Lab 0: Physical Pen Testing

Description

In this lab, your goal is to obtain access to a physical flag. The flag is kept inside the pen testing lab lockbox. As a real pen tester, it might be easier or faster to use social engineering to gain access to a restricted physical area. Other times, however, you may have to resort to lock picking. Some locks can only be opened during certain times of the day and on certain days. To simulate this, you must pick the lock during the second hour of class. You will have all semester to do this lab.

Objectives

* Acquire practical skills that can be applied to physical penetration testing in a structured, guided manner under the direction of a faculty member.Learn about different lock picking methods
* Engage in critical thinking and analysis to apply those practical skills to a simulated real-world problem.
* Develop an enhanced appreciation for the importance of hardened physical security through a greater understanding of physical vulnerabilities.

Scope

For the purposes of this lab, you are authorized to pick the lock on the lockbox, as well as any practice locks provided by the instructor or TA. You may use the lock picking tools provided by the instructor or bring your own. **DO NOT PICK ANY OTHER LOCKS THAT YOU DO NOT OWN OR HAVE EXPRESS PERMISSION TO PICK.** You will probably be arrested if caught. Laws about lock picking vary by state, with some states considering possession of lock picking tools to be prima facia evidence of criminal activity and you may be arrested (although this is not currently the case in Utah). In some countries, it is illegal to even own lock picking tools without a license. Always check local laws regarding lock picking before attempting it in a physical pen test. Laws about lock picking tools in the state of Utah are found in Title 76, Chapter 6, Part 2, Section 205 of the Utah Code.

Method

1. Learn about the different lock picking tools and their functionality, as well as general lock picking techniques.
2. Be present during the second hour of class. Picking the lock during other days or times will result in a zero.
   1. If you are unable to attend the second hour of class for the entire semester, talk with the instructor or TA about alternate times.
3. If a practice lock is available, it may be helpful to begin with this lock in order to get the feel of moving the pins around.
4. Pick the lock on the box
   1. This is not a social engineering lab. You may not have someone else pick the lock for you.
   2. Try different tools and methods if you are having trouble.
5. Once inside the box, take a picture with the flag. Sign the log and add a small message if you would like (although this is not required for credit).
   1. The picture must include some kind of evidence that it was taken during the second hour of class.
6. Reset the box for other students to use.

Submission

Extend your Behemoth report with a brief description of the tools and methods you used to pick the lock, as well as the image described above.

Grading Rubric

|  |  |
| --- | --- |
| You pick the lock on the box during the appropriate time and document it correctly. | 100% |
| Anything else. | 0% |

Resources

YouTube lock picking tutorials

Various lock picking websites

The instructor/TA

Lab 0: Physical Pen Testing

Setup:

The lock box can be left in the pen testing lab, or brought into class by the TA or instructor each week depending on instructor preferences. The box should be locked with some sort of pickable lock, and the flag[[1]](#footnote-0) along with a log and writing implement should be kept inside. As a backup, the engraving of Tux The Penguin on the underside of the lid may be used in documentary pictures until the main flag is replaced.

Student Process:

Start by learning how to pick locks through online resources. Resources:

* <https://www.artofmanliness.com/articles/how-to-pick-a-lock-pin-tumbler-locks/>
* <https://www.art-of-lockpicking.com/how-to-pick-a-lock-guide/>
* <https://www.youtube.com/watch?v=mO3mMYwKkKs> (Good basic info on locks and a demonstration. Music is annoying, watch on mute)
* <https://www.youtube.com/watch?v=YhrEJQq-6WE>

Practice on the clear next to the box (if the instructor has provided a clear lock).

Pick the lock that is on the box.

Sign the sheet to show you got in (if they want to).

Take a picture with the flag (the turtle) and add it to your report.

* Include the classroom clock in the picture to prove you got in in the allocated time slot

Learning Outcomes:

1. Students will acquire practical skills that can be applied to physical penetration testing in a structured, guided manner under the direction of a faculty member.
2. Students will engage in critical thinking and analysis to apply those practical skills to a simulated real-world problem.
3. Students will develop an enhanced appreciation for the importance of hardened physical security through a greater understanding of physical vulnerabilities.

1. The flag is currently a small plastic blue and yellow turtle, although if a student should steal the flag this may need to be replaced. The turtle came from a Kinder Joy, so it may be difficult to obtain another one. A hard to find item was chosen purposefully in order to reduce the ability of a lazy student to purchase a copy of the flag and take a picture with it during the second hour of class. [↑](#footnote-ref-0)