**a) Did you find any vulnerability with the computer you scanned?**

Yes, I was able to find several possible vulnerabilities belonging to the computer that I was scanning. The most apparent is associated Port 80 (HTTP) which was open. For instance, the HTTP service is not encrypted and so all data passed between the server and any client is insecure and open to MITM attack. When mail is transmitted over the internet it lacks encryption (except for HTTPS) and can therefore be intercepted by hackers containing login details or even personal details.

Further, an open HTTP service put the system in risk to several web-related attacks like Cross-Site Scripting (XSS) or SQL Injection if the web applications and servers that is being used or implemented are not properly installed and updated or else has vulnerabilities. The scan results showed the server giving 404 – Not Found and 503 – Service Unavailable for some of the requests which means that while the server is online, it may not be fully operational. But it is a disadvantage to have the service open to the public in some parameters because if the server is old or configured wrong.

Over that, the other opened port may include for instance, port 2000 accessing a MikroTik bandwidth-test server and since this is a type of service other than those within well-known port range this type of service may be misused to consume resources, deny service.

**b) What operating systems are running on the hosts you visited?**

The scan also revealed that the host is Linux and have a kernel of the version 5.x. In other words, it can be assumed that the system uses a kernel from the 5.10 to 5.15 range. These versions are rather new, so it appears the operating system is most likely rather recent and somewhat safe if it has been updated with patches. since its MAC address is related to Routerboard.com that means this device is presumably a MikroTik router which is used in networks.

**c) List several services running on each computer?**

The scan revealed several services running on the computer:

1. Port 53 (DNS): This port is filtered, which indicate that DNS might be running , it can be accessed by the computer but a firewall or other security device is denying the access. DNS is the abbreviated form of the domain name system which is an organization that helps to link the domain names to the specific internet protocol address.

2. Port 80 (HTTP): This port is open; it can be noted that there is a web service on this host. From the response I have received here; the server is alive but it is not fully operational or maybe the access is fully limited.

3. Port 443 (HTTPS): This port is also open but what is written is tcpwrapped which means that the service available might be protected of hidden behind some kind of wrapper for example an encrypted connection to serve from a simple scan.

4. Port 2000 (Bandwidth Test): This port is open, the server is running MikroTik bandwidth-test. This service is used to test the network throughput and still a common service commonly seen on MikroTik devices.

5. Port 8291 (Winbox): This port is opened but the tcp connection is wrapperd. It might possibly be running what is called Winbox where administrators use this tool to configure the device from a MikroTik router firm.

**d) Identify one high-severity vulnerability for each computer (if there is one). Describe the vulnerability and discuss control(s) to minimize the risk from the vulnerability.**

The most serious vulnerability is the **open HTTP service on Port 80**. HTTP is inherently insecure because it transmits data in plaintext, which makes it vulnerable to interception by attackers. An attacker could exploit this vulnerability to launch a **Man-in-the-Middle (MITM)** attack, intercepting traffic between the client and the server. In addition, if the web server is running an outdated or poorly configured application, it could be vulnerable to **Cross-Site Scripting (XSS)**, **SQL Injection**, or other web-based exploits.

**Steps to minimize the risk:**

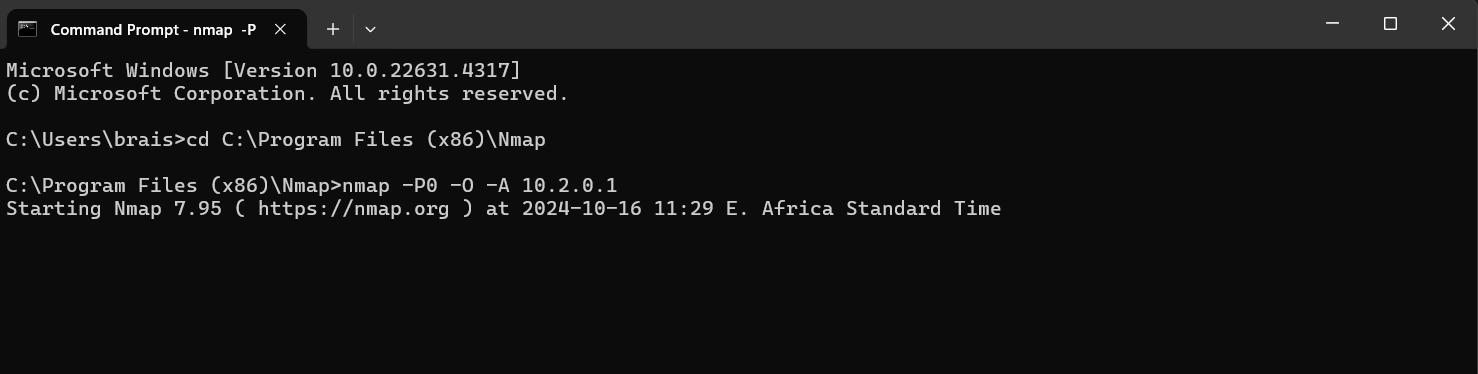
1. Upgrade to HTTPS: The most sensitive control is simply blocking HTTP and resolving to HTTP on port 443. HTTP secure (or shortly, HTTPS) adds security to the HTTP protocol by employing SSL/TLS to encrypt the info exchanged between the client and the server so that no attacker can capture/alter it. Another advantage arises from this approach, and they include; The data is also free from any outside interference and is also original.
2. Web Application Firewall (WAF): Using a WAF can assist to safeguard the server from typical web threats such as XSS and SQL Injection by defensing against them before penetrating the web application.
3. Patch and Update: The web server software should be the latest version and so should any applications that are in use on the server. Some of the best and quite simple practices are to update everything, as attackers love hitting systems with known outdated vulnerabilities.
4. Access Control: Restrict HTTP to its service to only the allowed users only. It is possible to do it with help of access to site IP address list, geographical limitations or using more secure types of authentications, such as OAuth or two-factor authentication.
5. Disable Unnecessary Services: But if the HTTP service is not required, then it has to be turned off. The first is to close as many ports/ services as possible that are connected to the internet which has the advantage of limiting choices for the attacker.

Overall, the lesson learned in this scan is the existence of the HTTP service which has not been encrypted to protect any data that may be flowing through the connection as well as serve as a gateway for malicious individuals. Moving the service to HTTPS will greatly decrease the likelihood of its exploitation, and adding the following controls will also help:

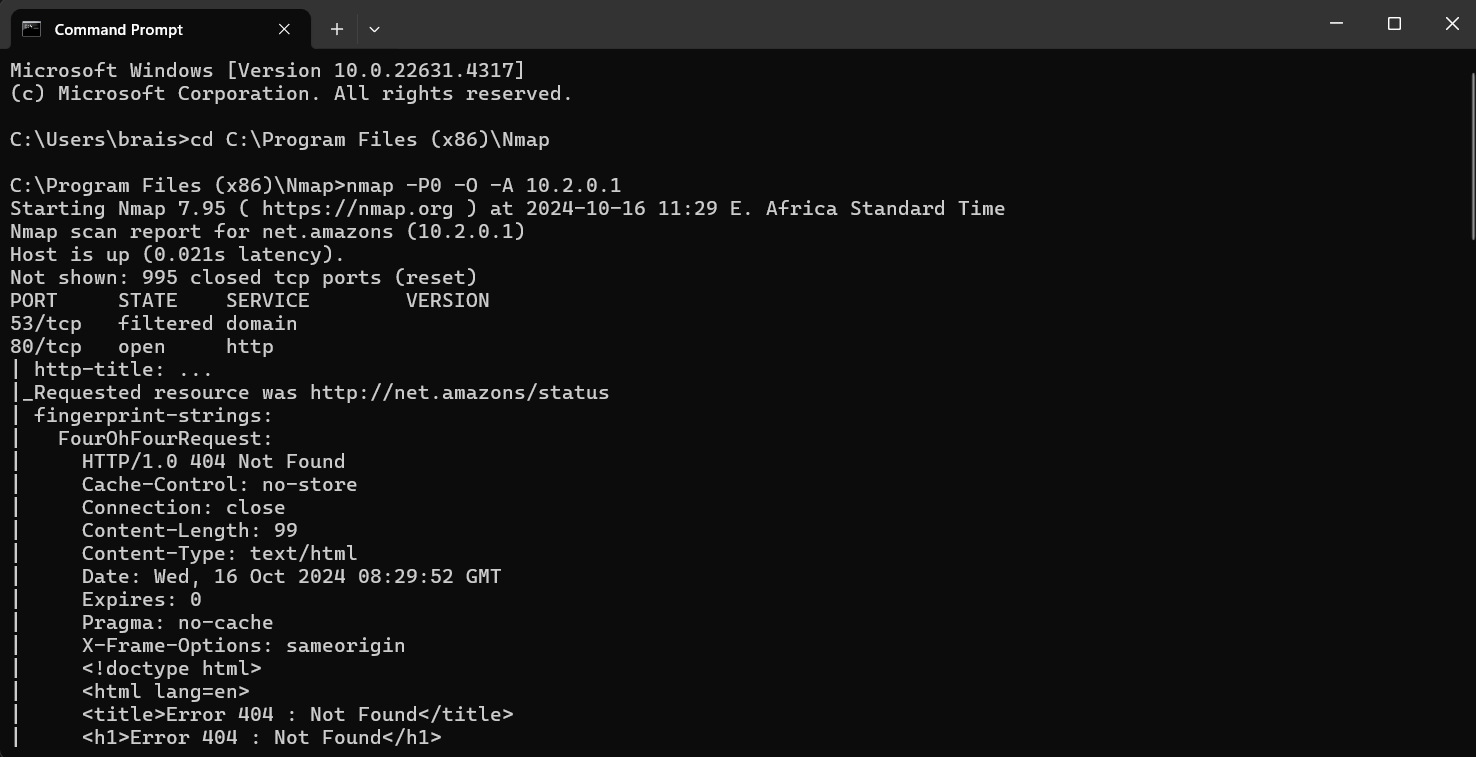
**Screenshots Based on the Nmap scan results**

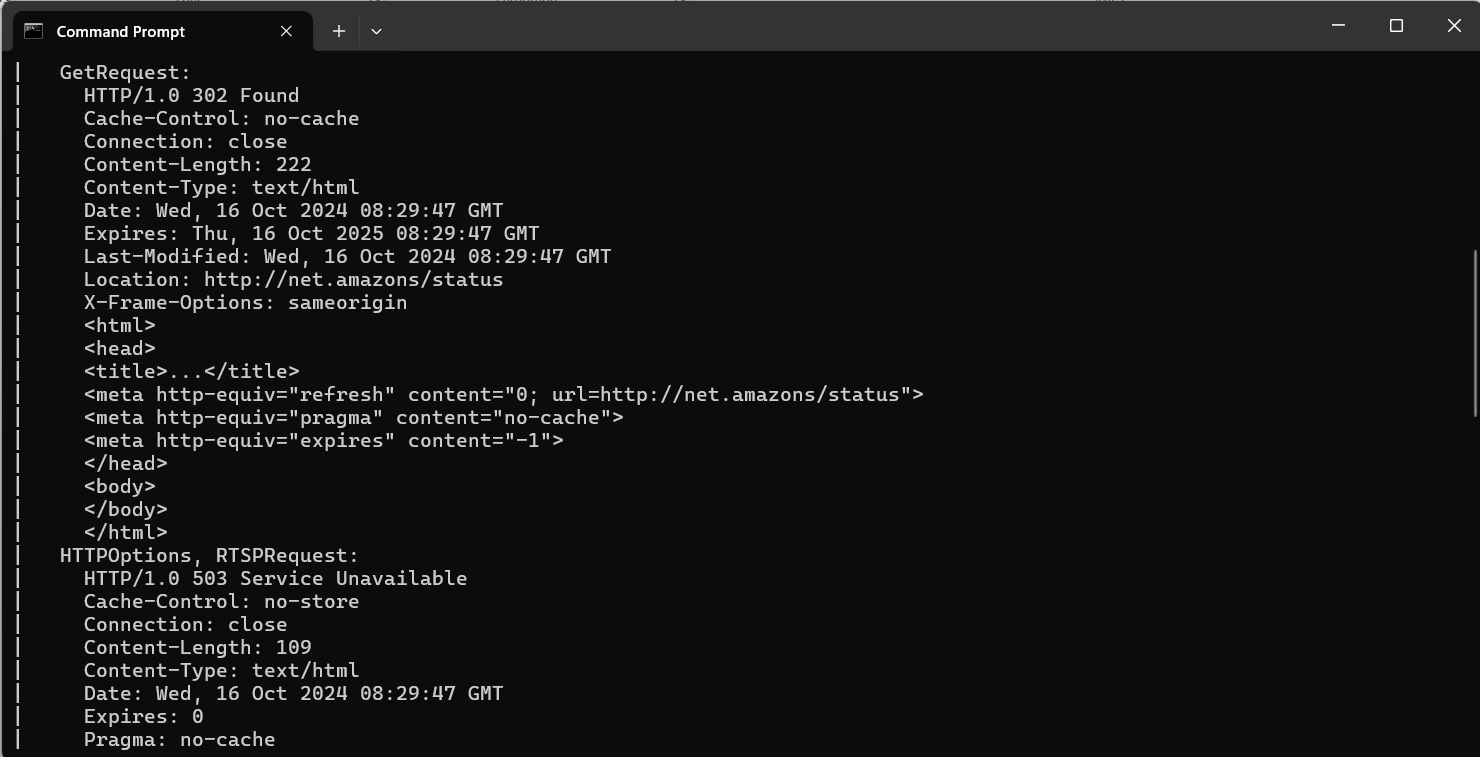


Screenshot 1: Navigating to the Nmap folder using “**cd C:\Program Files (x86)\Nmap**”

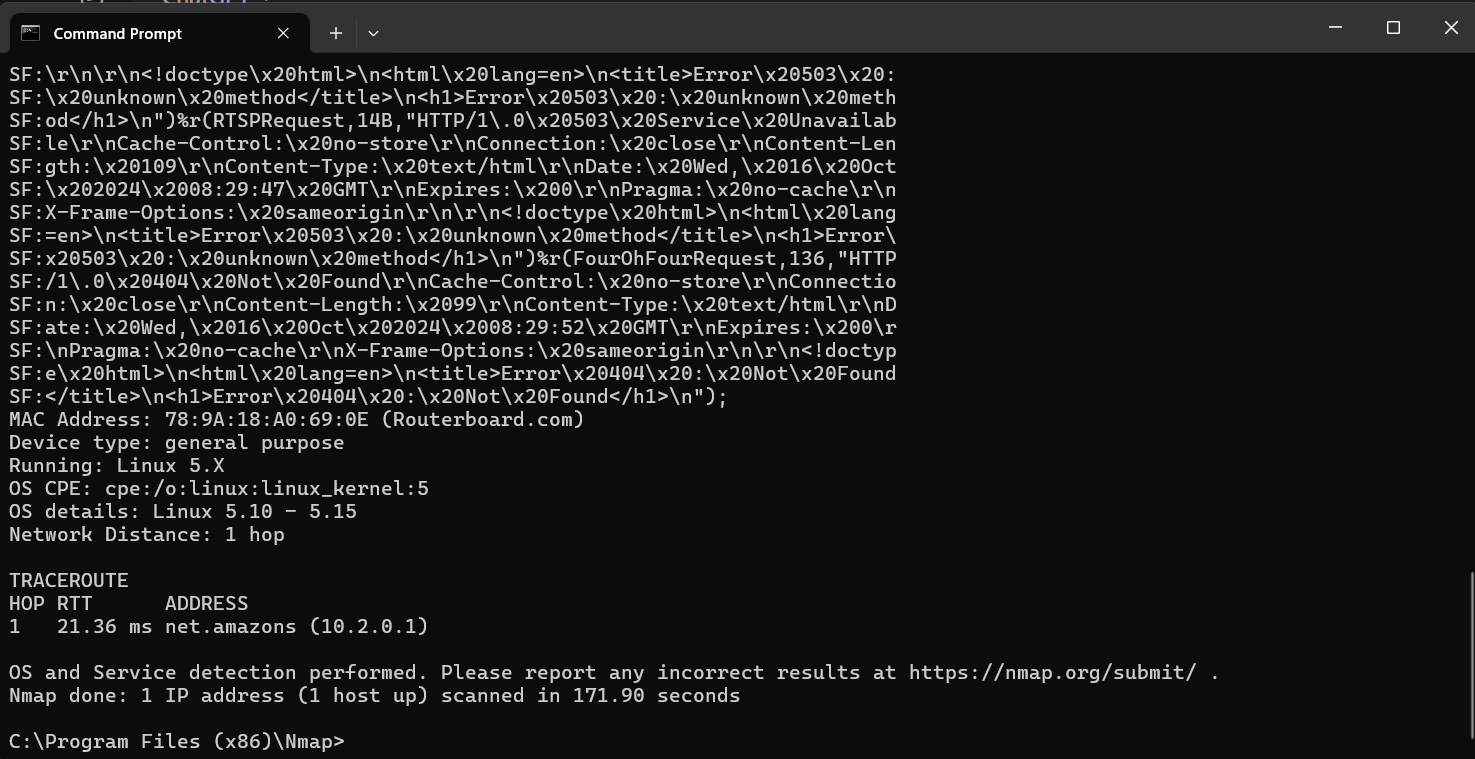


Screenshot 2: Running the command “**nmap -P0 -O -A 10.2.0.1**” to initiate the scan





Screenshot 3: Result of the scan



Screenshot 4: Result of the scan