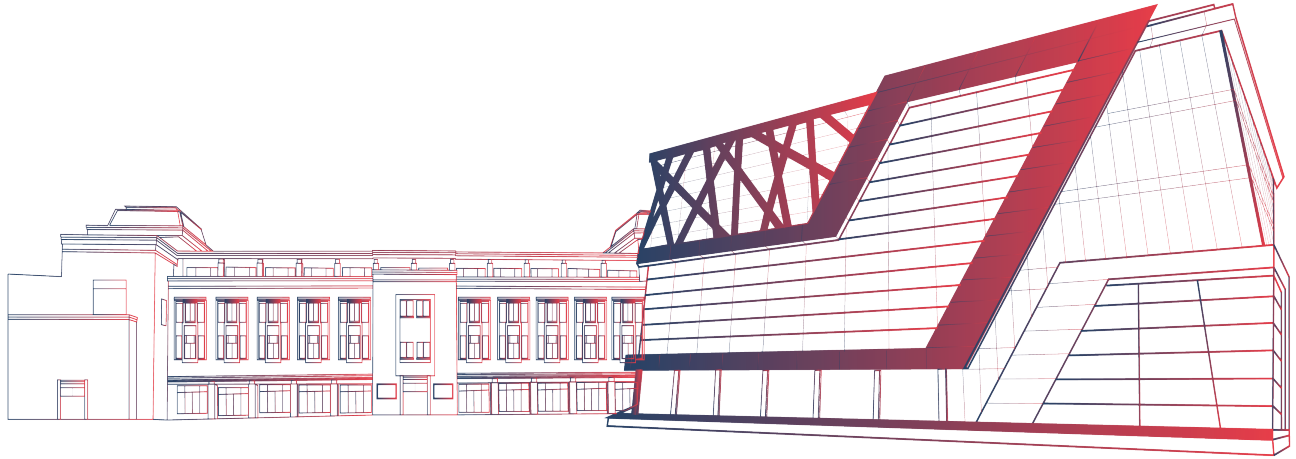
THE NORTHCAP UNIVERSITY

Scanning and Enumeration



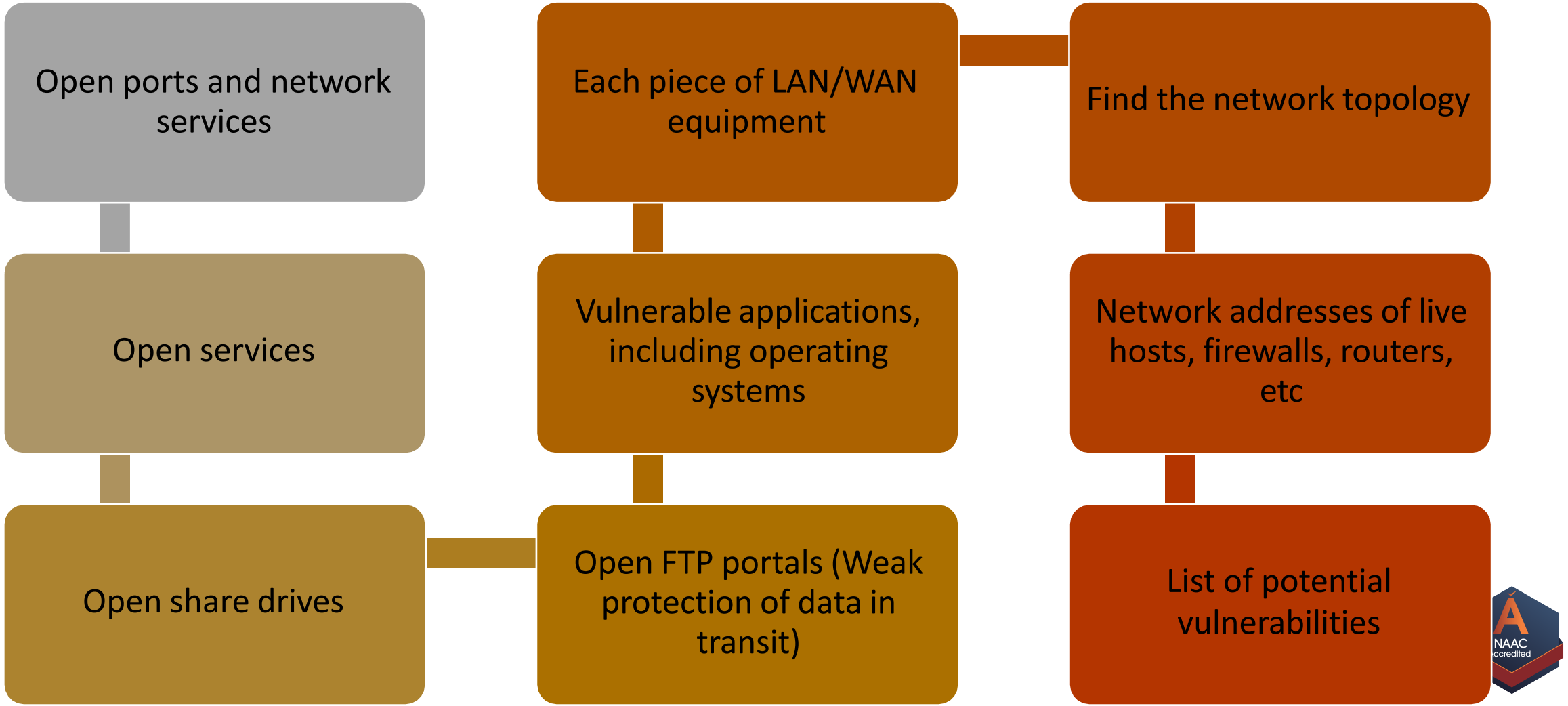
30 YEARS OF EXCELLENCE

NAAC Accredited

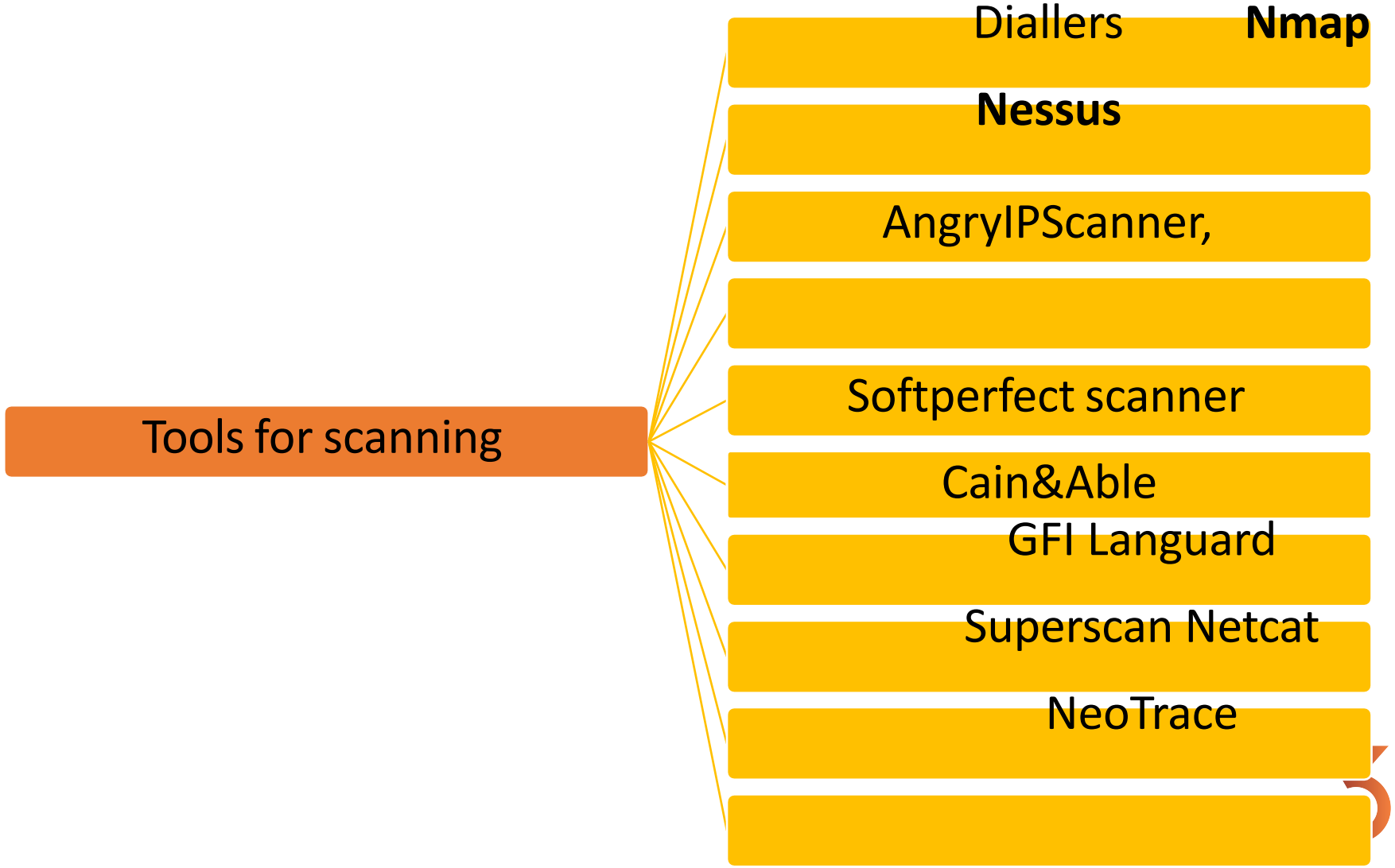
Scanning

- **Active reconnaissance** is commonly referred to as *scanning*.
- Take the information discovered during reconnaissance and use it to **examine the network.**
- The process of **scanning perimeter and internal network devices** for weaknesses.
- Looking for information **that can help to perpetrate attack**

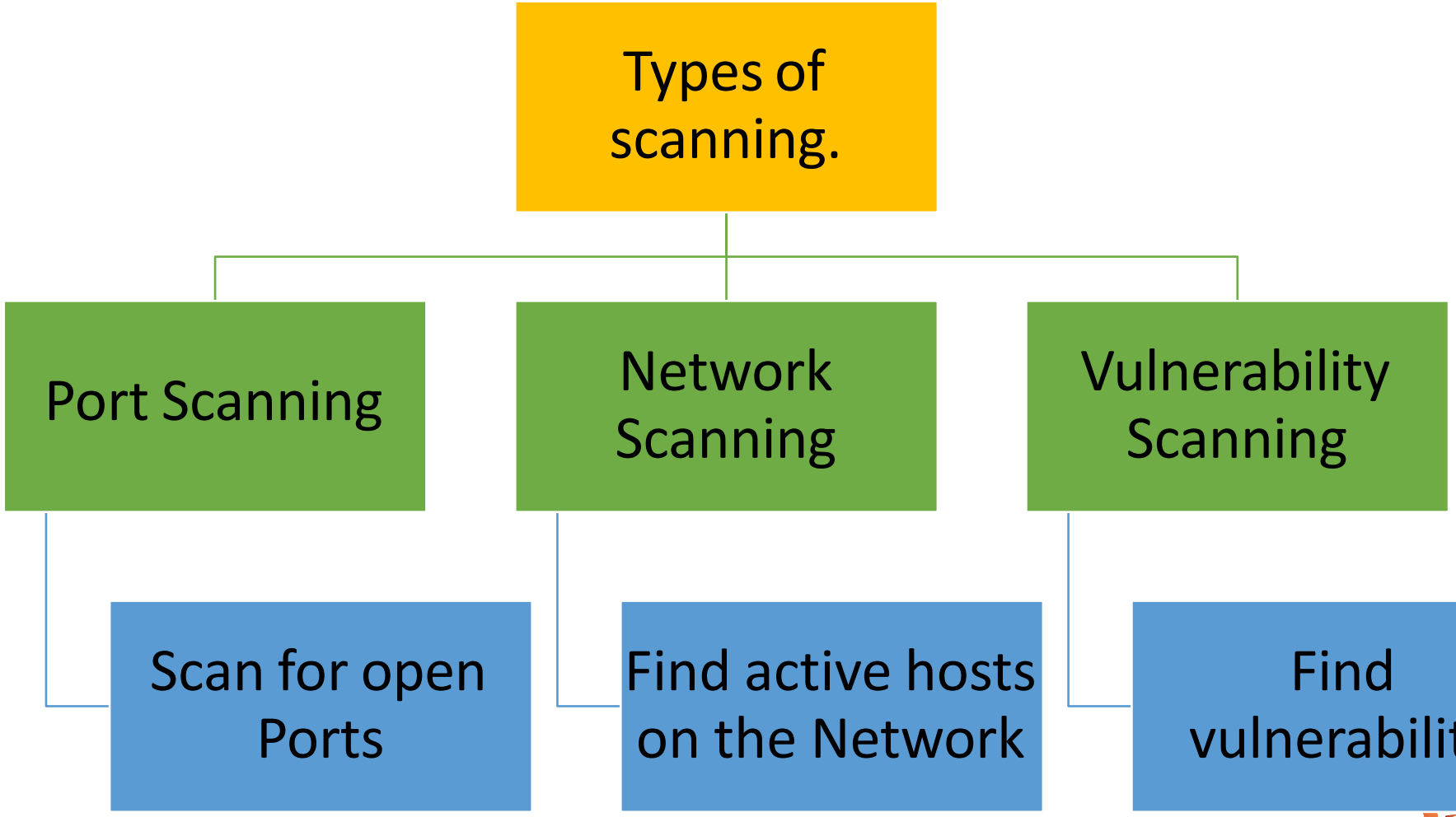
Scanning


Open ports and network services
Open services
Open share drives
Each piece of LAN/WAN equipment
Vulnerable applications, including operating systems
Open FTP portals (Weak protection of data in transit)
Find the network topology
Network addresses of live hosts, firewalls, routers, etc
List of potential vulnerabilities

Scanning tools



Types of Scanning



THE NORTHCAP UNIVERSITY

Port Scanning

30 YEARS OF EXCELLENCE

NAAC Accredited

What is a port? Why we need it?

THE NORTHCAP UNIVERSITY

An **IP Address** identifies what *host* we want our data to go to, but not which of the many ***processes***. In **Internet** this is the ***port number***.

Ports are used to route incoming information to specific applications on a designated machine.

A Port is associated with an IP address of the host

Example: Port no.

Web servers usually "listen on" port 80.

Web servers **open this port, listen for incoming connections** from web browsers.

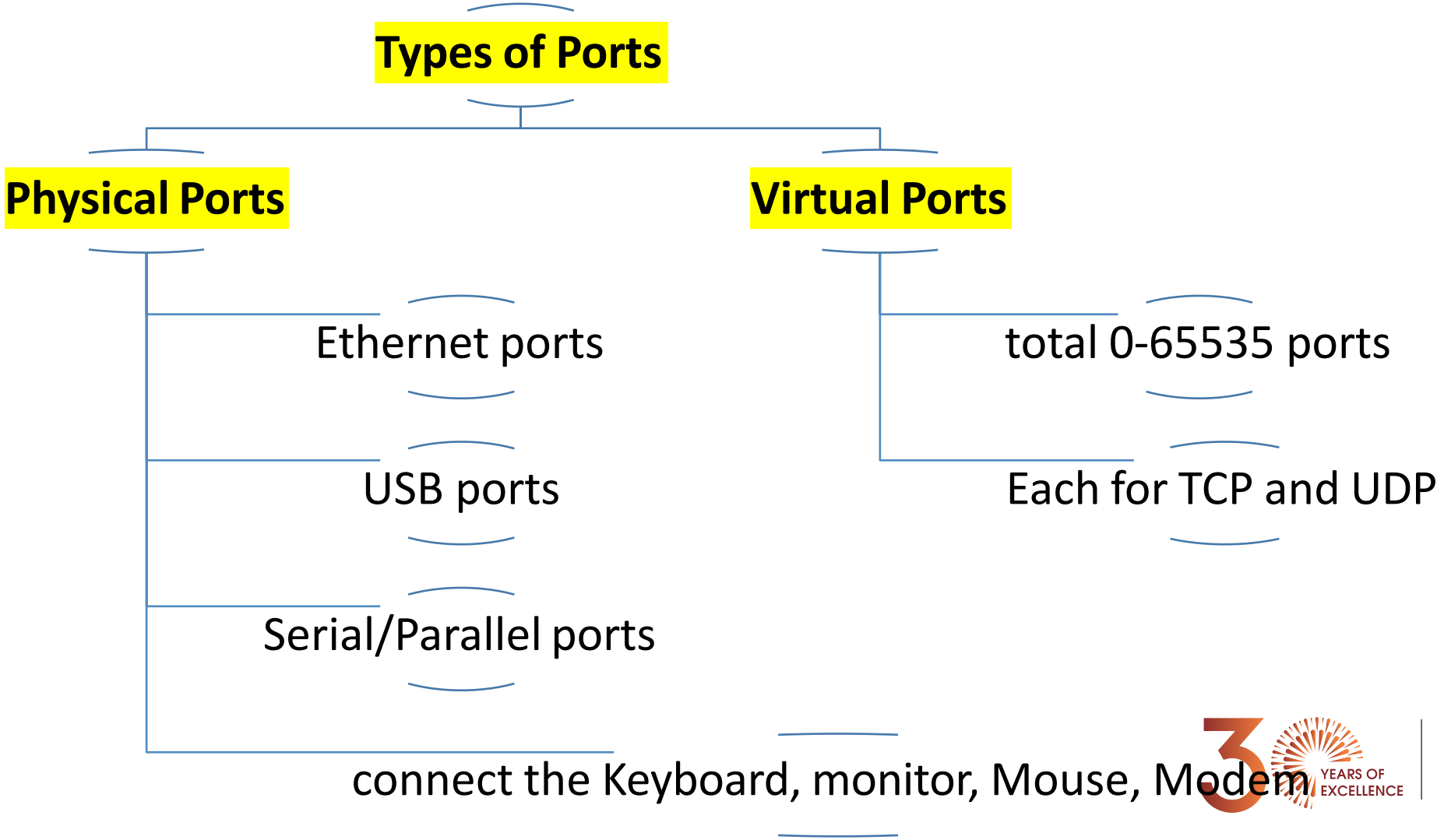
So, when you give the **URL** http://www.usna.edu/,

the **browser** asks **DNS to resolve name** to IP 136.130.88.145

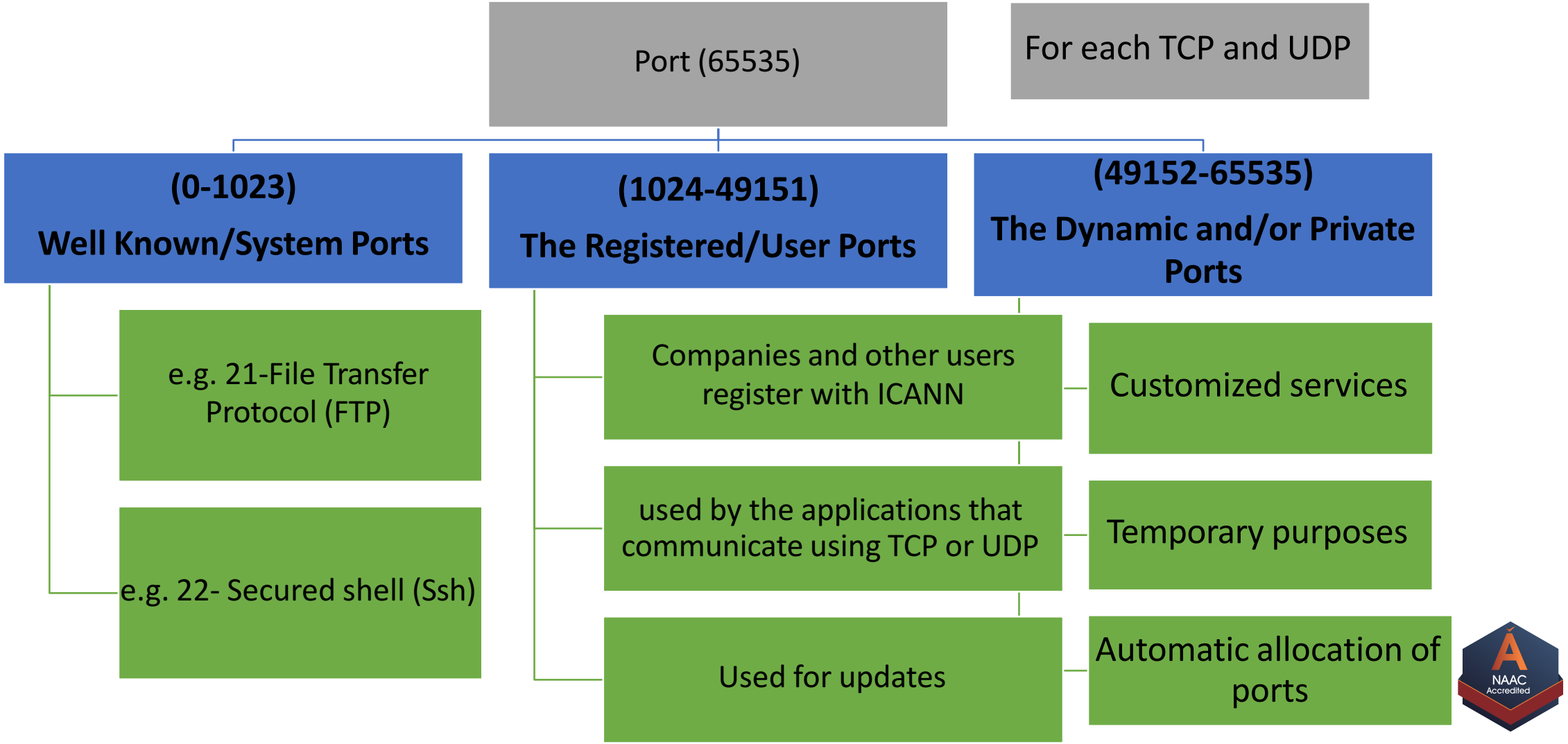
Then sends its **GET** request to 136.130.88.145 on port 80

because web servers uses port 80.

PORTS


Types of Ports
Physical Ports
Virtual Ports
Ethernet ports
USB ports
Serial/Parallel ports
connect the Keyboard, monitor, Mouse, Modem
total 0-65535 ports
Each for TCP and UDP

Ports are divided into



Registered and Private Ports

THE NORTHCAP UNIVERSITY

Registered ports :

- 1234 : VLC media player
- 1241 : Nessus Security Scanner
- 1604: DarkComet
- 1812: RADIUS protocol
- 3306 : MySQL
- 5269 : XMPP
- 5500, 5800, 5900 : VNC
- 25565 : MySQL

30 YEARS OF EXCELLENCE | NAAC Accredited

In class Task: To identify OS

445, 135 -> Microsoft is using this port to provide service

Ping 127.0.0.1

TTL=128

cmd (windows)

See the response ?? TTL

Windows Based Machine

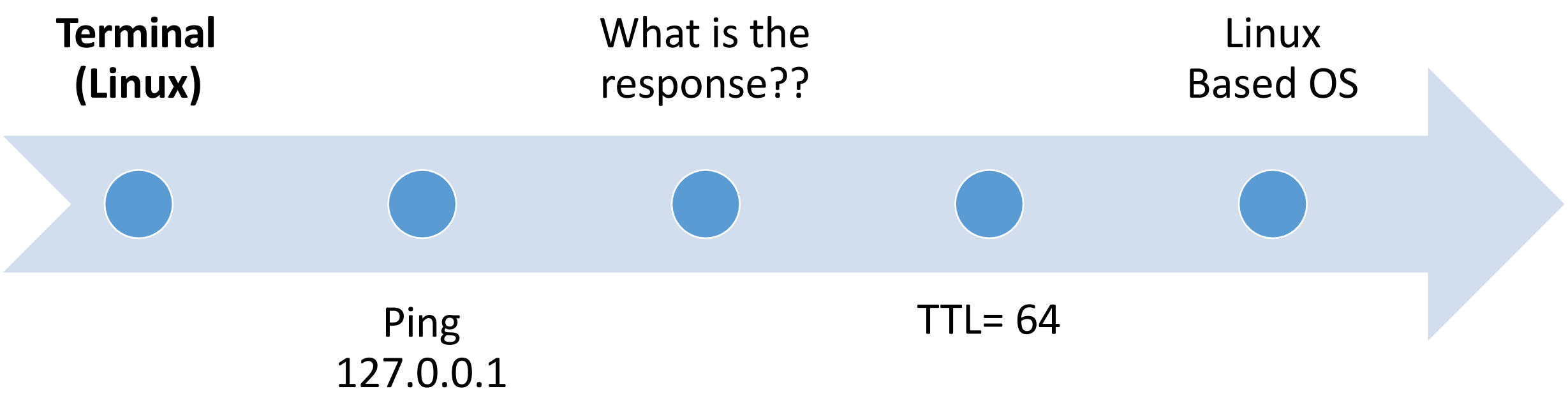
```
C:\Users\Mehak Khurana>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Mehak Khurana>
```

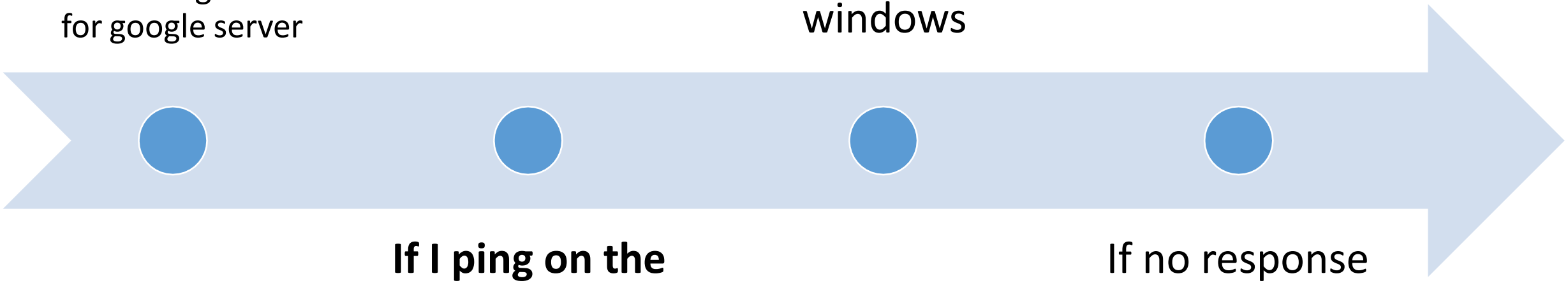
In class Task: To identify OS



To identify server

If it is a server

- Then TTL might variate e.g. ttl=53 for google server

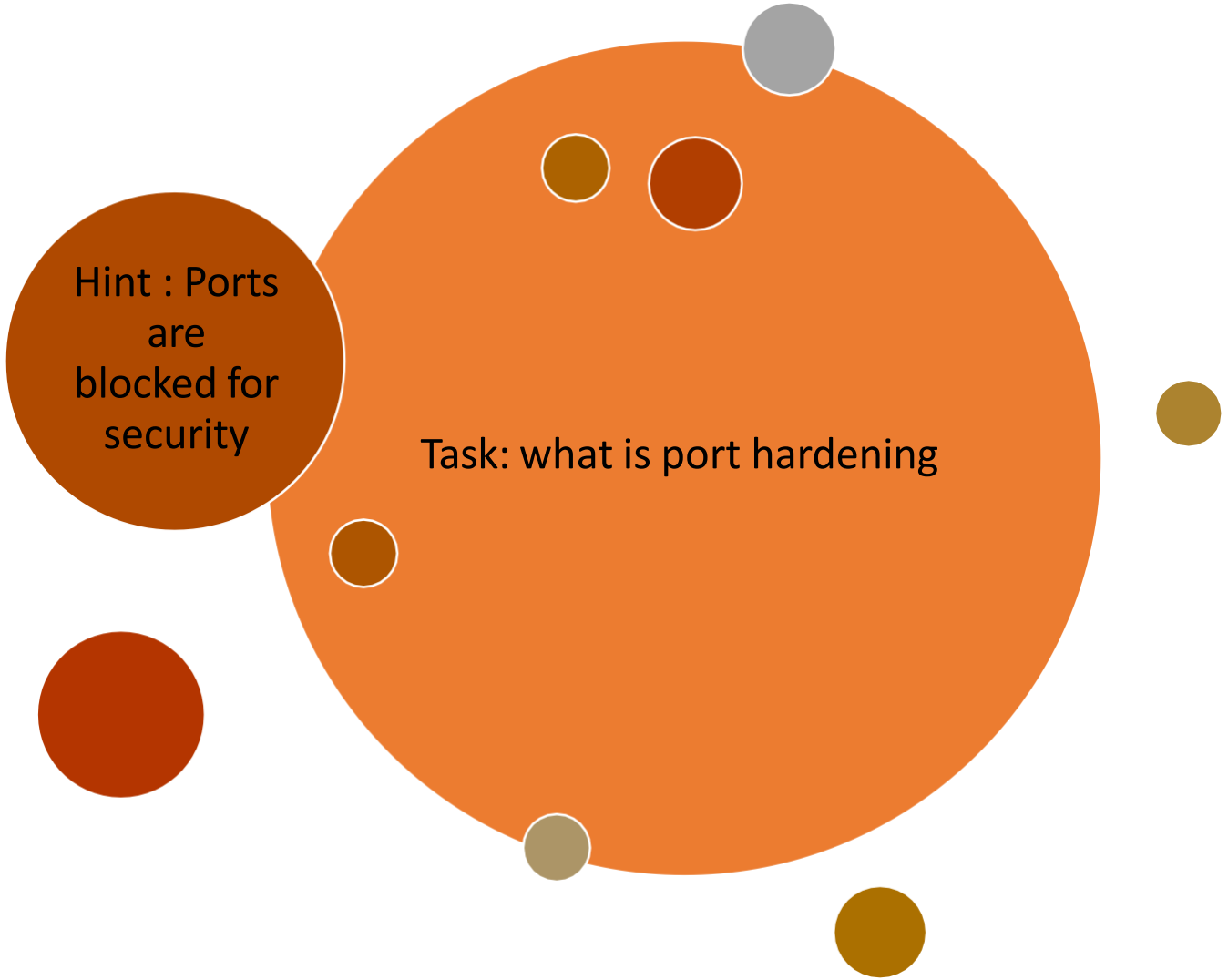


If I ping on the system on port 445

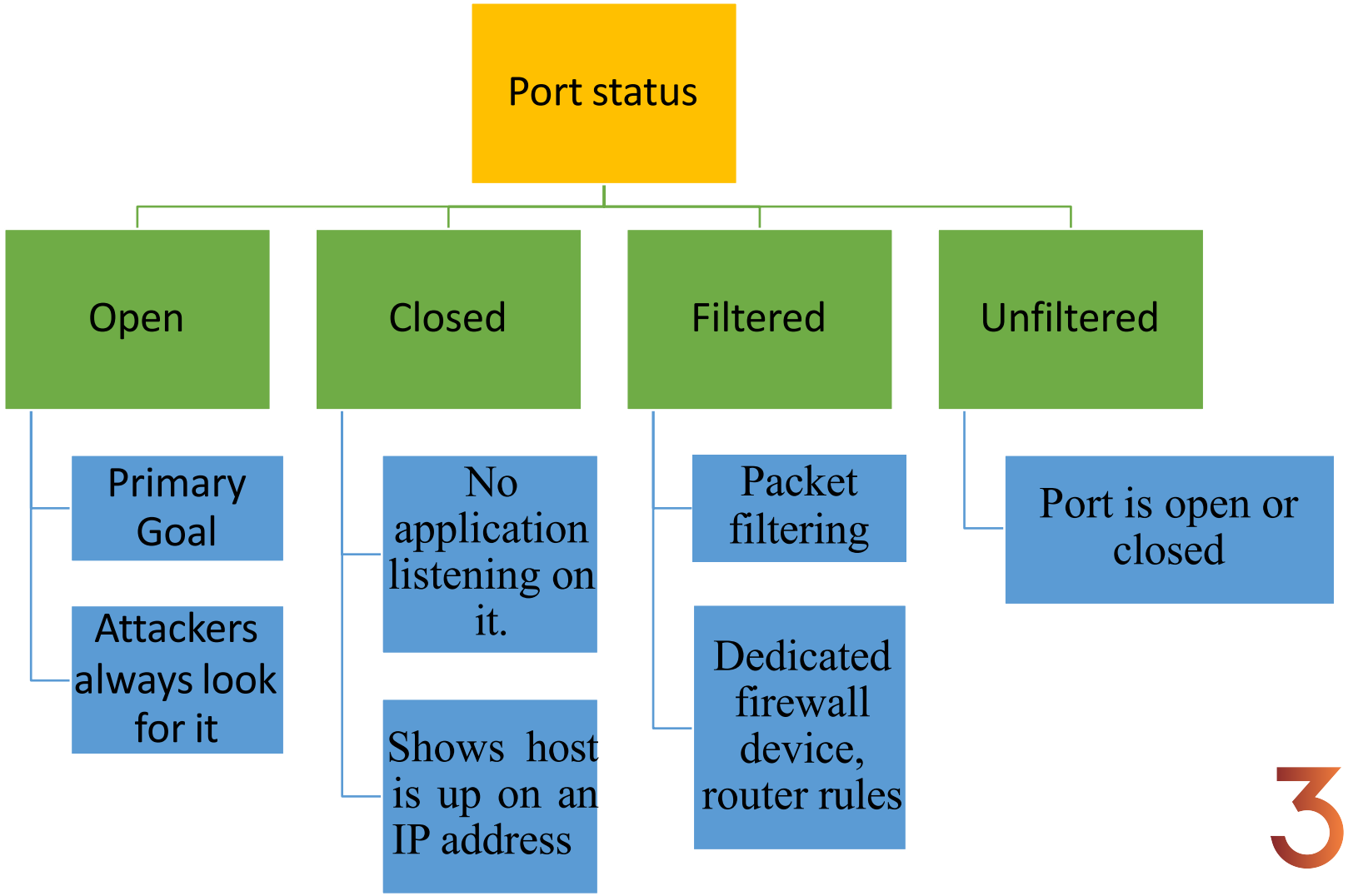
If I get a response, it is windows

If no response it is Linux

In class task



Port Scanning



Port Scanning

THE NORTHCAP UNIVERSITY

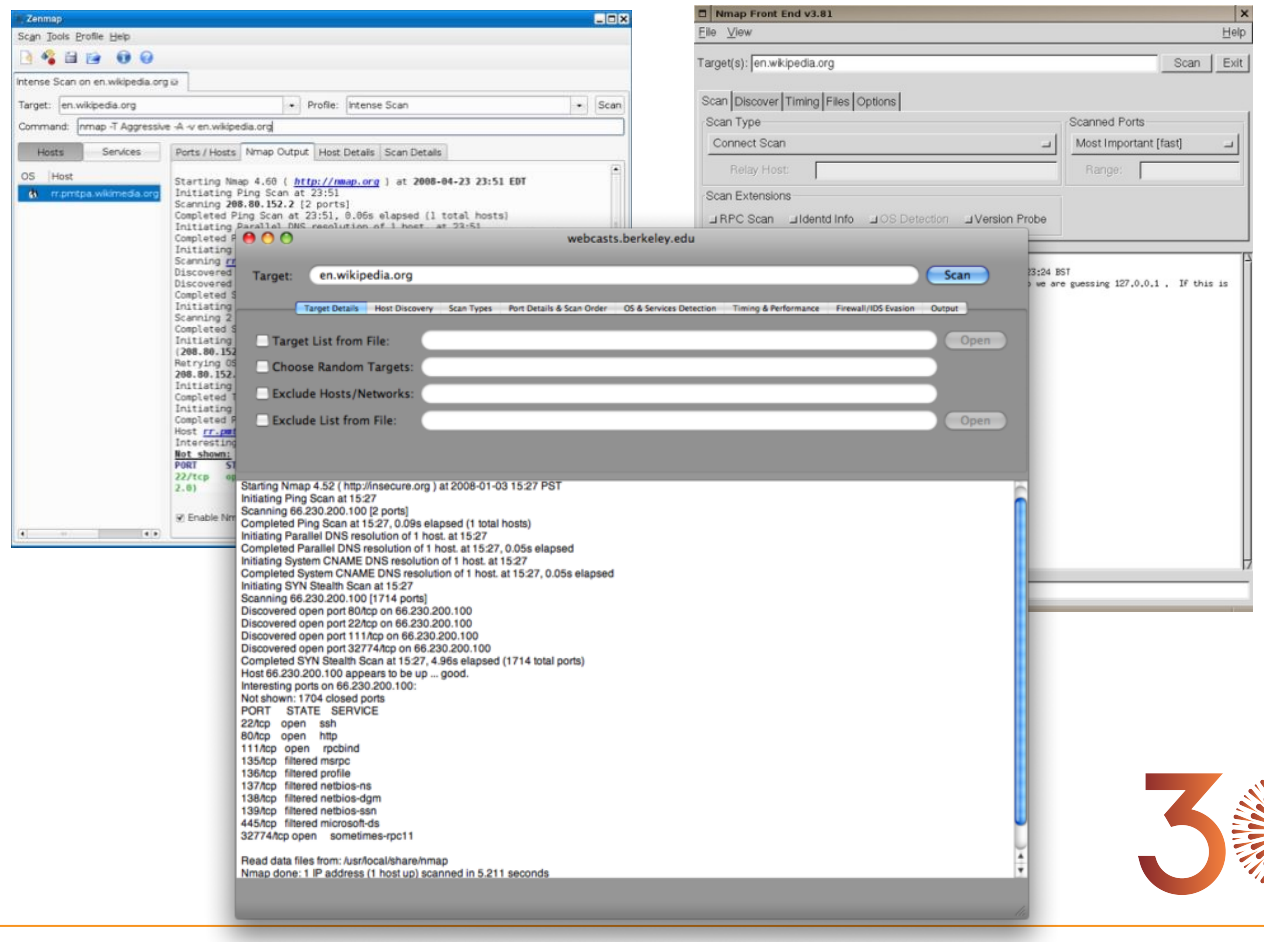
Tool for Port Scanning: Nmap-CLI and GUI based

30 YEARS OF EXCELLENCE

NAAC Accredited

Tool Environment

- Runs on Linux, Windows, Mac OS X and other smaller operating systems
- GUI options:
  - Zenmap
  - XNMap
  - NmapFE



NMap

THE NORTHCAP UNIVERSITY

Nmap (Network Mapper) was released in **September 1997**

It is a **free and open source utility** for

- Network discovery
- Security auditing

Determines the following

- The **up or down status of a host**
- **Network services** available on a host
- **Presence of a firewall**
- **Operating system and version** used on host
- **Name and version of services** running on host

How Nmap Works?

THE NORTHCAP UNIVERSITY

It uses DNS lookup- It matches **name with IP address**

It **pings** the remote target **with 0-byte packets** to each port

Sends different **packets with different timing to determine filtered/unfiltered, version, etc.**

30 YEARS OF EXCELLENCE

NAAC Accredited