|  |  |
| --- | --- |
| Machine Description | Anthem is a TryHackMe Windows machine vulnerable to insecure web application exposure, sensitive data leakage, and weak credentials leading to full system compromise. |
| Target IP | 10.201.7.149 |
| Vulnerability Name | Sensitive Information Disclosure and Weak Credential Management leading to Privilege Escalation. |
| Service / Version | TCP / 80 HTTP httpd 2.0 |
| CVSS Score / Severity | 8.8 High |
| Attack Vector | CVS3.0 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| Proof Of Concept | STEP 1 – Scanning target for Open Ports    STEP 2 - Enumerating Web page hosted on HTTP 80     * Robots.txt Details we have here some Text It might be password      * Found Login Page      * Here We don’t have credentials for login but we got some kind of poem on blogpost      * If you check the hint’s it says search on your favourite search engine, So let’s just copy the whole poem and search it on the google (my favourite search engine) and we get the name of admin.      * But the login page demands for email of the user. * So, let’s find the email address of the admin. * If you check on the hints then it says there is another email on the website which follows the pattern of admin’s email.      * And if you look at the first blog post on the website, it has email address of the author of the post which has the pattern of **initials of user’s name** @ **domain name of the site**.      * We got login     STEP 3 – We have creds of admin user so we can connect to the rdp service     * We got Remote Login      * After we enumerate some details and folder we found that there is hidden backup file      * If we try to access the content inside it say we do not have permissions     STEP 4 - Let’s try to modify permissions for file       * Now try to access the file got pass for admin : ChangeMeBaby1MoreTime      * Let’s try to access root flag      * Got ROOT flag and solved the machine |
| Impact | * attacker gains valid credentials and remote access. * privilege escalation leads to full SYSTEM compromise. * potential data breach from sensitive file disclosure. |
| Remediations | * remove hardcoded or exposed credentials from web content. * enforce strong password policy and credential rotation. * restrict remote service access and apply least privilege on accounts. * regularly audit and patch Windows services with escalation vectors. |
| Reference | <https://tryhackme.com/room/anthem> |