BOFH meets SystemTap

Adrien Kunysz
adrien@kunysz.be
Krunch @ Freenode
GSM:9397

27C3, Berlin, Germany
30 December 2010

SystemTap as a rootkit framework for lazy hackers

- three lines of ”code” to sniff IM conversations out of libpurple (bypassing all encryption)
- snooping on pty: 5 lines
- preventing users to play .mp3 files: 5 lines
- sniffing all keyboard input (fully decoded): 13 lines
- hiding the stap modules themselves: 30(ish) lines
- [your evil idea here]

References

- `http://stapbofh.krunch.be/`
- `adrien@kunysz.be`
- Krunch on Freenode
- 27C3 GSM 9397
- I am looking for a job :)