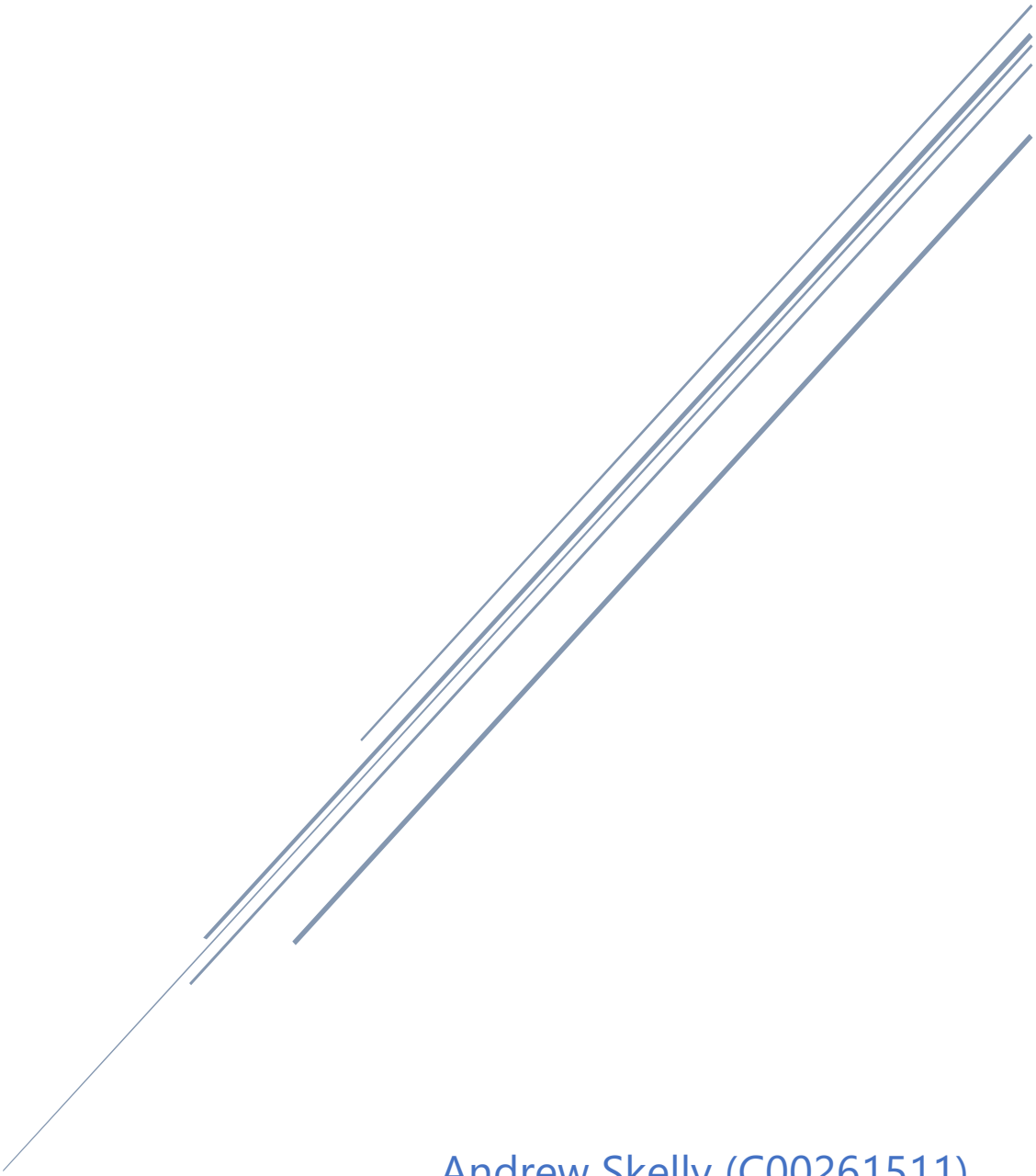
ASSET IDENTIFICATION AND RISK ASSESSMENT FOR SME'S

Research Report



Andrew Skelly (C00261511)
Cybercrime and IT Security

Abstract

This research report aims to investigate the technologies, and knowledge needed to create an effective tool for the identification of assets and risk assessment for Small and Medium-sized Enterprises (SMEs). This document will aid in coming to conclusions on what decisions and approaches are best for this asset identification and risk assessment project. It will outline things such as implementation tools, platforms, and any required algorithmic approaches as well as demonstrate why these decisions have been made.

The application that I am developing is called Apollo Defender and will be referred to as such throughout the rest of this document.

Apollo Defender is intended to be a network security vulnerability detection tool, that uses technologies such as the Nmap scanning tool, as well as the vulnerability database provided by the National Vulnerability Database (NVD). Apollo Defender intends to use these technologies to scan a company's network and keep a log of all detected vulnerabilities along with details as to when these vulnerabilities were resolved, to help SMEs meet compliance guidelines.

Table of Contents

Abstract 1
Introduction 4
Overview of Areas, Technologies and Topics Researched 5
SME Network Security 5
The Basics 5
Network Discovery 6
What is Network Discovery 6
Pre-existing Tools for Network Discovery 7
Comparing Nmap (ZenMap) and Angry IP Scanner 8
Risk Management 8
What is Risk Management? 8
How Do You Perform Risk Management? 9
Why is Risk Management Important? 10
Reviewing a Similar Pre-existing Tool – Lansweeper 10
How Often Do Companies Run These Scans 10
How to Mitigate Threats Without Network Security Software 11
Reasoning for Providing the Information Collected 12
How will Apollo Defender Traverse Networks? 12
NVD API 13
How to send data to it 13
How I'll interpret the data I receive 13
Development 14
Tools 14
IDE Option 1: PyCharm 14
IDE Option 2: Visual Studio Code 15
Server Hosting Option 1: Xampp 16
Server Hosting Option 2: Digital Ocean 18
Ways to Test Apollo Defender 18
Languages 19
Python 19
Java 20

3
PHP 20
Security Implications 21
Summary and Conclusions 22
Appendix 23
Glossary 24
Bibliography 25

Introduction

This research report investigates the research done to gain the knowledge and understanding required to complete this project to a standard that makes its use both simple and effective. It intends to provide information for the successful and smooth development of a network vulnerability scanning tool aimed towards SMEs.

The report first delves into the areas, technologies and topics researched and the information gathered from this research.

The first area of research is the basics of SME Network Security. The basics of SME network security include practices such as using Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and Virtual Private Networks (VPNs). All of these technologies come with their own vulnerabilities that need to be mitigated as well. One way of detecting these vulnerabilities is by using a network vulnerability scanner.

Next, network discovery techniques and approaches will be investigated, as well as pre-existing tools that perform similar tasks to the intended tasks of Apollo Defender. In this section, two pre-existing tools will be compared. Those tools are Nmap and Angry IP Scanner. They will be compared in such a way as to help me conclude which program will be most useful when developing Apollo Defender.

Importantly, Risk Management will be investigated. Risk management will play a crucial role in the successful implementation of Apollo Defender in a network. The tool can be installed in an environment, but until a user understands how and when to use the application, the application will not be of any benefit to the user. This is where risk management comes into play. Proper use of risk management protocols will help a user define how best to use the application.

Following this, topics like the review of a similar pre-existing tool will be investigated along with other topics such as the frequency at which companies run network vulnerability scans, how companies mitigate threats without network scanning tools, why Apollo Defender will be sharing the information it collects, and how will Apollo Defender traverse through networks.

Lastly, for the areas, technologies and topics researched, a vital topic will be investigated. This will be looking into how Apollo Defender will communicate with the NVD API, this will help the product determine if any hosts are vulnerable, and if so, what vulnerabilities are they exposed to.

The document will then pivot towards investigating technologies that will benefit the physical development of Apollo Defender. This will include areas such as a comparison between IDEs such as VSCode and PyCharm. Coding language will also be compared and from these comparisons, conclusions will be drawn on which language will be best to use. Ways to test Apollo Defender will also be investigated.

In the penultimate section of this document, possible security implications are discussed, which consider the possible security issues that may arise from developing such an application as well as how exactly the application will be useful to SMEs.

Finally, a detailed summary and conclusion is discussed, in which a review of all previous information and research is conducted. It outlines concrete conclusions gained from the research and provides reasoning for the decisions that affect the overall flow and direction of the project.

Apollo Defender intends to fill a gap in an area of technology that does not currently have any viable options available to SMEs. It intends to provide SMEs with a simple and secure way in which to scan their network, receive appropriate recommendations for mitigation, and provide documents which will help an SME prove their compliance when following mainstream compliance frameworks.

Overview of Areas, Technologies and Topics Researched

SME Network Security

The Basics

According to a report posted on the RTE website, a survey of over 250 business owners in Ireland concluded that 43% have experienced up to five cyber-attacks in the last 3 years(Brian O'Donovan, 2022). This post also states that, according to the survey, 60% of SMEs felt unprepared for a cyber-attack. The article also mentions a study conducted by Microsoft and Vodafone which concluded that the average financial loss for a business from a cyber-attack is €8,500 or €2.3 billion across the entire industry. These attacks can range from phishing scams to data breaches.

Network Discovery

What is Network Discovery

Network discovery is the practice of using network-based scanning tools to find out information about the structure and layout of a network as well as see the "systems and nodes" that allow devices "to connect and communicate on the same network"(SolarWinds, no date). Information that can be gleaned from network scans can vary widely, but the main information that is collected during network discoveries can include things like:

- Device names
- MAC addresses
- IP addresses/schemes
- Port numbers
- Operating system
- Ping times
- Network Services
- Firewall rules
- Software information

All of this information can be used to help a security professional or network administrator gain a better understanding of their network and is vital in the process of asset identification and risk assessment. However, this practice is also undertaken by threat actors as a form of reconnaissance where possible, and as such, the information that is discovered during one of these scans is highly sensitive and must be kept confidential.

Network discovery will be the central part of this application as it will be used to gather all the necessary information that will be fed to the NVD API to assess what vulnerabilities the environment is susceptible to. Because of this, we will take a look at some pre-existing network scanning tools that will help complete scans and gather as much information as possible to allow the SME to create a detailed understanding of their network. It is vital this the tool that we use is robust and reliable.

Pre-existing Tools for Network Discovery

Two very popular network discovery tools are Nmap (Nmap, no date) (and its GUI counterpart ZenMap) and Angry IP Scanner(Angry IP Scanner, no date). Figures 1.1 and 1.2 are screenshots of both ZenMap and Angry IP Scanner respectively showing a scan of my home network.

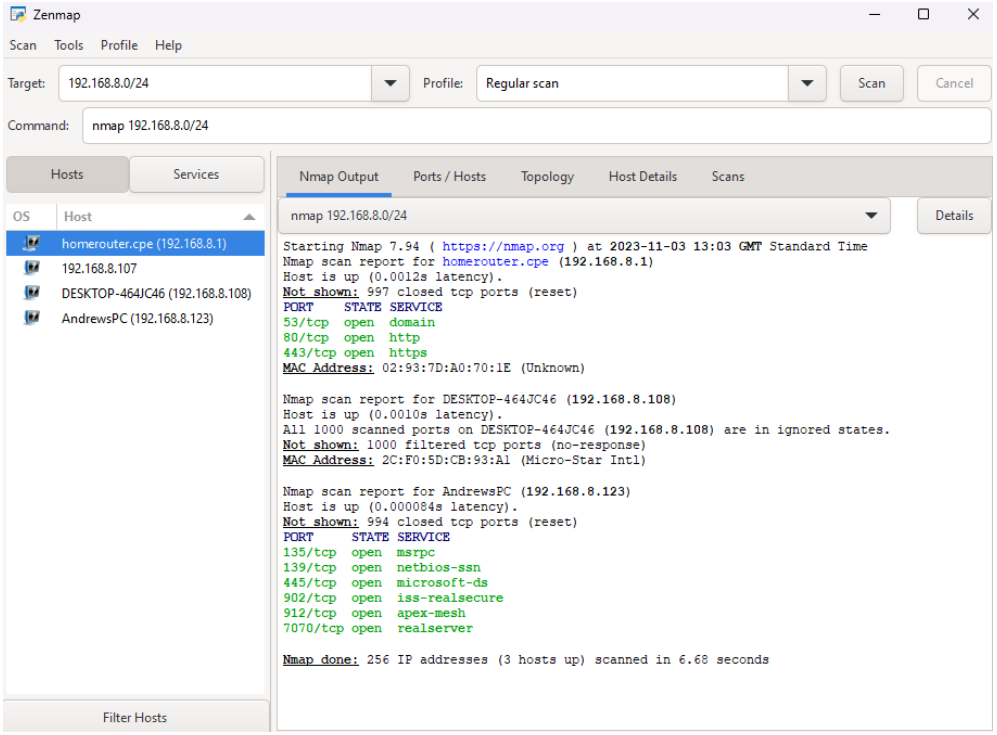


Figure 1.1: ZenMap Screenshot

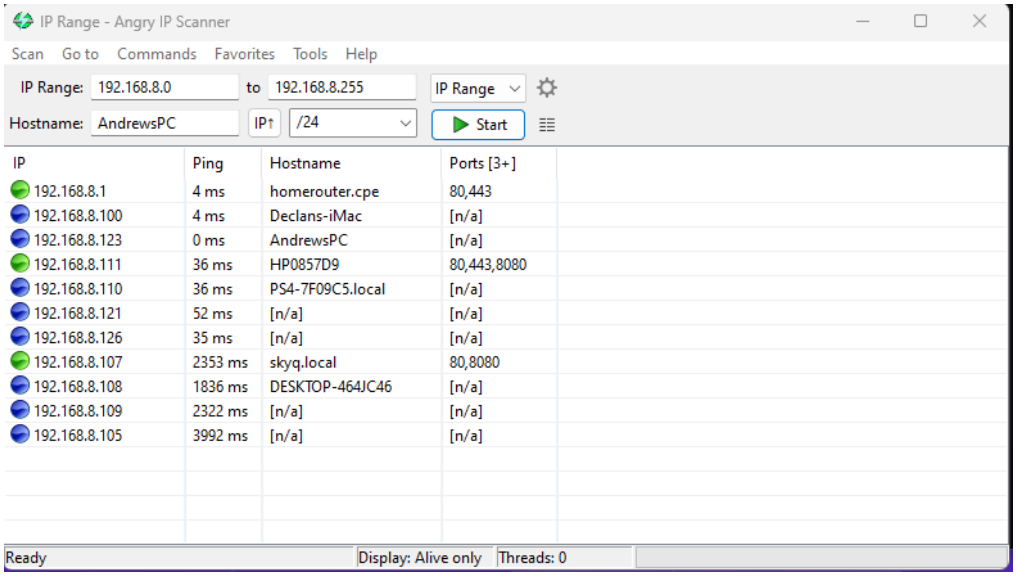


Figure 1.2: Angry IP Scanner Screenshot

Comparing Nmap (ZenMap) and Angry IP Scanner

Both of these network scanners have their benefits. The most obvious difference that we can immediately spot from the two screenshots above is the difference in the complexity of the UI. Angry IP Scanner is much more simplistic than ZenMap and makes it much easier for a user to open it and complete scans. ZenMap on the other hand has many more options and even allows the user to customise the command that will be used for scanning the network. This gives the user more options but makes it more difficult for a new user to open ZenMap and immediately start a scan. This, however, does have its benefits. It allows the user to customise their scan based on the kind of environment they are scanning in, doing things such as fragmenting packets, stealth scanning, or running less strenuous scans to not affect network bandwidth as much. Since all of this customisation is available and will allow us to save and run multiple different scans using different commands, Nmap will be used for the scans of networks in my application. It will allow me to run a more intensive scan on an environment when the tool is first put in place and then run fewer intensive scans later on when only updating the list of known devices on the network.

Risk Management

What is Risk Management?

"Risk management is the practice of using processes, methods and tools for managing" the risks that could impact an organisation's objectives. (ISO 37000:2018 - Risk management | Enhanced Reader, 2018).

According to IBM (What is risk management? | IBM, no date), there are three important steps when performing risk management, those being Identifying the risks, risk analysis and assessment, and risk mitigation and monitoring. Let's look at each of these steps in a bit more detail.

A good and successful risk management strategy helps a business identify and consider all of the threats that it faces. Not only does a risk management strategy help mitigate risks that could cause harm to a business, but it also helps a business evaluate positive risks. Positive risks are risks that may help increase the value of a business if taken and damage its value if not taken.

All things considered, a risk management strategy should not be put in place with the aim to remove all risk, it should help a business preserve and increase its value by making smart decisions regarding the risks that they take.

How Do You Perform Risk Management?

Identifying the risks

This section is fairly self-explanatory. We know that there are risks that are posed to a company or business and we must first find and identify those risks before we start to attempt to mitigate them. These risks can come in many different forms such as financial threats, accidents, natural disasters, and IT security threats. We will focus on IT security threats for the remainder of these headings.

Risk analysis and assessment

This step involves analysing the risk and establishing the likelihood that a threat may occur as well as the outcome of that event. The way that this can be categorised is by using a risk matrix, which categorises threats based on their likelihood and severity. Figure 2.1 shows an example of a risk matrix that a business may use to help them categorise their threats.

Figure 2.1: 5x5 Risk Matrix (Scarfone, 2022)*used for categorisation of threats.*

Another important thing to consider in risk analysis and assessment is the link between a business's organisational strategy and its risk management strategy. The two can be linked by establishing a risk appetite. A risk appetite is the amount of risk that a business is willing to accept to help it achieve its objectives. Depending on the risk appetite, some risks can be accepted without any further action, while other risks may be outside of the range that a business is willing to accept, and so these risks will be mitigated.

Risk mitigation and monitoring

Finally, risk mitigation and monitoring is the process that is undertaken to plan and develop methods of either mitigating a threat or reducing the likelihood of that threat. These mitigations will be developed to suit the risk appetite of the company.

Why is Risk Management Important?

Risk management is arguably more important now than it ever has been, especially in a time when globalisation is fuelling more complex and dangerous risks. The benefits of a good risk management strategy are many. An effective risk management strategy helps an organisation identify and understand the risks that are posed to them from multiple different sources, such as financial, legal, and technological risks. As stated in an article posted on BusinessTech Weekly, "A solid Cyber security risk management plan helps manage the risks daily. It also helps decision-makers take steps to identify the likelihood of cyber attacks the business is vulnerable to." (Adams, 2022) The strategy will help the organisation mitigate risks that may cause harm to the value of their business as well as help the organisation decide whether certain risks are worth taking to help increase their value.

Reviewing a Similar Pre-existing Tool – Lansweeper

Lansweeper (Lansweeper, no date)is a pre-existing tool that has similar functions to what my application intends to bring. The main difference between Apollo Defender and Lansweeper is that Lansweeper is more focused towards larger companies and networks, whereas Apollo Defender will cater to the smaller businesses that may not be able to afford software such as Lansweeper.

Lansweeper is not to be disregarded though. It boasts a large array of features such as IT discovery, asset inventory, asset details, integrations with popular apps, risk insights, and full network diagrams for visualising your network and topology. Many of these features and capabilities are well outside the scope of Apollo Defender and its timeline, but Lansweeper can be a good inspiration for how an application such as Apollo Defender should operate.

How Often Do Companies Run These Scans

According to a blog posted on thecysphere (Mirza, no date) companies that use cybersecurity frameworks such as ISO 27001 will often complete vulnerability scans every quarter or based on the specific needs of the company and the environment they are working with. More thorough tests like penetration tests or deep network scans may take place on a less frequent basis; usually annually

How to Mitigate Threats Without Network Security Software

If a company or business were to operate without any sort of technology (e.g., Lansweeper) to help them detect and protect their environment from possible vulnerabilities, there are multiple steps that companies could take to protect their environment. It must be said from the outset that any plans of network and environment protection without any such technology will be much more limited and create more work for employees such as system administrators.

One of the first and most important things that should be ensured for the protection of a company's environment is to make sure that all end devices have their operating systems and software updated to the latest stable and safe version. Updating to the newest version isn't always necessarily the best option, as brand-new versions of operating systems and software can contain bugs and exploits that have not yet been discovered and so increases the attack surface of the environment.

Another important thing that should be done by a company without network security software should be to implement essential network security features, such as firewalls and Access Control Lists (ACLs), Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Subdividing the network into more manageable smaller virtual local area networks or VLANs also helps increase security and ease of management. All of these security features will help limit the amount of harmful traffic that is allowed into the network.

Finally, another very important thing that a company should do to ensure their security, even if they aren't using specialised network security software, is to follow compliance guidelines. The NIST Cybersecurity Framework 2.0 (CSF) (NIST, 2023) is one of the most comprehensive frameworks that a company can follow to help them achieve their desired level of security. There are now 6 functions to guide the process, those being Govern, Identify, Protect, Detect, Respond and Recover. Each function can have categories which "are the subdivisions of a Function into groups of related cybersecurity outcomes". These categories are created at the discretion of the company and help them better pinpoint the outcomes they desire. Following a framework like the NIST CSF can help a company manage their environment in an efficient way that benefits security.

Reasoning for Providing the Information Collected

During scans performed by Apollo Defender on a client's network, a large amount of information will be collected, such as hostnames, IP addresses, MAC addresses, OS type and version, and software and software versions. All of this information will be necessary in determining whether a network or any section of a network is vulnerable to attack. This information, however, can also be used for another purpose to benefit the company. The information gathered by Apollo Defender can be compiled into a report which can be accessed by the company as an aid to proving compliance.

When a vulnerability is found using Apollo Defender, the time of this vulnerability detection will be logged alongside the host on which the vulnerability was detected. When the company then mitigates said vulnerability, Apollo Defender will then be able to pick up on this and make a record of when the vulnerability was mitigated. Information such as this can then be compiled into a report that can be used to show that a company mitigated a threat in a reasonable amount of time and that any damage caused by the vulnerability in that time was minimised.

How will Apollo Defender Traverse Networks?

When scanning the network of an SME, Apollo Defender will undoubtedly come across VLANs that need to be traversed. Luckily, Nmap allows for this to be done by specifying multiple network addresses in the target specification parameter. In my opinion, after doing research into the different ways that these networks can be specified to Nmap, I believe that creating a section in the application where the user can add subnet addresses before scanning would be the best option. These network addresses would then be saved to a text file in a specific format that Nmap can interpret, and when the scan command is issued to the application, it will use this file to determine which network addresses to scan.

NVD API

The NVD Application Programming Interface (API) will be vital in the function of Apollo Defender. The NVD API (NIST, no date) will be where information about the company's network like OS versions, OS types and software types will be sent to help determine if certain hosts are vulnerable to attack.

How to send data to it

The NVD website details how to send data to the API so I will be following this. The website also provides separate detailed documentation on how to connect with and send data to the API. This format is generalised and will be able to be adapted to allow communication with the API using Python.

How I'll interpret the data I receive

The NVD API returns data in an XML format. When trying to interpret this data, I think that the easiest way of doing so will be to convert the returned data into JSON format and then use functions to read this JSON file. There are Python modules that can convert XML data into JSON format so I will be using this and then interpreting the JSON for here. I have chosen to go down this route as I have used JSON before, and I understand the format and how to interpret it using code. Pythons' heavy usage of dictionaries and lists will be very beneficial in this process as JSON is formatted in a way that will be very easy to read into dictionaries.

Development

Tools

Apollo Defender will be comprised of many different technologies working together to complete its tasks, and as such, I will be using multiple different tools to help me integrate all of these technologies into the application. Here are the tools that I have chosen to help me with this technology integration.

IDE Option 1: PyCharm

PyCharm is one of the tools available to me for code development. It is a powerful IDE developed by JetBrains, which is specifically focused on Python development. It is capable of version control, debugging and database management within the app to name a few.

Advantages of using PyCharm

a. Powerful and specifically designed for Python development.
   PyCharm is an IDE that has been developed specifically for the development of Python code and as such, it is very good at completing tasks related to Python. There are built-in Python consoles in the IDE which allow you to run your code in real time with a pre-set-up Python console. It also has a built-in package manager which allows the user to add any necessary Python libraries without having to input commands to do so.

Disadvantages of using PyCharm

a. Not a free program
   For most developers, PyCharm and any of the other JetBrains products will not be available to them, as these IDEs usually require a valid license and license key to activate the IDE. Luckily for me, as part of the GitHub student pack, all of the JetBrains IDEs are free for me to use for the duration of my college education, and as such, I will be taking full advantage of this by using PyCharm.

PyCharm Interface

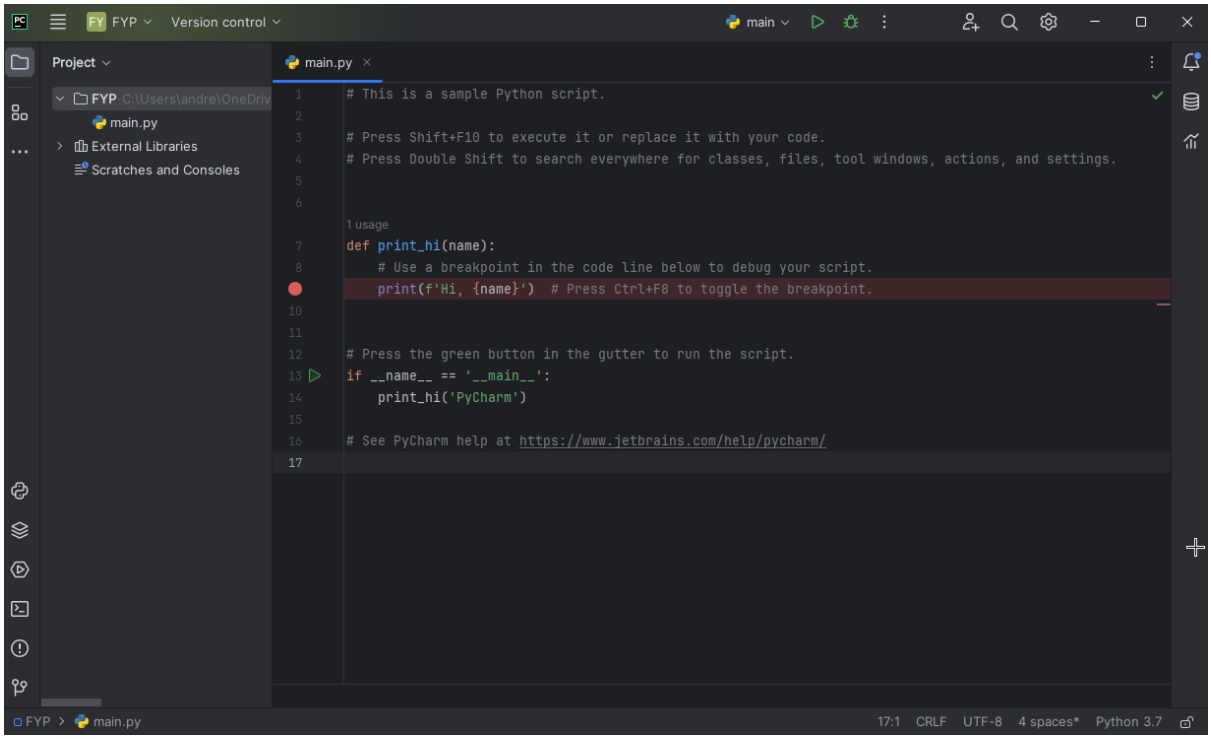


Figure 3.1: PyCharm interface when the user first creates a project.

IDE Option 2: Visual Studio Code

Visual Studio Code (VSC) (Microsoft, 2023) is a free and easy-to-use, comparatively lightweight code editor that is beginner-friendly but is highly customisable using plugins and add-ons.

Advantages of using VSC

VSC is a simple and easy-to-set-up code editor that is friendly to beginners and is a lot more lightweight as it is more so a code editor rather than a full-blown IDE. This will make it much easier to run on lower-end machines, making it more portable.

Disadvantages of using VSC

I have tried using VSC for pushing commits to my GitHub repositories in the past and have had some issues doing so. I also find that some of the plugins for VSC can be unreliable at best and some do not work at all. I also am not as fond of the interface as much as PyCharm's, as I have used JetBrains products extensively in the past and am comfortable with how everything works.

VSC interface

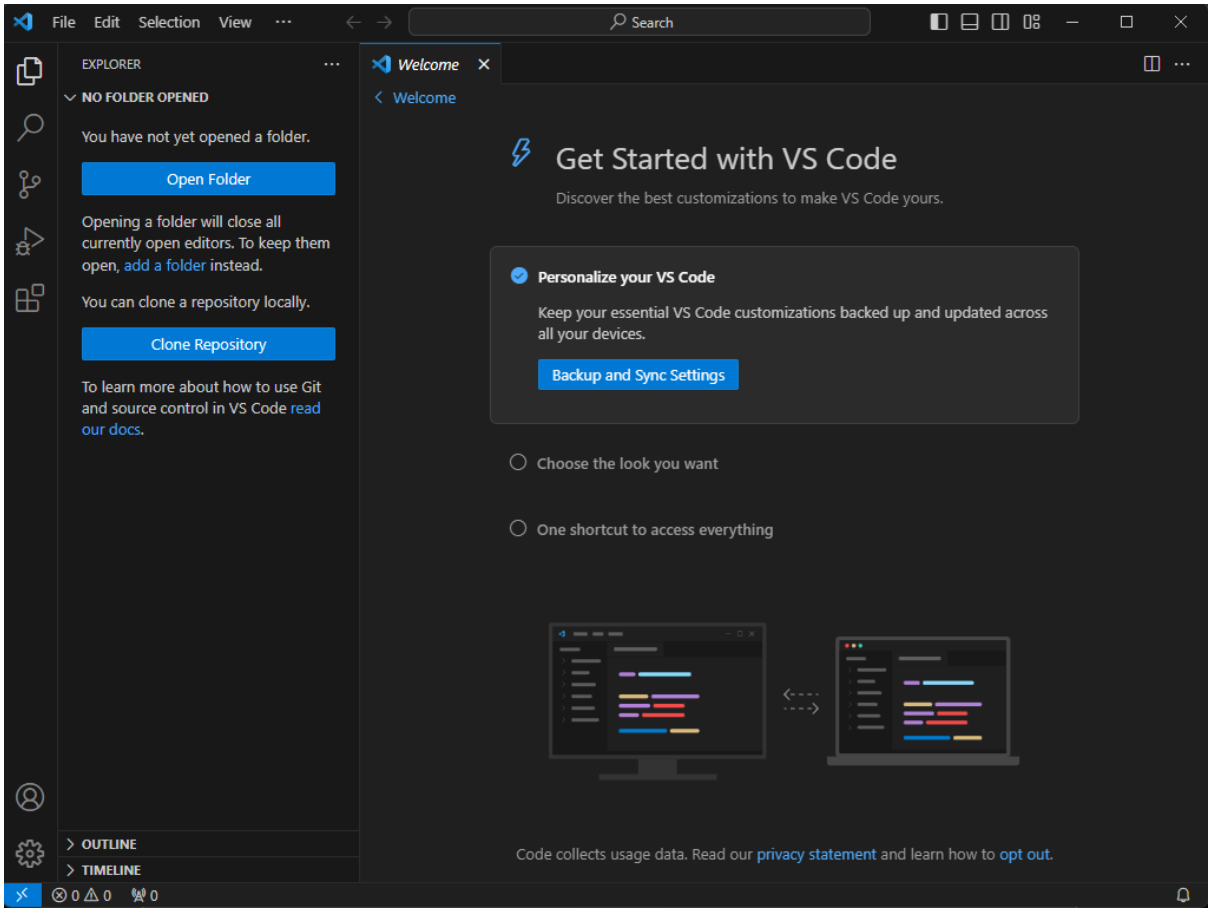


Figure 3.2: Visual Studio Code interface when the user first opens the application.

Server Hosting Option 1: Xampp

XAMPP (XAMPP, no date) is a free and open-source cross-platform web server hosting application that consists of MariaDB and PHP. XAMPP is a very popular application as it is free to use and easy to set up. It does, however, limit the usability of the database as it is created using the local host address of the machine that it is hosted on. This would make it more difficult to connect to and communicate with the database from multiple different sources at different sites. XAMPP is designed for use with web servers, and as such, it is much easier to access over the network. This is ideal for websites but can cause security concerns for a production database such as one that will be needed for Apollo Defender.

XAMPP Interface

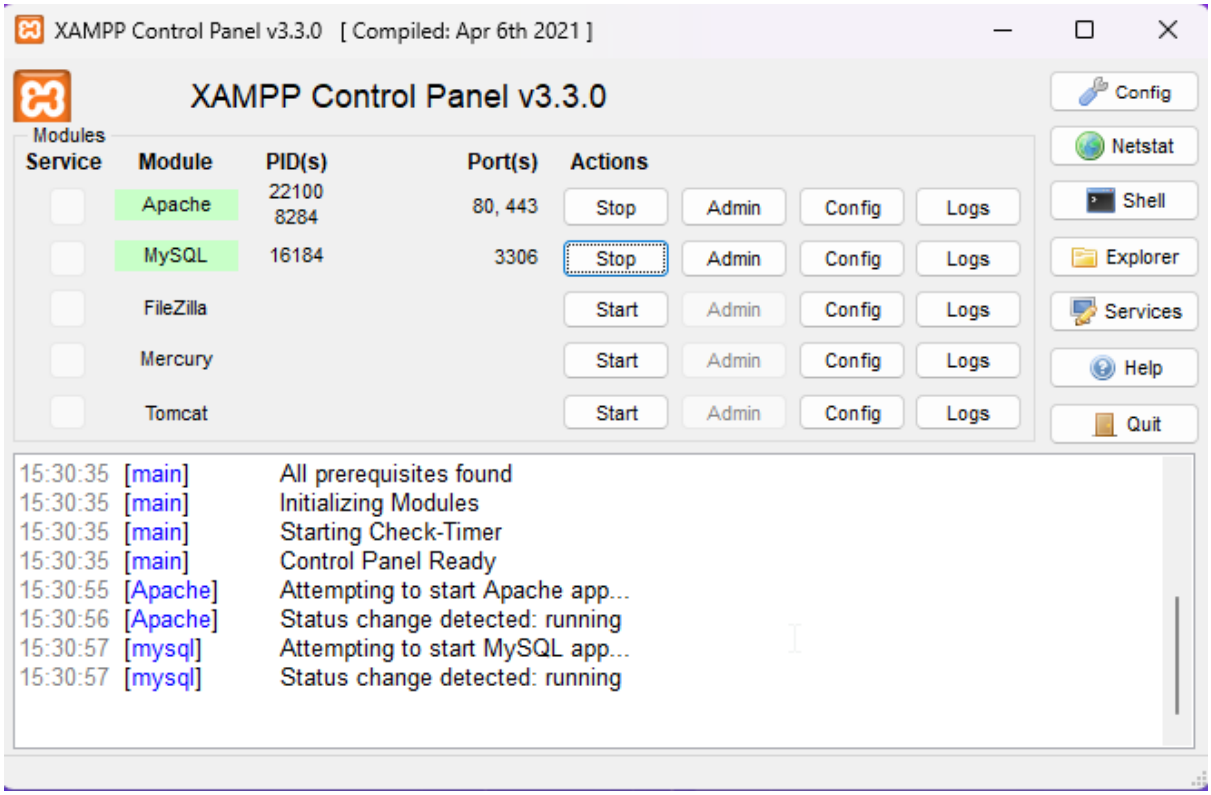


Figure 3.3: Control Panel for XAMPP with Apache and MySQL started.

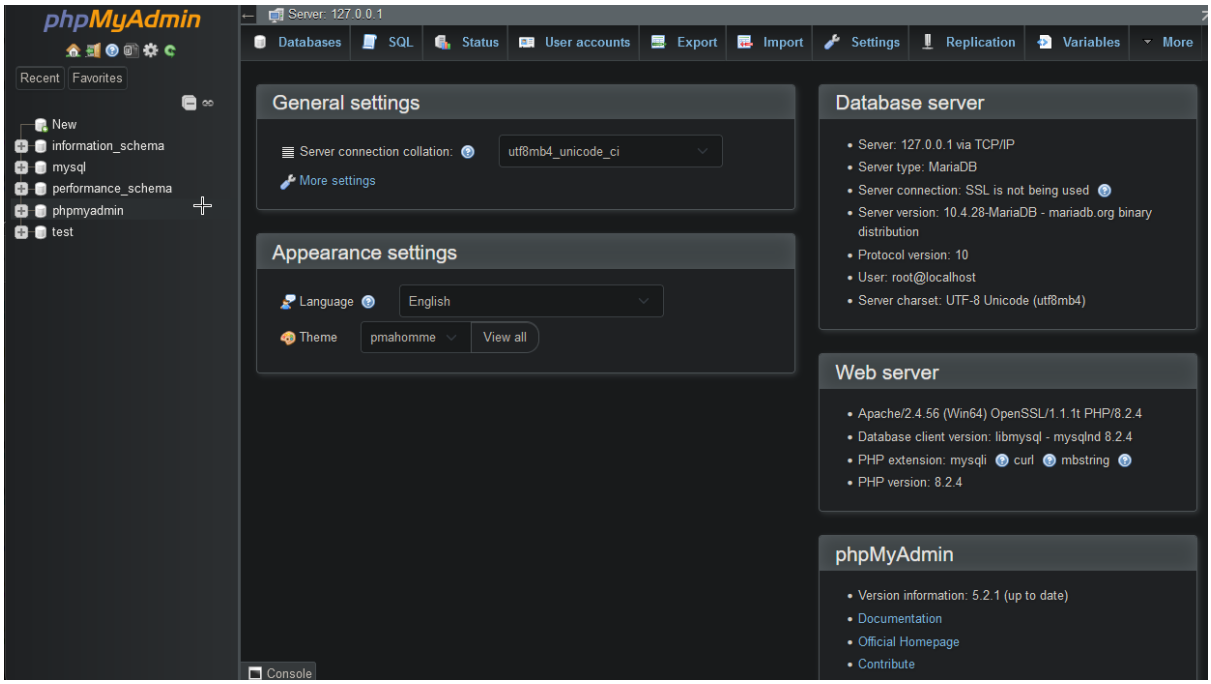


Figure 3.4: PhpMyAdmin interface upon first opening. This is the admin panel for MySQL.

Server Hosting Option 2: Digital Ocean

Digital Ocean (DigitalOcean, no date) is a good option for hosting a database as it is cloud-based and will be accessible to any host that tries to connect. Only one server would need to be set up rather than a server per customer. This would decrease the setup required per customer and would make it much easier in terms of troubleshooting. A downside to Digital Ocean is that it is paid and requires a subscription. Hopefully, this should not be an issue with the GitHub Student Developer Pack

Ways to Test Apollo Defender

During my time doing work experience at Trend Micro as part of my third-year course, I met a colleague who hosts his own servers and would be able to create a dummy network for me to use to test Apollo Defender on. This will be a good testing ground as it can be isolated and set up in many different ways to test possible network configurations that Apollo Defender may encounter.

This setup will be ideal for me as it will allow me the freedom to test my application as often as necessary without worrying about impacting the bandwidth of the network. When testing an application such as Apollo Defender, which will be scanning an entire network, care must be taken to optimise the scans to not affect network performance too heavily. Depending on the size of the network, these scans could take hours to days to complete, based on preliminary testing completed on my home network and as such, the impact on network performance must be minimised to allow for normal network operation to continue as the scans are happening.

Languages

Python

Python is a simple, high-level, lightweight scripting language that was built with an emphasis on speed and compilation at runtime rather than before. Python was conceived in the late 1980s and is now up to the latest stable release of version 3.12 as of November 2023. These are some of the pillars that were kept in mind while developing Python, mentioned in an article about the history of Python on learnpython.com (Ostrowska, 2022)

- Beautiful is better than ugly.
- Explicit is better than implicit.
- Simple is better than complex.
- Complex is better than complicated.
- Sparse is better than dense.
- Readability counts.

Python is highly extensible through the use of libraries and modules. Its syntax is based almost solely on indentation rather than the use of brackets, making it more beginner-friendly. Python is also not a typed language, meaning that variables do not necessarily require a type when creating them; the user can simply assign a value to a variable (string, integer, Boolean, float, etc) and the type of the variable will be determined during runtime. Python is known for being used in the cybersecurity world for scripting due to its speed and efficiency.

I have not learned Python before so using Python for this project would mean learning as I go, but with the simplicity of Python, that would not be difficult. I am also very interested in learning Python as I believe that it will be a very useful language for me to know in the future.

Java

Another option to be considered for languages to use for this project is Java. Java is a high-level programming language that is the polar opposite of Python in many ways. Java is a lot more demanding on the system that it is running on and is not as lightweight or as fast as Python. Java uses a syntax system that is a lot more declarative than Python. All objects in Java have a type, no matter what it is that the user is trying to create. Java is used on billions of devices worldwide and is highly popular. Java is the first language that I learned in college and therefore I have a good understanding of it and would be capable of creating this project using it without having to learn the language. However, I have had many issues with database connections with Java especially and would be wary that this may cause problems further down the line during the development process.

PHP

PHP is a general-purpose scripting language that was designed with a focus on web development and "can be embedded into HTML"(PHP, no date). It is usually interpreted on the side of the web server rather than being executed by a host machine. For this project, PHP will be vital for communicating with databases that are created to store a company's information and as such, I will be using it in my project to do exactly that. I will use prepared statements and pass the necessary parameters to my database for storage in a safe way.

Security Implications

Many security implications must be considered when designing an application such as this. Who will be using the application? How can the application be exploited? What kind of groups would exploit this application? All these questions must be considered when designing an application aimed at improving the cyber security of a business or enterprise.

This application will be of great use to SMEs, as it will allow them to not only identify their assets but also identify the risks that could be posed to them from Advanced Persistent Threats (APTs) and any other maluser.

In the modern age, where new cyber threats are evolving every day, it is vital for all businesses to not only be aware of the threats posed to their assets but also to be aware of tactics that they can use to actively protect these assets. This can include actions such as following frameworks (ISO 27001 & 27002, COBIT, etc) when designing their infrastructure and ensuring that devices are updated regularly. However, following these guides can only get you so far. An SME must have an intimate understanding of the assets they possess and the risks that are posed to them so they can effectively and efficiently mitigate risks. This application aims to help SMEs gain an intimate understanding of their environment.

One very large implication that must be considered is the idea that an APT could use this application to also gain that same understanding of a business's network. Due to this application, in essence, being a network scanner, the utmost caution must be taken to ensure that the functions of the application are secure and cannot be used maliciously. In this regard, this application will take a security-by-design approach.

Summary and Conclusions

In this section, I summarise the research that I have done and come to conclusions on what technologies and languages will best suit my project.

When I first considered how the user would interface with my application, I considered two options: a command line version and a GUI version. In the end, I opted to go for a GUI version, as it would allow me to make it easier for users to perform actions such as scanning multiple VLANS at once. It will also mean that it would not require any complex syntax for a command line version and will allow me to create a simple and appealing GUI version that is both easy to use and understand.

The second conclusion that I have come to during my time doing research for this project is that I should build Apollo Defender from the ground up with security in mind throughout the entire development process. This will ensure that all data handled by the application will be secure.

Next, the technologies that I will be using. From the research that I have conducted, I have concluded that specific languages and technologies will be required to complete this project, such as the NVD API and the use of the PHP language. The NVD API will be vital in finding and categorising the vulnerabilities present on a network. The PHP language will be necessary to allow Apollo Defender to interface with the databases that store the gathered information.

As for the language that Apollo Defender itself will be written with, I have decided that Python is the best option. I have come to this conclusion for many reasons. First of all, Python is an excellent scripting language and is well suited to this type of implementation. Secondly, as mentioned in the section about the NVD API, Python will be ideal for converting and interpreting the data returned from the API due to its excellent use of dictionaries and lists. Finally, Python is a language that I have wanted to learn and program with for quite some time now and I feel that it will benefit me greatly in the future.

Now for the IDE that I will use to program Apollo Defender. After careful consideration, I have concluded that PyCharm will be the ideal IDE to use for the development of the application. I have come to this conclusion based on the fact that I have been using JetBrains products now for many years and am very comfortable with how their products operate, as well as the fact that PyCharm was created specifically for programming in Python. Another plus is that it has more capabilities than VSC as it is a full IDE, rather than a code editor like VSC.

Finally, on to server hosting and testing of the application. I have decided that an implementation using Digital Ocean will be the most ideal route to take as it allows for much more reliable and widespread connectivity to a database associated with a customer.

For testing purposes, I believe that using the servers and hosts provided to me by one of my colleagues from Trend Micro would be the ideal testing ground, as it provides me with an isolated environment in which to test Apollo Defender securely and easily.

Appendix

One of the things that must be taken into consideration when creating Apollo Defender is the order in which the customer will be shown the vulnerabilities on their network. To do this, an algorithm will be required to effectively sort the vulnerabilities so that they can be displayed in a list which orders them from most to least serious. This will link back to the 5x5 risk matrix that was discussed on page 8. When a vulnerability appears in an environment, multiple factors will determine how much of a risk it poses to the customer. Those factors are likelihood, severity, and the extra thing to be considered for this project, the percentage of hosts affected. For example, a high severity, high likelihood vulnerability may appear in an environment, but only affect one host. This will still be an issue but will not rank as high as the same vulnerability if it existed on a large majority of hosts on the network.

Upon receiving the JSON reply from the NVD API, I will convert the information into a dictionary list, which operates on a key: value pair basis. This is very similar to how JSON stores information and therefore it will be simple to convert it from JSON to Python dictionary format. One restriction when using a dictionary list in Python is that the inbuilt sorting method sort() and sorted() can not be applied to a dictionary list as a whole, but the sorting must occur based on dictionary keys. I don't believe that this will be an issue as this is exactly the result that we are looking for, as we wish to sort the vulnerabilities by score, as these scores indicate the severity of the vulnerability. Also due to Python's comparable high speed and efficiency, sorting the returned vulnerabilities using the inbuilt Python sorting methods will be ideal for this task. Writing my own sorting algorithm will not be necessary.

Glossary

SME	->	Small to Medium Enterprise
NVD	->	National Vulnerability Database
IDS	->	Intrusion Detection System
IPS	->	Intrusion Prevention System
VPN	->	Virtual Private Network
API	->	Application Programming Interface
GUI	->	Graphical User Interface
IBM	->	International Business Machines
ACL	->	Access Control List
VLAN	->	Virtual Local Area Network
NIST	->	National Institute for Standards and Technology
CSF	->	Cybersecurity Framework
IP	->	Internet Protocol
MAC	->	Media Access Control
OS	->	Operating System
JSON	->	JavaScript Object Notation
XML	->	Extensible Markup Language
IDE	->	Integrated Development Environment
VSC	->	Visual Studio Code
PHP	->	Hypertext Preprocessor
APT	->	Advanced Persistent Threat

Bibliography

XAMPP (no date) *About the XAMPP project*. Available at: https://www.apachefriends.org/about.html (Accessed: 12 November 2023).

Angry IP Scanner (no date) *Angry IP Scanner - the original IP scanner for Windows, Mac and Linux*. Available at: https://angryip.org/ (Accessed: 16 December 2023).

Adams, M. (2022) *Benefits of Cyber Risk Management: What are the Advantages? - Businesstechweekly.com*. Available at: https://www.businesstechweekly.com/cybersecurity/risk-management/cyber-risk-management/ (Accessed: 16 December 2023).

Brian O'Donovan (2022) *Almost half of Irish SMEs hit by multiple cyber attacks*. Available at: https://www.rte.ie/news/business/2022/1020/1330199-cyber-attacks/ (Accessed: 31 October 2023).

DigitalOcean (no date) *DigitalOcean | Cloud Hosting for Builders*. Available at: https://www.digitalocean.com/ (Accessed: 16 December 2023).

ISO 31000:2018 - Risk management | Enhanced Reader (2018). Available at: https://www.iso.org/publication/PUB100464.html (Accessed: 3 November 2023).

Lansweeper (no date) *Lansweeper | Complete Visibility into Your Technology Assets*. Available at: https://www.lansweeper.com/ (Accessed: 16 December 2023).

Microsoft (2023) *Visual Studio Code - Code Editing. Redefined*. Available at: https://code.visualstudio.com/ (Accessed: 16 December 2023).

Mirza, S.M.S. (no date) *Vulnerability Scanning Frequency | Best Practices*. Available at: https://thecyphere.com/blog/vulnerability-scanning-frequency/ (Accessed: 6 December 2023).

NIST (2023) 'Public Draft: The NIST Cybersecurity Framework 2.0 National Institute of Standards and Technology Note to Reviewers'.

Nmap (no date) *Nmap: the Network Mapper - Free Security Scanner*. Available at: https://nmap.org/ (Accessed: 16 December 2023).

Ostrowska, K. (2022) *A Brief History of Python | LearnPython.com*. Available at: https://learnpython.com/blog/history-of-python/ (Accessed: 6 December 2023).

PHP (no date) *PHP: What is PHP? - Manual*. Available at: https://www.php.net/manual/en/intro-whatis.php (Accessed: 16 December 2023).

Scarfone, K. (2022) *How to Perform a Data Risk Assessment, Step by Step*. Available at: https://www.techtarget.com/searchsecurity/tip/How-to-perform-a-data-risk-assessment-step-by-step (Accessed: 20 November 2023).

NIST (no date) *Vulnerability APIs*. Available at: https://nvd.nist.gov/developers/vulnerabilities (Accessed: 16 December 2023).

SolarWinds (no date) 'What is Network Discovery? - IT Glossary | SolarWinds'.

IBM (no date) *What is risk management? | IBM*. Available at: https://www.ibm.com/topics/risk-management (Accessed: 3 November 2023).