External Penetration Test Report

PEN-DOC-202308190007

Golden Egg Labs, INC., https://goldenegglabs.com

19-08-2023

Contents

1 Document Overview

1.1 Confidentiality

This document is the exclusive property of Demo Company (DC) and TCM Security (TCMS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both DC and TCMS. TCMS may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

1.2 Legal Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period. Time-limited engagements do not allow for a full evaluation of all security controls. TCMS prioritized the assessment to identify the weakest security controls an attacker would exploit. TCMS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

2 Executive Summary

Golden Egg Labs, INC. (GEL) was contracted by Family Life Communications, INC. (FLC) to conduct an external penetration test in order to examine the susceptibility to exploitation from a remote attacker attempting to gain acces to the internal network without host resources or inside knowledge. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against FLC with the goals of:

- Enumerating all possible entry points accros the attack surface and locating potential vulnerabilities.

- Identifying if a remote attacker could penetrate FLC's defenses through exploitation.
- Determining the impact of a security breach on the internal infrastructure and availability of FLC's information systems.

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-1151 with all tests and actions being conducted under controlled conditions. Initial reconnaissance of the MegaCorp One network resulted in the discovery of a misconfigured DNS server that allowed a DNS zone transfer. The results provided us with a listing of specific hosts to target for this assessment. An examination of these hosts revealed a password-protected administrative webserver interface. After creating a custom wordlist using terms identified on the MegaCorp One 's website we were able to gain access to this interface by uncovering the password via brute-force. An examination of the administrative interface revealed that it was vulnerable to a remote code injection vulnerability, which was used to obtain interactive access to the underlying operating system. This initial compromise was escalated to administrative access due to a lack of appropriate system updates on the webserver. After a closer examination, we discovered that the compromised webserver utilizes a Java applet for administrative users. We added a malicious payload to this applet, which gave us interactive access to workstations used by MegaCorp One's administrators. Using the compromised webserver as a pivot point along with passwords recovered from it, we were able to target previously inaccessible internal resources. This resulted in Local Administrator access to numerous internal Windows hosts, complete compromise of a Citrix server, and full administrative control of the Windows Active Directory infrastructure. Existing network traffic controls were bypassed through encapsulation of malicious traffic into allowed protocols.

2.1 Summary of Findings Identified

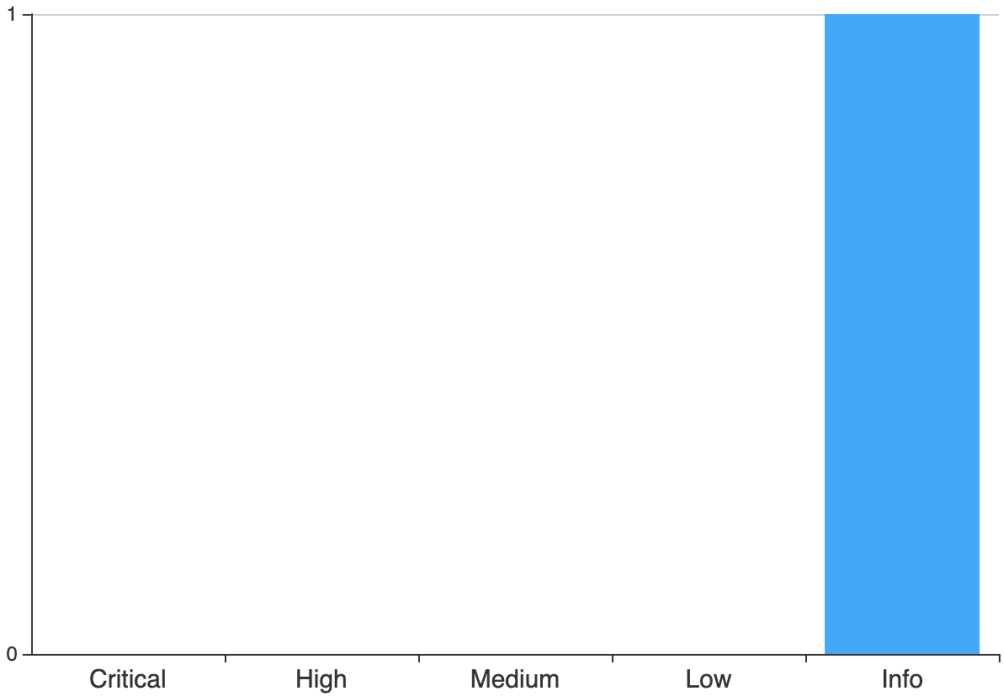

Figure 1: Executive Summary

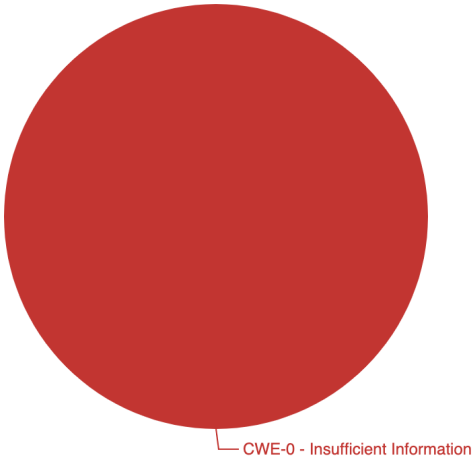

Figure 2: Breakdown by Categories

> **# 1 Info** About Golden Egg Labs, INC.

2.2 Scope

2.2.1 In Scope

TBC

2.2.2 Out of Scope

TBC

2.3 Methodology

TBC

2.4 Recommendations

TBC

3 Findings and Risk Analysis

3.1 About Golden Egg Labs, INC.

Severity: Info
CVSS Score: 0.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

CWE

0 - Insufficient Information

Description

Offensive Security advocates penetration testing for impact as opposed to penetration testing for coverage. Penetration testing for coverage has risen in popularity in recent years as a simplified method of assessments used in situations where the goal is to meet regulatory needs. As a form of vulnerability scanning, penetration testing for coverage includes selective verification of d iscovered issues through exploitation. This allows service providers the ability to conduct the work largely through the use of automated toolsets and maintain consistency of product across multiple engagements. Penetration testing for impact is a form of attack simulation under controlled conditions, which closely mimics the real world, targeted attacks that organizations face on a day-to-day basis. Penetration testing for impact is a goal-based assessment, which creates more than a simple vulnerability inventory, instead providing the true business impact of a breach. An impact-based penetration test identifies areas for improvement that will result in the highest rate of return for the business. Penetration testing for impact poses the challenge of requiring a high skillset to successfully complete. As demonstrated in this sample report, Offensive Security believes that it is uniquely qualified to deliver world-class results when conducting penetration tests for impact, due to the level of expertise found within our team of security professionals. Offensive Security does not maintain a separate team for penetration testing and other activities that the company is engaged in. This means that the same individuals that are involved in Offensive Security's industry leading performance-based training, the production of industry standard tools such as Kali Linux, authors of best selling books, creators of 0- day exploits, and maintainers of industry references such as Exploit-DB are the same individuals that are involved in the delivery of services. Offensive Security offers a product that cannot be matched in the market. However, we may not be the right fit for every job. Offensive Security typically conducts consulting services with a low volume, high skill ratio to allow Offensive Security staff to more closely mimic real world situations. This also allows customers to have increased access to industryrecognized expertise all while keeping costs re asonable. As such, high volume/fast turn-around engagements are often not a good fit for our services. Offensive Security is focused on conducting high quality, high impact

assessments and is actively sought out by customers in need of services that cannot be delivered by other vendors.

Location

TBC

Impact

TBC

Recommendation

TBC

References

TBC

Additional notes

THE TITLE

4 Additional Notes

4.1 THE TITLE

THE DESC