Objective--Network Traffic Forensics (Part 1)

What you can learn from this

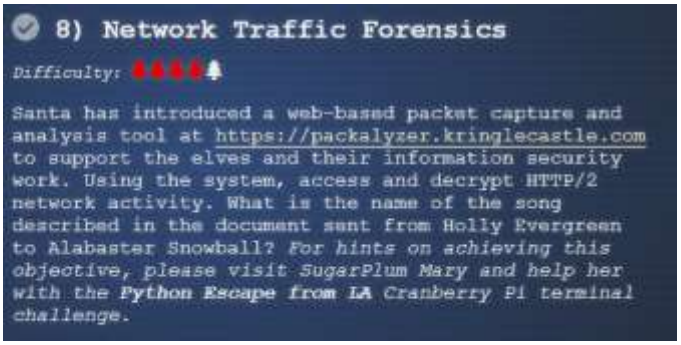
Most of the examples you see in textbooks and Wireshark packet captures are of HTTP 1.1. As you saw in Chris Elgee and Chris Davis' talk, HTTP/2: Because 1 Is the Loneliest Number, most major sites now use HTTP/2 because it is much more efficient.

One reason we don't see more HTTP/2 is that it is almost always encrypted. If you want to view encrypted web traffic from your own browser for troubleshooting or analysis, Firefox and Chrome both save the pre-master keys that you need to decrypt the traffic. Wireshark can use these keys to display the decrypted traffic to you. This talk, HTTP/2 Decryption and Analysis in Wireshark, by Chris Davis explains how it works.

It is essential that an IT security professional be able to decrypt HTTP/2. Also, Chris' talk will let you know what you should be looking for, to solve this objective. Watch the talk now.

Getting Started

For this challenge, you'll be working with Santa's new site, https://packalyzer.kringlecastle.com/.

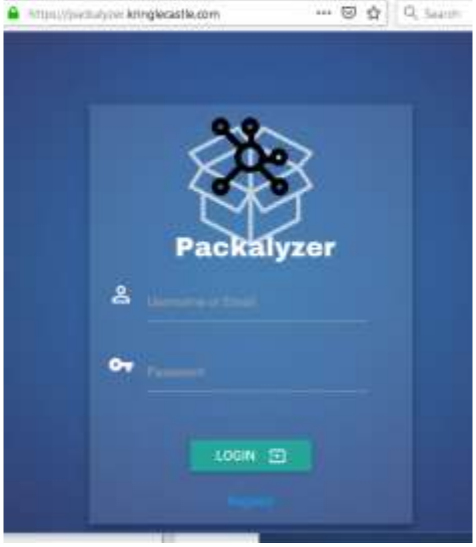


8) Network Traffic Forensics

Difficulty:

Santa has introduced a web-based packet capture and analysis tool at https://packalyzer.kringlecastle.com to support the elves and their information security work. Using the system, access and decrypt HTTP/2 network activity. What is the name of the song described in the document sent from Holly Evergreen to Alabaster Snowball? *For hints on achieving this objective, please visit SugarPlum Mary and help her with the **Python Escape from LA** Cranberry Pi terminal challenge.*

Create an account for yourself and log in. I've heard that the registration page only likes lower case letters.

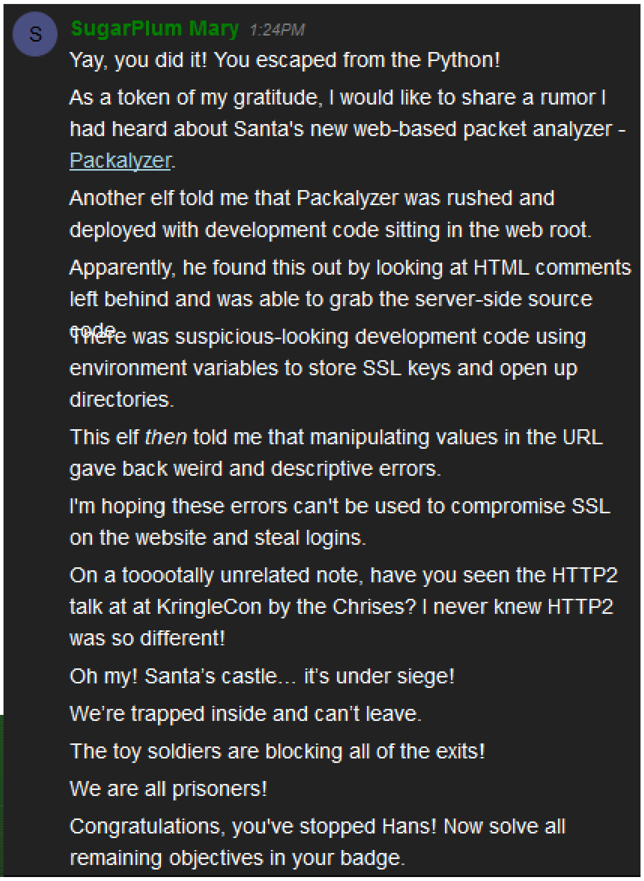


Once you can log in, you can take packet captures and download them. If you attended Chris' talk, you'll know that you are missing a file, though.

Much of this challenge will involve trying to get the packalyzer site to give you the file you need.

Hints

The talk in the badge hint is the one we mentioned before, HTTP/2 Decryption and Analysis in Wireshark, by Chris Davis. Without that you won't know what to look for. Take careful note of Mary's comments about comments, environment variables that expose directories, and weird descriptive errors from the URL.



SugarPlum Mary 1:24PM

Yay, you did it! You escaped from the Python!

As a token of my gratitude, I would like to share a rumor I had heard about Santa's new web-based packet analyzer - Packalyzer.

Another elf told me that Packalyzer was rushed and deployed with development code sitting in the web root.

Apparently, he found this out by looking at HTML comments left behind and was able to grab the server-side source code.

There was suspicious-looking development code using environment variables to store SSL keys and open up directories.

This elf *then* told me that manipulating values in the URL gave back weird and descriptive errors.

I'm hoping these errors can't be used to compromise SSL on the website and steal logins.

On a tooootally unrelated note, have you seen the HTTP2 talk at at KringleCon by the Chrises? I never knew HTTP2 was so different!

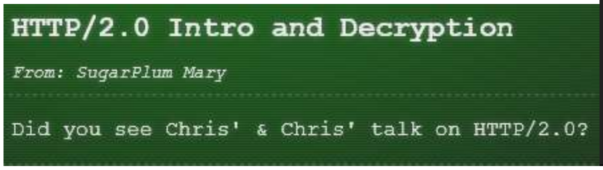
Oh my! Santa's castle… it's under siege!

We're trapped inside and can't leave.

The toy soldiers are blocking all of the exits!

We are all prisoners!

Congratulations, you've stopped Hans! Now solve all remaining objectives in your badge.



HTTP/2.0 Intro and Decryption

From: SugarPlum Mary

Did you see Chris' & Chris' talk on HTTP/2.0?

Hand In

1) Look for a one-line comment in the HTML index that mentions a file name that might contain source code.

2) Find that file using your browser. There aren't too many directories you have to look in.