SECURITY ASSESSMENT

Year Of They Jellyfish Report

Submitted to: Sprints

Security Analyst:

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

Date of Testing: 23/10/2024
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 vulnerabilities in the Year of the Jellyfish environment. The goal was to identify potential security weaknesses, offer remediation guidance, and improve the overall security of the system. Both automated and manual testing methods were utilized during the assessment.

Scope

The scope of this engagement included the entire Year of the Jellyfish TryHackMe room environment.
The focus was on identifying weaknesses related to open services, weak authentication mechanisms, and potential privilege escalation paths.

Executive Risk Analysis

The overall risk level of the Year of the Jellyfish environment was assessed as Medium.
Key vulnerabilities identified include weak SSH credentials and potential privilege escalation paths, which if exploited could lead to full system compromise.

Executive Recommendation

It is recommended to prioritize addressing the weak SSH credentials and securing privilege escalation paths.
Additionally, service misconfigurations should be reviewed, and stronger authentication mechanisms should be implemented to prevent unauthorized access.

Significant Vulnerability Summary

1. Privilege Escalation via Misconfigured Sudo Permissions (High)
2. Weak SSH Credentials (Medium)
3. Misconfigured Services (Open ports exposing unnecessary services) (Low)

Significant Vulnerability Detail

Privilege Escalation via Misconfigured Sudo Permissions

Risk Level: High

Improper sudo permissions allowed the 'jellyfish' user to escalate privileges to root without requiring a password. This presents a critical risk if exploited, as it grants attackers full control over the system.

Weak SSH Credentials

Risk Level: Medium

The SSH service running on port 22 was vulnerable to brute-force attacks due to weak credentials ('jellyfish:password').
An attacker could use these credentials to gain unauthorized access to the system.

Misconfigured Services

Risk Level: Low

Unnecessary services were exposed, including RabbitMQ (port 5672), which may provide additional information to attackers and increase the system's attack surface.
Disabling or securing these services can help reduce potential risks.

Methodology

The following steps were taken during the assessment of the Year of the Jellyfish environment:

1. **Reconnaissance**:
  - Nmap was used to perform a port scan and identify open services.
   - Command: nmap -sV -A [target IP]
   - Result: SSH (22) and RabbitMQ (5672) were discovered.

2. **Password Cracking**:
  - Hydra was used to brute-force SSH login credentials for the 'jellyfish' user.
   - Command: hydra -l jellyfish -P /usr/share/wordlists/rockyou.txt ssh://[target IP]
   - Result: Successful login with 'jellyfish:password'.

3. **Privilege Escalation**:
  - Misconfigured sudo permissions allowed the 'jellyfish' user to execute commands as root without requiring a password.
   - Command: sudo su -
   - Result: Root access was obtained through privilege escalation.

Assessment Toolset Selection

The following tools were used during the Year of the Jellyfish assessment:

1. **Nmap**: For scanning and identifying open ports and services.
2. **Hydra**: For brute-forcing weak SSH credentials.
3. **Manual Testing**: Used to validate privilege escalation vulnerabilities through misconfigured sudo permissions.