90-Day Offensive Security Master Plan

- Total Commitment: 14 focused hours per week (~180 hours total).
- Zero domain switching for 90 days.
- All work must be public (writeups + exploit scripts).
- Build evidence of skill, not just knowledge.
- Primary repository: offsec-workshop.

Month 1 – Foundations Reset

- Deep Linux CLI usage daily.
- Understand process memory layout (stack, heap, ELF structure).
- Master GDB (breakpoints, stack inspection, memory examination).
- Learn readelf and objdump for binary analysis.
- Solve 8–10 beginner pwn challenges.
- Write detailed structured writeups for each challenge.

Month 2 – Exploit Development

- Use pwntools properly in exploit scripts.
- Reproduce classic buffer overflow exploit from scratch.
- Learn and implement ret2libc.
- Learn and implement basic ROP chains.
- Understand and exploit format string vulnerabilities.
- Introduction to heap basics and simple heap exploitation.
- Create your own vulnerable C binary and exploit it.

Execution Breakdown (Weekly Structure)

- 8 hours – Solving challenges & exploit development.
- 4 hours – Deep debugging & failure analysis.
- 2 hours – Theory reinforcement directly related to active problems.

Week 1–2: Foundations

- Master GDB workflow.
- Understand stack frames and calling conventions.
- Solve first 5 easy pwn challenges.

Week 3–6: Volume & Depth

- Solve additional 5–10 pwn challenges.
- Use pwntools consistently.
- Document debugging logs in writeups.
- Push all work to offsec-workshop repository.

Week 7–8: Medium-Level Topics

- ret2libc exploitation.
- Basic ROP chains.
- Format string vulnerabilities.
- Heap basics.

Month 3 – Positioning & Applications

- Refactor GitHub into a clean security-focused profile.
- Organize challenges by category (stack, ROP, format string, heap).
- Write strong README explaining offensive journey.
- Build one small offensive automation tool.
- Apply to junior security internships and boutique security firms.
- Send applications with direct links to specific writeups.