SECURITY ASSESSMENT

Year Of The Rabbit Report

Submitted to:
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

Security Engagement Summary

Engagement Overview

This engagement was requested by the TryHackMe Security Team to assess the vulnerabilities within the Year of the Rabbit environment. The goal of this assessment was to identify security weaknesses, provide recommendations for remediation, and improve the system's overall security. The assessment was performed using both automated and manual testing methods.

Scope

The scope of this engagement included the entire Year of the Rabbit TryHackMe room environment.
The focus was on identifying vulnerabilities related to weak credentials, open ports, and privilege escalation opportunities.

Executive Risk Analysis

The overall risk level of the Year of the Rabbit environment was assessed as Medium.
Key vulnerabilities identified included weak SSH credentials, misconfigured services, and privilege escalation opportunities. Exploiting these vulnerabilities could lead to full control over the system.

Executive Recommendation

It is recommended to prioritize the remediation of privilege escalation vulnerabilities, as they pose the highest risk. Additionally, stronger password policies should be implemented to prevent brute force attacks on SSH, and misconfigured services should be secured or disabled.

Significant Vulnerability Summary

1. Privilege Escalation via Sudo Misconfiguration (High)

2. Weak SSH Credentials (Medium)

3. Misconfigured Services (Open ports exposing unnecessary services) (Low)

Significant Vulnerability Detail

Privilege Escalation via Sudo Misconfiguration

Risk Level: High

The sudo configuration for the 'rabbit' user allowed privilege escalation to root without requiring a password. This could result in complete control of the system if exploited.

Weak SSH Credentials

Risk Level: Medium

The SSH service was found to be vulnerable to brute-force attacks due to weak credentials ('rabbit:password'). This could allow an attacker to gain unauthorized access to the system.

Misconfigured Services

Risk Level: Low

Open ports such as RabbitMQ (5672) were exposed unnecessarily, providing additional information that could be exploited.
Disabling or securing these services can reduce the attack surface.

Methodology

The following steps were followed during the assessment of the Year of the Rabbit environment:

1. **Reconnaissance**:
   - Nmap was used to scan the target machine for open ports and running services.
   - Command: nmap -sV -A [target IP]
   - Result: Open ports for SSH (22) and RabbitMQ (5672) were identified.

2. **Password Cracking**:
   - Hydra was employed to perform brute-force attacks on SSH, which revealed weak credentials.
   - Command: hydra -l rabbit -P /usr/share/wordlists/rockyou.txt ssh://[target IP]
   - Result: Successful login with 'rabbit:password'.

3. **Privilege Escalation**:
   - After logging in as 'rabbit', sudo misconfigurations were discovered that allowed privilege escalation to root without requiring a password.
   - Command: sudo su -
   - Result: Full root access was obtained.

Assessment Toolset Selection

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

1. **Nmap**: Used for port scanning and service enumeration.
2. **Hydra**: Employed for brute-force attacks on weak SSH credentials.
3. **Manual Testing**: Used for privilege escalation testing and validation of sudo misconfigurations.