Exploit Discovery — Sanitized (Exam-safe)

Sanitization note: This document is exam-safe. It contains high-level guidance for handling version banners and vulnerability hints. All step-by-step exploit instructions, PoC run commands, and external walkthrough links have been removed.

Context: interpreting a version banner (policy-first)

- A version banner (e.g., 'vsftpd 2.3.4') is an indicator to investigate—not an instruction to run exploits automatically.
- Follow a policy-first approach: verify applicability, avoid untrusted PoCs, and prefer lab-tested exploits executed only when

Safe workflow (conceptual, sanitized)

1) Record the banner and save scan output (e.g., nmap results).
2) Search for public references for awareness only (do NOT copy/run public PoCs directly in the exam environment).
   - Use public exploit databases as research references before the exam; do not paste or execute unverified PoCs live.
3) Verify affected component and version relevance manually (check service paths, config files) before considering any expl
4) If a verified, lab-tested exploit is required and permitted by exam rules, document your intent and all commands you will ru
5) Always capture outputs, timestamps, and screenshots for reporting and reproducibility.

Allowed syntax examples (safe, non-actionable)

- nmap -sC -sV -Pn <IP> # capture version banner
- search public references offline before exam to map potential CVEs (do not run PoCs live)
- Note: use of Metasploit or other frameworks must follow exam policy (some exams restrict these tools)

What to avoid in exam notes (explicitly)

- Do NOT include copied exploit scripts or PoC code blocks.
- Do NOT keep step-by-step commands to run exploits (e.g., cp /path/to/exploit.py .; python3 exploit.py) in your local exam fi
- Do NOT include direct links to exploit-db, GitHub PoCs, or walkthroughs in files you will open during the exam.

Reporting & evidence (must-do)

- Clearly document: banner text, how you verified the service, rationale for attempting any exploit, exact commands run, and
- If you use a public PoC after lab verification, note where it was obtained (offline research) and demonstrate you tested it in

Sanitization: This file was created to be exam-safe. It contains conceptual guidance and safe syntax examples only; no exploit PoCs, reverse shells, or external writeup links are included.