Lab 11: Exploiting a Vulnerable Web Application

Lab report template Name: Kevin Ubilla

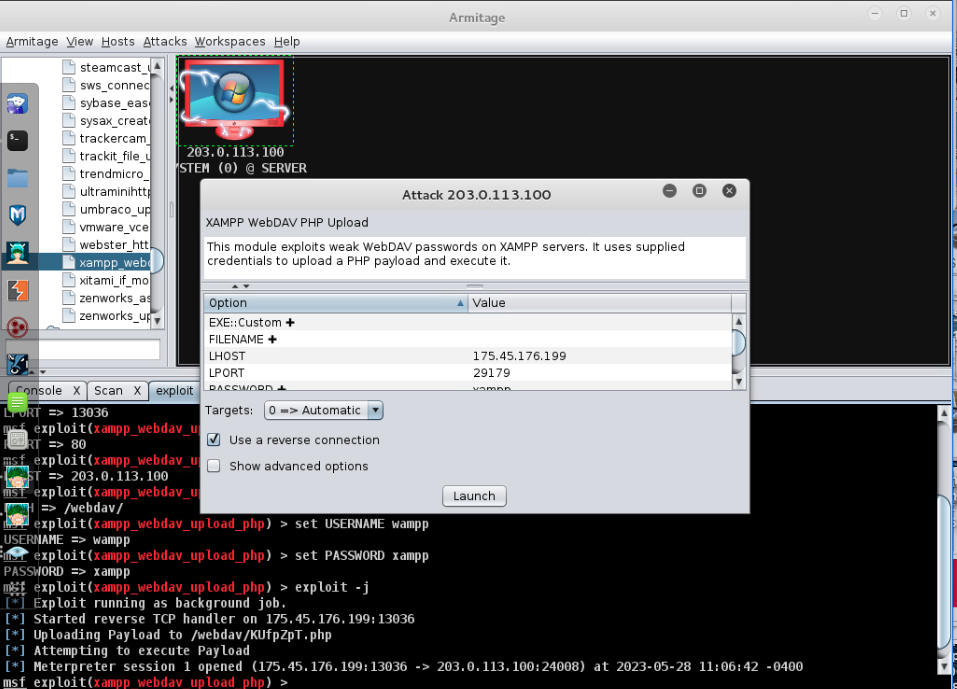
This Lab is required for Unit 6. It is worth 15 points. The Challenge exercise is worth 2.5 Extra Credit points.

1. **Scanning and Finding an Exploit, Step 8:** Highlight the line in the Zenmap report of the scan of 203.0.113.100 that shows port 80 is open, capture the full Zenmap screen and paste it below:

**→ A screenshot of a computer

Description automatically generated ←**

1. **Attacking the Target, Step 16:** Capture the entire Armitage screen that shows the dialog box that launches the XAMPP WebDAV PHP Upload exploit and paste it below:

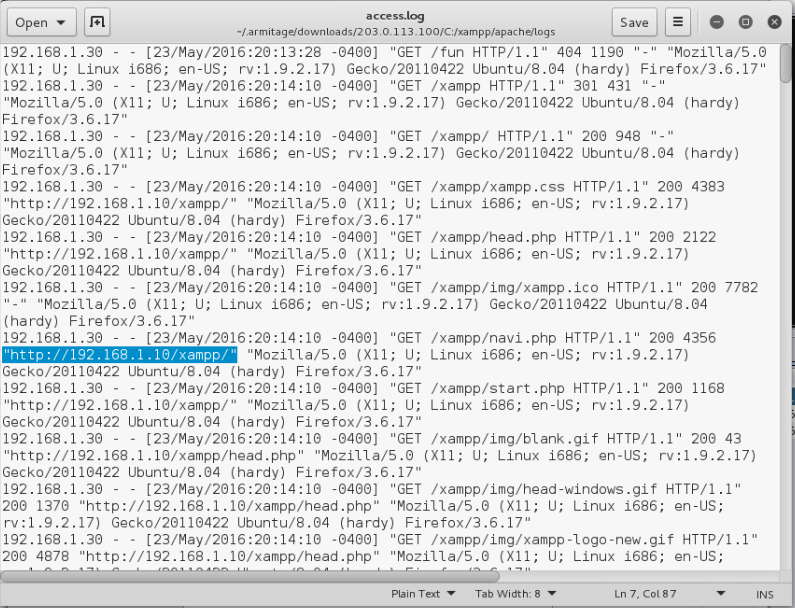
**→ ←**

1. **Attacking the Target, Step 19:** Capture the hierarchy of boxes that shows your arrival at the Browse Files step in Armitage as you examine 203.0.113.100 – capture it before you click on Browse Files.

**→ A screenshot of a computer

Description automatically generated←**

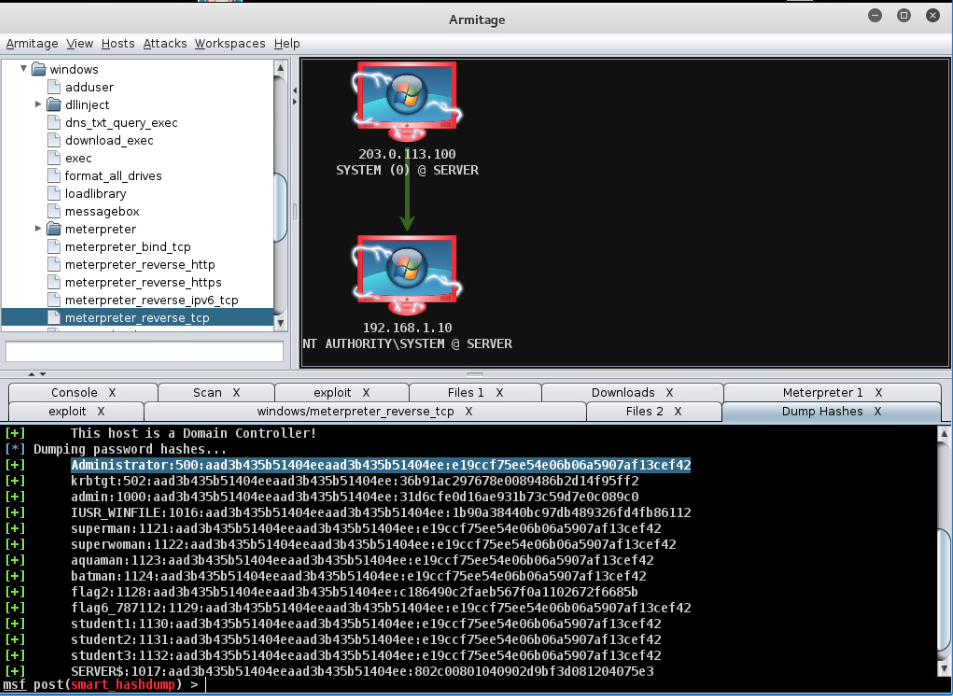
1. **Attacking the Target, Step 38:** Highlight the access.log entry that shows the internal IP address for the web server in the contents of the downloaded log entries, capture that entry and several entries above and below and paste it below:

**→ ←**

1. **Post Exploitation, Step 5:** Please, in your own words, explain how we came to know the IP address (192.168.1.10) used in the Add Hosts command, and put it below:

**→ We found it on the access.log file that was accessed previously by exploiting the target machine. Xampp is the web server being used by the target and thus, it will maintain a copy of their internal IP address. ←**

1. **Post Exploitation, Step 39:** Capture the screen showing the Administrator's password hashes on the Armitage screen (please include both upper and lower panes if possible) and paste it below:

**→  ←**

**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.**

**→ It took me a while to discover the ports; it kept saying that the host was down so I had to run -Pn.A computer screen with white text

Description automatically generated with low confidence←**