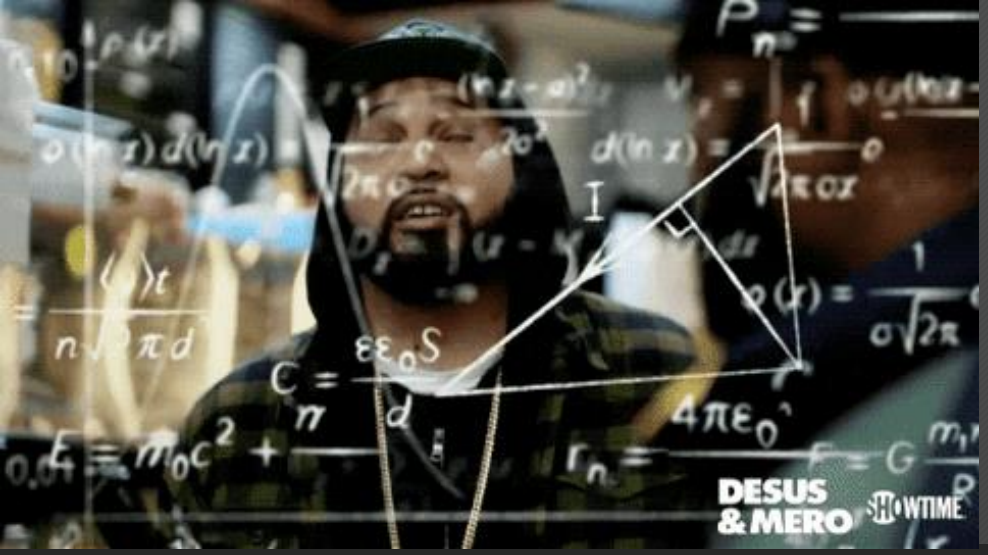
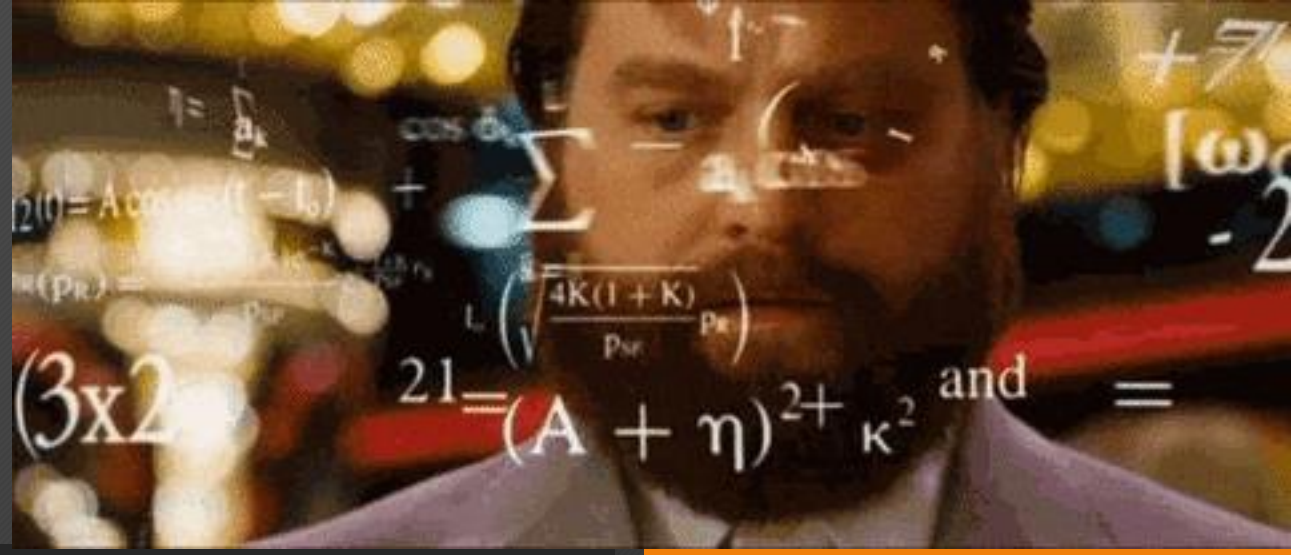




OSINT?

The gateway drug your mom never told you about.

Charles Hein Wroth
@AngusRedBlue
Lead Technical Security Recruiter

GOV-X
Innovation Challenge

Outline

- Introduction: /whoami /ipconfig all
- What is OSINT?: What is open-source intelligence?
- Why OSINT?: Why conduct OSINT?
- The drug: Why it is so awesome?
- The highs: The result
- The side effects: What can you gain indirectly?
- What now?: Feed the supply!
- Questions: Hopefully plenty!

Introduction – $ career/ ls -a

Charles H Wroth – Lead Technical Security Recruiter (USA/EU/UK/RSA)

***6 Years: Former British Airborne (3 PARA) UK**
***6 Years :High Risk Security Advisor (PhysSec)**
***4 Years: Technical Security Recruiter**
-Technically advanced security hiring (USA, UK, RSA)
-B Sides Cape Town Co-Organizer (Logistics)
-Working to become a DFIR Consultant
-Hack South (Founder)

TRACELABS OSINT'er!
Highest ranking P3 (First was 53rd)

OSINT: The gateway drug your mom never told you about.

What is OSINT

OSINT: The gateway drug your mom never told you about.

What is OSINT?

Definition

- **Open-source intelligence** (**OSINT**) is a multi-methods (qualitative, quantitative) methodology for **collecting, analyzing and making decision about data accessible in publicly available sources to be used in an intelligence context**. In the intelligence community, the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources). It is not related to open-source software or collective intelligence.
- OSINT under one name or another has been around for hundreds of years. With the advent of instant communications and rapid information transfer, a great deal of actionable and predictive intelligence can now be obtained from public, unclassified sources.

OSINT: The gateway drug your mom never told you about.

What is OSINT?

Sources:

OSINT sources can be divided up into six different categories of information flow:[2]

- **Media**, print newspapers, magazines, radio, and television from across and between countries.
- **Internet**, online publications, blogs, discussion groups, citizen media (i.e. – cell phone videos, and user created content), YouTube, and other social media websites (i.e. – Facebook, Twitter, Instagram, etc.). This source also outpaces a variety of other sources due to its timeliness and ease of access.
- **Public Government Data**, public government reports, budgets, hearings, telephone directories, press conferences, websites, and speeches. Although this source comes from an official source they are publicly accessible and may be used openly and freely.
- **Professional and Academic Publications**, information acquired from journals, conferences, symposia, academic papers, dissertations, and theses.
- **Commercial Data**, commercial imagery, financial and industrial assessments, and databases.
- **Grey literature**, technical reports, preprints, patents, working papers, business documents, unpublished works, and newsletters.
- OSINT is distinguished from research in that it applies the process of intelligence to create tailored knowledge supportive of a specific decision by a specific individual or group.[3]

OSINT: The gateway drug your mom never told you about.

Why OSINT?
What I/we use it for?

OSINT: The gateway drug your mom never told you about.

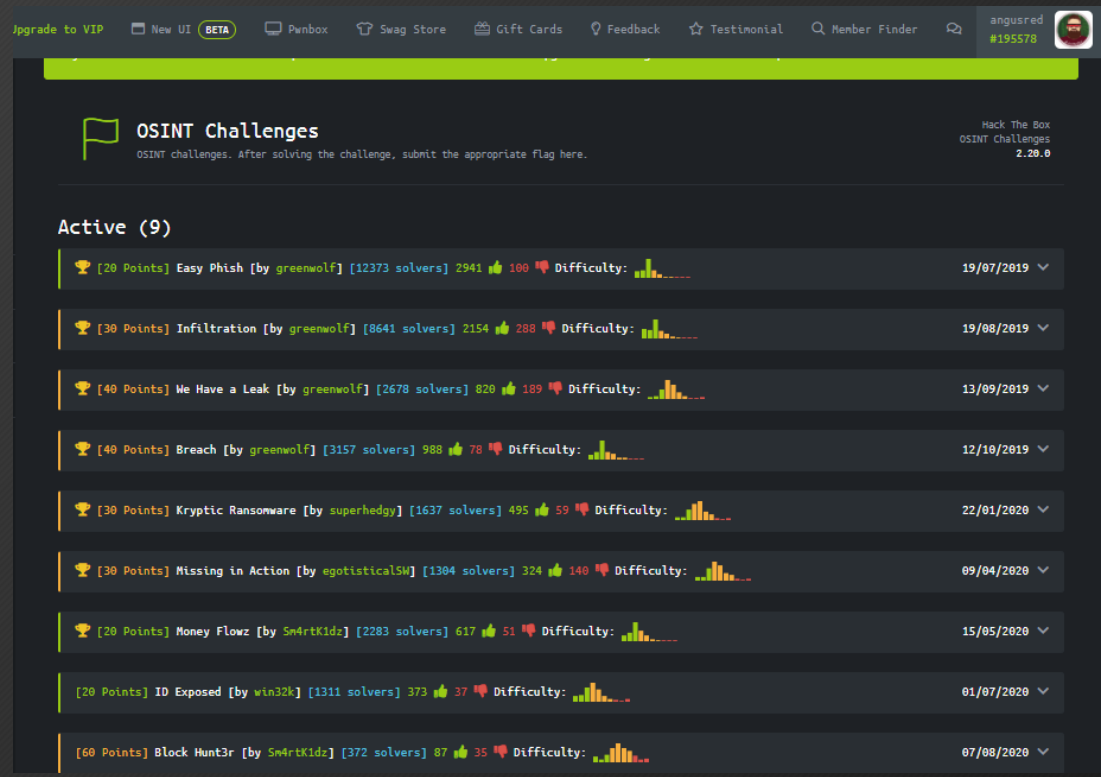
Why OSINT?
What I use for?

CTF's/Challenges

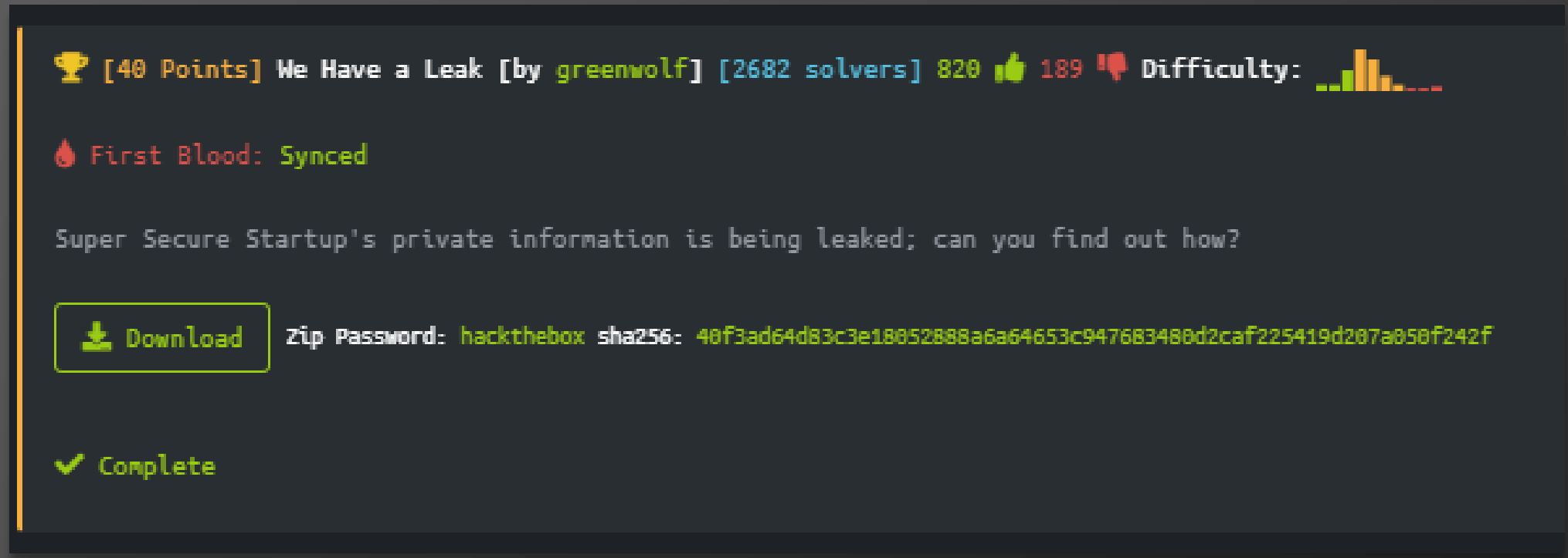
- Usually based on fake info/accounts in order to test someone's ability to gather intel and piece it together to form a hypothesis.

Example

- Hack The Box Challenges
- Personally developed challenges @Bushido
- #OSINTchallenge (Finding a location of a photo)



OSINT: The gateway drug your mom never told you about.



Why OSINT?
What I use for?

HTB OSINT Challenges

OSINT: The gateway drug your mom never told you about.

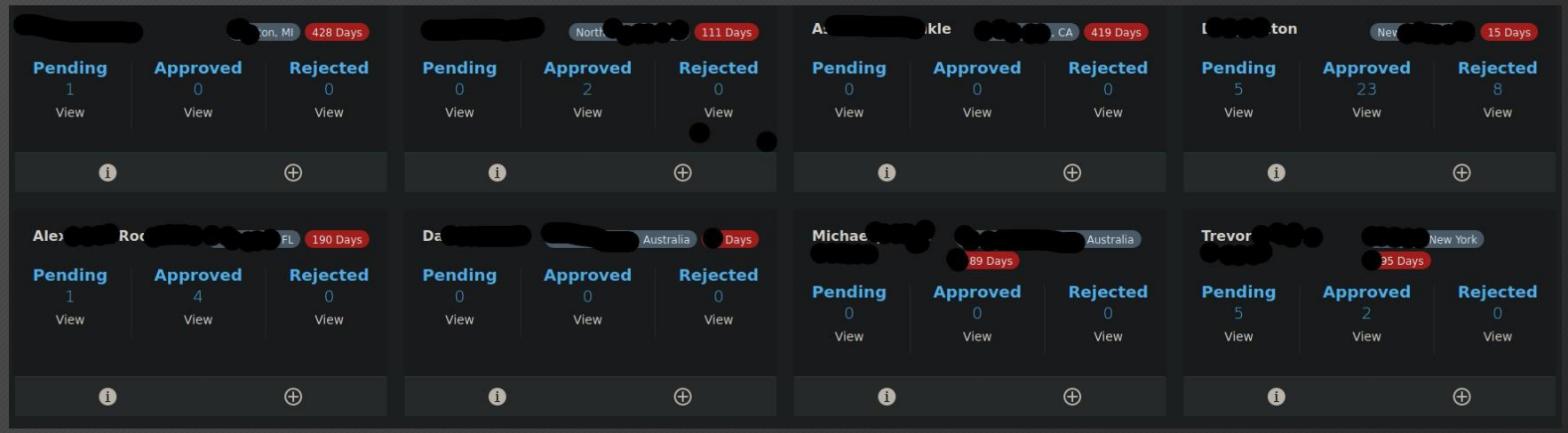
Why OSINT? What I use for?

#OSINTchallenge

Why OSINT?
What I use for?

TraceLabs

- A CTF based on 8-12 missing persons cases. It is to challenge someone's ability but is based in real people and real cases and so has a real outcome (Intel passed to law enforcement) in an effort to locate missing person.



OSINT: The gateway drug your mom never told you about.

Why OSINT?
What I use for?

OSINT: The gateway drug your mom never told you about.

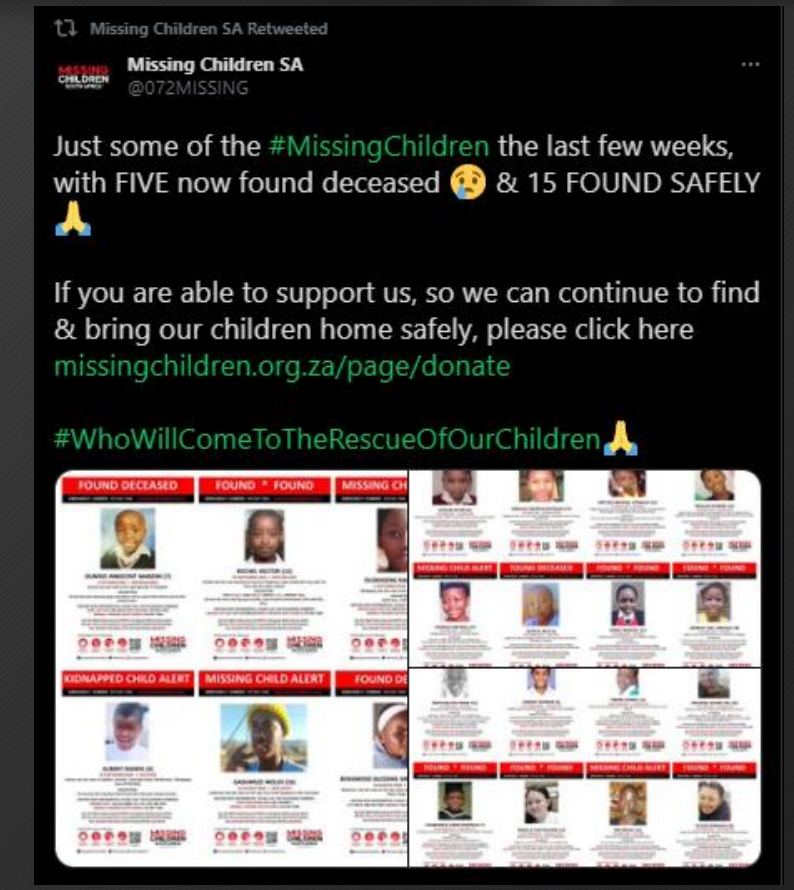
Why OSINT?
What I use for?

MISSING CHILDREN SOUTH AFRICA®

OSINT: The gateway drug your mom never told you about.

MISSING PERSONS

- mcsa-noticeboard
- mcsa-feed
- hunt-resources
- media-posts
- general-chat
- dev-reflexions
- 25-h
- 16-s
- 26-k
- 13-i
- 16-c
- 15-r
- 14-m
- 8-t
- 28_f
- 49-m
- analyst-vc-chat
- Analyst VC



Why OSINT?
What we use it for?

Red Teaming and Social Engineering

- Many red teamers will use OSINT to gather intel on proposed targets. They will use that information to build a picture on their clients in order to exploit vulnerabilities, such as with the human factor using Social Engineering and other exploitation tactics.
- This often forms part of the recon phase of an engagement.

Why OSINT?
What we use it for?

Business Development

- As a recruiter I do extensive OSINT to understand my clients or potential clients, what makes them tick and how to string pieces of information together to execute a better pitch to a client.

Example

- To get an “in” with companies I will find some people I can talk to
- Will conduct basic research on “target” and people I know, know them
- Build a picture of the company and people I want to contact
- Execute outreach using some basic info to help break ice and build familiarity
- Nothing over the top, nothing intrusive

Why OSINT?
What we use it for?

Interview Prep

- As an interviewee when I was a contractor, I would do extensive research into the company I am interviewing with.

Example

- To show my interest in a company I would always do extensive research.
- Who am I interviewing with? What is their story? Where did they study?
- What does the company do, where do they operate, how do they operate?
- On an interview, when asked about what I know about the company, I can show my understanding which holds me in good stead.
- I gets the job!

OSINT: The gateway drug your mom never told you about.

Why OSINT?
What we use it for?

Candidate Vetting

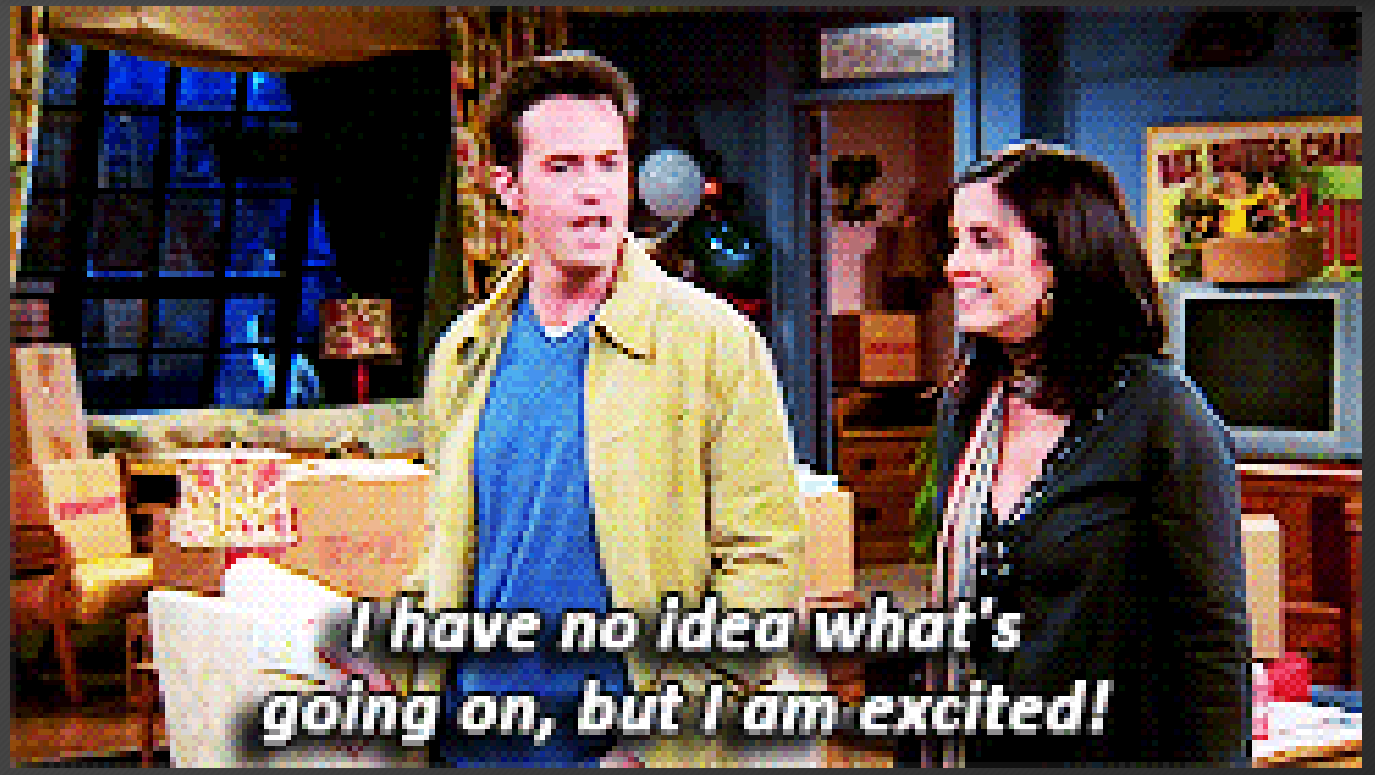
- As an interviewer or a recruiter I am sometimes asked to do some background checks on candidates.
- Using OSINT tactics one can do some basic research into a candidate.
- What do they do on the weekends, what does their online presence say about who they are as a person and whether there are any red flags.

Why OSINT?
What we use it for?

Police and Military Intelligence

- Track down threat actors
- Investigate high net worth people (Lifestyles) by SARS
- Track down missing children
- Track down criminals
- Prosecution

The drug
Why it is so awesome?



OSINT: The gateway drug your mom never told you about.

The drug
Why it is so awesome?

Easy of entry

Prerequisites

- A computer/smart phone
- Internet
- Curiosity
- Understanding of ROE
- Understanding what you want as an outcome
- Understanding of what you might find (Violence, Sex, Nudity, Death)

OSINT: The gateway drug your mom never told you about.

The highs
What is the result?

The highs
Why it is so awesome? What is the result?

Satisfaction

- The find!
- The new client, new job
- When you know, you know
- Many small pieces, make one pretty puzzle
- The knowledge

The side effects
What can you gain indirectly

OSINT: The gateway drug your mom never told you about.

The side effects
What can you gain indirectly

A champion of OpSec

The hunger

The intent

The path

The career

What now?
Feed the supply

OSINT: The gateway drug your mom never told you about.

What now?
Feed the supply

Going clean?

- At least you tried
- Better OPSEC/PERSEC awareness
- Mindfulness
- Remember the good ol days

What now?
Feed the supply

Show and tell

- Show your friends and family what OSINT is, what you are able to do, and how that makes them vulnerable.

Understand the ease of entry and get involved!

- Get involved with Trace Labs, get involved with other orgs. Take a swing. It can lead to new avenues of interest and potentially a new career in information security.

Evolve into a new career

- Walk the path that OSINT takes you. Learn and grow!

OSINT: The gateway drug your mom never told you about.

Takeaway/Summary

OSINT: The gateway drug your mom never told you about.

Takeaway/Summary

- Get involved with OSINT, in whatever form, you are probably doing it already!
- Scared? Remind yourself of the easy of entry and take a swing!
- Remember the ROE
- Tell your friends, family and colleagues about OSINT
- Follow the path where OSINT takes you
- If you like it, keep learning and evolve your skills
- Learn new things

OSINT: The gateway drug your mom never told you about.

Links and Attribution

Wikipedia: https://en.wikipedia.org/wiki/Open-source_intelligence

Look us up!
Hack South

OSINT: The gateway drug your mom never t

Hack South

Events Code of Conduct Posts Categories Tags

Hack South

Home of the ubiquitous South.

We welcome hackers, makers, breakers, security professionals, students - even the curious! Join our Discord community.

- South Africa
- HTB Meetup
- CTFtime
- LinkedIn
- Twitter
- YouTube

DISCORD 103 Members Online

MEMBERS ONLINE

MadBrickHour
AOxSPy
AlanTheBlank
AldeBaran (Allen)
AngusRed, ROOT
aoighost
apb
AtomicNicos
Azeard

Connect

Hack South InfoSec Community

Recent Posts

Those damn hackers hacked my Facebook!

"Don't watch the video I inboxed you, my FB has been Hacked by Hackers!" Seen this before? Seen this more than once? You probably have. Accounts on Facebook have been hacked and taken over by hackers and they are working hard to hack your friends and families accounts... Or have they? Are they really? Who are these Hackers? And whilst we are on this subject, what are Hackers? Read further to understand what is usually actually going on, who is doing all these account takeovers and what the difference is between a Hacker and a criminal actor/criminal.

Public Service Announcement Facebook Instagram Hacked Hackers Passwords 2FA

SARS and the eFiling quagmire with Adobe Flash discontinuation

After many years of faithful service, Adobe announced in 2017 it would discontinue support for Adobe Flash from 31 December 2020 and blocked Flash content from running in Flash Player.Many have been caught unprepared. The South African Revenue Service (SARS) recently announced it would start using its own browser. We aim to tackle the challenge this presents and what to think about and also why with a 2+ year warning things are not in place.

SARS South African Revenue Service

SARS eFiling Adobe Adobe Flash Vulnerability

eNCA Interview on the WhatsApp Privacy Policy Changes

I had the distinct privilege of being interviewed on eNCA yesterday ! eNCA -- a.k.a. e-News Channel Africa -- is the first and most watched news service in South Africa. You can imagine that it came as a bit of a shocker to me to receive a message request in my Twitter DM's from one of their guest bookers, asking me if I'd like to come on and discuss these policy changes. So I decided to do it:

Media Privacy WhatsApp Original Content External

0x04 - Password Cracking

The Hack The Box Meetup is a monthly online event hosted on the first Tuesday of every month by Hack South. The meetup is an opportunity to connect with other InfoSec enthusiasts, learn new tools and tricks, exchange knowledge and of course Hack The Box.

HackTheBox Password Cracking Hashcat John the Ripper

Is that you Hack South? Is this me?

What is Hack South? Many have asked, what is Hack South, why Hack South and where is this all going? This blog will try to lay out the foundation, the activity and the vision for Hack South, Home of the ubiquitous South. We will also highlight some things we are working on, highlight some roles, channels and activities.

Infosec Community Hack South History

Previous 1 2 3 Next

Hack South InfoSec Community

Recent Posts

TraceLabs Missing Persons CTF Podium

A few weeks ago, a rag tag motley crew from Hack South took part in the TraceLabs missing persons CTF as part of conINT 2020. It was our 4th shot as team Hack South, but this time we scored a podium finish and just missed out on 2nd place. This is the story of how we did it, with no case specifics.

TraceLabs OSINT Missing Persons

0x03 - Getting started with Reverse Engineering

This post summarises the Meetup held on 1 December 2020. Agenda An introductory presentation on Software Reverse Engineering. A theory presentation will cover the types of outputs reverse engineers may investigate for CTFs and in practice. De-obfuscation, disassembly and decomplication will be discussed. We will look at the difference between static and dynamic analysis and how to use some of the common tools. The second half of the Meetup will feature two practical challenges: One guided, for attendees to follow along. The second one will be an exercise for attendees to try.

HackTheBox SRE Ghidra gdb

Announcing 0xcon 2020

0xcon 2020 is around the corner! We have some interesting local speakers sharing the hard work they have done over the year, and a privesc challenge that will be interesting to all of us. All of this will be done online due to COVID-19, but we are setting this up to maintain the collaborative nature of the event.

0xcon Announcements

0x01 - First steps towards a foothold

This post summarises the Meetup held on 6 October 2020. Agenda An introductory session focussed on the first step when beginning on a new box: enumeration. A short presentation and a live demo will introduce on the theory and practice of initial enumeration and commonly used tools. Two Hack The Box 1-month VIP vouchers will be awarded to the top two contestants in a multiple-choice quiz! The second half of the Meetup will be dedicated to hacking together on the lab while sharing tips, tricks and advice.

HackTheBox Enumeration Nmap AutoRecon Zerologon

0x00 - Starting from zero on Hack The Box

This post summarises the Meetup held on Tuesday 1 Sept 2020. Agenda An introductory session with the goal of getting everyone to pop a shell with EternalBlue. The backstory of WannaCry will be presented after a quick introduction. Then we will walk through the EternalBlue exploit and help everyone practice it in the HTB lab. Advanced attendees can skip forward to do other boxes on the private lab provided by HTB. The hosts will focus on walking new people through getting registered, set up, connected, and popping that 1st shell.

HackTheBox WannaCry EternalBlue

Previous 1 2 3 Next

Look us up!
Hack South

OSINT: The gateway drug your mom never told you about.

Look us up! Hack South

Hack South

Internet · Cape Town · 181 followers

✓ Following ···

We welcome hackers, makers, breakers, security professionals, students - even the curious! Join our Discord community.

Visit website

Home

About

Jobs

People

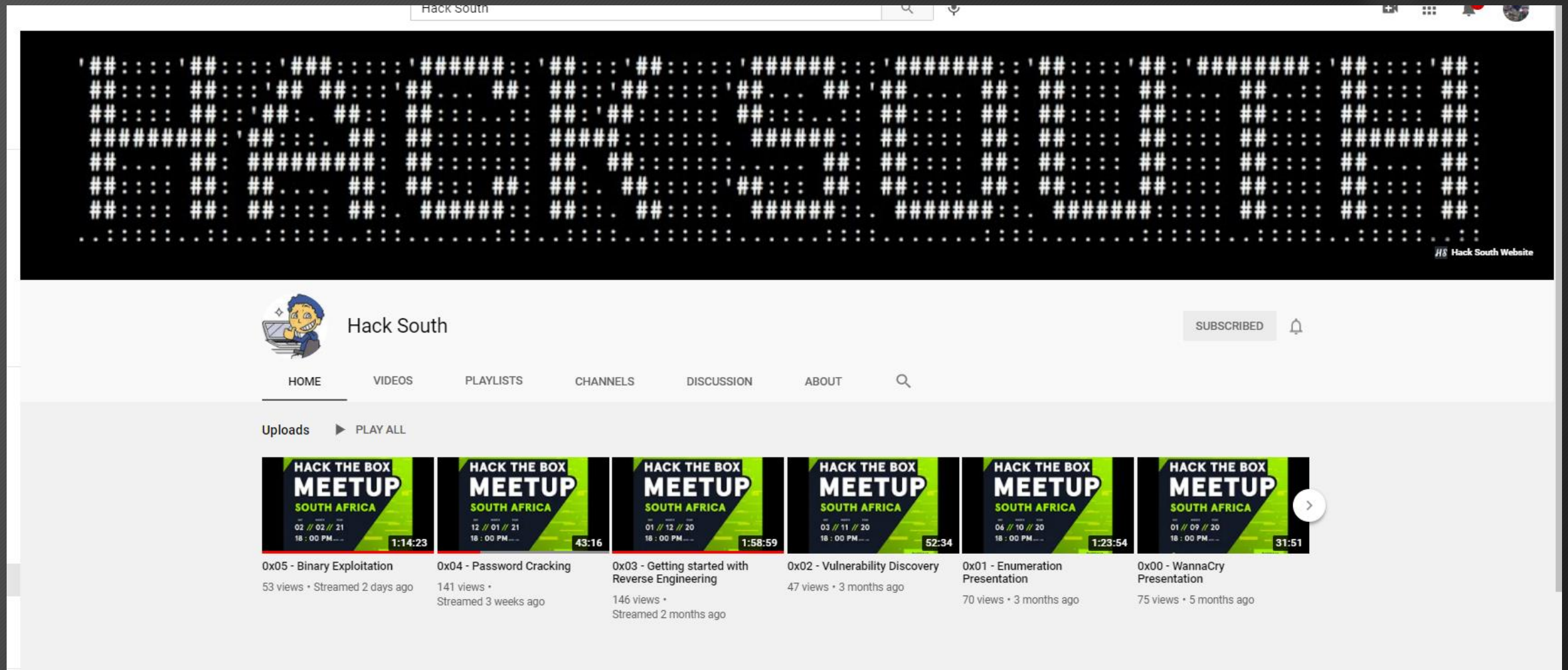
Overview

Hack South is a small community dedicated to information security professionals in South Africa. Whether you are working in Infosec, have an interest in it or just curious, all are welcome!

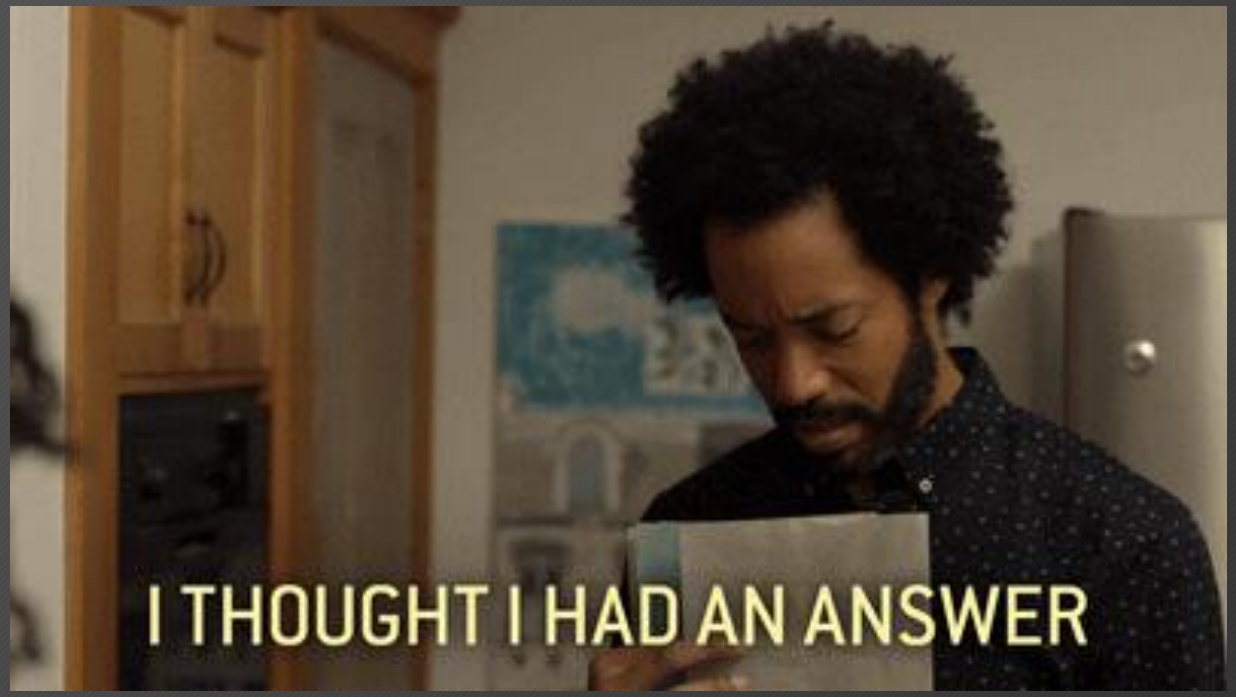
We take part in Capture The Flags, host speakers and help mentor the up and coming talent in this sphere.

Website	https://hacksouth.africa
Industry	Internet
Company size	201-500 employees
Type	Educational Institution
Founded	2020
Specialties	Hacking, HackTheBox, TryHackMe, Mentorship, Learnership, Students, Cyber Security, Information Security, and Memeology

Look us up!
Hack South



Questions?



OSINT: The gateway drug your mom never told you about.

@AngusRedBlue

@hack_south

https://github.com/AngusRed

/in/chwroth/

HTB User/195578

OSINT: The gateway drug your mom never told you about.