InfoSec Ramp up

Disclaimer: Follow all rules of the creator of the tools you use. Some of these tools have offensive capability which should only be exercised in a controller lab environment. Use at your own risk. This document is subject to change at any time and is not an all-Inclusive list of resources that can be leveraged to learn about Information Security.

TRAINING AND KNOWLEDGE FOUNDATION:

1. Cybrary: Free security analyst, IT skills, and pen testing e-learning. https://www.cybrary.it/
    a. Security + - Excellent Beginner's Certification.
    b. Penetration Testing and Ethical Hacking
    c. Sniffing traffic - https://www.cybrary.it/video/sniffing-traffic-intro/
2. Hacksplaining: Excellent walk through of common web attacks. https://www.hacksplaining.com/
3. Wireshark (WS is a key tool to know) (download- www.wireshark.org)
    i. https://www.wireshark.org/#learnWS
    ii. Youtube Wireshark playlist setup to able to apply learning https://www.youtube.com/playlist?list=PLnKJHZhW_BuCPcIg6Ja2boDeHIRwoHMT-
    iii. Basic how to videos or self study https://mnex.biz/index.php/videos/ and https://mnex.biz/index.php/wireshark/
    iv. https://wiki.wireshark.org/SampleCaptures
4. Explanation of the "Kill Chain" http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
5. Massive open online courses (Free to low cost college level courses)
    a. University of Maryland Cybersecurity Specialization: https://www.coursera.org/specializations/cybersecurity?utm_medium=courseDescripTop
    b. edX Information Security courses: https://www.edx.org/course?search_query=cybersecurity
    c. Coursera Information Security courses: https://www.coursera.org/courses?query=cybersecurity
6. Metasploit Unleashed – Free Ethical Hacking Course. https://www.offensive-security.com/metasploit-unleashed/

Foundational IT skill training:

Command line: https://www.codecademy.com/learn/learn-the-command-line
Command line: https://learnpythonthehardway.org/book/appendixa.html
Command line: https://www.udacity.com/course/linux-command-line-basics--ud595
Command line: http://blog.commandlinekungfu.com/p/index-of-tips-and-tricks.html
Linux: https://training.linuxfoundation.org/free-linux-training
https://www.edx.org/course/introduction-linux-linuxfoundationx-lfs101x-1
REGEX: Learn regex in 55 minutes - https://qntm.org/files/re/re.html

http://www.rexegg.com/
http://www.regular-expressions.info/tutorial.html
Python: https://www.tutorialspoint.com/python/python_environment.htm
https://automatetheboringstuff.com/#toc
https://learnpythonthehardway.org/book/
Powershell: https://www.edx.org/course/windows-powershell-basics-microsoft-inf210x
https://mva.microsoft.com/learning-path/powershell-beginner-12
https://mva.microsoft.com/learning-path/powershell-advanced-13
Networking fundamentals: https://www.udacity.com/course/computer-networking--ud436
https://mva.microsoft.com/en-US/training-courses/networking-fundamentals-academic-edition-12452?l=j8Xm7GLPB_3105192806
Microsoft Windows Learning Paths: https://mva.microsoft.com/LearningPaths.aspx

TOOLS:

Build your virtual lab:

Virtual Software:

Virtual Box: https://www.virtualbox.org/wiki/Downloads
VMWare player:
https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/12_0

Virtual Pen testing or digital forensics OS Images/installations:

Kali: https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/
Parrot: https://www.parrotsec.org/download.fx
BackBox Linux: https://backbox.org/download
Digital Evidence and Forensic Toolkit: http://www.deftlinux.net/download/
BlackArch Linux: https://blackarch.org/downloads.html
SANS Investigative Forensic Toolkit (SIFT) Workstation: http://digital-forensics.sans.org/community/downloads

Vulnerable OS Images:

Metasploitable 2: https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
Metasploitable 3:
https://community.rapid7.com/community/metasploit/blog/2016/11/15/test-your-might-with-the-shiny-new-metasploitable3
Vulnhub – https://www.vulnhub.com/
OWASP vulnerable Web App:
https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project
Exploit Exercises practice VMs: http://exploit-exercises.com/
Microsoft Windows 7-10 OS and IE/Edge Browsers developer VMS:
https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/

Free security tools – Seek approval from your network admin!
http://sectools.org/
www.snort.org
http://www.splunk.com/view/SP-CAAAE8W
Security Onion for a one-stop-shop IDS/IPS/Reporting OS:
http://blog.securityonion.net/p/securityonion.html

Live Simulated Environments
https://hack.me (by eLearnSecurity – can be downloaded and virtualized if desired)
http://www.overthewire.org/wargames/
https://pentesterlab.com (can be downloaded and virtualized if desired)
http://securityoverride.org/news.php
http://smashthestack.org/
https://www.hacking-lab.com/Remote_Sec_Lab/
http://www.root-me.org/?lang=en
http://www.enigmagroup.org

NEWS AND BREACH REPORTS: - Stay up to date!
www.Krebsonsecurity.com
https://isc.sans.edu/
http://www.sans.org/security-resources/blogs
https://www.sans.org/newsletters/ - RSS feed
www.Reddit.com/r/netsec
www.reddit.com/r/blackhat
/r/pwned
/r/asknetsec
/r/netsecstudents
/r/malware
/r/homelab
www.schneier.com/
http://www.darkreading.com/
https://nakedsecurity.sophos.com/
http://www.sans.org/reading-room/
https://www.sans.org/webcasts/
https://www.sans.org/top25-software-errors/
https://www.sans.org/critical-security-controls/

Bugtraq mailing lists. There's also the 'new' FD mailing list. Both have archives available on seclists.org:
http://seclists.org/bugtraq/
http://seclists.org/fulldisclosure/

More technical information –
http://www.sans.org/reading-room/
https://www.sans.org/webcasts/
https://www.sans.org/top25-software-errors/
https://www.sans.org/critical-security-controls/
Basic Linux Privilege Escalation
https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
Windows Privilege Escalation
http://www.fuzzysecurity.com/tutorials/16.html
Hot Potato Attack
https://foxglovesecurity.com/2016/01/16/hot-potato/
Windows Privilege Escalation
https://toshellandback.com/2015/11/24/ms-priv-esc/
Web Application Security
https://www.owasp.org/index.php/Main_Page
http://www.securitytube.net/

BOOKS:
The Tao of Network Security Monitoring
The Practice of Network Security Monitoring: Understanding Incident Detection and Response
The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy 2nd Edition
Blue Team Field Manual
Blue Team Handbook: Incident Response Edition
Red Team Field Manual
The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws

INFOSEC ENTRY LEVEL CERTIFICATIONS to consider:
CompTIA Security + - Could be best bang for the buck.
CompTIA Cybersecurity Analyst +
EC-Council Certified Ethical Hacker