ClubHACK

Android Tamer

By

Anant Shrivastava

http://anantshri.info

ClubHACK

Agenda

- Android and Security
- Tool set available Right Now
- Android Tamer VM
    - Source Code Analysis
    - Application Development
    - Security Analysis Applications
    - ROM analysis
    - Code Injection
- Demo's

ClubHACK

Android

- +40% Phone Market
- +10% Tablet Market
- Manufacturer support : LG,Samsung,SE & more
- Supported by Google
- Linux Based

ClubHACK

Why Security Review

- Emerging Market.
- Smart phones.
- Easily acessible
- Emerging Target for malware distribution.
- Simply Put whole PC malacious life cycle is getting repeated in Mobile Domain

ClubHACK

How and What to perform

- We Need to perform
  - Application / Platform / Protocol Testing
  - Malacious Apps / website testing
  - Rom Analysis / Modification
- How We perform
  - Setup toolset on every machine and still no standards.

ClubHACK

What's the solution

- Define Some standards.
  - OWASP is working on it.
- Design some ToolKit
  - Basically we need BT style toolkit for android.

Presenting

Android Tamer

ClubHACK

What is Android Tamer

- VM environment Giving you the freedom to perform
  - Application Pentesting
  - Malware Analysis
  - Rom Modification (Core + kernel)
  - ROM Analysis
  - App / Malware / Native Code Development

ClubHACK

Salient Features

- Based on Ubuntu 10.04 LTS
- All non needed software removed.
- Minimum mix of foreign repositories to avoid upgrade issues.
- Not just tool dump but integrated solution.
- Browser bookmarks.
- Tamer Repository configured to avoid re-download of complete VDI image. (contains only one package as of now)

ClubHACK

Tools : Application Pentesting

- OWASP ZAP
- TSOCK Proxy
- Emulator configured with ZAP certificate.
- Custom Link Given to launch specific AVD.
- DDMS configured

ClubHACK

Tools : Malware Analysis

- DroidBox
- APKInspector
- Apktool
- Dex2jar /JAD / DED / JD-GUI
- Smali / baksmali
- androguard

ClubHACK

Tools : ROM Analysis / Modification

- DSIXDA Android Kitchen
- Unyaffs2
- Split_bootimg
- DDMS

- Refer Tools : Development and Malware analysis

ClubHACK

Tools : Development

- Eclipse + ADT
- NDK
- CodeSourcery C++ lite
- ARM DS-5 CE

ClubHACK

Tools : Rooting tools

- Scripts
  - Rageinthecage
  - Psneuter
  - Gingerbreak
  - ZergRush
- APK's
  - Z4root
  - Superoneclick
  - Universal Androot

Note : tools provided AS-IS, usage is a responsibility of USER

ClubHACK

Important Links

https://sourceforge.net/p/androidtamer/

ClubHACK

Future

- Plan to keep it going.
- Applications will be distributed using Tamer Repository (preconfigured)
- Tools and Categories to add
  - Agnitio: Source code review
  - Forensics Section.
- If you know some other cool tools that could be added send in a mail.

ClubHACK

About Me

Anant Shrivastava
CEH, RHCE
Interested in Android, Linux, Web 2.0
Member of Null and G4H

•Email : anant@anantshri.info
•Web : http://anantshri.info
•Blog : http://blog.anantshri.info