h_da

HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Darmstadt University of Applied Sciences
– Faculty of Computer Science –

Compromised Server Investigation Report

Qualification exercise

by
Lennart Eichhorn
Matriculation number: 759253
Email: lennart.eichhorn@stud.h-da.de

ABSTRACT

Participating in the hacker contest course requires a submitting a solution for the qualification exercise [Goh24].

TABLE OF CONTENTS

Part I

FORENSIC INVESTIGATION REPORT

INTRODUCTION

1.1 BACKGROUND

A small company hired an IT consultant to generate certificates for various services. As soon as the consultant completed the work and left the building, the Intrusion Detection System (IDS) used in the company detected an attack on the server set up specifically for this purpose. Concerned about the security of the generated certificates, the company requests a forensic investigation of the server to determine whether there has been an attack on the system and, if so, what data has been stolen from the system. Any information that can be found about the attacker is also of importance.

The server itself has the IP address `192.168.0.1`. The consultant used the username `root` and either worked directly on the computer or from the addresses `192.168.5.23` and `192.168.23.5`. Otherwise, no one else should have had access to the computer. The consultant set up the computer in the morning and generated the certificates. Immediately afterward, he left the premises. Shortly thereafter, the IDS system reported the attack.

1.2 OBJECTIVES

1.2.1 *Tasks*

Questions

- Should the certificates still be used?

- Can the system still be used?

- If there was an attack:

- How did the attacker get into the system?

- What did the attacker do?

- What has to be done to secure the system?

- Which details about the attacker can be found?

Additional Questions

- Is the configuration of the server secure?

- Should a CA be operated in this manner?

- How should the software written by the consulatant be assessed?

1.2.2 *Hypotheses*

Table 1. Compromised server disk image

Attribute	Detailed Information
Filename	HDD.raw
sha256sum	9ad970f9df238dc266f58f17689d4049ab40e5c10296a3ff0620ba95612f166c
Size (bytes)	1.00 GiB (1,073,741,824 bytes)
Date of acquisition	Unknown
Aquired by	Customer
Description	The disk image was created by the customer and handed over to the investigator

1.4 SUSPECT INFORMATION

1.4.1 *Domain terms*

List term in the domain. We need define domain related terms, e.g., terms used when we investigate a fraud related to accounting. • Accounts payable: fill out the definition here. • Accounts receivable: fill out the definition here. • Certified public accountant: fill out the definition here.

INVESTIGATOR ACTIVITY LOGS

I did not work on any live data, so there is no risk of contaminating the evidence.

4

CONCLUSION

4.1 RECOMMENDATIONS FOR SECURING THE SERVER

LIST OF ABBREVIATIONS

IT
Information Technology

IDS
Intrusion Detection System

REFERENCES

[Goh24]   Matthias Göhring, Tobias Hamann, Tim Wörner
               Anmeldeaufgabe, Sommersemester 2024
               [Online; archived 17.4.2024]
               transfer.usd.de/index.php/s/ZPS9KT2NRsk42MA 📁

5