**Security & Vulnerability Assessment Reports**

**Title:** *Penetration Testing and Compliance Scanning Report for Smart 5G Platform*

**A. Assessment Scope**

| **Area** | **Focus** | **Tools Used** |
| --- | --- | --- |
| Network Perimeter | Firewall and external-facing interface security | Nmap, Nessus, Qualys |
| API Security | OWASP Top 10 vulnerabilities testing | OWASP ZAP, Burp Suite |
| Authentication & IAM | MFA, token validation, role permissions | Custom scripts, manual review |
| Container & Cloud Security | Container hardening, secrets management | Aqua Security, Trivy, Prisma Cloud |
| Compliance Checks | GDPR, 3GPP security standards, local regulations | Compliance scanners, manual checklist |

**B. Findings Summary**

| **Vulnerability** | **Severity** | **Description** | **Remediation Recommendation** |
| --- | --- | --- | --- |
| Open Ports on Firewall | Medium | Unnecessary ports open increasing attack surface | Close unused ports, enforce least privilege |
| Broken Authentication | High | Weak token expiry policy | Implement short-lived tokens and refresh mechanisms |
| Insecure API Endpoints | Medium | Lack of rate limiting on public APIs | Add throttling and IP blacklisting |
| Container Image Vulnerabilities | High | Outdated base images with known CVEs | Patch images, automate vulnerability scanning |
| Insufficient Logging | Low | Limited audit logs for admin actions | Enhance logging and monitoring |

**C. Recommendations**

* Apply security patches and updates promptly.
* Implement strict access control policies and MFA enforcement.
* Use automated vulnerability scanning integrated into CI/CD pipelines.
* Conduct regular penetration tests and security training for staff.
* Maintain compliance documentation and audit trails.