|  |  |
| --- | --- |
| Machine Description | A deliberately vulnerable lab machine for practicing web app exploits, privilege escalation, and post-exploitation to gain user and root access. |
| Target IP | 192.168.0.106 |
| Vulnerability Name | * Information disclosure via an exposed SMB (Samba) share. * Authenticated arbitrary file upload → Remote Code Execution (RCE) in the Koken CMS. * Misconfigured SUID binary → Local privilege escalation. |
| Port / Service | Port 80 – HTTP (Apache)  Port 139 – SMB  Port 445 – SMB  Port 8000 – HTTP (Web application) |
| Severity | 7.4 (High). |
| Attack Vetor | CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H . |
| Proof of Concept (PoC) | STEP 1 – Nmap to find the IP of the target machine.    **STEP 2** – Nmap Scan to discover open ports and Services  # nmap –p- -r -sC –sV 192.168.0.106 –open.  **This scan was used to identify all open ports along with default scripts and service versions.**    Step 3- Files and Directory brute-forcing was performed on the web server on port 80; however, no sensitive files were discovered at this stage.   * **wfuzz** A web application fuzzing tool used to discover hidden files and directories.           Step 4 – Files and directory brute-forcing was performed on the web server running on port 8000, which resulted in the discovery of several files and directories e.g. **192.168.0.106:8000/admin**.  1.      2.          Step 5- We found a Sambashare using enum4linux on this machine.    **Step 6- Trying to login as null user and found.**    **Step 7- We downloaded the mailsent.txt and found an email and potential password(babygirl).**    **Step 8: We filled out the information on the page we discovered on port:8000/admin in step 4 and entered the email address and password we discovered above.**    **Step 9- Remember your notes about the Koken file upload exploit. Slide to**[**pentestmonkey.net**](http://pentestmonkey.net/tools/web-shells/php-reverse-shell)**and download the php reverse shell script.**    **Step 10- Change the IP to your host’s IP and select a port. You will have netcat listen on this same port.**    **Step 11- First, we need to save reverse shell file with .jpg extension.**    **Step 12- Start Burp and on the admin page, in the lower right corner select “Import content”. Upload your exploit, your request will be intercepted by Burp and Remove the .jpg extension and forward the request e.g.: - offsec.php.jpg to offsec.php .**  **1.**    2.    3.    4.      5.        **Step 13-Now forward the packet that go the koken page.**    **Step 14-** **Go back to your terminal, you’ve got a shell!!, start a netcat listener and we got our first flag in user.txt .**    **Step 15- After further enumeration we found a file with set user id permissions i.e php7.2.**  **Execute the following command to locate all SUID executables on this host:**  ***#find / -perm -u=s -type f -exec ls -al {} \; 2>/dev/null***    **Step 16- we run the following commands for root**  **We’ve found a php7.2 binary! Head on over to**[**https://gtfobins.github.io/**](https://gtfobins.github.io/)**to get a curated list of binary exploit commands. I used the following**  ***#php -r “pcntl\_exec(‘/bin/sh’, [‘-p’]);”***    **Step 17- Find out who you are and then find the root flag!**  1.    2.    NOTE: - I didn't solve this machine in a single day, which is why my IP address is different than before. |
| Remediation | * Disable unnecessary services and restrict access to SMB if not required. * Apply proper authentication and access controls to web application endpoints. * Remove sensitive or unused files from the web server. * Keep the operating system and web applications updated with the latest security patches. * Implement network-level restrictions and firewall rules to limit exposure of internal services. |
| Impact | Successful exploitation of the identified vulnerabilities allows an attacker to enumerate internal services, access sensitive web application endpoints, and potentially gain unauthorized access to the system. This may lead to exposure of confidential data, service disruption, and full system compromise if privilege escalation is achieved. |
| References | * Nmap Official Documentation – <https://nmap.org/book/man.html> * Wfuzz Documentation – https://wfuzz.readthedocs.io * <https://pentestmonkey.net/tools/web-shells/php-reverse-shell> * https://portswigger.net/web-security/access-control |