|  |  |
| --- | --- |
| Describe | Vulnerability |
| Service | ftp,http |
| Port | 21,80 |
| Versions | 1.3.3c |
| Severity | easy |
| Cve id | N/A |
| Cvss score | 4/10 |
| Remendiations | 1. Regularly Update and Patch Systems:  Vulnerability: Outdated software may contain known vulnerabilities that can be easily exploited using publicly available tools.  Remediation:  Implement Patch Management: Ensure all software, applications, and operating systems are up-to-date with the latest security patches. This reduces the number of exploitable entry points.  2. Strengthen Network Defenses:  Vulnerability: Open or unused ports can be targeted for unauthorized access.  Remediation:  Disable Unnecessary Services: Turn off services and close ports that are not in use to minimize potential attack vectors.  Deploy Firewalls: Utilize firewalls to monitor and control incoming and outgoing network traffic based on predetermined security rules, effectively blocking unauthorized access attempts.  3. Enhance Authentication Mechanisms:  Vulnerability: Weak or default passwords can be easily compromised using automated tools.  Remediation:  Enforce Strong Password Policies: Require complex, unique passwords and mandate regular password changes to enhance account security.  Implement Multi-Factor Authentication (MFA): Add an extra layer of security by requiring additional verification methods beyond just a password.  4. Monitor and Analyze Network Traffic:  Vulnerability: Unusual or unauthorized activities may go undetected without proper monitoring.  Remediation:  Deploy Intrusion Detection Systems (IDS): Implement IDS to monitor network traffic for suspicious activities and potential threats.  Analyze Logs Regularly: Consistently review system and network logs to identify and respond to unauthorized access attempts promptly.  5. Educate and Train Employees:  Vulnerability: Lack of cybersecurity awareness can lead to inadvertent security breaches.  Remediation:  Conduct Regular Training Sessions: Educate staff on recognizing phishing attempts, the importance of strong passwords, and adherence to security protocols to reduce the risk of human error.  6. Secure Web Applications:  Vulnerability: Standardized or vulnerable web architectures can be targeted using common exploits.  Remediation:  Develop Unique Web Architectures: Avoid using default templates or plugins. Collaborate with developers to create customized solutions that are less susceptible to generic attacks. |
| POC | Step 1  First I find my ip in arch linux    After that I found target ip with the help of “netdiscover”    Now I find open ports in target ip with the help of “nmap”    Step 2  Lots of ports are open but first I check website ‘http’    As we see firewall didn’t allow a my system for opening website    Now I do nano /etc/hosts for override, allowing a system to resolve domain names without querying an external DNS server.    Now I see website without any issue  Now I gathering information about this website for gaining access  Step 3  So first I use dirb for seeing opening directory    I get lot of directorys so now check one by one    I get login page of wordpress so I get hint this websiste work on wordpress if I didn’t get any intresting so I do wpscan for gathering the information  After checking all the directory I didn’t get any intresting thing so now I do wspscan for attacking in different in different way      As we see I get the superuser ‘admin’ so now I do bruteforce attack with the help of wpscan for cracking password of admin      Step 4  Didn’t get any intresting thing after doing ‘dirb’ and ‘wpscan’ so now I find exploit from Metasploit “msfconsole” lets see what I get now    So I do exploit with the support of ftp    As we see I get exploit of ‘funbox’ so I giving details for gaining access    I set RHOST  Now I do exploit    Exploit fails due to payload not selected so I do research and put this payload as you see  (cmd/unix/reverse)  After that I put my lhost as you see    Now my payload is ready its time to attack lets see I get success or not this time    This time exploit success as you see  Step5  lets see I get admin access or not    As we see I get admin access with the help of backdoor  Lets get root flag now    Getting success root flag this time!!! |
| Remediations | https://www.infosecinstitute.com/resources/capture-the-flag/funbox-scriptkiddie-vulnhub-capture-the-flag-walkthrough/ |

Csv :-