EPT Final Exam Grading Rubric

The final exam is designed to test your knowledge of everything you have learned in the course so far. You will have until the end of the class period to attack three (3) machines. To get full credit, you will be required to submit a hash AND a short description of how you exploited the machine. To get partial credit, you will be required to prove that you have identified the right vulnerability and have worked toward exploiting it.

Total Points: 100

Exploit and explanation: Post the hash and 2-5 sentences describing what you did to exploit the host. A hash with no explanation is worth **nothing**.

Two (2) hosts have **only** a proof hash. One (1) has a local **and** proof hash. The local hash will count as full credit for that host, the proof of that host will be worth 20 **bonus** points.

Host #1: 50 points
Host #2: 30 points
Host #3: 20 points

You will assign which host you deem as 1, 2, and 3. This allows you to get the most points for the hosts you do the best on.

Partial write-up: If you **do not** successfully exploit the machine, you can receive some credit for a partial write-up. You must prove to the instructors that you are on the correct path to exploitation.

15 points per host to include:

- Host IP address (2 points)
- ALL open ports and services (3 points)
- Correctly identified vulnerability (10 points)
  - Scanner results, if applicable
  - Exploitation attempt(s)

Rules of Engagement
In-scope: 10.20.160.0/24
Exclusion: 10.20.160.1

*The customer has reported that another pen testing team has identified a SQL Injection vulnerability (see below) on one of the hosts but did not have time to test it. They have requested that you do so during your assessment.

Notes:

- The target hosts are on the same subnet. There will be no need for routing or port forwarding.
- The targets can be exploited independent of each other.
- The exploits are basic in nature and will test your ability to use the tools that have been covered in the course.
  - Every exploit may not be a Metasploit module. Use your knowledge to scan the machine and identify attack vectors.
- Nessus will be available (you must start the service) but should not be used as a crutch.
  - Remember, some vulnerabilities are simply just misconfigurations.
- It is recommended to take notes on paper or other means while you are working. You don't want to take the risk of losing your work if Canvas and LEAPfwd go sideways.
- If you feel a host needs rebooted, the easiest way is to close out of the exercise and load it up again. This is another reason why notes should be taken "offline".
- Like the quizzes, you will be permitted to use any resource, including the Internet. Absolutely no communication can be done with other students, this will result in a 0 grade on the exam.
