

Interview: SANS Pen Test Summit Part 1 - Ed Skoudis

The field of penetration testing, or ethical hacking as it is commonly described, is one of the fastest growing areas in the realm of Information Security. Whether that is attributable to the growing number of regulations such as HIPAA, SOX, GLBA et al or perhaps it is the fact that many hackers have grown up and now have families to support. Or just maybe it is the real fear today that many organizations are garnering more press attention for recent data theft incidents as opposed to their products. No matter how you look at it, penetration testing is becoming a maturing and legitimate profession.

Ed Skoudis of Intelguardians has been an author, instructor and professional penetration tester for the better part of 15 years. The SANS Institute has been a highly regarded organization extolling the virtues of security education, certification and research for quite some time as well. Together they have put together a summit specifically dealing with penetration testing as a profession. 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!

del.icio.us

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

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

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

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?

Regarding how I got to where I am… I was hatched in pod 0728690101, was a high-school computer geek (I adored my Commodore-64 and lusted after Amigas), studied Electrical Engineering undergrad, and got my Masters from… do you really care about that? Seriously… I think that some folks get a little too hung up on educational credentials in this business. At my company (Intelguardians), when we look at new hires, we focus on people who can do

amazing work, regardless of their formal educational background. I've seen some absolute wizards with no formal training, yet I know some managers who won't hire such a person at all. That's a darn shame.

Anyway, when I got out of college (Carnegie Mellon, if you insist), I started working at Bellcore, originally in operator services ("What city, please?") and then on payphones ("Please deposit 25 cents"). Both arenas were rife with fraud, so I started getting involved in investigating anti-fraud technology when this whole Internet thing exploded in 1993. I moved from anti-fraud work directly into information security, helping the Baby Bells secure their legacy telephone networks and burgeoning IP networks. I began doing penetration testing, incident response, architecture reviews, and forensics. Man, those were the days! I remember thinking how cool it was to be working on that stuff. "Just a few years out of college, and now, you're going to pay me a salary to hack the telephone companies?" It was an incredible blessing.

Through various acquisitions and divestitures, I started doing the same kind of work for banks, government agencies, and many other organizations. Throughout, I've tried to learn as much as I can about given waves of technology changes. That's a beautiful thing about infosec. Things change so quickly that even new people can dig in, learn a lot about a new technology, and then help improve its security.

For career advice, I encourage people to do some sort of security research and publish their results. One of the beautiful things about information technology is that it has democratized and egalitarianized (Is that a word? It is now!) research. You can come up with interesting and useful findings without a million-dollar lab. Just sit in front of a Windows box and take a hard look at the nooks and crannies of the OS. You'll find weird and wonderful stuff that might be flawed. Kick tires. See what blows up. Use search engines to discern the limits of other people's knowledge and explore where they've left off. For example, about three years ago, I decided to embark on researching the Windows command shell (cmd.exe), to see if I could make it do stuff that people didn't know about. I learned a lot about WMIC, FOR loops, the SC command, and much more, and began writing articles about them. The cost? Nothing but my time. The benefits? I'm better at doing my job, and I hope I've helped others.

Another bit of career advice involves writing. Having the ability to express deep technical ideas in a grammatically correct, understandable, and engaging way is vital. If your writing stinks, take a writing course. It'll do wonders for your career. Good writing should work on many levels, rather like a protocol stack. Perhaps we should call it the Writing Control Protocol (WCP). In my view of writing, Layer 1 involves having decent grammar and spellig.* Layer 2 involves sentence structure. Vary the length, structure, and style of your sentences so that they are not merely noun-verb-prepositional-phrase again and again. Mix it up a bit. Layer 3 involves the topic itself. Choose something interesting to write about. Layer 4 is about passion. Make sure you write about something that you love or at least find interesting. If the topic is dull, try to convince yourself that it is interesting. Layer 5 is about style. Try to use unusual words now and then. Think about crazy but potentially meaningful analogies that people might gravitate to or remember. Be quirky without being freakish. If you can't write well at one or more of these layers, take a course to help you improve on a given layer, mastering Layer 1 first and then working your way up the WCP stack. Also, realize that Layers 3 and higher need to be tailored to specific audiences. I don't write with the same style in a technical deliverable that I do in, say, interview responses for Ethicalhacker.net.

Of course, I hesitate to jot down any of this advice about writing techniques, as I've probably made at least one faux pas at each of these levels in this interview so far, with many more mistakes to come. Think of those mistakes as purposeful, designed as a way of teaching through counter-example. Yeah, that's it.**

* I know; that was on purpose. Just seeing if you are paying attention.

** Of course, if you do discover any mistakes, they were on purpose, done for pedagogical reasons.

*** Oh, and too many meaningless footnotes can get annoying. Call that WCP Layer 6.

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?

Much of the information security community is a lively, friendly place, with fascinating people looking to explore technology and improve the sorry state of modern security. Sure, there are some sociopaths in the mix. But, for the most part, we are part of a great extended family of infosec folks. Every one of us that is responsible for securing a system is

part of that family, and we can help each other. You don't have to be a flashy researcher or infosec genius to come up with real-world experiences and advice to help others. Have you come up with a good way of doing something in your job? Have you learned a lesson the hard way? Sanitize your findings and share with others. Don't charge for everything. I know... you've gotta feed your family, but at least put some things out there for free to help others. It's the right thing to do, and can help you make some great friends. Humans are social creatures, and knitting yourself into the fabric of the information security world by giving back is incredibly rewarding.

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?

It may sound simplistic, but I recommend that folks stay on the good side, because... well... it's good. Of course, there is an inherent benefit to society for people to avoid criminal and/or unethical behavior. Beyond the societal benefits, I would suggest that there are also some important selfish reasons for staying on the good side. First off, it keeps you out of jail. Yes, you can make some serious cash by being evil, but you have to be really careful and skilled to avoid prison, at least if you operate in a country with reasonably diligent enforcement of cyber crime laws. It must be a huge headache for evil people to have to look over their shoulder constantly, knowing that they will likely make a careless mistake someday and end up in an orange jump suit with a free multi-year gym pass in the Big House. Secondly, you can make some reasonably decent money by being good. Companies and government agencies desperately need hard-working, talented information security pros, and are usually willing to pay them a decent wage. And, thirdly, outside of jail and monetary factors, being evil can have a significant negative impact on your whole being — your body and soul. Over time, your evil will manifest itself not only in your career choice, but in everything you do, and ultimately, your physical appearance. Check out Oscar Wilde's *The Picture of Dorian Grey*. Dude... that's a creepy story, but based on a lot of truth.

Questions Specifically for Ed Skoudis:

1. There comes a time in one's career when a professional leap of faith must be considered. What pushed you over the edge to leave the safety of your gainful employment and start your own company?

Over ten years ago, back when I was working in the Bell System, I started doing some side jobs, writing an article here, doing a presentation there, just trying to contribute to the community as best I could. People then started to pay me money for doing these side jobs. It's kinda funny how it started out — I was so naïve. I was doing presentations at various infosec conferences for free, not even thinking about getting paid. I then did my first talk for SANS back in May 1999. A few weeks after the session, I got a check in the mail. I thought there must be some mistake, so I called SANS and told them that they mistakenly sent me some money, and that I'd be happy to send it back or tear up the check. They told me that there was no mistake, and that I had earned the money. I remember thinking how cool that was. I should have saved the check.

I proceeded to do more talks, write more articles, and eventually wrote my original *Counter Hack* book, making a little money on each item, using my evenings to work on these side jobs. Then, one morning in 2002, I was driving to work at my day job. Idly passing time on my 30-minute commute, I started to calculate how much I was making on my side jobs. I had never really brought it all together before, but I just sat there in my car calculating that income in my head, waiting to pay a toll on the Garden State Parkway. What I came up with astounded me. It's not just that I was making more money on my side jobs than on my day job, but I was making twice as much! I couldn't believe it. You know how in the movies when a character makes a major discovery, and everything just changes in the cinematography — the camera angles get all different, the color saturation alters, the characters look different? Remember how the Grinch looks when he hears the Whos starting to sing at the end of that Seussian video? That's what happened to me at that point. I'd like to say that I turned my car around and drove home, but I went to work that day, put in a full day's effort, and resigned within the week. I started my own company within a month.

That's my story. I encourage other folks to do work on the side, provided that they are allowed to do so by their employers. See where it leads. Do some things for free to help the community. Do other side work for pay, making sure you try to provide immense value to people.

2. How does IntelGuardians decide who to hire, what services to offer and how to market security services in a highly competitive space?

We focus on hiring the very best people we can find, folks who have great skills and vision in the information security

space, who have contributed to the community. We're looking for well-rounded people. And, no, I'm not referring to their waistlines. Instead, we want folks that can operate in many technical areas instead of just one (primarily penetration testing, digital forensics, architecture review, and deep software analysis). We also focus on people that have stellar communications skills – people that are comfortable speaking to large audiences, talking one-on-one with customers on both technical and business topics, and writing with clarity and in an interesting style. We typically hire people that we've known for some time, having had the opportunity to observe their capabilities in action.

Let me give you a couple of examples. We brought Tom Liston on board based on the stellar writing of his handler diaries at the Internet Storm Center, his amazing work on the free LaBrea Tarpit tool, and the great malicious code research he does. We hired Kevin Johnson because of his excellent work on the free BASE front-end for Snort, his presentations for SANS, and the excellent research he's done. We look for people like these when we are hiring. In fact, shortly after Tom joined Intelguardians, Mike Poor and I were discussing what kind of person we should look for in our next hire. I said simply, “We need Listons... lots of Listons.” Matrix fans should recognize that quote. Sorry, I couldn't resist.

No, two giant racks of virtual Tom Listons did not immediately appear around Mike and me. Tom is unique, thank goodness. But, he is a great example of the kind of people we look for in building our company.

3. You recently completed a new course specifically on network penetration testing and ethical hacking. Can you share with us the birth of the idea for the SANS 560 Course and why you decided to share so many experiences in the class from your own career as a penetration tester?

I've never worked harder in my life than over the five months I spent writing SANS Security 560. I'm extremely happy with the results. But, let me back up a bit. Over the last year or so, SANS started getting a lot of requests from attendees about offering training in professional penetration testing. People told us that they wanted in-depth, hands-on pen testing training that covered both hard-core technical stuff and a solid methodology for performing high-quality tests in a safe manner. Based on all these requests, I was extremely honored when SANS asked me to write a brand-spanking-new course on network penetration testing and ethical hacking.

I don't take these kinds of opportunities for granted, so I put everything I have into the course. I worked every single day for five months (weekends, Thanksgiving, Christmas, New Years, and more). I wrote it based on over a decade of my own penetration testing experience, but I wanted to go even further than my own background. I contacted some of the best penetration testers I know, close friends who could help guide me on what the course should include. I canvassed them for their best tips and secrets, ways to avoid significant risk, methods for saving immense amounts of time, and little technical tricks that differentiate world-class pen tests from more average faire. I contacted Mike Poor for in-depth protocol stuff and false positive reduction. I spoke with Matt Carpenter about the best ways to use exploits in real-world tests. I worked with Jay Beale on a lot of the hard-core UNIX and Linux kung fu in the class, along with really deep password tests. I contacted Kevin Johnson for some nifty web app attack concepts. Tom Liston provided some Windows wizardry here and there. I even sent some requests via Jay Beale to HD Moore for a few small tweaks to Metasploit for the exercises I was writing, and he made the changes, for which I'm immensely grateful.

Throughout the development process, I would call most of these guys on a regular basis, telling them what I'd put in the course so far and asking them how to make it even better. Sometimes, in these discussions, I'd give them a trick that was new to them, and they'd thank me. And, rather often, they'd take a technique I'd been using for years, and showed me how to make it even better. While I wrote every word on every slide, the influence of these guys permeates the course.

And then, a funny thing happened. You see, each guy that I consulted with knew about the stuff I addressed to him. But, none of my collaborators knew about the contents of the similar discussions I was having with all the others. Thus, an idea that I might have had originally was refined by my discussions with Matt Carpenter, and then bounced off of Jay Beale, and then further improved through interactions Mike Poor. In the end, when each of these guys saw the final course, they told me that they were stunned by the amount of useful methodology, technical tips, and powerful tricks included in the course. I was delighted by their response.

My ultimate goal for the SANS 560 course is to help people become better penetration testers, whether they do testing in-house for their own enterprises or as third-party testers working for security consulting firms. Even for those people who don't perform testing themselves, I wanted the course to show what a professional penetration test should

include, so that they can evaluate the tests that they are paying for to make sure they are getting the value they deserve.

4. A great way to advance your career is to teach. What advice would you give to those who would like to become instructors?

I'll share some advice that Alan Paller gave me long ago when I started doing presentations for SANS – make sure every presentation you give has something that will help people do their jobs better, regardless of the length or topic of the talk. If the presentation is 15 minutes, 30 minutes, 1-hour, 1-day, or 6-days, make sure there is always a take-away technique or concept that will make people better at their profession. I've tried very hard to live by that rule, and apply it across all of my public speaking.

I've found that the notion applies especially well when writing slides. If my gut tells me something isn't quite right with a slide, I apply Alan's advice – Does this slide help people do their jobs better? If the answer is “No”, I either change it so that it does, or kill it. You have to be truthful and ruthless in judging your own material. It's not easy throwing out a slide that you just spent an hour writing, but sometimes it is necessary.

Oh, and one more thing… practice. I'm not talking in front of a mirror here. Instead, practice delivering your presentation in front of real people. Present in front of your friends. Present in front of your family. Heck, present in front of anything that has a pulse, just so you can work on your delivery and timing. Test what works and what doesn't. That should help make you a better presenter.

5. It's been said that companies have lost numerous man-hours from employee participation in the Skillz Hacking Challenges on The Ethical Hacker Network. Why are these challenges so near and dear to your heart?

I really love writing these movie-themed technical challenges, because they give me a chance to try to be creative and technical at the same time. It's fun blending a movie theme into a technical challenge that will keep people's interest. I brainstorm for several days trying think of a movie theme and technology that match.

If you think about the challenges, we actually write them under several constraints, designed to make the challenges appeal to more people. These “challenge design criteria” are carefully integrated into each challenge to maximize the chance that people will actually read them and work on them. The criteria include:

- • They should be one to two pages long.

- • We try to write them so that pretty much everyone will think it is straightforward to solve, but, at the same time, we want really hard-core technical people to be able to chew on them for a couple of hours.

- • However, we don't want to require people to spend more than three hours solving them. These shouldn't be multi-day affairs.

- • We want people who work on the challenge to learn subtle but useful information, security principles and technical facts.

- • And, of course, we want them to be playful in their integration of the theme and the technical issues.

We try to work across all these constraints simultaneously, while delivering something interesting and fun.

But, at the same time, I don't want the challenges to be formulaic, following a simple pattern of a paragraph or two about a system that gets hacked, the same type of overlaid movie theme, a joke here and there that plays on the movie idea, a presentation of the evidence, and then the same set of four stale questions at the end. I like each one of the challenges to be as different as possible from all of the others. If you look at the challenges in their totality, some of them are set in the back story of the movie (When Trinity Hacked the IRS D-Base), some are set long after the movie timeframe (Hackers of the Lost Ark), some riff on themes from a movie without actually being set in it (A Christmas Story, Willie Wonka and the Chocolate Hackery, Charlotte's Website), and others are set inside a scene of the movie

(Star Hacks: Episode IV, a New Hack and Star Hacks: Episode V, The Empire Hacks Back). Another way to make the challenges different was to get my friends involved, having Mike Poor, Tom Liston, Kevin Bong, and Matt Carpenter write them from their own twisted and unique perspectives. I'm happy with how different each of their challenges were, especially Kevin Bong's Simpsons Challenge which was in comic book form for an awesome change of pace.

Now, here's the real magic of the challenges for me. The list of constraints, while hard to meet, actually forces us to be more creative, coming up with challenges that are better than they would be if we relaxed any one or more of the criteria. And, that's actually a major philosophy that I use when living my life. I have many predictable patterns (call them constraints if you want to) in my life. I have a simple car that gets me where I need to go, without a lot of flash. I think of it as /dev/car. Don't get me wrong — I want /dev/car to be very reliable, but it doesn't need to be out of the ordinary. I eat at a certain set of restaurants, often ordering the same kind of food. I guess that's /dev/food. I like tasty /dev/food, but it doesn't need to be highly varied or require a lot of thought. I wear pretty much the same kind of clothes each day (/dev/clothes). I wake up at about the same time, and go to bed at the same time.

Some would consider this a self-made prison, but I find that having this predictability allows me to build much more creatively on top of it all. If I had to choose what to wear each day, or what to order at my favorite restaurant, that's creative energy that I could better direct to my work or my family. From a work perspective, I'm constantly trying to brainstorm about what is new or interesting in the information security world, and how we at Intelguardians or SANS can help people cope with change in a creative way. From a family perspective, my wife and I try to do fun and different adventures for our kids, like hosting a formal Annual Daddy-Daughter Ball in our house, or doing a big camp trip with all the neighborhood kids in our backyard. The predictability and rhythm of the underlying minutiae of life allows me to do funky, quirky, and weird stuff on top of it. And, that makes life a lot more interesting and enjoyable for me. Thus, as weird or pretentious as it may sound, those simple little challenges are actually a manifestation of my philosophy on life.

--Ed Skoudis

Intelguardians

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](#)