|  |  |  |  |
| --- | --- | --- | --- |
| **Criteria** | **Simple (5-7 points)** | **Moderate (8-10 points)** | **Complex (11-15 points)** |
| **Scope & Coverage** | Single vulnerable machine or website with basic security flaws | Multiple systems/services with moderate security controls | Enterprise-like environment with layered defenses (e.g., AD environment, segmented networks) |
| **Reconnaissance** | Basic passive reconnaissance (e.g., Whois, Google Dorking) | Active scanning (e.g., Nmap, DNS enumeration, OSINT) | Advanced OSINT, custom scanning scripts, stealth reconnaissance |
| **Scanning & Enumeration** | Uses automated tools (e.g., Nessus, Nikto) with minimal analysis | Uses multiple tools, manual verification of results, identifies misconfigurations | Deep analysis, manual fuzzing, custom enumeration scripts |
| **Exploitation** | Executes known exploits without modification (e.g., Metasploit default payloads) | Modifies exploits to bypass defenses, performs privilege escalation | Writes custom exploits, bypasses security controls (e.g., IDS/IPS evasion) |
| **Post-Exploitation** | Basic access verification, minimal persistence techniques | Explores file systems, extracts sensitive data, covers tracks | Maintains access, escalates privileges, uses Backdoor..etc |

**Complexity Scoring:**

**25-35 points** → **Simple Project**

**36-50 points** → **Moderate Project**

**51-75 points** → **Complex Project**