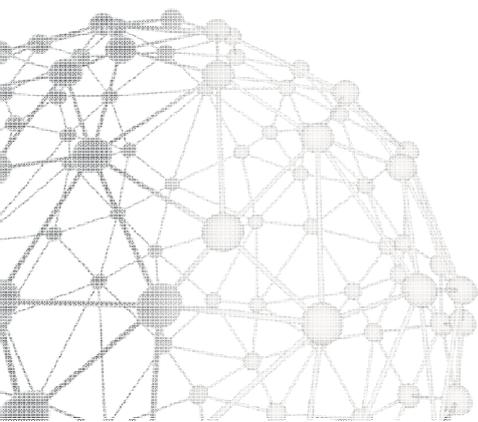


]Hacking**Team**[

REMOTE CONTROL SYSTEM  
GALILEO

Advanced Training Agenda

VERSION  
1.4.3



## 1<sup>st</sup> Session: Welcome and Introduction

10:00 am

**Mostapha Maanna** Key Account Manager  
**Alessandro Scarafile** Field Application Engineer

## 2<sup>nd</sup> Session: RCS Galileo Architecture

10:30 am

**Alessandro Scarafile** Field Application Engineer

- Advanced Architecture and Systems Requirements
- Backend and Frontend Advanced Configuration (scripts)
- Anonymizers Configuration

### Lunch break

## 3<sup>rd</sup> Session: Accounting and Operations

02:30 pm

**Alessandro Scarafile** Field Application Engineer

- Users, Groups and Advanced Permissions Configuration
- Operations and Targets Configuration

*HANDS-ON: Creating training local Users, Groups, Operations and Targets*

## 4<sup>th</sup> Session: Intelligence

04:30 pm

**Alessandro Scarafile** Field Application Engineer

- Intelligence Logic and Capabilities
- Entities and Links Creation

*HANDS-ON: Creating training local Person, Position and Virtual Entities*

## 5<sup>th</sup> Session: Desktop Factories Configuration

10:00 am

**Alessandro Scarafile** Field Application Engineer

- Desktop Factories Introduction
- Desktop Events, Actions and Modules Configuration

*HANDS-ON: Creating and configuring desktop advanced Factories*

Lunch break

## 6<sup>th</sup> Session: Desktop Infection Agents

02:30 pm

**Alessandro Scarafile** Field Application Engineer

- Silent Installer Explanation
- Melted Application Explanation
- U3 Installation Explanation
- Offline Installation Explanation
- Exploit Explanation
- Network Injector Explanation

*HANDS-ON: Building desktop Agents*

## 7<sup>th</sup> Session: Tactical Network Injector

10:00 am

[Alessandro Scarafile](#) Field Application Engineer

- Tactical Control Center Overview
- Rules Creation and Configuration
- Target Identification Methods
- INJECT-EXE Infection Explanation
- INJECT-HTML-FLASH Infection Explanation
- INJECT-FILE Infection Explanation
- REPLACE Infection Explanation
- Wireless Intruder Usage
- Fake Access Point Usage

*HANDS-ON: Configuring Tactical Network Injector rules based on different infection actions*  
*HANDS-ON: Practicing with Wireless Intruder and Fake Access Point tools*

Lunch break

## 8<sup>th</sup> Session: Network Injector Appliance

02:30 pm

[Alessandro Scarafile](#) Field Application Engineer

- Connecting the Appliance

## 9<sup>th</sup> Session: Mobile Factories Configuration

10:00 am

**Alessandro Scarafile** Field Application Engineer

- Mobile Factories Introduction
- Mobile Events, Actions and Modules Configuration

*HANDS-ON: Creating and configuring mobile advanced Factories*

Lunch break

## 10<sup>th</sup> Session: Mobile Infection Agents

02:30 pm

**Alessandro Scarafile** Field Application Engineer

- Local Installation Explanation
- Installation Package Explanation
- Melted Application Explanation
- Wap Push Message Explanation
- QR Code / Web Link Explanation
- Exploit Explanation

*HANDS-ON: Building mobile Agents*

## 11<sup>th</sup> Session: Dashboard and Alerting

10:00 am

**Alessandro Scarafile** Field Application Engineer

- Understanding Evidences
- Data Export, Tagging and Report Creation
- Alerting Events, Types and Auto-Tagging

*HANDS-ON: Tagging evidences and creating a report*

*HAND-ON: Creating alerts based on incoming evidences*

## 12<sup>th</sup> Session: System Maintenance

11:00 am

**Alessandro Scarafile** Field Application Engineer

- Backup: Jobs Configuration
- Connectors: Data Export for Third-Party Software
- Audit: Understanding Audit Entries
- Monitor: Tracking RCS Components
- Investigation Wizard and Archive Wizard

Lunch break

## 13<sup>th</sup> Session: Q&A

02:30 pm

**Mostapha Maanna** Key Account Manager  
**Alessandro Scarafile** Field Application Engineer

- Specific Scenario Analysis
- Training Questions and Answers



]Hacking**Team**[

RELEASE DATE  
Nov 20, 2013