CTF Player Cheatsheet

Reconnaissance

- Enumerate all services, ports, and files (check those .git folders!)
- Read the challenge description carefully - hints are often hidden in plain sight
- Google is your best friend (and StackOverflow is your therapist)
- Check file metadata - authors love to hide flags in exif data

Web Exploitation

- Always check source code and developer console first
- Test for common injections: SQL, XSS, SSTI, etc.
- Abuse cookie values - they're usually just base64 with extra steps
- Remember that robots.txt exists for a reson [sic]

Cryptography

- Recognize common encodings: base64, hex, binary (it's never actual encryption)
- Try classic ciphers before complex ones (Caesar would be proud)
- Use CyberChef for quick transformations
- When in doubt, just XOR everything with 0x42

Binary Exploitation

- Buffer overflows: the gift that keeps on giving
- Use pattern generators to find exact offset
- Check for canaries and PIE - or just pray they're disabled
- Remember: segmentation fault is just the computer asking for more input

Forensics

- Always run strings and binwalk on mystery files
- Check for steganography in images (LSB is so hot right now)
- Memory dumps contain passwords, just like your brain doesn't
- Wireshark can find everything except your lost self-esteem

Reverse Engineering

- Static analysis before dynamic analysis (unless your're [sic] impatient)
- Look for interesting strings and function names
- Analyze control flow to understand program logic
- Use debuggers to examine program state during execution

Misc Tips

- Sleep is for the weak (or people who solved the challenge already)
- Energy drinks count as a food group during competitions
- Team up with people smarter than you
- The real flag was the friends we made along the way