Investigate S3 Bucket

This objective involves two distinct parts: finding a unpotected S3 storage bucket, then determining the content of the bucket.

Objective

> When you unwrap the over-wrapped file, what text string is inside the package? Talk to Shinny Upatree in front of the castle for hints on this challenge.

`Difficulty: 1/5`

Shinny Upatree's dialog

> Hiya hiya - I'm Shinny Upatree! Check out this cool KringleCon kiosk! You can get a map of the castle, learn about where the elves are, and get your own badge printed right on-screen! Be careful with that last one though. I heard someone say it's "ingestible." Or something... Do you think you could check and see if there is an issue?

Hints

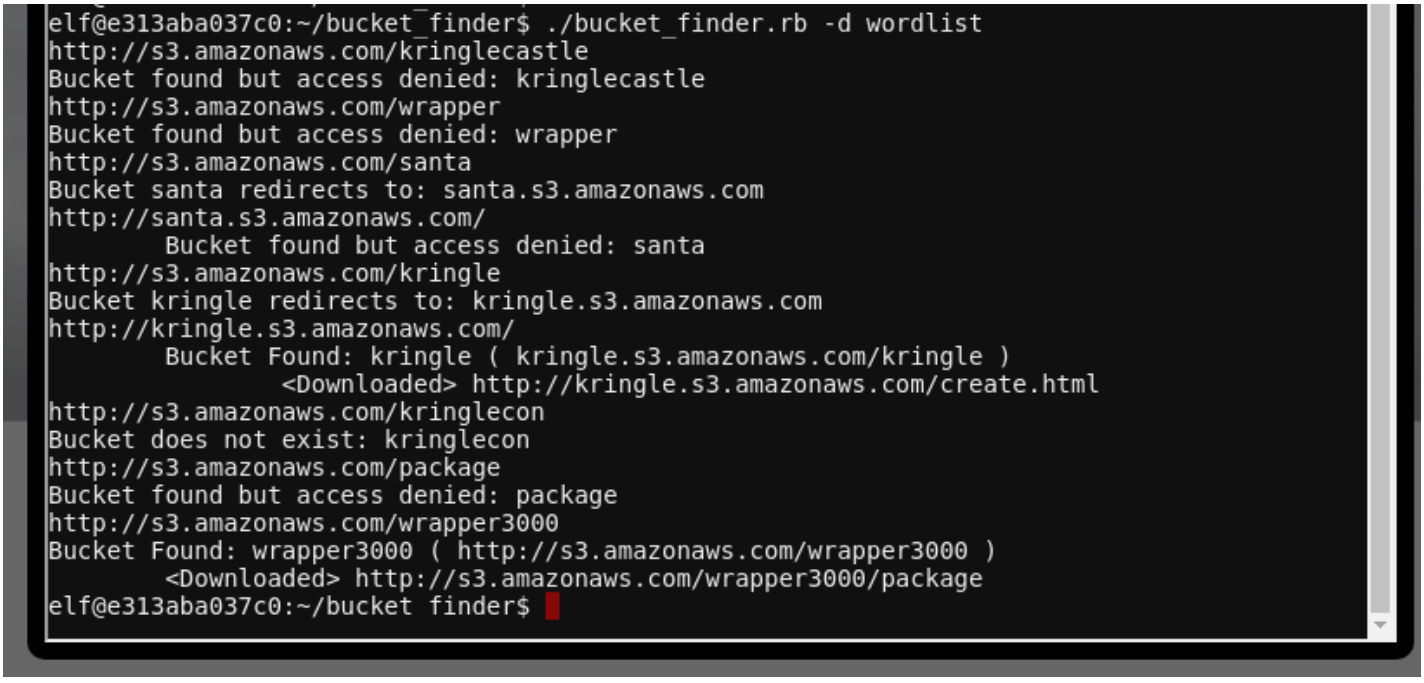
> It seems like there's a new story every week about data exposed through unprotected Amazon S3 buckets. Robin Wood wrote up a guide about finding these open S3 buckets. He even wrote a tool to search for unprotected buckets! Find Santa's `package` file from the cloud storage provider. Check Josh Wright's talk for more tips! Santa's Wrapper3000 is pretty buggy. It uses several compression tools, binary to ASCII conversion, and other tools to wrap packages.

Solution

To find the unprotected S3 bucket, we'll use the tool `bucket_finder` installed on the terminal labeled `Investigate S3 Bucket`. There is a sample wordlist included in the `bucket_finder` directory:

Unfortunately, running `bucket_finder -d wordlist` doesn't find the relevant data, so we'll need do some guesswork on what the bucket we're looking for will be named. We try a few guesses, based on the hints and dialog:

And have some success:



The `-d` flag passed to `bucket_finder` specifies that we want any content in the bucket downloaded locally. We see it downloaded the file `package` from `http://s3.amazonaws.com/wrapper3000`. Let's see what's in it:

```
elf@e313aba037c0:~/bucket_finder$ cd wrapper3000/
elf@e313aba037c0:~/bucket_finder/wrapper3000$ ls
package
elf@e313aba037c0:~/bucket_finder/wrapper3000$ file package
package: ASCII text, with very long lines
elf@e313aba037c0:~/bucket_finder/wrapper3000$ ls -l package
-rw-r--r-- 1 elf elf 829 Dec 10 17:03 package
elf@e313aba037c0:~/bucket_finder/wrapper3000$ cat package
UEsDBAoAAAAAAIAwhFEbRT8anwEAAJ8BAAAcABwAcGFja2FnZS50eHQuWi54ei54eGQudGFyLmJ6MlVUCQADoBfKX6
AXyl91eAsAAQT2AQAABBQAAABCWmg5MUFZJlNZ2ktivwABHv+Q3hASgGSn//AvBxDwf/xe0gQAAAgwAVmkYRTKe1PV
M9U0ekMg2poAAAGgPUPUGqehhCMSgaBoAD1NNAAAAyEmJpR5QGg0bSPU/VA0eo9IaHqBkxw2YZK2NUASOegDIzwMXM
HBCFACgIEvQ2Jrg8V50tDjh61Pt3Q8CmgpFFunc1Ipui+SqsYB04M/gWKKc0Vs2DXkzeJmiktINqjo3JjKAA4dLgLt
PN15oADLe80tnfLGXhIWaJMiEeSX992uxodRJ6EAzIFzqSbWtnNqCTEDML9AK7HHSzyyBYKwCFBVJh17T636a6Ygyj
X0eE0IsCbjcBkRPgkKz6q0okb1sWicMaky2Mgsqw2nUm5ayPHUeIktnBIvkiUWxYEiRs5nFOM8MTk8SitV7lcxOKst
2QedSxZ851ceDQexsLsJ3C89Z/gQ6Xn6KBKqFsKyTkaqO+1FgmImtHKoJkMctd2B9JkcwvMr+hWIEcIQjAZGhSKYNP
xHJFqJ3t32Vjgn/OGdQJiIHv4u5IpwoSG0lsV+UEsBAh4DCgAAAAAAgDCEURtFPxqfAQAAnwEAABwAGAAAAAAAAAAA
AKSBAAAAAHBhY2thZ2UudHh0LloueHoueHhkLnRhci5iejJVVAUAA6AXyl91eAsAAQT2AQAABBQAAABQSwUGAAAAAA
EAAQBiAAAA9QEAAAAA
elf@e313aba037c0:~/bucket finder/wrapper3000$
```

It's base64-encoded data. We can decode it with `base64 -d package > package-1`. Running `file package-1` shows that it's a .ZIP file. Checking the content of the ZIP file reveals a very strangely named file:

```
elf@e313aba037c0:~/bucket_finder/wrapper3000$ unzip -v package-1
Archive:  package-1
 Length   Method    Size  Cmpr    Date    Time   CRC-32   Name
--------  ------  ------- ---- ---------- ----- --------  ----
     415  Stored      415   0% 2020-12-04 11:04 1a3f451b  package.txt.Z.xz.xxd.tar.bz2
--------          -------  ---                            -------
     415              415   0%                            1 file
elf@e313aba037c0:~/bucket_finder/wrapper3000$ unzip package-1
Archive:  package-1
 extracting: package.txt.Z.xz.xxd.tar.bz2
```

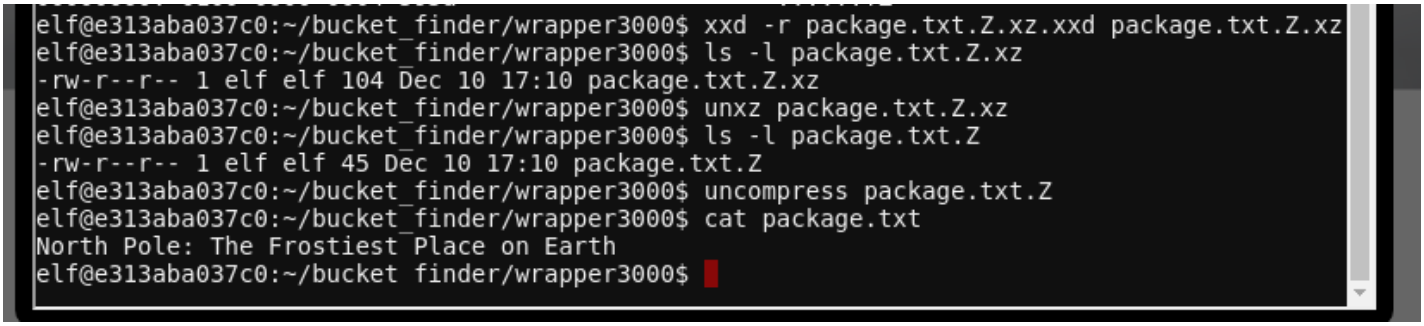
From the list of extensions on the file, we'll need to use the following utilities to extract the file:

1. bunzip2
2. tar
3. xxd
4. unxz
5. uncompress

`xxd` may not be familiar to some users. It's a tool for displaying files as hexdump, or re-creating a binary file from a hexdump:

```
elf@e313aba037c0:~/bucket_finder/wrapper3000$ more package.txt.Z.xz.xxd
00000000: fd37 7a58 5a00 0004 e6d6 b446 0200 2101  .7zXZ......F..!.
00000010: 1600 0000 742f e5a3 0100 2c1f 9d90 4ede  ....t/....,...N.
00000020: c8a1 8306 0494 376c cae8 0041 054d 1910  ......7l...A.M..
00000030: 46e4 bc99 4327 4d19 8a06 d984 19f3 f08d  F...C'M.........
00000040: 1b10 45c2 0c44 a300 0000 0000 c929 dad6  ..E..D.......)..
00000050: 64ef da24 0001 452d 1e52 57e8 1fb6 f37d  d..$..E-.RW....}
00000060: 0100 0000 0004 595a                      ......YZ
elf@e313aba037c0:~/bucket finder/wrapper3000$
```

We use `xxd -r` to re-create the .xz file, and proceed to extract the final `package.txt` and see it's contents for the objective:



Answer

`North Pole: The Frostiest Place on Earth`