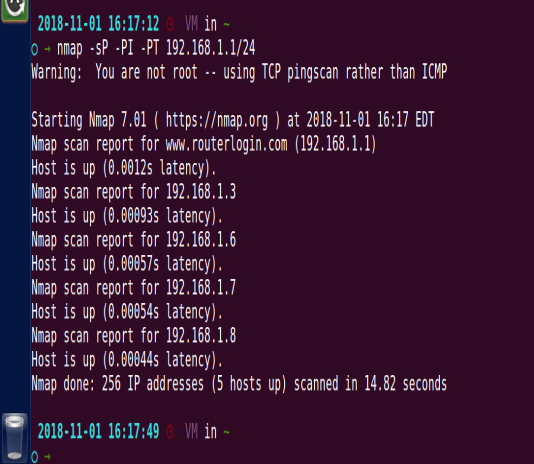
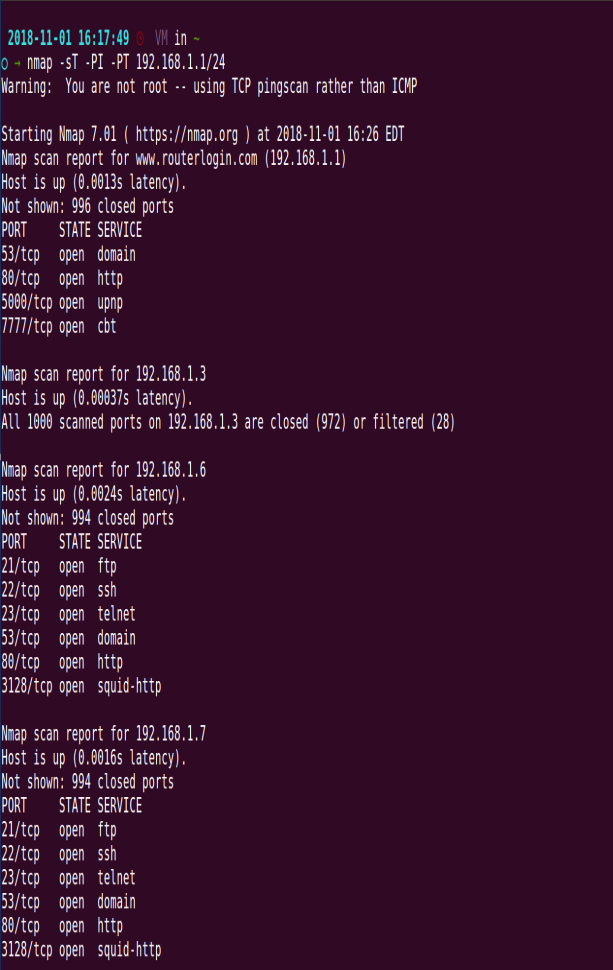
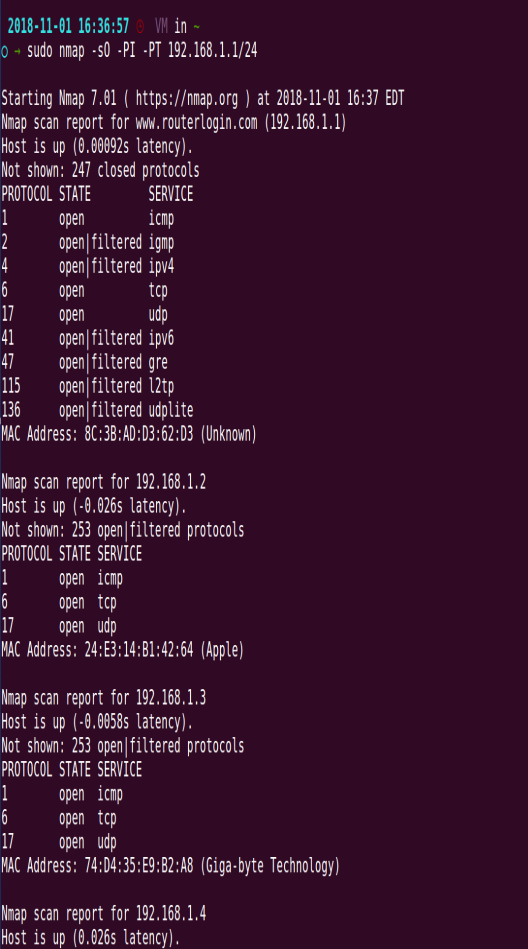
Lab 4

Task 1: 

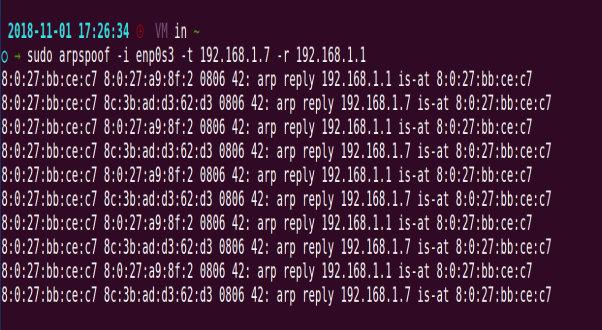




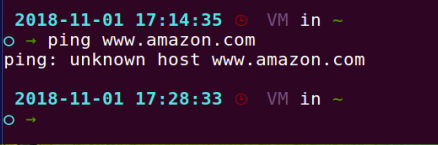
I was only able to run 3 different scans. For some reason, some scans (such as IP Protocol Scan and UDP scan) hanged and never finished. The 3 tests I successfully ran gave me the hosts that were on my network along with information specific to those scans.

Task 2:

Arp Spoofing



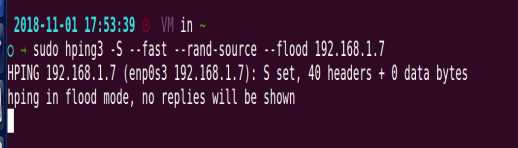
Effect



Through ARP Cache Poisoning for a specific computer on the network, we were able to knock out its internet connectivity. The target was not able to connect to a DNS server so it could not resolve the name ‘www.amazon.com.’

Task 3:

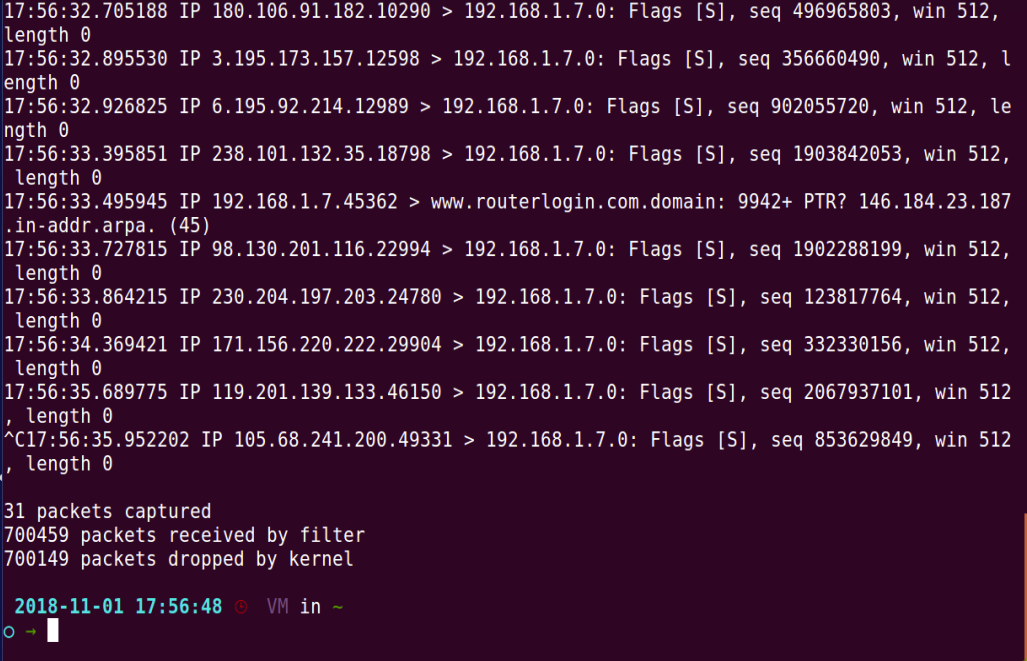
Using hping3 to flood the target



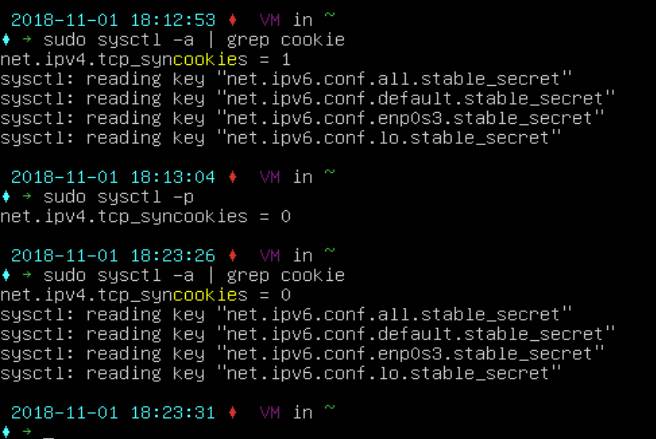
Target computer is sending random packets to random addresses



Target computer TCP dump



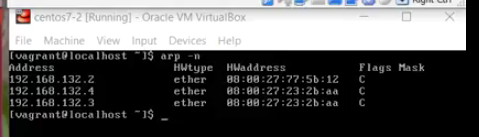
With SYN cookies enabled and disabled



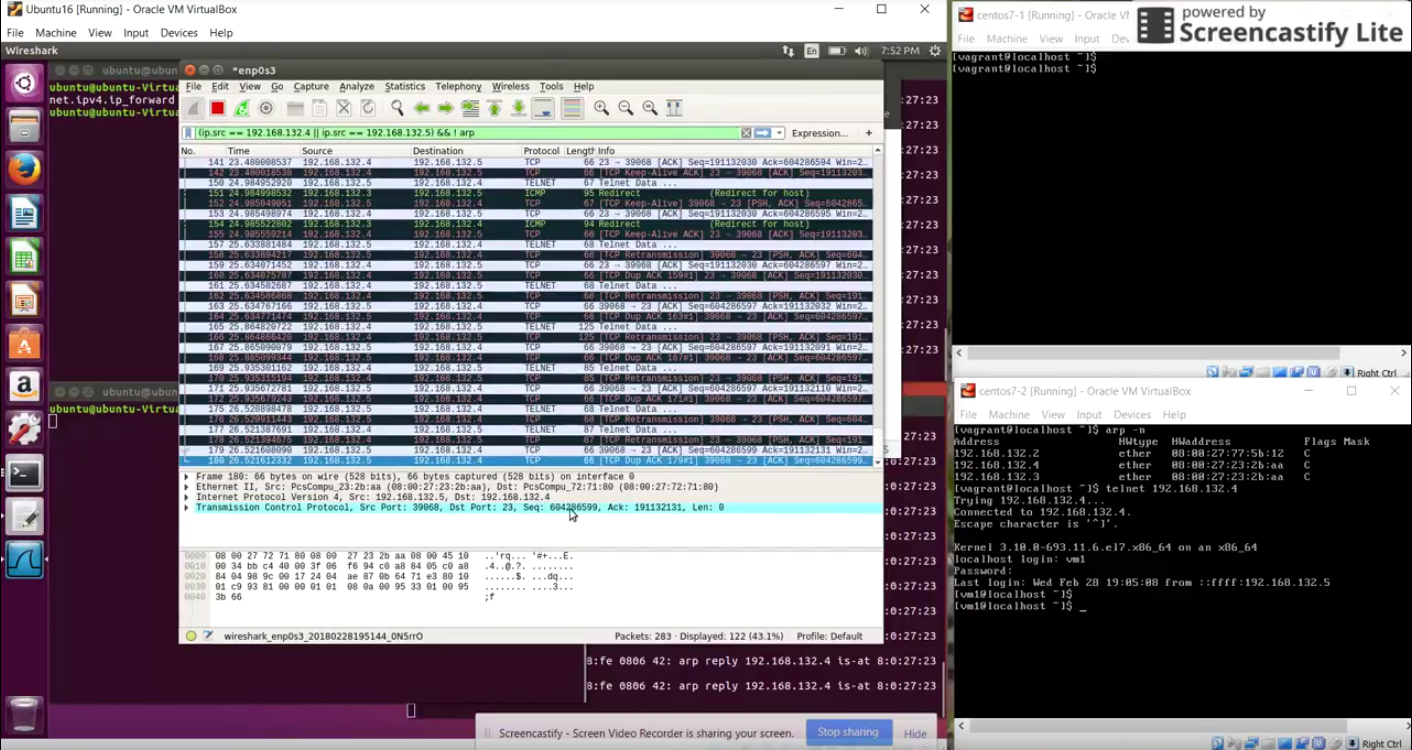
For some reason, disable syncookies had no effect on the attack. This may be due to security vulnerabilities within linux being fixed.

Task 4:

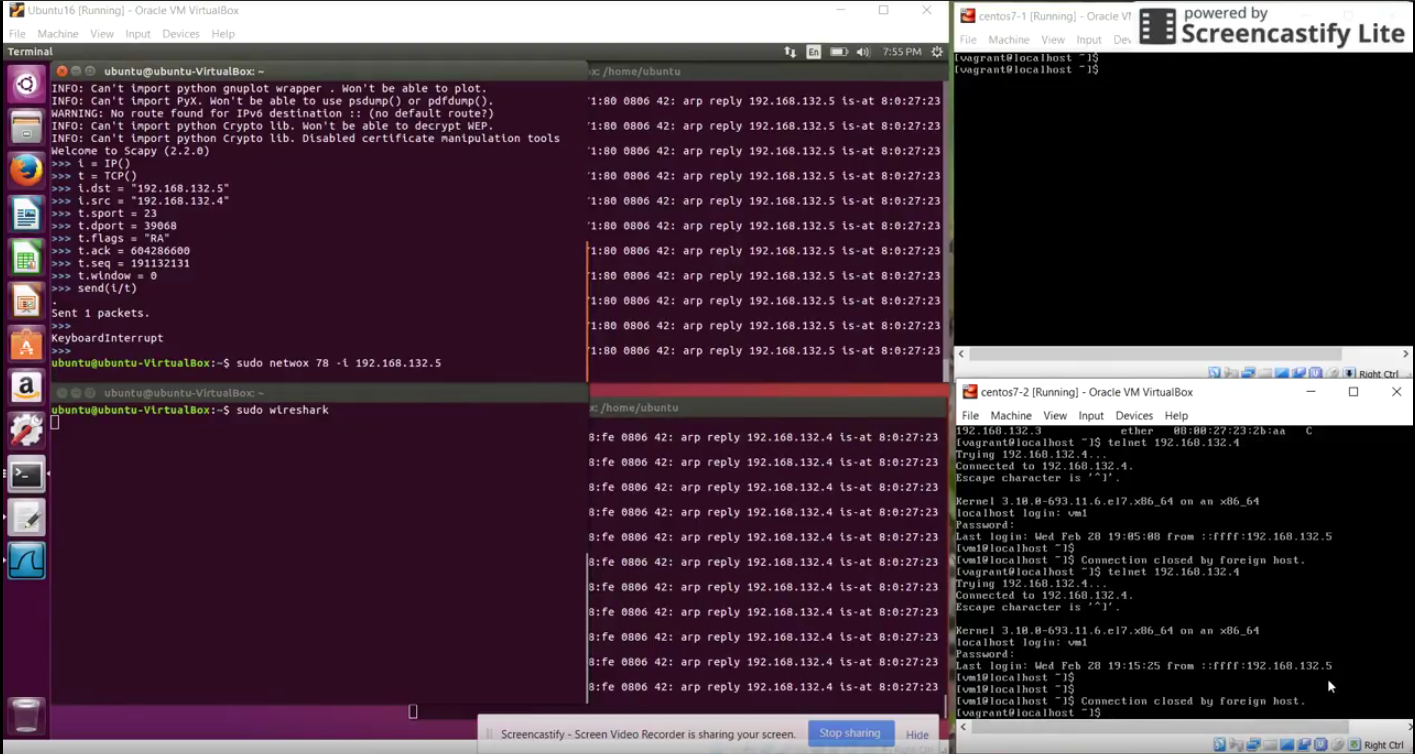
Performing the ARP spoofing between the 2 computers



Showing the network traffic after the spoof

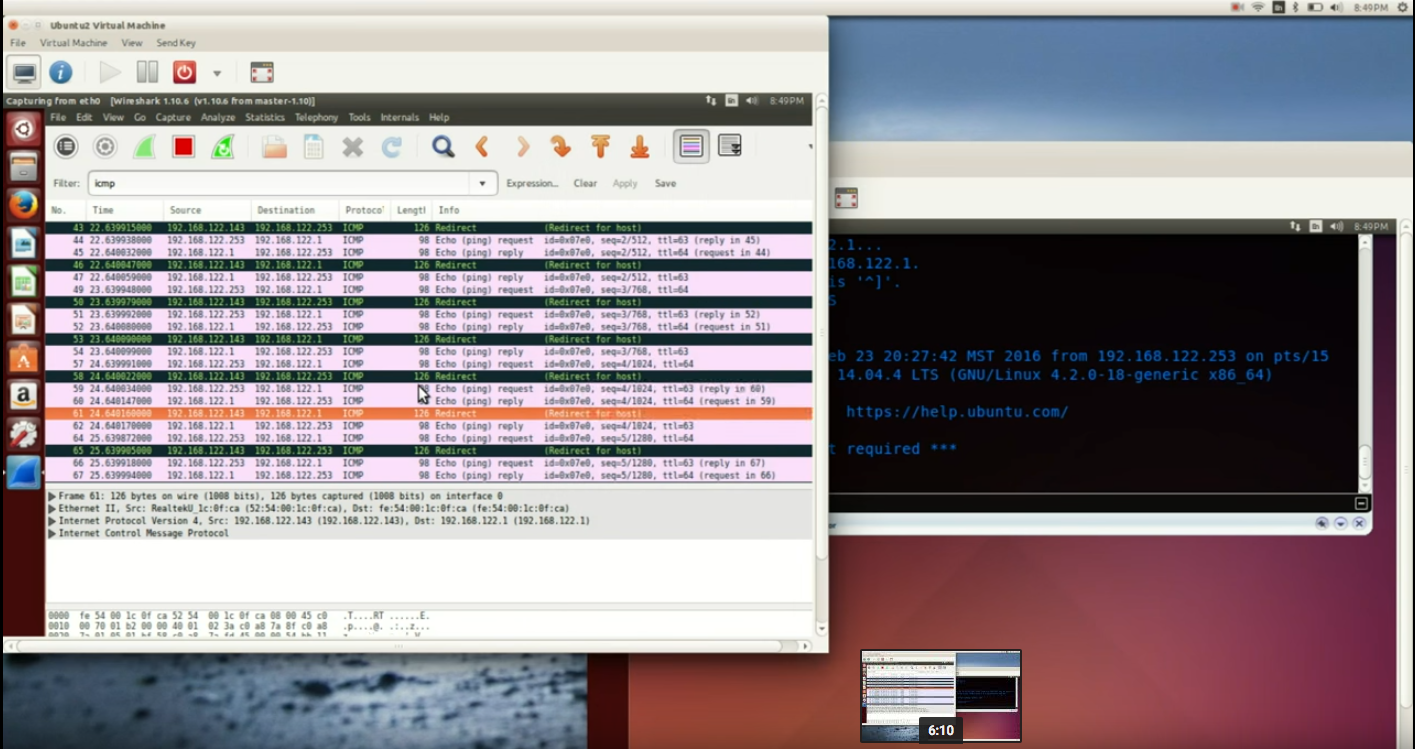


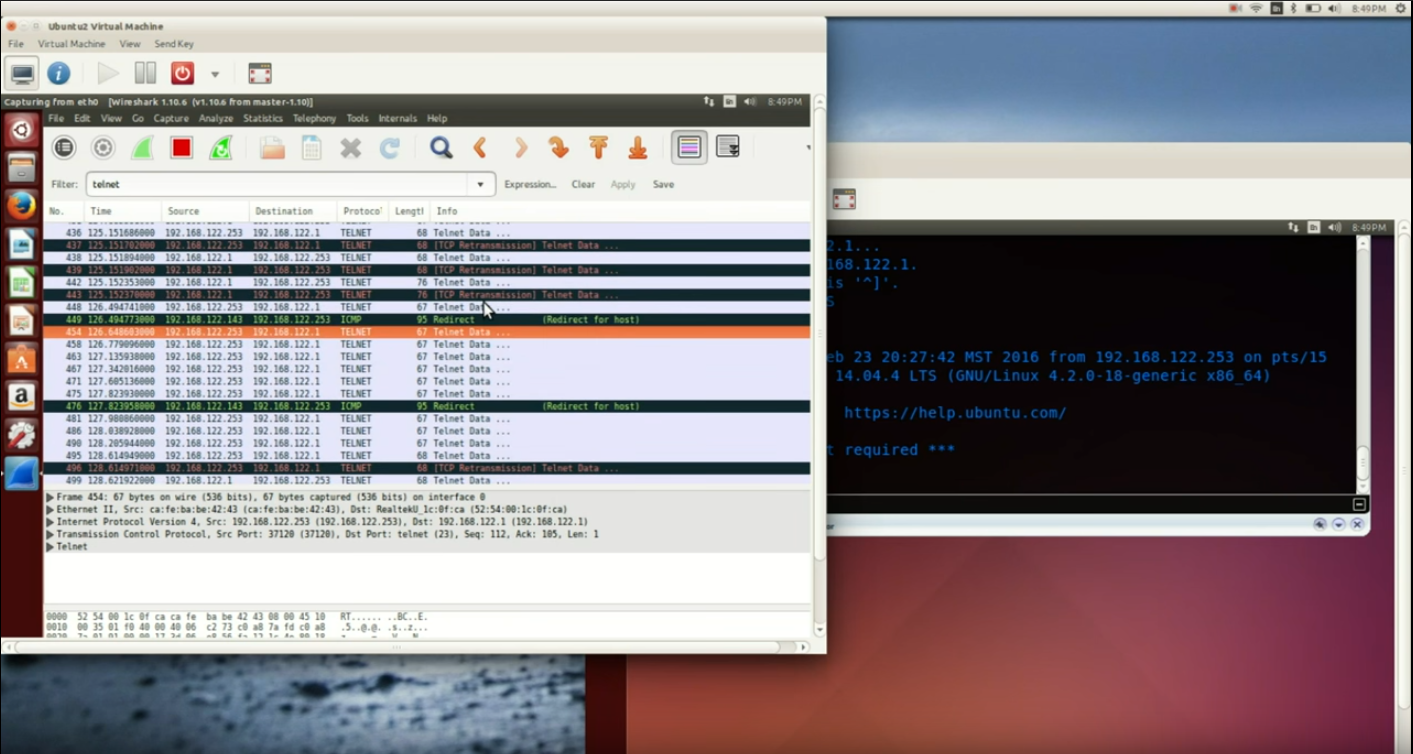
Performing the attack and shutting down the target computer network connection

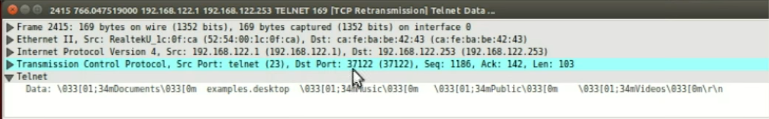


Target computer says that foreign host shut it down.

Task 5:







Using Shijack after ARP spoofing

