'What expertise do penetration testers need?'

Student: Pragya Kaushik (a1840097)

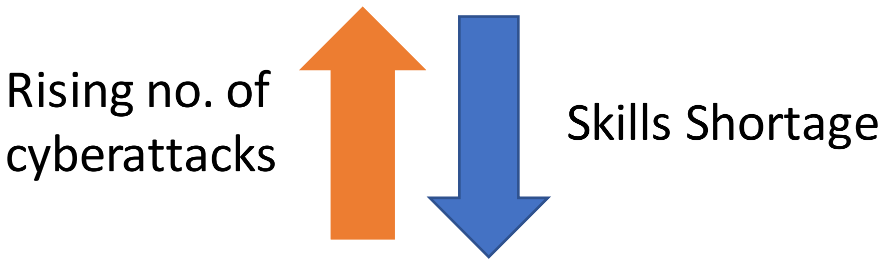
Supervisor: Dr Faheem Ullah

What is a 'penetration tester'?

- a.k.a. a pen tester or ethical hacker
- performs authorized simulated cyberattacks on computer systems, to evaluate their level of security.

Research Question: ‘What expertise do penetration testers need?’

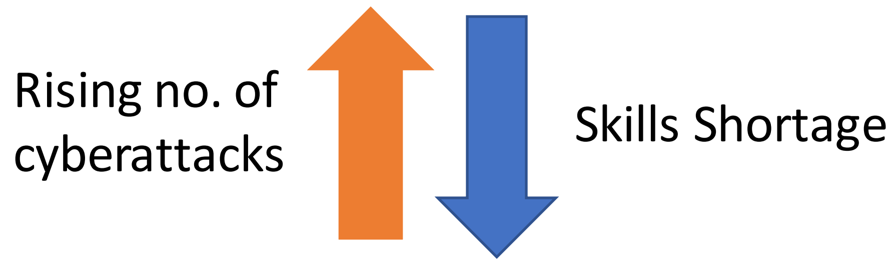
Research Question: ‘What expertise do penetration testers need?’



Rising no. of cyberattacks

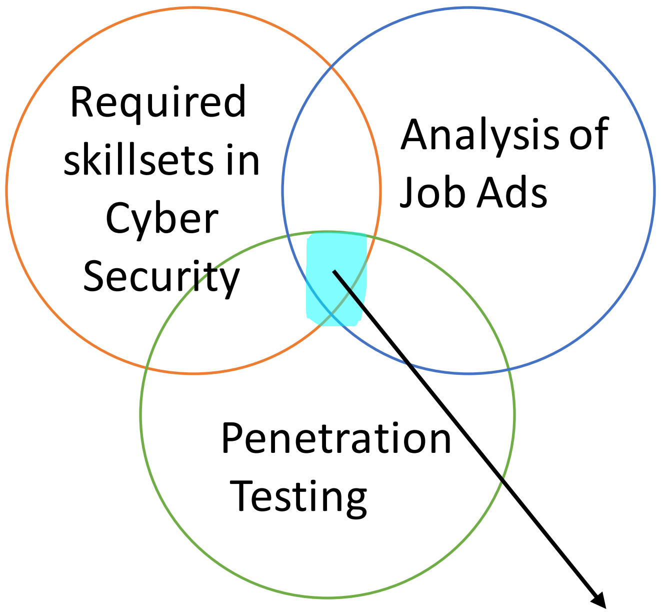
Skills Shortage

Research Question: ‘What expertise do penetration testers need?’



Rising no. of cyberattacks

Skills Shortage



Required skillsets in Cyber Security

Analysis of Job Ads

Penetration Testing

No research has ever been done to identify the required skillsets for the job title of 'penetration tester'.

Australian recruiters believe that penetration testing is:

- second-most technical security skill in demand
- second-most challenging to find

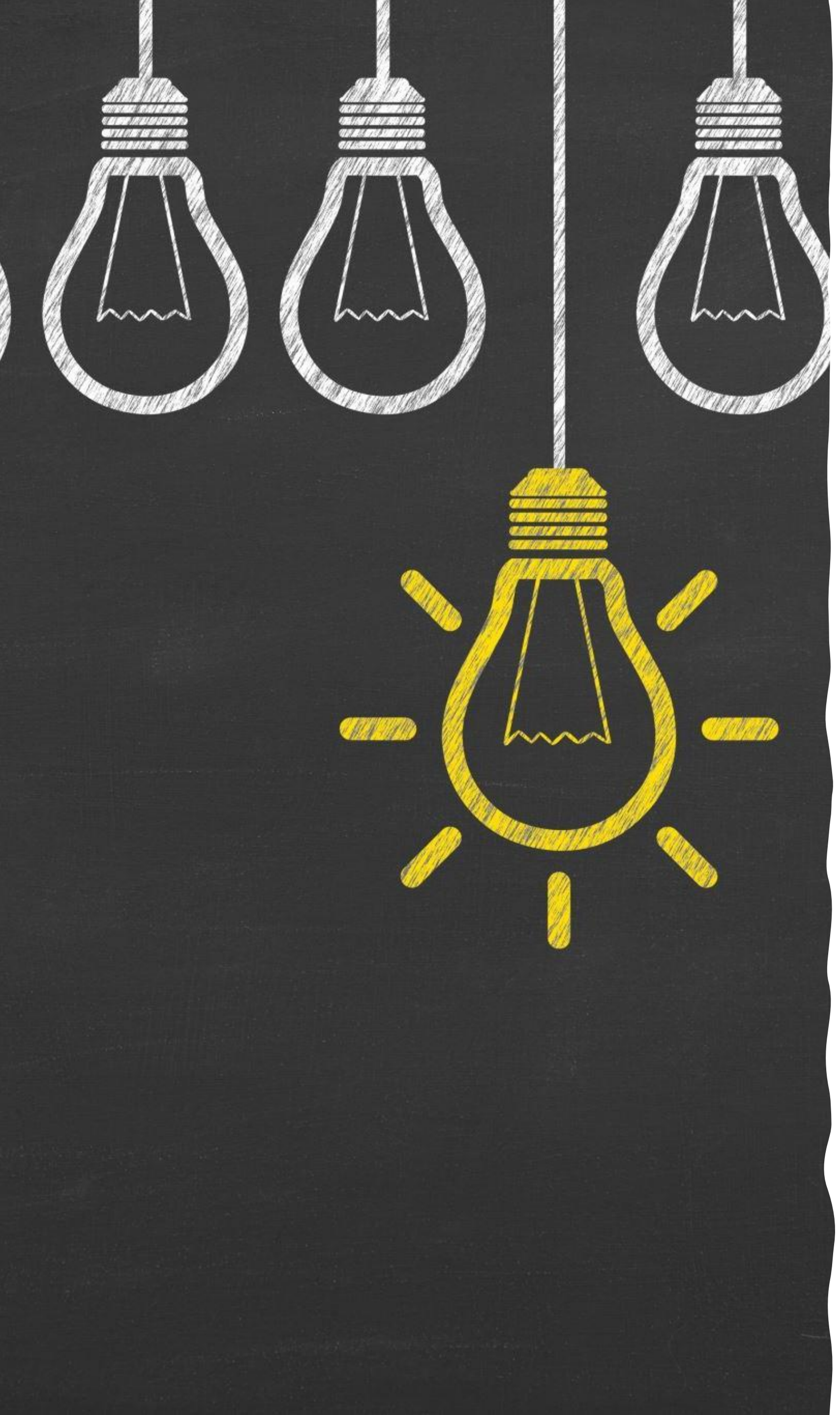
Potential Benefits

Companies - hire the right talent and train existing employees correctly.

Government - develop policies and programs that support the development of the cybersecurity workforce.

Job Seekers - focus their efforts and resources efficiently.

Education institutes - better align their curriculums with the needs of the industry



The Strategy

- Data Analysis on ~500 online job advertisements
- Analyse job descriptions in 7 different categories: technical skills, soft skills, programming languages, tools, professional certifications, as well as the expected level of qualification, and experience.
- Create data visualizations.

Methodology

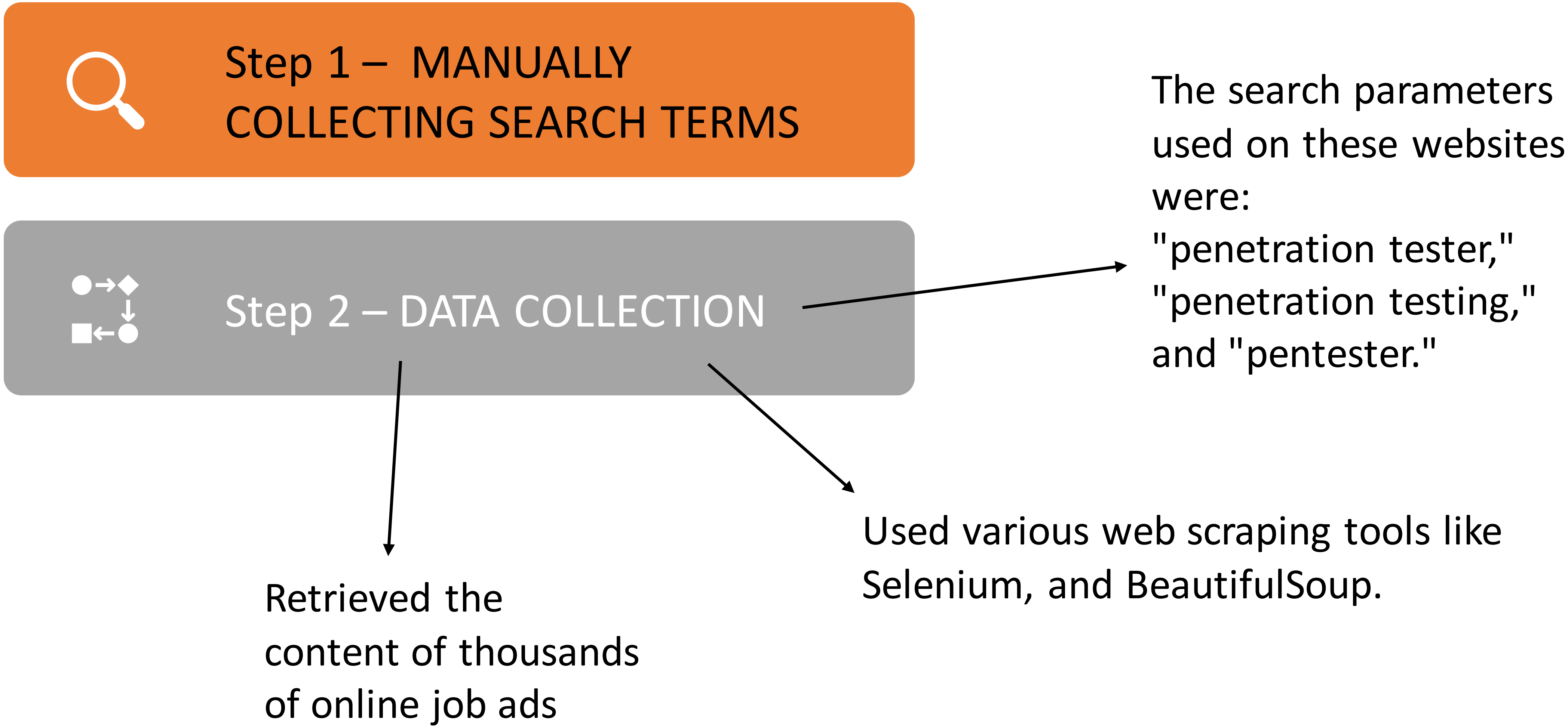
Step 1 – MANUALLY COLLECTING SEARCH TERMS

Looked through 60 job ads to identify the most common terms used for each of the 7 categories.

Search terms served as reference points to analyse and compare job ads based on the presence or absence of these specific terms.

Examples of search terms for the sub-topic of soft-skills include: ‘communication’, ‘leadership’, ‘team’, etc.

Methodology



Step 1 – MANUALLY COLLECTING SEARCH TERMS

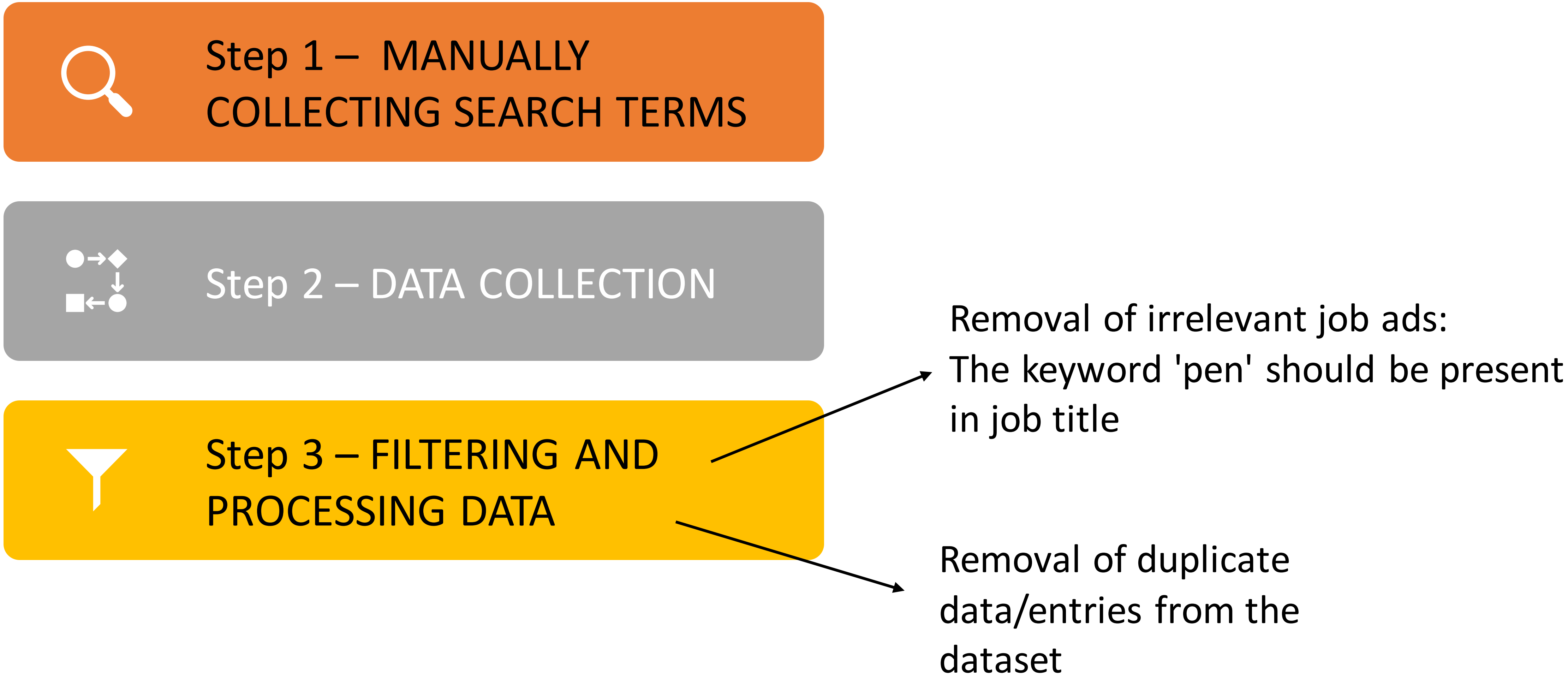
Step 2 – DATA COLLECTION

The search parameters used on these websites were:
"penetration tester,"
"penetration testing,"
and "pentester."

Used various web scraping tools like Selenium, and BeautifulSoup.

Retrieved the content of thousands of online job ads

Methodology



Step 1 – MANUALLY COLLECTING SEARCH TERMS

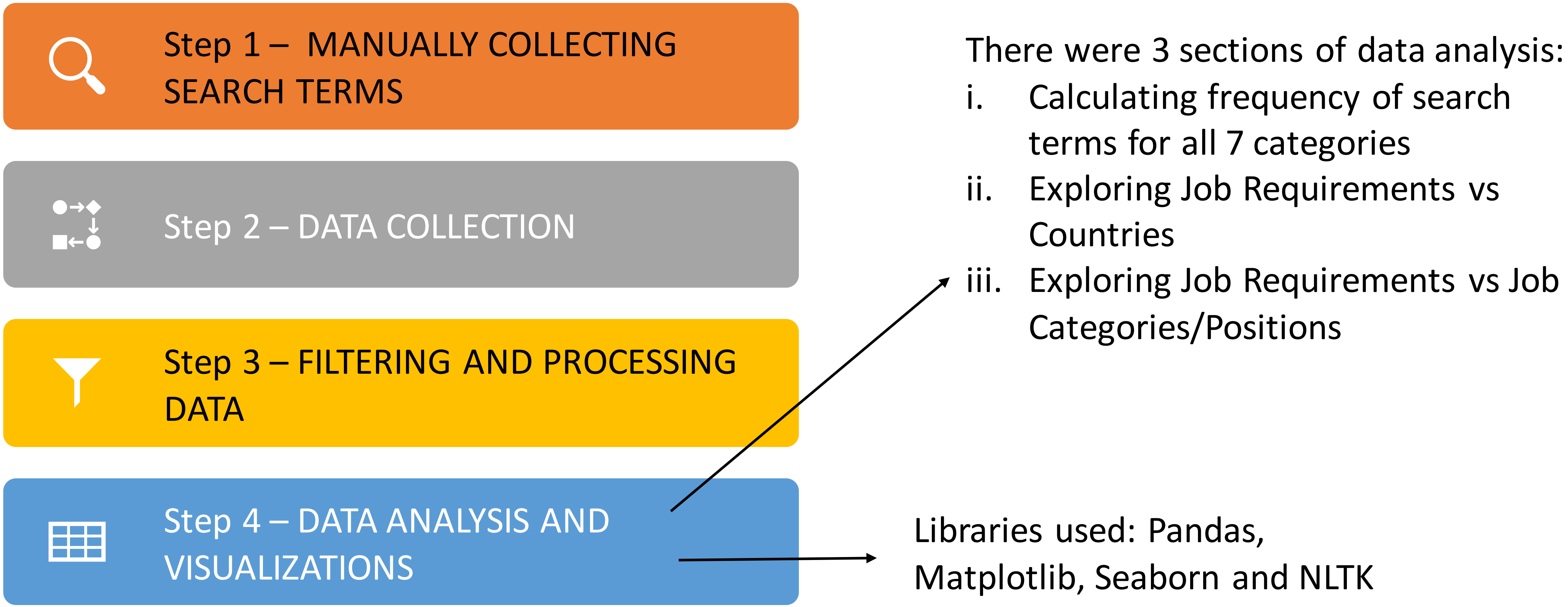
Step 2 – DATA COLLECTION

Step 3 – FILTERING AND PROCESSING DATA

Removal of irrelevant job ads: The keyword 'pen' should be present in job title

Removal of duplicate data/entries from the dataset

Methodology



Step 1 – MANUALLY COLLECTING SEARCH TERMS

Step 2 – DATA COLLECTION

Step 3 – FILTERING AND PROCESSING DATA

Step 4 – DATA ANALYSIS AND VISUALIZATIONS

There were 3 sections of data analysis:

i. Calculating frequency of search terms for all 7 categories
ii. Exploring Job Requirements vs Countries
iii. Exploring Job Requirements vs Job Categories/Positions

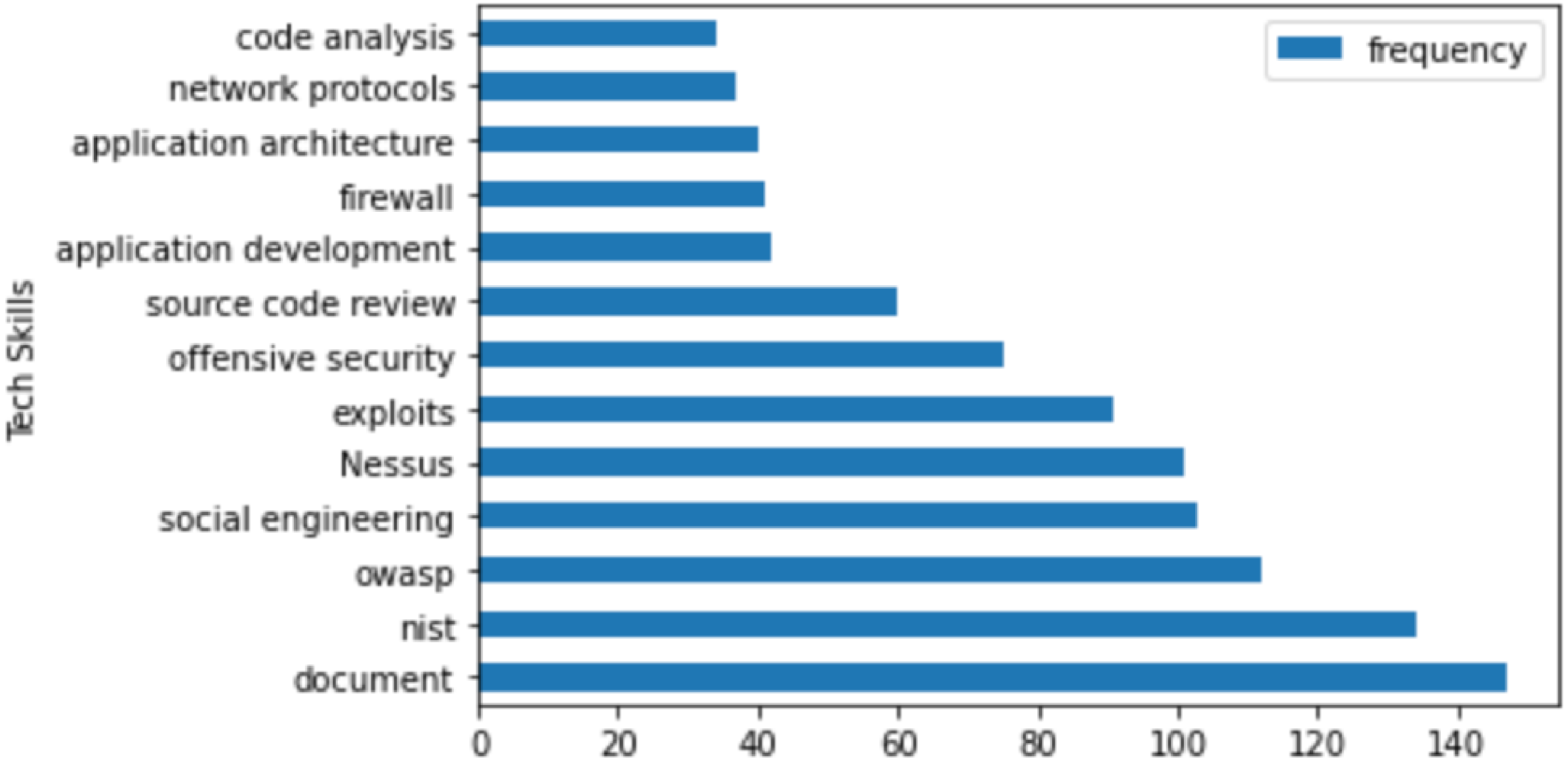
Libraries used: Pandas, Matplotlib, Seaborn and NLTK

Results

> 20 graphs were generated

For this presentation, I’ll share overall observations rather than going through each graph.

1st Section: Frequency of search terms



The graphs look like the one on left.

X-axis: Frequency Count

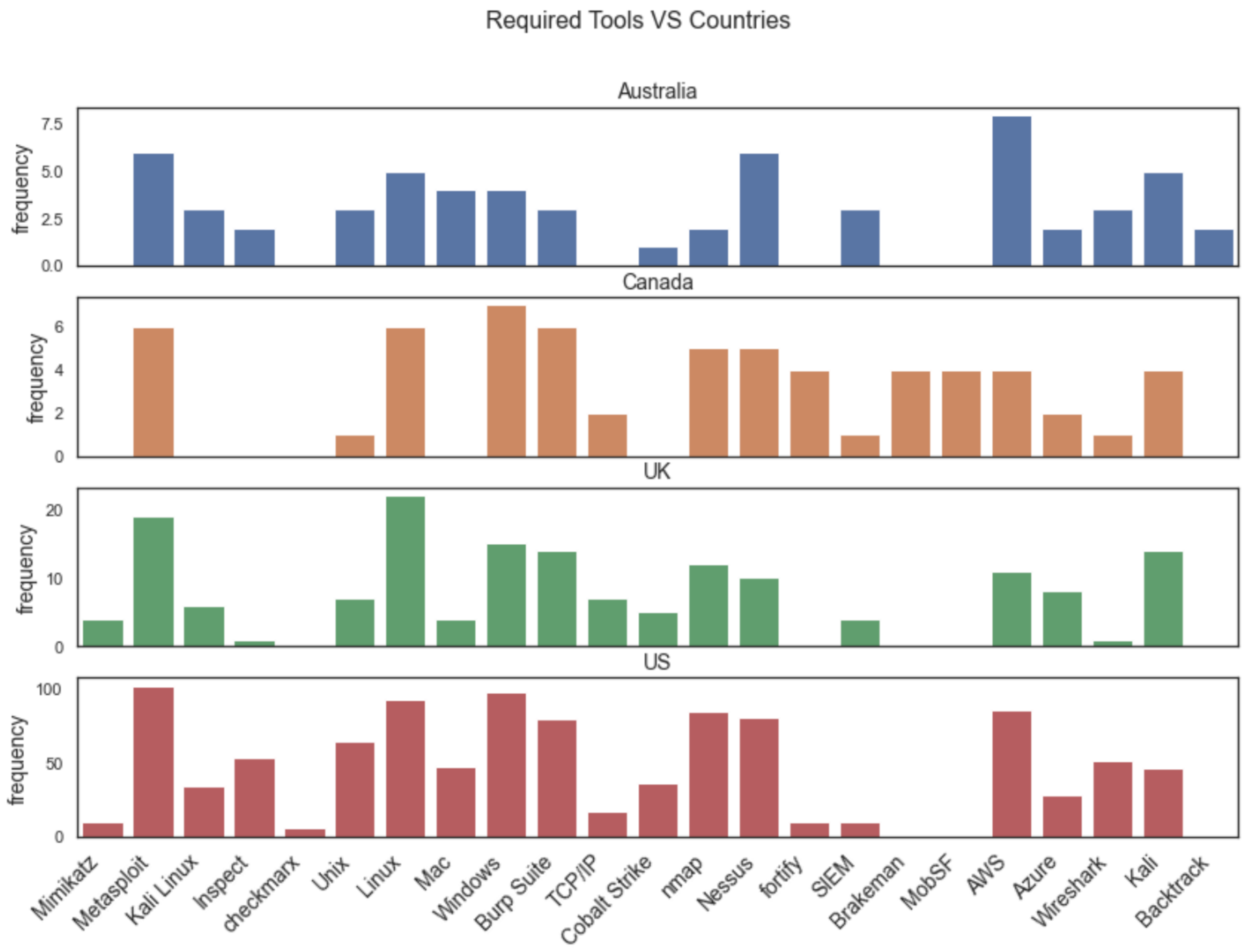
Y-axis: Job Requirement Category

1st Section: Frequency of search terms

Most in-demand required skills/background of each category:

- Technical skills: documentation skills, NIST familiarity, OWASP (web application security)
- Soft skills: teamwork, communication and management
- Expected qualification and experience: A combination of theoretical knowledge (Bachelor's degree) and practical experience (ranging from 1 year to 5+ years)
- Certifications: OSCP (dominant demand), CEH and GPEN
- Programming languages: Go, ASP, Python, Java, and Rust
- Tools: Metasploit, Linux, Windows AWS, and Nmap

2nd & 3rd Section: Job requirements across Countries and Job Categories



The graphs look like the one on left.

X-axis: Search Terms

Y-axis: Frequency Count

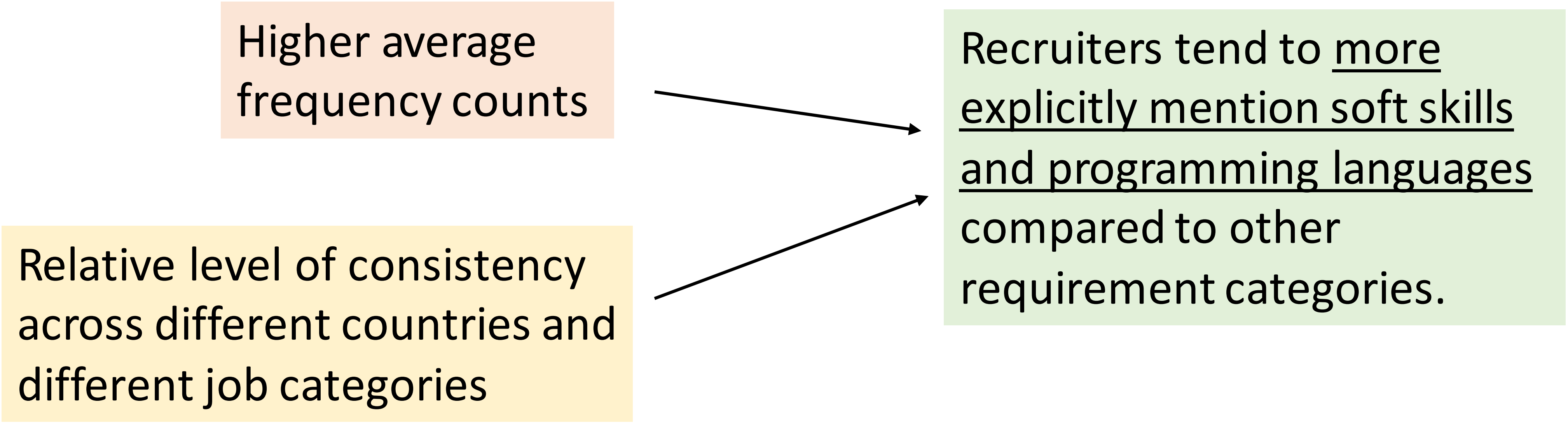
Note: each country or category is displayed as a separate subplot.

2nd & 3rd Section: Job requirements across Countries and Job Categories

- Different countries and different job categories may have distinct technical expertise requirements within the penetration testing field.

- Adapting to these specific skill requirements can enhance one's competitiveness and effectiveness in the pen-testing field.

Further Observations



Higher average frequency counts

Relative level of consistency across different countries and different job categories

Recruiters tend to more explicitly mention soft skills and programming languages compared to other requirement categories.

Potential Solution: To bridge the skills gap → Recruiters should be more specific and explicit about the technical expertise requirements too

Potential Further Research:

- Investigate how the skills in high demand vary across different industries or companies.
- Investigate how demand varies in other geographical locations, e.g. developing countries

Thank you!

Any questions? ☺