So You Want to be a Mentor: Taking Someone from Noob to Knowledgeable

# Overview

This is intended to be a framework; there are almost certainly gaps in the knowledge base here and some things will change over time. I have set this up on github as noob2knowledgeable. I’d also like to invite anyone using it to let me know how it went with someone you’ve mentored as well as to help me correct, flesh out and update it as time goes on. I can be contacted at [nmoore9041@gmail.com](mailto:nmoore9041@gmail.com) or @sec\_nmoore on Twitter.

# Security Basics and Philosophy

* Confidentiality, Integrity and Availability: also known as the **CIA triad**, is a model designed to guide policies for information security within an organization. In this context, [confidentiality](https://whatis.techtarget.com/definition/confidentiality) is a set of rules that limits access to information, [integrity](https://searchdatacenter.techtarget.com/definition/integrity) is the assurance that the information is trustworthy and accurate, and [availability](https://searchstorage.techtarget.com/definition/data-availability) is a guarantee of reliable access to the information by authorized people. <https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA>, <https://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/>, <http://www.pearsonitcertification.com/articles/article.aspx?p=1708668>
* Least privilege: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. <https://nvd.nist.gov/800-53/Rev4/control/AC-6>, <https://www.centrify.com/lp/gartner-best-practices-for-privileged-access-management/?&ls=320-750-sem&utm_source=google&utm_term=least%20privilege&utm_campaign=NA-NB-Services-Infrastructure-Search-EX&utm_medium=cpc&utm_content=mkwid_skKBd7Coh-dc_pcrid_261039965948_pkw_least%20privilege_pmt_e_PIM-LeastPrivilegehttps://www.centrify.com/lp/gartner-best-practices-for-privileged-access-management/%3F&_bk=least%20privilege&_bt=261039965948&_bm=e&_bn=g&gclid=Cj0KCQjwrLXXBRCXARIsAIttmRP7GsILLZlYVycnPf3K3bvIg9MLFuDYR8u-iiqELLF1sxujr6I9UUEaArsOEALw_wcB>, <https://www.us-cert.gov/bsi/articles/knowledge/principles/least-privilege>
* Reducing the attack surface: Attack Surface Analysis is about mapping out what parts of a system need to be reviewed and tested for security vulnerabilities. The point of Attack Surface Analysis is to understand the risk areas in an application, to make developers and security specialists aware of what parts of the application are open to attack, to find ways of minimizing this, and to notice when and how the Attack Surface changes and what this means from a risk perspective. <https://www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet>, <https://www.sans.edu/cyber-research/security-laboratory/article/did-attack-surface>, <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/attack-surface-reduction-exploit-guard>
* Risk management: Risk management involves understanding, analyzing and addressing risk to make sure organizations achieve their objectives. So it must be proportionate to the complexity and type of organization involved. Enterprise Risk Management (ERM) is an integrated and joined up approach to managing risk across an organisation and its extended networks. <https://www.theirm.org/the-risk-profession/risk-management.aspx>, <http://www.marquette.edu/riskunit/riskmanagement/whatis.shtml>
* Authentication, Authorization, Accountability: Authentication, authorization, and accounting (AAA) is a term for a framework for intelligently controlling [access](https://whatis.techtarget.com/definition/access) to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security. <https://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting>, <https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-35/101-aaa-part1.html>
* Passwords and multi-factor authentication: Pretty straightforward stuff: passwords should be upper and lower case, have special characters, numbers, longer is better and shouldn’t be dictionary words. Two factor authentication can be simply summed up as something you know plus something you have or are.  <https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd>, <https://pages.nist.gov/800-63-3/sp800-63b.html>, <https://www.securenvoy.com/two-factor-authentication/what-is-2fa.shtm>

# Cryptography

* SSL
  + Overview: SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.
  + SSL vs TLS: SSL and TLS are both cryptographic protocols that provide authentication and data encryption between servers, machines and applications operating over a network (e.g. a client connecting to a web server). SSL is the predecessor to TLS. Over the years, new versions of the protocols have been released to address vulnerabilities and support stronger, more secure cipher suites and algorithms. <https://www.globalsign.com/en/blog/ssl-vs-tls-difference/>
  + TLS 1.3: The TLS 1.3 update was published in August 2018 and brings a ton of additional security and performance enhancements. <https://kinsta.com/blog/tls-1-3/>
* IPSec
  + IPSec is used for tunneling and encryption of data between two hosts. In the past it was used for both client to site and site to site encryption, but today client to site is less common. <https://searchsecurity.techtarget.com/definition/IPsec-Internet-Protocol-Security>
* VPNs
  + A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.  VPN technology is widely used in corporate environments. <https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html>
* Certificates and how they are used
  + Digital Certificates are a means by which consumers and businesses can utilize the security applications of Public Key Infrastructure (PKI). PKI comprises of the technology to enables secure e-commerce and Internet based communication. The number of people and businesses online is continuing to increase. As access becomes faster and cheaper such people will spend even more time connected to the Internet for personal communication and business transactions. Digital Certificates provide the following:
    - **Identification / Authentication:** The persons / entities with whom we are communicating are really who they say they are.
    - **Confidentiality:** The information within the message or transaction is kept confidential. It may only be read and understood by the intended sender and receiver.
    - **Integrity:** The information within the message or transaction is not tampered accidentally or deliberately with en route without all parties involved being aware of the tampering.
    - **Non-Repudiation:** The sender cannot deny sending the message or transaction, and the receiver cannot deny receiving it.
    - **Access Control:** Access to the protected information is only realized by the intended person or entity.
  + Symmetric encryption: Symmetric-key algorithms are [algorithms](https://en.wikipedia.org/wiki/Algorithm) for [cryptography](https://en.wikipedia.org/wiki/Cryptography) that use the same [cryptographic keys](https://en.wikipedia.org/wiki/Key_(cryptography)) for both encryption of [plaintext](https://en.wikipedia.org/wiki/Plaintext) and decryption of [ciphertext](https://en.wikipedia.org/wiki/Ciphertext). The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a [shared secret](https://en.wikipedia.org/wiki/Shared_secret) between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to [public-key encryption](https://en.wikipedia.org/wiki/Public_key_encryption) (also known as asymmetric key encryption)
  + Public-key cryptography, or asymmetric cryptography, is any cryptographic system that uses pairs of [keys](https://en.wikipedia.org/wiki/Cryptographic_key): *public keys* which may be disseminated widely, and *private keys* which are known only to the owner. This accomplishes two functions: [authentication](https://en.wikipedia.org/wiki/Authentication_protocol), where the public key verifies that a holder of the paired private key sent the message, and [encryption](https://en.wikipedia.org/wiki/Encryption), where only the paired private key holder can decrypt the message encrypted with the public key.
  + Hash Algorithms: A hash function is any [function](https://en.wikipedia.org/wiki/Function_(mathematics)) that can be used to map [data](https://en.wikipedia.org/wiki/Data_(computing)) of arbitrary size to data of a fixed size. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes. Hash functions are often used in combination with a [hash table](https://en.wikipedia.org/wiki/Hash_table), a common data structure used in computer software for rapid data lookup. Hash functions accelerate table or database lookup by detecting duplicated records in a large file. One such application is finding similar stretches in DNA sequences. They are also useful in [cryptography](https://en.wikipedia.org/wiki/Cryptography). A [cryptographic hash function](https://en.wikipedia.org/wiki/Cryptographic_hash_function) allows one to easily verify that some input data maps to a given hash value, but if the input data is unknown, it is deliberately difficult to reconstruct it (or any equivalent alternatives) by knowing the stored hash value. This is used for assuring [integrity](https://en.wikipedia.org/wiki/Data_integrity) of transmitted data, and is the building block for [HMACs](https://en.wikipedia.org/wiki/Hash-based_message_authentication_code), which provide [message authentication](https://en.wikipedia.org/wiki/Message_authentication). <https://en.wikipedia.org/wiki/Hash_function>

# Networking Basics

* 7 layer OSI model - the seven layers refer to the Open Systems Interconnection (OSI) model, a conceptual framework that describes the functions of a networking or telecommunication system. <https://www.networkworld.com/article/3239677/lan-wan/the-osi-model-explained-how-to-understand-and-remember-the-7-layer-network-model.html>
* LAN/WAN basics – Video <https://www.youtube.com/watch?v=Tu3B2CGe6Rs>
* Protocols – While there used to be many in the 90s, today IP is the dominant protocol used in the world’s networks. <https://www.1and1.com/digitalguide/server/know-how/what-is-internet-protocol-ip-definition-etc/>
* MAC and Layer 2 communications: <https://community.cisco.com/t5/network-architecture-documents/overview-of-layer-2-switched-networks-and-communication/ta-p/3128423>
* Routing: Video - <https://www.youtube.com/watch?v=8qtKpZGoNdI>
* Addressing and Subnetting: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>
* Default Gateway: <https://www.techopedia.com/definition/2184/default-gateway>
* ARP: <https://en.wikipedia.org/wiki/Address_Resolution_Protocol>
* NAT: <https://computer.howstuffworks.com/nat.htm>
* TCP: <https://searchnetworking.techtarget.com/definition/TCP>
* UDP: <https://searchnetworking.techtarget.com/definition/UDP-User-Datagram-Protocol>
* ICMP: <https://searchnetworking.techtarget.com/definition/ICMP>
* HTTP: <https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol>
* DNS: <https://www.cloudflare.com/learning/dns/what-is-dns/>
* SSH: <https://searchsecurity.techtarget.com/definition/Secure-Shell>
* SMB: <https://en.wikipedia.org/wiki/Server_Message_Block>
* DHCP: <https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top>
* SSL: <https://www.instantssl.com/ssl.html>
* Services and ports: <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>
* Ethernet: <https://searchnetworking.techtarget.com/definition/Ethernet>
* Wifi: <https://en.wikipedia.org/wiki/Wi-Fi>
* Cellular: <https://en.wikipedia.org/wiki/Cellular_network>
* Routers: <https://en.wikipedia.org/wiki/Router_(computing)>
* Switches: <https://en.wikipedia.org/wiki/Network_switch>
* Firewalls: <https://en.wikipedia.org/wiki/Firewall_(computing)>
* WAP: <https://en.wikipedia.org/wiki/Wireless_access_point>
* WAF: <https://en.wikipedia.org/wiki/Web_application_firewall>
* Identity Management: <https://searchsecurity.techtarget.com/definition/identity-management-ID-management>

# OS Basics

* Windows: A family of the most commonly encountered host operating systems.
  + Permissions – File and service permissions are given in two types: NTFS permissions and share permissions. Please note that there are subtle differences between different versions of Windows (7, 10, Server 2016….) <https://www.dell.com/support/article/us/en/19/sln156352/understanding-file-and-folder-permissions-in-windows?lang=en>
  + Getting your hands on some Windows products for free (at least virtually): <https://azure.microsoft.com/en-us/free/virtual-machines/search/?&OCID=AID719825_SEM_TI6Ea78a&lnkd=Google_Azure_Brand&gclid=EAIaIQobChMIztSApIHc3QIVE8pkCh38rAmpEAAYAiAAEgIcEfD_BwE&dclid=CJDP9KuB3N0CFc95YgodJMgD0A>
  + Useful Windows tools and utilities:
    - Cygwin – My favorite: an application that allows for Unix/Linux style interface on Windows. <http://www.cygwin.com/>
    - PuTTY – an application that allows you to telnet, SSH from Windows. SSH is particularly useful in infosec. <https://www.putty.org/>
    - Netcat: A computer networking utility for reading from and writing to network connections using [TCP](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) or [UDP](https://en.wikipedia.org/wiki/User_Datagram_Protocol). Netcat is designed to be a dependable [back-end](https://en.wikipedia.org/wiki/Front_and_back_ends) that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and investigation tool, since it can produce almost any kind of connection its user could need and has a number of built-in capabilities. <https://en.wikipedia.org/wiki/Netcat>
    - [**Burp Suite**](https://portswigger.net/) **by Portswigger** - The community edition of the Burp Suite is a free tool that provides a comprehensive solution for web application security checks. Their proxy feature is quite useful during penetration testing to manually inspect and fiddle with web traffic. It also includes a scanner that provides automated vulnerability scans for web applications. https://portswigger.net/
* \*nix - includes MacOS, BSD, Linux, UNIX: These are all very similar, but the ones you will see most often are MacOS and Linux. Once you go to the terminal in MacOS, the commands are very similar to anything you would see across all the \*nix operating systems out there. The best thing about Linux is that the OS and a large selection of applications are free/Open Source. Here are some basics that everyone should know about \*nix:
  + Changing and creating directories: cd and mkdir <http://linuxcommand.org/lc3_man_pages/cdh.html> and <http://man7.org/linux/man-pages/man1/mkdir.1.html>
  + Permissions: <https://www.linux.com/learn/understanding-linux-file-permissions>
  + Man pages – You can google “man <command>” for any Linux command and get information on how to use the command plus examples. Also, from the CLI in most systems, you can just type in the same string, “man <command>” for the explanation locally on your Linux system. Sometimes very helpful if you don’t have Internet access.
  + Useful commands: Just look for the man pages on these. It’s not an exhaustive list, but covers most of what the novice will need:
    - ifconfig – lists interfaces and if they are up or down and allows the admin to up/down an interface
    - netstat – depending on the switches (read the fine man page), this command is useful for seeing what ports are listening on the machine and also how the machine will route a packet.
    - route – will show, add or delete routes.
    - chmod – will change permissions on a file or directory
    - ps – will display running processes
    - mv – will move a file
    - rm – will delete a file/directory
    - ls – will list a directory’s contents
    - find – very useful for finding where you put that file you need to see right now….
    - cat – will list a file’s contents on the terminal. Remember to use the “ | more” switch to read it one page at a time. It can also be used to append files; read the man page. ;)
    - kill – will kill an active process. Sometimes useful, sometimes dangerous. Use it like you would really powerful weed killer; great for getting rid of dandelions but may inadvertently kill some of the good stuff too.
    - apt or yum – The former is used on Debian/Ubuntu flavors of Linux; the latter, on CentOS/Fedora/Redhat flavors. Used to install precompiled applications and libraries.
  + Shell basics: sometimes you have a repetitive task and you want to automate it. Or you want to execute one or more commands at a specific time or under specific conditions. This is one of the many reasons to script your tasks. <http://tldp.org/LDP/Bash-Beginners-Guide/html/Bash-Beginners-Guide.html>
  + vi: This is the mother of all text editors and while it is likely the least popular one on the planet, it is installed on EVERY SINGLE instance of \*nix I have ever seen. Since there is a good chance your favorite text editor may not be on a system you’ll have to work on, having some elementary vi skills will come in handy someday. Plus, it makes you look like one of the cool kids. <https://www.cs.colostate.edu/helpdocs/vi.html>
  + Compiling from source: I get the most pushback from people on this, but compiling from source rather than using precompiled applications gives you greater control over how and where the app is installed and in some cases is the only way you can get some apps. It’s like eating your vegetables: it’s good for you and as you mature, you’ll find you enjoy it. The most difficult part is the permissions and dependencies, but learning about these is also very helpful for the budding Linux enthusiast. <https://github.com/OpenEmu/OpenEmu/wiki/Compiling-From-Source-Guide>

# Cybersecurity Basics

* Endpoint security:
  + AV and anti-malware – Anti-virus has been around for over 20 years and is often the last line of defense against attacks. As a rule, AV relies on preventing attacks by matching a black list of known bad files. The main problem with this approach is that the number of known bad files increase significantly every year and scanning the host system can take a long time and consume lots of system resources. Further, the best of them when tested independently catch only about 40-45% of attacks. Anti-Malware often incorporates other techniques to catch more host attacks.
  + Host firewall – Windows and MacOS have a host firewall built in and Linux has an application called iptables. There are lots of additional free and for charge host firewall products available. Little Snitch is popular <https://www.obdev.at/products/littlesnitch/index.html>
  + OS hardening: Making an operating system more secure. It often requires numerous actions such as configuring system and network components properly, deleting unused files and applying the latest patches. There are hardening checklists available for popular operating systems that administrators can follow. <https://security.utexas.edu/content/operating-system-hardening-checklists>
* Network security basics:
  + Groups: grouping like users together (accounting, human resources, sales…) can be a great way to control user access to resources in the organization. A good example might be that sales does not need to access the general ledger server, but accounting does. A good primer on these concepts can be found in <https://en.wikipedia.org/wiki/Software-defined_networking>
  + Access – As a general rule, it is a best practice to allow users to as few resources as possible. One buzzword used to describe this approach is Zero Trust Architecture. <https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture>
  + Policy – It is also a best practice to map out an organization’s security policy on paper first and then translate that to the equipment you have. In some cases, compliance with certain standards applies (PCI, HIPAA, GLBA, GPDR….). One general guideline that is a good place to start is NIST <https://www.nist.gov/cyberframework>
* IDS/IPS – Intrusion Detection/Intrusion Prevention Systems can be either standalone or integrated into a next generation firewall. An **intrusion detection system** (**IDS**) is a device or [software application](https://en.wikipedia.org/wiki/Software_application) that monitors a [network](https://en.wikipedia.org/wiki/Computer_network) or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a [security information and event management](https://en.wikipedia.org/wiki/Security_information_and_event_management) (SIEM) system. A SIEM system combines outputs from multiple sources, and uses [alarm filtering](https://en.wikipedia.org/wiki/Alarm_filtering) techniques to distinguish malicious activity from false alarms. <https://en.wikipedia.org/wiki/Intrusion_detection_system> and <https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips>
* File inspection (AM) - Antimalware (anti-malware) is a type of software program designed to prevent, detect and remove malicious software (malware) on IT systems, as well as individual computing devices. <https://searchsecurity.techtarget.com/definition/antimalware>
* Content Filtering - URL filtering limits access by comparing web traffic against a database to prevent employees from accessing unproductive, harmful sites such as phishing pages. It is also commonly used to filter out potentially offensive content such as pornography. <https://www.paloaltonetworks.com/cyberpedia/what-is-url-filtering>
* DLP - Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer. <https://whatis.techtarget.com/definition/data-loss-prevention-DLP>
* Patching - A patch is a set of changes to a [computer program](https://en.wikipedia.org/wiki/Computer_program) or its supporting data designed to update, fix, or improve it.[[1]](https://en.wikipedia.org/wiki/Patch_(computing)#cite_note-news.com-1) This includes fixing [security vulnerabilities](https://en.wikipedia.org/wiki/Security_vulnerability)[[1]](https://en.wikipedia.org/wiki/Patch_(computing)#cite_note-news.com-1) and other [bugs](https://en.wikipedia.org/wiki/Computer_bug), with such patches usually being called bugfixes or bug fixes,and improving the [usability](https://en.wikipedia.org/wiki/Usability) or [performance](https://en.wikipedia.org/wiki/Computer_performance).
* Vulnerability Scanning - Vulnerability scanning is an inspection of the potential points of exploit on a computer or network to identify security holes. <https://searchsecurity.techtarget.com/definition/vulnerability-scanning>
* Cloud Computing - shared pools of configurable computer [system resources](https://en.wikipedia.org/wiki/System_resource) and higher-level services that can be rapidly [provisioned](https://en.wikipedia.org/wiki/Provisioning) with minimal management effort, often over the [Internet](https://en.wikipedia.org/wiki/Internet). Cloud computing relies on sharing of resources to achieve coherence and [economies of scale](https://en.wikipedia.org/wiki/Economies_of_scale), similar to a [public utility](https://en.wikipedia.org/wiki/Public_utility).
  + AWS Free Tier - <https://aws.amazon.com/free/>
  + Azure Free - <https://azure.microsoft.com/en-us/free/search/?&OCID=AID719825_SEM_hDTj6HPx&lnkd=Google_Azure_Brand&gclid=EAIaIQobChMI2Y_17KPc3QIVi8hkCh1SEgjVEAAYASAAEgLU_fD_BwE&dclid=CL_bgu-j3N0CFZ4YrQYdX44G6Q>

# Home Lab Requirements

As a best practice, I’d strongly recommend setting up a separate part of your home network as a lab using a switch that you can connect directly to your Internet router if at all possible. There is nothing worse than doing something to your lab network that takes the rest of your family/roommates... off line. If you decide you are going to play with malware or attack software, I’d recommend doing so on a wired network that has no Internet connectivity. Treat those sorts of things like live Anthrax samples as a guideline.

* PC - 16 G RAM, 500GB disk, multi-core processor – More is always better, especially if you are running virtual machines. One of the great things about Linux is that you can take your old desktop and convert it to Linux and it will likely run fine.
* High speed Internet – You’re going to be googling and downloading lots of stuff.
* One or more switches – cheap ones are fine, but if you can get an old Cisco one that supports span ports, that will come in handy. This is not a commercial for Cisco, but they are the most common and you can easily find TONS of documentation on how to do what you want with them. Having a couple to keep your networks physically separate can help to avoid headaches of upset family/roommates.
* Raspberry Pi – Great device that is cheap and allows you to do a lot of projects that can be not only fun, but useful.
* One or more Wifi routers – Chances are that your Internet Service Provider gave you a box with Wi-Fi on it. Sometimes it’s nice to have a second one for remote parts of your house or as part of a lab, especially if you want to start playing with Kismet or WiFi Pineapple.

# Useful Tools and Learning Projects

* Virtualbox – this is a free virtualization system that allows you to run virtual machines on your desktop. VMWare provides the same functionality, but it is licensed software that costs money. <https://www.virtualbox.org/>
* Wireshark – The de facto standard packet capture tool used by nearly every infosec professional at some time in his/her career. <https://www.wireshark.org/>
* Nessus - **Nessus is the de-facto industry standard vulnerability assessment solution for security practitioners.** Nessus helps the security pros on the front lines quickly and easily identify and fix vulnerabilities - including software flaws, missing patches, malware, and misconfigurations - across a variety of operating systems, devices and applications. <https://www.tenable.com/products/nessus-home>
* Snort – Snort if the de-facto industry standard for IDS/IPS. Many systems out there can import Snort rules and Cisco continues to support it as an Open Source project. There is an online support forum for it as well as several set up guides. <https://snort.org/>
* Python – Probably the most commonly used scripting language by infosec professionals and companies today. <https://pythoninstitute.org/free-python-courses/> <https://www.netacad.com/courses/programming/pcap-programming-essentials-python> <https://www.hashicorp.com/training>
* Kali Linux – a popular collection of infosec tools in a self-contained Linux instance. There are tons of books and free training sites available online. Here are a few links on their home page: <https://www.kali.org/>