|  |  |
| --- | --- |
| Describe | Vulnerability |
| Service | SSH |
| Port | 55077 |
| Version | 2.4.29 |
| Severity | Easy |
| CVE id |  |
| Cvss score | 5/10 |
| Remediation | 1. **Anonymous FTP access with exposed credentials**  * **Issue:** theFTP service allows anonymous login, granting access to sensitive files like *cred.txt,* which contains base64-encoded credentials. * **Remediation:** * **Disable anonymous FTP access:** configure the ftp server to disallow anonymous logins. * **Implement strong authentication:** require valid user credentials for ftp access. * **Secure sensitive files:**  ensure that sensitive files are not stored in publicly accessible directories.  1. **Weak web application authentication**  * **Issue:** theweb application accepts weak credentials (champ:password), allowing unauthorized access. * **Remediations:** * **Enforce strong password policies:** require complex, unique passwords for all user account. * **Implement account lockout mechanism:** prevent brute-force attacks by locking accounts after multiple failed login attempts. * **Regularly audit user account:** remove or disable unused accounts and monitor for unauthorized access attempts.  1. **Sensitive information hidden in image file (steganography)**  * **Issue:** files like funny.jpg and funny.bmp contain hidden data extracted using steganography tools like *steghide*. * **Remediation:** * **Avoid storing sensitive data in media files:** do notembed confidential information within image or other media files. * **Implement data loss prevention (DLP) measures:**  use DLP tools to detect and prevent unauthorized data storage or transmission. * **Educate Employees:** train staffto recognize and avoid improper data storage practices.  1. **Use of weak encryption (rot13)**  * **Use strong encryption standards:** employrobust encryption algorithm like AES for protecting sensitive data. * **Avoid obfuscation for security:** do not rely on simple obfuscation techniques as a means of securing data. * **Regularly review encryption practices:** ensure that encryption methods meet current security standards and best practices.  1. **Unrestricted sudo privileges**  * **Issue:** users haveunrestricted sudo access, allowing them to execute any command as root * **Remediation:** * **Implement principle of least privilege:** grantusers only the privilege necessary for their roles. * **Configure sudoers file carefully**: specify allowed commands for each user in the /etc/sudoers file. * **Monitor sudo usage:** regularly review and audit sudo command usage for unauthorized or suspicious activity. |
| POC | Step 1  First I find our ip in kali Linux    Now I find the target ip using netdiscover.    Now I finding open ports on my target machine.    The open ports on target machine are 21,80,55077(ssh)  Step 2  So first I take a look at FTP files    As you see I can login successfully with “anonymous”    I get 2 files ‘credit.txt & welcome’ now I download both files in my terminal    Here the first file welcome (nothing important I found here) after this I open ‘cred.txt’ file    So in this stage the data I get in cred.txt is encoded, so I decode this data with echo command as you see I get value “champ:password”  Step 3  After this I try to login ssh with this data but I can’t so I go to the website for collecting some details    Here the first page of website so here I put the data I get in cred.txt file    Now I can access the website here I start collecting data’s from website  First I try to dirb & gobuster I I didn’t get anything so I come back here again, but I get one hidden data in “about us”    After clicking the “about us”I get “downloads.rar” so now I extracts the file    In downloads I get one more directory ‘downloads’ now I get inside the directory I get 3 data “funny.bmp” & “funny.jph” and text file ‘sudo’  Step 4  First I open sudo file with cat command and I get this    It’s says “Did you notice the file name? isn’t is interesting? ” it’s give me hint something about username or password    So here I use ‘steghide’ cmd for extract data from image and for password I already get hint ‘sudo’  Steghide:- steghide is a tool to hide data inside images or audio files. If support JPEG, BMP, WAV and AU files. It can also encrypt the data while embedding.  So here I extract data from funny.bmp file  Now I extract from another image as I done    And from another one I get result from ‘funny.jpg’ to ‘funny.jpg.out’  Now I examine both file after extraction    Here the result    So now I open funny.jpg.out file so I get  The message  ‘this is\_not a python file but you are revolving around well, try\_ to rotate some words too.  After this I open another file    It’s look likes a uname & pass so here I use chatgpt to know about this file    Step 5  As you see this a encode data from ‘ROT13’ and after decrypt I get the result “wtf:this one is simple one”  So it’s a username and password of ssh I guess so now I try to access ssh with this credential      It’s a right credentials of ssh now I find flags in this machine    Here I get my first flag now I get a hint “well, look for the thing you want. It’s just 2 steps ahead :) ”  I get a idea to do sudo -l    And yes I get full permission so now I become root without any problem, so let’s do it    As you see I completed this machine easily |
| References | https://medium.com/@SR7/noob-1-walkthrough-6bd8de66c7d9 |

Csv :-