Contents

Introduction

I am planning to create a tool to make network mapping and scanning more user friendly by creating a GUI to quickly invoke common scan types at the click of a button. In addition to the inbuilt scanning, the tool will facilitate the end user to extend the application functionality by allowing users create their own customised scan types and incorporate these scans into the tool for future use.

In this report I will give an overview of network scanning, the types of network scans, the tools available for network scanning, different scanning techniques and more. I will also discuss the technologies I have decided to use in my implementation of a network scanner application and why I chose to use these technologies.

Overview of areas, technologies or topics researched:

Network Scanning

Network scanning involves systematically scanning a computer network to identify active hosts, open ports, and other vital information. It helps assess network security, detect vulnerabilities, and maintain network health and performance. (Anon., n.d.) Network scanning is an essential capability used by both IT professionals and cybercriminals.

Scanning a network enables network engineers to manage maintain and secure networks. Proactive management can help find issues before they turn into serious problems and cause network downtime or compromise of confidential data. (Orebaugh & Pinkard, 2008)

Cybercriminals use the same tools and protocols as network admins to scan potential targets. (Kirvan, 2024) Cybercriminals use these tools to identify vulnerabilities within a network that they could exploit such as open ports.

Why is Network Scanning Important?

There are a variety of different usages for network scans that vary on a case-to-case basis. Here I will outline some of the most common reasons why an individual or organisation would scan their networks.

When considering just how large modern networks have become it would be practically impossible for network engineers to fully assess a network let alone maintain a networks health. With the number of cyber-attacks on the rise and the much lower

barrier to entry for aspiring cyber criminals keeping your network secure is more important now than ever before. By scanning networks, identifying possible vulnerabilities and patching them network engineers can keep their networks safe from potential cyber-attacks.

Aside from the security benefits of frequent network scans, they can also help to improve network performance. When scanning a network, you are provided with extensive knowledge about each device on the network. When analysed this data can be used to identify areas in the network that are bottlenecking traffic or potential misconfiguration such as logical loops in spanning tree protocol.

For many organisations network scanning is also essential for asset identification. Whether it's for security purposes or for risk assessment its essential for an organisation to have a comprehensive list of the assets on their networks and without network scanning it may be impossible for large organisations to get a comprehensive list.

When considering securing your network through the use of tools such as EDR products it's important that every endpoint on the network has the product deployed on it. If an endpoint is not identified and does not have the EDR product installed, then there will be a blind spot in your security. By scanning your network, you will be able to identify and account for all hosts in your environment and ensure that they all meet the same security requirements.

Types of Network Scans

There are conflicting sources on what "types of network scans" refers to.

The first definition refers to the scope of the scans, whether that be a scan of your network internally, externally or specific subsections of the network. Sources that use this definition include: (Anon., n.d.) , (Mikka Convocar, 2023)

The second definition refers to the specific network component the scans target such as TCP/UDP (Transmission Control Protocol/User Datagram Protocol) enabled ports and scanning for known vulnerabilities. Sources that use this definition include: (Anon., n.d.), (InfosecTrain, 2023), (Anon., n.d.).

The clear distinction between these two groups of sources is that the latter is written from a penetration testing perspective. In other words, from the perspective of a threat actor. This is an important distinction as it clearly indicates that network engineers and threat actors view and approach the use of network scanners differently. For the purposes of this project, I will be considering the use cases of both network engineers and penetration testers.

Network Scan Scope

The scope of a network scan refers to exactly how much of a network is being scanned. With the majority of networks being divided into many different subnetworks that may not e able to communicate with each other. In other cases, it is only possible to scan a network form the external internet in which case the possible scope of the scan will be much more limited.

From a pentesting perspective scope can refer to the areas of a network you are allowed to scan. In most cases pentesting is limited to certain parts of the network so it does not interfere with day-to-day operation of the business. If a pentest exceeds this scope legal action can be taken against the pentester for breach of contract so its important to know exactly what is inside and outside of the scope.

Active and Passive Scans

There are two main categories of network scans: Active and Passive scans. Active scans, as the name suggests, actively sends traffic around a network in an attempt to identify the devices present. Passive scans on the other hand attempt to identify the devices on a network by listening for traffic coming and going across the network. Both types of scans have their uses when it comes to network scanning and neither one is capable of getting the full picture of a network without the other.

Port Scans

Port scans as the name suggests targets specific ports throughout a network to see if they are open, closed or filtered. This is very valuable information as it can give us information on the services that a device is running which can be useful for both network engineers and pentesters. Knowing which services are running on a device can allow pentesters to identify vulnerabilities in these services that they can use to gain access to the machine. Network engineers can use it similarly to identifying possible vulnerabilities and take measures to protect against them. They can also be used to identify services slowing down the network or services that should not be running on a machine that may suggest malicious activity.

As previously mentioned, it is important to have a specific scope in mind when performing a scan. When scanning ports, you must choose a scope of what ports you will scan. There are 65,535 ports available to scan on a device, this is a huge number and if you were to scan them all your scan would be unbearably slow. To prevent this a scope is set of port you want to target. Most network scanning tools have this scope set to the 1000 most commonly used ports which will generally be the most useful for a general scan. This greatly increases the speed of a scan but can leave out ports that you

specifically want to target. In these cases, you must select your own scope of ports to scan to look for specific services on the target machines.

Scanning Techniques

TCP

TCP scans are one of the most basic types of network scans available. It is done by sending a SYN (synchronise) packet to the port being targeted, if the port is open, you will get an ACK (acknowledge) packet and a SYN packet in response. The scanner then replies with an ACK packet to complete the three-way handshake. The scanner then sends an RST (reset) packet to reset the connection

If there is no response to the initial SYN packet, then the packet was dropped or blocked by a network security device such as a firewall or IPS (intrusion prevention system) which tells us that the port state is filtered.

If we only get an RST packet in response to the initial SYN packet, then the port is closed.

TCP SYN

This type of scan is commonly referred to as stealth or half-open scanning as it does not open a full TCP connection. For this scan type a SYN packet is sent to the target and if it is open it will respond with a SYN and ACK packet. Rather than replying with an ACK packet to complete the scan we immediately terminate the connection by sending an RST packet. If the port being targeted is filtered or closed it will behave the same as for standard TCP scans.

This has the advantage of being harder to detect than a standard TCP scan as the connection is never completed.

UDP

This scan is also known as connectionless protocol, it works by sending UDP packets to the target. If the target port is open then there will be no response, if the port is closed it will respond with an ICMP packet informing us the port is unreachable.

ICMP

For this scan type an ICMP echo request is sent to the target port, if there is a response from the target it is considered to be “live”. This scan type is very simple but is often not very successful as most firewalls will be set to block ICMP requests.

ACK

This type of scan is unique as it is not used to check for the number of machines on a network or open ports, this scan is used to determine firewall information. This information includes firewall rulesets, if they are stateful or stateless and which ports are filtered.

For this scan an ACK packet is sent to the target, if the target port is open or closed it will respond with an RST packet, these ports are labelled as unfiltered. If the port responds with an ICMP error message or if there is no response, then it is labelled as filtered. This is the basic function of the scan, but it is capable of finding out more information about the firewall using a combination of packets specified in the command before the scan starts.

TCP FIN

For this scan type no connection is established to the target. The scanner sends a FIN packet to the target. If there is no response then the port is open, if the port is closed the target will respond with an RST and ACK packet.

This type of scan only works against Linux and older versions of Windows, never versions have protections in place.

XMAS

This type of scanning sends packets to the target with multiple flags such as FIN, PSH and URG, this “lights up the packet like a Christmas tree” (Srivastava, 2021) which is where the name XMAS scan comes from. If the target port is open, it will be unable to process the packet and it will drop it, if the port is closed it will respond with and RST and ACK packet.

Null

For this scan a TCP packet is sent to the target that contains a series of zeroes. As there are no flags set the target will not be able to process the packet so it will discard it. This tells us that the port is open as if it was closed it would not have attempted to process the packet. If the port is closed, we will receive a response from the target in the form of RST and ACK packets.

(Srivastava, 2021)

(Lyon, n.d.)

Challenges and Limitation of Network Scanners

Network scanners are not perfect, they can miss things on the target network as well as come back with false positives/negatives. These can give network engineers a false sense of security believing that their network is fully secure when it is not

Network scanners are also notoriously resource intensive especially when the target network is large. Some scanners intentionally slow their processes down when scanning which will prevent any crashing, but it can take hours to days to scan larger networks at these speeds. Alternatively, some scanners utilise multi-threading to scan networks as quickly as possible using resources as efficiently as possible. This works great for simple scans but cannot be used for more complex scan types as they would require too many resources to be completed quickly.

Network Scanner Applications in Cybersecurity

Network Scanners are used for two main purposes: by network administrators/engineers to maintain their networks and by threat actors looking for network vulnerabilities.

Network administrators use network scanning tools to get an up-to-date picture of their networks. By doing this they can keep the network healthy by identifying possible vulnerabilities or irregularities in network traffic and attending to them to keep the network secure.

Threat actors use network scanners in much the same way as network engineers however they are trying to exploit any possible vulnerabilities.

Commonly used Network Scanning Tools

There are a variety of network mapping tools available both open source and proprietary tools. Some of these tools are more general while some are specialised for specific roles

Nmap “Network Mapper”:

Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. (Anon., n.d.) Nmap is a very powerful tool as it has a vast range of scan types that can be further extended using custom scripts that give advanced functionality. Nmap is powerful but it is held back by the fact it does not have a GUI and has a steep learning curve.

Nessus API:

python-nessus is an Apache 2 Licensed Nessus library, written in Python, for security auditors and pentesters. (Kaiser, 2014) The most obvious drawback to using Nessus is the high cost. As a licenced product Nessus is very expensive, especially for my use case in this project. Putting the price to the side Nessus API is limited in its capabilities ‘Note: Beginning with Nessus Professional version 7, some endpoints, such as those used to create and launch scans, are no longer available from the API. This only impacts Nessus Professional.’ (Anon., 2024) This is rather disappointing as when using the Nessus API your capabilities are more limited than just using the Nessus application. These limitations make it unsuitable for my use case as I would require the ability to launch scans using the API.

Masscan:

Masscan prioritises speed, according to its author Robert Graham, it only takes "6 minutes at around 10 million packets per second" to fully scan the entire Internet. (Dewan, 2017) This speed can be an advantage if time of the essence. However, this focus on speed comes with limited capabilities as advanced features would slow the scan down considerably.

Advanced IP Scanner:

Advanced IP Scanner is a powerful, free network scanner with a user-friendly GUI. The power Advanced Ip Scanner gives a user alongside its ease of use and the fact its freely available, have made it extremely popular among network engineers and cybercriminals alike. Some advanced users may find that Advanced IP Scanner is a bit lacking in features they may need to fully customize their scans, however this is only a small percentage of users and for most use cases it will get the job done with no fuss.

Wireshark

Unlike the other network scanners I have talked about Wireshark is a passive network scanning tool. It operated by capturing packets traversing the network giving the user insight into the devices sending traffic across a network and the types of traffic on the network.

This can be very limiting as Wireshark will need to be deployed on the network and if the network is properly segmented then it will be blind to sections other than the section its on. Furthermore, if there are devices that do not send or receive much information over the network then Wireshark may not see this machine leaving the data collected incomplete.

My Choice of Network Scanning Tool

For the purposes of my project, I have decided to use Nmap. I have decided on this because of its huge variety of features, ensuring that users will not be limited when using the tool. It also provides me with the opportunity to fully customise the application to suit my needs and allow some level of customisation to other users to meet theirs.

Coding Language

When it comes to programming languages there is no one language that is better than every other but different languages are better suited for different tasks. I will be going over some popular programming languages and determine which one is best suited for this project.

JavaScript:

JavaScript is the single most used programming language in the world. (Anon., 2024) It's easy to see why JavaScript is almost ubiquitous across the web, it allows developers to increase the functionality of their websites and web applications far beyond what is possible using html and CSS. JavaScript also has some lesser known uses such as in developing browser extensions. Across the board JavaScript is a functional programming language with a huge userbase and wide variety of uses. For this project JavaScript shines as a language used to develop applications with high amounts of functionality and its access to the Nmap API.

Python:

Python is considered to be one of the easiest languages to learn as it has simple syntax and is very human readable. Python has a huge variety of open-source libraries that make it extremely versatile which often leads to it being called the 'Swiss army knife' of programming languages. This ease of use and versatility are what have led to python being the third most used programming language in the world. (Anon., 2024) For the purposes of this project python has libraries for backend frameworks, network scanners and GUI's.

Java

Despite their names, java and JavaScript have no relation. Java is a low language closer to C than it is to JavaScript. Despite their differences both Java and JavaScript are used for application development. Java is commonly used because of its portability; java will run on most platforms seamlessly once written. This harkens back to primary goal of Sun Microsystems when Java was developed "write once, run anywhere" (Anon., 2007). For the purposes of this project Java would excel at building an application that would

word across a variety of platforms. Similarly to Python, Java has libraries for backend frameworks that would make development much quicker and easier.

My choice of Programming Language

For the purposes in this project Python is the most suitable language as it offers many features I will be using as importable libraries, simplifying development. JavaScript does not have an easily importable backend framework; Java lacks the ease of use that Python and JavaScript have as it is a lower-level language which would complicate development. These factors alongside the huge Python community and easily available resources pushed me to use Python for this project.

Backend Framework

For the purposes of my project, I will require a backend framework for my application. A Web framework is a collection of packages or modules which allow developers to write applications or services without having to handle such low-level details as protocols, sockets or process/thread management. (Anon., 2024) There are many backend frameworks available with a variety of advanced features and ease of use features for people at every stage in their development journey. I am not experienced in web development so I will be prioritising ease of use and clear, readily available documentation when choosing a backend framework to use for this project. As previously mentioned, I will be using Python for the functionality of my app. This decision along with my inexperience with backend development have heavily contributed to my decision to use a Python backend framework for this project. I am already familiar with Python and many Python backend frameworks are extremely well documented with very active communities where information may be easily found.

Django:

'The Django python framework is the most popular Python web framework for rapid web development. It helps experienced developers save time by allowing them to focus on their website's content rather than coding from scratch.' (Ojumoro, 2022) Django is most suitable for developing large scale applications. It includes features such as authentication, admin interfaces and Object-Relational Mapping. This wealth of included features appeal to developers as it can save a lot of time and allows developers to use advanced features without in-depth knowledge of how everything works.

Flask:

Unlike Django, Flask is considered a micro web framework as it lacks certain features present in true web frameworks. This makes it much more lightweight and flexible than Django making it more suitable for smaller applications. Due to Flask's small size it I fast compared to other web development frameworks that are more complex. A

disadvantage of this lightweight construction is that a developer using Flask will have to manually add and configure any additional functionality required. This requirement to manually configure additional features appeals to some developers who want more control over their project.

Pyramid:

Pyramid is neither a micro web framework nor a mega framework. It was created with the idea to fill in this gap between the two extremes for developers. ‘Pyramid was made for just this. It's a Goldilocks Solution: not too small, not too big, just right.’ (Anon., n.d.) Pyramid is designed to start small and lightweight and then scale with the project over time allowing it to support the smallest and largest of projects.

References

Anon., 2007. *JAVASOFT SHIPS JAVA 1.0*. [Online]
Available at:
https://web.archive.org/web/20070310235103/http://www.sun.com/smi/Press/sunflash/1996-01/sunflash.960123.10561.xml
[Accessed 10 November 2024].

Anon., 2024. *An introduction to the Nessus API: Generating session tokens and API keys*. [Online]
Available at: https://community.tenable.com/s/article/An-introduction-to-the-Nessus-API-generating-session-tokens-and-API-keys?language=en_US
[Accessed 5 October 2024].

Anon., 2024. *Most used programming languages among developers worldwide as of 2024*. [Online]
Available at: https://www.statista.com/statistics/793628/worldwide-developer-survey-most-used-languages/
[Accessed 18 October 2024].

Anon., 2024. *WebFrameworks - Python Wiki*. [Online]
Available at: https://wiki.python.org/moin/WebFrameworks
[Accessed 19 September 2024].

Anon., n.d. *Network Scanning*. [Online]
Available at: https://www.greycampus.com/opencampus/ethical-hacking/network-scanning
[Accessed 20 September 2024].

Anon., n.d. *Chapter 1. Getting Started with Nmap | Nmap Network Scanning*. [Online]
Available at: https://nmap.org/book/intro.html
[Accessed 5 October 2024].

Anon., n.d. *Network Scanning*. [Online]
Available at: https://www.atera.com/glossary/network-scanning/
[Accessed 23 September 2024].

Anon., n.d. *Welcome to Pyramid, a Python Web Framework*. [Online]
Available at: https://trypyramid.com/
[Accessed 25 September 2024].

Anon., n.d. *What is Network Scanning? What Are Different Types of Scanning in Ethical Hacking?*. [Online]
Available at: https://www.tutorialsfreak.com/ethical-hacking-tutorial/what-is-network-

scanning-and-its-types
[Accessed 20 September 2024].

Dewan, C., 2017. *Master Penetration Testing with Masscan: Scan the Internet in Minutes | Infosec*. [Online]
Available at: https://www.infosecinstitute.com/resources/penetration-testing/masscan-scan-internet-minutes/
[Accessed 8 October 2024].

InfosecTrain, 2023. *Types of Network Scanning for Ethical Hacking*. [Online]
Available at: https://medium.com/@Infosec-Train/types-of-network-scanning-for-ethical-hacking-254de2876091
[Accessed 20 September 2024].

Kaiser, Q., 2014. *PyNessus : Nessus REST API client.*. [Online]
Available at: https://python-nessus.readthedocs.io/en/latest/#api-documentation
[Accessed 5 October 2024].

Kirvan, P., 2024. *What is network scanning? How to, types and best practices*. [Online]
Available at: https://www.techtarget.com/searchnetworking/definition/network-scanning
[Accessed 23 September 2024].

Lyon, G. ". , n.d. *Chapter 5. Port Scanning Techniques and Algorithms | Nmap Network Scanning*. [Online]
Available at: https://nmap.org/book/scan-methods.html
[Accessed 26 10 2024].

Mikka Convocar, J., 2023. *What is Network Scanning? (& Why is It Important for Your Business?)*. [Online]
Available at: https://www.itsasap.com/blog/what-is-network-scanning
[Accessed 18 September 2024].

Ojumoro, I. F., 2022. *The Top 4 Python Backend Frameworks for Your Next Project*. [Online]
Available at: https://pieces.app/blog/the-top-4-python-back-end-frameworks-for-your-next-project
[Accessed 21 September 2024].

Orebaugh, A. & Pinkard, B., 2008. *Introducing Network Scanning*. [Online]
Available at: https://www.sciencedirect.com/topics/computer-science/network-scanner
[Accessed 23 September 2024].

Srivastava, A., 2021. *Demystifying Nmap Scans At The Packet Level ≈ Packet Storm*. [Online]

Available at: https://packetstormsecurity.com/files/163710/Demystifying-Nmap-Scans-At-The-Packet-Level.html
[Accessed 25 10 2024].