

# 1 With what shall we commune this evening?

Neighbors, please join me in reading this eighth release of the International Journal of Proof of Concept or Get the Fuck Out, a friendly little collection of articles for ladies and gentlemen of distinguished ability and taste in the field of software exploitation and the worship of weird machines. If you are missing the first seven issues, we the editors suggest pirating them from the usual locations, or on paper from a neighbor who picked up a copy of the first in Vegas, the second in São Paulo, the third in Hamburg, the fourth in Heidelberg, the fifth in Montréal, the sixth in Las Vegas, or the seventh from his parents' inkjet printer during the Thanksgiving holiday.

We begin our show tonight in Section 2 with something short and sweet, an executable poem by Morgan Reece Phillips. Funny enough, `0xAA55` is also Pastor Laphroaig's favorite number!

We continue in Section 3 with another brilliant article from Micah Elizabeth Scott. Having bought a BD-RW burner, and knowing damned well that a neighbor doesn't own what she can't open, Micah reverse engineered that gizmo. Sniffing the updater taught her how to dump the firmware; disassembling that firmware taught her how to patch in new code; and, just to help the rest of us play along, she wrapped all of this into a fancy little debugging console that's far more convenient than the sorry excuse for a JTAG debugger the original authors of the firmware most likely used.

In Section 4, Pastor Laphroaig warns us of the dangers that lurk in trusting The Experts, and of one such expert whose witchhunt set back the science of biology for decades. This article is illustrated by Boris Efimov, may he rot in Hell.

In Section 5, Eric Davisson describes the internals of TCP/IP as a sermon against the iniquity of the abstraction layers that—while useful to reduce the drudgery of labor—also cloud a programmer's mind and keep him from seeing the light of the hexdump world.

Ange Albertini is known to our readers for short and sweet articles that quickly describe a clever polyglot file in a page or two. In Section 6, he finally presents us with a long article, a listing of dozens of nifty tricks that he uses in PoC||GTFO, Corkami, and other projects. Study it carefully if you'd like to learn his art.

In Section 7, BSDaemon and Pirata extend the `RDRAND` trick of PoC||GTFO 3:6—with devilish cunning and true buccaneer daring—to actual Intel hardware, showing us poor landlubbers how to rob not only unsuspecting virtual machines but also normal userland and kernel applications that depend on the new AES-NI instructions of their precious randomness—and much more. Quick, hide your AES! Luckily, our neighborly pirates show how.

Section 8 introduces us to Ryan O'Neill's Extended Core File Snapshots, which add new sections to the familiar ELF specification that our readers know and love.

Recently, Pastor Laphroaig hired Count Bambaata on as our Special Correspondent on NASCAR. After his King Midget stretch limo was denied approval to compete at the Bristol Motor Speedway, Bambaata fled to Fordlandia, Brazil in a stolen—the Count himself says “liberated”—1957 Studebaker Bulletnose in search of the American Dream. When asked for his article on the race, Bambaata sent us by WEFAX a collection of poorly redacted expense reports<sup>1</sup> and a lovely little rant on Baudrillard, the Spirit of the 90's, and a world of turncoat swine. You can find it in Section 9.

Section 11 is the latest from Ben Nagy, a peppy little parody of Hacker News and New-Media Web 2.0 Hipster Fashion Accessorized Cybercrime in the style of Gilbert and Sullivan. Sing along, if you like!

Finally, in Section 12 we do what churches do best and pass around the old collection plate. We don't need alms of Dollars or Euros, so send those to Hackers for Charity in Uganda.<sup>2</sup> Rather, we pass the plate to ask for your doodles and your sketches, your crazy ideas that work well enough to prove the concept, well enough to light up the mind, well enough to inspire the next lady or gentleman to do something clever and strange.

---

<sup>1</sup>*Bambaata, if you're reading this, please call me. Your Amex is beyond its limit after you expensed two “Charlie Miller kitchens,” and we had to reject payment in the amount of \$20,000 USD to “You Better Belize It Bail Bonds.” Oh, and if by chance you happen to be arrested in Brazil, please ask the Federales when the impounded H2HC 2013 conference badges will appear on Ebay. —PML*

<sup>2</sup>This isn't a joke, and we're not being snarky. Send money to HFC.