PenTest magazine

FREE

MOST WANTED PENETRATION TESTING SKILLS

ISSN: 2084-1117 04/2016

Managing Editor: Anna Kondzierska
anna.kondzierska@pentestmag.com

Proofreaders & Betatesters: Lee McKenzie, Robert Vanaman

Special thanks to the Betatesters & Proofreaders who helped with this issue. Without their assistance there would not be a PenTest Magazine.

Senior Consultant/Publisher: Pawel Marciniak

CEO: Joanna Kretowicz
joanna.kretowicz@pentestmag.com

DTP: Anna Kondzierska

Publisher: Hakin9 Media Sp.z o.o. SK 02-676 Warsaw, Poland
ul. Postepu 17D
Phone: 1 917 338 3631 *www.pentestmag.com*

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concering the results of content usage. All trade marks presented in the magazine were used only for informative purposes.

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.

Contents

Dear PenTest Readers,

We would like to present you our white paper about most wanted pentesting skills. We've talked with pentesters from all around the world to see what skills perfect pentester should have.

In this short issue you will find information about technical and soft skills that are highly appreciated in this field. You can also read an interview with some tips for acquiring a position of pentester. You will find opinions both from pentesters and recruiters side.
Note: some of the authors wanted to stay anonymous due to their working procedures.

We would also want to thank all the authors for the support. We appreciate it a lot. If you like this publication you can share it and tell your friends about it! Every comment means a lot to us.

Again special thanks to the Proofreaders who helped with this issue. Without your assistance there would be no PenTest Magazine.

We hope you will find a lot of useful and inspiring information in this paper.

Enjoy reading,
PenTest Team

Most wanted penetration testing skills

Sometimes we receive questions from people who want to start their career in IT: ''How to start? What should I learn? What are the most wanted pentesting skills?'' Of course, there is no correct answer, but we can point out some basic and most valuable skills that every pentester should have.

We asked pentesters simply ''What are the most wanted pentesting skills?'' Here we present you some answers that we received.

Justin, the pentester listed four skills:

1. Familiarity with specific tools, such as Metasploit, CORE, SAINT, Nessus, Mexpose, Wireshark, and NMap.
2. In depth knowledge of the protocols in use that will be attacked
3. Ability to work well in a team
4. Strong writing skills

As the knowledge of protocols and tools where quite obvious, we have asked about the third point, why should the pentester be good team player?

Justin said: *There are multiple people working on a specific penetration testing engagement. We all have to work together and compromise so that we get the job done. If someone can't work as a member of the team, it slows down the amount of work done and makes it harder for everyone who is part of the team where the one person who can't work as a member of the team is. Sometimes, it can be overcome, but, other times, without the team cohesion, we may be unable to complete the engagement. As an example, once there was one person who was on the same team as me and a couple other people.*
We all agreed to use Open Vas for the vulnerability scanning on a single server, but he constantly tried to use Nessus even though the rest of the team was using Open Vas. This lead to confusing and, for one potential vulnerability, contradicting results. It took two whole days to sort through the Nessus output and matching what we could match with our Open Vas output. It was not good for productivity. There are also other examples with the same person where he would not cooperate and be a team player, which had a negative impact on whichever team he was assigned to.

The other independent ethical hacker, Shawark Khan, agreed with this opinion:
I have met some researchers who share their knowledge with other researchers, which is a great thing. I have also seen researchers who hide things and don't want to share their experience. This is the worst pentester type. Every pentester should share experience and

knowledge so other people can learn new things and methodologies.

Semi Yulianto paid special attention to another ability:

Most important is the "report writing skills" since it's the deliverable that will support your findings and be communicated to the top management.

There were also other skills mentioned:

- *I'd say that the ability to pentest is actually at the top. I'm not joking. Many people claim to be pentesters, but can only run Nessus and hand over results. If you can do things at the level of someone with an OSCP or a GPEN, I'd say you're good.*
- *The ability to enumerate networks remotely, the ability to exploit known vulnerabilities to gain control of systems, the ability to think outside of the box and the "attacker mindset" are probably the most valuable skills.*
- *I think one of the best abilities is to really think outside of the box. Any dummy can run an automated scan and hand in a report. For example, at my job that's just one step. You then validate those vulnerabilities if they are false-positives or actually affecting. After that is the "real" pen-test in my eyes, in which I have to manually not only test the web application, but also the network behind it.*
- *I think one of the best pentesting skills an individual can have is pure passion. That results in people doing research outside of work that's so underrated. Security changes so much, it's unfortunate a lot of people do not bother to actually read the newest feeds out there.*

Although, out of all skills you gain, there are also complaints on the job market. How to gain the experience without the experience? One pentester confessed:

It was very hard to get my first pentesting job due to my only experience being a VM environment on my home network. Same goes for current pen testing roles. App pen testing is very popular but unless you have experience with burp(paid)/XSS/SQLi within a work environment, you probably will not get the job.

Most employers confirmed: knowledge and experience is more important than any other skills. Most companies claim that this is the first thing they pay attention to while reading someone's resume. Without the experience, you probably won't be even invited for the interview.

Larry Moore, Senior Information Risk Management Consultant at Dell, claims that there are two skills he requires from pentesters:

1. *Understand the environment you are testing. Too many pentesters rely on tools instead of understanding the TCP/IP and ethernet architectures. Sometimes, a good pentester can see something possible to exploit that novices may miss.*
2. *Never be afraid to test the limits of the system. A good pentester usually asks, "Hmm, I wonder what would happen if I tried this?" Good pentesters usually fail 9 times out of 10 but it is that 10th find that is usually something very valuable. Good pentesters realize they will fail the majority of the time but realize that ALL systems have flaws; it's just a matter of finding one specific flaw.*

Following the job offers, we asked some people who are currently looking for the position of pentester about the requirements and their answers were pretty simple. First of all, experience in ethical hacking and red team, then a few relevant certifications. One of the requirements was also understanding of mentioned processes, not only a knowledge about pentesting but also being familiar with the company structure.

Professional pentester also had advice for candidates on this position:

Advice: Don't come looking for a more 'senior' role on the penetration testing team without actual penetration testing experience. Again and again I see folks looking for senior roles with ZERO experience. I could see someone coming for a job as a penetration tester if they've got some serious experience in reverse engineering or something highly technical and similar. People coming with "I use nessus and nmap" or "I'm the master of AppScan/WebInspect" don't seem to understand what actual pentesting is. If you are wanting to switch careers and focus on penetration testing, do some work on your own. Get a CVE to your name, and then be happy with an associate/entry level position. You don't get to start at the top in pro football because you can play golf. Why would you think you can start as a senior penetration tester because you can administer a Windows network?

Frederic Mohr, CTO & IT Security Consultant at LastBreach, also has some points for pentesters:

Since many aspiring, young pentesters are asking themselves how to get a job, I thought I'd let you know what we usually look for in a pentester (even though we're not hiring atm).
Sorted by importance:
- A thirst for knowledge and desire to understand how things work in detail,
- Loyalty to the ethical hacker codex,
- Ability to think outside the box,
- Solid understanding of networking, Linux and basic web technologies,
- Solid security basics (For us, this is more about understanding why something is (in)secure than about knowing how to exploit it).

This is what we're usually looking for in a junior pentester, the rest is more about experience than skills. The more web applications or networks you test, the better you'll get at it. But the points mentioned above are much harder to teach (except for the last two, but you gotta start somewhere).

As you can see, pentesters and recruiters pointed out a lot of skills. Keep in your mind that nobody's perfect and it's impossible to follow them all. But on the other hand, it's never too late to improve yourself and we should try to be the best at what we do, which equals learning new skills and gaining knowledge.

Thank you for reading,
PenTest Team

Interview with Frederic Mohr

Interview with Frederic Mohr, CTO & IT Security Consultant at LastBreach UG.

Frederic Mohr is at home in both the offensive, and defensive side of security, coming from an administrative background he enjoys the challenges both worlds have to offer. Whether he is testing the boundaries of systems and software to find vulnerabilities or developing solutions that withstand those tests – the common denominator is his fascination with technology and security.

[PM]: What are the most important skills a pentester should have?

[FM]: Well, I could say that knowing most of the vulnerability types and how to exploit them is important, but to be honest that is something you pick up rather fast if you are working as a penetration tester full-time.

So for me, someone who wants to become a pentester, would have to prove to me that the time it takes to show them the ropes is a good investment, and that is done by showing genuine interest.

That means that they already have solid basics in networking, are proficient with their OS of choice, and able to use the other two big ones if needs be. They should know at least one programming or scripting language well enough to automate simple tasks, and maybe already have had a look at a few protocols up close. I do not really care which protocols, because what I am looking for is the general interest in the matter and not being afraid to dig in deep. I am also not looking for developers or network engineers, but a good pentester must find their way through all those topics, so good basics are an absolute must have. Most applicants have had some tech job before, so depending on their prior role, they might have to brush up on their network skills, or finally take a look at that OS they hate so much, or maybe take another shot at programming.

[PM]: Are there any character traits which make the job easier?

[FM]: Being resourceful and persistent is definitely way up the list. Pentesting is a lot about finding ways to use something in ways it was not intended to be used. So being resourceful, and coming up with solutions that require outside-the-box thinking, is absolutely helpful. Besides that, being persistent and not giving up on your target is something many have to learn first, on the other hand, being too persistent can work against you if you are on the clock, which you usually are when you're on an assignment. Outside of pentests, being able to lose yourself in research, or at least having fun digging through specs and standards for hours, will definitely help your career. In my opinion, being interested in how things work is the cornerstone of learning how to exploit things. In other words, there are no shortcuts to pentesting; Therefore, just have fun learning and develop a thirst for knowledge.

[PM]: How can someone gain experience in pentesting?

[FM]: Simple, by doing it. There are tons of applications out there that let you test and improve your skills, such as the OWASP DVWA (damn vulnerable webapp) or the Kioptrix and Metasploitable VMs. There are also websites that are hosting challenges, CTFs that players can participate in either remotely or on-site, which is usually held at some security conference. I also suggest visiting conferences, especially the BSides, which are held every year in multiple cities all over the globe and are usually free to attend. And then there is of course working as a pentester.

[`PM]: What are the skills candidates can gain in such a job?

[FM]: The technical skills highly depend on your work as a penetration tester, and can include things like exploit development, code analysis, vulnerability assessments, and the like. Beyond that, there are skills that apply to all those areas and include outside-the-box thinking, working towards a goal persistently, summarizing findings and writing detailed reports – which incidentally is one of the most important tasks of a penetration tester – and weighting the risk and impact of vulnerabilities.

[PM]: When you lead the interview on what do you pay attention the most?

[FM]: As I said, showing interest is definitely what is most important to me, especially when I'm interviewing rookies.

[PM]: When you look at the pentester's resume, what makes you call such a person?

[FM]: Projects and hobbies. I am more interested in how they spend their free time then what they have done in past jobs. If a candidate works on a security related project in their free time and their code is hosted on, say, Github, than that tells me far more than reading "Worked as $JOBROLE for $MONTHS" in the resume. That does not mean that I am only considering applicants with Github repositories though, I am just trying to learn more about the person, and past jobs usually do not say much about that.

[PM]: There is lack of professional pentesters for companies. How would you explain such a situation?

[FM]: I think the biggest problem that newcomers face is that they think they are not good enough yet to work as a pentester. The fastest way to gain experience and learn about pentesting is by doing it every day; especially if you have experienced colleagues who can teach you a thing or two. Anyone who is interested in pentesting, should apply for a job as soon as possible. Worst case, you do not get the job. Best case, you will learn on the job faster than ever before. Penetration testing is not a job that is taught the way software development or system administration are, and security companies are aware of that. So my recommendation for any aspiring pentesters out there would be; apply for a job as a junior, mention your interest in the field and whatever you have done so far and hope for the best.

[PM]: Please describe the best pentester you have ever met.

[FM]: I have had the pleasure of working with some great people and competing against very skilled pentesters in CTFs, and both have impressed me in one or the other way. There is more to being a good penetration tester than “getting in”, it includes writing good reports, being able to explain what the problem is and how to fix it among other things. One of my former colleagues, Maxi, was not only good at explaining vulnerabilities and their exploitation, but actually made writing reports fun, which is an impressive skill all in itself. There were some pentesters I met in conferences who found unique solutions to the CTF challenges that just wowed me and of course there are lots of speakers on those events with mind-blowing presentations. But I could not say who is best.

The PenTester’s Tale

by Tyler Wall

People ask me, “What do you do?” When I answer with, “I am a penetration tester,” I find that people generally just nod along and pretend they know what it is that I actually do. However, on the day where I am in the mood to razzle dazzle, I answer with “I am a hacker!” The reactions can vary between priceless disbelief and excitement. Every time I answer that I’m a hacker, I see the gleam of curiosity grow in their eyes. Then I get asked the million dollar question: “How did you become a hacker?”

When people find out that I am a “professional hacker” some assume that I just go around hacking everyone and everything. That I am “In the know” about every little secret. The media has portrayed hackers to be like the character “Mr. Robot”, drug users and misfits who live a secret hidden life filled with frills and excitement. While I find what I actually do incredibly interesting and fulfilling, for me the reality of a professional hacker is much like any office job I’ve ever had. If you were to stand behind my desk and watch what I do every day, I assure you that you would want to stab yourself in the eye with a fork. There is a lot of paper pushing, documents to write and meeting after meeting with what seems like every team in the company. The exciting parts, the actual hacking, can be a very tedious slow process. To manipulate something you have to understand it. Which means, research is your best weapon.

I say this to tell you that unless you want to live a miserable clock punching existence as a penetration tester, you have to live for the hack. Hacking needs to flow through your veins. If this is your cup of tea, then keep reading because I am about to explain to you what it took for me to get my “big break” demonstrating my hacking skills in front of an audience during an interview at a Fortune 100 company.

What about the education?

It was always taught to me that education was the way to go. That advice has not failed me. Your battle when breaking into this industry will be getting the first job. Do everything you can do to stack those odds in your favor. I went to college and worked for a Bachelors of Science in Computer Information Systems. Degrees are great to have because they never expire. You don’t have to get credits to keep your degree. What gave me my first infosec job was a degree and a Network+ certification. I was working as a computer technican when I received an offer for an entry level Security Operations Center job working as a Network Security Analyst.

During the time working as a Network Security Analyst, I met a few penetration testers and spoke with them. I knew then that I had to continue learning. I set up a home lab with hackables like Mutilidae and Metasploitable. I got involved with Capture the Flag (CTF) teams. I went to OWASP meetings. I hung around IRC and got to know more people in the industry. The greatest thing about this first job was that they would pay for my certifications. I took advantage of this like any self respecting hacker does with anything. They paid for my Security + and Certified Ethical Hacker (CEH). I can’t stress enough that you have to spend some of your time investing in yourself. You have to allocate some money (and time) to invest in yourself. If you’re investing wisely, the return on investment is unimaginable.

Tips:

- In Information Security, what is taken into consideration and highly valued is the extra-curricular activities that you might be involved with at the school.

- The cost of an Education is important. If you have to take out a loan, it's not free money. You have to pay this back. Try to choose a school that is in your budget. The jury is out whether the institutional name means a ton after you've already established yourself as a professional.

- While choosing the school, decide what kind of schedule you need. Are you the type that needs a lot of structure in a classroom setting? Do you prefer to work at your own pace, however faster or slower than your average student?

- Keep in contact with your professors. They can do a lot more for you than grade your paper.

- As stated above, try to get involved with clubs, societies, even fraternities/sororities. These people will be your peers for a long time. Branch out and get to know people. Joining these communities can even add flavor to your resume.

> ***Study hard and invest in yourself. Meet people, get involved and most importantly remember who you are.***

Getting your first job

Now I was equipped with a Bachelor's degree, a Network+, a Security+ and a CEH with about a year and a half worth of network security experience. I started applying for jobs and a few months later a Fortune 100 company responded. A hiring manager glanced through the available resumes looking for the right alphabet soup after someone's name. In just a short couple of years I had that right alphabet soup. That is what put me in front of the interviewers. This is only the first step. Remember how I mentioned before that I set up labs and competed in CTF's? Ultimately, this lab work, and the resulting skill that I was able to demonstrate, is what landed me the job. Half the battle is getting in front of the interviewers and the other half is having the skill to back it up. Both parts matter equally.

Not only did I need my foot in the door but I needed the ability. I don't pay certification bashers much attention because what certifications will absolutely do for you is give you an advantage. It is very possible that you can get a certification and not learn a thing. It is also very possible that you will be overlooked because you did not have the right credential. My personal experience has shown me that I had a very competitive advantage by having the right pedigree. What set me apart from the other candidates, however, was the skill that I was able to demonstrate. This skill was not obtained by any letters after my name. This skill was obtained because at one point in my life I was just a kid who liked to kick his teacher offline and I haven't forgotten that.

The most important advice I can give you: I don't think I would have landed any job I have ever had in Information Security if I didn't convince the hiring manager that I really enjoyed this. There are a lot of facets of this industry so try everything you can until you find your niche. Trust me, you'll know your niche when you find it. Find what you like and are good at and come and join us. We need you!

To sum up everything we asked Tyler a few questions about the most wanted pentesting skills:

[PM]: What skills should a person who wants to become a pentester have?

[TW]: I think the skills a person needs who wants to become a pentester would be a fundamental background in programming and/or networking. Part of being a pentester is editing/managing scripts. It will be invaluable to you to know how to use common scripting languages such as Python or Perl. An understanding of networking will also take you a long way. Know how protocols and packets function. Understanding the concepts of networking will help you maneuver and pivot from subnet to subnet, host to host.

[PM]: What skills can he gain working in a pentester position?

[TW]: Pentesting will push your limits. Not a day that goes by on an engagement that I have ever felt like there wasn't a library of things I didn't know how to do. You will always be presented with new technologies and new challenges that will require you to start from the beginning and research. Some of the best in the industry that I admire the most have always told me even they feel like a complete beginner. I think we all feel this way. The skills that you will gain on a pentest is as broad as the Library of Congress. Anything from people skills to hard technical ability. You will be challenged.

[PM]: Which of those skills helped you to become good at what you do?

[TW]: Curiosity. Absolutely, curiosity. I believe this is the basis of who a hacker is at his very core. Without my curious nature, I would never have had the motivation to keep this up.

[PM]: Which one pentesting skill do you value the most?

[TW]: Teamwork. I think working together is very important. Whether you're on a red team at an organization or you're a consultant working with the client. There is a lot of ground to cover in most engagements. You need to be able to pull resources and skill sets from team mates to complement one another.

[PM]: What kind of person was the best pentester you have ever met, who was the worst?

[TW]: The kind of person that was the best pentester I have ever met was someone that has incredible technical aptitude. He has an incredible amount of respect from the community. But this isn't what makes him the best pentester. The worst pentester I know has all this. What makes this guy great is that not only was he a technical genius, but he was available to help anyone that ever approached him. That is what makes him great. It's not anyone's sheer technical aptitude, but it's about what they're willing to contribute to others or the community as a whole. It's not enough to be great at being a pentester.

Interview with Shawar Khan

Shawar Khan

Independent Web Application Security Researcher. He started his career in Information security at an early age. He has been acknowledged by many top companies, including Google, Microsoft, Oracle, AOL, Amazon, Ebay, Adobe, Blackberry, and many others.

[PM]: Why did you decide to be an ethical hacker?

[SK]: There are two sides in the world of Hacking, The Black Hat Hacking and The White Hat Hacking; black hat is based on exploitation and damages while white hat (ethical hacking) is based on securing a system so no black hat can exploit it. Black hat is illegal and it's a crime if damage is done to a system, where as patching security holes is a legal way. Getting fame and bounties is much better than getting behind bars. That's why I chose this.

[PM]: What do you like the most in this job?

[SK]: The most important thing is the experience and knowledge I have gained during this work. Testing multiple web-applications and patching different web-application security holes will help us get more knowledge about how things work and how the security holes are made. Besides that, bounties are also a great thing. In this field, most companies give higher bounties which makes it increase our testing duration so we can focus more on the web-application we are performing penetration tests on.

[PM]: What skills should a person have who wants to become a pentester?

[SK]: Every penetration tester must have a lot of knowledge about the web-application flaws and about how the web-application works. In-depth knowledge is necessary if you are going to pentest a web-application. If the person does not have much knowledge, he will not be able to find flaws in the web-application. The person should know exploitation and detection techniques of different security flaws. Without that, the person will not be able to find anything in the vulnerable web-application.

[PM]: What skills can he gain working on a pentester position?

[SK]: As a Penetration Tester, the person who is doing this job will get much experience while doing this work. This experience is gained while testing different web-applications. In every web-app, there are different scenarios and each time the security flaw is in a different condition and its exploitation and testing is different every time. By solving this type of problem in penetration testing, the person will learn the new techniques to test a web application in different conditions and scenarios. By testing web applications, the person will get information about the online security and the mechanisms that protect the client-side as well as server side areas. Knowledge and experience is gained in this job which is a very important thing in the world of computers.

[PM]: Which of those skills helped you to become good at what you do?

[SK]: There are many web application flaws now a days and I have mastered some of the most high risk flaws which are common in web application now a days. Mastering the exploitation and testing techniques of these security flaws allows me to find and detect them whenever there is a possibility. It helped me detect and find these flaws in modern web applications. These skills are also gained by testing multiple web applications and practice.

[PM]: Which one pentestng skill do you value the most?

[SK]: If I am asked about the skill I need to choose then I'll choose the skill I have mastered, the Cross-Site Scripting (XSS). I have bypassed many web application firewalls and protection mechanisms and have XSSed the world's top sites, including Google, Microsoft, Ebay, Amazon, Dell, Intel and some other sites. I am able to bypass 98% of the firewalls and protections and have learned different techniques of exploitation and bypasses so this is the skill I am good at. So if I am asked about the skills to be chosen, I'll select XSS.

[PM]: There is a lack of professional pentesters for the companies. How would you explain such situation?

[SK]: According to my personal experience, what I have observed is that most of the companies, including top companies of the world, don't take their web application security seriously. They don't understand the risk of security holes until they are exploited by a Black Hat Hacker and damage is done to their server. Companies should hire security researchers and penetration testers like us so we can protect their web application from different web application flaws and after performing a full pentest over the web-app, the company will be safe from sensitive data leakage. If the security flaws are not patched in time, they can be exploited, which can cause data leakage, such as credit card information leakage or any other sensitive information. So the companies should hire pentesters before the security holes are exploited and they should understand the risk.

[PM]: What kind of person was the best pentester you have ever met, who was the worst?

[SK]: I have met many penetration testers, some of them are very skilled whereas some of them use Scanners to pentest the Web Application. Most people are doing manual testing, which is the best method of pentesting whereas some people are using automated-scanners which automatically find bugs in sites. This is the worst thing to do as a pentester and should be avoided. Scanners cause the web application to get under large traffic sent by the scanner and they are based on an algorithm which is not always the same in all web applications. Manual testing is based on logic and concept by which we are able to bypass and detect any bugs in the web app, no matter if the scenario is different or not. I have met some researchers who share their knowledge with other researchers, which is a great thing, but I have also seen researchers who hide things and don't want to share their experience. This is the worst pentester type. Every pentester should share experience and knowledge so other people can learn new things and methodologies.

How to get the job and what to expect

by Recreational Viking (@RecViking)

It doesn't matter whether you are changing careers entirely or just looking to make a jump to the next level of your current path, having realistic expectations is the only way you will prevent yourself from a big let down or wasting your time. Penetration testing is one of the coveted positions within the security community and it is often very difficult to break into. It is also forced to be heavily guarded due to the raw number of completely unqualified applications ,interviewers are often forced to sift through. Salary requirements, experience, interpersonal skills and technical skills all play into your likelihood of landing a penetration testing job. The interview process for highly specialized jobs like this can be demanding both mentally and from a time perspective. However, from my point of view, it is worth it.

Salary is often a big sticking point and it warrants a discussion first to clear the air. Penetration testing jobs can be very lucrative, as they require both skills and experience, and the people who work in this field are often rewarded for the combination. If you don't have both skills and experience, your salary and ranking will reflect this if you are offered a job.

From what I've seen, it is absolutely necessary to define experience in terms of what counts as experience and what does not when talking about penetration testing. Experience in penetration testing is hands on keyboard doing actual penetration testing work. When looking for higher level (and higher paying) penetration testing jobs, experience is key. The experience that reflects this kind of work includes:

- Web application testing - by hand, not using vulnerability scanners or static analysis tools
- Application testing - by hand, not using vulnerability scanners or automated sandboxing environments
- Network service testing - by hand, not using vulnerability scanners
- Communications hardware testing - by hand, not using vulnerability scanners
- {insert type of testing here} - by hand, not using vulnerability scanners

Are you beginning to see the pattern? Using vulnerability scanners, source code scanners, and other automated tools does not count as penetration testing experience. Are these tools often utilized by experienced penetration testers? Absolutely, but they are only utilized to catch the low hanging fruit. The value of an experienced penetration tester comes from their ability to discover and *EXPLOIT* vulnerabilities beyond what automated tools can discover. A few years doing actual penetration testing goes a long way.

Your interpersonal skills also come into play when trying to land a penetration testing job. To pick up a job on a team with me, you must be humble, enthusiastic about the work, and be willing to ask for help. In the interview, arrogance will get you sent right back out the door with the same level of employment (or unemployment) you started with. Most penetration testing is done in small teams and if you are not able to work well with the folks around you, you will fail.

Gauging enthusiasm for penetration testing is often done through asking a candidate about their extracurricular activities related to penetration testing, such as education, independent research, publications, and conference participation. Showcasing your development work on github, running a blog, or even talking about your home lab are also good ways of showing you have enthusiasm about your work.

The most desired technical skills of a penetration tester are always up for discussion, due to the number of technologies that may need testing.

Being humble and having a willingness to ask for help go hand in hand. It is OK to admit defeat (within reason), and ask for help. Nobody is expected to know everything and rather than talking out of your backside when answering questions, simply say “I don’t know” or “I’m not sure on this one, but I’d imagine it is like…”. This shows you know your limitations. Knowing what you know is good, knowing what you don’t know is even better, because it helps to prevent errors and oversights.

The most desired technical skills of a penetration tester are always up for discussion, due to the number of technologies that may need testing. There are many different types of penetration testing and due to the wildly varying types of systems being tested, the skills required for individual positions will have significant variation as well. The thing I'm most interested in seeing on a resume is a varied background, even if it appears to include a hefty amount of job hopping. This shows that the candidate has been exposed to a broad variety of technologies and is not likely to get scared or slam on the brakes when presented with a new technology or unfamiliar system. In addition to a variety of exposure, programming experience is an absolute necessity. If you claim to be a penetration tester and you are not programming or scripting, you are doing it wrong. Do you have to be a kernel hacker as well as be capable of converting hex to instructions in your head? No, but only being capable of writing a "hello world" application in Python won't cut it either. If you are looking for a more web application-centric career, the more you know about the underlying back end technologies and front end scripting, the more useful you are. If you are looking for just about any other type of penetration testing position, just being proficient in a higher level scripting language or two is usually sufficient. When penetration testing is done right, every discovered vulnerability is exploited to its fullest and every new vantage point is recursively inspected for additional vulnerabilities and then exploited. Knowing only web technologies while doing web application testing will not take you to root very easily. On the other hand, nearly every network device and service comes with a fancy new web interface, so only having system level knowledge often won't give you the necessary foothold to even begin evaluating a system. Broad, varied knowledge and skills in using a number of technologies are necessary for effective penetration testing.

> *The thing I'm most interested in seeing on a resume is a varied background, even if it appears to include a hefty amount of job hopping.*

The interview process itself is going to be different at every place you apply. In most cases, you'll have some kind of HR/pre-screening interview to make sure your background meets requirements. There will be a technical Q&A "stump the chump" session, possibly multiple sessions, or even a panel interview. In addition to this, it is common for more technical positions to include some form of hands-on work and possibly even a 'homework' aspect. My interviews include a small capture the flag challenge where we stare over your keyboard while asking you questions about why you are doing everything you do. This helps us figure out your thought process when examining a new system. Some employers also incorporate a social session at lunch/dinner where the candidate may not even know they are being evaluated on how they interact with others on the team. This is something I also do during my interviews and it has both made and destroyed certain candidates' chances with my team.

During the interview, neither the candidates themselves nor interviewers should expect a candidate to know all of the answers. As a candidate, if you think you do know all of the answers, you are likely getting a number of questions wrong or you probably won't work for that employer unless you like the big fish -> little pond scenario. I have my interviews designed purposely to test the limits of all candidates. The "stump the chump" sessions are done with the most senior team member in each of these categories: web app, network, Windows, Linux/Unix, and development. These sessions are intended to find your limits and we'll continue asking questions until you fail. Again, nobody is expected to know everything and this type of interview is simply designed to see how well your skillset will augment the team and at what level you'll be placed.

Some of the above may seem harsh, but it is what is necessary to acquire talent for a high-performance team. The interview process will not be fun for most people, but if you make it through, the job is very rewarding and it will always challenge you. Remember to set your expectations realistically. If you don't have years of experience in penetration testing, be ready to accept an entry level position and entry level compensation package. If your skills and experience in other related areas are good, they will push you along faster than someone fresh out of school and you'll be able to reach a more senior position in short order. Always be open to learning new technologies (no matter how ridiculous 'the cloud' or 'big data' sounds), you never know when your organization will adopt them. Good luck in landing your penetration testing job.

Preparation tips

1. Know your tools. You don't need to be a human man page for every tool, but if asked about a tool, you should know that a switch exists for something even if you don't remember the exact word/letter or format.
2. Know the common methodologies. Study up on what is given by the penetration testing execution standard. Take a look at what Offensive Security has out there.
3. Be able to talk about recent vulnerabilities discovered. Ensure you can explain how these vulnerabilities are exploited on a technical level, familiarity alone will not get you there.
4. Don't put anything on your resume you cannot speak about in depth. Most interviewers are interviewing you based on both their requirements and what you've got in your resume.
5. Some certifications are useful, others are not. Don't put less respected certifications at the top of your resume. I won't bash any particular certification publicly, but if you know penetration testing, you know what is embarrassing and what is not.

About the Author: Recreational Viking (@RecViking)

I've worked in state government, federal government, the education sector, as an instructor, and in the financial industry. I have 10 years of experience in security with three of those years focused on penetration testing and reverse engineering. I currently work as a penetration tester in the financial industry. I enjoy running CTF contests at conferences. I do Viking things.

Main Pentesting Skills

by Roberto Oscar Sanchez

When recruiting a team of pentesters, there are certain basic skills that are considered necessary to be part of a high performance, aligned and motivated team.

To begin with, there are two large skill groups, the two being present either in the same person or spread over more than one member.

Soft skills

These are the skills necessary for good communication with the customer, prior to any activities, to the regulation of expectations for the task and the delimitation of the scope process. These skills should include the legal context of the country where you are performing the task. The member of the team who has this ability more present is usually the leader, both because of interactions with the client and the technical team, facing new project findings or unexpected conditions.

Empathy

The ability to understand and comprehend ideas and emotions of others, having the ability to put oneself in the other's place.

Negotiation

The effort to interact between two or more people with the intent to make a profit for those involved; this ability greatly facilitates both the start of the project and the presentation of results.

Continuous learning

Having continuous learning increases the technical capacity of a pentester. It is better for one to have a large group of previously acquired tools to consider when it's necessary to build something because of a new added condition on a future project.

Up-to-date Information

We must have a willingness to be informed through different channels; feeds, emails, social media. One needs to be aware of news, incidents, vulnerabilities, zerodays, etc.

Hard Skills

The technical world is vital to the team's success. Without a solid education on it, one cannot move forward with the project results at reasonable levels. Whereas the obsolescence of knowledge in technology may be one year or even months, these needs become increasingly critical. There are a lot of them, but here are details for some of the basic ones.

Networking

A strong background in networking is a pretty good base for firewall tasks, and other perimeter evasion techniques. Building packages in different protocols is a very useful skill in different scenarios.

Programming

If programming experience exists, there is a great advantage in different projects, not only for binary analysis, but for capacity building some software components necessary for the attack during the project and on a whim.

Web applications

One must have strong knowledge in web applications, because usually, one of the first attack surfaces are web applications or web services. This skill is closely tied to programming, it is recommended that one dedicates a year to work in web application development before turning to perform safety checks in web environments.

Cryptography

Knowledge of algorithms, symmetric and asymmetric systems, and different forms of cryptanalysis are of great value against theft cookies, browser hijacking, attacks on wireless networks, and other cases. Having prior knowledge of algorithms can greatly facilitate the task of even preliminary recognition.

Linux

Most hacking tools are developed in open-source environments, and because of that, the pentester should feel very comfortable working on different Linux distributions, even if the TOE is on another operating system.

Windows

Windows is the most widely used system in production systems online, and it is necessary to have good knowledge of its architecture, processes, libraries, and internal dependencies.

Vulnerabilities

The concepts of scanning and exploitation should be kept in mind, as well as being informed about new appearances to date of different tools and suites, free or licensed. You must be able to handle a wide spectrum of tools for scanning and attack.

Mobile

If the project is geared more towards the mobile world, it is vital to have a good grounding on the mobile infrastructure (Android, iOS, Windows). There are situations where this skill is vital, and there are others where the scope determines that it is not necessary. Perhaps a malicious app can be the first point of attack, and in this case, programming skills need to be combined.

Social

This quality could also fall into the soft skill spectrum, but social skills determine the success of a project. Phone calls, costumes and approaching key people in an organization can be very valuable attack points at certain scenarios

Conclusions

Those include some of the large group of skills that are handled in a strike team, of course there are loads more, according to each reader's experience. For example, IoT (Internet of Things) has been omitted, and so has the industrial environment systems' mixed control production. Not to mention the medical environment, and many other markets with very frequent vulnerabilities.

About the author: Roberto Oscar Sanchez

Buenos Aires-Argentina
Twitter: @rsanchez3270
Linkedin: ar.linkedin.com/in/rsanchez3270

The PenTester Interview

by Eric Schultz

Let's be honest. Cyber Security is a hot field right now. Cisco currently puts the number of global open cyber security positions at one million. You can get a job as long as you've got a related college degree, a basic security certification, flexibility to move, and basic hygiene. Still, maybe you need a little help. Getting into any industry can be challenging if you don't have the skills on paper and pentesting can be especially tough as the interviews can cover a large range of topics. The more you know about interviews, the better your chances of getting the job. To help you out, here's an inside look from my experience on both ends of the interview process.

Getting the Initial Interview

The biggest door opener is a security certification (CEH, Security+, CISSP, OSCP, etc.). To understand why, you need to understand how Human Resources (HR) at most large companies work. When a technical spot opens up, the manager of that position (the "hiring manager") puts together a list of qualifications and phone screen questions and sends it to HR who then distributes that list to recruiters. The main problem is that HR and the recruiter are not highly technical. To them, a Security Analyst is the same as a Security Engineer, Penetration Tester and a Vulnerability Analyst. To be fair, it's not their fault. The only guidance they have are the materials the hiring manager has provided.

Certifications are important because they are something HR and recruiters can understand. Recruiters find applicants by comparing keywords in resumes to keywords on the job description. They may not know the difference between CISSP, OSCP and CCNA, but if the hiring manager provides a sheet of paper that says 'candidate should have the XYZ certification,' you can bet they're going to focus on resumes that have the XYZ certification. The scary part is that HR are the gate keepers to getting a job, and if they don't select your resume, you can't get the job.

If the keywords align, and HR selects you for a phone screen, the recruiter will throw a few softball questions your way. As they're not technical people, they don't always understand the answers. If they do ask technical questions, they try to ask close ended questions to keep it easy on the recruiter. If what you say is confident and remotely close, they'll give you a pass.

The Technical Interview

The interview process can differ by location (on site, phone, Skype, etc.), but you'll be speaking to someone technical. It can be the hiring manager, a senior security analyst, or a team lead.

They'll start off with some more softball questions and progress into more complicated ones. There are exceptions, but generally, here's what the technical interviewer is looking for in order of priority:

- Honesty
- Team Chemistry
- Technical Knowledge
- Passion

Technical Interview: Honesty

Good technical interviews are designed to explore your knowledge in depth. You will come across questions you don't know. No one knows everything. Be honest about it. You may think your social engineering skills are top notch, but hopefully, you're talking with another expert, so any BS will be noted.

Technical Interview: Team Chemistry

Upper management is tough to understand. It takes up a lot of a technical manager's time trying to understand the corporate world and how it relates to the team. The last thing a manager wants is to baby sit and hold hands because of some internal nerd fight.

Everyone doesn't have the same background and knowledge, so internal communication should be natural. Weird issues come up during pentests (Why does this Windows server have an SSH server? Why is my payload not working?) and teammates may have experienced the same thing in previous tests. Good communication can resolve these issues as soon as possible.

Technical Interview: Technical Knowledge

Pentesters don't have experience with every tool and environment. Sometimes clients need a pentester specifically for those environments. If the team feels that you're a good fit for the team, and you don't have the exact technical background, the team may hire you anyway. You can always be trained.

Other times, clients may be on a deadline and need to bring on a pentester in a hurry. Nothing brings change faster than the eye of a CEO, industry regulators, and the national media. When big companies get cracked open by malicious hackers, or an auditing agency coughs up a bunch of findings, getting a pentester into those environments becomes a strong priority. If you've got those skills, you'll be in the door before you know it.

Technical Interview: Passion

The security industry is constantly evolving. It can be hard to stay on top of everything. In the last three or four years, there's been Shellshock, Logjam, Heartbleed, BEAST, FREAK, and countless other vulnerabilities. There's Apache, NGINX, Oracle, Windows Server, MySQL, MSSQL, SSH, FireFox, Edge, and thousands of others in any given large corporations. Each of those has their own versions and vulnerabilities. In addition to those, you've got new technologies like distributed web application firewalls, HTML5, IPv6, VoIP, Cloud Storage, NoSQL, Data Warehouses, and many more. There's also internal corporate policies, security standards (NIST 800-53, PCI compliance, HIPAA) and risk scoring (CVSS). We haven't even mentioned new programming languages like Golang and the constant flood of new security tools and frameworks.

That's a lot to know. Unless you work in a very fast paced and large environment, you're not going to keep up with the world from your 9-5 job. It takes a passionate individual to keep up. Hiring managers know this and love to have a team member that learns this knowledge and can pass it on to the rest of the team. Showing that you learn on your own time also means that you can hit the ground running soon after you start.

How do you show passion? When you get a question you don't know, ask for the answer. Have a home lab that you work with. Start a blog, do independent research, or write for a magazine (hint, hint). Talk about those hobbies during the interview!

Miscellaneous Info

- The technical interviewer will generally have a very limited time reading your actual resume. Fifteen minutes is usually the average.
- Anything you mention on your resume is fair game for the interviewers to ask.
- If you miss a question in an earlier interview, look it up! Some interviewers will double check in later interviews to see if you learned the answer.
- If you show up in street clothes, you'd better be a rock star, or have a good excuse.
- If the interviewer makes a mistake, don't be afraid to correct them on it. Just don't be a jerk.
- Never give your current salary to the recruiter. Ask for the position's rate or salary instead.
- Never stay too long at your first job unless you receive a large pay increase or initial offer. If you get hired in at $50k, you'll only get a 2% to 10% raise per year ($52k to $60k after two years). After one or two years of experience, you can get a job at another company for $70k to $80k.