# Full Study Plan – 6 Months: Low-Level Bug Bounty & Reversing (Final)

# 📅 Full Study Plan – 6 Months: Low-Level Bug Bounty & Reversing (Final)

This plan is designed for focused development in low-level security research, bug bounty, and exploitation. It excludes Web App vulnerabilities and focuses on Linux, binary exploitation, reverse engineering, cryptography, and Python tooling.

Each week includes:

* 📘 Learning: curated resources (TryHackMe, YouTube, Docs)
* 🛠️ Practice: hands-on scripting, reversing, exploitation
* 🧾 Summary: documented insights and results

## 🧩 Month 1: Python for Low-Level Work

### Week 1: Reading/Writing Binary Files

* open(), rb/wb mode, reading headers, hex/ASCII printing
* Practice: Read first 64 bytes of ELF file, print hex + ASCII, save to file

### Week 2: struct and Memory Formats

* struct module, endian formats, unpacking integers/floats
* Practice: Unpack 16 bytes from ELF, print in decimal/hex

### Week 3: Sockets and Binary Protocols

* socket module, TCP client, sending/receiving binary data
* Practice: Build client to send struct-packed data to a server and log response

### Week 4: pwntools Basics

* process(), p32(), cyclic(), sending payloads
* Practice: Send 40 bytes padding + 0xdeadbeef to local process, test with GDB

## 🧩 Month 2: Cryptography, Hashing & Digital Signatures

### Week 5: Hashing & Encoding

* bytes, base64, hex, hashlib (md5, sha256)
* Practice: Create script to hash a file, compare values

### Week 6: Symmetric Encryption

* cryptography library – AES encryption/decryption, modes (CBC, ECB)
* Practice: Encrypt/decrypt text + files using AES

### Week 7: Digital Signatures

* RSA & ECDSA basics, private/public key, verification
* Practice: Sign a file with private key, verify with public key using Python

### Week 8: Ghidra Introduction

* Ghidra overview, strings, xrefs, disassembly navigation
* Practice: Reverse a binary to find password check and patch

## 🧩 Month 3: Stack Overflow Exploitation

### Week 9: GDB Basics & Stack Analysis

* breakpoints, disassemble, stack, memory inspection
* Practice: Run binary, inspect parameters, modify values

### Week 10: Stack Overflow 1 (Protostar)

* buffer overflow, control EIP
* Practice: Exploit Stack0–Stack2, document offset to return address

### Week 11: Stack Overflow 2 (Protostar)

* shellcode basics, nop sled
* Practice: Exploit Stack3–Stack5, inject shellcode if possible

### Week 12: Protections: ASLR + DEP

* Identifying active protections, disabling ASLR, DEP concepts
* Practice: Analyze effect of ASLR with/without, test shellcode execution

## 🧩 Month 4: Heap, Format Strings & Low-Level Tools

### Week 13: Heap Overflow

* malloc, free, memory layout
* Practice: Exploit Heap0–Heap2 (Protostar), observe memory behavior

### Week 14: Format String Attacks

* printf(), %x, %n, memory disclosure
* Practice: Exploit format string vuln to leak values

### Week 15: IDA Free & AIDA Usage

* Static analysis, navigation, decompilation
* Practice: Reverse small binary, map control flow

### Week 16: Linux Permissions & System Internals

* sudoers, permissions abuse, basic Sysinternals tools on Windows (optional)
* Practice: List setuid binaries and test for privilege escalation

## 🧩 Month 5: Exploit Mitigations & Bypasses

### Week 17: Stack Canaries

* what are they, how to detect, bypass theory
* Practice: Run binary with/without canary, observe crash/log

### Week 18: NX / DEP and Return-to-libc

* Non-executable stack, ROP chains
* Practice: Use pwntools to build ret2libc payload

### Week 19: PIE + ASLR Bypass

* PIE-enabled binaries, GOT/PLT usage
* Practice: Use leaked address to compute base and hijack flow

### Week 20: Practice – Full Exploit Chain

* Combine all learned protections and bypasses
* Practice: Solve a full protected binary (CTF-style)

## 🧩 Month 6: Final Projects, Repos & Bug Bounty Entry

### Week 21: CrackMe + Writeup

* Apply all reversing tools
* Practice: Solve and write full explanation

### Week 22: Exploit + pwntools

* Build a stable exploit for remote or local vuln
* Practice: Automate exploit chain (offset, leak, shell)

### Week 23: GitHub + Portfolio Building

* Document learning + projects
* Practice: Organize weekly folders, summaries, screenshots

### Week 24: Bug Bounty Prep / Job Readiness

* Explore ZDI, HackerOne (binary scopes)
* Practice: Submit one binary-related report / apply to intern role