BlackHat 2012 , DefCon XX, and NoP Sled Goodness!

Josh Michaels, 2012-31-07

Hello all!   I just landed back in seattle, after 11 days in Las Vegas. It was a rambunctious 11 days! I was in training classes with the Offensive Security Crew, then time at BlackHat briefings, and finally Defcon 20.

BlackHat Trainings:

If you have ever considered taking a class from the folks at Offensive Security, stop considering it. Take it. Stop reading right now and go sign up. Seriously. I had the pleasure of taking the Pentesting with Backtrack Course at BlackHat. The class was lead by Johnny Long, along with a whole pack of 1337 Offensive Security folk. In 4 longs days, we learned about everything from creative NoP Sledding (and other assembler fun), payload injection, testing frameworks, and of course a slew of tools, including BackTrack.

Why do I think this course is outstanding? Excellent teachers, challenging material, and the ability to go as deep as you want to into each topic. By the end of the second day, we had already hand crafted different attacks and debated different ways to fix it.

As for the other

BlackHat Briefings:

A slew of great talks, but even more important.. a lot of great hallway conversations.

Defcon XX

It was.. Spectacular. The talks were great, the crowds were deal-able and the contests were groovy! I tried my hand at Capture the Packet again this year, after our team won it last year. We rolled in ready to fight. It was a fun match, but in the end, we didn't make it. Capture the Packet is a network forensics "jeopardy" contest, run by the Aries Security. Riverside and his crew put together a great game. The network flow included new,custom stenography, traffic floods, fluff, and evil payloads in the packets that would crash poor contestants systems/apps. Let me tell you, there is nothing more frustrating than being mid stream on a tcpdump to have your wireshark lock in the middle of a contest. Hats off to the winners and to the Aries group for all their AWESOME work.

For those who have never been to Defcon, let me give a little insight into the diverse populous that attends Defcon. I spend my time at Defcon working as a Security Goon (with the best team anyone could ask for). I was working a door for a talk on Sunday morning and took a moment to chat with the humans(attendees) waiting in line. First person I spoke with a programmer from a midwest medical institute. The next person was a barista at "" while taking some courses here and there in security. Behind him was an older lady, waiting patiently. We got to talking and it turns out, she was a retired Air Force General (from the cyber side).

So in the span of 3 people, I had a code monkey, a coffee master, and a commanding officer, all hanging out with the same purpose, to learn.   It just proved the point again that Defcon provides opportunities and interesting topics for people from all walks of life.

If you missed defcon 20… you missed out, but all is not lost! Snag the DVD's when they come out, and enjoy.

Alright, off to bed for this tired monkey!