|  |  |
| --- | --- |
| Describe | Vulnerability |
| Service | Ssh, http |
| Port | 22/80 |
| Versions | 2.2.22 |
| Severity | Low |
| Cvc I’d |  |
| Ccvss score | 5/10 |
| Remediations | 1. **Exposure of sensitive information in *‘robot.txt’*:**  * **Vulnerability**: storing sensitive data or hints within the *robot.txt* file can inadvertently discloser information to unauthorized disclose * **Remediations**: ensure that robot.txt file can inadvertently disclose information to unauthorized users.  1. **Use of weak or default credentials:**  * **Vulnerability:** utilizing easily guessable or default username and passwords can lead to unauthorized access. * **Remediations:** * Enforce strong password policies requiring complex and unique passwords. * Regularly audit and update default credentials on all system.  1. **Outdated software and kernel versions:**  * **Vulnerability:** running outdated software, especially kernel with known vulnerability, can be exploited for privilege escalations. * **Remediation:** implement a regular patch management process to keep all software and system components updated with the latest security patches.  1. **Insufficient network segmentation:**  * **Vulnerability:**  Lack of proper network segmentation can allow attackers to move laterally within the network after initial compromise. * **Remediation:** design and implement network segmentation to limit access between different network segments based on necessity.  1. **Insecure Docker configurations:**  * **Vulnerability:** Misconfigured docker services can be exploited to gain elevated privileges or unauthorized access. * **Remediation:** * Follow Docker security best practices, such as running containers with the least privileges necessary. * Regularly review and update docker configurations to align with security guidelines. |
| POC | Step 1  First I find our Ip add in kali    After that I find victim ip add with the help of netdiscover    As you see I get victim IP Add Now I find open ports in victim Ip    I get open ports in victim IP port no 22 and 80 are open  So first I see website for gathering some information about victim and then I try to gain access with the help of SSH(22)  Step 2  As I say, So first I look website for getting some information    Here the website  So now I do first dirb. Dirb scans a target website for hidden or unlisted directory and files by making http requests based on a wordlists.    As you see I get some directories now I open one by and check all of them  But first I check *“robot.txt”*  file  Robot.txt is a text file used by website to control how to search engine bots (like Googlebot) crawl and index their pages. Robot.txt also specifying which pages or directories should be allowed or disallowed from indexing.  So that’s why I see first, let see what I get inside    I get something in robot.txt but it’s encryption from so now I ty ot do decrypt with the help of “**cyber chef”**      As you see I get first flag in robot.txt file  Now I find some another direction for getting something more after victim  After finding some more directories I didn’t get anything about it  Now I see source code of website for getting something different      And yes I get username: ‘itsskv’ in source code so now I username now I want find password and then I can login ssh  So now I searching again to get some clues about victim password.  After giving sometime in website I get the password of ssh its ‘***cybersploit{youtube.com/c/cybersploit}’*** this I get in flag1 after decrypt in cyberchef  Step 3  So now I login with ssh without any doubt    And yea I successfully login with ssh with the username of ‘itsskv’  So I find out some more user flags    So now I get flag2, but flag2 also encrypted  now I again use cyber chef for decrypt this encryption    As you see I get flag2 successfully now I try to find another flag or root user  Step 3  After this I didn’t get anything so, now I try to become root  first I find the version of victim machine    As you see I get the version so now I now I can find exploit of cybersploit    I get exploit of cybersploit (ubuntu) now I download this exploit and upload in target machine    As you see I download exploit (37292.c) now I upload in target machine with the help of python server  So first I open my python server “Pythone -m http.server 8080”  Step4  after this I put payload in tmp file as you see    Now I use gcc cmd  gcc cmd is use to compile a c program and specify the output filename for the compiled exucutable  gcc -o crack 37237.c    As you see I get the file name  ***‘crack’*** so now I exucate with cmd “ ./” and then I get root access  Like this I done    After executing “./crack” I become root    So now I find root flag and end this machine    Finally, I completed the machine by opening ‘finalflag.txt’ with the cat command. |
| Reference | https://www.infosecinstitute.com/resources/capture-the-flag/cybersploit-1-vulnhub-ctf-walkthrough/ |

Csv :- [..\cybersploit.csv](../cybersploit.csv)