

# ■■ Bug Bounty / Pentesting Enumeration Methodology

## 1. Host Assessment (Infrastructure / IPs)

Objective: Discover live hosts, open ports, services, versions, and misconfigurations.

### Step 1: Host Discovery

```
naabu -host target.com -p - -o ports.txt  
nmap -iL ips.txt -sV -sC -Pn -T4 -oA nmap_scan
```

### Step 2: Service Enumeration

- SMB: smbmap, enum4linux, crackmapexec
- RDP: rdpscan, ncrack
- SNMP: snmpwalk
- Databases: mysql, redis-cli

### Step 3: Vulnerability Checks

- Default creds (admin:admin, guest:guest)
- CVE checks with nuclei -t cves/
- Misconfigured services (FTP, MongoDB, Redis)

## 2. Web Assessment (Domains / Subdomains / Web Apps)

Objective: Map web apps, discover hidden content, find parameters, and detect exposures.

### Step 1: Subdomain Enumeration

```
subfinder -d target.com -o subs.txt  
httpx -l subs.txt -o live.txt
```

### Step 2: Content & Directory Discovery

```
ffuf -u https://site.com/FUZZ -w wordlist.txt -mc 200,403,401
```

### Step 3: Parameter Discovery

```
waybackurls site.com | gf xss  
arjun -u https://target.com/page
```

### Step 4: Tech Fingerprinting

- httpx -tech-detect
- Wappalyzer
- CVE checks

### Step 5: Common Exposures

- Config files: .env, .git/, web.config
- Error messages leaking stack traces

## 3. API Assessment (REST, GraphQL, SOAP, gRPC)

Objective: Identify endpoints, parameters, logic flaws, and broken access controls.

### Step 1: Endpoint Discovery

```
ffuf -u https://api.target.com/FUZZ -w api-endpoints.txt
```

### Step 2: Testing REST APIs

- Tools: Burp, Postman
- Check headers, JWTs, API keys
- Try verb tampering (GET, POST, PUT, DELETE)

### Step 3: GraphQL APIs

- Check for introspection (`__schema`)
- Fuzz queries/mutations

### Step 4: SOAP / gRPC

- SOAP: Check `?wsdl` for functions
- gRPC: grpcurl for service enumeration

### Step 5: Common Vulnerabilities

- IDORs
- Weak authentication / missing rate limiting
- Data exposure
- API key leakage

## **4. Continuous Recon (Optional but Powerful)**

- Automate with cronjobs: subfinder, amass, httpx, nuclei - Screenshotting: gowitness, aquatone - Monitor with: Shodan, Censys, LeakIX

### **■ Fact Check Notes**

- Tools and commands are current as of 2025. - Workflow aligns with OWASP Testing Guide, NIST 800-115, and common bug bounty playbooks.