**Walkthrough: LinkVortex HTB Machine**

This report details the penetration test of "LinkVortex," a retired HackTheBox machine. The objective was to gain user access and retrieve the user flag.

**1. Initial Reconnaissance and Service Enumeration**

An Nmap scan was performed on the target machine, revealing two open ports:

* **Port 22/tcp:** Running SSH.
* **Port 80/tcp:** Running Apache.

The domain name was added to the /etc/hosts file. Initial web reconnaissance included checking /robots.txt, which revealed a hidden directory /ghost leading to an authentication page. However, no credentials were available at this stage.

A computer screen with many white text

AI-generated content may be incorrect.

**2. Subdomain Enumeration and Git Repository Discovery**

ffuf was used for subdomain enumeration, which identified the dev subdomain. The command used was ffuf -w /usr/share/wordlists/amass/bitquark\_subdomains\_top100K.txt -H "Host:FUZZ.linkvortex.htb" -u http://linkvortex.htb -ic -fs 230. The -ic flag was used to ignore case sensitivity, and -fs 230 filtered out "not found" errors.

Further directory enumeration on http://dev.linkvortex.htb using gobuster revealed a .git directory. The command used was gobuster dir -u http://dev.linkvortex.htb -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt.

A screenshot of a computer program

AI-generated content may be incorrect.

**3. Gaining a Foothold - Git Repository Dump and Credential Disclosure**

The .git repository was dumped, and by examining the git status, a committed change to authentication.test.js was discovered. Restoring this file revealed the password for admin@linkvortex.htb using grep -r 'pass' ../../../../../ghost/core/test/regression/api/admin/authentication.test.js.

A screenshot of a computer program

AI-generated content may be incorrect.

**4. Lateral Movement - Arbitrary File Read and User Flag Retrieval**

Inside the system, it was identified that the application was running version 5.58.0, which is vulnerable to an Arbitrary File Read (CVE-2023-40028). A Proof-of-Concept (POC) for this vulnerability was used to gain further access, which also revealed another username, bob, with the password fibber-talented-worth.

SSH access was then established using bob's credentials, and the user flag was successfully retrieved.