# Santa’s SMB Server--Exploiting Letters to Santa Part 1, Ground Rules and Getting Started



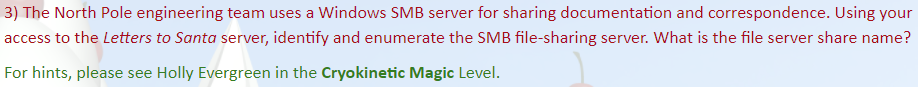
Penetration Testing is fun. After all, people pay you to see if you can break into their networks! However, your ability to find holes in the client’s network means nothing if you cannot demonstrate to the client why they need to improve security and help them improve security. As you do this challenge, take notes at each stage on what the vulnerabilities were and how Alabaster and Santa could fix them. The most important question will come at the end: 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.

This technical challenge assumes that you have already completed the Letters to Santa challenge. In fact, you cannot do this challenge until you have stolen Alabaster’s credentials in the Letters to Santa Challenge.

This challenge will give you practice in network scanning and in Server Message Block (SMB) protocol, which is used by Microsoft Windows for file and printer sharing. It also drives home the point that once attackers gain a valid set of credentials, their attacks become more damaging and harder to detect.

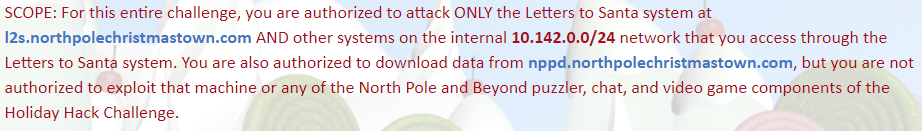
## Goal

According to the [SANS Holiday Hack Challenge web site](https://www.holidayhackchallenge.com/2017/), we need to find the file server share name for the North Pole Windows SMB server. If we can access the file share, we will also want to plunder any loot we can find there.



## Scope

As before, you are only authorized to attack the Letters to Santa system at l2s.northpolechristmastown.com. In addition, you can now use the Letters to Santa server to attack hosts on the 10.142.0.0/24 network. Exciting!



You don’t often have authorization to attack targets on the Internet, so use this challenge wisely and be careful that your attacks do not reach other addresses by mistake.

## Hints

Holly Evergreen is your helper for this challenge. Hints from Holly are available in your Stocking once you complete the Cryokinetic Magic Linux Challenge. Her first hint mentions Nmap. That is sensible, since all we know about the North Pole SMB server is that it is on their internal network.

## Questions

Since this challenge seeks data from an SMB server, it would be a good idea to learn something about SMB.

1. What is SMB, and what protocol (TCP/UDP) and port does it use? Note: ignore the older NETBIOS ports.
2. What methods (both Windows and Linux) can be used to find (enumerate) and connect to SMB file shares?
3. Before you start noisy scanning, use an SSH connection to l2.northpolechristmastown.com to see what you can learn about other hosts on the network from the l2s server. What is the /etc/hosts file, and does it contain useful information? Will the netstat command work?
4. Nmap does not check every possible port when it is looking for hosts, which Nmap calls host discovery (also called a probe or ping.) Search for Nmap host discovery in your favorite search engine. What methods does Nmap use by default to discover hosts? What could a host do to avoid appearing on an Nmap host discovery, but still be active on the network?
5. You have terminal on l2s via SSH, but no GUI. Therefore, you will need to use the Nmap command line to scan, and not the Zenmap GUI you used before. What is an Nmap command that will scan the in-scope internal network, 10.142.0.0/24, to locate hosts? Be sure to include the /24 in your target network description! You don’t want to scan anything else.
6. It is possible to perform Nmap TCP [scans through an SSH](https://www.sans.org/reading-room/whitepapers/testing/tunneling-pivoting-web-application-penetration-testing-36117) tunnel, [but it isn’t simple](https://cybersyndicates.com/2015/12/nmap-and-proxychains-scanning-through-a-socks-piviot/). Fortunately, Alabaster has installed Nmap on the l2s server for us! SSH to the l2s server and perform an Nmap scan of the 10.142.0.0/24 network. What did you find?