Honeypot

Honeypots are a pretty big deal and a very interesting way of implementing proactive security to your infrastructure. Sadly, not enough are using them. (Properly due to a lack of knowledge about them).

Norse is a company that provides honeypots to companies that wish to add them to their infrastructure. They have a very cool presentation on the traffic that is going on for some of these honeypots. Visit their site and enjoy the show over a cup of coffee.
URL: http://www.norse-corp.com (click the "Live Attack" button)

Kippo (SSH honeypot)

I have setup a Kippo/Cowrie honeypot. It can be found at:
Web interface: http://home.im2b.dk:8005/kippo-graph
SSH access: root@home.im2b.dk

- Try to go the web interface, and get a bit familiar with all the information that is being provided.
- Next try to SSH into the box. (Username: root Password: password) – Try to mess around on the box and see what you can do.
- Go to the web interface again and try to play the recording of you playing around inside the honeypot.

Setup a Kippo/Cowrie honeypot

Why not setup a honeypot yourself? If you have a Raspberry Pi, you can easily run it from that one (just like I am right now.).

In case you do not have a Pi right now, we can make a virtual machine that emulates the Pi and use that one for the entire setup. (You can also use any other Linux box of your choice – Pixel is just so tiny and sweet…).

Pixel VM

You can run install or install Pixel OS in a virtual machine (Vbox, VMWare, XenServer, ect.) – If you like, then you can also just use an already install Ubuntu VM.

Pixel OS: http://downloads.raspberrypi.org/pixel_x86/images/pixel_x86-2016-12-13/2016-12-13-pixel-x86-jessie.iso

Cowrie setup

Kippo is no longer being maintained. But there is a fork called Cowrie that is still under development. Below you will find some installation information about the honeypot.

- Cowrie: https://github.com/micheloosterhof/cowrie/blob/master/INSTALL.md

- Kippo-Graph: https://github.com/micheloosterhof/cowrie/tree/master/doc/kippo-graph

Web Security

There is a lot of nice training materials out there. Here are some of the sites available, where we/you can test your skills and learn more:

Hack this site

URL: https://www.hackthissite.org

On this page, you can test (and learn) a lot of different things when it comes to web security. Start out by creating an account and then I recommend doing the challenges in:

- Basic missions
- Realistic missions
- Javascript missions
- Programming missions
- Application missions

The order you choose to solve the challenges in is completely up to you. ☺

OWASP Vulnerable Web Applications Directory Project

OWASP has a lot of training materials. You can find it all (as downloadable images) on the following site:

URL:
https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project#tab=Virtual_Machines_or_ISOs

You can pick anyone you like, they all have good challenges. If you are not sure how to run the application, you will be able to find a good guide by with the powers of google (or duckduckgo.com)