**TODAY’S Detailed Approach (Scenario).**

### **Initial Setup & OSINT (Pre-Engagement)**

1. **Connect via AnyDesk:**
   * Get access to the VMBox/Docker environment.
   * Confirming tools are installed (or request installation):
     + Pentesting: Burp Suite, Nmap, Metasploit, OWASP ZAP.
     + OSINT: theHarvester, Shodan, SpiderFoot.
     + Code Analysis: SADT, Bandit (Python), Semgrep.
     + Monitoring: Wazuh, Sysinternals.
2. **OSINT Reconnaissance:**

* Running theHarvester to find subdomains/emails
* Checking for leaks with Shodan
* Documenting findings on GitHub.