CTF Writeup Template

Metadata

Title *Challenge / room name*	
Platform *Platform (THM, HTB, CTF name, etc.)*	
Category *Web, pwn, forensics, crypto, misc, etc.*	
Difficulty *Easy / Medium / Hard (platform rating or your view)*	
Author *Your name / handle*	
Date *Date you completed the challenge*	
URL *Link to the room / challenge*	
Writeup URL *(Optional) Where this writeup will live (blog, GitHub, etc.)*	

Overview

Target *Target host / app / scope summary*	
Objective *What is the main objective? (Get flag, specific access, data, etc.)*	
High-level summary *2–3 sentence overview of how you solved it*	

Recon

Initial enumeration *What scans / tools did you run first (nmap, dirb, gobuster, etc.)?*	

Findings
Key ports, services, directories, or files discovered

Reasoning
Why these findings looked interesting or suspicious

Screenshots / evidence
List planned screenshots (e.g., nmap results, directory listing)

Initial Access

Vulnerability
What vulnerability did you exploit first? (e.g., SQLi, RCE, misconfig)

Discovery
How you found this vuln (which clue, scan result, or error message)

Exploitation steps
Step-by-step commands or actions to gain initial access (summarised)

Payloads
Key payloads / requests used (with brief explanation)

Reasoning
Why you chose this path and alternative ideas you considered

Dead ends
Short notes on approaches that failed and why

Screenshots / evidence
Screens you will include (e.g., login bypass, shell pop)

Privilege Escalation / Lateral

Starting point
Initial level of access (user, low-priv shell, etc.)

Enum for privesc
Commands / tools used (linpeas, winPEAS, manual checks)

Key privesc finding *Misconfig / vuln that enabled escalation*	
Exploitation steps *How you escalated privileges or moved laterally*	
Creds / reuse *Any credentials, tokens, or keys reused and where*	
Persistence *Any persistence techniques (if relevant to the challenge)*	
Reasoning *Why you focused on certain vectors (SUID, services, cron, etc.)*	
Dead ends *Attempts that did not work and what you learned*	
Screenshots / evidence *Planned screenshots (e.g., before/after id, proof of privesc)*	

Flag / Objective

Flag location *Where you eventually found the flag / objective*	
Access path *Shortest clear description of how you got there*	
Proof *Flag value redacted or partially masked, or hash/screenshot reference*	
Notes *Any quirks about retrieving or submitting the flag*	

Lessons Learned

What worked well *Techniques / tools that were especially effective*	
What you'd do faster next time *Places you wasted time or over-enumerated*	

Patterns recognised
Vuln patterns or behaviours you've seen in other boxes

New tools / tricks
Commands, tools, or methods you learned from this challenge

Open questions
Anything still unclear you want to research later

Audience / Reporting

Intended reader
Who you're writing this for (future you, recruiters, community)

Clarity check
Key points you want a reader to take away

Dead-end highlights
1–3 short examples where explaining a failure is useful

Screenshots / Code / Ethics

Screenshot plan
List key screenshots you will capture (path / description)

Privacy
What needs blurring or redaction (usernames, IPs, domains)

Platform rules
Spoiler / disclosure rules for this platform (delay, restrictions)

Code snippets
List important snippets to include (payloads, scripts)

Logging
Decide what log output is necessary vs. noisy

Client / program rules
For bug bounty / client work: note permissions and what must stay private

Summary

One-paragraph story *Short narrative from recon to flag, focusing on decision-making*	
Key impact *If this were a real system, what would the risk / impact be?*	
Follow-up actions *Things you want to practise or build next (labs, tools, blog posts)*	