Walkthrough: Chemistry HTB Machine) which is used on the web application running internally to read the root flag.

This report details the penetration test of the "Chemistry" machine, an easy-difficulty Linux target. The primary objective was to gain root access and retrieve the root flag.

**1. Initial Reconnaissance and Service Enumeration**

An Nmap scan was performed on the target IP address, 10.10.11.38, revealing two open ports:

* **Port 22/tcp:** Running OpenSSH 8.2p1.
* **Port 5000/tcp:** Running Werkzeug httpd 3.0.3 (Python 3.9.5). This port hosts a web application titled "Chemistry - Home," identified as a "Chemistry CIF Analyzer."

A screenshot of a computer

AI-generated content may be incorrect.

**2. Gaining a Foothold - Remote Code Execution via CIF Analyzer**

The "Chemistry CIF Analyzer" website allows users to upload Crystallographic Information Files (CIF) for analysis. Upon registering an account and exploring the application, it was discovered that the pymatgen Python library, used by the CIF Analyzer, is vulnerable to a Remote Code Execution (RCE) (CVE-2024-23346) through the upload of a malicious CIF file.

Initially, an attempt to upload an exploit.py file directly was met with a "Method Not Allowed" error. However, by downloading an example CIF file from /static/example.cif and embedding the exploit code within it, a reverse shell was successfully obtained upon "viewing" the crafted exploit.cif file. This provided a shell as the "app" user.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**3. Lateral Movement - Cracking Hashes and SSH Access**

As the "app" user, access to rosa's flag was denied. However, within the /app directory, a database.db file was discovered. This database contained stored user accounts and password hashes.

One of the hashes was successfully cracked using CrackStation, revealing the password for the rosa user. Using these credentials, SSH access was gained to the target as the rosa user, allowing retrieval of the first flag located at /home/rosa/user.txt.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.



**4. Privilege Escalation - Path Traversal via AioHTTP**

Further investigation of the listening ports on the machine from the rosa user's perspective revealed another web application running on 127.0.0.1:8080, identified as aiohttp/3.9.1. This version of AioHTTP is known to be vulnerable to a Path Traversal vulnerability (CVE-2024-23334) leading to Arbitrary File Read.

Direct access to this internal web application was not possible from the rosa shell. To access it, an SSH tunnel was established, forwarding local port 8081 to the target's 127.0.0.1:8080.

After tunneling, the internal web application became accessible via http://127.0.0.1:8081. While initial attempts to exploit the AioHTTP vulnerability directly were unsuccessful, a specific curl command was found to successfully exploit the Path Traversal vulnerability:

curl --path-as-is http://127.0.0.1:8081/assets/../../../../../root/root.txt

This command successfully read the contents of /root/root.txt, thus achieving privilege escalation and completing the objective.

A screen shot of a computer

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen shot of a computer program

AI-generated content may be incorrect.