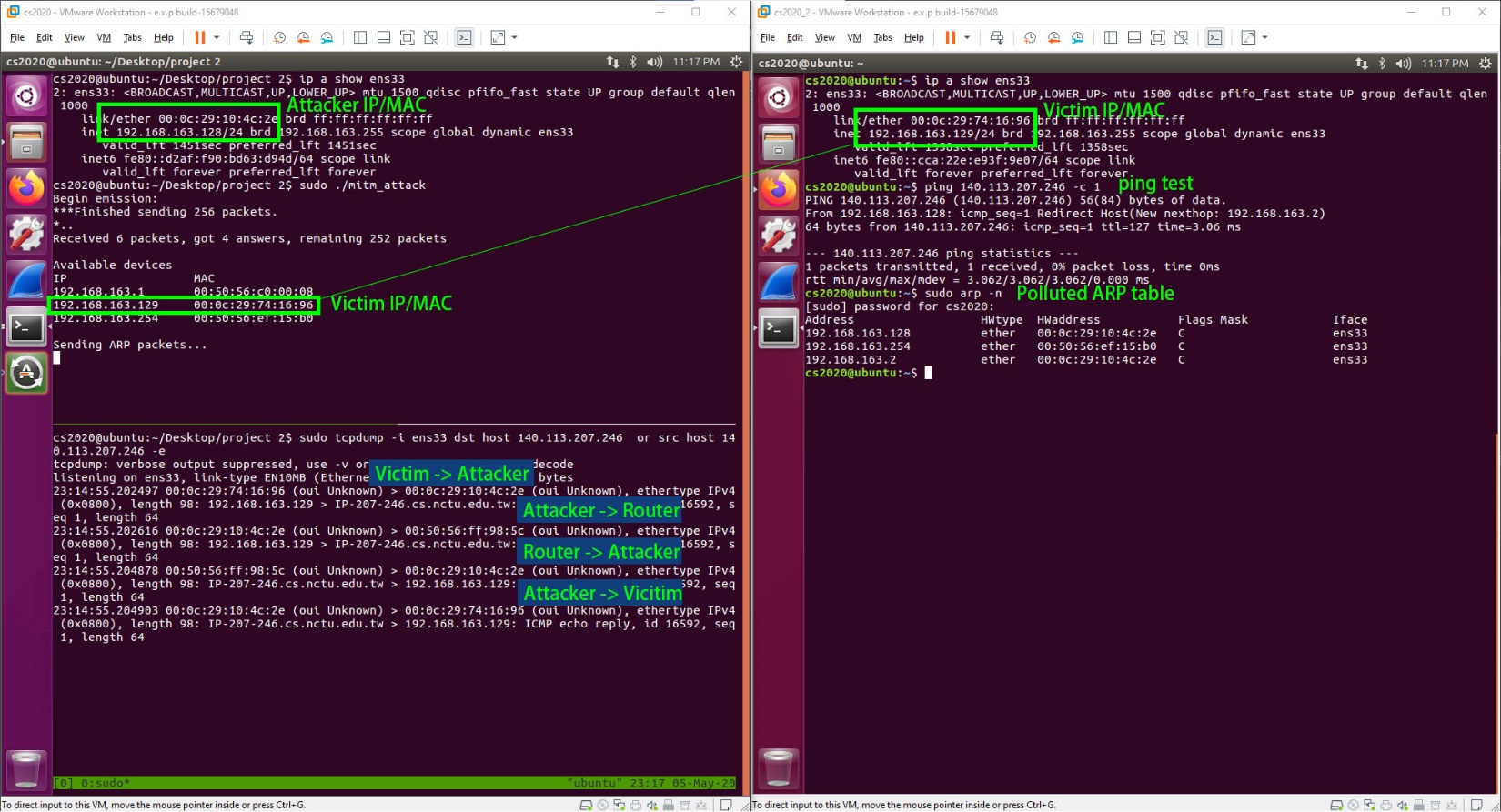
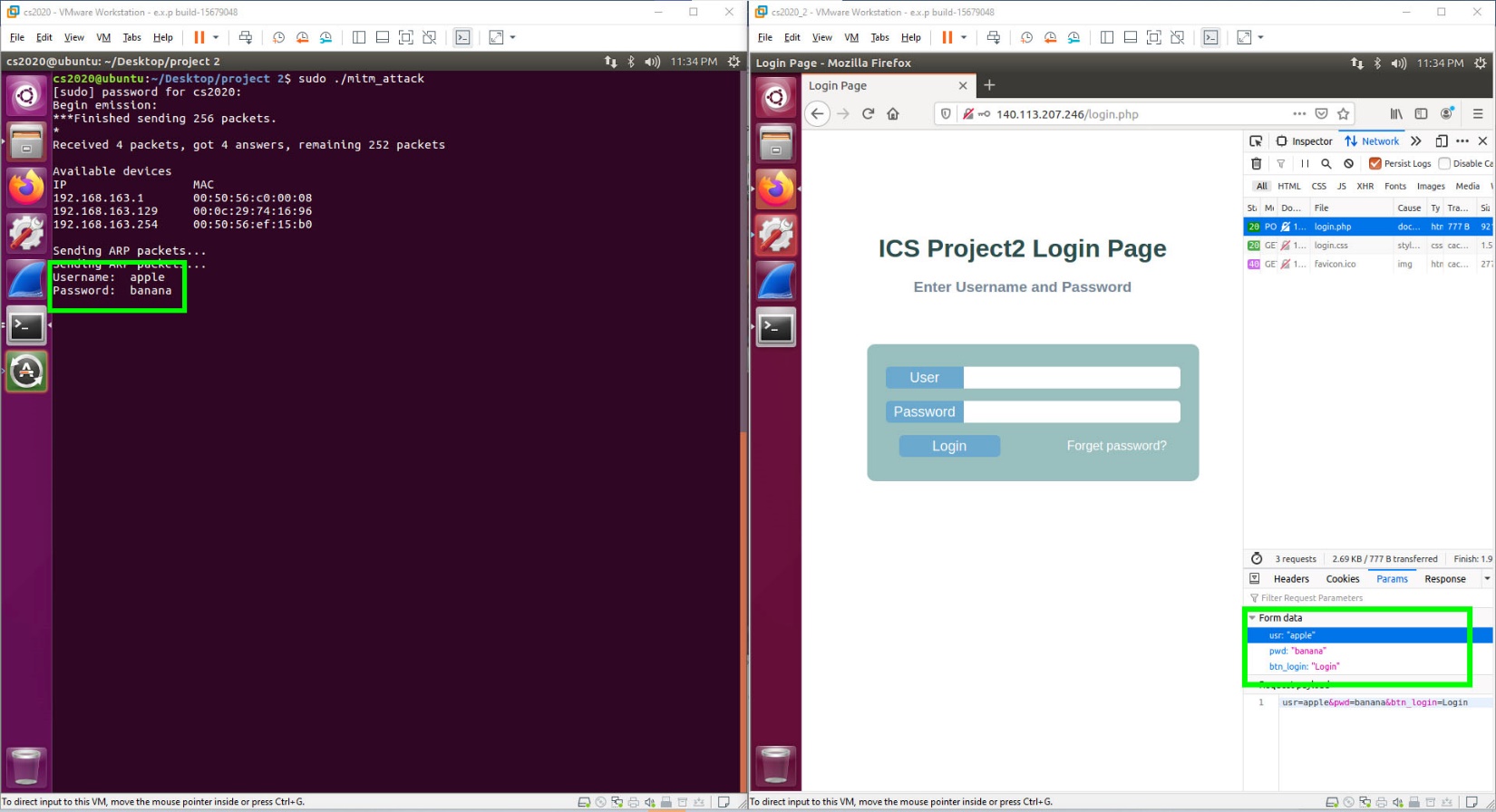
All testing is done under test scenario 2

Item 1 (10%): please give evidence that you have finished the MitM attack

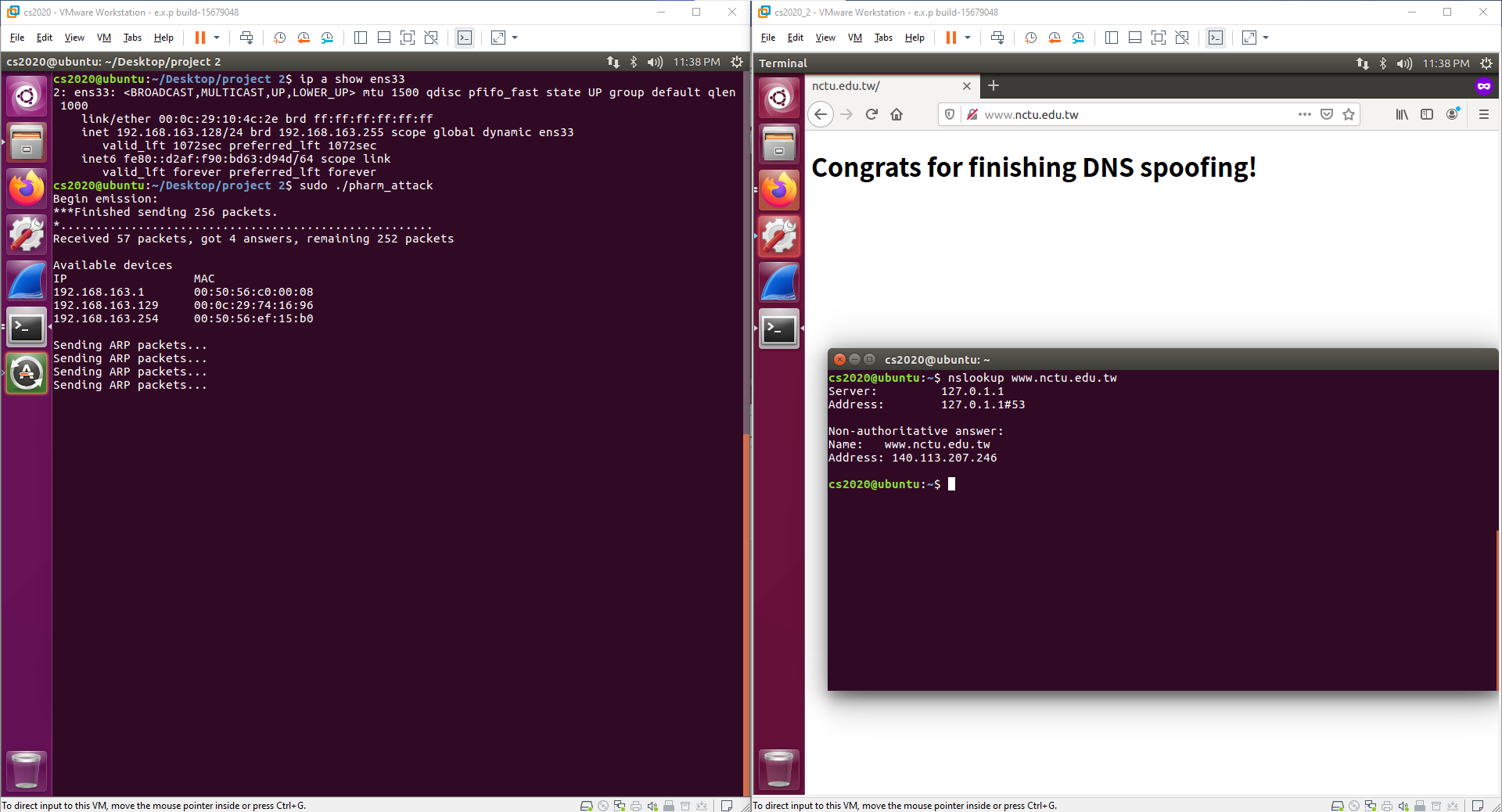


As shown in the picture, I am able to print out local clients and pollute their ARP table, therefore, the ping request is routed to the attacker instead of directly to the router.



Also, the program can print out login data sent to 140.113.207.246.

Item 2 (10%): please give evidence that you have finished the pharming attack



As shown above, the victim is redirected to a fake website when it connects [www.nctu.edu.tw](http://www.nctu.edu.tw).

Item 3 (10%): please propose a solution that can defend against the ARP spoofing attack

Whenever a client receives an ARP response, it can verify it by sending another request. For example, if a client receives an ARP packet that claims 192.168.0.1 is AA-BB-CC-DD-EE-FF, it can send another packet asking who is 192.168.0.1 and if the client receives conflicting responses, it will know that its network might be under attack. We can also encrypt all connections so the middleman cannot modify or read anything. For instance, using DNS over TLS will render our second attack useless.