Project Title: DeathnoteObjective

The goal of this project was to gain root access to the Deathnote VulnHub machine through penetration testing.

Environment Setup  
The virtual machine was set up using Oracle VirtualBox, with the target IP address configured as 10.10.0.2.

Tools Used

* Nmap
* Gobuster
* WPScan
* Hydra

Vulnerabilities Exploited

1. **OpenSSH (Port 22)**: Version 7.9p1 was detected, which is known for various vulnerabilities.
2. **Apache HTTP Server (Port 80)**: Version 2.4.38 was identified, which may have known issues.
3. **WordPress**: The machine was running an outdated version of WordPress (5.8) and the Twenty Twenty-One theme, both of which are susceptible to various vulnerabilities.
4. **Insecure Permissions**: The authorized\_keys file in the kira user's .ssh directory had world-readable permissions, allowing unauthorized access if the private key was compromised.
5. **Weak Passwords**: The password kiraisevil was relatively simple and could easily be guessed or cracked.

Steps Taken

1. **Port Scanning**:
   * Conducted a port scan using Nmap, revealing open ports 22 (SSH) and 80 (HTTP).
   * Identified the services running on these ports.

Command line: nmap -sV -sC -sS -p- -T4 10.10.0.2

1. **Directory Enumeration**:
   * Used Gobuster to enumerate directories on the web server.
   * Discovered the following:
     + /index.html (200 OK)
     + /robots.txt (200 OK) containing a hint: "added hint on /important.jpg"
     + /wordpress/ (301 Redirect)

Command line: gobuster dir -u http://10.10.0.2 -w /usr/share/wordlists/dirb/common.txt -t 50

1. **Image Analysis**:
   * Downloaded important.jpg from the robots.txt hint.
   * Converted the image to a text file to extract hidden content.

Command line: wget http://deathnote.vuln/important.jpg  
converted important.jpg to important.txt

1. **WordPress Enumeration**:
   * Conducted another Gobuster scan on the WordPress directory.
   * Found the login page and several important directories.

Command line: gobuster dir -u http://deathnote.vuln/wordpress/ -w /usr/share/wordlists/dirb/common.txt -t 50

1. **Vulnerability Scanning**:
   * Ran WPScan to identify vulnerabilities in the WordPress installation.
   * Key findings included:
     + XML-RPC enabled, which could be exploited for brute force attacks.
     + WordPress version 5.8 identified as insecure.
     + User kira discovered.

Command line: wpscan -e --url http://deathnote.vuln/wordpress/

1. **Brute Force Attack**:
   * Used Hydra to brute force SSH login using the identified username and a password list derived from notes.txt.
   * Successfully obtained the credentials:
     + Username: l
     + Password: death4me

Command line: hydra -L user.txt -P notes.txt ssh://10.10.0.2

1. **Privilege Escalation**:
   * Logged in as user l via SSH using the discovered credentials.
   * Explored the file system and found the kira user's home directory.
   * Created an authorized\_keys file in .ssh with the private key found earlier.
   * Used the private key to SSH into the kira account.
   * Discovered a file named case.wav in the /opt/L/fake-notebook-rule directory.
   * Decoded the contents of case.wav using CyberChef, revealing the password kiraisevil.
   * Used sudo with the kiraisevil password to gain root access.

Outcome  
The objective of gaining root access to the Deathnote machine was achieved. The successful exploitation of vulnerabilities in the WordPress installation, SSH service, and insecure permissions allowed for privilege escalation to the root user.

Lessons Learned

* **Importance of Enumeration**: Thorough enumeration of services and directories is crucial in identifying potential attack vectors.
* **Vulnerability Awareness**: Keeping software updated is essential to mitigate known vulnerabilities.
* **Brute Force Techniques**: Tools like Hydra can effectively exploit weak passwords, emphasizing the need for robust password policies.
* **Secure File Permissions**: Ensuring proper permissions on sensitive files, especially SSH keys, is critical to prevent unauthorized access.