|  |  |
| --- | --- |
| Describe | vulnerability |
| Service | FTP, SSH, HTTP |
| Port | 21,22,80 |
| Version | 2.4.41 |
| Severity | Medium |
| Cve id |  |
| Cvss score | 7/10 |
| Remediation | 1. **Anonymous FTP access with sensitive files**  * **Issues:-**  the ftp service allows anonymous login, granting access to the files like “***respectmydrip.zip”*** * **Remediation:** * **Disable anonymous FTP access:** configure the FTP server to disallow anonymous logins. * **Implement strong authentication:** require valid user credentials for FTP access. * **Restrict File Permission:** Ensure sensitive files are not accessible via FTP or are adequately protected.  1. **Exposer of sensitive directories via “*robot.txt”***  * **Issue:** The *robot.txt* file lists directories that are disallowed for crawlers but can still can accessed directory, potentially revealing sensitive information. * **Remediation:** * **Avoid listing sensitive directories:** Do not include sensitive paths in *robot.txt.* * **Implement access controls:** Use proper authentication and authorization mechanisms to protect sensitive directories. * **Regularly review** *robot.txt*: Ensure it doesn’t inadvertently expose critical paths.  1. **Password-proteected ZIP files with week Encryption**  * **Issue:** the ZIP file obtained via FTP iss password-protected but can be easily cracked, revealing sensitive information. * **Remediation:** * **Use strong Encryption:** Employrobustencryption algorithms for protecting files. * **Avoid storing sensitive data in easily accessible Locations:** ensure that sensitive files are stored securely and are not accessible via insecure channels. * **Regularly Audit stored files:** periodically check for and remove unnecessary or outdated sensitive files.  1. **Use of vulnerable** *pkexec*  **version**  * **Issue:** the system uses a version of pkexec that is susceptible to privilege escalation attacks. * **Remediation:** * **Update pkexec:** ensure that pkexec and packages are updated to the latest patched versions. * **Monitor for Vulnerability:** Stay informed about known vulnerabilities and apply patches promptly. * **Limited use of privileged tools:** Restrict the use of tools like ‘*pkexec*’ to trusted users and processes.  1. **Weak SSH credentials**  * **Issue:** theSSH service is accessible using weak or easily guessable credentials, compromising system security. * **Remediation:** * **Enforce strong Password policies:** require complex**,** uniquepasswords for all user accounts. * **Implement Multi-factor authentication(MFA):** Add an extra layer of security for SSH access. * **Regularly Audit users accounts:** Removeor disable unused accounts and monitor for unauthorized access attempts. |
| POC | Step 1  First I find our ip in kali linux    After that I find target machine ip with the help of netdiscover    I get my target ip add  (192.168.1.109)  After that I find open port with the support of ‘nmap’    As you see I get open port of target machine  21(ftp), 22(ssh), 80 (http)  Now first I download the *“respectmydrip.zip”* form target machine because ftp didn’t have any password so I can easily login with “anonymous”    Step 2  I know ‘***respectmydrip.zip’***  is zip file so first I use zip2john cmd  ***‘Jip2john***’ is a command-line interface utility that’s part of the **john the ripper** password-cracking suite. It is used to extract the hach from a password-protection ZIP file so that john the ripper can try to crack the password    After that I use cat cmd for looking the crack.txt file    And it’s done perfectly no I use john cmd ofr cracking the password of crack.txt (respectmydrip.zip)    And password has been crack successfully so now I use “-show” cmd in john for getting password of zip file    As you see I get the password of “respectmydrip.txt” is **“072528035”** so now I can access zip file easily  So first I look in my kali what I get after cracking zip file    As you see after cracking the zip file one i get **txt** file and one **zip** file  So I do same with secret.zip file but I didn’t get any interesting thing in that so now I read “***respectmydrip.txt”*** file with cat cmd    Step 3  After reading the txt file I get hint “just focus on ‘drip’ ” so after this I going to look now website of dripping blue    After looking the website I get some message and 2 name travisscott & thugger probably it can be use in ssh  So now I do dirb for getting directories    As we see I get three directories 2 are working and one are close  The first result in “index.php” which return a status code 200 this means the file exists and is accessible. It is likely the main page of website, and could provide useful information or serve as an entry point for the further exploitation  As the same as robot.txt also the status code 200 means the file is usually used to guide search engine on which parts of the website to crawl and ignore. Sometimes, it can reveal hidden or sensitive directories that are worth investigations furture  So now its time to look robot.txt directory because we already know about index.php    After this I get 2 more hidden directories so now I access both directories one-by-one    After access first one I get this message and didn’t get valuable information so now I access another one    After opening another directory same result I get like first one  So now, after doing some research I get back to to our terminal because I  remember about my ***“respectmydrip.txt”*** file  in that file will be written “focus on drip” so now I back to my web browse and put “drip” and add both hidden directories that I get in robot.txt    After including second hidden directories I get the the password the password so now I my doubt is clear    This is the username of SSH and the Password is “***imdrippinbiatch”*** but now I try do login both one by by in ssh after that I know about which one is real  Step 4    And yea I login with thugger successfully so now its time to find user flag and root flag  After getting acces of user so first flag I get in /home/thugger    So now it’s time to find another user/root flag  After doing some more research I know only root flag left over now so it’s time to find root    First I know about version of pkexec after that I find exploit in github (<https://github.com/ly4k/PwnKit/blob/main/PwnKit>)    After downloading the pwnkit, now I transfer this exploit in ssh with the support of python    But first I move myself in temp after that I upload and run that PwnKit exploit      Now I use chmod for making this PwnKit executable      As we see I become root user after run PwnKit  So it’s time to find root flag    After doing  cd /root  cat root.txt  I get final flag |
| Reference | <https://medium.com/@cybertodash/dripping-bluevulnhub-walkthrough-212f68db2875> |

**Csv :-** [**..\dripping blue.csv**](../dripping%20blue.csv)