Intro to Malware Analysis

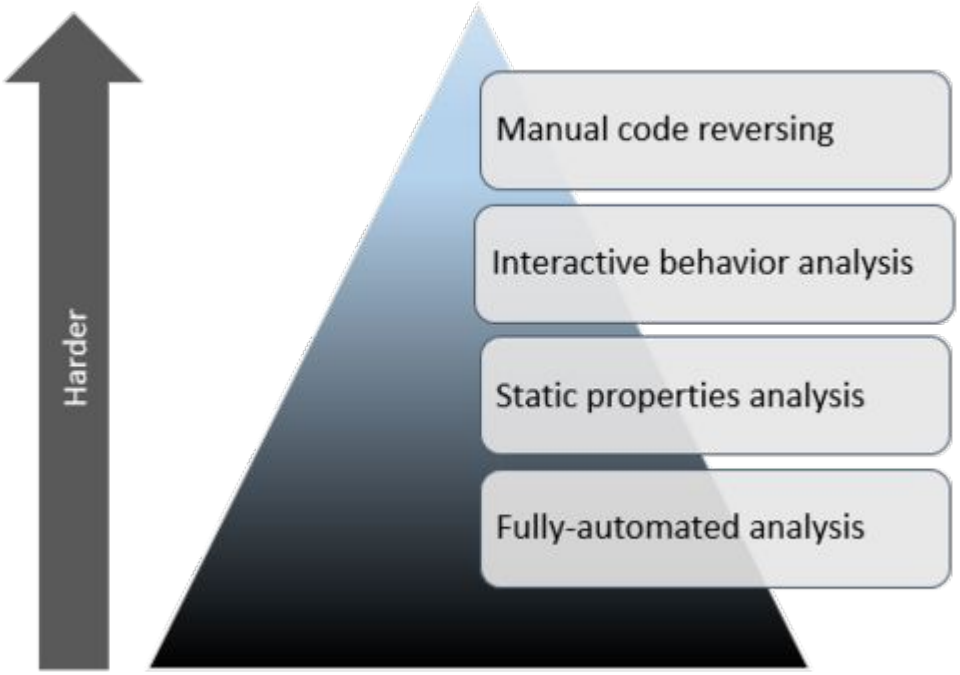
Trevon

/bin/bash echo $NAME

- Trevon (blackmanta) on slack
  - Check out #re
- Graduate Student
- **I DO NOT CLAIM TO BE AN EXPERT**

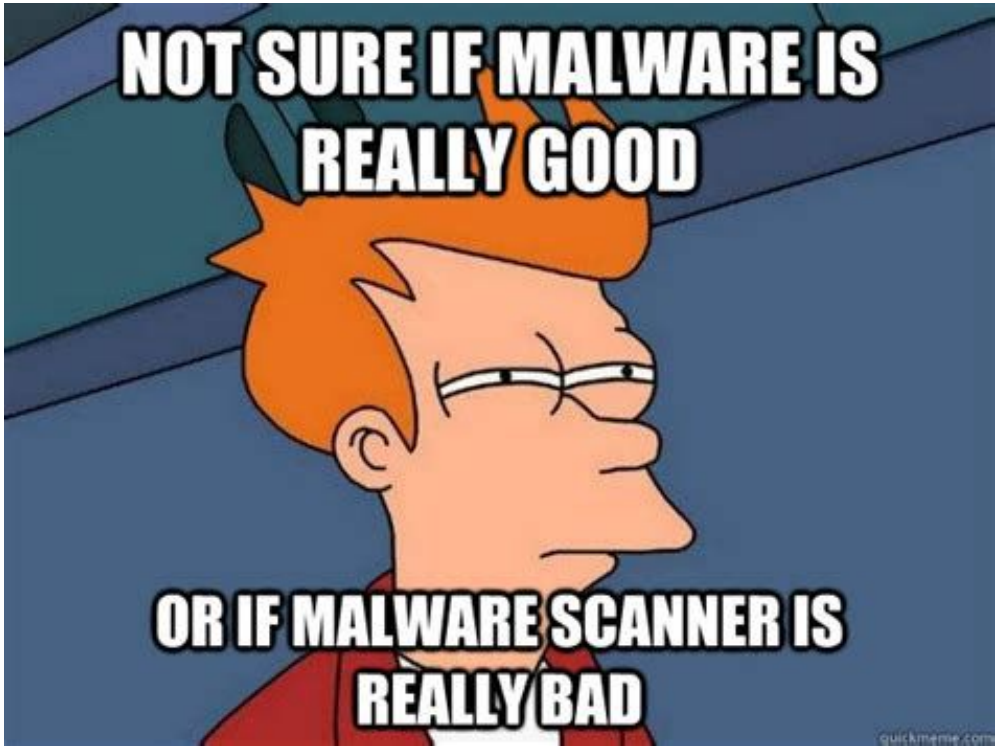
What is Malware Analysis?

The process of learning how a malicious program functions and its potential repercussions.



Types of Analysis

- Static Analysis
  - Code Analysis
  - Strings in binaries
  - Packed Malware
- Dynamic Analysis
  - Behavioral Analysis
  - Debugging
  - Registry changes
- Symbolic Analysis?



Malware Types

- Virus
  - Requires human interaction to run and propagate
- Trojan
  - Malware that hides in legitimate files
- Worm
  - Similar to a Virus but it does not need human interaction to run or propagate in a network
- Rootkit
  - Extremely hard to detect and impossible to remove without formatting a system
- Spyware
  - Installed on a system to monitor and/or record activities

Notable

- Petya
- WannaCry
- BadRabbit
- Industroyer
- Kronos
- Trickbot

What about top threats now?

https://www.cisecurity.org/blog/top-10-malware-august-2019/

Virtual Environment

Preparing your Windows Environment

- Install Windows 10 or Windows 7 iso
  - Premade Windows VM's
- Create and install virtual machine environment
  - You can also look into premade OVA's (Flare-VM)
- Turn off Virus and Threat protection
- **Disable Windows Defender**
- **Install Visual Studio Code**
- Install tools (This will be an ongoing processes)
  - Sysinternals suite, Ollydbg, IDA, Wireshark, ApateDNS, PE-Bear, dnSpy (decompiler), de4bot (Deobfuscator), Resource Hacker, 7zip, Process Explorer, HxD, python2 (strings.py)
- **Advanced Guides**

Automated Coolness

- Cuckoo
- S2E

Where can you find Malware Samples?

Free Sandbox Environments

- https://www.hybrid-analysis.com
- https://www.virustotal.com
- http://www.malshare.com/
- https://virusshare.com/
- http://thezoo.morirt.com/

Communities

- https://beta.virusbay.io/
- https://malwaretips.com

List of Useful Things

Automated analysis

- https://www.hybrid-analysis.com
- https://www.virustotal.com

Environments

- https://remnux.org
- https://www.fireeye.com/blog/threat-research/2017/07/flare-vm-the-windows-malware.html

Writeups

- https://zeltser.com/malware-analysis-reports/

Books

- Practical Malware Analysis
- Malware Analyst's Cookbook

Helpful Sources

- https://hshrzd.wordpress.com/how-to-start/
- https://zeltser.com/media/docs/intro-to-malware-analysis.pdf
- https://drive.google.com/file/d/1lSEps7jDX6an_iXJ0Wokdjh0rnBgY9l7/view
- https://www.malwaretech.com/2017/11/creating-a-simple-free-malware-analysis-environment.html
- https://reverseengineering.stackexchange.com
- https://github.com/RPISEC/Malware
- https://github.com/rshipp/awesome-malware-analysis