

Interview: SANS Pen Test Summit Part 3 - HD Moore

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 agreed to answer a few questions to help you with your career. 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}

Questions Answered by HD Moore:

Can you describe a typical day as a professional penetration tester?

(My answer to this is a little off-base, since I don't do pen-testing all day like I used to, and even then it was highly dependent on the specific job).

I joined BreakingPoint Systems in 2005 to head the security research group. Previously, I was splitting time between penetration testing, vulnerability scanner maintenance, and tool development. These days, I work on a wide range of projects, including vulnerability discovery, exploit development, reverse engineering, and application protocol research, with only a small part of my time going towards penetration testing and vulnerability assessments. My daily schedule has not changed much and my current role is still heavily focused on vulnerabilities and exploits.

On a typical day, I spend the first hour reading security mailing lists, browsing exploit repositories, chatting on SILC, and otherwise keeping up to date with the latest vulnerabilities. I've found that cramming my skull with the latest bug index helps with all sorts of tasks, including system administration (what do I need to patch), providing advice to IT (what should they patch and workaround), software development (what stupid problems do I need to avoid), and of course, penetration testing. Having a historical view of a product's vulnerabilities is invaluable when faced with a fully-patched application that is sitting between me and my target.

Once I catch up with the latest news, I make notes about which vulnerabilities I need to reproduce, write tools for, or otherwise investigate further. These notes are added to the queue, which feeds into my exploit development and research time.

When a serious vulnerability is identified in a software product, there is often a limited time window between when an advisory is published and when the vulnerable software is no longer available to the public. This is not the case with most open-source projects, but commercial vendors tend to be quick about removing the vulnerable versions of their software. Even if I don't have time to work on an exploit that day, getting a copy of the vulnerable software quickly is critical for future work.

After obtaining copies of the buggy software, the next step is reproducing the vulnerability. This is easy when there is a public exploit or example available, but can be time-intensive in cases where no information was released and the only thing I have is a copy of the patched and unpatched software versions. In situations like this, tools such as IDA Pro and BinDiff are required to nail down exactly where the problem is. Even with commercial tools, it's often easier to just prod at the service with a Ruby script or two instead of starting a full reverse engineering session.

Once I have code to reproduce the bug, the fun part starts. This involves making the crash reliable and finding ways to control the data in memory and the flow of execution. Finished exploits are rolled into the BreakingPoint product, often targeting multiple vectors for a particular issue.

The Metasploit Framework started from your our needs as a security professional. What prompted your desire to expand the project and eventually share it with the world?

In the original version of the framework, there were only sixteen exploits and a handful of payloads. I hoped that by opening the project to the world, it would convince other exploit developers to contribute and make the project better. In the long run, this worked out by bringing talented people in as developers and building a community of contributors.

Many organizations frown upon employee extra-curricular activities not specifically tied to the company. How does your employer, BreakingPoint Systems, feel about Metasploit, speaking engagements and the instructing you do? What advice can you offer those who are hitting a brick wall with their employers?

My freedom to work on outside projects was one of the key reasons I joined BreakingPoint back in 2005. The management at BreakingPoint realize that my side projects, such as Metasploit, directly improve the quality of the company's products and provide us with credibility in the field. With that said, I rarely spend work time on outside projects. My advice for anyone hitting a brick wall -- find a business reason to justify your work. If you can show the value of a project to your employer, you will have a much higher chance of getting it approved. In the case of open-source project, it's often easier to justify contributing to an existing project instead of trying to start a new one.

Metasploit is partnering with Offensive Computing's Val Smith and the SANS Institute to offer an intensive two-day training class on Tactical Exploitation at the Summit where the focus is on techniques that are not affected by patch levels. Can you expand on this and the course as a whole?

The Tactical Exploitation course expands on the talk Val Smith and I gave at BlackHat and Defcon last year. The premise is that vulnerabilities are transient and that effective penetration testing is knowing how to piece together enough information to identify relationships, then exploit those relationships to get access. The class covers a wide range of techniques, from data mining social networks, to stealing kerberos tickets, to attacks against wireless clients. With the abundance of information already available on tasks like port scanning, vulnerability assessments, and exploit use, we decided to go a different route and cover all of the odd-ball, but useful tricks we have picked up over the years. The result is a grab-bag of interesting techniques and exploit methods that alternate between hands-on labs and lecture.

Someone I know (who is the host of an upcoming Summit on Penetration Testing with SANS) suggested as a compliment that the song 'Cult of Personality' by Living Colour is the perfect theme song for you based mostly on the lyric, 'I exploit you. Still you love me.' You have also been the poster boy for the hacking community as of late. Do you feel that this detracts from or adds to your body of work?

There is a culture of fear within the security industry and nowhere is it felt more than within the ranks of the security analysts and engineers. For every warning of a major new exploit, there's an equal (implied) warning that sharing information about the issue will somehow result in Bad Things (TM) to the person or company who shares it. The worry is that if information gets out or an exploit is released, the company providing it will lose customers or be caught up in a lawsuit. The result is that the technical folks who need detailed exploit information can't find it and the security researchers who discovered it can't share it.

A large part of what the Metasploit Project stands for is sharing information, to those who need it, without censorship. The Metasploit Framework became a vehicle for doing this, along with a number of other smaller projects (anti-forensics, proxy decloaking, debian openssh keys, google malware searches, etc). If anything, my "poster boy" status is indicative of the frustration many security researchers feel when trying to share their own work. Having occasional access to a media soapbox helps me bring awareness to new security issues and get the word out about new projects that could benefit the community. -HD

-- HD Moore

<http://www.metasploit.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](#)