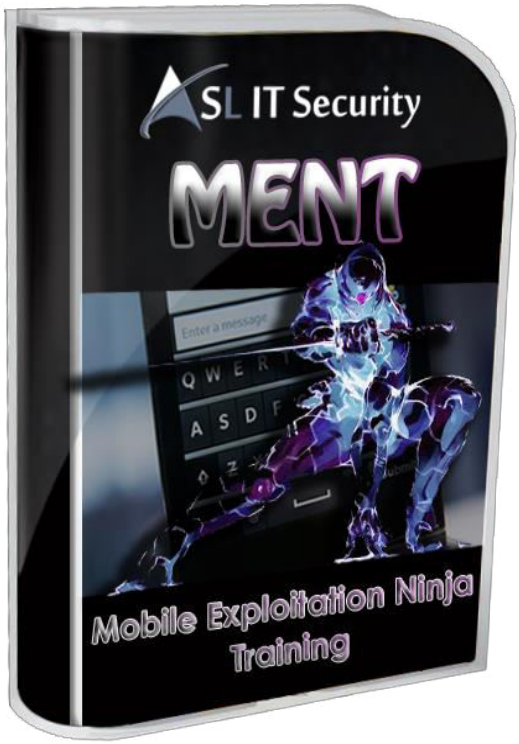
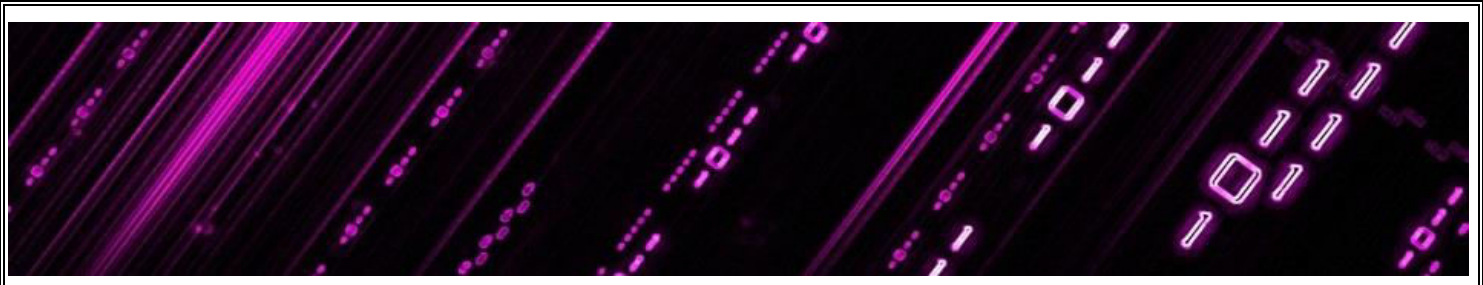
ASL IT SECURITY

MOBILE EXPLOITATION NINJA TRAINING



V 1.0

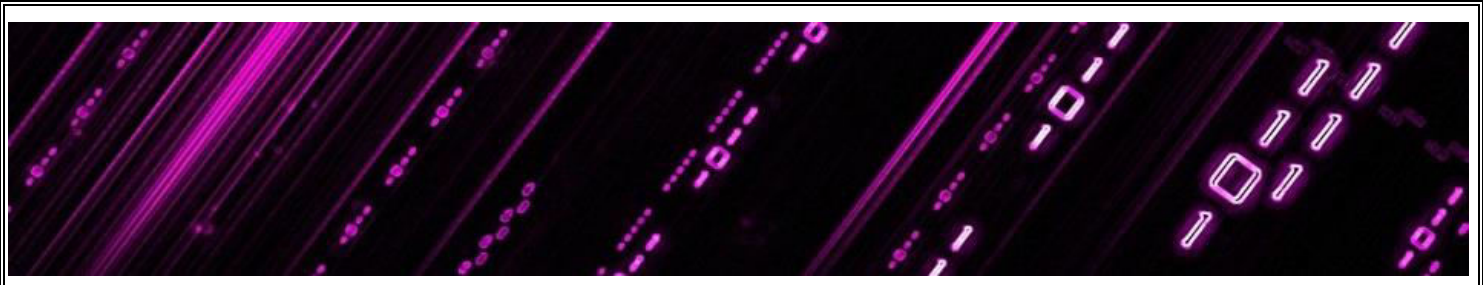


Overview: This training is an advanced and offensive version of Android, iOS and ARM Exploitation. It covers much in-depth security issues and automation in terms of security analysis and creating own tools for analyzing mobile applications and code.

Description: Mobile Exploitation Ninja Training is a unique training which covers security and exploitation of the two dominant mobile platforms - Android and iOS. This is a three day action packed class, full of hands-on challenges and CTF labs, for both Android and iOS environment. The entire class will be based on a custom VM which has been prepared exclusively for the training. The training will take the attendees from the ground level upwards to be able to audit any real world applications on the platforms.

Some of the topics that will be covered are Advanced Auditing of iOS and Android Applications, Reverse Engineering, Bypassing Obfuscations, Automating security analysis, Exploiting and patching apps, Advanced ARM Exploitation, API Hooking and a lot more.

The 3-day class is designed in a CTF approach where each of the module is followed by a complete hands-on lab, giving the attendees a chance to apply the knowledge and skills learnt during the class in real life scenario. Students will also be provided with the author signed copy of the book "Learning Pentesting for Android Devices", printed reference materials and handouts to be used during and after the training class, and private scripts written by the trainer for Android and iOS app security analysis.



Trainers:

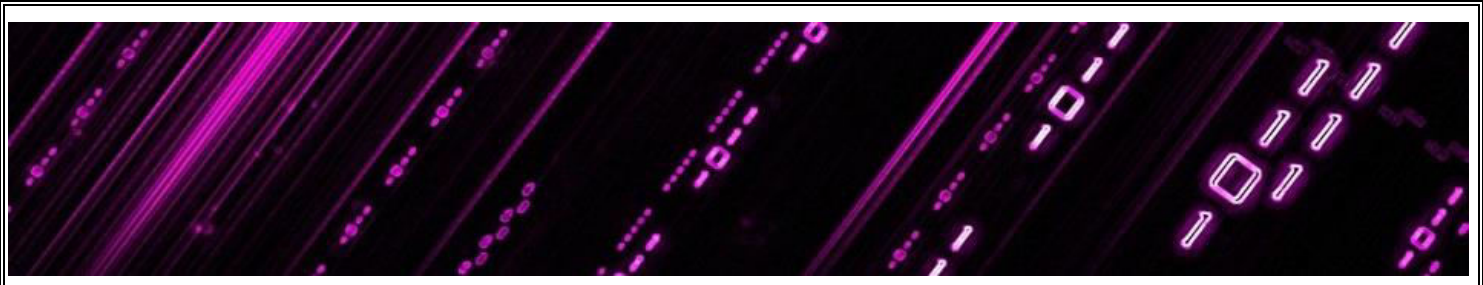
Aditya Gupta is a leading mobile security expert and evangelist. Apart from being the lead developer and co-creator of Android framework for exploitation, he has done a lot of in-depth research on the security of mobile devices, including Android, iOS, and Blackberry, as well as BYOD Enterprise Security.

He is also the author of the popular Android security book "Learning Pentesting for Android" selling over 5000+ copies, since the time of launch in March 2014. He has also discovered serious web application security flaws in websites such as Google, Facebook, PayPal, Apple, Microsoft, Adobe, Skype, and many more.

In his previous work at Rediff.com, his main responsibilities were to look after web application security and lead security automation. He also developed several internal security tools for the organization to handle the security issues. He has also previously spoken and trained at numerous international security conferences including BlackHat, Syscan, OWASP AppSec, Toorcon, Clubhack, Nullcon etc, along with many other corporate trainings on Mobile Security.

Deliverables :

Learning Pentesting for Android Devices - Author signed Copy
Custom VM Labs ISO for the entire training
Training Reference Material
Students Handouts
Additional Reading Materials for iOS, Android and ARM(PDF)

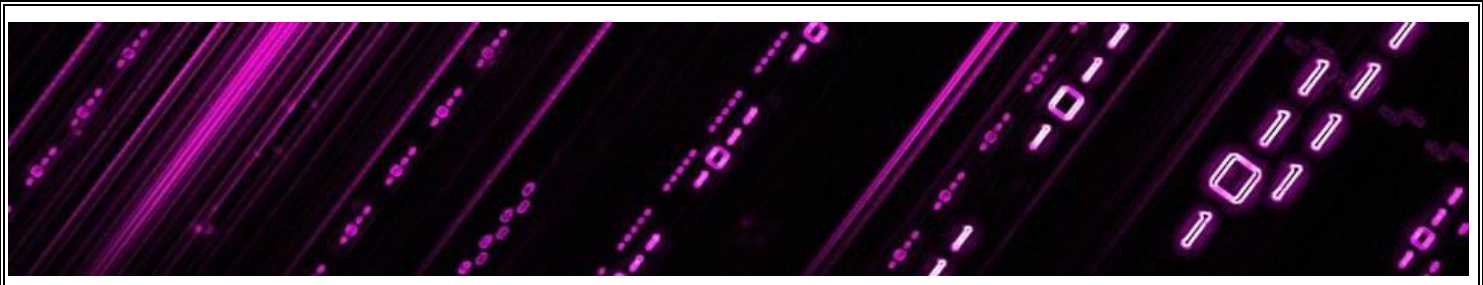


Module 1 : Diving into Android

1. Setting up a Mobile Pentest Environment
2. Android Security Architecture
3. Permission Model Flaws
4. Getting familiar with ADB
5. Activity and Package Manager Essentials
6. API level vulnerabilities
7. Rooting for Pentesters Lab
8. Android ART and DVM Insecurities

Module 2 : Android App for Security Professionals

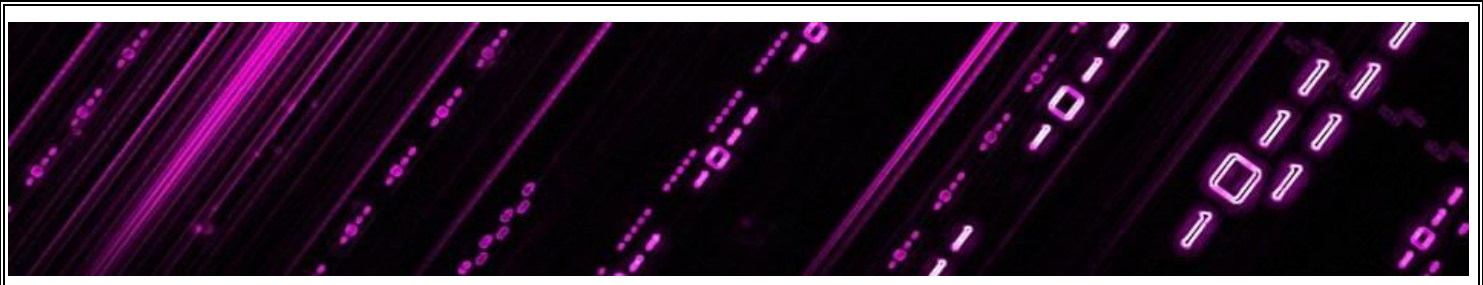
1. Security Analysis of AndroidManifest.xml
2. Reverse Engineering for Android Apps
3. Smali for Android 101
4. Smali Labs for Android
5. Cracking and Patching Android apps
6. Understanding Dalvik
7. Dex Analysis and Obfuscation
8. Android Application Hooking



9. Using JDB and Andbug
10. Dynamic Dalvik Instrumentation for App Analysis
11. Introspy for Android
12. Creating custom Hooks

Module 3 : Application Specific Vulnerabilities

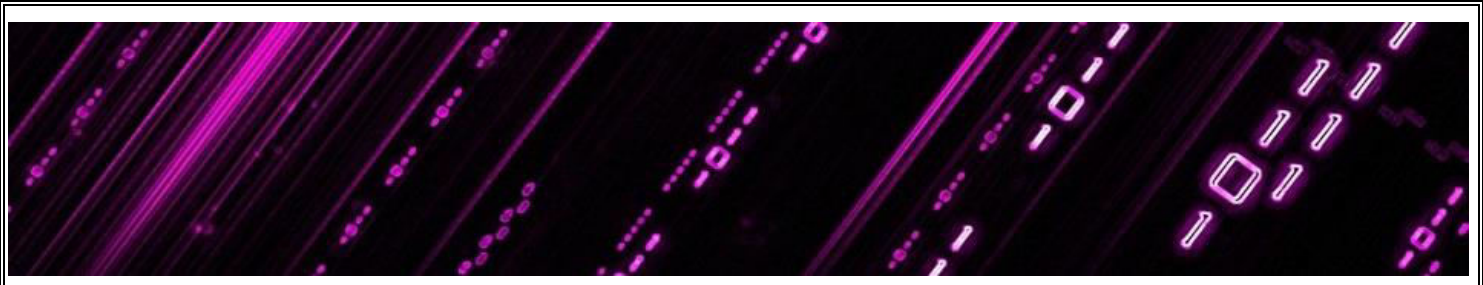
1. Static Analysis of Android Apps
2. Attack Surfaces for Android applications
3. Exploiting Side Channel Data Leakage
4. Exploiting and identifying vulnerable IPCs
5. Exploiting Backup and Debuggable apps
6. Exploiting Exported Components
7. Webview based vulnerabilities
8. Dynamic Analysis for Android Apps
9. Logging Based Vulnerabilities
10. Insecure Data Storage
11. Network Traffic Interception
12. Analysing Network based weaknesses
13. Exploiting Secure applications



14. Analysing Proguard, DexGuard and other Obfuscation Techniques
15. OWASP Mobile Top 10
16. Using Drozer for Exploitation
17. Writing custom Modules for Drozer
18. Analysing Android apps using Androguard
19. Analysing Native Libraries
20. Security Issues in Hybrid Apps

Module 4 : ARM for Android Exploitation

1. Getting familiar with Android ARM
2. ARM Architecture and Calling conventions
3. Debugging with GDB
4. Using IDA for Android
5. Exploiting Overflow based vulnerabilities
6. ROP Labs for Android
7. Use After Free vulns
8. Writing your own reliable exploit
9. Race Condition vulns
10. Hardware Exploitation Techniques
11. Exploit Mitigation and Protections



Module 5 : Getting Started with iOS Pentesting

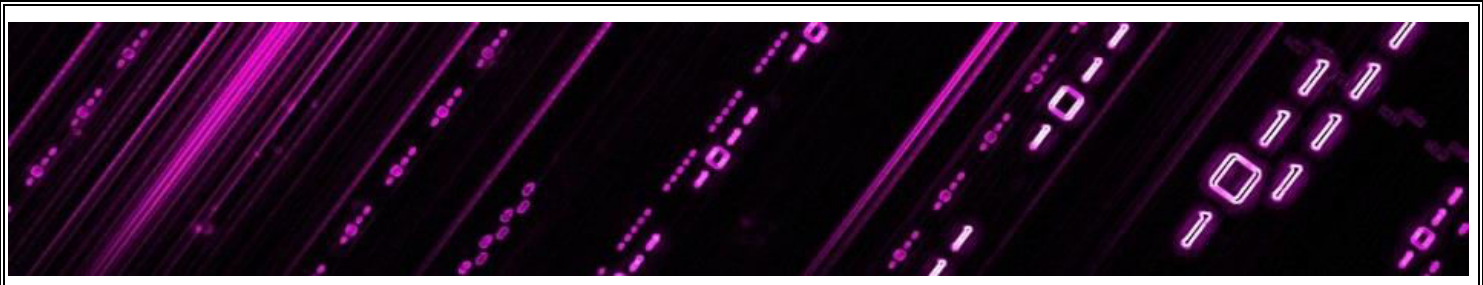
1. iOS security model
2. App Signing, Sandboxing and Provisioning
3. Setting up XCode
4. Changes in iOS 8
5. Exploring the iOS filesystem
6. Intro to Objective-C and Swift

Module 6 : Setting up the pentesting environment

1. Jailbreaking your device
2. Cydia, Mobile Substrate
3. Getting started with Damn Vulnerable iOS app
4. Binary analysis
5. Finding shared libraries
6. Checking for PIE, ARC
7. Decrypting ipa files
8. Self signing IPA files

Module 7 : Static and Dynamic Analysis of iOS Apps

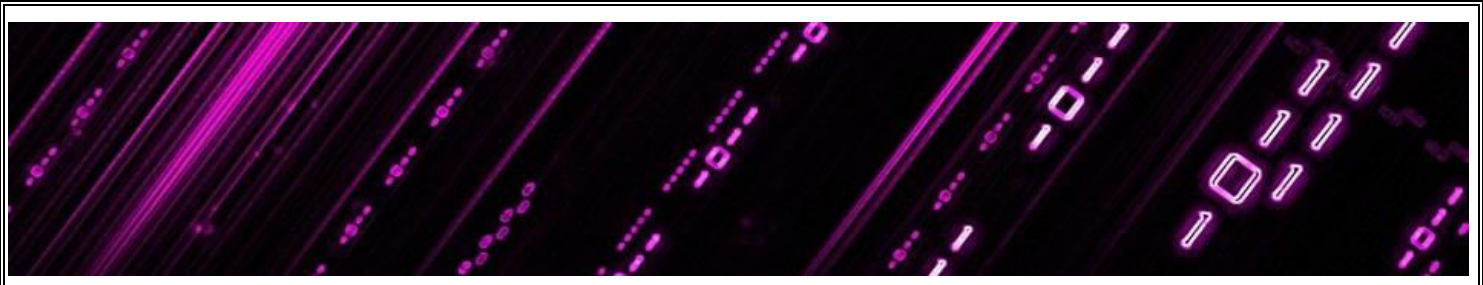
1. Static Analysis of iOS applications
2. Dumping class information



3. Insecure local data storage
4. Dumping Keychain
5. Finding url schemes
6. Dynamic Analysis of iOS applications
7. Cycript basics
8. Advanced Runtime Manipulation using Cycript
9. Writing patches using Theos
10. Method Swizzling
11. GDB basic usage
12. GDB kung fu with iOS

Module 8 : Exploiting iOS Applications

1. Broken Cryptography
2. Side channel data leakage
3. Sensitive information disclosure
4. Exploiting URL schemes
5. Client side injection
6. Bypassing jailbreak, piracy checks
7. Inspecting Network traffic
8. Traffic interception over HTTP, HTTPs
9. Manipulating network traffic



10. Bypassing SSL pinning

Module 9 : Reversing iOS Apps

1. Introduction to Hopper
2. Disassembling methods
3. Modifying assembly instructions
4. Patching App Binary
5. Logify, Introspy, iNalyzer, Snoopit

Module 10 : Securing iOS Apps

1. Securing iOS applications
2. Where to look for vulnerabilities in code?
3. Code obfuscation techniques
4. Piracy/Jailbreak checks
5. iMAS, Encrypted Core Data