

Ethical Student Hackers

OSINT



The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.
- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.
- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.
- Relevant UK Law: <https://www.legislation.gov.uk/ukpga/1990/18/contents>



Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at
<https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf>



OSINT - What is it?

Open **S**ource **I**ntelligence - Using publicly available information to collect details about a person or group



OSINT - What is it?

Open Source Intelligence - collecting valuable insights about an individual , event or group that is free for anyone to access on the internet (public twitters, blog posts, uploaded pictures) or otherwise (publications, phone books)

Uses

- Cyber criminals
- Cybersecurity defense
- Marketing



FAMOUS EXAMPLES

In November 2017 more than 3 trillion individual GPS data points were released by Strava (A sports social media) of every single activity uploaded as a heatmap.

This was very pretty and intriguing but also terrible for operational security. For example US international bases were easily visible and easy to map due to there being not many other strava users in certain areas e.g Syria, Afghanistan

One cyclist mapped out the whole west side of the famous area 51.

After all of this happened. Many people would have had to sit through some very stern talking tos from their leadership



WHY?

OSINT allows us to monitor everything in real time completely **legally** and **ethically**.

In everyday life the information we empower ourselves with can give us the slight edge in such a media driven world. As well as verifying the authenticity of sources and info given by others.

It equips us decision makers to make better, more informed decisions by monitoring and analyzing public opinions and sentiments.

As ethical hackers we can use OSINT to investigate potential security threats or vulnerabilities to prepare an attack.

It can also enhance traditional intelligence gathering which can prepare us for a social engineering attack and help us make better decisions later on in the attack.



USEFUL WEBSITES/TECHNIQUES

<https://archive.org/web/> - A wayback machine that allows us to view previous versions of websites

<https://www.192.com/> - A UK based directory of People, businesses, electoral data and property info

Social media + search engines - Information about everyone + everything. Advanced search and filtering options can be particularly useful

Government websites - provide access to public records. E.g Companies house



PRACTICAL

DAVID BECKHAM.

1. What primary school did he attend
2. Where did he meet his partner?
3. Where was he on the 27th of March 2023?
4. What date + time did he purchase his website?



Clue

He didn't purchase the website himself - his agent at SFX sports did



Shodan

the world's first search engine for Internet-connected devices

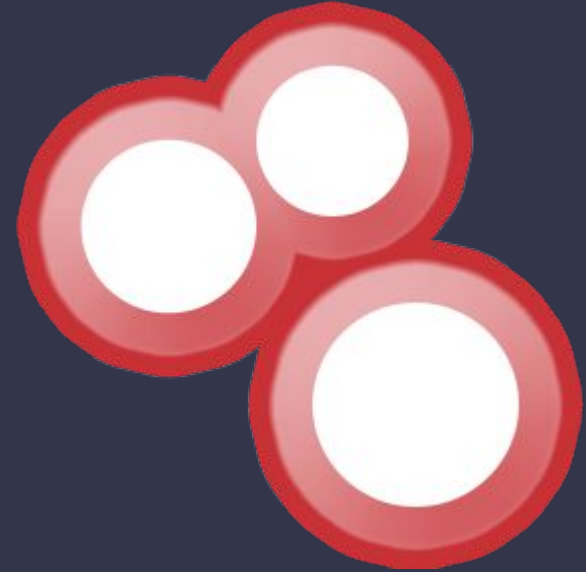
Works by randomly finding IPs and testing a random port

Used by defenders to understand what's publically available

Shodan interacts with only services running on the devices

Helps identify vulnerable services

```
Copyright: Original Siemens Equipment
PLC name: S7_Turbine
Module type: CPU 313C
Unknown (129): Boot Loader          A
Module: 6ES7 313-5BG04-0AB0 v.0.3
Basic Firmware: v.3.3.8
Module name: CPU 313C
Serial number of module: S Q-D9U083642013
Plant identification:
Basic Hardware: 6ES7 313-5BG04-0AB0 v.0.3
```



Maltego

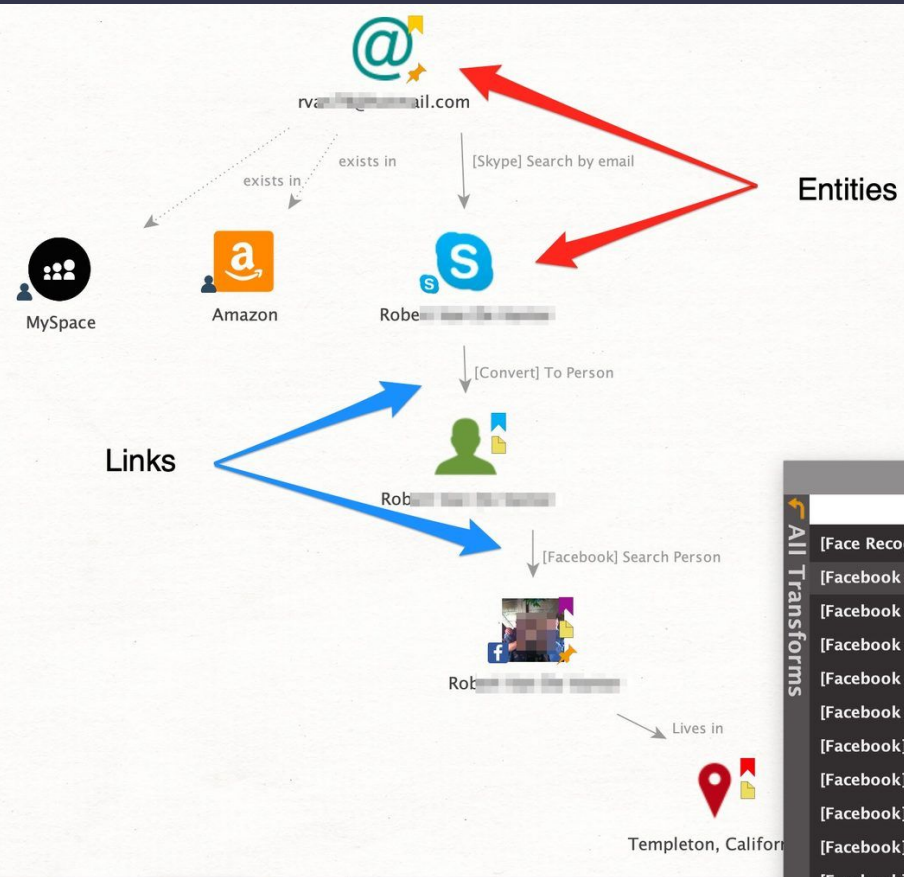


- On kali
- Gathers data on an entities and graphically represents its relationships
- Run functions on entities
- Create your own

Example Functions

- Facebook search , Facebook friends
- whois lookup
- DNS lookup





Entities

Links

Run Transforms

- All Transforms
- [Face Recognition] Search
- [Facebook F] Friends
- [Facebook MF] Create additional MF entities
- [Facebook MF] Create Mutual Friends Entity
- [Facebook MF] Search Relations
- [Facebook MF] To FB profiles
- [Facebook] Followers
- [Facebook] Get User Albums
- [Facebook] Get User Details
- [Facebook] Get User Posts
- [Facebook] Pages Liked by User



Google Advanced Search

Taking advantage of advanced search features on google to find vulnerables indexed websites.

Examples:

Intitle:'login'

filetype:'.mp4'

Find .env files, password files, etc.

List of commands of exploit db

```
intitle:index.of jpg
```

Finds sites image directories



DON'T BREAK THE LAW



()	Group a set of words/operators separately (gun pistol) ammo
-	Exclude results including this word chicago baseball -cubs
\$	Search for a certain price "apple watch" \$299
cache:	Most recent cached version of a domain cache:boston. gov
filetype:	Only search for specific filetype, ext: works the same filetype:pdf "confidential" or ext:pdf "confidential"
related:	Search for sites related to a domain related:sony.com
intitle:	Find pages with a term in the page title intitle:sabotage
inurl:	Find pages with a term in the url inurl:private
around(x)	Find pages with terms in X words proximity of each other microsoft (7) surface
info:	Sometimes shows related pages, cache date etc. in- fo:chicago.gov



Images - Location

- Reverse image search to find the image
 - <https://tineye.com/>
 - <https://images.google.com/>
- Find similar images
 - Google lens
- Look for clues in the image
 - Signs
 - Buildings
 - Terrain
- Location Metadata



Images - Metadata

- What is metadata
- Types of data
 - How
 - Where
 - When
- Tools
 - Properties in photo viewer
 - Special tools (exiftool etc.)
 - Online tools



Practical

<https://shefesh.com/pictures>

<https://shefesh.com/passport>

https://shefesh.com/medical_form

Mug challenge: https://shefesh.com/assets/images/location_mug.png

First person to send the location of the the user by email to ethicalhackers@sheffield.ac.uk wins the mug.



EGM Reminder

Apply via the google form sent out via email or Discord.



Upcoming Sessions

What's up next?

www.shefesh.com/sessions

16th October: Reconnaissance/Enumeration

EGM

Kali Virtual Machine

Bartolome House DB13

23rd October: Policing in the Digital Age - Guest Talk

Diamond Workroom 2

Any Questions?



www.shefesh.com
Thanks for coming!

