**Part A:**

In this section I will be discussing why there is a shortage of security personnel worldwide, the measures that need to be taken to address this, whether I have the skills to be a security expert and what traits I have that would make me a good security expert and how I could improve upon these traits.

There are a set number of basic traits that an individual must possess to become a security expert which are listed below, I will go further in depth about other traits that are important to be a security expert after outlining the basics.

* **Having the right mindset:** To be a security expert, it is very important to think like an individual who wishes to compromise the system you are dealing with. You need to keep in mind what the weaknesses of the system are, how these could be attacked and how to mitigate the damage of these attacks.
* **Intrusion Detection:** This is the ability to be able to monitor systems and to be able to spot unusual behaviour in the system and to detect whether this is a malicious intrusion into the system. This is important to spot malicious software that slips past any software that’s job is to stop intrusions.
* **Analysing Risks:**  Analysing risk entails looking at the systems in place to try find where damage could be done to the system and how to lessen the risks. This is mainly done to see how risky the current systems are to use and how they could affect the infrastructure of a company or organization.
* **Analysing Malware:** This is comparable to intrusion detection and being able to notice unusual behaviour in a system. However, this step involves recognising a malware attack and being able to reverse the damage and effects that it could invoke.

Above are a baseline of skills needed to become a security expert but there is more to being a security expert than just the baseline. There is a long list of certifications that are expected from an individual who wants to become a security expert. These include the “Certified Information Systems Security Professional”, or CISSP for short, certificate and the “Certified Information Security Manager”, or CISM, certificates. These certificates are used to prove that an individual has the necessary skills to become a security professional.

In my opinion there is a shortage of security personnel because there is a very high level of skills required for these jobs. The skills and certificates required are needed on top of a traditional computer science degree, so this increases the amount of time needed to get the qualifications for such a job. This time investment can make a career in security hard to justify to someone when other lines of work are easier to come by and require just a computer science degree. To address this, steps such as offering more internships to students studying related fields, introducing young people to the concept of security and more open online learning resources could help this shortage.

In my opinion I do not think that I have the necessary to become a security expert. I am almost finished gaining my computer science degree, but I have not had the chance to work on projects that are applicable to real life situations. Also, I have not attained any of the certificates listed through college to gain a job in the field.

**Part B**

Basic Operators:

**+ :** This operator is used to force an exact match search on a single word or phrase. For example, if a user were to search for *restaurants +Ireland* the search engine would be forced to include Ireland in any results that appear. This also works for searches for +*used cars +€5000 .. €7500*, this would force the search engine to only show used cars that cost between €5000 and €7500.

**- :** This operator works in the opposite sense to the plus operator. This operator forces the search engine to exclude terms that follow the – symbol. For example, when searching *restaurants -Ireland* the search engine would make sure Ireland does not appear in any search results and -*used cars +€5000* would exclude any used cars and only include new cars that cost €5000.

**~ :** This search term is used to search for synonyms for specific terms. This term does not function anymore as Google search includes synonyms by default, however using double quotes on this symbol makes Google exclude synonyms for example typing *“~”book*  will make Google search exclude terms like literature or scrolls and searching *“~”car -Audi* will stop Google search from using terms like automobile and exclude Audis.

**. :** This operator is used to give a range of numbers to search for. For example, if a user searched *car €50 .. €1000* this operator would return cars within the price range of €50 to €1000, the same works for years where a user could search for *footballers born 1999 ..2005* *-Liverpool* to return a list of footballers born between 1999 and 2005 that do not play for Liverpool.

**\* :** The asterisk symbol is also called the wild card operator and is used to return a match for a word or phrase. For example, *Dublin \** will return results for tourist sites for Dublin and *car \* -Dublin* will return results for car dealerships outside of Dublin.

**“” :**  Using quotation marks will force an exact-match search result in a similar way to how + functions. An example of this includes searching for *“United States”* will only return results about the US and “*United States” -Europe* will exclude any websites about the US that include information about Europe.

**| :** This is the OR operator and is used to make search results show results for either search term. For example, *chicken | fish*  will show results about either chicken or fish and *car | truck* *-tractor* will show results about cars or trucks but not tractors.

Advanced Operators:

**allintext :**  This operator is used to specify the exact words that appear in a search result. For example, *allintext:Liverpool FC* *fixtures* will only show pages that contain information about Liverpool FC fixture.

**allintitle :** This operator is used to ensure that all the words used in the search term are included in the results page’s title. For example, *allintitle: Audi A5*would only return articles about the Audi A5.

**allinurl :** This operator has the same functionality as allintext and allintitle, but it is used for specifying that a term must appear in the URL of a website. For example, *allinurl: ps5* would only return sites that have ps5 in their URL.

**cache :** This operator is used to return the most recent cached version of a website. This operator can be used like *cache:youtube*.

**define :** This operator is used as a dictionary in Google Search. This operator returns results in a card format.

**filetype :** This operator is used to specify what filetype you want results to be. For example, *google filetype: pdf* will only return articles about google in pdf format.

**info :** This operator is used to find information about a page such as the most recent cache and other similar pages, this operator has been depreciated however it can still be useful in finding the indexed version of a URL. An example of it in use would be searching for *info:facebook.com*.

**intext :** This is used to find pages that contain a certain word somewhere in the content of a page. For example, using *intext:china* will return websites that mention China on their page.

**intitle :** This command is used to find pages that contain a certain word in the title, for example searching *intitle:cheese* will search for titles where the word cheese is included.

**inurl :** This command is used to find pages that include a certain word in the URL. For example, searching *inurl:egg* will only return sites which URL contains the word egg.

**link :** This command is used to find pages that link to a certain domain or URL. For example, searching *link:facebook.com* will only show results from Facebook. This command was depreciated in 2017.

**related :**  The related command is used to find sites related to a specified domain. For example, *related:sony.com* will only show results of sites that relate to Sony’s website,

**site :** This command is used to limit search results to only appear from the specified site. For example, searching *site:www.irishtimes.com* will only show results from the Irish Times website.

**numrange :** This operator is used to search for numbers within a desired range. For example, searching for *numrange:1500-1600*will return search results for numbers within the range 1500 to 1600.

**daterange :** This is used to find results from a certain date range; however, it only works with the Julian date format. An example of a search query using this would be *daterange:11278-11578*. Even though it is not depreciated it is not consistent in its results.

These operators are mostly supported by Bing, apart from the following operators: related, allintitle, allinurl, info, cache, \*, ~, link.

Listed below are 10 other search engines besides Google Search. I will discuss the advantages and disadvantages of these.

|  |  |  |
| --- | --- | --- |
|  | Advantages | Disadvantages |
| Ecosia | Environmentally conscious, for every 45 searches completed, a tree is planted. | UI is a bit outdated. |
| DuckDuckGo | Very privacy oriented and does not track users. | Is slightly less accurate than Google. |
| Yahoo | Search results are powered by both Google and Bing. | No maps integration. |
| Baidu | Accessible worldwide and has comprehensive Chinese language support. | Only available in the Chinese language. |
| Yandex.ru | Good Russian language support. Has 65% market share in Russia. | Cluttered interface. |
| Ask.com | The top results are determined by expertise and not how many clicks an answer gets. | Search results are editable by any end user and as such can have reliability issues. |
| AOL. | Easy to use UI. | Slow search engine. |
| Dogpile | Like adblocker, this search engine removes ads from results. | Difficult UI to use, |
| CC Search | Allows users search for content that is free to use under the Creative Commons License. | Does not have support for text and audio, just images. |
| Internet Archive | Allows users to look at how websites appeared in the past | Can be difficult to use. |

**Part C:**

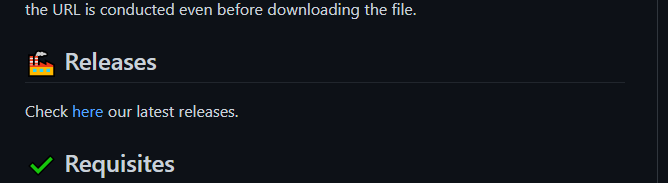
Below is a list of attacks and exploits that a security expert should be able to spot:

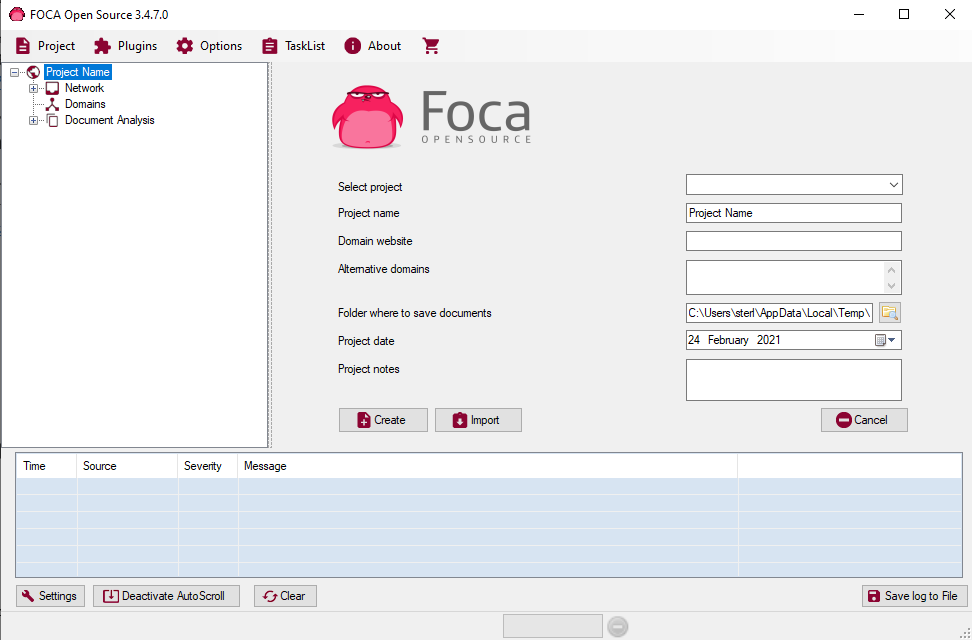
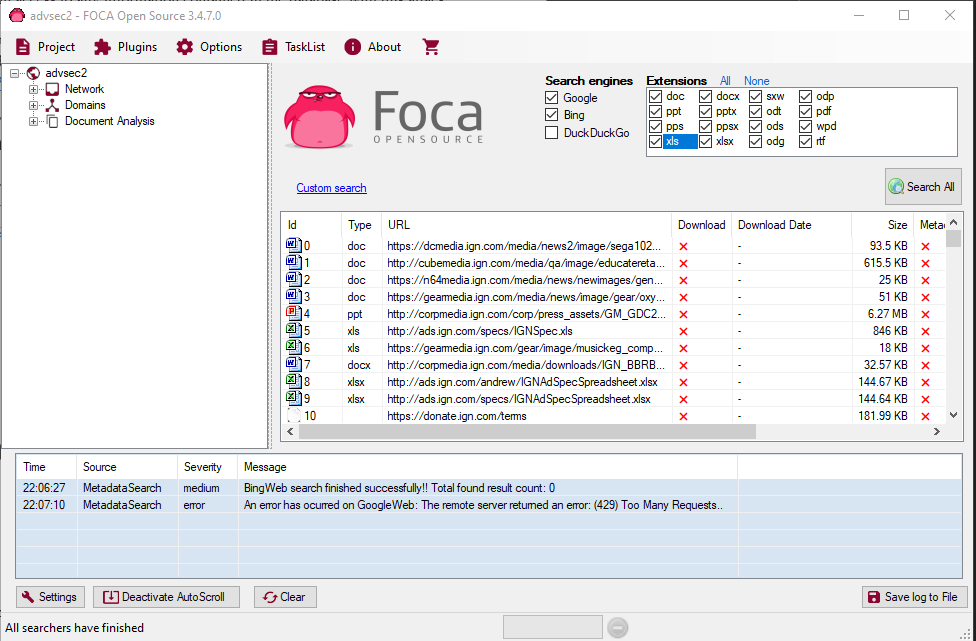
1. **Privilege Gaining:**  This is where a user can gain administrator privileges by exploiting a bug or design flaw in a software system.
2. **Remote Command Execution:** This is where an attacker can attack someone else’s computer and make changes remotely. This can give the attacker access to sensitive information.
3. **Authentication Bypassing:** Attackers use these attacks to change configuration settings and to utilize SQL injections.
4. **Buffer Overflow:** This is when attackers try use more than the allocated amount of memory that a program can use to try force the program to access memory the attackers could exploit.
5. **Cross Site Scripting:** This is where an attacker stores malicious script data that is usually stored in a website contact form.
6. **Email Header Injection:** This is when an attacker appends additional information to an email that is being sent. This is usually in MIME format and allows attackers to disguise themselves as a friend of a company.
7. **SQL Injection:** This attack involves manipulating SQL databases by using commands. The attacker can gain access to any information contained in the database with this attack.
8. **Reflective Cross site Scripting:** This involves the attacker typing commands in search that could return a dangerous result. For example: [https://insecure-website.com/status?message=<script>/\*+Bad+stuff+here...+\*/</script](https://insecure-website.com/status?message=%3cscript%3e/*+Bad+stuff+here...+*/%3c/script)>
9. **DDOS Overflow:**  This is when an attacker sends a large amount of data packets to a system, which overflows a system and can take it down.
10. **Unvalidated Redirects:** This method is often used to redirect a user to a malicious website to take user information. An example of a redirect that’s unvalidated is <http://www.samplewebsite.com/redirectURL=malicious.com>

**Part D:**

The following steps show how to use FOCA (Fingerprint Organisations with Collected Archives). This is a tool that is used to extract metadata from websites.

1. Go to the [FOCA GitHub](https://github.com/ElevenPaths/FOCA), scroll down and then click here to see their latest releases. Then download a zip of the latest version, extract it at a desired location and run FOCA.exe.



1. Create a new project with a name and the domain name of the website you wish to download metadata from.
2. Select the extensions and browsers you wish to use and then click search all to extract metadata. You can then right click any documents you find and download them to view them.

**Part E:**

In this section I will discuss six major vulnerability databases that are currently in use. These databases are used to collect information about security vulnerabilities.

1. [**Common Vulnerabilities and Exposures (CVE)**](https://cve.mitre.org/)**:** This database contains a list of standardised names for listed vulnerabilities. Each vulnerability contains an identification number, a description and at least one public reference. This database aims to standardize the names of publicly known vulnerabilities and security databases.
2. [**National Vulnerability Database (NVD)**](https://nvd.nist.gov/)**:** This database is a United States government repository of standards-based vulnerability management data. This data is represented using the Security Content Automation Protocol (SCAP). This database contains security checklist references, security0related software flaws, misconfigurations, and product names.
3. [**Chinese National Vulnerability Database (CNVD)**](http://www.cnnvd.org.cn/)**:** This is a vulnerability database that is run by the Chinese government. This database has been the centre of controversy for some time now as experts are saying that Chinese intelligence organizations are delaying posting vulnerabilities on it so they can first assess their use in intelligence missions. It is much larger than its US counterpart and is 2 times faster at posting vulnerabilities than the US version.
4. [**BugTraq (BID)**](https://www.securityfocus.com/bid/): BugTraq is a high-volume mail disclosure list that is used for the discussion and announcement of computer security vulnerabilities. This database is used as the cornerstone of internet security community and is widely used by security experts.
5. [**VULDB**](https://vuldb.com/)**:** VULDB is a very useful vulnerability database that has been documenting security vulnerabilities since 1997.
6. [**Seclists Full-Disclosure**](https://seclists.org/fulldisclosure/)**:** Seclists is a public, vendor-neutral forum that has a detailed discussion of different exploit techniques. It also has an archive that can help users learn above previous vulnerabilities.

**Software Applications that can help with vulnerability finding:**

1. [**Nessus**](https://www.tenable.com/products/nessus)**:** Nessus is a vulnerability assessment tool by tenable that can scan your PC and report any issues. It is very handy for finding network vulnerabilities; however, it can cost up to $1500 so it is well suited for larger companies.
2. [**OpenVAS**](https://www.openvas.org/)**:** OpenVAS is a free network security scanner and is a good alternative to Nessus. It features many different industry trusted protocols, scanning and testing. Most components of it are included in the GNU General Public Licence.