EC-Council

ETHICAL HACKING: CHOOSING THE RIGHT PATHWAY!

EC-Council Cyber Research

A. Ethical Hacking IS NOT Pentesting

We hear it on the internet: 'XYZ certification is better than a C|EH because you have to do an actual penetration test and submit a report.' The comparison is inaccurate and those who make it misunderstand the nature and content of the C|EH course and certification test. There is a reason the C|EH does not have a penetration reporting component: *C|EH is not a penetration testing certification*.

The C|EH program provides a broad foundation to all cyber security professionals, *not just penetration testers*. Penetration testing represents a small (albeit vocal) percentage of all cyber security jobs. Penetration testing certainly garners the most attention in cyber security, but it is far from the largest pool of job openings.

For example, one or two penetration testers can effectively run a test on an entire enterprise. To defend that same enterprise 24/7, it requires 3-5 people *for every chair that needs coverage*. Put another way, if a SOC needs a staff of 8 people to run for any given shift, then the SOC must hire between 24 - 40 staff to be fully operational 24/7/365. This means that for *every single penetration testing job there are approximately 20x more defense jobs*.

C|EH is a foundational course and qualifies you for a wide range of careers within cyber security. Just look at the 8570 mapping. C|EH is required for 4 very different jobs including incident responder and auditor. By slamming the C|EH for being something it is not, you are not only showing your lack of understanding of the course, but also the job market.

B. ANSI Is Very Important

Anyone can make and teach a course, make a test, and print off a certificate. Just because you can build a lab and run some VMs doesn't mean that your course, exam, and labs follow sound educational principals. Anyone out there can write a test no one can pass. Likewise, anyone out there can write a test that a kitten can pass. This means that not all certifications are equal. One of the most important questions to ask about whatever certification path you take is: is it ANSI certified?

ANSI is a certification body using international standards to ensure your certification meets proper criteria. Gaining ANSI accreditation is time consuming and rigorous and its purpose is clear: to provide third party verification that your certificate program meets the highest of standards, is crafted with sound learning principles, and can create a competency-driven workforce. Don't just believe me, head to ANSI website and look at who recognizes ANSI certification because it states that 'it provides confidence and trust in the outputs of an accredited program' - the US DoD. ANSI is the only accreditation program recognized for 8570 (If you don't know what that is...you really should do your research before making comments). Don't invest in a certification course because some blog told you it was a good cert. Take the time, do the research and invest in a certification that is accredited by a third party and recognized across the industry. Anyone can host a lab and offer a certification. Anyone can post on the internet. Not just anyone can achieve ANSI certification.

C. Make Sure Your Cert is Recognized Worldwide, Especially in DoD 8570

So, you want to get a job in cybersecurity. Have you heard of DoD 8570? If not, here's the quick summary - anyone who wants to work on a US government network needs a cert from the list on 8570. It's that simple. It includes government and military networks. It includes people who work directly for the government or the contractors they hire. This is not optional. It is non-negotiable. 8570 does not care how you feel about the issue. 8570 does not care if you think your awesome cert that is not on the list should count.

It is ok if you don't agree with 8570. It is ok if you think poorly of the certifications listed there. However, keep in mind that the US government (including DoD) and the contractors that support them; represent the largest cyber security job pool in the world. So go ahead and get your little cert and grumble about how unfair 8570 is. Do your research, take charge of your career and own your success.

D. Cost Considerations

How much is your future worth? Investing in your future takes thought. Some certificate programs cost a couple hundred dollars, others over $5,000 (plus hotel, airfare, and food). So how do you choose which one? How much money do you want to burn? If you are getting this certification for your first job; understand something - you will not get your money back. Your employer will not pay you back, this is your investment in you and your future.

One thing to keep in mind. The cost of the wrong certificate is not just the money you spent for the materials and the exam, but it is also the time you spent studying AND the time and money you will have to spend again getting the correct cert. For example, you choose to save money and go with a cheaper cert. It costs you $349 and 60 days of studying. You get the cert, but still can't get a job. On the few interviews you get, they all come back to the same thing, you need a different certificate. You now decide to go and get the other cert. The cost of that cert is not $1899 plus the 60 days of studying. The actual dollar cost is now $349+ $1899+ lost income. The actual time cost is 60 days + 60 days + the time in between job searching.

Be smart about your choices. Going on price now may just cost you more later.

E. Hands-on Lab Platform

Everyone has a hands-on lab platform. Stick around in this field and you'll see any number of labs and ranges. They all offer the similar things. 'We can build a network of 1,000 machines in an hour' and 'test your skills here'. They also all fail at the same thing - useful feedback. Cyber security labs and ranges are about useless without integrated assessment and feedback. This is like going to a pistol range and shooting by yourself. No feedback beyond whether or not you hit the target where you wanted it to. No one is there to provide help on how to improve. No one is there to help critique your technique, your load out, anything. You are just slinging lead down range in the hope that if you do it enough, you'll get better. The good news is that you will. The bad news is that without feedback and assessment you will learn by trial and error (and only then if you keep very detailed logs and review them before and after every range day). This system works and only takes about 5-8 hours of range time per day, 5 days a week for 3 months (slight sarcasm).

Until a better lab system comes along, you want to know the number one question I ask anyone who approaches me for career advice; "Can you describe to me your home lab?". If I get a blank stare, then I know that person is not committed or passionate about cyber security. Every classroom and lab exercise out there is already dated by the time it hits the street. Take ownership of your skillset, build your own home lab and get down to learning.

F. Jobs

Go to monster.com and pick a city you either are living in or want to live in. Enter C|EH and look at how many jobs.

Here's a great example. Go to monster.com and enter OSCP in the search and Philadelphia for the city. Every one of the jobs listed requires at least 6-8 years' experience and some also require a bachelor's degree on top of that. These are not entry level positions. If you have no experience and are looking to get your first job in the business OSCP is not the route to go. Change the city, look at New York, NY. Same thing. Bachelor's degrees, 5-9 years of experience. If you are new to this profession quick going after certifications for jobs you do not qualify for. Human resources are going to receive hundreds of applications and they are looking for any reason to go through the pile quickly and not meeting the minimum requirements is one quick way to do that.

G. Instructor Availability

I'm all for self-motivated and self-educated professionals. In cyber security you must take a proactive approach to keeping your skills up to date. And while that works for some people and some content, sometimes you really need an instructor. This is especially true to those just getting started or to those moving on to acquire skills outside their comfort zone. In those times, you really need an instructor. Think about it. How many professional athletes work out on their own, without a personal trainer? Not many and those that do have been in the gym for decades. Cyber security, like fitness, is a broad category of skills. Are you training for the 100-meter dash or an ultra-marathon? Both involve running, both involve very different training programs. Both require the athlete to be able to clearly state their goals, accept input from a trainer or training program and train to the task at hand. Cyber security is no different.

Identify your career goals, find the certification path to get you there and then find a trainer. Not sure where to start? Then look at trainer/instructor availability...the more there are the more need there is for the certification. Another example from the fitness realm; CrossFit. There are CrossFit Boxes (gyms) all over. Why? Because there is a great demand for access to certified trainers. There is a great demand for access to their knowledge and ability to help people reach their goals.

Cyber security is just another skillset, just like fitness. Take a look around. Ask hard questions. What are my training options? Online, instructor led? What about classroom or mentoring? If it turns out that there is just one instructor, or just a single class offered every three months...you might want to consider another route. I'm not saying those classes are not valuable. However, if you are starting out in this career, you might want to pick a starting point that is widely available and accessible. Staring off in a niche will end in a niche.

H. Time to Achieve

"Time is of the essence" - the motto of every working professional. With 24 hours in a day, of which 8-9 hours is spent behind a desk and 8 hours to rest (if you get a proper rest), it is important to find a program that can be accommodated within your busy schedule.

It is here that certification programs play a large role. The C|EH training session is spread over 5 days, with 20 modules (including sniffing, session hacking, SQL Injection, hacking web applications, IoT hacking, cloud computing, and much more), 340 attack techniques, 140 labs, and approximately 2285 tools!

In just five days, you can learn the different skills required to become a Certified Ethical Hacker!

I. Exam Availability

Where and when you must sit to attend an examination and how you do so is highly important! EC-Council's Certified Ethical Hacker (C|EH) is available at various authorized testing centres located at various areas across the world. Or for the convenience of those who prefer to attempt the exam virtually, EC-Council gives the option to attend the examination while being proctored virtually through ProctorU.

J. Relevance to Your Job Profile

It's always important to keep in mind what type of recognition a certification can give you. Some certifications are created for the sake of creating one, while others possess a deep-rooted benefit. Knowing how the credential can be an added benefit to your career growth ought to be among your reasons to pick a certification.

While the C|EH adds credibility as it is ANSI accredited and a recognized GCT, one of the very important points to keep in mind is that this certification is created and updated keeping in mind the NICE framework. The NICE Framework encompasses the most detailed combination of cybersecurity works which are comprised of precise skills, abilities and knowledge needed to perform certain tasks in a work role. By mapping the program to the NICE 2.0 Framework's Protect and Defend specialty area, EC-Council ensures that their program is directly mapped to a wide variety of job roles.

K. International Appeal

Looking for better job opportunities often means relocating. In today's highly mobile society; it is highly unlikely that you will attend high school, college and find a job in, the same town. Furthermore, jobs in the IT sector allow a great degree of mobility. Digital Nomads now work from the many corners of the world; delivering code and consulting services remotely to the other corners of the world. University degree standards vary from country to country and program to program. Even when it comes to basic job requirements like a degree, it is not an easy feat for everyone to attain one from a university that is recognized globally. The same applies to certifications.

The Certified Ethical Hacker is recognized just about everywhere around the world, especially since it is accredited by ANSI and recognized by DoD 8570 and GCT.

EC-Council also has a vast multitude of training options such as instructor-led training, online training, mobile learning, computer-based learning, hands-on experience with the EC-Council cyber range (iLabs), customized learning, and live-online training.

Source:

1. https://blog.eccouncil.org/ethical-hacking-choosing-the-right-pathway/

EC-Council