

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 &gt; /proc/sys/net/ipv4/ip-_forward</pre>	<pre>traceroute &lt;destination&gt;</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 &lt;@IP machine</pre>
<pre>~/vnet/netadm.tgz</pre>	sauvegardé	<pre>route -n</pre>	<pre>ifup eth0</pre>	<pre>machine qui va se faire pwned&gt;</pre>
Administration réseau local		<pre>route add default gw &lt;@IP passerelle&gt;</pre>	<pre>ifdown eth0</pre>	<pre>&lt;@IP machine dont on souhaite usurper l'identité&gt;</pre>
<pre>ifconfig</pre>	lister les interfaces allumées	<pre>route del default gw &lt;@IP passerelle&gt;</pre>	<pre>ifdown eth0</pre>	<pre>wireshark -i eth0 -k</pre>
<pre>ifconfig -a</pre>	lister toutes les interfaces	<pre>ip route</pre>	<pre>/var/www/html</pre>	capture le trafic qui passe sur le réseau
<pre>ifconfig &lt;if-ace&gt; &lt;@IP&gt; netmask &lt;netmask&gt;</pre>	configurer l'interface	<pre>ip route add default via &lt;@IP passerelle&gt;</pre>	<pre>/etc/hostname</pre>	
<pre>ifconfig &lt;if-ace&gt; up</pre>	allumer l'interface	<pre>ip route del default via &lt;@IP passerelle&gt;</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>ifconfig &lt;if-ace&gt; down</pre>	éteindre l'interface	<pre>route add -net &lt;@IP réseau&gt; netmask &lt;netmask&gt; gw &lt;@IP passerelle&gt;</pre>	<pre>terminal NEmu</pre>	
<pre>ip -br addr</pre>	lister toutes les interfaces	<pre>ip route add &lt;@IP réseau&gt; /&lt;netmask&gt; via &lt;@IP passerelle&gt;</pre>	<pre>quit()</pre>	
<pre>ip addr add &lt;@IP&gt;/&lt;netmask&gt; dev &lt;iface&gt;</pre>	configurer l'interface	<pre>ssh &lt;login&gt;@&lt;-destination&gt;</pre>	<pre>save()</pre>	
<pre>ip link set &lt;if-ace&gt; up</pre>	allumer l'interface	test la communication entre 2 machines	<pre>reboot()</pre>	
<pre>ip link set &lt;if-ace&gt; down</pre>	éteindre l'interface		<pre>quit()</pre>	
<pre>ping &lt;ip&gt;</pre>	ping sur la machine local l'ip d'une machine		<pre>save()</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
agréab-
lement
```

```
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
```

