SECURITY ASSESSMENT

Looking Glass Report

Submitted to: Sprints

Security Analyst:

Mohamed Awad Mohamed
Mary Alfons Shokry
Mohamed Gamal
Yomna Mohamed Abdelfatah
Mahmoud Mohamed Ismail

Date of Testing: 22/10/2024
Date of Report Delivery: 24/10/2024

Table of Contents

Contents

Security Engagement Summary

Engagement Overview

This engagement was requested by the TryHackMe Security Team to assess the security vulnerabilities within the Looking Glass environment.

The goal of the engagement was to identify potential security weaknesses, provide remediation guidance, and improve the overall security posture.

The assessment was conducted using both automated and manual testing methods to ensure thorough coverage of possible attack vectors.

Scope

The scope of this engagement included the entire Looking Glass TryHackMe room environment.

The focus was on identifying vulnerabilities related to web service misconfigurations, potential directory traversal, and weak password policies.

This scope was chosen to address critical attack vectors specific to this machine.

Executive Risk Analysis

The overall risk level of the Looking Glass environment was assessed as **Medium**.

Key vulnerabilities identified include directory traversal opportunities, misconfigured web services, and weak password policies, which could allow unauthorized access.

While these vulnerabilities do not pose an immediate high risk, they could be exploited to gain sensitive information or unauthorized control.

Executive Recommendation

It is recommended to address directory traversal vulnerabilities as a priority, as they represent the most immediate threat.

Remediation efforts should also focus on improving password policies to enforce complexity and mitigating web service misconfigurations to prevent exploitation.

Significant Vulnerability Summary

Medium Risk Vulnerabilities

- Directory Traversal
- Weak Password Policies
- Cross-Site Request Forgery (CSRF)

Low Risk Vulnerabilities

- Weak Password Policies

Significant Vulnerability Detail

Directory Traversal

Risk Level: MEDIUM

A directory traversal vulnerability was identified, which allows attackers to access files outside the intended directory. This vulnerability was validated through manual testing by accessing sensitive files on the web server. The impact of this vulnerability includes the potential exposure of sensitive configuration files and user information. It is recommended to properly sanitize user input and restrict file access to authorized directories only.

Weak Password Policies

Risk Level: MEDIUM

Weak password policies were identified during the assessment, with passwords that did not meet complexity requirements. This increases the risk of brute force attacks or unauthorized access. It is recommended to enforce stronger password policies that require a mix of uppercase, lowercase, numbers, and special characters, along with multi-factor authentication.

Web Service Misconfigurations

Risk Level: LOW

Misconfigured web services were identified, including the exposure of unnecessary services and potential information leakage through error messages. While the risk is low, it is recommended to review and correct these configurations, disabling unnecessary services and ensuring error messages do not disclose sensitive information.

Methodology

The assessment followed a systematic approach to identify vulnerabilities and exploit weaknesses within the Looking Glass environment. The following steps were taken:

1. Reconnaissance: Nmap was used to scan for open ports and services running on the machine.
   - Command: nmap -sV -A [target IP]
   - Result: Open ports such as HTTP (80), SSH (22), and others were discovered.

2. Service Enumeration: Services like HTTP were enumerated to discover potential misconfigurations, hidden files, and sensitive data exposure. Manual inspection of HTTP responses was done to identify the directory

traversal vulnerability.

3. Password Policy Testing: Hydra was used to test weak password policies for potential brute-force attacks on SSH.
    - Command: hydra -l user -P /usr/share/wordlists/rockyou.txt ssh://[target IP]
    - Result: Weak passwords were successfully brute-forced.
4. Vulnerability Validation: The directory traversal vulnerability was confirmed by manually accessing files outside the web server's intended directory.
    - Manual input tests validated that the directory traversal allowed access to configuration files.

Assessment Toolset Selection

The following tools were selected and used during the Looking Glass lab assessment:

1. Nmap: Used for network scanning to identify open ports and running services.
2. Hydra: Used for brute-forcing weak SSH credentials to test password strength.
3. Manual Testing: Directory traversal testing and manual validation of web server misconfigurations.