Adressage réseau et ip Cheat Sheet

by Yohan33 via cheatography.com/208543/cs/44699/

Terminal régulier

/mnt/netta/apps/vnet/nemu-vnet netadm	sert à lancer le réseau virtuel
/mnt/netta/apps/vnet/nemu-restore ~/vnet/netadm.tgz	restaurer le réseau virtuel précédemment sauvegardé

Administration réseau local

ifconfig	lister les interfaces allumées
ifconfig -a	lister toutes les interfaces
ifconfig <iface> <@IP> netmask <netmask>	configurer l'interface
ifconfig <iface> up	allumer l'interface
ifconfig <iface> down	éteindre l'interface
ip -br addr	lister toutes les interfaces
ip addr add <@IP>/<netmask> dev <iface>	configurer l'interface
ip link set <iface> up	allumer l'interface
ip link set <iface> down	éteindre l'interface
ping <ip>	ping sur la machine local l'ip d'une machine

Administration réseau local (cont)

echo 1 > /proc/sys/net/ipv4/ip_forward	ransmettre les paquets qui ne lui sont pas destinés
route -n	lister toutes les routes
route add default gw <@IP passerelle>	ajouter une route par défaut
route del default gw <@IP passerelle>	supprimer une route par défaut
ip route	lister toutes les routes
ip route add default via <@IP passerelle>	ajouter une route par défaut
ip route del default via <@IP passerelle>	supprimer une route par défaut
route add -net <@IP réseau> netmask <netmask> gw <@IP passerelle>	indiquer une passerelle spécifique par réseau de destinatio
ip route add <@IP réseau>/<netmask> via <@IP passerelle>	indiquer une passerelle spécifique par réseau de destinatio
ssh <login>@<destination>	test la communication entre 2 machines

Administration réseau local (cont)

traceroute <destination>	trace le chemin des échanges
/etc/network/interfaces	permet de modifier le fichier de configuration réseau
ifup eth0	redémarre l'interface
ifdown eth0	éteins l'interface
/var/www/html	écrire une page simple html dans le fichier
/etc/hostname	Configurez le nom de chaque machine
auto eth0 iface eth0 inet static address 192.168.0.1 netmask 255.255.255.0 gateway 192.168.0.254	Configuration Statique dans le fichier /etc/network/interfaces

terminal NEmu

quit()	quitter le réseau virtuel
save()	sauvegarder le réseau virtuel
reboot()	redémarrer violemment le réseau virtuel

Attaque sur un réseau

arp -n, ip neigh	permet de consulter la table IP
arpspoof -t <@IP machine qui va se faire pwned> <@IP machine dont on souhaite usurper l'identité>	permet d'exécuter une attaque de spoofing ARP en redirigeant les paquets destinés à une adresse IP spécifique (la machine ciblée) vers l'attaquant, en faisant croire à la machine ciblée que l'attaquant est la passerelle ou une autre machine sur le réseau.
wireshark -i eth0 -k	capture le trafic qui passe sur le réseau

Attaque sur un réseau (cont)

echo "/:<username>:$(busybox httpd -m '<password>')" > /etc/httpd.conf Exemple: echo "/:monsuperuser:$(busybox httpd -m 'monsupermotdepasse')" > /etc/httpd.conf	ajoute une authentification au site web
busybox httpd -f -vv -h /var/www/html -r "Restricted Area:" -c /etc/httpd.conf	démarre un site web

Attaque de type Deny Of Service

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

Réseau étendu

/sbin/ifconfig	pour récuperer les adresses ip du poste physique
/mnt/netta/apps/vnet/nemu-vnet netadm [nemu]-> slink()	lance le serveur pour le premier réseau
/mnt/netta/apps/vnet/nemu-vnet netadm [nemu]-> clink('<@IP du groupe principal>')	lancer le deuxième groupe

compte admin

startx	démarre l'interface graphique
id: root mdp: plop	connexion au compte admin
reboot()	redémarre la machine
poweroff,halt	arrête proprement la machine virtuel
passwd <login>	changer le mot de passe
adduser <login>	ajoute un nouvel utilisateur
login <login>	se connecter sur un nouvel utilisateur
exit()	quitte le compte courant
hostname <name>	change le nom de la machine
/etc/hostname	change dans le fichier le nom
nano <fichier>	exécute un fichier

Sécuristaion serveur SSL/TLS

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

Sécuristaion serveur SSL/TLS (cont)

cat	permet de lire le contenu du certificat
openssl x509 -in alcest.crt -text	permet de lire le contenu plus agréablement
cat alcest.key alcest.crt > alcest.pem	créer un fichier pem pour le serveur web. Ce type de fichier contient à la fois le certificat du serveur ainsi que sa clé privée
etc/lighttpd/conf-enabled/tls.conf	fichier permetttant d'activer SSL/TLS
server.modules += ("mod_openssl") $SERVER["socket"] == "0.0.0.0:443" { ssl.engine = "enable" ssl.pemfile = "/etc/lighttpd/security/alcest.pem" }	permet d'activer SSL/TLS dans un fichier

Sécuristaion serveur SSL/TLS (cont)

echo "<username>:$(busybox httpd -m '<password>')" > <auth file>	ajoute une authentification au site web
systemctl start lighttpd	lance le serveur web
systemctl status lighttpd	vérifie l'état du serveur