Updated Apr 21, 2022

Final Pentest Report

Over the course of the next two weeks, several targets will be deployed on the SHIRE and RIVENDELL networks. Your team's objective is to exploit at least two of these targets and thoroughly document the pentest. You will need to include a Target section that lists your successfully compromised systems. Again this includes at least 2 shire.local or rivendell.net systems

Team arrangement. You can work with 1 other student. Let the instructor know or use canvas to add yourselves to a team so that you can be teamed together in CANVAS. You can also go solo but you will still need to do 2 targets.

Metasploit Usage: You can use metasploit, though exploiting by hand is likely more educational. Also, metasploit will not work on some of these targets.

Final Project Discussion. Make heavy use of the discussion assignment that will accompany this project. If another team is having difficulty, help them out without providing spoilers. A nudge in the right direction or a link to a helpful resource is sometimes all that is needed as opposed to giving them the cracked password or fuzzed file path.

`Deliverable. Final Pentest Report as a docx file. This should be formatted similar to the cupcake report, however you will have multiple targets as opposed to just one.`

Targets (potentially more to be added over the next couple weeks)

SHIRE.ORG

- arwen
- fw-rivendell/wp-rivendell
- prancingpony
- bree
- boromir
- bifur (EthHack2 Target)

RIVENDELL.NET (these targets are dependent on a fw-rivendell hack)

- boromir (EthHack2 Target)
- shadowfax (a very hard EthHack2 Target)

Updated Apr 21, 2022

Grading Criteria

Note, this assignment is in the 20% - Quiz and Assessment Category.

Each Target is worth 10 points. For each Target provide:

Deliverable 1. Provide the Following Information to include commands and screenshots. Provide all this information within a Pentest Report for this target. 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.

- Target IP Address
- Open Ports
- Discovered Vulnerabilities (includes foot hold/remote and local privilege escalation)
- How you achieved a foothold (show commands used)
- User Flag (cat this file)
- How you achieved root/Administrative level compromise (show commands and techniques used)
- Root Flag (cat this file)
- Loot, did you find anything that could be used on other targets?
- Mitigation. How might the vulnerabilities be mitigated by the system administrator? Be specific.