Mobile Exploitation – NSC Training

Abstract

Even wondered how different attacking a Mobile application would be, from a traditional web application? Gone are the days when knowledge of just SQL Injection or XSS could help you land a lucrative high-paying infoSec job.

After a sold out class as multiple conferences over the last few years, we have revamped the material to include a host of new tools and techniques. This will be an introductory course on exploiting iOS and Android applications, suited well for both beginners as well as advanced security enthusiasts. We now also cover ARM and OS exploitation techniques. The training will be based on exploiting Damn Vulnerable iOS app, Android-InsecureBankv2 and a large range of real-world applications in order to give an in-depth knowledge about the different kinds of vulnerabilities in Mobile applications. This is an extensive hands-on class where the students will be exploiting all of these taught vulnerabilities. The course will also discuss how an attacker can secure their application using secure coding & obfuscation techniques. After the workshop, the students will be able to successfully pentest applications running on the various operating systems.

The training will also include a CTF challenge in the end where the attendees will use their skills learnt in the training to solve the CTF challenges. The students will be provided with Slides, tools and VMs used during the course. The students will also be provided with video guides to replicate all of the techniques learnt in the class for once the training ends.

Course Outline

Part 1 - iOS Exploitation

Module 1 : Getting Started with iOS Pentesting

iOS security model

App Signing, Sandboxing and Provisioning

Setting up XCode 8

Changes in iOS 11

Primer to iOS 11 security

Exploring the iOS filesystem

Intro to Objective-C and Swift4

What's new in Swift 4 ?

Setting up the pentesting environment

Jailbreaking your device

Cydia, Mobile Substrate

Getting started with Damn Vulnerable iOS app

Binary analysis

Finding shared libraries

Checking for PIE, ARC

Decrypting ipa files

Self signing IPA files

Module 2: iOS exploitation basics

How jailbreak exploits are written ?

Diffing for Patches

Intro to ARM assembly

ROP, KASLR and KPP

Use after free, Heap overflow basics

Reversing the Kernel

Code signing bypass techniques

Sanbox bypass techniques

Exploiting Mach Ports

Chaining exploits

Patching the Kernel

Achieving persistence

Module 3 : Static and Dynamic Analysis of iOS Apps

Static Analysis of iOS applications

Dumping class information

Insecure local data storage

Dumping Keychain

Finding url schemes

Dynamic Analysis of iOS applications

Cycript basics

Advanced Runtime Manipulation using Cycript

Method Swizzling

GDB basic usage

Modifying ARM registers

Basic App Exploitation techniques using Frida

Advance App Exploitation techniques using Frida

Module 4 : iOS application vulnerabilities

Exploiting iOS applications

Broken Cryptography

Side channel data leakage

Sensitive information disclosure

Exploiting URL schemes

Client side injection

Bypassing jailbreak, piracy checks

Inspecting Network traffic

Traffic interception over HTTP, HTTPs

Manipulating network traffic

Bypassing SSL pinning

Module 5 : Reversing iOS Apps

Introduction to Hopper

Disassembling methods

Modifying assembly instructions

Patching App Binary

Logify

Module 6 : Securing iOS Apps

Securing iOS applications

Where to look for vulnerabilities in code?

Code obfuscation techniques

Piracy/Jailbreak checks

iMAS, Encrypted Core Data

Part 2 - Android Exploitation

Module 1

Why Android

Intro to Android

Android Security Architecture

Android application structure

Signing Android applications

ADB – Non Root

Rooting Android devices

ADB – Rooted

Understanding Android file system

Permission Model Flaws

Attack Surfaces for Android applications

Module 2

Understanding Android Components

Introducing Android Emulator

Introducing Android AVD

Module 3

Proxying Android Traffic

Reverse Engineering for Android Apps

Smali Learning Labs

Smali vs Java

Dex Analysis and Obfuscation

Android App Hooking

Module 4

Exploiting Local Storage

Exploiting Weak Cryptography

Exploiting Side Channel Data Leakage

Manual and Automated Root Detection and Bypass

Exploiting Weak Authorization mechanism

Identifying and Exploiting flawed Broadcast Receivers

Identifying and Exploiting flawed Intents

Identifying and Exploiting Vulnerable Activity Components

Exploiting Backup and Debuggable apps

Analysing Proguard, DexGuard and other Obfuscation Techniques

Exploiting Android NDK

Manual and Automated SSL Pinning Bypass techniques

Module 5

App Exploitation using Drozer

Basic App Exploitation techniques using Frida

Advance App Exploitation techniques using Frida

App Exploitation using AppMon

Automated source code analysis

Detecting Leaks in Android Apps