Cybersecurity Lab Portfolio Roadmap

# ✅ Phase 1: Completed Labs

|  |  |  |
| --- | --- | --- |
| Lab Name | Focus | Status |
| Cloud IAM Lab | Access management, AWS IAM | ✅ |
| Brute Force SIEM Lab | Log analysis, SIEM correlation | ✅ |

# 🚧 Phase 2: In Progress / Next Labs

|  |  |  |
| --- | --- | --- |
| Lab Name | Focus | Status |
| Malware Analysis Lab | Reverse engineering, behavior analysis | 🛠️ |
| SQL Log Attack Lab | SQL injection, log forensics | 🛠️ |
| 3-Lab Roadmap Package | Combined use-case portfolio PDF | 🛠️ |

# 🔜 Phase 3: Next-Level Labs (To Complete Final Portfolio)

|  |  |  |
| --- | --- | --- |
| Lab Name | Focus | Benefit |
| Threat Hunting with SIEM | Create custom correlation rules, dashboards (Splunk or Wazuh) | Shows real-time threat detection skills |
| Phishing Email Analysis | Decode headers, analyze payloads, link to C2 servers | Proves Blue Team analytical thinking |
| Incident Response Walkthrough | Mock IR scenario with timeline, decisions, report | Shows leadership and decision-making |
| File Integrity Monitoring | Use OSSEC/Wazuh to detect changes in critical files | Covers 'Integrity' pillar |
| Mini Threat Intel Feed | Monitor abuse IPs, Tor exits, hash lookups via APIs | Shows proactive defense and scripting |
| Custom Portfolio Website | Host on GitHub Pages with links to labs + resume PDF | Next-level polish for recruiters |