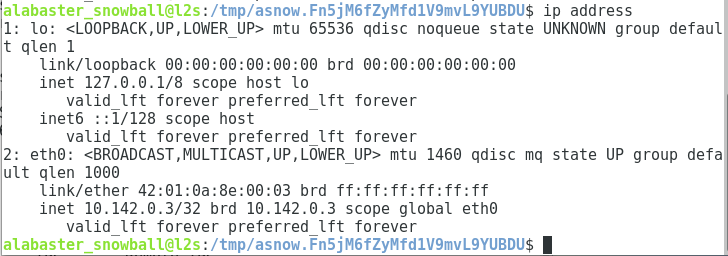
# Santa’s SMB Server--Exploiting Letters to Santa Part 4, Pillage

## Question from Part 3

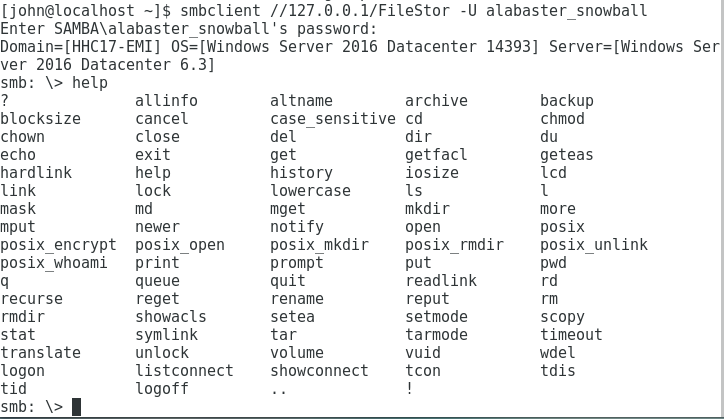
The internal address of the l2s server is 10.142.0.3, and the address of the SMB server is 10.142.0.7. When Nmap probes an address on the local network it uses an ARP request. Why didn’t the Nmap scan find 10.142.0.7?



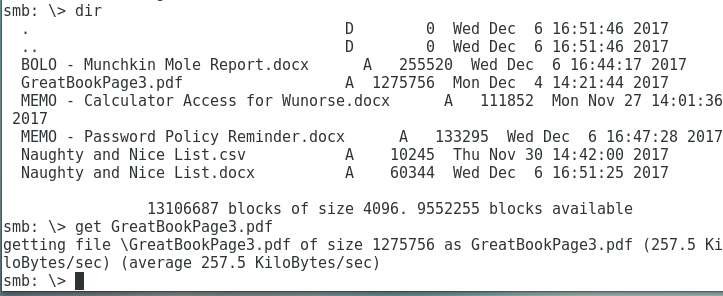
The IP address l2s is using for eth0 is 10.142.0.3/32. The “/32” is CIDR notation for the subnet mask which corresponds to a mask of 255.255.255.255. If the network included all hosts 10.142.0.1-254, the mask would be 255.255.255.0. The mask they are using says that 10.142.0.3 is the only host on the network. Therefore, Nmap thinks all other hosts are on a different network and skips the ARP request.

## Connect to FileStor

Using the syntax found [here](https://help.ubuntu.com/community/Samba/SambaClientGuide) (Manual Configuration) or in man smbclient, we connect to the share. We still need the SSH tunnel, and smbclient connects to localhost. Smbclient is designed to act like an FTP client, so we can get instructions with help.  
smbclient //127.0.0.1/FileStor -U alabaster\_snowball



We get a directory using dir, and download files using get.



Almost all the files are useful for later parts of the challenge. The BOLO and Naughty and Nice List are helpful for question 5 in the [challenge](https://www.holidayhackchallenge.com/2017/), which asks about Santa’s Naughty and Nice database and insider threat moles. The Calculator Access Memo is useful for the phishing attack in question 7. The Password Policy Memo is fun because Alabaster tells his users not to reuse passwords.

## Question

There is one big thing that Alabaster could have done to prevent this attack, and several lesser things he could have done. Name two ways Alabaster could have blocked this attack.