



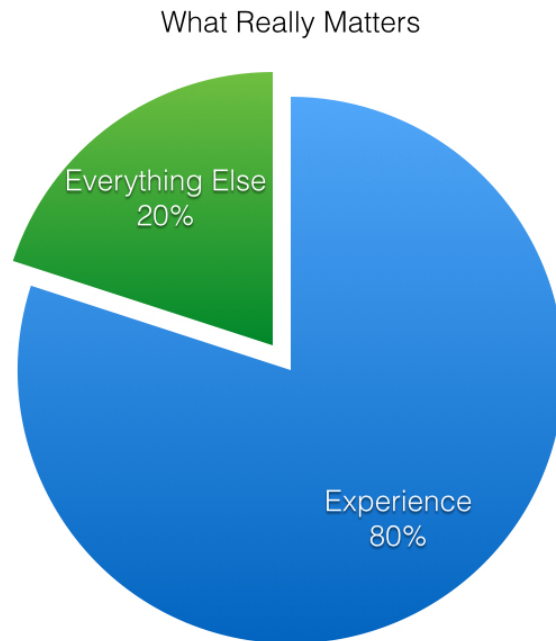
LOOKING TO JOIN THE IT
SECURITY WORKFORCE

HOW TO BECOME A PENTESTER

I used to be where you are - most likely a technical person not fully enjoying what you do at your day job and wanting to make the move to a job that you would actually enjoy in the security field.

For me specifically, that was conducting vulnerability assessments, penetration testing, hacking, auditing and anything in IT Security.

On the About Me page I described a little bit about how I got where I am. Now I'm going to share with you exactly what I would do if I could do it all over again, but first I'm going to answer a few popular questions about the industry.



Is a Computer Science degree necessary to be a pentester?

So you want to learn how to hack and think you need a degree. If you have the time and the money to pursue a degree in computer science, by all means take the opportunity and pursue it. While it is not necessary to have this degree, it would be one of the optimal paths to take under perfect conditions to get your foot in the door at an entry-level position.

You might be pursuing or have other technical degrees already that could substitute nicely. I personally had a Computer Information Systems (CIS) degree when I set out on my journey.

To go a bit further I decided to get a Masters in Information Security and Assurance, but this isn't necessary for everyone. If you were coming from a non-technical field though, a switch to a more technical masters program could be just the path for you.

Don't let the BS and MS degree talk deter you though if getting one isn't an option. Technical degrees are always an option as well.

While you will always find that companies are looking for a degree, if you have the right experience and certifications it surely wouldn't hold you back at all.

Let's take a look at two sample information security job postings:

Security Engineer

JOB REQUIREMENTS

Qualifications / Requirements:

- 4 year Degree in Computer Studies or Information Technology is preferred but not required.
- Holder of CCNP/CCNA/CCNA Security professional certificates preferred.
- Additional preferred certifications include; GIAC Security Essentials - GISF, CEH, CISSP, CISM, LPT, CompTIA Security+.
- Min. 2 years hand-on experience in Network / Security.
- Knowledge of DDoS attack types will be advantageous (Distributed Denial of Service).
- Experience in implementing and administrating core routers, routing protocol, cluster firewalls, load balancer & web proxy farm.
- Qualities: leader, responsible, service and customer-oriented, well organized, hard-working, mature, independent, self-motivated, strong communication skills.

Sr. Network Security Penetration Tester

Knowledge/Skills : Required Experience

**Notice that it is all about
experience here**

- BA/BS in Computer Science or equivalent practical experience.
- Experience in a security consulting role
- Experience performing network security assessments including wireless
- Experience with network/wireless analysis tools, and vulnerability scanners (Nmap, Kali Linux, Metasploit, Kismet, etc.)
- Experience with VoIP Security & War Dialing
- Experience with social engineering techniques (remote pre-texting, spear phishing, etc.)
- Experience physical security assessments (lock picking, camera evasion, etc.)
- Familiarity with various network architectures, network services, system types, network devices, development platforms and software suites
- Experience developing custom scripts or tools
- Strong technical writing and communication skills

Does where I go to school matter?

In my opinion, it doesn't matter where you obtain your degree. You would just use this as a stepping stool to gain some fundamentals and get your foot in the door so that potential clients feel comfortable with you. Sometimes they will actually ask for your resume and a degree looks good on there.

Surprisingly, Vo Tech and Community Colleges often have programs that are just as good as the more prestigious schools. Many times, you can get just as good an education for half the cost and in half the time.

What matters most though is the amount and type of experience that you will be able to gain along the way as was hinted in the graph above.

You should note that even the most expensive college or university does not necessarily have the best educational programs for this particular field. At this point in time this field is in its infancy, which also means

that this is actually a great time to get into the field before it becomes crowded.

Most computer science programs available today place the majority of emphasis on programming, although I foresee them moving heavily in the cyber security direction over time, including Pentesting.

Some schools now even have cyber security degrees, so if you know for sure that this is the area you want to be in then I would take a hard look at that.

That large programming aspect of the computer science programs will also be very beneficial to you later without a doubt.

Which certifications should I have?

Certain certifications will be indispensable when it comes to getting your foot in the door, especially if you pick the right ones.

It may seem like putting the cart before the horse by getting one of these before you get the experience and it is, but having one will give you a leg up over another candidate who doesn't have one.

It is also very doable to get one in a relatively short period of time, unlike a degree.

This is why if you already have a Bachelor's degree I wouldn't recommend going back to get a computer science degree, but instead going after some of the sought after certifications such as: SANS – GPEN, GWPT, GSEC, GAWN; Offensive Security – OSCP, OSWP, OSCE, OSEE; EC-Council – C|EH, ECSA, ECSA L|PT.

There are also others that you can find with a simple Google search or by looking at job postings online.

While it's not necessary that you obtain all of these certifications, you will want to be able to prove that you have the required experience to perform the job and some of these certifications will help you do just

that.

You'll also want to consider some networking certifications such as Network+ to start, or even better the CCNA. You will commonly see the CCNA certification listed on pentesting job requirements.

These certifications will go a long way towards helping you obtain a penetration-testing job and can be just the thing that propels you ahead of another candidate vying for the same job.

Penetration Tester / Cyber Security

General Description of Duties:

1. Conduct both remote and on-site penetration testing based on specific rules of engagement.
2. Test penetration testing tools for potential use.
3. Perform web application vulnerability assessments.
4. Other duties as assigned.

QUALIFICATIONS

Education: Bachelor's and Master's degrees or equivalent experience. Certified Information Systems Security Professional (CISSP), Certified Authorization Professional (CAP), NSA INFOSEC IAM/IEM, and/or Certified Ethical Hacker (CEH) are highly desirable.

What experience should I have?

Don't make the mistake of getting a ton of certifications and forgetting that above all else experience is king. You may make it to the interview, but when the interviewer starts asking about experience, things could start to go downhill fast for you.

While you may not need experience for some entry-level positions, it is critical to get some if you expect to succeed and for a leg up on other entry-level applicants.

A solid understanding of networks is also critical for you. You don't have to be an expert and can learn along the way, but you need to have a somewhat solid overview of how they work.

I was given an IP address in an interview some years back and asked what the broadcast address was. You need to be able to answer simple questions like this, so if you can't you probably need more training in this area.

Building a home lab network environment is critical for a penetration tester and will allow you to get a better understanding of penetration testing, hacking, networking and help you meet the experience requirement you will need.

You will also want to become well versed in working and testing Web Applications and Cloud technologies such as SaaS. Web Application testing is very hot right now and you might have already noticed this while looking at some of the new pentesting positions available.

Because everything is moving out to the Cloud, companies are actively looking for people with the specific skills to test these applications and being advanced in this area can help you stand out from the competition.



Full Time 90k-110k



Web Application Testing, Burp Suite

Job Description

We currently have a full time opportunity with a local VOSB in the Cyber Security Space. My client is currently looking for a **WebApp Penetration Tester** to join their growing team in the DC area. This individual will have the ability to work remotely and will just need to be open to about 25-50% travel throughout the region.

Required Skills:

- CISSP, CEH or equivalent security certification
- 3 years professional experience conducting web application assessments, with a clear understanding of manual methods and tools in addition to automated scanners
- Bachelor's degree in IT related field or equivalent technical certifications
- Programming ability in one or more web/scripting languages such as PHP, JavaScript, Perl, Python, Ruby, ASP .NET
- Proficiency in MVC framework and good knowledge of popular web frameworks like Rails, Django and CodeIgnitor
- Strong understanding of encryption (SSL/TLS, hmacs, PKI) and authentication methods
- Strong experience with tools used for penetration testing such as Metasploit, BurpSuite, w3af, BackTrack/Kali Linux, Nessus, Skipfish, SQLMap
- Excellent written and verbal communication skills, especially when dealing with large reports and datasets with a high standard of documentation and experience writing Rules of Engagement, security test plans, risk/vulnerability assessments, and findings reports
- Ability to translate technical information into business impact for non-technical audiences

Another great way to get experience is by reaching out to people in the industry already and working for them for free in your spare time.

This will give you documentable work experience beyond your own home lab and you may even get an opportunity to work with that company as well.

What skills do I need and is a networking background required?

You must know the fundamentals. That being said, I part ways with some in the industry here as some believe you need many years of experience as a network administrator or security engineer etc. first before moving on to pentesting. I actually believe that this isn't a requirement and think you can learn both concurrently depending on your skill level and willingness to learn. They complement each other.

If you are dedicated you can read both types of books, take both types of classes and experiment with both sides of the same coin. Learning how to pentest doesn't prevent you from concurrently learning how networks work.

However, learning how to pentest and hack without learning how networks work is never going to happen for you, so go get those fundamentals down.

Do I need to know how to code?

While you don't need to be an advanced level coder to penetration test, it would be very wise to start learning some basic scripting in order for you to hack together some tools that you need.

The key here is to get some basic things to work, not to build out some huge application. You might have specific needs according to a penetration test that you are conducting and may need to tweak an already existing application or build your own.

You may commonly run into a Metasploit module that doesn't meet your needs at the moment and you may need to either modify one or write it from scratch.

World's most used penetration testing software

Most penetration testers can code in many languages because after you learn one language it isn't difficult to branch out to others.

In my opinion you should focus on learning Ruby or Python because most of the code and job prerequisites you will come across will be written in one of the two. Both are often used in the penetration world and are the de facto standards. Build it once and then use it forever.

Consultant-IT Penetration Tester



📍 Broomfield, CO

📅 3 Weeks Ago

[Apply Now](#)[★ Save](#)[✉ Email](#)[↻ Share](#)

DESIRED

- Proficient with Windows/UNIX/Linux operating systems HIGHLY DESIRED
- Scripting ability **python, C++, Perl, Ruby, shell scripting, Java Script, etc...** HIGHLY DESIRED
- Security certifications such as CISSP, CEH, GWAPT, CPT HIGHLY DESIRED
- Ability to automate routine tasks

As you gain experience, you can start to branch out to some other languages as well. This knowledge base will make you more attractive in interviews and make you a much better pentester.

Start by watching some YouTube videos and then go and modify or try to recreate those applications on your own.

What is the best way to find a job?

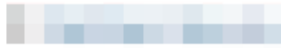
The best way to find a job is to first look at your current employer to see if you can tweak your position or move to another in the company. The next best route would be to intern somewhere if you can.

If you can't do it those ways you can always start your search by going to job searching sites such as the Federal Government (USAJobs.gov), CareerBuilder, Monster.com, Indeed.com and Dice.com.

Be on the lookout for titles such as Information Security Analyst, Information Security Auditor, Information Security Engineer, IT Security Consultant, and of course Penetration Tester. Of course you can search for common keywords such as Kali, Nessus, Wireshark, Metasploit, Burp Suite and nmap.

These will always vary and change over time, but you should be able to come up with a few different combinations and find some openings without issue.

Senior Penetration Tester



📍 Woodbury, MN

📅 1 Week Ago

[Apply Now](#)[★ Save](#)[✉ Email](#)[↪ Share](#)

Requirements

- A passion for helping people and information security
- College degree in Computer Science, MIS, Information Security or equivalent experience
- Approximately 5 years+ of penetration testing experience
- Demonstrated work history of penetration testing experience
- Able to work independently or part of a team
- Motivated, ambitious, professional, strong work ethic and self-directed
- Superb technical writing skills (grammar, spelling)
- Superb verbal communication skills
- Excellent listener and able to identify client needs effectively
- Capable of passing a background check
- Ability to travel up to 25% regionally
- Experience with: Nessus, Metasploit, Burp Suite Pro, Kali Linux tools
- Programming / scripting experience (Python, Perl, C, PHP, Bash)
- One or more certs: OSCP, OSCE, CEH, GPEN, GWAPT, LPT, CPT, CEPT, eCPPT, CWAPT or CISSP

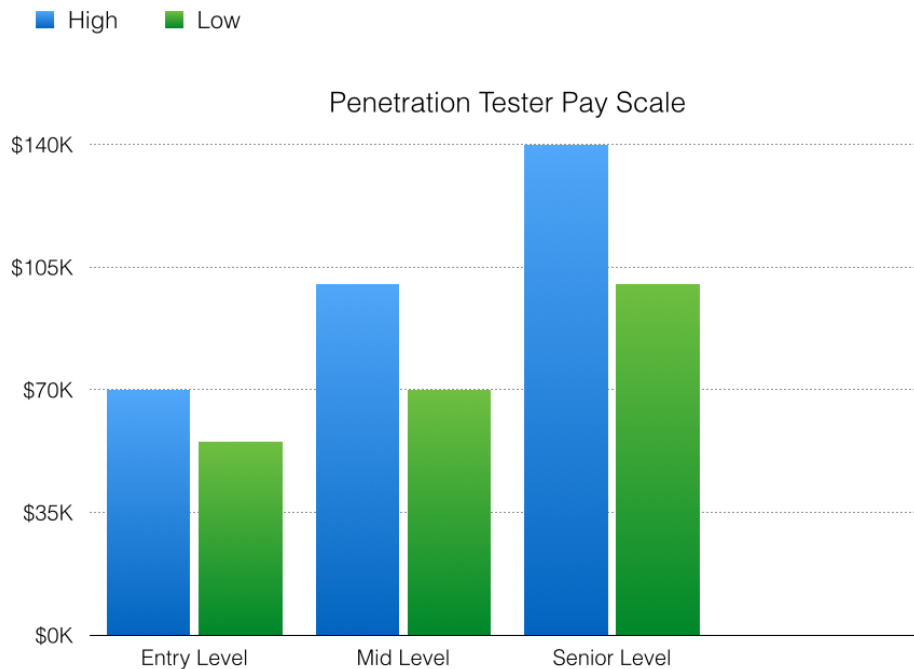
Companies are looking for people who are willing to learn and do what it takes to get the job done.

If you don't have a specific skill but are willing to pick it up along the way then it doesn't matter at all. Presenting yourself to the company that way will significantly increase your chances of obtaining the position.

When interviewing for my first position, I personally had some good education but the direct experience wasn't there. However, the company decided to take a chance on me based on my willingness to learn and get the certifications I obtained.

How much money do pentesters make?

As with any job this depends on many variables, but I've included a general range for you here:



It isn't uncommon for entry-level positions to be between 55k-70k, mid-level to be between 70k-100k and senior level to be between 100k-140k.



Penetration Tester needed for awesome consulting firm! -

[View similar jobs](#)

Job type: Full-Time | Pay: \$90k - \$120k/year
I have an immediate need for a Penetration Tester in downtown Chicago. This is a full...

[View full job description](#) [Save to MyCareerBuilder](#) [Email to a friend](#)



Network and Application Penetration Tester

[View similar jobs](#)

Job type: Contractor | Pay: \$50.00 - \$60.00/hour
Contract position for a Network and Application Penetration Tester. Responsibilities include ... Minimum 3 years experience with network penetration...

[View full job description](#) [Save to MyCareerBuilder](#) [Email to a friend](#)



Penetration Tester / Cyber Security - [View similar jobs](#)

Job type: Full-Time | Pay: \$120k - \$125k/year
Penetration Tester / Cyber Security *Contract to Hire* Role Summary: The Penetration Tester ... Penetration Tester / Cyber Security *Contract to Hire...

[View full job description](#) [Save to MyCareerBuilder](#) [Email to a friend](#)

If I had to do it all over again this is what I would do:

Step #1: I would evaluate my day job

I would evaluate my current position at my job and see if there was any way that I could gain some experience right where I am.

If there were a way to focus on some networking fundamentals or administration fundamentals I would start there. Many of you are already in technical positions, so take a look around, start reading more networking/hacking/pentesting books and see how you can apply it all to your current position.

Step #2: Set up my home lab

At the same time as I'm evaluating my day job, I would be setting up a virtual lab at home to start studying how everything works. To see how I would do that you can take a look at this page here.

In the process I would start looking at some basic videos on networking, hacking, pen testing, Ruby and Python. I'd utilize SecurityTube (<http://www.securitytube.net/>) and YouTube for this. As my skills got better and my knowledge base expanded I would also expand on this home lab network as well so I could run more tests.

Step #3: I would get web application testing down

After I got pretty confident on how things work in my own home lab I would be looking for other web applications and networks to learn on. OWASP, the Open Web Application Security Project, has an awesome complete list of vulnerable websites that you can learn on. You can find that list here:



Page [Discussion](#)

Read [View source](#) [View history](#)

OWASP Vulnerable Web Applications Directory Project

https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project#tab=On-Line_apps

Step #4: I would become the go-to security guy

After I became more confident I would then proceed to utilize what I've been learning at my current position with permission.

After I got some basic fundamentals down or if I already had the fundamentals down I would let my manager know that I would be happy to evaluate the current security situation in my own time if he/she would allow me.

I would try to position myself as the security guy on the team and make it my responsibility to learn all that I could. This would get my resume looking pretty good when it comes to experience and allow me to get even more much needed experience.

Step #5: Get a mentor

If it weren't possible to get some experience at my current job, I would start by doing a cursory search of LinkedIn looking for people who are current penetration testers, security engineers or analysts, and reach out to them to do unpaid internships. I would let them know that I would help out in any way I could.

The great thing about LinkedIn is that the people that you find in your search will be 1st and 2nd connections to you, which is great as it will make it easier to connect to them and they are most likely in your area as well.

Some other searches to try:

IT Security Consultant
Information Security Engineer
Information Security Analyst
Information Security Auditor
Information Security Analyst

This internship could help you get your foot in the door at the company or at the very least you will gain experience that you can now put on your resume.



Step #6: Get certified in something

I would look at getting a certification to supplement the experience that I am getting. I would focus on **ONE** sought after certification that I am able to get based on my current experience and the experience requirements of the certification.

I would spend the rest of my time trying to gain that valuable experience that I need as nothing is going to replace it.

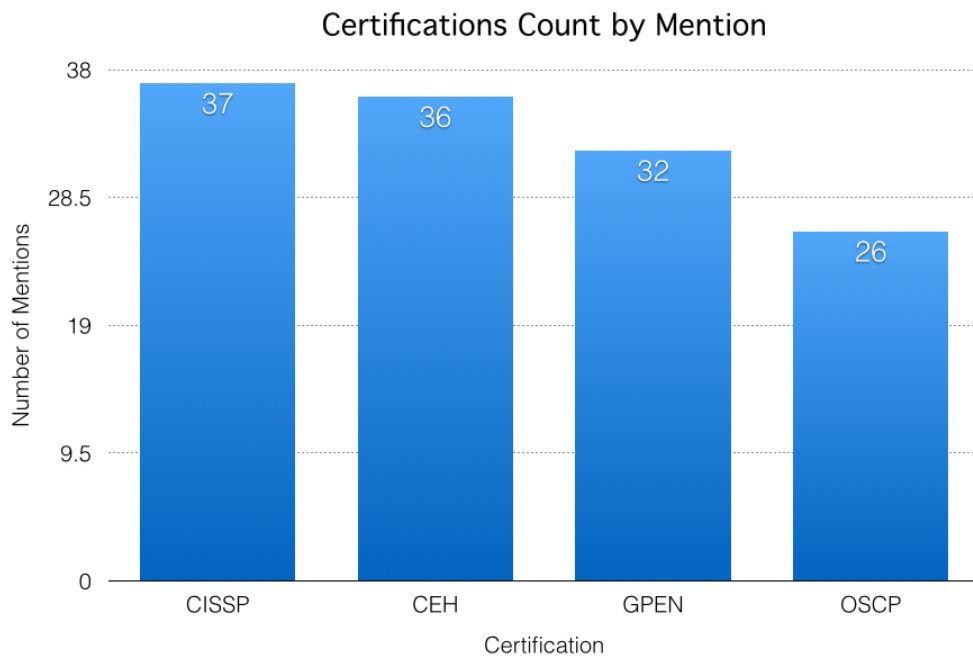
The four certifications that I would choose from at the beginning are the OSCP, CISSP, CEH or GPEN. This is completely my opinion and you probably have a different list.

Most penetration testers will tell you that a OSCP, CISSP, CEH OR GPEN certification will not make you a penetration tester, that only experience will, and that is absolutely true.

Only your experience and skill will make you a penetration tester. However, most wouldn't deny that companies actively make their interview/hiring decisions based on certifications. The four certifications were chosen based on my quick research online of job postings.

To see what certifications companies were looking for, I searched for penetration testing or info security jobs and looked at the first 50 that I came by.

Of course this isn't very scientific - I was only looking for the top 4 mentioned certifications and there should be a larger sample size - but I went with 50. The results actually surprised me but here they are:



If you do this test yourself you will get different results because of a different sample, but you will most likely see fairly similar results.

I did not expect the CISSP to be mentioned as often as it was for penetration testing positions, but it just goes to show how popular that certification is in the eyes of employers no matter what spectrum of IT Security you land on.

Some of you may argue that the OSCP certification is the best of these to get and I wouldn't argue with you. Again, this isn't scientific and I don't have an opinion at all, but this should give you an idea of what companies are looking for.

Of course there were other certification mentions such as the CCNA, but I decided to go with the top four mentioned here. I encourage you to take a look at these jobs and see what they are looking for as well.

Now, let's take a look at what the hit will be like for your wallet.

OSCP

| PENETRATION TESTING WITH KALI LINUX – DETAILED COURSE PRICING | |
|---|---------------|
| ONLINE TRAINING | LIVE TRAINING |
| Item | Price in USD |
| Penetration Testing with Kali Linux Online + 30 days Lab access + Certification | USD 800.00 |
| Penetration Testing with Kali Linux Online + 60 days Lab access + Certification | USD 1000.00 |
| Penetration Testing with Kali Linux Online + 90 days Lab access + Certification | USD 1,150.00 |
| PWK Lab access – extension of 90 days | USD 600.00 |
| PWK Lab access – extension of 60 days | USD 450.00 |
| PWK Lab access – extension of 30 days | USD 250.00 |
| PWK Lab access – extension of 15 days | USD 150.00 |
| Upgrade from PWB v.3.0 to PWK | USD 200.00 |
| Upgrade from PWB v.2.0 to PWK | USD 300.00 |
| Upgrade from PWB v.1.0 to PWK | USD 400.00 |
| OSCP – Certification retake | USD 60.00 |

CISSP



2015

| | CISSP Exam (6 Hours)* | CISSP- ISSAP/ISSEP/ISSMP (3 Hours)* |
|---|--------------------------|---|
| <i>Americas and all other regions not listed below</i> | | |
| Standard Registration | USD 599 | USD 399 |
| <i>Asia Pacific</i> | | |
| Standard Registration | USD 599 | USD 399 |
| <i>EMEA (Europe, Middle East and Africa)</i> | | |
| Standard Registration | EUR 520 | EUR 350 |
| United Kingdom: Standard Registration | GBP 415 | GBP 280 |
| Middle East: Standard Registration | USD 599 | USD 399 |
| Africa: Standard Registration | USD 599 | USD 399 |

CEH

| Live, Online, Instructor-led | Client-site | iLearn (Self-Paced) | Courseware Only (Self-Study) |
|---|---|---|---|
|  |  |  |  |
| \$2,895 | TBD | \$1,899 | \$825 |

Live, Online Instructor-Led

Live, Online courses delivered Live, Online by a Certified EC-Council Instructor! Courses run 8 am to 4 pm Mountain time, Monday thru Friday. Training Includes:

- Official Courseware
- iLabs, Online Labs (6 Months Access)
- Certification Exam Voucher
- Test Prep Program

Client-Site

EC-Council can bring a turn-key training solution to your location. Call for a quote. Training Includes:


- Official Courseware
- iLabs, Online Labs (6 Months Access)
- Certification Exam Voucher
- Test Prep Program
- Test Pass Guarantee

Courseware Only

We recognize that some folks have the background and experience to forgo training, so Official courseware is available for self-study. Click [HERE](#) to request the self-study exam application form.

Note: The exam is available through Prometric or VUE.com and runs \$500 with \$100 application fee.

GPEN

| | | | |
|----------------------|---------|----------|--|
| GPEN | \$1,099 | 4 months | Register Now  |
|----------------------|---------|----------|--|

Affiliate Pricing for GIAC Certification in conjunction with SANS training

Affiliate Pricing for GIAC Certification in conjunction with SANS training is \$629 (2015)

Affiliate SANS Alumni Pricing for GIAC Certification after SANS training

SANS alumni receive a discounted rate of \$949 for an exam attempt associated with a previously taken training course. For example, if you previously took SANS SEC401 (Security Essentials) through any of the SANS training venues, you will pay the affiliate \$949 alumni rate for the GSEC certification attempt.

The objective for us right now is to get to a point where we can get that experience, and these certifications are still some of the more popular certifications that a HR Manager at some company will be looking for.

We can educate ourselves on our own and we will, but other than our own hard work nothing will get you where you want to be quicker than being forced to learn at your day job.

Lets take a look at some experience requirements for these certs:

OSCP

Offensive Security Certified Professional – OSCP



DEMONSTRATES YOUR EXPERTISE IN PENETRATION TESTING TOOLS AND TECHNIQUES.

The Offensive Security Certified Professional certification (OSCP) is the accompanying certification to the **Pentesting with Kali Linux** course and is unique in its field in that it is the only security certification in the market that requires a fully "hands on" approach, leaving no space for multiple choice questions. The student is placed in a lab network with several vulnerable machines and points are awarded if a successful hack is performed. The student must demonstrate their depth of understanding by submitting both the steps they took to penetrate the box as well as the proof.txt file.

Note: you must complete the Kali Linux course first

[OSCP – LEARN MORE](#)

CISSP

CISSP® - Professional Experience Requirement

Requires years of experience

Do you have the proper experience for your CISSP credential?

You must have a minimum of five years of direct full-time security work experience in two or more of these 10 domains of the (ISC)® CISSP CBK®:

- **Access Control** – a collection of mechanisms that work together to create security architecture to protect the assets of the information system.
- **Telecommunications and Network Security** – discusses network structures, transmission methods, transport formats and security measures used to provide availability, integrity and confidentiality.
- **Information Security Governance and Risk Management** – the identification of an organization's information assets and the development, documentation and implementation of policies, standards, procedures and guidelines.
- **Software Development Security** – refers to the controls that are included within systems and applications software and the steps used in their development.
- **Cryptography** – the principles, means and methods of disguising information to ensure its integrity, confidentiality and authenticity.
- **Security Architecture and Design** – contains the concepts, principles, structures and standards used to design, implement, monitor, and secure, operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity and availability.
- **Operations Security** – used to identify the controls over hardware, media and the operators with access privileges to any of these resources.
- **Business Continuity and Disaster Recovery Planning** – addresses the preservation of the business in the face of major disruptions to normal business operations.
- **Legal, Regulations, Investigations and Compliance** – addresses computer crime laws and regulations; the investigative measures and techniques which can be used to determine if a crime has been committed and methods to gather evidence.
- **Physical (Environmental) Security** – addresses the threats, vulnerabilities and countermeasures that can be utilized to physically protect an enterprise's resources and sensitive information.

Note that if certain circumstances apply and with appropriate documentation, candidates are eligible to **waive one year of professional experience**:

CEH

In order to be eligible to attempt EC-Council CEH, CHFI v8 or ECSA v8 certification examination, candidate may opt to :-

> Attend Official Training

If a candidate attends an official instructor-led training (ILT), computer-based training (CBT), online live training, or academic learning, candidate is eligible to attempt the relevant EC-Council exam.

> Attempt Exam without Official Training

In order to be considered for the EC-Council certification exam without attending official training, candidate must:

- Have at least two years of information security related experience.
- Educational Background that reflects specialization in information security.
- Remit a non-refundable eligibility application fee of USD 100.00
- Submit a completed Exam Eligibility Application Form.
- Purchase an official exam voucher DIRECTLY from EC-Council through www.eccouncil.org/store.aspx

Notice that if you don't attend the official training you need to have experience.

GPEN

GIAC Penetration Tester (GPEN)

[View Professionals](#) →



Target

The GPEN certification is for security personnel whose job duties involve assessing target networks and systems to find security vulnerabilities. Certification objectives include penetration-testing methodologies, the legal issues surrounding penetration testing and how to properly conduct a penetration test as well as best practice technical and non-technical techniques specific to conduct a penetration test.

*No Specific training is required for any GIAC certification. There are many sources of information available regarding the certification objectives' knowledge areas. **Practical experience is an option;** there are also numerous books on the market covering Computer Information Security. Another option is any relevant courses from training providers, including [SANS](#).*

We can see that the CISSP certification requirement is heavy, so if you don't meet the experience requirements I would come back to it at a later date. I actually did that myself. I started with a couple others such as C|EH before later getting the CISSP. Another CISSP option is by becoming an associate and getting the experience along the way until you reach the requirements for the full certification.

After getting some certifications, I considered getting even more until I realized that it really just doesn't matter all that much. It is just my personal opinion that certifications should be used as a tool to get you where you need to be, but after you are there, experience alone is king.

It would be awesome if you got all of these certifications, but nothing beats having the right experience and that is now where I focus most of my time.

It is important however that you get a few certifications just to demonstrate your competency both from a job standpoint and client standpoint. At the end of the day though, clients and employers will primarily be looking for you to have relevant past experience of conducting these tests in the field.

Certifications are mainly good to get your foot in the door at a security firm so just pick one and run with it!

Step #7: I would Capture The Flag and take challenges

At Hack This Site (<https://www.hackthissite.org>) there are many free challenges that you can take. It doesn't get much better than that. I would start basic and work my way up from there. After I did a few of these I would move on to Capturing The Flag events.

At CTF Time (<https://ctftime.org/event/list/>) there are a ton of online and offline Capture The Flag events that you can be a part of.

When I felt my skills were up to the task I would try my best to be a part of a team and get involved in some of these events. For me this would be both a good time and give me the ability to practice in a scenario that is closer to "real-world".

Step #8: Look for entry-level positions

At the beginning I would be looking to get my foot in the door, understanding that I may take a hit on pay for a bit while I gain the much needed experience so that I can transition to another field.

If you truly see this as your passion you should be willing to take less in order to make a move into something you love and the money will follow. "Choose a job you love, and you will never have to work a day in your life." - unknown

People will always need and be looking for pentesters, so after you have gotten your experience, certifications etc. the employers will start looking for you rather than the other way around.

You will always feel as though you need more certifications, more experience and someone to knight you. You don't; just go get started and get into the industry.