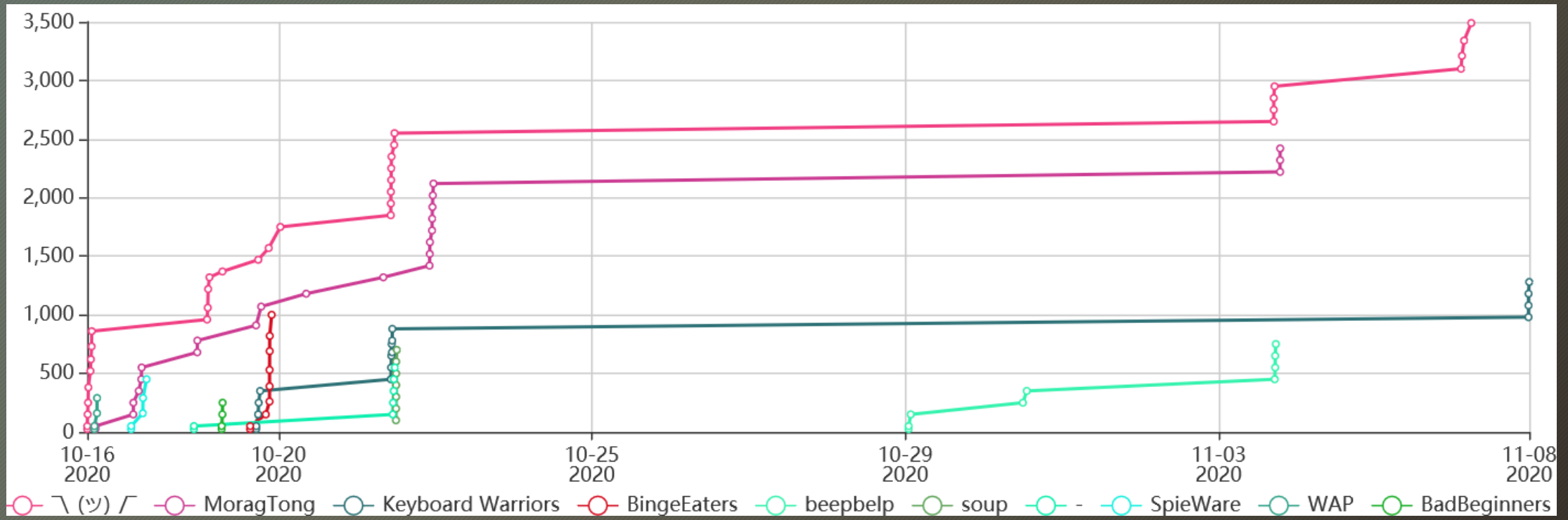
OSINT & Social Engineering

Coventry University ComSec

By Jack Orcherton

Update

- New HOPR challenges on CTFd!
- Catch up with Richie!

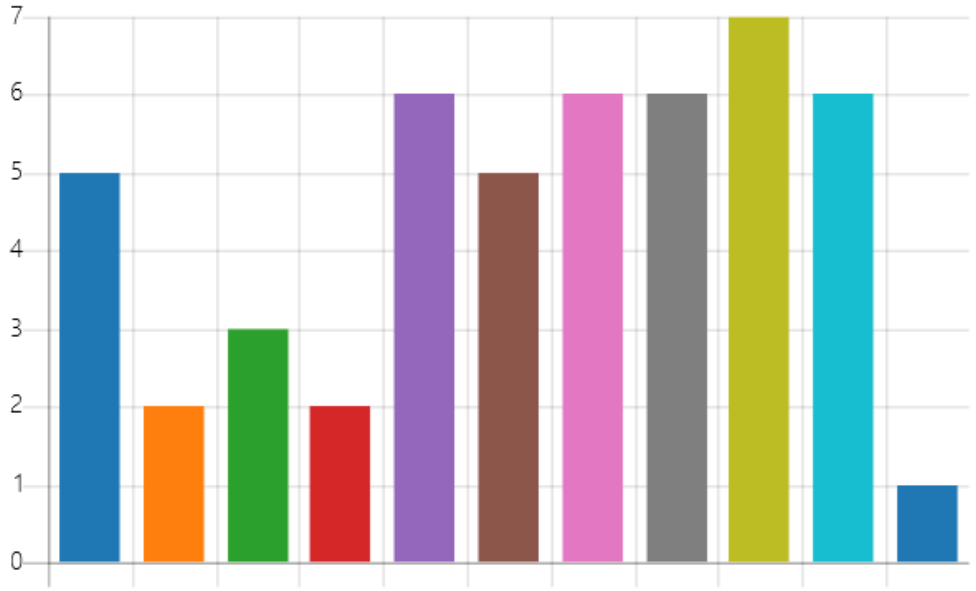


This Week By Popular Demand

10. What topics would you like to be covered in ComSec?

More Details

Metasploit	5
Password Cracking - brute for...	2
Burpsuite	3
XSS	2
PWN	6
Tools (SQLmap, Nessus, Nikto,...	5
Cryptography	6
Social Engineering	6
OSINT	7
Steganography	6
Other	1



What is OSINT?

- Open Source Intelligence – finding information from publicly available sources.
- Foundation of pentesting (as the more you know about the company you are hacking – the easier it can become)
- Find Information
- Form of passive reconnaissance (so legal)

Good Places to Look

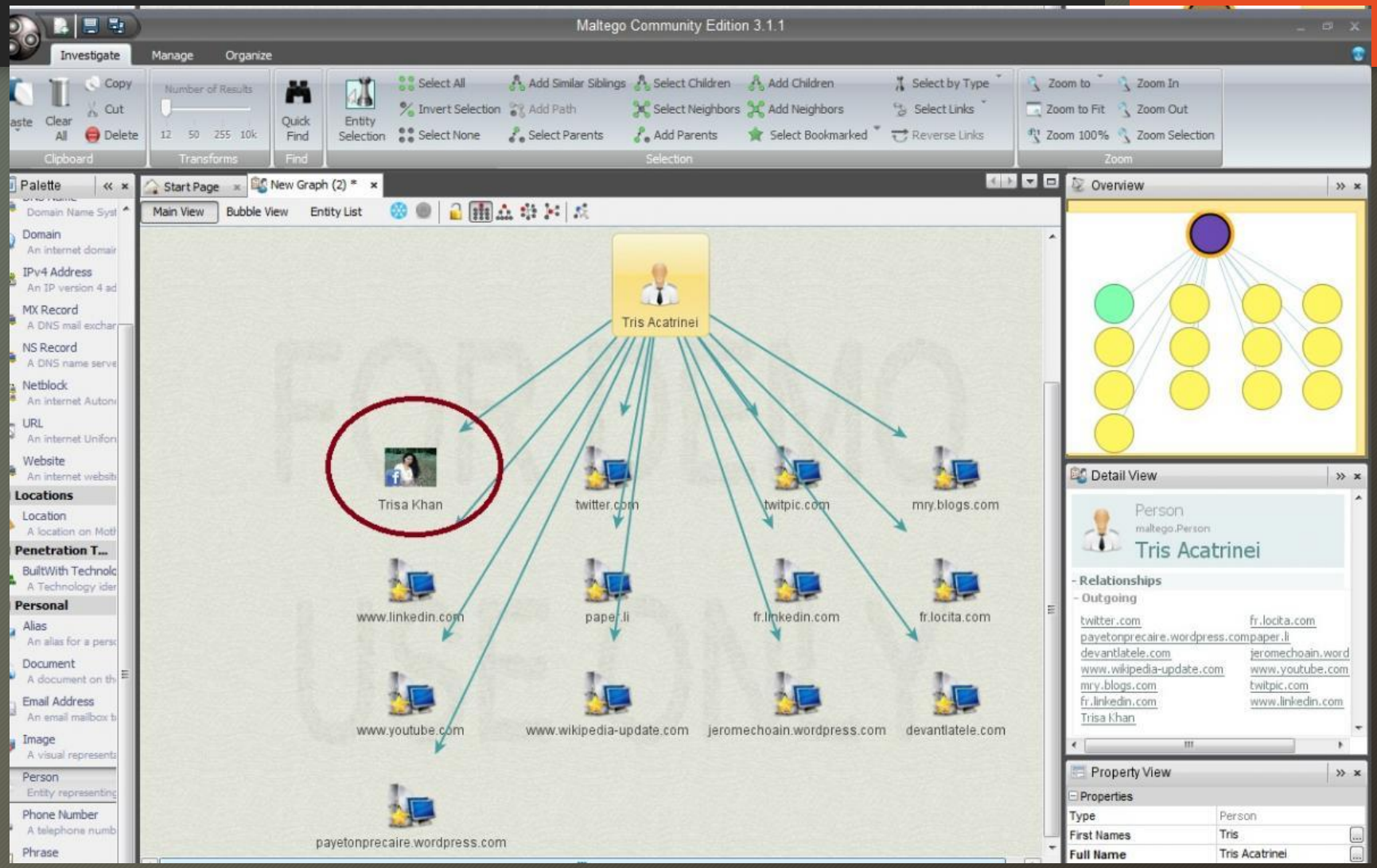
- Google
- Social Media
- Electoral-role
- Companies House
- Wayback Machine
- GitHub Repositories

Image Metadata

- Find an image – check its Metadata:
  - Location data
  - Device type
  - Dates
- What's inside the image?
  - Employee badge number
  - Signs (to tell location)
  - Confidential documents
  - What’s on their computer screen (may give away confidential information/IT programs & systems they use)
  - Faces (can you identify anyone?)
- Exiftool

OSINT Yourself

- Sherlock
- Maltego



Old Websites & GitHub Repositories

- Ever accidently published private information to a website – well it may have been cached by either google or Wayback Machine.
- Ever done the same to GitHub? Check old Git commit history!

Social Engineering

The Hacking of the Mind!

What is Social Engineering?

- The art of faking people into trusting you, or doing things that they would not normally do.
- Normally involves you making people believe you have authority (high Vis Test).
- This is because we like to be trusting and helpful to others (generally). For example, if someone helps you, you are more likely to help them

- A test – pick a random number between 1 & 10!


7

Why it works? Cognitive Bias

- Humans make unconscious decisions, without thinking, there are many different types:
  - Stereotyping
  - ‘Going with the Group’
  - Bias Blindness
  - Matching
  - Social
  - Resistiveness
  - Confirmation Bias

Uses in the real world

- Scams
- Phishing
- Gaining unauthorised access (tailgating)

- See Social Engineering Toolkit

Find our Flags

- OSINT the picture on the website (use the techniques I did).
- Flag hidden in GitHub
- Complete the Office Space challenge on CTFd

Go Further

- Research more cognitive biases
- Look at TraceLabs
- Complete the OSINT room on TryHackMe
- Complete the Google Dorking room on TryHackMe