ThreatModeler™ streamlines and automates the entire threat modeling process by reducing the manual work. It incorporates abuse case modeling, to generate more targeted threats to individual functionality and associates mitigation steps to these threats. Below are the key features:

- Centralized threat management
- Threat pattern library
- Threat intelligence
- Policy compliance
- Actionable output
The Most Comprehensive Exhibition of the Fastest Growing Sectors of recent years in the Center of Eurasia

ISAF Safety & Health
Occupational Safety and Health Exhibition

ISAF IT Security
Information, Data and Network Security Exhibition

ISAF Smart Houses
Smart Houses and Building Automation Exhibition

ISAF Security
16th International Security and RFID Exhibition

ISAF Fire
15th International Fire, Emergency Rescue Exhibition

www.isaffuari.com

SEPTEMBER 20th - 23rd, 2012 / IFM ISTANBUL EXPO CENTER (IDTM)

THIS EXHIBITION IS ORGANIZED WITH THE PERMISSIONS OF T.O.B.B. IN ACCORDANCE WITH THE LAW NUMBER 5174.
Dear Readers!

You have asked us how to successfully begin your career and be successful on the job market as a skilled professional. Cut-throat competition and growing expectations towards the employees are factors that CEO’s as well as beginners have to face on a daily basis. This issue of PenTest Market strives to solve your dilemmas. We present the beginnings of those who are now on the top. We hope that their life stories, experience, opinions and solutions can be inspiration and motivation for you.

Our first meeting is with Carric Dooley, director of Foundstone. He tells about his first jobs and gaining experience in companies such as Coca Cola. You will learn which soft skills are the most important especially if you have to face clients. Carric, called “a walking technical encyclopaedia” shares with us his idea of a dream team. And if you want to know how speaking many languages can help you in various places and situations – this interview is for you.

In our next interview Anurag Agarwal, founder of MyAppSecurity describes his companies and its services. He judges the competence of a web application security professional. Switching between the jobs is never easy. Anurag tells us about his way to fit into a new role. Do you believe that secure coding is a myth? Check what he has to say.

Section Successful Pentester features Randy Naramore who will tell you what you should know before you pentest to make it as successful as possible.

Alexandro Fernández Rodríguez and Sameh Sabry are two security consultants who talk about their careers. From Alejandro you can also learn about the state of Information Security in Latin America. Furthermore, Alex speaks about some of the risk management frameworks he has used and top security risks when it comes to Financial Institutions. Moreover, the importance of coaching and mentoring for young talents is presented. Sameh Sabry reveals some challenges in the banking sector and latest pentesting tools and technologies that he finds interesting. For Sameh certifications do not mean you are a rock star. Find out what do they mean for him.

What are the good and bad sides of working for somebody and being your own boss? You can read about it in the interview with Stefano Maccaglia. He will also tell you about importance of education and his opinions on the idea that appliances can replace people.

In the interview with Tal Argoni you can read about approach to build an application and large scale code review. What is more, Tal presents some of the challenges he faces in application-based pen testing and his ways to stay motivated.

Johan Snyman prepared a small survey on the pentesting market in South Africa. If you are interested in situation and competition there – take a look. We end this issue with the program of Hack in Paris.

We hope that you will find this issue interesting and noteworthy. Thank you all for your great support and invaluable help.

Enjoy reading!
Malgorzata Skora
& PenTest Team
SECURITY TRAINING
Think about this – you must be able to sell
Carric Dooley, Director of Foundstone Services EMEA talks about dream employees and dream teams
by PenTest Team

WEB APPLICATION SECURITY
Web Application Security, Secure Coding with a glass of scotch – Aby Rao talks with Anurag Agarwal, Founder of MyAppSecurity
by Aby Rao
Is Secure Coding a myth?
Secure Coding and Secure Architecture is the most critical part of any application. I don't know why it's considered a myth. If we look at the problem as a whole, the web applications have been around for a long time and security has only been the focus very recently.

SUCCESSFUL PENTESTER
Before You Pentest
by Randy Naramore
Before you perform a penetration test you need to know what your end goal will be, whether it is to better secure your network or to gain compliance a penetration test is an in-va-luable tool if used correctly.

CONSULTING
About passion, teamwork, quality and loyalty with Alejandro Fernández Rodríguez, Specialized IT Security Consultant
by Aby Rao
Mr. Alejandro Fernández has a bachelor degree in computer science and a diploma in telecommunications and other one in management skills.

“Certifications don’t really mean you’re a rock star”
Sameh Sabry talks with Aby Rao about Crisis Management, Wireless Hacking... and Music
by Aby Rao

MALWARE
Stefano Maccaglia talks with PenTest about importance of Academic Education and Appliances Replacing People
by PenTest Team
I hate the idea that a software or an appliance can replace the skill and abilities of a good team of Pen Testers. I've heard this concept often, especially from the mouth of Sales people or from high ranked managers. Often I have demonstrated they are wrong...

HANDS-ON
The vulnerabilities out there are waiting to be found Tal Argoni, Penetration test team leader at 2BSecure for PenTest Market speaks about experience, motivation and challenges
by Aby Rao
At age 13, I met my cousin, and he showed me how two command lines cause denial of service to an Israeli Web site. I was intrigued by this and started looking for information at every opportunity that I had. Quickly I learned TCP and got answers about client-server application.

SURVEY
Penetration Testing in South Africa
by Johan Snyman
The pen-testing market in South Africa is small when compared to developed (and some developing) countries. To some extent this can be attributed to the slow growth of internet usage in the country and the difficulty faced by business to turn a profit with such a small target market.

MEETING
The Program of Trainings and Conferences for Hack in Paris
by Aby Rao
The event will be presented next June at the Convention Center to Disneyland Paris will include six training and 16 conferences: the opportunity for the ecosystem of IT security to be form on the practices of hacking and meet around international experts to inform about the reality of hacking, its challenges and its consequences.

Sameh Sabry is an experienced Security Consultant. He started his career at the age of 14 during his tenure with IBM, multinational firms while as well recently joining the banking sector.
PenTest Team: Please tell us about your technical background and professional services experience.

Carric Dooley: I got my start in information security in 1997 working for a company in Atlanta that did medical billing. They let a few of us dig around the network and identify security issues. I think contracted for Coca Cola Enterprise in Atlanta, and eventually wound up at Internet Security Systems for five years delivering various assessments. I joined the Foundstone Services team in the US in March of 2005, and stayed in that role as a Principal Consultant until June of 2008. I left McAfee to work for Microsoft in the UK on the ACE team, which provides security consulting services both internally and externally. I was then invited to return to the Foundstone Services team to help build a local presence in EMEA in December of 2009, and was subsequently offered the directorship to lead this effort.
in July of 2010. Since then we have grown from 1 (me) to 8 delivering consultants across 5 countries.

PT: You are the Director of Foundstone Services which is McAfee’s Professional Services team. Please tell us about your role and responsibilities within your team.

CD: As the director of Foundstone Services EMEA, my responsibilities range from business development to management of the financials and strategy, and sometimes I still deliver assessment services. I wear many hats, but I am focusing on business development and growth at the moment.

PT: How do you go about choosing a strong team to lead an engagement?

CD: To date, I have mostly sought candidates who have certain personality traits, interests, and certain level of community participation. Through my involvement with organizations like BlackHat and Defcon being able to interact with some of the people that shape this industry, and having been fortunate enough to have worked with some brilliant community rock stars along the way, I would say people who excel as consultants have an identifiable set of common traits. Confident, but not unjustifiably arrogant, able to work well with others, but not overly conformist (independent thinkers who challenge accepted conventions), self-motivation, and mature (at least in terms of work ethic). A little juvenile behavior is par for the course.

I have tried to lay a foundation of superlative industry thought leadership talent, with the intent to diversify more as we build the team, i.e. identifying and recruiting the next generation of “rock stars” that may not have the experience, but do have the right mix of aptitude and passion. In fact, right now we are looking for focused skill sets, like a web application and infrastructure penetration testing guru.

Long term, I feel balance is key with a focus on core business like penetration testing and forensics/IR, but my goal is to maintain as much harmony as possible for as long as possible, while allowing people to express themselves, and pursue their passion. If you love what you do, it doesn’t really feel like work.

PT: What are some of the soft skills you look for particularly from professionals who are client-facing?

CD: Having been a consultant for “a little bit”, there are some key soft skills I look for when considering a candidate.

Communication
Can you effectively communicate your point, and make your client feel like he/she is in the best possible hands for whatever situation they are in, be it a catastrophic compromise, or a routine assessment? This will often tie back to how well you can establish a rapport with a wide range of people, as well as level of confidence and mastery of the subject matter. I find alienating the client, or making them feel stupid isn’t all that productive, but seems to be a common tactic among security professionals. ;)

Capability
One thing I feel sums up a truly exemplary consultant is that you can put him or her in almost any challenging situation, and he/she will turn it into a windfall (like a quote from the movie “On Deadly Ground”: “You could drop this guy off at the Arctic Circle wearing a pair of bikini underwear, without his toothbrush, and tomorrow afternoon he’s going to show up at your pool side with a million dollar smile and fist full of pesos”). I have seen some amazing consultants take a frustrated, disappointed client who is complaining about the engagement, who after a short meeting, are ready to write songs about how much they now adore the delivery team. This is someone who will succeed at whatever they do. Consulting is expectation management – remember Scotty from Star Trek (under-promise/over-deliver).

This statement may turn off some of the more technical guys, but think about this – you must be able to sell. No matter what you do in life, you will be selling something, whether that be a product, a service... yourself, so it’s critical to be able to inspire and compel your client to allow you to assist them. The best way to achieve that in an honest way is to just believe in what you are saying. It’s not learning a sales pitch – it’s knowing your product, and being personally convinced about the quality and results. Everyone on the Foundstone Services team, first and foremost, wants to make our clients more secure than when we met them. The rest tends to work itself out.

PT: Within EMEA (Europe, Middle East and Asia – Africa; APAC is actually a different team), which is the most upcoming region when it comes to Information Security Architecture and implementation?

CD: Without even having to think about it: the Middle East. While the sales cycles can be long and painful, I have to say that this is a market ripe with opportunity. As stories of cybercrime become more and more the
norm, and the regularity of computer security incidents rises, pretty much everyone with an Internet presence is feeling the pain. Our investment in this region is just starting to pay off as the need for IT security consulting becomes apparent.

**PT: You have done extensive work in PCI section 11.3? What is section 11.3 and how did you contribute.**

**CD:** I have worked with a few clients since around 2005 on this subject (in fact one of my first projects at Foundstone was to help make sure we passed the certification testing). I also worked on assessing the PCI environment at Microsoft when I was on the ACE team.

PCI 11.3 basically says you need to have someone with penetration testing expertise beat on your PCI environment. A vulnerability assessment is a far cry from a penetration test (of course, depending on who you ask).

If you have ever heard George Carlin’s comparison of baseball to American football, this is a great basis (and general tone) for comparing the two (his routine is on YouTube, and it’s funny):

In a vulnerability assessment, you are scanning to identify vulnerabilities in the environment that might be used in an attack.

In a pen test, you are trying take advantage (with prejudice) of any mistake that the IT team has made, to do “the most damage possible”, exploiting any discovered data or hole to gain as much control as you can in the allotted time, with complete and systemic compromise being the end-goal.

I’m not saying don’t scan/assess – it’s essential as part of the strategy. I am saying don’t skip the hardcore testing, or your perception of the security of your environment will likely be incomplete (pronounced “flawed”).

**PT: You are the lead instructor of the Ultimate Hacking series. The course sounds fascinating, please tell us more.**

**CD:** Ultimate Hacking is really a track of courses. The first is a basic penetration testing methodology class. It covers material similar to some of the more popular certification courses, but the intent is to teach the student how to approach testing using a standard framework versus how to use specific tools. If you are asking the right questions in a structured, framework approach, then what you are testing is less important since knowing a specific tool or tools isn’t all that relevant. It’s a little like troubleshooting.

Ultimate Hacking Expert, is the next step on the infrastructure track, and adds more advanced testing techniques and concepts like what a basic stack overflow is, and how to exploit one.

Ultimate Hacking Web is focused on **Web Application Penetration Testing (WAPT)** methodology. Nick Murison is our lead instructor for that content.

Ultimate Hacking WiFi is something we added a few years ago, and was written by Brad Antoniewicz (he worked on Free-Radius WPE with Aruba Network’s Joshua Wright and presented a new tool at Shmoocon in 2007 for attacking WPA Enterprise). This covers wireless technology, and how to attack and defend mostly 802.11 with some coverage of RFID and Bluetooth security.

All of the classes are intended to be a practical, hands-on attack and defend experience. Images with a range of tools are provided to the student with various guided labs and then test case scenarios to allow them to try out what they learn during the course.

**PT: You have spearheaded several an enterprise risk assessment based on NIST 800-30, can you please share with us some high-level key observations or findings?**

**CD:** First and foremost – most companies do not have a true risk management strategy (or any security strategy in some cases), and “never” is a pretty typical interval for conducting a full IT Risk Assessment. Often information security managers find themselves adrift in a sea of “latest and greatest” shiny marketing terms and scare tactics with vendors brandishing new technology promising to make the whole headache of security go away forever. It becomes a vicious cycle of rolling out new tools to try and get ahead of the threat curve, but just like in our own lives, we often fail to take pause and think about what we are actually trying to achieve – what is our purpose.

First off – do you know what you have? I would argue that in any environment with more than a few hundred servers, the honest answer is “no”, or at the very least “not really”. Assets include your servers, buildings, data, people, applications, etc. If you don’t have a definitive list (or asset register), this is a good starting point.

Now figure out what’s important on a scale of say 1 – 4, 4 being “I can no longer make or deliver my widgets”, and 1 being “it would hurt, but we can still function”. Once you know what you have and what is important, determine the threats to those assets, and then enumerate the vulnerabilities. The last piece of this equation is Impact – what are the ramifications of the incident?

Once you can quantify the risk, the business can decide how it would like to treat it. Suddenly your information security program becomes a contextual risk
management program, and everything makes sense. You are guiding the business on how they can do what it is they do, but securely.

Now one thing is key because people tell me all the time “this is 101 basics Carric. I thought you would have something I haven’t heard before”. Knowing and doing are different things. When was your last pen test? Who did it? What were the results? What did you do with the results? If you want to know if all the stuff you bought was both worthwhile, and effectively deployed, ask someone who knows what they doing to break it for you. Consider it a pop quiz, and learn from it. You must have tactics to support the strategy, and one doesn’t really stand without the other.

I have worked with many clients who were convinced they were pretty secure. That was what their staff had been telling them after all. Presentation of findings often resulted in surprise, shock, bewilderment, a little soft crying... But seriously, don’t ask the butcher to bake your bread. It’s not his core competency.

**PT:** On your LinkedIn profile, someone mentioned that you are a walking technical encyclopedia. Did you ever consider writing a book?

**CD:** Well, someone was being very generous. I have helped other people with books (How to Break Web Applications by my friend Mike Andrews, and I have contributed a little content to the latest edition of Hacking Exposed 7th Edition). I do not feel anything I have is original enough to warrant a whole book. I’ll stick to collecting what I feel is interesting and useful information, and sharing it with clients, friends, and colleagues for now.

**PT:** If you were asked to build an Information Security Dream Team and you have the option to pick 5 team members, who would you pick and why?

**CD:** If I’m being completely honest – I don’t think I could do better than the current McAfee Foundstone Services team (both North America and EMEA). I am blessed to work with some of the brightest, well-rounded, expert, passionate (and sometimes almost scary) individuals in the world of security consulting. I left McAfee for a year and a half and came back because it’s home. It’s like the Cheers TV show song. Everybody knows your name, and they’re always glad you came. It’s a family.

**PT:** You have lived in several different countries. If you were to rate them based on most-livable place, which one would you choose and why?

**CD:** My honest answer – each place has its advantages and disadvantages. In the US, we can’t go see 1000 year-old castles, but have you ever seen Niagara Falls or the Grand Canyon? Wow! Since university, I have been fascinated by other cultures and languages, and I feel learning is living and vice versa. There are a lot more places I would like to live!

**PT:** In addition to English, you are fluent in Russian and conversational German. Has knowing several languages helped you in your professional career? Please give us any anecdotal examples.

**CD:** Well actually, my 2nd best language is French, but I would be over stating the case at this point to claim fluency. I was fairly fluent at one point, but find I don’t make the time I should to continue to improve my mastery. I should...

One reason I enjoy other cultures so much is that there is nothing like catching someone completely off guard with a question like “Nihon jin desu ka?” or “Er du Norsk?” Usually, there is initial shock that this bearded, 1m95 bald guy is attempting to speak something other than English, follows by a “How do you know that?”, but then it becomes something else rather quickly. It’s a rapport that you can’t really get any other way, and its exile rating and fun.

**PT:** We are curious to know how you got involved in studying Russian, Japanese, Spanish, Portuguese, Norwegian, and Gaelic?

**CD:** Honestly, each one kind of has its own story. I finished 1 1 years of French my senior year in high school, and my teacher said “I had a knack”. My dad spoke a little Russian, so I always wanted to learn some. My father was stationed in Japan for 2 years, and was fortunate enough to spend a summer in Yokosuka Chuo. Spanish is the US 2nd language, and we have vacationed in Mexico a couple times. We had some Brazilian friends back in Atlanta. One of my best friends is Norwegian. And with a name like Carric Dooley, could really not at least try and pick up a little Irish? I was recently in the Royal Berkshire hospital for a few days, and easily 60% of the nurses were Irish, so butchering a few phrases was a great way to pass some time (and they were delightful as well).

*Interview done by PenTest Team*
Aby Rao: You transitioned from a professional to an entrepreneur fairly recently. How are you fitting into your new role?

Anurag Agarwal: I started MyAppSecurity (http://www.myappsecurity.com) in May 2010. My experience at WhiteHat Security had been immensely valuable in being an entrepreneur. MyAppSecurity released a free product on threat modeling called ThreatModeler which can be downloaded from our website. Building a product has been an extremely challenging job but the great feedback from my peers in the industry just made every second worth the effort.

AR: Please, tell us about your company and services you provide.

AA: MyAppSecurity provides end to end software security risk management solutions in Web Application Security starting from the design to implementation phases of development. By integrating security starting from design phase, developing and maintaining secure applications are far more cost effective than the insecure applications.

MyAppSecurity helps companies establish processes, promoting awareness throughout the company and ensuring the processes are adopted by various development and QA teams. MyAppSecurity has released two products ThreatModeler and SDL+ which helps companies in helping developers build secure applications.

AR: You are involved in the OWASP Threat Modeling project. Please tell us about that effort and what professionals can gain out of that project.

Secure Coding and Secure Architecture is the most critical part of any application. I don’t know why it’s considered a myth. If we look at the problem as a whole, the web applications have been around for a long time and security has only been the focus very recently. Most of the applications were designed and coded insecurely in the past but it’s not feasible to rewrite the entire applications using secure coding practices. Those applications have to be patched rather than rewritten which is what is happening now. In my experience, more and more companies have started focusing on secure coding and have trained developers too but it’s more of a culture shift than just implementing a process and will take some time.
AA: OWASP Threat Modeling project was started last year after meeting with a lot of fellow owasp members at the OWASP summit. The existing threat modeling methodologies are not best suited for web or mobile applications. The project aims at building a standard threat modeling methodology which organizations can use internally.

AR: In what capacity are you involved in OWASP and WASC activities.
AA: I am a WASC officer. I started the Web Application Security Scanner Evaluation Criteria (WASSEC) but later on stepped down as a project leader when I joined Whitehat Security due to conflict of interest. Currently I am a project leader for OWASP Threat Modeling methodology. I have been associated with many other projects at both WASC and OWASP.

AR: As far as Web Application Security is concerned, there isn’t a single certification that stands out, do you have any recommendations or any thoughts on certifications in general.
AA: Web Application Security is a very broad field and goes beyond just the security professionals. With developers, architects, QA team, business owners and other stakeholders also responsible for various activities in a software development, it is difficult to have one certification trying to cater to all of them. That being said, I know SANS has come up with a certification (GWEB) which I personally think is better than the other certifications out there.

AR: If you are asked to judge the competence of an Web Application Security professional, what are some of the core competencies you would look for?
AA: Like I said earlier, it is difficult to have one person looking at all the aspects of web application security. Though there are few such professionals out there but they are few and far between. Due to the complex nature of the problem and various perspectives on this problem, OWASP also changed it’s approach in helping the community. Now with three different perspectives (Breakers, Builders and Defenders), it’s easy for people to understand, learn and approach web application security in a more structured way. I guess at some point in time, the certifications will come around and follow the same structure.

AR: Is Secure Coding a myth in reality? Can you give us some examples where embedding secure coding in SDLC has worked successfully?
AA: Secure Coding and Secure Architecture is the most critical part of any application. I don’t know why it’s considered a myth. If we look at the problem as a whole, the web applications have been around for a long time and security has only been the focus very recently. Most of the applications were designed and coded insecurely in the past but it’s not feasible to rewrite the entire applications using secure coding practices. Those applications have to be patched rather than rewritten which is what is happening now. In my experience, more and more companies have started focusing on secure coding and have trained developers too but it’s more of a culture shift than just implementing a process and will take some time. The other challenge is lack of tools for developers. We have tools for security testing but there is virtually nothing for developers to help in writing secure code. This is why we created ThreatModeler and as the product gets adopted; you will see a lot more secure applications by default as ThreatModeler helps developers in integrating security in various phases of an SDLC.

AR: Agile development has several benefits, how can one integrate security with the Agile Development Lifecycle?
AA: A common misconception in the industry is security is an overhead. Writing secure code does not take any additional time if you understand secure coding aspects irrespective of any development methodology. For e.g. using preparedstatement instead of createstatement is not going to take any extra time for a developer but it will go a long way in preventing sql injection. Similarly, checking for null is done by almost every developer, instead if they can check against a regex, they can implement a whitelist based input validation mechanism which will prevent against so many web application attacks. It’s about awareness, security tools and culture shift than any development methodology.

AR: You have some experience in education services, what is the best learning methodology to use when training people in Information Security?
AA: Any kind of training to developers would go a long way if you can make them work on one of their application or something which comes close to them. Developers want to understand the concept, they want to know inner workings and if it is something which is close to what they are already working on, it makes it easier for them to relate to their job. We at MyAppSecurity use a live ecommerce application in our training which they see so often when they do online shopping and as a result our training has been extremely appreciated by the developers.

AR: If you were to pick two top security conferences, which ones would you choose and why?
AA: Although there are many conferences, which cater to web application security these days but then again you cannot have one size fits all approach. Just like the Breaker, builder and defender concept for people, the conferences have to have the same approach. There are many conferences out there with information for breaker community but for builder and defender, I only know two – OWASP AppSec and SANS Application Security Summit.

AR: What role has professional networking played in your career?
AA: Professional networking is always helpful for various reasons. I personally enjoy meeting my peers and exchanging ideas and engage in thought provoking discussions. I was able to learn so much at OWASP Summit at Portugal last year where hundreds of appsec professionals gathered from all over the world. Apart from that, professional networking helped me in taking my product to the next level. I was able to tap into the experience and knowledge of my peers and gather feedback from them which helped me improve my product immensely.

AR: How do you de-stress yourself from the daily rigors of life?
AA: A glass of scotch. Maybe two :)

Interview done by Aby Rao

ABY RAO
Aby Rao has several years experience in IT industry and has working knowledge in applying various security controls and implementing countermeasures related to Web Applications and Database. He is skilled at planning and leading all phases of Software Development Life Cycle, Project Management and Agile Software Development. Aby has a Bachelor Engineering in Computer Science, Master of Science in Information Science, Master of Science in Television Management and various IT certifications including CISSP, CISA– Security+, ITIL, ISO/IEC 20000 etc. He is also an independent filmmaker and currently resides with his wife in Durham, North Carolina, USA.
Keep up to date on the latest developments in the world of digital forensics

Read Feature Articles on:
/ Training and Certification
/ Management issues
/ Tools and Techniques
/ eDiscovery/eInvestigation
/ Incident Response/First Response
/ Hardware and Software
/ Network Forensics
/ Cyber Forensics
/ and much more...

Apple Autopsy:
/ A Digital Forensics look at all things Apple

From the Lab:
/ In depth technical articles on products and techniques

Legal Section:
/ In-depth articles on legal matters affecting Digital Forensics along with the latest legal news from around the world

VISIT DIGITALFORENSICSMAGAZINE.COM for the latest news and views from the digitalforensic community with special articles for registered users.

NEXT ISSUE OUT SOON
SUBSCRIBE NOW

Prospective authors should contact editorial@digitalforensicsmagazine.com for information on submissions.
Both of these are valid points independently but combined they make a much stronger environment for your customers and/or investors.

**Reasons for Pen-Test: Regulatory Issues**

IT Security Compliance regulations and guidelines (GLBA, FFIEC, HIPAA, NCUA, FDIC etc) require an organization to conduct independent testing of the Information Security Program, to identify vulnerabilities that could result in unauthorized disclosure, misuse, alteration, or destruction of confidential information, including Non-Public Personal Information (NPPI).

- HIPAA: Health Information Privacy Protection
- GLBA: Gramm–Leach–Bliley Act
- FFIEC: Federal Financial Institutions Examination Council
- NCUA: National Credit Union Association
- FDIC: Federal Depository Insurance Corporation

There are others that may apply to you more specifically but these are some of the major regulations that must be complied with as part of the banking industry. Penetration testing is one of the oldest, most trusted methods used for assessing security risks. Because the process is designed to simulate a real-world attack using the tools and techniques employed by actual hackers, the primary reason organizations will conduct a penetration test is to find and fix vulnerabilities before a criminal finds them.

**Before You Pen-Test: Know who to hire**

The very definition of “Imposter” is a person who pretends to be somebody else, often to try to gain financial or social advantages. As individuals in a modern world we have to be ever mindful of people who present themselves as experienced penetration testers. These people attempt to charge companies for performing pen-tests when they have no intention of doing the kind of in-depth work needed to truly assess the network of the unsuspecting customer. Often these people do simple network scans with Nessus (a popular vulnerability scanner) give the customer a standard report then move on the next victim. This is not and should never be considered a pen-test. Penetration tests are in-depth tests performed from the inside as well as outside of a target network meant to expose any security weaknesses potential hackers can use to gain access to your network. True penetration tests are not possible without the individual doing extensive research on the customer to discover as much knowledge as possible from the internet such as Facebook, Google, etc. many times in the course of your research you find job postings for this company advertising the need for an experienced Windows Server Administrator or...
may be even for a firewall admin with Cisco experience. This type of information is invaluable in determining the type of vulnerabilities that may exist in a network. It is recommended that you not supply all the formation about your network (better known as Black Hat test). It is the job of the pen-tester to do the research the same way a hacker would. In my opinion it is better to do a “Black Hat” test so as to simulate the way an attacker would approach your network.

A Reputable Service Provider (RSP) should not only be skilled in penetration testing but should also be able to manage a project and to report in a non-technical way to a company’s management. The following items are recommended in helping to pick a RSP.

- Ask your colleagues and industry peers if they can recommend a vendor.
- Ask the vendor for examples of projects they have undertaken.
- Agree on a detailed scope of exactly what will be tested.
- Ask for any certifications or qualifications that the testers may have, but don’t base your decision solely on certifications because a lot of people can pass a test but not necessarily do the work.
- Confirm how long the firm has been performing penetration tests – you should use firms that have experience performing tests.

When allowing a pen test to be done, you are letting someone look through your computers and networks. That person is looking for ways to circumvent controls and gain access to sensitive information. You have brought them in to find holes before the bad guys do. And, it needs to be done discretely. “Imposter” pen-testers do not take the time to examine the details of your network making sure that all vectors of exploit are being considered. Experienced RSPs are very detailed in their methodology realizing that their reputation is at stake and a satisfied customer will mean repeat business in the future.

Before You Pen-Test: Know what you are paying for
Planning and Preparation

In order to make the penetration test done on an organization a success, a great deal of preparation needs to be done. Ideally a kickoff meeting should be called between the organization and the penetration testers. The kickoff meeting must discuss matter concerning the scope and objective of the penetration test as well as the parties involved. There must be a clear objective for the penetration test to be conducted.

An organization that performs a test for no clear reason should not be surprise if the outcome contains no clear result. In most cases the objective of a penetration test is to demonstrate that exploitable vulnerabilities exist within an organization’s network infrastructure. The scoping of the penetration test is done by identifying the machines, systems and network, operational requirements and the staff involved. The form in which the results or outcome of the test is presented should also be agreed upon the penetration testers and the organization. Another important agenda to discuss during the meeting is the timing and duration the penetration tests are performed. This is critical, as it will ensure that while penetration tests are being conducted during normal business and everyday operations of the organization will not be disrupted. When allowing a pen test to be done, you are letting someone look through your computers and networks.

- Ask your colleagues and industry peers if they can recommend a vendor.
- Ask the vendor for examples of projects they have undertaken.
- Agree on a detailed scope of exactly what will be tested.
- Ask for any certifications or qualifications that the testers may have, but don’t base your decision solely on certifications because a lot of people can pass a test but not necessarily do the work.
- Confirm how long the firm has been performing penetration tests – you should use firms that have experience performing tests.

When allowing a pen test to be done, you are letting someone look through your computers and networks. That person is looking for ways to circumvent controls and gain access to sensitive information. You have brought them in to find holes before the bad guys do. And, it needs to be done discretely. “Imposter” pen-testers do not take the time to examine the details of your network making sure that all vectors of exploit are being considered. Experienced RSPs are very detailed in their methodology realizing that their reputation is at stake and a satisfied customer will mean repeat business in the future.
must understand that penetration testers performing the tests in most cases are breaking the law. It is also critical to make sure the organization understands that any information or data obtained during the penetration tests will be treated as confidential and will be returned or destroyed accordingly after the tests. Prior to any penetration test engagements legal documents protecting the penetration testers and the customer must be signed. Because of the legal issues involved, this is a very important step and should be completed before conducting any penetration test on any organization. Even if the penetration testers are staff conducting tests on their own systems and network, they should make sure permission is granted in writing from all the necessary parties. This serves as a protection to penetration testers should anything go wrong during the tests. Accidents can happen and no penetration testers would like to be sued as a result of doing their job.

**Information Gathering and Analysis**

After doing the necessary planning and preparation with the organization (or target).

The next step is to gather as much information as possible about the targeted systems or networks. There’s a ton of tools and online resources available for you to do the necessary information gathering. If the intended target has an online website, this is a good place to start your information gathering. We should always remember that any kind of information gathered during this stage may prove useful to us in the other stages of the penetration test.

**Vulnerability Detection**

After having gathered the relevant information about the targeted system, the next step is to determine the vulnerability that exists in each system. Penetration testers should have a collection of exploits and vulnerabilities at their disposal for this purpose. The knowledge of the penetration tester in this case would be put to test. An analysis will be done on the information obtained to determine any possible vulnerability that might exist. This is called manual vulnerability scanning as the detection of vulnerabilities is done manually.

**Penetration Attempt**

After determining the vulnerabilities that exist in the systems, the next stage is to identify suitable targets for a penetration attempt. The time and effort that need to put in for the systems that have vulnerabilities need to be estimated accordingly. Estimations on how long a penetration test takes on a particular system are important at this point. The target chosen to perform the penetration attempt is also important. One practice that most organizations do is to name their machines in a way that they can distinguish what the machine does. The computer name of the target is sometimes a decisive factor for choosing targets. Often after a network scan you would find computer names like ProxyServer01 and others that give penetration testers an idea of what the machine does. By choosing their target properly, penetration testers will not waste time and effort doing any redundant job. Normally penetration tests have a certain time constraint and should not waste any time unnecessarily. There are many ways to choose a target system.

**Analysis and Reporting**

After conclusion of all the tasks listed above, the next task ahead is to generate a report for the organization. The report should start with an overview of the penetration testing process done. This should be followed by an analysis on critical vulnerabilities that exist in the network or systems. High level vulnerabilities are addressed first as to highlight it to the organization. Low level vulnerabilities should then be highlighted. The reason for separating the high risk vulnerabilities from the low risk ones helps the organization in decision making process. Some organizations might accept the risk incurred from the low risk vulnerabilities and only address to fix the more vital ones that pose more of a risk to the organization.

**Conclusion**

The above steps should serve as a guide to conducting a penetration test at any organization. Pen-tests are configurable and should be conducted according to what your organizational needs.

**RANDY NARAMORE**

Randy Naramore is a family man whose beautiful wife and 4 kids keep him very busy, he enjoys camping with his family and is an avid outdoorsman. Professionally his interests lie in the Information Security and Forensics fields, his primary functions tend to be directed towards the enterprise web security and forensics field. He is a member of the Birmingham Infragard Chapter and is the Vice President of the International Information Systems Forensics Association chapter in Alabama. Randy currently holds a number of industry recognized certifications such as C|EH, GWAS, CNE, SFCP, BCCPA.
smart security interface®
the multiplatform security connector integrated with all major PKI applications and TMS platforms; it fully supports all widespread smart cards and architectures for government, corporate and bank projects; it also interfaces with smart phones, pre-boot systems and TPM

iEnigma®
the software application that turns your smart phone into a PKI smart card; unparalleled convenience for digital identity management; unbeatable security thanks to the support of NFC chips and micro SD cards

plug´n´crypt®
the product line for logical and physical access control covering different form factors: USB token, smart card, micro SD card, soft token, also in combination with encrypted flash memory and the most common RFID technologies

CSTC®
PKI made simple and accessible to SMB: card initialization, management of PINs, certificates, keys and objects without having to necessarily invest on a TMS infrastructure

contact:
team@charismathics.com

www.charismathics.com
Aby Rao: You have a strong technical background in computer science and telecommunications, tell us how you ended up in IT Security.

Alexandro Fernandez: I ended up in IT Security because in the beginning of 2001, Citigroup Bank bought Avantel (This company was part of grupo financiero Banamex, largest bank in Mexico) and they decided to create a special department with responsibilities related to Information Security, Business Continuity, Change Control management procedures, Physical security access, System development life cycle methodologies, Internet Management, Contracting & Outsourcing and Problem Management among others, so the CEO decide to form this team.

AR: You have worked for a telecommunications company, International Bank and Global technology company. Where were you most challenged in your job and what did you learn?

AF: My most challenging job was at BBVA Bancomer when I was working as the service delivery manager responsible for over 80 persons, more than 16 security
services, more than 2,000 devices and around 8,000 tickets to solve monthly. Why was so challenging? Because we had a very aggressive service level agreement in terms of service continuity and of penalties; we had to operate in 10 countries, 8 from Latin-American and 2 from Europe, with a 7X24X365 schedule and with a very tough customer.

AR: Currently you work for Sm4rt Security Solutions, tell us more about this company, it’s size, services and your role.
AF: Sm4rt is a Mexican company with over 100 employees dedicated to maintain and improve the security strategies for more than 20 customers in Mexico and Europe. Our services are:

• Diagnostic Services: Ethical hacking, Risk analysis, Privacy impact analysis and Information value Analysis.
• Best Practices: Implementation of best practices for comply with PCI-DSS, SOX and other Mexican regulations.
• Specialized Security Consulting: “Taylor made” projects to satisfy customer needs in terms on information security.
• Incident Response: Incident contention and forensics.
• Fraud Prevention: Process analysis for improve the detection and prevention of fraud in IT systems.

Basically I have 2 roles in the company; the first one is related to project management, where I act as the leader responsible for the delivery of the whole project. My secondary role is as a specialized consultant giving advice (writing security recommendations for our customers and for our new methodologies) and supporting other projects as needed.

AR: What is the state of Information Security in Latin America. Are companies doing their due diligence and how much are they focusing on security risks?
AF: The state depends on the regulations of each country in Latin-American, but in general the companies are trying to do their best to comply and mitigate their security risks. Fortunately, in the last 2 or 3 years the CEOs and CIOs are more sensible to information security than in other years. An example of this, is the increased information security awareness in senior managers across our countries. Also, many companies are spending more money in issues related to security risks. Still, we have a lot of work to do, a lot of things to accomplish and a long way to go. But the good news is that our C levels are more interested every day in our topics.

AR: Is there sufficient demand for IT Security Professionals in Mexico and Latin America?
AF: I think the problem is that the demand overcomes the offer of security professionals in LATAM. In the past years, there had been an important raise of IT Security Professionals.

AR: What skill set is in high-demand?
AF: Mostly, the skills that are in high demand are related to security management, Business continuity and pent testing.

AR: How does your company stand apart from other companies and why should they hire you?
AF: It can be defined in one word; “Focus”, we don’t get involved in projects that are not related with IT risk, compliance or security matters. Also, we consider that one of our most important value added is the transfer of our methodologies to our customers so they can used and applied them later. Why they should hire me? Sm4rt is a very specialized company and for this reason, we are always trying to hire the best talent in Mexico. The principal characteristics that our human resources department is looking for, are passion, teamwork, quality and loyalty. These principles are the basis for working at Sm4rt.

AR: When you are hired by a client/company how do you educate them about Security and mitigation techniques?
AF: In our first approach to a new customer or prospect, is to make him aware of the security risks that his company face today. For example, if our new customer or prospect, is a company that make electronic transactions, we mount a virtual lab to show
him the easiness of hacking a company like his if he is not properly protected.

**AR:** What are some of the risk management frameworks you have used and how effective are they?

**AF:** We used some of the most famous and well accepted frameworks. These frameworks are COBIT, ISO 27001, PCI-DSS and OSA Model. Each of these frameworks has their strengths and opportunities, but I have found that PCI-DSS is very useful, because it focuses on giving protection to very specific targets (for example, PCI tries to protect the information related to credit and debit cards only). And OSA model is also very useful because it provides us with something that they called “security patterns”, that can help any company to identify what “group of controls” needs to implement, not only an individual control but a set of controls.

**AR:** As a security consultant, what advice would you offer to a small business that has no knowledge of security and have no program in place?

**AF:** I will recommend them to perform a security risk assessment in order to identify what security risks faced their organization. And if possible, I will give them a security awareness presentation for them to understand a little bit of what is and why information security is so important for them (Of course, it will depend on the activities of the company).

**AR:** What are some of the top security risks when it comes to Financial Institutions. Please share some of your experiences.

**AF:** The first topics that come into my mind, talking about financial institutions, are two: The protection of payment systems and the protection of sensitive data. It is very important for a financial institution to protect their payment systems, not only from the IT perspective but also from the processes optics, so they can minimize the risk of doing something unauthorized. Either they need to have implemented controls to assure the correct segregation of duties and that the people involved has the “least privilege” concept in place.

By other hand, the organizations must identify where, who and when is their confidential information being accessed. Is well know that the financial institutions manages a lot of information, and that organized crime looks for this information because they know that it represents money and good gains for them. What we need to do is to classify the Information so that they can know where do they need to put more, better and strict controls. It is inconceivable that an financial institution does not recognize the importance of this activity, so they need to achieve this if they want to keep existing and avoiding to appear in some international daily morning news.

**AR:** What role does coaching and mentoring play in shaping new IT security talent?

**AF:** When you manage a team or a group of people, it is very important to understand that as a leader, you must develop some soft skills in order to give great results and exceed customer expectations. By the other hand, It has been mentioned that we need to develop the persons in our team and we have to keep this in mind if we spent with them to much time. The most important issue here is know the people you are working with, we need to identify and understand what are their strengths and opportunities so we can potential there best qualities and minimize their opportunity areas as well. Coaching and mentoring are tools that can shed some light while dealing and managing our team, they can help us to achieve the results that we desire. They are also useful for building strengths in our relations between our people and us, they can give us the level of trust and intimacy that can make the difference between a simple worker and a trusted worker.

I remember one time, when I was working in a large bank when one of my direct report ask me if I can do anything for her. You can’t coach a person that doesn’t want to be coached, sometimes you can make it in a “Unconscious” manner (this means, that the other person is not aware of this) and this technique is good, but it’s more important to do it in a “conscious” way, so that the communication will flow more softly.

**AR:** How do you keep your knowledge up-to-date?

**AF:** For any IT Security professional is very challenging to keep their knowledge up-to-date, in my case I try to read articles or specialized magazines (like Hakin9) as much as I can. Also, I instruct for some security well recognized security certifications, and I need to review, each year, all the official material for teaching this certifications. I love to go to national and international conferences, where I found some interesting information regarding trends in information security field. I belong to International organizations (ISACA, IRCA, EC-COUNCIL, ISC2, ISO), where some of these organizations sends articles related to my professional field. Talking to my peers is another way to keep me informed and updated about new trends, evolving threats and “fashion” topics.

*Interview done by Aby Rao*
Web Based CRM & Business Applications for small and medium sized businesses

Find out how Workbooks CRM can help you

- Increase Sales
- Generate more Leads
- Increase Conversion Rates
- Maximise your Marketing ROI
- Improve Customer Retention

"""

AJ Thompson
Sales Director, Northdoor

We now have better visibility of business metrics, have streamlined our sales order processing and reduced our operational costs significantly.

Contact Us to Find Out More
+44(0)118 3030 100
info@workbooks.com
“Certifications don’t really mean you’re a rock star”

Sameh Sabry talks with Aby Rao about Crisis Management, Wireless Hacking… and Music

Sameh Sabry is an experienced Security Consultant. He started his career at the age of 14 during his tenure with IBM, multinational firms while as well recently joining the banking sector. His main specialties include security design, penetration tests, security compliance and advanced networking. Sameh has been also one of the early open source pioneers in the whole region. He has also completed OSCP, L|PT, C|HFI, C|EH, SANS PCI/DSS, Security+,Linux+, RHCE, LPI, CCNA amongst many.

Aby Rao: Sameh, you grew up in Egypt. What was it like growing up and how did you end up being a security professional?

Sameh Sabry: As a matter of fact I was not born in Egypt. I was born in Asia, the Arabian Gulf area to be more specific. Life there was simple for a kid. I had the chance to get a good education, practice sports and also had enough time to read. Due to the general serenity of the area 15 years ago, I had ample time to meditate, imagine, think and be curious to try I also had a good computer and good internet connection back in the day that is. (I was lucky enough to have a 28.8Kbps connection). In 1997, as a teenager, I was going through different chat rooms whereby I was shocked to encounter what is called a “Ping Attack” and I was instantly disconnected. A furious teenager + a computer + time + summer was the perfect concoction and catalyst to drive my one-way ticket to the world of Cyber Security.

AR: Can you describe IT Security industry in Egypt in terms of talent and recruitment opportunities?
SS: Egypt is a country that has existed since the 10th millennium BC. Egyptians were always the pioneers in the history of mankind, be it cultural such as the endless myths of pharaohs, or in the arts of war, revolution, science, culture, music, wine making, no culture on earth has come as close the Egyptians perfection of mummification, the ingenuity of the pyramids and architecture in that era is staggering, as are the spiritual richness of all concepts and beliefs that address life after death and much more.

In a country like that, I would expect nothing less than having impressive and genuine talents.

As for today’s jobs, the IT Security industry is massively expanding; increasing demands for dedicated security teams are rising every day within IT departments for security purposes only. Egypt is an open market for all enterprise scale IT products and that should also include enterprise security products. Teams constructed of professionals with security backgrounds are tasked to demonstrate concepts, design, sell, implement or support.

Security is growing as well from an auditing/compliance perspective, especially in banks and financial institutions that account for a considerable share of the Egyptian market.

AR: You have extensive experience in Linux/Unix and then you transition into security. How has the *nix experience helped you in your career.

SS: Actually, the reason I got into Linux/Unix was the need of having certain tools such as c compilers, scripting environment, open source and freely available. After all, Linux was made by hackers. I can still recall my first 18 hours of trying to start my x server under Slackware GNU/Linux back in 1999.

Linux helped me immensely in learning how to think, challenge and tackle different circumstances. I had an endless number of code lines to explore and to hack into!

Before Security prospers and became well recognized, Linux helped me a lot by broadening my vision, understandings and interpretations as well as granting the opportunity to implement open source security solutions such as the world’s most famous Open Source Intrusion Detection System, Snort.

AR: Currently you are working in the Banking Sector. Based on your experience what are some of the challenges banking industry faces compared to other industries?

SS: Banking information is strictly confidential, accounts, balances and credit cards, so the main challenge is providing the legitimate information, to the right people at the right time. The business units are always seeking to provide online banking services, for ease of use to the customers, that’s basically the publishing or viewing constituent of your banking system to the world! Risk probabilities are very high and equals to the number of users on the World Wide Web. The slightest exploit could prove catastrophic.

Might I also add, stopping this information leak from the corporate network is another major challenge.

AR: Crisis Management is such an important aspect of Security, what kind of Crisis Management Models have you worked on?

SS: I have actually had a couple of opportunities where I was highly involved with Crisis Management units. Our job was trying to detect, prepare and prevent, control damage, recover and learn! You may be surprised to learn that being in Egypt during the revolution had a paramount effect in understanding the real need of a good Crisis Management Team and Plan.

AR: What are some of the latest Penetration Testing tools and technologies you find really interesting?

SS: Rapid7 Metasploit Pro. Their database of exploits, payloads and post-exploitation modules is HUGE! New features such as VPN pivoting is very interesting, VPN pivoting is basically running any network traffic from any network-based tool, e.g. nmap or Nexpose vulnerability scanner, through a compromised host as if you had a NIC on the target network. Automated features to avoid IDS, IPS, anti-virus and endpoint protection with advanced evasion techniques!

The W3af project is another great open source Web Application Attack and Audit Framework. It identifies most web application vulnerabilities. After identification, vulnerabilities can be exploited in order to gain different types of access to the remote system. Vulnerabilities like cross-site scripting (XSS), SQL injections (blind), OS commanding, remote file inclusions (PHP) could be easily identified, confirmed and exploited!

It is also available for a various number of operating systems such as Microsoft Windows, Linux, Mac OS X, FreeBSD and OpenBSD.

AR: You have several certifications under your belt. How has it helped you?

SS: Certifications don’t really mean you’re a rock star, but they surely help you in being recognized by Human Resources Officers. Competition is a fact of life, and the need for a work force proficient in the principles and practices of Information Security is a central concern of many banks and companies. Certification is a definitely
mark of excellence. It demonstrates that the certified individual has the knowledge to assure quality of products and services.

**AR:** What role does penetration testing and ethical hacking plays in PCI DSS compliance?

**SS:** The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholders' information for the major debit, credit, prepaid, e-purse, ATM, and POS industry.

The standard was created to increase controls around cardholders' data to reduce credit card fraud via its exposure, as defined by the Payment Card Industry Security Standards Council. Validation of compliance is performed annually, by an external *Qualified Security Assessor* (QSA) for organizations handling large volumes of transactions, or by *Self-Assessment Questionnaire* (SAQ) for companies handling smaller volumes.

One area where merchants struggle with PCI compliance relates to PCI DSS Requirement 11. It is comprised of seven sub-requirements and 14 testing procedures. It mandates that any business handling cardholder information "regularly test security systems and processes," a requirement that is intended to secure the network environment in which most merchants operate.

"11.3 Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:

11.3.1 Network-layer penetration tests

11.3.2 Application-layer penetration tests"

As with any security standard, of course, performing with more diligence than the minimum requirements is generally the best way to stay digitally secure. This is why performing multiple penetration tests instead of merely the one required by PCI DSS to the entire network every year is highly recommended!

**AR:** You have done some extensive research in wireless hacking. Please tell us more about it.

**SS:** Wireless connections in general became really huge during the last 10 years. There are at least 30 hotspots where I live and you would at least find another one or two at any given place. Restaurants, cafes, bars, airports, clinics, libraries, malls, companies and sometimes banks.

As a security professional/researcher I had to do a study with regards to both securing and penetrating the same. At first, 95% of all hotspots had very common passwords that could be found by simple dictionary attacks, passwords were mainly “123456789”, “987654321”, “godislove”, “ingodwetrust”, “iloveyou" etc. And even access points were left with default passwords “admin, admin” or "root, root".

But of course by time things started to become slightly harder to break through and access.

I had to read a lot and understand the different types of security controls offered on routers and access point such as WEP, WPA/WPA2. Made several proof of concepts on the same.

I have only used open source tools and wrote a simplified and easy to understand paper on how to crack into wireless networks that was published on several websites and security magazines.

**AR:** In January 2012 you wrote an article titled „Hacking Through Printers. uPrint. iHack.“ The title itself sounds very fascinating. Please give us a brief idea of what that article was about.

**SS:** As I have mentioned earlier, regular attacks are easily blocked, so hackers are ought to think out of the box in order to do more tests, proof of concepts and of course remediate.

Simply printers are available everywhere, not well configured and that could be very dangerous, especially with having a Microsoft vulnerability in Print Spooler Service that could allow remote code execution whereby a computer could be fully and remotely compromised!

The vulnerability could allow remote code execution if an attacker sends a specially crafted print request to a vulnerable system that has a print spooler interface exposed over *Remote Procedure Call* (RPC). On Windows XP, the guest account is enabled by default, which allows anonymous users to access printer shares. On Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2, an attacker must be authenticated in order to exploit this vulnerability unless password based sharing is disabled. If password-based sharing is disabled, attackers could exploit these systems without authentication.

**AR:** You have written several technical articles. How has writing benefited you at a professional and personal level?

**SS:** It is indeed a great pleasure to transfer knowledge to others, because it is only fair to give in order to take. You have to empty your cup in order to take more.
The world of open source taught me that knowledge is shared and development is mainly based on contribution. On the professional level, writing has helped me a lot in gaining more recognition and exposure, more trust and self-confidence.

AR: There are lot of technical experts out there who would like to transition into more managerial position, what advice would you offer them?

SS: This is a very common problem among all technical experts as they don’t really want to leave their comfort zone. But my boss taught me a couple of things that I could pass on, and I am trying to do the same myself. First, learn to follow in order to lead. Second, wearing a suit doesn’t necessarily mean you have sold out. If you are capable of penetrating networks, finding vulnerabilities, writing codes and proving concepts then kindly rest assured you can learn how to deal with people outside your lab. You just need to believe and act accordingly.

AR: Who are some of your role models in the Security industry?

SS: Mikko Hypponen, Chief Research Officer for F-Secure. A great leader says his team. He has been through the largest digital security outbreaks in history. His team took down the world-wide network used by the Sobig.F worm. He was the first to warn the world about the Sasser outbreak, he named the infamous Storm Worm and he has done classified briefings on the operation of the Stuxnet worm. His intellect and technical know-how match his clear precise and eloquent communication skills!

HD Moore, the creator of Metasploit and Chief Security Officer at Rapid7. His software helped so many. Started as a free open source project and remains so to this day despite being the world’s most known/used software for penetration testing.

AR: How did you get into drumming and what kind of music do you enjoy?

SS: Well, I was told that even when I was a kid I used to drum/hit on anything my hands could reach, being the high energy kid I was, I needed a way to let all that energy out. I guess I was a little noisy at first because it took my family a while to accept my talent but I eventually started a small band in 1996, was a lot of fun.

Ironically, I enjoy heavy metal music. I love the contrast between being clear, precise and calm at work, and letting loose with heavy metal when I’m off duty. It’s the perfect sense of balance to me. I believe in balance.

Interview done by Aby Rao
PenTest: It will be a good point to start our conversation with a few words on how did you get your first job? How did the interview look like? Were you already a skillfull and knowledgeable information security expert? Was it anyhow connected to what you do at the moment?

Stefano Maccaglia: I've started from Digital Inc. as a first level technician, a field engineer for storage networking more than 15 years ago. But my hobbies include ICT Security and hacking/cracking programs, something dated back to the early nineties when I was 15 years old. I've worked in many countries thanks to Digital, especially Australia and NZ.

At the time I've also studied networking and operating systems and then I landed on Networking, where I've been part of many important project in Europe and US.

In 2003 I decide to work on ICT Security and I've put in practice what I've studied and learned for passion in many years... In 2007 I've built my team and I'm still working here...

PT: How your experience changed over the years after working for more than one employer and being your own boss?

SM: I've constantly growth by passing from an experience and challenge to the next. In this matter I've built my career and myself as a person. I love the challenge. I like to be under pressure and to find creative solutions for a very problematic situation. I'm very productive in this way. My team is built with this approach in mind. Fortunately my Company have granted me the freedom to select my team.

PT: Could you list three most important things (or features of the person) that are crucial for you while hiring a new employee?

SM: Focus, quick wit and endurance. As I always say: “In enduring grows the strongest”.

PT: Do you prefer to hire personnel using an external company or do you prefer to shake the persons hand yourself?

SM: I always look personally to the people in my team. But also I leave the HR do his job by looking to the psychology of every potential new member.

PT: Is getting an academical degree connected to information security essential in getting a dream-come-true job? Trainings, courses or universities? Or none of them but pure practice?

SM: In my experience training and schools are very important, especially in the hacking field, but the passion is something that cannot miss. Without the
passion and the interest everything is just routine and it could become boring, one day or another.

**PT:** Does the recruiting staff set any traps for the youngsters wanting to find a job? Do you use any recruitment techniques?

**SM:** I’m used to some tricks but my HR is by far the most skilled person I know. However, my usual interview is focused on technical question where I test the skills but also the resistance of the candidate under pressure.

I start asking simple, wide questions and then I’ll adapt my requests to the responses of the candidate. This is an important aspect of my interview. I want to be sure about the candidate so I try initially to setup a good communication and then I go deep into technical questions. During the latest part of the interview I frequently stop the candidate during his explanation asking more details. This gives him a lot of pressure… only a few, in my experience, have remained calm after this stage…

**PT:** What skills do you find the most wanted on the market these days?

**SM:** In ICT every skill worth something. However, talking about ICT Security, I think Assembly and C++ programming are the most valuable, together with System and Networking skills. Anyway, the most important aspect is „motivation“, without it the candidate appears a shallow person.

**PT:** Is there anything that makes you mad about your work or our market as a whole?

**SM:** I hate the idea that a software or an appliance can replace the skill and abilities of a good team of Pen Testers. I’ve heard this concept often, especially from the mouth of Sales people or from high ranked managers. Often I have demonstrated they are wrong… No technologies can substitute our brain and our intellectual capabilities.

**PT:** Are there any other tools (than all the already existing ones) which can be invented and revolutionise pentesting market?

**SM:** I don’t like depending on tools. I think that every Pen Tester must be able to work in a flexible way. He must adhere to the Methodologies, but he should adapt to the situation, he should think as a cybercriminal in order to spot exploitable weakness. I don’t see that in our market today. Many are too dependable on tools and applications. Changing the approach is the true revolution of our market.

**PT:** How important is it for an average person to have knowledge in information security? Is our personal data in danger, will it be in future?

**SM:** It is essential. I think it would be so in the future too.

**PT:** What do you think Stefano Maccaglia will be doing professionally in 5, 10 and 20 years? How the future of IT security is plausible to look like?

**SM:** I think I continue my researches and I will continue to teach people how to hack and how to think outside the box. This is what I like. This is what I’ll do. If I look to the future I see a very dependable society. A society dependable on technologies. All that means it is up to the hackers to fill the blanks, protecting the society from cybercriminals.

---

**Stefano “Korolev” Maccaglia**

Stefano “Korolev” Maccaglia is a malware researcher with more than fifteen years of experience in Networking and Security. He’s the founder of Black Sun Factory an Italian security Company that is focused on Cybercrime, Pen Testing and Incident Response. He has previously worked for top ICT companies in Italy, Australia and United States.
The vulnerabilities out there are waiting to be found

Tal Argoni, Penetration test team leader at 2BSecure for PenTest Market speaks about experience, motivation and challenges

At age 13, I met my cousin, and he showed me how two command lines cause denial of service to an Israeli Web site. I was intrigued by this and started looking for information at every opportunity that I had. Quickly I learned TCP and got answers about client-server application. This is when I discovered the concept of Trojan horse. I started to play with Back Orifice [cultdeadcow] and Sub 7 [mobman]. I developed some social engineering and antivirus bypassing techniques and skills. I found it boring after a while, I didn’t like the idea that I depend on my victim’s click and started to look for more information. I was stimulated again when my cousin performed a DOS attack to my own machine (win95 ping of dead). I was hungry for more information regarding remote code execution. I started to download exploits, compile them and scan the internet for victims. After a few years of hacking I noticed that the internet websites became more and more popular and dynamic. SQL injection led to XSS led to file upload exploiting, to CSRF, application dos and I found a new world of interest.
Aby Rao: What do you do at 2BSecure and what are your responsibilities?
Tal Argoni: I am responsible for the penetration testing area. It includes:
- Pre-sale, evaluation of project hours, answering RFPs, performing kick-off meetings and coordination meeting expectations, preforming the technical job and operating my co-workers (my team includes 2 consultants), producing reports, board/developers current security state of the system meeting presentations, guiding developers and administrators for secure application development and network security, real-time code solutions against cyber-crime attacks (israeli’s exchange, hospitals, cellular, banks and many more sites that’s falls to the cyber war) and more.

AR: You graduated from Ha’Universita Ha’Petuha in Israel, how much does a formal education help a professional penetration tester?
TA: I started university while working a full time job in 2Bsecure. This was after I completed successfully my CEH certification so I took only a few courses to perfect my knowledge in subjects I felt I was weak in. I never graduated a full BA. As well, I took a private course in secure programming.
These studies changed my thinking manner and increased my development skills.

AR: What are your technical strengths?
TA: Only my customers can give you an authentic and objective answer. You can read some linkedin recommendations at: [http://il.linkedin.com/in/talargoni](http://il.linkedin.com/in/talargoni).

AR: What is the difference between black/gray/white box application penetration testing and which one do you prefer to be involved in?
TA: Black box testing – Testing objects based on output requirements and without any knowledge of the internal structure or coding in the object. Wireless, network, FW, IDS, DLP, AV, website, applications, databases and many more.
White box testing – Testing objects with the knowledge of the internal structure and coding inside the object, configuration, policies and any information about the object.
Gray box testing – Testing objects while already having some knowledge of its underlying code or logic. It implies more understanding of the internals of the program than black box testing, but less than white box testing. An integration of black box testing and white box testing.
I prefer to be involved in black box testing. I like to challenge myself. This is the fastest tool to evaluate the security state of an object.

AR: You might have experienced that security is often not baked into an application but is usually an after thought. If you were given the opportunity to build an application, what would be your approach?

TA: SDL Approach proves itself with the best ROI. My experience teaches me that applications that were not developed with a security orientation from the beginning are significantly more vulnerable.

AR: When it comes to large-scale code review, what is your process of analysis?

TA: I had only few large-scale code review projects. I start with automatic free tools. Then I use internal regex tools. I interview the developer to understand his security thinking. Then I manually examine specific issues like: authentication, authorization, encryptions, password policy, interfaces, logging and auditing, exception handling, input validation, session management, configuration and more.

AR: What advice would you offer entry-level penetration testers? Can you share some of your own experiences when you joined the workforce?

TA: My advice to entry-level penetration testers is to never stop believing in themselves because the vulnerabilities out there are waiting to be found, so stop learning to hack and hack.

At age 21 I joined the workforce. I will never forget the clients’ faces when they met me, it was like a shocked face thinking: “this kid can do that?!”.  

AR: Project Management can be as critical as conducting technical tasks such as Penetration Testing or Risk Assessment. Any thoughts on that?

TA: Project Management requires different skill then technical. Project Managers needs to deeply understand the project scope, assemble a testing-team, synchronize their activity and result with minimum time and maximum productivity. The project manager must deeply understand the testing result and their impact on the business.

AR: What are some of the challenges you face in application-based pen testing?

TA: Testing applications that have Web-Application-Firewalls or applications that were written with good input validation rules, has become quite challenging.

Sometimes I’m called to perform testing on self-implementation of binary protocol communicating over TCP. Testing applications of this sort calls for out-of-the-box thinking and strong technical capability.

On another level, testing huge forms with lots of parameters that are protected with CAPTCHA, can be exhausting.

AR: Who are some of people in the IT Security field you have respect for?

TA: Rafel Ivgi – At age 15, we found hacking as common hobby. We have learned and hacked together. Rafel inspired me a lot. Rafel is a hacking guru and a friend that helped me believe in myself.

Erez Metula – my first meeting with Erez was my interview join 2bsecure. It was an hour and a half and we talked about advanced exploitation of web application vulnerabilities. Erez was my manager in 2bsecure, he always gave me answers to questions when I challenged him. We worked together for 3 years and we had lots of common projects.

AR: What keeps you motivated?

TA: Diversity, every time it’s a new project, different developers, different environments. The biggest motivation injection is to discover some new vulnerability while fighting robust objects.

AR: Do you attend security conferences? What are the benefits of attending various technical events?

TA: I go to conferences in Israel, I have been in Black hat and Defcon in 2009 in Vegas. I have lectured in Microsoft Israel (.net security user group) about information gathering.

I found conferences very productive, I meet new people, learn new information, share information and promote cooperation.

AR: What does Tal do when he is not PenTesting or working on security projects?

TA: Having beer with friends, going to the beach, traveling in new countries I have never been to, cooking, swimming, GYM, learning new information about our life on earth thus The Torah.

Interview by Aby Rao
Isn’t there a better way to reunite friends and family in disaster?

Please, Volunteer your Technology Skills in Disaster

FEMA Photo: Hurricane Katrina—Houston Astrodome 2005

Information Technology Disaster Resource Center
www.itdrc.org
In simple terms, until fairly recently, many companies were not connected to public networks and security risks were low. This often meant that companies would develop security policies only when absolutely necessary (think online banking) or after an attack.

In recent years, the arrival of newly laid undersea cables brought with it much needed bandwidth. The state owned telecommunications company, Telkom, lost its monopoly on the market, and with the greater competition, internet usage has become affordable. There has been an enormous growth in the number of internet users and it is set to continue to grow, with the arrival of smart phones and even more bandwidth. Business has embraced connectivity and with it the challenges of security arise.

Currently there is a big need for skilled security professionals to secure the number of networks being exposed to public networks. There is also a major shortage of skilled people that can fill these roles. This is especially true for pen-testers and companies with the expertise to conduct these tests.

Often pen-testing is conducted by small security teams within an organization. At times some of the large international auditing firms have set up pen-testing teams, only for them to be absorbed elsewhere. Below we mention two home grown info security companies that are highly regarded both here and internationally where they also operate.

---

### SensePost
Best known for training they provide at Black Hat conferences, also offices in the UK.  
[http://www.sensepost.com](http://www.sensepost.com)

### MWR InfoSecurity
Well known in the UK market, operates in both countries.  
[http://www.mwrinfosecurity.com](http://www.mwrinfosecurity.com)

---

Johan Snyman has a B.Sc in Information Technology and Computer Science and a keen interest in the world of Info Security. With enough years behind a computer to require him wearing him glasses, Johan remembers booting up on a 360 Kb floppy disk and having infected his mother’s computer with the Stoned virus. He dislikes sand in his food.
Boundless helps integrate and improve organizational ARC’s – Audit, Risk, and Compliance activities – to safeguard reputation and fiduciary integrity.

Expert Training.
Entertaining Speaking.
Candid Consulting.

For more information call (267) 297-0706. www.boundlessllc.com
Paris, April 25th, 2012 – Organised for the second time by Sysdream, Hack in Paris, event in France exclusively in English, matching together IT security professionals (CTO, CSO) and technical experts of hacking, will be held from 18 to 22 June at the Convention Center to Disneyland Paris.

The event Hack in Paris will be held in two steps
6 trainings conducted by technical experts on 3 days (from June 18 to 20):

Training 1
Corelan Live – Win32 Exploit Development conducted by Peter Van Eeckhoutte, Corelan founder and author of the training «Win32 Exploit Development»

The Corelan Live Bootcamp is a truly unique opportunity to learn both basic & advanced techniques from an experienced exploit developer. During this 3 day course, students will be able to learn all ins and outs about writing reliable exploits for the Win32 platform. The trainer will share his “notes from the field” and various tips & tricks to become more effective at writing exploits.

Training 2
iOS Applications – Attack and Defense conducted by Sébastien Andrivet, co-founder of Advtools

Learn the secrets of the iOS platform, how to attack iOS applications and how to correctly implement secure iPhone and iPad apps.

This training starts with a short introduction about security concepts and iOs. It is then highly practical: you will learn how to take the control of your iOS device, how to intercept communications, how to reverse engineer applications and find security defects. Then in the second part of the training, you will learn how to correctly implement secure ios applications: what are the most common security mistakes and the corresponding solutions. The training concludes with some advanced hacking techniques.

Training 3
Malware Reversing Laboratory conducted by Lee Ling Chuan, researcher

This class focuses on the advanced malware combating and defending mechanisms that target on common platform, such as Windows OS and web browser. Advance and complex malware analyses techniques will be introduced include anti-debugging techniques, anti-analysis and more to guide students when facing the sophisticated malware.

Training 4
Metasploit for Penetration Testing conducted by Georgia Weidman, researcher

The event Hack in Paris will include six training and 16 conferences: the opportunity for the ecosystem of IT security to be form on the practices of hacking and meet around international experts to inform about the reality of hacking, its challenges and its consequences.
Training on the basics of using the Metasploit Framework, on the methodology of penetration testing using Metasploit and to create vulnerable systems. The training will also allow participants to write their own modules Metasploit and to create complex client-side attacks. Training appropriate to the initiated and the uninitiated who want to add the Metasploit Framework to their expertise.

Training 5

Hacking IPv6 networks conducted by Fernando Gont, specialist of security of communication protocols

Training about security of IPv6 protocol permitting to assess and mitigate threats and consequences on security of IPv6 environments. This course will include learning how each feature of IPv6 protocol and related technologies can be exploited for malicious purposes. Participants will use a variety of evaluation tools of security to put into practice the theory taught.

Training 6

Reverse-engineering of Android applications and malwares conducted by Anthony Desnos, specialist security open-source

This training deals with the analysis of Android application. The Android system is now widespread, and very used by many user and Professional. This training aims to show how it is possible to analyze an Android application with various Open Source tools in order to change the behavior of the latter. In addition, this training will explore how Open Source tools analyze malicious applications in order to learn to create their own signatures to detect malware.

Beyond trainings, a validation committee composed of experts selected and retained:

16 conferences, including two keynotes, with speeches by world-renowned experts (June 21 and 22):

• Keynote 1: Measuring Risk with Time Based Security by Winn Schwartau
• Keynote 2: Where Are We And Where Are We Going by Mikko H. Hypponen

Conference 1

Got your Nose! How to steal your precious data without using scripts by Mario Heiderich

Cross Site Scripting techniques and quirky JavaScript have received a lot of attention – thus more and more ways to get hands on this threat are being developed and practiced: Security aware people simply switch JavaScript off, developers use sand-boxed IFrames and CSP to protect their applications and NoScript, XSS filters and HTMLPurifier do a great job in keeping people from getting “XSS’d”. But what about attacks in the browser that don’t require any scripting at all – but still steal your precious data, right before you know it? What about attacks so sneaky and sophisticated or just simple, even your best Anti-XSS solution won’t prevent them? Attacks, that don’t use any scripting – but fierce markup tricks from outer space? This talk will introduce and discuss those kinds of attacks, show how attackers steal plain-text passwords, read CSRF tokens and other sensitive data and create self-spying emails and worse without executing a single line of JavaScript. Deactivating scripts and eliminating XSS as a good level of protection? Not anymore!

Conference 2

A bit more of PE by Ange Albertini

Among other things, I briefly introduced in Hashdays 2011 (cf hashdays2011.corkami.com) my recent PE experiments, already failing all the tools I tried. I will focus this time only on the PE format, describing in detail the weirdness of the format, pushing it as usual to its limits.

Conference 3

Windows Phone 7 platform and application security overview, by David Rook

Security features of Windows Phone 7 and directions gave to developers to create secure applications for Windows Phone 7.

Conference 4

SCADA Security: Why is it so hard? by Amol Sarwate
Attacks and technical challenges of security for SCADA environments. Examples of exploits and security controls in mitigating risk.

Conference 5
*Attacks and technical challenges of security for SCADA environments. Examples of exploits and security controls in mitigating risk.*

*Conference 5*
*Attacking XML Processing by Nicolas Grégoire*

Based on results obtained after more than a year of research on XML technology, this conference will detail the security issues related to XML and handling practices.

Conference 6
*What are the new means for cybercriminals to bypass and evade your defenses? by Klaus Majewski*

In October 2010, Stonesoft R&D brought to light Advanced Evasion Techniques (AET), a new form of evasion with techniques that can be combined to generate a limitless number of other techniques. AET’s are able to bypass any security device.

Conference 7
*PostScript: Danger Ahead! by Andrei Costin*

Capabilities of the PostScript language and dangerous aspects of PostScript on a PC or other terminal.

Conference 8
*Non verbal Hacking by Chris Hadnagy*

How did the term Neuro Linguistic Hacking? Explanations on the mixture of the principles of NLP, body language and micro expressions used to manipulate the target in an emotional state which allow to control them.

Conference 9
*Bypassing the Android Permission Model, by Georgia Weidman*

Different ways to contum the Android system by taking advantage of practices of storage offered by installed applications and how to introduce on the non-secure applications.

Conference 10
*Results of a Security Assessment of the Internet Protocol version 6 (IPv6) by Fernando Gont*

Fernando Gont will present the results of a project conducted during last years on security of IPv6. It will also provide advice on how to deploy IPv6 protocols securely, highlighting a number of vulnerabilities that have been found in several IPv6 deployments. Exclusive: demonstration of the use of certain tools of attack!

Conference 11
*HTML5: Something wicked this way comes by Krzysztof Kotowicz*

Finding the weak link by combining several attack techniques to update the latest security vulnerabilities in a successful exploit.

Conference 12
*The road to hell is paved with the best practices by Frank Breedijk & Ian Southam*

Are best practices ensure better security? Is a strong password policy is effective thanks to strong passwords? When do we consider there are too many system administrators?

Conference 13
*Securing the Internet: You’re doing it wrong (an INFOSEC Intervention), by Jayson Street*

How to involve the management of a company in security? How to give responsibilities to the end users? How to participate in the INFOSEC industry?

Conference 14
*You spent all that money and you still got owned? by Joe McCray*

Practical methods of identifying and bypassing security solutions dedicated to companies such as Load Balancers, Network and Host-based Intrusion Prevention Systems (IPSs), Web Application Firewalls (WAFs), and Network Access Control Solutions (NAC).

The full program is available at: [http://www.hackinparis.com/talks](http://www.hackinparis.com/talks).

About Sysdream
Sysdream is a French leading provider of IT security audits and security training. Sysdream is born to satisfy a growing need of competence transfer and audits (penetration testing) from the attacker point of view (offensive security or ethical hacking) for companies with an important security need.

For more information: [http://www.hackinparis.com](http://www.hackinparis.com)
In February 2002, Mile2 was established in response to the critical need for an international team of IT security training experts to mitigate threats to national and corporate security far beyond USA borders in the aftermath of 9/11.

A Network breach... Could cost your Job!

GLOBAL INFORMATION ASSURANCE SERVICES

Other Mile2 services available Globally:
1. Penetration Testing
2. Vulnerability Assessments
3. Forensics Analysis & Expert Witnesses
4. PCI Compliance
5. Disaster Recovery & Business Continuity

www.mile2.com

Available Training Formats
1. F2F Classroom Based Training
2. CBT Self Paced CBT
3. LOT Live Online Training
4. KIT Study Kits & Exams
5. LHE Live Hacking Labs (War-Room)

Other New Courses!!
ITIL: Foundations v.3 & v.4
CompTIA Security+, Network+
ISC2 CISSP & CAP
SANS GLSI: GIAC Sec. Leadership Course
SANS 440: Top 20 Security Controls
SANS GCIH: GIAC Cert Incident Handler

(ISC)² & CISSP are service marks of the IISSCC. Inc. Security+ is a trade mark of CompTIA. ITIL is a trade mark of OGC. GSLC & GCIH are trademarks of GIAC.
In the next issue of PenTest Market magazine,

PenTest Extra
Digital Forensics

Available to download on June 13th

If you would like to contact PenTest team, just send an email to maciej.kozuszek@software.com.pl or ewa.dudzic@software.com.pl. We will reply a.s.a.p.

PenTest Magazine has a rights to change the content of the next Magazine Edition.
hitbsecconf2012
AMSTERDAM
May 21st - 25th @ Okura Hotel Amsterdam

REGISTER ONLINE
http://conference.hitb.org/hitbsecconf2012ams/

The Third Annual HITB Security Conference in The Netherlands featuring keynote speakers:

Bruce Schneier (Chief Security Technology Officer, BT)
Andy Ellis (Chief Security Officer, Akamai)
OWASP Foundation

“We help protect critical infrastructure one byte at a time”

- 140+ Checklists, tools & guidance
- 150 Local chapters
- 20,000 builders, breakers and defenders
- Citations: NSA, DHS, PCI, NIST, FFIEC, CSA, CIS, DISA, ENISA and more..

Learn More: http://www.owasp.org