BOFH meets SystemTap

Adrien Kunysz
adrien@kunysz.be
Krunch @ Freenode

DC4420, London, UK
22 March 2011

BOFH

BOFH

+

SystemTap

Blah blah blah.

Demo time!

purplesniff.stp

sniffing IM conversations
out of libpurple

ptysnoop.stp

eavesdropping on
a pseudo terminal

nomp3.stp

forbidding access
to specific file names

kbdsniff.stp

a keylogger

hidemod.stp

hiding SystemTap
with SystemTap

Questions?

http://stapbofh.krunch.be/
adrien@kunysz.be