**Cactus Hack-the-box machine write-up**

1. Firstly, I did a Nmap scan to scan for any open ports and their information. SSH and HTTP 8080 ports are open. Port 8080 uses a PHP server.

A computer screen shot of a program

Description automatically generated

1. After noticing port 8080 is open, I entered the IP address. The Cacti website was running version 1.2.22. There is an exploit found on the internet, CVE-2022-46169. I created a file with that exploit name and added the commands to that file. This exploit allows an RCE to obtain a reverse shell.

A green and white rectangle with numbers

Description automatically generated

A screenshot of a computer error

Description automatically generated

A screenshot of a phone

Description automatically generated

1. I started a reverse shell for port 443 (the listening port) and ran the exploit found. It was successful!

A computer screen with white text

Description automatically generated

A screen shot of a computer

Description automatically generated

1. Once I got in, I changed the directory into the home and found a flag.txt file. I opened it and the flag was there!

A screenshot of a computer

Description automatically generated