Family Life Communications, INC.

External Penetration Test Report

PEN-DOC-202308190007
Golden Egg Labs, INC.

https://goldenegglabs.com

August 08, 2023

Contents

1 Document Overview

1.1 Confidentiality

This document and all information contained within are confidential and proprietary to Family Life Communications, INC. (FLC) and Golden Egg Labs, Inc. (GEL). Extreme care should be excercised when handling, referring, or copying this document. GEL authorizes FLC to view and disseminate this document as they see fit in accordance with FLC's data handling policies.

FLC may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

1.2 Legal Disclaimer

All information presented throughout this document is provided as-is and without warranty. Penetration tests and vulnerability assessments are a "point-in-time" analysis. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

1.3 Contact Information

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:

- Probing all host ip addresses to reveal running services and map the attack surface.
- Gathering information through open-sourcce intelligence (OSINT) and passive DNS.
- Scanning entry points accros the attack surface to locate 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 sy>

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 Int> accordance with the recommendations outlined in NIST SP 800-1151 with all tests and actions being conducted under controlled conditions.

3 Security Strenghts

Stuff

4 Security Weaknesses

4.1 Unrestricted login attempts

During the assessment, GEL performed multiple 100 password attacks against login forms found on the external network. For all logins, unlimited attempts were allowed.

4.2 Summary of Findings Identified

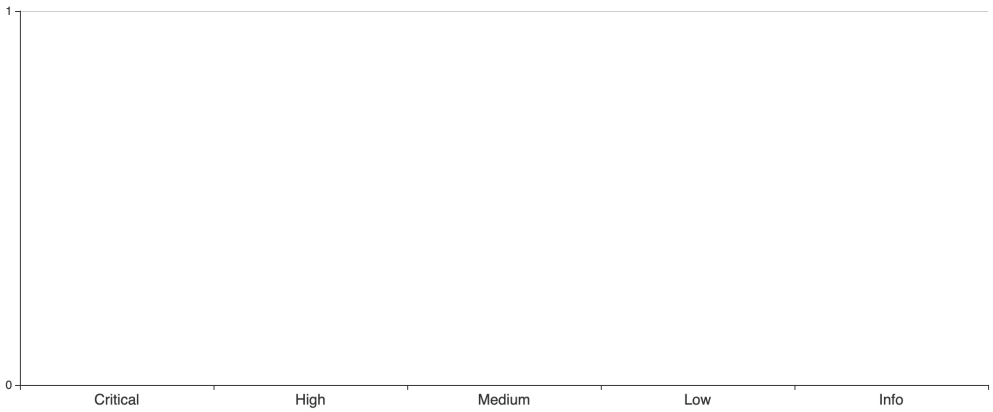

Figure 1: Executive Summary

Figure 2: Breakdown by Categories

4.3 Scope

4.3.1 In Scope

Family Life Communications, INC. provided our team with 12 host ip addresses to investigate:

45.63.58.149	50.227.91.130	50.227.91.131	50.227.91.132
50.227.91.138	50.227.91.139	50.227.91.141	74.122.162.18
74.122.162.19	74.122.162.20	74.122.162.21	74.122.162.23

4.3.2 Constraints and Limitations

With all hosts running live in a production environment, FLC requested that we do not perform any Denial of Service attacks during testing. As such, we did not conduct aggressive brute-force attacks on these systems. During our security assesment, we discovered 2 hosts that are vulnerable to a Denial of Service attack but we did not exploit this.

4.3.3 Out of Scope

Table 2: Contact Information

Golden Egg Labs, INC.		
Name	**Position**	**Contact Information**
Andy Novocin	Executive Manager	Email: andy@novocin.com
Teddy Katayama	Lead Pentetration Tester	Email: katayama@udel.edu
Daniel Li	Pentetration Tester	Email: djli@udel.edu
Family Life Communications, INC.		
Name	**Position**	**Contact Information**
Todd Williams	IT Manager	Email: twilliams@flc.org

4.4 Methodology

Golden Egg Labs employed a security assessment methodology that entailed the application of the Penetration Testing Execution Standard (PTES) framework, which was then tailored to integrate with Family Life Communications' external environment. The following subsections describe and outline our approach for engagement and analysis.

4.5 Information Gathering & Discovery

The information gathering and reconnaissance phase is the critical starting point for determining the full scope and size of the attack surface. The objective of this step is to perform reconnaissance against a target in order to identify all possible entry points and gather as much information as possible to be prioritzed and categorized as supporting artifacts when penetrating the target during the vulnerability assessment and exploitation phases. During our assessment, we used the latest scanning tools and techniques to perform a comprehensivethe audit of all IP addresses within our scope. This includes but is not limited to:

- Conventional TCP and UDP port and banner scanning
- Service enumeration & operating system and service fingerprinting
- Active DNS discovery and subdomain enumeration using Virus Total passive DNS
- Reviewing certificate transparency records
- Network mapping and monitoring HTTP requests and response
- Performing protocol negotiations with VPN devices that service Internet Key Exchange (IKE)

4.6 Vulnerability Assessment and Threat Modeling

In this phase, we correlate artifact indicators retreive from the previous phase and service port and versioning The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

4.7 3.3 Sample Report - Penetration

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, John was able to successfully gain access to X out of the X systems.

4.8 3.4 Sample Report - Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred (i.e. a buffer overflow), we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

John added administrator and root level accounts on all systems compromised. In addition to the administrative/root access, a Metasploit meterpreter service was installed on the machine to ensure that additional access could be established.

4.9 3.5 Sample Report - House Cleaning

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organizations computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After the trophies on the exam network were completed, John removed all user accounts and passwords as well as the meterpreter services installed on the system. Offensive Security should not have to remove any user accounts or services from the system. katayama@"

4.10 Recommendations

TBC

5 Findings and Risk Analysis

6 Additional Notes