PenTest Market magazine

Vol.1 No.1 Monthly ISSN 2084-1116
Issue 01/2012(01) March

Derek Manky
TALKS ABOUT HIRING FOR THE FORTIGUARD RESEARCH TEAM

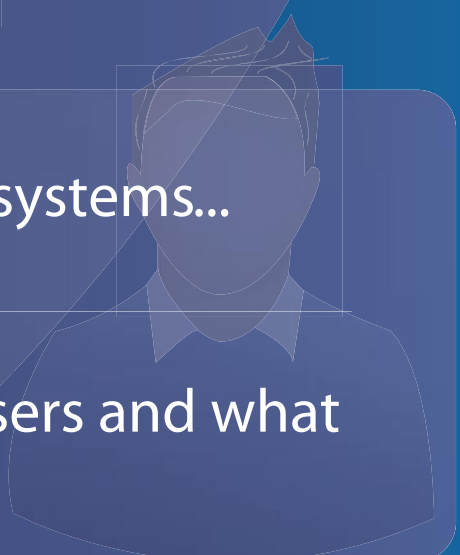
A BUSINESS NEED TO SUCCESS
INTERVIEW WITH ARMANDO ROMEO
THE HUNT FOR PENTESTERS
INTERVIEW WITH ERDAL OZKAYA
PENTESTING YOUR OWN EMPLOYER?

idtheft protect

Be reactive...

- Your systems are being attacked 24 hours a day...
- You understand the threats and are protected against them...

Be proactive...



- My users' behaviour threatens our systems...
- I understand what motivates my users and what threats are coming my way...

ID Theft Protect provides information on threats from a user perspective.

Visit: **http://id-theftprotect.com**

Something Fresh, Something New – PenTest Market!

March is going to be an extraoridary month for the PenTest gang! We can finally present to you our new project – PenTest Market. This magazine is going to make all the difference. You will see pentesting from a different perspective. Our contributors come from the IT security world but not exclusively. Especially for you we invited potential clients of pen testers to show the other side of the barricade. This is a great opportunity to learn about their expectations.

The thing that makes this magazine unique is structure. PenTest Market will consist mainly of interviews with IT security specialists, who will share their experience with you. We will also include some reports about pentesting market in different parts of the world and several guides, for example: „How to recruit a pentester?, etc. I am sure that we have many great issues of this magazine ahead. Now, however, let's focus on what we have in this pioneer issue.

On the cover you can see Derek Manky, who is the Senior Security Strategist of Fortinet, where he is in charge of directing the FortiGuard research team. We have talked with Derek about hiring for the FortiGuard, cyber war and some more interesting subjects, which you can find on page 06.

These days it is hard to find good pentesters or any other IT security specialists. This is a quite big problem for companies. That matter is described by Fabiana Schütz in a revealing article „The Hunt for Pentesters". If you want to know who hires pentesters, or how to get to them, just open page 10 and enjoy reading.

As I said before this magazine consists mainly of interviews. On the next few pages you will find two of them with Armando Romeo and Ian Moyse. I suppose that some of you may know them but if you are one of those who hear their names for the first time, jump to page 14 and meet these great people.

„Pentesting your own emplyer?" – a really intriguing title. Yves Lepage in his article discusses a new trend among companies, creating own internal team of pentesters. If you want to know what challenges you may face and what benefits you may achieve by going this way, just open on page 22.

The further, the more interviews. Erdal Ozkaya and Peter Wood are world-renowned speakers, who can be met during many popular events. You didn't have opportunity to listen to them live? Go to the page 26 and read what they have to say.

In the next article, Manuel Castro says that under his concern penetration testing is a lot more complex than state an opinion. Pentesting services help companies in being trustworthy and get more clients. More benefits of pentesting are desribed on page 34.

Probably not many of you know Nethemba but believe me this company is worth your attention. They provide all kinds of penetration tests, comprehensive web application security audits andprofessional consulting & training in various security areas and more. The father of Nethemba's success is Pavol Lupták, who found some free time for us and answered our questions. To read the interview go to page 36.

We give the floor to Asia. Semi Yulianto researched and described penetration testing in Indonesia. The second piece is an interview with Harish Thakral, Director of Information Security for Indian company, TechBharat. If you would like to explore pentesting in Asia pages 40 and 42 are for you.

Our last but not least interview in this issue features Jeromie Jackson, security expert with over 20 years of experience. He claims that references play a key role in looking for good pentesting services. He has also described professions that bring the biggest financial benefits. The whole interview can be read on page 44.

Finally, we can present to you article by Harish Parmar who is a Senior Consultant Information Security at Barclay Simpson. I think that the title of his article „Penetration Testing – Continuous demand outweighs supply" should tempt you to open page 46.

We hope you will find the first issue of PenTest Market absorbing and uncommon. Thank you all for your great support and invaluable help.

Enjoy reading!
Krzysztof Marczyk
&Pentest Team

PenTest magazine

TEAM

Editor: Krzysztof Marczyk
krzysztof.marczyk@software.com.pl

Associate Editor: Małgorzata Skóra

Betatesters / Proofreaders: George Bormes, Massimo Buso, Daniel Distler, Alexandre Lacan, Michael Munty, Rishi Narang, Ankit Prateek, Davide Quarta, Aby Rao, Jonathan Ringler, Dave Small, Johan Snyman, Jeff Weaver, Edward Werzyn, Daniel Wood

Senior Consultant/Publisher: Paweł Marciniak

CEO: Ewa Dudzic
ewa.dudzic@software.com.pl

Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl
DTP: Ireneusz Pogroszewski

Production Director: Andrzej Kuca
andrzej.kuca@software.com.pl

Marketing Director: Ewa Dudzic
ewa.dudzic@software.com.pl

Publisher: Software Press Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.pentestmag.com

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Interview with

Derek Manky

Derek Manky is the Senior Security Strategist of Fortinet Inc., where he is in charge of directing the FortiGuard research team. With over 130 professionals, FortiGuard is responsible for updating the protections for the different products of Fortinet Inc. Derek Manky also is responsible for preparing the Fortinet security blog and the "Threatscape Report" monthly summaries, available at http://www.fortiguard.com. Derek resides in Vancouver where the rest of the Fortiguard team is located.

We'd like to know a bit more about your background. How did you make the progression from developer to a security expert?

Derek Manky: I started off supporting threat related backend system develop at FortiGuard Labs. For example, automated systems, which help detection and mitigation, while escalating to researchers and analysts. Naturally this made me work close with the security team. At the same time, the systems I helped develop contained a plethora of data and information which I also studied to ramp up knowledge on the threat landscape.

What would you suggest to anyone who wants to have a career in security?

DM: Follow the space since trends and attack methods are always changing. It's very dynamic, so keeping up to date with blogs, patches and the latest security developments is very important. This allows one to stay on top of the latest threats, while building a knowledgebase of everything that has happened in the past. Network, build skills and even blog yourself.

Also, be careful of what blogs and news you read since there are often inaccuracies or inconsistent details, which should lead you to dig further.

What are some of the skills that you look for individuals to have when hiring for the FortiGuard Research Team?

DM: It entirely depends on the position. If it is an analyst position, we are typically looking for reverse engineering skills for various instruction sets / languages (x86, ARM, javascript/actionscript). Since we do a lot of work with data sets, SQL / DB query skills are usually essential as well.

Understanding of network concepts is a must, since we will follow malicious servers, domain registrations, etc.

What are some of the tasks that individuals on the FortiGuard Research Team do on a daily basis?

DM: Our team has a broad reach due to the fact Fortinet started in the *unified threat management* (UTM) space. We have experts dedicated to tasks in various positions. Tasks across our team of experts include: reverse engineering viruses and code (x86, ARM, etc), studying malicious Web code (ie: JavaScript), botnet research (protocols, command and control IPs), rootkit research, mobile threat research (malicious applications) and we battle cybercrime (partnerships with security industry, law enforcement) and perform zero-day vulnerability research. The latter is a rather specialized space,

where we put our white hat hacker suits on and find security flaws ahead of the bad guys.

Then, we report this to vendors so they can fix the problem – and we can roll out detection in advance for our clients. Here's an example of ones that are still waiting to be fixed: *http://www.fortiguard.com/advisory/UpcomingAdvisories.html*.

How much do you expect mobile malware in general to take off now that mobile apps are becoming so complex?

DM: It's going to be a hot area. We have seen mobile-based vulnerabilities and public exploit code, which means hackers are able to get their malware into mobile devices with ease. This naturally means that more malware will start to be developed for both mobile applications and malware that hit phones from Websites, links, etc. There is more drive from cyber criminals to do so since there are simply more victims – more victims, means more money. As a heads up, look for a war on mobile applications from the vendors – Look at the Android Marketplace as an example. I think this will turn into a cat and mouse game: as the marketplace tries to vet code to keep malware out, malicious app developers will find more ways to sneak their malware past these barriers.

How do you think this type of malware would affect big industry, in particular?

DM: The bigger the industry, the more potential malicious endpoints you are going to have entering and exiting your network. So, it definitely has an impact – mitigation against this is tough and requires a blend between a valid security solution, education and also updated and reviewed policy and enforcement protocols. What devices should be allowed into a network? Are they up to date? What access do these devices have to others on the local and external network? Do on-net / off-net policies exist? I think it is very important to have an active administration team which drafts and enforces these protocols while working with a manageable security solution and the team of experts behind it. Here, we have a worldwide team at FortiGuard Labs constantly updating our platforms with our expert view and analysis.

Do you think that mobile malware would affect some company's bottom line enough that they would invest in researching it?

DM: It depends how you define research. As far as awareness and developing mobile security policies, absolutely. In terms of researching the malware itself, this would take a lot longer. I often work with SOC (*security*

operation centers) and VRT (*vulnerability research teams*) which are in-house research operations at larger organizations. These are not as focused on mobile yet, but these type of organizations likely would invest some resources into mobile research in the future.

What are the fastest growing threats that you are seeing today?

DM: Mobile as discussed in this article, as well as second-stage / targeted attacks. These are often referred to *Advanced Persistent Threats*, which is just a buzz word for something that has existed for some time now – it is just now getting more attention as marketing campaigns are trying to tap onto this. Critical infrastructure based threats (cyber warfare / SCADA, smart grid) are also a growing concern. Botnets, of course, continue to be a very hot threat, since almost any threat nowadays needs to communicate with an attacker somewhere in cyberspace.

What is the hardest threat to provide security for in a UTM device?

DM: Good question. Of course, I am going to have to reword it to *What is the hardest threat to provide security for*? :) I say this because UTM truly covers many aspects / vectors of security threats, so it's really just beefier body armor compared to other security solutions out there. I would have to say mobile and zero-day threats. Mobile because it is really fragmented, instead of just one operating system / platform (ie: Windows) on endpoint you are really dealing with many more vulnerabilities (patches you need to enforce) and potential threats. Couple that with the fact they are mobile and can breach a gateway to enter the network. It's similar to a laptop, but worse because of the multiple platforms and 3/4G/LTE access point you have to worry about as well. We approach this with endpoint and gateway inspection (segmenting mobile from the network and enforcing access), along with mobile botnet inspection through the gateway and carrier for 3/4G/LTE.

Zero-day threats are also difficult because, well, they are zero-day, meaning that at their inception in theory nobody knows about and can protect against this threat. Actually, this is where beefy body armor (UTM) helps, since if you cannot, for example, protect against a zero-day exploit, you may be able to mitigate at other layers. For example, the zero-day threat may reach out to a third party server that is known to be malicious – or use a botnet protocol that is known and can be blocked. As discussed previously, we also try to tackle zero-day exploits by finding them ahead of attackers and rolling out protection in advance (in zero-day state) before the affected vendor rolls out a patch.

With multiple Next Generation UTM security device companies in the market what separates Fortinet from its competition.

DM: We really pioneered this space, so, simply put – we know what we are doing.

We have always prided ourselves on building from the ground up, we have a very large R&D group that continues to execute and enhance existing technologies while building new ones, led by our upper management team and of course Ken and Michael Xie who founded Fortinet with a wealth of experience from Netscreen at the time. We have patented and great technology across the UTM spectrum thanks to this. Everything from a solid antivirus development team that works in-house with our researchers, to intelligent automated systems, cross-intelligence and event correlation and our in-house zero-day threat research team. Our in-house approach at the core allows us to accelerate our approach to security since there really are not that many road blocks. This view is backed by Gartner as we continue to lead their UTM Magic Quadrant.

What do you think about cyber war?

DM: I think it is often abused in terms of marketing and hype. However, there is certainly a real element to it and it should be of concern. My largest concern with cyberwar is critical infrastructure. Elements like DDoS attacks, espionage are certainly valid components of cyberwar. However, once critical infrastructure is affected, you are truly crossing the barrier of virtual and physical space, potentially putting lives and human health at risk. One of our predictions this year was activity on these threats: *http://blog.fortinet.com/2012-threat-predictions/.*

Unfortunately, the truth is that critical infrastructure security is just not where it should be right now considering, well, the *critical* part of this infrastructure.

Do you think that we have reached a stage where war is being waged by states, or are we more likely to see different forms of hactivism?

DM: I think there is some truth to this, but this is certainly one of the hardest things one can attribute. Attribution is difficult because of laws and regulations – it often comes down to tracing one IP address and pointing the finger at a state. Let me just say this. Nowadays with crime services (hackers for hire), and malicious infrastructure (botnets, code for sale) – it is quite easy for any state to outsource their cyberwar activities.

Now Hiring

Teamwork

Innovation

Quality

Integrity

Passion

Sense of Security

Compliance, Protection and Business Confidence

Sense of Security is an Australian based information security and risk management consulting practice. From our offices in Sydney and Melbourne we deliver industry leading services and research to our clients locally, nationally and internationally.

Since our inception in 2002, our company has performed tremendously well. We thrive on team work, service excellence and leadership through research and innovation. We are seeking talented people to join our team. If you are an experienced security consultant with a thorough understanding of Networking, Operation Systems and Application Security, please apply with a resume to careers@senseofsecurity.com.au and quote reference PTM-TS-12.

info@senseofsecurity.com.au
www.senseofsecurity.com.au

The Hunt for Pentesters

As the world of IT becomes more and more sophisticated, so does the demand for experienced IT professionals. Good pentesters are particularly hard to find because they need to be both deeply technical, and highly communicative.

When a company hires a penetration tester, trust is everything. Indeed, a company will have to expose its internal security operations and all sorts of secrets to pentesters, should they be internal or hired through a consulting company. Because of this, the recruitment process should not only assess the technical skills but should also assess the personality and background of a potential pentester.

The aim of this article is to give the reader and idea of the criteria assessed by headhunters to identify trustworthy and technically capable pentesters. By shedding light on those aspects, this article will therefore give the readers an understanding of the usual education, competencies and soft skills a valuable pentester should demonstrate.

Who hires pentesters?

Due to a high level of due diligence to ensure the confidentiality, integrity and availability of customer transactions, pentesters are often sought at banks and other financial companies. However, IT security is also an issue in other industries such as pharmaceutical, consumer goods, manufacturers, telecommunications, etc. These companies need to rely on an IT infrastructure that must be efficient at all time to ensure performance not only for internal people but also for external audience, such as clients, investors, suppliers, etc.

Another aspect to point out in order to define the types of clients is the cost of IT security. It is often seen as a preventive medicine: *You don't really know if it's working or exactly how well it's working, but you do know when it fails* (Sperling, 2009). As such, companies often hire consulting companies that will not only perform penetration testing but will also offer complete security audit services. Therefore, consulting companies such as the Big-4 and other smaller ones, make the big part of the companies employing pentesters.

In short, there are two types of employers: end clients such as financial institutions, and consulting companies. As we will discuss further in this article, assessing the soft skills part of a pentester for a consulting company should be well processed and mastered. The reputation of a consulting company could be seriously damaged if the pentester was to fail to demonstrate honesty and professionalism in delivering projects to its customers.

Ed Sperling, (02/09/2009). Measuring IT Security Costs. Forbes, Retrieved from *http://www.forbes.com/2009/02/07/security-information-tech-technology-cio-network_0209_security.html*.

How to get to pentesters?

Like in other industries, good talent is hard to find. The best pentesters are not on job boards because they don't need to be. Employers understand their value and, unless economic situations force them to cut back, make them stay and feel comfortable in their position.

That's where the headhunter's job begins-- finding the best suitable candidate for a potential client. In the ethical hacking area, it is often said that the tester should think like a hacker to be able to identify vulnerabilities; so do the headhunters to identify pentesters profiles. An expert headhunter will have to jump into a pentester's shoes in order to reach his network and find the suitable candidate. This can be done by reviewing the pentesting blogs and contacting the most active members, getting names from relevant certification exam subscriptions, consulting popular social media networks, reaching personal contacts that would recommend a headhunter to expert candidates, etc.

An important subject that I feel should be discussed here is whether a company should hire a *blackhat* hacker as a penetration tester. There is no clear answer on that matter and the decision should be pondered; however there are several points to consider before hiring a *blackhat* hacker:

Risk

Even though hackers can test the system to its limit, a consulting company takes a high risk in hiring past criminals (convicted or not) in their teams. If you do not trust the individual to do what they were hired for, and nothing more, then you should not use the resource.

Testing methodology is different

The *blackhat* hacker will often exploit a weaknesses to fully penetrate the system, whereas the well-trained penetration tester may test an identified vulnerability to the point of confirming it, then move on to finding additional vulnerabilities.

Understanding the business is key

A *blackhat* hacker might have valuable technical skills, but he might not have the necessary business acumen to communicate the risk behind the vulnerability. Security is only taken into account by CIOs when there is an identified risk to the business that could lead to potential financial losses.

What will headhunters look for in a pentester's resume?

Education

There is no specific program focused either on IT security or on penetration testing. Pentesters have usually a MSc degree in IT. The work of a pentester is demanding and hands-on knowledge is needed. Penetration testing is also one aspect of IT security and the entry level of a career that could lead to more auditing or risk assessment, hence the requirement for a higher level of education.

The academic criteria should not be a prohibitive criteria. Expert pentesters often have lower education backgrounds and when it comes to penetration testing, one should also value the weight of practical experience.

Penetration testing is an ever-changing art. A good penetration tester will have to constantly ensure a technology watch in order to stay informed on the latest threats and the evolution of the IT infrastructure. Constantly working with new technology enables the tester to anticipate system vulnerabilities, to address them, and master the detection tools. An indication of extra-professional activities such as blogging, participation in seminars or other *ethical hacking* meetings will confirm that the candidate is keeping up to date on the technics and will furthermore demonstrate curiosity, tenacity, and passion; qualities that are essential to be a valuable pentester.

Certifications and further education

Eventually, a pentester would feel the need to certify his practical knowledge or to get further trainings. Headhunters and companies will highly value certifications in IT security, especially consulting companies which services can be sold with high added value.

I have listed below the most common certifications in IT security. While penetration testing is a component of IT/security audit, the here below certifications/trainings will either focus on penetration testing or IT audit. See Table 1.

After the selection process that consists in reviewing the resumes, the soft skills assessment can start in the framework of interviews.

Soft skills

Let's have a look at the soft skills needed to perform as a pentester.

The main qualities required for a position of penetration tester are:

- *Being an information sponge – Curiosity and willingness to constantly learning*. As mentioned earlier, expert pentesters are the ones that keep up to date on the latest technologies and that can also anticipate new potential threats.
- *Solution-oriented and investigative skills*. The work of a pentester is to find what should not be found; a pentester need to be comfortable with ambiguous and complex situations.
- *Big picture orientation*. A pentester should understand the contribution and impact of his work to the overall company structure.

Table 1. *Certifications*

Certification	Description	Requirements
IT AUDIT		
ISACA (www.isaca.org)	Certified Information Security Audit (CISA)	
	This is the basic and the most important among the audit certifications. Companies do require more and more this certification as a proof of mastering the concepts of security, control and audit of information systems.	Taking the exam requires a minimum of 5 years of professional information systems auditing, control or security work experience (as described in the CISA job practice areas). The CISA exam consists in a multiple-choice exam of 200 questions to be answered in 4 hours. Under certain circumstances, the certification can be done prior to the 5-year work experience (see the website for further details).
	Certified Information Security Manager (CISM)	
	Certified Information Security Manager (CISM) The CISM is designed for (Aspiring) Information Security Managers but also for IT/IS consultants. While CISA exam is the most popular, CISM is more geared towards security management. You do not need CISA to earn CISM.	The CISM exam consists in a multiple-choice exam of 200 questions to be answered in 4 hours. A candidate must receive a score of 450 (out of 800) or higher to pass the exam.
ISC2 (www.isc2.org)	Certified Information Systems Security Professional (CISSP)	
	There is a competition between CISA and CISSP. A lot of professionals I have talked with are saying that the CISSP is more valuable and demanding in terms of technical skills. The CISSP CBK consists of the following ten domains: • Access Control • Telecommunications and Network Security • Information Security Governance and Risk Management • Software Development Security • Cryptography • Security Architecture and Design • Operations Security • Business Continuity and Disaster Recovery Planning • Legal, Regulations, Investigations and Compliance • Physical (Environmental) Security	The candidate must possess a minimum of five years of professional experience in the information security field or four years plus a college degree. There are some exceptions to those requirements (see website for further details). A candidate that passes the CISSP exam must be endorsed by another $(ISC)^2$ certified professional before the credential can be awarded. Passing candidates will be randomly selected and audited by $(ISC)^2$ Services prior to issuance of any certificate.
	Lead auditor ISO/IEC 27001	
	The certification is to ensure that the candidate has the knowledge and the skills to audit an Information Security Management System (ISMS) based on ISO 27001 and to manage a team of auditors by applying widely recognized audit principles, procedures and techniques.	
ETHICAL HACKING		
EC-Council (www.eccouncil.org)	Certified Ethical Hacker (CEH)	
	The Certified Ethical Hacker certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.	You need to earn the ENSA certificate before taking the CEH exam.
	Certified Hacking Forensic Investigator (CHFI)	
	The CHFI certification validate the candidate's skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute in the court of law.The CHFI certification will benefit: • Police and other law enforcement personnel • Defense and Military personnel • e-Business Security professionals • ystems administrators • Legal professionals • Banking, Insurance and other professionals • Government agencies • IT managers	Computer forensics profiles are in high demand in the US and in government agencies as cyber criminality is on the rise
	Licensed Penetration Tester (LPT)	
	This certification s a natural evolution and extended value addition to its series of security related professional certifications. The LPT standardizes the knowledge base for penetration testing professionals by incorporating best practices followed by experienced experts in the field. The objective of the LPT is to ensure that each professional licensed by EC-Council follows a strict code of ethics, is exposed to the best practices in the domain of penetration testing and aware of all the compliance requirements required by the industry. The objective of Certified Security Analyst "pen testing" certification is to add value to experienced Information Security professionals.	You must achieve both CEH and ECSA to apply for the certification.
GIAC (www.giac.org)	GIAC Certified Incident Handler (GCIH)	
	GIAC Certified Incident Handlers (GCIHs) have the knowledge, skills, and abilities to manage incidents; to understand common attack techniques and tools; and to defend against and/or respond to such attacks when they occur. This certification is for individuals responsible for incident handling/incident response; individuals who require an understanding of the current threats to systems and networks, along with effective	SANS Institute delivers training for all the GIAC certifications. (www.sans.org)
	GIAC Penetration Tester (GPEN)	
	The GPEN certification is for security personnel whose job duties involve assessing target networks and systems to find security vulnerabilities. Certification objectives include penetration-testing methodologies, the legal issues surrounding penetration testing and how to properly conduct a penetration test as well as best practice technical and non-technical techniques specific to conduct a penetration test.	SANS Institute delivers training for all the GIAC certifications. (www.sans.org)
	GIAC Web application Penetration Tester (GWAPT)	
	Web applications one of the most significant points of vulnerability in organizations today. Most organizations have them (both web applications and the vulnerabilities associated with them). Web app holes have resulted in the theft of millions of credit cards, major financial loss, and damaged reputations for hundreds of enterprises. The number of computers compromised by visiting web sites altered by attackers is too high to count. This certification measures and individuals understanding of web application exploits and penetration testing methodology.	SANS Institute delivers training for all the GIAC certifications. (www.sans.org)
	GIAC Certified Exploit Developer (GXPN)	
	This exam certifies that candidates have the knowledge, skills, and ability to conduct advanced penetration tests, how to model the abilities of an advanced attacker to find significant security flaws in systems, and demonstrate the business risk associated with these flaws.	SANS Institute delivers training for all the GIAC certifications. (www.sans.org)
ISECOM (www.isecom.org)	OPST (OSSTMM Professional Security Tester)	
	The OPST is a certification of applied knowledge designed to improve the work done as a professional security tester. This is a certification for those who want or need to prove they can walk the walk in security testing, the discipline which covers network auditing, ethical hacking, web application testing, intranet application testing, and penetration testing. And it is a critical, eye-opening class for security auditors, network engineers, system and network administrators, developers, network architects, security analysts, and truly anyone who works in IT from systems to networks.	OSSTMM stands for Open Source Security Testing Methodology Manual. Many researchers from various fields contributed because they saw the need for an open method, one that was bound towards truth and not commercial gain or political agendas.

- Analytical capacity. To be able to find vulnerabilities, a pentester need to have a methodological and deductive approach. Analytical skills will also help him to write good reports and to summarize his findings.
- Capacity to explain technical terms to non-technical people. This is essential to define a common ground from which to begin in explaining problems and recommending remediation steps in a way that is easily understandable by the client.
- Honesty and ability to deal with sensitive data. It is particularity essential for pentesters in consulting companies as they will have access to data at their clients. These skills are even more important in the forensics area (cyber criminality).
- Writing skills. A critical part of the job as a pentester is being able to write reports
- Language skills if not English speaking

In addition, more skills can be required when working in consulting companies:

- *Versatility*. These companies will highly value the fact that a pentester has various experiences in different industries and IT infrastructures. It will give the headhunters the evidence that a pentester is flexible in different environments.
- *Customer service*. A pentester consultant will have to take action and make decisions that successfully build customer value; customer must be put at the central of all thinking.

In conclusion, both technical and soft skills aspects need to be evaluated to hire a valuable and expert penetration tester. I believe that this article has drawn what is the common profile of a penetration tester with respect to both sets of skills. Now you know that headhunters are watching you!

FABIANA SCHÜTZ

Fabiana Schütz graduated in Work and Organizational Psychology at the University of Neuchatel (Switzerland) in 2006 where she spent one year studying at the California State University of Long Beach. Co-founder of Mensys Group, a recruitment agency specializing in niche markets within IT, Engineering and LifeSciences, they operate in Europe with offices in Switzerland and Poland.

Interview with
Armando Romeo

Armando Romeo is the founder of eLearnSecurity, responsible for day-to-day management as well as content creation and delivery of all company courses. Prior to founding eLearnSecurity, Armando served as administrator and head of security for the Hackers Center Research Group and IT Security Services Manager for the Italian Security Brigade. Armando's has extensive experience and expertise in the areas of network security, information security, secure coding and design, Web application security, penetration testing and security awareness.

During his career, Armando has conducted hundreds of web application and network security assessments. Armando is author of the seminal work on Internet security, titled Penetration testing course – Web App Security. He holds a Master's Degree in Computer Engineering from the Universita di Pisa.

What made you decide to start an endeavor like eLearnSecurity?

Armando Romeo: Since my early days in the industry, I strongly felt the need to share with others what I had to learn with a great deal of hard work, focus and passion. At that time you had to figure everything out on your won and mostly through trial and error... This was not easy at times.

From the age of 13, I started creating newsletters where I shared my findings. Throughout the years, I understood there was a need for training courses that attracted those professionals who were not happy to use tools or information without knowing what they did.

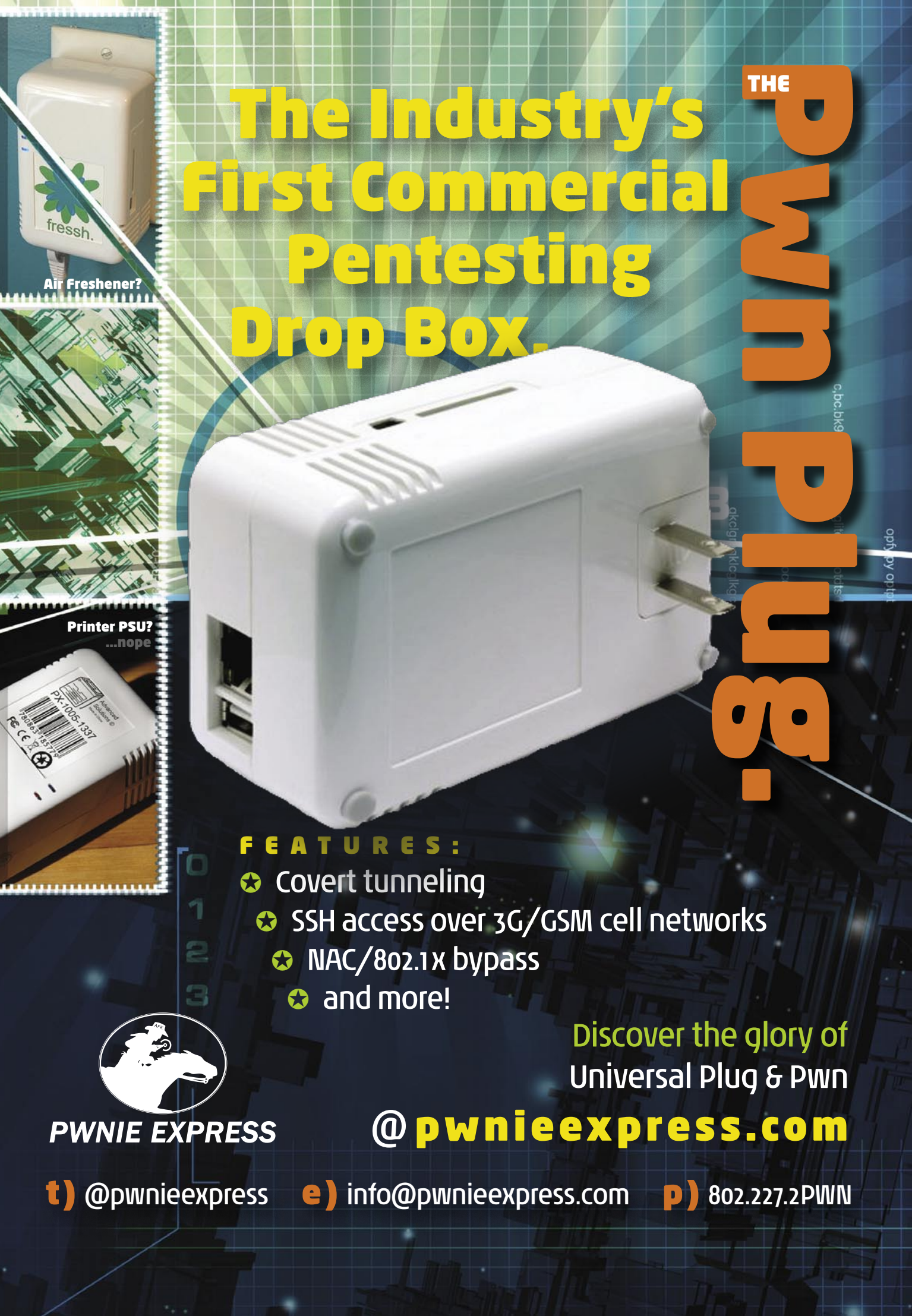
We really wanted to provide this kind of student the intimate details of each technique and all of the necessary hands-on practice to reach their *Multimate* understanding – that *A-Ha!* Moment!

Another problem was the reputation of the penetration tester, which was too related to that of the (Malicious) Hacker. Although the penetration tester has hacking skills and (hopefully) the hacking mind-set, they are a high profile and competent individual. One of our goals was to professionalize the profession.

What skills does the industry expect from various levels of penetration testers (novice, mid-level and experts)?

AB: Novices are usually not asked to take over project management tasks, such as reporting or negotiation of the scope of engagement. They are usually employed during the testing phase on less critical targets.

Mid-level and expert pen testers often deal with the strategy for the whole penetration testing engagement, determining priorities and best approaches. In some


fressh.
Air Freshener?
Printer PSU?
...nope
PX-1005-1337
THE
Pwn Plug.
The Industry's First Commercial Pentesting Drop Box.
FEATURES:
Covert tunneling
SSH access over 3G/GSM cell networks
NAC/802.1x bypass
and more!
Discover the glory of
Universal Plug & Pwn
@pwnieexpress.com
PWNIE EXPRESS
t) @pwnieexpress
e) info@pwnieexpress.com
p) 802.227.2PWN

Interview with
Ian Moyse

Ian Moyse has over 25 years of experience in the IT Sector, with nine of these specialising in security and over 23 years of channel experience Starting as a Systems Programmer at IBM in the mainframe environment, he has held senior positions in both large and smaller organisations including Senior Vice President for EMEA at CA and Managing Director of several UK companies. For the last 7 years he has been focused on Security in Cloud Computing and has become a thought leader in this arena.
Moyse has been keynote speaker at many events and runs one of the largest Channel Groups worldwide on LinkedIn. He sits on the board of Eurocloud UK and the Governance Board of the Cloud Industry Forum (CIF) and in early 2012 was appointed to the advisory board of SaaSMax.
Moyse was recently awarded global 'AllBusiness Sales AllStar Award for 2010' and The 'European Channel Personality of the Year Award for 2011 and was named by TalkinCloud as one of the global top 200 cloud channel experts in 2011 and listed on the MSPMentor top 250 list for 2011 which tracks the world's top managed services experts, entrepreneurs and executives. He has also recently been awarded the accolade of Channelnomics 2011 Influencer of the year for Europe.
For those wishing to connect to this Technology Cloud Thought Leader his linkedin profile is at http://uk.linkedin.com/in/ianmoyse and he can be followed on Twitter @imoyse

Should cloud providers allow penetration testers use their services to perform penetration tests?

Ian Moyse: Cloud providers as a definition covers a spectrum of solutions from SaaS, IaaS, PaaS etc. Pen testing is of high value to cloud providers to ensure security is not only conformant, but also that it is demponstrable to clients. However the testing possible will vary on the level and type of services being provided. Also the pen testing will need to conform to rules around consent and notification and as a cloud provider typically has multi-tenancy of customers it

Workbooks.com

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

Pentesting your own employer?

Consulting firms offering pentest services abund, and they constitute the bulk of the employment market for pentesters. As the acceptance of pentests as a value added service has reached even the most conservative businesses, a new trend is developping by which organizations create they own internal team of pentesters.

This article covers some of the motivation for such organizations to go this route, as well as some of the challenges along the way.

Where do pentesters work?

Becoming a pentester, or at least a competent one, takes time and expertise. A good pentester will have expertise in multiple areas: web, mobile, assembler, databases, networks, Unix, Windows, etc. Developing that expertise is a long process and learning how to use it to exploit vulnerabilities is an even longer process. Of course, after such a significant investment in terms of learning, experimenting, and eventually starting to pentest, a good pentester would like to generate revenue and make a living out of it. Most pentesters will end-up working for consulting companies that provide pentesting services. Some ill-advised pentesters will choose the dark side. There is however another option for those who know where to look and that is internal pentesting.

A significant number of organisations now have their own internal pentesting team. They are organisations for which security of their systems and application is mission critical and who have purchased external pentesting services in the past and have choosen to use an internal penetration team instead, for tactical and strategic motives. Such organisations hire pentesters to test internal application, systems and networks on a continuous basis.

Why bother with an internal team?

Most external firms maximize profits by minimizing the work done, usually through automation. Unless of course the firm provides a manual pentest service in which case the customer has to be patient and willing to pay large amounts of money. Manual pentests cost a premium because they are normally done by senior pentesters, they usually require more than one person working at it and they take time.

So, as a rule of thumb, if a pentest is relatively inexpensive, it's probably largely automated. Pentests are never cheap, but manual ones are particularly expensive. The problem with automated pentests is not that they are automated; it is that they are executed by a tool, or a set of tools that hackers can also use. If you fix all the vulnerabilities that a tool exposes, a hacker using manual techniques can still compromise the application or system.

The only economically viable way for an organization to benefit from manual pentests is to have its own pentest team. For the price of a one or two manual pentests, an organisation can hire a permanent resource. However, the creation of an internal team of pentesters should be done seriously and a minimum of two people is really what it takes, not only to form an actual team, but to ensure complementary expertise, brainstorming capability, ability to run two tests concurrently, and provide more down to earth features

Interview with
Erdal Ozkaya

Erdal Ozkaya is the founder and Senior Microsoft Instructor of CEO IT Training, which has now merged with Fast Lane Asia Pacific; one of Australia's Silver certified Microsoft Learning Partners.
Erdal travels across Australia teaching IT workshops and has served as Project Manager/Engineer for several large organisations in Australia, China, Philippines and the USA.
Erdal actively participates in worldwide events as a Technical Lead and Speaker. He was awarded "Best Technical Learning Guide" and "Best Speaker" in Microsoft Technical Education Seminars (TechEd) Australia.
He specialises in Active Directory; Windows Client and Server O/S's; Security/Exchange 2007/2010; Sharepoint2007/2010; EC-Council Security and ISO 27001/27002/ 27005.
The passion and commitment that Erdal has shown to his work has been recognized by Microsoft. In 2009, 2010, 2011 Erdal Ozkaya was awarded the Microsoft Most Valuable Professional (Windows Expert -IT Pro) award. Erdal is also a Security Consultant and Certified Ethical Hacker Trainer.
Recently, in April 2010, Microsoft went one step further and announced Erdal Ozkaya as the FIRST Microsoft Certified Leaning Consultant in Australia. There are only 16 recipients of this award in the world, with only one recipient in Australia.
Even more recently EC Council announced Erdal Ozkaya as the Global Instructor of the Year Award (2011). The award was in recognition of instructors that have contributed significantly, and made a difference to the information security community by providing leading EC-Council certification programs.
Erdal is also leading some User groups of PASS, GITCA (Culmins) & INETA


HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS
www.htbridge.ch
ORIGINAL SWISS ETHICAL HACKING
Digital Forensics
Malware Analysis
Penetration Testing
Source Code Review
Security Audit & Consulting
GENEVA WORLD TRADE CENTER II T. +41 22 723 24 24 F. +41 22 788 35 71 info@htbridge.ch

Interview with
Peter Wood

Peter Wood is a world-renowned security evangelist, speaking at conferences and seminars on ethical hacking and social engineering. He has appeared in documentaries for BBC television, provided commentary on security issues for TV and radio and written many articles on a variety of security topics. He has also been rated the British Computer Society's number one speaker.

Peter has worked in the electronics and computer industries since 1969. He has extensive experience of communications and networking, with hands-on knowledge of many large-scale systems. He founded First Base Technologies in 1989, providing information security consultancy and security testing to commercial and government clients. Peter has hands-on technical involvement in the firm on a daily basis, working in penetration testing, social engineering and awareness.

First Base has been on the market since 1989. Can you give us some tips how to survive in the IT field for so long?

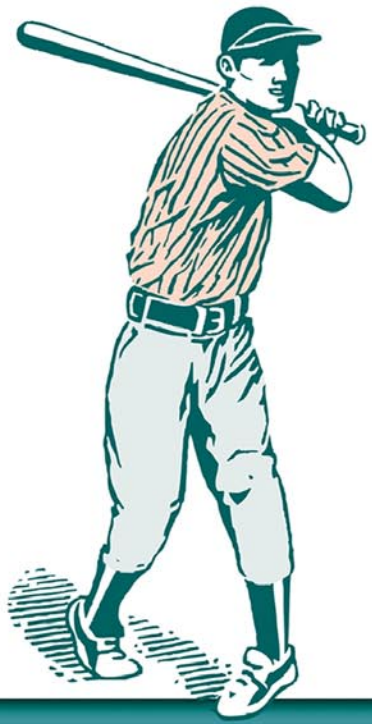
Peter Wood: I think it's because we live by these words: „Ethical, Pragmatic, Professional". Firstly „Ethical": we do what we say, we promise only what we can deliver, we never to pretend to know something when we don't.

- Secondly „Pragmatic": we don't try to demonstrate how clever we are, but instead we try to give something of real value to the client's business. We look for simple problems as well as interesting, complex ones!
- Thirdly „Professional": we try to provide a service which we would want to buy ourselves if we were the client. We have systems which record everything we do, that ensure that we do what we promise, when we promise, in the way that we promise.

What we *don't* do is look for a fast profit – we want clients who want to work with us for the long term.

Why did you choose pentesting over computer software or programming language?

PW: Because it's interesting, it suits the way my mind works and because it's profitable. I've always been fascinated in how things work and why they don't work when they're broken. Pen testing is like being a combination of Sherlock Holmes and a child!



FIRST BASE technologies

You're in safe hands

The information security consultancy

www.firstbase.co.uk

+44 (0)1273 45 45 25

Visit us on stand A30 at Infosecurity Europe

24 - 26 April 2012, Earls Court, London

Pen Test:

A business need to success

The fact is that nowadays, it could be very obvious when it comes to our minds those basic "techs" needs that we are used to. You may certainly name a variety of devices that at this very moment you could not live without – laptops, smart phones, tablets, etc. Allow me to take you a little further and think of a moment over the services you may access online through these basic "techs" needs we just defined – social networks, emails, stocks, payments, etc.

Information Technologies had helped companies among the time to cover almost every type of services, satisfying our needs and also making new ones for us. From the simplicity of surfing the Internet to the complex networks and systems that supports every imaginable critical service we use. Consequently, companies aim resources to maintain the services just mentioned above, focusing their budgets over developing and implementing advance technology. Different flavors of cloud computing, virtualization, mega data storages and super fast networks have not stop being profitable over almost every type of business, and if not it will at their next plan to expand.

From ancient civilizations we have witnessed the most varied nature of threats to any kind of organization that succeeded on it purposes and convictions, 21st century's organization are not excluded to this fact, and it might be worse, I can bet bad intentions had being mastered… no need to go in depth at this matter, it is quite easy to be concluded by yourself, the question would be – Is your castle shielded and your guards ready?

The expression

Penetration Testing is a wide term and also has different points of views according to security expert's statements, the most conservators agree that is essential to perform it continuously and if you fail on this duty you may sit and wait the punishments of hell, others just think is a waste of time. Under my concern penetration testing is a lot more complex than state an opinion.

The truth is that we need to understand what the concept really means. Because when it comes to relate the term *Pentest* by anyone that is not familiar with our geek expressions, and even worse abbreviated expressions like xss, sql injection or DDoS, an expected reaction could be perfectly an automatic denied of the grammatical term Penetration Test. Think of an example, out of the geek bubble, like *Let's hire some ethical burglar to try to break into our houses*? – Don't think so.

Pentest it is not just breaking into networks or systems like in the movies, it is a set of actions that leads to results throughout methodologies exclusively to take countermeasures against vulnerabilities that expose the mission of a certain organization interested to accomplish this purpose and also have good reasons to protect their assets against potential threats, specifically hacking attacks.

Business should take penetration testing as any other service with its respective priority to accomplish their business goal neither more nor less. According to this simple statement penetration testers should offer and must grant what a business need out of a service, improve its value.

Interview with
Pavol Lupták

Pavol Lupták gained his BSc. at the FEI-STU in Bratislava and MSc in Computer Science at the Czech Technical University with a master's thesis focused on ultra-secure systems. He holds many prestigious security certifications including CISSP and CEH, He is a Slovak OWASP chapter leader, co-founder of Progressbar and SOIT organizations where he is responsible for IT security. Pavol has given regular presentations at various worldwide security conferences (in the Netherlands, Luxembourg, Berlin, Warsaw, Krakow, and Prague). In the past, he has demonstrated vulnerabilities in the public transport SMS tickets in all major cities in Europe, together with his colleague Norbert Szetei, he demonstrated vulnerabilities in Mifare Classic RFID cards. He has 14 years of experience in IT security, penetration testing and security auditing including social engineering and digital forensic analysis. He is co-author of the OWASP Testing Guide v3, has a deep knowledge of the OSSTMM, ISO17799/27001 and many years of experience in exploring and discovering vulnerabilities. He has knowledge of many programming languages (ASM, C, C++, XSLT, Perl, Java, PLSQL, Lisp, Prolog, scripting languages) and operating systems. He is also focused on VoIP and some interesting IT security research. PGP key. SMIME key, LinkedIn Profile.

When did you decide to bind your future with IT security?

Pavol Lupták: When I was 18, during my studies at the University I discovered the magic of Ultrix, Digital Unix and IRIX :) My first brush with IT security was with buffer overflows and Aleph1 shellcode in 1997.

Can you give examples of challenges that you found the most demanding at the beginning of your career?

PL: Slovakia was and still is a small market for IT security, especially penetration testing. The situation is a bit better in the Czech Republic. Most Slovak/Czech

ITonlinelearning group

Free Demos

ITOnlinelearning offers Network Security courses for the beginner through to the professional.
From the CompTIA Security+ through to CISSP, Certified Ethical Hacker (CEH),
Certified Hacking Forensic Investigator (CHFI) and Security Analyst/Licensed Penetration tester (ECSA/LPT).

e-Learning

- Cost Advantage
- Tailored Solution
- Monitor Progress
- Flexible Study
- Certify Anywhere, Anytime
- Refresh Skills
- Explore New Courses
- Expert Help

Course Direction

- Project Management
- Support
- Networking
- Server
- Security
- Database
- Developer
- Office

Tailored Advice and Discounts

0800-160-1161 or Livechat

Please Call one of our Course Advisors for help and Tailored Advice -during office hours
(Mon-Fri 9am-5.30pm)

Telephone: 0800-160-1161
International: +44 1795 436969
Email: sales@itonlinelearning.co.uk
support@itonlinelearning.co.uk
Registered Office: 16 Rose Walk, Sittingbourne, Kent, ME10 4EW

Penetration Testing
in Indonesia: A Case Study

The Indonesian Central Bank (Bank Indonesia) had released the national regulation which includes policy and procedures regarding the protection of information assets based on Risks.

This regulation has been triggering the Information Security Awareness in Indonesia's banking industry. It is stated that banks and other financial institutions have to conduct vulnerability assessment and penetration testing at minimum once every three years in order to protect and maintain their critical information assets from current and future threats.

Every three years, the Indonesian Central Bank will regularly performs information systems auditing (IS Audit) to conform that organizations under their authorities comply with their regulations. IS Audit will focus on some areas which includes Data Center operations, IS Security, Risk Assessment, etc. Information security awareness program has been promoted actively and this is also one of the vital subjects to be audited and at minimum must be done once a year and should be continuously updated to reflect the current and future threats, vulnerabilities and attacks. The objective is to increase the general awareness on how to handle and protect information assets as per organization as well as privacy protection.

Surprisingly ITIL, COSO, COBIT, ISO 27001 and other International Standards have been quite successfully adopted by most of organizations especially government agencies, banking and other financial institutions. Even BSI (*Badan Standarisasi Nasional*), the national standardization agency have successfully adopted and publish the localize version of ISO 27001 for most organizations throughout Indonesia. BSI provides training, implementation guidelines and assistance for new and existing organizations to ensure that the standard can be implemented smoothly.

Vulnerability Assessment & Penetration Testing

Penetration testing and assessment standards for auditing: systems, network and applications follows most commonly implemented IT industry standards and methodologies. Assessment standards and methodologies such as *NIST SP 800-115, OISSG – ISSAF,OSSTMM, OWASP Application Security Assessment Standards and SANS Security Assessment Guidelines for Financial Institutions have been* adopted and implemented successfully. Vulnerability assessment & penetration testing has also been conducted in many organizations as part of ISO 27001 implementation and certifications with the assistance of other authorized implementers and auditors. *Request for Proposal* (RFP) of most organizations will specifically request that those international and IT industry standards and compliance should be addressed.

Part of the ISO 27001 standard is that the organization must have established en effective IT Security Policy with procedures or guided steps. At minimum, external IS Auditors and penetration testers must review the

Interview with
Harish Thakral

Harish Thakral is the Director of Information Security for TechBharat Consulting with 5 years of experience and achievement across the whole spectrum of management aspects of Information Security. Apart from conducting training, his expertise includes design, implementation and the management Windows and Linux-based networks, etc. Currently, he conducts training for EC Council and other groups. His role also includes working with the technical team for Vulnerability Assessment & Penetration Testing.
Harish Thakral has been pretty active in this field for quite some time. He has solved many cases: fake profile cases, email spoofing cases, phishing cases, espionage cases, credit card fraud cases, cyber pornography cases, and SMS spoofing cases in association with many Security Agencies.

What does TechBharat Consulting specialize in?

Harish Thakral: TechBharat Consulting is an Information Security Company started with the aim of delivering Information Security Standards all across the globe. TechBharat is an accredited training center for the EC Council, offering the most prestigious certification starting from Certified Ethical Hacker (DoD 8570 Approved), Computer Hacking Forensic Investigator, EC Council Certified Security Analyst, and Licensed Penetration Tester. EC Council certifications are designed to provide the foundation needed by every IT Security Professional. EC Council curriculum provides the broad range of skills and knowledge needed to build and manage an organization's networking and security operations, and to use effectively various resources to achieve operational excellence.

What inspired you to start this company?

HT: After the Cyber Attacks over the Indian CBI Central Bureau Of Investigation, a big question arose with regard to the security risk of the Nation due to the lack of proper knowledge in dealing with the Information Security Standards. NASSCOM predicts a requirement of 10 lacs professionals by the year 2010. Currently, the number of security professionals in India is around 22,000.

You are a worldwide company. In which parts of the world do you have the most customers?

HT: We have clients from the United States, Australian, Russia, Dubai, Sri Lanka and many more.

Which countries have the best perspectives as far as IT development is concerned?

HT: The United States would be the best considering information technology development.

Interview with
Jeromie Jackson

Mr. Jeromie Jackson is a seasoned security expert with over 20 years of experience leading security consultancies providing information security services for Fortune 500, large enterprise, and mid-sized businesses. A well-known speaker, President of the San Diego OWASP Chapter, SANS Mentor, and previous Vice President of the San Diego ISACA Chapter, Mr. Jackson is well networked. Covered on Forbes Magazine, Mr. Jackson is a frequent speaker, author, and interviewee for many industry and technology related media outlets. Mr. Jackson works with several vendors to test the security of their software, and has recently published vulnerabilities in several security counterm easures and business applications. Mr. Jackson holds CISSP, CISM, COBIT, & ITIL certifications and is a SANS Mentor for the CISSP curriculum. Primary areas of expertise include penetration testing, physical penetration testing, PCI and other regulatory readiness services, governance, and IT risk management.

What are the services of Nth Generation?

Jeromie Jackson: We provide a wide range of services including internal & external vulnerability assessments, penetration tests, social engineering, physical penetration tests (Red Team), web application assessments, PCI-DSS & regulatory gap assessments, risk assessments, and security roadmapping, controls portfolio development, and training.

What the notion of „pentesting business" means to you?

JJ: It would depend on the context. I am in the *pentesting business* per-say. There is also the process of attempting to break business processes. For example, if I understand how a supply chain works, I may be able to order product @ a discounted price, re-route shipping, source alternative vendors, etc.

Could you share with us more details about different types of companies that use pentesting services?

JJ: The companies vary widely. Most are under at least 1 regulation, generally several. I find both sides of the security spectrum. Some are truly interested in protecting their assets, while others are simply interested in checking the box and satisfying audit. From an industry perspective I primarily work with financial, retail, heathcare, energy, and state & local government. Our customers are generally on the larger of the *small-to-midsize-business* (SMB) market, and large enterprise.

What should characterize such a company? How to recognize good pentesting services?

JJ: References are key! Length of time in the industry and strong certifications are useful. A track record of

Penetration Testing – Continious demand outweighs supply

Penetration Testing has been an area where demand has outweighed supply in recent years and this is gradually increasing. This is a result of existing Penetration Testing consulting businesses aggressively hiring and a real surge in other companies entering this market and requiring experienced Penetration Testers to help establish themselves in this very active space.

In the UK candidates who hold CREST or TigerScheme certifications are most sought after by all these companies, whether they are large multinational consultancies or small boutiques whose service offerings include penetration testing for government clients. The CREST scheme and TigerScheme, which are commercial equivalent to the CHECK scheme, allow penetration testers who pass exams to be recognised and work as CHECK Team Leaders or CHECK Team Members. The lack of supply of CHECK certified penetration testers is resulting in companies taking an increasing interest in less experienced penetration testers who can demonstrate abilities to achieve CHECK Team Leader or CHECK Team Member status. As a result certifications that demonstrate more practical ability such as those offered by Offensive Security (OSCP, OSCE, OSWP) are becoming more sought after. This trend is likely to increase in 2012.

One reason there are fewer candidates at the higher end of the experience and skills chain is that not every penetration tester specialising in this area earlier in their career will keep up the specialisation. Often they will diversify into other areas, gaining new skills and operating as a generalist or a specialist in a different niche. This may be due to lack of interest or ability in penetration testing, or due to interest in other areas. This type of movement is not unique to the penetration testing market, or indeed information security. It is quite common in general, that early in a career an individual will try various roles before settling into one area. Penetration Testing however is somewhat different as new threats and technologies are constantly emerging and therefore demand tends to be for full time penetration testers rather than Security Consultants who do this as one of many tasks. Successful candidates are those who see Penetration Testing as a passion of theirs rather than an interest, therefore specialist penetration testers at mid to senior levels with a provent track record are always in most demand and in shortest supply.

It should also be noted that to move across to penetration testing from another area of information security is harder further along in a career, and can mean starting over in a junior or entry level role, which is why more experienced security experts do not regularly make this transition.

At the higher end of the experience and skills chain, where there is the widest gap between supply and demand, it is not that there are fewer skilled penetration testers in the market, but that roles in this area have increased year on year, and the candidate pool has not increased at the same rate. While there are more penetration testers working today than a decade ago, there are far more penetration testing roles now than there were ten years ago.

In the next issue of

PenTest Market magazine

Available to download on April 15th

Soon in PenTest Market!

- How to recruit a good pentester
- Interview with Michael Brozzetti
- Pentesting market in Brazil
- Interview with Alexandro Fernandez
- Pentesting business startup

and more...

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



Get the best real-world Android education anywhere!

Attend AnDevCon III

The Android Developer Conference

May 14-17, 2012

San Francisco Bay Area

AnDevCon is the biggest, most info-packed, most practical Android conference in the world!

- Choose from over 65 Classes and Workshops!
- Learn from the top Android experts—including speakers straight from Google!

"AnDevCon had a good mix of presentations — some explored the newer cutting-edge technologies, and others offered a deep dive into existing ones."

—Priyanka Kharat, Software Engineer, Intel

"AnDevCon is great for networking, learning tips and tricks, and for brainstorming innovative, new ways to create apps."

—Joshua Turner, Software Engineer, Primary Solutions

Google Keynote!


Romain Guy and **Chet Haase**

Register Early and SAVE!

Follow us: twitter.com/AnDevCon

A BZ Media Event

Register NOW at www.AnDevCon.com