

# Letters to Santa--a real world attack

## 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 then 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: **What mistakes did Alabaster make that allowed us to compromise this server, and how could he fix them? List at least three mistakes and solutions.**

This technical challenge gives you an opportunity to apply an attack against a [vulnerability](#) in [Apache Struts](#) servers that was discovered in 2017. There were two vulnerabilities, one in March and one in September. The [first vulnerability](#) was used in a [famous attack](#), most likely after a company failed to patch it quickly. Hopefully after all the publicity surrounding the Struts vulnerabilities, companies have applied the proper patches to their web servers and this challenge is just an enlightening exercise.

We will learn important things about the way our sites can be attacked, and how to use some attacker tools.

1. Simple reconnaissance of a web site
2. The Host field in the HTTP header
3. The difference between shell, reverse shell, and terminal
4. Configuring a simple Virtual Private Server (VPS), an AWS instance in this case
5. Using tcpdump to monitor network traffic
6. Using Netcat to create a listener and a reverse shell, and to transfer files
7. Creating a simple PHP web shell
8. Using Base64 encoding
9. Using grep to look for passwords
10. Using SSH and SCP

This challenge is presented in several parts to prevent spoilers. Questions and hints from later parts give away the answers to earlier parts. Please show, or submit, your answers for each part before proceeding to the next part.

Note: This lesson assumes you have completed the Linux Challenge Winconceivable: The Cliffs of Winsanity, available in the [SANS Holiday Hack Challenge 2017](#) web site. That will give you access to the hints from Sparkle Redberry. The challenges are accessed through the Play tab, and the Hints appear in the Stocking tab.



## Goal

According to the [SANS Holiday Hack Challenge web site](https://l2s.northpolechristmastown.com), we need to find a document on the Letters to Santa site, <https://l2s.northpolechristmastown.com>.

2) Investigate the Letters to Santa application at <https://l2s.northpolechristmastown.com>. What is the topic of The Great Book page available in the web root of the server? What is Alabaster Snowball's password?

For hints associated with this challenge, Sparkle Redberry in the *Winconceivable: The Cliffs of Winsanity* Level can provide some tips.

## Scope

Sorry, but this challenge is not a wholesale license to attack anything you see on the Internet; it is very limited.

SCOPE: For this entire challenge, you are authorized to attack ONLY the Letters to Santa system at [l2s.northpolechristmastown.com](https://l2s.northpolechristmastown.com) AND other systems on the internal **10.142.0.0/24** network that you access through the Letters to Santa system. You are also authorized to download data from [nppd.northpolechristmastown.com](https://nppd.northpolechristmastown.com), but you are not authorized to exploit that machine or any of the North Pole and Beyond puzzler, chat, and video game components of the Holiday Hack Challenge.

You are authorized to attack the Letters to Santa system at [l2s.northpolechristmastown.com](https://l2s.northpolechristmastown.com), the IP address that goes with that name, and nothing else. The internal 10.142.0.0/24 network features in later challenges.

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

Since you have completed the Linux terminal challenges, the hints for this challenge from Sparkle Redberry should be in your stocking. Hints one and two suggest that Sparkle and Alabaster were rushed in creating the site and may have left things in the site that should not be there (please read the hints.) Sparkle's hints three through five suggest that you should set up a PHP web shell on the target. There's a "gotcha" with the web shell that foiled me, and most of the other contestants. We will find other ways to complete the attack and will return to the web shell later. Hints six and seven are key, however, and hint seven has a very useful link.

## Questions, part 0

- 1) What are the names and CVE numbers of the two Apache Struts vulnerabilities from 2017? (The links in the first paragraph of this lesson will be helpful.)
- 2) Which vulnerability was part of the famous attack?

- 3) Which vulnerability did Alabaster say that he patched?

#### Part 1

Inspect the website <https://l2s.northpolechristmastown.com>. View Page Source, or Chrome or Firefox Developer Tools should be helpful. Based on the hints, look for any development content that might be useful to an attacker.

#### Questions, part 1

- 1) What would be the best path to pursue next? What did you find to support that?