

Assessing the Security Health of Public WiFi Environments Using Mobile Devices

I. Abstract

IV. Contents

V. List of Figures

VI. List of Tables

1. Introduction

1.1 Overview

1.2 Introduction

1.3 Mobile Threats

1.3.1 Classification of mobile threat

1.3.2 Most Targeted Mobile Platform in 2014

1.4 Honeypot Approach

1.4.1 Advantages & Benefits of Honeypot

1.4.2 Honeypot types based on interaction levels

1.4.3 Honeypot classifications

1.4.4 Honeypot requirements

1.5 Problem statement

1.6 Research Challenges

1.7 Objectives and desirable outcomes

1.8 Project Outline

2. Literature Review

2.1 Introduction

2.2 New Types of Honeypots

2.3 Honeypot Data Consumption

2.4 Configurations of Honeypots

2.5 Smartphone Honeypots

3. Design and Implementation

3.1 Introduction (Linux-based application "HosTaGe")

3.2 Implementation (HosTaGe Honeypot works)

3.2.1 Implementation Steps

3.2.1.1 Remote Procedure Call Attack (RPC)

3.2.1.1.1 Remote Procedure Call Attack Result

3.2.1.2 Scanning Attack using nmap

3.2.1.2.1 Scanning Attack Result

3.2.1.3 Metasploit Attack

3.2.1.3.1 Metasploit Attack Result

3.2.1.4 Nessuss Attack

3.2.1.4.1 Nessus Attack Result

3.3 Performing Attacks in Khalifa campus wireless

4. Data Collection

4.1 Introduction

4.2 Transferring Data from HosTaGe Database

5. Analysis

5.1 Introduction

5.2 Data Analytic and Intelligence

5.2.1 Add Data to Splunk

5.2.2 Search in Splunk

5.2.2.1 Summarized Analysis

6. Conclusion

6.1 Summary

6.2 Future work

7. References