

19:13 What clever things have you learned lately?

*from the desk of Pastor Manul Laphroaig,
Tract Association of PoC||GTFO.*

Dearest neighbor,

Our scruffy little gang started this самиздат journal a few years back because we didn't much like the academic ones, but also because we wanted to learn new tricks for reverse engineering. We wanted to publish the methods that make exploits and polyglots possible, so that folks could learn from each other. Over the years, we've been blessed with the privilege of editing these tricks, of seeing them early, and of seeing them through to print.



Now it's your turn to share what you know, that nifty little truth that other folks might not yet know. It could be simple, or a bit advanced. Whatever your nifty tricks, if they are clever, we would like to publish them.

Do this: write an email in 7-bit ASCII telling our editors how to reproduce *ONE* clever, technical trick from your research. If you are uncertain of your English, we'll happily translate from French, Russian, Southern Appalachian, and German.

Like an email, keep it short. Like an email, you should assume that we already know more than a bit about hacking, and that we'll be insulted or—WORSE!—that we'll be bored if you include a long tutorial where a quick explanation would do.

Teach me how to falsify a freshman physics experiment by abusing floating-point edge cases. Show me how to enumerate the behavior of all illegal instructions in a particular implementation of 6502, or how to quickly blacklist any byte from amd64 shellcode. Explain to me how shellcode in Wine or ReactOS might be simpler than in real Windows.

Don't tell us that it's possible; rather, teach us how to do it ourselves with the absolute minimum of formality and bullshit.

Like an email, we expect informal language and hand-drawn diagrams. Write it in a single sitting, and leave any editing for your poor preacherman to do over a bottle of fine scotch. Send this to pastor@phrack.org and hope that the neighborly Phrack folks—praise be to them!—aren't man-in-the-middleing our submission process.

Yours in PoC and Pwnage,
Pastor Manul Laphroaig, T.G. S.B.

Studebaker

**"Studebaker wagons
certainly last a long time"**

"I have had this wagon twenty-two years, and during that time it cost me only \$6.00 for repairs, and that was for setting two tires."

"And after twenty-two years of daily use in good and bad weather and over all kinds of roads, I will put this wagon against any *new* wagon of another make that you can buy today."

"Studebaker wagons are built of air-dried lumber and tested iron and steel. Even the paint and varnish are subjected to a laboratory test to insure wearing qualities."

"No wagon made is subjected to as many tests or is more carefully made than a Studebaker. You can buy them of Studebaker dealers everywhere."

"Don't listen to the dealer who wants to sell you a cheap wagon, represented to be 'just as good' as a Studebaker."

Farm wagons, trucks, dump wagons and carts, delivery wagons, buggies, surreys, depot wagons—and harness of all kinds of the same high standard as the Studebaker vehicles.

See our Dealer or write us.

STUDEBAKER **South Bend, Ind.**

NEW YORK CHICAGO DALLAS KANSAS CITY DENVER
MINNEAPOLIS SALT LAKE CITY SAN FRANCISCO PORTLAND, ORE.