|  |  |
| --- | --- |
| Describe | Vulnerability |
| Service | SSH |
| Ports | 22 |
| Version |  |
| Severity’s | Beginner |
| CVE id |  |
| Cvss score | 4/10 |
| Remediation | 1. **Anonymous Vulnerabilities And Remediation Strategies**  * **Issue:** the ftp service allows anonymous login, granting access to files like backup, which contains hashed credential. * **Remediation:** * **Disable anonymous ftp access:** configure the FTP server to disallow anonymous logins. * **Implement strong authentication:** requirevalid user credentials for FTP access. * **Restrict file permission:** Ensuresensitive files are not accessible via ftp or are adequately protected.  1. **Exposer Of Password-Protected ZIP Files**  * **Issue:** the accessiblebackup files is a password-protected zip archive containing hashed passwords, which can be cracked using tools like john the ripper with the common wordlists. * **Remediation:** * **Avoid storing sensitive archive in public directories:** ensure that backup file stored securely and not accessible via public services. * **Use strong passwords:** protect archive with complex, unique passwords to prevent brute-force attacks. * **Encrypt sensitive data:** Utilize strong encryption methods for storing sensitive information.  1. **Weak SSH credentials**  * **Issue:** cracked credentials from the backup file allow SSH access, indicating the use of weak passwords. * **Remediation:** * **Enforce strong password policies:** Requirecomplex, unique passwords for all user accounts. * **Implement Multi-Factor Authentication (MFA):** Add an extra layer of security for SSH access. * **Regularly Audit User Accounts:** Remove or disable unused accounts and monitor for unauthorized access attempt  1. **Privilege Escalations Via Sudo Misconfigurations**  * **Issue:** the user have sudo privileges that can be exploited to gain root access without proper restrictions. * **Remediation:** * **Review sudoers configuration:** Ensure that users have only the necessary privileges and cannot execute arbitrary commands as root * **Implement principle of least privilege:** limit user permissions to the minimum required for their role. * **Monitor sudo usage:** regularly check logs for unauthorizedsudoactivities. |
| POC | Step 1  First I find our ip In kali terminal    After this i find target ip with netdiscover    I get ip (192.168.1.153) now I find open port in this machine    After doing nmap I get 2 ports 21, 22 (ftp & ssh)  As you see in ftp in can login ‘anonymously’ so now first I access ftp for some information like ‘username’ and ‘password’ for SSH  Step 2    I can login ftp successfully so now I find “backup” file    Now I downloaded this file in my terminal.  After download I open backup file with cat command    So now I copy this credentials and make new file “hashes.txt” then decrypt this encryption      Now I crack this file with john command (for encryption victim use “sha512” so now I add “—format=sha512cyrpt” in john command)  John –format=sha512crypt (filename) –wordlist=/use/share/wordlists/rockyou.txt    I get username and password so now I access with this credential in SSH  Step 3    I login successfully so now I find flags in machine    First flag I get in sunset directory so now I find another flags  I didn’t get any flag so now I find root flag, for finding root flag I use sudo -l    no password in root so means I login easily For become root user I use command “sudo /usr/bin/ed” and then I become root like this I done    Like this I became root easily so now I find root flag    And done, I get root flag and I complete this machine also |
| References | https://www.hackingarticles.in/sunset-vulnhub-walkthrough/ |

Csv :-