|  |  |
| --- | --- |
| Describe | Vulnerability |
| Service | SSH |
| Port | 22 |
| Version | 2.4.38 |
| Severity | Low |
| cvc I’d |  |
| Cvss score | 5/10 |
| Remediation | If your’re seeking to remediate or secure system against the types of vulnerabilies showcased in the “deathnote” VM, consider the following general steps:   * ***Regularly update and patch system:-*** ensure all software and services are up-to-date to protect against known vulnerabilities. * ***Implement strong authentication mechanism:-*** use complex passwords and multi-factor authentication to prevent unauthorized access. * ***Conduct regular security assessment:-*** perform vulnerability scans and penetrations tests to identify and address potential weaknesses. * ***Monitor system logs:-*** keep an eye on logs for unusual activities that might indicate attempted or successful breaches. * ***Educate users:-*** Train users on security best practies to reduce the risk of social engineering attacks.   By adopting these proactive measures, you can enhance your system’s security posture and mitigate risks associated with common vulnerabilities. |
| POC | Step 1  First, we find our Ip in kali Linux    Step 2  Then we find Ip of death note  Netdiscover: - 192.168.1.104    Step 3  Then we do Nmap for checking open port in death note    Step 4  we see HTTP open lets check it!!    Its open but firewall stop us  Step 5  We do nano /etc/host    After that    Ctrl + O  Enter  Ctrl + X  Step 6  After that we by-pass the firewall    After reading everything carefully we know there two users “l” and “kira”    In this we want to find ‘note.txt’ in this server  Step 7  After that we want to check ‘robot.txt’ I thing we get something in there    After doing “ dirb <http://deathnote.vuln> “  We get robot.txt  Step 8  Lets check “robot.txt”  dirb <http://deathnote.vuln>/robot.txt    After that we found message just like you see  And we get hint about ‘/important.jpg’  Step 9  So lets replace and check what happen if we replace ‘robot.txt’  To ‘important.jpg’    After replace we can see site didn’t show us that page  Step 10  We use ‘curl’ for seeing what inside that page  Curl “ <http://deathnote.vuln/important.jpg> ”    As we see we get message In that we get login username but we didn’t get password so lets find out  Step 11  We do again “dirb http://deathnote.vuln/wordpress ”  For find more information    We get content upload file so lets check out what inside this    After this we get file ‘2021’    First we check what inside in 07/    We Found “note.txt” and “user.txt”    Step 11  Now we download that file with “wget”  Wget “ <http://deathnote.vuln/wordpress/wp-cont/uploads/2021/07/user.txt> ” for downloading  “user.txt”  Wget “ <http://deathnote.vuln/wordpress/wp-count/uploads/2021/07/notes.txt> “ for downloading “notes.txt”    After downloading that we use HYDRA command for bruteforce attack  Hydra -L user.txt -P notes.txt ssh://192.168.1.104    After that you see we get login and password  Step 12  After that lets try to do login in ‘l’ user while using  Ssh l@192.168.1.104    After login and password, I access in ‘l’ user  After reaching here I get the “first flag” after this lets try to find another flag    After that we get something in encrypted form  For decrypted we use brainfuck for decrypted that word    After decrypted we get message  “I think u got shell, but you wont able to kill me -kira”  Step 13  Now lets try to access with ‘kira’ user  Ssh kira@192.168.1.104    And yes we can access with kira  Lets try!  Step 14    And here we get another encrypted value  Lets try to decrypted this with ‘echo’ commad    After using ‘eco command’ we get 2 options lets try with first one  After that lets try to access ‘super user’    After that we get one more encrypted value  lets decrypted this one also with ‘cyberchef’    After that we get one more encrypted value lets decryptd this one also    After that we get password for ‘superuser’  Step 15  let’s try to access ‘superuser’ |
| Reference | https://medium.com/@x3r/deathnote-1-vulnhub-writeup-6d0b63b2d69b |

Csv :-[C:\Users\Ayush\Downloads\deathnote.csv](file:///C:\Users\Ayush\Downloads\deathnote.csv)