Humility and hacking

This is my year of change. One of the things on my list is to become a better hacker. Another is to tell more of my stories, lest I finally go insane or die in a bizarre hangliding accident involving a sheep and lose them all. This post kinda covers both.

There's a saying: "everyone knows the good hackers are; nobody knows who the great ones are". Well, I know some of the great ones: the ones who broke things way ahead of everyone else, who pulled off unbelievable stunts but never ever went public, and they taught me a lot when I was younger (they didn't always realise they were teaching me, but hey, it's in the blood). And yes, I broke into a lot of things; I hated the privilege of secrets, enjoyed the finesse of entering without being seen and yes, on occasion the privilege of being a young woman in a world that saw young women as a non-threat (I loved that prejudice, but only in that particular setting). (side note: people and organisations are really very mundane, with the occasional interesting highlight. This might also be why I'm very very difficult to surprise).

And then I grew up, went straight and worked for the government (kinda sorta: there was a bit of overlap there). I don't think I ever lost my hacker spirit, in the original sense of hacker: that of drilling down into a system to really understand how it works, how it could work, and all the other possibilities within its build but outside its original design. There's an argument that I may have hacked a few large organisations, and not in the breaking in sense, and at one time made a living out of doing it; I might also have a bad habit of fixing things just because they're there.

But I have missed the breaking-in part, and although I'm now at a stage in life when most people have settled down happily with their families, with steady jobs and responsibilities they'll stay with for probably a long while, I find myself alone again with the freedom to do almost anything. And yes, I fill my spare time with social-good things like journalism credibility standards, crisis support, teaching and belief hacking research, but I still feel the pull of trying to understand something physical, to have the language to talk to my tribe.

All of which was an over-grandiose preamble to "I'm getting old and rusty and I should get humble about my current lack of skills, get my ass in gear and learn to break stuff". This note is really for anyone thinking about doing the same thing, a breadcrumbs of places to start. I'm using my background in AI as a guide for what I'm aiming at, and I've started by:

- going to local and not-so-local infosec groups (nysecsec, defcon, bsides, mlsec)
- asking hacker friends for pointers on how to get started (turns out I have a *lot* of friends who are hackers...)
- following people who put out interesting hacker news, and reading the things they point at
- reading books, sites and posts on theory
- most importantly, starting with the practicals: course exercises and capture the flag to tune my brain up, examining code from attacks, doing some light lockpicking, thinking round the

systems I have.

There's no malice in this: I'm not about to break into military servers, or dump out sensitive site contents; I'll be content to break my own stuff, to tune my brain back up again (with the plus side of choosing a better gym lock for myself) and work on the intersection of hacking and DS/AI. It's been a long year already, and the conflicts around us on the internet aren't likely to let up anytime soon, and we'll need more people who can do this, so it seems sensible to me to be prepared...

Some of those places to start:

- https://isc.sans.edu/forums/diary/What+Can+You+Learn+On+Your+Own/22386/
- Books, e.g. https://github.com/Hack-with-Github/Free-Security-eBooks/blob/master/README.md
- Conference recordings, e.g. from https://www.irongeek.com/ (I'm liking the Bsides talks at the moment)
- Online capture the flags, e.g.:
    - https://microcorruption.com/login (you might find these pages helpful: fun with assembly, MSP430 manual, ascii)
    - ctftime.org
    - http://pwnable.kr/
    - http://reversing.kr/
    - https://cryptopals.com/
- Online and IRL practical courses

It's a long time since I manipulated assembler and read logs and intent as easily as reading English, but I'll get back there. Or at least to the point where I can build things that do that themselves.