]HackingTeam[

Remote Control System

Da Vinci

Knowledge transfer agenda

November 17th – December 12th

Week 1 - Day 1

Fulvio de Giovanni, Field Application Engineer
Alessandro Scarafile, Field Application Engineer

Network configuration and setup for RCS

- Environment preparation
- Switch configuration and setup

Week 1 - Day 2

Fulvio de Giovanni, Field Application Engineer
Alessandro Scarafile, Field Application Engineer

RCS 8.1.5 Installation

- Installation of RCS 8.1.5 Backend
- Installation of RCS 8.1.5 Collector
- Installation of RCS Consoles on 2 PC's

Week 1 - Day 3

Fulvio de Giovanni, Field Application Engineer
Alessandro Scarafile, Field Application Engineer

Introduction to RCS

- Brief introduction to RCS

RCS Console: Accounting & Dashboard

- Accounting Menu
  - Users
  - Groups
- The RCS Dashboard

Week 1 - Day 4

Fulvio de Giovanni, Field Application Engineer
Alessandro Scarafile, Field Application Engineer

Operations Management

- Operations “tree”
- A person as a Target
- Concept of Factory

Week 1 - Day 5

Fulvio de Giovanni, Field Application Engineer
Alessandro Scarafile, Field Application Engineer

Conclusions

- Q&A
- Next week agenda

Week 2 - Day 1

Fulvio de Giovanni, Field Application Engineer

A Glance on computer networks

- TCP/IP
  - Ip addressing
  - Computer ports
- Some Application Layer Protocols
  - DNS
  - DHCP
  - HTTP
  - HTTPS
- Switches, Firewalls and vlans

Week 2 - Day 2

Fulvio de Giovanni, Field Application Engineer

Server-side infrastructure

- Da Vinci system suggested architecture
  - Vlans creation and firewall rules
- Processes and services
  - RCS Folders
  - Collector (Collector & Network Controller)
  - Masternode (RCS-DB, RCS-Master)
  - Database (Workers and Shards)
- Data Flow

Week 2 - Day 3

Fulvio de Giovanni, Field Application Engineer

Mission management

- Target lifecycle
- Agent statuses
- Factories Vs Agents
    - Configuration changes
- Basic conf. Vs. Advanced conf.
- The Event-driven schema
    - Events
    - Actions and sub actions
    - Modules
    - Connecting arrows
- Interacting with your agent
    - Best practices
- What you should never do

Week 2 - Day 4

Fulvio de Giovanni, Field Application Engineer

System Management

- Backup Management
- Status check and configuration tools
  - rcs-configure
  - rcs-log
  - rcs-status
- System monitoring and Troubleshooting

Accessing the Support Portal

- HackingTeam Ticketing system
- Installing certificates and connecting to http://support.hackingteam.com

Week 2 - Day 5

Fulvio de Giovanni, Field Application Engineer

Conclusions

- Q&A
- Next week agenda

Week 3 - Day 1

Marco Catino, Field Application Engineer

Recap on RCS Server-side infrastructure

- Da Vinci Components
  - Anonymizer
  - Collector
  - Masternode
  - Shards
- Processes and services
  - Collector (*Collector & Network Controller*)
  - Masternode (*RCS-DB, RCS-Master*)
  - Database (*Workers and Shards*)
- Data Flow

Operations Management

- Operations
- Target
- Factories vs Agents
- Desktop Agent basic configuration

Week 3 - Day 2

Marco Catino, Field Application Engineer

Desktop Infection

- Desktop Agent advanced configuration
- Agent management
- Silent Installer build and infection test
- Hands On: Desktop Agent advanced configuration

Week 3 - Day 3

Marco Catino, Field Application Engineer

Evidence Analysis

- Evidence Analysis
  - Detailed view
  - Summary view
  - Relevance
  - Report customization
- Evidence export

Week 3 - Day 4

Marco Catino, Field Application Engineer

Desktop Advanced Configuration Recap & Hands On

- Desktop Agent advanced configuration: Recap
- Hands On: Desktop Agent advanced configuration

Week 3 - Day 5

Marco Catino, Field Application Engineer

Week 4 - Day 1

Marco Catino, Field Application Engineer

Desktop Infection Vectors

- Infection vectors for Desktop
- Hands on: tests with different infection vectors

Desktop Advanced Configuration Recap & Hands On

- Desktop Agent advanced configuration: Recap
- Hands On: Desktop Agent advanced configuration

Week 4 - Day 2

Marco Catino, Field Application Engineer

Desktop Agent Management

- Browsing the File System
- Downloading files when you know the path
- Uploading files and executing processes
- Checking the commands output
- Hands on: exercises

Desktop Infection Vectors and Advanced Configuration Hands On

- Infection vectors for Desktop
- Advanced Configuration for Desktop
- Hands on: test with different infection vectors

Week 4 - Day 3

Marco Catino, Field Application Engineer

RCS 8.2

- System update to RCS 8.2.2
- New Features in RCS 8.2
- First contact with the Scout Agent

Week 4 - Day 4

Marco Catino, Field Application Engineer

Monitor & System

- Console: Monitor section
- Console: System Section

Troubleshooting

- Usage of rcs-scripts
- Reading of logs

Week 4 - Day 5

Marco Catino, Field Application Engineer

Conclusions

- Q&A
- Next Session:
  - TNI
  - Troubleshooting
  - RCS for Mobile
  - Other Platforms

Contacts:

Mostapha Maanna	+393351725432 mostapha@hackingteam.com
Marco Catino	+393665676136 m.catino@hackingteam.com
Fulvio de Giovanni	+393666335128 fulvio@hackingteam.com
Alessandro Scarafile	+393386906194 a.scarafile@hackingteam.com