SECURITY ASSESSMENT

Wonderland 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 security engagement was requested by the TryHackMe team to assess the vulnerabilities within the 'Wonderland' room.

The goal was to identify potential weaknesses that could allow attackers to gain unauthorized access and escalate privileges.

This assessment was completed using both automated and manual tools, and it is part of regular testing to enhance security.

Scope

The scope of the engagement included the entire 'Wonderland' room on TryHackMe, focusing on identifying vulnerabilities related to SSH, privilege escalation, and weak authentication mechanisms.

Executive Risk Analysis

The overall risk level for the 'Wonderland' environment is assessed as **Medium** due to the combination of weak SSH credentials and misconfigured sudo permissions, which can lead to full system compromise if exploited. While not immediately critical, the impact of successful exploitation is severe.

Executive Recommendation

Remediation efforts should focus on hardening SSH credentials by enforcing stronger passwords and properly configuring sudo permissions. The highest priority is to mitigate privilege escalation risks, as this poses the most significant threat to the environment.

Significant Vulnerability Summary

High Risk Vulnerabilities

Privilege Escalation via Misconfigured Sudo Permissions

Medium Risk Vulnerabilities

Weak SSH Credentials

Low Risk Vulnerabilities

- Unnecessary Open Ports (RabbitMQ)

Significant Vulnerability Detail

Privilege Escalation via Misconfigured Sudo Permissions

Risk Level: **HIGH**

Vulnerability detail

- Summary: The user 'rabbit' was able to escalate privileges to root due to misconfigured sudo permissions. This allowed the 'rabbit' user to run all commands as root without needing a password. If exploited, this vulnerability gives attackers complete control over the system.
- Remediation: Review and correct sudo permissions to restrict unauthorized root access.

Weak SSH Credentials

Risk Level: MEDIUM

Vulnerability detail

- The SSH service running on port 22 was vulnerable to brute-force attacks due to weak credentials ('rabbit:password').
  An attacker could use these credentials to gain initial access to the system.
- Remediation: Enforce stronger password policies and consider disabling password-based SSH authentication in favor of public key authentication.

Unnecessary Open Ports (RabbitMQ)

Risk Level: LOW

Vulnerability detail

- Port 5672 (RabbitMQ) was found open, exposing unnecessary services. Although not immediately exploitable, such open ports increase the attack surface and can provide additional information to attackers.
- Recommendation: Disable or secure unnecessary services and limit open ports to only those required for operation.

Methodology

The assessment followed a structured approach to identify and exploit vulnerabilities within the Wonderland environment.
The following steps were performed:

1. Reconnaissance: ‘
    - Nmap was used to scan the target for open ports and services.
    - Command: nmap -sV -A [target IP]
    - Result: Open ports such as SSH (22) and RabbitMQ (5672).
2. Password Cracking:
    - Hydra was used to brute-force the SSH credentials for the 'rabbit' user.
    - Command: hydra -l rabbit -P /usr/share/wordlists/rockyou.txt ssh://[target IP]
    - Result: Successful login with the credentials 'rabbit:password'.
3. Privilege Escalation:
    - After logging in as 'rabbit', misconfigured sudo permissions were identified, allowing the user to run commands as root without a password.
    - Command: sudo su -
    - Result: Full root access was achieved.

Assessment Toolset Selection

1. Nmap: Used to scan for open ports and running services.
2. Hydra: Used to brute-force weak SSH credentials.
3. Manual Testing: For validating privilege escalation via sudo misconfigurations.