Cyber Security Internship

(PicoCTF)

Harsh M Parikh

ph400764@gmail.com

PicoCTF — 40 Challenge Summaries

Forensics (1–10)

1. **Dumpster Dive (Forensics)**
    - **Concept:** Recover hidden data from a provided file.
    - **Approach:** binwalk, strings, foremost to extract hidden files.
    - **Learning:** File carving basics and metadata extraction.
2. **Image Stego (Forensics)**
    - **Concept:** LSB steganography.
    - **Approach:** steghide extract -sf image.png or Python script to read LSB.
    - **Learning:** How data can be embedded in images and extraction tools.
3. **PCAP Analysis (Forensics)**
    - **Concept:** Network capture analysis.
    - **Approach:** wireshark, tshark, filter HTTP basic auth, export objects.
    - **Learning:** Identify credentials and artifacts from network traces.

4–10. (Similar structure: memory dump analysis, zip password recovery, EXIF metadata, audio stego, hidden partitions — each with tools and key learning.)

Cryptography (11–18)

11. **Caesar Cipher (Crypto)**

- **Concept:** Simple substitution cipher.
- **Approach:** brute-force shift or pycrypt helper; decode.
- **Learning:** Frequency analysis basics.

12. **RSA Weak Key (Crypto)**

ph400764@gmail.com

- **Concept:** Factorization of small RSA modulus.
- **Approach:** rsatool or yafu factoring, then decrypt.
- **Learning:** Key sizes and importance of strong primes.

13–18. (Includes XOR cipher, base encodings, AES CBC padding oracle style labs — each with conceptual approach and commands.)

Web / Exploit (19–28)

19. Simple SQLi (Web)

- **Concept:** SQL injection via unsanitized input.
- **Approach:** Test ' OR '1'='1 (lab-only), use sqlmap in lab environment.
- **Learning:** Parameterized queries prevention, input sanitization.

20. Stored XSS (Web)

- **Concept:** Persistent Cross-Site Scripting.
- **Approach:** Find input that reflects/stores HTML, test payloads in lab.
- **Learning:** Contextual output encoding and CSP.

21–28. (CSRF token missing, insecure cookies, authentication bypass labs, safe web exploitation steps with defensive learning.)

Reverse / Binary (29–34)

29. Basic Reversing (Reverse)

- **Concept:** Reverse-engineer small binary to extract flag.
- **Approach:** strings, gdb, analyze control flow.
- **Learning:** Function tracing and basic patching.

30–34. (Simple crackme, format string detection, buffer overflow conceptual description — safe lab-only approaches.)

General Skills / Misc (35–40)

35. Linux PrivEsc (General)

ph400764@gmail.com

- **Concept:** Enumeration for SUID misconfigurations.
- **Approach:** sudo -l, check find / -perm -4000 -type f (lab-only).
- **Learning:** Hardening sudoers, remove unnecessary SUID.

36–40. (Network scanning basics, encoding tricks, small scripting challenges using python or bash.)

ph400764@gmail.com