

Target 3 - Exploiting Boromir (10.0.6.51)

💡 Your job is to conduct a Penetration test on Boromir within 2 weeks. Boromir is on the RIVENDELL network so you will need to pivot to it via fw-rivendell. Consider how you might conduct host discovery and open ports via another host. Make sure to briefly discuss how you got access to the pivot point. A full pentest report of fw-rivendell is not required.

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 the target 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.