**Assignment #2 (21st Dec 2020)**

**2.1 Performing Passive Reconnaissance**

The best way to learn passive information gathering is to use the tools. In this exercise,  you will perform reconnaissance on several organizations. Acquire only the  information requested.

**Estimated Time:** 20 minutes.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Domain**  **Name** | **IP**  **Address** | **Domain**  **Expiration** | **Location** | **Registrar** | **Contact  Person** | **Phone**  **Number** | **Address** |
| iisc.ac.in |  |  |  |  |  |  |  |
| rutgers.edu |  |  |  |  |  |  |  |
| drdo.gov.in |  |  |  |  |  |  |  |
| bbc.com |  |  |  |  |  |  |  |

**1.** Review Table to determine the target of your passive information gathering. **2.** You can use a tool such as *Whois* or any of the other tools mentioned  throughout the chapter. Some of these include:

⮚ www.betterwhois.com

⮚ www.allwhois.com

⮚ http://geektools.com

⮚ www.all-nettools.com

⮚ www.dnsstuff.com

⮚ www.samspade.org

⮚ https://talosintelligence.com/

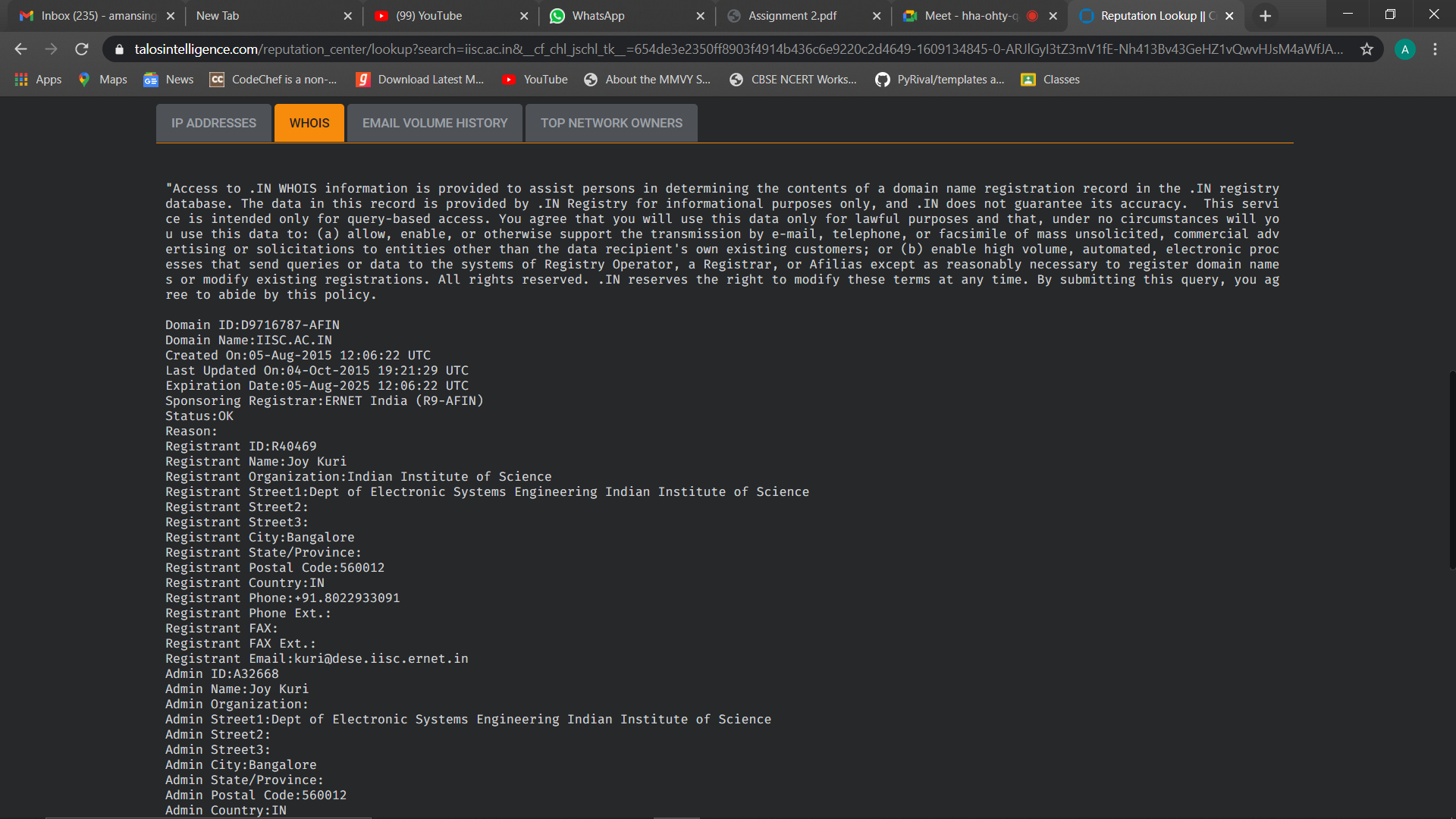
**3.** To verify the location of the organization, perform a *traceroute* or a ping with  the –r option.

Answer:

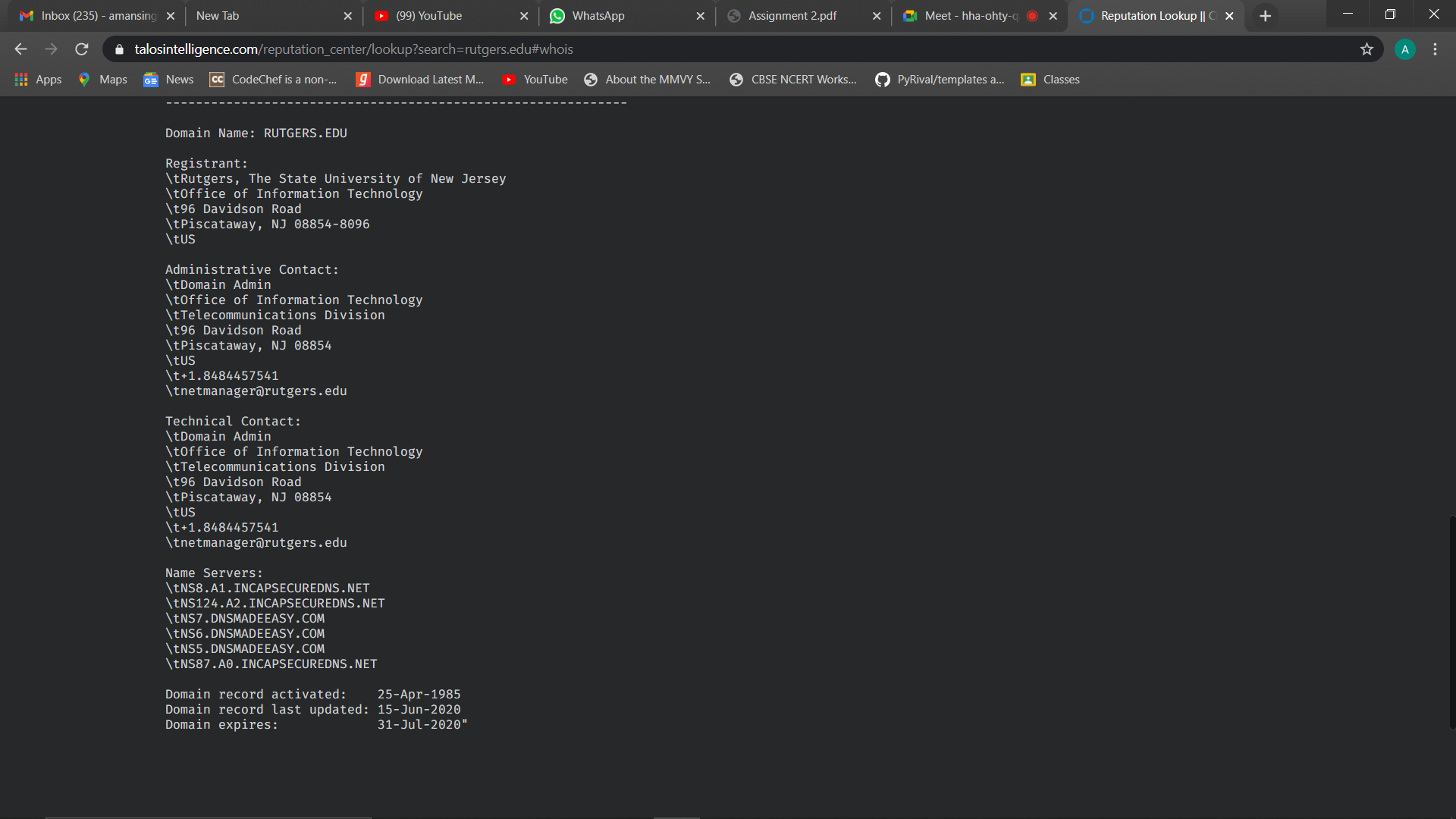
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Domain**  **Name** | **IP**  **Address** | **Domain**  **Expiration** | **Location** | **Registrar** | **Contact  Person** | **Phone**  **Number** | **Address** |
| iisc.ac.in | 52.172.211.104 | 5/8/2025 | INDIA | ERNET.India | [Kuri@dese.iisc.emet.in](mailto:Kuri@dese.iisc.emet.in) | +91 8022933091 | 0 91 Indian Institute of Science, Dept of Electronic Systems Engineering, Postal Code:560012  Country: India |
| rutgers.edu | 128.6.46.111 | 31/7/2023 | United States | Rutgers, The State University of New Jersey, Office of Information Technology | netmanager@rutgers.edu | +1 848445754 | Rutgers, The State University of New Jersey, Office of Information Technology 96 Davidson Road Piscataway, NJ 08854-8096 |
| drdo.gov.in | 164.100.77.87 | 30/4/2021 | India | National Informatics Centre | NA | NA | Defence Research & Development Organisation (DRDO), Delhi |
| bbc.com | 107.178.239.195 | 14/7/2021 | Great Britain UK | Tucows Domains INC | domainabuse@tuco ws.com | +1416530123 | British Broadcasting Corporation, London |

Screenshots

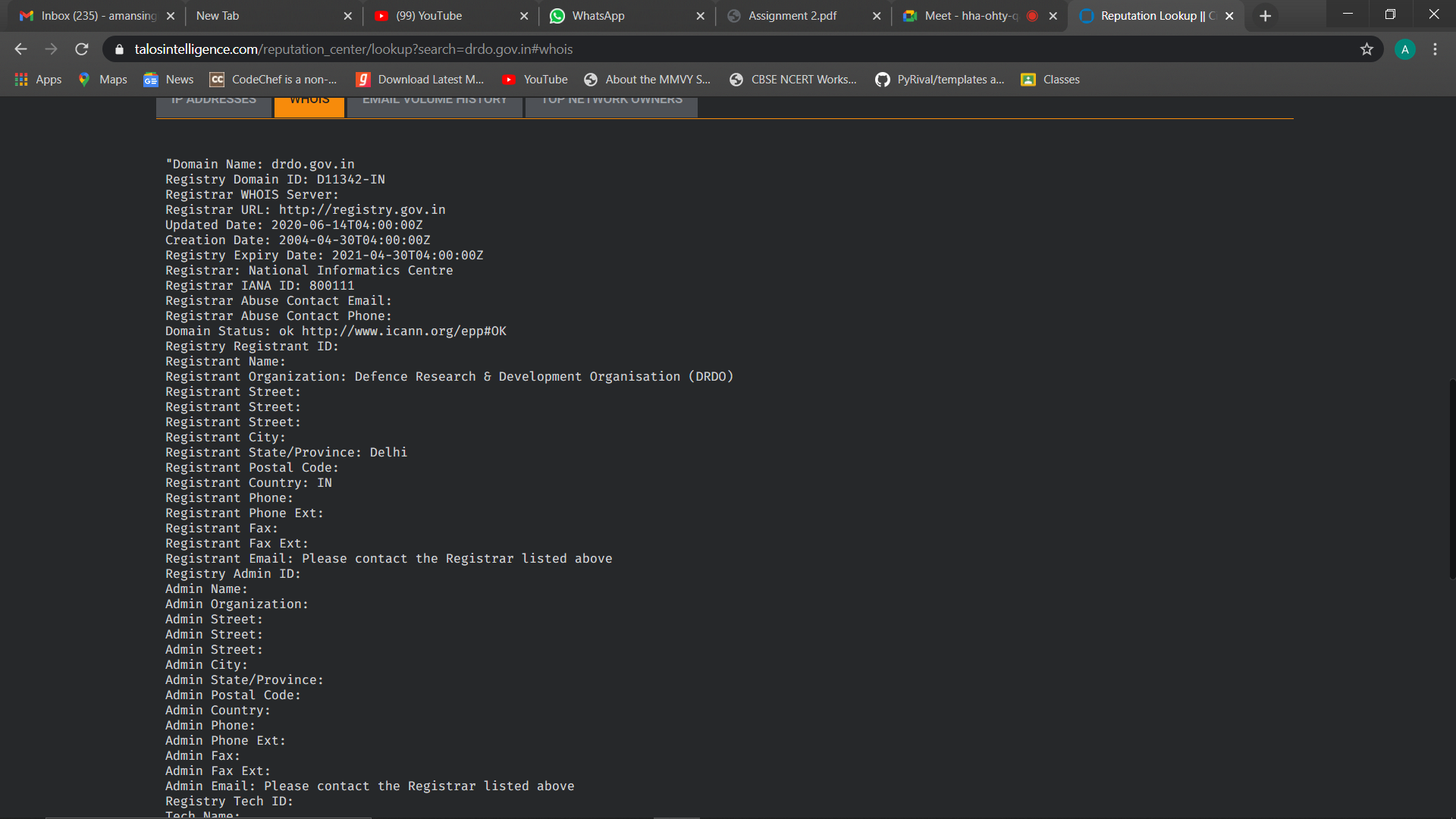
1) iisc.ac.in



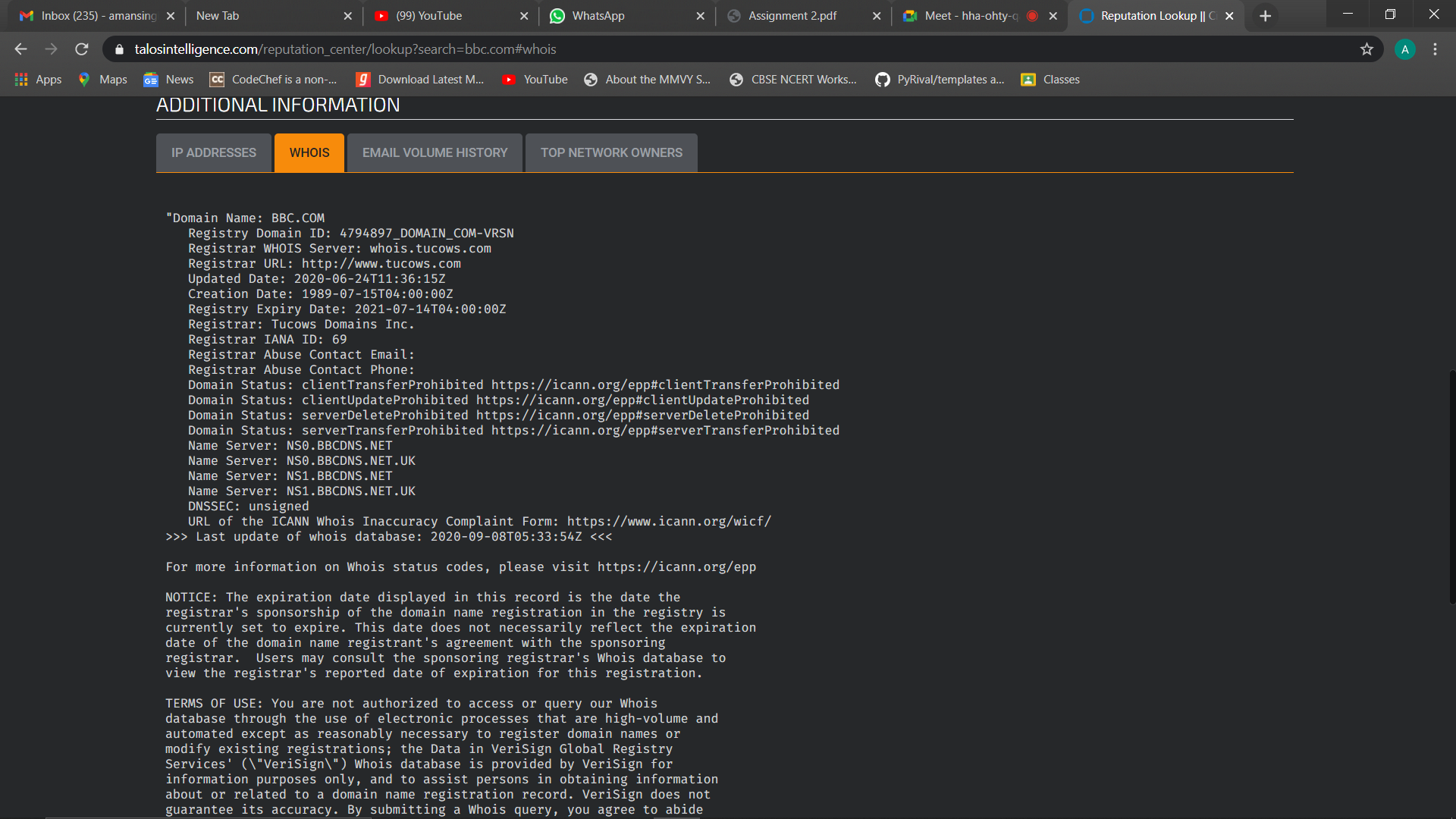
2) rutgers.edu



3) drdo.gov.in



4) bbc.com



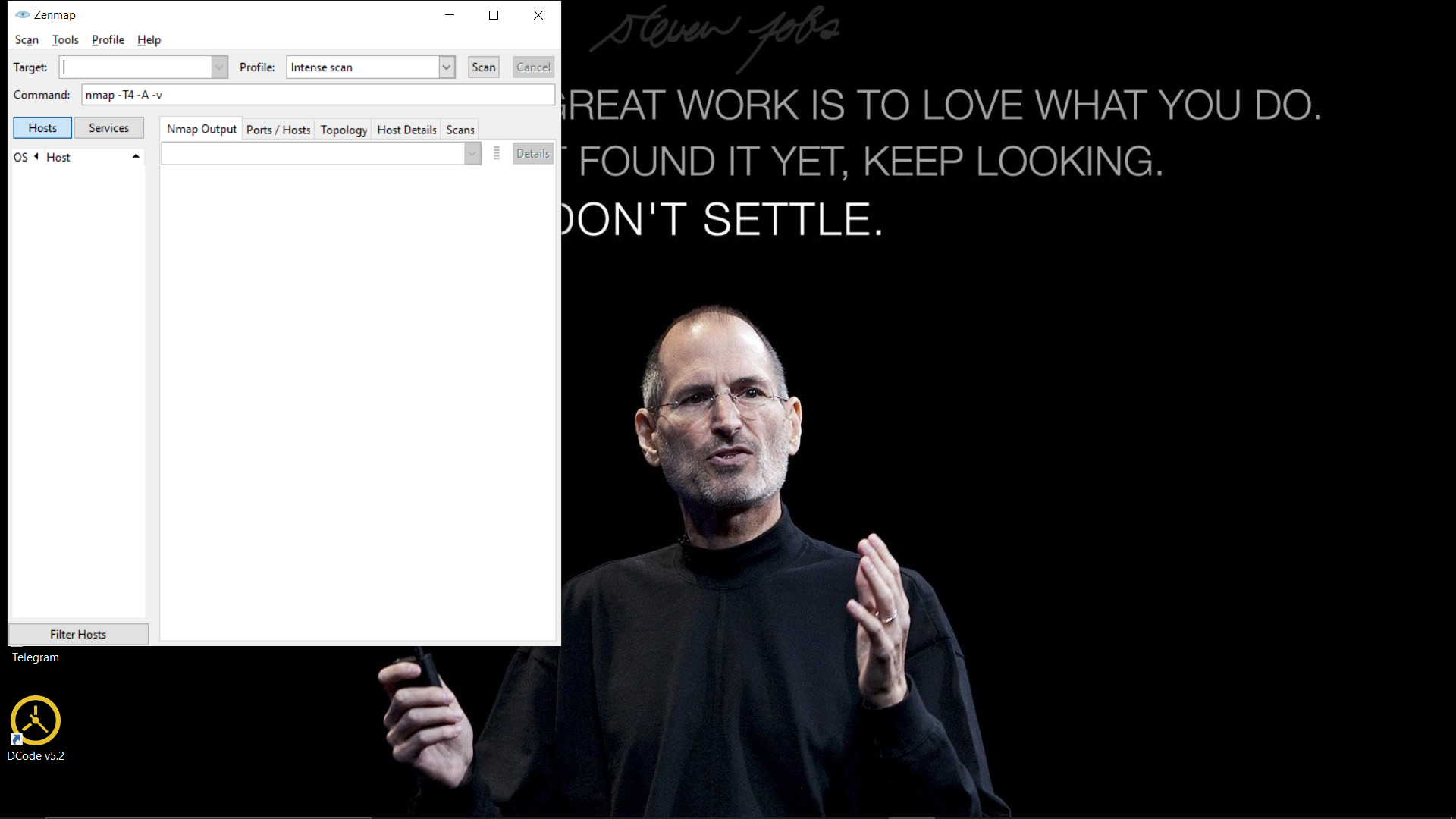
**2.2 Performing Active Reconnaissance**

The best way to learn active information gathering is to use the tools. In this exercise,  you will perform reconnaissance on your own internal network. If you are not on a test  network make sure you have permission before scanning or it may be seen as the  precursor of an attack.

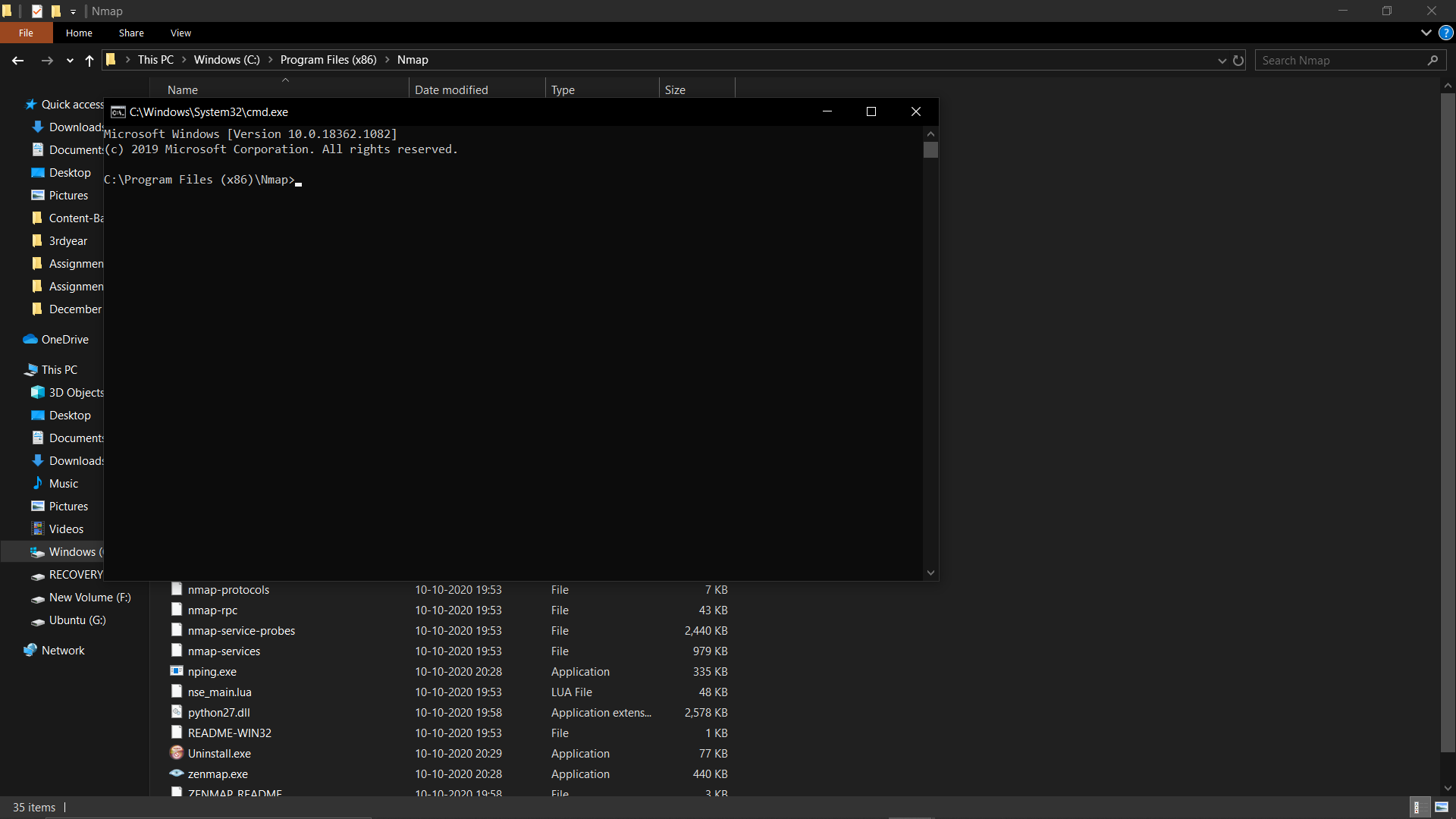
**Estimated Time:** 20 minutes

**1.** Download the most current version of Nmap from  [www.insecure.org/nmap/download.html](http://www.insecure.org/nmap/download.html).

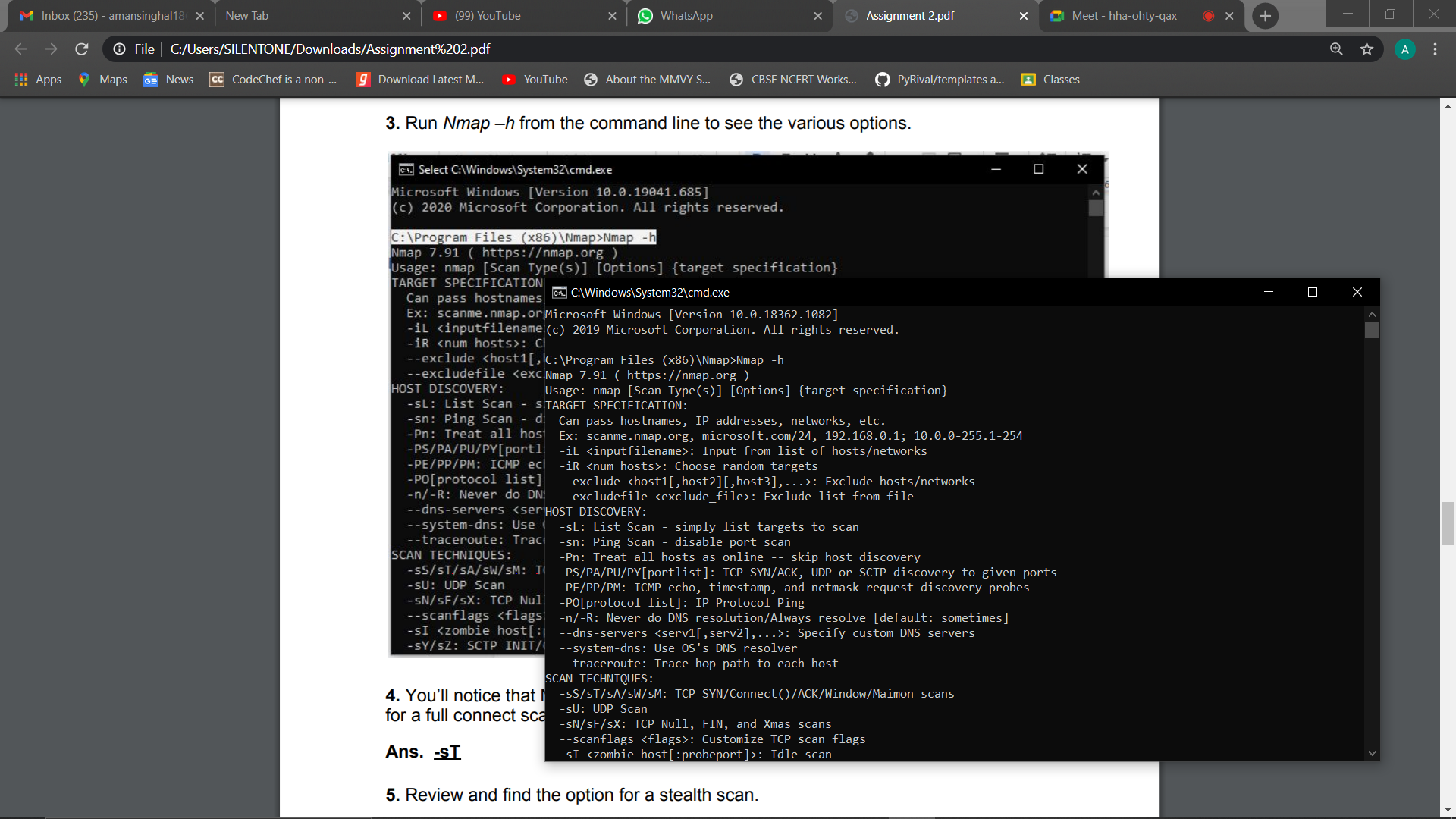
- Downloaded Nmap Version 7.91



**2.** Open a command prompt and go to the directory that you have installed Nmap  in.

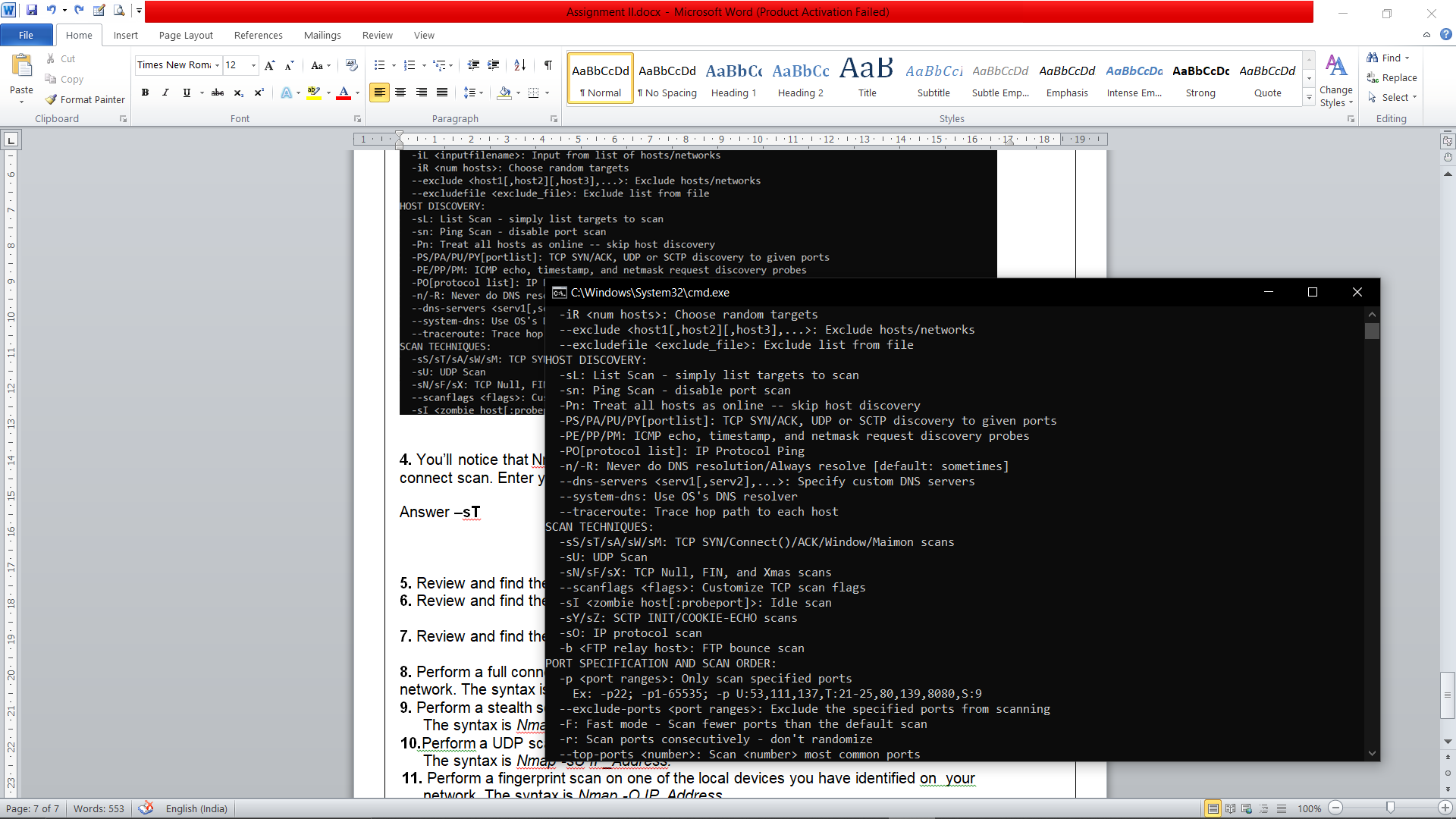


**3.** Run *Nmap –h* from the command line to see the various options.



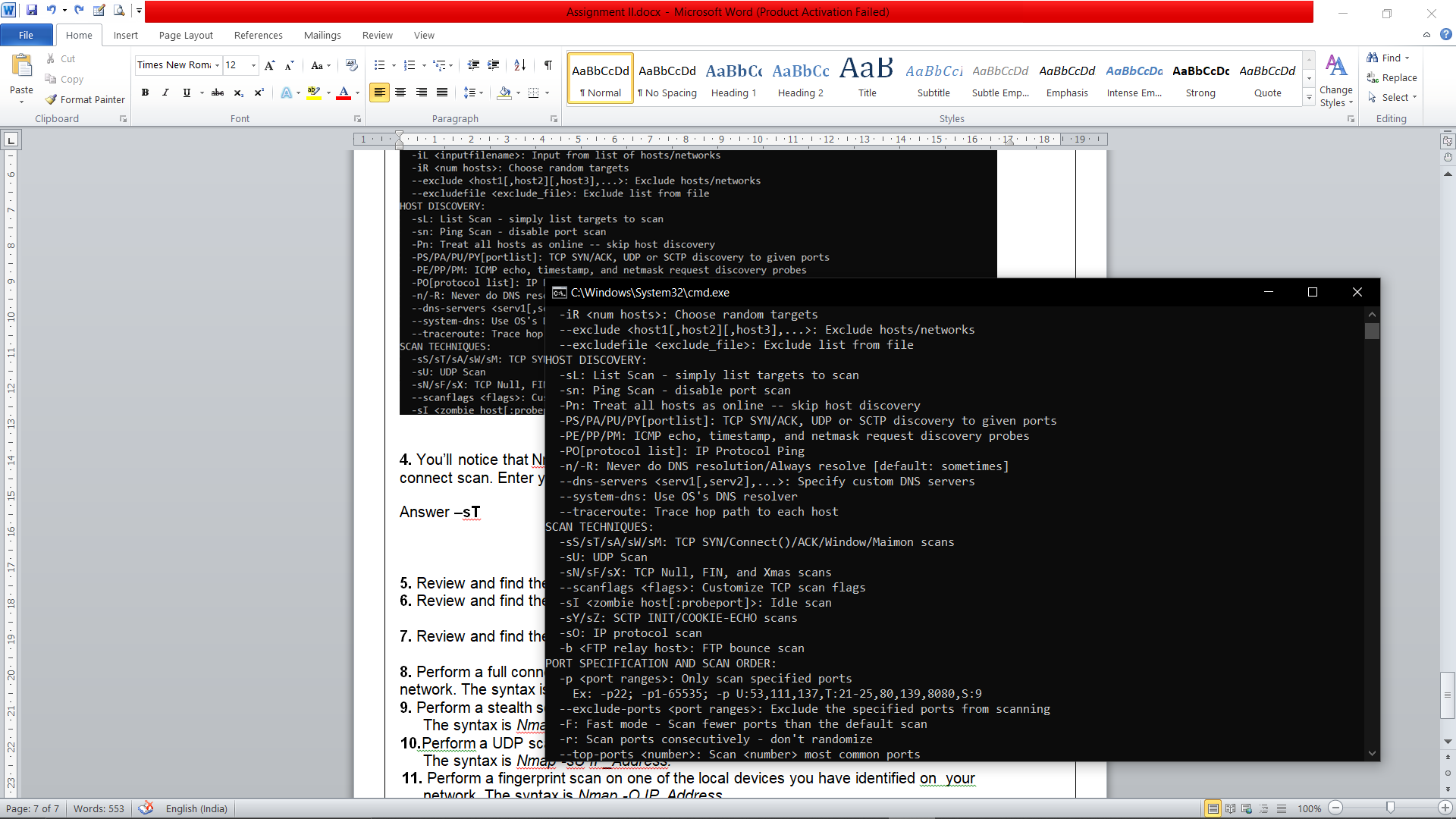
**4.** You’ll notice that Nmap has many different options. Review and find the option for a full connect scan. Enter your result here: \_\_\_\_\_\_

Answer **–sT**



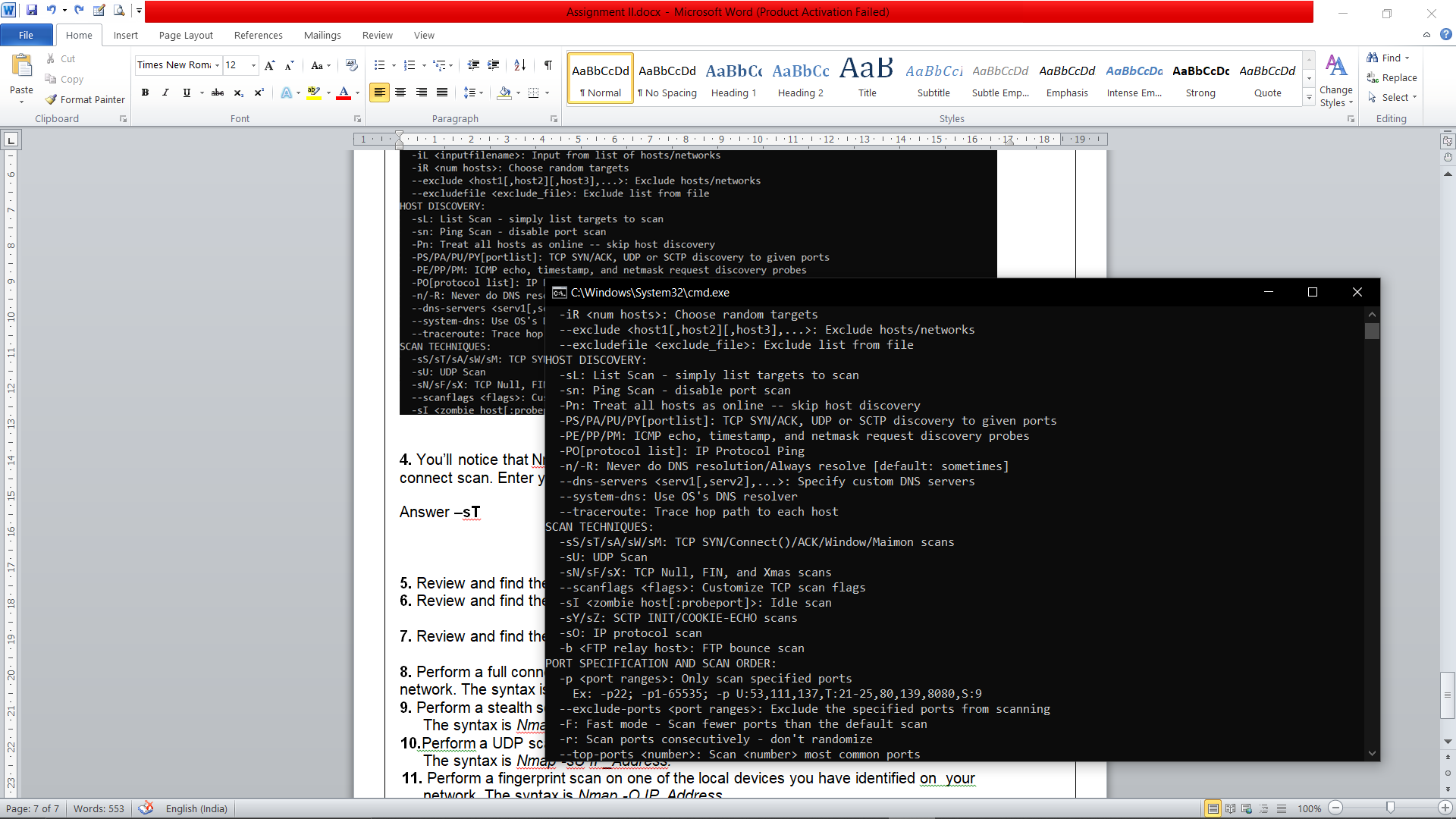
**5.** Review and find the option for a stealth scan. Enter your result here: \_\_\_\_

Answer **–sS**



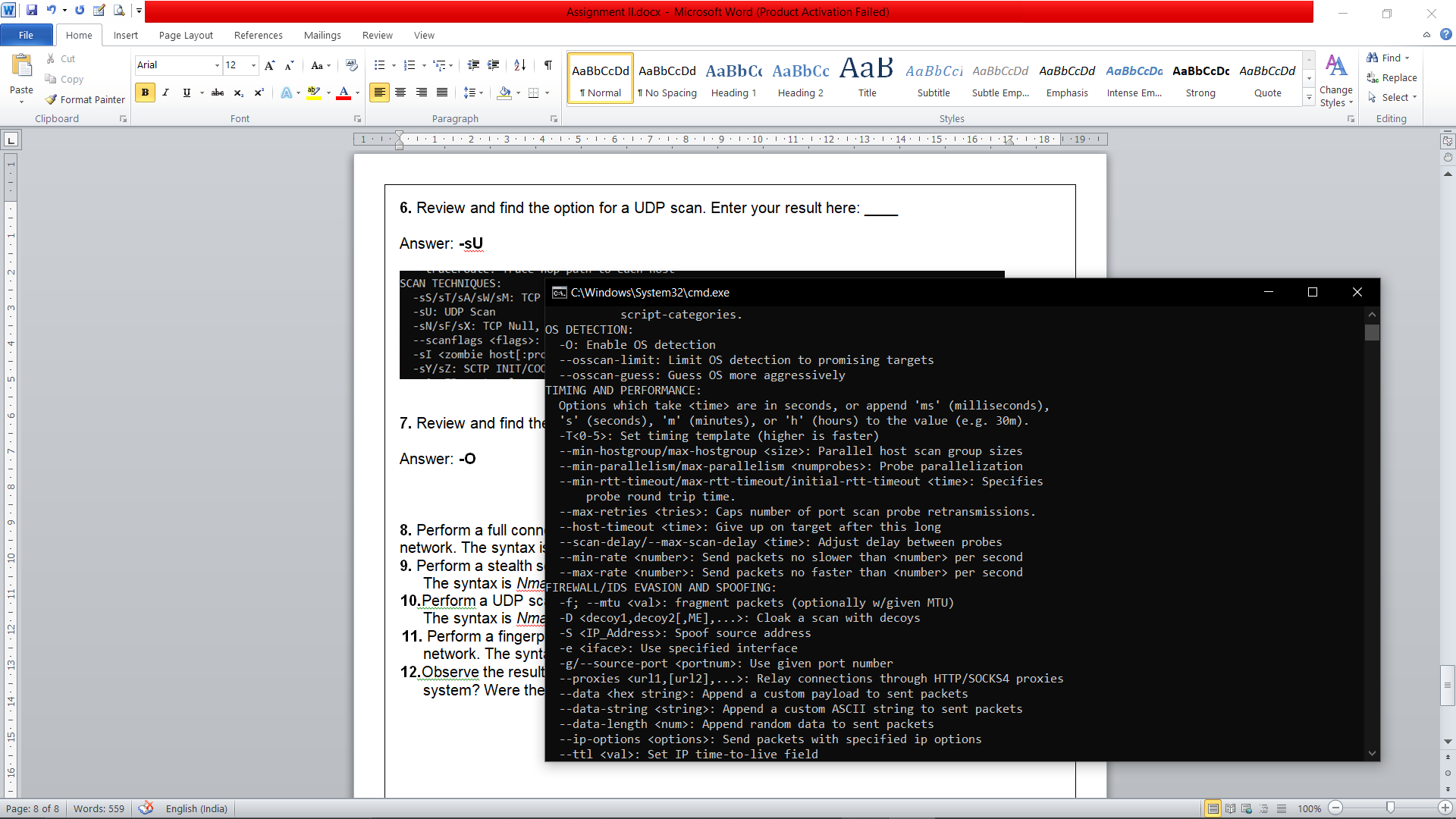
**6.** Review and find the option for a UDP scan. Enter your result here: \_\_\_\_

Answer: **-sU**



**7.** Review and find the option for a fingerprint scan. Enter your result here: \_\_\_\_

Answer: **-O**



**8.** Perform a full connect scan on one of the local devices you have identified on your network. The syntax is *Nmap -sT IP\_Address.*

**9.** Perform a stealth scan on one of the local devices you have identified on your network. The syntax is *Nmap -sS IP\_Address.*

**10.**Perform a UDP scan on one of the local devices you have identified on your  network. The syntax is *Nmap -sU IP\_Address.*

**11.** Perform a fingerprint scan on one of the local devices you have identified on  your network. The syntax is *Nmap -O IP\_Address.*

**12.**Observe the results of each scan. Was Nmap capable of successfully identifying the system? Were the ports it identified correct?

Yes, Nmap was able to successfully identify the system, and also all the ports were identified correctly, none of them were unknown or unidentified.

------------------------------------------------------------------------------------------------------------------------