Brute It

Penetration Test Report

Executive Summary

This report outlines the security assessment performed against the target IP **10.10.198.193**. The assessment was conducted utilizing various security tools and techniques to identify vulnerabilities and to gain unauthorized access to the system for demonstrating potential security risks.

Methodology

The penetration test followed an organized approach that included the following steps: reconnaissance, scanning, gaining access, maintaining access, and covering tracks. Below are the specifics of the activities performed during the test:

Reconnaissance & Scanning

- An Nmap scan was conducted on the target IP address to identify open ports and services.

```
nmap -A 10.10.198.193
```

Scanning Results:

- Two open ports were identified:
  - Port 22/tcp: Running OpenSSH 7.6p1 Ubuntu 4ubuntu0.3
  - Port 80/tcp: Running Apache httpd 2.4.29

Web Application Enumeration

- A directory brute force attack was performed using Gobuster, revealing two directories:
  - /admin
  - /index.html

Brute Force Attack

- The admin directory led to a login page. A brute force attack was carried out using Hydra to identify valid credentials:

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.198.193 http-post-form
"/admin/index.php:user=^USER^&pass=^PASS^:F=Username or Password invalid"
```

  - The successful credentials obtained:
    - Username: admin
    - Password: xavier

Post-Exploitation

- Login to the admin page revealed an RSA private key which was then converted using **ssh2john** and cracked with John the Ripper to reveal the passphrase:

```
john bi -wordlist=/usr/share/wordlists/rockyou.txt
```

    - The passphrase obtained: **rockinroll**

Privilege Escalation

- Using **sudo -l**, it was found that **/bin/cat** could be executed as a sudo command without a password.
- Utilizing this, the **/etc/shadow** file was accessed, and the root user's hash was extracted and cracked using John the Ripper:

```
john roothash --wordlist=/usr/share/wordlists/rockyou.txt
```

    - The password for the root user was obtained and used to escalate privileges to root.

Conclusion

Following the security assessment, it was determined that the target system is vulnerable to a series of exploits, including brute force attacks and privilege escalation due to misconfigurations. The findings suggest a critical need for security enhancements and further investigation.

Recommendations

- Regularly update and patch all software to prevent exploitation of known vulnerabilities.
- Implement strict password policies to protect against brute force attacks.
- Conduct a thorough review of system permissions and enforce the principle of least privilege.
- Regular security audits and staff training are recommended to improve overall security posture.