Getting Into Information Security

"How do I get started in information security?"

- 10-Step Playbook

Primary Advice

1. **What do you want to do?** There is a wide variety of infosec-related trades, and though the path into any one of these roles may share some commonalities, there is no one-size-fits-all approach to becoming a cybersecurity professional. For this reason, the first thing I ask is - *Do you have an idea of what role specifically you'd like to pursue?* If you're not sure, don't worry! This is common for those new to the field. A little research into possible positions and titles is easy enough. To do so, I recommend perusing employment sites such as Monster, LinkedIn, SimplyHired, CareerBuilder or simply Googling what you are interested in. Within these job listings you should find not only the titles of potential jobs but also the sought-after skills and general qualities being asked of the respective applicants. During the course of this research, you may stumble across an abundance of job titles which resemble "Information Security Analyst" or "Cybersecurity Engineer". This sort of job-role-normalization is common but can be misleading as responsibilities for those who wield these titles are often far more specialized and nuanced than the description would have you believe. With that said, many of us in the field do indeed have responsibilities which are more *generalist* in nature but typically, entry-level positions will ask that applicants have a modicum of skill in a specific domain. In any case, some infosec domains/job titles you may be interested in can be seen here!
2. **Learning**. OK, so maybe you know what you'd like to do in infosec or maybe you don't - either way, you're likely going to need to learn some stuff. Across any specific infosec discipline, there are certain concepts or skills that will almost always be useful. I've created a list of these fundamental information security domains and would recommend those new to the field begin learning the basics of each. For diving into this list, Google is your friend - simply search for any of those concepts and how they apply to infosec. For a more targeted approach, there is of course a multitude of online resources available. For example, I maintain a list of various infosec-related resources. Even better, check out this massive list of training, both free and paid. If you'd like to read about *my* journey into infosec and beyond, I've catalogued this is great detail. Infosec is great in that you really can learn *just about* anything online - **for free**. Where you can't find it for free, it's probably available at a reasonable cost. The hard part is narrowing down exactly what you want to learn. But that's what also makes the field so exciting! To make this (hopefully) easier, I've put together a practical playbook which may help you begin your journey.
3. **Certifications**. In my experience, recruiters, hiring managers, other infosec pros (to some degree) and the infosec industry at large **love** certifications. Take for example, the CompTIA Security+ certification. The Security+ is a great entry-level cert which can not only demonstrate that you are serious about getting into infosec but it also is a great introduction to a lot of the foundational infosec concepts you will use throughout your career. I think the return on investment in getting this cert is well worth it (I in-

fact started out my infosec career with this cert so I can attest to its worthiness). The infosec field has countless certification and training offerings, you need only research what may be interesting to you. For those who are figuring out what certification or training to take next, I've personally reviewed a variety of certifications/training courses I have taken over the years. Some popular training vendors are listed below in this guide. Check out Paul Jerimy's awesome Security Certification Roadmap as well!

4. **The job search**. Job hunting with little-to-no actual relevant work-experience can be a disheartening exercise when many of the entry-level job descriptions you come across require applicants already *have* several years of experience. This is an annoying paradox of the infosec field - how can *entry* level positions ask for several years of experience! My advice is to apply to these (entry-level) jobs anyway! You may be surprised to find that hiring managers can be willing to take risks on a less-experienced but highly motivated candidate. It may also be that the job req was written in a way that was far more limiting then the hiring company intended, thus scaring away many potential qualified candidates. I would also recommend not to be afraid of taking an entry-level infosec position that may not exactly be what you you are primarily interested in. Certifications are great, but experience will always be king and getting that first job can be tricky. It is, in my experience, easier to find additional opportunities in the field after getting that first infosec position and getting that first crucial bit of experience on your resume.
5. **Professional networking**. This is as true for this field as it is for any other and I can't stress this enough - meeting people, talking with people and expanding your professional network is a great way to discover new opportunities. So create a ~~Twitter~~ Mastodon account, create a LinkedIn account, check out relevant sub-reddits (or this or this), join an infosec-related discord server or two, go to local meetups, engage with online communities, introduce yourself to your coworkers you don't normally interact with, go to career fairs, you never know where your next opportunity will come from. (To start, feel free to connect with me!)

Auxiliary Advice

- **About college degrees…** Do you need a computer science, IT or infosec-related degree to get a job in infosec? - The short answer is **no**. The long answer is that a degree can certainly help you stand out in the eyes of recruiters and hiring managers. It can give you a leg up on candidates who don't have one, it helps you bypass certain hiring filters (filters that would exclude non-degree-holding candidates) and of course the curriculum in a related degree program will likely be helpful in demonstrating experience and relevant knowledge to a prospective employer.
- **That first job**. Starting out in a help desk, software developer or other IT-related role (even if this role is not explicitly "information-security-related") is a common path for many infosec professionals. These jobs will give you valuable experience in the knowledge areas that are critical for infosec professionals. For example, as a software developer you will learn how to create awesome, functional code. Now let's say you want to pivot into being an application security professional. That previous experience learning to *write* code will be instrumental in you learning how to now secure that code. This same paradigm applies to all IT roles - including everything

from help desk (learning how to troubleshoot common problems with operating systems) to network engineer (learning to build, maintain and architect IT networks) to database administrator.

- Demonstrate and exercise your **passion**. This can be done in innumerable ways. Create a Github account and commit your own projects or contribute to others. Stand up a home-lab and practice networking, hacking or web development. Create a cloud account and learn about cloud architecture. Listen to infosec podcasts. Heck, create your own podcast! These are just a few ideas. What's important is that you embrace the field so when speaking with others (for example a recruiter or hiring manager) you can demonstrate your passion and skills which will help you stand out.
- **Join the community**. The infosec community is, I think in total, a friendly, thriving, and dynamic community. There are countless meetup groups, conferences, online forums and more that can be joined. Networking and learning from others in the community helps you accelerate growth and demonstrate your passion.
- **GOOGLE!** Just about everything you could want to learn is available online. With a little motivation, determination and will-to-learn, you can learn just about anything in infosec.
- **Spin up a "Homelab"**. You can get a lot of experience with enterprise-grade tools right from the comfort of your own home. Nessus, Splunk, Burp Suite and Snort are just a few examples of tools used in organizations that offer free or open-source versions of their software you can download and learn to use. Your homelab can serve as a place to hone these skills before ever even applying to your first infosec position.

Fundamental Information Security Domains

The domains below represent my take (generally) on the foundational knowledge areas for infosec professionals. You certainly do not need to be an expert in each but knowing as much as you can in each will ensure you are well-rounded.

- **Security Fundamentals** (e.g confidentiality/integrity/availability, risk management, least privilege, access control, defense-in-depth, etc…)
- **Scripting/Programming** (e.g. Python, Ruby, Powershell, Bash, Java, C, C#, etc…)
- **OS Fundamentals** (e.g. Linux, Windows, MacOS etc…)
- **Networking** (e.g. TCP/IP, Networking Protocols, Routing/Switching, etc…)
- **Web Applications** (e.g. HTTP, PHP, HTML, JavaScript, REST, SQL, etc…)

Resources

Learning to Google for things is probably the most valuable piece of advice I can give. With that said, I've compiled a list of (introductory) resources below which can help you get started on your infosec journey… I also maintain a more comprehensive list of infosec tools if you'd like to take things a step further. Finally, there is an amazing wealth of infosec content out there on the Internet. I'm making an attempt to index that content here.

Where to Learn Stuff

There are plenty of online training/learning sites. Below are some of my favorites. Check out this post for a more comprehensive list!

- Awesome Free Training List - This individual has been maintaining a pretty fantastic list of free resources, everything from training to podcasts.
- Stack Overflow - Can’t figure something out, stack’s got your back.
- YouTube - Believe it or not, tons of great instructional videos here.
- Cybrary - Free IT training.
- edX - Free online courses across a variety of disciplines.
- Pluralsight - Paid online video training but has a vast library of courses.
- Microsoft Virtual Academy - Free training from Microsoft.
- NIST Special Publications - Computer Security Resources from NIST (take a look at SP 800-53). Can be dry reading, but it will help you talk the talk.
- NIST CSF - The Cyber Security Framework. More reading from NIST.
- ioc.wiki

Stay Up To Date

Infosec is a fast-moving field. Keeping up to date on everything going on is a large part of being a successful infosec practitioner. The resources below can help you keep track of it all…

- Infosec.Exchange on Mastodon
- RSS - I like to use Feedly to manage my RSS feeds.
- Reddit - Front page of the internet and a great place for security news (and plenty of other stuff).
- Global CERTs/CSIRTs/ISACs
- Security Newsletters
- Talkback
- AWS Security Digest Newsletter

Check out this (massive) list of infosec blogs! I have an importable OPML file too if you’d like to go the rss route.

Learn to Code

Coding is **SUPER** important for security professionals. So go learn some!

- Github - Create an account, create code, share code and contribute to others code!
- W3Schools - Learn the web and how to develop.
- CodeSignal - Coding challenges, brought to you!
- Codeacademy - Free site to learn coding.
- Python.org - Official Python site.
- Official Python Tutorial - Python tutorial from python.org.
- Ruby - Official Ruby site.
- Rubyfu - Enhance your Ruby-fu.

- Bash Scripting Tutorials - Bash scripting tutorials.
- Free eBooks from Github - Free eBooks from Github.

OS Fundamentals

You're likely going to be using one or more OS'es to secure the same or other OS'es. In other words, you should probably learn about OS stuff.

- Windows Tutorials - Learn about Windows.
- Powershell - Do everything in Windows, from the CLI!
- Ubuntu - Popular open source workstation-class Linux distribution.
- Kali Linux - Download Kali, learn security tools, learn Linux.
- SS64 Command Line References - Assorted command line references.

Networking

Packets. Segments. Datagrams. Data. It moves from place to place and knowing how that happens is pretty useful.

- Nmap - Available in the Kali distribution - Learn network scanning and a little TCP/IP while you're at it!

Web Applications

The Internet. Ever heard of it? It's full of web apps!

- OWASP - First stop for all things web-app security.
- RFC 2616 - HTTP/1.1 - Learn more about HTTP/1.1.

Penetration Testing

Fancy yourself a Mr. Robot-type?

- VulnHub - Test your might against vulnerable VMs developed by the community.
- Metasploit Unleashed - Hacking tutorial by the guys at offsec.

Certifications

Certs. Love 'em or hate 'em, they can be helpful. I have a bunch of documented thoughts on certifications.

- CompTIA Security+ - Entry level certification but provides invaluable entry-level knowledge to the field of infosec.
- SANS - Fantastic cybersecurity training but very expensive.
- OSCP - Practical penetration testing training (and highly regarded certification in the industry).

- CISSP - Need to improve resume? This cert can often help.
- eLearnSecurity - Practical, hands-on infosec training. They have a great catalog of courses.

Cloud

The cloud is just someone else's computer right? Well if you're putting stuff on someone else's computer you should probably learn to secure it even better.

- AWS - Heard of the cloud? AWS can give you your own chunk of the cloud to play in.
- Azure - Microsoft is also in the cloud game.
- Google Cloud - Not to be outdone, Google. Also in the cloud.
- A Cloud Guru - I personally recommend this online training for learning more about the various cloud platforms. (It is a paid service!)

Infosec Podcasts

- The Shellsharks Podcast
- Getting Into Infosec - This is my favorite podcast recommendation for newcomers to the field.
- Black Hills Information Security - A great podcast with lots of technical stuff.
- StormCast - Podcast from SANS with daily information security news.
- Brakeing Down Security
- Security Weekly
- Defensive Security
- The Southern Fried Security Podcast
- OWASP Podcast
- Security Now!
- Purple Squad Security
- Hacker History

Online Communities

- Black Hills Information Security Discord
- Cyber Mentor DoJo Discord
- Cyber Study Cafe- Bishop Fox RedSec
- Cyberwox Academy Discord
- DEFCON Discord
- HackTheBox Discord
- InfoSec Community Discord
- Infosec Knowledge Sharing Discord
- InfoSec Prep
- InsiderPriDe
- Introduction to Coding/Hacking and CyberSecurity Discord
- Kali Linux Discord
- Laptop Hacking Coffee Discord
- netsecstudents Discord

- Offensive Security Discord
- OWASP Slack
- Porchetta Industries Discord
- Red Team Village Discord
- RedTeamSec Discord
- The Ruby Zoo Discord
- SANS Offensive Operations Discord
- Shellsharks Community Discord
- TCM Security
- Threat Hunter Community Discord
- TrustedSec Discord
- TryHackMe
- Wild West Hackin' Fest Discord
- Women Cyber Jutsu Slack

Other Getting Into Infosec Guides

Don't take it from me! Check out some of these other guides.

- How to Build a Cybersecurity Career - A prescriptive guide from Daniel Miessler.
- New To Cyber Field Manual from SANS
- Getting Started In Information Security - Thoughts on getting into the field from Endgame.
- How to Get Into Cybersecurity Regardless of Your Background - A guide for all, from Springboard.
- Infosec Newbie - A collection of resources, courtesy of mubix.
- How to Get Into Information Security - A guide from the guys and gals over at Black Hills Information Security.
- Getting Started in Cybersecurity with a Non-Technical Background - A guide from the one and only SANS.

Getting Into Infosec Playbook

If you've read this piece in its entirety and are still thinking, "*now what do I do?*" I've provided a short, practical, step-by-step guide to getting started below. The goal of this playbook is to get you the highest value introductory skills and other *stuff* to put on a resume, *and into your brain*, to help you break into the cybersecurity field. Though it will vary from person to person, and depends on the depth in which you approach each of the items below, I estimate you could get through all of these in a meaningful capacity in 1 week. Yup! From *zero* to *good-looking-resume* in just a **single week**!

1. **Establish**: Tell the world who you are, what you do and how you can help. Personally, I think a blog or site is the best way to express your self. Getting started with blogging is easy and there are *plenty* of ways to do it. Don't worry about having the perfect look, niche, content, or any of that quite yet. Just getting something out there will help you build momentum. *It does take a little bit of work though*, so for an easier path to establishing your identity, simply create a Linkedin and/or Mastodon account (I recommend creating a separate, "professional"

Mastodon identity)! Having this identity helps you build a historical record of your contributions to the field while also helping others learn who you are and where else they can find you on the Internet and in the world.

2. **Connect**: Alright, so you should now have some professional, social real-estate. It's time to get out there and meet others in the industry. One easy way to get started is to simply connect with me Mastodon ! Don't be afraid to just message people, connect, follow, w/e - that's what these sites exist for. Beyond social media, try checking out the variety of online communities which provide (near) real-time opportunities to chat, ask questions and grow your network. I even have a Discord server that you are more than welcome to join! Networking has and might always be the best way to find opportunity.
3. **Update**: The world of infosec is pretty dynamic. New tools, breakthrough research, zero-days, breaches, you name it. I find that an RSS system, some Podcasts and a sprinkling of Mastodon is a great way to learn, find inspiration and never miss a thing. Check out the embedded links for getting started.
4. **Code**: I see a lot of people ask, "*do I need to know how to code to get into infosec?*" The short answer is "not really", but the better answer is - *give it a shot!*. Learning to do some basic scripting is really easy and doesn't require you to even understand all of the complexities that may be introduced to you in a formal computer science curriculum. More importantly, having a basic understanding of how to do some coding/scripting will undoubtedly make you a more attractive candidate.

   So learn a *little bit*, create a Github account, commit literally whatever you have written, add your Github account to your resume and **profit** from having done really not that much work.
5. **Cloud**: No way around it, understanding the "cloud", specifically platforms like AWS, Azure and GCP is increasingly important for modern IT/infosec professionals. What's awesome is that getting started with these platforms is incredibly easy! You can create a free AWS or Azure account and both Amazon and Microsoft offer free training! It doesn't take long at all before you have real, practical experience and something to throw on your resume.
6. **Tooling**: The infosec industry is dominated by tools. Having *documented* experience with these tools helps you land a job and will likely help you succeed *in* that job. You can learn about what tools are in use at a given company or in a particular role by searching open job reqs (Tip #1). From there, you can (typically) find the free or open-source-alternative version of those tools, download/install them (in and lab environment) and get experience with them in the comfort of your own home! Before too long, you'll have *enough* know-how to not only put it on your resume, but speak to it somewhat intelligibly in an interview setting. How's *that* for leveling up!
7. **CTFs**: In the spirit of *easy* things to do that will help you get quick experience and valuable bullet points for your resume - try participating in a CTF! CTF Time is a great resource for finding CTFs, SANS Holiday Hack Challenge has years worth of awesome, interactive challenges and platforms like Hack The Box provide live hacking targets to practice and level up your skills. IPPSEC has a great resource for write-ups that can help you with your CTF-ing. I even have a few write-ups if you're interested!
8. **Train**: Training and self-study will help you fill in gaps and gain domain-specific depth/breadth. There are countless resources for training - try not to focus too much

on what resources are best and just dive in. If a particular resource is not working for you, try something else out! If all else fails, getting a cert (like the Sec+) is always a good way to boost the resume. For more on what cert you should take or detailed thoughts on certs/trainings I have taken, check out this piece.

9. **Resume**: *Alright*! We've come pretty far now, time to put a bow on the package that is you - as *you* are what you present to prospective employers (not just your "resume"). Here I've provided my (somewhat modified) resume as a template you can use. Simply remove the stuff about me and replace it with stuff about you! Feel free to take out things you don't have (i.e. if you didn't create a blog or haven't gotten a certification yet). Remember to include your professional social identities, your Github portfolio, mention your cloud knowledge, your tools experience, the CTFs you've participated in and any relevant trainings you've taken and what skills you may have gained from said trainings.