|  |  |
| --- | --- |
| Describe | Vulnerability |
| Service | SSH |
| Port | 22 |
| Version | 2.4.38 |
| severity | Easy |
| Cve id |  |
| Cvss score | 5/10 |
| Remediation | 1. **Anonymous FTP access with sensitive files**  * **Issue:**  the FTP service allows anonymous login, granting access to files like ‘*secret.jpg*’, which may contain critical information. * **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. **Weak Wordpress password policies:**  require complex, unique passwords for all users accounts.  * **Issue:** the WordPress site user weak credentials (e.g., username: albert, password: scotland1), making it susceptible to brute-force attacks. * **Remediations:** * **Enforce strong password policies:** require complex, unique passwords for all user accounts. * **Implement login attempt limits:** use plugins or server configuration to limit repeated login attempts. * **Regularly audit user account:** remove or disable unused accounts and monitor for unauthorized access attempts.      1. **Privileges escalation via nmap scripting engine**  * **Issue:** the system allows the userof nmap’s scripting engine to execute arbitrary commands, leading to privileges escalation. * **Remediation:** * **Restrict nmap usage:** limit access to namp or configure it to prevent the execution or arbitrary scripts. * **Implement principle of least privilage:** ensure users have only the permission necessary for their roles. * **Monitor for suspicious activitly:** use intrusion detection system to dectect unusual executions.  1. **Insecure file uploads**  * **Issue:** the wordpress site may allow file uploads without proper validation, potentially leading to remote code execuation. * **Remediation:** * **Validate uploads securely:** place uploaded files outside the web root or in directory with restricted execution permissions. * **Store uploads securely:** place uploaded files outside the web root or in directories with restricted execution permissions. * **Regulary scan for malicious files:** use antivirus or malware tools to dectect and remove harmful files |
| Poc | Step 1  First I find our ip in kali linux    Now i find victim ip with the help of netdiscover    Here I found ip of victim machine  So now I use nmap to find open ports    Here the open ports of target machine  Open ports are:- 21,22,80 (FTP,SSH,HTTP)  In ftp I can login with anonymous and get that “secret.jpg” image file    After this I Do ‘ls’ cmd for looking secret.jpg file    And here I open my secret.jpg file    Step 2  But in this image I didn’t found anything user full so now I access http for getting some usefull things    After access the website I get message no mutant allowed  so now first use nano /etc/hosts  Nano /etc/hosts opens the hosts file in a txt editor to manually map domain names to ip addresses.  So here I put ip and DNS name    And now I try to access again let’s see what I get  After try to access website again I get same result like last time so now I use “drib” I think it’s work now    After doing drib I get new directory “blog” so now I access new directory for getting something interesting    This the blog website I get something poem/rhyming about crosscut saw now I use gobuster fo getting directory/hidden directory in webserver    So I get 3 directory in blog file so first I look wp-admin directories    As you see it’s a login page of wordpress so now I want to find username and password  But first I remember about the blog site I get one hint at the end page of blog says ‘ proudly powered by WordPress’    Step 3  Now, I start with information gathering and use wpscan to get in depth info      As you see I get username ‘albert’ now I want to find password only and them I can access wordpress  For the password I use wpscan to perform a brute force attack and then I try to obtain the password      Now I have username & password so now I can login wordpress    After login in dashboard I get one pop-up “PHP update required” here I get one clue so here I upload “reverse shell php” in website so I get reverse connection in my linux  First I go to appearance then them file editor after that 404 template  After this I find “php-reverse-shell” payload and then I upload in this 404 theme  Payload:- ( <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php> )    After this I assign my ip and port no as you see  So now I click on ‘update file’ and done  Now I return to blog again and reading source code carefully and I find “twenty twenty-one” directory    As you see I find this directory so now I can run my payload but I want to do some changes in this URL    Like this so now I can execute my reverse shell easily but first I want to start my listener in my terminal so I can run my payload  Step 4    I am ready now I can execute my payload    After running my payload I get reverse connection on my linux (I spawn python for better using experience)  Now it’s time to find user/root flag    Here I found one user but I cant access due to permission deny, so now I find another way to get access  Now I do ‘ls -all’ it’s gives me a detailed list of all files (including hidden) in the current directory.    After using ls -all I get list of directories and I also get ‘.ssh’ directories also. so now I do cd .ssh and then I get id\_rsa, so now I run cat id\_rsa to view the private key, copied it, creating a new file using nano, and then upload it.    Like this I done,  Step 5  Now i do chmod for making this key executable, after that I access with ‘freddie’ while using his private key    So now I can access first flag    Step 6  So it’s time to find root user, now I do sudo -l that show me what sudo have permission I have    This like shows me you are allowed to run the /usr/bin/nmap command as root (superuser), And WITHOUT having to enter your password.  Here I upload nmap payload to get root access    As you see I become root user so now its time to find root user    Here I get rot user (something strange happen I can’t see my own cmd but I can see response)  I did  Whoam I “root”  cd /root “root.txt”  and done! |
| References | https://infosecwriteups.com/driftingblues-2-vulnhub-write-up-walkthrough-e694b2cffab3 |

Csv:- [..\drifting blue 2.csv](../drifting%20blue%202.csv)