Classification: PROTECTED

Hey!

So, starting in security can be really overwhelming, there’s so many resources and disciplines in security… Here’s a bunch of links and info to help you get started. Before I start, there is a community driven versions of this that does a great job of answering the “How do I even start in security?” question. [Infosec Reference](https://github.com/rmusser01/Infosec_Reference), [Infosec Newbie](https://gist.github.com/mubix/5737a066c8845d25721ec4bf3139fd31), [Infosec Getting Started](https://github.com/gradiuscypher/infosec_getting_started), [Security Compendium](http://www.securityramblings.com/2016/01/breaking-into-security-compendium.html), and [Vulnhub Resources](https://www.vulnhub.com/resources/" \t "_blank). Also, two books I can’t highly recommend enough are [The Tao of Network Security Monitoring](https://www.amazon.com/Tao-Network-Security-Monitoring-Intrusion/) and/or [The Practice of Network Security Monitoring](https://www.amazon.com/Practice-Network-Security-Monitoring-Understanding). These were recommended to me when I first started in security and are eye opening reads. (if you know where to look, I'm sure you could find these online for free!)

**Github**  
Bro’s have put together “awesome lists” using github, they are just massive community curated lists of tools and resources similar to this email!

[awesome-security-feed](https://github.com/mrtouch93/awesome-security-feed) - EASILY ONE OF THE BEST aggregated lists of security news, tools etc. Does a better job than me.  
[awesome-security](https://github.com/sbilly/awesome-security)  
[awesome-incident-response](https://github.com/meirwah/awesome-incident-response) – FANTASTIC!  
[SecLists](https://github.com/danielmiessler/SecLists) - A list of security lists  
[awesome](https://github.com/sindresorhus/awesome) - A list of lists  
[awesome-awesomeness](https://github.com/bayandin/awesome-awesomeness) - Another list of lists  
[awesome-hacking](https://github.com/carpedm20/awesome-hacking)  
[awesome-web-security](https://github.com/qazbnm456/awesome-web-security)  
[A-Good-Cyber-Security-List](https://github.com/emtuls/A-Good-Cyber-Security-List)  
[lists](https://github.com/jnv/lists) - List of lists  
[Security\_list](https://github.com/zbetcheckin/Security_list) - Another list of lists  
[The Art of a Hacker](https://github.com/The-Art-of-Hacking/h4cker) - FANTASTIC!  
[Awesome Infosec](https://github.com/onlurking/awesome-infosec)  
[Awesome Malware Analysis](https://github.com/rshipp/awesome-malware-analysis)

**Industry & Connections:**  
It’s important to get yourself immersed in the New Zealand security community. Set up a [LinkedIn](https://linkedin.com/), attend the [1st Tuesday](https://twitter.com/1sttuesdaynz),[NZISIG](https://isig.org.nz/). [NZISF](https://security.org.nz/about-nzsa/nzisf/) meetups. Attend[Kiwicon](https://www.kiwicon.org/), [BSides](https://www.bsides.nz/" \t "_blank), [OWASP](https://www.owasp.org/index.php/OWASP_New_Zealand_Day_2018) conferences. It’s vital to make connections and soak up as much knowledge as you can.

**Certifications & Courses:**  
Here's the list of common certifications that are always recommended.

[Blueteamsacademy](https://www.blueteamsacademy.com/) - One of the best free resources online for learning  
[CCNA](http://www.cisco.com/web/learning/certifications/associate/ccna/index.html)  
[CCNA Security](http://www.cisco.com/web/learning/certifications/associate/ccna_security/index.html)  
[Security+](http://certification.comptia.org/getCertified/certifications/security.aspx)  
[Cybrary](https://www.cybrary.it/) - Possibly one of the best IT Security education sites on the internet.  It contains full-length college course videos for everything from basic networking up to and including training for certifications, explanations of secure coding, penetration testing and everything else security related. The majority of it is free.  
[Udemy](https://www.udemy.com/courses/search/?ref=home&src=ukw&q=security) – Provides cheap and amazing courses and lectures on all security domains.  
[StationX](https://www.stationx.net/) – Similar to Udemy   
[Netresec.com](https://www.netresec.com/?page=PcapFiles) - Packet capture exercises  
[Malware-traffic-analysis.net](https://www.malware-traffic-analysis.net/) - Malware pcap exercises

**Tools we use on a daily basis that you can set up for free on a home lab:**  
Data analytics: [Splunk](https://splunkbase.splunk.com/develop/), [Kibana (ELK)](https://www.elastic.co/webinars/introduction-elk-stack), [Gray Log](https://www.graylog.org/)  
Scripting: [Python](http://learnpythonthehardway.org/book/), [Bash](https://learnxinyminutes.com/docs/bash/), [Perl](https://www.perl.org/books/beginning-perl/)  
Scanning Tools: [Nmap](https://nmap.org/), [Nessus](https://www.tenable.com/products/nessus-home), [OpenVAS](http://www.openvas.org/), [Security Center](https://www.tenable.com/products/securitycenter)  
Packet Analysis: [Wireshark](https://www.wireshark.org/),  [tcpdump](http://www.tcpdump.org/" \t "_blank)  
Other Tools: [MobaXterm](http://mobaxterm.mobatek.net/" \t "_blank), [Notepad++](https://notepad-plus-plus.org/)  
Intrusion Detection: [Snort](https://www.snort.org/), [Suricata](https://suricata-ids.org/), [BRO](https://www.bro.org/)  
SIEM: [Splunk ES](https://www.splunk.com/en_us/software/enterprise-security.html), [IBM Qradar](https://www-01.ibm.com/marketing/iwm/iwm/web/reg/download.do?source=swg-qradarcom&S_PKG=ov60294&lang=en_US&cp=UTF-8), [AlienVault](https://cybersecurity.att.com/products/ossim)  
Threat Hunting: [GRR](https://github.com/google/grr), [OSQuery](https://osquery.io/" \t "_blank)   
  
**Tool Lists:**[ToolsWatch.or](https://www.toolswatch.org/)  
[Network Security](http://seclist.us/)  
[KitPloit - PenTest Tools!](http://www.kitploit.com/)  
A Complete Penetration Testing & Hacking Tools List for Hackers & Security Professionals - LEGENDARY REDDIT POST

**Other tools which are free or open source:**  
Open source Snort based Intrusion detection Systems (IDS): [Bro](https://www.bro.org/), [Security Onion](https://security-onion-solutions.github.io/security-onion/), [OSSEC](http://ossec.github.io/),  
Free Snort rules: [Emerging Threats](https://rules.emergingthreats.net/)  
Open source SIEM’s (Security information and event management ):   [Alienvault](https://www.alienvault.com/" \t "_blank), [Kibana (ELK)](https://www.elastic.co/webinars/introduction-elk-stack), [Gray Log](https://www.graylog.org/)  
Open source IDS/IPS NSM (Network Security Monitoring): [Suricata](http://suricata-ids.org/)  
Open source penetration testing Linux Distro’s: [BackTrack](http://www.backtrack-linux.org/" \t "_blank) , [Kali Linux](https://www.kali.org/) , [Cyborg Hawk](http://cyborg.ztrela.com/) – These contain hundreds of tools preinstalled and configured.  
Open source penetration testing tools/frameworks/scanners: [Metasploit](http://www.metasploit.com/), [Burp](https://portswigger.net/burp/download.html), [OpenVAS](http://www.openvas.org/)  
Commercial penetration testing tools/frameworks/scanners: [Netsparker](https://www.netsparker.com/web-vulnerability-scanner/" \t "_blank), [Acunetix](http://www.acunetix.com/" \t "_blank), [Qualys](https://www.qualys.com/enterprises/qualysguard/web-application-scanning/)  
I would highly recommend setting up a homelab and play around with these tools, a low cost solution could be a cheap VPS (virtual private server). I would recommend [Ramnode](https://www.ramnode.com/vps.php" \t "_blank), who offerings which start at $15 USD per year. Or alternatively use old hardware you might have spare, or just use [Vmware Player](https://www.vmware.com/products/player" \t "_blank) or [VirtualBox](https://www.virtualbox.org/) and set up a virtual machine. Buying a ex-lease low spec box from [PBTech](https://www.pbtech.co.nz/category/computers/exleased/desktop-pcs" \t "_blank) and running a free hypervisor like [vSphere](https://www.vmware.com/products/vsphere-hypervisor.html) community edition.  
Familiarize yourself with a Unix terminal, basic navigation and searching of files. Start by downloading and installing [Ubuntu](http://www.ubuntu.com/download). [Ubuntu tutorials](https://ubuntu-tutorials.com/)

**Learn a scripting language:**  
like [Perl](https://www.perl.org/) or [Python](https://www.python.org/). [Learn Perl](http://learn.perl.org/), [Learn Python](http://www.learnpython.org/)

**Great reading:**[How to write a great cybersecurity resume](https://cvcompiler.com/blog/how-to-write-a-great-cybersecurity-resume/)  
[The First Steps to a Career in Information Security (Errata Security - Marisa Fagan)](http://blog.erratasec.com/2010/04/first-steps-to-career-in-information.html#.WFrbofkrIuU)  
[How to Start a Career in Cyber security](https://www.concise-courses.com/security/how-to-start-your-career/)  
[How to Get Into Information Security (ISC^2)](https://www.isc2.org/how-to-get-into-information-security.aspx)  
[How do you begin an information security career (SC Magazine - Israel Bryski](https://www.scmagazine.com/how-do-you-begin-an-information-security-career/article/558803/)  
[Starting your career in information technology (Tripwire - Zoe Rose)](https://www.tripwire.com/state-of-security/off-topic/starting-your-career-in-information-technology/)  
[How to start your information security career? (Adriano Leite)](https://www.linkedin.com/pulse/20140825234615-654073-how-to-start-your-information-security-career)  
[Starting in Information Security](https://www.eanmeyer.com/2015/07/starting-in-information-security.html)  
[Starting an Infosec Career](https://tisiphone.net/2015/10/12/starting-an-infosec-career-the-megamix-chapters-1-3/)  
[Breaking in to security](https://digi.ninja/projects/breaking_in_part_1.php)   
[Simplycyber.io/](https://www.simplycyber.io/free-cyber-resources) - Massive List of Free Cyber Security Resources

**Security news sources -**Make sure you keep up to date with the latest in industry news:  
[SANS ISC](https://isc.sans.edu/) – Information, news, podcasts and blogs.  
[Krebs On Security](https://krebsonsecurity.com/about/) – Excellent blog and security news resource.  
[Schneier On Security](https://www.schneier.com/blog/about/) – Another great blog on security news and topics.  
[SANS Security Blogs](https://www.sans.org/security-resources/blogs)  
[Risky.Biz](http://risky.biz/) – Australia/NZ security podcast.  
[Paul’s Security Weekly](http://securityweekly.com/) – US security podcast.  
[Threatpost](https://threatpost.com/) – Industry news.  
[The Register](http://www.theregister.co.uk/security/) – Industry news.  
[ZDNet](http://www.zdnet.com/topic/security/) – Industry news.  
[Bleeping Computer](https://www.bleepingcomputer.com/news/security/) – Industry news.  
  
**Subreddits:**  
[/r/Pentesting](http://r/Pentesting)  
[/r/Homelab](https://www.reddit.com/r/homelab/)  
[/r/Information\_Security](https://www.reddit.com/r/Information_Security/)  
[/r/Security](https://www.reddit.com/r/security/)  
[/r/netsec](http://www.reddit.com/r/netsec)  
[/r/compsci](https://www.reddit.com/r/compsci/)  
[/r/netsecstudents](http://www.reddit.com/r/netsecstudents) – They have an AMAZING wiki on how to get started in Security @ [here](https://www.reddit.com/r/netsecstudents/wiki/index#wiki_where_to_start) and [here](https://www.reddit.com/r/netsecstudents/wiki/resources).  
[/r/blueteamsec](https://www.reddit.com/r/blueteamsec/) - THE BEST SECURITY OPERATIONS REDDIT EVER  
[/r/SecurityBlueTeam](https://www.reddit.com/r/SecurityBlueTeam/)  
[/r/computerforensics](https://www.reddit.com/r/computerforensics/)

[/r/sectraining](https://www.reddit.com/r/sectraining/)

[/r/deepweb](https://www.reddit.com/r/deepweb/)  
[/r/ReverseEngineering](https://www.reddit.com/r/ReverseEngineering/)  
[/r/SocialEngineering](https://www.reddit.com/r/SocialEngineering/)  
[/r/computerforensics](https://www.reddit.com/r/computerforensics/)  
[/r/HowToHack](https://www.reddit.com/r/HowToHack/)

Looking forward to talking soon.

Thanks,

|  |  |  |
| --- | --- | --- |
| **Julian Garthwaite**  Head of Cyber Detect & Respond  Cyber Security / ISG Mob:   +64 27 306 5361 | | |
|  | Westpac New Zealand Limited Level 7SS, 16 Takutai Square Auckland Central, 1010 |  |