ANALYZING AND INTERPRETING OF DOMAIN NETWORKS USING NMAP

BY

SOMKENE RICHARD

10th OCTOBER, 2024.

EXECUTIVE SUMMARY

A thorough scan, including ping and traceroute scan, was conducted on two domains (alphablocks.tech and gtbank.com) to assess their network details. The key finding from the scan revealed that over 300 ports were open on gtbank's network, while none were detected on alphablocks' network. The presence of so many open ports poses a significant risk, making gtbank's network vulnerable to potential attacks by threat actors.

INTRODUCTION

Nmap, a powerful tool for network discovery and security auditing, plays a crucial role in the cybersecurity field. By deploying Nmap on a domain, organizations can identify and address vulnerabilities in their networks before threat actors can exploit them.

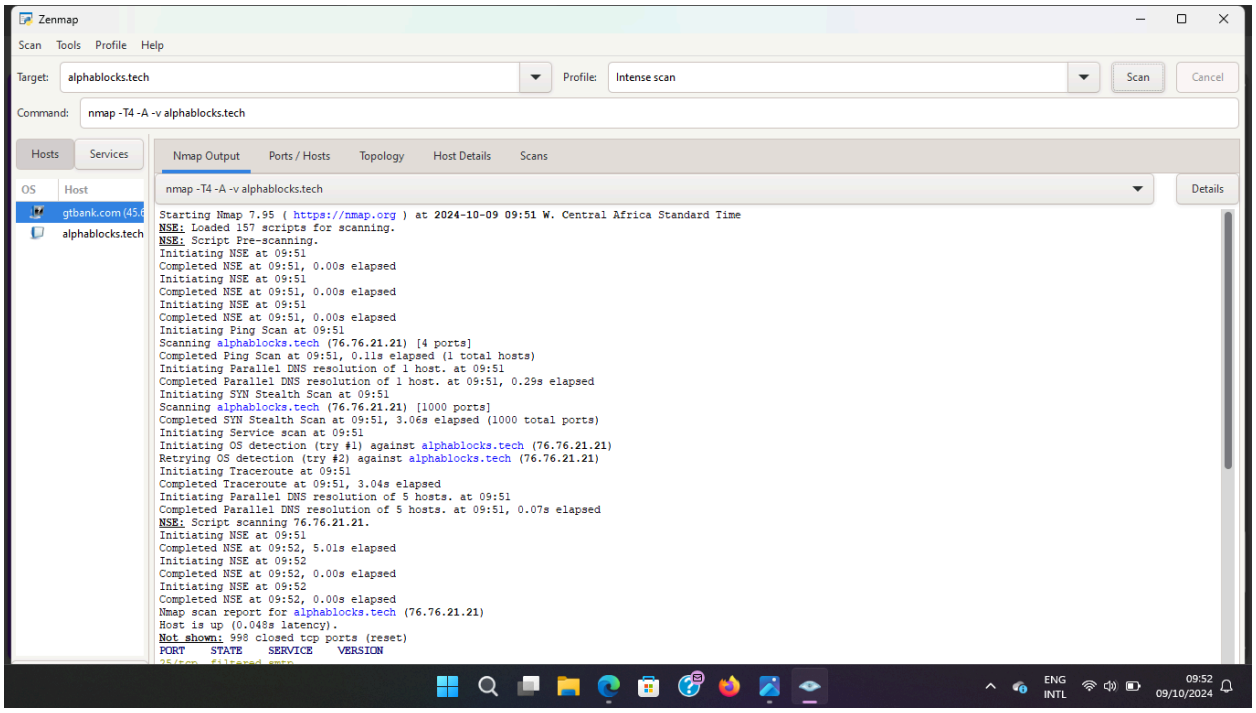
In this report, Nmap was used to conduct an in-depth scan, including ping and traceroute scans, on two domains (alphablocks.tech and gtbank.com) to assess their network details and uncover any potential vulnerabilities.

TOOL

Nmap

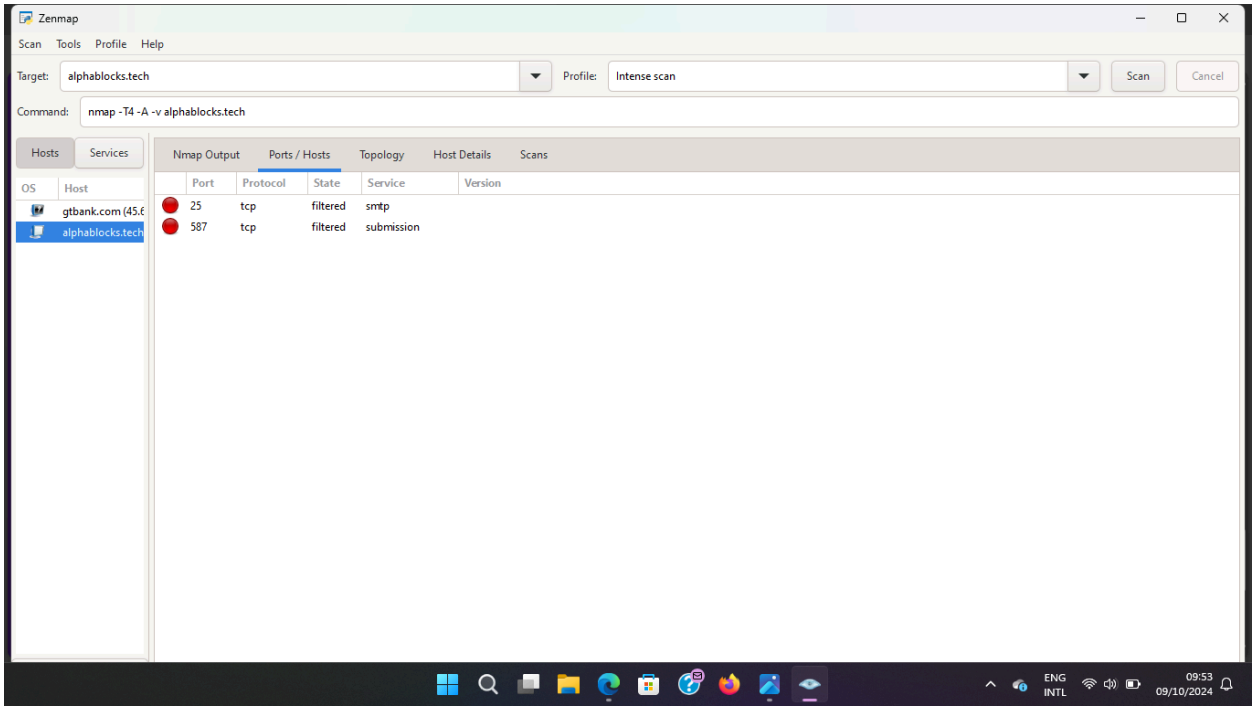
ANALYSIS

alphablocks.tech



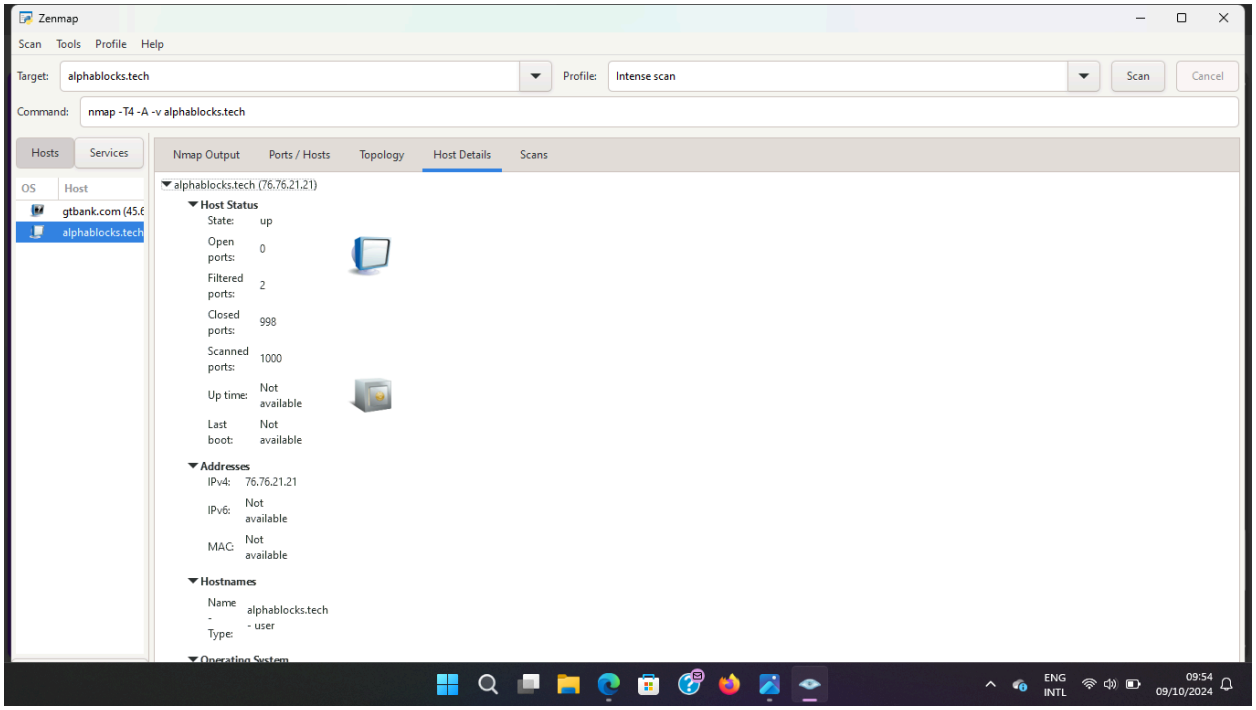
Nmap output of an intense scan result for alphablocks.tech

The Nmap output shows an overview of the intense scan done on the domain.

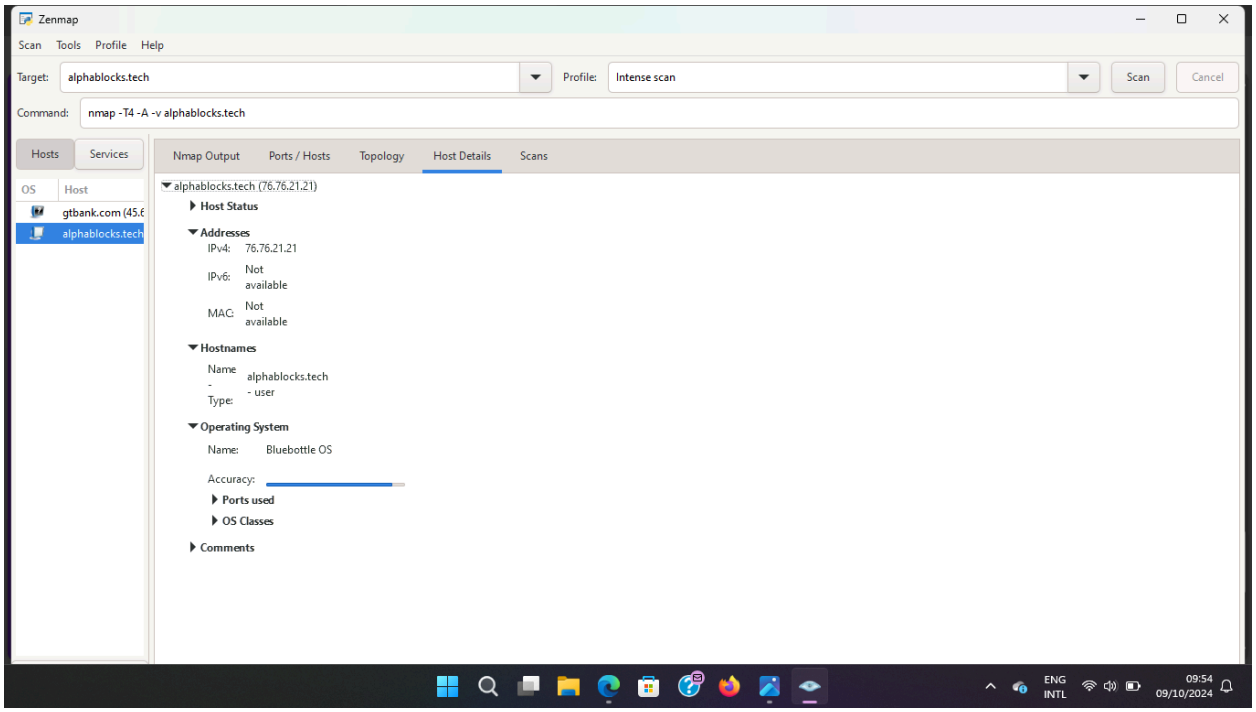


Port status from the intense scan on alphablocks.tech

The state of ports 25, 587 were filtered indicating that access to them and their services are protected by firewall. In respect to that, they can't be exploited.



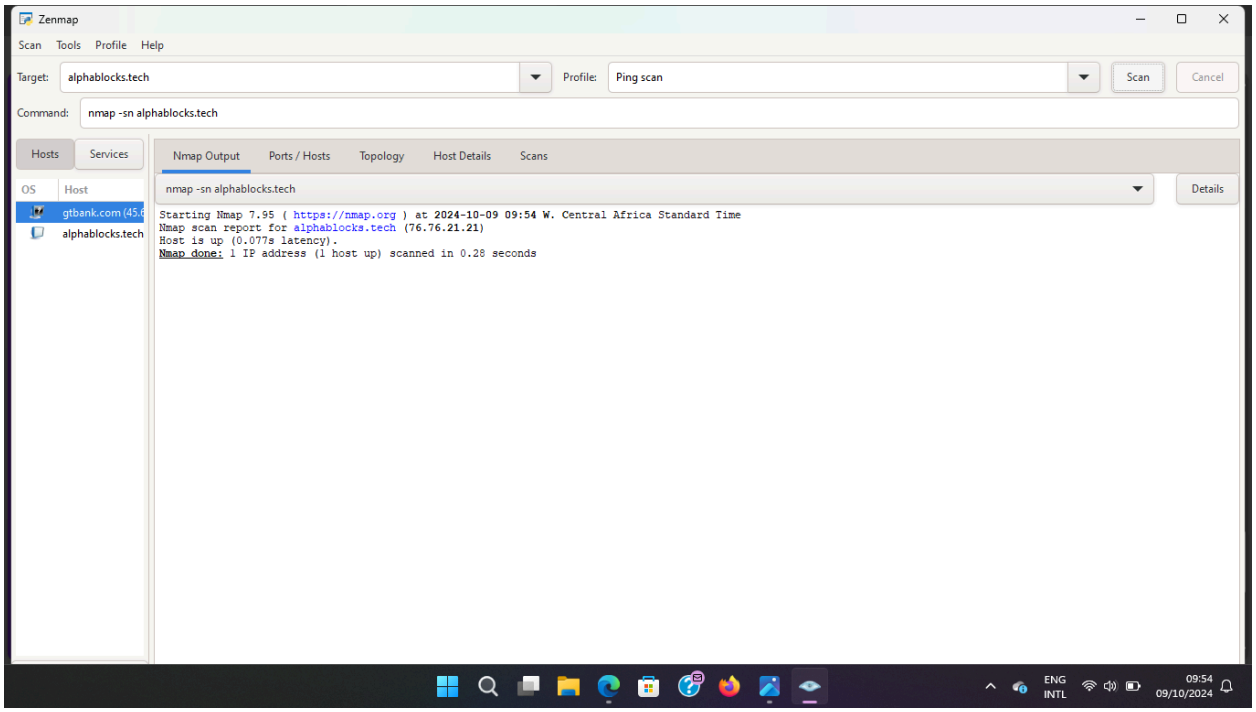
More details from the intense scan on alphablocks.tech



Based on the intense scan result above:

- Out of 1000 ports scanned, none were found open.

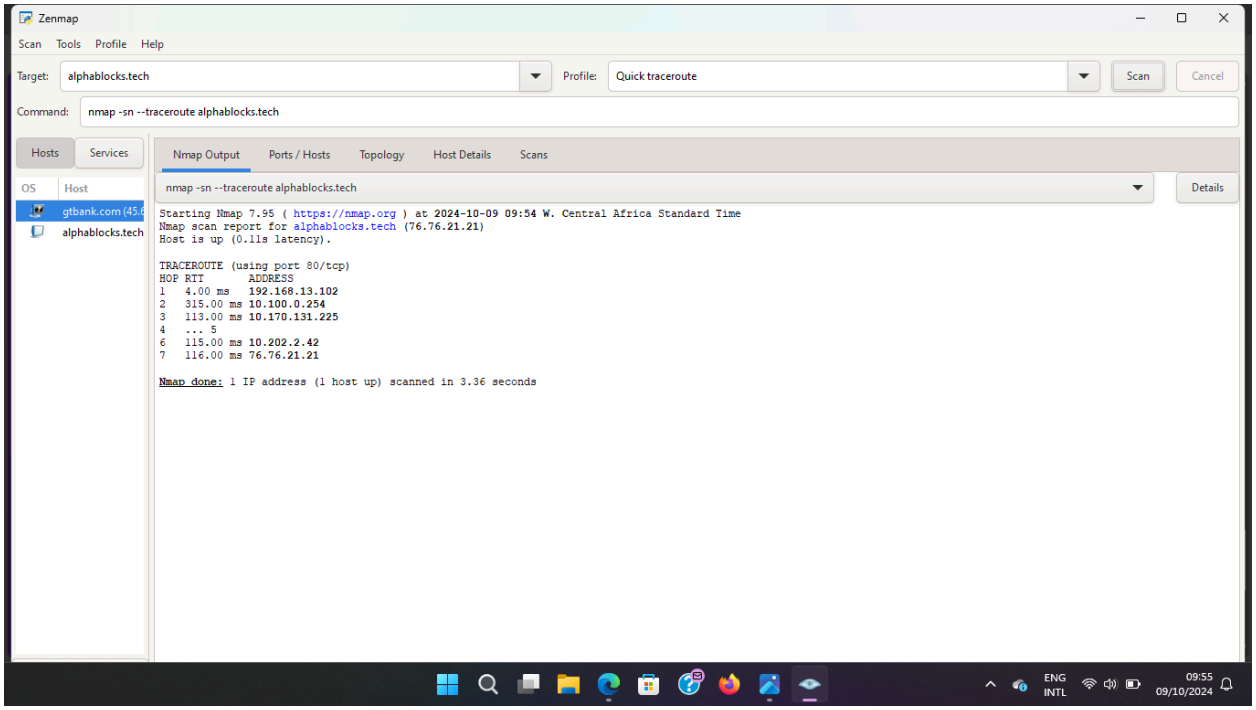
- 998 of the ports were confirmed to be closed, while 2 were marked as 'filtered' due to firewall interference.
- The IPv4 address of the domain was detected.
- The host was identified as running the Bluebottle operating system.



Ping scan result for alphaBlocks.tech

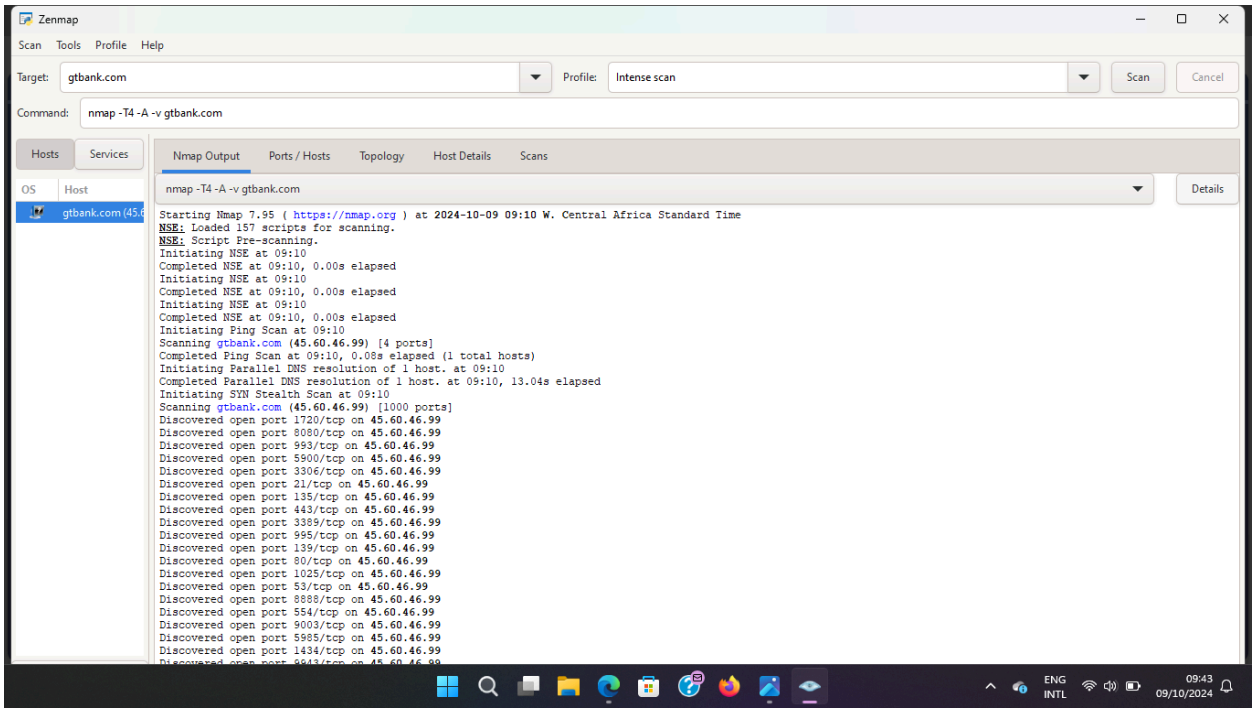
Based on the scan result:

- The IPv4 address of the domain was detected
- The status of the host is active hence the "host is up"

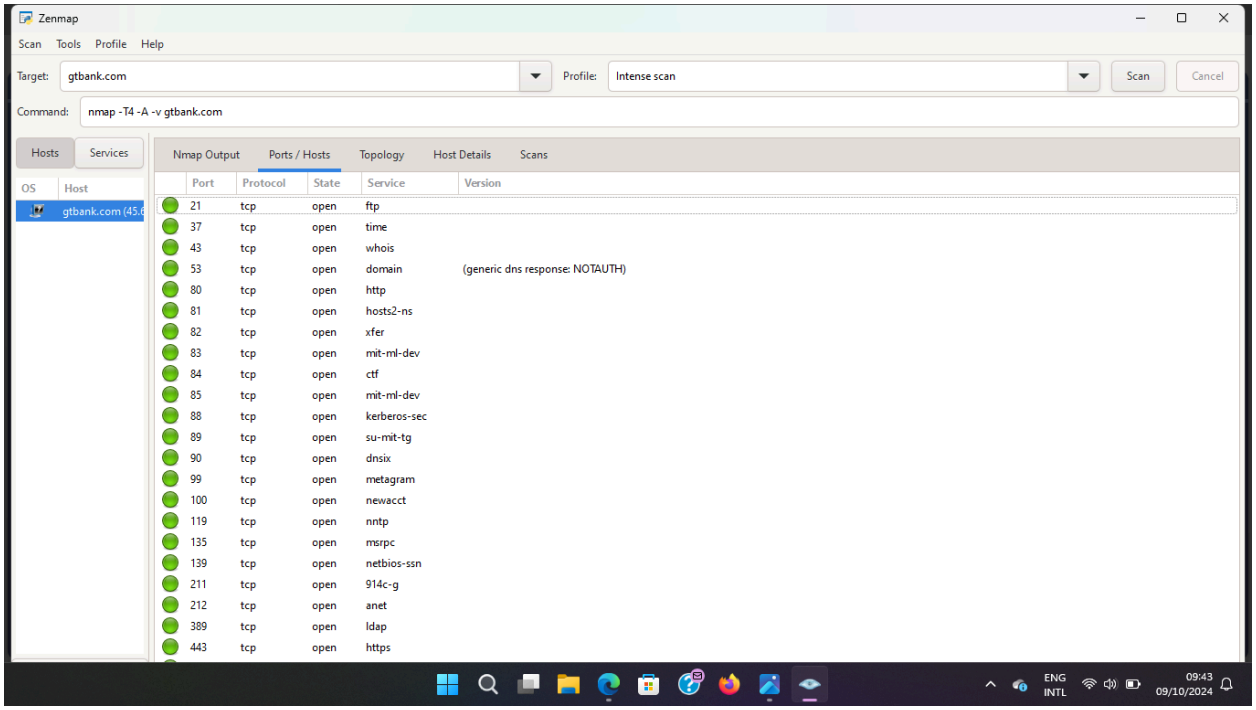


Traceroute scan result for alphablocks.tech

Gtbank.com

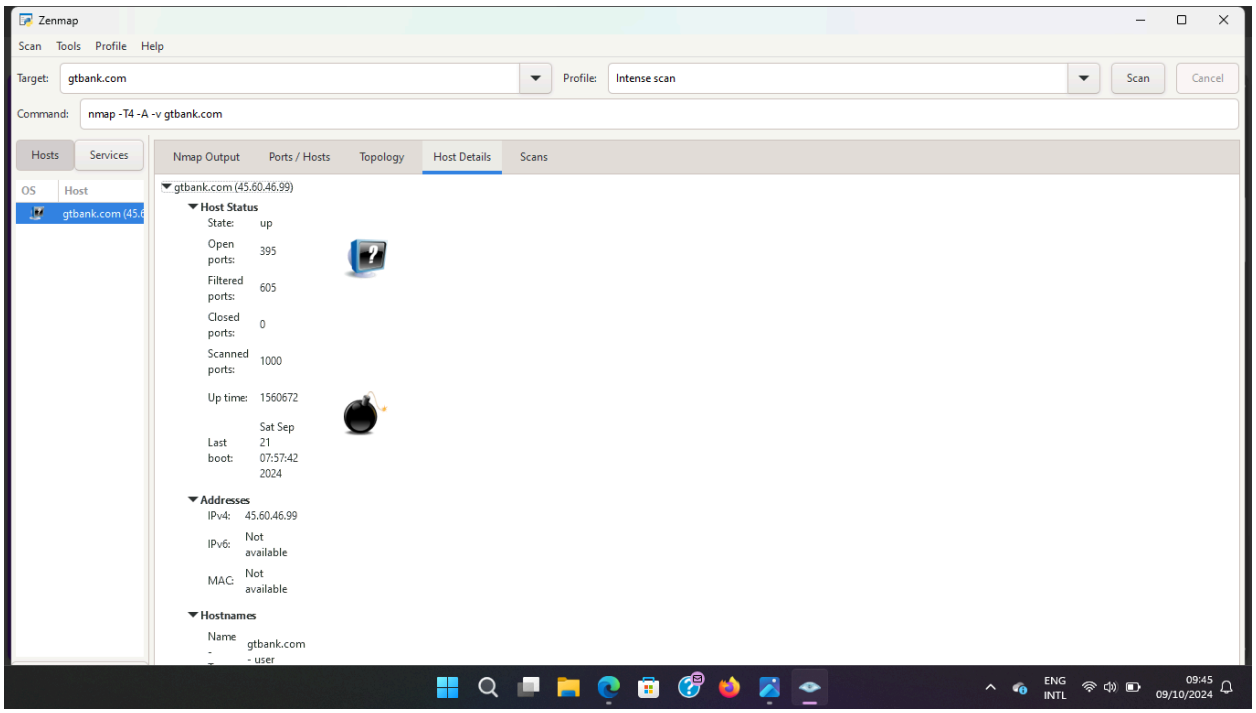


Nmap output of an intense scan done on gtbank.com



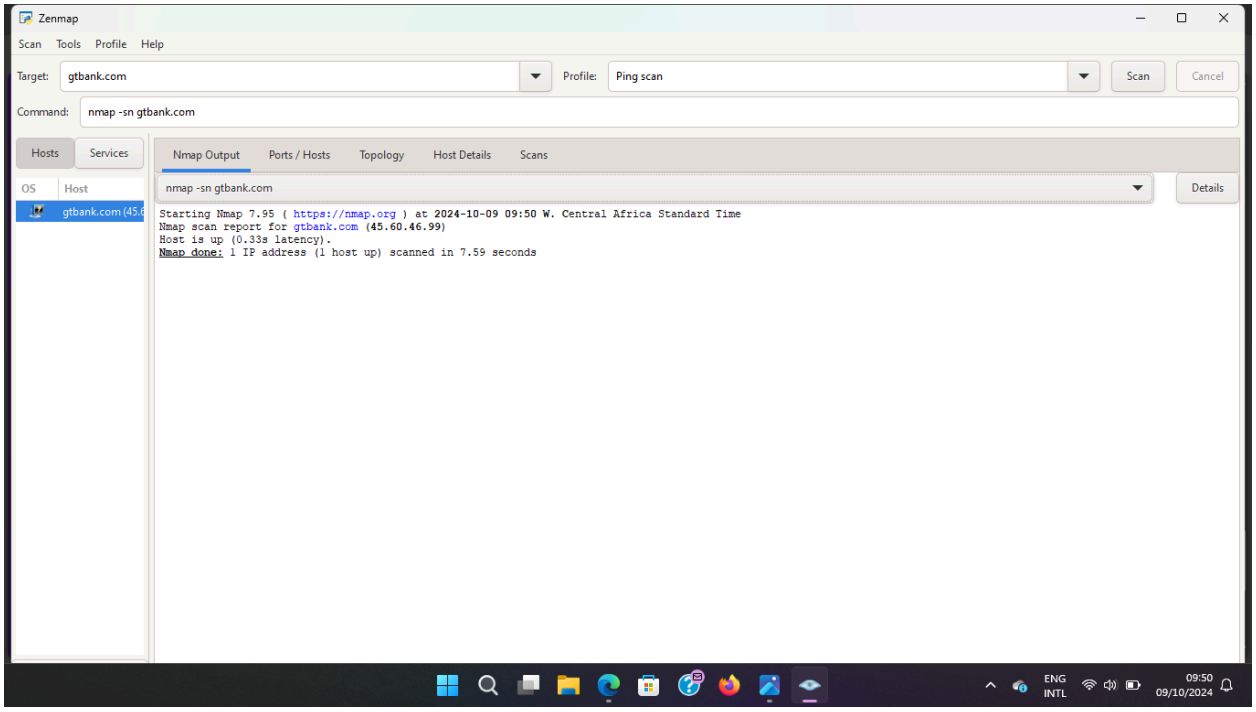
Port status from the intense scan of gtbank.com

Lots of ports on the gtbank.com network were seen to be open, making the system vulnerable to threat attacks.



Based on the scan result above:

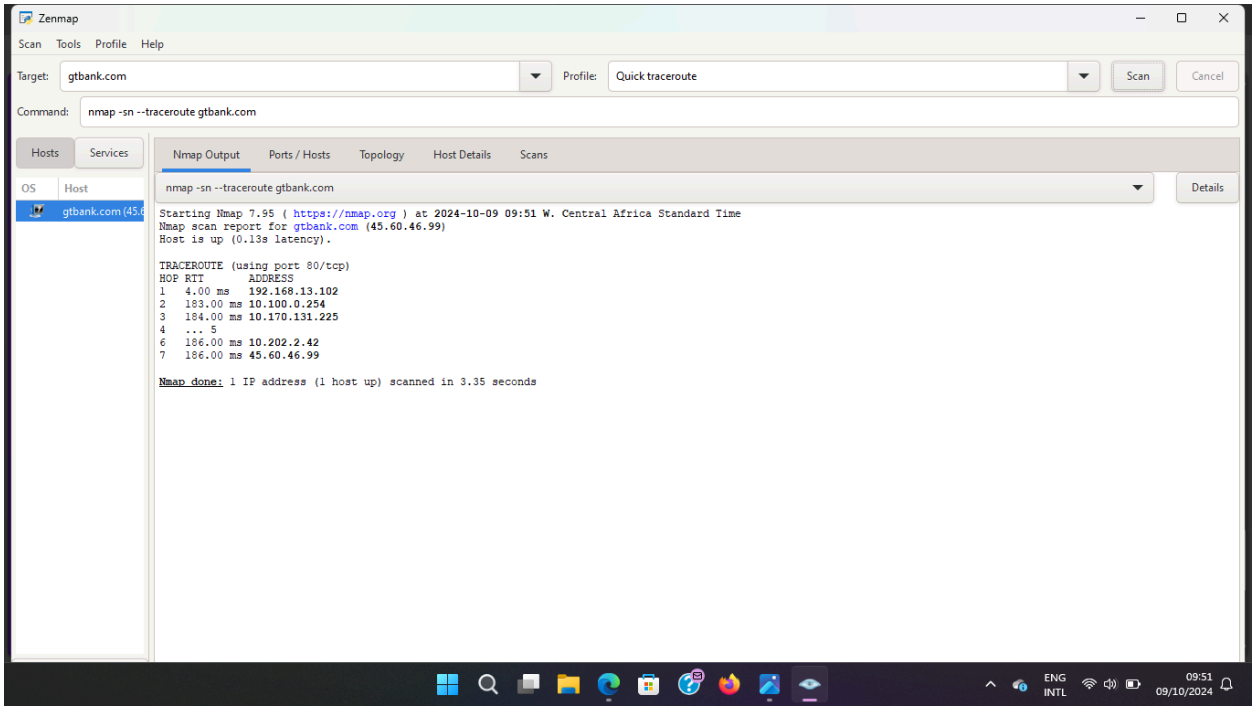
- Out of 1000 ports scanned, 395 were found to be open
- None of the ports were seen to be closed, while 605 were marked as 'filtered' due to firewall protection.
- The IPv4 address of the domain was detected.
- The operating system of the host wasn’t identified



Ping scan result for gtbank.com

Based on the scan result:

- The IPv4 address of the domain was detected
- The status of the host is active hence the "host is up"



Traceroute scan result for gtbank.com

RECOMMENDATIONS

Based on the analysis of the network for gtbank.com, I suggest the following actions to improve security:

1. Close Unused Ports: Any ports that are not actively needed should be closed to reduce exposure. This helps minimize the attack surface.

2. Restrict Access with Firewalls: Configure firewalls to limit access to open ports, ensuring only authorized users or systems can connect. This adds a crucial layer of protection.

3. Implement IDS/IPS: Deploy an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to monitor for suspicious activity and block potential threats targeting open ports.

4. Keep Services Updated: Regularly update and patch all services running on open ports to address known vulnerabilities and reduce the risk of exploitation.

CONCLUSION

While attackers often use tools like Nmap to find vulnerabilities, organizations can use the same tool proactively to strengthen their security. By carefully monitoring, securing, and minimizing the number of open ports, they can significantly reduce their attack surface and better protect their network from potential threats.