

Interview: SANS Pen Test Summit Part 2 - Johnny Long

The SANS WhatWorks in Penetration Testing & Ethical Hacking Summit with Ed Skoudis brings together a number of authors, researchers, and actual practitioners of pen testing, the summit will not only give a view as to where we stand as a community right now but also where we are headed in the future. Joining Ed will be a number of celebrated hackers (the positive connotation of the term) including Google Hacking Expert, Johnny Long, and the man behind the Metasploit Project, HD Moore.

I once had a conversation of Ed Skoudis regarding career choices and advice. He indicated that he often gets asked how others can have a career like his. Barring the inevitable warnings of "careful what you wish for," he graciously shared a story with me. In short, he and a number of other friends in the industry sat down for dinner to answer the same question that others now put to Ed. "Hey. I want to do what that guy does. How do we do it?" This special set of interviews will give you a brief glimpse into what will be explored at the summit itself as well as a look into the how these gentlemen "Did it." Each of these three superstars will be asked the same three questions followed by additional questions specifically focused for that individual. Here we go!

Part 1 - Ed Skoudis | Part 2 - Johnny Long | Part 3 - HD Moore

del.icio.us

Discuss in Forums {mos_smf_discuss:Editor-In-Chief}

First three questions to be answered by Ed, Johnny and HD (All answers below provided by Johnny Long):

1. I would love to have a career just like yours. How did you get where you are and what career advice can you give?

The best career advice I can give is to build your work around what you love. If you pursue your passions, you will be successful. Oh, and work to live. Don't live to work.

2. Could you share with us your thoughts on balancing your special projects with your day jobs and why it's important to you to give back to the security community?

I think the term "community" tends to confuse things. What we're really talking about here is basic relationships between people. No successful relationship is one-sided. In an academic (security) environment, the goal is to advance the field and to learn. This is difficult in a vacuum. If you share what you know with one person, that person will likely return the favor. To flip that around, if all you do is leech, the relational ratio will eventually shut you down.

3. All three of you are very successful while remaining on the ethical side of hacking. Can you offer words of wisdom to

encourage others to follow the same path?

No matter how fun it seems at the time, think twice before doing it. Keep clean because trust is difficult to reclaim.

Questions Specifically for Johnny Long:

1. What prompted the creation of johnny.ihackstuff.com but more importantly your willingness to share your techniques and the GHDB with the security community at large?

My URL was meant to be a simple, concise "business card". By handing someone my web address, they know exactly who I am and what I do. Cute, huh? The GHDB started as a list of silly things my team and I found on Google. But it was the commentary that made it fun and kept it alive. Eventually people started sending in their own findings, and it was perfectly natural for me to post them and attribute the source. I've never been one to pass off someone else's effort as my own, despite what some have said. Those that work with me know that I attribute, and they back that up with their actions--they're still there supporting me.

2. Google Hacking for Penetration Testers, Volume 2 was recently released. Can you give us a quick idea as to what is new/updated in this version?

We dug into Google services, like the API, Google Calendar, Gmail, etc. We also talk quite a bit about open source information gathering, showing how an individual can single handedly launch a very effective infogathering campaign, with amazing results. I've also got to mention that every single query, screenshot and bit of text from the first volume has been updated, to make sure that everything works as expected. A lot changes in four years.

3. Your talk entitled "No Tech Hacking" was given at a number of events last year and has now been expanded into a book of the same name. You have also been on the speaking circuit for years as well as contributed to several other books. If one of our readers wanted to advance their career through speaking and writing, what would be the first step you would recommend they take?

I can give the same advice for both writing and speaking: do it a lot. Even if you don't have anything to write or say, just do it. These are skills that get better with practice. You have to be comfortable in your own skin to excel at either of these, and they aren't easy things to do. So if you want to be a writer, sit down every day and write. Set a schedule and word count and stick to it. When it comes time to write something real, organize your thoughts (outline!!), and be prepared for your first half hour to suck. Ignore the voices in your head telling you your writing skills suck. Focus on your intended audience (not the ivory-tower types in your industry) and create a work you would like to read. Handle editing separately. Writing is "hot" (as Stephen King would say) and rolls to a boil. Editing is cool and objective. Don't mix them. Handle them in separate sessions. Read books about writing (Stephen King's On Writing, Lamotte's Bird by Bird are both excellent, even if geared towards fiction) and just do it. With regards to speaking, spend time crafting your talk. Know it intimately before you share it with the world. Video tape yourself and watch it critically--over and over and over again until you don't annoy yourself with your own preso. Then, unleash it on a peer, then a group of peers, crafting as you go along. Once you hone your craft you won't need to do this every time... You'll know what sucks and what doesn't.

4. You are very well known not only for Google hacking but also for your philanthropic endeavors. For example, all of the proceeds of "No Tech Hacking" goes to www.aoet.org, an organization aimed at empowering widows and orphans left in the wake of the HIV/AIDS pandemic. You also founded Hackers for Charity which is a great way for those looking to advance their careers to donate to a worthy cause and in turn get credible experience to add to a resume. Can you tell us how inform our readers on what is expected and what can be learned by getting involved in Hackers for Charity?

From a volunteer standpoint, Hackers for Charity is about sharing your gifts, whatever they may be. Our community is such an amazing place, chock full of amazing talent. A very small percentage of that talent focusses on breaking things and doing illegal stuff. Your "unimportant" gifts can change lives when applied properly. By volunteering for Hackers for Charity, you can make a difference in this world, and by working on projects, you can also advance your career. Whether or not you care about being all altruistic, I think volunteers will discover that amazing things happen when they shift their focus to the world around them.

--Johnny Long

<http://johnny.ihackstuff.com/>

Donald C. Donzal

Editor-In-Chief

The Ethical Hacker Network

Additional Resources:

[EH-Net Page on GPEN](#)

[EH-Net Forum Discussion on GPEN](#)

[SANS 560 - Network Pen Testing & Ethical Hacking](#)

[SANS What Works in Penetration Testing Summit](#)