HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

COMPUTER SCIENCE

Studythesis

Readiness for Tailored Attacks and Lateral Movement Detection

Authors:

Claudio Mattes
claudio.mattes@hsr.ch

Lukas Kellenberger
lukas.kellenberger@hsr.ch

Supervisor:

Cyrill Brunschwiler
Hochschule für Technik Rapperswil
cyrill.brunschwiler@hsr.ch

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

October 11, 2018

Abstract

Management Summary

Initial Situation

Procedure

Results

Outlook

Task Definition

Contents

Part I

Technical Report

1.1 Introduction and Overview

1.1.1 Research

1.1.2 Test environment

A virtual network was set up on Azure-Cloud as a test environment. The test network was set up in the cloud so that the development team can access the network regardless of its location. The test network consists of a Windows server and two Windows clients. Active Directory service was configured on the server to manage the client computer. The following operating systems were installed in this testnetwork:

Server:

- Windows Server 2016

Clients:

- Windows 10 Pro, Version 1709

The network is structured as followed:

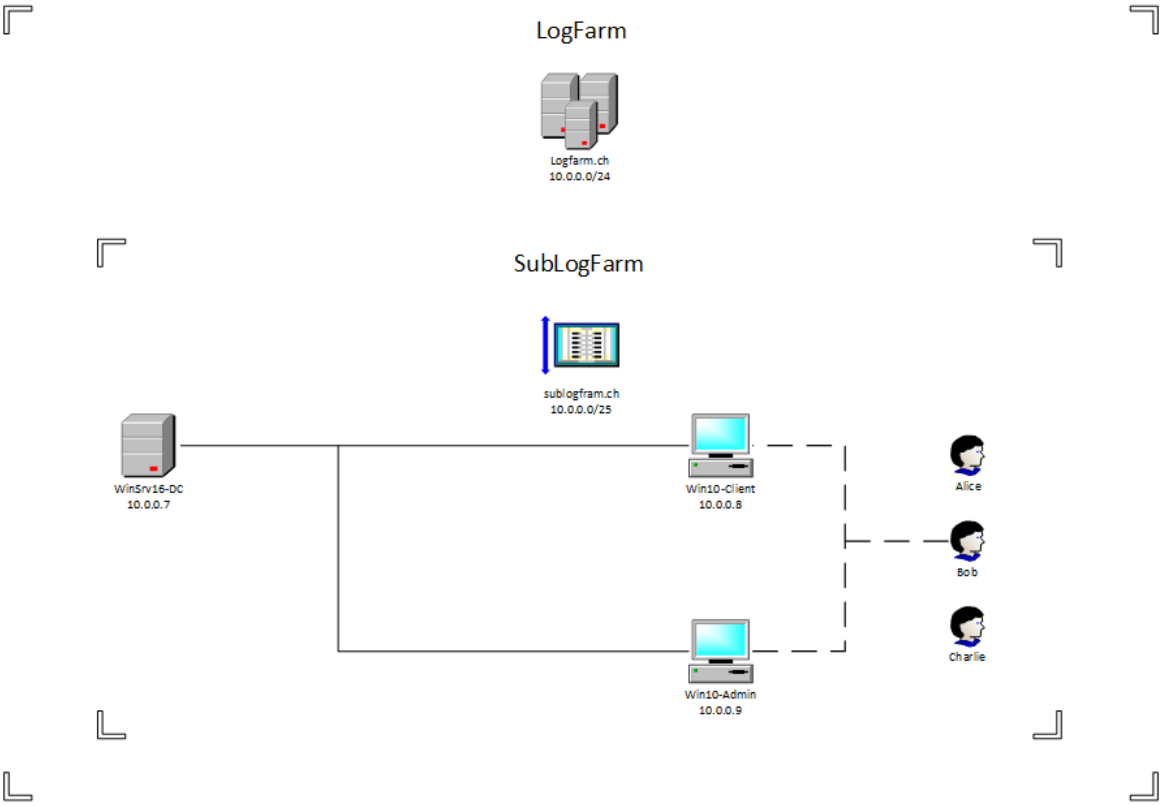

Figure 1.1: test environment

Users

Three different users were configured:

Name	**Permissions**
alice	administration
bob	user
charlie	user

Table 1.1: Angaben Lukas Kellenberger

1.2 Analysis

1.3 System Architecture

In this section the following main question is answered: *”How would a system architecture look like to fulfill the described problem domain?”*

1.4 Results

1.5 Conclusion

Glossary

List of Figures

List of Tables