COLLEGE OF INFORMATION TECHNOLOGY EDUCATION

IT 021 – Usable Security

FINALS

BELTRAN, JOHN RED **BORRAS, JEFERSON** **CRUZ, KIM** **MENDOZA, JAMES RAFAEL**	**Date: june 1, 2022**
Program/Section: BSIT/IT31S1	**Instructor: Mr.Jerry Borromeo**
Assessment Task: Laboratory Activity 5 - Identifying Port Scanning Threats	

Laboratory Activity: Identifying Port Scanning Threats

Data File

Identifying Security Threats\nmap-7.40-setup.exe

Before You Begin

You will work with a partner in this activity.

You will be using Nmap, a network scanning tool. Nmap has a GUI frontend called Zenmap.

Scenario

Some threats are targeted, like the threats to your DNS servers. However, in order to craft a targeted threat, attackers will often gather intelligence through your networking infrastructure. This intelligence helps them make decisions about what to attack and how. So, you decide to identify how network scans, particularly port scans, can threaten the security of your computing environments.

1. Install Nmap.

a) In File Explorer, from the course data files, double-click the **nmap-7.40-setup.exe** file.

b) In the **Nmap Setup** wizard, on the **License Agreement** page, select **I Agree**.

c) On the **Choose Components** page, uncheck **Npcap 0.78-r5** and select **Next**.

Nmap requires a packet capture library like Npcap, but your existing WinPcap installation will suffice.

d) On the **Choose Install Location** page, select **Install**.

e) When installation completes, select **Next**.

f) On the **Create Shortcuts** page, select **Next**.

g) Select **Finish**.

2. Run a port scan.

a) On the desktop, double-click the **Nmap - Zenmap GUI** shortcut to open it.

b) Maximize the **Zenmap** window.

c) In the **Target** text box, type ***Server##***, where ***##*** is your partner's student number.

d) Select the **Profile** drop-down list and select **Quick scan**.

e) In the top right of the **Zenmap** window, select the **Scan** button to start the scan.

3. Examine the scan results.

a) When the scan is complete, verify that several TCP ports were detected as open.

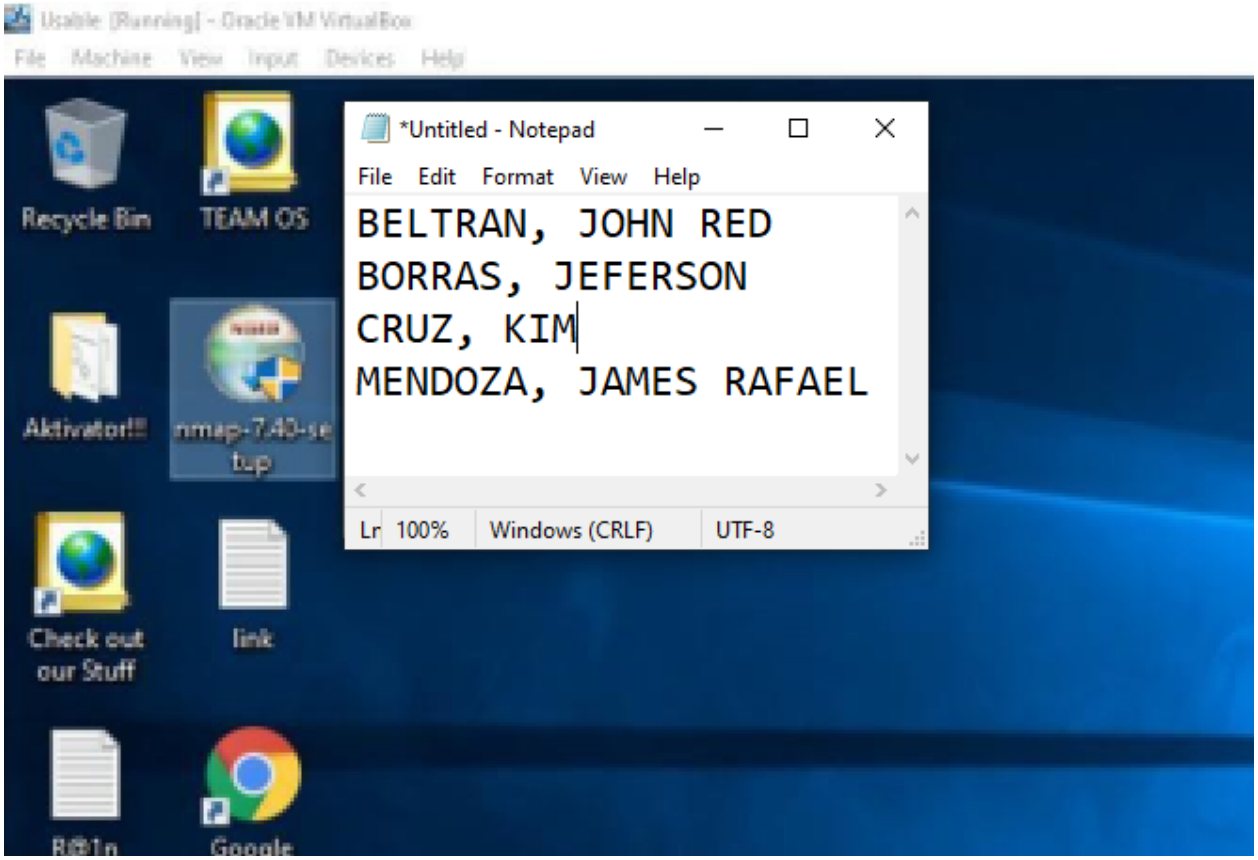
```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-05 06:20 Pacific Daylight Time
Nmap scan report for Server01 (192.168.36.101)
Host is up (0.0013s latency).
Not shown: 91 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
443/tcp  open  https
445/tcp  open  microsoft-ds
1723/tcp open  pptp

Nmap done: 1 IP address (1 host up) scanned in 5.47 seconds
```

b) Close **Zenmap** without saving the report.

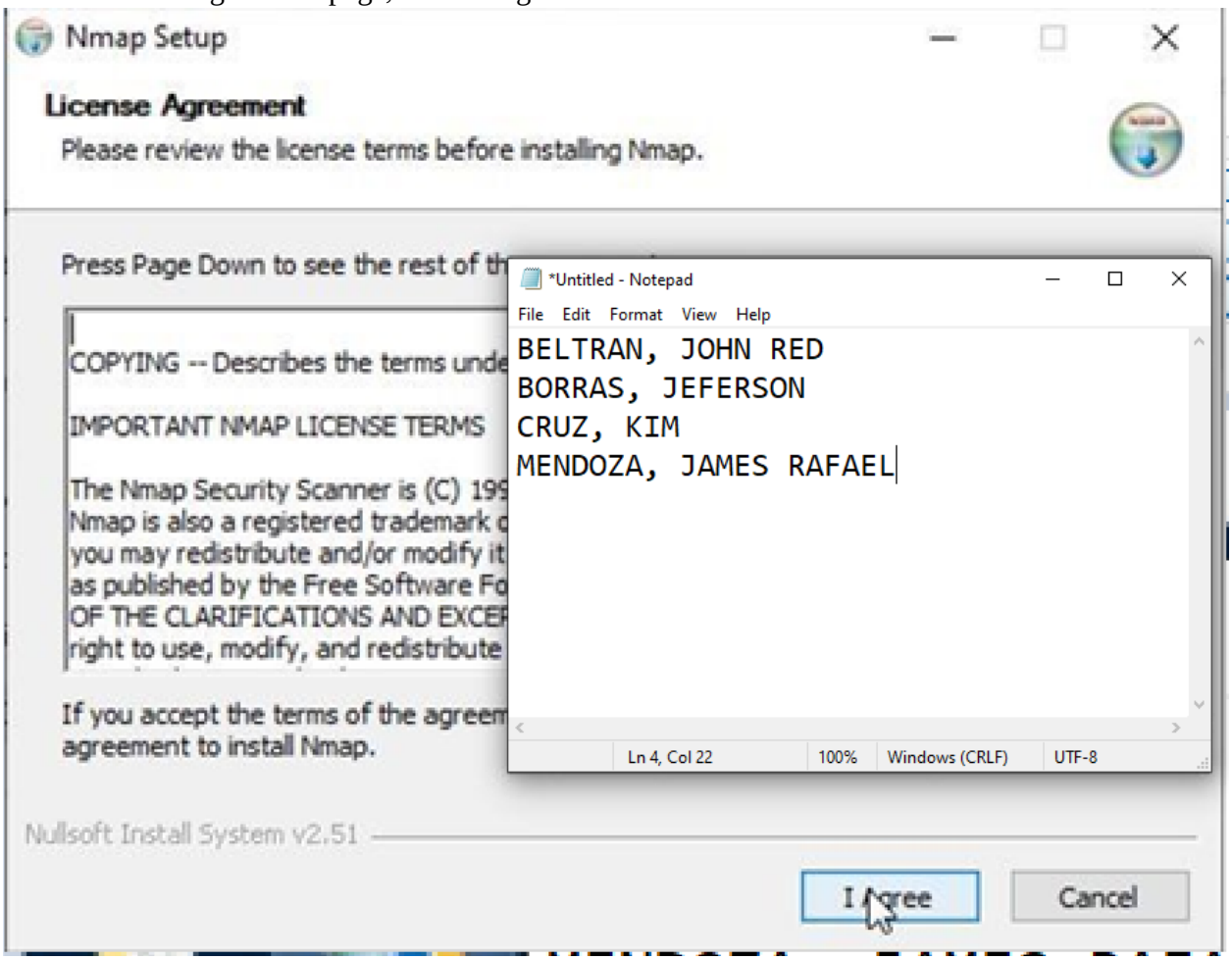
Instructions:

1. Document this process/output through screenshots and provide brief description of it.

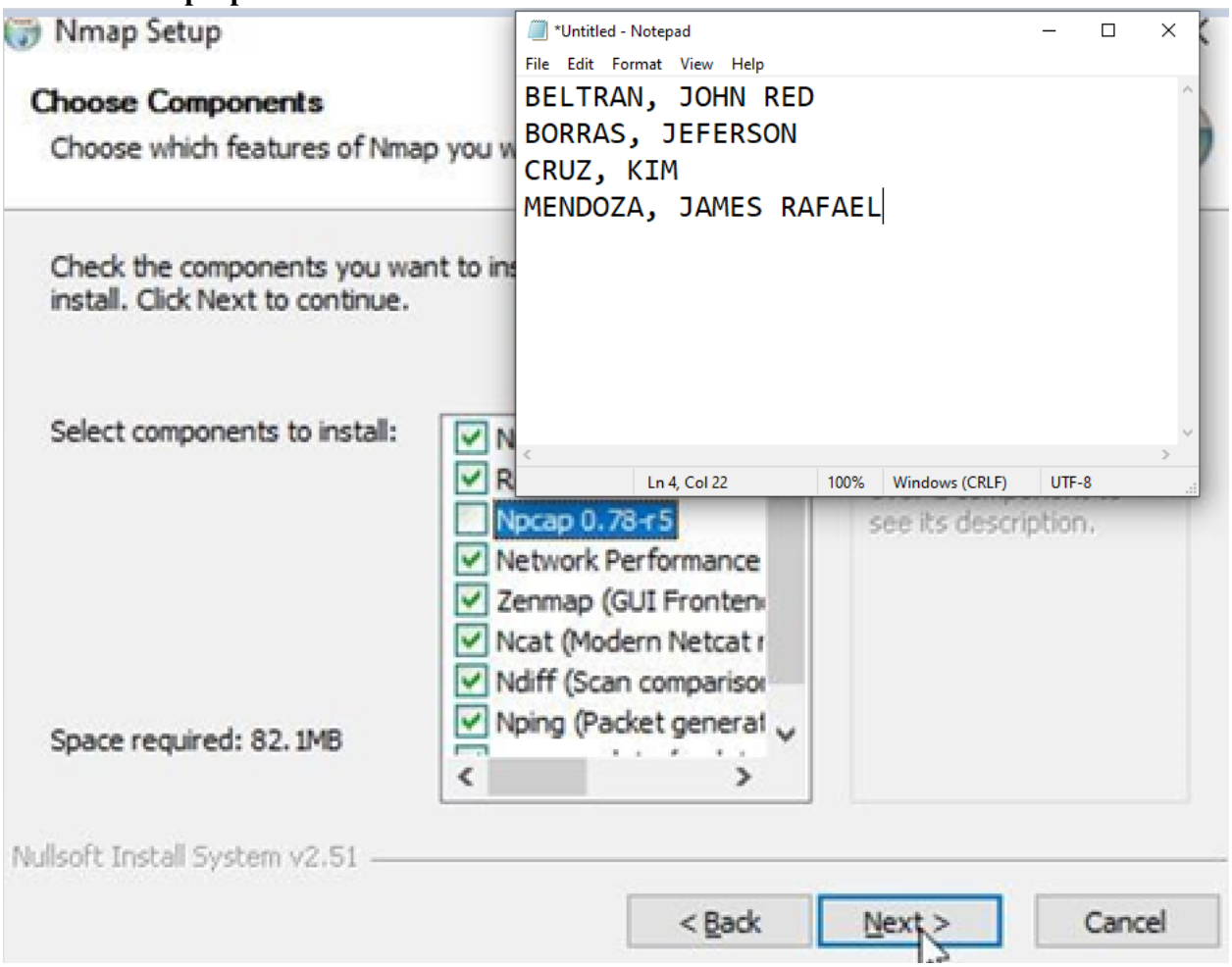
Double-click the **nmap-7.40-setup.exe** file



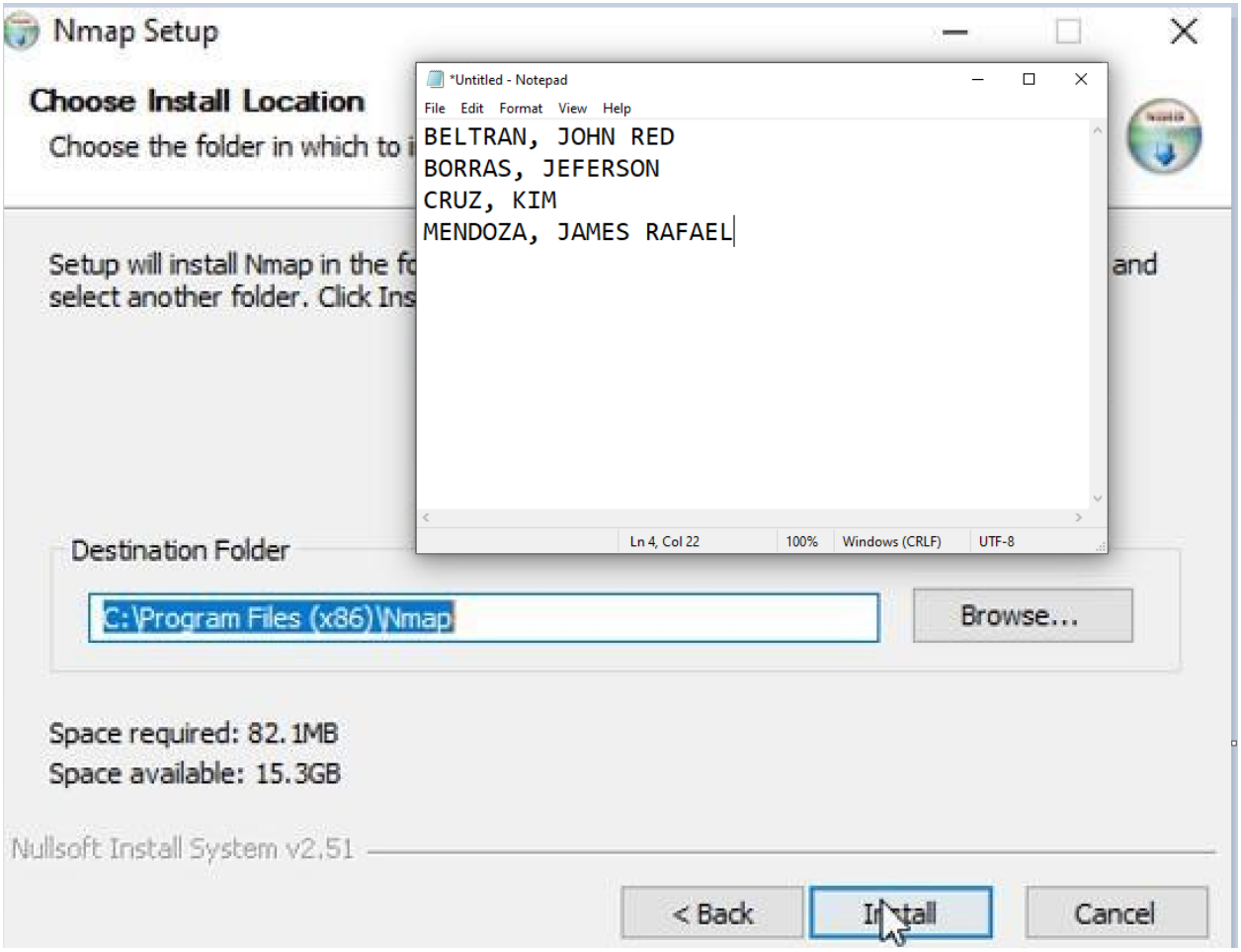
On the License Agreement page, select I Agree



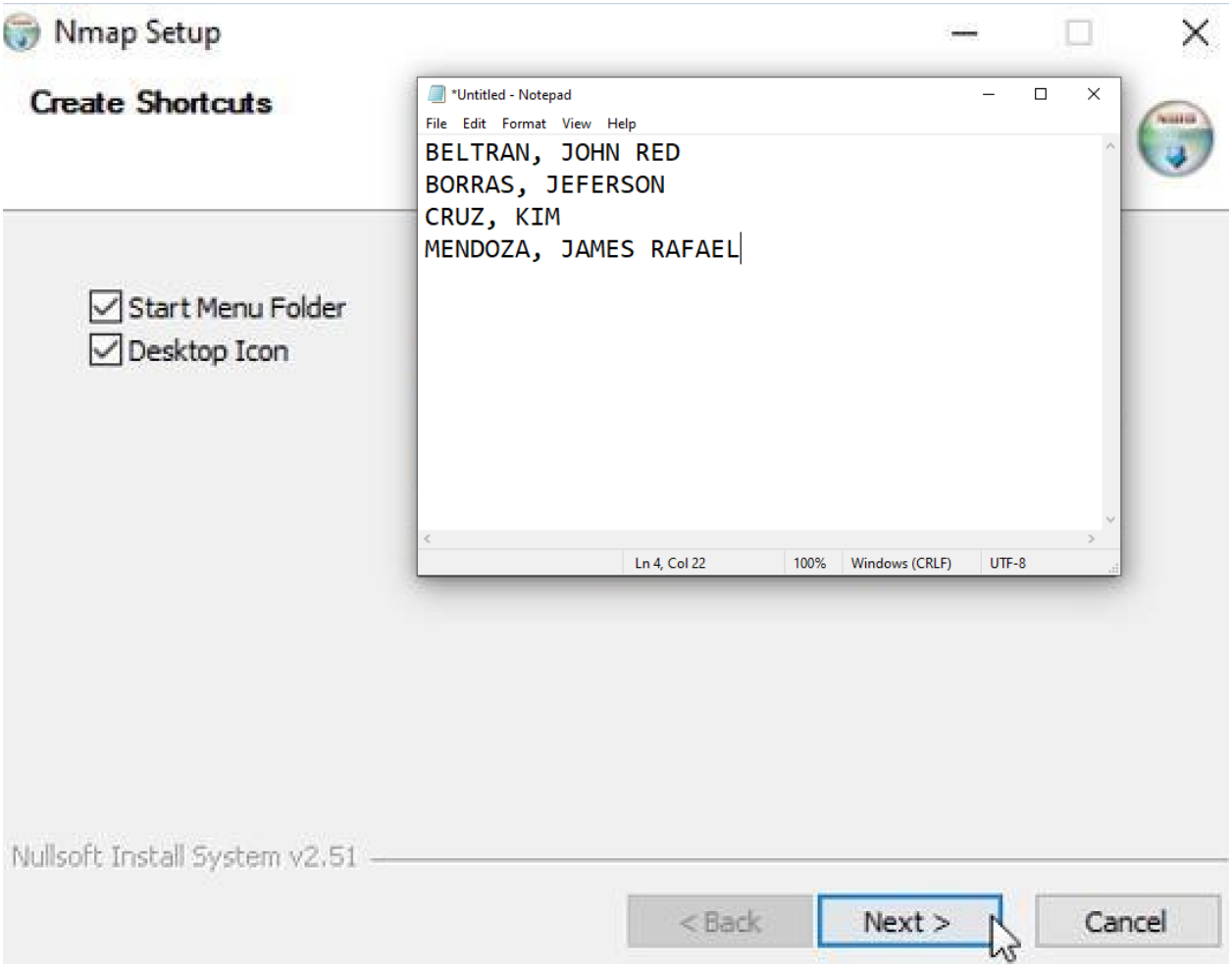
Uncheck the **Npcap 0.78-r5** and select next



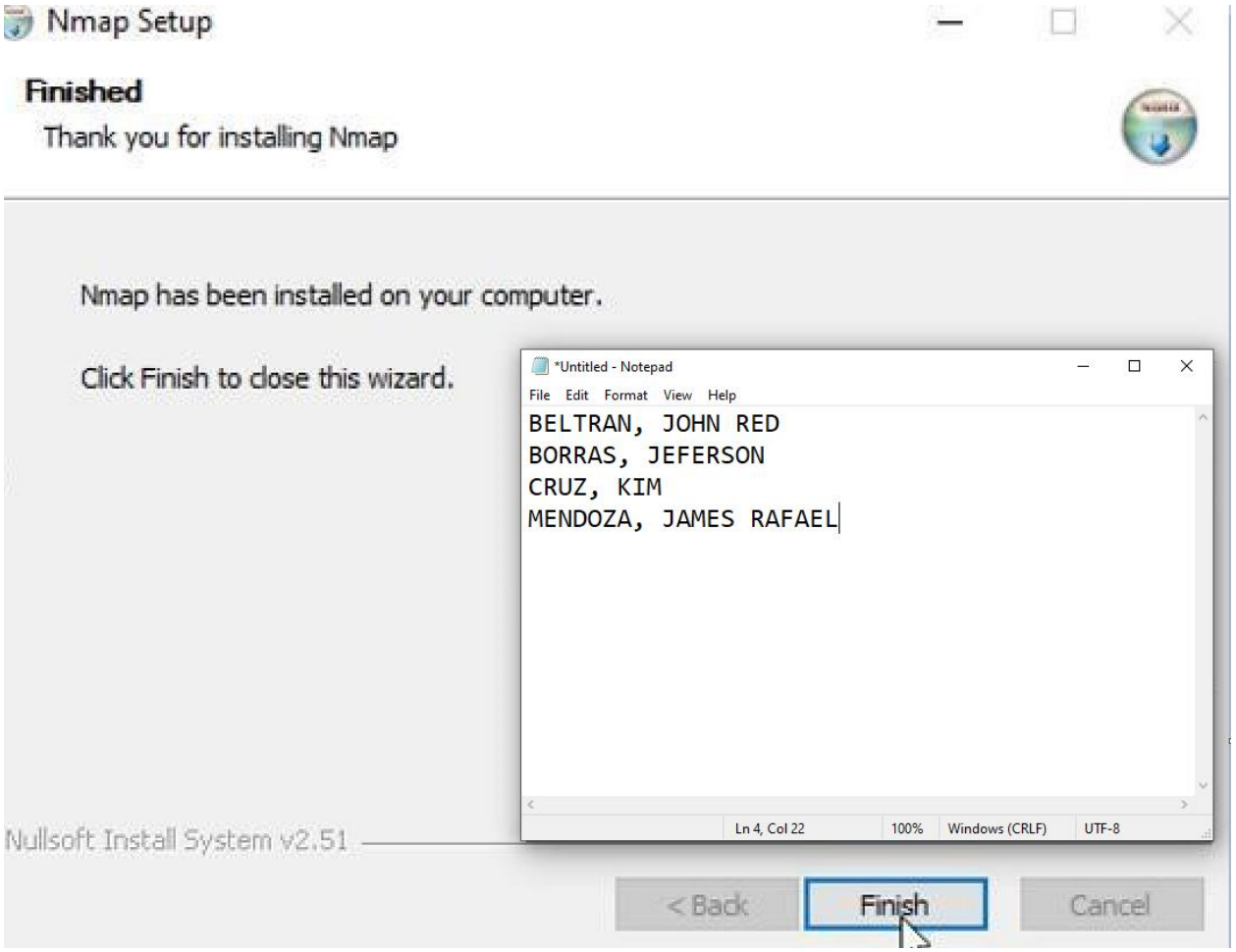
Click Install



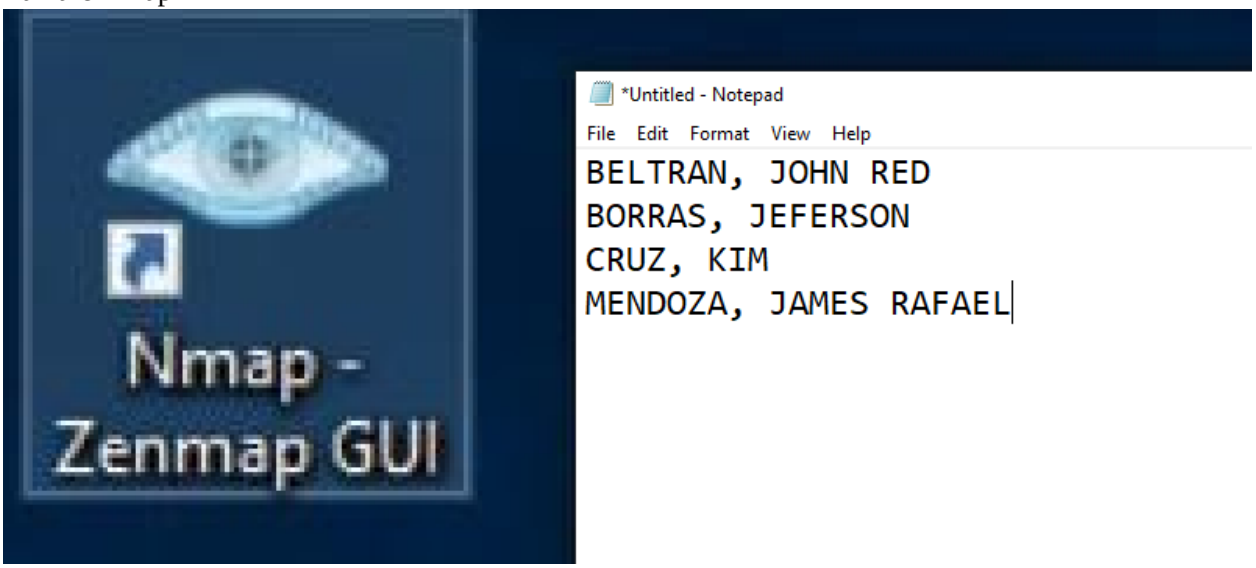
Click Next


Nmap Setup
Create Shortcuts
*Untitled - Notepad
File Edit Format View Help
BELTRAN, JOHN RED
BORRAS, JEFERSON
CRUZ, KIM
MENDOZA, JAMES RAFAEL
Ln 4, Col 22
100%
Windows (CRLF)
UTF-8
Start Menu Folder
Desktop Icon
Nullsoft Install System v2.51
< Back
Next >
Cancel

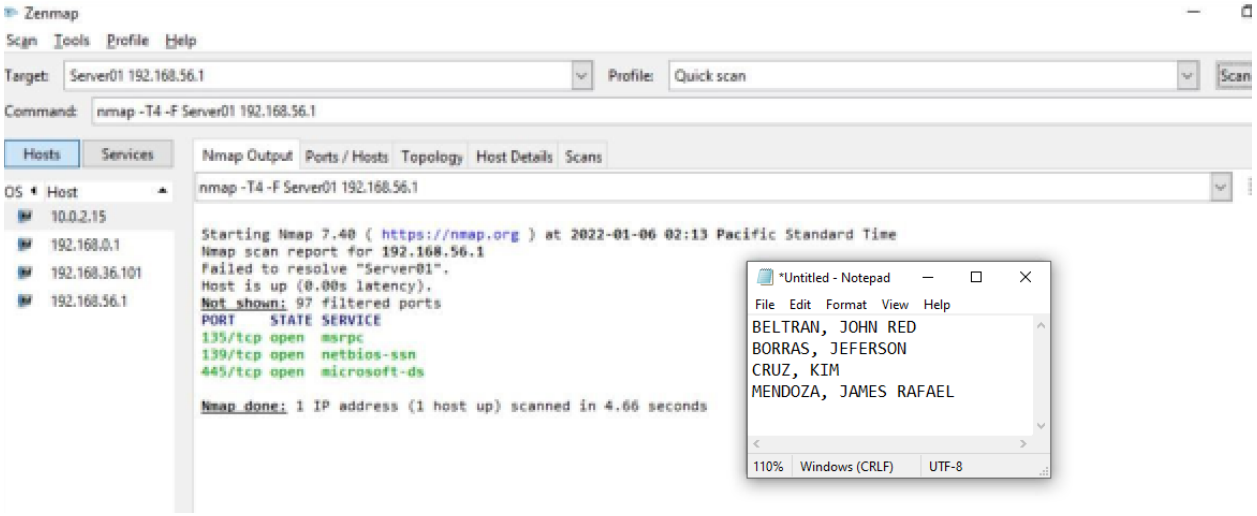
Click Finish

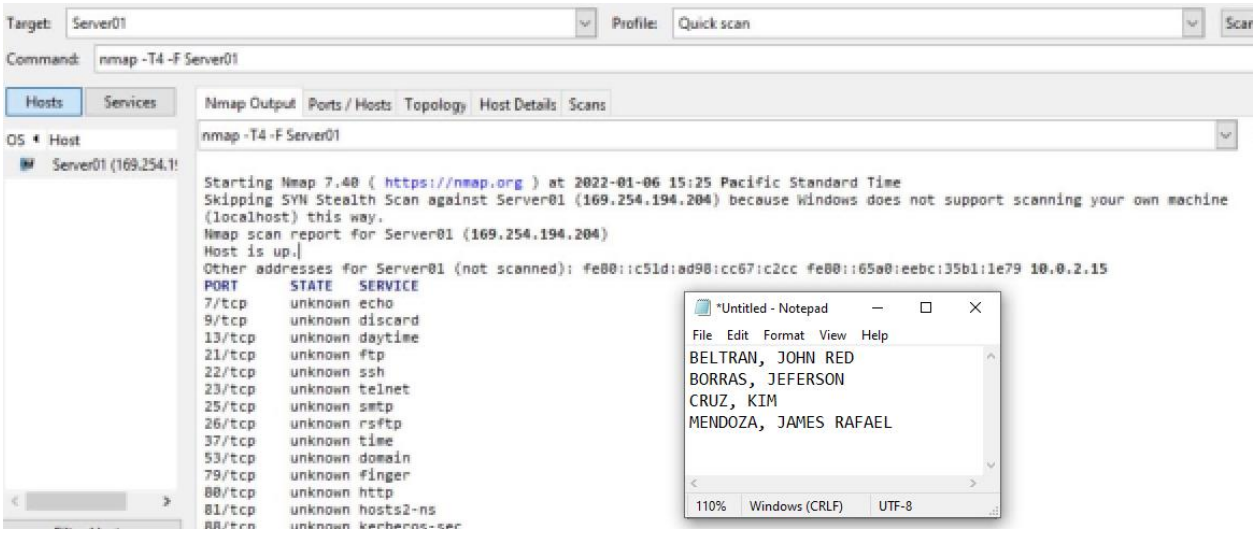


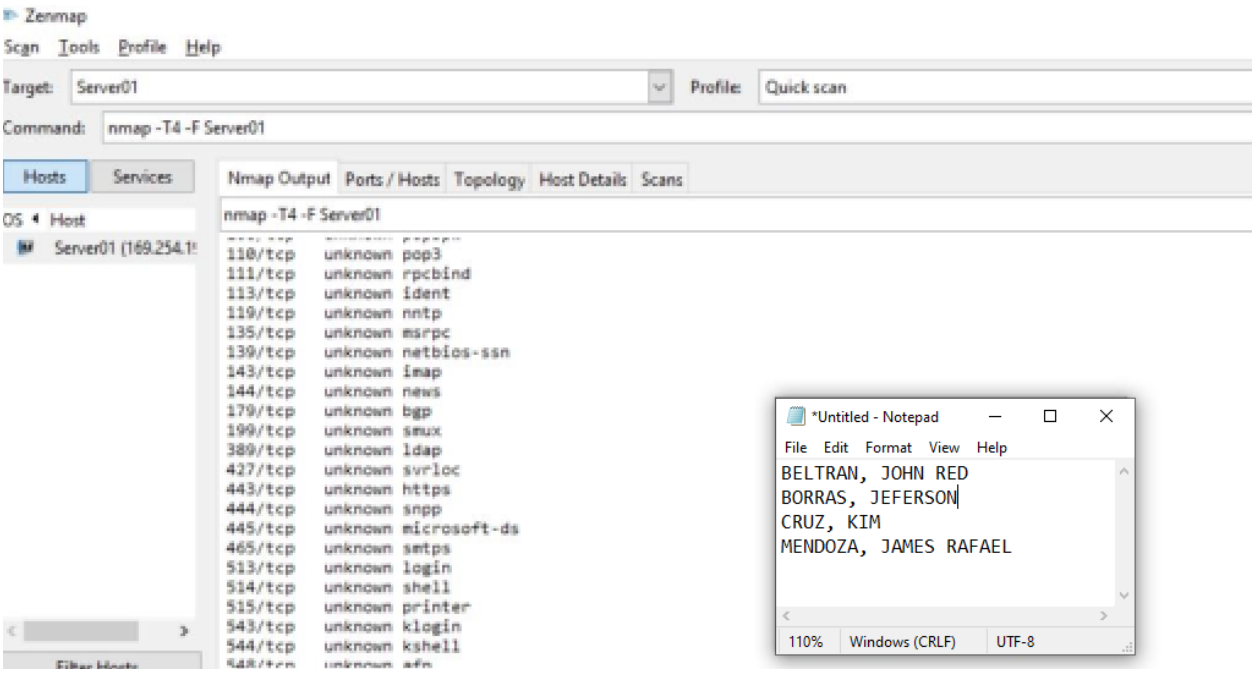
Run the Nmap



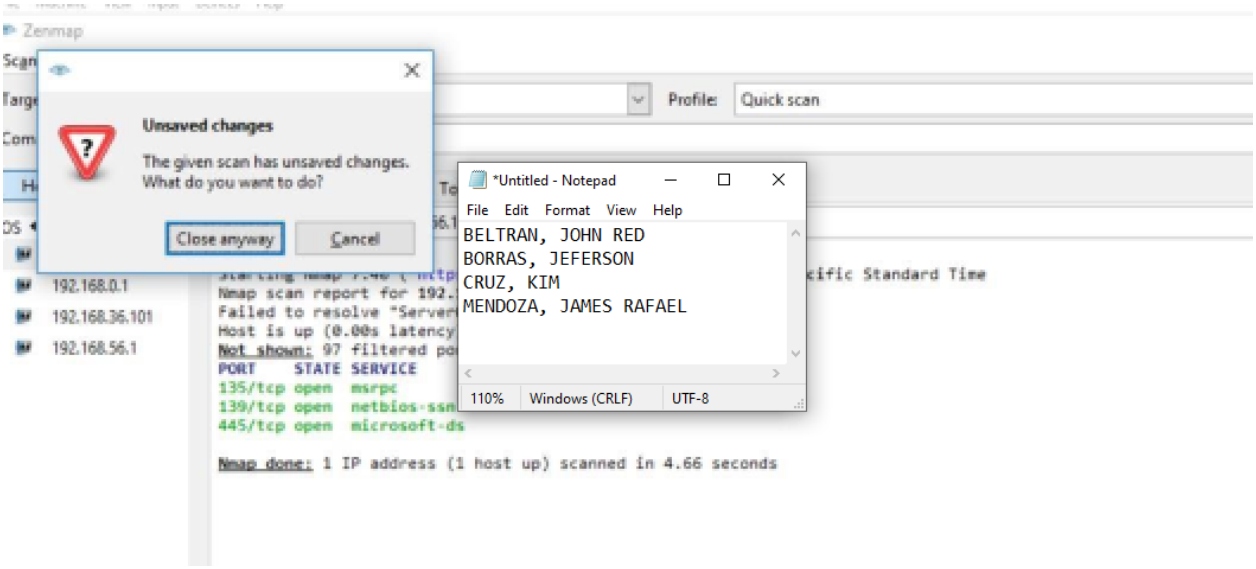
In the target text box, type Server## , where ## is your partner's student number.
In the Profile drop -down, select quick scan and click the scan button to start the scan.
After the scan, several TCP ports were detected as open.







Lastly, close the Zenmap.



Answer the following questions:

a) **What type of attack is of the most concern in your environment?**

- The type of attack that is most concerned about in our environment is probably the phishing attack, since we are in a pandemic and almost every one of us is using the internet, more people are vulnerable to these types of attacks.

b) **Which type of attack do you think might be the most difficult to guard against?**

- The most difficult attack to guard is probably ransomware because with one wrong click of a website or a file, your whole computer will be affected and all of your files will be encrypted, it will cost a huge amount of money to recover your systems data.

"We affirm that we have not given or received any unauthorized help on this assignment and that this work is our own."