Interview with Rod Soto

Rod Soto is a security researcher and board member of HackMiami. He is a regular speaker at hacking conferences all over the country on the topics of penetration testing tools and methods, as well as the topic of digital civil liberties. Rod Soto was the winner of the 2012 Black Hat Las Vegas Capture the Flag hacking competition, and is the founder and lead developer of the Kommand&&Kontrol competitive hacking tournament series. He is currently a senior security engineer with the emergency response team of an information security corporation engaged in digital crime intelligence analysis, vulnerability assessments, penetration testing, and malware reversal.

You won the Black Hat hacking competition last year. How were you preparing for this competition? Is there any way to prepare? What advice you would give to those who would like to try themselves in such competition?

It was not easy and it took a lot of effort. I advise those who want to get better at playing CTFs to play as many as they can, save and follow write ups of those challenges you couldn't get and study and research as much as you can. Create your own lab and create challenges.

How do you improve your skills? Do you have any methods that have proven to be more effective than others? Could you share some with our readers?

Improving your skills depends on your dedication and willingness to learn new things. You need to be up to date and willing to learn new technologies and techniques that may not be easy at first and that require studying hard.

Why did you choose Information Security field for your profession instead of other Information Technology domains?

My background is mainly in system architecture, integration and administration. Throughout the years I became more focused on Information Security as it became more significant in the organizations I was working for, plus I always thought of information security as a very challenging and changing industry.

What do you consider so challenging in the field of Information Security? It seems that you have a thing for competitions, is this it or something else as well?:)

I do... :) It is a way of challenging myself to learn new things and to face and adapt to unknown scenarios.

What were the biggest challenges that you have ever experienced in the past, especially when you worked as a Junior Information Security professional?

Mostly access to the right information, I started becoming more knowledgeable as I started networking with colleagues, going to conferences and visiting hackerspaces. In many aspects of infosec you pretty much have to become an autodidact. You have to put in time, discipline and persistence to learn completely new things and in many cases with a high level of dificulty.

Do you have any suggestions for our readers? Especially for those who would like to become pentesters?

There are many books you can read or courses you can take but in reality you need a base knowledge and understanding in networking, operating systems, programming/scripting languages, application vulnerabilities and finally exploit creation even if you will never create one yourself.

Are there any specific personality traits that one should have in order to achieve success? What personality features are valued in this job?

Like many jobs I believe patience, persistence, tolerance to frustration, a strong work ethic and ability to adapt to change are fundamental personality traits needed to be successful.

What are the top 5 challenges for the junior IT professional who would like to learn and master skills in Information Security?

- Orientation on career direction
- Efficient learning habits
- Mentorship
- Financial Aid
- Time

Sounds like a good plan, but how to find a mentor? How did you found yours?

I am mostly self taught. I did take some courses and read lots of books but as far as a mentor – I have never had one nor do I have one now. I did find lots of help by attending a local hackerspace HackMiami and I met some great people at DEFCON. Basically going into the community helped me a lot when I was trying to learn new things. Finding a mentor is not easy but there are certainly people in the community that are willing to help newcomers. We do that at HackMiami.

Could you give few examples of learning habits that appeared to be efficient in your case? Maybe this will inspire our readers to look for their own...

I read at least one relevant book per month, I recreate as many vulnerabilities as I can as they are

published in my own lab. If I find I need to learn further about certain application or technology I then research about white papers, books and authors.

On the basis of your experience and expertise, what is the best methodology for learning and mastering Information Security?

Patience, persistence, discipline and the ability to tolerate frustration. This is not a field for the faint of heart.

How is the career path for being Information Security professional in terms of salary and position? Is the Information Security professional career path more promising and better than other IT professions?

Right now it is. the Information Security job market is dominated by employees. There are simply not enough people and there probably won't be for the near future. Financially speaking It is definitely one of the best places to be in the IT industry. As a career it has also become a very relevant and challenging field, but as with any industry one should not rely on it for unsubstantiated longevity.

What are the best pentesting tools in your opinion? Could you recommend some to our readers?

I am metasploit kind of guy but I always try to replicate vulnerabilities and exploits without using it. I think burp and acutenetix are great webscanners and of course there are plenty of open source tools. I look at pentesting as mix and match. I always have to be prepared to think outside the box and try new tools some of them I have to learn on the run.

What are your favorite methods for penetration tests? The ones you consider the most effective? Do you have a set with which you start each task?

Know your target very well and your tools and the rest will follow. Take your time to footprint, analyze and understand the environment you are probing. There are no "one" clicks.

What does HackMiami do? Is it a Information Security platform/group for Information Security minded people?

HackMiami is hackerspace based in Miami, FL. It is composed of mostly information security professionals and we focus on information security research and education. We also have a maker wing that focuses on open source robotics and general maker projects.

This maker wing sounds great. Could you tell us more about it? On what projects you are working on now?

Current projects are: Un-maned submarine, Micro drones, Fighting robots. Here is a video of the quadcopter built by one of our members: *http://www.youtube.com/watch?v=qn9Eq1mJ6Ks*.

Could you describe one of the completed and successful projects of this open source section?

See quadcopter video.

There are some areas that don't have such a nice initiative like HackMiami yet. Is it hard to establish a hackerspace? What things are required?

It is not easy. There are many challenges starting from financial support, potential liability and dealing with many different personalities. At the end of the day it depends on people's willingness to participate and support the hackerspace. You can always find a place to meet but if people are not showing up or participating then you won't get very far.

Malware, trojan as well as the latest cyber attacks are often ahead and unpredictable compared with most of the information security technology and tools. What suggestions do you have to prevent and minimize these kind of attacks?

I do believe that offense must drive defense. Understanding, analyzing, reversing and using malicious tools in your own lab environment will provide you the ability to visualize malicious attacker's mindset and preferred attack vectors. You can never be 100% secure but you can minimize and mitigate potential threats by keeping yourself up to date on tools, vulnerabilities and doing your own research, not only technical but also using open source intelligence tools.

Could you recommend some good links or reads about creating your own lab environment?

There are 3 books that will get you started in my opinion. One of then is Metasploit the Pentester Guide. Second is Professional Penetration Testing and third I would recommend the Web Application Hacker's Handbook.

How should one proceed with their own research? Could you give some tips for those who haven't done it yet?

Set up your lab. It does not cost much but it is important to have your own environment where you can experiment and break things without getting in trouble. You can use some of the open source hypervisors and operating systems publicly available on the internet.

What are best open source intelligence tools in your opinion? I think our readers will be interested in this very much.

In my opinion those tools have yet to be developed. I have experimented with some commercial and open source tools and I do not think they are at the right place yet. There is a lot of work to be done in this area.

If there were cyber attacks targeted a specific destination at the specific country, would that be possible to trace back the attacker(s) accurately?

Attribution is always very challenging and very difficult to prove. There are many methods and tools though that may give you a certain level of confidence that an attack came from a specific source. Again there will be a level of uncertainty. As to how an organization or country deals with that level of uncertainty would depend on their own policies and rules of engagement.

What is the most dangerous, unpredictable and untraceable cyber attacks that happened in the past few years based from your experience? Which industry was the main target of this kind of attack?

I have seen attacks directed to certain industries such as financial, infrastructure and major corporations. I definitely believe that SCADA infrastructure attacks are the most potentially dangerous attacks and the ones that may likely cause human casualties. I am not aware such event has happened yet, although governments and military contractors are training for these types of attack scenarios, both offensive and defensive. If a large scale SCADA attack takes place that results in loss of life, the most likely culprit would be a state sponsored attack.

How did it happen you became a founder and developer of competitive hacking tournament series?

I wanted an excuse to hang out with my friends and party doing what we love the most :). I thought it was cool to travel and do it in different places with different people and make it fun and challenging.

What was your objective to form Kommand && KonTroll competitive hacking tournament series?

Kommand && KonTroll is a computer security competition in a private environment where players are faced with different challenges. Most of those challenges are web based or infrastructure. We also have some binary reversal challenges, but that is not our focus. We try to make it as close to the "trenches" as we can, as we try to give players a view of the underground. We use publicly available software and vulnerabilities, or we modify targets to be vulnerable. The game also implies defense as players are allowed to attack other players. This game allows players to learn, experiment and practice with many information security tools and wares that they would otherwise not be able to use or work with at their current organizations.

How do you prepare the tasks for such tournament? Does it take long? Where you are searching for inspiration?

Yes it takes long... between 100 to 150 hours. I do heavy research on scenarios, cultures, characters, personalities, music, videos, history and real life scenarios. Every challenge tells a story, in some instances challenges could branch into whole new ctf. I try to make it relevant and I try to make it fun. I distribute challenges difficulty level in a way that allows players with different skills to be able to play and win the ctf.

You are involved in digital crime intelligence analysis, can you tell us more about it?

I can't without breaking my NDA. Sorry.

Cloud Computing and Virtualization technologies are getting more popular day by day. Do you think both technologies might be a new target for cyber attacks? Have you ever discovered the latest attack techniques done by attackers in Cloud Computing environment?

I do believe those technologies definitely introduce new risks and vectors of attacks. I do not believe that those technologies change attack methodologies I believe they simply add more attack surface and possible single points of failure for many organizations. Organizations must be careful of putting all their eggs in the "cloud", I myself have been involved in situations where cloud outages presented a level of availability that organizations were simply not willing to tolerate.

You give talks about digital civil liberties... What are the biggest threats in this area for computer users and mostly for security specialists and pentesters?

I gave a talk at DEFCON XX Skytalks along with some of my colleagues where we warned that regulation of such tools was not farfetched, and the need to address these tools as a right for law abiding citizens to research, study and to defend themselves. It does look though we are marching towards more regulation and possibly strict limitation and even prohibition like in some countries.

As far as digital civil liberties are concerned, what is your opinion about “hacktivism”? Is it a good way to prove the politicians wrong?

I am all for the right of people to dissent and protest as long as they do not break the law.

Do you have any plan to setup your own Information Security company in the future?

I have my own IT company called EITS and I also do work with with Information Security Services, Inc out of Miami, FL

Can you tell us few words about EITS? How it started and what kind of solutions/ products it offers?

My work was mostly system administration and support. It is now more towards security assessments and penetration testing.

Thank you Rod for this interview.

By PenTest Team