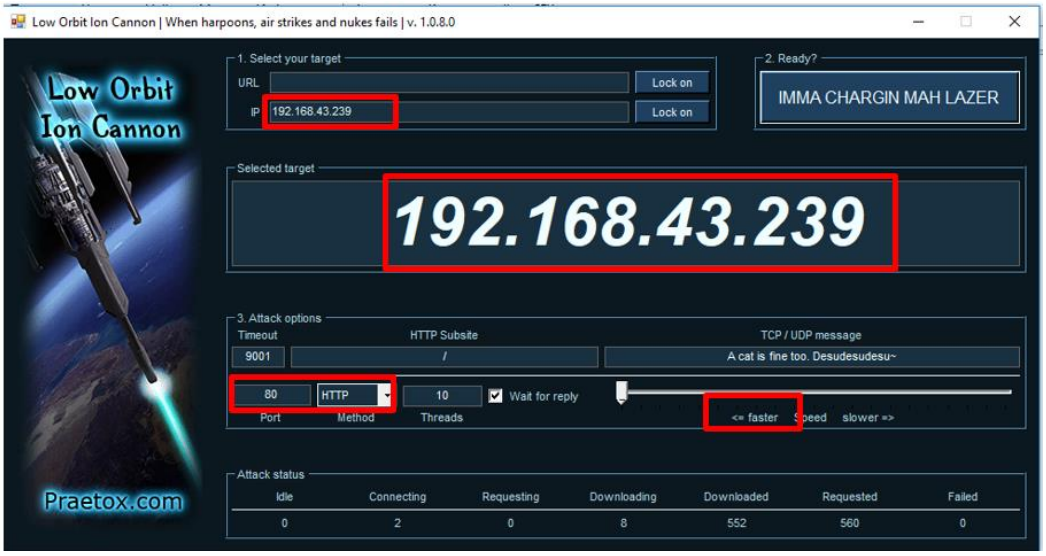


Figure 3-37. Attaque http Flood LOIC.

- **Analyse du paquet :**

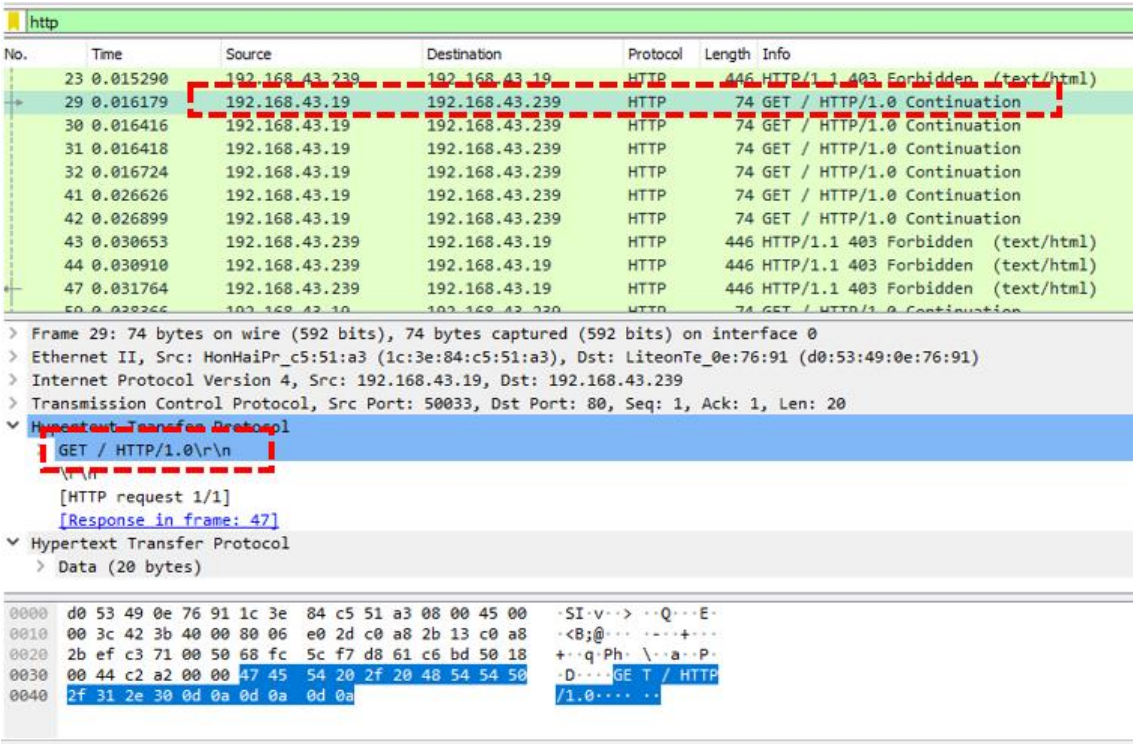


Figure 3-38. Analyse de paquets http Flood LOIC.

Pendant l'attaque on analyse les paquets et on remarque la présence de paquets http sous la forme **GET/http/1.0\r\n**, ces paquets proviennent de l'adresse 192.168.43.19 (attaquant).

3.11 Http

Pour capturer les paquets http on visite le site www.google.fr et on capture les paquets au même temps.

Pendant l'analyse on remarque que les paquets http sont sous la forme suivante : **http/1.1 200 OK\r\n** et proviennent de plusieurs adresses IP.

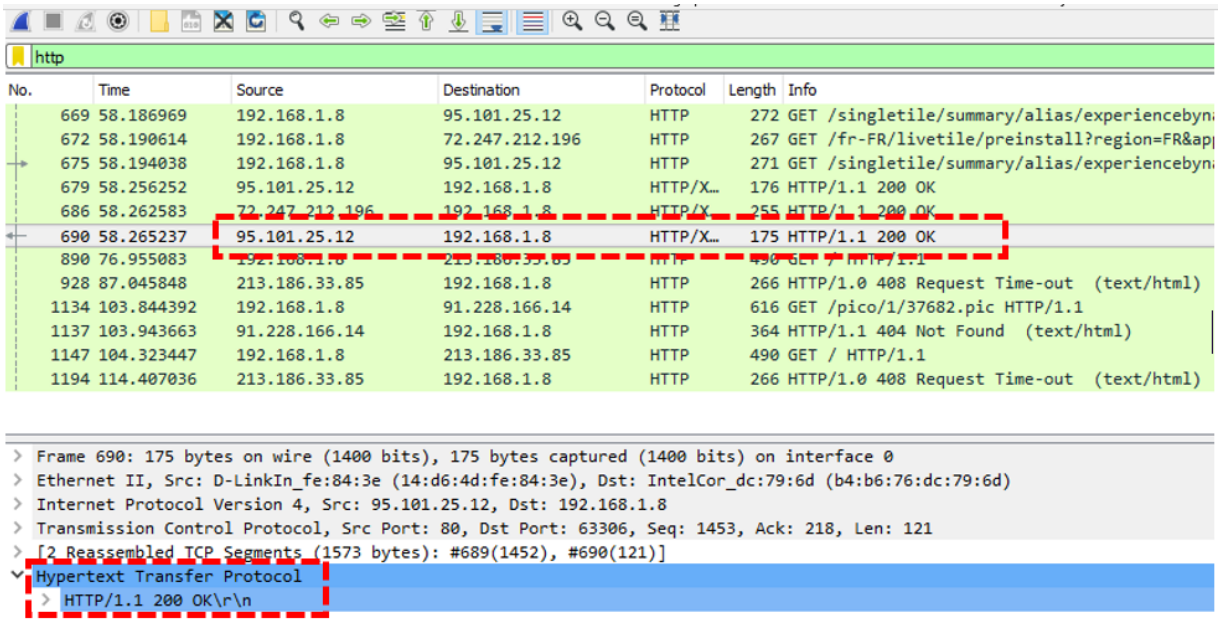


Figure 3-39. Analyse de paquets http.

3.11.1 Signature http

	Paquet http normal	Attaque Http	Différence
Formule de la requête HTTP	Http/1.1 200 OK\r\n	GET/http/1.0\r\n	Malformation

Tableau 3-5. Signature http.

Conclusion

Dans ce chapitre on a pu terminer le premier volet de notre travail, nous avons simulé plusieurs attaques DOS ensuite analysé leur trafic et obtenu leurs signatures grâce à une comparaison entre les paquets des attaques et les paquets du cas normal, cette partie nous a pris beaucoup de temps vu qu'on a eu quelques difficultés parmi eux la disponibilité des outils d'attaques et leur lancement sous Windows qui a échoué dans nos premiers tests, ce qui nous a mené à travailler sous Kali Linux.

Cette étude va nous permettre d'écrire nos propres règles de détection sous IDS Snort et tester leur efficacité dans le prochain chapitre.

4.1 Introduction

Il est nécessaire de nos jours de protéger les réseaux et les systèmes informatiques et de détecter les attaques avant qu'elles ne puissent causer des dommages, la meilleure façon de protéger ces systèmes d'information est de mettre en place un système de détection d'intrusion.

Le système de détection d'intrusion le plus répandue et qui prend une part importante dans la sécurité des systèmes d'information actuels est Snort.

Au cours de ce chapitre, nous allons découvrir ce système de détection d'intrusion réseau (NIDS), ainsi que les paramétrages nécessaires pour son fonctionnement.

Dans ce qui suit, nous allons créer des nouvelles règles de détection à base de signature obtenues au chapitre précédent. Enfin, nous testerons la fiabilité de notre solution en lançant les attaques vues déjà dans le but de suivre son comportement.

4.2 Les démarches suivis

Au cours de cette expérience, nous intéressons à :

- Comprendre le rôle de Snort dans la sécurité des réseaux.
- Effectuer les configurations nécessaires pour le bon fonctionnement de Snort.
- Ecrire de nouvelles règles de détection à base de signatures obtenue dans le chapitre précédent qui sont résumées dans le tableau ci-dessus.
- Effectuer des tests avec Snort en utilisant un mécanisme (BASE) capable d'afficher les alertes remontées par Snort.

Attaque	Signature
UDP Flood avec LOIC	Nombre de paquets/S > 250
ICMP Flood avec Hping3	Nombre de paquets/S≤84
Ping of death	Taille du ping > 32 octets
TCP Flood avec Hping3	Flags=FIN(FIN=1) et PSH(PSH=1)
TCP Flood avec SYN-Flood Python	Flags=SYN(SYN=1) et nombre de paquets/S≤ 6
TCP Flood avec LOIC	Flags=PA (PSH=1 et ACK=1)
TCP Flood avec Slowloris	Flags=PA (PSH=1 et ACK=1) et A (ACK=1)
TCP Flood avec Pyloris	Flags=SYN (SYN=1)
TCP Flood avec Xerxes	Flags=PA (PSH=1 et ACK=1)
Http Flood avec LOIC	Forme http = GET/http/1.0\r\n

Tableau 4-1. Signatures des attaques.

4.2.1 Schéma de travail

Dans notre expérience, nous allons utiliser deux machines, la première est utilisée comme un PC attaquant pour lancer les attaques. La deuxième machine (PC Victime) sur laquelle nous avons mis en place le logiciel Snort et les services nécessaires à son bon fonctionnement (**Apache, MySQL, PHP, BASE).**

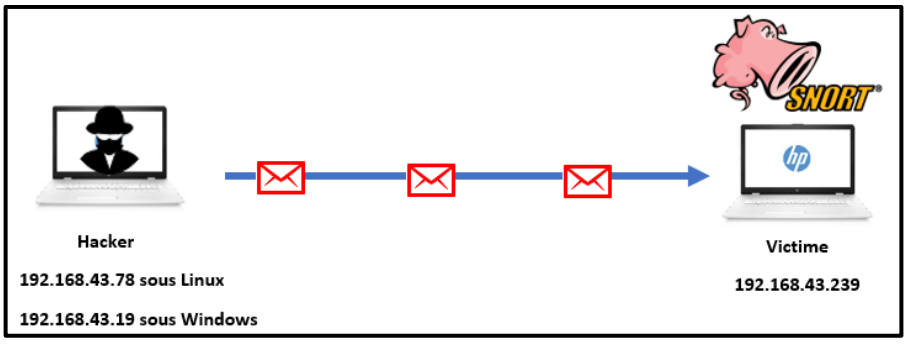


Figure 4-1. Schéma utilisé durant l'expérience.

4.2.2 Description des stations

		Fonction	Services	Système d'exploitation
PC1	Attaquant	Logiciel d'attaque	Hping3, LOIC, Pyloris, Python, Xerxés, Slowloris, SYN-Flood Python.	Linux, LOIC sous Windows 7.
PC2	Victime	Snort	Apache, MySQL, PHP, BASE	Windows 7

Tableau 4-2. Description des stations.

4.3 Configuration de Snort

Pour la configuration de Snort, nous avons édité le fichier **snort.conf** qui se trouve au niveau du répertoire ***C:\snort\etc\snort.conf*.**

Nous avons uniquement modifié la première partie du fichier qui contient les variables réseaux. Voici les modifications que nous avons apportées dans ce fichier :

- **var HOME_NET any** : indique l'adresse de l'interface réseau qui écoute le trafic, la valeur par défaut est **any.**
- **var EXTERNAL_NET any** : indique le réseau externe à « écouter », la valeur par défaut est **any**, ce qui signifie que le trafic venant de n' importe quel réseau est analysé.

Dans notre cas, on a attribué l'adresse IP de notre machine : **192.168.43.239**

```
19
20  ##################################################
21  # Step #1: Set the network variables.  For more information, see README.variables
22  ##################################################
23
24  # Setup the network addresses you are protecting
25  var HOME_NET 192.168.43.239/24
26
27  # Set up the external network addresses.  A good start may be "any"
28  var EXTERNAL_NET
```

***Figure* 4-2.** Modification de l'adresse de l'interface réseau .

Le fichier **snort.conf** est bien configuré, on peut maintenant entamer la création des règles.

4.4 Création des règles pour la détection des attaques

Dans le fichier local qui se trouve au niveau de **c : snort1/etc/snort/rules/local.rules**. On doit créer nos propres règles pour déclencher des alertes dès qu'une intention malveillante ou un comportement anormal ressemble à une attaque DOS arrive dans le réseau.

Les signatures élaborées lors de l'analyse des attaques, seront implémentées dans Snort pour détecter ces attaques.

4.4.1 Attaque UDP Flood

a Règle de détection d'attaque UDP Flood lancé par l'outil Hping3

Figure 4-3. La règle de détection UDP Flood avec Hping3.

La règle suivante va remonter une alerte de message « attaque UDP_ Hping » lorsqu'il y a une tentative d'accès par un nombre de paquet UDP qui dépasse 235 paquets/s de n'importe quelle adresse (any) et n'importe quel port (any).

b **Règle de détection de l'attaque UDP Flood lancé par LOIC :**

Figure 4-4. Règle de détection d'attaque UDP Flood avec LOIC.

Cette règle de détection de l'attaque UDP Flood, permet au système de détection d'intrusion Snort de mettre en état une alerte de message « attaque udp loic » si cette machine reçoit une quantité importante de paquets (>300 paquets/s) de type UDP.

4.4.2 Attaque ICMP

a Règle de détection de l'attaque ICMP Flood lancé par l'outil Hping3

```
# LOCAL RULES
#alert icmp any any -> any any (msg:" attaque Ping Flood"; threshold:type threshold , track by_src, count 100 , seconds 2
; sid:100000003 ;rev:1 ;)
```

Figure4-5. Règle de détection d'attaque ICMP Flood.

D'après la signature d'attaque ICMP Flood obtenue dans le chapitre précédent, nous avons créé une règle de détection qui permet à Snort d'analyser les paquets ICMP de toutes les adresses IP source et de générer des alertes avec un message « attaque Ping Flood » si la machine victime recevrait un nombre élevé de paquets ICMP request (dépasse le 100 paquets/s).

b Règle de detection de l'attaque Ping of death

```
20  # LOCAL RULES
21  #alert icmp any any -> any any (msg:"attaque ping of death"; disize> 1000; itype:8; icode:0; sid:10000002; rev:1;)
```

Figure 4-6. Règle de détection d'attaque Ping of death.

Cette règle permet à Snort de détecter tous les pings (requests) vers la cible. Dans notre cas, les critères de ces paquets sont :

- Paquets de type ICMP.
- Provenant de n'importe quelle source, et de n'importe quel port, à destination de la cible.
- Paquets de taille supérieure à 65 octets.
- Paquets de type 8 et de code 0.

Grâce à cette règle, Snort détecte tous les paquets correspondant aux critères précités avec le message « ping of death detected ».

4.4.3 Attaque TCP Flood

On va créer les règles de détection d'attaque TCP Flood lancée par les outils : Hping3, SYN-Flood Python, Xerxès, Slowloris, Pyloris et LOIC.

Ces règles se caractérisent par :

- Les messages d'alerte qui doivent être affichés.
- Les déférents états de flags (SYN, PSH, FIN ou PSH/ACK).
- Le nombre de paquets qu'il ne faut pas dépasser.
- Le temps nécessaire pour générer l'attaque.
- L'identifiant de notre signature dans la base de signature (Sid).
- Le motif dans la charge d'un paquet (content).

a Règle de détection de l'attaque TCP (flag : PSH) lancé par Hping3 :

```
# LOCAL RULES
#alert tcp any any -> any any (msg:" attaque tcp hping_p "; flags:p ; threshold:type threshold , track by_src, count 200 ,
seconds 2 ; sid:10000010 ;rev:1 ;)
```

Figure 4.7. Règle de détection d'attaque TCP Flood avec Hping3 (flag : p)**.**

À l'aide des signatures conçues lors de l'analyse, nous avons défini nos règles de détection de l'attaque TCP Hping3 identifié par le paquet dont le flag PUSH est positionné (flags :P) et un count de 200 paquets/s.

b Règle de détection de l'attaque TCP (flag : FIN) lancé par Hping3

```
# LOCAL RULES
#alert tcp any any -> any any (msg:" attaque tcp hping_f "; flags:f ; threshold:type threshold , track by_src, count 200 ,
seconds 2 ; sid:10000009 ;rev:1 ;)
```

Figure 4-8. Règle de détection d'attaque TCP Flood avec Hping3 (flag : F).

Cette règle est identifiée par un nombre d'occurrences de 200 paquets provoquant une alerte, un intervalle de temps de 2s et paquets dont le flag FIN est positionné (flags : F) avec le message d'affichage « attaque tcp hping _f ».

c Règle de détection de l'attaque SYN-Flood lancé par SYN-Flood Python

```
# LOCAL RULES
#alert tcp any any  -> any any (msg:"attaque SynFlood_Python"; flags:s ; threshold:type threshold , track by_src, count 50,
seconds 20 ; sid:100000008 ;rev:1 ;)
```

Figure 4-9. Règle de détection d'attaque TCP Flood avec Python**.**

Comme le montre la ***Figure 4-9,*** le système de détection d'intrusion Snort, fait remonter des alertes avec le message « attaque SynFlood_Python » lors d'une réception d'une quantité de paquets qui dépasse le 50 paquet/s et de flag SYN.

d Règle de détection de l'attaque SYN Flood lancé par LOIC

```
# LOCAL RULES
#alert tcp  any any -> any any (msg:" attaque tcp loic "; flags:pa ; threshold:type threshold , track by_src, count 20 ,
seconds 3 ; sid:100000011 ;rev:1 ;)
```

***Figure* 4-10.** Règle de détection d'attaque TCP Flood avec LOIC.

Cette règle de détection est définie par :

- Un message d'affichage « attaque tcp loic ».
- Paquet de flags (**PSH/ACK).**
- Un count de 20 paquets /s.
- Intervalle de temps de temps de 3s.

e Règle de détection de l'attaque SYN Flood lancé par l'outil Slowloris

```
# LOCAL RULES
alert tcp any any  -> any any (msg:"attaque SynFlood_Slowloris"; flags:a ; threshold:type threshold , track by_src, count
300, seconds 1 ; sid:100000016 ;rev:1 ;)
```

***Figure 4.11*.** Règle de détection d'attaque SYN Flood avec Slowloris**.**

Snort va générer une alerte de message « attaque SynFlood Slowloris » si la machine victime reçoit 300 paquets/s de demandes de connexion TCP avec le flag SYN.

f Règle de détection de l'attaque SYN Flood lancé par l'outil Pyloris

```
# LOCAL RULES
alert tcp any any  -> any any (msg:"attaque SynFlood_Pyloris"; flags:s ; threshold:type threshold , track by_src, count
100, seconds 3 ; sid:100000019 ;rev:1 ;)
```

Figure 4-12. Règle de détection d'attaque SYN Flood avec Pyloris.

Le système de détection d'intrusion Snort remonte une alerte de détection avec le message « attaque SynFlood_Pyloris » lorsque la machine cible recevrait un nombre de paquets dépasse le 100paquets/s.

g **Règle de détection de l'attaque SYN Flood lancé par l'outil Xerxès :**

```
# LOCAL RULES
alert tcp any any  -> any any (msg:"attaque SynFlood_Xerxes"; flags:ap ; threshold:type threshold , track by_src, count
100, seconds 1 ; sid:100000017 ;rev:1 ;)
```

Figure 4-13. Règle de détection d'attaque SYN Flood avec Xerxes.

D'après la signature d'attaque obtenue déjà, nous avons créé cette règle avec le message « attaque SynFlood_Xerxes », qui est caractérisé par un count de 100 paquets/s et de flags (ASK/PSH).

4.4.4 Attaque HTTP Flood

a ***Règle de détection de l'attaque Http Flood lancé par LOIC***

```
# LOCAL RULES
# alert tcp any any -> any any (msg:"attaque HTTP_LOIC"; flags:pa ; content:"|47 45 54 20 2f 20 48 54 54 50 2f 31 2e 30 0d
0a 0d 0a 0d 0a|"; sid:100000020 ; rev:1;)
```

Figure 4-14. Règle de détection d'attaque HTTP Flood avec LOIC.

D'après les résultats de la partie précédente, on a utilisé le content [(http/1.0/r/a)] |47 45 54 20 2f 31 2e 30 0d|et les flags : PSH/ACK, avec le message « attaque http_LOIC ».

4.5 Tests et évaluations de performance d'IDS Snort

Après avoir installé et configuré les services nécessaires et activé les règles créées, nous allons tester le fonctionnement de notre système.

Pour passer au test, on doit lancer des attaques de type (UDP, ICMP, TCP, HTTP) Flood à partir du PC attaquant au PC victime qui contient l'IDS Snort, pour voir s'il va détecter les attaques qui viendront de l'extérieur ensuite alerter l'administrateur.

4.5.1 Lancement de Snort sous Windows

La première chose sera de vérifier quelles sont les interfaces actives au niveau de notre machine, nous allons utiliser la commande : **snort –W.**

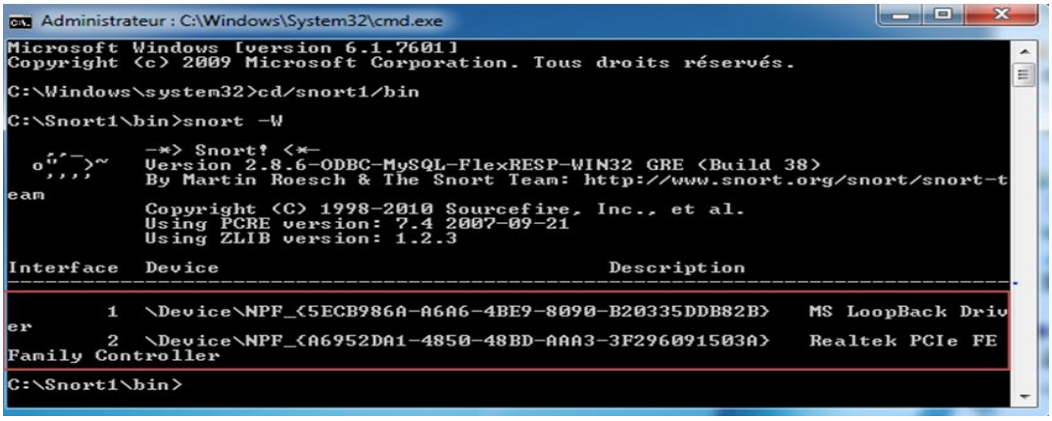


Figure 4-15. Les interfaces actives au niveau de la machine.

Comme le montre la figure 4-15, nous avons deux interfaces actives, nous allons utiliser l'interface 2 du réseau local.

On lance Snort avec la commande suivante :

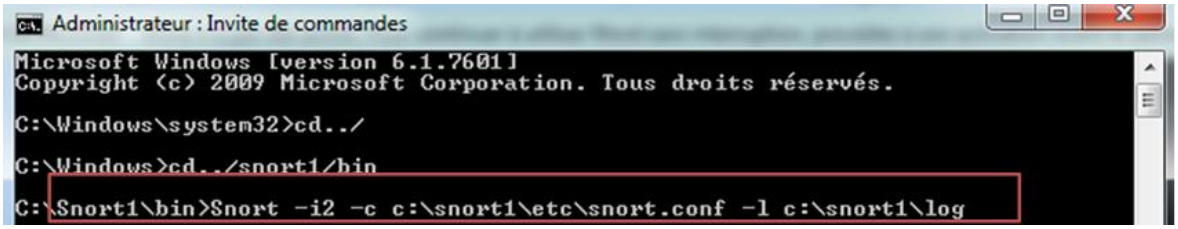


Figure 4-16. Mise en marche de Snort sur Windows.

-i2 : l'interface (2) à écouter.

-c:\snort1 \etc\snort.conf : le chemin du fichier snort.conf

-l : connexion au répertoire.

La figure ci-dessus montre que ***Snort*** marche bien d'après le résultat de la commande précédente.

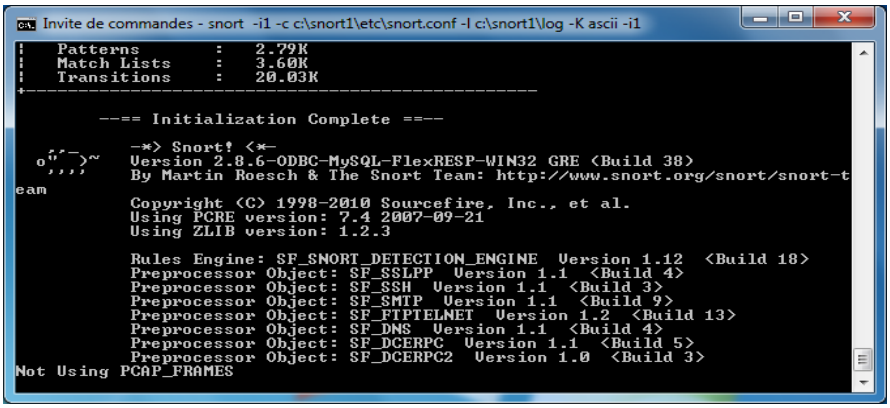


Figure 4-17. Démarrage de Snort**.**

Pour tester la fiabilité de nos règles, on va lancer quelques attaques et analyser les alertes au niveau de l'interface Web (BASE).

4.5.2 Lancement de BASE

BASE sert à fournir une représentation visuelle des données concernant les éventuelles intrusions. Après l'installation de ce dernier, on lance dans le navigateur : **127.0.0.1/base/.**

Sur la page d'accueil, nous remarquons que nous pouvons déjà tirer quelques informations comme le pourcentage du trafic suspect pour les protocoles TCP, UDP et ICMP et le nombre d'alertes.

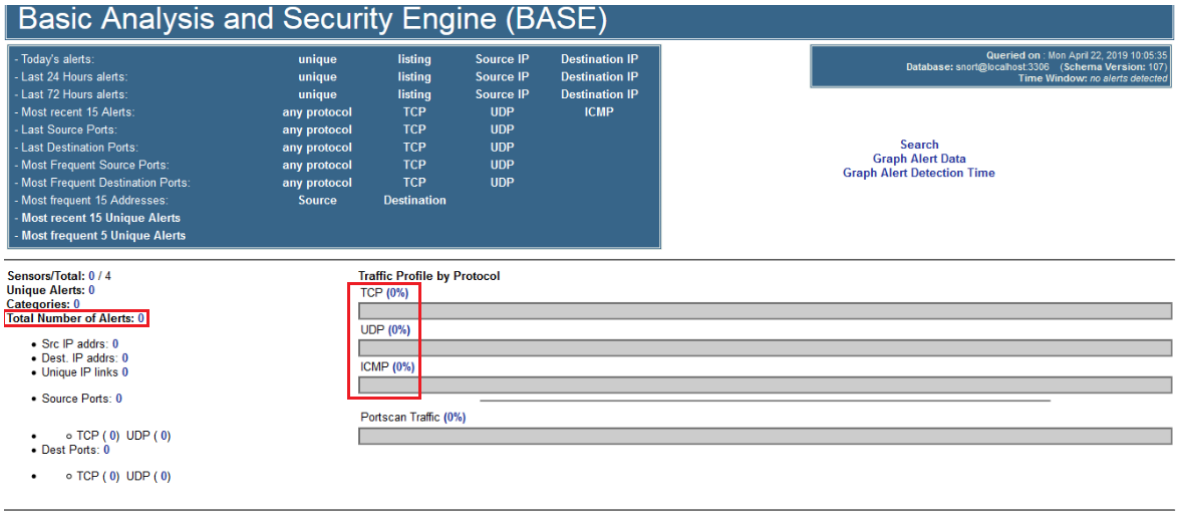


Figure 4.18. L'interface BASE.

4.5.3 Les tests

a Attaque UDP Flood

Après avoir effectué les attaques, on va accéder à « BASE » pour visualiser ce qui passe au niveau de Snort.

Nous voyons en rouge le pourcentage d'alerte ajouté, si on clique sur le protocole UDP, nous serions redirigés vers une autre page qui nous affichera les informations de ces alertes d'une manière plus détaillée sous forme d'un tableau.

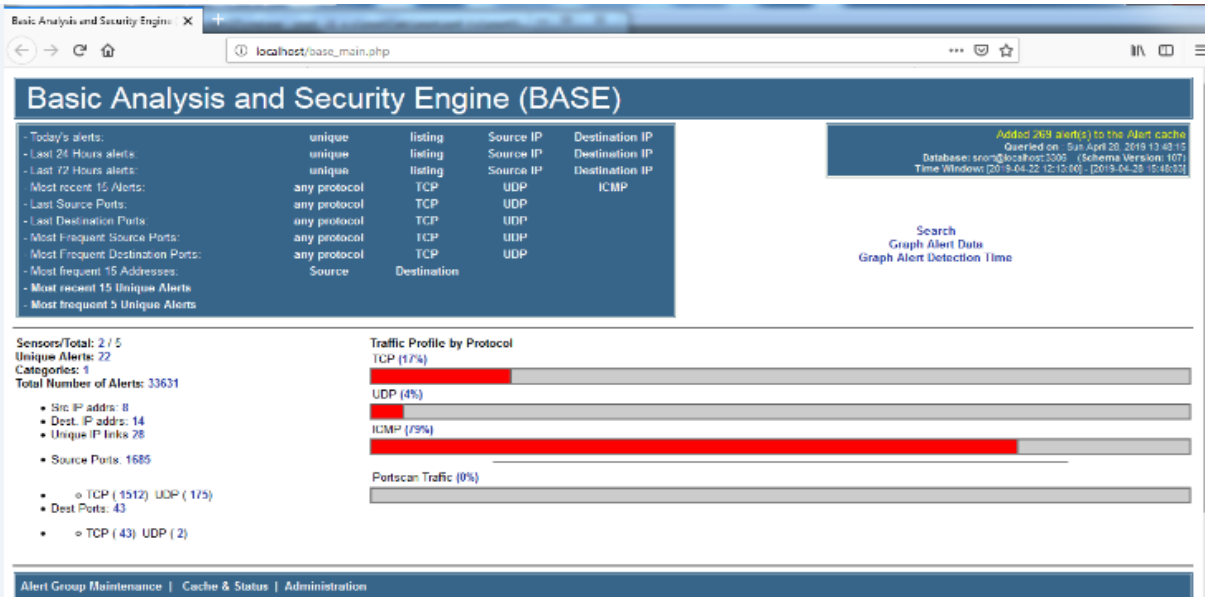


Figure 4-19. L'accueil base après l'attaque UDP.

- **Les alertes générées par la règle de détection « UDP-Hping3 »**

Snort a détecté des actions qui étaient définies comme une intrusion. Et on remarquera aussi qu'il y'a beaucoup d'alertes qui sont générées.

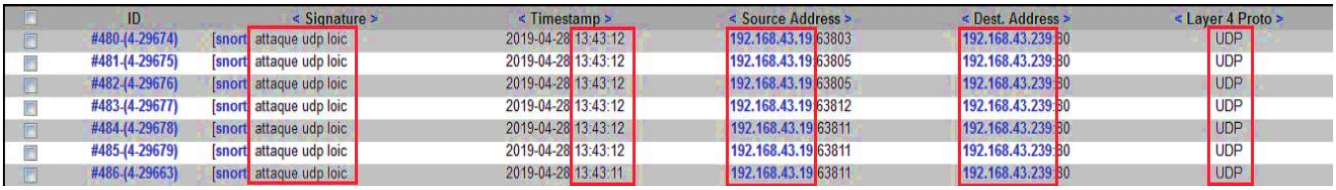
ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(4-32894)	[snort Attaque UDP_Hping	2019-04-28 15:31:02	192.168.43.48 9256	192.168.43.239 0	UDP
#1-(4-32893)	[snort Attaque UDP_Hping	2019-04-28 15:31:01	192.168.43.48 9206	192.168.43.239 0	UDP
#2-(4-32892)	[snort Attaque UDP_Hping	2019-04-28 15:31:01	192.168.43.48 9156	192.168.43.239 0	UDP
#3-(4-32891)	[snort Attaque UDP_Hping	2019-04-28 15:31:00	192.168.43.48 9106	192.168.43.239 0	UDP
#4-(4-32890)	[snort Attaque UDP_Hping	2019-04-28 15:30:59	192.168.43.48 9056	192.168.43.239 0	UDP
#5-(4-32889)	[snort Attaque UDP_Hping	2019-04-28 15:30:59	192.168.43.48 9006	192.168.43.239 0	UDP
#6-(4-32888)	[snort Attaque UDP_Hping	2019-04-28 15:30:58	192.168.43.48 8956	192.168.43.239 0	UDP

Figure 4-20. Les alertes de détection d'attaque UDP avec Hping3.

Après avoir réalisé l'attaque UDP avec l'outil Hping3, on remarque qu'il y'a trop d'alerte du type UDP qui sont générées à partir de l'adresse « 192.168.43.48 » vers la

machine victime « 192.168.43.239 » de différent port chaque seconde, en affichant le message qu'on a déjà mis dans la règle « Attaque UDP_Hping ».

- **Les alertes générées par la règle de détection « UDP LOIC »**



ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#480-(4-29674)	[snort attaque udp loic	2019-04-28 13:43:12	192.168.43.19 63803	192.168.43.239 80	UDP
#481-(4-29675)	[snort attaque udp loic	2019-04-28 13:43:12	192.168.43.19 63805	192.168.43.239 80	UDP
#482-(4-29676)	[snort attaque udp loic	2019-04-28 13:43:12	192.168.43.19 63805	192.168.43.239 80	UDP
#483-(4-29677)	[snort attaque udp loic	2019-04-28 13:43:12	192.168.43.19 63812	192.168.43.239 80	UDP
#484-(4-29678)	[snort attaque udp loic	2019-04-28 13:43:12	192.168.43.19 63811	192.168.43.239 80	UDP
#485-(4-29679)	[snort attaque udp loic	2019-04-28 13:43:12	192.168.43.19 63811	192.168.43.239 80	UDP
#486-(4-29663)	[snort attaque udp loic	2019-04-28 13:43:11	192.168.43.19 63811	192.168.43.239 80	UDP

Figure 4-21. Les alertes de détection d'attaque UDP avec LOIC.

Après avoir lancé l'attaque UDP Flood avec l'outil LOIC, Snort a déclenché plusieurs alertes de type UDP affichant le message attribué déjà dans la règle « attaque udp loic ».

Ces alertes sont générées chaque seconde, pour alerter l'administrateur qu'une attaque UDP a eu lieu à partir de l'adresse <source Adress>192.168.43.19 vers la machine cible <Dest.Adress> 192.168.43.239 de différents ports.

b Attaques ICMP

- **Les alertes générées par la règle de détection « ICMP Flood »**

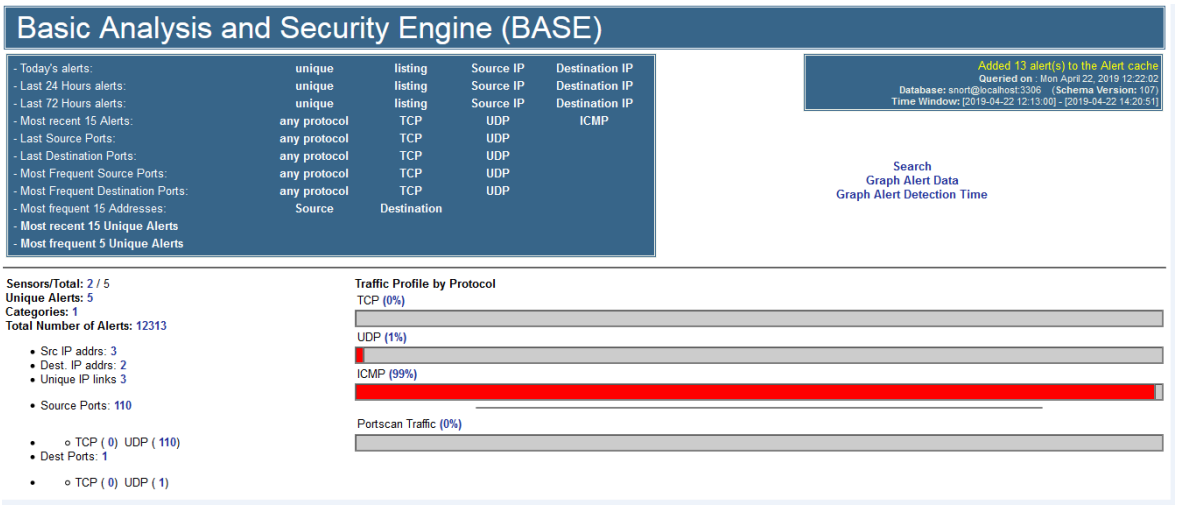


Figure 4-22. L'interface BASE après l'attaque ICMP Flood.

Après avoir lancé une attaque de type ICMP Flood avec l'outil Hping3, on remarque dans Snort un pourcentage d'alerte ICMP très élevé (85%).

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(4-30130)	[snort] attaque ping flood	2019-04-28 13:51:04	192.168.43.48	192.168.43.239	ICMP
#1-(4-30129)	[snort] attaque ping flood	2019-04-28 13:51:04	192.168.43.48	192.168.43.239	ICMP
#2-(4-30128)	[snort] attaque ping flood	2019-04-28 13:51:04	192.168.43.48	192.168.43.239	ICMP
#3-(4-30127)	[snort] attaque ping flood	2019-04-28 13:51:04	192.168.43.48	192.168.43.239	ICMP
#4-(4-30126)	[snort] attaque ping flood	2019-04-28 13:51:04	192.168.43.48	192.168.43.239	ICMP
#5-(4-30125)	[snort] attaque ping flood	2019-04-28 13:51:04	192.168.43.48	192.168.43.239	ICMP
#6-(4-30124)	[snort] attaque ping flood	2019-04-28 13:51:04	192.168.43.48	192.168.43.239	ICMP

Figure 4-23. Les alertes de détection d'attaque ICMP Flood.

La figure 4.23, affiche les alertes de détection d'attaque ICMP Flood lancé par l'outil Hping3. Ces alertes ont été généré chaque seconde, pour nous informer qu'une attaque ICMP provient de l'adresse 192.168.43.48 vers 192.168.43.239 en affichant le message « attaque Ping Flood ».

- **Les alertes générées par la règle de détection « Ping of death »**

Après la réalisation de l'attaque Ping of death, on remarque la présence des alertes de type ICMP sont générées avec le message « attaque Ping of death ».

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(4-33083)	[snort] attaque ping of death	2019-04-28 15:41:47	192.168.43.19	192.168.43.239	ICMP
#1-(4-33082)	[snort] attaque ping of death	2019-04-28 15:41:42	192.168.43.19	192.168.43.239	ICMP
#2-(4-33081)	[snort] attaque ping of death	2019-04-28 15:41:37	192.168.43.19	192.168.43.239	ICMP
#3-(4-33080)	[snort] attaque ping of death	2019-04-28 15:41:32	192.168.43.19	192.168.43.239	ICMP
#4-(4-33079)	[snort] attaque ping of death	2019-04-28 15:41:27	192.168.43.19	192.168.43.239	ICMP
#5-(4-33078)	[snort] attaque ping of death	2019-04-28 15:41:22	192.168.43.19	192.168.43.239	ICMP
#6-(4-33077)	[snort] attaque ping of death	2019-04-28 15:41:21	192.168.43.19	192.168.43.239	ICMP

Figure 4.24. Les alertes de détection d'attaque Ping of death.

c Attaque TCP Flood

- **Les alertes générées par la règle de détection « TCPHping3 PSH »**

Après avoir effectué l'attaque « TCP Flood » par l'outil Hping3 avec des flag (PSH), Snort détecte les paquets malveillants et affiche les alertes qui définissent ce type d'attaque.

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(4-32755)	[snort] attaque tcp hping_p	2019-04-28 15:23:28	192.168.43.48:7307	192.168.43.239:0	TCP
#1-(4-32754)	[snort] attaque tcp hping_p	2019-04-28 15:23:25	192.168.43.48:7125	192.168.43.239:0	TCP
#2-(4-32753)	[snort] attaque tcp hping_p	2019-04-28 15:23:24	192.168.43.48:7025	192.168.43.239:0	TCP
#3-(4-32752)	[snort] attaque tcp hping_p	2019-04-28 15:23:23	192.168.43.48:6925	192.168.43.239:0	TCP
#4-(4-32751)	[snort] attaque tcp hping_p	2019-04-28 15:23:20	192.168.43.48:6747	192.168.43.239:0	TCP
#5-(4-32750)	[snort] attaque tcp hping_p	2019-04-28 15:23:19	192.168.43.48:6647	192.168.43.239:0	TCP
#6-(4-32749)	[snort] attaque tcp hping_p	2019-04-28 15:23:18	192.168.43.48:6547	192.168.43.239:0	TCP

Figure 4.25. Les alertes de détection d'attaque TCP Flood Hping3 (PSH).

On remarque un grand nombre d'alerte de type TCP qui ont été affiché avec le message « attaque tcp hping_p » chaque seconde, ces attaques ont été lancé par la machine 192.168.43.48 vers la machine 192.168.43.239.

- **Les alertes générées par la règle de détection « TCP Hping3 FIN »**

Avec le même outil Hping3, on lance une seconde attaque avec le flag (FIN).

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(4-32839)	[snort] attaque tcp hping_f	2019-04-28 15:26:47	192.168.43.48:5460	192.168.43.239:0	TCP
#1-(4-32838)	[snort] attaque tcp hping_f	2019-04-28 15:26:47	192.168.43.48:5410	192.168.43.239:0	TCP
#2-(4-32837)	[snort] attaque tcp hping_f	2019-04-28 15:26:46	192.168.43.48:5360	192.168.43.239:0	TCP
#3-(4-32836)	[snort] attaque tcp hping_f	2019-04-28 15:26:45	192.168.43.48:5310	192.168.43.239:0	TCP
#4-(4-32835)	[snort] attaque tcp hping_f	2019-04-28 15:26:45	192.168.43.48:5260	192.168.43.239:0	TCP
#5-(4-32834)	[snort] attaque tcp hping_f	2019-04-28 15:26:44	192.168.43.48:5210	192.168.43.239:0	TCP
#6-(4-32833)	[snort] attaque tcp hping_f	2019-04-28 15:26:44	192.168.43.48:5160	192.168.43.239:0	TCP

Figure 4-26. Les alertes de détection d'attaque TCP Flood Hping3 (FIN).

D'après ces alertes, On remarque que ces attaques sont du type TCP et avec un flag (FIN) comme nous avons déclaré au niveau des règles. Ces attaques ont été lancées par la

machine 192.168.43.48 vers la machine victime 192.168.43.239 chaque 1s avec le message « attaque tcp Hping_f ».

- **Les alertes générées par la règle de détection « SYN Flood_Python »**

La **figure 4-27**, affiche les alertes de détection de l'attaque SYN Flood lancée par l'outil Python. Ces alertes sont générées chaque seconde, de l'adresse 192.168.43.78 vers 192.168.43.239 avec le message « attaque SYN Flood_Python » et utilisant différents ports.

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(4-34907)	[snort] attaque SynFlood_Python	2019-04-28 16:07:43	192.168.43.78:34162	192.168.43.239:33713	TCP
#1-(4-34906)	[snort] attaque SynFlood_Python	2019-04-28 16:07:43	192.168.43.78:34162	192.168.43.239:19739	TCP
#2-(4-34905)	[snort] attaque SynFlood_Python	2019-04-28 16:07:43	192.168.43.78:34162	192.168.43.239:39952	TCP
#3-(4-34904)	[snort] attaque SynFlood_Python	2019-04-28 16:07:43	192.168.43.78:34162	192.168.43.239:45053	TCP
#4-(4-34903)	[snort] attaque SynFlood_Python	2019-04-28 16:07:43	192.168.43.78:34162	192.168.43.239:47686	TCP
#5-(4-34902)	[snort] attaque SynFlood_Python	2019-04-28 16:07:43	192.168.43.78:34162	192.168.43.239:27721	TCP
#6-(4-34901)	[snort] attaque SynFlood_Python	2019-04-28 16:07:43	192.168.43.78:34162	192.168.43.239:25023	TCP

Figure 4-27. Les alertes de détection d'attaque SYN Flood Python.

- **Les alertes générées par la règle de détection « TCP LOIC »**

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(4-28597)	[snort] attaque tcp loic	2019-04-28 13:36:12	192.168.43.19:50927	192.168.43.239:80	TCP
#1-(4-28596)	[snort] attaque tcp loic	2019-04-28 13:36:12	192.168.43.19:50925	192.168.43.239:80	TCP
#2-(4-28595)	[snort] attaque tcp loic	2019-04-28 13:36:12	192.168.43.19:50922	192.168.43.239:80	TCP
#3-(4-28594)	[snort] attaque tcp loic	2019-04-28 13:36:12	192.168.43.19:50926	192.168.43.239:80	TCP
#4-(4-28593)	[snort] attaque tcp loic	2019-04-28 13:36:12	192.168.43.19:50922	192.168.43.239:80	TCP
#5-(4-28592)	[snort] attaque tcp loic	2019-04-28 13:36:11	192.168.43.19:50928	192.168.43.239:80	TCP
#6-(4-28591)	[snort] attaque tcp loic	2019-04-28 13:36:11	192.168.43.19:50928	192.168.43.239:80	TCP

Figure4-28. Les alertes de détection d'attaque TCP Flood LOIC.

Après avoir effectué l'attaque SYN Flood avec l'outil LOIC, Snort affiche les alertes de détection du protocole TCP avec le message « attaque tcp loic » déclaré déjà au niveau de la règle, ces attaques sont lancées par la machine 192.168.43.19 vers cette machine à travers différents ports.

- **Les alertes générées par la règle de détection « SYN Flood avec Slowloris »**

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(4-34115)	[snort] attaque SynFlood_Slowloris	2019-04-28 15:52:45	192.168.43.239:80	192.168.43.78:48390	TCP
#1-(4-34114)	[snort] attaque SynFlood_Slowloris	2019-04-28 15:52:45	192.168.43.239:80	192.168.43.78:48382	TCP
#2-(4-34113)	[snort] attaque SynFlood_Slowloris	2019-04-28 15:52:45	192.168.43.239:80	192.168.43.78:48376	TCP
#3-(4-34112)	[snort] attaque SynFlood_Slowloris	2019-04-28 15:52:45	192.168.43.239:80	192.168.43.78:48366	TCP
#4-(4-34111)	[snort] attaque SynFlood_Slowloris	2019-04-28 15:52:45	192.168.43.239:80	192.168.43.78:48360	TCP
#5-(4-34110)	[snort] attaque SynFlood_Slowloris	2019-04-28 15:52:45	192.168.43.239:80	192.168.43.78:48354	TCP
#6-(4-34109)	[snort] attaque SynFlood_Slowloris	2019-04-28 15:52:45	192.168.43.239:80	192.168.43.78:48340	TCP

Figure 4-29. Les alertes de détection d'attaque SYN Flood avec Slowloris.

Après avoir réalisé l'attaque SYN Flood avec l'outil Slowloris, on remarque beaucoup d'alertes du protocole TCP qui ont été généré, l'outil Slowloris a falsifié l'adresse de l'attaquant par celle de la machine victime comme une adresse source.

- **Les alertes générées par la règle de détection « SYN Flood avec Pyloris »**

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(4-34630)	[snort] attaque SynFlood_Pyloris	2019-04-28 16:00:31	192.168.43.239:80	192.168.43.78:51044	TCP
#1-(4-34629)	[snort] attaque SynFlood_Pyloris	2019-04-28 16:00:31	192.168.43.239:80	192.168.43.78:51032	TCP
#2-(4-34628)	[snort] attaque SynFlood_Pyloris	2019-04-28 16:00:31	192.168.43.239:80	192.168.43.78:50992	TCP
#3-(4-34627)	[snort] attaque SynFlood_Pyloris	2019-04-28 16:00:31	192.168.43.239:80	192.168.43.78:50952	TCP
#4-(4-34626)	[snort] attaque SynFlood_Pyloris	2019-04-28 16:00:31	192.168.43.239:80	192.168.43.78:50912	TCP
#5-(4-34625)	[snort] attaque SynFlood_Pyloris	2019-04-28 16:00:31	192.168.43.239:80	192.168.43.78:50872	TCP
#6-(4-34624)	[snort] attaque SynFlood_Pyloris	2019-04-28 16:00:31	192.168.43.239:80	192.168.43.78:50550	TCP

Figure 4-30. Les alertes de détection d'attaque SYN Flood avec Pyloris.

Après avoir réalisé l'attaque SYN Flood avec l'outil Pyloris, on remarque que plusieurs alertes de type TCP sont générées, avec le message « attaque SynFlood_Pyloris », l'outil Pyloris falsifie l'adresse IP de l'attaquant en prenant celle de la machine victime (192.168.43.239) et le port 80 comme port source.

- **Les alertes générées par la règle de détection « SYN Flood Xerxès »**

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(4-33719)	[snort] attaque SynFlood_Xerxes	2019-04-28 15:48:03	192.168.43.78:48032	192.168.43.239:80	TCP
#1-(4-33718)	[snort] attaque SynFlood_Xerxes	2019-04-28 15:48:03	192.168.43.78:48124	192.168.43.239:80	TCP
#2-(4-33717)	[snort] attaque SynFlood_Xerxes	2019-04-28 15:48:03	192.168.43.78:48066	192.168.43.239:80	TCP
#3-(4-33716)	[snort] attaque SynFlood_Xerxes	2019-04-28 15:48:03	192.168.43.78:48088	192.168.43.239:80	TCP
#4-(4-33715)	[snort] attaque SynFlood_Xerxes	2019-04-28 15:48:03	192.168.43.78:47938	192.168.43.239:80	TCP
#5-(4-33714)	[snort] attaque SynFlood_Xerxes	2019-04-28 15:48:02	192.168.43.78:47908	192.168.43.239:80	TCP
#6-(4-33713)	[snort] attaque SynFlood_Xerxes	2019-04-28 15:48:02	192.168.43.78:48054	192.168.43.239:80	TCP

Figure 4-31. Les alertes de détection d'attaque SYN Flood avec Xerxès.

D'après ces alertes, On remarque que ces attaques sont de protocole TCP et sont lancées par la machine 192.168.43.78 vers la machine victime 192.168.43.239 par différents ports avec le message « attaque SynFlood_Xerxes ».

d Attaque http

- **Les alertes générées par la règle de détection « http Flood »**

Après avoir réalisé l'attaque http Flood avec l'outil LOIC, on remarque la présence de beaucoup d'alertes de protocole TCP qui sont générées, en affichant le message « attaque http_LOIC » par la machine 192.168.43.19 utilisant plusieurs ports.

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(4-38604)	snort] attaque HTTP loic	2019-04-28 16:15:58	192.168.43.19:57802	192.168.43.239:80	TCP
#1-(4-38603)	snort] attaque HTTP loic	2019-04-28 16:15:58	192.168.43.19:57801	192.168.43.239:80	TCP
#2-(4-38602)	snort] attaque HTTP loic	2019-04-28 16:15:58	192.168.43.19:57800	192.168.43.239:80	TCP
#3-(4-38601)	snort] attaque HTTP loic	2019-04-28 16:15:58	192.168.43.19:57799	192.168.43.239:80	TCP
#4-(4-38600)	snort] attaque HTTP loic	2019-04-28 16:15:58	192.168.43.19:57798	192.168.43.239:80	TCP
#5-(4-38599)	snort] attaque HTTP loic	2019-04-28 16:15:58	192.168.43.19:57797	192.168.43.239:80	TCP
#6-(4-38598)	snort] attaque HTTP loic	2019-04-28 16:15:58	192.168.43.19:57796	192.168.43.239:80	TCP

Figure 4-32. Les alertes de détection d'attaque http Flood avec LOIC.

- **Note *:***

Les outils Xerxès et Slowloris réalisent l'attaque http avec l'envoi massif de paquets TCP, ce qui mène à un blocage du serveur web dès le début de l'attaque.

4.6 Constatation

Après l'analyse de toutes les alertes générées par Snort, on remarque que les adresses sources sont ceux de l'attaquant 192.168.43.78 sous Kali Linux et 192.168.43.19 sous Windows 10, cela veut dire que les règles n'ont pas provoqué des fausses alertes.

On remarque aussi que le nombre des alertes générées par les règles est très grand car les attaques se font dans un petit intervalle de temps.

Snort 2.9.2 a pu détecter les attaques DOS en temps réel, dans ce cas-là on peut confirmer la fiabilité de nos règles.

Conclusion

Les systèmes de détection d'intrusion sont utilisés dans la sécurité informatique car ils viennent compléter les autres systèmes de sécurité en détectant le maximum d'intrusions possible.

Dans ce chapitre nous avons vu comment mettre en place un système de détection d'intrusion réseau (NIDS) et l'exécuter sous Windows. Dans un premier temps Snort a pu détecter les attaques DOS en temps réel à l'aide de nos règles de détection et l'interface BASE nous a facilité l'accès au alertes générés par Snort et nous a permis de vérifier le contexte des alertes afin de déterminer si on a bien affaire à une attaque ou non pour ne pas tomber dans des fausses alertes.

Après les résultats expérimentaux, nous avons pu confirmer la fiabilité de nos règles.

Nous avons essayé à travers ce mémoire d'aider les étudiants du domaine des réseaux et télécommunication de mieux comprendre et maitriser les attaques DOS ainsi que les systèmes de détection d'intrusion réseau NIDS en concevant une plateforme expérimentale pour améliorer leurs connaissances dans la sécurité informatique ce qui leur sera utile dans le futur.

Le but principal de ce travail était de mettre en place un système de détection d'intrusion réseau NIDS open source Snort et tester sa fiabilité à la détection des attaques DOS. En premier lieu on a simulé les attaques UDP Flood, ICMP Flood, Ping of death, TCP Flood et Http Flood, que nous avons pu extraire leurs signatures lors de la phase d'analyse du trafic. Ces mêmes signatures nous ont permis d'élaborer des règles de détection dans le logiciel Snort open source.

Les résultats expérimentaux de notre recherche ont confirmé la fiabilité de nos règles ce qui veut dire que notre système de détection d'intrusion réseau NIDS est capable de compléter la politique de sécurité d'un réseau informatique.

Ce thème nous a permis d'approfondir nos connaissances dans les réseaux informatiques et les protocoles, comprendre comment réellement une attaque DOS peut endommager un système ou un réseau et surtout avoir une idée plus claire sur la conception de signatures d'attaques et également la compréhension d'un système de détection d'intrusion réseau tel que Snort open source.

[1] Cisco, 'Cisco Certified Network Associate 1', Version 6 : Notion de base sur les réseaux, support de cour Cisco, Avril 2019.

[2] 'Cours sur les réseaux informatiques', support de cour, récupéré sur : http://www.aidexam.com/ en Avril 2019.

[3] François Goffinet, 'CCNA Chapitre3 Protocole IPv4', Cour CCNA, 30 Janvier 2019.

[4] Keycdn, 'TCP Flags', article d'un site web, 4Octobre2018, récupéré en Avril 2019 sur : https://www.keycdn.com/support/tcp-flags.

[5] Christian Bulfone, 'Les protocoles UDP et TCP', support de cour.

[6] Pierre MORIN, 'La cybercriminalité', article, 27 Octobre 2017, SUPINFO International University, récupéré en Mai 2019 sur : https://www.supinfo.com/articles/single/6381cybercriminalite.

[7] Le monde, ' L'OTAN s'alarme des cyberattaques dont est victime l'Estonie', 18 Mai 2007, récupéré en Juin 2019 sur : https://assiste.com/Botnet.html.

[8] Vincent Destouches, 'Les 10 plus grands coups de piratage informatique', article d'un journal, L'actualité Octobre 2011.

[9] Martin Untersinger, 'Stuxnet : comment les Etats-Unis et Israël ont piraté le nucléaire iranien', article d'un journal, L'OBS, 4 Juin 2012.

[10] Dominique Filippone, 'Skygofree un spyware multifonctions qui s'attaque à Android', article Le monde Informatique, article d'un site web, 17 Janvier 2018, récupéré sur : https://www.lemondeinformatique.fr.

[11] 'TOP 10 des plus grandes cyberattaques', SECLUD AHEAD OF SECURITY, 20 Septembre 2017, article d'un site web récupéré en Juin 2019 sur : https://secludit.com/blog/top-10-des-plus-grandes-cyberattaques/

[12] 'Sécurité Informatique', 2007, article d'un forum, récupéré en Juin 2019 sur : http://xenod.free.fr/.

[13] David Burgermeister et Jonathan Krier, 'Les Systèmes de Détection d'Intrusions', document, 22 Juillet 2006.

[14] Laurent Poinsot, ' Introduction à la sécurité informatique', support de cours, Paris.

[15] Nicolas Baudru, 'Sécurité des systèmes informatiques ', support de cour, ESIL, 2008/2009.

[16] DOGNION Tiphaine et VANDAMME Julien, 'Le piratage informatique', rapport, ENSICAEN, 2005/2006.

[17] N. RASAMOELY, 'Gestion des certificats par LDAP', Septembre 2002, article, récupéré en Mai 2019 sur : http://www-public.imtbs-tsp.eu.

[18] CGI, 'Cryptographie à clé publique et signature numérique', Etude technique, Septembre 2002.

[19] 'PHISHING', document, Gendarmerie nationale de France.

[20] Véronique Sainson et Arnaud Jacques, 'Le mail Bombing', article de Sécurité Info, 2001-2016, récupéré en Juin 2019 sur : https://www.securiteinfo.com/.

[21] Lilia GAOUA, ' DOS avec Hping3', article, récupéré sur : http://belkhir.nacim.free.fr/.

[22] 'Déni de service distribute (DDOS)', article, publié en 2014, récupéré sur NTT Security en Mai 2019 : https://www.nttsecurity.com/fr-fr?help=true.

[23] HOTTE Marion, LUTUN Quentin-Edouard et ASCOET Thomas, 'Protection contre les attaques de déni de service dans les réseaux IP', rapport, Paris.

[24] 'Understanding a [Distributed] Denial of Service (DOS / DDOS) Attack', récupéré en Mai 2019 sur Securi: https://sucuri.net/.

[25] Harshita, ' Detection and Prevention of ICMP Flood DDOS Attack', International Journal of New Technology and Research, Volume3 Pages 63-69, Publication, publiée le 3 Mars 2017.

[26] Humeau, 'Analyse de l'outil de DDOS LOIC', article récupéré sur NBS System: https://www.nbs-system.com/en Juin 2019.

[27] DENY ALL, 'Slowloris une attaque visant les serveurs web', Flash Presse, Paris, 3 Juillet 2009.

[28] 'DDOS Attack Definitions DDOS Pedia', article récupéré en Mai 2019 sur Radware : https://security.radware.com/dDOS-knowledge-center/dDOSpedia/pyloris/.

[29] A. ELBAKKALI, 'Xerxes De The Jester', Un outil de DOS qui fait peur, article récupéré en Juin 2019 sur : https://www.parlonsgeek.com/xerxes-the-jester/.

[30] DOUAS Youssef CHAIKHI, 'Les types d'attaques informatiques', rapport, Office de la Formation Professionnelle et de la Promotion du Travail, Tetouan, 2010.

[31] 'Cours sur Les menaces informatiques', cour, Récupéré sur : cours gratuit : https://www.cours-gratuit.com/cours-informatique/cours-sur-les-menaces-informatiques.

[32] DABOUR Imane, 'Etude et mise en place d'un système de détection et prévention d'intrusion', 2013-2014.

[33] Darties et Benoit, rapport, 'Tutoriel d'utilisation de Wireshark'.

[34] Windows 7, Futura tech, publication, récupéré sur : https://www.futurasciences.com/tech/definitions/informatique-windows-7-5488.