Criptografía Aplicada – Taller: Herramientas Criptográficas (http://www.gpul.org)

1. Experimento 1: Peligros del sniffing

Uso de sniffit

- `sniffit -i <ifaz de red>`

Uso de arpspoof

- `arpspoof -i <interfaz> -t <ip a spoofear>`

2. Experimento 2: Esteganografía

Uso de steghide

Codificación de la información

- `steghide embed -cf <objeto a codificar> -ef <archivo de texto>`

Descodificación de la información

- `steghide extract -sf <objeto a descodificar>`

Tipos de objetos:

AU, JPEG, BMP, WAV

3. Sesiones seguras: Cryptcat

Uso de netcat

Escuchar en un puerto

- `nc -l -p <puerto a escuchar>`

Escribir en un puerto

- `nc <host> <puerto>`

Uso de Cryptcat

Escuchar en un puerto

- `cryptcat -k clave -l -p <puerto>`

Escribir en un puerto

- `cryptcat -k clave <host> <puerto>`

Uso de SSH:

Uso habitual

- `ssh <usuario>@host [-v]`
- `ssh <host>`

Copia segura de ficheros: de local a remoto

- `scp [-r] <ficheros a copiar> <usuario>@<host>:<fichero remoto>`

Copia segura de ficheros: de remoto a local

- `scp [r] <usuario>@<host>:<fichero remoto> <directorio local>`

Generación de llaves

- `ssh -keygen -t dsa (llaves: id_dsa, id_dsa.pub)`
- Fichero: `.ssh/config`

  `Host <host>`

  `StrictHostChecking <ask|yes|no>`

  `IdentityFile ~/.ssh/id_dsa #llave priv.`
- `cat id_dsa.pub >> .ssh/authorized_keys`

Forwarding de X

- `ssh -X <usuario>@<host>`

Túnel SSH directo

- `ssh <host remoto> -L <puerto local>:<host remoto>:<puerto remoto>`

Túnel SSH inverso

- `ssh <host remoto> -R <puerto local>:<host remoto>:<puerto remoto>`

Atajos en SSH

- ~. Aborta una sesión.
- ~? Ayuda.
- ~# Ver conexiones forward.

4. VPN: OpenVPN

Configuración básica

- `modprobe tun`
- `mknod /dev/net/tun c 100 20`
- `echo 1 > /proc/sys/net/ipv4/ip_forward`

Túnel sin seguridad

Fichero de configuración en `/etc/openvpn`

Directivas

- `dev <tun|tap>`
- `lport <puerto local>`
- `rport <puerto remoto>`
- `ifconfig <ip local túnel> <ip remot.túnel>`
- `up <script arranque>`

Parámetros que se envían al script de arranque:

- `interfaz`
- `mtu local`
- `mtu remoto`
- `ip túnel local`
- `ip túnel remota`
- `init`

Túnel con clave

Generación de llaves

- `openvpn –-genkey –-secret <llave>`

Directivas

- `secret <llave>`

Túnel con certificados

Generación de autoridad certificadora

- `openssl req -nodes -new -x509 -keyout <llave-ca> -out <certificado-ca>`

Generación y firma de certificado

- `openssl req -nodes -new -keyout <llave> -out <petición de firma de certif.>`
- `openssl ca -out <certificado> -in <petición de firma de certif.>`

Generación parámetros Diffie-Hellman

- `openssl dhparam -out <parametros> <bits>`

Directivas

- `tls-server` (indica servidor)
- `tls-client` (indica cliente)
- `dh <parámetros diffie-hellman>` (en serv.)
- `ca <cert. CA>`
- `key <llave privada>`
- `cert <certificado>`

Otras directivas y tunning

- `persist-tun`
- `persist-key`
- `down <script>`
- `inetd <wait|nowait>`
- `comp-lzo`
- `ask-pass`
- `ping <segundos>`
- `ping-exit <segundos>`
- `ping-restart <segundos>`