**PROGRESS TEST 2**

Course code: IAO202

|  |  |
| --- | --- |
| **Student name:** | **Nguyen Tran Vinh** |
| **Student ID:** | **SE160258** |

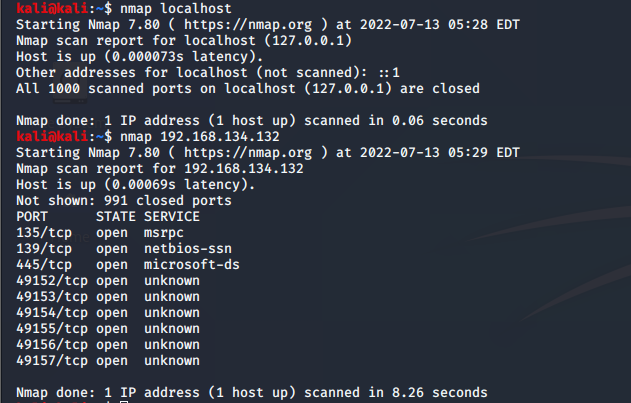
**Part 1: Explain in your words: (2 marks)**

Nmap is a powerful tool for network exploration and management. How can Nmap help with network security? How can Nmap be used by a threat actor as a nefarious tool?

Answer: Nmap can be used to scan an internal network for specific open ports to identify the extent of a security breach. It can also be used to inventory a network to ensure that all the systems are probably patched against security concerns. On the other hand, nmap can be used for reconnaissance to determine open ports and other information about the network.

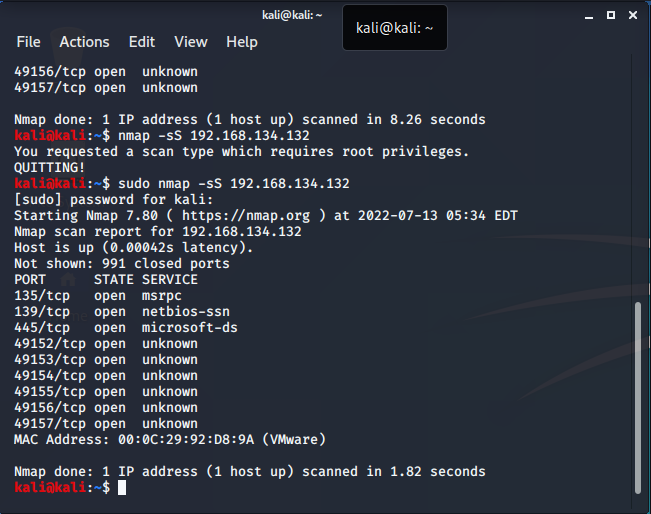
**Part 2: Scan with nmap (4 marks)**

Based on the results of “nmap localhost or any IP address”. Explain your results:



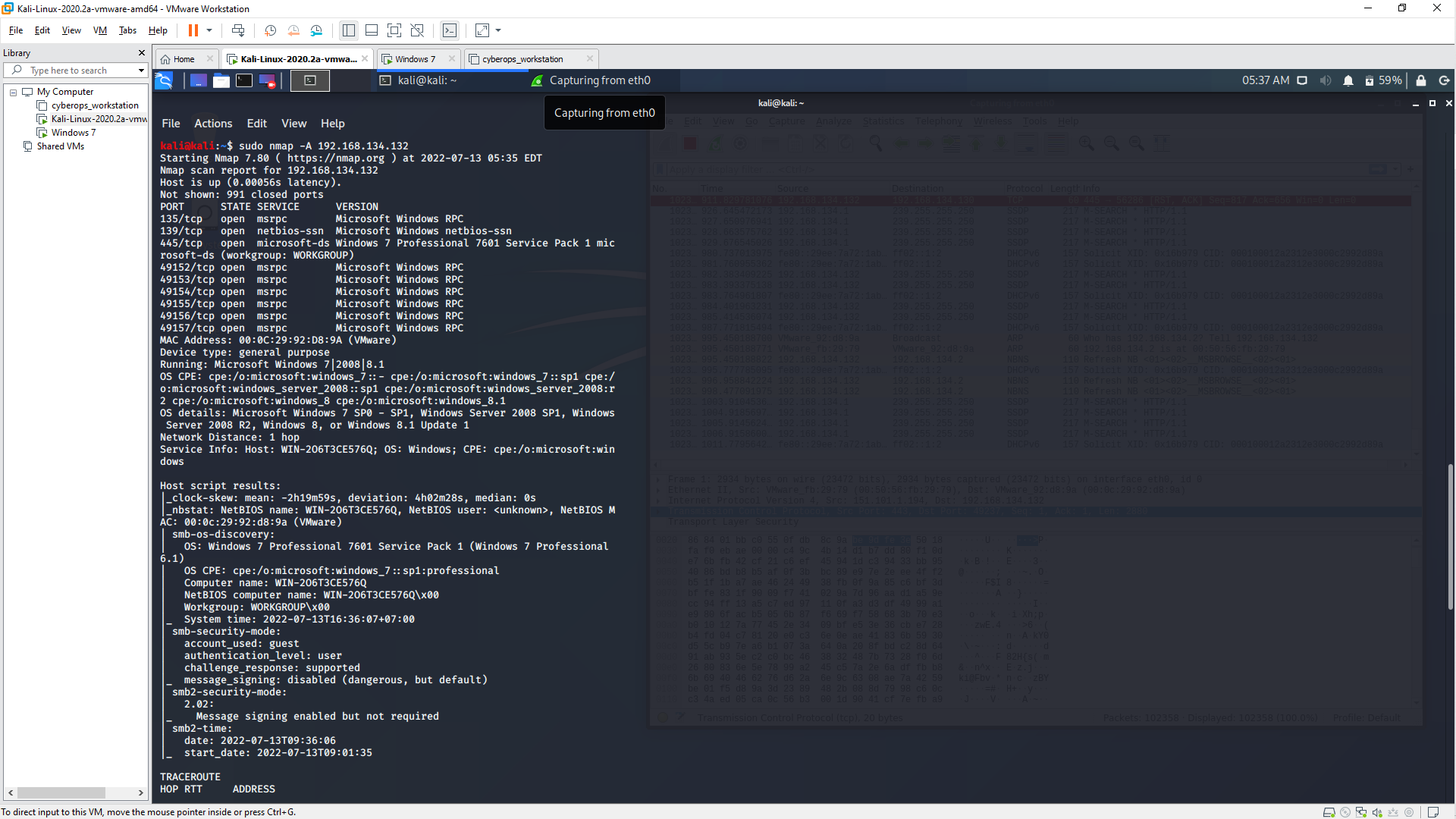
Explain: By default nmap scans only 1000 ports for any given protocol (tcp, udp, whatever)

Based on the results of “nmap –sS localhost or any IP address”. Explain your results:



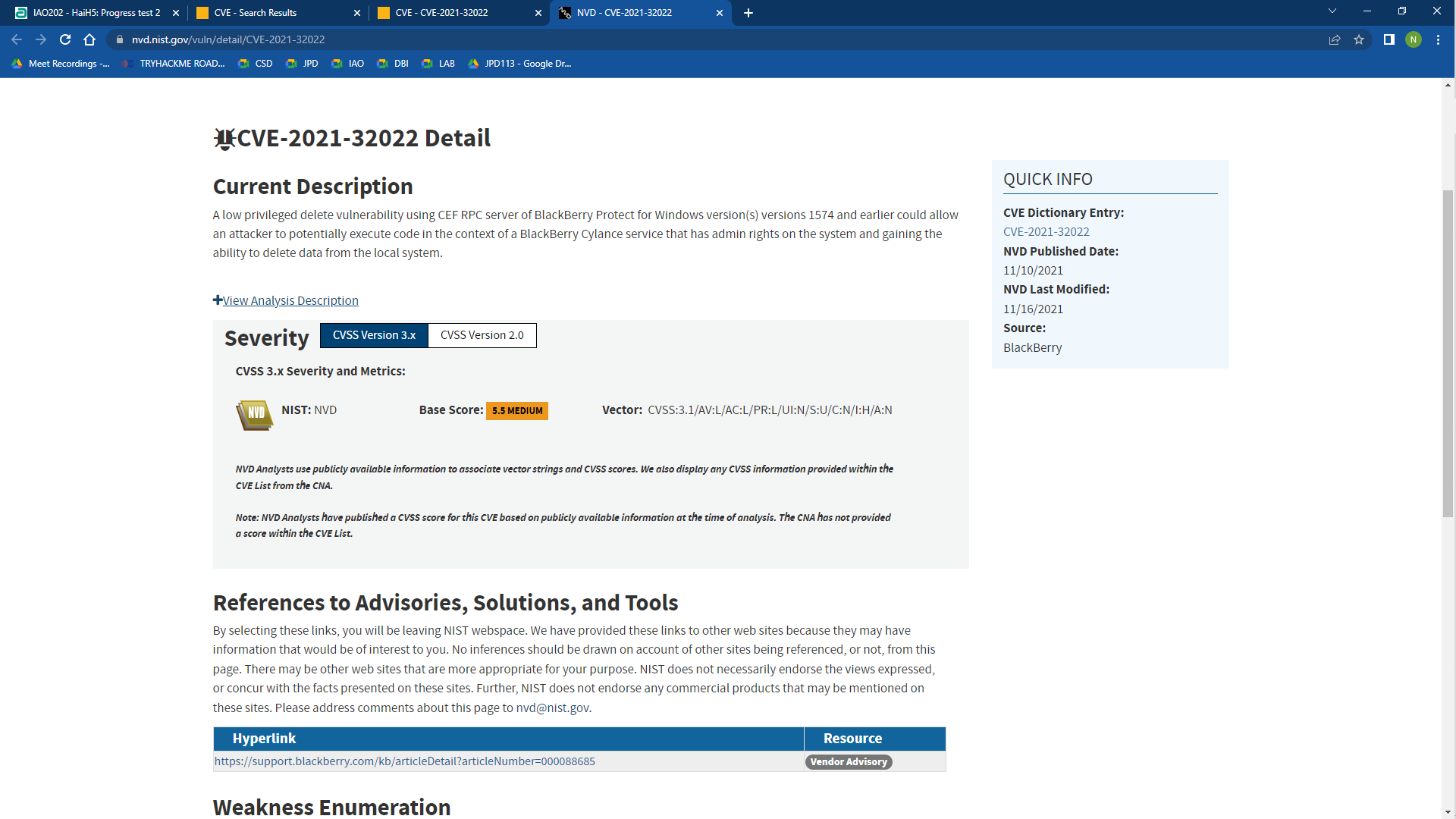
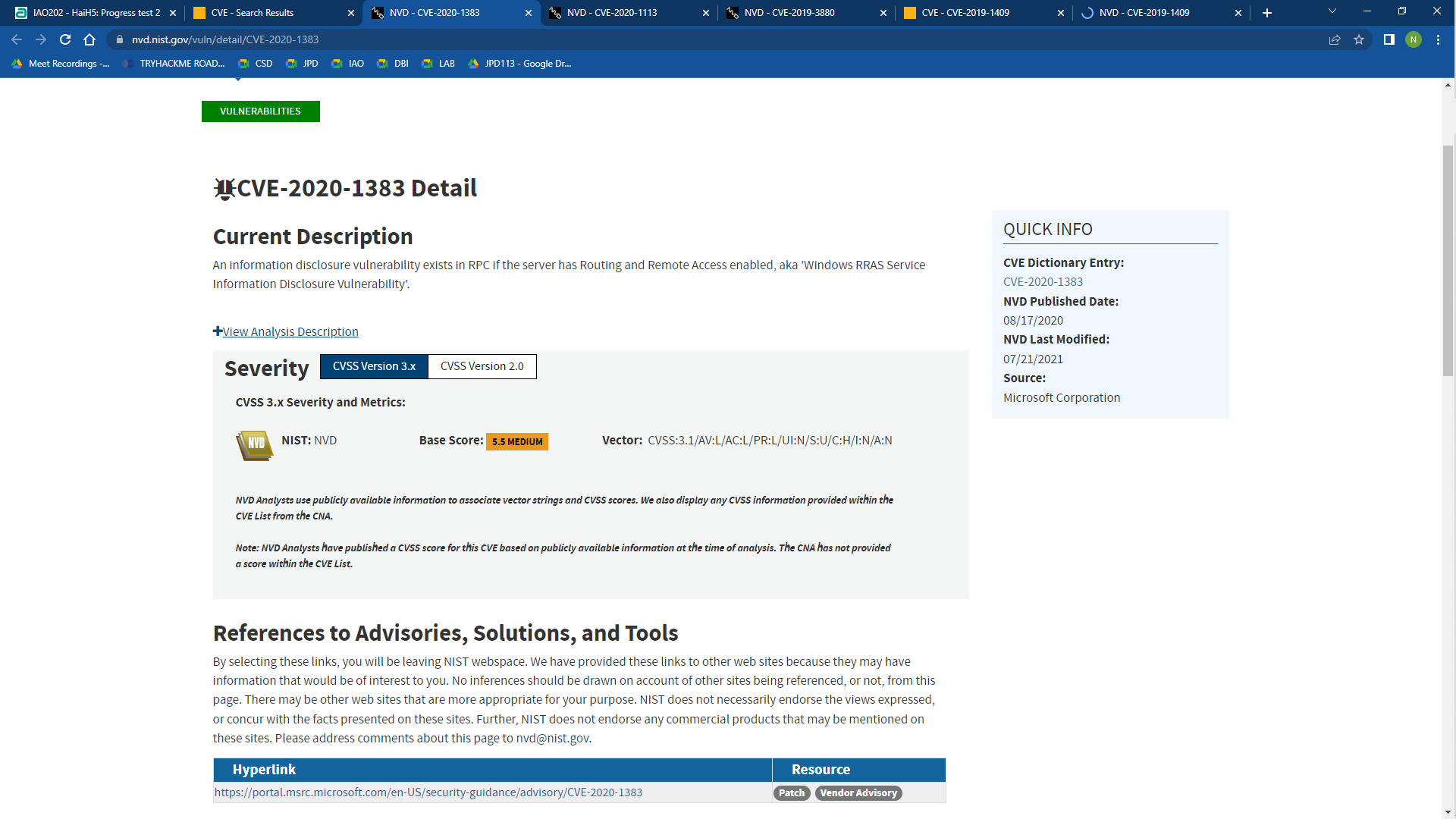
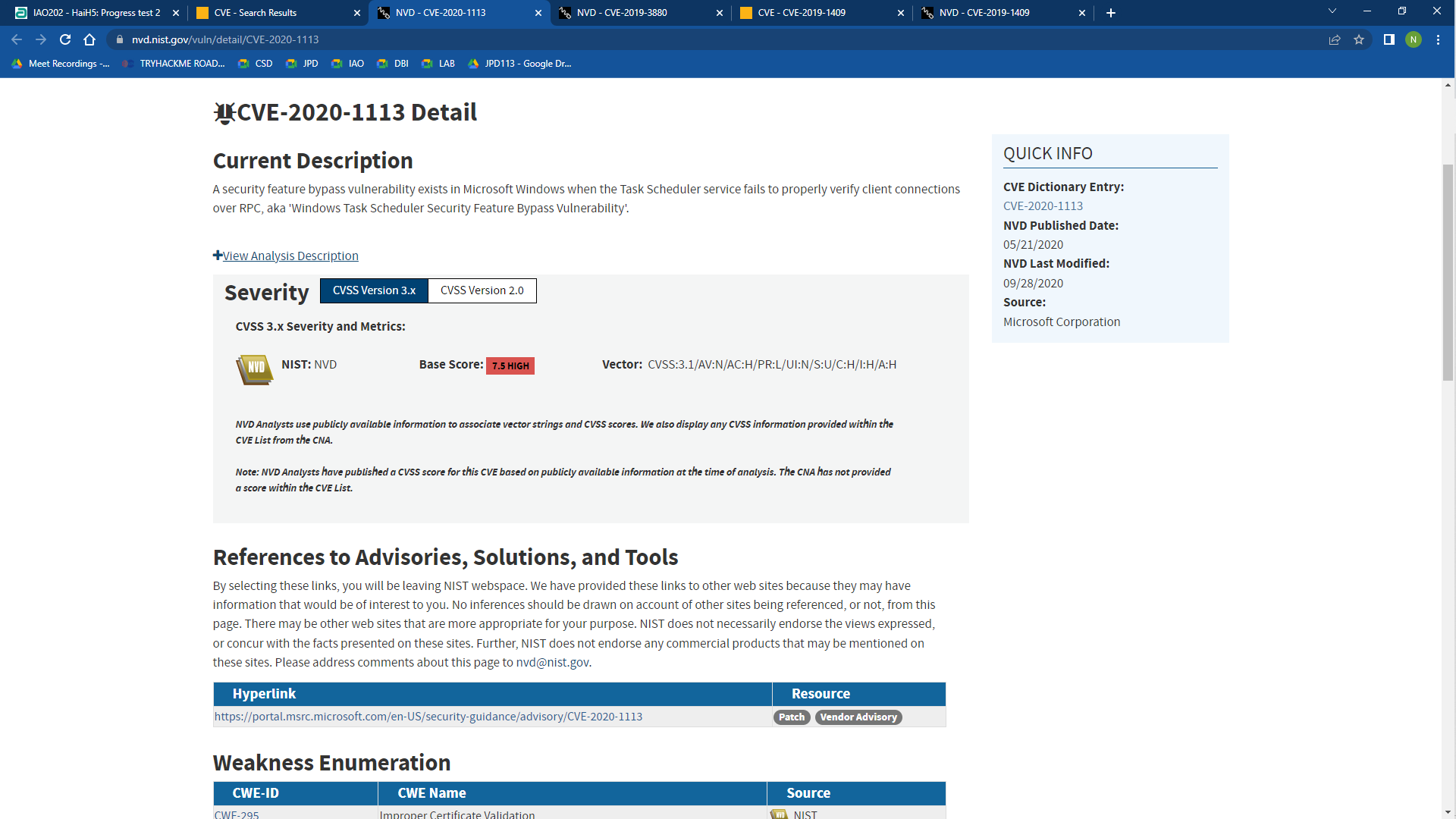
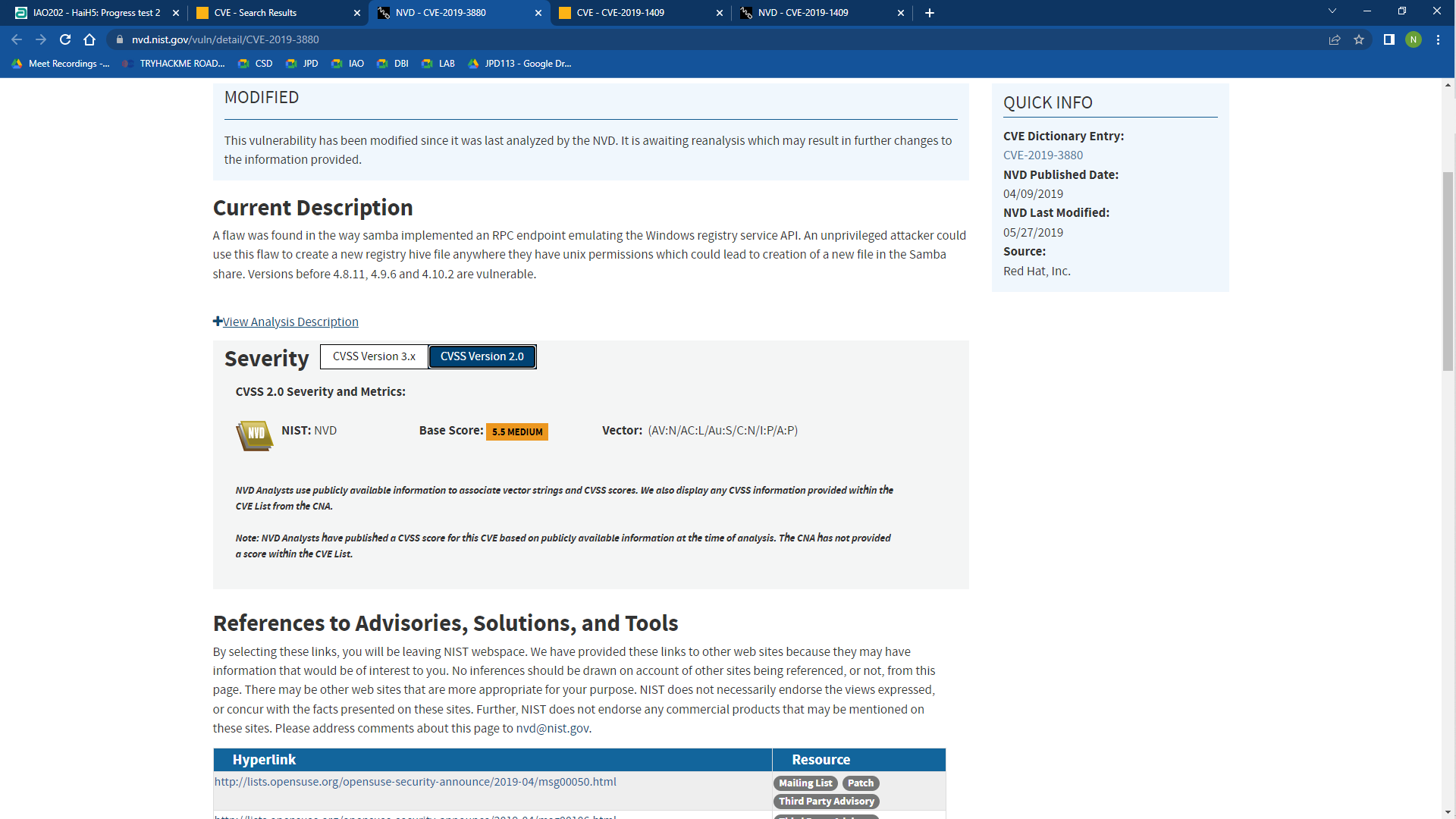
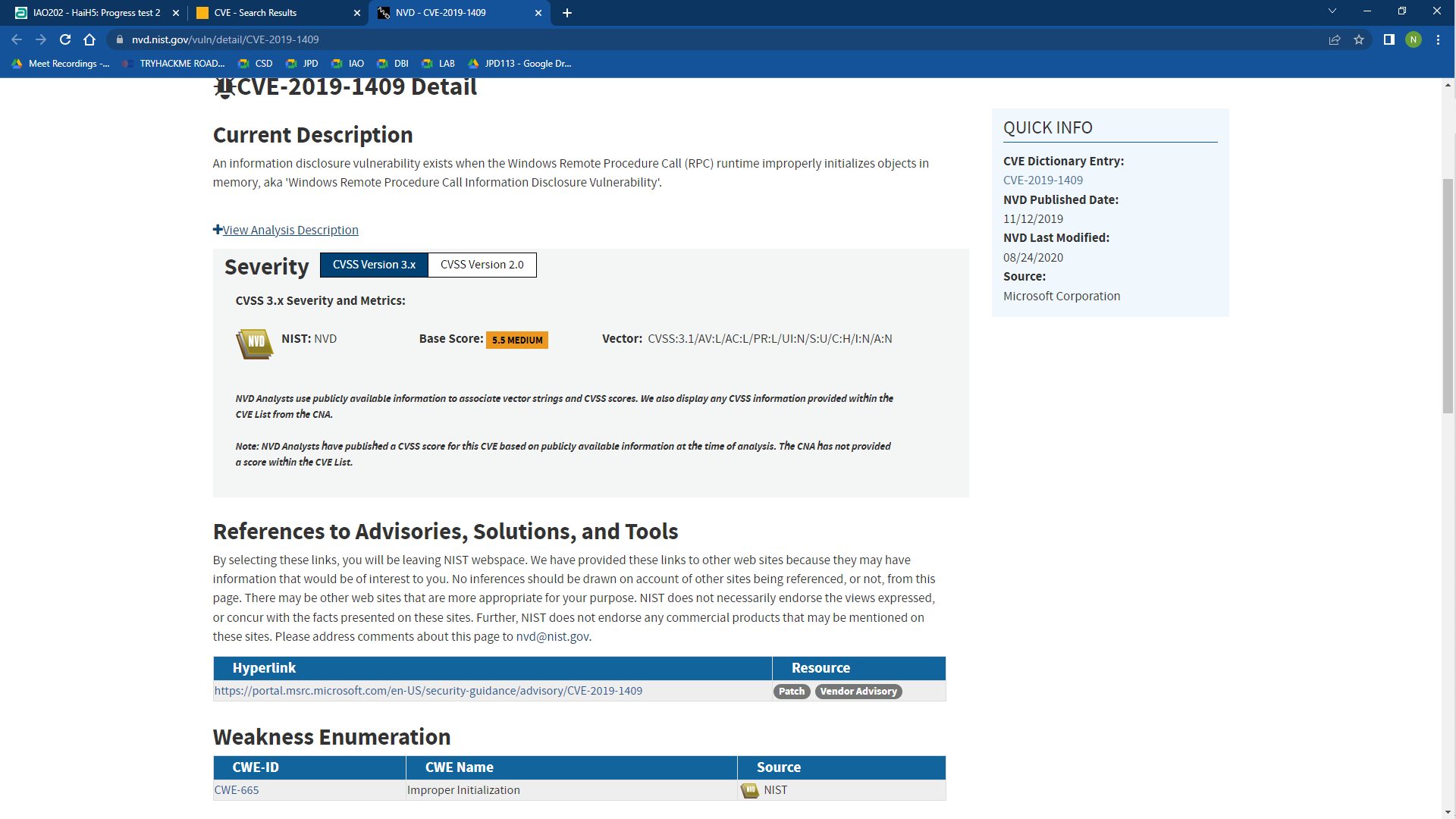
Explain: TCP SYN/Connect()/ACK/Window/Maimon scans

Based on the results of “nmap –A localhost or any IP address”. Explain your results:



Explain: Enable OS detection, version detection, script scanning, and traceroute

**Part 3: based on https://cve.mitre.org/, list 5 vulnerabilities on your computer (2 marks)**

**Part 4: Compare SYN scan và XMAS scan. What is XMAS used for? Why? (2 marks)**

Answer:

- SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. XMAS scan exploit a subtle loophole in the TCP RFC to differentiate between open and closed ports, advantage is that these scan types are a little more stealthy than even a SYN scan.

- In the Xmas scan, Nmap sends packets with URG, FIN, and PSH flags activated. Because this has the effect of "lighting the packet up like a Christmas tree" and can occasionally solicit a response from a firewalled system. Not all systems will respond to probes of this type.

**Note: YOU MUST SUBMIT A FULL-SCREEN IMAGE TO GET FULL CREDIT!**

**END**