Bluetooth remote Mount Beta tutorial by P3lo

Tested on a BT4 landscape

Voici un tutorial assez a l'arrache que je n'ai pas encore fini mais qui pourrais vous mettre sur la voie du phreak bluetooth.A noter que l'ordre des commandes sont surement décalés , ok c'est un bout de console mais sa peut aider. Les addresses mac ont été censurées. Ces bouts de code s'utilise avec un moteur de recherche.

lsusb
Bus 005 Device 002: ID 0a5c:2101 Broadcom Corp. A-Link BlueUsbA2 Bluetooth

root@bt:~# hcitool dev
Devices:
	hci0	00:13:36:F5:0F:CA
root@bt:~# bluetoothd apt-get install gnome-vfs-obexftp
root@bt:~# apt-get install gnome-vfs-obexftp
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  gnome-vfs-obexftp
0 upgraded, 1 newly installed, 0 to remove and 131 not upgraded.
Need to get 31.8kB of archives.
After this operation, 147kB of additional disk space will be used.
Get:1 http://archive.offensive-security.com pwnsauce/universe gnome-vfs-obexftp 0.4-1build1 [31.8kB]
Fetched 31.8kB in 0s (52.5kB/s)
Selecting previously deselected package gnome-vfs-obexftp.
(Reading database ... 259797 files and directories currently installed.)
Unpacking gnome-vfs-obexftp (from .../gnome-vfs-obexftp_0.4-1build1_i386.deb) ...
Setting up gnome-vfs-obexftp (0.4-1build1) ...

root@bt:~# sudo apt-get install nfs-kernel-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libgssglue1 libnfsidmap2 librpcsecgss3 nfs-common portmap
The following NEW packages will be installed:
  libgssglue1 libnfsidmap2 librpcsecgss3 nfs-common nfs-kernel-server portmap
0 upgraded, 6 newly installed, 0 to remove and 131 not upgraded.
Need to get 458kB of archives.
After this operation, 1417kB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://archive.offensive-security.com pwnsauce/main libgssglue1 0.1-2 [22.3kB]
Get:2 http://archive.offensive-security.com pwnsauce/main libnfsidmap2 0.20-1

[23.2kB]
Get:3 http://archive.offensive-security.com pwnsauce/main librpcsecgss3 0.18-1 [32.4kB]
Get:4 http://archive.offensive-security.com pwnsauce/main portmap 6.0-6ubuntu1 [36.2kB]
Get:5 http://archive.offensive-security.com pwnsauce/main nfs-common 1:1.1.2-4ubuntu1.1 [192kB]
Get:6 http://archive.offensive-security.com pwnsauce/main nfs-kernel-server 1:1.1.2-4ubuntu1.1 [152kB]
Fetched 458kB in 3s (118kB/s)
Preconfiguring packages ...
Selecting previously deselected package libgssglue1.
(Reading database ... 259806 files and directories currently installed.)
Unpacking libgssglue1 (from .../libgssglue1_0.1-2_i386.deb) ...
Selecting previously deselected package libnfsidmap2.
Unpacking libnfsidmap2 (from .../libnfsidmap2_0.20-1_i386.deb) ...
Selecting previously deselected package librpcsecgss3.
Unpacking librpcsecgss3 (from .../librpcsecgss3_0.18-1_i386.deb) ...
Selecting previously deselected package portmap.
Unpacking portmap (from .../portmap_6.0-6ubuntu1_i386.deb) ...
Selecting previously deselected package nfs-common.
Unpacking nfs-common (from .../nfs-common_1%3a1.1.2-4ubuntu1.1_i386.deb) ...
Selecting previously deselected package nfs-kernel-server.
Unpacking nfs-kernel-server (from .../nfs-kernel-server_1%3a1.1.2-4ubuntu1.1_i386.deb) ...
Processing triggers for man-db ...
Setting up libgssglue1 (0.1-2) ...

Setting up libnfsidmap2 (0.20-1) ...

Setting up librpcsecgss3 (0.18-1) ...

Setting up portmap (6.0-6ubuntu1) ...
Starting portmap daemon....

Setting up nfs-common (1:1.1.2-4ubuntu1.1) ...

Creating config file /etc/idmapd.conf with new version

Creating config file /etc/default/nfs-common with new version
Adding system user `statd' (UID 121) ...
Adding new user `statd' (UID 121) with group `nogroup' ...
Not creating home directory `/var/lib/nfs'.
Starting NFS common utilities: statd.

Setting up nfs-kernel-server (1:1.1.2-4ubuntu1.1) ...

Creating config file /etc/exports with new version

Creating config file /etc/default/nfs-kernel-server with new version
Starting NFS common utilities: statd.

Exporting directories for NFS kernel daemon....
Starting NFS kernel daemon: nfsd mountd.

Processing triggers for libc6 ...
ldconfig deferred processing now taking place
root@bt:~#

installation de p3nfs
http://www.koeniglich.de/p3nfs.html
P3nfs

Description:

P3nfsd is a Symbian (Psion/Nokia/Sony-Ericsson/etc) to UNIX/Linux communication program. It allows you to mount the file systems of the Phone/PDA on your UNIX machine. This means that you see all the filesystems of the Phone/PDA as a filesystem on your UNIX machine, and you can copy/backup/edit any file on the Phone/PDA with your preferred tools on the UNIX machine.

Notes:

o The NFS protocol is only used between the server and the OS, the server and the client on the deivce talk a primitive proprietary protocol.

o Since some files on the phones are opened exclusively by applications (Calendar/etc), these files cannot be read. p3nfs right now is not the tool of choice for backuping phones

---

wget http://www.koeniglich.de/packages/p3nfs-5.19.tar.gz
root@bt:~# cd /root/bluetooth\ hack/
/!\ si ya des erreur lors du make c'est pas trés grave
root@bt:~/bluetooth hack# tar xf p3nfs-5.19.tar.gz
root@bt:~/bluetooth hack# cd p3nfs-5.19

root@bt:~/bluetooth hack/p3nfs-5.19# sh configure
checking for gcc... gcc
checking for C compiler default output file name... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ANSI C... none needed
checking for gcc... /usr/bin/gcc
checking for AIX... no
checking for strerror... yes
checking for additional libraries... checking for socket in -lsocket... no

```
checking for gethostbyname in -lnsl... yes
checking for svcudp_create in -lrpcsoc... no
checking how to run the C preprocessor... gcc -E
checking for egrep... grep -E
checking for ANSI C header files... yes
checking for sys/types.h... yes
checking for sys/stat.h... yes
checking for stdlib.h... yes
checking for string.h... yes
checking for memory.h... yes
checking for strings.h... yes
checking for inttypes.h... yes
checking for stdint.h... yes
checking for unistd.h... yes
checking sys/ioctl.h usability... yes
checking sys/ioctl.h presence... yes
checking for sys/ioctl.h... yes
checking sys/errno.h usability... yes
checking sys/errno.h presence... yes
checking for sys/errno.h... yes
checking sys/ttold.h usability... no
checking sys/ttold.h presence... no
checking for sys/ttold.h... no
checking for stdlib.h... (cached) yes
checking for mount table... /etc/mtab
checking for default serial line... /dev/ttyS0
checking EPOCR5 SDK... missing
checking Series60.V1 SDK... missing
checking Series60.V2 SDK... missing
checking Series80.V1 SDK... missing
checking Series80.V2 SDK... missing
checking UIQ.V2 SDK... missing
configure: creating ./config.status
config.status: creating Makefile
config.status: creating server/Makefile
config.status: creating pkg/p3nfs.spec
config.status: creating client/epoc32/nfsapp/Makefile
config.status: creating client/epoc32/nfsapp/version
config.status: creating doc/p3nfsd.1
config.status: creating server/config.h
```

```
root@bt:~/bluetooth hack/p3nfs-5.19# make
cd server; make all
make[1]: Entering directory `/root/bluetooth hack/p3nfs-5.19/server'
gcc -O2 -Wall -I.   -c -o mp_main.o mp_main.c
gcc -O2 -Wall -I.   -c -o mp_mount.o mp_mount.c
mp_mount.c: In function 'dosystem':
mp_mount.c:243: warning: missing sentinel in function call
gcc -O2 -Wall -I.   -c -o nfs_prot_svc.o nfs_prot_svc.c
gcc -O2 -Wall -I.   -c -o nfs_prot_xdr.o nfs_prot_xdr.c
```

```
gcc -O2 -Wall -I.   -c -o mp_pfs_ops.o mp_pfs_ops.c
gcc -O2 -Wall -I.   -c -o mp_serial.o mp_serial.c
mp_serial.c: In function 'close_012':
mp_serial.c:220: warning: ignoring return value of 'dup', declared with attribute
warn_unused_result
gcc -O2 -Wall -I.   -c -o mp_inode.o mp_inode.c
gcc -O2 -Wall -I.   -c -o mp_xmit.o mp_xmit.c
mp_xmit.c: In function 'dump_data':
mp_xmit.c:133: warning: pointer targets in passing argument 1 of 'sprintf' differ
in signedness
mp_xmit.c:144: warning: pointer targets in passing argument 1 of 'puts' differ
in signedness
mp_xmit.c:151: warning: pointer targets in passing argument 1 of 'puts' differ
in signedness
mp_xmit.c: In function 'getbyte':
mp_xmit.c:349: warning: pointer targets in passing argument 1 of 'dump_data'
differ in signedness
gcc -O2 -Wall -I.   -c -o crc.o crc.c
gcc -O2 -Wall -I.   -c -o pty.o pty.c
pty.c: In function 'init_pty':
pty.c:201: warning: missing sentinel in function call
pty.c:144: warning: ignoring return value of 'dup', declared with attribute
warn_unused_result
pty.c:145: warning: ignoring return value of 'dup', declared with attribute
warn_unused_result
pty.c: In function 'shell_feed':
pty.c:224: warning: ignoring return value of 'write', declared with attribute
warn_unused_result
gcc -O2 -Wall -I.   -c -o tcp.o tcp.c
tcp.c: In function 'init_tcp':
tcp.c:65: warning: pointer targets in passing argument 3 of 'getsockname'
differ in signedness
tcp.c:77: warning: pointer targets in passing argument 3 of 'accept' differ in
signedness
gcc -lnsl  -o p3nfsd mp_main.o mp_mount.o nfs_prot_svc.o nfs_prot_xdr.o
mp_pfs_ops.o mp_serial.o mp_inode.o mp_xmit.o crc.o pty.o tcp.o
cp p3nfsd ../bin
make[1]: Leaving directory `/root/bluetooth hack/p3nfs-5.19/server'
cd client/epoc32/nfsapp; make all
make[1]: Entering directory `/root/bluetooth hack/p3nfs-
5.19/client/epoc32/nfsapp'
make -sf Makefile.UIQ.v2 clean
make[2]: Entering directory `/root/bluetooth hack/p3nfs-
5.19/client/epoc32/nfsapp'
Makefile.UIQ.v2:7: /local/gcc-3.0-psion-98r2/lib/makerules/eikon: No such file or
directory
Makefile.UIQ.v2:8: /local/gcc-3.0-psion-98r2/lib/makerules/defines.UIQ.v2: No
such file or directory
make[2]: *** No rule to make target `/local/gcc-3.0-psion-
98r2/lib/makerules/defines.UIQ.v2'.  Stop.
make[2]: Leaving directory `/root/bluetooth hack/p3nfs-
5.19/client/epoc32/nfsapp'
```

```
make[1]: *** [all] Error 2
make[1]: Leaving directory `/root/bluetooth hack/p3nfs-
5.19/client/epoc32/nfsapp'
make: *** [all] Error 2
```

```
root@bt:~/bluetooth hack/p3nfs-5.19# make install
mkdir -p //usr/bin
install server/p3nfsd //usr/bin
mkdir -p //usr/share/man/man1
cp doc/p3nfsd.1 //usr/share/man/man1
mkdir -p //usr/share/doc/p3nfs-5.19
cp doc/* //usr/share/doc/p3nfs-5.19
cp bin/*.sis client/*/opl/*.opl client/epoc16/nfsc/nfsc.app //usr/share/doc/p3nfs-
5.19
```

```
root@bt:~/bluetooth hack/p3nfs-5.19# cd /mnt
root@bt:/mnt# mkdir psion
```

```
root@bt:/mnt# /etc/init.d/bluetooth restart
Stopping bluetooth: bluetoothd.
Starting bluetooth: bluetoothd.

root@bt:/mnt# hcitool scan
Scanning ...
        00:12:34:56:D4:94       n/a
        00:1F:9D:B2:CD:5D       n/a

root@bt:/mnt# hcitool dev
Devices:
        hci0    00:50:13:37:0F:CA
```

```
root@bt:/mnt# rfcomm bind /dev/rfcomm0  00:12:FD:C0:D4:94 13
root@bt:/mnt# ls -l /dev/rfcomm0
crw-rw---- 1 root dialout 216, 0 Mar 23 23:46 /dev/rfcomm0
root@bt:/mnt# p3nfsd -series60 -tty /dev/rfcomm0 -user root
```

Greetz xxello
ES, CWH