Penetration Test Report: Year Of The Rabbit

Executive Summary

During the course of our penetration testing activities against the specified target IP **10.10.182.228**, we successfully identified multiple service vulnerabilities, gained unauthorized access to internal accounts, and escalated privileges to obtain root access. This document outlines the methodologies employed, findings, and recommended corrective actions.

Methodology

Our approach adhered to standard penetration testing phases:

1. **Reconnaissance**:
    - Conducted an nmap scan with the command **nmap -A 10.10.182.228**.
2. **Scanning and Enumeration**:
    - Employed **gobuster** to discover hidden directories.
    - Utilized **hydra** for brute-forcing FTP credentials.
3. **Gaining Access**:
    - Accessed the FTP server with obtained credentials.
    - Deciphered an encoded message using a brainfuck language decoder.
4. **Maintaining Access**:
    - Logged into the SSH server with the credentials obtained from decoding the message.
5. **Privilege Escalation**:
    - Exploited a vulnerability in **sudo** (CVE-2019-14287) to gain root access.

Findings & Exploits

1. **Open Ports & Services**:
    - Discovered open ports: 21 (FTP), 22 (SSH), 80 (HTTP).
    - Identified services: vsftpd 3.0.2, OpenSSH 6.7p1, Apache httpd 2.4.10.
2. **Hidden Directories & Files**:
    - Located **/assets** and **/sup3r_s3cr3t_fl4g.php** using **gobuster**.
    - Uncovered a hidden message in the stylesheet linking to an intermediary page, which eventually led to the discovery of **Hot_babe.png**.
3. **Credentials Harvesting**:
    - Extracted a list of potential FTP passwords from the **Hot_babe.png** file.

- Obtained FTP credentials for **ftpuser** via a **hydra** brute-force attack.
- Decoded a brainfuck language message revealing SSH credentials for user **eli**.

4. **Internal Account Compromise**:
    - Accessed SSH with **eli**'s credentials.
    - Located a message intended for user **gwendoline** revealing her password.
    - Used the password to switch to the **gwendoline** user.
5. **Privilege Escalation**:
    - Discovered a **sudo** misconfiguration allowing execution of **vi** as a privileged command.
    - Identified **sudo** version as 1.8.10p3, vulnerable to CVE-2019-14287.
    - Exploited the vulnerability to gain a root shell.

Recommendations

1. **Service Updates & Configuration Management**:
    - Update all services to their latest stable versions to mitigate known vulnerabilities.
    - Ensure proper configuration management, limiting access to sensitive files and directories.
2. **Password Policy Enforcement**:
    - Implement a strong password policy, enforcing complexity requirements and regular changes.
3. **Regular Security Audits**:
    - Conduct regular security audits, including vulnerability scanning and penetration testing, to identify and mitigate potential security issues.
4. **Access Control Lists**:
    - Review and update Access Control Lists (ACLs) to enforce the principle of least privilege.
5. **Patch Management**:
    - Establish a regular patch management process to apply critical security patches and updates in a timely manner.
6. **User Education**:
    - Provide security awareness training to users to prevent the use of weak passwords and to recognize social engineering attempts.
7. **Incident Response Plan**:

- Develop and maintain an incident response plan to quickly respond to and recover from security breaches.

By addressing these recommendations, the organization can significantly improve its security posture and resilience against future attacks.

Conclusion

The successful penetration of the target IP **10.10.182.228** indicates a need for immediate action to secure the network environment. Through diligent application of the recommended measures, the organization can enhance its security and protect against unauthorized access and data breaches.