SUCCESS

D5.4 v1.0

Penetration Testing Procedures

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700416.

Project Name	SUCCESS
Contractual Delivery Date:	31.10.2018
Actual Delivery Date:	31.10.2018
Contributors:	DNV-GL
Work package:	WP5 - Demonstrating secure solution for Smart Metering
Security:	PU
Nature:	R
Version:	1.0
Total number of pages:	11(81)

Abstract:
This document serves as a penetration testing procedure for the Irish, Italian and Romanian trial site charging stations. Notes regarding the test results can also be added, as well as references to detailed descriptions of the findings.

Keyword list:
Test Program, Penetration Testing, Cyber-security, Irish Trial Site, Romanian Trial Site, Italian Trial Site.

Executive Summary

Penetration testing work is a key procedure carried out at system, sub-system and component levels to determine their robustness against cyber attacks. This exercise is very time consuming and expensive as a wide range of attack vectors are present that could affect all parts of industry, be it manufacturing, financial or healthcare just to name a few. With the rapid growth of more powerful computing systems, the hackers are devising more sophisticated ways of inflicting their attacks on all types of critical infrastructures. The resiliency of these critical infrastructures is becoming more pronounced and measures to combat these highly sophisticated cyber-attacks must be incorporated at the design stage.

The tasks of ethical hackers as used by DNVGL in this work are to be one step ahead of the malicious hackers which can be one person, a group of people or even a country. The vast number of attack vectors and the way they could be combined to infect a system makes testing against such attack vectors very difficult. The concept of having a completely cyber-safe system is virtually non-existent, but every system or component manufacturers must take all due precautions though proper penetration testing at certified establishments to prevent catastrophic shut-down of critical infrastructures against cyber-attacks that could paralyse big areas of a country over a long period of time as was evident in the Ukraine in December 2015.

Due to the limited resources available in this project, only the test procedures required to carry-out a full and comprehensive penetration test for each of the system used in the project's three trial sites, were executed. Comprehensive data on each of the system deployed at the field trial sites were collected to give the ethical hackers employed to carry out these tasks a good understanding of the system under trial and how and where their vulnerabilities to cyber-attacks lies.

Authors

Partner	Name	e-mail
KEMA NEDERLAND BV (DNV GL)		
	Mate Csorba,	
	Elisabet Haugsbø	
	Mirnes Alic	
	Ganesh Sauba	

Table of Contents

1. Introduction

1.1 Scope of this Deliverable

Cybersecurity is a serious and ongoing challenge for Critical Infrastructures (CIs), such as the electricity, gas and water grids. Addressing cybersecurity is critical to enhancing the security and reliability of these Cis thus enabling their continuous, safe and reliable operation to provide comfort and security in all aspects of life. A tried and very successful way of achieving these goals is to carry out penetration testing on systems, sub-systems and components forming part of such critical infrastructures. These tests are design to carry out an exhaustive number of penetration attacks representing the wide spectrum of attack vectors that are being used by hackers trying to undermine the resilience of these CIs.

This report has been compiled to represent the procedures requires to carry out a full and comprehensive penetration test of a system, sub-system or individual component. The systems used in this report are from the three field trials of this project and are in Ireland, Romania and Italy. The trial system for all three sites are covered in detail in D5.1, D5.2 and D5.3. All three test sites were visited to collect pictorial data of the test set-ups and there have been included in this report. The test procedures are current as used by the penetration testing team at DNVGL's Cyber-security laboratories. Pictorial details of each set-up have been included in this report with a brief description of each component where appropriate.

This report is an outline of the test program required to achieve penetration testing on the set-up of the three SUCCESS trial sites located in Ireland, Romania and Italy and are presented in the appendix. If a penetration testing is required in future, this document will provide a good insight on the requirements to be met for a successful outcome.

1.2 Relationship to the work of the project

This report must be used in conjunction with deliverables D5.1, D5.2 and D5.3 where the system used, and their architecture are described in detail. The context of the trials in relation to the use cases addressed in this project are also highlighted in those deliverables. The penetration test procedures identified in this work can be readily used to caring out a full test at any accredited penetration testing laboratory. The work presented here will also give a good insight on the requirements to be addressed for such tests and can be a stepping stone to deal with more complex system of this project such as the CI-SOC or the CI-SAN.

1.3 How to Read This Document

This document should be read together with D5.1, D5.2 and D5.3 to get the full benefit of the procedures required to carry out a full penetration test of the system in question. In this report we have used the three field trial sites that have been selected in SUCCESS to reflect particular use cases as employed by the DSOs in the consortium.

2. Test Objective

The general test objectives are:

- To search/scan for known vulnerabilities related to any components in the target system.
- To verify that components are configured in a way which maintains a sufficient level of cyber security.
- To verify that the communication network(s) is/are sufficiently resilient against unexpected traffic such as data flood or invalid data.
- To verify that the system has sufficient failure tolerance, i.e. is able to resume operation despite expected (single) failures.

The test activities will involve attempts to gain access to parts of the target system by applying different methods normally used by malicious hackers. The test will also involve attempts to otherwise disrupt the operation of the target system. All attempts to breach or disrupt the system will be within the agreed rules of engagement. Any vulnerabilities found during the test will be reported such that the system owner can apply solutions and mitigations.

3. Potential future work

The work carried out in this document can be used as reference test procedures in future projects where penetration testing work is required. These procedures are very up-to-date as far as cyber-attack vectors are concerned, but as with any cyber security measures, these cyber-attack vectors must be updated on a regular basis to keep pace with the range of malicious hackers trying to bring harm to critical infrastructures.

4. Conclusion

All the relevant test data were collected successfully from the three SUCCESS trial sites and supplied to the DNV-GL team in Norway to prepare for the report.

The report provided all the required test procedures to achieve a full penetration test of a set-up similar to the ones dealt with here.

These test procedures could be extended to cover more complex set-ups such as CI-SOC or CI-SAN.

This work can be used in other projects where similar testing are required as the most up-to-date procedures have been used in this document.

The cyber-attack vectors for these test cases are very relevant in today's environment, but there is a constant need to updated these attack vectors so as to provide comprehensive protection to critical infrastructures under test.

5. References

[1] D3.5 Information Security Management Components and Documentation, version 2
[2] D3.7 Next Generation Smart Meter, version 1
[3] Description of Available Components for SW Functions, Infrastructure and Related Documentation, version 2
[4] D4.5 Description of Available Components for SW Functions, Infrastructure and Related Documentation, version 19
[5] D4.2 Solution Architecture and Solution Description, version 27
[6] D5.1
[7] D5.2
[8] D5.3

6. List of Abbreviations

B2B Business to Business

BMS Building management system

CAPEX CAPital EXpenditure

CENELEC European Committee for Electro Technical Standardization CEP Complex Event Processing

COTS Commercial off-the-shelf

CPMS Charge Point Management System CSA Cloud Security Alliance

EMS Decentralized energy management system DER Distributed Energy Resources

DMS Distribution Management System DMTF Distributed Management Taskforce

DSE Domain Specific Enabler

EAC Exploitation Activities Coordinator

ERP Enterprise Resource Planning

ESB Electricity Supply Board

ESCO Energy Service Companies

ESO European Standardization Organizations ETP European Technology Platform

ETSI European Telecommunications Standards Institute GE Generic Enabler

HEMS Home Energy Management System HV High Voltage

I2ND Interfaces to the Network and Devices

ICT Information and Communication Technology

IEC International Electro-Technical Commission

ANNEX Test Cases