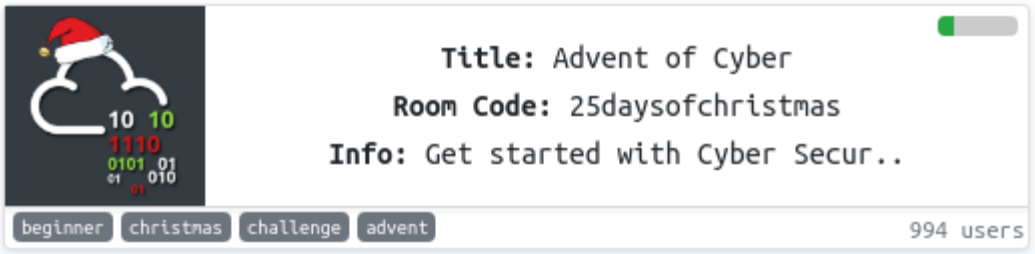
4 DECEMBER 2019 / GUIDE

Ho-Ho-Hosint

Ho-Ho-Ho!

Check our Christmas Challenge out! https://tryhackme.com/christmas
This blog post will explain some typical open source intelligence (OSINT) techniques. Use these to solve the challenge 5 of the Christmas Advent of Cyber!



Advent of Cyber Room Image

Do this challenge in the Christmas room!
https://tryhackme.com/room/25daysofchristmas

What is OSINT?

OSINT is data collected from publicly available sources to be used in an intelligence context. If an attacker were to run a target phishing campaign (which is sending fraudulent emails pretending to be from a reputable company, in order to have them reveal personal information or click on a malicious link), it looks more credible if you have prior knowledge about the individual being targeted.

Its amazing at how much information people share about themselves on social media platforms, both intentionally and un-intentionally. The OSINT framework is https://osintframework.com/ is a collection of resources and tools you can use for your intelligence gathering.

In the challenge, there will be three main OSINT techniques, which are as follows:

Image Metadata

Image metadata is text information that is pertaining to an image file, that is embedded into the file.

This data includes details relevant to the image itself as well as the information about its production. For example, if you take a photo in the park, your smartphone will attach GPS location metadata to the image. Back in the day, social networks wouldn't strip an images metadata, which mean't a celebrity could take a photo at home and upload it, revealing their location.. Creepy right?

Image Metadata can also include camera details, such as aperture, shutter speed and DPI.. it can also include the creator (author) or the individual taking the image.

Exiftool is a free and open-source program for reading metadata on files. Lets use this program to read a photo's metadata. If you don't have exiftool installed, you can download it here or you can deploy and access your own Kali machine with it pre-installed here.

Run the following command: `exiftool <image file>`

The output will look similar to below:

```
ben@cloud ~/Pictures $ exiftool yy.jpg
ExifTool Version Number         : 10.10
File Name                       : yy.jpg
Directory                       : .
File Size                       : 314 kB
File Modification Date/Time     : 2018:12:16 15:21:40+00:00
File Access Date/Time           : 2019:12:04 10:42:37+00:00
File Inode Change Date/Time     : 2018:12:16 15:21:43+00:00
File Permissions                : rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Exif Byte Order                 : Little-endian (Intel, II)
Software                        : Google
Exif Version                    : 0220
User Comment                    :
Image Width                     : 1744
Image Height                    : 981
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1744x981
Megapixels                      : 1.7
```

Example exiftool output

WayBack Machine

The WayBackMachine is a digital archive of the World Wide Web. It takes a snapshot of a website and saves it for us to view in the future. For example, here is what Google looked like on 8th Feb 1999: https://web.archive.org/web/19990208004515/http://google.com/

This can be used to gather information regarding how a website used to look.

Does the day 5 challenge give us any websites to navigate to? I wonder if there are any interesting pages that have been snapshot...

Reverse Image Search

Wouldn't it be cool if you could search the internet with an image? Well we can! Google actually lets you search the net for an image you have.

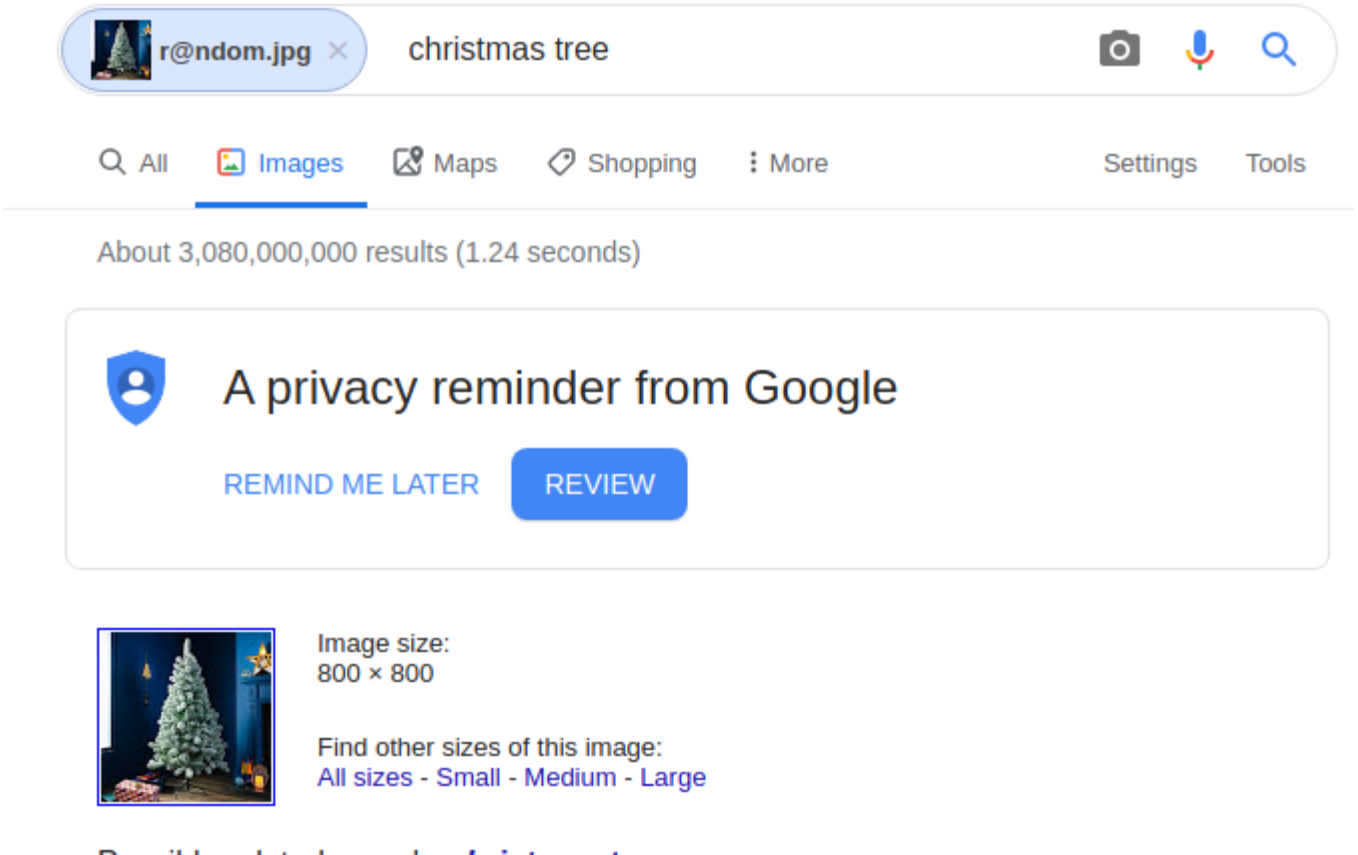
If a user has a profile picture of themselves on one social media, its most likely they've re-used the same photo on lots of other different social media sites. You can take that one image, search all other sites for that image and identify where that user has also signed up.

It can also be used to identify who or what is in an image. So if you are ever unsure on who someone in an image is (providing its a clear image of just that one individual), Google will most likely tell you.

For example, suppose we don't know what the following image is:

Standard Christmas Tree Image

We can search the internet for the image. Go onto Google Image Search (https://www.google.com/imghp?hl=en) and click the camera icon to search by an image. Then select the image! It will tell us what the image is! Oh look, its a Christmas tree!



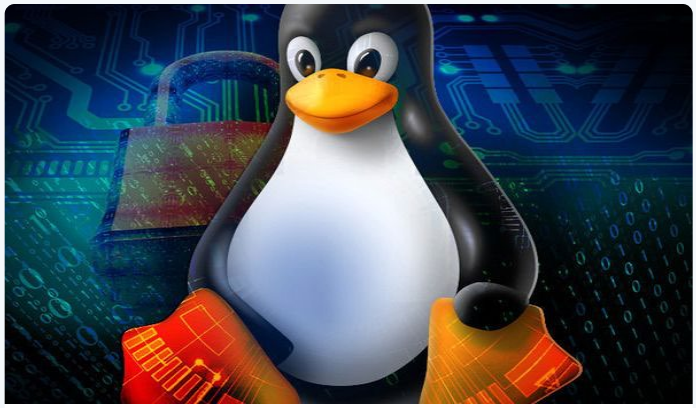
Reverse Image Search showing image object being recognised

Are you able to use image metadata, the WayBackMachine and Reverse Image Searching to solve the Day 5 of the Christmas challenge?

Ben Spring

Read more posts by this author.

Read More



CHRISTMAS

Linux Privilege Escalation: SUID

Set owner User ID up on execution Check our Christmas Challenge out! https://tryhackme.com/christmasThis blog post will explain what privilege escalation is and how we can escalate our privileges using SUID

4 MIN READ

Setting Up Burp

Burp Suite (referred to as Burp) is a graphical tool for testing Web application security.In this set of tutorials we will go through how to set up Burp to intercept traffic on

5 MIN READ