

# Advanced Security Assignment 1

---

## Part A

---

Security is a complicated field, to be proficient professionals need to be competent in numerous areas such as

- Reverse Engineering & Analysis

- Network Security
- Risk analysis & Mitigation
- Cryptography
- Computer Forensics
- Penetration Testing

Each of these fields requires in-depth knowledge of the subject matter often far beyond what would be required to program a related application. This can make security an intimidating field to enter for graduates and self-taught individuals.

To address this shortage of Security professionals, many intelligence agencies such as Britain's GCHQ have developed programs to encourage entry to the field at a school level through competitions, hackathons, Capture the flags and general puzzles which identify talent early. Much effort has also been put into attracting women and other underrepresented groups in cyber security through role models and targeted programs.

My own skillset matches quite well with certain fields of Cyber Security, I have a strong knowledge of networking and how the internet functions. This helps with penetration testing & Network security. I also have a strong knowledge of Javascript which helps when attempting XSS attacks & exploiting unsecured APIs.

My primary weaknesses would be a relative lack of knowledge of Cryptography and a lack of experience in programming in low-level languages which an understanding of helps when exploiting networks.

## Part B

---

## Basic Operators

**AND (&):** This is the most used operator, it returns only results which match both the key words. For example Rain AND Wind would return only results that reference both rain and wind.

**OR (|):** This Operator is similar to the AND operator in the sense it takes two keyword arguments. However unlike the AND operator if we were to search for Rain | Wind, the engine would return results that matches both or either of the keywords.

**Exclusion (-):** This Operator excludes a certain term from results. For example Rain - Wind would only return results that mention rain and do not mention wind.

**Synonym (~):** This Operator is used when we wanted to include synonyms, Google however by default includes [synonyms](#).

**Wildcard (\*):** This Operator replaces any missing words with any possible matches. For example "Steve \* Apple" would return results that match Steve Jobs time at Apple as it inserts the missing word Jobs.

**Match (""):** This Operator is used to search for exact matches to the search term, for example searching for the phrase "Let It Shine" will return only results that have that exact phrase in the given order.

## Advanced Operators

**AllInText:** This operator forces the search engine to only return results that contain all the search terms in the text. For example searching "allintext: Cyber Security Training" will only return results that have all 3 terms at least once in the text.

**AllInTitle:** Similar to allintext, this operator only returns results that contain all the search terms in the title. For example searching "allintitle: Cyber Security Training" will only return pages with the 3 search terms at least once in the title.

**Define:** This operator asks the search engine to define the search term. Similar to a dictionary Google will attempt to define the word using what it believes to be the most authoritative source and will display it in a nice box above any any results. For example "define: Superfluous" will return the definition of the word pulled from Oxford Dictionary.

**Filetype:** This operator is used to find results that match a specific filetype. This can be useful for finding research papers that you know are directly accessible as they have a PDF download. For example searching "filetype:pdf Cyber security papers" will return direct links

to PDF's of cyber security papers.

**Info:** This Operator returns info and popular pages of a particular website. For example searching "info:dit.ie" will return the dit.ie pages and popular pages such as the exams repeat page.

**Cache:** This Operator returns the cache of a specific page, this can be useful for finding deleted information alongside sources such as the internet archive. An example is "cache:dit.ie" will return an older version of the DIT website.

**Related:** This operator returns sites that are related to the search website. Searching "related:dit.ie" returns results for UCD, Trinity, DCU and other universities which are related.

**AllInUrl:** This operator returns results that have all the search terms in the URL of the site. Similar to AllInTitle. An example is searching "allinurl: dit" this will only return sites with DIT in the URL such as dit.ie

**InUrl:** Similar to the above allinUrl this operator returns results that have some of the search terms in the url so searching "inUrl: dit trinity dcu" will return the respective websites of the universities at the top of the list.

**NumRange:** Is a deprecated operator, it allowed you to specify a range of numbers to limit search results to, so for example you could search for the third to the tenth page of results on each site.

**DateRange:** This is a very useful search operator which limits your search to pages indexed within a the specified date range. This can be very useful when searching for up to date information on news such as "daterange:11278-13278 economy" returning results mentioning economy within the date range.

**Site:** This operator allows you to search all the pages Google has indexed on a certain site, for example searching site:irishtimes.ie economy will return only results from the Irish Times site that mention the economy.

## Comparisons

Comparing Bing to Google, Bing supports all the basic search operators however it lacks support for most of the advanced search operators. It also has far smaller indexing footprint leading to less relevant results.

- Ecosia: Less Tracking than Google, profits go towards saving the environment as opposed to shareholders.

- DuckDuckGo: Doesn't perform any tracking allowing you to maintain your privacy while searching. Lack of tracking data can make it less accurate than other search engines.
- Yahoo: No real advantages to use, tech stack is far behind competitors however it remains popular and more useful in some non English speaking countries such as Japan.
- Baidu: China's alternative to Google, it's very complete and competitive however it's largely censored so it's of less use to western users.
- Yandex: Russia's home grown alternative to Google, like Baidu it's very complete and useful however suffers from state censorship removing critical pages.
- Internet Archive: Designed to preserve Websites and the history of the internet this site is extremely useful for finding older versions of websites.
- Wiki.com: This search engine only searches wiki's which makes it very useful for research on specific topics.

## Part C

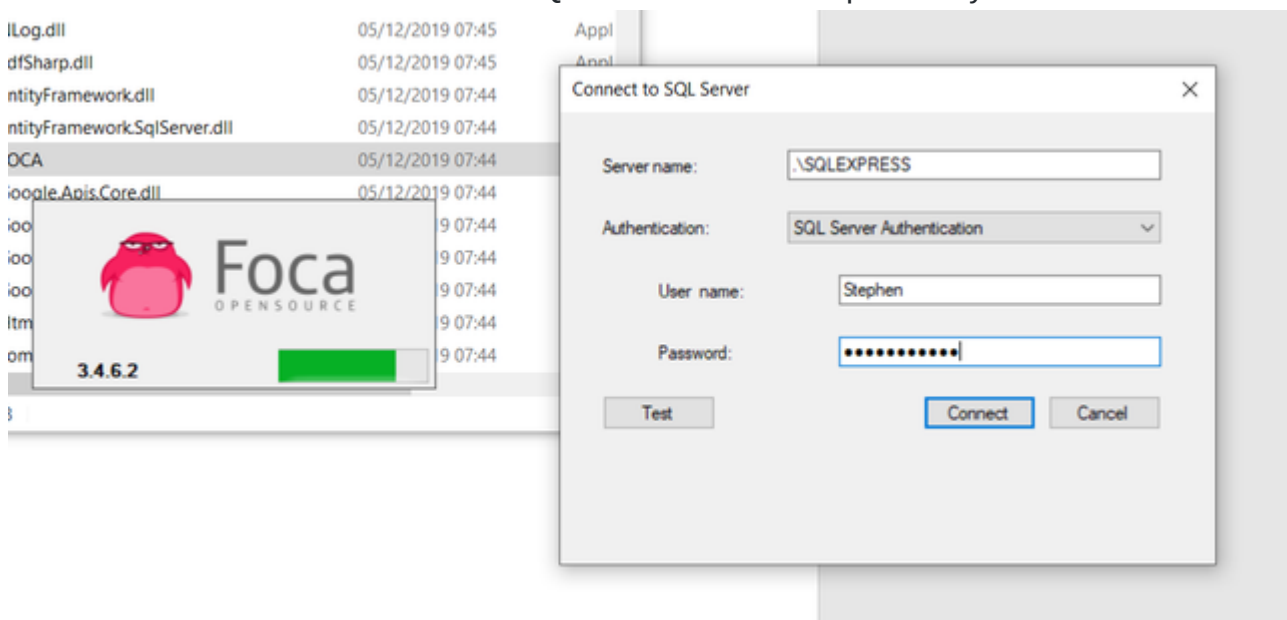
---

1. DOS (Denial of Service Attacks) - These involve overwhelming the target system with requests so that other users are unable to use the system. It takes numerous forms from botnets of machines flooding requests in DDOS's to clever amplification attacks or slowdown attacks.
2. SQL Injection - These attacks involve sending malicious SQL statements such as drop statements to databases through applications that don't properly deal with user input such as escaping and using prepared statements.
3. XSS - This involves exploiting Javascript hooks on websites to execute malicious code on the client system, this code can be used to then extract authentication cookies and numerous other purposes.
4. MITM (Man in the Middle) - These attacks involve situating the attacker between two communicating entities, the attacker then eavesdrops into the traffic and can discover valuable information.
5. Credential Stuffing: This involves taking credentials breached from other website and using them to attack different websites in the hope of finding reused credentials.
6. Command injection – This is when arbitrary commands on the host operating system are executed via a vulnerable application. This may occur when an application passes unsafe user supplied data (forms, cookies, http headers) to a system shell.

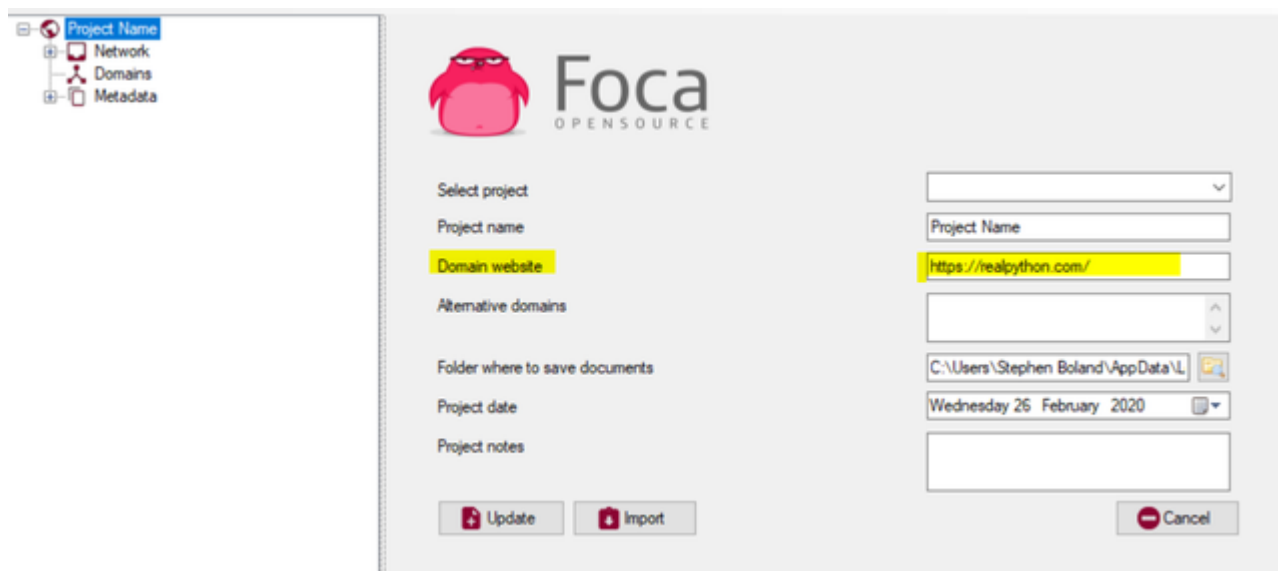
7. Bruteforce Attacks - Uncommon but these attacks involve enumerating all the possible values for a credential until the correct value is found. This is often used in conjunction with other attacks.
8. Downgrade Attacks: Often used on the TLS protocol, these are attacks that try force a connection between two systems to use outdated version of the protocol which are vulnerable to information leakage and the like. For Example SSL 3.0
9. Phishing Attacks: These attacks involve spoofing emails or other communications that look official in an attempt to get a user to download malicious files or get them to false login pages to steal their credentials.
10. Social Engineering: Usually used to extract information from targets this involves impersonating a victim or someone in authority to gain information or access.

## Part D

First, to obtain FOCA, I downloaded it from this following - <https://github.com/ElevenPaths/FOCA/releases> I also had to install SQL Server as it's a dependency.

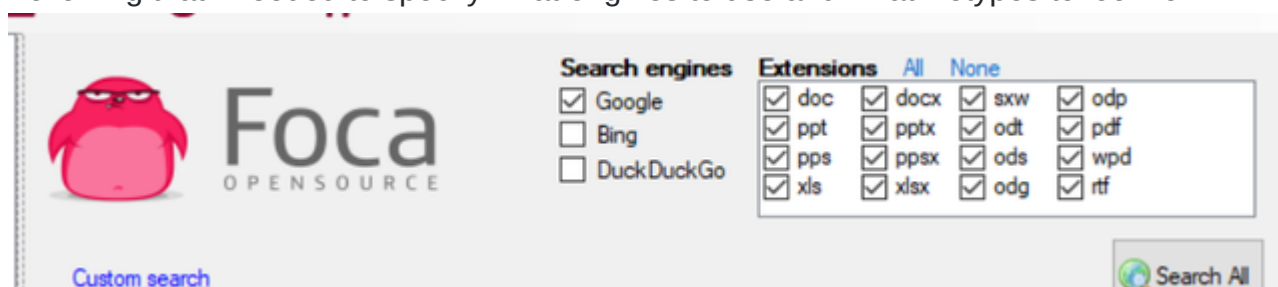


I then needed to create a project.



The image shows the Foca OpenSource project configuration window. On the left is a sidebar with a tree view containing 'Project Name', 'Network', 'Domains', and 'Metadata'. The main area has a pink penguin logo and the text 'Foca OPENSOURCE'. Below this are several input fields: 'Select project' (a dropdown), 'Project name' (a text box), 'Domain website' (a text box containing 'https://realpython.com/'), 'Alternative domains' (a dropdown), 'Folder where to save documents' (a text box containing 'C:\Users\Stephen Boland\AppData\Local'), 'Project date' (a date picker set to 'Wednesday 26 February 2020'), and 'Project notes' (a text area). At the bottom are 'Update' and 'Import' buttons, and a 'Cancel' button on the right.

Following that I needed to specify what engines to use and what filetypes to look for.

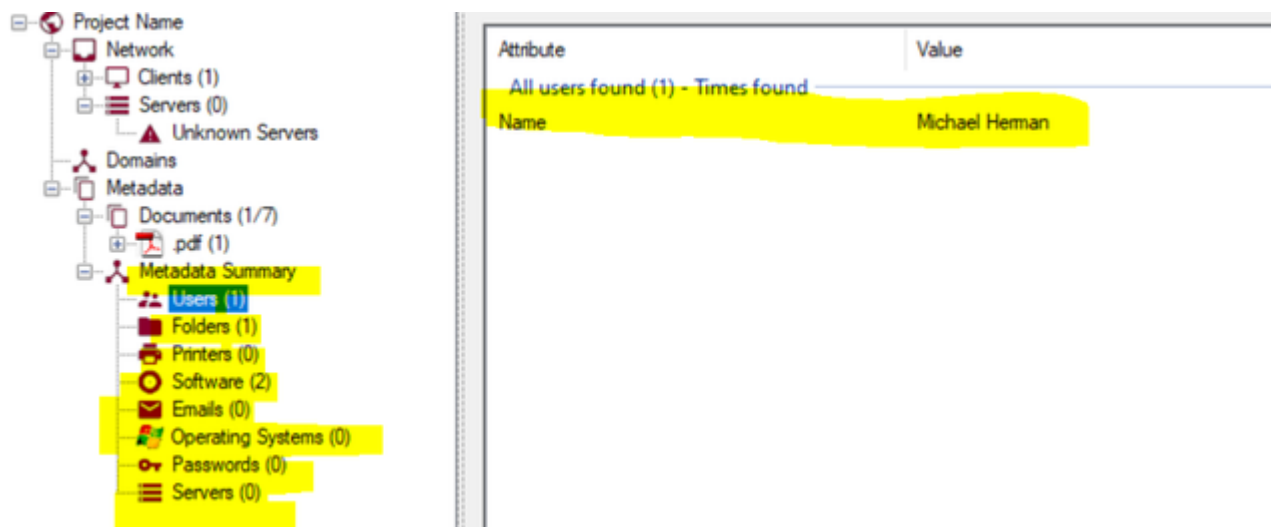


The image shows the Foca OpenSource search configuration window. It features the same pink penguin logo and 'Foca OPENSOURCE' text. Below this are two sections: 'Search engines' with checkboxes for 'Google' (checked), 'Bing', and 'DuckDuckGo'; and 'Extensions' with two columns of checkboxes. The first column has checkboxes for 'doc', 'ppt', 'pps', and 'xls' (all checked). The second column has checkboxes for 'docx', 'pptx', 'ppsx', and 'xlsx' (all checked). To the right of these are checkboxes for 'sxw', 'odt', 'ods', and 'odg' (all checked). Further right are checkboxes for 'odp', 'pdf', 'wpd', and 'rtf' (all checked). At the bottom left is a 'Custom search' link, and at the bottom right is a 'Search All' button with a magnifying glass icon.

I then Searched on realpython.com this produced a number of files

Id	Type	URL	Download	Download Date	Size
0	pdf	https://realpython.com/files/python_cheat_sheet_v1.pdf	✗	-	
1		https://realpython.com/python-tricks-sample-pdf	✗	-	
2	pdf	https://static.realpython.com/Python3CheatSheet.pdf?sr...	✗	-	
3	pdf	https://static.realpython.com/python-basics-sample-chap...	✗	-	
4	pdf	https://static.realpython.com/guides/pdb-command-refer...	✗	-	
5	pdf	https://static.realpython.com/guides/numpy-learning-res...	✗	-	
6	pdf	https://static.realpython.com/guides/rest-api-python-guid...	✗	-	

The Metadata for these files were then displayed and you could see the software and user who created all the found PDF's.



## Part E

### Vulnerability Databases

- The National Vulnerability Database(NVD) -  
[\[https://nvd.nist.gov/\]](https://nvd.nist.gov/)[\(https://nvd.nist.gov/\)](https://nvd.nist.gov/)  
 The NVD is the American governments repository of vulnerability data. The data provided enables automation of vulnerability management, security measurement and compliance. The database allows security checkl referencing, security related software flaws, misconfigurations, product names and impact metrics.
- CVE Details “The ultimate security vulnerability datasource” -  
[\[https://www.cvedetails.com/\]](https://www.cvedetails.com/)[\(https://www.cvedetails.com/\)](https://www.cvedetails.com/)  
 This website provides an easy to use web interface to vulnerability data. It allows a user to browse for vendors, products and versions, as well as view cve(common vulnerabilities and exposure) entries. The idea behind this website is to make the information as clear as possible and easily accessible.
- The CVE ( Common Vulnerabilities and Entries) -  
[\[https://cve.mitre.org/\]](https://cve.mitre.org/)[\(https://cve.mitre.org/\)](https://cve.mitre.org/)  
 The CVE is a list of entries for publicly known cybersecurity vulnerabil and is used for the NVD.
- [\[Synk.io\]](https://synk.io/product/vulnerability-database/)[\(https://synk.io/product/vulnerability-database/\)](https://synk.io/product/vulnerability-database/)

Unlike the other 4 databases talked about previously, this is not a publicly available database, it requires payment for its use. However the website quotes that it goes far beyond the CVE vulnerabilities and includes many additional non-cve vulnerabilities, with “67% more vulnerabilities than the NVD.

- The Chinese National Vulnerability Database (CNVD) - [<https://www.cnvd.org.cn/>](<https://www.cnvd.org.cn/>)  
The CNVD is the largest non-English vulnerability database, which is ran by the Chinese government. It is similar to the American NV however much the information is Chinese.

### *Vulnerability Detecting Programs*

#### 1. Nessus - <https://www.g2.com/products/nessus>

Nessus was built by security professionals to perform point-in-time assessments to allow security professionals to quickly and easily identify and fix vulnerabilities. It displays software flaws, missing patches, malware and misconfigurations, across a variety of devices, applications and operating systems.

#### 2. Netsparker - <https://www.g2.com/products/netsparker>

Netsparker is a web application security solution with scalable properties. The application will automatically prove every vulnerability that it finds, as well as providing formal proofing and reports.