Advanced
ANDROID & iOS
Hands-on Exploitation

By **Attify**

Trainers

Aditya Gupta

Prerequisite

The participants are expected to have a basic knowledge of Mobile Operating Systems. Knowledge of programming languages (**Java and C, and Python for scripting**) will be an added advantage to grasp things quickly.

Hardware Requirements

Minimum **2GB RAM** and **20 GB free Hard Disk space**
Android (preferably Rooted) >= 2.3
iPhone/iPad/iPod (optional, as we will be providing individual iOS based devices for each participant during the training)

Software Requirements

Windows XP SP2/3, Windows 7/8 or *Nix
Mac OSX 10.5+ (compulsory for iOS Exploitation or a OSX VM)
Administrative privileges on your laptop
Virtualization Software
Custom VM labs will be provided for exploitation
SSH Client

COURSE STRUCTURE

Day I (Android and ARM Exploitation):

Module 1:

Android Basics

- Introduction to Android
- Android Architecture
- Digging into Android kernel

Android Security Model

- Android Security Architecture
- Android Permission model
- Application Sandboxing
- Bypassing Android Permissions

HelloWorld : Android

- Android Application Components
- Android Debug Bridge
- Creating a Simple Android Application

Introduction to ARM Exploitation

- Introduction to ARM
- Instruction set and Registers
- Debugging with GDB
- Stack Overflows on ARM
- Format String vulnerabilities
- Ret2ZP Attack and ROP
- Shellcoding on ARM
- Exploit Mitigations and Bypasses
- ARM Based rootkits

Module 2:

Setting up the Environment

- Setting up Android Emulator
- Setting up a Mobile Pentest Environment

App Kung-fu

- Application Analysis
- Reverse Engineering
- Traffic Interception (Active and Passive) of Android Applications
- OWASP Top 10 for Android
- Sniffing Application and phone's network data
- Unsecure file storage
- Having fun with databases

Exploiting Logic and Code flaws in applications

- Exploiting Content Providers
- SQL Injection in Android Application
- Local File Inclusion/Directory Traversal
- Drive by Exploitation
- Tapjacking
- HTML 5 Attacks
- Phishing Attacks on Android

Module 3:

Exploitation with AFE

- Introduction to Android Framework for Exploitation
- Finding application vulnerabilities using AFE
- Creating a malware + botnet (HTTP and SMS based)
- Crypt an existing malware/botnet to bypass Android Anti-malwares
- Extending the framework with custom plugins
- Cracking Android Applications
- Hands-on on Vulnerable Social Networking Application
- Creating and Exploiting custom ROMs
- Exploiting USB connections with Android

Dex Labs

- Introduction to Dalvik File Format
- In-depth to Smali
- Manipulating smali files and cracking Applications
- Cracking Application Licenses
- Dex file manipulation
- Obfuscating applications with dex obfuscator

Day 2 (Advanced Android and ARM Exploitation)

Module 4:

Android Forensics & Malware Analysis

- Extracting text messages, voice mails, call logs, contacts and messages
- Recovering information stored in SD Card
- Reversing and Analyzing Android malwares using Apktool, dex2jar and JD-GUI
- Introduction to IDA Pro
- Analyzing malwares and exploits using IDA

Further Exploitation:

- Creating custom Bootloaders
- Android Root Exploits – Recreating the exploit
- Fuzzing Android components
- Webkit Exploitation
- Use After Free vulnerability and exploitation
- Writing a reliable exploit for Android
- More ROP Exploitation
- Finding ROP gadgets and building ROP Chains
- Using GDB for Android debugging
- Information Leaks in Android

Being secure

- Android in the Enterprise
- Writing Secure Code
- Pentest before you publish

- Writing Python Scripts for automating android pentests
- Source Code Auditing for Applications

Day 3 (iOS Exploitation)

Module 5:

iOS Background

- Understanding iOS Architecture
- iOS Security Features
- iOS Application Overview

iOS Security Model

- Code Signing
- Sandboxing
- Exploit Mitigation
- Encryption

Setting up the Environment

- Setting up XCode
- Setting up iPhone/Simulator

Module 6:

iOS Hello-World

- iOS Application components
- Introduction to Objective C
- Writing a simple Hello World application in your own iDevice/Simulator

iOS App Analysis

- Reverse Engineering iOS Apps
- Decrypting Appstore Binaries
- Locating PIE (Position Independent Executable)
- Inspecting Binary
- Manipulating Runtime

Module 7:

Auditing Insecure API

- Evaluating the Transport Security
- Abusing Protocol Handlers
- Insecure Data Storage
- Attacking iOS keychain

App Assessments

- Setting up pentesting environment for assessment
- Passive app assessment
- Active app assessment
- Application analysis

App Kungfu

- Exploiting XSS in Apps (UIWebViews)
- Attacking XML processor
- SQL Injection
- Filesystem Interaction
- Geolocation
- Logging
- Background-ing

Memory Corruption Issues:

- Format strings
- Object use-after free
- ROP for iOS
- Exploit Mitigations in iOS

Module 8:

iOS Forensics

- Analysis of Backed up data in iTunes
- Extracting SMS, Call Logs, etc., from an iOS backup
- Imaging the whole device

Being Secure

- iOS App compliance checklist
- Writing Secure Codes
- Pentest your App before you publish