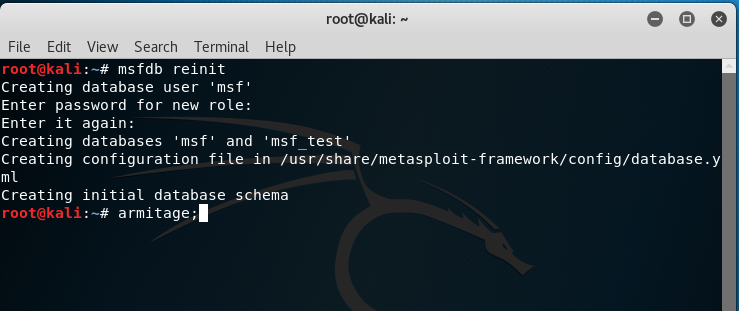
Derrick Sung

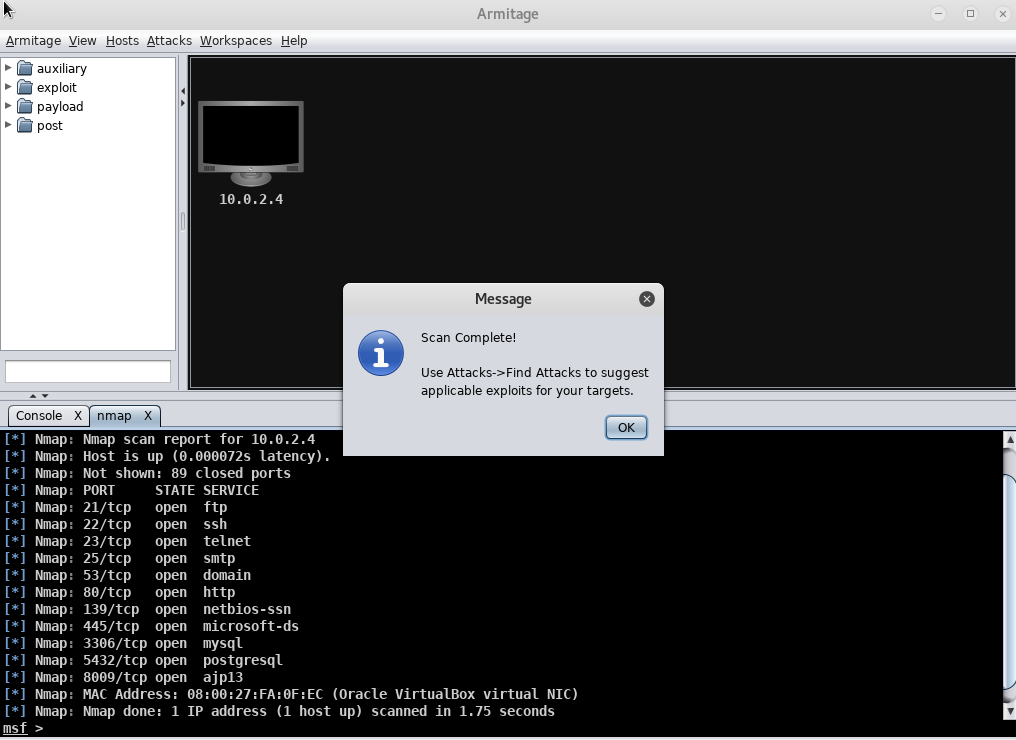
Pentesting

Victim 1 - Meta 1: 10.0.2.4 Victim 2 - Meta 2: 10.0.2.6

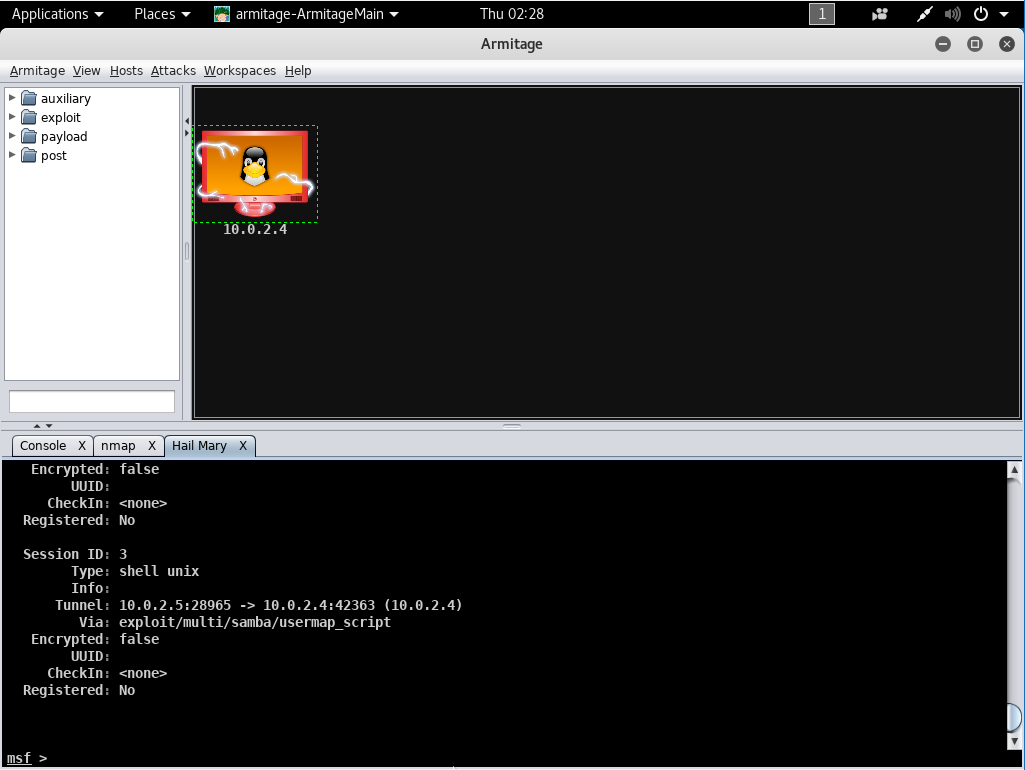
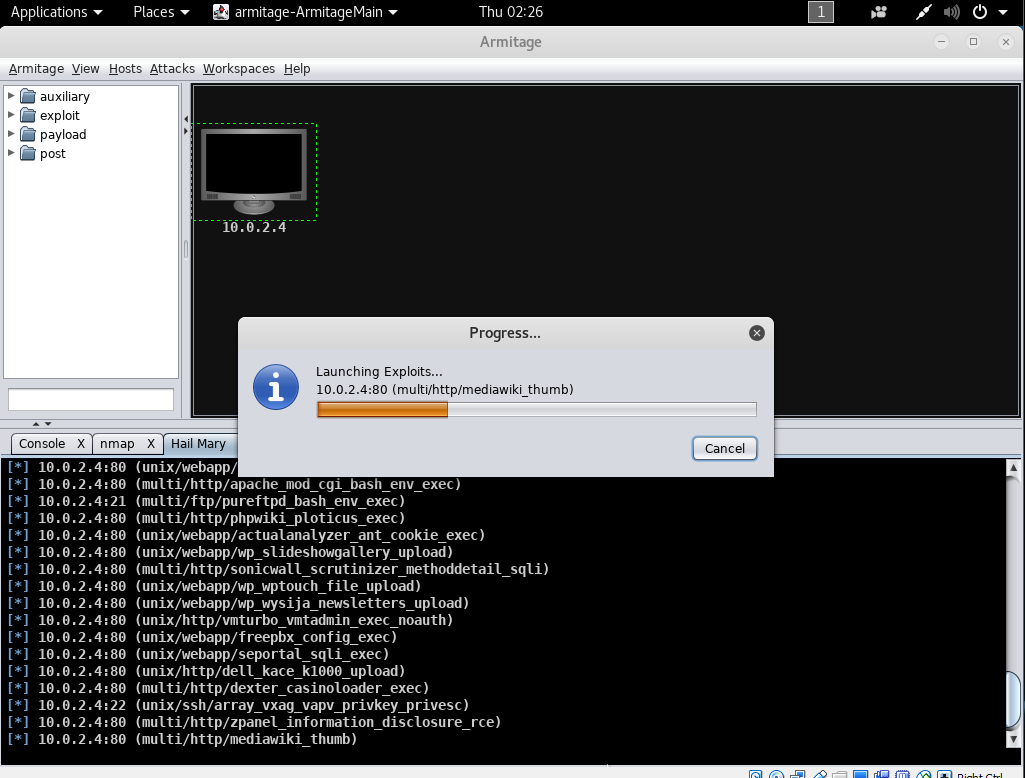
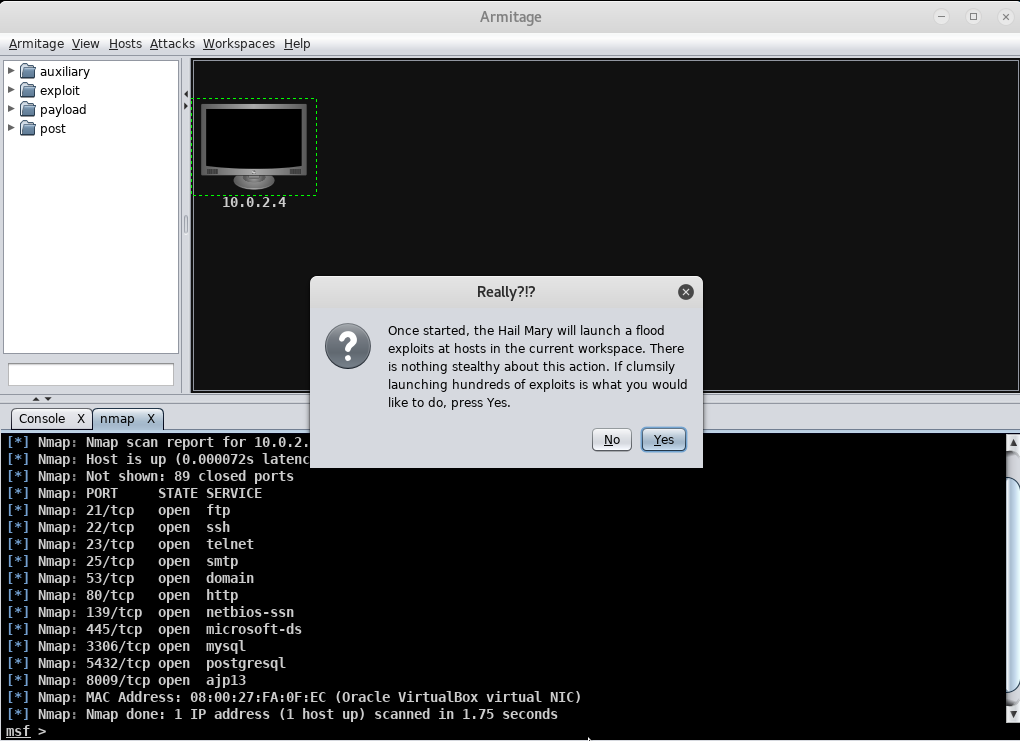
1. **To open Armitage: Open a new terminal -> msfdb reinit -> Armitage; -> click yes**



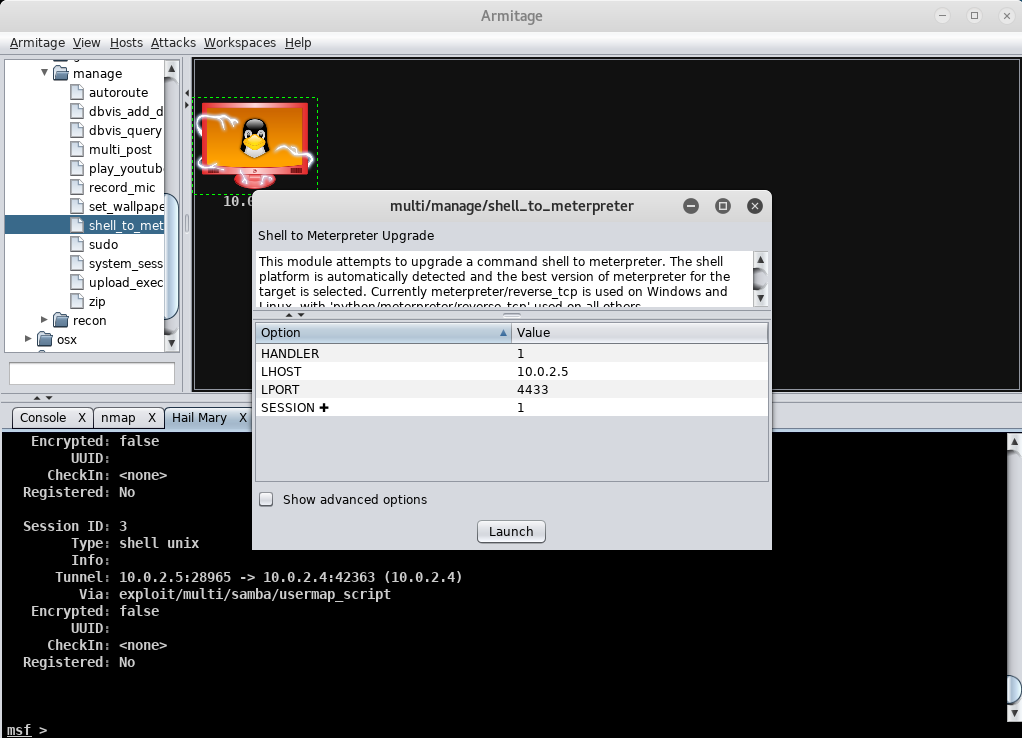
1. **To scan Meta 1: In the Armitage window, click host -> nmap -> quick scan -> Scan Victim 1 IP**



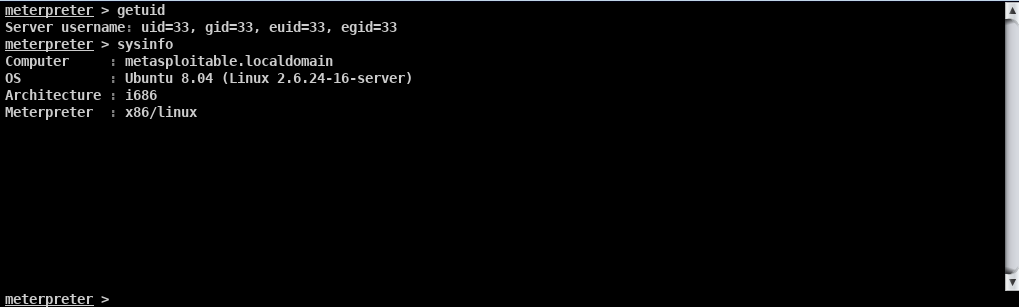
1. **Highlight the victim and attack with Hail Mary: Go to Attacks -> Hail Mary (From here, when the Attack is finished, use the given Session info number given in the console.)**



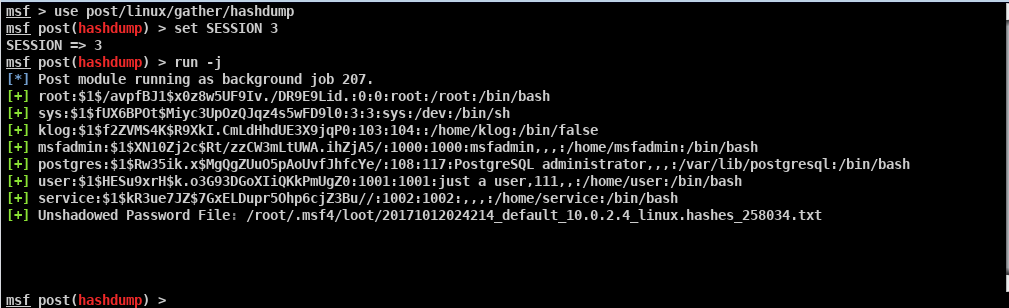
1. **Add meterpreter to the Victim IP: In the side directories go to post -> multi -> manage -> shell\_to\_meterpreter -> double click to launch. (Be sure to change the session info to the number given from the Hail Mary Attack.)**



1. **Right click the Victim IP and navigate to the meterpreter number -> interact -> meterpreter shell.**

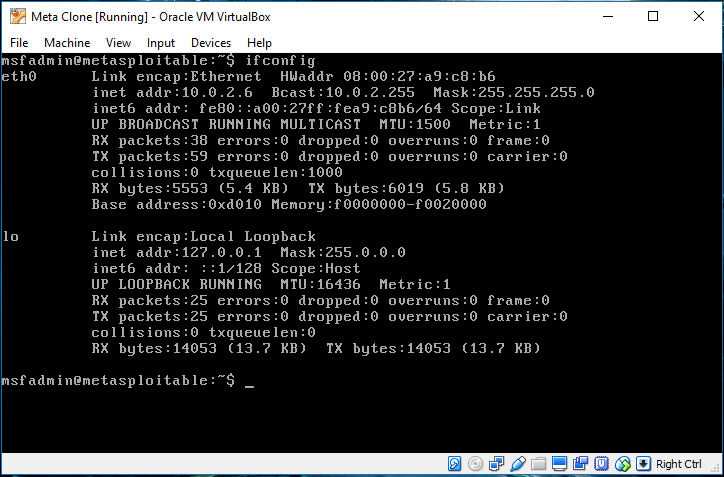


1. **Run ‘post/linux/gather/hashdump’ in the meterpreter shell.**

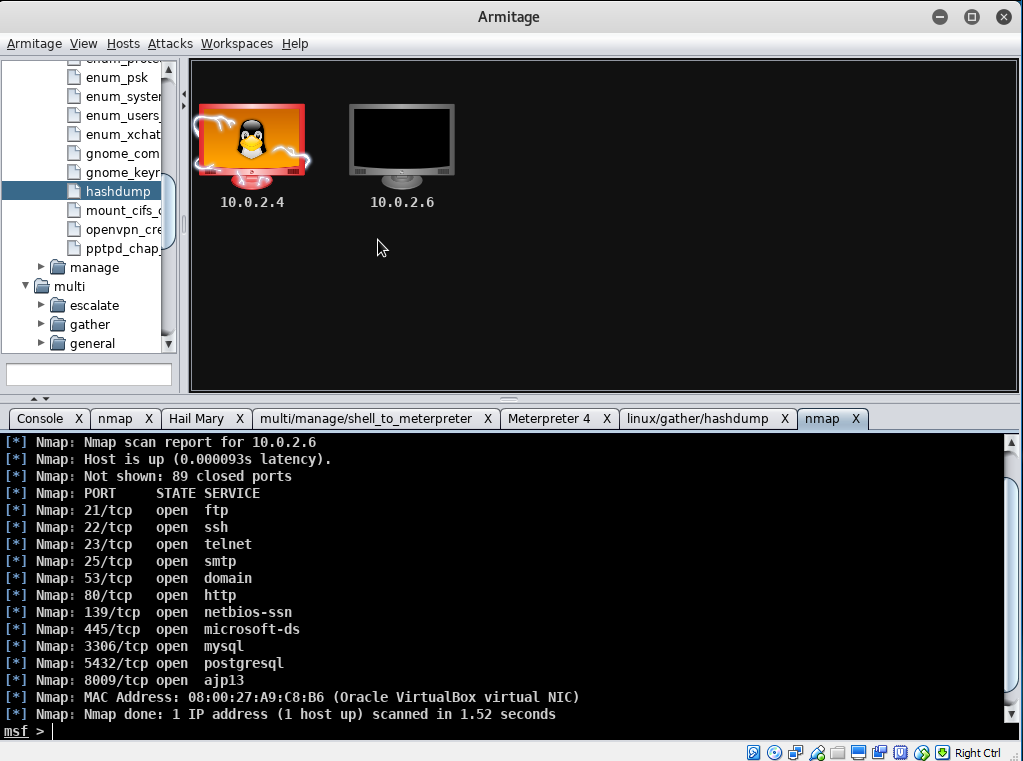


**This step is done for Hail Mary.**

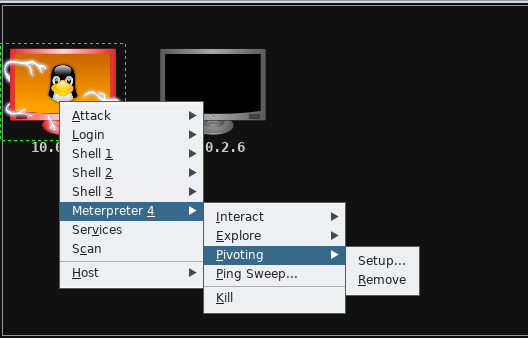
1. **To continue onto pivoting, create a clone of Metasploitable. Go to the original metasploitable -> right click -> clone**



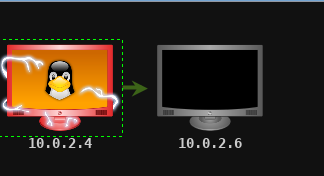
1. **Scan for the metasploitable clone. (The same way we scanned the original metasploitable.)**



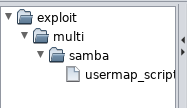
1. **To pivot: Right click the Victim IP(10.0.2.4) -> meterpreter # -> pivoting -> setup**



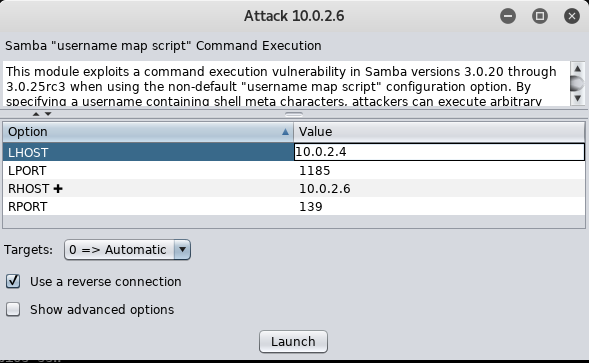
**This allows a pivot connection route to be created from the Victim IP which will be used in the attack towards the 2nd Victim IP.**



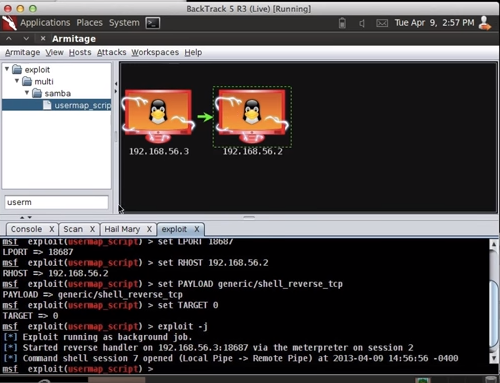
1. **Search for usermap\_script for the next attack in the directories: exploit -> multi -> samba -> usermap\_scripts**



1. **Change the LHOST to the attacking Victim IP (10.0.2.4)**



**Result: After roughly 2 hours of waiting for the usermap\_script to run. The attack did not complete itself. This goes to show that not all attacks are 100%.  
  
Side Note\*: The pivot part of this lab was not shown in class. I researched how to do pivoting via YouTube. The actual result that should have come out while setting up the usermap\_script, should have looked like this.  
The attacking Victim IP will infect the 2nd Victim IP. The pivot route will turn to a bright green, and a command shell for the session should have opened.**



**Research purposes: The YouTube tutorial video to show how pivot works is here:** [**https://www.youtube.com/watch?v=DYsI\_rIhtA8&feature=youtu.be&list=LLNU8wwyogMiTyuanQdic-qw&t=192**](https://www.youtube.com/watch?v=DYsI_rIhtA8&feature=youtu.be&list=LLNU8wwyogMiTyuanQdic-qw&t=192)