# Ethical Student Hackers

## Open Source Intelligence (OSINT)

SHEFFIELD Ethical Student Hackers

Breaking into security.

# 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.

# 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

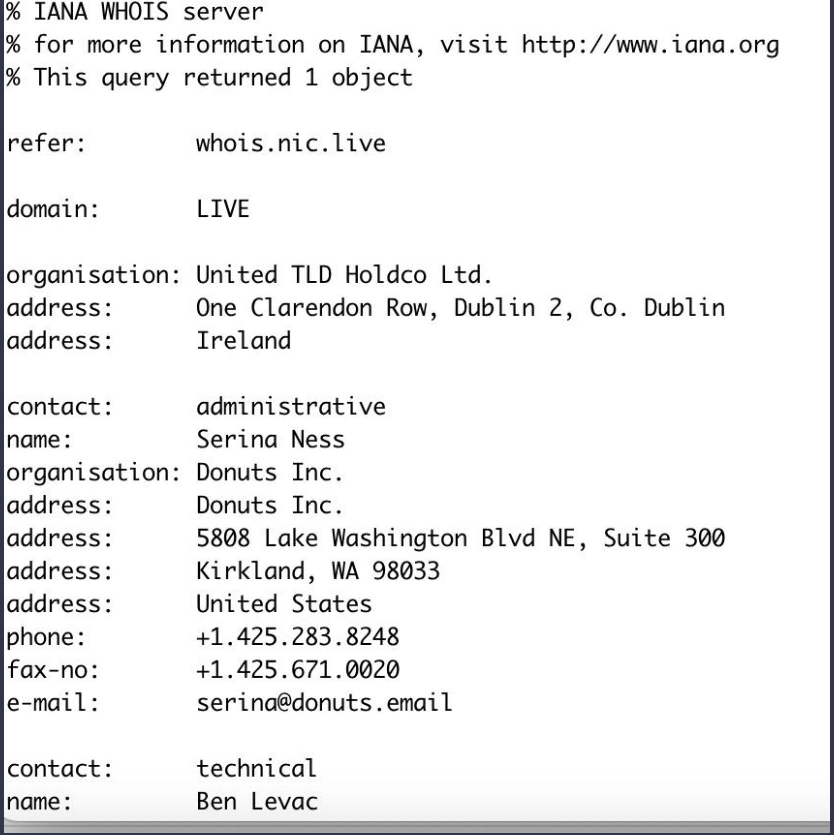
# OSINT - What is it?

**O**pen **S**ource **Int**elligence - collecting information about a person 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

# Online Presence



```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.nic.live

domain:       LIVE

organisation: United TLD Holdco Ltd.
address:      One Clarendon Row, Dublin 2, Co. Dublin
address:      Ireland

contact:      administrative
name:         Serina Ness
organisation: Donuts Inc.
address:      Donuts Inc.
address:      5808 Lake Washington Blvd NE, Suite 300
address:      Kirkland, WA 98033
address:      United States
phone:        +1.425.283.8248
fax-no:       +1.425.671.0020
e-mail:       serina@donuts.email

contact:      technical
name:         Ben Levac
```

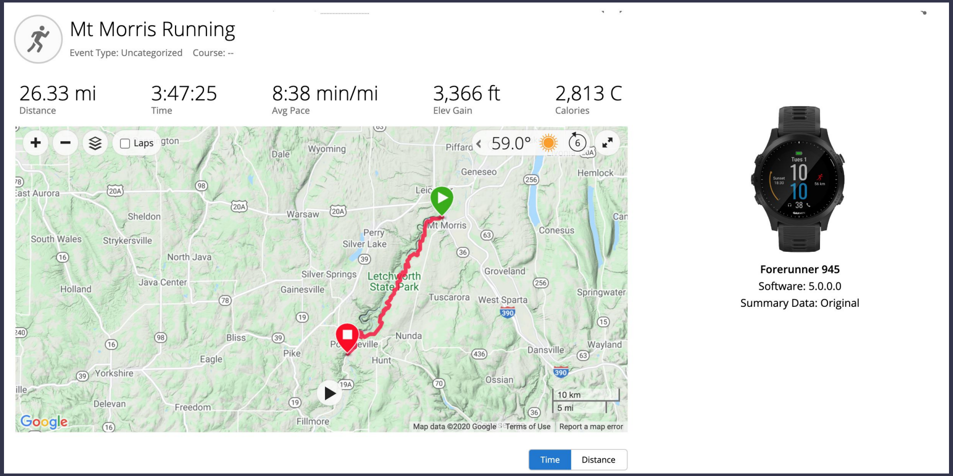
- Image Locations
  - Jeffrey's Image Metadata Viewer
  - Reverse Image Search
- Habits and associations
  - Fb-sleep-stats
  - Location when you post
  - Private info eg Tony Abbott’s boarding pass
  - Usernames can be tracked
- IP Address
  - Location
  - WHOIS
  - ExoneraTor

# Online Presence

- Criminal records
- Vehicles
- Gaming platforms
- Reverse phone lookup
- Wayback Machine
- Search Facebook uses based on school, interested in , etc. (https://searchisback.com/)
- https://spoonbill.io/ (tracks twitter profile changes)
- Wordpress or Blogger
- Advanced Twitter search
- Google Maps

# Garmin and Relive

By making information shareable via public links the data becomes available to anyone who knows how to search it.



Mt Morris Running

Event Type: Uncategorized Course: --

26.33 mi Distance

3:47:25 Time

8:38 min/mi Avg Pace

3,366 ft Elev Gain

2,813 C Calories

Forerunner 945

Software: 5.0.0.0

Summary Data: Original

Relive

- share a map of your travels

Garmin

- Can see people's activities
- May reveal home location if they start running there

# Shodan

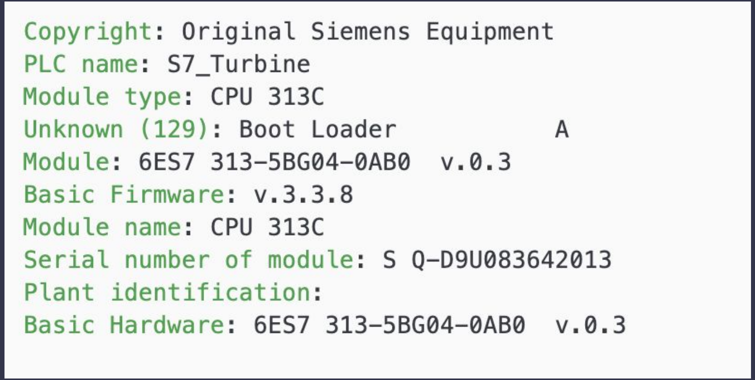
*the world's first search engine for Internet-connected devices*

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



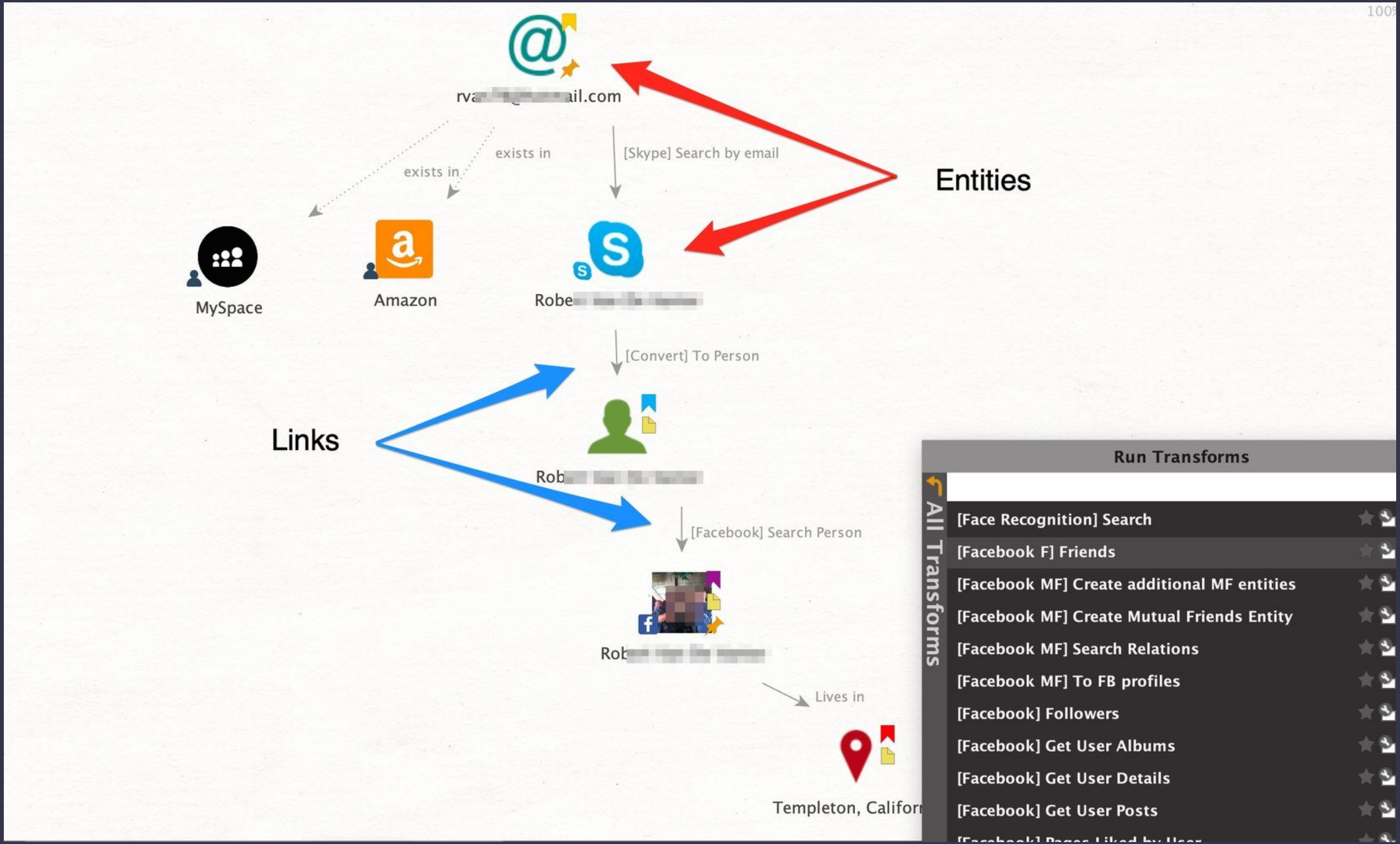
```
Copyright: Original Siemens Equipment
PLC name: S7_Turbine
Module type: CPU 313C
Unknown (129): Boot Loader           A
Module: 6ES7 313-5BG04-0AB0  v.0.3
Basic Firmware: v.3.3.8
Module name: CPU 313C
Serial number of module: S Q-D9U083642013
Plant identification:
Basic Hardware: 6ES7 313-5BG04-0AB0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


rva[redacted]il.com
exists in
exists in
[Skype] Search by email
MySpace
Amazon
Robe[redacted]
[Convert] To Person
Rob[redacted]
[Facebook] Search Person
Rob[redacted]
Lives in
Templeton, Califor
100
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

Entities

Links

# Google Dorks

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

Examples:

Intitle:’login’

filetype:’.mp4’

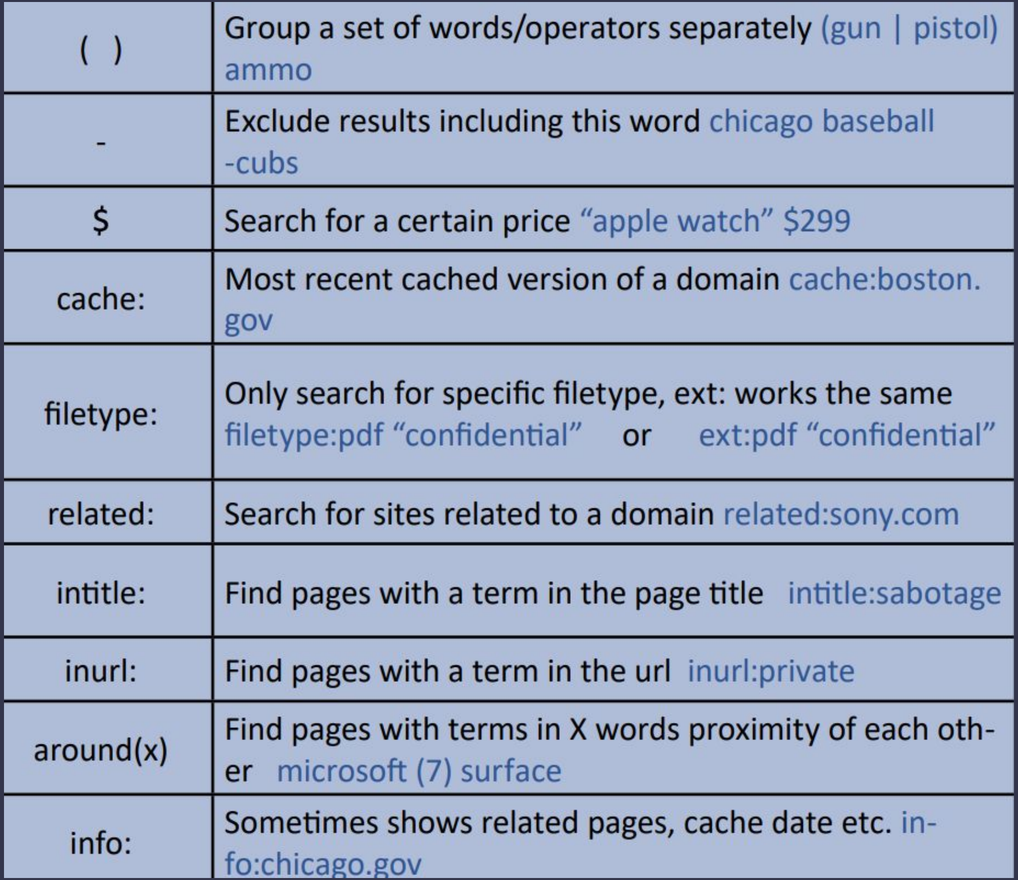
Find .env files, password files, etc.

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. info:chicago.gov |

# To Find Out More:

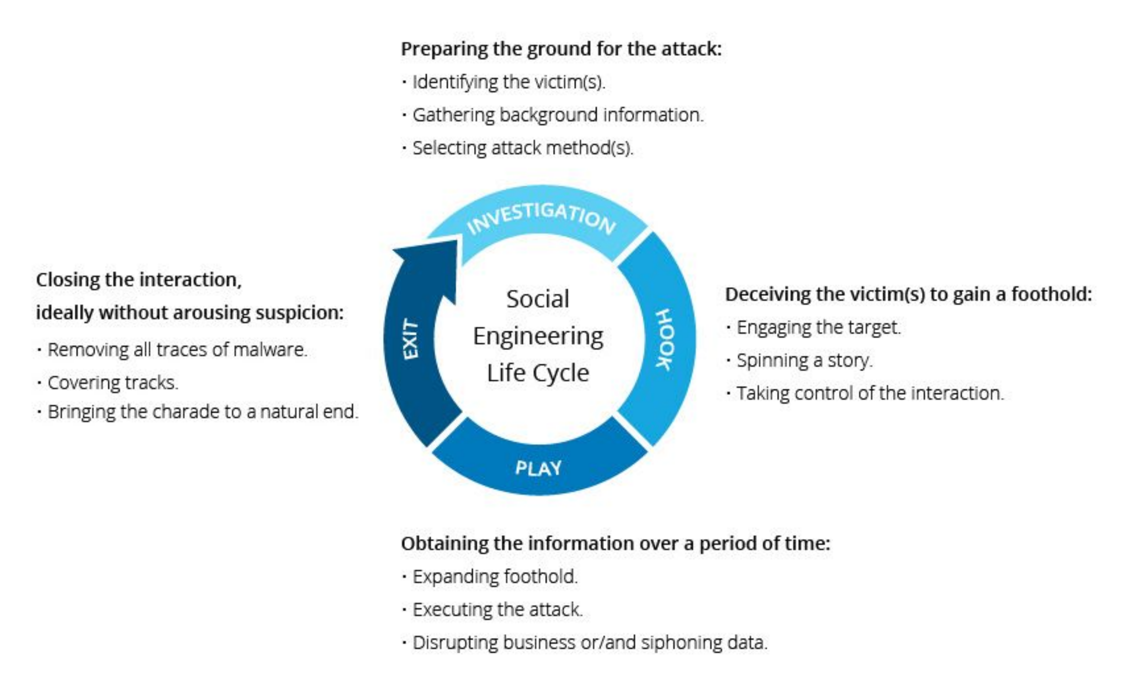
- Week In OSINT Blog: sector035.nl
- OSINT Cheatsheets
- Bellingcat, online news and guides
  - https://www.bellingcat.com/category/resources/how-tos/?fwp_tags=osint

SHEFFIELD Ethical Student Hackers

Breaking into security.

# Social Engineering

- Tricking someone into divulging information or taking action, usually through technology
- Take advantage of a potential victim's natural tendencies and emotional reactions.



**Preparing the ground for the attack:**

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).

**Deceiving the victim(s) to gain a foothold:**

- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

**Obtaining the information over a period of time:**

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

**Closing the interaction, ideally without arousing suspicion:**

- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.

# Baiting / Quid Pro Quo

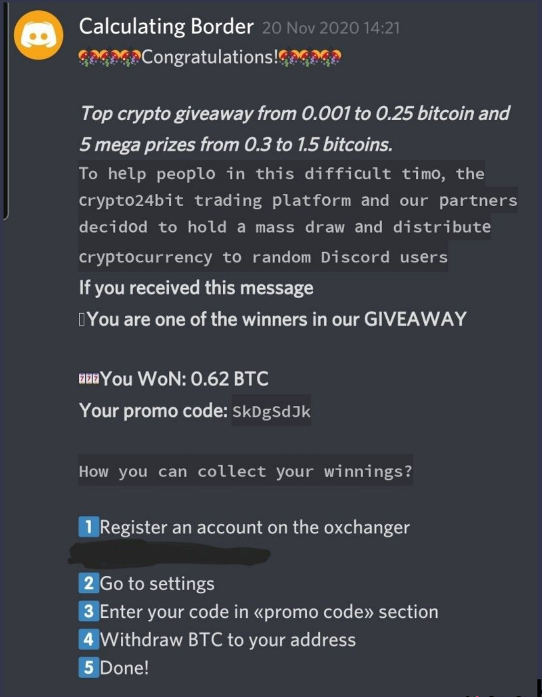
*Someone at Microsoft said the weakest link in cybersecurity is* [*human*]

## Baiting

- Promises an item or good to entice victims
- Can be free music, movie download, torrent files
- Also can be physical exploiting human curiosity
    - USB stick in the bathroom, office floor or lift

## Quid Pro Quo

- Similar to baiting, but it promises services
- Impersonate to be an IT consultant or customer support trying to get credentials of victims
- It can take a form of survey



Calculating Border 20 Nov 2020 14:21

🎉🎉🎉🎉🎉🎉Congratulations!🎉🎉🎉🎉🎉🎉

***Top crypto giveaway from 0.001 to 0.25 bitcoin and 5 mega prizes from 0.3 to 1.5 bitcoins.***

`To help peoplo in this difficult timo, the crypto24bit trading platform and our partners decidod to hold a mass draw and distribute cryptocurrency to random Discord users`

**If you received this message**

**□You are one of the winners in our GIVEAWAY**

🎰**You WoN: 0.62 BTC**

**Your promo code:** `SkDgSdJk`

`How you can collect your winnings?`

1️⃣Register an account on the oxchanger

[redacted]

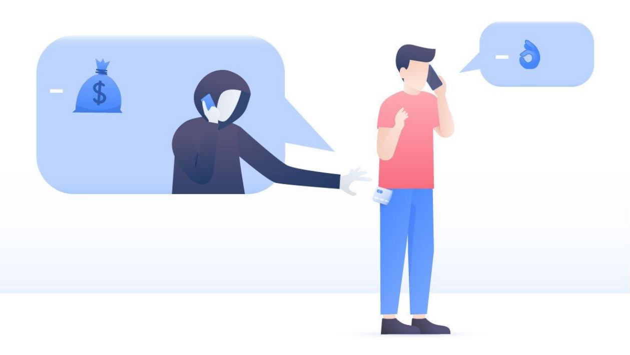
2️⃣Go to settings

3️⃣Enter your code in «promo code» section

4️⃣Withdraw BTC to your address

5️⃣Done!

# Pretexting / Vishing / Tailgating



## Pretexting

- Preys on human’s desire to trust
- Requires a lot of research on the part of a scammer to make it plausible for the victim to believe
- Pretends to be an employee from another branch, an auditor, or a new employee

## Vishing

- Same as phishing but over the phone

## Tailgating

- Used to gain access to a secure building by blending in

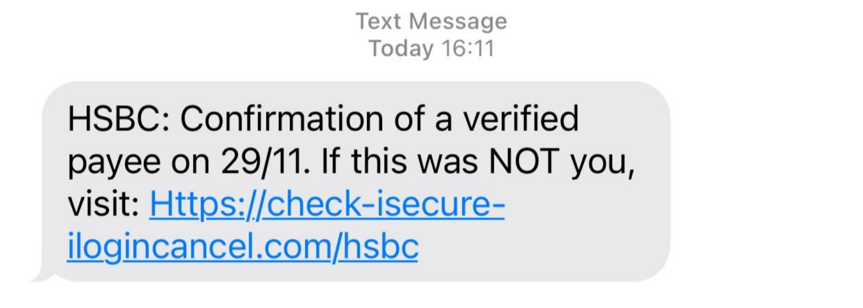
SHEFFIELD Ethical Student Hackers

Breaking into security.

# Phishing

The most common social engineering technique

- Obtain personal information such as names, addresses and Social Security Numbers.
- Use shortened or misleading links that redirect users to suspicious websites that host phishing landing pages.
- Incorporate threats, fear and a sense of urgency in an attempt to manipulate the user into responding quickly.

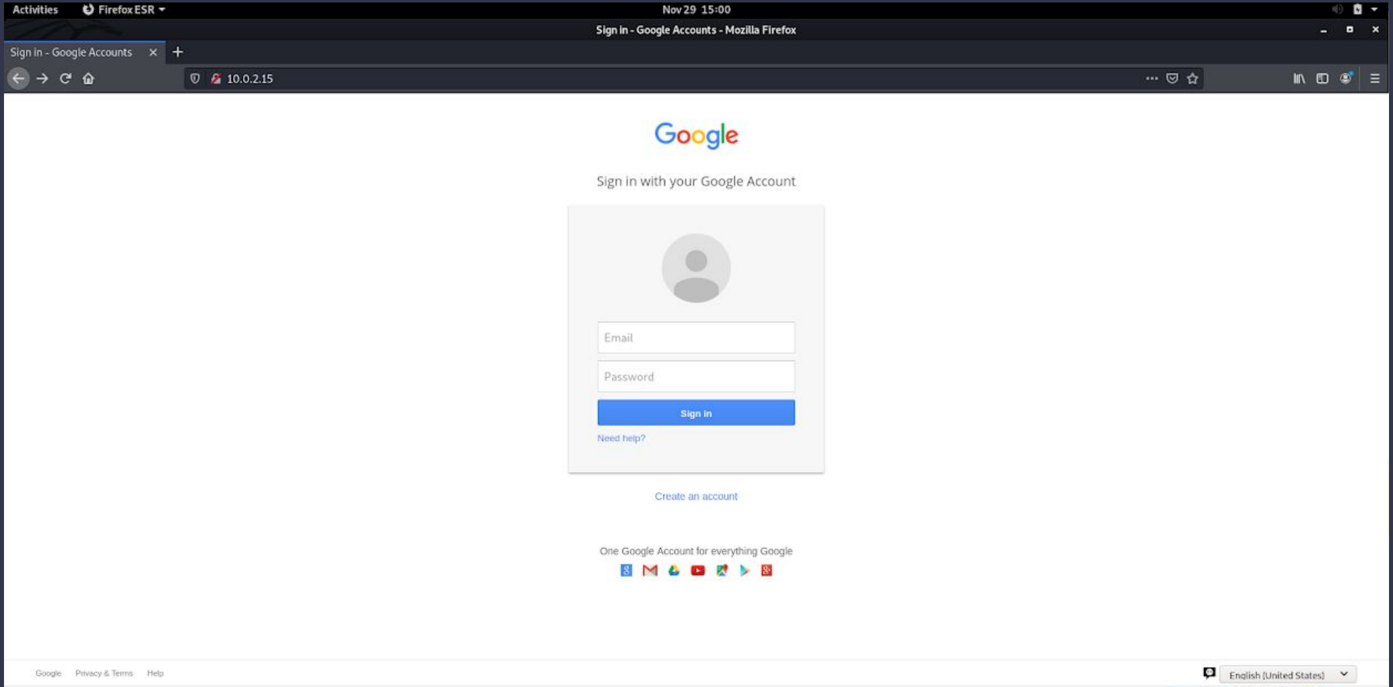


Text Message
Today 16:11

HSBC: Confirmation of a verified payee on 29/11. If this was NOT you, visit: Https://check-isecure-ilogincancel.com/hsbc

SHEFFIELD Ethical Student Hackers
Breaking into security.

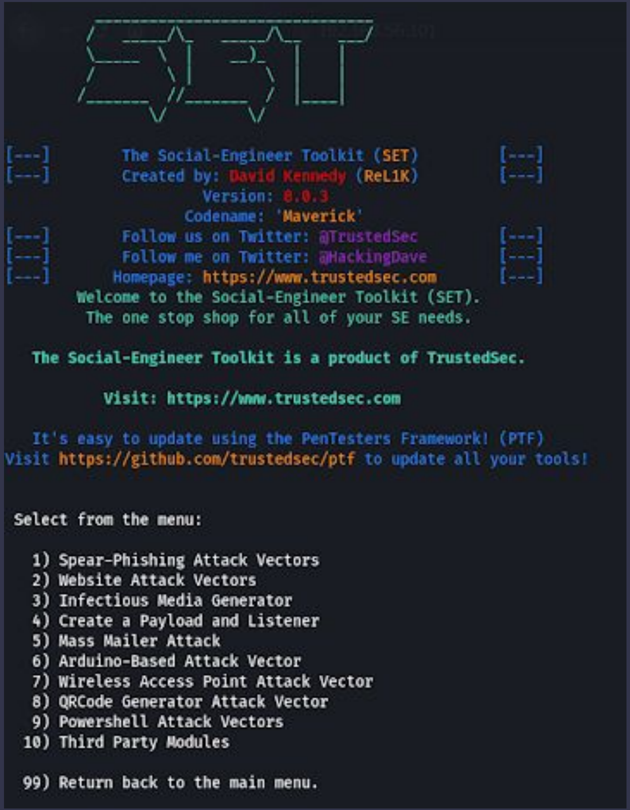
# Credential Harvester Attack



SHEFFIELD Ethical Student Hackers

Breaking into security.

# Social Engineering Toolkit (SET)



```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.
```

- Open source python tool aimed at penetration testing around social engineering
- Installed on kali, can be installed on Linux and Mac machines

https://github.com/trustedsec/social-engineer-toolkit

# msfpc

- Tools that generate various payloads based on user-specific options
- Automate the processes involved in working with Metasploit and msfvenom
- Instructions with msfpc -h

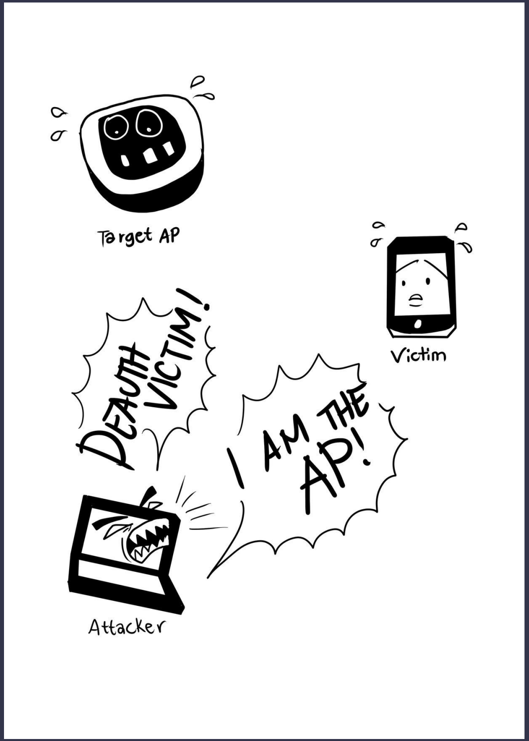
Automatically generate a Windows reverse Meterpreter payload, using the IP address of the eth0 interface as the LHOST parameter.

- msfpc windows eth0

Semi-interactively create a Windows Meterpreter bind shell on port 5555.

- msfpc windows bind 5555 verbose
- msfpc linux
- msfpc apk

# Wifiphisher



Need USB WiFi Adapter to use this tool… :(

- Achieve a man-in-the-middle position against wireless clients by performing targeted Wi-Fi association attacks
- Mount victim-customized web phishing attacks against the connected clients in order to capture credentials (e.g. from third party login pages or WPA/WPA2 Pre-Shared Keys)
- Infect the victim stations with malwares.

Uses a number of techniques to obtain a man-in-the-middle position

- Evil Twin
- KARMA
- Beacons

https://github.com/wifiphisher/wifiphisher

# OSINT CTF

*-> Use techniques covered together to find out about someone in the opposite group*

# Upcoming Sessions

What's up next?

www.shefesh.com/sessions

30th Nov – OSINT

7th Dec – Hack the Box

14th Dec – Xmas Session

# Any Questions?

www.shefesh.com

SHEFFIELD Ethical Student Hackers

Breaking into security.