- **Let's learn new ICT skills every week**
- **To enhance your expertise**

# Foot printing

# Exercise model

# Foot printing

- **Port availability** => target system's port
- **Banner grabbing** => target system's Banner
- **Netcraft** => target system's OS

# Foot printing #1
# Check port availability

# Ports

- **Ports 0 to 1023 => Well-Known Ports**

- Ports **1024** to **49151** => are Registered Ports (*Often registered by a software developer to designate a particular port for their application)

- Ports **49152** to **65535** => are Public Ports

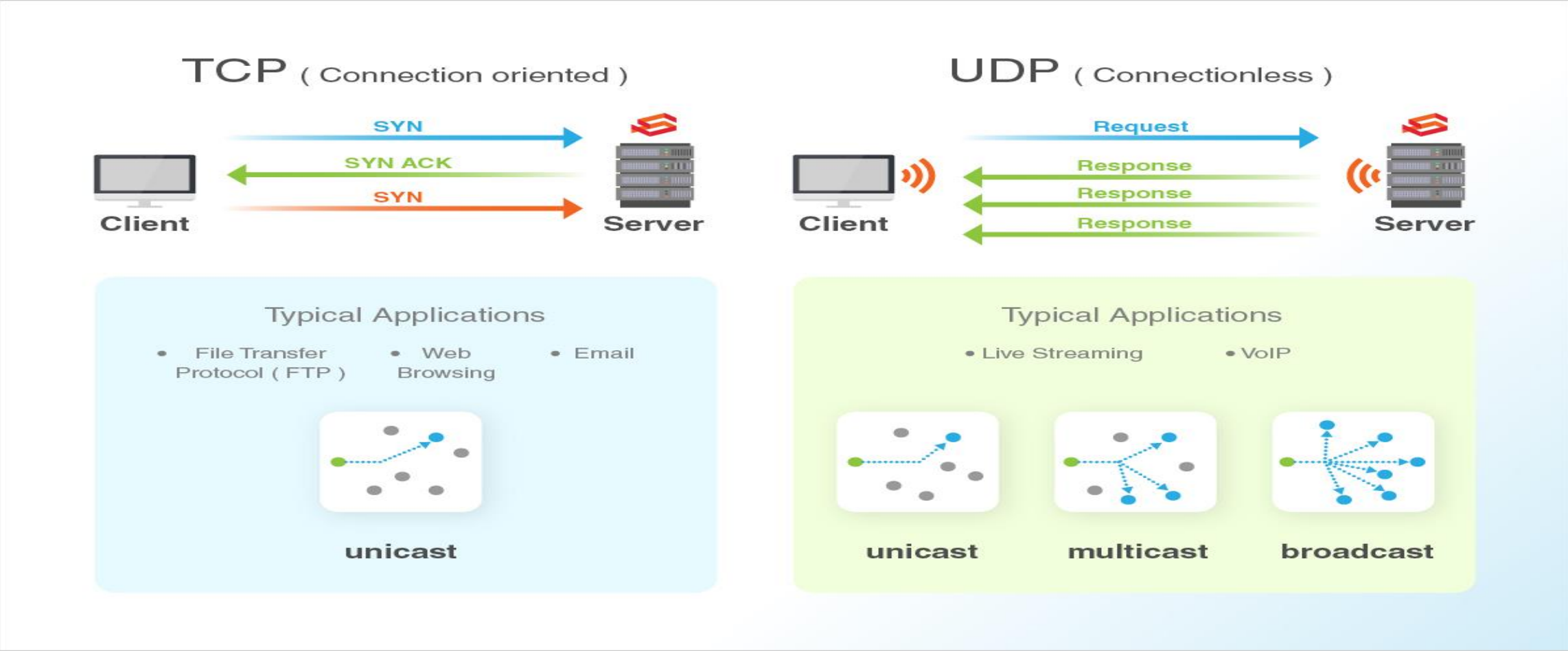
# How to check if TCP / UDP port is open on Linux & Windows Cloud Servers

**Vulnerable open ports** can be the cause of severe security breaches in a server.

It is a must that such ports are found out and closed/disabled.

https://www.layerstack.com/resources/tutorials/How-to-check-if-TCP-UDP-port-is-open

# TCP / UDP Ports




https://www.layerstack.com/resources/tutorials/How-to-check-if-TCP-UDP-port-is-open

# Determine which ports are open

This guide outlines the basic steps
to determine which all ports are open in a service

in Linux server
lsof, netstat and nmap

on Windows server
netstat

# list open files

**lsof** (list open files) is a command that is used to display the list of all open files in a server and the services that have opened them.

The general syntax of the lsof command :

# sudo lsof -i -P -n

# Files that are listening on different ports

Using pipe and grep commands,
the result of the above command can be filtered
to show the result of files that are listening
on different ports in the server.

# sudo lsof -i -P -n | grep LISTEN # doas lsof -i -P -n | grep LISTEN (for OpenBSD systems)

# Foot printing #2

# Banner grabbing

# Banner Grabbing

- **“Banner Grabbing”** is often termed as **“Service Fingerprinting”**.

- **Banner refers to a text message received from the host, usually, it includes information about the open ports and services with their version numbers.**

# Banner Grabbing

- **Banner Grabbing** allows an attacker to discover network hosts and running services with their versions on the open ports and moreover operating systems so that he can exploit the remote host server.

- **Banner Disclosure** is the most common vulnerability with a **"CWE-200 i.e. Exposure of Sensitive Information to an Unauthorized Actor"** and a **"CVSS Score of 5.0 with the Risk factor as Medium."**

https://www.hackingarticles.in/multiple-ways-to-banner-grabbing/

# Whatweb banner grabbing using Kali Linux

**banner grabbing using Kali Linux**

“WhatWeb” recognizes websites, which helps us to grab the web-applications banner by disclosing the server information with its version, the IP address, the webpage Title and running operating system.

whatweb <website URL>

```
whatweb http://192.111.0.11
```

# Whatweb package on ubuntu

## whatweb package on ubuntu.

```
sudo apt install whatweb
```

# Netcat

**banner grabbing using Kali Linux**

Netcat is a network utility that will again help us to grab the **FTP banner** of the remote host server.

```
nc  192.111.0.11 21
```

From the above image, you can check that it dumbs up **“220 (vsFTPd 3.0.3)”**

# Foot printing

## Netcraft #3

**Shows various information about the OS of the target.**

# Netcraft

Netcraft is one of the most operatable information gathering web-interface which help us to check the technologies and the infrastructure of the web-applications.

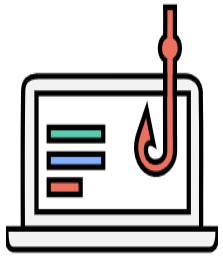
grab some service banners and capture all the possible information

가동시간,운영체제,ip주소,웹서버, 네임서버,사용되는기술

# Netcraft


https://sitereport.netcraft.com/
https://searchdns.netcraft.com/

# Search nformation



**Protect your customers from cybercrime**

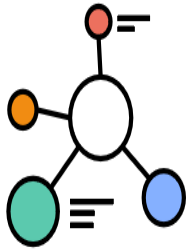
With our ever-expanding and highly automated range of cybercrime disruption services, we're always ready to respond to online threats targeting your organisation and customers.

Learn More

**Keep your network safe**

Have your application or network tested by experienced security professionals, ensuring that the risk of a cybercrime attack against your organisation is minimised.

Learn More



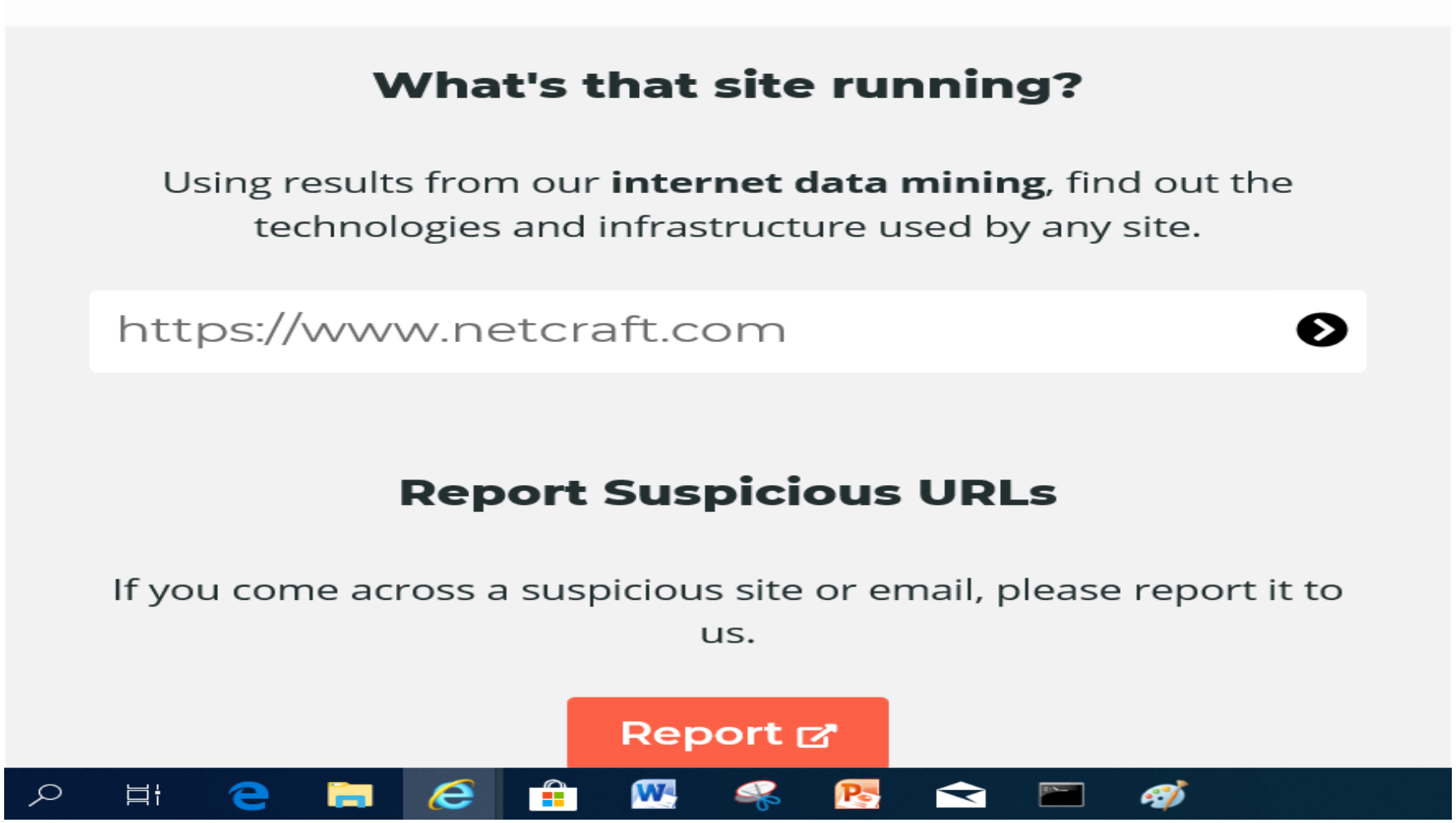
**Explore the internet's growth**

We have been surveying the web since 1995 and can provide insights into trends and movement patterns on hosting companies, certificate authorities and web technologies.

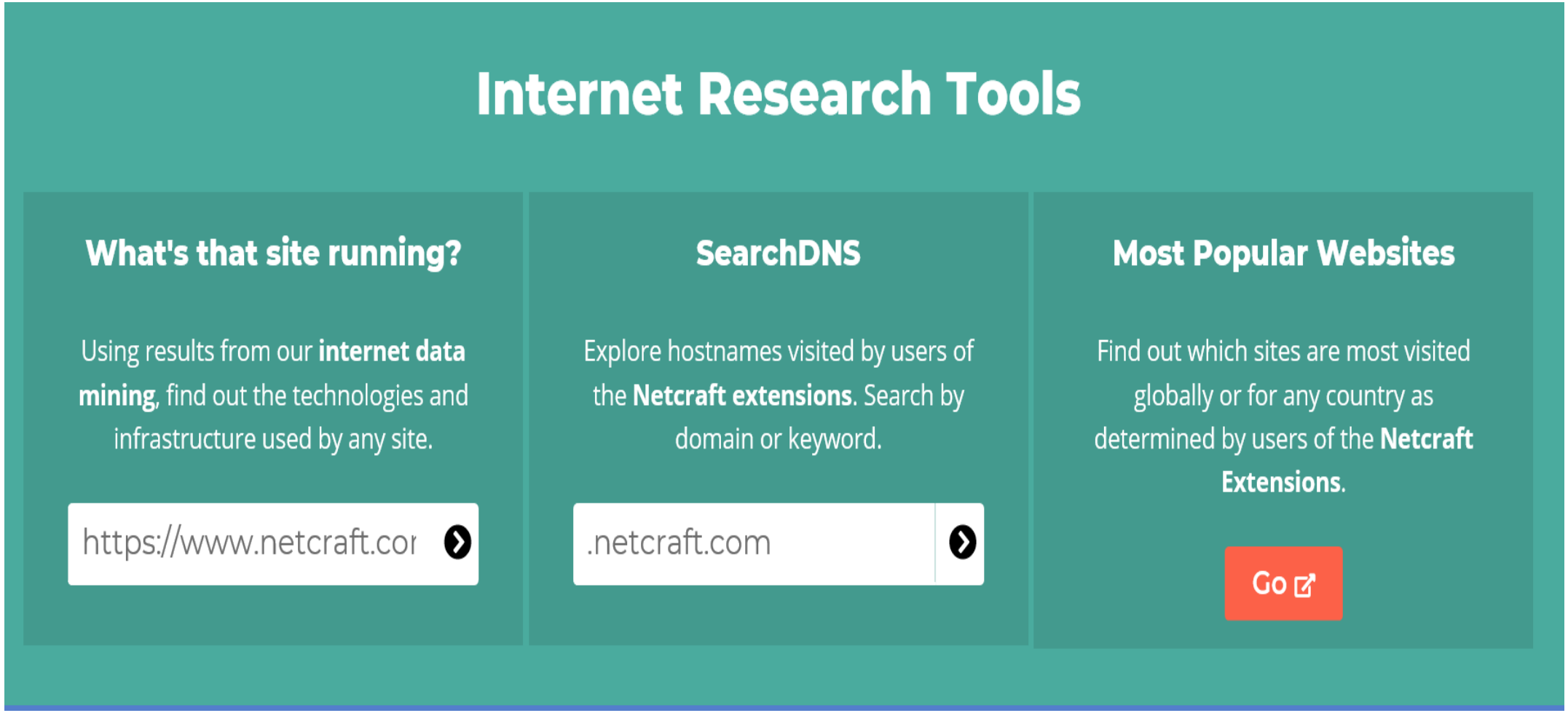
Learn More

https://www.netcraft.com/

# Netcraft

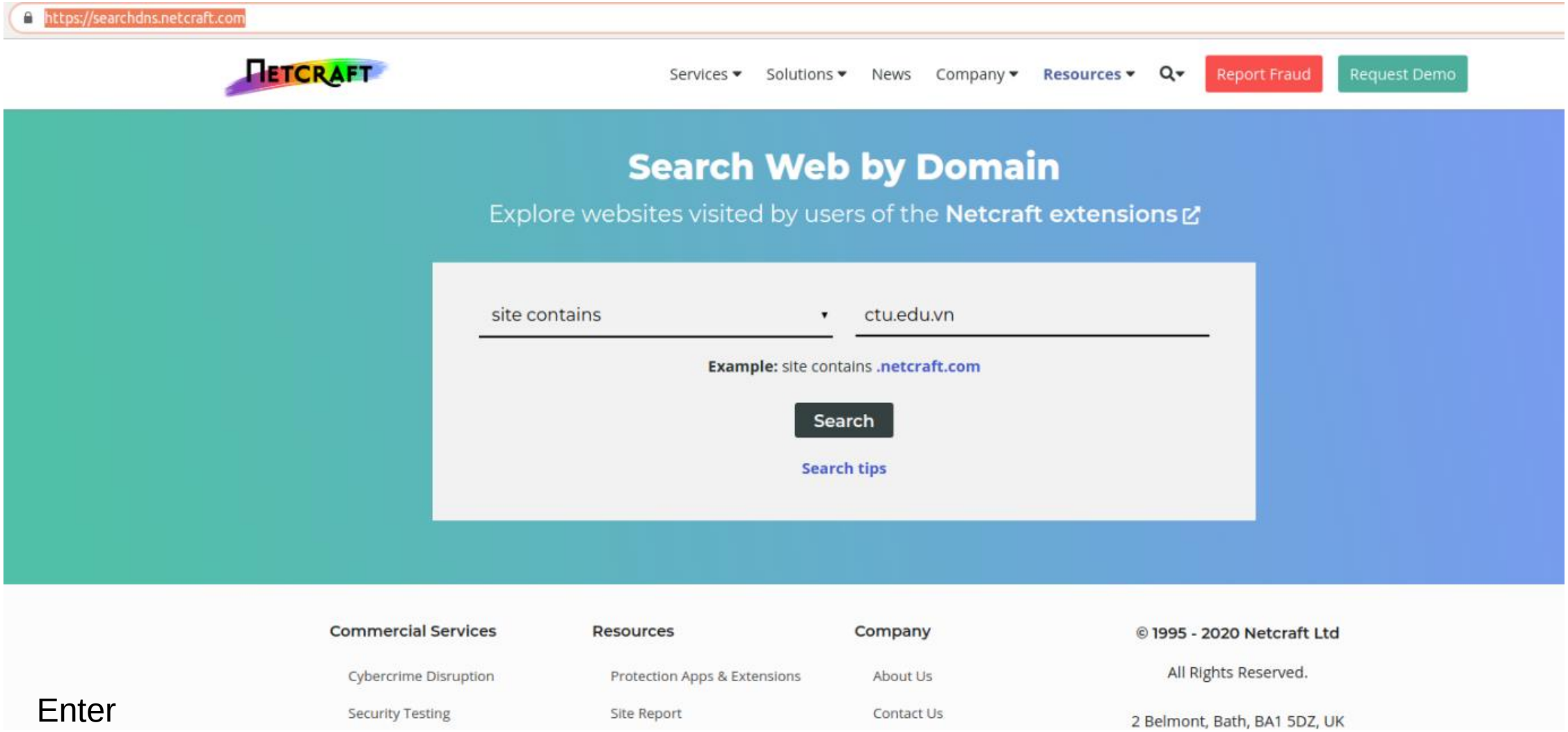

What's that site running?
Using results from our internet data mining, find out the technologies and infrastructure used by any site.
https://www.netcraft.com
Report Suspicious URLs
If you come across a suspicious site or email, please report it to us.
Report

# Netcraft



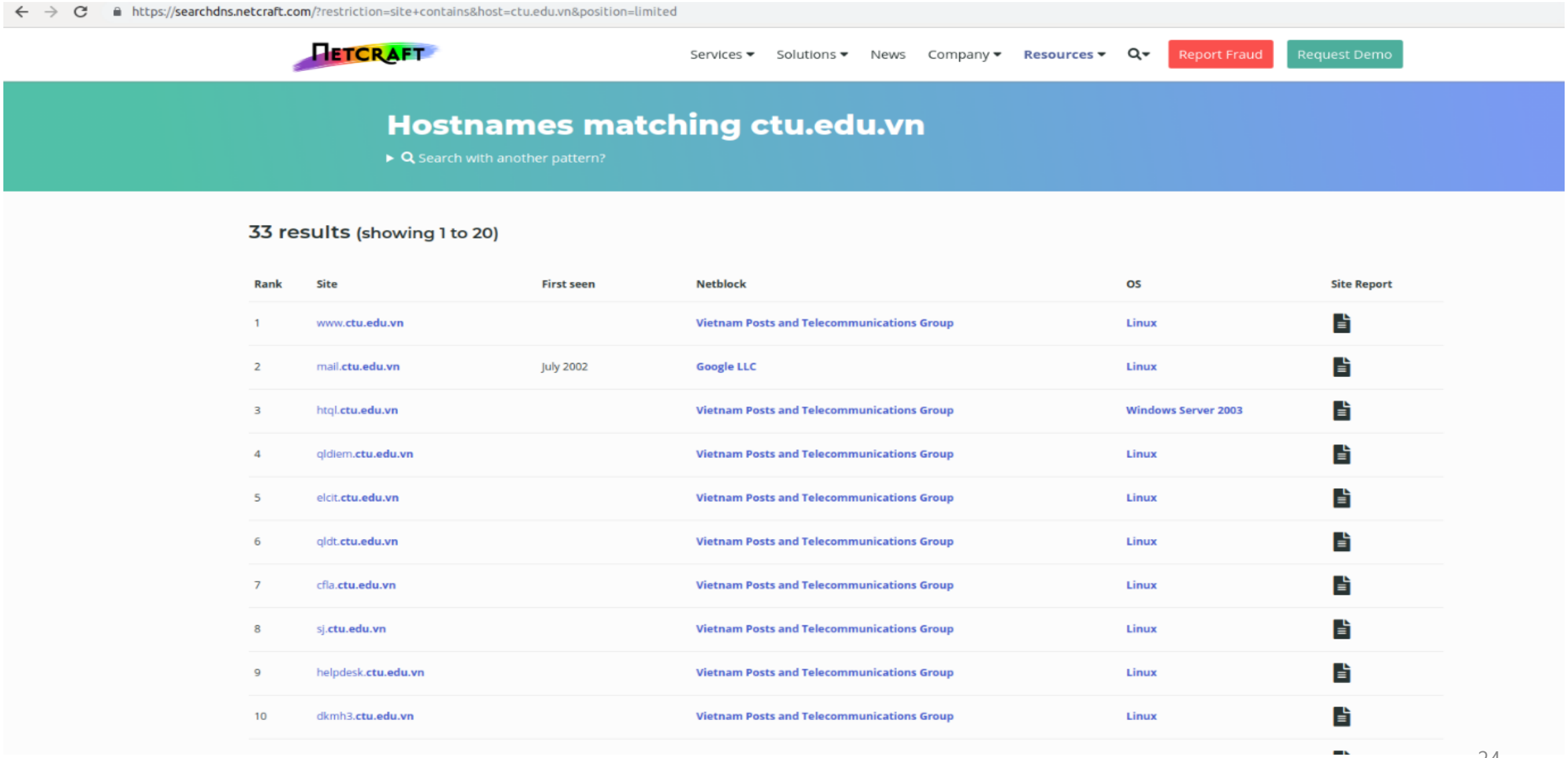

https://www.netcraft.com/

# Netcraft https://sitereport.netcraft.com/




Enter
host name, in this case is ctu.edu. vn
https://sitereport.netcraft.com/?url=https%3A%2F%2Fctu.edu.vn

# Netcraft


https://searchdns.netcraft.com/?restriction=site+contains&host=ctu.edu.vn&position=limited
NETCRAFT
Services
Solutions
News
Company
Resources
Report Fraud
Request Demo
Hostnames matching ctu.edu.vn
Search with another pattern?
33 results (showing 1 to 20)
Rank | Site | First seen | Netblock | OS | Site Report
1 | www.ctu.edu.vn | | Vietnam Posts and Telecommunications Group | Linux
2 | mail.ctu.edu.vn | July 2002 | Google LLC | Linux
3 | htql.ctu.edu.vn | | Vietnam Posts and Telecommunications Group | Windows Server 2003
4 | qldiem.ctu.edu.vn | | Vietnam Posts and Telecommunications Group | Linux
5 | elcit.ctu.edu.vn | | Vietnam Posts and Telecommunications Group | Linux
6 | qldt.ctu.edu.vn | | Vietnam Posts and Telecommunications Group | Linux
7 | cfla.ctu.edu.vn | | Vietnam Posts and Telecommunications Group | Linux
8 | sj.ctu.edu.vn | | Vietnam Posts and Telecommunications Group | Linux
9 | helpdesk.ctu.edu.vn | | Vietnam Posts and Telecommunications Group | Linux
10 | dkmh3.ctu.edu.vn | | Vietnam Posts and Telecommunications Group | Linux