Security Assessment Report (SAR) – Capstone Project Template

July 2021
Version 2.0

Securible, LLC

This page is left intentionally blank

TABLE OF CONTENTS

1. OVERVIEW 4

A. INTRODUCTION 4
B. INSTRUCTIONS 4

2. TARGET SYSTEMS 5

A. INSTRUCTIONS 5
B. SYSTEM A - DESCRIPTION 5
C. SYSTEM B - DESCRIPTION 5
D. SYSTEM C - DESCRIPTION 5

3. VULNERABILITIES 6

A. INSTRUCTIONS 6
B. SYSTEM A - VULNERABILITIES 6
C. SYSTEM B - VULNERABILITIES 6
D. SYSTEM C - VULNERABILITIES 6

4. ATTACK VECTORS 7

A. INSTRUCTIONS 7
B. SYSTEM A – INTRUSIONS 7
C. SYSTEM B – INTRUSIONS 7
D. SYSTEM C – INTRUSIONS 7

5. ROOT CAUSE 8

A. INSTRUCTIONS 8
B. SYSTEM A – ROOT CAUSE 8
C. SYSTEM B – ROOT CAUSE 8
D. SYSTEM C – ROOT CAUSE 8

6. RECOMMENDATIONS 9

A. INSTRUCTIONS 9
B. GENERAL - RECOMMENDATIONS 9
B. SYSTEM A – RECOMMENDATIONS 9
C. SYSTEM B – RECOMMENDATIONS 9
D. SYSTEM C – RECOMMENDATIONS 9

1. Overview

A. Introduction

Welcome to the Capstone project for your Cybershield Intro to Kali Linux course. The purpose of this exercise is to have you write a Security Assessment Report (SAR) and provide guidance on how to mitigate potential offensive cyber intrusions.

B. Instructions

This document has been put together to have to walk through assessing the security of an environment and provide guidance on how to mitigate the issues. You'll notice this document is broken into the following areas:

1. Target Systems – In this section, you want to document the systems you will be assessing.
2. Vulnerabilities – In this section, you want to document all the vulnerabilities you've identified as part of your assessment. This can include a host of different tools and methods you might use to collect the vulnerability information.
3. Attack Vectors – In this section, you want to document the vectors you used to attack the system.
4. Root Cause – In this section, you want to describe the set of factors that allowed the system to be compromised.
5. Recommendations – In this section, you want to identify how you would recommend the organization mitigate the issues so intrusions noted in the Attack Vector section would be minimized or stopped.

2. Target Systems

A. Instructions

Describe the boundary of the system or systems that are involved in the assessment. This description includes the hardware, software, firmware components that make up the system to the best of your knowledge. If there is more than one system, include a description for each system.

B. System A - Description

____
____
____
____
____
____
____

C. System B - Description

____
____
____
____
____
____
____

D. System C - Description

____
____
____
____
____
____
____

3. Vulnerabilities

A. Instructions

Identify the weaknesses and vulnerabilities identified in the systems. These will most likely be technical but could be operational, managerial, or physical. If you have more than one system you are assessing, describe the vulnerabilities for each system separately.

B. System A - Vulnerabilities

C. System B - Vulnerabilities

D. System C - Vulnerabilities

4. Attack Vectors

A. Instructions

Document the vectors that you have been able to use against each system here. Do not yet describe the reason for the intrusion, but instead describe how you could access the system. Describe the methods and processes you could implement to gain access - document the vector on a system-by-system basis.

B. System A – Intrusions

____

____

____

____

____

____

____

C. System B – Intrusions

____

____

____

____

____

____

____

D. System C – Intrusions

____

____

____

____

____

____

____

5. Root Cause

A. Instructions

Identify the cause which allows the intrusion to occur. Describe the lack of security control or process that resulted in allowing the compromise to happen. If you have multiple systems with different attack vectors, describe each one individually.

B. System A – Root Cause

C. System B – Root Cause

D. System C – Root Cause

6. Recommendations

A. Instructions

Provide recommendations on how to prevent this type of event from occurring in the future. You may provide general recommendations if you feel the recommendation applies to more than one system, or you can provide system-specific recommendations below.

B. General - Recommendations

B. System A – Recommendations

C. System B – Recommendations

D. System C – Recommendations