# Elf Web Access--Encryption Gone Wrong 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 questions will come at the end: How could Alabaster fix his cookie scheme to prevent the vulnerability that we exploited? What other things can Alabaster do to protect his server?

This technical challenge assumes that you have already completed the Linux challenge “There’s Snow Place Like Home” so you can read hints from Pepper Mintstix. It also assumes you have completed the Letters to Santa technical challenge so that you know Alabaster’s user name and password on the Letters to Santa server, and the SMB challenge so you know the IP addresses of the North Pole servers.

This challenge is a dramatic demonstration of the bad things that can happen when a developer tries to “roll their own” encryption, even if they use a gold standard algorithm like AES. Alabaster’s cookie scheme for Elf Web Access is just another validation of [Schneier’s Law](https://www.schneier.com/blog/archives/2011/04/schneiers_law.html):

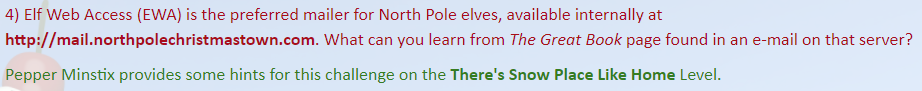
*Anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he himself can't break. It's not even hard. What is hard is creating an algorithm that no one else can break, even after years of analysis. And the only way to prove that is to subject the algorithm to years of analysis by the best cryptographers around.*

Note: This challenge delves into code for encrypting and decrypting text using AES. If code bothers you, come along for the ride anyway. The questions in one part are followed by detailed answers in the next part, which should help you. The key question to answer should be, “How did something as apparently simple as an AES function and a cookie go so badly wrong?” If you gain a feel for that, this challenge has been worthwhile.

This challenge also takes you further into the subjects of SSH tunnels, web site cookies, and manipulating what a web browser sends to the server. (What’s that, you say? The web browser and page content control what the browser sends back in cookies, and the user can’t change that? Really? Well then, stay tuned!)

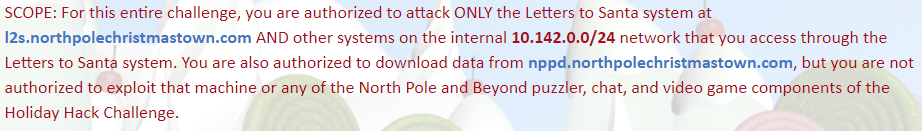
## Goal

According to the [SANS Holiday Hack Challenge web site](https://www.holidayhackchallenge.com/2017/), we need to break in to Santa’s mail server, EWA, and recover a Great Book Page. Of course, we will also 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 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

Pepper Mintstix is your helper for this challenge. Her first and last hints talk a lot about cookies, so perhaps we should look at the cookie scheme that Alabaster has concocted. Also, the first hint includes, “I just hope that he cleared up all his dev files. I know he was working on keeping the dev files from search engine indexers.” Hmm, you may want to Google the phrase, “keeping files from search engine indexers.”

## Step 1

First you will need to connect to <http://mail.northpolechristmastown.com>. Go ahead and click on the link, but you will probably find that it does not work. The mail server is on Santa’s internal network, and if you still have the results from your Nmap scan from your attack on Santa’s SMB server you already know the IP address.

The only host we have direct access to is the Letters to Santa server, <https://l2s.northpolechristmastown.com>. In the SMB challenge we used an SSH tunnel to port 445 on the internal SMB server. We can do the same thing here, except make the tunnel to the mail server IP address on the HTTP port. The document included in this package, “SSH Extras.docx”, includes instructions on browsing through SSH using both local and dynamic tunnels.

Some servers in this Holiday Hack challenge only respond when you put the IP address in the browser navigation bar, and others only respond when you put the DNS name in the navigation bar. The browser sends your entry in the navigation bar to the server in the Host field of the HTTP header. See the sidebar in “Letters to Santa Part 3.docx” for an explanation. If you connect to the mail server but get a generic “this is a web server page” instead of Elf Web Access, you need to try the other way. Also, the server seems to respond to ewa.north… and mail.north… slightly differently.

You may ask, “How can I put the DNS name in the browser bar? When I do that the browser tries to use the Internet instead of the SSH tunnel!” The answer is, “Put an entry in your hosts file.” Your DNS client checks the hosts file before it goes to the DNS server to look up names, so an entry in hosts preempts the Internet lookup. The path to the hosts file is /etc/hosts in Linux and C:\Windows\System32\drivers\etc\hosts in Windows. The entry should include the DNS name, and the loopback IP address 127.0.0.1. The format is simple, but you can also Google it.

## Step 2

Pepper’s hint that Alabaster is “keeping files from search engine indexers” is most helpful. Google that phrase to see what she is talking about. You should find the name of a text file. Look to see if that text file is on the web site (as you browse through the SSH tunnel) and follow where it leads you.

## Step 3

Try to log in to EWA with Alabaster’s credentials. See if you can discover the proper format for user names.

## Questions

1. What is the content of the file about search engines?
2. What is the proper format for user names on the EWA site?