Great 🔥 you’re moving into **WSTG-INFO-05: Enumerate Infrastructure and Application Admin Interfaces**.  
This is a **recon + discovery** step to find **hidden or exposed admin panels**, both for infrastructure and web apps.

**🛠 Enumerate Infrastructure & Application Admin Interfaces**

**🎯 Goal**

Identify **administrative portals** that, if exposed, can be brute-forced, bypassed, or abused.

**1. Common Admin Paths**

Attackers try **default directories** or wordlists:

* /admin/
* /administrator/
* /controlpanel/
* /manage/
* /phpmyadmin/
* /wp-admin/
* /cms/
* /login/

👉 **SecLists** has Discovery/Web-Content/admin-panels.txt with hundreds of common admin endpoints.

**2. Tools & Methods**

**a) Nmap (Port + Service Discovery)**

Check for open admin services:

nmap -sV -p 22,23,80,443,3389,8080,8443 target.com

* **22/SSH** → Infrastructure admin
* **23/Telnet** → Legacy admin
* **3389/RDP** → Windows admin
* **8080, 8443, 10000** → Often Tomcat, Webmin, Jenkins

**b) FFUF / Gobuster / Dirsearch**

Bruteforce admin panels:

ffuf -u http://target.com/FUZZ -w /usr/share/seclists/Discovery/Web-Content/admin-panels.txt

**c) WhatWeb / Wappalyzer**

Identify CMS or frameworks → predict admin panel:

whatweb target.com

Example:

* WordPress → /wp-admin/
* Joomla → /administrator/
* Drupal → /user/login

**d) Search Engines (Google Dorking)**

Find exposed panels indexed by mistake:

inurl:/admin site:target.com

inurl:/login site:target.com

intitle:"phpMyAdmin" "Welcome"

**e) Shodan / Censys**

Enumerate infrastructure remotely:

* Shodan query:
* http.title:"phpMyAdmin"
* http.title:"Jenkins"
* port:3389 country:PK

**3. Examples of Admin Interfaces**

* **Infrastructure**: SSH, RDP, Webmin, cPanel, Plesk
* **Applications**: WordPress Admin, Drupal Console, Tomcat Manager, phpMyAdmin, Jenkins Dashboard

**4. Risk**

* If found, attackers may:
  + Try **default credentials** (admin/admin, root/toor)
  + Attempt **brute force**
  + Exploit **known CVEs** for outdated panels

✅ **Summary**

* Start with **Nmap** for infra ports.
* Use **ffuf + seclists** for admin panel fuzzing.
* Fingerprint apps with **WhatWeb/Wappalyzer** to predict admin paths.
* Search engines (Google/Shodan) can reveal exposed dashboards.

👉 Do you want me to prepare a **step-by-step challenge lab** for this (like “find an exposed WordPress admin” or “locate Tomcat manager”) so you can practice?