Machine

**Date:**

**Prepared by:** (Author name you want to showcase)

**Difficulty:** Medium

**[Machine-Name]**

**Introduction \***

Skills and vulnerabilities needed

**Passwords \***

Username (List all users) = password

Root = password

**Running Processes \***

* Describe running processes or services on machine such as apache2, nginx, ftpd, etc
* Crons / Scheduled tasks (Add source code of script and if script is bigger in size then attach file)
* Explain if there are any additional elements that should be noted or understood

**Writeup \***

* Provide a detailed, step-by-step walkthrough for completing the machine from beginning to end. Organize your walkthrough according to below sections and include images or screenshots to help the user through the exploitation process.

**Enumeration \***

* Describe enumeration process

**Exploitation \***

* Describe exploitation process

**Lateral Movement (optional)**

* Describe lateral movement (With all screenshots).

**Privilege Escalation \***

* Explain in detail privilege escalation (With all screenshots)

Challenge

**[Challenge-Name]**

**Date:**

**Prepared by:** (Author name you want to showcase)

**Difficulty:** Medium

**Summary \***

* Provide a brief explanation of the steps the user needs to take to solve this challenge.

**Description \***

* Brief description

**Skills Required \***

* Python
* Wireshark
* RE tools (i.e. Ghidra, IDA)

**Skills Learned \***

* Scripting

**Enumeration \***

* Describe the source files included in the provided zip/rar file.
* Explain in detail about the workflow and goal behind it.
* Additionally, provide a summary of the various related items.

**Solution \***

* Give in detail explanation about the solution or vulnerability.

**Exploitation \***

* How to perform all solution or exploitation to get the flag (Add detailed screenshots explaining everything)