**Resources List for Beginners 2021**

Here is my recommended starting point:

* A great place to start if you're a complete beginner is TryHackMe (https://tryhackme.com/), which provides you with an attack machine and hands-on tutorials on a variety of topics

Some of the rooms require a paid subscription, but the beginner ones are free. If you're interested in pen testing, a great place to start would be their offensive pentesting track: <https://tryhackme.com/path/outline/pentesting>

* If you’re interested in ***defence*** and administration, here are a couple things to get you started:
  + <https://www.youtube.com/playlist?list=PLqux0fXsj7x3WYm6ZWuJnGC1rXQZ1018M> ⇒ although it’s for the cyber games competition, it goes over how a lot of very important services work as well as how to setup/configure them, including things to think about from a defensive perspective
  + <https://www.youtube.com/watch?v=o42dgCOBkRk> ⇒ a lot of this may not be applicable to the industry since large companies use paid software like SIEMs to monitor their networks. However, it’s a great showcase of what’s out there if you don’t have them at your disposal, especially for use in cybersecurity competitions
* If you’re interested in ***offence***, another way to go would be to check out the Zero to Hero Pentesting streams on YouTube provided by The Cyber Mentor: <https://www.youtube.com/watch?v=qlK174d_uu8&list=PLLKT__MCUeiwBa7d7F_vN1GUwz_2TmVQj>. While TryHackMe focuses on specific tasks hands-on, this videoseries gives a more comprehensive overview of many aspects of pentesting with live demos. The Cyber Mentor also has a separate series for web attacks if that's something you're interested in: <https://www.youtube.com/watch?v=ZBi8Qa9m5c0&list=PLLKT__MCUeixCoi2jtP2Jj8nZzM4MOzBL>.

Once you've gotten your feet wet, here are additional resources to help you out along the way:

* Here's a comprehensive overview of cybersecurity resources I've used: <https://docs.google.com/document/d/1USipV0CtxLibqxJ3xJL2-5_yuJXb-q_CUnL6N4cKt3g> (this document). If there's something specific you're interested in, you'll likely find it there or feel free to reach out to me at any time! I also run an emailing list, and anytime I'm working on something cool that's pentesting related, I send out an email about it. Let me know if you'd like to be added to that by emailing [jford11@hawk.iit.edu](mailto:jford11@hawk.iit.edu).
* It's nearly impossible to remember all the commands you'll need during a pentest. That's why I've put together a Kali commands cheat sheet: <https://docs.google.com/document/d/1MYIUJ-HvIDI1A8RPldMEcrVAOQzABeT_E0yaaN8rKKs>. It's organised by attack stage with clickable links for each section, so although 65 pages long, it should be pretty easy to navigate!
* Check out our unofficial (run by me and another exec member) CyberHawks YouTube channel: <https://www.youtube.com/channel/UCuYP-AZUcHEZMmUyb1MpZyw>. You'll find a lot of cool stuff on there, especially in the Illinois Tech Cyber Challenge Competition playlist intended for beginners. All the videos from our website are on there and more! For example, I do an in-depth look into Metasploit here: <https://www.youtube.com/watch?v=QSTInIeuVTI&list=PLSpsCUl2cY8a1DTONY5pQa1aAK_RdrfvL&index=8>.

To be added to this document:

* <https://pwn.college/>
* <https://www.root-me.org/>
* <https://www.abatchy.com/2017/03/how-to-prepare-for-pwkoscp-noob>
* [https://docs.google.com/document/d/100O1KszmoTufqHwHxY\_ZKux4JfejieIM\_kQ8tMUzfmM/](https://docs.google.com/document/d/100O1KszmoTufqHwHxY_ZKux4JfejieIM_kQ8tMUzfmM/edit?usp=sharing)
* [https://docs.google.com/document/d/1BbYJhduq0b3pEWsuWsqqtoMPlYH-SASrU8kwzdT9yeI/](https://docs.google.com/document/d/1BbYJhduq0b3pEWsuWsqqtoMPlYH-SASrU8kwzdT9yeI/edit?usp=sharing)
* <https://docs.google.com/document/d/1vJxoHrjW607NJDLC1Zln1llrEIqrS6Ea3j9ihJTdblg/edit?usp=sharing>

**Comprehensive Resources Email 2019**

As promised, this email should provide you with some resources you may find helpful for getting started with cybersecurity. For those of you who were unable to make it to the seminars, [here](https://docs.google.com/presentation/d/1quKoExucVwVWacmhDGjbfqGaQUtf_qqeFa5hWGCKIk8/edit?usp=sharing) is a link to the presentation. It details all you need to know about setting up an environment in which to practice your attacks. It will be updated with topics covered throughout the seminar series.

When it comes to learning the entirety of the process of cybersecurity, especially server-side exploits, I think it best to watch tutorials on how to break into specific machines as well as attempt to break into them yourself. For this, I recommend seeing what you can find on [VulnHub](https://www.vulnhub.com/resources/), especially in its “Custom Personal Targets” section, which contains collections of individual VMs for you to download and attempt to exploit yourself. Of these, one of the most popular that I have looked into is [HackTheBox](https://www.hackthebox.eu/individuals), which contains a number of cybersecurity-related challenges. If you are ever stuck on one of these or don't know where to start, Google it! Many of the more basic boxes (target machines) have video tutorials on YouTube that go along with them. Some channels worth checking out are [HackerSploit](https://www.youtube.com/channel/UC0ZTPkdxlAKf-V33tqXwi3Q), who additionally has a video series in "Ethical Hacking and Penetration Testing" that might be good, though I haven't had the chance to check it out, and [IppSec](https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA), who posts lots of walkthroughs of practice boxes. Be sure to see how a variety of people go about breaking into such boxes, because each individual brings their own knowledge and set of tools to the table, and the more you are exposed to, the more potential avenues you have for going about an attack. I know [NetSecNow](https://www.youtube.com/user/NetSecNow/featured) has a number of good videos as well, including an "Ethical Hacking - Hacking For Fun And Profit!" playlist.

Shoutout to Przemek Warias for introducing me to [TheCyberMentor](https://www.youtube.com/channel/UC0ArlFuFYMpEewyRBzdLHiw), who provides courses on pen testing and especially privilege escalation: he has two Udemy courses on this. A great starting point for getting into pen testing is his free YouTube [Zero to Hero Pentesting course](https://www.thecybermentor.com/zero-to-hero-pentesting). I haven’t gone through the whole thing myself, but what I have looked at has been very helpful and filled a lot of holes in my knowledge.

If you want to understand how exploits (the actual portions of code used to break into a machine) are written and work on the lowest level, I highly recommend LiveOverflow's [Binary Hacking Course](https://old.liveoverflow.com/binary_hacking/index.html), which walks you through the creation of exploits for vulnerabilities found in the [Protostar](https://exploit-exercises.lains.space/protostar/) exercises. The course is only an overview, and there will be times at which you will have to do your own independent research, especially for heap exploits, but it will provide you with a solid foundation to build off of while completing the exercises. My solutions to these exercises can be found [here](https://github.com/TheCatLover/Protostar-Solutions). Familiarity with debugging code in a number of languages, mostly C, Python, and Java, is very helpful in this, as is experience with Assembly (but don't worry if you don't have that because I didn't). In fact, being able to understand, debug, and analyse code in a variety of languages is crucial to the exploitation of server-side attacks, the core of hacking, because you will often find community exploits that need to be modified in order to work correctly for the specific machine you are targeting under the specific circumstances. There are a number of sites for finding community-released vulnerabilities, but probably the most useful one is [exploit-db](https://www.exploit-db.com/). In Kali Linux OS, one of the two most widely-used penetration testing specific Operating Systems along with Parrot OS, exploit-db exploits can also be searched via the [searchsploit](https://www.exploit-db.com/searchsploit) command.

Other topics not covered above include wireless attacks, sniffing and spoofing, hash cracking, and client-side attacks. For these, I recommend looking up YouTube videos (you'll notice that Google and YouTube are my go-to), and I'll provide some keywords here to get you started:

Wireless attacks, or attempting to gain unauthorised access to wireless access points such as routers, are boring plugging and chugging of commands. Honestly, for most of these, you can look at the commands in the cheat sheet I linked below, though it's good to get an understanding of what they are doing. The two types of security encryption are WEP, which is extremely vulnerable but still in use, and WPA/WPA2, which is safe under most circumstances but can be bruteforced, especially when WPS is enabled. To learn about these, I would search something along the lines of "Kali Linux WEP" or "Kali Linux WPA" and you'll find plenty of good resources. Another attack worth checking out here is the Evil Twin access point attack, in which the attacking machine acts as a duplicate of the router and forces all other machines off of the actual router so that they automatically reconnect to the attacking machine instead. MAC address spoofing is a type of wireless attack in which the attacking computer changes its unique identifier (MAC address) in order to resemble another machine on the network. This is useful in situations where public Wi-Fi is only available to certain users, usually those who pay for it, because it allows an attacker to pretend to be one of these users, granting unauthorised access to the internet.

Sniffing and spoofing is primarily comprised of data sniffing to reveal passwords or other sensitive information, which may or may not make use of man in the middle attacks (attacks in which two end computers, one of which is the target, communicate to each other through the attacking machine). A popular man in the middle attack is ARP poisoning, in which the attacking computer poses as the router and routes all traffic to and from other computers in the network through it, allowing for the retrieval and tampering of data. How this is done really depends on the tool you're trying to use. I familiarised myself with Man in the Middle Framework (mitmf), but this is now outdated due to having been replaced by more high-end tools such as BetterCAP, which I have yet to look into. All wireless data is transmitted in packets, and each packet abides by a communication protocol. Probably the most well-known data packet sniffing tool is [Wireshark](https://www.wireshark.org/#learnWS). It can be used to see all data packets transmitted over a network interface, whether that interface is wired or wireless. Sniffing such data is called "capturing" it, and Wireshark has useful capture filters (filters for specific keywords or packet attributes applied during the capture) and display filters (filters for specific keywords or packet attributes applied to data viewed after the capture has been completed).

Hash cracking is a whole topic in and of itself, but it comes up in so many other areas that I don't recommend focusing studies on it per se unless you're interested explicitly in cryptography and hashing (the real math-heavy stuff). For example, breaking into WPA/WPA2 security may require hash cracking in the bruteforcing of the WPA/WPA2 key. Obtaining the plaintext of a password found after "dumping hashes" on a compromised machine or sniffing on a network will require some sort of hash cracking method. The two most useful tools for hash cracking, in my opinion, are [John the Ripper](https://github.com/magnumripper/JohnTheRipper) and [hashcat](https://hashcat.net/hashcat/).

Client-side attacks (attacks targeting users of the machines rather than the machines themselves) include the phishing attack, which I will demonstrate in the next seminar using the [social engineering toolkit](https://github.com/trustedsec/social-engineer-toolkit) and various methods of delivery and execution of malware. This includes the previously-mentioned ARP poisoning and more specifically script injection, something very much worth checking out, as well as any creative ways you can think of that can fool the target into downloading and executing a file. There are a variety of different tools that aid in this, whether that be [veil evasion](https://github.com/Veil-Framework/Veil-Evasion) for bypassing antivirus and faking updates or email spoofing with an external mail server such as [smtp2go](https://www.smtp2go.com/). When it comes to client-side attacks, it's important to know about the individual you are targeting, and there are many good tools for gathering this sort of information, the most popular one being [Maltego](https://www.maltego.com/product-features/), which allows you to conveniently search through social media accounts and online mentions.

If you're interested in learning how to write your own malware that can evade antivirus, there are two primary considerations: bypassing static/signature analysis (AV looks at the actual contents of the code) and dynamic analysis (AV runs the code in a sandbox environment to see what it does). For learning how to bypass dynamic analysis, I found [this](https://wikileaks.org/ciav7p1/cms/files/BypassAVDynamics.pdf) to be by far the best resource. For bypassing static analysis, feel free to look up how to write your own crypter. There are many good methods for doing this, including [this one](https://blog.sevagas.com/?Code-segment-encryption). There are also a number of advanced AV evasion techniques that I will not discuss here because I have yet to learn them, but I will come back in and update this doc when I do <https://www.youtube.com/watch?v=8lk6VhmlhoI>\*\*\* [Virustotal](https://www.virustotal.com/) is one of the most popular methods of checking the code you write against the most common antivirus engines, but beware that this will distribute the results directly to the antivirus companies, so your malware will not stay undetectable for long. Aside from AV evasion, the rest of the malware depends on what you want it to do. Most of this entails writing code to automate other things you'd normally do yourself as a pentester, such as escalating privileges and post exploitation.

A vast majority of server vulnerabilities can be found on server websites, making web exploitation a key part of the exploitation process. In terms of web exploitation, the most common types of attacks are file inclusion vulnerabilities, command/code execution vulnerabilities, cross-site scripting, and SQL injections. Searching up any of these terms along with keywords such as "tutorial" or "Kali Linux" will yield plenty of instructional videos on the subject.

If you are willing to pay a price for your learning, you can't go better than Offensive Security's official [Pen-testing With Kali (PWK) course](https://www.offensive-security.com/pwk-oscp/), which provides you with written and video demonstrations of attacks, a virtual lab network to practice your penetration testing skills, and an optional Offensive Security Certified Professional (OSCP) 24-hour certification exam that is seen by many employers as the equivalent of a college degree in cybersecurity. Mind you, few pass it on their first try, and I failed my first and only attempt. The PDF provided in the course is exceptional. It details many of the various tools provided in Kali and is undoubtedly one of the best cybersecurity resources I have. Unfortunately, I cannot share it with you unless you purchase the course due to copyright restrictions.

Lastly, it's nearly impossible to memorise all the commands needed to break into a machine, so I created a [Kali Linux Cheat Sheet](https://docs.google.com/document/d/1SH06nkyrDmV0TPZMcuNOQZvYJeRSqZ5yk8MVQEbS5SY/edit?usp=sharing) that is my go-to for just about any scenario and that I highly recommend checking out. I additionally attached my bookmarked pages from research I have done over the years to this email, and you should be able to open it with any web viewer, but I don't entirely remember all the sites that are on there.

If you have trouble viewing the links in this email, please let me know. I realise this is a lot of information, but I hope it provides you with a good starting point from which to expand your knowledge-base. I wish you all the best of luck in your hacking endeavours! If you are interested in client-side attacks such as phishing and email spoofing or bruteforce attacks, come join me for my next seminar. I will send details about the exact time/location at some point down the line. If you have any further questions about anything or would like more focused information on a specific cybersecurity topic, feel free to reach out to me, and I'd be glad to help in any way that I can.

Cheers,

John Ford