



1. Introduction

Safety online is now more important than ever as there are new ways being constantly developed to breach systems, therefore it is important to ensure users how simple it can be to take steps to keep themselves safe. There is a gap for this in research as it describes to people what the technologies are and what their potential is but it does not detail effective countermeasures and how technologies can also be used to great benefits even at an entry-level for non-specialist individuals.

This project aims to highlight the importance of integrating new and upcoming technologies into preexisting technologies and networks. Its focus is on researching and applying various tools and methods to a network environment to study the benefits of security they can offer but also analyse the tools for any vulnerabilities and how they can synergise with other tools/methods.

2.Aims & Objectives

Aim:

The aim of the project is to research and implement methodologies and tools into a network to ensure its security in a home/small business setting.

Objectives:

- Develop/simulate a pre-existing network to conduct penetration testing within said network
- Research capabilities of both general and specialist use applications
- Apply penetration testing tools to conduct reconnaissance of my structure network
- Use any found vulnerabilities to attempt to penetrate the network and evaluate the effectiveness of defensive tools
- Correct vulnerabilities using a range of methods and tools
- Write up and record findings and evaluate the importance of defensive tools to keep system secure

3. Research

The research conducted for the project looked into security technologies and new upcoming technologies being introduced into industry such as NGFW'S, vulnerability scanners and AI machine learning:

NGFW'S: NGFW'S have integrated features such as application awareness, deep packet inspection, and intrusion detection capabilities.

These new features of NGFW's are a significant improvement from their predecessor as they provide a system with a simple secure solution that can be easily applied to any device.

Vulnerability scanners: Vulnerability scanners such as Nessus and OpenVAS are used to identify security weaknesses in systems and applications. These tools are extremely beneficial to make use of within a network environment as they perform automated assessments, scan the system for known vulnerabilities, outdated software, and misconfigurations.

AI Machine learning: The integration of Explainable AI (XAI) in cybersecurity tools is being explored to address the interpretability issue [12]. XAI models aim to make AI decision-making processes more transparent and understandable to human users, enabling cybersecurity professionals to trust the AI's findings and take appropriate action. This is especially important in network security, where decisions need to be made rapidly and accurately.

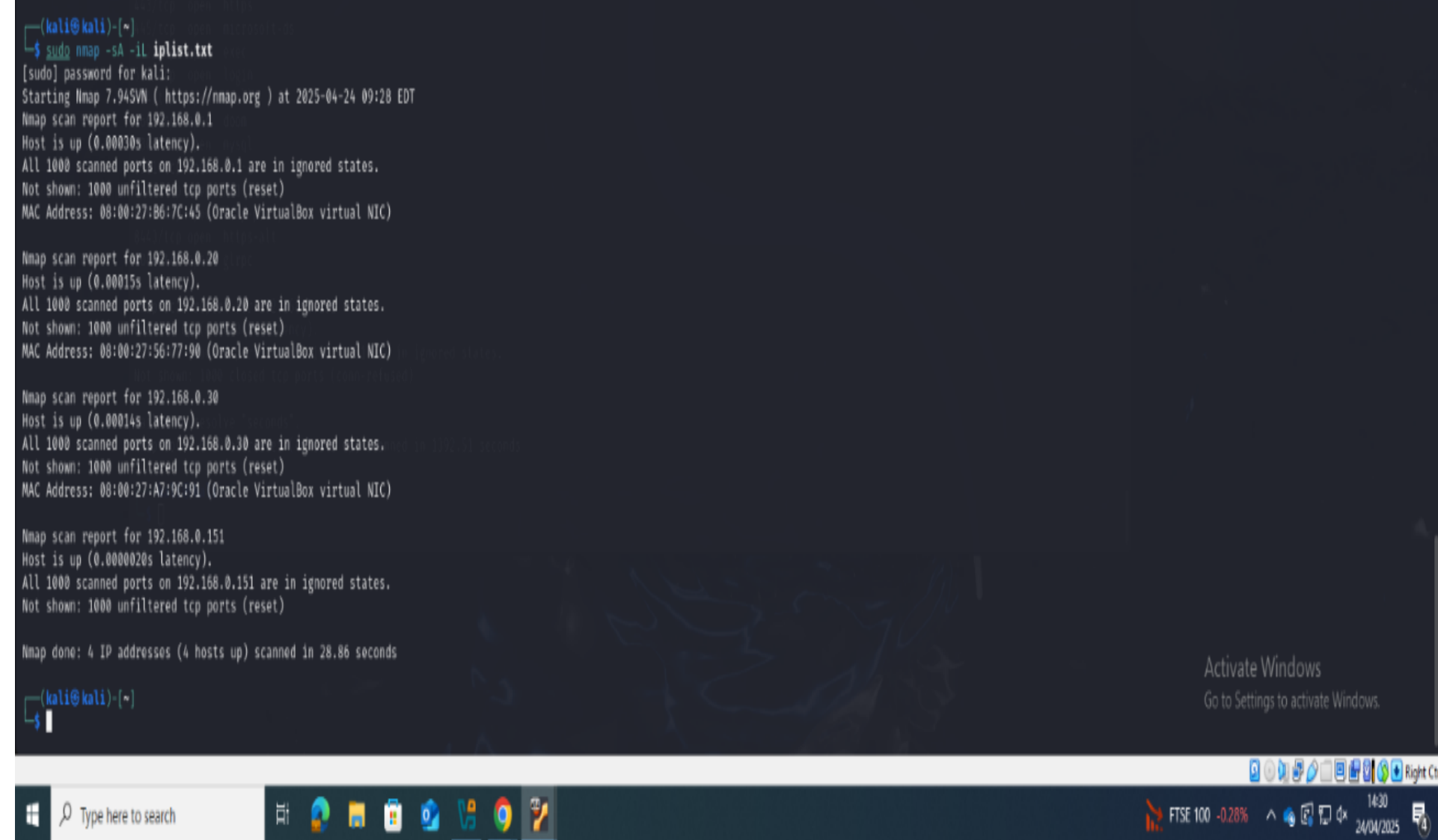
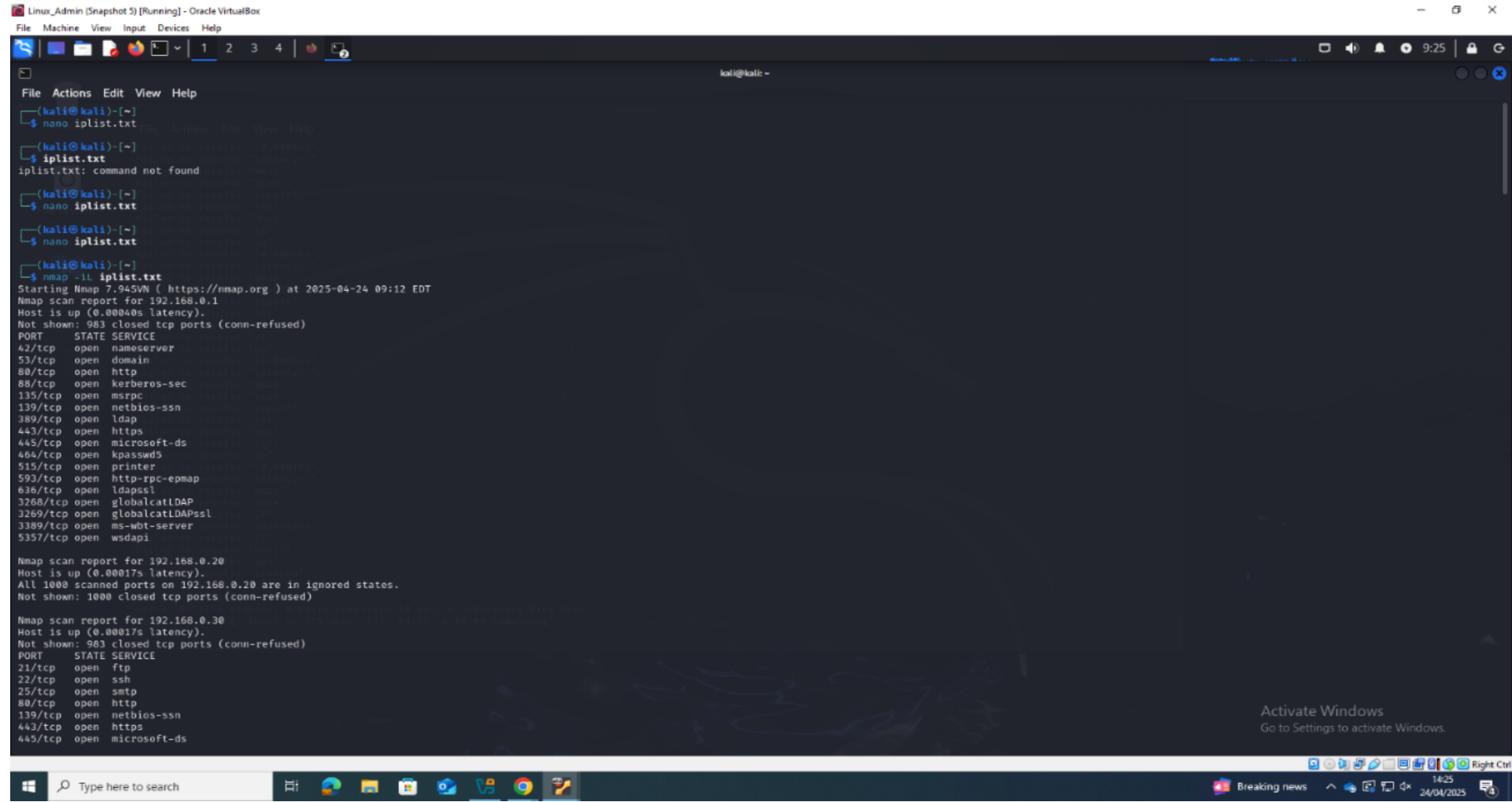
4. Design & Implementation

The final model of my network used a set list of devices I included within my final report draft this list details the devices used within the network along with their IP address and subnets also included with the list is my scope and test boundaries which include the devices/software I wanted to test during the security testing stage of the project this helped throughout the course of the project as I was always aware of what I needed to be testing and the limits I needed to stay within

IP Address	IP Addresses	Hostname	Primary Role	Roles	Sysname	Machine Type	Vendor	Location	Contact	System Description	Poling Method
192.168.0.30	192.168.0.30:f...	192.168.0.30	SNMP Node	SNMP N...	bee box	net-emp - Linux	net-emp	Every bee ...	Your mast...	Linux bee-box 2.6.24...	SNMP
192.168.0.1	192.168.0.1	Practise_Tas...	ICMP Node	ICMP N...		Unknown	Unknown				ICMP
192.168.0.20	192.168.0.20	192.168.0.20	ICMP Node	ICMP N...		Unknown	Unknown				ICMP
192.168.0.151	192.168.0.151	192.168.0.151	ICMP Node	ICMP N...		Unknown	Unknown				ICMP
		IP Range192...	Network Segm...	Network...		Unknown	Unknown				None

5.Testing & Results

The findings from my project directly support the theories and arguments presented in my literature review. Specifically, I found that combining and synergizing various cybersecurity tools creates a more robust and secure framework for network functionality. This layered defence approach not only strengthens the overall system architecture but also acts as a deterrent to potential malicious activity by limiting exploitable entry points. I partially met my aims and objectives in this project. I successfully used reconnaissance tools to identify and map out the target system, effectively gathering valuable data on the network. However, I encountered challenges when attempting to exploit the system due to issues with the simulated network environment. These complications prevented me from fully executing that part of the project, although the results I was able to gather still aligned with the expectations outlined in my original hypothesis.



6.Conclusion

In this project, I focused on addressing the fear and misunderstanding around new technologies—especially in cybersecurity—by showing how simple tools and methods can be used to keep a small network secure. A lot of existing research talks about what technologies like AI can do, but not how everyday users can actually use them to protect their own systems. That's the gap I wanted to explore. To do this, I created a simulated network that mirrors a typical home or small business environment. I then applied real industry-standard tools—like Nmap, Metasploit, Nessus/OpenVAS, Wireshark, and Cisco Packet Tracer—to conduct penetration testing, vulnerability scanning, and security assessments. My goal wasn't just to find and exploit vulnerabilities but also to show how easy it can be for regular users to understand and improve their network security.

References

- [1] T. Zhang, H. Qiu, M. Mellia, Y. Li, H. Li and K. Xu. T. Zhang, H. Qiu, M. Mellia, Y. Li, H. Li and K. Xu. Interpreting AI for networking: Where we are and where we are going. Interpreting AI for networking: Where we are and where we are going. *IEEE Communications Magazine* *IEEE Communications Magazine* 6060(2), pp. 25–31. pp. 25–31. 2022. Available: <https://ieeexplore.ieee.org/abstract/document/9722797>. DOI: 10.1109/MCOM.001.2100736.
- [2] L. Song, X. Hu, G. Zhang, P. Spachos, K. N. Plataniotis and H. Wu. L. Song, X. Hu, G. Zhang, P. Spachos, K. N. Plataniotis and H. Wu. Networking systems of AI: On the convergence of computing and communications. *IEEE Internet of Things Journal* 99(20), pp. 20352–20381. pp. 20352–20381. 2022. Available: <https://ieeexplore.ieee.org/abstract/document/9766416>. DOI: 10.1109/JIOT.2022.3172270.
- [3] M. Latah and L. Toker. M. Latah and L. Toker. Artificial intelligence enabled software-defined networking: A comprehensive overview.