DAY14_advent_of_the_cyber

Day 14: Where's Rudolph?:

'Twas the night before Christmas and Rudolph is lost
Now Santa must find him, no matter the cost
You have been hired to bring Rudolph back
How are your OSINT skills? Follow Rudolph's tracks...

Task #1

While hunting and searching for any hints or clues
Santa uncovers some details and shares the news
Rudolph loved to use Reddit and browsed aplenty
His username was 'IGuidetheClaus2020'

Many OSINT investigations start with only a username. A user's posting history can possibly lead to further information. Sometimes, it's the smallest of clues that help us out. Comb through Rudolph's Reddit history and answer questions #1-5 below. You may need to use partial clues with a search engine to fill in the gaps.

Watch TheCyberMentor's video on solving this task!

Learning Objectives:

1) Identify important information based on a user's posting history.
2) Utilize outside resources, such as search engines, to identify additional information, such as full names and additional social media accounts.

Additional Resources:

While Rudolph's posting history is enough for us to identify that he has other social media accounts, sometimes we are not that lucky. Great tools exist that allow us to search for user accounts across social media platforms. Sites, such as https://namechk.com/, https://whatsmyname.app/ and https://namecheckup.com/ will identify other possible accounts quickly for us. Tools, such as https://github.com/WebBreacher/WhatsMyName and https://github.com/sherlock-project/sherlock do this as well. Simply enter a username, hit search, and comb through the results. It's that easy!

Task #2

Well it looks like you have uncovered Rudolph's Twitter
Now we can read into all of his chitter
Go through his profile and give it some views
The deeper you dig, the better the clues

By finding another account belonging to our user, we open up the possibility of gathering even more information. Utilize the information found on Rudolph's Twitter account to answer questions #6-11.

Learning Objectives:

1) Identify important information based on a user's posting history.
2) Use reverse image searching to identify where a photo was taken and possibly identify additional information, such as other user accounts.
3) Utilize image EXIF data to uncover critical details, such as exact photo location, camera make and model, the date the photo was taken, and more.
4) Use discovered emails to search through breached data to possibly identify user passwords, name, additional emails, and location.

Additional Resources

This task was created to identify common critical steps in an OSINT investigation. Reverse image searching can help not only identify where an image was taken, but it can assist with identifying websites where that photo exists as well as similar photos (possibly from the same photoset), which can be incredibly useful in an investigation. While Google Images is used in our example, other sites should also be utilized to be as thorough as possible. No one site is perfect when it comes to reverse image searching (or any tool for that matter). Sites like https://yandex.com/images/ , https://tineye.com/ and https://www.bing.com/visualsearch?FORM=ILPVIS are great as well. Additionally, do not neglect the possibility of EXIF data existing in an image. While a lot of sites strip this data, not all do. It never hurts to look and can provide a wealth of information when the data is still there.

Finally, breached data can be incredibly useful from an investigative standpoint. Breach data does not just include passwords. It often has full names, addresses, IP information, password hashes, and more. We can often use this information to tie to other accounts. For example, say we find an account with the email of v3ry1337h4ck3r@gmail.com. If we search that email for breached data, we might find a password or hash associated with it. If unique enough, we can search that password or hash in a breach database and use it to identify other possible accounts. We can do the same with usernames, IPs, names, etc. The possibilities are vast and one email address can lead to a slew of information.

Websites such as https://haveibeenpwned.com/ will help identify if an account has ever been breached and will, at a minimum, inform us if an account existed at one point. However, it does not provide any password information. Free sites such as http://scylla.so/ will provide password information and are easy to search through. The data on free sites can tend to be older and not up to date with the latest breach information, but these sites are still a powerful resource. Lastly, paid sites such as https://dehashed.com/ offer up to date information and are easily searchable at affordable rates.

Exif data:

using : exiftool -h rudolph.jpg

ExifTool Version Number	11.88
File Name	rudolph.jpg
Directory	.
File Size	50 kB
File Modification Date/Time	2021:04:20 10:20:55+05:30
File Access Date/Time	2021:04:20 12:45:36+05:30
File Inode Change Date/Time	2021:04:20 12:45:36+05:30
File Permissions	rw-rw-r--
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
JFIF Version	1.01
X Resolution	72
Y Resolution	72
Exif Byte Order	Big-endian (Motorola, MM)
Resolution Unit	inches
Y Cb Cr Positioning	Centered
Copyright	{FLAG}ALWAYSCHECKTHEEXIFD4T4
Exif Version	0231
Components Configuration	Y, Cb, Cr, -
User Comment	Hi. :)
Flashpix Version	0100
GPS Latitude Ref	North
GPS Longitude Ref	West
Image Width	650
Image Height	510
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)
GPS Latitude	41 deg 53' 30.53" N
GPS Longitude	87 deg 37' 27.40" W
GPS Position	41 deg 53' 30.53" N, 87 deg 37' 27.40" W
Image Size	650x510
Megapixels	0.332