

Interview: John Strand of Lake Missoula Group, PaulDotCom and SANS

By Brandon Harms, CISSP, CCNP, FCNSP, et al

A quick review of the Bureau of Labor Statistics Occupational Outlook shows us that ethical hackers will be in higher and higher demand over the next decade. With this demand, the need for a supply of highly qualified and professional information security personnel increases. The supply of highly qualified and professional personnel can only be created by organizations that can train and mentor them en masse, or rather, a large quantity of them relatively quickly. For ethical hackers the training material must be relevant, organized, and able to lay down the foundation on which one can build with real world experiences. More importantly, the delivery of said material must be engaging and from a respected source.

I recently traveled, metaphysically anyway, to the underground bunker in the Black Hills of such a source. The purpose of my journey was to interview SANS instructor, PaulDotCom staff member and Professor, John Strand. John has a unique background working with the government, commercial, and consulting industries prior to teaching that gives him insights into the art, learning path, and career outlook of the ethical hacker. During the week of the interview I sat through the SANS vLive! course, "Metasploit Kung Fu for Enterprise Pen Testing," and I was impressed not only with the material but more importantly, as emphasized above, the delivery of the material.

del.icio.us

Discuss in Forums {mos_smf_discuss:/root}

Before we dive into the interview, here's John's bio to get you up to speed:

John Strand currently is a senior security researcher with Lake Missoula Group and an instructor with the SANS Institute. As a certified SANS instructor he teaches: 504 "Hacker Techniques, Exploits and Incident Handling," 517, "Cutting Edge Hacking Techniques," and 560 "Network Penetration Testing" and is an author for SANS 464 "Security for Systems Administrators" and 580 "Metasploit Kung Fu for Penetration Testers." He is also member of PaulDotCom Security Weekly, the world's most listened to security podcast. He also regularly posts videos demonstrating the latest computer attacks and defenses at <http://www.youtube.com/user/strandjsgmail>. He started the practice of computer security with Accenture Consulting in the areas of intrusion detection, incident response, and vulnerability assessment/penetration testing. John then moved on to Northrop Grumman specializing in DCID 6/3 PL3-PL5 (multi-level security solutions), security architectures, and program certification and accreditation. In his spare time he writes loud rock music and makes various futile attempts at fly-fishing.

vLive! from SANS is their live, online training platform.

This isn't a prerecorded study aid -- these are live classes with top instructors!

SEC504: Hacker Techniques, Exploits & Incident Handling (starting 11/9) taught by Bryce Galbraith and John Strand

SEC542: Web App Penetration Testing and Ethical Hacking (starting 12/6) taught by Kevin Johnson and Seth Misenar

For 10% Off Everything SANS use Coupon Code: Connect_EHN10

And just in case you didn't get a good look...

'Nuff said? Then to the interview we go.

Brandon Harms (BH): Please describe your background and how you became interested in information security.

John Strand (JS): I became interested in information security while working with my family business growing up. We installed inventory and cash-register systems, and there were so many ways to break them. I remember spending hours in my father's office getting in trouble for messing things up. It occurred to me that the only way you really learn about something is by breaking it, then fixing it.

Later, when I was working at Accenture Consulting, I still had a knack for breaking things and fixing them. A penetration testing team came through that owned DOI as part of the Cobell lawsuit. They came to Accenture and asked if we could help prevent it from happening again. We said yes, and I jumped down the rabbit hole for good. Up until that point I had no idea you could make money doing this for a living.

BH: PaulDotCom was established long before you joined the team. How did you become part of the crew?

JS: Funny story... At the end of my interview, Paul said something to the effect of "come back any time!" The next week I did. I also brought another Tech Segment, so they let me hang out. The same thing happened the week after that. After about three weeks of this Paul asked if I wanted to become a member of the crew. He said it was contingent on me improving the beer I drank on the show. I live in South Dakota and getting anything other than Coors and Bud is a bit of a challenge.

They still have not kicked me off, so I must be doing OK.

Also, Paul, Larry, Carlos, Mick and Mark all have a belief that what we are doing is making the Internet a safer place. We all consider ourselves very lucky to do what we love and contribute to the world in a positive way. Plus, the fact that we get to do it while drinking is awesome.

Name one other activity where drinking is a tax-deductible activity.

BH: SANS has a makeshift farm system of recruiting instructors. What was the process like for you in becoming one of SANS premier instructors?

JS: SANS is tough. There is a special intersection of brilliance and insanity that is required to do what we do. To become an instructor I had to teach two Mentor classes, four community SANS classes and something like four live fire conferences. It took me two years to get to certified level. BTW, "certified" means that you are cleared to teach at the major conferences and to groups greater than 50.

To become certified I had to go through the following:

• Teaching in below freezing temperatures when the heat went out in Oklahoma City in winter;

• Getting my crotch sniffed by a seeing-eye dog. Once is more than enough, but three times an hour leads you to believe that you need to bathe more;

- Getting lit on fire by another, unnamed SANS instructor;
- Teaching through ridiculous food poisoning (BTW, as an aside, don't ever take drugs from students);
- Having Mick Douglas as a student;
- And surviving the SANS Murder Boards.

What are the SANS Murder Boards? Good question! It is where you present 10 slides to the class author. While teaching the class author asks you the most insane, difficult and upsetting questions he/she can think of. I had my Murder Boards with Ed Skoudis. I still have nightmares. But this is a great process. There are a number of people who think that teaching this stuff is easy. It is a great way to introduce them to the difficult situations they will encounter in class in a safe and constructive environment.

BH: As a university professor, SANS instructor, and professional consultant you have a unique insight on career paths in InfoSec. What training path would you recommend for upstart pen testers or anyone looking to move forward with a career in information security?

JS: Do it as a hobby. Take your television and remove it from your house. Preferably with a very special blend of psychology... and EXTREME VIOLENCE. Replace it with VMs that you can attack. Start a blog and share your experiences, no matter how mundane you think they are. On PaulDotCom the basic Tech Segments get the most hits. The same is true with our videos. Why? Because there are a great number of new InfoSec pros looking for help and guidance. Be that guidance, even if you are just starting. Learn something new today? Post it. Tweet it. Blog it. Do a video.

Share everything, leave nothing behind. Then you will be on the right path.

BH: Describe the process of keeping information current in the courses you teach?

JS: There are a couple of things that can keep you in the loop. First, simply doing what we teach is a valuable asset. SANS is quite big on having instructors that are active in their subject area. They don't like to see full-time instructors. The second thing that is great is doing PaulDotCom. It takes a lot of work to come up with new stories and Tech Segments every week. Finally, interacting with students. There is a lot to be said for meeting 100+ InfoSec pros every month. We have one hell of a community, and we are so much better at sharing than we were a few years ago.

BH: Your vLive training is exciting and informative. Your passion for information security really comes through. What motivates you to help others learn what you know?

JS: I honestly feel that we have to get this right. I was having dinner with another member of the InfoSec community a few weeks back, and he said to me that security "gets in the way." The world would be a better place if we did not have to worry about attackers destroying things. I view what we do in the same light as Structural Engineering. These massive

buildings and awe inspiring structures would not be possible if it was not for the fact that countless other designs had failed before it. In security, we are constantly looking for flaws so as to make our environments more resilient to not just attacks, but other stress factors as well.

Also, I say this to all of my classes, if we do not get this right, a massive attack is going to happen. Then, we will have to deal with some ridiculous level of oversight either by the government, private sector or both. I do not want an Internet where all access is tracked by a unique certificate given to each user where their access is monitored and tracked. Some believe we are very close to that as it is now. The reason this scares me is that the bad guys will continue to find ways to bypass the controls that may be put in place. So the net security effect will be minor. However, it will place a tremendous burden on users. Further, years from now it could have a chilling effect on free speech.

BH: What's it like instructing in SANS vLive format?

JS: I can do it from home. That, and I seem to develop closer relationships with my students. It is nice to be able to take 6 days of material and spread it out over 6 weeks. It gives students a great opportunity to digest the information.

BH: What are your thoughts on industry trends and employment opportunities for information security?

JS: You are all going to have employment for a long time...

BH: With these industry trends in mind, what opportunities are out there specifically for pen testers?

JS: It is scary. I talk with a number of different people in this field, and it seems like there is no shortage of poorly secured environments. But they need to move beyond simple "I hacked your network!" views. The goal of a penetration test is to identify the risk associated with a particular set of vulnerabilities. It is not about getting shell. Chris Nickerson mentioned that you should never go to management bragging that you got shell in their environment, because they don't care. He is so right. My God, I just referenced Nickerson. Anyway, he is right. This is what we strive to teach our students in SANS 560: Network Penetration Testing. There is a lot of work preparing for a test and presenting the results in such a manner that management will understand the results and take action to mitigate the overall risk to their environment.

Also, as a tester, please look to describe the meta-issues that were discovered. For example, if you find an un-patched server the problem is not the missing patch. The problem is the organization lacks the processes and procedures to validate their patch deployment. There is always an underlying process failing.

BH: What resources do you use to keep up on the latest pen testing techniques?

JS: PaulDotCom, Ethicalhacker.net, Darknet, Attack Research, Eurotrash podcast, the GPWN mailing list, the PaulDotCom mailing list, Exotic Liability and the Metasploit mailing list. Most importantly, all of my students feed me cool tips and techniques.

BH: Is there a networked resource out there that you cannot gain access to? :)

JS: Of course there is. Any network can become one that a pen tester cannot break into. Just set the scope so it is hyper-restrictive. I have had tests where I have not gotten in. I know it is not kosher to say this, but it is true. I get a bit tired of hearing some people in our industry say they can get into anything. Complete crap. I had a customer who wanted a penetration test of their "environment" and they reduced the scope down to one IP address running SSH with key-based authentication. Everything else was off limits. Never mind the fact they had 32 other servers. Never mind the fact they had little to no SPAM filtering. No, management believed that if they were going to be hacked, it was going to be through their SSH server.

There were two lessons I learned from this engagement. The normal, rational people you work with in the proposal phase may not be the people you will work with to set the scope. The second thing I learned was that it is OK to fire customers every once in a while.

BH: Thanks John for your time and insights.

Brandon Harms is a Senior Information Security Consultant at Infogressive, Inc., headquartered in Lincoln, Nebraska. Infogressive is a security-centric information technology consulting firm. Brandon has held four industry accepted certifications:

• CISSP: Certified Information Systems Security Professional

• CEH: Certified Ethical Hacker

• FCNSP: Fortinet Certified Network Security Professional

• CCNP: Cisco Certified Network Professional

Mr. Harms is pursuing a Bachelor of Arts in Philosophy from the American Public University. He has worked for large telecom and financial firms in a variety of technology roles, including network security engineering, for eleven years. For four years Brandon was a System Engineer with a Cisco Gold Partner specializing in the architecture and deployment of security, telephony, and wireless systems across the country. He has also worked for the Dept. of Defense as a Russian linguist and network engineer. Prior to joining Infogressive as a security consultant, Brandon was a Senior Network Engineer in the Omaha area. In his free time, Brandon is a member of American Mensa and the Freemasons. He is married with three children and spends most weekends traveling to BMX tracks across the Midwest to support (finance) his 9 year old son's budding BMX career.