🔎 Complete Enumeration Flow for bug bounty

✂️ Scope & TLD Enumeration

Goal: Identify all root domains and shadow assets within scope.

Tools: recon-ng, amass (intel mode)

✒️ Subdomain Enumeration

Goal: Discover maximum subdomains (primary attack surface).

Tools: subfinder, amass, recon-ng

🛏️ Host Discovery / Alive Check

Goal: Filter subdomains that resolve and expose reachable services.

Tools: dnsx, httpx

🌂 Technology Fingerprinting

Goal: Identify server, framework, CMS, cloud, and WAF to map likely vulnerabilities.

🌡️ Content Discovery (Directories & Files)

Goal: Find hidden paths, admin panels, backups, and APIs.

🎒 Endpoint & Parameter Discovery

Goal: Identify user-controlled inputs (parameters, API routes, endpoints).

🎓 Manual Testing

Where real bugs live:

- Broken authentication
- Broken access control (IDOR)
- Business logic flaws
- Privilege escalation
- Input validation issues (XSS, SQLi)

🎩 Automation & Validation (Optional)

Goal: Assist manual testing and validate known issues.

Key Principle

> Enumeration finds attack surface. **Manual testing finds real bugs.**

by adilmuhammad