]HackingTeam[

REMOTE CONTROL SYSTEM

GALILEO

Self Assessment Test
(Trainer)

VERSION
1.2

Purpose

This Self Assessment Test consists of 8 sections that aim to test the proper use of RCS Galileo.

The test is intended to be executed after RCS Galileo Advanced Training held at the client's premises or at Hacking Team headquarter.

According to client's product license, one or more sections of this document may be not available for client's installation: these sections (4, 6) will not eventually be considered for final evaluation.

Section	Points Available	
1. RCS Galileo Architecture	15	
2. Accounting Management	10	
3. Operations Management	10	
4. Intelligence Management	10	*optional*
5. Factories Configuration	25	
6. Network Injector Management	10	*optional*
7. Alerting Management	5	
8. System Maintenance	15	

The highest score the trainees can get is 100, which can drops to 90 and 80 due to optional sections.
The thresholds to consider the test passed are respectively 75, 65 and 60.

1. RCS Galileo Architecture

15 PTs

1.1 Choose the minimum set of components for RCS Galileo installation and usage

3 PTs

a. ○ 1 Master Node, 1 Shard, 1 Collector and 1 Anonymizer
b. ➲ 1 Master Node, 1 Shard, 1 Collector, 1 Anonymizer and 1 Console
c. ○ 1 Master Node, 2 Shards, 1 Collector, 2 Anonymizers and 2 Consoles
d. ○ 2 Master Nodes, 2 Shards, 2 Collectors, 2 Anonymizers and 1 Console
e. ○ None of above

1.2 Choose the correct path followed by evidences from device to database

3 PTs

a. ○ Agent > Collector > Anonymizer 1 > Anonymizer 2 > Master Node
b. ○ Agent > Collector > Master Node > Anonymizer 1 > Anonymizer 2
c. ○ Anonymizer 1 > Anonymizer 2 > Master Node > Collector
d. ➲ Agent > Anonymizer 1 > Anonymizer 2 > Collector > Master Node
e. ○ None of above

1.3 Choose the most safe network configuration for RCS Galileo

3 PTs

a. ➲ Master Node on LAN, Collector on DMZ and Anonymizer on Internet
b. ○ Master Node on DMZ, Collector on LAN and Anonymizer on Internet
c. ○ Master Node, Collector and Anonymizer on Internet
d. ○ Master Node and Collector on DMZ and Anonymizer on Internet
e. ○ None of above

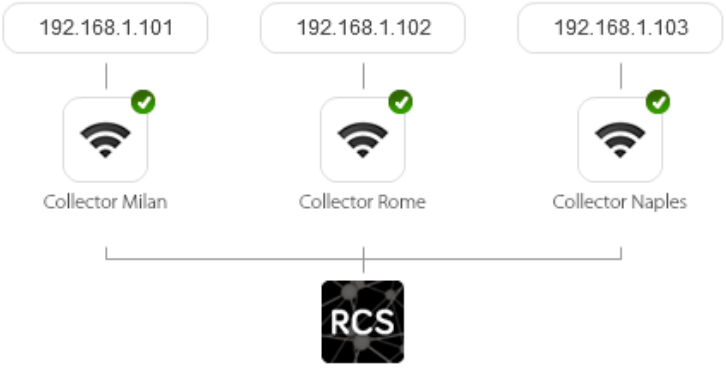
1.4 According to image below, how many additional Shards have been added?

3 PTs

a. ○ 0, because 2 Shards are automatically created during RCS Galileo installation
b. ○ 0, because 3 Shards are automatically created during RCS Galileo installation
c. ➲ 1, because 1 Shard is automatically created during RCS Galileo installation
d. ○ 2, because no Shards are created during RCS Galileo installation
e. ○ None of above

1.5 According to image below, how many Anonymizers need to be configured?

3 PTs



a. ○ 0, because it's possible to directly synchronize evidences on the 3 Collectors
b. ○ 1, because RCS Galileo can serve multiple Collectors just configuring 1 Anonymizer
c. ○ 2, because the first Collector is managed independently
d. ➲ 3, because each Collector needs at least 1 Anonymizer in order to work
e. ○ None of above

2. Accounting Management

10 PTs

2.1 What are the four different User roles in RCS Galileo?

2 PTs

a. ○ Administrator, Console Administrator, Technician and Evidence Analyst
b. ○ Administrator, Operator Manager, Agent Builder and Evidence Analyst
c. ○ Console Administrator, System Administrator, Operator and Analyst
d. ○ System Administrator, Administrator, Technician and Operator
e. ➲ Administrator, System Administrator, Technician and Evidence Analyst

2.2 Which User role is allowed to create Users and Groups?

2 PTs

a. ○ Evidence Analyst
b. ○ Technician
c. ○ System Administrator
d. ➲ Administrator
e. ○ System Administrator and Administrator

2.3 Which User role is allowed to update RCS Galileo license?

2 PTs

a. ○ Evidence Analyst
b. ○ Technician
c. ○ System Administrator
d. ➲ Administrator
e. ○ System Administrator and Administrator

2.4 Which User role is allowed to create and configure Factories?

2 PTs

a. ○ Evidence Analyst
b. ➲ Technician
c. ○ System Administrator
d. ○ Administrator
e. ○ Technician and Administrator

2.5 How many Users can be assigned to the same Group?

2 PTs

a. ○ 1
b. ○ 5
c. ○ 10
d. ➲ The maximum number allowed by the license
e. ○ None of above

3. Operations Management

10 PTs

3.1 How many Operations can be active simultaneously?

2 PTs

a. ○ 1
b. ○ 10
c. ➲ Unlimited
d. ○ It depends on the license
e. ○ None of above

3.2 Choose the correct order for RCS Galileo objects creation

2 PTs

a. ➲ User > Group > Operation > Target > Factory > Agent
b. ○ User > Group > Operation > Factory > Target > Agent
c. ○ User > Group > Target > Operation > Factory > Agent
d. ○ User > Group > Operation > Agent > Factory
e. ○ None of above

3.3 Choose the movements you can perform on objects within Operations tab

2 PTs

a. ○ Can move an Operation between two Groups
b. ○ Can move a Target between two Operations
c. ○ Can move an Agent between two Targets
d. ➲ b. and c.
e. ○ None of above

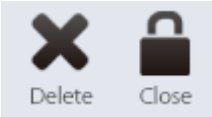
3.4 Choose the objects you can add to the Dashboard within Operations tab

2 PTs

a. ○ User, Group, Operation and Target
b. ○ Group, Operation, Target and Agent
c. ➲ Operation, Target and Agent
d. ○ Target and Agent
e. ○ None of above

3.5 Which is the difference between Close and Delete actions on an Agent?

2 PTs



a. ○ Close will uninfect the device, Delete will delete evidences keeping the device infected
b. ➲ Close will uninfect the device, Delete will Close and also delete all collected evidences
c. ○ There're no differences between Close and Delete actions if applied on an Agent
d. ○ It's not possible to delete an Agent, you can only close it
e. ○ None of above

4. Intelligence Management

10 PTs

4.1 How Operations are created within Intelligence tab?

2 PTs

a. ○ Manually, by console operator
b. ○ Manually, duplicating it from Operations tab
c. ○ Manually (within Operations tab) or automatically (within Intelligence tab)
d. ➲ Automatically, according to the number of Operations
e. ○ Automatically, according to the number of Operations and Targets

4.2 How many different types of Entities can you create within Intelligence tab?

2 PTs

a. ○ 1: Target
b. ○ 2: Person and Position
c. ➲ 3: Person, Position and Virtual
d. ○ 4: Target, Person, Position and Virtual
e. ○ None of above

4.3 How many different types of Links can you create within Intelligence tab?

2 PTs

a. ○ 1: Peer
b. ➲ 2: Peer and Know
c. ○ 3: Peer, Friend and Knowledge
d. ○ Unlimited: Peer, Know and others defined by console operator
e. ○ None of above

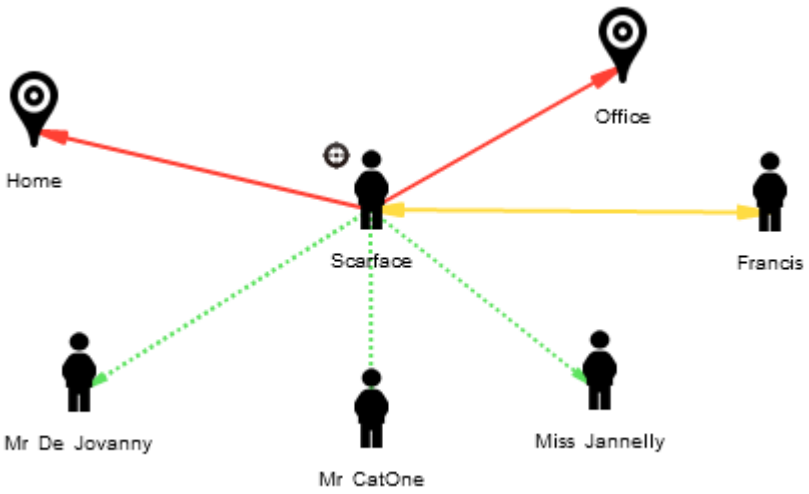
4.4 Choose the available ways to quickly move between Entity and Target

2 PTs

a. ○ Jump directly from Target to Entity
b. ○ Jump directly from Entity to Target
c. ○ Jump directly from Target to Entity, but not from Entity to Target (evidences needed)
d. ➲ a. and b.
e. ○ a. and c.

4.5 According to graph below, how many partners in crime our target Scarface has?

2 PTs



a. ○ 0
b. ➲ 1
c. ○ 2
d. ○ 3
e. ○ 4

5. Factories Management

25 PTs

5.1 How many Agents can you build with the same Factory?

2 PTs

a. ○ 1
b. ○ The maximum number chosen during system installation
c. ○ The maximum number allowed by the license
d. ➲ Unlimited
e. ○ None of above

5.2 What is a Scout?

2 PTs

a. ○ It's the first backdoor configuration sent to the Target
b. ➲ It's a lighter version of the real backdoor (Elite) for Windows platform only
c. ○ It's a lighter version of the real backdoor (Elite) for Desktop platforms only
d. ○ It's a modified version of the real backdoor (Elite) in case of antivirus detection
e. ○ None of above

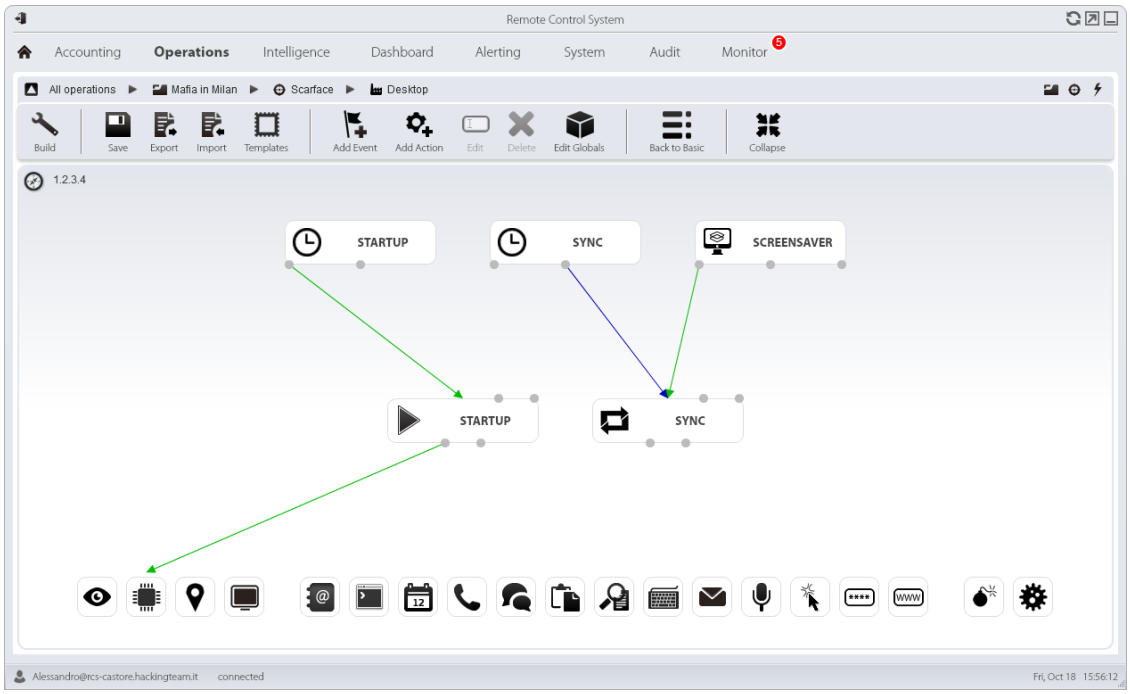
5.3 Which Module allows to record Target's Facebook friends?

3 PTs

a. ○ Device
b. ○ Application
c. ○ Chat
d. ○ Url
e. ➲ None of above

5.4 What the following Factory configuration does?

3 PTs



a. ◯ Synchronizes evidences every time the target configures the screensaver
b. ◯ Synchronizes evidences continuously while the screensaver is running
c. ◯ Synchronizes evidences every time the screensaver ends
d. ⬬ Synchronizes evidences every time the screensaver starts
e. ◯ None of above

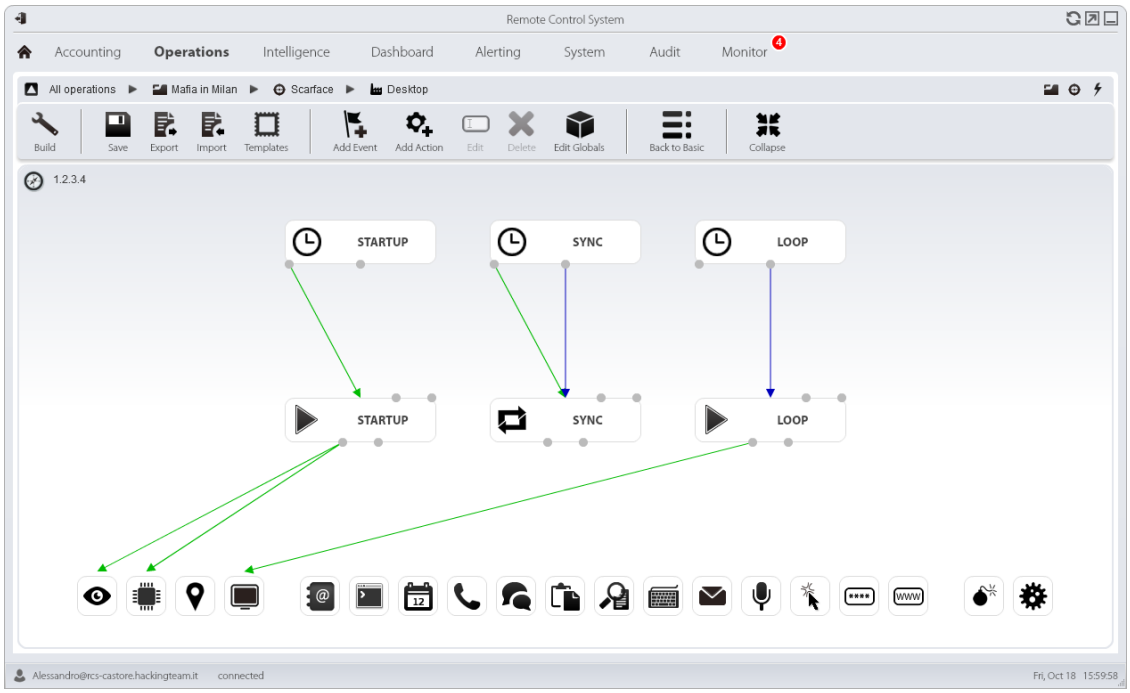
5.5 How many different Synchronization sub-actions can you create?

3 PTs

a. ◯ 1
b. ⬬ Unlimited
c. ◯ It depends on the Collectors number
d. ◯ It depends on the license
e. ◯ None of above

5.6 What the following Factory configuration does?

3 PTs



a. ○ Records 1 Camera snapshot and 1 Screenshot
b. ○ Records multiple Camera snapshot and multiple Screenshots
c. ○ Records multiple Camera snapshots and 1 Screenshot
d. ● Records 1 Camera snapshot and multiple Screenshots
e. ○ None of above

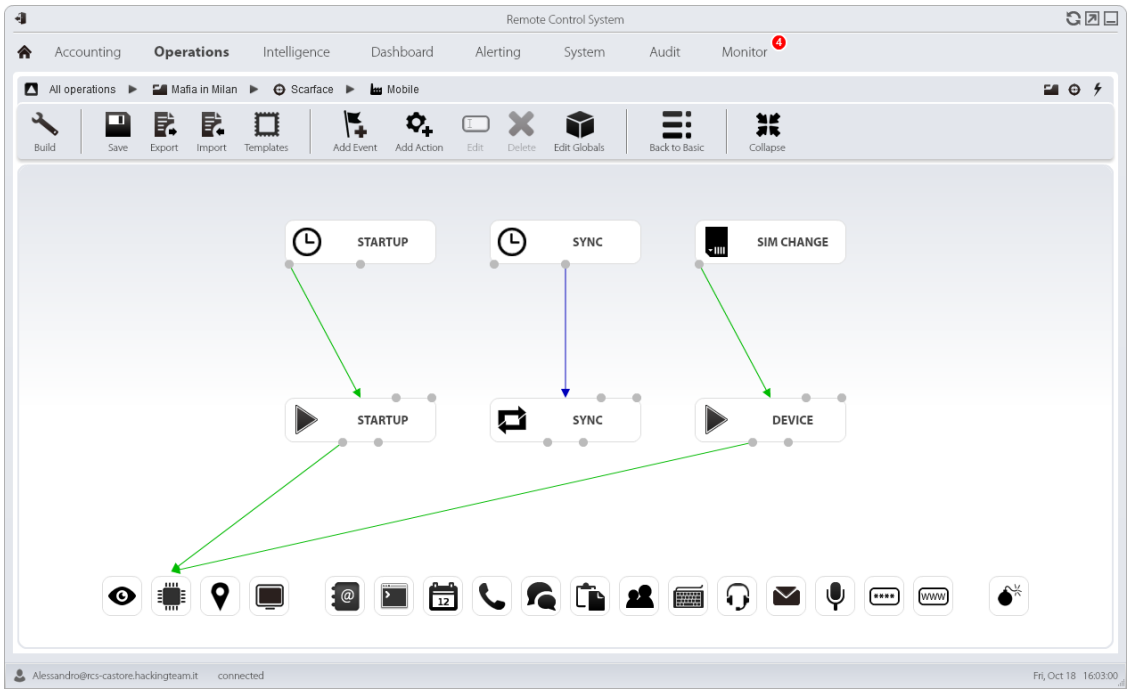
5.7 Which Event can you use to allow to the Agent detect that Skype is running?

3 PTs

a. ○ Event = Process, Type = Process ID, Value = *skype*
b. ○ Event = Process, Type = Window title, Value = *skype*
c. ● Event = Process, Type = Process name, Value = Skype.exe
d. ○ Event = WinEvent, Event ID = 1, Source = *skype*
e. ○ None of above

5.8 What the following Factory configuration does?

3 PTs



a. ○ Records Device information every time the SIM card is removed
b. ➲ Records Device information every time the SIM card is changed
c. ○ Records Device information every time the SIM card is activated
d. ○ Records Device information every time the device enters standby mode
e. ○ None of above

5.9 What does the “Force Cell” flag within Mobile Synchronization configuration?

3 PTs

a. ○ Allows Synchronization via GSM only if Wifi is disabled
b. ○ Forces Synchronization via GSM avoiding Wifi (even if enabled)
c. ➲ Allows Synchronization via GSM after Wifi check
d. ○ Forces Synchronization via GSM using a custom APN
e. ○ None of above

6. Network Injector Management

10 PTs

6.1 Which User role is allowed to create and update Network Injectors?

2 PTs

a. ○ Administrator
b. ➲ System Administrator
c. ○ Technician
d. ○ Evidence Analyst
e. ○ None of above

6.2 Which User role is allowed to create and modify Network Injectors rules?

2 PTs

a. ○ Administrator
b. ○ System Administrator
c. ➲ Technician
d. ○ Evidence Analyst
e. ○ b. and c.

6.3 How many Network Injectors can you create within System tab?

2 PTs

a. ○ Unlimited
b. ○ It depends on the Collectors number
c. ○ It depends on the Anonymizers number
d. ➲ It depends on the license
e. ○ None of above

6.4 Which are the correct Action and Resource pattern to infect any EXE files?

2 PTs

a. ○ Action = INJECT-EXE, Resource pattern = exe
b. ○ Action = INJECT-EXE, Resource pattern = *.exe
c. ➲ Action = INJECT-EXE, Resource pattern = *.exe*
d. ○ Action = INJECT-HTML-FILE, Resource pattern = [exe]
e. ○ None of above

6.5 What does the "INJECT-HTML-FLASH" Action within Rule configuration window?

2 PTs

a. ○ Allows to infect a target that is updating Adobe Flash Player
b. ➲ Allows to infect a target that is trying to open a video on YouTube website
c. ○ Allows to infect a target that is viewing HTML source code of a web page
d. ○ Allows to infect a target that is visiting Adobe website
e. ○ None of above

7. Alerting Management

5 PTs

7.1 Choose the objects you can add to Alerting within Operations tab

2 PTs

a. ○ User, Group, Operation, Target, Factory and Agent
b. ○ Operation, Target, Factory and Agent
c. ○ Target, Factory and Agent
d. ➲ Factory and Agent
e. ○ None of above

7.2 Which types of Alerts are available within Alerting tab?

3 PTs

a. ○ Log
b. ○ Mail
c. ○ SMS
d. ➲ a. and b.
e. ○ b. and c.

8. System Maintenance

15 PTs

8.1 Which path provides access to Backend's maintenance scripts?

3 PTs

a. ○ C:\RCS\DB\
b. ➲ C:\RCS\DB\bin
c. ○ C:\RCS\DB\config
d. ○ C:\RCS\setup
e. ○ None of above

8.2 How many Anonymizers can you add within System tab?

3 PTs

a. ○ 2
b. ○ Unlimited
c. ➲ It depends on the license
d. ○ It depends on the Collectors number
e. ○ None of above

8.3 Which is the right Backup type for Users restoration only?

3 PTs

a. ➲ Metadata
b. ○ Full
c. ○ Operation
d. ○ Target
e. ○ Any

8.4 How often are old entries deleted from Audit tab?

3 PTs

a. ○ Every Console restart
b. ○ Every month
c. ○ Every year
d. ➲ They are never deleted
e. ○ None of above

8.5 What the Monitor tab does?

3 PTs

a. ➲ Allows to monitor all RCS Galileo services and provides license information
b. ○ Allows to monitor all RCS Galileo services and provides access to Support System
c. ○ Allows to monitor all Backend (Master Node) services
d. ○ Allows to monitor all Frontend (Collector) services
e. ○ None of above

]HackingTeam[

RELEASE DATE
Nov 20, 2013