Target 2 - Exploiting Bifur

> 💡It's safe to guess that Bifur may have some of the vulnerabilities that we've discussed in this module. Your job is to conduct a Penetration test on Bifur within 2 weeks. A foothold is definitely achievable on this system but full system compromise is a harder nut to crack. A lab next week might give you a hand in privilege escalation. But for now, enumerate Bifur to the best of your ability and begin the hard work of penetrating the target.

IF you have issues

- Check the target discussion for tips and tricks from your instructors and peers, NO SPOILERS please.

Grading Criteria

Deliverable. Pentest Report on bifur as a docx file. This should be formatted similar to the cupcake report. Provide the Following Information to include commands and screenshots. Come up with your own Title Page and Pen Test Organization (A Tolkien theme is preferred). Here's a sample prepared by a student on the cupcake target. The following markdown template is also a good guide for those data elements you need to capture.

See the rubric for exactly how you will be assessed.

- You have a well formatted, constructed penetration test report that meets the data elements illustrated in the template.
- You have a executive level Target Overview Section
- For each vulnerability discovered, you have a Title, Explanation, Links to CVE/ExploitDB/References. You have an associated severity and recommended mitigation strategy.
- You have a list/screenshot of open ports and services
- You show how you discovered the vulnerabilities.
- You show how you got a foothold on the system that allows you to perform remote code execution and eventually a shell.
- You show the incremental elevation of privileges to the penultimate privilege of root/Administrator.
- In some cases there are user and root flags. Where these are not present you can issue commands equivalent to: hostname, whoami, ifconfig.
- Acquire any data such as password, account names, hashes, ssh keys, sensitive documents that you can use on future targets or to speed your access to this one.