APPLICATION SECURITY

Application Security

Refers to the hardening of an application to prevent it from being misused or exploited and is not limited to just code scanning.

Application Security Threats

Passive Threats

- Weak key management
- Information disclosure
- Storage of credentials in plain text

Application Security Threats

Active Threats

- SQL Injection
- XSS Attacks
- Brute force attacks
- Man-in-the-middle attacks

Application Security Tools

Can be categorized into

- Code
- System
- Availability
- Databases
- Containers

Application Security Tools

Tools for Code

- White box scan (tester has access to all network and system information)
- Peer review
- Tracing function to requirements

Application Security Tools
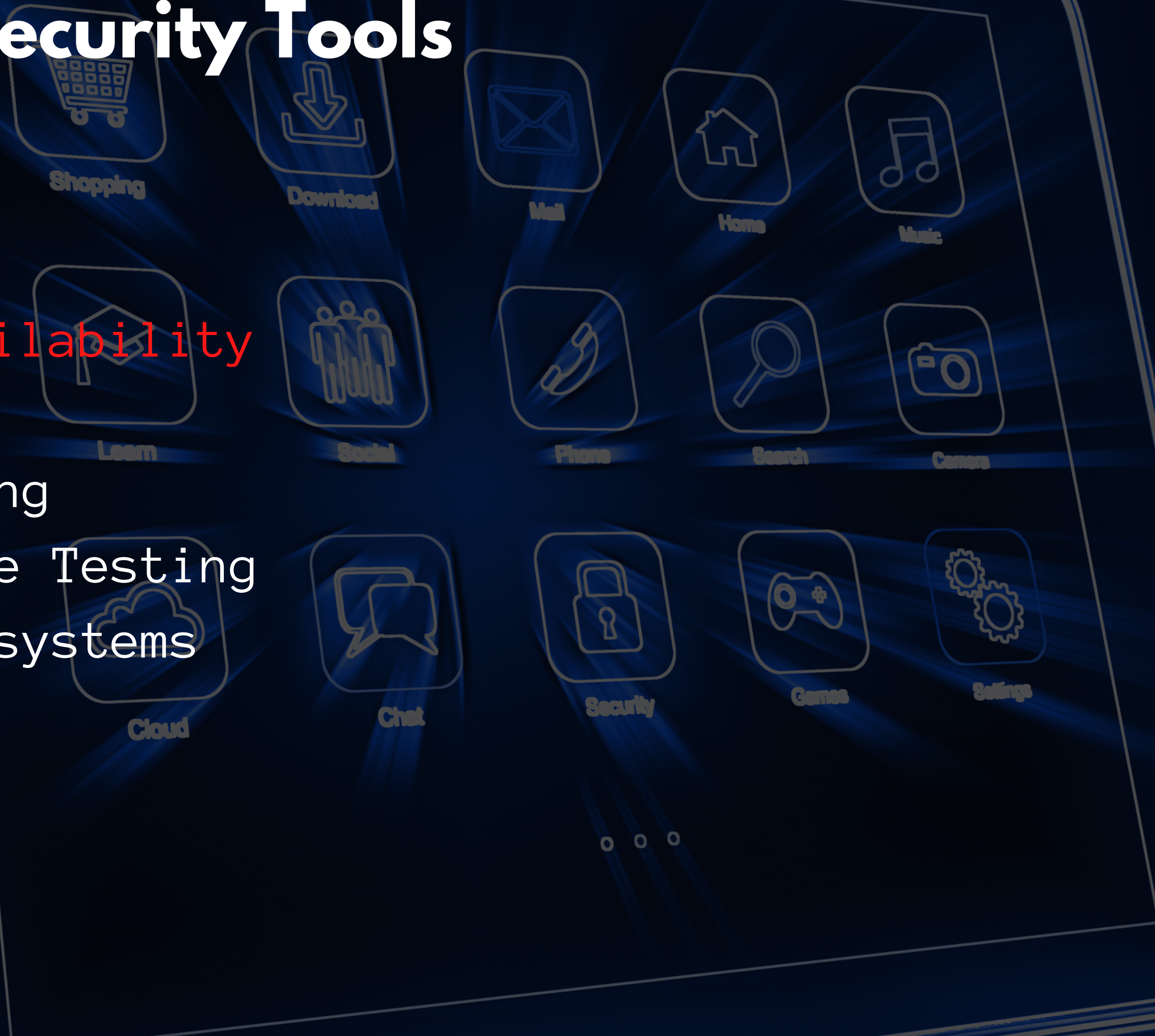
Tools for System

- Black box scan (no info is provided to the tester)
- Penetration testing
- Application firewalls

Application Security Tools

Tools for Availability

- Load Testing
- Performance Testing
- Dependent systems

Application Security Tools

Tools for Databases

- Activity Monitoring
- Limit access channels
- Configuration Management

Application Security Tools

Tools for Containers

- Isolation (Namespaces)
- Cgroups
- Seccomp (used in Linux to restrict the actions available within the container)