Breaking the Lab

V1.33-- Last update: 10/19/2022 by Tamas Pasztor ([Tamas.pasztor@verint.com](mailto:Tamas.pasztor@verint.com))

Documentation for the excercise scripts breaking / fixing the recorder functions.

## Overview

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Status** | **Role** | **Function name** | **Impact to the recording (what’s seen by the user?)** | **Root cause (what’s broken?)** |
| 1 | QA | Recorder | Break-AvayaMRPassCode | MultipleRegistration stations will fail to register | Extension password changed |
| 2 | QA | Recorder | Break-NICConfiguration | Capture will fail | invalid network interface |
| 3 | QA | Archiver | Break-ArchiveMedia | Archive media will become faulty | invalid share name |
| 4 | QA | Recorder | Break-CallsBuffer | Capturing stops | missing buffer |
| 5 | QA | RIS | Break-TSAPI | Missing CTI from Avaya TSAPI | AES disconnected |
| 6 | DEV | RIS | Break-Extensions | Extensions no longer being monitored / recorded | ? |
| 7 | QA | Agent PC | Break-SCMRis | Screen capturing will fail always | incorrect RIS address specified |
| 8 | TODO | RIS | Break-HuntGroup | Tagging will fail | non-defined hunt group |
| 9 | TODO | (multiple) | Break-AppServerAddress | No marking and archiving | App server location changed |
| 10 | PLAN | RIS |  | Remove CTI adapter |  |
| 11 | PLAN | RIS |  | Disable CTI adapter |  |
| 12 | PLAN | DC?? |  | Archive user account – change password |  |
| 13 | PLAN | archiver?? |  | Local drive maopping – change name |  |
| 14 | PLAN | RIS |  | Breaking TLINK definition in adapter conf |  |
| 15 | PH2 | RIS |  | Insecure (TLS) without actual tls |  |
| 16 | PLAN | Agent PC |  | Stop capture service |  |
| 17 | PLAN | RIS |  | Agent lan datasource entry removed |  |
| 18 | PLAN | RIS |  | Screen subnet change |  |
| 19 | PLAN | RIS |  | Screen recording rule percentage to 0% -generic |  |
| 20 | PLAN | RIS |  | Screen recording rule percentage to 0% -per user |  |
| 21 | PLAN | Agent PC |  | Stop listener + wcapw32b |  |
| 22 | PLAN | Recorder |  | Wcap.dll removed |  |
| 23 | PLAN | RIS |  | RecordAlways vs. DoNotRecord |  |
| 24 | PLAN | Recorder |  | Enter MAINTENANCE MODE |  |

## Specifications

(TODO)

How to run PS1 file AS administrator?:???

At the moment..

Desired: doubleclick shortcut..

A shortcut is put onto the desktop with Powershell.exe <script.ps1>

Target: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle hidden "C:\Users\installuser.WFO\Documents\btl\_v1.ps1"

Any functionality that is broken should be explicitly described as „alarm seen” / „this or that not working”. User must be able to find the root cause and fix the problem.

The config files determined by the individual scripts will have a file name format of [\\server\d$\folder\etc\FileName.xml](file:///\\server\d$\folder\etc\FileName.xml)

We presume %IMPACT360SOFTWAREDIR% is uniform, pointing to E:\Impact360\Software\.

Although in the current lab, each role has exactly one server assigned, but breaking anything should be applied to all the roles available. (or random)

Breaking the agent PC should be treated as an exception, since none of the agent pc addresses can be determined from the existing configuration002Eus

In order to work on desktop…

Hostname needs to be determinable. Currentlz hardcoded

Win RM needs to be enabled as automatic$$$

Innovation lab – consolidated

## Installuser should be part of CONSTRAINING1\Remote Management Users

To solve the problem, UAC filtering for local accounts must be disabled by creating the following DWORD registry entry and setting its value to 1:

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] LocalAccountTokenFilterPolicy

Additional Information

Set-Item WSMan:\localhost\Client\TrustedHosts -Value \*

Enable-PSRemoting -Force

Set-Service WinRM -ComputerName $servers -startuptype Automatic

## PS WSMan:\localhost\Service> winrm qc

## WinRM service is already running on this machine.

## WinRM is not set up to allow remote access to this machine for management.

## The following changes must be made:

## Configure LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.

## GUI

The script needs to be run as administrator (rightclick, run as administrator) in order to be able to perform the admin operations.

Table

Description automatically generated with medium confidence

Each row corresponds to a given excercise, „Fix” will only work once „Broken”.