# Santa’s SMB Server--Exploiting Letters to Santa Part 5, Lessons Learned

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.

## Password Reuse--the Big One

If Alabaster followed his own procedures and did not reuse his password, this part of the attack would have been stopped in its tracks.

## Protect SSH

This is a repeat from Letters to Santa, but it bears repeating. This first question to ask is whether the l2s server needs to be accessible to SSH from the Internet at all. If there is not a good business reason for using it, it should be blocked. If it is necessary, it should be protected with 2FA or digital certificates at a minimum, and closely monitored.

## DMZ

Typically, servers exposed to the Internet are sequestered in a DMZ. Not only their contact with the Internet is monitored, but also their contact with the internal network is controlled. Is there a need for the l2s server to connect to any internal host, on any port? Probably not. The known, documented cases where the l2s server should contact internal hosts should be allowed. All others should be blocked.

## Monitor

The Nmap scan we did is very noisy and should appear in IDS or network monitor logs. A server that scans the entire internal network should be a cause for alarm! Also, why is a Linux web server connecting to an SMB share on a Windows server? There are times when this is legitimate, but many more when it is not. Monitoring the network, servers, and workstations is a critical part of IT Security.

## Credentials are Important

Once attackers establish a beachhead in an environment, their first goal is to steal as many user names and passwords (credentials) as possible. From then on, they try to compromise other hosts (also known as move laterally) using the credentials they already have. A connection to another host with valid credentials will not trigger any alarms in systems that are looking for exploits or attacks. It may look like normal activity. The best the defender can do is look for unusual activity: why is a server connecting to a computer that it has no business connecting to? Why are workstations connecting to each other instead of to network shares or servers? Why is someone’s computer connecting to others when the user isn’t there?

## Two Factor Authentication (2FA) Everywhere

It is much harder to bypass 2FA than to steal a user name and password. It is completely reasonable to require 2FA inside the network as well as outside.