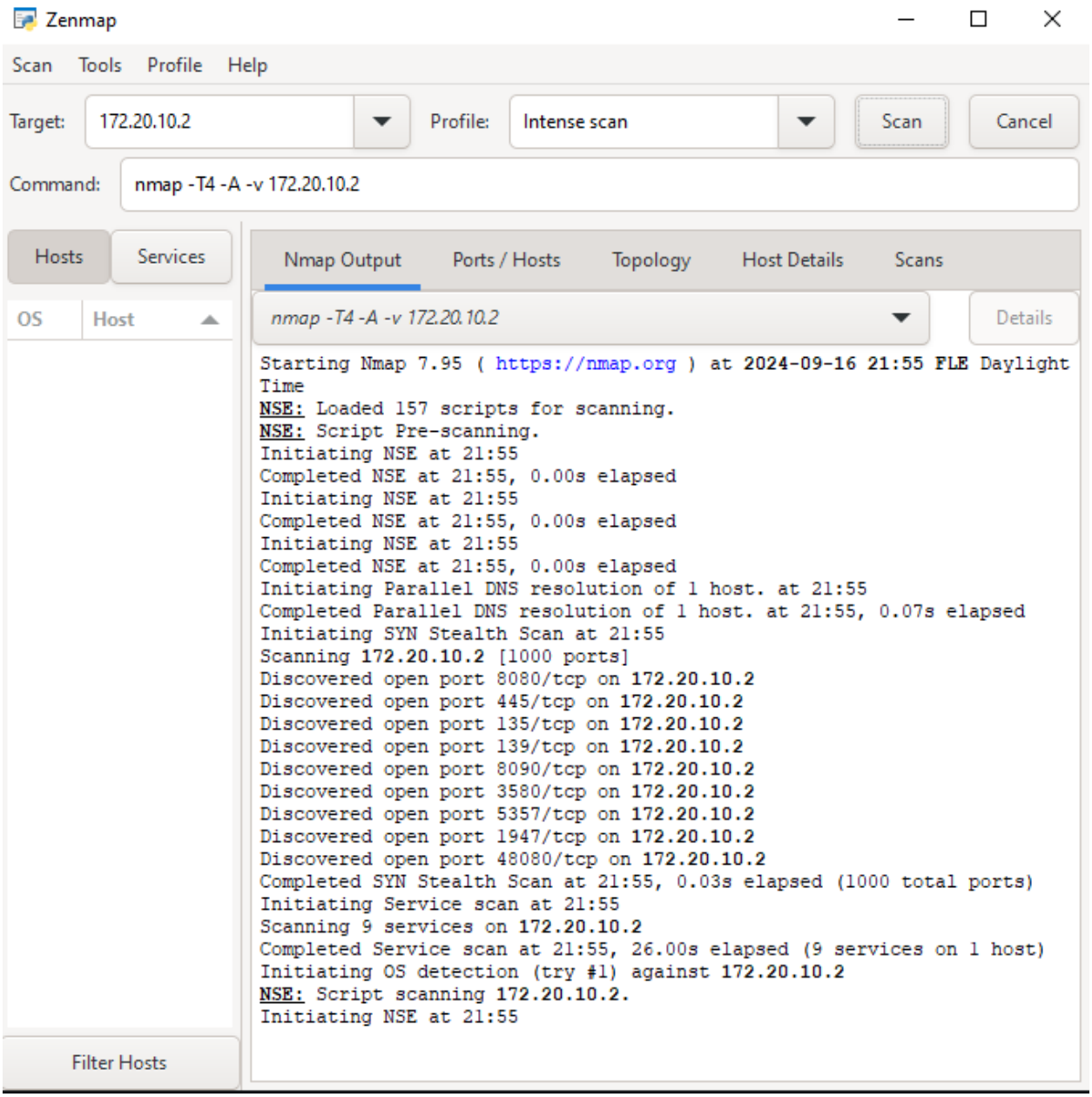
4A:

Personal Security Audit Report

1. Network Scan Overview

I performed a network scan using Zenmap, the graphical user interface for Nmap, to assess the security of my personal network. The scan targeted the IP address 172.20.10.2, and I utilized the "Intense scan" profile to thoroughly explore any open ports, services, and potential vulnerabilities within the network.



2. Findings

- **Devices Discovered:**
    - During the scan, the primary device identified was associated with the IP address 172.20.10.2. This device was recognized as part of my network. The topology map clearly indicated a connection between this device and the localhost (my scanning machine).
- **Open Ports:**
    - The scan revealed several open ports on the device:
        - **Port 445/tcp (Microsoft-DS):** Commonly used for file sharing in Windows environments.
        - **Port 139/tcp (NetBIOS-ssn):** Another port associated with SMB (Server Message Block) services.
        - **Port 8080/tcp (HTTP-proxy):** Typically used for web services or proxy servers.
    - **Should Any Ports Be Closed?**
        - Yes, the open ports, particularly those related to SMB (445/tcp and 139/tcp), are often associated with vulnerabilities. It is advisable to close these ports if they are not necessary for network operations to reduce the risk of exploitation.
- **Vulnerabilities Identified:**
    - The scan did not highlight any explicit vulnerabilities through Nmap scripts during this audit. However, the presence of open SMB-related ports suggests that the device could be susceptible to common exploits targeting these services, such as the EternalBlue exploit used in the WannaCry ransomware attack.

3. Screenshot of the Topology

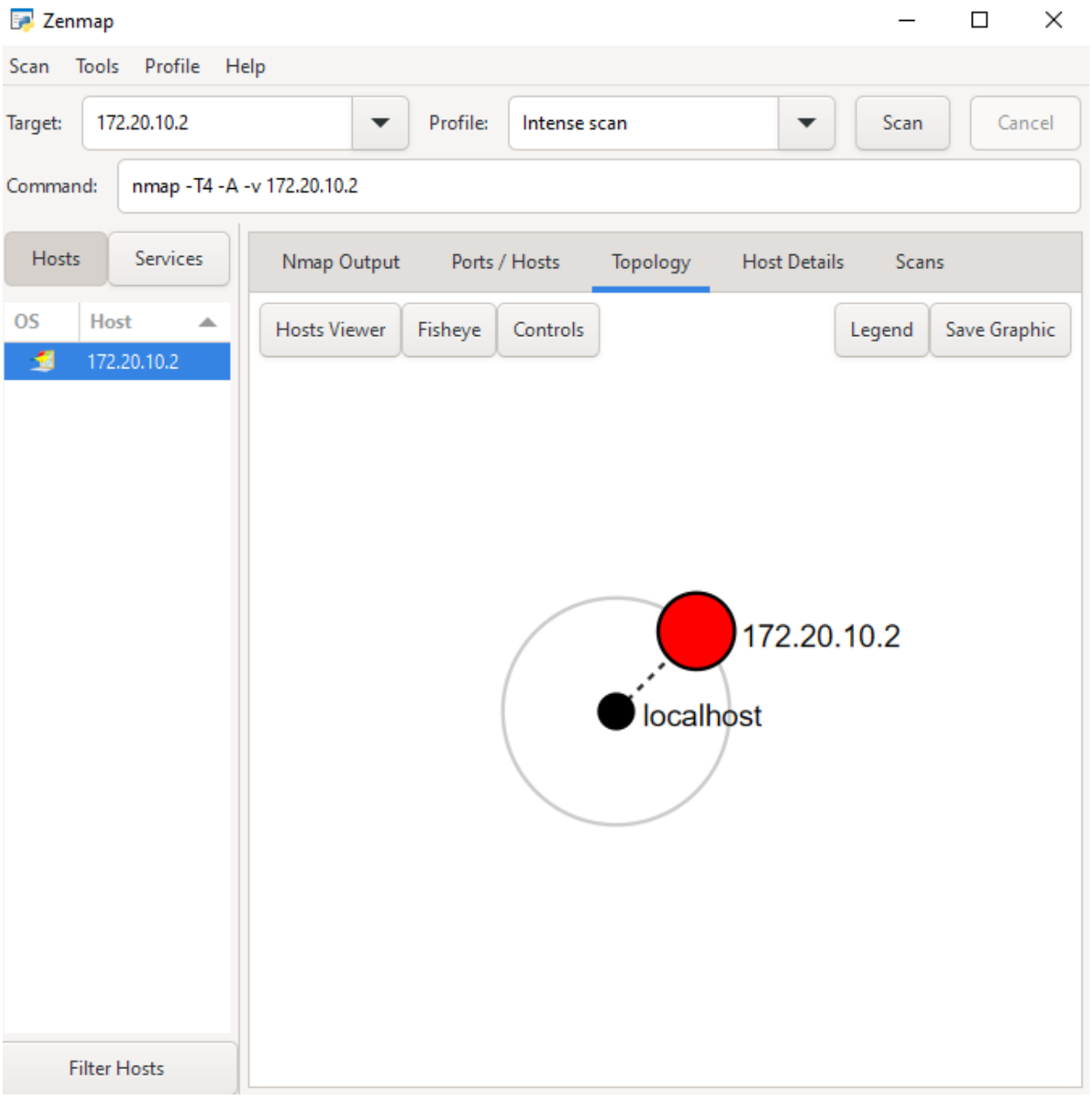
Below is the screenshot of the topology generated by Zenmap:

This topology map visually represents the devices found during the scan. The primary device (172.20.10.2) is connected to the localhost (my computer performing the scan), as depicted in the diagram. The map helps identify the relationships and connections between devices on the network.

4. Conclusion and Next Steps

The network scan provided valuable insights into the state of my network security. The discovery of open ports, particularly those associated with SMB services, indicates potential vulnerabilities that should be addressed. Moving forward, I plan to:

- **Close Unnecessary Ports:** Disable or restrict access to ports 445 and 139 if they are not required for any network functions.
- **Regular Monitoring:** Continue to monitor the network regularly using tools like Zenmap/Nmap to identify and address any emerging security issues.
- **Enhanced Security Measures:** Consider implementing additional security measures, such as firewall rules, to further protect the network from unauthorized access.



4B:

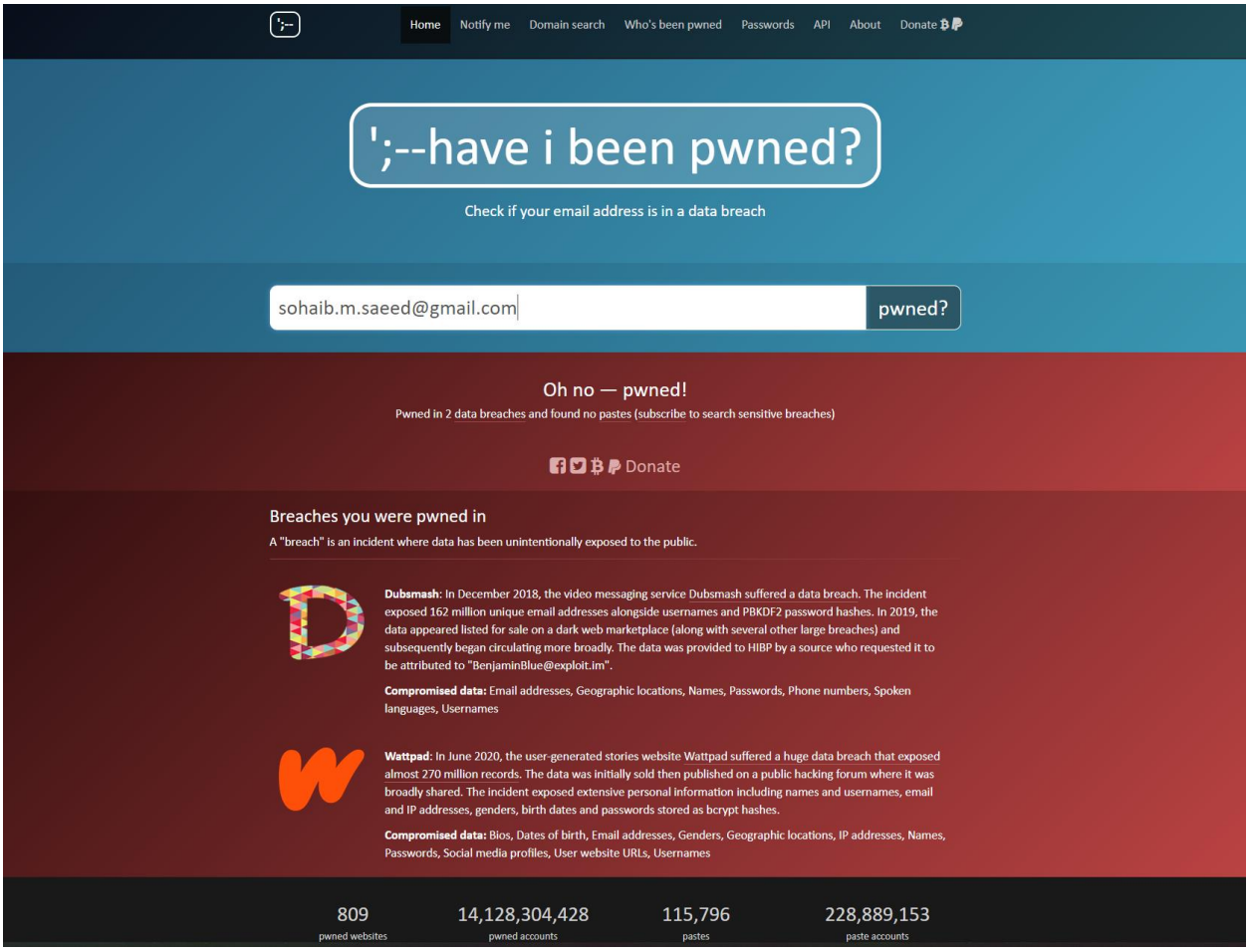
Account Security Report

1. Overview

As part of the network security audit, I conducted an account security check using the "Have I Been Pwned?" service. This tool checks whether my email address has been involved in any known data breaches, revealing the types of compromised information and the services involved.

2. Results

- Email Address: sohaib.m.saeed@gmail.com
- Breaches Detected: Yes, the email address was found in two data breaches.
    - Breach 1: Dubsmash (December 2018)
        - Details: The video messaging service Dubsmash suffered a data breach that exposed 162 million unique email addresses alongside usernames and PBKDF2 password hashes. The data was later found for sale on a dark web marketplace and began circulating more broadly.
        - Compromised Data: Email addresses, Geographic locations, Names, Passwords, Phone numbers, Spoken languages, Usernames.
    - Breach 2: Wattpad (June 2020)
        - Details: The user-generated stories website Wattpad suffered a large data breach that exposed almost 270 million records. This data was initially sold and then published on a public hacking forum.
        - Compromised Data: Bios, Dates of birth


Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if your email address is in a data breach
sohaib.m.saeed@gmail.com
pwned?
Oh no — pwned!
Pwned in 2 data breaches and found no pastes (subscribe to search sensitive breaches)
Donate
Breaches you were pwned in
A "breach" is an incident where data has been unintentionally exposed to the public.
Dubsmash: In December 2018, the video messaging service Dubsmash suffered a data breach. The incident exposed 162 million unique email addresses alongside usernames and PBKDF2 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".
Compromised data: Email addresses, Geographic locations, Names, Passwords, Phone numbers, Spoken languages, Usernames
Wattpad: In June 2020, the user-generated stories website Wattpad suffered a huge data breach that exposed almost 270 million records. The data was initially sold then published on a public hacking forum where it was broadly shared. The incident exposed extensive personal information including names and usernames, email and IP addresses, genders, birth dates and passwords stored as bcrypt hashes.
Compromised data: Bios, Dates of birth, Email addresses, Genders, Geographic locations, IP addresses, Names, Passwords, Social media profiles, User website URLs, Usernames
809
pwned websites
14,128,304,428
pwned accounts
115,796
pastes
228,889,153
paste accounts