HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

COMPUTER SCIENCE

User Manual

System Readiness Inspector

Authors:

Claudio Mattes
claudio.mattes@hsr.ch

Lukas Kellenberger
lukas.kellenberger@hsr.ch

Departement Computer Sciences
HSR University of Applied Sciences Rapperswil
CH-8640 Rapperswil, Switzerland

December 15, 2018

Contents

General Information

1.1 System Overview

The "System Readiness Inspector" is a PowerShell tool that helps you to check the readiness of a system to detect advanced persistent threats and lateral movement.After the SRI ran successfully it generates a PDF-Document showing wrong or missung configurations. The SRI was developed during a student research project by the two bachelor of science in computer science students, Claudio Mattes and Lukas Kellenberger.

The SRI has four different modes: Online, Offline, GroupPolicy, AllGroupPolicies. The online mode is limited to the current system and thus determines readiness. The offline mode is used to be able to make a statement about any system by means of exports. The GroupPolicy mode is limited to a specific Group Policy, which is checked for its audit settings. In the AllGroupPolicies mode, all group policies of the current domain are examined.

1.2 Organization of the Manual

The user manual consists of five parts:

- **General Information:**
  The General Information section explains the tool and the purpose for which it is intended.

- **System Requirements:**
  The System Requirements section provides a general overview of the system requirements. Which operating systems are supported, what software must be pre-installed, and what authorizations the user must have.

- **Getting Started:**
  The Getting Started section explains how to obtain and install the SRI on your device.

- **Using SRI:**
  The Use SRI section provides a detailed description of the system functions.

System Requirements

2.1 Operating System

The SRI runs on all Windows 10 Pro operated systems as well as on all servers with the operating system Windows Server 2016.

2.2 User Authorizations

To run the SRI successfully the user needs administrator rights.

2.3 Pre-Installed Software

To enable the SRI to read the Resultant Set of Policies, the Remote Server Administration Tools must be installed on the device.

This Microsoft tool can be downloaded here:
https://www.microsoft.com/en-us/download/details.aspx?id=45520

It is easy to install with just a few clicks.

Getting Started

3.1 Download

You can find the latest version of the SRI in this GitHub repository:

https://github.com/clma91/studythesis/

You download a ZIP folder, which has to be unpacked first.

3.2 Installation

You have either downloaded SRI from the official GitHub repository or received it from another source. No further installation is required. The SRI is ready to use.

Using SRI

4.1 Starting SRI

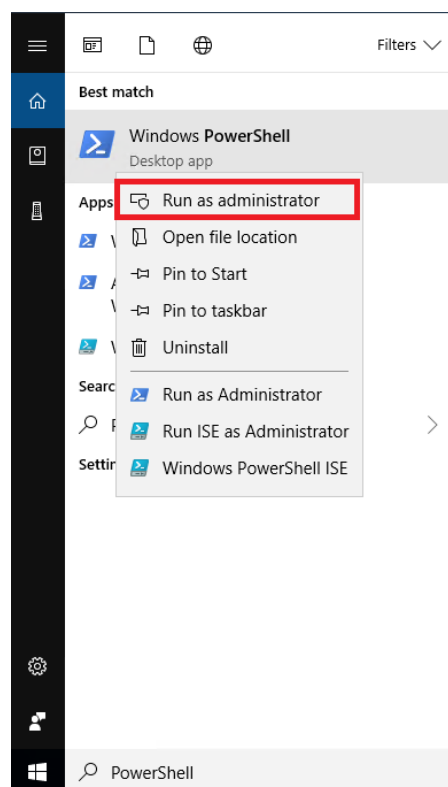Open Windows PowerShell as administrator:

Figure 4.1: Open PowerShell as Administrator
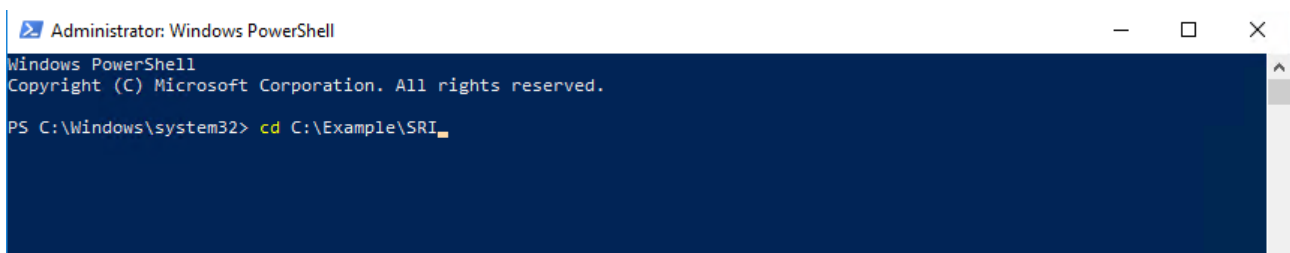
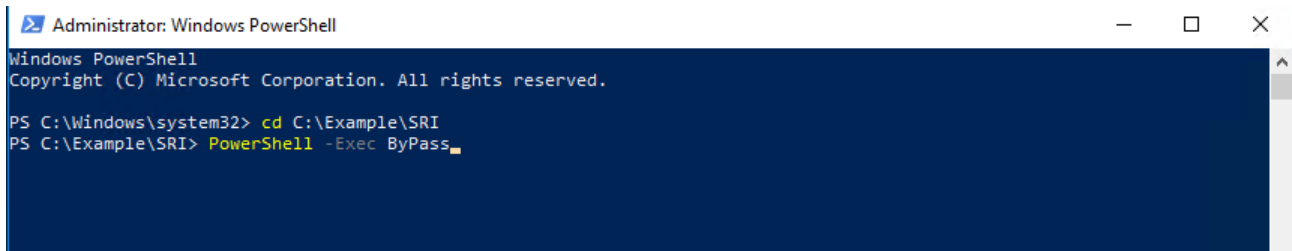Navigate to the path the SRI is saved:

Figure 4.2: Navigate to SRI

PowerShell is by default not allowed to run scripts. We have to change that to be able to run the SRI.
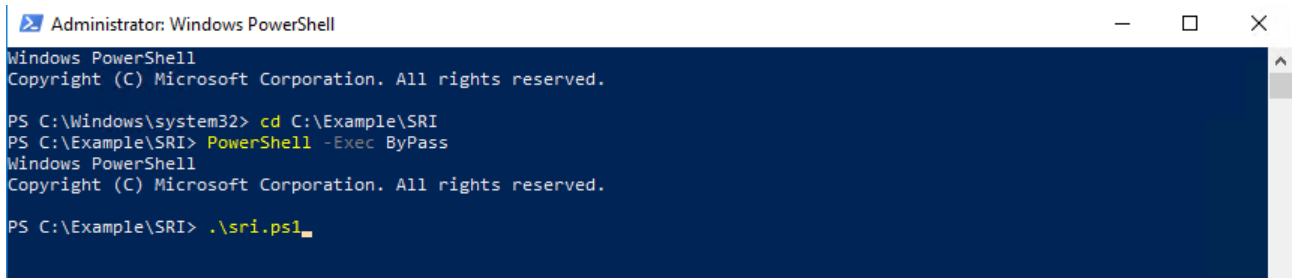Enter the command "PowerShell -Exec Bypass".

Figure 4.3: PowerShell Bypass

Now you can run the SRI by open the sri.ps1 file. You find more details to the different modes in the
section below.

Figure 4.4: PowerShell Bypass

4.2   SRI modes

As described in General Information there are four different modes to run the SRI. These modes are
described more precisely in this chapter. These are the four modes:

- *-Online, -Offline, -GroupPolicy and -AllGroupPolicies*

```
1  PS C:\>./sri.ps1 [-Online] [-OnlineExportPath <String>] [-CAPI2LogSize <Int32>]
2
3  PS C:\>./sri.ps1 [-Offline] [[-AuditPolicies]] [[-EventLogs]] [-ImportPath] <String>
4                  [[-ExportPath] <String>] [-CAPI2LogSize <Int32>]
5
6  PS C:\>./sri.ps1 [-GroupPolicy] [-GroupPolicyName] <String>
7
8  PS C:\>./sri.ps1 [-AllGroupPolicies]
```

The parameters "-OnlineExportPath", "-ImportPath" and "-ExportPath" are Strings, for example:

```
1    "C:\Example\Path"
```

The parameters "-CAPI2LogSize" is a Integer, for example:

```
1    4194304
```

The parameters "-GroupPolicyName" is a String, for example:

```
1    "Default Domain Policy"
```

NOTE: *Mandatory parameter are* <u>*underlined*</u>.

<u>-Online</u>

The current system which is calling the script will be checked on its readiness.

PARAMETER	
No parameter	The result PDF will be saved to the current path
-OnlineExportPath	The result PDF will be saved to this path
-CAPI2LogSize	Definition of the CAPI2 log size suitable for the environment. By default this value is set to 4MB as recommended from Microsoft

---

These are all possible parameter combinations for the -Online mode:

```
1    .\sri.ps1 -Online
2
3    .\sri.ps1 -Online -CAPI2LogSize 4194304
4
5    .\sri.ps1 -Online -OnlineExportPath "C:\temp\test\targetpath"
6
7    .\sri.ps1 -Online -OnlineExportPath "C:\temp\test\targetpath" -CAPI2LogSize 4194304
```

User Manual
4 Using SRI

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
COMPUTER SCIENCE

-Offline

Some system will be checked on its readiness - by default audit policies and event log are analysed. Export files of this system are required.

<div align="center">PARAMETER</div>

-ImportPath	Defines where the required files rsop.xml[a], windowslogs.csv[b], appandservlogs.csv[c] remain for analysis.
	The result PDF will be saved to the current path
-AuditPolicies	Checks only the audit policies.
	The result PDF will be saved to the current path
	-ImportPath requires rsop.xml
-EventLogs	Checks only the event logs
	The result PDF will be saved to the current path
	-ImportPath requires windowslogs.csv and appandservlogs.csv
-ExportPath	The result PDF will be saved to this path
-CAPI2LogSize	Definition of the CAPI2 log size suitable for the environment. By default this value is set to 4MB as recommended from Microsoft

[a]XML-Export of Resultant Set of Policy
[b]Export of Windows logs "System" & "Security" from EventViewer, check example_windowslogs.csv
[c]Export of Application and Service logs "TaskScheduler", "WindowsRemoteManagement"and "LocalSessionManager" from EventViewer, check example_appandservlogs.csv

These are all possible parameter combinations for the -Offline mode:

```
1    .\sri.ps1 -Offline -ImportPath "C:\temp\test"
2
3    .\sri.ps1 -Offline -ImportPath "C:\temp\test" -CAPI2LogSize 4194304
4
5    .\sri.ps1 -Offline -ImportPath "C:\temp\test" -ExportPath "C:\temp\test\targetpath"
6
7    .\sri.ps1 -Offline -ImportPath "C:\temp\test" -ExportPath "C:\temp\test\targetpath"
         -CAPI2LogSize 4194304
8
9    .\sri.ps1 -Offline -EventLogs -ImportPath "C:\temp\test"
10
11   .\sri.ps1 -Offline -EventLogs -ImportPath "C:\temp\test" -ExportPath
         "C:\temp\test\targetpath"
```

```
12
13    .\sri.ps1 -Offline -AuditPolicies -ImportPath "C:\temp\test"
14
15    .\sri.ps1 -Offline -AuditPolicies -ImportPath "C:\temp\test" -CAPI2LogSize 4194304
16
17    .\sri.ps1 -Offline -AuditPolicies -ImportPath "C:\temp\test" -ExportPath
          "C:\temp\test\targetpath"
18
19    .\sri.ps1 -Offline -AuditPolicies -ImportPath "C:\temp\test" -ExportPath
          "C:\temp\test\targetpath" -CAPI2LogSize 4194304
```

-GroupPolicy

Audit policies from a specific group policy are analysed.

PARAMETER

-GroupPolicyName	The name of the group policy to be analysed

These is an example for the -GroupPolicy mode:

```
1    .\sri.ps1 -GroupPolicy -GroupPolicyName "Default Domain Policy"
```

-AllGroupPolicies

All audit policies from every group policy in the current domain are analysed.
The result PDF will be saved to the current path

These is an example for the -GroupPolicy mode:

```
1    .\sri.ps1 -AllGroupPolicies
```