Updated 8/31/22

Target 1.1 - Warmup

💡A summer or year away from Pentesting will likely affect your performance, this warmup module is designed to refresh your skills so that we can get on to more advanced work in the upcoming weeks.

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

Step 1 - Connect to the Range

Kali: Here's a link to the SEC335 Lab that walks you through setting up chrome remote desktop

Step 2 - BIOS

Revisit this target from SEC335. The passwords have been changed but some of the new credentials will be useful later in this course. Concentrate on guessing peregrin.took's ssh credentials using a mangled wordlist. Elevate your privileges and then grab the http and OS hashes. Crack them using the same techniques and mangled wordlists you used back in SEC335. You may find some other users from middle earth that you will need to use a larger list like rockyou on. Start building up a text or csv file of users and passwords.

BIOS hint, as you've done this before we will speed things up by the following hint: Pippin Tooks non mangled password starts with a P.

Step 3 - SHIRE.ORG Warm Up Targets 10.0.5.0/24 (one of these)

Pick a target from the list below that you've not gone after before (these are the SEC335 final targets, though with new passwords). Work with a teammate that has had SEC335 in the last year. This is due in 2 weeks, however we will be starting a new module next week.

- fw-rivendell.shire.local (note, this is not what it seems)
- prancingpony.shire.local (you will want to visit gloin first)
- bree.shire.local (you will want to visit bios first)
- arwen.shire.org

IF you have issues

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

Updated 8/31/22

Grading Criteria

Deliverable 1. Provide a screenshot that shows your crack of peregrin.tooks password on bios.

Deliverable 2. Provide a screenshot that shows the cracked http and ssh hashes, try to get at least 2 http passwords and two more ssh passwords cracked.

Deliverable 3. Pentest Report on your selected warmup 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. You can also consider the use of a target specific template similar to this one.

- 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). You just might not get root, if not what did you try?
- 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.