Hi, Jonathan.

Thank you very much for writing and congratulations in advance on your event. I'm happy to help however I can.

Forgive me, but this will be a long note. Also, feel free to email me directly at marc.blackmer@1nterrupt.com, and I'm on Skype as marcblackmer. My travel schedule is very hectic, so these are the best ways to get a hold of me.

OK, so...

Most of the participants at 1NTERRUPT events are high school-age with no technical computer experience, so we try to educate in a "non-traditional" way so it doesn't seem like another day of school, and more importantly, in a way that demystifies computer science. Where so many non-technical people think of computers as some deeply complicated, esoteric field, we want to replace that concept with one that lets them know they are just as capable as those of us in the profession.

My apologies if I repeat what Connor had written in his blog, but I want to make sure I at least cover the basics. First, the day was designed around a scenario or story, rather than just lessons. The participants were dubbed as new pen testers hired by an online gaming company called Xstation. The company is about to release their new online gaming experience that will change the whole industry, but they suspect an insider is leaking information to the bad guys. Not only are the participants asked to find vulnerabilities in their networks, but find the insider, if possible.

To set them up for the challenge, we covered the basics of ports and protocols, as well as general HTML, including commenting within the HTML. Then we introduced tools and concepts such as ipconfig/ifconfig ping, NMAP, mapping/mounting drives, and how to look at HTML code within the browser. The idea here was to develop a process for each stage of the challenge. For example, connect to the wireless network, determine your IP, run NMAP against the default gateway (we didn't want them scanning the subnet because other participants' machines would be subject to the scan), map/mount a drive if a share was open or fire up a browser and see what was on the page. By creating a repeatable process for each stage (a stage was defined by accessing a new network), we wanted them to build confidence and worry less about technology, and start using their critical thinking skills, which we all have - to one degree or another.

For the bulk of the participants, we more or less hid things in plain sight to give them clues, but by the same token, emulate how data can be leaked in real life. For instance, there would be a web page with text in white on a white background, so they either had to do a "select all" or look at the source to see the hidden message from the insider. We also used techniques like steganography for the more advanced participants like Connor and his friends.

Now, for the technical side:

We ran everything on Raspberry Pis, and I don't recommend that, unless you'll just have a handful of people. We crushed them, even with two mirrored networks to split the load. I would recommend real access points, at least, in front of the Pis. We had never load-tested, so we're putting together a new architecture which will use some old Linksys, or similar, wifi routers and VMs in the background. These will definitely get beat on to make sure they can handle it.

A buddy of mine put together the install scripts for each AP, but I heavily modified them. I'd written up all of the configs for somebody previously, and I'll find those for you along with the link to the original install script on GitHub. He was using Python to emulate web services, and I'd replaced that with Apache, because I wanted to build out the web pages and links more fully. In hindsight, I should have used lighttpd.

There was also a problem with keeping hostapd and dhcpd running at the same time. For instance, hostapd would start just fine, but wlan0 wouldn't have its IP address, so dhcpd wouldn't start as it was supposed to hand out addresses on wlan0. I specifically had to use ifconfig to re-assign wlan0's IP address and subnet mask. If I used, ifdown/ifup, it would kill hostapd. I'd since come across an article that recommend removing a specific utility on the Pi, but the name fails me at the moment. Once I'd done that, I haven't had this issue yet, but again, I haven't tested under load.

All of the APs were hidden around the building in order to get the participants up and moving, and I highly recommend that. Sitting all day kills them, and who wants to do that on a Saturday?

OK. I'll end it here, but am happy to answer any questions you have.

Thanks.

- Marc