Penetration Testing Report: Mustacchio

Objective: Conduct a penetration test on a target machine to identify vulnerabilities and gain root access.

Initial Steps:

1. **Aggressive Nmap Scan**: Start with an aggressive scan on the target IP using **nmap -A 10.10.222.57**. This reveals open SSH and HTTP servers, indicating potential entry points.

Website Analysis:

1. **Initial Exploration**: A preliminary look at the website hosted on the HTTP server doesn't reveal anything immediately noteworthy.
2. **Directory Enumeration**: Utilize **feroxbuster** with the command **feroxbuster --url http://10.10.222.57 --wordlist /usr/share/wordlists/dirb/common.txt** to discover hidden directories.
3. **Discovering Backup File**: In the **/custom/js** directory, a backup file **users.bak** is found, which turns out to be a SQL file.

Database Analysis:

1. **Accessing Database**: Use **sqlite3 users.bak** to access the database.
2. **Extracting User Data**: Execute **SELECT * from users;** to retrieve user data, revealing a potential admin username and a hashed password.

Password Cracking:

1. **Hash Identification**: The password hash appears to be SHA1.
2. **Online Cracking**: Use an online service like crackingstation.net to crack the hash, revealing the password **bulldog19**. It's unclear if this is for SSH or another service.

Further Scanning:

1. **Extended Nmap Scan**: Run a more comprehensive Nmap scan to check for additional open ports, discovering an HTTP server on port 8765 with an admin login panel.

Website Exploitation:

1. **Admin Panel Access**: Use the previously discovered credentials to log into the admin panel.
2. **Source Code Review**: A comment in the source code suggests a username **Barry** and hints at SSH access via a key.
3. **Discovering XML File**: An XML file **auth/dontforget.bak** is found, containing a verbose paragraph by Barry Clad.

XXE Attack:

1. **Preparing Payload**: Modify the verbose paragraph from Barry Clad's XML file for an XXE attack, targeting the system's **/etc/passwd** file.
2. **Executing XXE**: Replace the author field with an XXE payload to extract the **/etc/passwd** file, revealing user names including **barry** and **joe**.

SSH Key Extraction:

1. **Locating SSH Key**: Modify the XXE payload to extract Barry's SSH key from **/home/barry/.ssh/id_rsa**.
2. **Preparing SSH Key**: Save the extracted key as **barryid** and prepare it for cracking using **ssh2john**.

Password Cracking:

1. **Using John the Ripper**: Crack the SSH key passphrase with John the Ripper, using the RockYou wordlist.
2. **Gaining SSH Access**: Log into the SSH server with Barry's credentials.

Root Access:

1. **Searching for SUID Files**: Use **find / -perm -4000 2>/dev/null** to locate SUID files, finding **live_log** in Joe's directory.
2. **Exploiting SUID**: Create a bash script to elevate privileges using the found SUID file.
3. **Achieving Root**: Execute the script to gain root access and locate the root flag.

Conclusion: The penetration test successfully identified multiple vulnerabilities, from a simple SQL file exposure to XXE and SUID exploitation, leading to root access on the target machine. The process demonstrates the importance of thorough scanning, persistent exploration, and exploitation of even seemingly minor weaknesses.