International Journal of PoC || GTFO
Issue 0x00, a CFP with PoC

An epistle from the desk of Rt. Revd. Pastor Manul Laphroaig
pastor@phrack.org

August 5, 2013

1 Call to Worship

Neighbors, please join me in reading this first issue of the International Journal of Proof of Concept or Get the Fuck Out, a friendly little journal for ladies and gentlemen of distinguished ability and taste in the field of computer security and the architecture of weird machines.

In Section 2, Travis Goodspeed will show you how to build your own antiforensics hard disk out of an iPod by simple patching of the open source Rockbox firmware. The result is a USB disk, which still plays music, but which will also self destruct if forensically imaged.

In Section 3, Julian Bangert and Sergey Bratus provide some nifty tricks for abusing the differences in ELF dialect between exec() and ld.so. As an example, they produce a file that is both a library and an executable, to the great confusion of reverse engineers and their totally legitimate IDA Pro licenses.

Section 4 is a sermon on the subjects of Bitcoin, Phrack, and the den on iniquity known as the RSA Conference, inviting all of you to kill some trees in order to save some source. It brings the joyful news that we should all shut the fuck up about hat colors and get back to hacking!

Delivering even more nifty ELF research, Bx presents in Section 5 a trick for returning from the ELF loader into a libc function by abuse of the IFUNC symbol. There's a catch, though, which is that on amd64 her routine seems to pass a very restricted set of arguments. The first parameter must be zero, the second must be the address of the function being called, and the third argument must be the address of the symbol being dereferenced. Readers who can extend this into an arbitrary return to libc are urged to do it and share the trick with others!

Remembering good times, Section 6 by FX tells us of an adventure with Barnaby Jack, one which features a golden vending machine and some healthy advice to get the fuck out of Abu Dhabi.

Finally, in Section 7, we pass the collection plate and beg that you contribute some PoC of your own. Articles should be short and sweet, written such that a clever reader will be inspired to build something nifty.