Penetration Testing Report: Anthem

Executive Summary

This document details the findings from a penetration test conducted on the target system with IP address 10.10.30.207. The test aimed to identify vulnerabilities in the system's network services, web applications, and remote desktop protocol (RDP) access.

Methodology

The penetration test followed a structured approach:

1. **Network Scanning**: Conducted an initial Nmap scan to identify open ports and services.
2. **Web Application Analysis**: Used Gobuster for directory enumeration and inspected the source code of the web application.
3. **Credential Discovery and Testing**: Analyzed accessible files (like robots.txt) and patterns to deduce potential credentials.
4. **Remote Desktop Protocol (RDP) Access**: Utilized discovered credentials to access the system via RDP.

Findings

1. **Initial Nmap Scan**:
    - Target IP: **10.10.30.207**
    - Open Ports:
        - 80/tcp (HTTP)
        - 3389/tcp (Microsoft RDP)
    - Note: An aggressive Nmap scan was attempted but unsuccessful. This was due to improper input via the tester.
2. **Web Application Enumeration**:
    - Target URL: **http://10.10.30.207**
    - Tool: Gobuster with common wordlists
    - Source Code Analysis: Revealed a possible flag.
    - robots.txt: Contained a potential password **UmbracoIsTheBest!**
3. **Credential Discovery**:
    - Administrator Username: Inferred as **SG@anthem.com** using a reference to a poem by Solomon Grundy and the organization's email scheme.
    - Credentials Used for Access:

        - Username: **sg@anthem.com**
        - Password: **UmbracoIsTheBest!**

4. **Further Web Application Analysis**:
    - Additional flags were discovered by examining the source code of various pages.
5. **Remote Desktop Protocol (RDP) Access**:
    - Command Used: **xfreerdp /u:sg /p:UmbracoIsTheBest! /v:10.10.30.207 /dynamic-resolution**
    - Accessed the system successfully and retrieved the **user.txt** file.
6. **Privilege Escalation**:
    - Admin Password Discovered: **ChangeMeBaby1MoreTime**
    - Admin Account Accessed to retrieve the final flag.

Conclusion

The penetration test successfully identified several vulnerabilities, including insecure web application configurations, predictable credentials, and insufficiently protected RDP access. It is recommended that the organization takes immediate steps to address these issues, such as securing web applications, enforcing strong password policies, and restricting RDP access.