

HAKING

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

VOL.17, NO.10

OPEN

LET'S TALK ABOUT CYBERSECURITY CERTIFICATES

'FOR ANY CERTIFICATION YOU SHOULD HAVE A COMBINATION OF WORKING KNOWLEDGE AND PREPARATION TO PASS THE EXAM.'

- PAUL JANES

'HOLDING A CERTIFICATE DOES NOT IMPLY REAL HANDS-ON KNOWLEDGE, BUT IT TAKES TIME AND EFFORT TO PASS THE EXAM AND IN SOME CASES LEARNING NEW SKILLS.'

- CHRISSA CONSTANTINE

'TIME MANAGEMENT IS THE MOST CHALLENGING PART OF PREPARING FOR SUCH CERTIFICATES. IT'S CRUCIAL TO DEDICATE YOUR TIME TO LEARNING.'

- GORAN UDOVICIC

AND MORE...

HAKIN9

TEAM

EDITOR-IN-CHIEF:

Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

CEO:

Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

MANAGING EDITOR:

Agata Staszelis
agata.staszelis@hakin9.org

MARKETING DIRECTOR:

Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

EDITORS:

Bartek Adach
bartek.adach@pentestmag.com

Ewa Dudzic
ewa.dudzic@eforensicsmag.com

Bruno Zwierz
bruno.zwierz@pentestmag.com

DTP:

Agata Staszelis
agata.staszelis@hakin9.org

COVER DESIGN:

Hiep Nguyen Duc
Joanna Kretowicz

PROOFREADER:

Lee McKenzie

SENIOR CONSULTANT/PUBLISHER:

Paweł Marciniak

PUBLISHER:

Hakin9 Media Sp. z o.o.
02-676 Warszawa
ul. Bielawska 6/19
1 917 338 3631
www.hakin9.org

All trademarks, trade names, or logos mentioned or used are the property of their respective owners. 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.

HAKIN9

Dear Readers,

In this open issue of Hakin9 Magazine, we created something special for you! We really wanted to bring you closer to the topic of cybersecurity certificates because we know that many of you have a hard decision to make - which certificate to choose. In this H9 edition, we brought to you 10 cybersecurity professionals: from people with over 20 years of experience to some who started their journey not so long ago. All of them share their cyber-certificates know-how and tell you how long it takes to prepare for each certification, which are more advisable, what is most important in the process of learning, and many more!

Since we know how crucial this topic is, we decided to make it an open issue!

Enjoy this issue's content and stay safe,

Agata Staszelis and Hakin9 Editorial Team

TABLE OF CONTENTS

4	<i>GAURANG BHATNAGAR</i>
9	<i>CHRISSA CONSTANTINE</i>
12	<i>PAUL JANES</i>
16	<i>GORAN UDOVICIC</i>
21	<i>FELIPE MARTINS</i>
25	<i>CEZARY KUBICKI</i>
29	<i>SAMY MABROUK</i>
35	<i>PIOTR DĘBSKI</i>
39	<i>SARTHAK THAKUR</i>
42	<i>CHAITANYA Y</i>

GAURANG BHATNAGAR



GAURANG HAS A STRONG PASSION FOR SECURITY RESEARCH, TOOL AUTOMATION AND ANDROID EXPLOIT DEVELOPMENT. HE'S CURRENTLY RUNNING PENETRATION TESTING AND RED TEAMING ACTIVITIES, AS PART OF HIS JOB.

[Hakin9 Magazine]: Hello! Thank you so much for agreeing to the interview! Please, tell us something about yourself.

[Gaurang Bhatnagar]: I'm currently working in a product-based company, where I'm working on managing their bug bounty program and performing pentest/red team activities. I'm a postgraduate in cybersecurity and have more than 6 years of experience working in the cyber industry.

[H9]: To begin with, what cybersecurity certificates did you obtain?

[GB]: Till now I have obtained OSCP, eJPT, eWPT, eWPTX, eMAPT and eCPPT.

[H9]: Why did you decide to pursue those certificates?

[GB]: I started to pursue certifications in 2015. CEH (certified ethical hacker) was the only known certification then. But, I wanted to work on certificates that provide me with practical knowledge. In 2015, I stumbled upon eJPT certification by elearnsecurity. However, I was concerned about this certification since I had never heard from anyone about it. Also, I could not see many reviews about this certification in the public space during that time. From their website and looking at the course content, I noticed that this is an entry-level certification and provides you with hands-on pentest experience, so I decided to enroll in it. And I have to say this was one of the best decisions I had made about any online certification. The course material and labs were so comprehensive and beginner-friendly that they cleared all my doubts and provided me with practical knowledge. This certification boosted my knowledge and helped me crack many interviews as a fresher. I further pursued eWPT, eMAPT and eCPPT certifications in the coming years. These certifications created my strong base in offensive security. I pursued OSCP in 2019 because of its higher market value and challenging exam. I would say clearing eCPPT created my strong foothold in the network pentest, and it was easy for me to pass the OSCP exam.

[H9]: From all of them, which one do you value the most?

[GB]: I value all of them. If you ask me about the market value, definitely offensive security certifications win here. But, if you ask me about the course content, labs and exam, I would rate elearnsecurity (now INE) certifications higher.

The passing rate for offensive security certifications is less than elearnsecurity certifications, mainly due to the time limitations and proctored exams.

Unlike offensive security certifications, elearnsecurity exams aren't proctored and give students 7 days to complete the exam (whereas it is 24-48hrs for offensive security certs).

Offensive security exams are more like capture the flag where you need to compromise a certain number of machines and obtain a certain level of score to pass the exam.

The elearnsecurity exams are based on a real pentest scenario. It simulates a real pentest environment where you have to achieve the goal of the pentest as defined in the scope of work and make a pentest report.

This is a plus for learners because this is how an actual pentest engagement works.

[H9]: From the current perspective, which one was the most difficult to achieve?

[GB]: Among all the certifications I did, eWPTX was the most difficult one. Although having 6 years of web pentest experience, I still found this exam very challenging. I managed to complete this exam in 6 days out of the provided 7 days. But I have to say that those 6 days really had me struggling and gave me many burnouts. The exam was all about bypassing web filters and evading firewalls.

[H9]: Which one do you consider the most useful?

[GB]: All the certifications I did have turned out to be really useful. eWPT and eWPTX have created my strong foundation in web application security. eMAPT has provided me with the mobile pentest skills. Certifications like eJPT, eCPPT and OSCP have equipped me with solid network pentest and exploitation skills and boosted my confidence.

[H9]: In what situations did the certificates prove most useful? How did they influence your career? Did anyone ever require any of them?

[GB]: Certifications have helped me provide practical skills and boost my confidence. The skills obtained helped me in clearing many interviews. I have to highlight that nobody is going to inquire about your certifications. Certifications can often create chances for your resume to be shortlisted. I have given several interviews during my cyber security career, and most interviewers are only keen to assess your skills.

[H9]: We're curious what your position on the 'certificates vs. skills' debate is. Do certifications always imply real knowledge and competences?

[GB]: Enrolling for certification is optional. What matters are the skills you achieve. Certifications can help in boosting up your confidence. I have also seen many people spin up the local environment and practice things on their own by reading articles and research papers on the internet and then practicing all they have learned in the created environment. This is yet another way to boost your skills. It is up to the people what path they wish to follow. In the end, what matters are the skills obtained.

[H9]: How long does it take to prepare to take an exam for such certificates?

[GB]: Most of these certifications are self-paced. It depends on the individual at what pace they will cover the course. On average, it took me about 8-12 months to complete the course content and labs (per certification) as I was already working full time.

[H9]: What is the most challenging part of preparing for such certificates from your point of view?

[GB]: The most challenging part is staying focused and ensuring that you follow the course content and practice labs regularly.

[H9]: Are there any certificates that you now consider a waste of time?

[GB]: I don't see any certification as a waste of time. Each one gives you something to learn and boosts your confidence.

[H9]: Let's now assume that our reader is at the beginning of his security path. What steps does he have to follow to prepare for and pass the exam for such certificates? Do you have any advice? What 'certificate roadmap' would you suggest?

[GB]: If you're a beginner, I would highly advise you to get an INE subscription and do the eJPT certification. That's not very expensive and is a perfect beginner-level certification. eJPT was my first stepping stone when I entered cyber security. Moving on, you need to decide which area you want to focus on (network, web, mobile, others?).

If you want to focus on network pentest, I would recommend the following path:

eCPPT > OSCP > eCPTX > CRT0 (Rastalabs)

Active Directory is a crucial topic when dealing with Windows operating systems during your pentest.

To improve your active directory pentest skills, you can consider the following certifications from the pentester academy:

CRTP > CRTE

You can even add this to your workflow of certifications:

eCPPT > OSCP > CRTP > CRTE > eCPTX > CRT0 (Rastalabs)

If you want to focus on web application security, you can approach the following path:

eWPT > portswigger web academy labs > eWPTX

If you want to focus on mobile security, first get familiar with basic android development. After that, you can consider any of the following courses/certifications:

eMAPT or Android and iOS app exploitation course by Attify

Important note:

Whatever you learn, remember to make notes (use github, gitbook, evernote, onenote etc.)

Also, while doing the labs, focus on automation :)

CHRISSA CONSTANTINE



**CHRISSA IS A CYBERSECURITY
PROFESSIONAL WITH A STRONG
BACKGROUND IN RESEARCH
AND WRITING, CYBERSECURITY,
VULNERABILITY ASSESSMENT,
WEB APPLICATION TESTING,
AND SECURITY TRAINING.**

[Hakin9 Magazine]: Hello! Thank you so much for agreeing to the interview! Please, tell us something about yourself.

[Chrissa Constantine]: I am a cybersecurity professional with a strong background in web application and API testing, security training, vulnerability assessment, security engineering, compliance and auditing.

[H9]: To begin with, what cybersecurity certificates did you obtain?

[CC]: International Information System Security Certification Consortium (ISC)² , Certified Information Systems Security Professional (CISSP), SANS GIAC Web Application Penetration Tester (GWAPT), EC-Council Certified Ethical Hacker (C|EH).

[H9]: Why did you decide to pursue those certificates?

[CC]: I was told that I needed CISSP for a job. I was offered C|EH training from an employer and took it. I was offered SANS training from an employer and took it.

[H9]: From all of them, which one do you value the most?

[CC]: I value CISSP and GIAC GWAPT the most due to obtaining job offers that require certifications as part of the requirements.

[H9]: From the current perspective, which one was the most difficult to achieve?

[CC]: They all were challenging to obtain for various reasons. I obtained CISSP when I had no prior work experience in cybersecurity. I obtained the C|EH not long after getting CISSP. The SANS training was fantastic, and was a challenging exam.

[H9]: Which one do you consider the most useful?

[CC]: I consider the CISSP and GIAC GWAPT the most useful.

[H9]: In what situations did the certificates prove most useful? How did they influence your career? Did anyone ever require any of them?

[CC]: The certifications were required for several jobs I have obtained.

[H9]: We're curious what your position on the 'certificates vs. skills' debate is. Do certifications always imply real knowledge and competences?

[CC]: Holding a certificate does not imply real hands-on knowledge, but it takes time and effort to pass the exam and in some cases learning new skills. I studied extensively and leveled up my skills in an attempt to pass each

certification exam. For individuals who want to break into the field, an opportunity to take an exam and get a certification can be a valuable experience.

[H9]: How long does it take to prepare to take an exam for such certificates?

[CC]: 3 months of preparation and study is usually how long it takes me to pass a new exam

[H9]: What is the most challenging part of preparing for such certificates from your point of view?

[CC]: It is challenging to fit in study time when working full time. It can be challenging to study a topic you may not have hands-on experience in.

[H9]: Are there any certificates that you now consider a waste of time?

[CC]: No. Each certificate has had value in terms of study and learning new things.

[H9]: Let's now assume that our reader is at the beginning of his security path. What steps does he have to follow to prepare for and pass the exam for such certificates? Do you have any advice? What 'certificate roadmap' would you suggest?

[CC]: I would consider what area of cybersecurity I wanted to enhance my skill set and pick a certification that meets that requirement. For example, if I wanted to work as a penetration tester, I would choose a certification such as OSCP or GIAC GWAPT. Another option would be to review job requirements to determine the certifications for a specific role.

Looking at a security certification roadmap can help, such as

<https://pauljerimy.com/security-certification-roadmap/>

After deciding which certification to take, I would consider how long I need to study and what study materials work best for me, such as an online course, practice exams, reading a book on the topic, or taking online labs for practice.

The National Initiative for Cybersecurity Careers and Studies (NICCS) Workforce Framework for Cybersecurity (NICE Framework) is a resource for anyone who seeks to learn more about cybersecurity and opportunities in the field. The framework can help understand categories of standard cybersecurity functions, specialty areas, and roles that show specific knowledge, skills, and abilities, identifying what certifications would be helpful. Here's the link: <https://niccs.cisa.gov/workforce-development/nice-framework>

PAUL JANES



**PAUL IS A CYBERSECURITY PROFESSIONAL
WITH OVER 20 YEARS OF EXPERIENCE
INCLUDING ZERO TRUST ARCHITECTURE,
NETWORK SECURITY, CLOUD SECURITY,
DATA PROTECTION, COMPLIANCE,
CYBER RISK, AND VULNERABILITY
MANAGEMENT.**

[Hakin9 Magazine]: Hello! Thank you so much for agreeing to the interview! Please, tell us something about yourself.

[Paul Janes]: My name is Paul Janes and I have over 20 years of experience working in the cybersecurity field. I have worked in manufacturing, healthcare, financial services, and consulting. My current passion is helping companies/organizations with zero trust readiness and architecture.

[H9]: To begin with, what cybersecurity certificates did you obtain?

[PJ]: CISSP, GISP, Zscaler ZIA cloud admin, Zscaler ZIA cloud admin – security specialist, and Zscaler ZPA cloud admin.

[H9]: Why did you decide to pursue those certificates?

[PJ]: I think the CISSP is a no-brainer and is pretty much a requirement for any cybersecurity professional. Many jobs that are available today in management will not consider someone without the CISSP. As for Zscaler, these came about from an SSE implementation at one of my previous employers.

[H9]: From all of them, which one do you value the most?

[PJ]: CISSP is of the most value as it has opened many doors for me from a career perspective.

[H9]: From the current perspective, which one was the most difficult to achieve?

[PJ]: CISSP was definitely the most difficult as it requires knowledge in multiple domains where you need to understand the topics an inch thick and 3 miles long...

[H9]: Which one do you consider the most useful?

[PJ]: CISSP is still the most useful as far as getting a job in the field. As for hands-on working knowledge, I think the Zscaler ones tend to benefit the security engineer today. Not that SSE = zero trust, but a number of the components of the architecture are included. In 2021, President Biden created Executive order 14028 where all federal government entities must move to a zero trust architecture by the end of 2024, making a lot of activity happen with the help of CISA, OMB, and other government agencies. Keeping the cyber community busy...

[H9]: In what situations did the certificates prove most useful? How did they influence your career? Did anyone ever require any of them?

[PJ]: For each of my positions that I have had over the last 10 years, the CISSP was a minimum requirement. It influenced my career by showing all the different aspects of cyber security and allowing me to take and adjust my career path with confidence.

[H9]: We're curious what your position on the 'certificates vs. skills' debate is. Do certifications always imply real knowledge and competences?

[PJ]: The debate is answered as follows: If I were in a situation where I was fighting an attack, I would much rather work with someone who has five years working experience and no certifications vs. someone who has three certifications and one year of experience. Working knowledge combined with the ability to identify, respond, and resolve an issue is where it is at.

Looking at a number of the cloud certifications today where they ask questions and you have to come up with solutions as an answer speaks a lot about the value and the knowledge required. I am more comfortable accepting these certificates as knowledge. Examples: AWS Architect, AWS Security Specialist...

Some certifications are simply study content, walk in and pass the test. These do not show skill but point to the fact that someone can memorize information in a text and use that information to pass an exam.

[H9]: How long does it take to prepare to take an exam for such certificates?

[PJ]: It depends on the certification. For the Cloud exams, I would recommend a year of hands on then a month of preparation. Can it be done sooner? Sure, it depends on how much someone understands the certification requirements.

[H9]: What is the most challenging part of preparing for such certificates from your point of view?

[PJ]: For me it is getting over the fact that you don't know everything and have to take the time out of your day to prepare as opposed to walking in cold and just being able to pass the exam. Preparation is required for any of these exams...

[H9]: Are there any certificates that you now consider a waste of time?

[PJ]: I wouldn't call out any certification as a waste of time. I think it all depends on the individual's career path and what they want to do.

[H9]: Let's now assume that our reader is at the beginning of his security path. What steps does he have to follow to prepare for and pass the exam for such a certificate/s? Do you have any advice? What 'certificate roadmap' would you suggest?

[PJ]: I actually get this question a lot, believe it or not. I would say everyone has a different path so it would depend on the path they have opted to take. I would say that for any certification you should have a combination of working knowledge and preparation to pass the exam.

My advice is to get started with a role such as a SOC analyst where you get to see all the activity going on in the network and be able to take that information in order to identify issues vs. false positives. Then, after two or three years, start looking at certifications that have to do with incident response. Once you have that knowledge down, I think you can choose where you want to go in your career and then work on the things that matter most for your path. CISSP is a requirement so get that out of the way once you hit the five year mark. Any other certifications in the cloud would be beneficial. AWS/Azure/GCP exams are all beneficial.

GORAN UDOVICIC



**GORAN IS A SENIOR SECURITY ANALYST
WORKING IN A CYBERSECURITY AREA FOR
OVER A DECADE. LATELY, HE HAS BEEN
WORKING ON INFORMATION SECURITY
AND PRIVACY IN THE CLOUD.**

[Hakin9 Magazine]: Hello! Thank you so much for agreeing to the interview! Please, tell us something about yourself.

[Goran Udovicic]: My name is Goran Udovicic, and I have been working in the security field for almost a decade. Throughout my career, I have acquired knowledge from different security domains. I have started with identity and access management, continued my career with network security and incident response, then worked on information security program management, shifted to cyber security governance, risk and compliance for some time. I also had a chance to work on vulnerability management and security standards. Lately, I have been working on information security and privacy in the cloud, being more and more interested in cloud architecture and improving security posture management in the cloud.

[H9]: To begin with, what cybersecurity certificates did you obtain?

[GU]: I am certified ISC2 CISSP, CCSP, SSCP in good standing. I obtained AWS Certified Cloud Practitioner and AWS Solutions Architect Associate certificates, together with Azure Fundamentals certificate, and I have obtained ITIL v3 foundation certificate in service management.

[H9]: Why did you decide to pursue those certificates?

[GU]: In general, there were three reasons I have pursued my current certificates. One of the reasons was to learn new things, enrich my skills and broaden my knowledge to get an opportunity to develop and land a better paying job or a job that would enable me to work on more interesting things. The other reason was to validate my knowledge by passing the certification and confirm the expertise in current roles. The third reason was out of curiosity to learn new things that might or might not be useful in the current role or future ones. I can say that my certification path was more dictated by the first two, than the third one.

SSCP from ISC2 was my first certificate. At that time, I was preparing and working on some other certificates such as CCNA and learning Linux, but at some point, I started exploring business continuity topics, CIA triad, AAA, IAM, etc., and ended up reading a SSCP book. I liked the topics very much, lots of different security domains, and I decided to go for it. Shortly after that, I decided to take the ITIL v3 exam because I had some free time, and a lot of people were going for it in my team, so I thought it would be useful to have it and to learn new things from the ITIL perspective. CISSP was my next goal for the following year, and I spent a lot of time and effort studying it thoroughly. At that time, my career steered in a certain direction, and it was the only logical next move to take after having passed the SSCP, and CISSP being one of the most respected and requested certificates in the labor market. After having successfully passed that, I was in doubt what to do next, in which direction to develop further. I was analyzing my skill set and skills I lack or want to improve. I realized that it was time for me to go into the cloud, get more technical. Between CCSK and CCSP, I chose the latter, because I liked their approach towards cloud security. Now that I have learned more about security in the cloud from a vendor neutral perspective, I decided to deep dive

and increase my knowledge from the biggest cloud providers out there. I started with Microsoft Azure by passing the Fundamentals exam. After that I took a break in certifications, then I decided to go work on AWS Certified Cloud Practitioner certificate. The whole AWS concept somehow impressed me in many ways, and I found it so clever and logical yet so simple, that it became my current certification path. Next, I passed the AWS Solutions Architect Associate exam, and I'm not stopping there.

There are many other certifications that I wanted to pursue at some point and was preparing for, but my life and career had other plans for me. Nevertheless, the knowledge stays and the things learned, with or without the certificate.

[H9]: From all of them, which one do you value the most?

[GU]: It's difficult to say, every certificate has its own value and importance in its own way, as each of them provided me with certain knowledge and a chance to grow and take the next one.

[H9]: From the current perspective, which one was the most difficult to achieve?

[GU]: Definitely CISSP. Not just because it requires five years of experience in different security domains, but also because it goes in depth on so many security topics, and tests not just your knowledge, but also other skills such as thinking skills, time management, etc.

[H9]: Which one do you consider the most useful?

[GU]: That would depend on the position and role. At the time I passed SSCP, it brought me the biggest value at that point in time, but overall, I can say that the CISSP certificate provided and validated the most knowledge on many different security domains, which is very useful for a wide variety of security positions and roles. In my opinion, that's the best value. It enabled me to become more knowledgeable and deep dive into some security domains. In the near future, I plan to continue pursuing more AWS certificates, as it aligns with my current role and responsibilities and my future career development plans and interests.

[H9]: In what situations did the certificates prove most useful? How did they influence your career? Did anyone ever require any of them?

[GU]: With the certificates, I was able to increase my knowledge, and for me, that's the most important thing. It also made me stand out not only among the applicants for a job interview, but also among the team members. My expertise in certain domains was always recognized in the company.

[H9]: We're curious what your position on the 'certificates vs. skills' debate is. Do certifications always imply real knowledge and competences?

[GU]: In my opinion, certificates validate the knowledge and skills gained by experience and/or learned while preparing for the certification. I can only speak for myself, but usually, I gained new knowledge while preparing for the certificate exam, which opened a door for me to change jobs and gain new skills, having the opportunity to apply that knowledge in practice, but sometimes it was just a confirmation of my skills. I didn't always have a chance in the particular role to apply all of my skills, so I had to validate them in some other way, like certificates. Skills are more important than certificates, that's what gets the job done, the end result counts, but certificates also help create and develop new skills that prepares us for the job. The best is to have both skills and certificates.

[H9]: How long does it take to prepare to take an exam for such certificates?

[GU]: It depends on many factors. One of them being the previous experience and knowledge, someone's ability to learn new things and how quickly, time management, how much time we are able to spend learning daily, weekly, is it something that we are able to apply in our current position and apply it on the exam, etc. It took me about six months to prepare for CISSP. I like to make sure that I'm very confident in my knowledge, that is why I used multiple resources while preparing for it, video courses, several books, practice exams, etc. Not just for CISSP, but also for other exams - I like to explore multiple resources for learning. For example, while preparing for SSCP, I was also reading a book of Comptia Security+, because most domains and topics overlap, it was a great additional source of knowledge. That extended my preparation. I could have just focused on SSCP and not bothered to explore outside of it. Also having passed CISSP, I immediately started preparing for CCSP in the same year. Just four months later, I have successfully passed the CCSP exam. In regards to AWS exams, the preparation time depends mostly on experience and cloud knowledge. The best learning path is having hands on the labs and experimenting a lot with it. That proved to be the best way for me, listen to it or read it, try it, test it, apply it.

[H9]: What is the most challenging part of preparing for such certificates from your point of view?

[GU]: Time management. It's crucial to dedicate your time to learning. CISSP for example requires time and dedication, there are no shortcuts to success, the same goes for AWS certificates that require a lot of practical knowledge, be sure to get your hands dirty and do the labs, that is the best way to learn in my opinion. Nowadays, my challenge is juggling between work and family and preparation for new certificates.

[H9]: Are there any certificates that you now consider a waste of time?

[GU]: Absolutely not. I have my least favourite and most favourite ones, but none of them was a waste of my time. I believe that any certificate we take or prepare for is not a waste of time, it doesn't matter if we are able to use the knowledge in the current positions or not at all, continuous learning is the key.

[H9]: Let's now assume that our reader is at the beginning of his security path. What steps does he have to follow to prepare for and pass the exam for such certificates? Do you have any advice? What 'certificate roadmap' would you suggest?

[GU]: I would suggest taking the time to explore what different paths in security there are, and to understand which one we are interested in the most. Having passion for something is very important. If you have a passion for compliance, then maybe pen testing would not be that interesting to you, or vice versa. Investing in resources is also important. There are a lot of free courses and tests out there, we should explore those, but I have to say that also purchasing courses and books is worth it. There are more and more beginner certificates for security. I believe that getting familiar with general knowledge, the security fundamentals is important before jumping into any specific field. That will serve us as a strong base for building the knowledge for more complicated things and to go into the desired direction of development.

FELIPE MARTINS



FELIPE IS A CYBER SECURITY ENGINEER,
AN INFORMATION SECURITY
PROFESSIONAL WITH 15 YEARS
OF EXPERIENCE IN SECURITY,
LINUX/UNIX INFRASTRUCTURE.

[Hakin9 Magazine]: Hello! Thank you so much for agreeing to the interview! Please, tell us something about yourself.

[Felipe Martins]: I'm an ex-musician and current security engineer by trade, specialized in penetration testing, and other cyber security testing. I love music, martial arts, puzzles and technology.

[H9]: To begin with, what cybersecurity certificates did you obtain?

[FM]: I've obtained several EC-Council, Offensive Security, eLearnSecurity, (ISC)2 certificates such as CISSP, CEH, OSWP etc.

[H9]: Why did you decide to pursue those certificates?

[FM]: Most of the certifications were basically market requirements, but I also pursued them due to two things, their value in my resume and also for the knowledge they would give me.

[H9]: From all of them, which one do you value the most?

[FM]: Not sure exactly if there is one I value above all. Any certification that you can get, where you can learn something, is a good certification. No matter if it is a multiple choice or hands-on one.

[H9]: From the current perspective, which one was the most difficult to achieve?

[FM]: All certifications can be doable when you study correctly, so I don't find them difficult, but the one that really got me a hard time, more due to the nature of the certification itself, rather than its difficulty was (ISC)2 CISSP. The process of getting certified can be a bit tedious in this one.

[H9]: Which one do you consider the most useful?

[FM]: None specifically, all of them complete each other. But for pentesters I would say, any from Offensive Security or eLearnSecurity.

[H9]: In what situations did the certificates prove most useful? How did they influence your career? Did anyone ever require any of them?

[FM]: Most of the certifications I got were market requirements, but now I'm in a position to choose the ones I want.

[H9]: We're curious what your position on the 'certificates vs. skills' debate is. Do certifications always imply real knowledge and competences?

[FM]: There are good points to both fronts, certifications are the way the market can pinpoint you among thousands of professionals, but it doesn't mean a highly certified professional has appropriate experience.

At the same time, I know hundreds of highly experienced professionals with no, or just a few certifications.

It all depends on the goal. If the goal is to learn something new and put it to practice, I would totally go for any certifications you can put your hands on.

[H9]: How long does it take to prepare to take an exam for such certificates?

[FM]: That is a very wide open question, it could vary due to the specific certification, personal time at the candidates disposal and also the experience of the candidate. I would say in general terms, for multiple choice exams it could take 1-3 months. For hands-on ones, it could take between 3 months to a year, depending on the difficulty of the subject and how experienced you are at that.

[H9]: What is the most challenging part of preparing for such certificates from your point of view?

[FM]: First of all the high prices some certifications are rated. SANS for example are too expensive (course and exams) for most of us to pay. Second would be finding time to continuously study. I would say time is always the biggest problem.

[H9]: Are there any certificates that you now consider a waste of time?

[FM]: I wouldn't say a waste of time, but I wouldn't take certifications where my current certifications would overlap or supersede them in terms of knowledge. I personally prefer to do hands-on exams rather than multiple choice ones.

[H9]: Let's now assume that our reader is at the beginning of his security path. What steps does he have to follow to prepare for and pass the exam for such certificates? Do you have any advice? What 'certificate roadmap' would you suggest?

[FM]: First would be choosing the field he wants to work and study deeper. Once that is chosen, he would start from scratch.

I would first start by learning TCP/IP (networks in general) and also at least 1-2 Operating systems, so you are prepared for your studies in security.

I would then start to get some 101 security knowledge, for that CompTIA and (ISC)2 exams can help, or any other course that can grab you by the hand and give you a bit of perspective and one inch deep knowledge of security.

I would then, if intrusive security is the path you chose, I would go for an INE subscription, it would give you access to all eLearnSecurity courses, they will prepare you from scratch.

If you are a bit more advanced, you could take Offensive Security right away.

CEZARY KUBICKI



**CEZARY IS A CYBERSECURITY
CONSULTANT FOCUSED ON ALL ASPECTS
OF BLUE TEAMING.**

[Hakin9 Magazine]: Hello! Thank you so much for agreeing to the interview! Please, tell us something about yourself.

[Cezary Kubicki]: Hello there, thanks for inviting me! My name is Cezary, and I'm a cybersecurity enthusiast. I'm 37 years old and living in Warsaw (Poland). Currently working as a Cybersecurity Consultant at EY. Focused on all aspects of blue teaming. I'm still at an early stage of my career in cyber, though.

[H9]: To begin with, what cybersecurity certificates did you obtain?

[CK]: Well, I have many certificates. Sometimes I feel like completing courses, collecting badges and certificates is my new hobby. Not all of them are industry-recognized, but they were still helpful in broadening my knowledge. Majority of them are security and cloud-related.

Some of them are important in the industry like my recent SC-200 issued by Microsoft. A relatively new certificate for security analysts working with Microsoft tools on a daily basis.

Another one is MITRE MAD, but it's more like a subscription model. It does contain multiple (five right now) certificates related to MITRE ATT&ACK - one of the most important framework and knowledge base.

[H9]: Why did you decide to pursue those certificates?

[CK]: Microsoft security tools like Sentinel are getting more popular among enterprises. In brief - it is a cloud-native SIEM with built-in SOAR capabilities perfect for detection, analysis, response and reporting. Definitely a game changer with huge potential. Still a bit expensive compared to other SIEM tools, but I think sooner or later Microsoft Azure and its solutions will become more accessible for SME. The latest Gartner's Magic Quadrant for SIEM places Microsoft as a leader.

MITRE MAD on the other hand, focuses on their behavior-based framework used by both defensive and offensive professionals (and probably adversaries as well...). Everyone with an active subscription has a chance to collect five certificates:

- Cyber Threat Intelligence
- Security Operation Centre Assessment
- Adversary Emulation
- Threat Hunting
- Purple Teaming

If you want to be good in cybersecurity you should be fluent with MITRE's framework.

[H9]: From all of them, which one do you value the most?

[CK]: Definitely MITRE MAD is my favorite between these two. It is a comprehensive bundle of five certificates which makes you proficient with MITRE ATT&CK. Not every business uses Microsoft tools, but they surely follow MITRE guidance and recommendations when mitigating the risk or responding to threats.

[H9]: From the current perspective, which one was the most difficult to achieve?

[CK]: Microsoft SC-200 was my most difficult exam so far. I passed at the second attempt.

It's purely focused on Microsoft security tools, and it is recommended to have some hands-on experience before attempting the exam. However, there are many free webinars, courses, and labs to broaden the knowledge and get some practice.

[H9]: Which one do you consider the most useful?

[CK]: Both are very useful, but MITRE MAD is more all-round like I suggested above. The best thing is that they both give best results when combined.

[H9]: In what situations did the certificates prove most useful? How did they influence your career? Did anyone ever require any of them?

[CK]: It depends on the business, but as a consultant I might be interviewed by an internal or external client before I am assigned to the project. None of the certificates were formally required, but surely both helped me to pass the shortlisting stage.

[H9]: We're curious what your position on the 'certificates vs. skills' debate is. Do certifications always imply real knowledge and competences?

[CK]: I would prefer to avoid terms like 'always' or 'never'. In fact, certificates can be a solid proof of knowledge. I know that professionals tend to state that only hand-on skills matter. I believe this is not true, and I am the best proof of that, as I joined the Cybersecurity industry without a proper experience. Yet, my CV was full of completed courses and trainings (even free ones) and this showed my dedication which was noticed and appreciated by my employer.

[H9]: How long does it take to prepare to take an exam for such certificates?

[CK]: It depends on your motivation and dedication (as always).

MITRE MAD can be completed relatively quickly as the syllabus is 100% focused only on ATT&CK framework. You should be able to complete all certifications within a month, assuming you also have other things to do in your life.

Bear in mind that Cybrary with its free account gives access to full MITRE MAD preparation. Yep, that's true. Not a single penny for the course.

But Microsoft's SC-200 might take you a while. My first try took place after two weeks of learning and I didn't pass, so I think that a month is the reasonable minimum here. Microsoft provides full e-learning free of charge.

[H9]: What is the most challenging part of preparing for such certificates from your point of view?

[CK]: Details. Exams can be tricky sometimes, and often you have to choose the 'best' possible answer which means that all answers might be correct in some way, but we need to choose the best one. I think I failed SC-200 at the first attempt as I gave not enough attention to details when learning. To pass the SC-200 you really need to understand how Sentinel/Defender work and be able to recommend the best possible solution in given scenarios.

[H9]: Are there any certificates that you now consider a waste of time?

[CK]: Absolutely not. Each course/certificate created an opportunity to increase my knowledge and build up my confidence to some extent.

[H9]: Let's now assume that our reader is at the beginning of his security path. What steps does he have to follow to prepare for and pass the exam for such certificates? Do you have any advice? What 'certificate roadmap' would you suggest?

[CK]: If I could go back in time, I would definitely start from Security+ and Network+ syllabus + free learning resources available on the internet. The knowledge required for these exams gives a really solid foundation needed for entry/junior roles in cybersecurity. I can't imagine a better starting point to be honest. Especially for people who decided to change their career, don't have any computer science degree etc.

Aside from technical knowledge, don't forget about people skills. These are even more important in our industry! So build up the right mindset where dedication, consistency and empathy are the main ingredients.

Also, don't forget to connect with like-minded people. The power of networking will skyrocket your possibilities. Sharing knowledge and experiences gives best results! I'm trying to stay active on my LinkedIn profile and share anything I believe is useful for early professionals, so don't hesitate to invite me to your network! I'd love to join :)

Here is a link to my profile - <https://www.linkedin.com/in/cyberstory/>

SAMY MABROUK



**SAMY IS THE HEAD OF OPERATIONAL
SECURITY AND CYBERDEFENSE CENTER IN
DOCAPOSTE GROUP. HE IS AN IT SECURITY
EXPERT WITH 17+ YEARS OF EXPERIENCE.**

[Hakin9 Magazine]: Hello! Thank you so much for agreeing to the interview! Please, tell us something about yourself.

[Samy MABROUK]: I am an IT security expert with 17+ years in the information security and cybersecurity fields. I held many positions as auditor, security architect, CISO, speaker, head of cyberdefense department, president of global security committee within big companies and groups.

Also, I worked in both public and private sectors and in many domains, like assurance, energy, industrial, banking, services, governmental and regional.

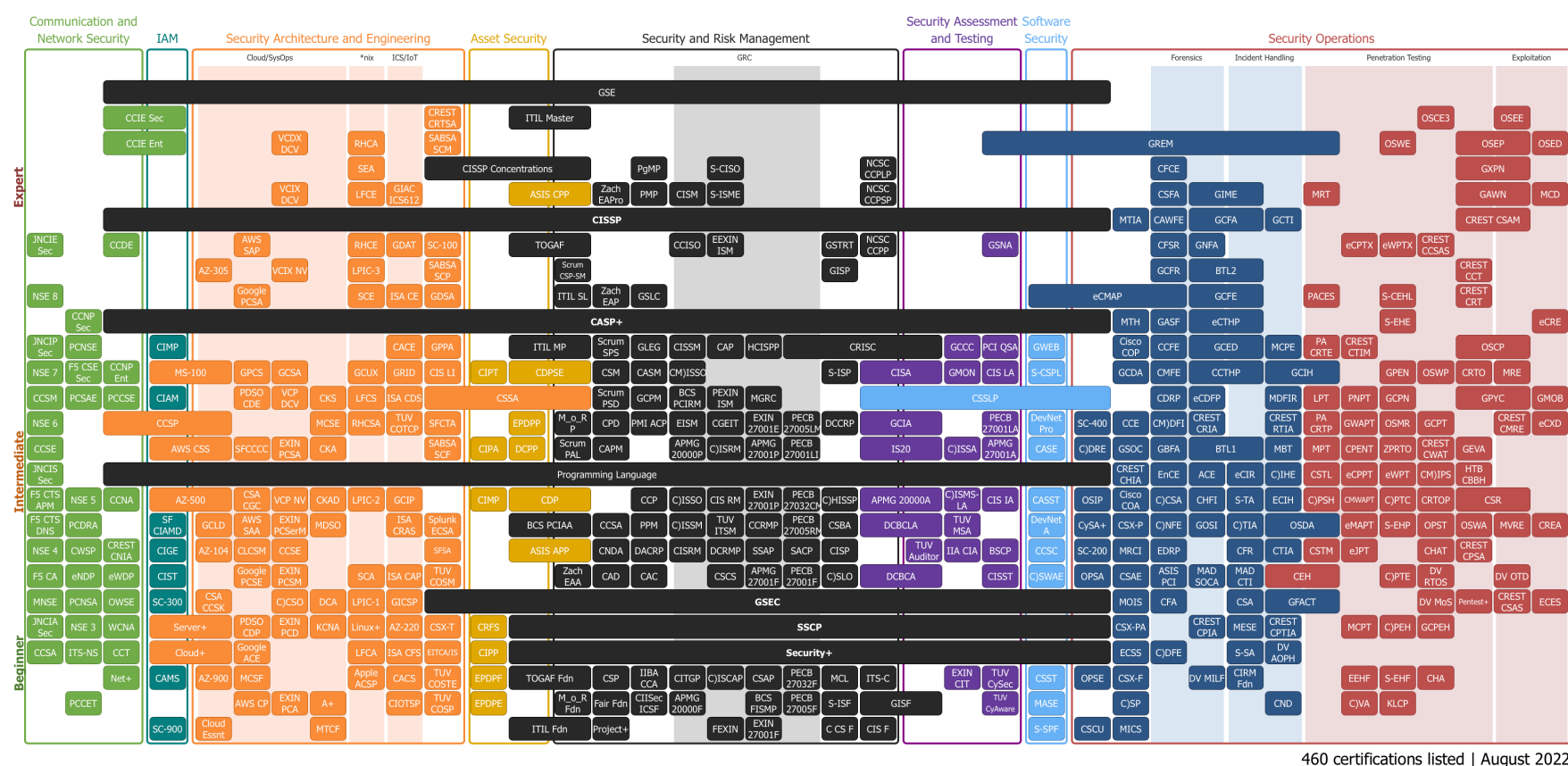
[H9]: To begin with, what cybersecurity certificates did you obtain?

[SM]: I obtained many certificates related to information security and cybersecurity. The most important ones are mainly CISSP (Certified Information Systems Security Professional) and GCFA (GIAC Certified Forensic Analyst).

[H9]: Why did you decide to pursue those certificates?

[SM]: The large scope of CISSP certificate makes it the most well-known certificate for information security experts and architects. It includes both management and technical aspects. The actual version of CISSP covers eight chapters:

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security



Pauljerimy.com arranged 460 IT security certifications on a chart with basic information and links to each certification's website (<https://pauljerimy.com/security-certification-roadmap/>).

This chart explains why I completed my CISSP with the GCFA certificate. My goal was to enlarge my skills domain to cover security operations expertise not deeply covered by CISSP (forensics and incident handling).

The GCFA (GIAC Certified Forensic Analyst) certification is related to the SANS institute FOR508 entitled Advanced Digital Forensics and Incident Response course.

The GCFA is very useful for those searching for expertise in SOC and CSIRT teams while the CISSP certificate guarantees a good expertise for CISO, security architects and defenders.

[H9]: From all of them, which one do you value the most?

[SM]: The large scope of the CISSP makes it the most valuable for me and for those who search for technical polyvalence.

[H9]: From the current perspective, which one was the most difficult to achieve?

[SM]: It really depends on our experience before doing the exam. For me, the GCFA was more difficult as it came after a long management and GRC (Governance, Risk and Compliance) experience (non-operational field).

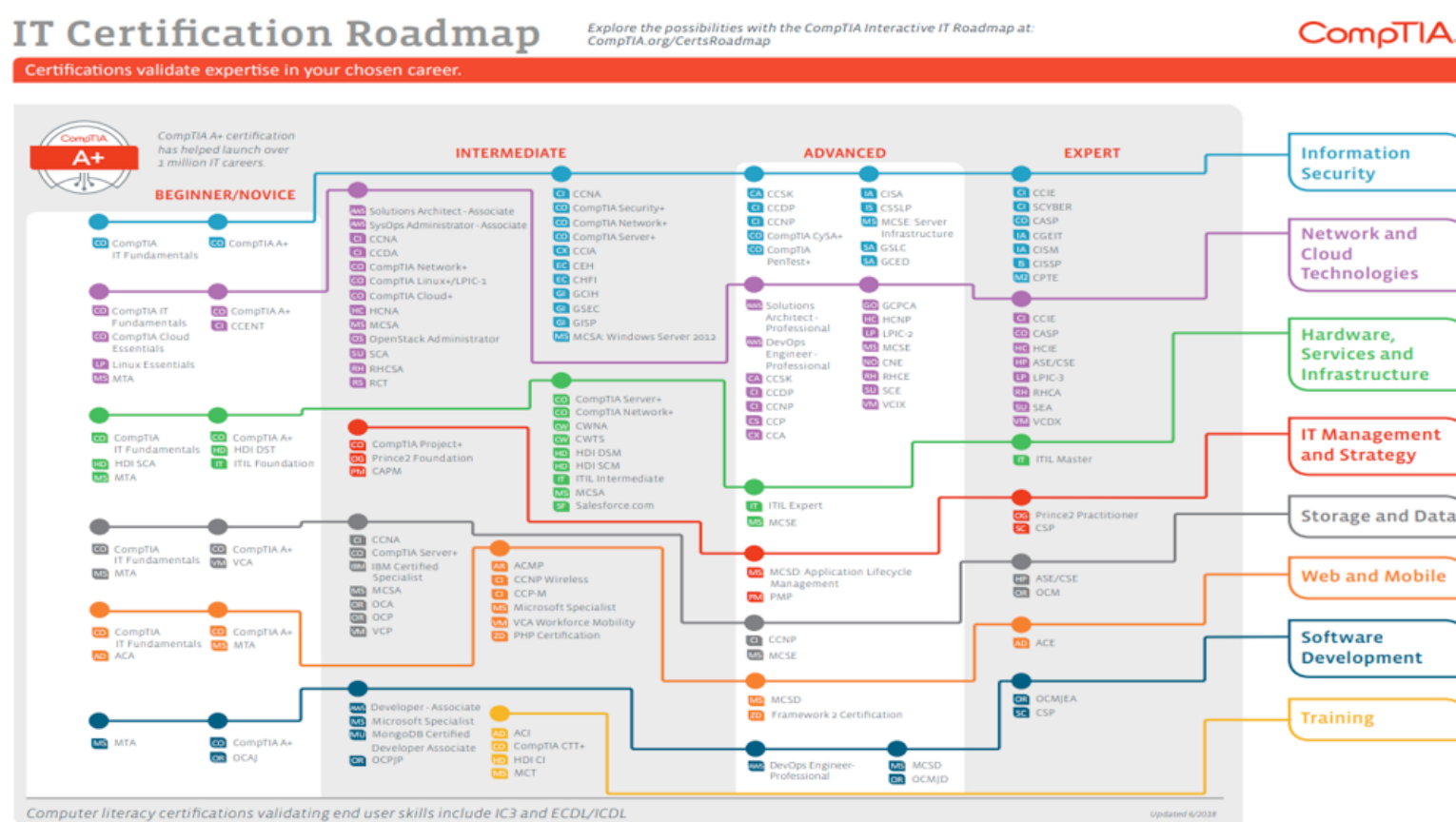
[H9]: Which one do you consider the most useful?

[SM]: The CISSP was/is most useful for me as I chose to be polyvalent and work on several information security and cyberdefense including identification, protection, detection and response fields.

[H9]: In what situations did the certificates prove most useful? How did they influence your career? Did anyone ever require any of them?

[SM]: The CISSP certificate is hugely requested for cybersecurity positions from the analyst to the CISO and the security architect. Its large scope (technical and not technical) makes it the most useful.

When you focus on the 'Expert' column of Information Security in the IT Certification Roadmap proposed by CompTIA (<https://cin.comptia.org/resources/comptia-it-career-roadmap.114/>) you will find that the CISSP is the only certificate that addresses management and technical aspects without being related to a specific technology or editor.



The CISSP certificate helped me more than the other certificates to acquire knowledge, be efficient in what I do and choose the position I like.

[H9]: We're curious what your position on the 'certificates vs. skills' debate is. Do certifications always imply real knowledge and competences?

[SM]: Unfortunately, not all certificates always imply real knowledge and competences. I met many certified persons with weak operational/hands on skills. Having a well-known certificate is a condition to be visible to more recruiters requiring certificates. But the technical interview will confirm our capacity to meet the job needs.

[H9]: How long does it take to prepare to take an exam for such certificates?

[SM]: The CISSP exam took two weeks of preparation including the training while the GCFA took three weeks as I had to do many lab setup and installations to practice and manipulate different cases.

[H9]: What is the most challenging part of preparing for such certificates from your point of view?

[SM]: The CISSP preparation challenge is mainly the memorization of many different concepts and regulations while the GCFA challenge was more related to the deep knowledge of artefacts, hives, filesystem and memory structures.

To guarantee passing the GCFA exam, we have to do many labs and manipulate different cases and tools in addition to the reading and comprehension of the FOR508 books.

To guarantee passing the CISSP exam, we have to train ourselves how to choose the best solution to manage or resolve a security issue.

[H9]: Are there any certificates that you now consider a waste of time?

[SM]: Absolutely no!

[H9]: Let's now assume that our reader is at the beginning of his security path. What steps does he have to follow to prepare for and pass the exam for such certificates? Do you have any advice? What 'certificate roadmap' would you suggest?

[SM]: This question is not easier than certificate questions :P

The response to this question requires some hypothesis as it depends on many parameters and goals:

- Specialization vs polyvalence
- Management vs technical
- Desired field and trajectory

First, I recommend starting with technical certificates (beginner or intermediate) in offensive or defensive security. This training and certificate will give you a deeper vision about what you want to do next.

Second, the choice will depend on the first parameter I put above; what profile you want to have, specialist or polyvalent expert.

If you want to be a specialist, you can go deeper and choose to learn about offensive security to become a vulnerability analyst, pentester, red teamer, technical auditor, vulnerability researcher, bug bounty expert, etc.

Most of the other security positions, like security architect or SOC analyst/manager, CISO and technical auditor, require a minimum of polyvalence in cybersecurity.

So, if you want to follow this way, you have to develop your skills in cyber defense and information security management and governance.

All management positions require a good culture in both strategic and operational security, especially for CISOs and SOC managers. If we refer to the NIST Cybersecurity Framework, you should have a good comprehensive view of the lifecycle for managing cybersecurity risk over time based on the five key functions – Identify, Protect, Detect, Respond and Recover.

Finally, I recommend choosing the certificate directly related to what we actually do or what we plan to do shortly. Remember that the certificate is a tool to prove the skills that we get by working in real cases and treating real cybersecurity issues.

PIOTR DĘBSKI



**PIOTR IS AN IT SECURITY CONSULTANT
WITH 5 YEARS OF EXPERIENCE, INVOLVED
IN ORGANIZING UNIVERSITY MEETINGS IN
THE TOPICS OF CYBERSECURITY.**

[Haking Magazine]: Hello! Thank you so much for agreeing to the interview! Please, tell us something about yourself.

[Piotr Dębski]: Hello and thank you for the opportunity to be here. So, I started my career in cybersecurity almost five years ago. Together with my friends, we have organized some meetings at our university to discuss cybersecurity topics, we prepared some presentations and hands-on activities. Then I started my first job as Security System Engineer, where I worked for three years, where I was mostly responsible for preparing, implementing and maintaining security systems like firewall, WAF, etc. I was running technical and non-technical training classes (security awareness) for customers. I have no specific hobby, I'm interested in everything, but cyber security has become my passion.

[H9]: To begin with, what cybersecurity certificates did you obtain?

[PD]: NSE 4, NSE 6, NSE 7 (NSE- Fortinet's certification path), CompTIA Security+ and now I'm preparing for CISSP certification.

[H9]: Why did you decide to pursue those certificates?

[PD]: Fortinet certification was strongly related to my previous job and it was valuable for my employer. CompTIA Security+ was my own decision. I was thinking that it would be a great start and enhance my basic knowledge about cybersecurity.

[H9]: From all of them, which one do you value the most?

[PD]: I think it will be CompTIA Security+ because that was my own decision. I prepared for this exam by myself without any pressure from my employer. It was my own effort.

[H9]: From current perspective, which one was the most difficult to achieve?

[PD]: I guess it will be CompTIA Security+. The certification covers almost all topics related to cyber security and it proves that you have some overview/basic knowledge about each topic. Secondly, I spent much more time preparing for CompTIA Security+ than for others.

[H9]: Which one do you consider the most useful?

[PD]: From a practical point of view - NSE7. Knowledge that I had to get was very helpful during my day-to-day work.

[H9]: In what situations did the certificates prove most useful? How did they influence your career? Did anyone ever require any of them?

[PD]: They turned out to be the most valuable during recruitment. In addition to the initial verification of knowledge, the certificates show the employer during the recruitment that someone is involved in this topic, that they have devoted their private time to training.

[H9]: We're curious what your position on the 'certificates vs. skills' debate is. Do certifications always imply real knowledge and competences?

[PD]: This never-ending story. Theory can never beat practice. Every person who goes to training wants to listen to the practitioner, not the theorist who scrolls only through the slides. For me, the certificates show that someone is involved in the learning process, that they are interested in it, that they want to deepen their knowledge and are a great candidate to implement it in the organization of the company and this is a huge value. There are a lot of different solutions in cybersecurity, but if someone knows what IPS is and has basic knowledge, they only need a short time to explore this topic. The security industry stands out from the rest in that you have to learn a lot and be up to date all the time. However, to achieve this, you need to have the right mindset, as well as the willingness to constantly learn, often devoting your private time and the desire to learn how something works very deeply. The good news is that I'm observing that people entering or already entering cybersecurity industries have this mindset. This will allow you to catch up with practice very quickly. The certificate is only a confirmation of commitment.

[H9]: How long does it take to prepare to take an exam for such certificates?

[PD]: For each Fortinet certification, I needed 2-3 weeks. It depended on how much time I could manage after work, but it was very helpful that I partly used this knowledge in my day-to-day work. For the CompTIA Security+, it took 120 days with method reading ten pages each day and going through the book twice.

[H9]: What is the most challenging part of preparing for such certificates from your point of view?

[PD]: To manage extra time after working hours and be focused only on this. It requires self-discipline.

[H9]: Are there any certificates that you now consider a waste of time?

[PD]: No, absolutely no. From my perspective, preparing for the certificate is a journey that can teach us something new and open new perspectives. Of course, I mean certification from respected worldwide certification centers like (ISC)2, Offensive Security, CompTIA, SANS Institute, etc. I assume that persons that are joining cybersecurity are smart and they can assess which certification will be perfect at the beginning. If not, I really recommend that they go through the CompTIA Security+ book and then assess if you are obsessed about that or not. One hint from me: always try to achieve more than you think you can.

[H9]: Let's now assume that our reader is at the beginning of his security path. What steps does he have to follow to prepare for and pass the exam for such certificates? Do you have any advice? What 'certificate roadmap' would you suggest?

[PD]: At the beginning try to do good research about certifications on the Internet - what it covers, how the exam looks, how much it costs, check out job offer descriptions which certification are most commonly mentioned. You can ask your manager which certificate will be valuable for the company. Then, if you finally find out which certificate is most suited to you, check out preparation materials and training (free and paid). My technique is to read all materials twice very carefully and find someone who wants to prepare for the same certification and go for it together!

Good luck and I hope, see you soon at conferences, training or as teammates in the same company!

SARTHAK THAKUR



**SARTHAK IS AN ETHICAL HACKER
AND WEB APP PENETRATION TESTER.**

[Hakin9 Magazine]: Hello! Thank you so much for agreeing to the interview! Please, tell us something about yourself.

[Sarthak Thakur]: My name is Sarthak Thakur, I'm pursuing my M.Sc. in Cybersecurity from Amity University Jaipur, India. I am a certified Network Penetration Tester, Web Application Penetration Tester, CEH and also currently working as a Security Researcher Intern in HackHunt CyberSecure LLP, India. I enjoy trying out new tools and exploiting new vulnerabilities. The more vulnerabilities I exploit, the more my urge to learn more increases.

[H9]: To begin with, what cybersecurity certificates did you obtain?

[ST]: I began with the certification from Udemy, a Cyber Security Course for Beginners, which helped a lot to understand the basic things. After that I did the Network Penetration Certification, CEH and Web application penetration certification to grow my knowledge in the field of pentesting.

[H9]: Why did you decide to pursue those certificates?

[ST]: It helps to gain both practical and theoretical knowledge, few companies who hire for cyber security jobs look for people with such certification.

[H9]: From all of them, which one do you value the most?

[ST]: For me, Web Application Pentesting is the most valuable because it helps me to gain the practical skills and techniques of several vulnerabilities. And it also helps me to report some of the bugs for several organizations.

[H9]: In what situations did the certificates prove most useful? How did they influence your career? Did anyone ever require any of them?

[ST]: Certification comes to play a huge role, especially in the IT field. A few of the benefits are getting higher pay and advancement opportunities.

In my case, while applying for campus recruitment, a few companies have put the eligible criteria as CEH certification to apply for the job. So it helped me to get shortlisted for the interview round.

[H9]: We're curious what your position on the 'certificates vs. skills' debate is. Do certifications always imply real knowledge and competences?

[ST]: Definitely knowledge, but yes, certifications also play an important role in some cases. But without knowledge and only certification, you won't get too far. Recruiters look for people who have the skills and expertise to perform in their organization. If you do not have your concepts clear, your certification holds no value.

[H9]: How long does it take to prepare to take an exam for such a certificate?

[ST]: I recommend giving 1 month for courseware (2 books from CEH) and 1 month just for lab exercises (1 lab manual from CEH).

[H9]: What is the most challenging part of preparing for such certificates from your point of view?

[ST]: The most difficult part is the time management. I am preparing for it and I am facing this time management issue a lot; being a student, I have to do my college assignment and project work simultaneously. So, sometimes it's a hustle for me to manage the work in time.

[H9]: Are there any certificates that you now consider a waste of time?

[ST]: No certificates are useless; if you have the eagerness and hunger for the knowledge, every small certification is useful. But if you are financially strong and stable then go for the professional level certifications, like OSCP, CISSP, CEH etc. These certifications cost a huge amount of money to do it or else my best suggestion will be to go for free resources on YouTube, GitHub, etc. You will get free resources and video tutorials from there.

[H9]: Let's now assume that our reader is at the beginning of his security path. What steps does he have to follow to prepare for and pass the exam for certificates? Do you have any advice? What 'certificate roadmap' would you suggest?

[ST]: The best way to learn and understand each concept is to set up a suitable LAB consisting of at least three or more systems with different operating systems installed. You should install the latest version of KALI LINUX OS with all built-in tools, software and scripts. Also, try building a network in this LAB.

CHAITANYA Y



**CHAITANYA IS A CYBERSECURITY TRAINER
AND A BEGINNING PENETRATION TESTER.**

[Hakin9 Magazine]: Hello! Thank you so much for agreeing to the interview! Please, tell us something about yourself.

[Chaitanya Y]: My name is Chaitanya, I have two years of experience as a Cyber Security Trainer and one and a half year of experience as a Penetration Tester. I am known as Xssmice to the infosec world. I have worked as a Training Reviewer with OWASP as a volunteer. I'm also a part-time bug bounty hunter, acknowledged by 10+ Companies.

[H9]: To begin with, what cybersecurity certificates did you obtain?

[CY]: CEH Practical.

[H9]: Why did you decide to pursue this certificate?

[CY]: In India, most of the HRs and Recruiting Managers consider the CEH Certification no matter if you are skilled also. CEH is considered an interview barrier in India. Due to that, I have done CEH.

[H9]: In what situations did the certificate prove most useful? How did it influence your career?

[CY]: Certificates are useful when we want to acquire a job. They influence the experience of knowledge.

[H9]: We're curious what your position on the 'certificates vs. skills' debate is. Do certifications always imply real knowledge and competences?

[CY]: Certificates will never imply real knowledge because in real life job situations, circumstances will never be in our control. But if we gain perfect skills, we can be ready for any type of situation.

[H9]: How long does it take to prepare to take an exam for such a certificate?

[CY]: Average of three to four months.

[H9]: What is the most challenging part of preparing for such a certificate from your point of view?

[CY]: Time management.

[H9]: Are there any certificates that you now consider a waste of time?

[CY]: CEH Theory

[H9]: Let's now assume that our reader is at the beginning of his security path. What steps does he have to follow to prepare for and pass the exam for such a certificate? Do you have any advice? What 'certificate roadmap' would you suggest?

[CY]: PortSwigger>Tryhackme>hackthebox>CEH > PNPT> CRT0/CRTP