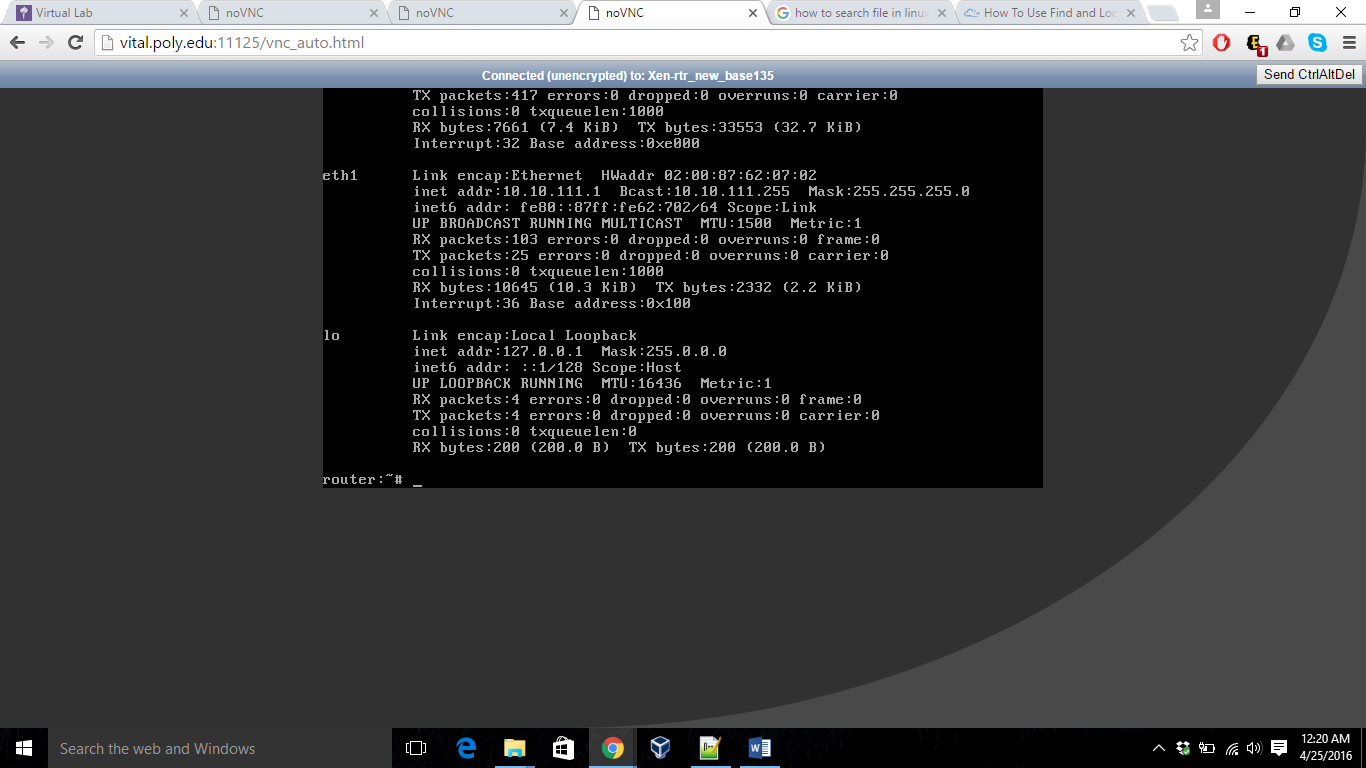
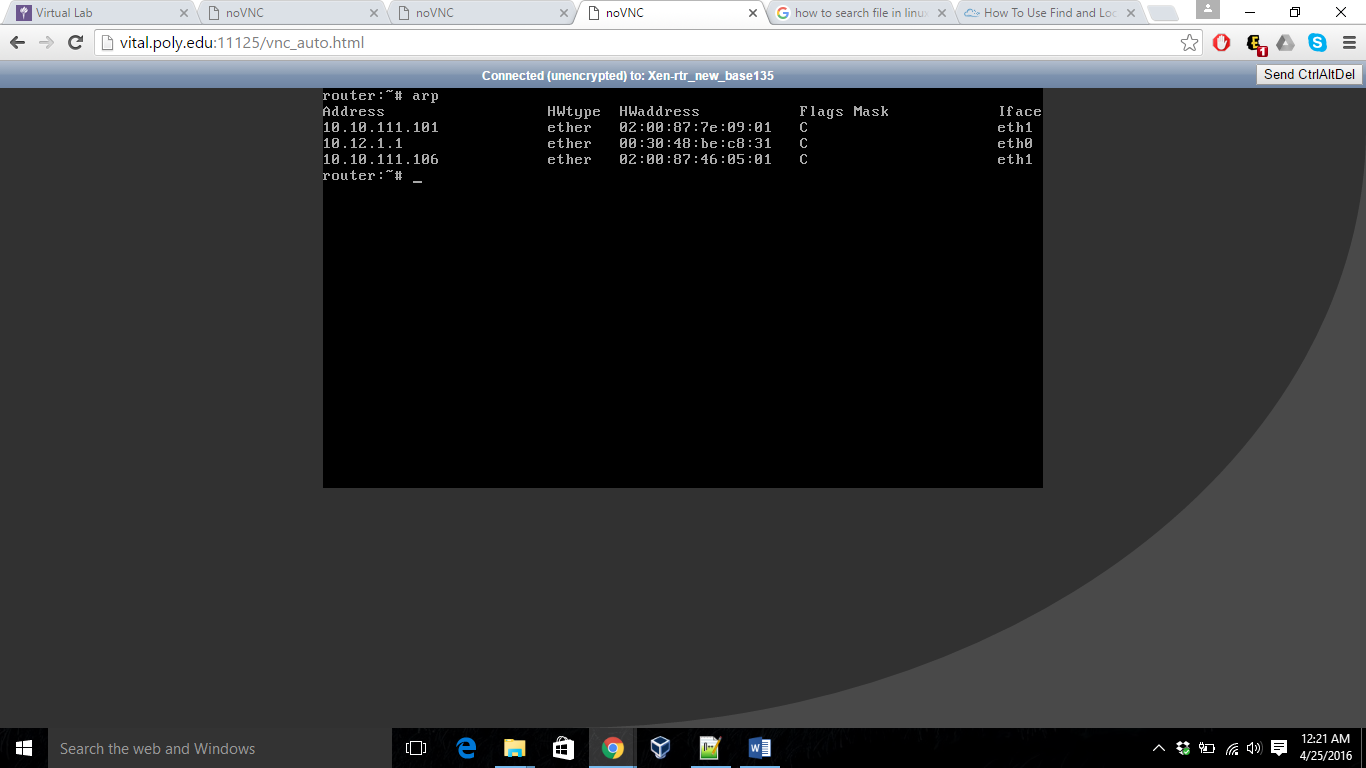
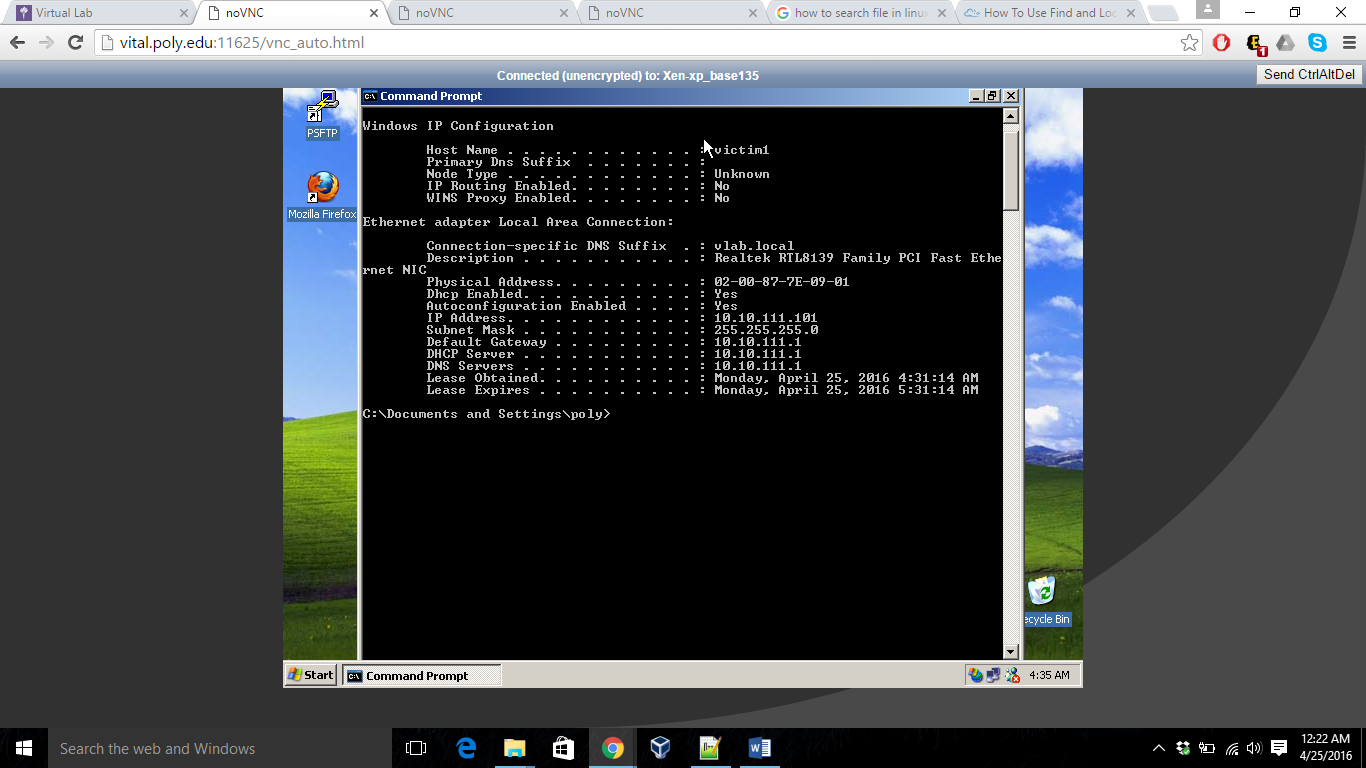
RTR IP and MAC addresses



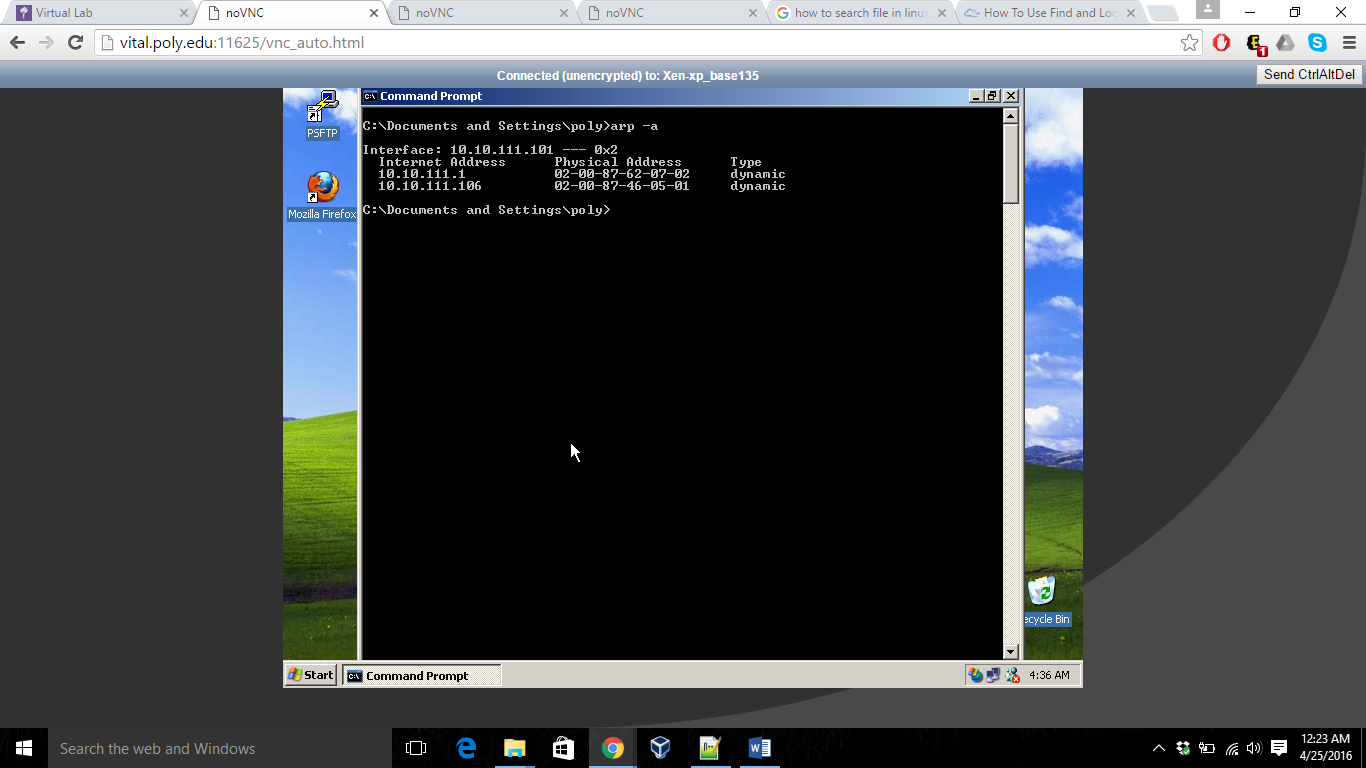
RTR ARP table



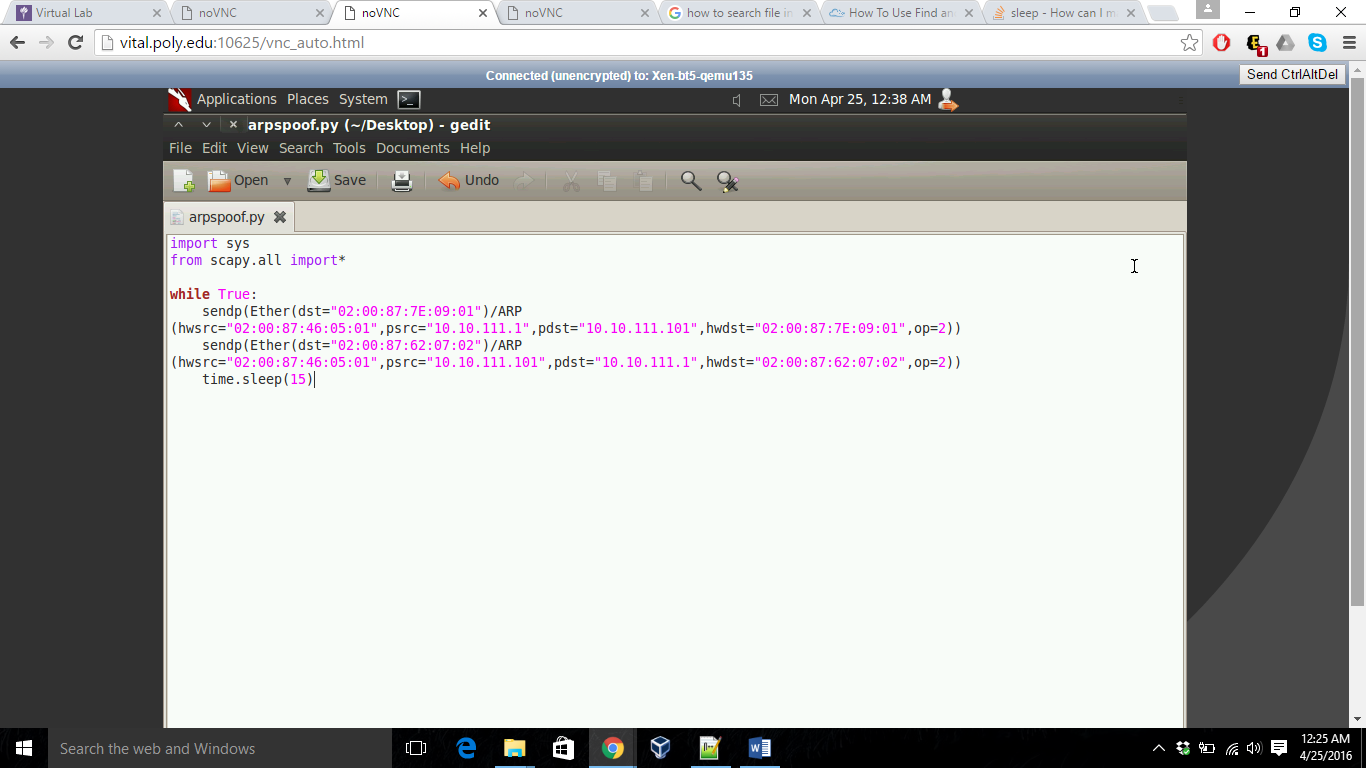
XP IP and MAC addresses



XP ARP table

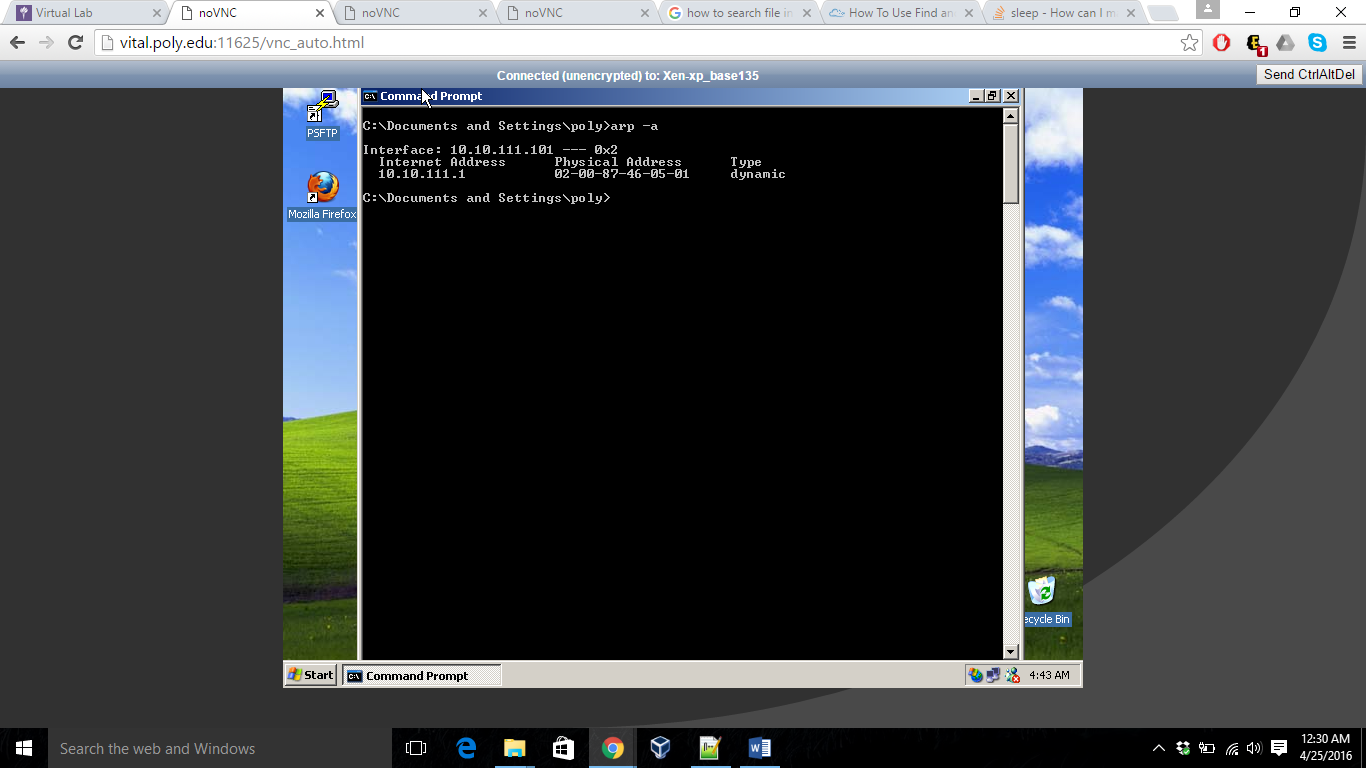


1. Write a SCAPY program on BT5 that sends gratuitous ARPs to XP and rtr so that BT5 is in the middle of the communication between rtr and XP.

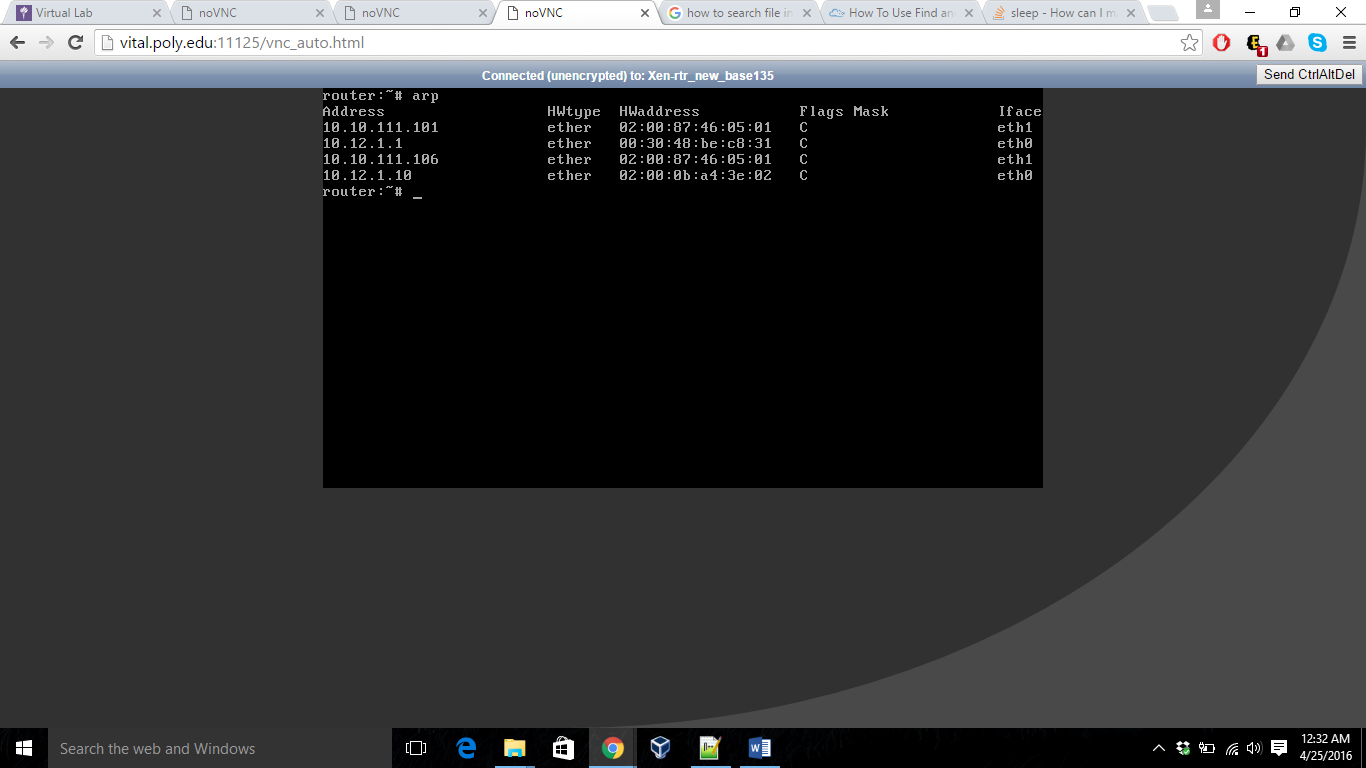


1. Show the results of successful ARP spoofing by taking screenshots showing the output of the arp command.

After running the script above from BT5, the ARP entries in XP machines looks like:

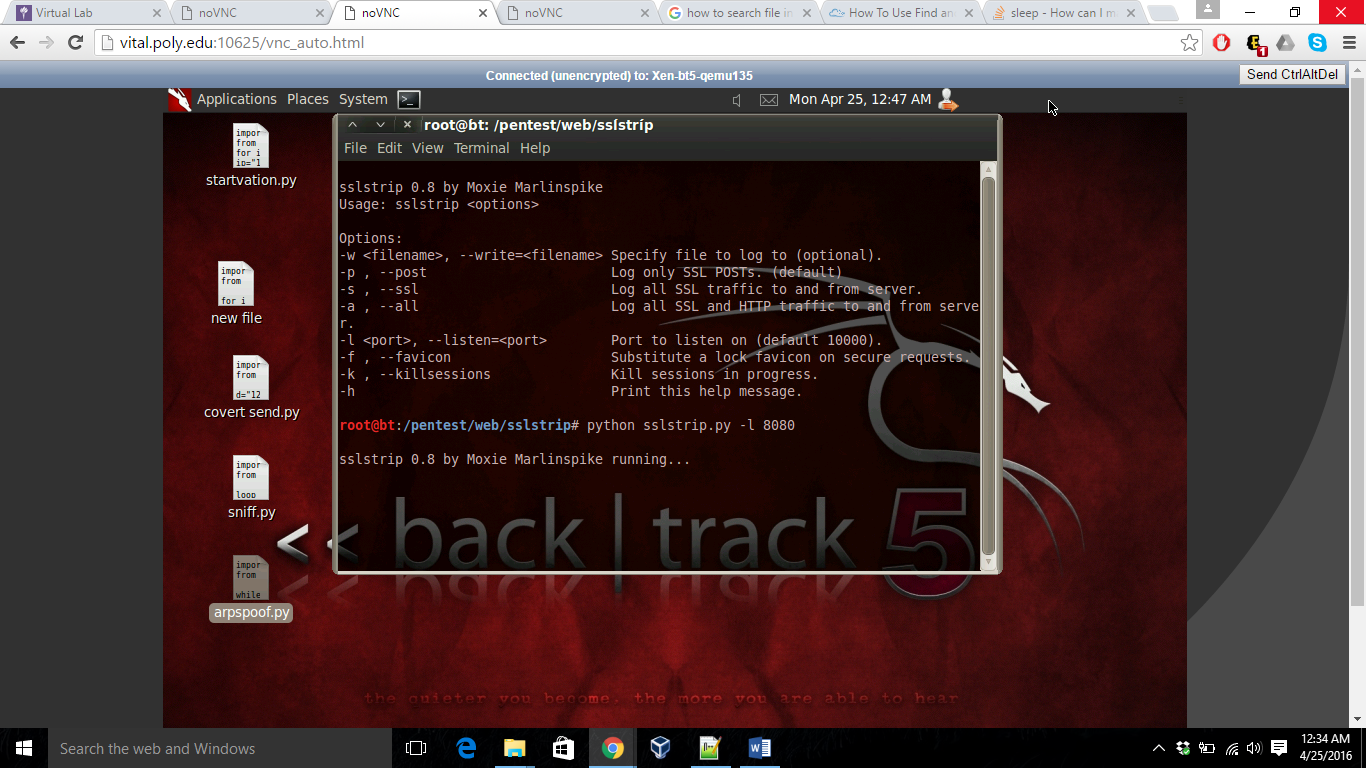


RTR machine ARP looks like:



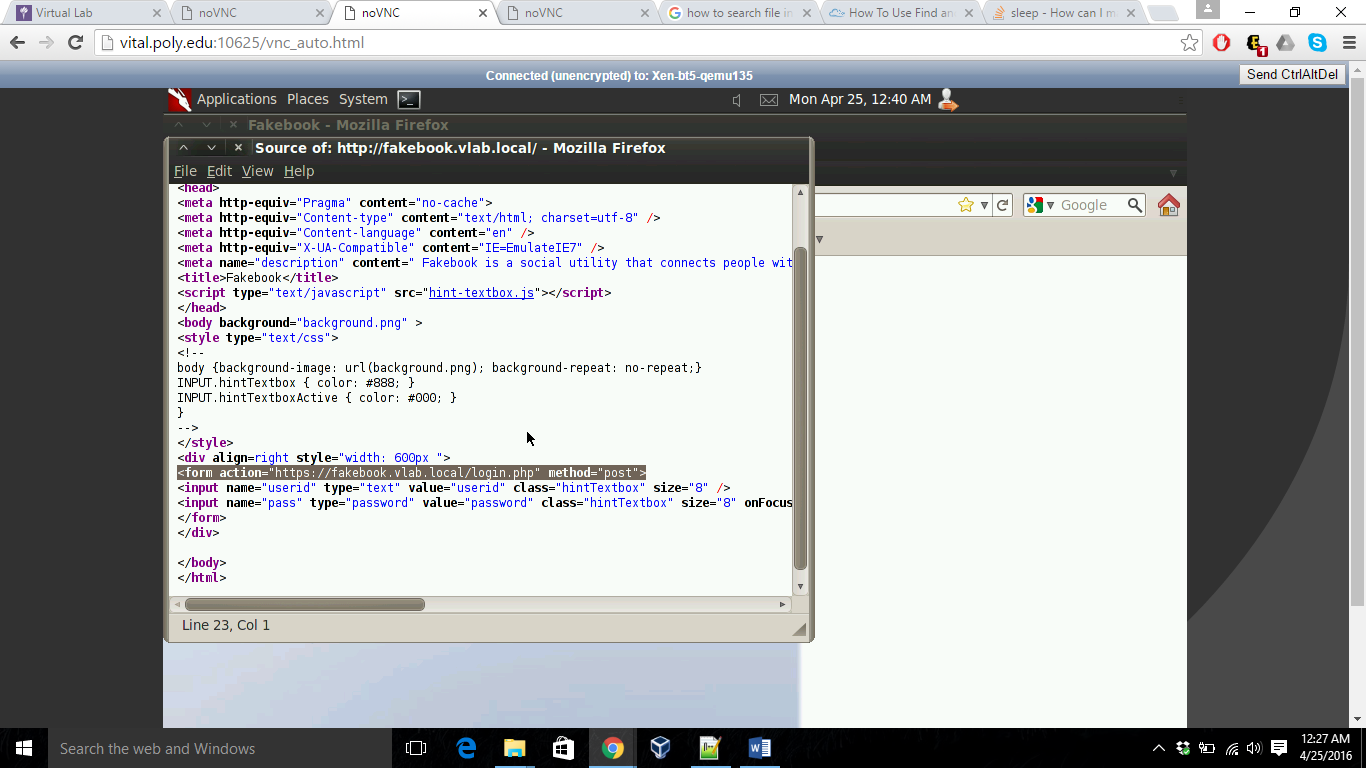
This causes ARP poisoning.

1. Perform sslstrip attack on the client accessing Fakebook.

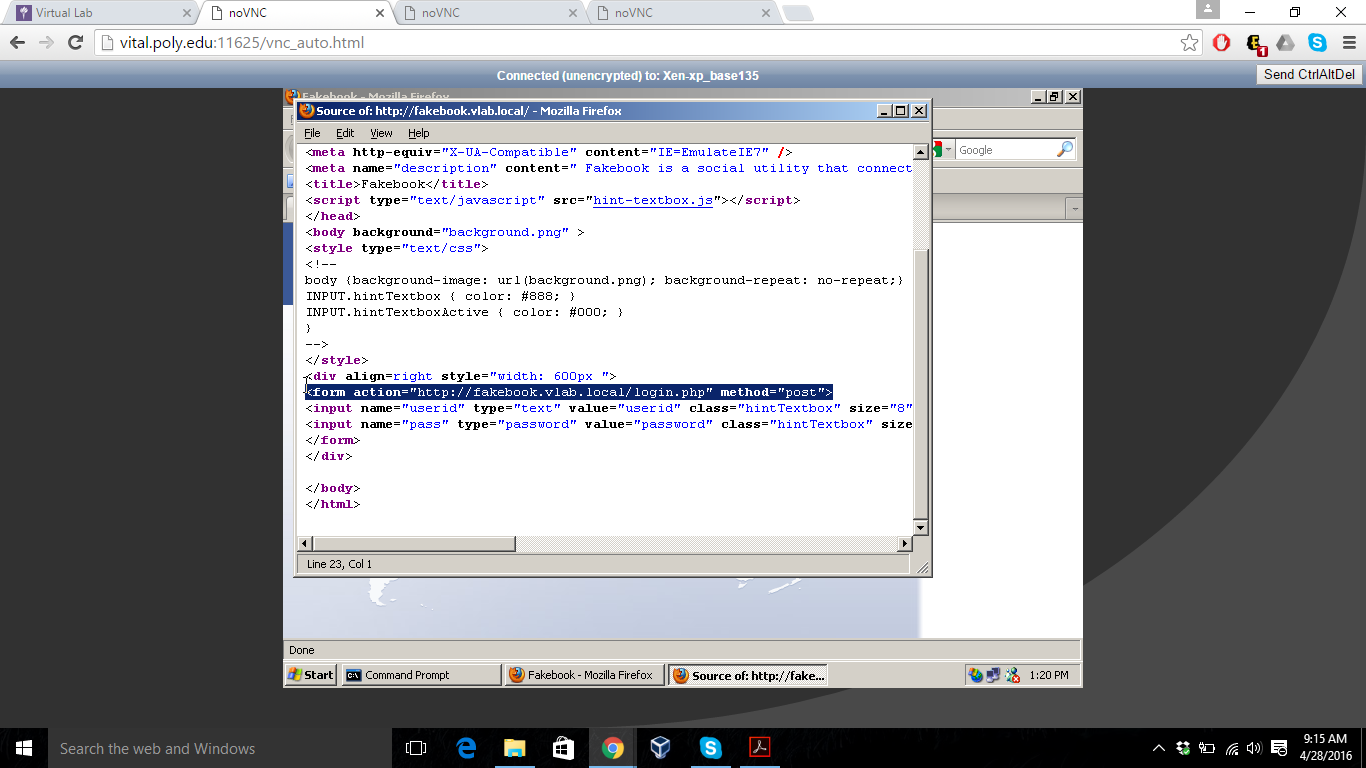


1. Record the new FORM post method and explain what is different.

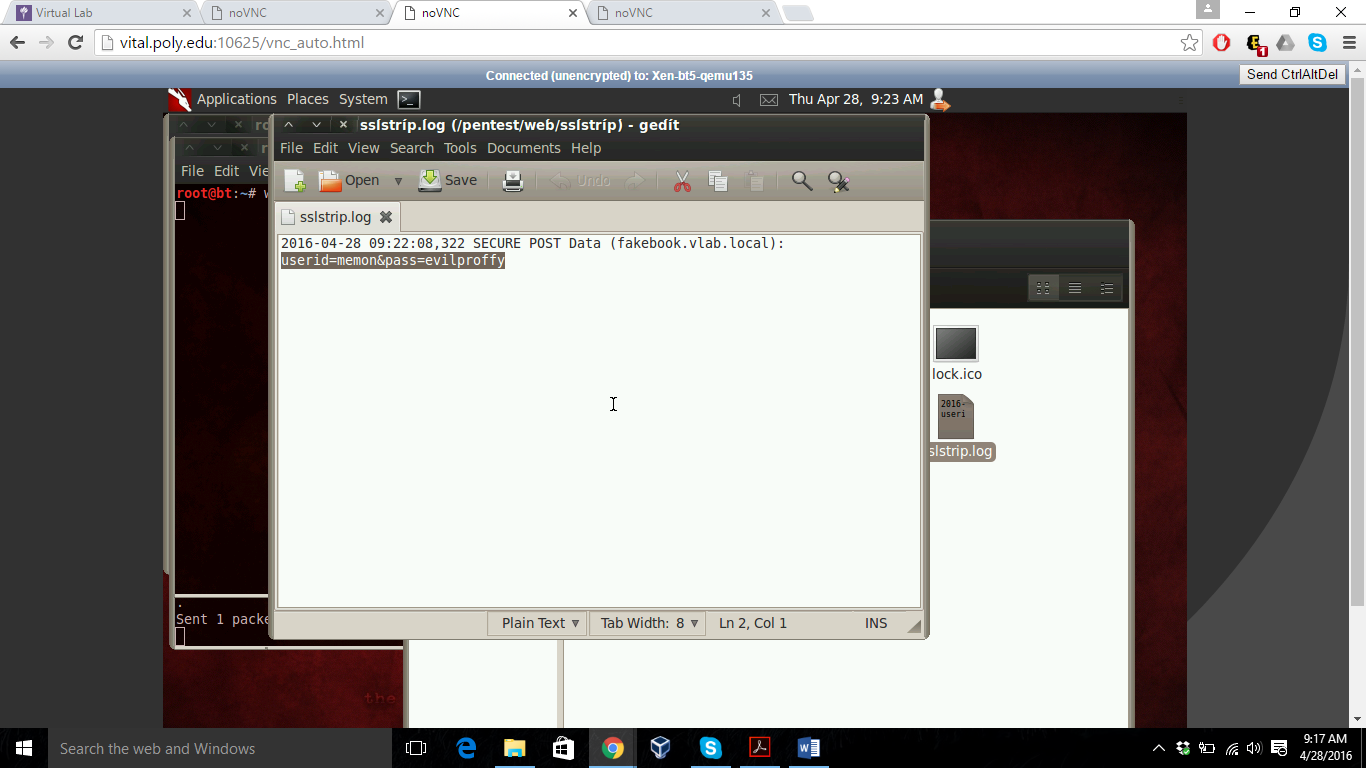
Before running SSL strip the page source looks like:



After running SSLstrip, it looks as:



1. Open this log file in your favorite text editor and find and record the captured login and passwords.



1. Fully explain in a paragraph or two how sslstrip works.

First, arpspoof convinces a host that our MAC address is the router’s MAC address, and the target begins to send us all its network traffic. The kernel forwards everything along except for traffic destined to port 80, which it redirects to 8080.

Any request through XP machine to RTR is sent via BT5 which changes the connection between XP and BT5 to http instead of https and from BT5 to RTR as a normal connection i.e., https.

The SSLstrip is running which is listening at port 8080 and logs down in SSLstrip.log .