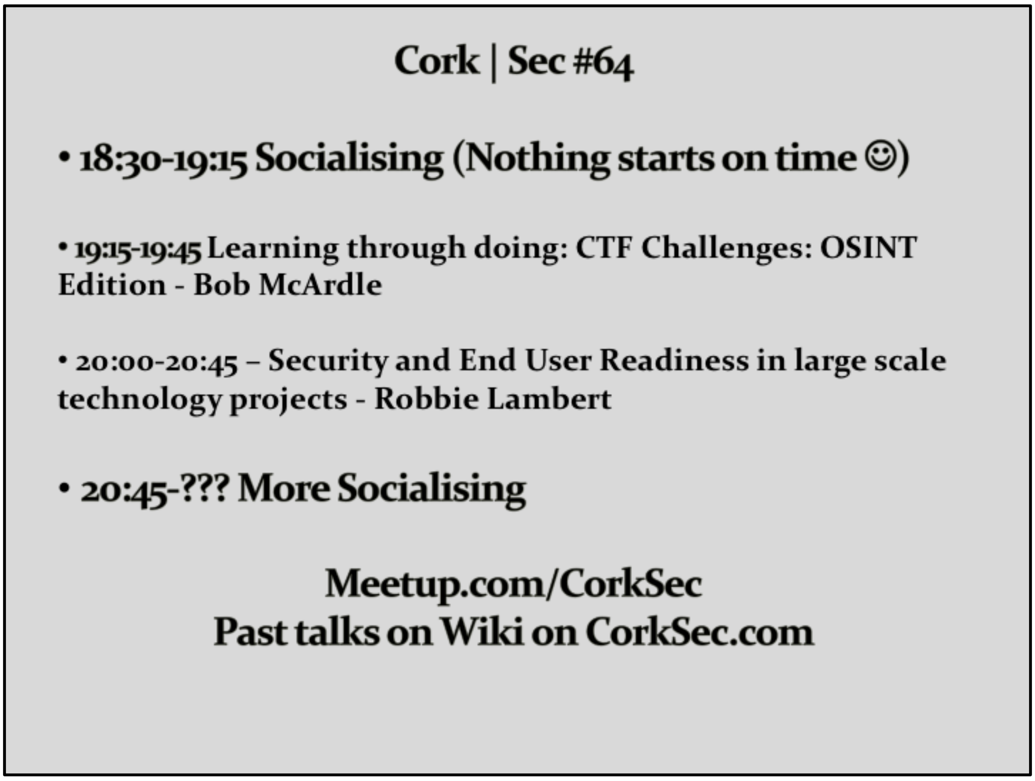
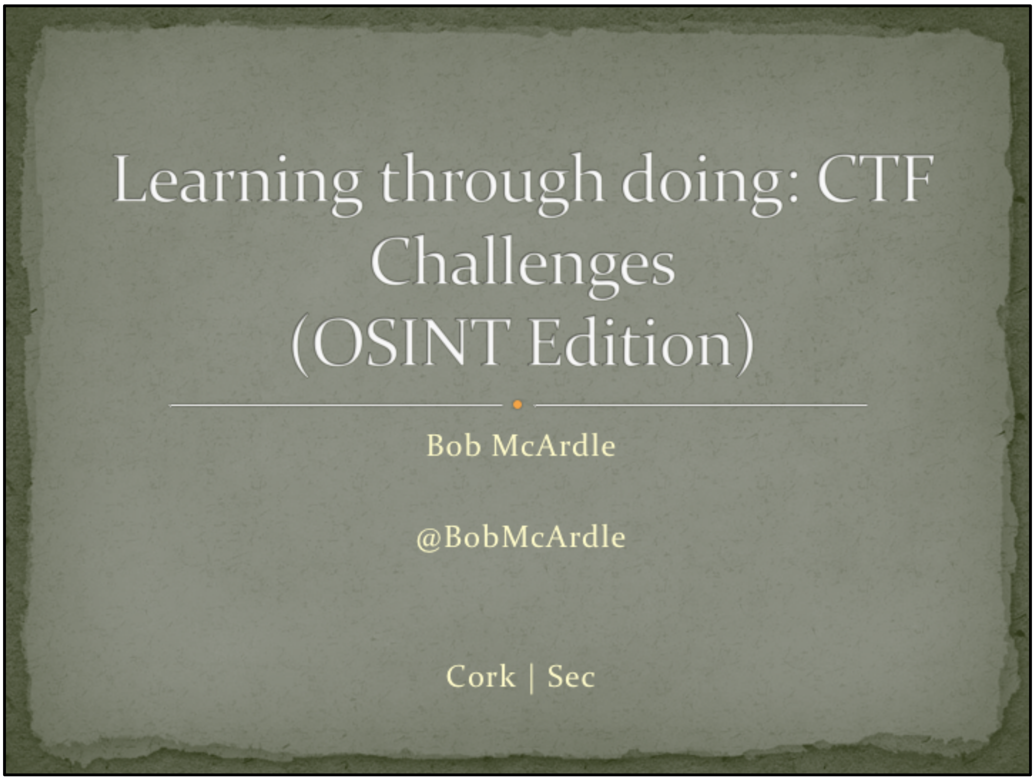


Cork | Sec #64

- 18:30-19:15 Socialising (Nothing starts on time ☺)
- 19:15-19:45 Learning through doing: CTF Challenges: OSINT Edition - Bob McArdle
- 20:00-20:45 – Security and End User Readiness in large scale technology projects - Robbie Lambert
- 20:45-??? More Socialising

Meetup.com/CorkSec
Past talks on Wiki on CorkSec.com



Learning through doing: CTF Challenges (OSINT Edition)

Bob McArdle

@BobMcArdle

Cork | Sec

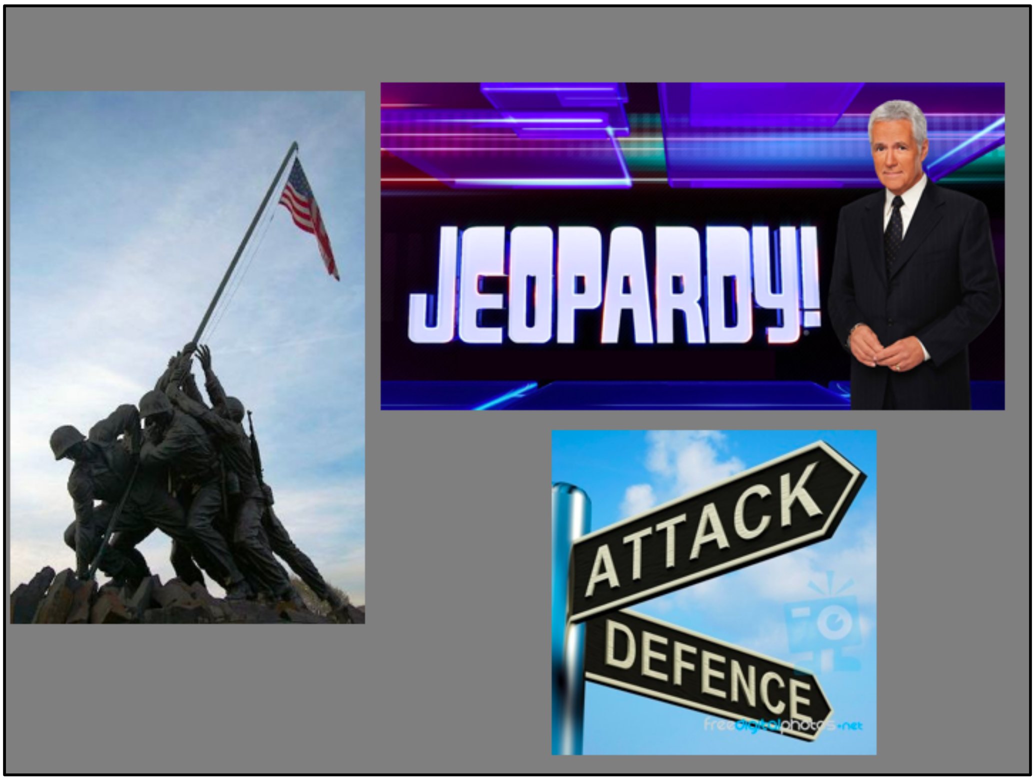
CAPTURE THE FLAG

EXPLAIN WHAT ONE IS

ALSO ONE OF THE BEST SOURCE OF LEARNING YOU CAN DO – ESPECIALLY ONLINE ONES.

GREAT PLACE TO TRY OUT SKILLS – WHY?

IT'S A HACKING CHALLENGE THAT GIVES YOU HINTS AS YOU GO!



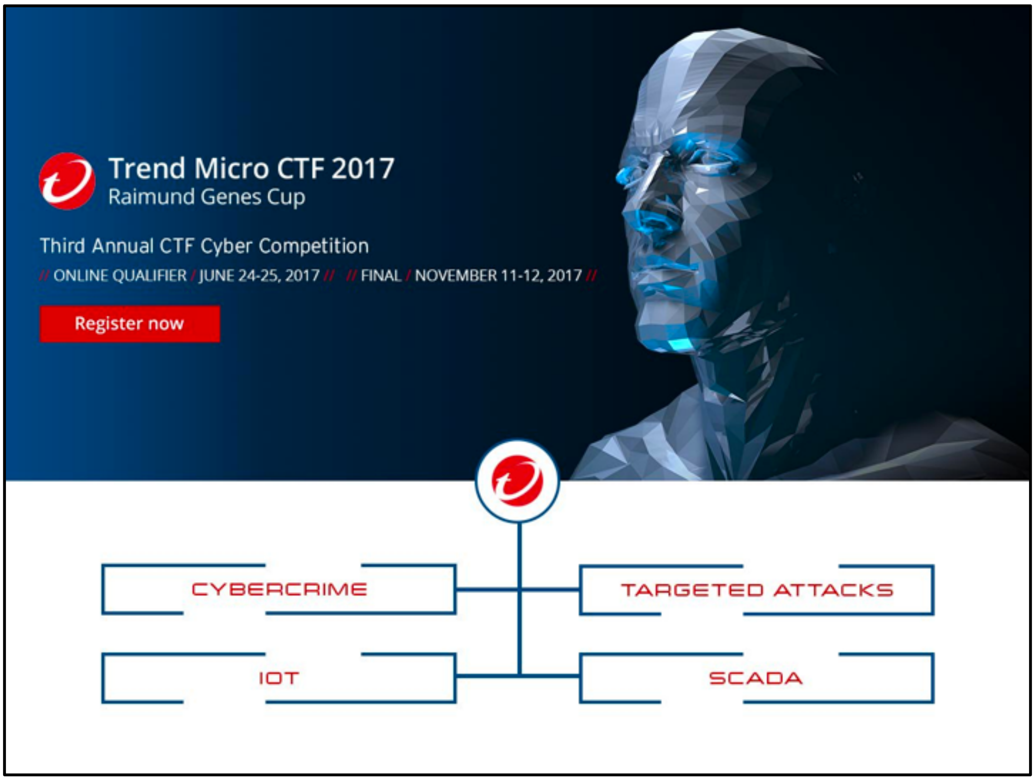
3 MAIN FORMATS – DESCRIBE EACH

POINTS OVER TIME

A&D ALSO RED VS BLUE

THEN DIFF TYPE – E.G. REVERSING, NETWORKING, WEB, EXPLOIT – OR SPECIALISED LIKE IOT, OSINT, ETC

DOES NOT REALLY MATTER – PICK THE TYPE THAT SUITS YOU



Trend Micro CTF 2017

Raimund Genes Cup

Third Annual CTF Cyber Competition

// ONLINE QUALIFIER / JUNE 24-25, 2017 // // FINAL / NOVEMBER 11-12, 2017 //

Register now

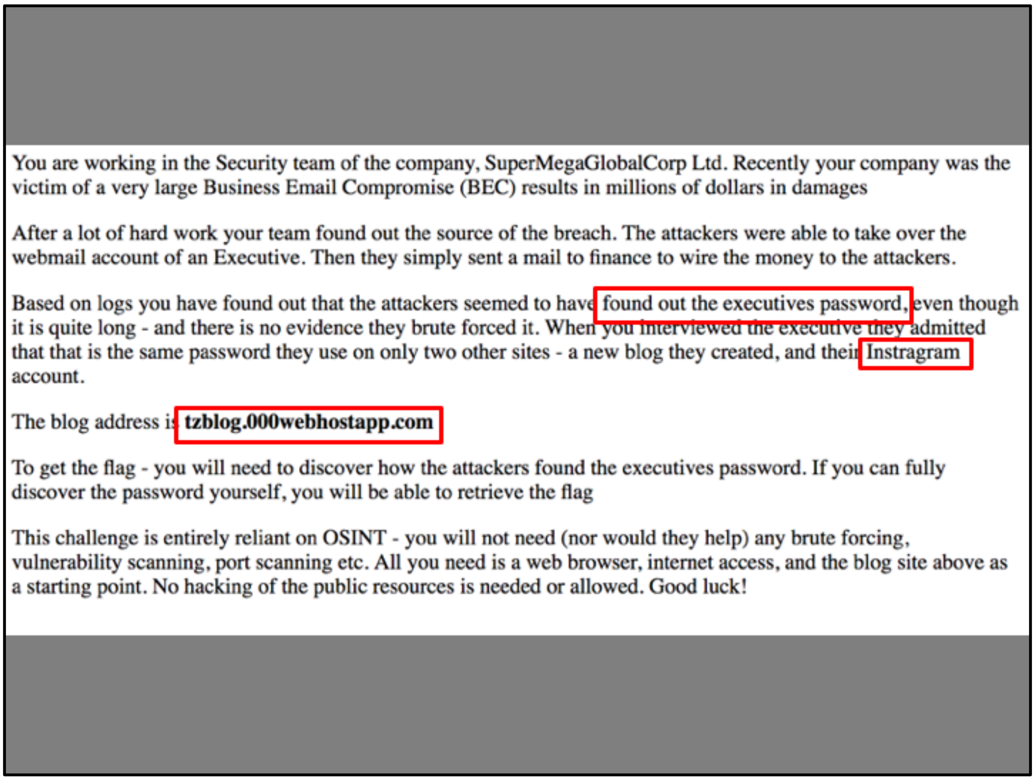
EXPLAIN RAIMUND GENES CUP

RAN SEVERAL YEARS – QUALIFIER FREE ONLINE / FINAL JAPAN

QUALIFIER ALREADY DONE FOR THIS YEAR

FOR TONIGHT WILL WALK YOU THROUGH ONE CHALLENGE FROM THE FINAL (SO YOU DEFINTIELY HAVE NOT SEEN)

AND LEARN TECHNIQUES AS WE DO IT



You are working in the Security team of the company, SuperMegaGlobalCorp Ltd. Recently your company was the victim of a very large Business Email Compromise (BEC) results in millions of dollars in damages

After a lot of hard work your team found out the source of the breach. The attackers were able to take over the webmail account of an Executive. Then they simply sent a mail to finance to wire the money to the attackers.

Based on logs you have found out that the attackers seemed to have found out the executives password, even though it is quite long - and there is no evidence they brute forced it. When you interviewed the executive they admitted that that is the same password they use on only two other sites - a new blog they created, and their Instragram account.

The blog address is **tzblog.000webhostapp.com**

To get the flag - you will need to discover how the attackers found the executives password. If you can fully discover the password yourself, you will be able to retrieve the flag

This challenge is entirely reliant on OSINT - you will not need (nor would they help) any brute forcing, vulnerability scanning, port scanning etc. All you need is a web browser, internet access, and the blog site above as a starting point. No hacking of the public resources is needed or allowed. Good luck!

HERE IS CHALLENGE USERS SEE – GO OVER

THIS WAS IN THE OSINT CATEGORY

A LOT IS FLUFF AND SCENE SETTING – ONLY A FEW USEFUL COMPONENTS

SO LETS GET STARTED – OBVIOUS STARTING POINT IS THE BLOG

- DEMO TIME!

1. The initial blog tzblog.000webhostapp.com has a number of clues. The most important starting point though is a commented out link to admin.php in the source code.

CLUES LIST:
- Email in Contact Us
- Location LA, USA
- First image associated to favourite actor of all time – funny surname
- Mentions he is from Alabama
- 2nd Pic of an Onion Dog
- Always look at the source

2. The admin.php page is designed to look like a 404 page, however at the bottom of the page is a password field (AGAIN – LOOK AT THE SOURCE). Any wrong answer gives the following hint

HINT: Favourite actors real first name + Favourite Sports team + Surname of politician I donated to + Year I bought my car
[ALL CAPS - NO SPACES - JOIN WORDS TOGETHER]

The teams need to discover those 4 bits in order to find the “password” that leads to the flag

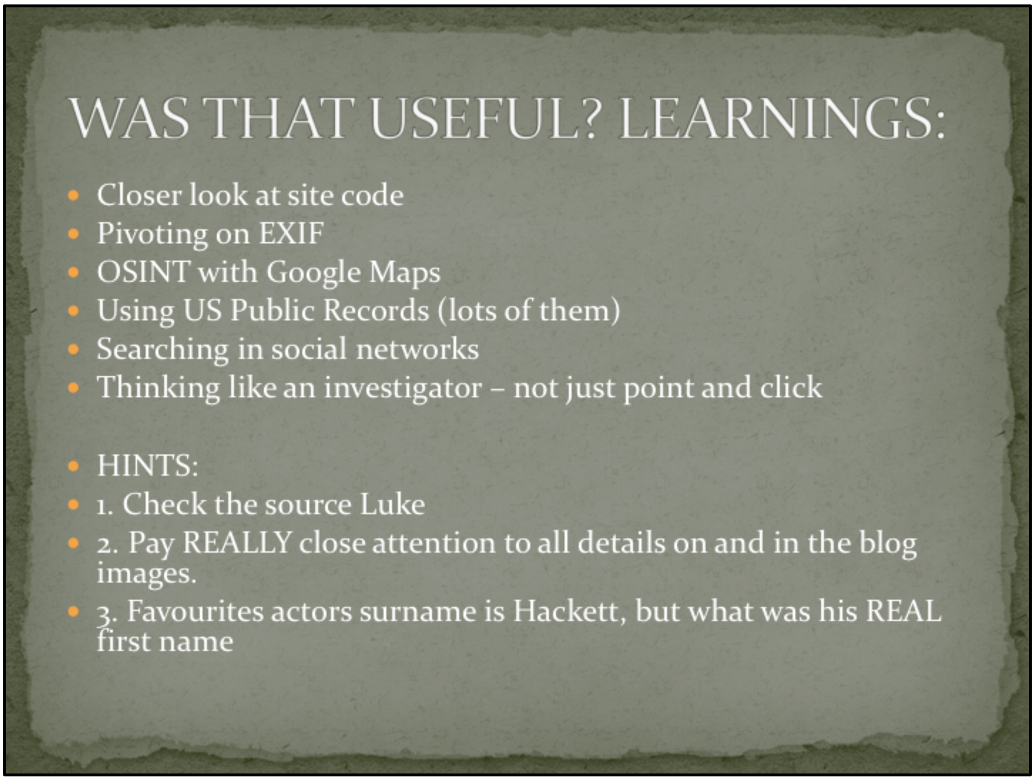
3. Favourite Actors Real First Name:
=== One the blog the first picture shows a street scene and mentions it was taken somewhere related to his favourite actor.
=== The image has a number of street signs that give hints of where it is . Searching these and narrowing down options in Google Maps will lead to this location on Hollywood Blvd
https://www.google.ie/maps/place/6834+Hollywood+Blvd,+Los+Angeles,+CA+90028,+USA/@34.10151,-118.3396638,3a,75y,7.83h,93.3t/data=!3m6!1e1!3m4!1smWrPED_xGYk_AsyFVqmpKA!2e0!7i13312!8i6656!4m5!3m4!1s0x80c2bf23e643b41f:0xa9ef54cbaa0289f5!8m2!3d34.101323!4d-118.339741
=== That is part of the famous Hollywood Walk of fame, and there are a number of stars listed at 6834 Hollywood Blvd
=== They can then check https://en.wikipedia.org/wiki/List_of_stars_on_the_Hollywood_Walk_of_Fame to check the stars there (several). Another clue on the blog says the InfoSec team find the surname funny.
=== This leads to actor Buddy Hackett - whose real name is Leonard Hacker
=== Password Part = LEONARD

4. Favourite Sports Team Name:
=== The 2nd picture in the blog is taken at one of Tony’s favourite locations. Checking the EXIF data reveals a GPS coordinate - 34.043000 degrees N, 118.267300 degrees W
=== This is the location of the Staples Centre, home to both the LA Clippers and LA Lakers.
=== You could just guess between the two, but there is a clue to help you tell. In the description he mentions that he has an Instagram page, and on the blog there is a contact us link with the email Tony.Zoghby@gmx.us. There is also a reference that suggests Tony has a Instragram page.
=== Searching for Tony Zoghby from Alabama (also mentioned in blog) leads to https://www.instagram.com/tonyzoghbyusa
=== On Tony’s page are several posts related to the Lakers. He also follows the teams stadium
=== Password Part = LAKERS

5. Surname of Politician I donated to:
=== The previous image also has a clue in the EXIF - a site https://www.fec.gov/data/
=== Searching for political donations by a Tony Zoghby on the site, and going back over the years will find 3 donations to Newt Gingrich (also ties with the Instragram posts showing he prefers the Republican Party)
=== Password Part = GINGRICH

6. Year I bought my car:
=== On the Instagram account is 2 posts showing 2 pictures of Tony’s car.
=== The 2nd picture has a licence plate - 45PM7
=== Check this on https://www.vehiclehistory.com/licence-plate-search/free-licence-plate-search-alabama.php
=== In the Vehicle history it shows it is from 2007
=== Password Part = 2007

7. Combining these together gives the password “LEONARDLAKERSGINGRICH2007”. Entering this will reveal the flag “TMCTF{HOPETHATWASFUN}”



WAS THAT USEFUL? LEARNINGS:

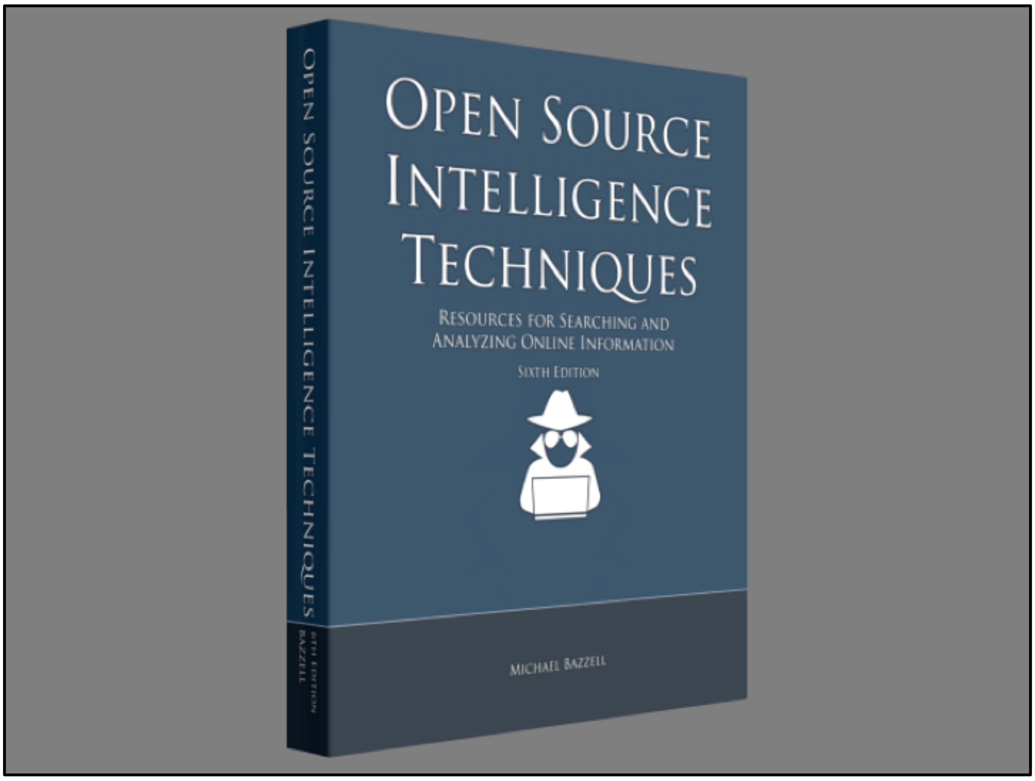
- Closer look at site code
- Pivoting on EXIF
- OSINT with Google Maps
- Using US Public Records (lots of them)
- Searching in social networks
- Thinking like an investigator – not just point and click

- HINTS:
- 1. Check the source Luke
- 2. Pay REALLY close attention to all details on and in the blog images.
- 3. Favourites actors surname is Hackett, but what was his REAL first name

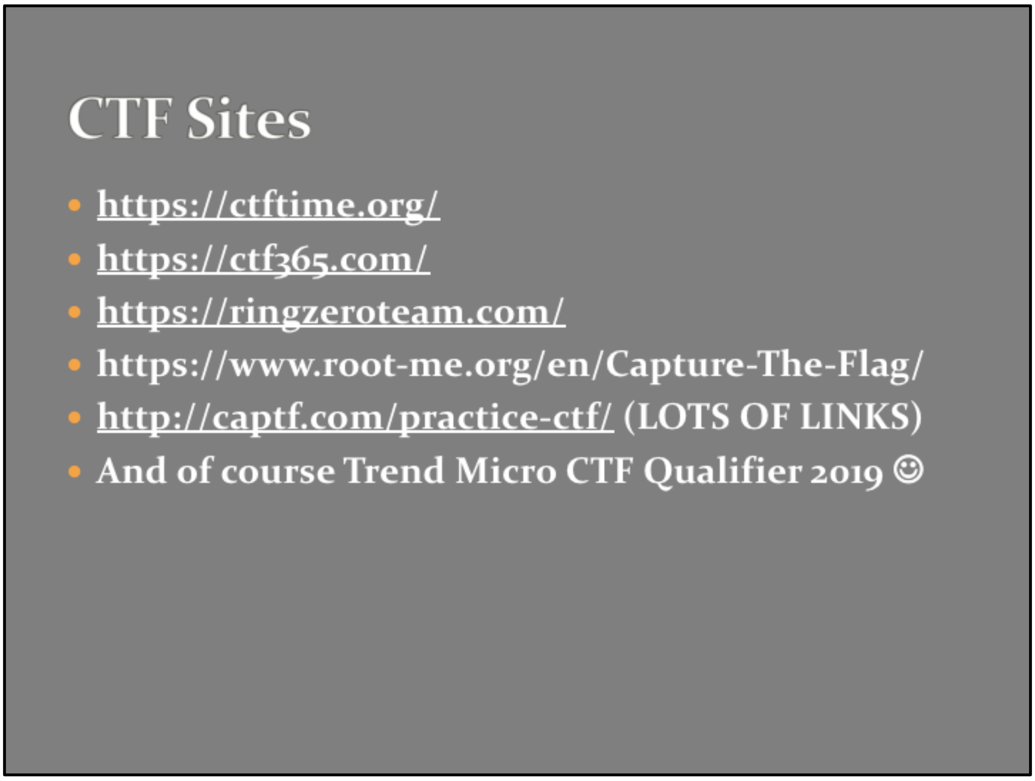
OTHERS COULD BE A NEW RE TECHNIQUE ETC

EXAMPLE OF HINTS GIVEN AS WE WENT

SO A GREAT SOURCE OF LEARNING – SO NOW WHAT


OPEN SOURCE INTELLIGENCE TECHNIQUES
RESOURCES FOR SEARCHING AND ANALYZING ONLINE INFORMATION
SIXTH EDITION
MICHAEL BAZZELL
OPEN SOURCE INTELLIGENCE TECHNIQUES
6TH EDITION
BAZZELL

IF INTERESTED IN OSINT – GO GET THIS BOOK, BEST OUT THERE BY FAR – FULL OF USEFUL TOOLS



CTF Sites

- https://ctftime.org/
- https://ctf365.com/
- https://ringzeroteam.com/
- https://www.root-me.org/en/Capture-The-Flag/
- http://captf.com/practice-ctf/ (LOTS OF LINKS)
- And of course Trend Micro CTF Qualifier 2019 ☺

CTFTIME – UPCOMING AND DETAILED WRITEUPS! FANTASTIC FOR LEARNING

That's all Folks!