Android Application Security Assessments

By Michael Born
Overview

- **Platform Terminology**
  - Component Names
  - Component Purpose
  - Activating Components

- **Lab Setup**
  - Physical Device
  - Android Virtual Device

- **Process**

- **Tools**

- **What To Look For**

- **Demo Assessment**
Platform Terminology

- **Components**
  - Activity
  - Content Provider
  - Service
  - Broadcast Receiver
Platform Terminology

• **Activity**
  – Screen Task

• **Content Provider**
  – Structured Data Task

• **Service**
  – Background Task

• **Broadcast Receiver**
  – System Broadcast Responder Task
Platform Terminology

- **Activation**
  - Intent
  - Intent Filters

- **Intent**
  - Explicit
    - FQCN
    - Own App
  - Implicit
    - General Action
    - Another App
Platform Terminology

- **Intent Filters**
  - Implicit Only
  - Advertises Receivable Intents
    - Action
    - Data
    - Category
  - Per Component
    - Exception: Service
Lab Setup – Physical Device

LAB – Physical Device
Lab – Android Virtual Device

LAB – Emulated Device
Assessment Process

• File System Snapshot
  – Pre-Installation
  – Post-Installation
  – Post-App Use

• File System Review
  – Cache
  – Logs
  – Configuration Files
Assessment Process

- **Application**
  - Authentication
  - Registration
  - Input Injection
  - Encryption
  - Information Storage

- **Web Services**
  - Server Configuration
  - Server Input Validation
  - Cipher Strength
Assessment Process

- Component Tests
  - Exported Activities
    - Permissions
    - Intent Filters
  - Content Providers
    - Permissions
    - Injection
    - Data Retrieval
    - URI Discovery
  - Exported Services
    - Permissions
Assessment Tools

- Linux Commands
  - tree
  - strings
  - diff
- Intercepting Proxy
  - Burp Suite Pro
  - Web Scarab
  - OWASP Zap
Assessment Tools

• Kali Tools
  – Dex2Jar
  – Nmap
  – Wireshark
  – Metasploit
  – JD Gui

• Drozer

• Drozer Agent

• Android SDK
What To Look For

• **OWASP Top 10**
• **Components**
  – Exported Permissions
  – Input Injection
  – Data Retrieval
  – Authentication Bypass
• **Encryption**
  – Present
  – Cipher Strength
  – SSL/TLS Version

• **Sensitive Data**
  – Cache
  – Logs
  – Manifest
• **Application**
  – Input
  – Authentication
  – Password Strength
  – Certificate Pinning
What To Look For

- **Web Services**
  - Server Misconfiguration
  - Server Side Validation
  - Enumeration
    - Payment Type
    - Payment Info
    - Usernames
    - Other Sensitive Information
Further Reading

• Android Developer Guides
  – http://developer.android.com

• Drozer User Manual
  – https://www.mwrinfosecurity.com/products/drozer

• Vulnerable Android App Sieve
  – https://www.mwrinfosecurity.com/products/drozer

• OWASP Mobile Top 10
Android Demo

DEMO
Thank You!