# Pentester Cheatsheet

## Reconnaissance

- Gather OSINT without leaving digital footprints (unlike your Instagram stalking)
- Map network topology before attacking
- Identify domain information using whios [sic] and DNS tools
- Document all potential entry points (except the ones labeled "TRAP")

## Scanning & Enumeration

- Conduct port scans with varying techniques to avoid detection
- Enumerate services and their versions (those Windows 2003 servers are gold!)
- Identify web technologies and frameworks
- Map out all potential vulnrabilities [sic] - quantity over quality!

## Gaining Access

- Exploit identified vulnerabilities ethically (wink wink)
- Use social engineering when technical approaches fail
- Deploy custom payloads that antivirus definitely won't catch
- Document successful entry points for the report you'll write at 3am

## Privilege Escalation

- Look for misconfigured services and weak permissions
- Search for hardcoded credentials (developers never dissapoint [sic])
- Exploit kernel vulnerabilities when possible
- Use living-off-the-land techniques to blend in like that plant in accounting

## Post-Exploitation

- Maintain access without being detected (or until Friday beer o'clock)
- Collect only authorized data per engagement scope
- Document exact exploitation paths for remediation
- Don't accidently [sic] delete production databases - we only did that once!

## Reporting

- Document findings with clear reproduction steps
- Include screenshots as proof (but blur out your Netflix tabs)
- Prioritize vulnerabilities based on actual risk
- Provide actionable remediation steps that aren't "burn it all down"