

| Terminal régulier | Administration réseau local | Administration réseau local (cont) | Administration réseau local (cont) | Attaque sur un réseau |
|--|--|---|---|--|
| <pre>/mnt/netta/a-pps/vnet/nem-u-vnet netadm</pre> | sert à lancer le réseau virtuel | <pre>echo 1 > /proc/sys/net/ipv4/ip-_forward</pre> | <pre>traceroute <destination></pre> | <pre>arp -n, ip neigh</pre> |
| <pre>/mnt/netta/a-pps/vnet/nem-u-restore</pre> | restaurer le réseau virtuel précédemment | <pre>route -n</pre> | <pre>/etc/network/interfaces</pre> | <pre>arp spoof -t <@IP machine</pre> |
| <pre>~/vnet/netadm.tgz</pre> | sauvegardé | <pre>route -n</pre> | <pre>ifup eth0</pre> | <pre>machine</pre> |
| Administration réseau local | | | | |
| <pre>ifconfig</pre> | lister les interfaces allumées | <pre>route add default gw <@IP passerelle></pre> | <pre>ifdown eth0</pre> | <pre>qui va se faire</pre> |
| <pre>ifconfig -a</pre> | lister toutes les interfaces | <pre>route del default gw <@IP passerelle></pre> | <pre>ifdown eth0</pre> | <pre>pwned></pre> |
| <pre>ifconfig <if-ace> <@IP></pre> | configurer l'interface | <pre>ip route</pre> | <pre>/var/www/html</pre> | <pre><@IP machine</pre> |
| <pre>ifconfig <if-ace> netmask <netmask></pre> | configurer l'interface | <pre>ip route add default via <@IP passerelle></pre> | <pre>écrite une page simple html dans le fichier</pre> | <pre>dont on souhaite usurper l'identité></pre> |
| <pre>ifconfig <if-ace> up</pre> | allumer l'interface | <pre>ip route del default via <@IP passerelle></pre> | <pre>/etc/hostname</pre> | <pre>l'attaquant est la passerelle ou une autre machine sur le réseau.</pre> |
| <pre>ifconfig <if-ace> down</pre> | éteindre l'interface | <pre>route add -net <@IP réseau></pre> | <pre>Configurez le nom de chaque machine</pre> | <pre>capture le trafic qui passe sur le réseau</pre> |
| <pre>ip -br addr</pre> | lister toutes les interfaces | <pre>netmask <netmask> gw <@IP passerelle></pre> | <pre>auto eth0 iface eth0 inet static address 192.16.8.0.1 netmask 255.255.255.0 gateway 192.16.8.0.254</pre> | <pre>wireshark -i eth0 -k</pre> |
| <pre>ip addr add <@IP>/<netmask> dev <iface></pre> | configurer l'interface | <pre>ip route add <@IP réseau>/<netmask> via <@IP passerelle></pre> | <pre>Config-uration Statique dans le fichier /etc/network/interfaces</pre> | |
| <pre>ip link set <if-ace> up</pre> | allumer l'interface | <pre>ssh <login>@<-destination></pre> | <pre>terminal NEmu</pre> | |
| <pre>ip link set <if-ace> down</pre> | éteindre l'interface | <pre>test la communication entre 2 machines</pre> | <pre>quit()</pre> | <pre>quitter le réseau virtuel</pre> |
| <pre>ping <ip></pre> | ping sur la machine local l'ip d'une machine | | <pre>save()</pre> | <pre>sauvegarder le réseau virtuel</pre> |
| | | | <pre>reboot()</pre> | <pre>redémarrer violemment le réseau virtuel</pre> |



Attaque sur un réseau (cont)

```
echo "[:<username- ajoute
me>:$(busybox httpd une
-m '<password>') > authen-
/etc/httpd.conf tification
Exemple: echo "[:m- au site
onsuperuser:$(b- web
usybox httpd -m
'monsupermotdep-
asse')" > /etc/http-
d.conf
```

```
busybox httpd -f -vv - démarre
h /var/www/html -r "- un site
Restricted Area." -c web
/etc/httpd.conf
```

Attaque de type Deny Of Service

```
hping3 --flood --syn -- inonde
spooof <@IP source d'une
usurpée> <@IP ip à
victime> l'autre
```

Réseau étendu

```
/sbin/ifconfig pour
recuperer
les
adresses
ip du
poste
physique
```

```
/mnt/netta/apps/vn- lance le
et/nemu-vnet serveur
netadm [nemu]-> pour le
slink() premier
réseau
```

```
/mnt/netta/apps/vn- lancer le
et/nemu-vnet deuxième
netadm [nemu]-> groupe
clink('<@IP du
groupe principal>')
```

compte admin

```
startx démarre l'interface
graphique
```

```
id: root connexion au
mdp: plop compte admin
```

```
reboot() redémarre la
machine
```

```
poweroff, halt arrête proprement
la machine virtuel
```

```
passwd changer le mot de
<login> passe
```

```
adduser ajoute un nouvel
<login> utilisateur
```

```
login <lo- se connecter sur un
gin> nouvel utilisateur
```

```
exit() quitte le compte
courant
```

```
hostname change le nom de
<name> la machine
```

```
/etc/h- change dans le
ostname fichier le nom
```

```
nano <fi- exécute un fichier
chier>
```

Sécuristaion serveur SSL/TLS

```
openssl génère une
req -new nouvelle paire de
-newkey clés RSA de 4096
rsa:4096 bits, crée un
-x509 - certificat auto-signé
sha256 - au format X.509
days 365 valide pendant 365
\ -nodes - jours, et enregistre
out le certificat dans le
alcest.crt fichier alcest.crt et
-keyout la clé privée dans
alcest.key le fichier alcest.key
```

Sécuristaion serveur SSL/TLS (cont)

```
cat permet de
lire le
contenu du
certificat
```

```
openssl x509 - permet de
in alcest.crt - lire le
text contenu plus
agrément
```

```
cat alcest.key créer un
alcest.crt > fichier pem
alcest.pem pour le
serveur web.
```

Ce type de fichier contient à la fois le certificat du serveur ainsi que sa clé privée

```
etc/light- fichier
tpd/conf- permettant
enabled/tls.conf d'activer
SSL/TLS
```

```
server.modules permet
+= ("mod_open- d'activer
ssl") $SERVE- SSL/TLS
R["socket"] == dans un
"0.0.0.0:443" { fichier
ssl.engine = "-
enable" ssl.pe-
mfile = "/etc/l-
ighttpd/securit-
y/alcest.pem" }
```

Sécuristaion serveur SSL/TLS (cont)

```
echo "<username- ajoute
>:$(busybox httpd - une
m '<password>') > authentif-
<auth file> ication au
site web
```

```
systemctl start lance le
lighttpd serveur
web
```

```
systemctl status vérifie
lighttpd l'état du
serveur
```

