Resources

Where to start…

Getting started of security whether it be pen testing, DFIR, reverse engineering, etc can be a little overwhelming. The good news is that there is a lot of resources out there and the community is very helpful. Depending on what you are trying to learn, there is some resources below to help you get started. I would recommend trying to stick to one thing at first and once you get some experience and gain some confidence then go ahead and branch out to other things.

In the beginning it might be useful to play around with a few different concepts and tools and once you find something that really grasps your interest, dig deeper into and try to master it. YouTube is your friend, the community shares a lot of stuff and there is a lot of good tutorials and information.

Things I recommend before you begin…

I highly recommend that you get started with some basic knowledge of networks and learn how to do some programming, especially in a scripting language. I highly recommend Python, because it is highly supported and a very powerful tool that you can use to write scripts as well as a full application.

For reverse engineering I recommend you learn assembly before you attempt to reverse any software/malware. You can start with something simple like MIPS and do some assembly coding so you can get an idea of how it works. Writing things in C and then disassembling the code to see what it looks like in assembly is greatly beneficial, this can help you learn some of the C constructs.

Books & Reading

- Software Engineering
    - Clean Code
    - The pragmatic programmer
    - Code Complete
    - The Mythical Man-Month

    - The Security Development Lifecycle [free ebook]
    - Threat Modeling: Designing for Security
- Reverse Engineering / DFIR
    - Practical Malware Analysis
        - Must have in my opinion (and many others =)) to get started in reverse engineering & malware analysis. If you can only get one book, this would be it for me.
    - The IDA Pro Book
        - Good reference guide for IDA Pro
    - Practical Reverse Engineering
    - Attacking Network Protocols
    - Windows Internals Part 1
        - Get a better understanding of Windows
    - Practical Binary Analysis
    - The Art of Memory Forensics
    - Practical Forensic Imaging: Securing Digital Evidence with Linux Tools

- Exploit Dev
  - The Shellcoder’s Handbook: Discovering and Exploiting Security Holes
- Pen Testing
  - Rtfm: Red Team Field Manual
  - Gray Hat Hacking
  - The Hacker Playbook series
  - Penetration Testing
  - The Web Application Hacker’s Handbook
  - Attacking Network Protocols
  - Windows Internals Part 1
    - Get a better understanding of Windows
  - Troubleshooting with the Windows Sysinternals Tools
    - Reference on how to get the most out of the Sysinternals suite
- Cryptography
  - Serious Cryptography: A Practical Introduction to Modern Encryption

(I suggest starting with this one)

    - Applied Cryptography: Protocols, Algorithms and Source Code in C
    - Cryptography Engineering: Design Principles and Practical Applications
- https://pagedout.institute/

Tools

- Software Engineering
    - VIM =)
    - Visual Studio Code
        - Extensions
            - Better Comments
            - Shell Launcher
                - Allows you to switch Shells (Super useful)
            - Bracket Pair Colorizer (very useful)
            - Indenticator

  - indent-rainbow
  - Bookmarks
  - Todo Tree
- Language Extensions
  - C/C++ – Microsoft
  - C# – Microsoft
  - PowerShell – Microsoft
  - Python – Microsoft
  - x86 and x64 Assembly
- Themes
  - Noctis
  - Material
  - Monokai Pro
  - Cobalt2
  - Dracula

      - Night Owl
      - Rainglow
  - Visual Studio IDE
  - Atom
  - Sublime Text
- General
  - VMWare Workstation Pro
    - Virtual Machine
    - Alternatively get VMWare Workstation Player which is free, but doesn’t have the ability to take snapshots.
  - VirtualBox
    - Virtual Machine
    - FREE
    - Snapshots!
  - WSL – Windows Subsystem for Linux
    - Super useful when doing command line stuff on windows without having to fire up a VM

  - PowerShell
    - Learn to use it, very powerful
  - Linux
    - Choose your flavor and learn to use it well
  - Cygwin
  - VirusTotal
    - Not too sure if that file you downloaded is safe? Upload it to VirusTotal!
    -
- Python Useful Modules
  - Scapy
  - RE
  - Socket
  - Scrapy
- Reverse Engineering
  - IDA Pro

- Binary Ninja
    - Plugins
        - Bookmarks
        - SyscallIdentify
- Ghidra
- Hopper
- Radare
- Frida – Dissasembler
- Binwalk
- Snowman
- JD-Gui
- x64Dbg
- WinDbg
- Wireshark
- Sysinternals

  - REMnux
  - FLARE VM
  - Frida.re – Dynamic Instrumentation Toolkit
  - .Net Stuff
    - dnSpy
    - dotPeek
    - dotMemory
- DFIR
  - Volatility
  - SIFT Workstation
- Penetration Testing
  - Metasploit
  - Nmap
  - Nessus
  - Hashcat

- Web Penetration Testing
    - Burp Suite
    - Firefox plugins:
        - FoxyProxy
        - Wappalyzer or BuiltWith
    - DirBuster
        - Enumerates directories/paths/subpaths in a given domain
    - Sublist3r
        - Uses OSINT from search engines to help enumerate subdomains
    - Knockpy
        - Enumerate subdomains using a provided word list
    - Striker
        - Cloudflare bypass
        - DNS Enum
        - Checks for WordPress use

    - And more

- Fuzzing
  - AFL
  - BooFuzz
  - Wfuzz
- Security Tools for All
  - CyberChef
  - SecLists

Reference

- Reverse Engineering
  - x86 Assembly Instruction Reference

Blogs

- https://0xdarkvortex.dev/

- https://www.malwaretech.com/
- https://malwareunicorn.org/
- https://mayahustle.com/
- https://0ffset.net/
- https://about.me/hasherezade
- https://msrc-blog.microsoft.com/category/srd/
- https://threatvector.cylance.com/
- https://www.fireeye.com/blog.html
-

Podcasts

- Risky Business
- Security Now

- Security Weekly

- Darknet Diaries
- BHIS Podcast
- TrustedSec Podcast

Conferences

- DEFCON
- Black Hat
- BSides
- S4
- INFILTRATE

Training

- SANS Institute
- OSCP

- Cybrary
- Pluralsight
- ISC2
- Cyber Aces
- Infosec Institute
- SecureNinja
- YouTube
- OpenSecurityTraining
- EC-Council
- NICCS
- ICS-CERT
- University/College
  - Computer Science Degree
  - Software Engineering Degree
  - Cyber Security Degree

Share this:

Twitter Facebook

Like this:

Loading...

Revx0r

I am a software engineer in security. I do fun stuff like reverse engineering, security testing, and playing with 1s && 0s

Home » Resources

Manuel Berrueta Follow

Manuel Berrueta Retweeted

Andrew Thompson 23h

Archives

September 2019

August 2019

July 2019

185.212.128\.146 windows-afx-update\.com 🗑 🚮 Coming to an inbox near you.

↩ 3 ♥ 31 Twitter

Manuel Berrueta Retweeted

Cyber FastTrack 15 Oct

Register your interest in Cyber FastTrack and start taking your first steps into a new career https://t.co/RQXvqBMk2r

↩ 3 ♥ 4 Twitter

Manuel Berrueta Retweeted

Zack Whittaker ✓ 14 Oct

"A vulnerable box that no-one knew about with a direct, remote connection to the [ship's] main engine." —@cybergibbons.

Christ alive. https://t.co/HzfTtAu0yc

↩ 39 ♥ 116 Twitter

Manuel Berrueta Retweeted

No Starch Press ✓ 12 Oct

Please share this as widely as possible. Why should we have to police Amazon? This problem is ongoing since 2017. These counterfeits are shipped and sold by AMAZON, NOT A THIRD PARTY. This is not Marketplace. https://t.co/QSP65CWJ7O

↩ ⟲ 1982 ♥ 2276 Twitter

⟲ Manuel Berrueta Retweeted

Basheer Ahmed Khan 5 Oct

52 powerful CyberSecurity Bloggers and Speakers influencing millions through their writings and talks, compiled by @basheer_a_khan on @Peerlyst
#52InfluentialCyberSecurityBloggersAndSpeakers
https://t.co/2Fy2OkKCyy

↩ ⟲ 13 ♥ 23 Twitter

Load More...

Powered by WordPress Theme by Neatly

©2019 Revx0r - Security Mindset Blog