INTRO TO BINARY ANALYSIS

WHO AM I

- Trevon (blackmanta)
- Graduate Student
- Linux Enthusiast

WHAT IS BINARY ANALYSIS

- Not only linux based
- Static and Dynamic
- System level understanding
- Helps with
  - Malware Analysis, Reverse Engineering, Digital Forensics

WHY IS IT IMPORTANT

- A good understanding goes a long way
- Learning gems from other programmers
- Finding bugs

ASSEMBLY REFERENCES

- A Low level language just above machine code
- x64 Cheet Sheet
- Intro to Arm Assembly Basics
- Crash Course in x86 Assembly

ELF FILES

Referencing The 101 of ELF files on Linux

- Executable and Linkable format (Linux Based)
- Defines the structure of a Binary
- readelf

DEBUGGER VS DISSAMBLER

- Dynamic analysis
- Static analysis
- behavior vs logic
- https://reverseengineering.stackexchange.com/questions/4635/whats-
  difference-between-a-disassembler-debugger-and-decompiler

FREE TOOLING

- GNU (Debugger) GDB [CLI based]
- Ghidra
- IDA Freeware
- Radare2 (Cutter is a GUI for this tool)
- Frida
- Viper
- Angr
- Pharos (Automated)

CODE SAMPLES

From book, Practical Binary Analysis

- https://practicalbinaryanalysis.com/file/pba-code.tar.gz

REFERENCES

- Practicalbinaryanalysis.com (Website)
- Practical Binary Analysis (Book)
- Learning Linux Binary Analysis (Book)
- The 101 of ELF files on Linux (Website)
- Dynamic Binary Analysis (Website)
- Reverse Engineering Resources (Medium)
- Binary Analysis Tools