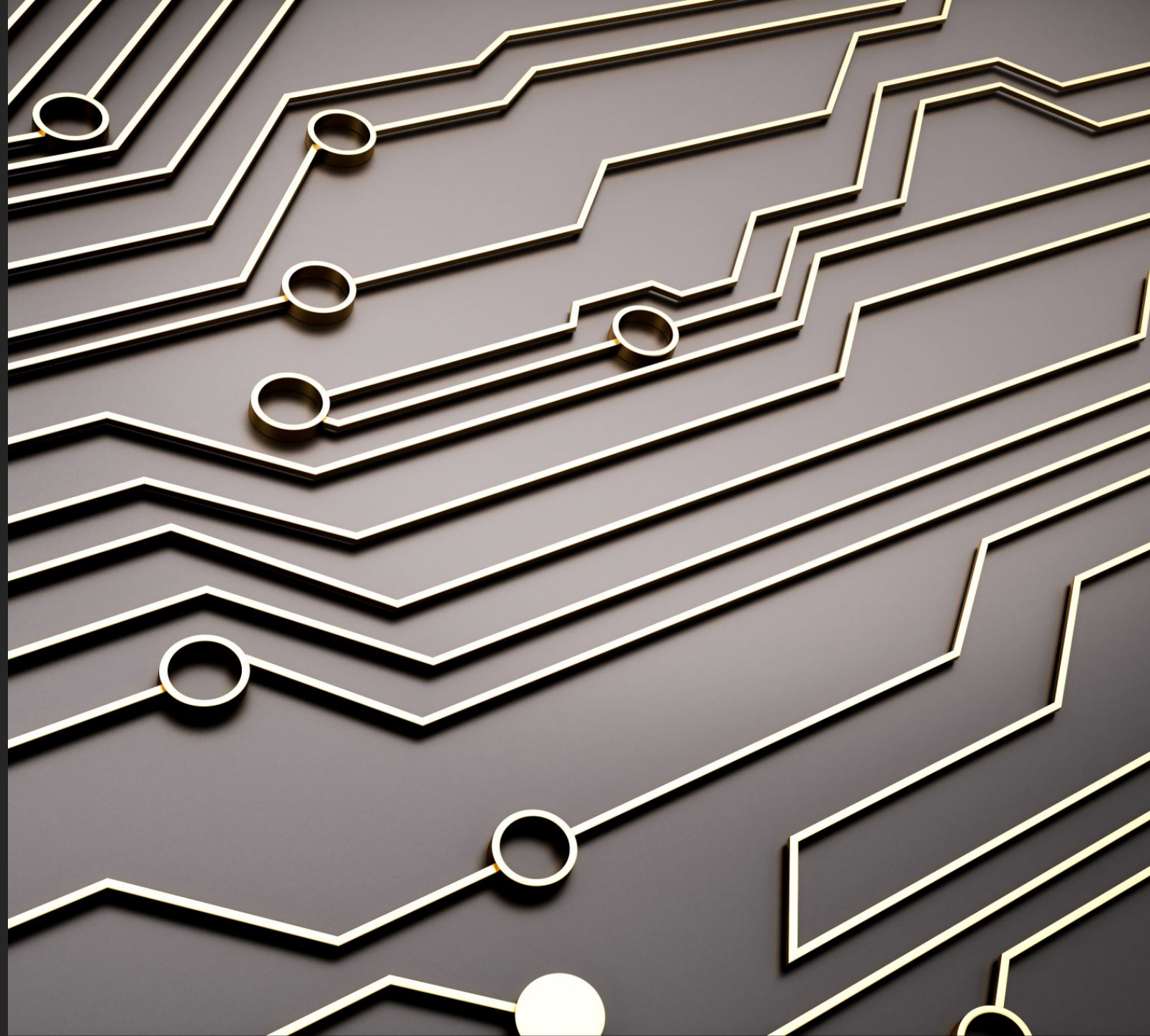
The Art of Hardware and Software Reverse Engineering

PRESENTED BY ORVILLE DILLON, JR.

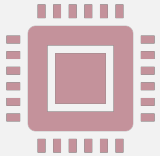


What is Reverse Engineering?

Reverse Engineering is the art of taking apart anything man-made to break it down and gain an understanding of its functions for the purpose of replication, renewal or just genuine interest.

Why Learn Reverse Engineering?

To understand the devices which we purchase, give, use and even repair.



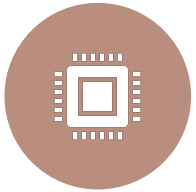
To learn about technology.

Recreate legacy software and vintage hardware.

Pre-requisites

THE WILL AND DRIVE TO LEARN... AND A COMPUTING DEVICE.

Uses of Reversing



Improve hardware and software.

Find vulnerabilities and develop exploits.

Prevent vulnerabilities and the development of exploits.

Replicate and upgrade outdated technology.

Cybersecurity operations.

Digital Forensics investigations.

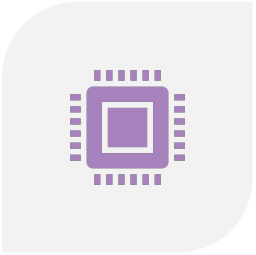
Nice to Haves:

FAMILIARITY WITH ASSEMBLY INSTRUCTION SETS(X86, X64, ARM, ETC.)

KNOWLEDGE OF SHELLCODE AND HIGH LEVEL PROGRAMMING LANGUAGES (C, C++, C#, OBJECTIVE C, ETC).

SCRIPTING LANGUAGE KNOWLEDGE: (PYTHON, RUBY).

HEXADECIMAL CALCULATOR



DISASSEMBLER AND HEX EDITING SOFTWARE.

DEBUGGER

Tools:

IDA Pro

radare2

Binary Ninja

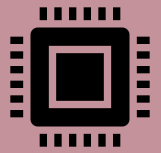
WinHex

Immunity Debugger

GNU Debugger (gdb)

Types of Analysis:

Dynamic – Executing and testing a program in real-time.



Static Analysis – Testing an application by viewing its binary.

RE-Related Resources

- PoCIIGTFO
- 2600 Magazine
- Immersive Labs
- PentesterLab
- HacktheBox
- Paged Out