Lab 10: Attacking Webservers from the WAN

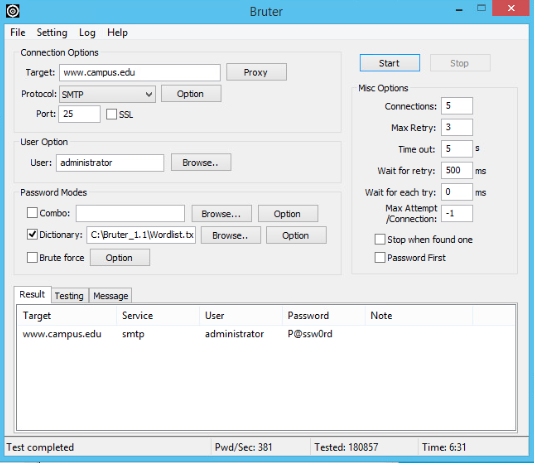
Lab report template Name: Kevin Ubilla

This Lab is Required for Unit 6. It is worth 15 points. The Challenge exercise is worth 2.5 Extra Credit points.

1. **Launching the Attack, Step 10:** Please use your own words to describe exactly what Bruter does and paste it here:

**→ Bruter uses a dictionary, or a type of list composed of commonly used passwords, to brute force a password authentication attack. It iterates through all the passwords in the dictionary until something works and then returns the successful password that works to gain access. ←**

1. **Launching an Attack, Step 19:** Please capture the Bruter screen showing both the username and password and paste it here:

**→  ←**

1. **Altering the Website, Step 14:** Please capture the screen that shows the contents of the xampp folder and paste it here:

**→ A picture containing text, screenshot, software, computer icon

Description automatically generated ←**

1. **Altering the Website, Step 24:** Please capture the screen showing the contents of the www.campus.edu web server as it has been altered and paste it here:

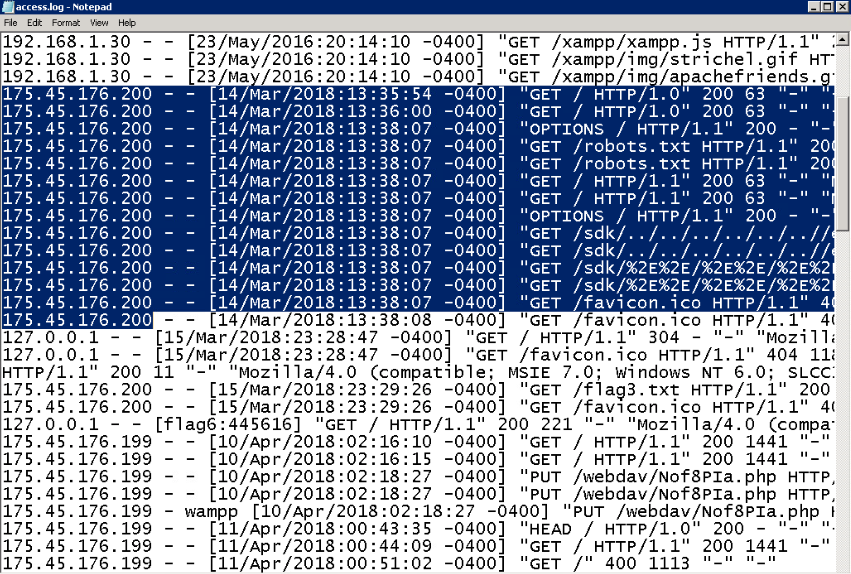
**→A computer screen shot of a web server

Description automatically generated with low confidence ←**

1. **Altering the Website, the whole section:** Please tell me, in your own words, what XAMPP is.:

**→ XAMPP is an open-source Apache web server solution written in PhP, MySQL, and Perl. It is used mainly for web app testing on a local server. Although it is widely used, it has its vulnerabilities. ←**

1. **Covering Tracks, Step 11:**  Please capture the screen of access log entries that shows the highlighted first access of 175.45.176.200 and subsequent accesses (perhaps a dozen entries) and paste it here:

**→ ←**

1. **Covering Tracks, Step 13:** Although you have removed evidence of your tampering with the web page, do you imagine that there are any tracks remaining in other logs at other levels in the system? Where might those other tracks remain? Please respond in your own words, in text, here:

**→ I believe there might be logs when clicking through the folders. Sort of like a keystroke logger but for folders. This should identify the permission level of the user who accessed the documents and provide info about their steps of clicking through folders. Furthermore, I think this might also depend on the type of security that the target has, and whether they have IDS or other vulnerability detection. ←**

**If you encountered any issues, either positive or negative, with this Lab, please let me know by commenting here. (This IS an experiment, after all.) I am tuning this according to what you say.**

**→ ←**