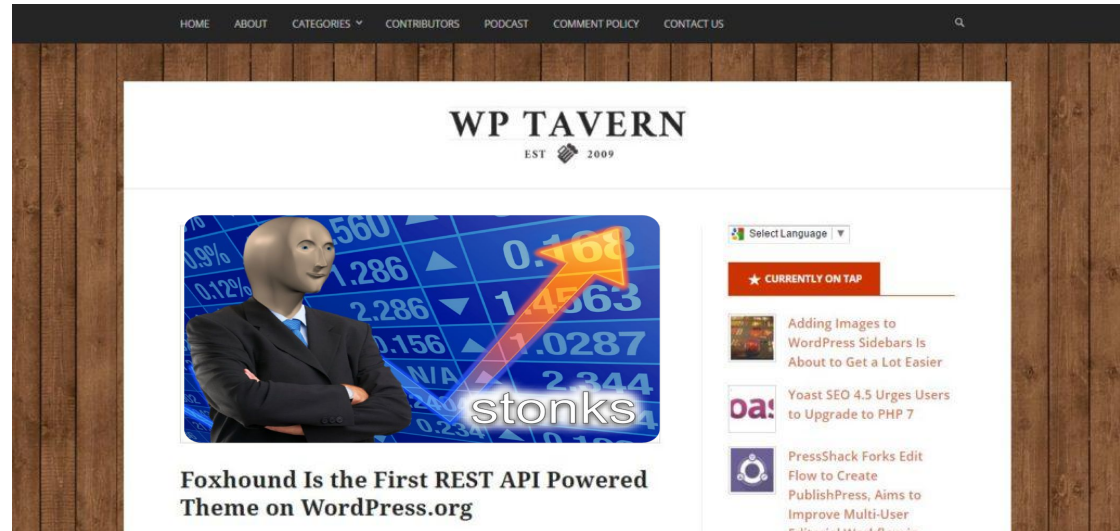




ISSS Beginner Talk Series: Networking 1

Matthew Pabst

Picture this:

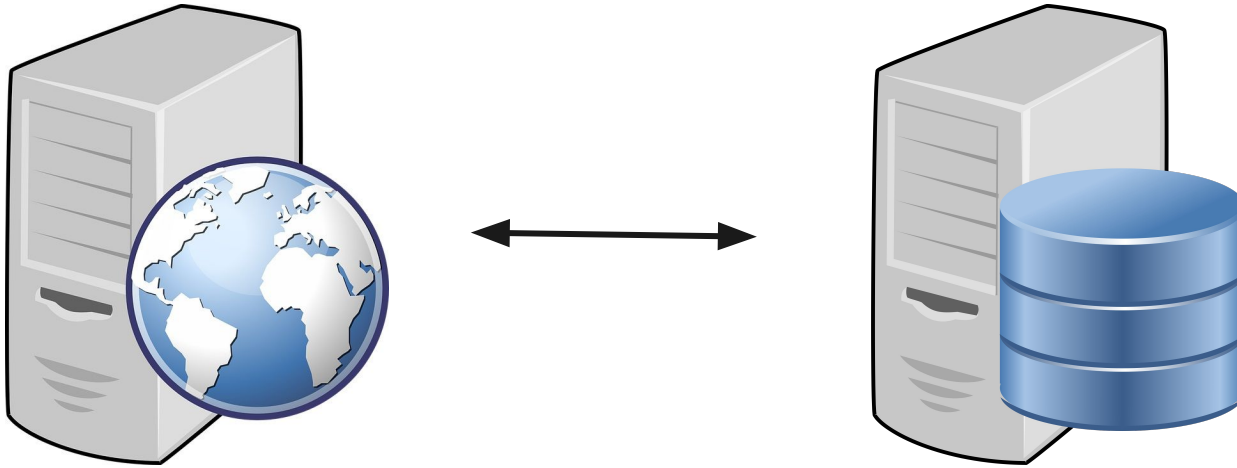




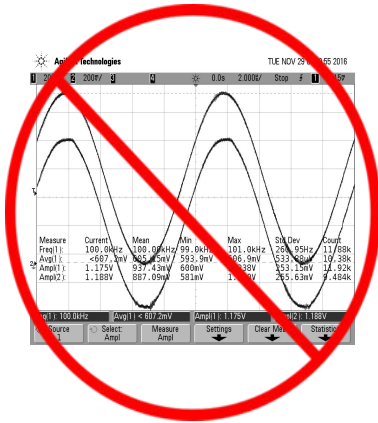
How the heck do you set this up?

- Somewhere to store the posts, comments, etc.
 - You'll need a database server- one that's not publicly accessible!
- Web server to handle requests to the site
- Domain name (bitcoinisgoingup.com), so that people can find your amazing content

How to setup the database server?



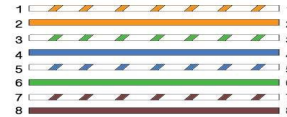
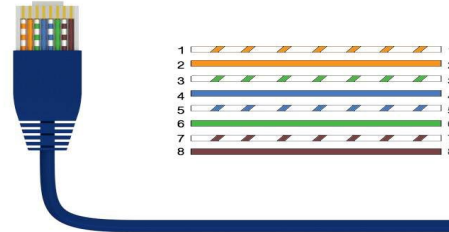
This is not an EE club, this is a CS club



Connector A



Connector B

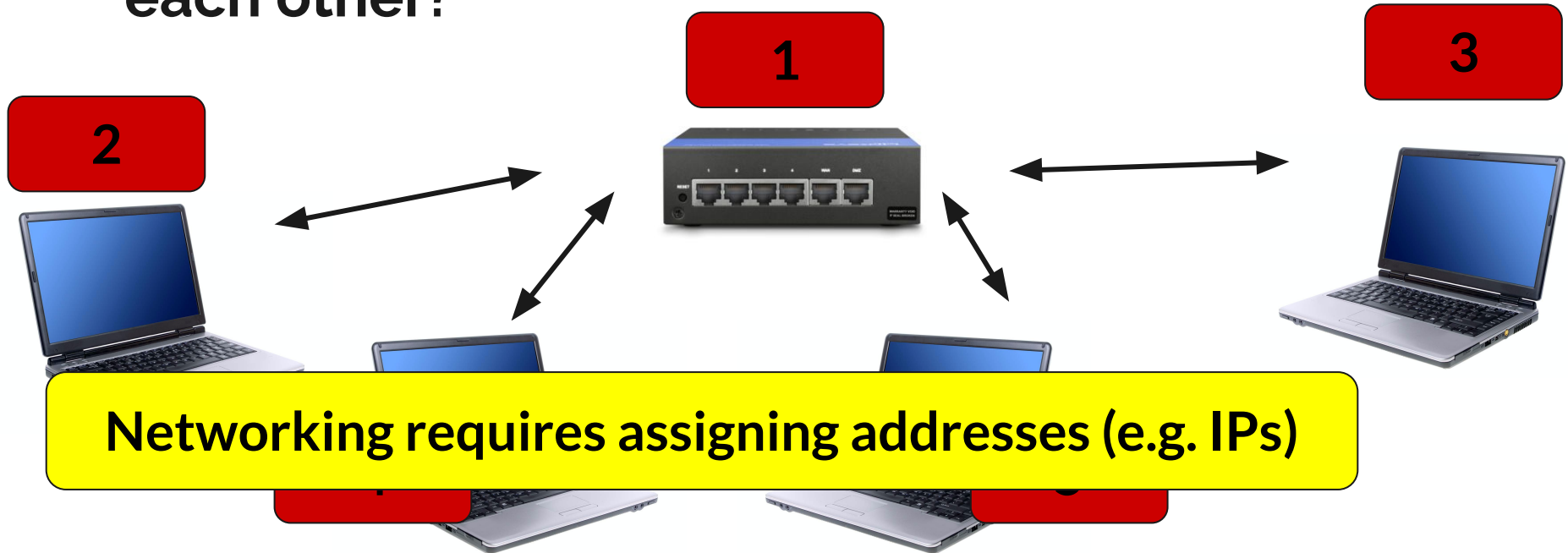


How to communicate between computers?

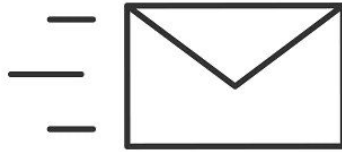


Communication requires common protocols

What if we want multiple computers to talk to each other?



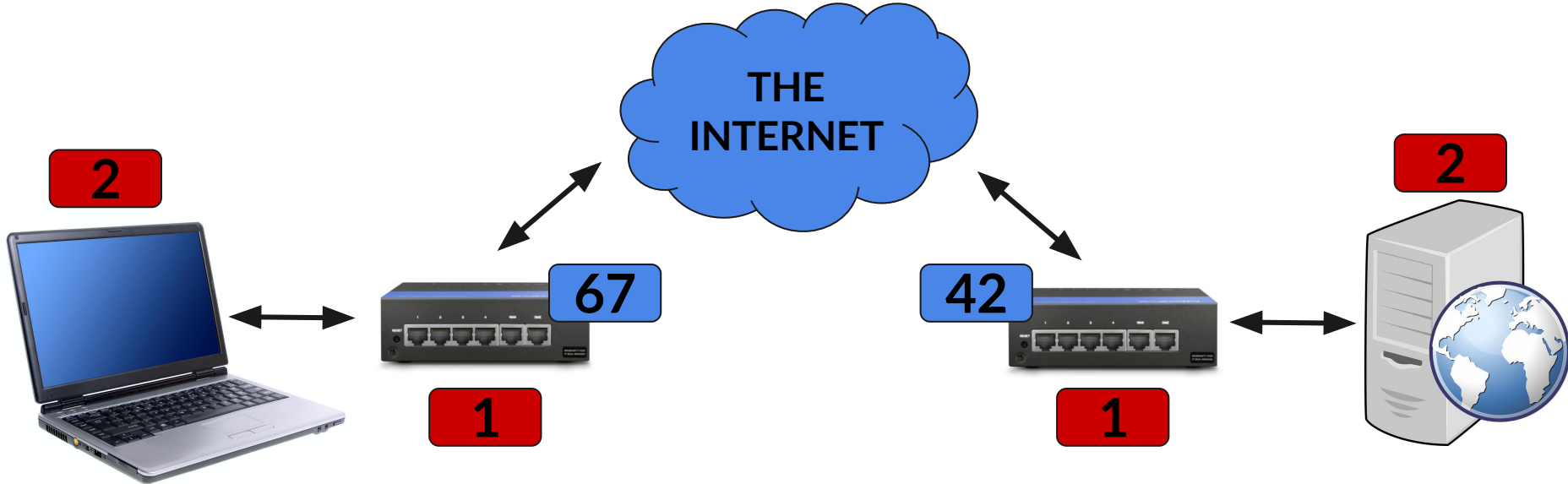
Actually talking to each other



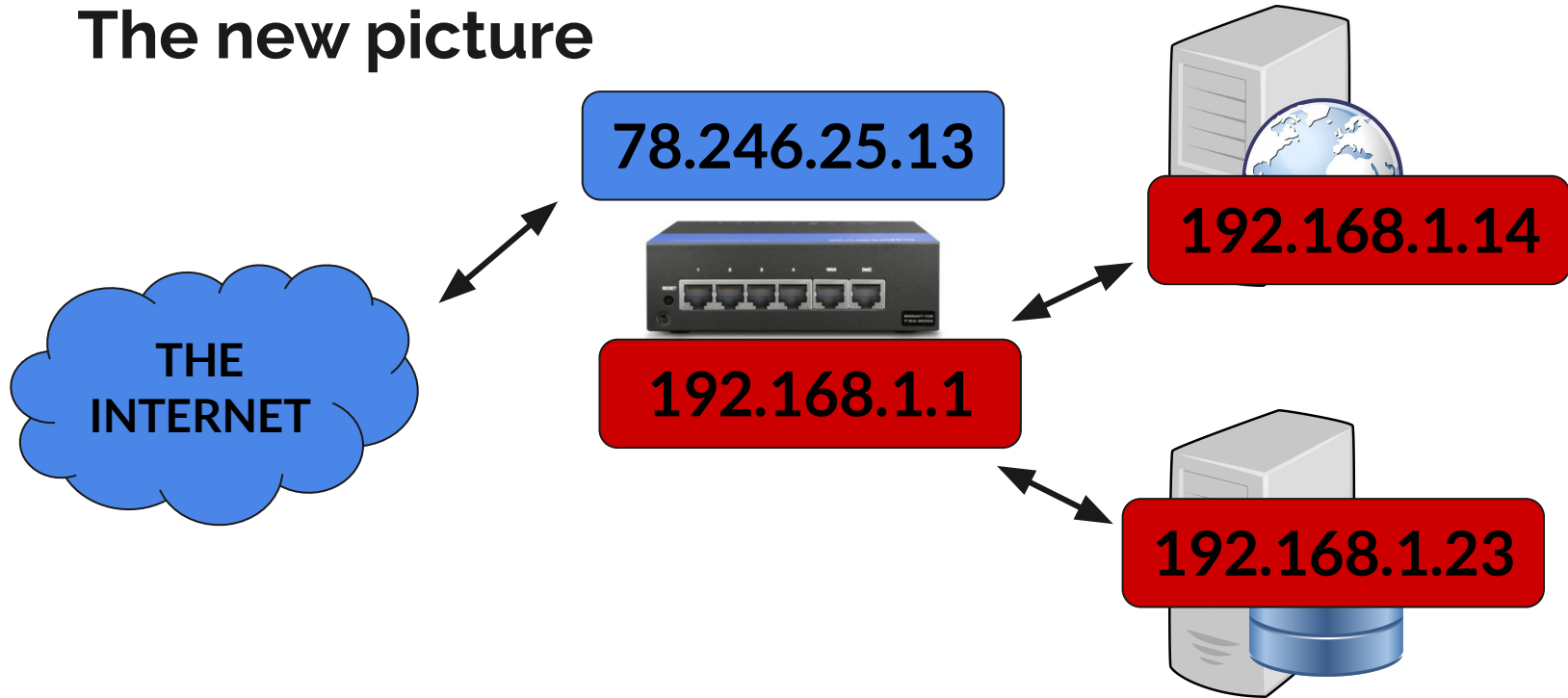
What do we need to include with our message to make sure it arrives in the right place?

The sender and receiver's addresses	→	Source and destination IP
How long the message is	→	Size field
Which message is this in the sequence	→	Sequence number
Which program should get this message	→	Port number

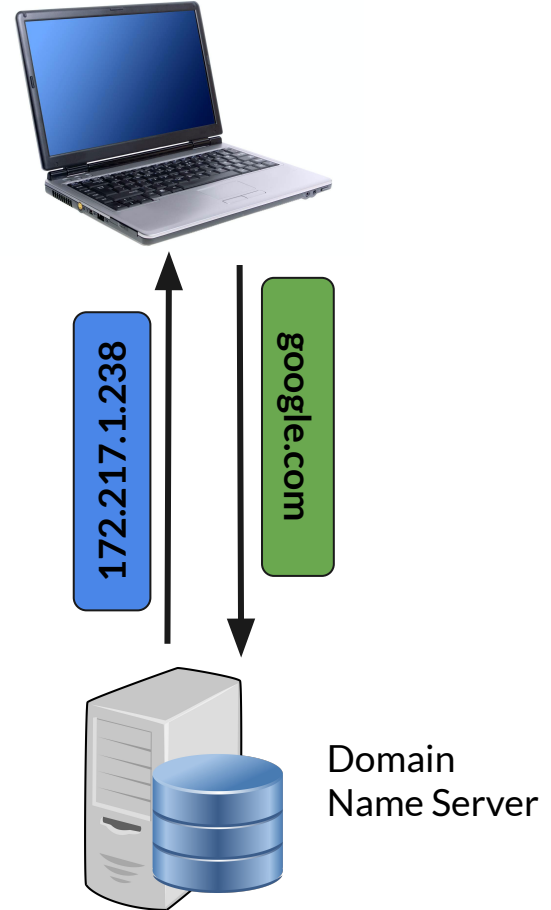
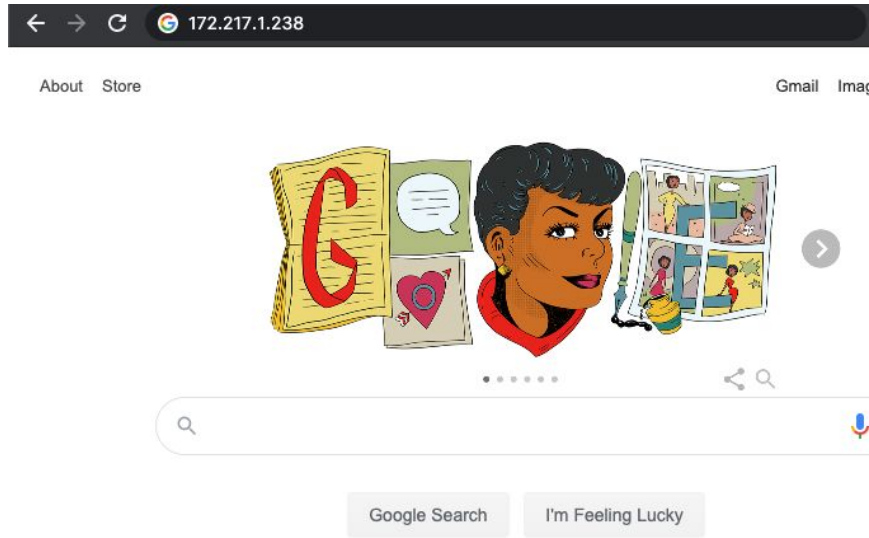
How to address the server externally?



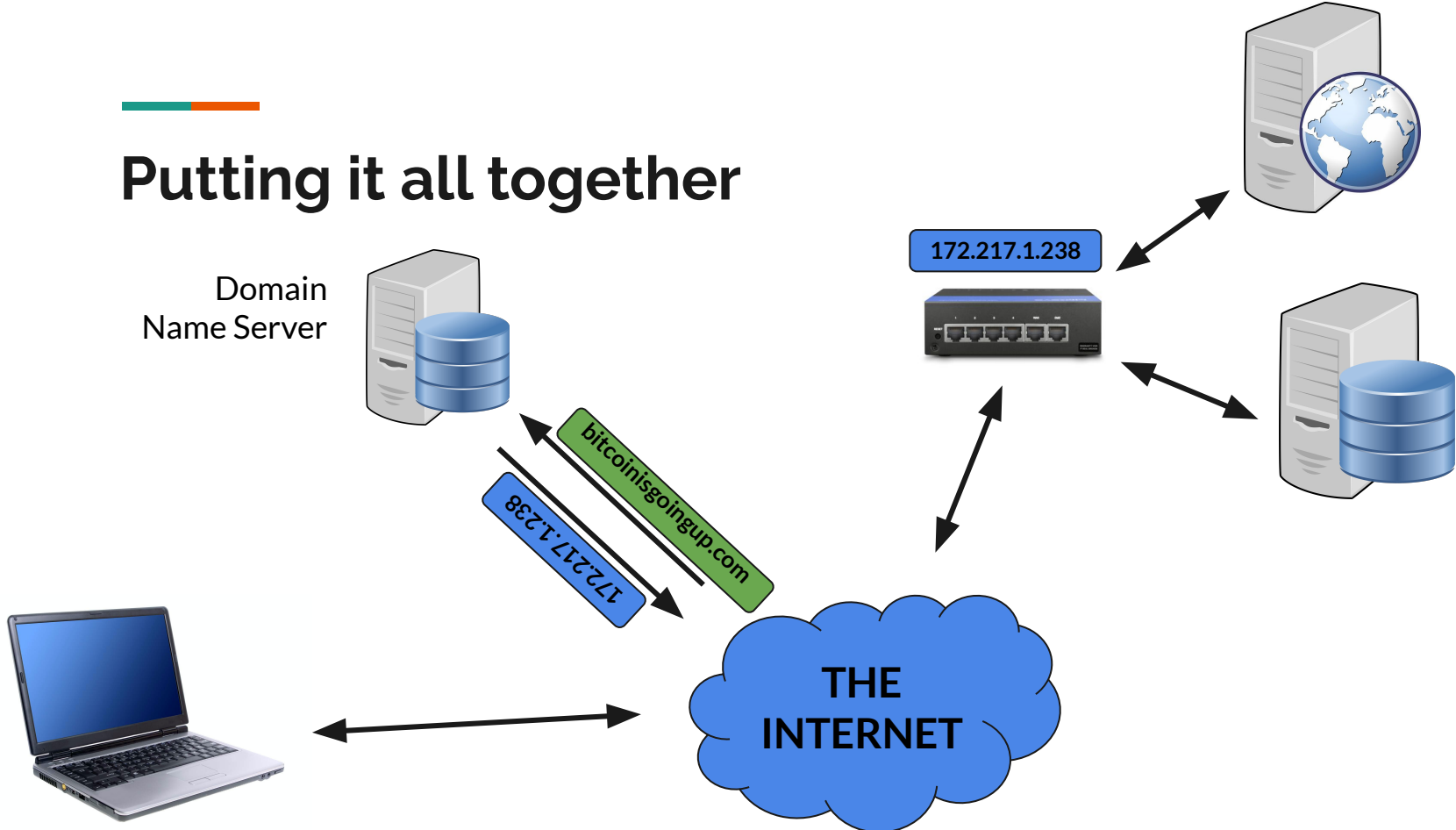
The new picture



Domain names

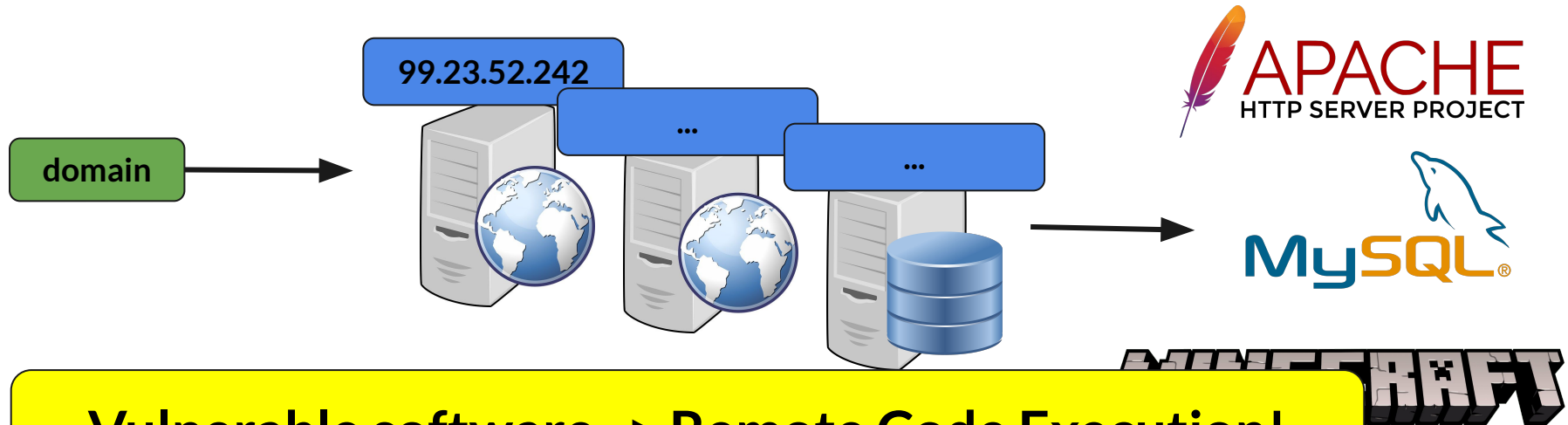


Putting it all together



Attacking Networks

What's the goal?



Vulnerable software -> Remote Code Execution!

Finding an organization's public servers


The screenshot shows a web browser window with the address bar displaying `utexas.edu`, which is highlighted with a red box. Below the address bar, there is a notification banner about COVID-19 updates. The main content area shows the University of Texas at Austin logo and a large image of a building with the text "WHAT STARTS HERE" overlaid. The browser's developer tools are open, showing the Network tab. The list of requests includes `www.utexas.edu`, which is selected. The details for this request show a status code of 200 and a remote address of `104.22.2.59:443`, which is also highlighted with a red box.

```
matthew@streetpizza:~$ nslookup www.utexas.edu
Server:           192.168.1.254
Address:          192.168.1.254#53

Non-authoritative answer:
www.utexas.edu canonical name = www.utexas.edu
Name:   www.utexas.edu.cdn.cloudflare.net
Address: 104.22.2.59
```

The WHOIS system:

Domain -> Contact info



Tools API Research Data

[ViewDNS.info](#) > [Tools](#) > **Domain / IP Whois**

Displays owner/contact information for a domain name or IP address

Need to lookup a large number of domains? Enquire about our [bulk v](#)

Domain / IP Address:

<https://viewdns.info/whois/>

Domain Name: UTEXAS.EDU

Registrant:

University of Texas at Austin
Office of Telecommunication Services
PO Box 7580
Austin, TX 78713-7580
US

Administrative Contact:

William Green
The University of Texas at Austin
ITS - Networking and Telecommunications
1 University Station Stop C3800
Austin, TX 78713-7580
US

+1.5124716387
net-admin@its.utexas.edu

Technical Contact:

Technical Contact
The University of Texas at Austin
ITS - Networking and Telecommunications
1 University Station Stop C3800
Austin, TX 78713-7580
US
+1.5124716387
net-tech@its.utexas.edu

Name Servers:

MARIANAS.ITS.UTEXAS.EDU
GLASS.ITS.UTEXAS.EDU
DNS1.ILLINOIS.EDU
DNS2.ILLINOIS.EDU
CHISOS.OTS.UTEXAS.EDU

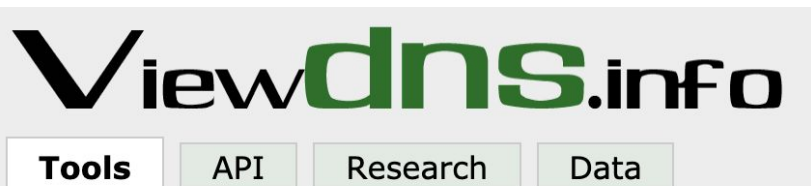
Domain record activated: 13-Aug-1985

Domain record last updated: 02-Jul-2020

Domain expires: 31-Jul-2023

The WHOIS system:

Contact info -> domains



[ViewDNS.info](#) > [Tools](#) > **Reverse Whois Lookup**

This free tool will allow you to find domain names owned by ar or company to find other domains registered using those same

Registrant Name or Email Address:

<https://viewdns.info/reversewhois/>

Reverse Whois results for net-admin@its.utexas.edu

=====

There are 151 domains that matched this search query.
These are listed below:

Domain Name
92longhornboys.com
bevo-enterprises.com
bevo.university
bevobeat.com
bevoenterprises.com
bevolaraza.org
bevolinks.com
bevosbookstore.com
bevoshop.com
bevoslandscaping.com
bevostrong.com
campuscomputerstore.net
campuscomputerstore.org
elonghorns.com
frankerwin.com
frankerwincenter.org
frankirwincenter.com
hirealonghorn.com
hook-em-horns.com
hook-em-horns.net
hook-emhorns.biz
hookem-horns.biz

Autonomous Systems:

Company name -> ASNs

ASN Lookup & Information

The ASN Information tool provides complete autonomous system (AS) information

Autonomous Systems are routable networks within the public Internet, administered by owners of networks. The ASN Information tool displays information about an IP (ASN) such as: IP owner, registration date, issuing registrar and the max range of

Enter an AS number, IP address, or a Company name.

<https://www.ultratools.com/tools/asnInfoResult>



AS20162

Country: US
Registration Date: 2001-04-02
Registrar: arin
Owner: UTDALLAS, US

AS26971

Country: US
Registration Date: 2003-01-03
Registrar: arin
Owner: UTHSCSA-AS, US

AS18515

Country: US
Registration Date: 2000-09-07
Registrar: arin
Owner: UTARLINGTON, US

AS11773

Country: US
Registration Date: 1998-12-15

Autonomous Systems: ASNs -> IPs

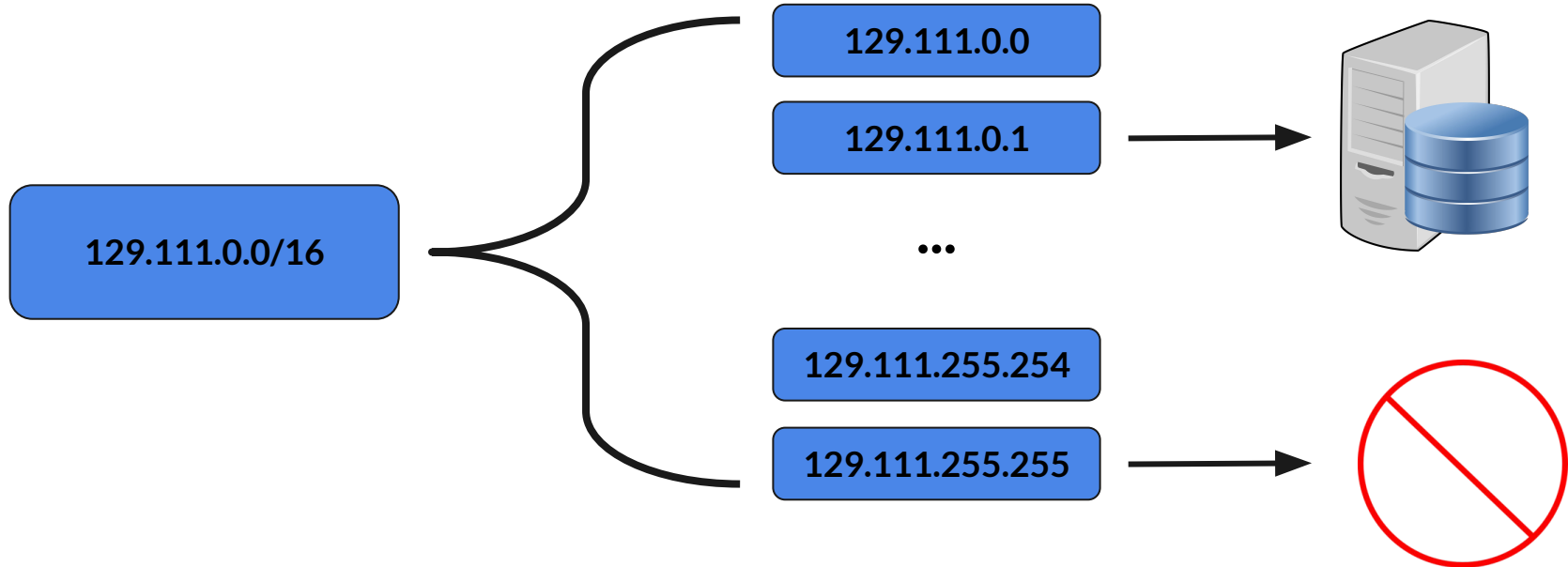
📍 AS26971 🔍

<https://ipinfo.io>

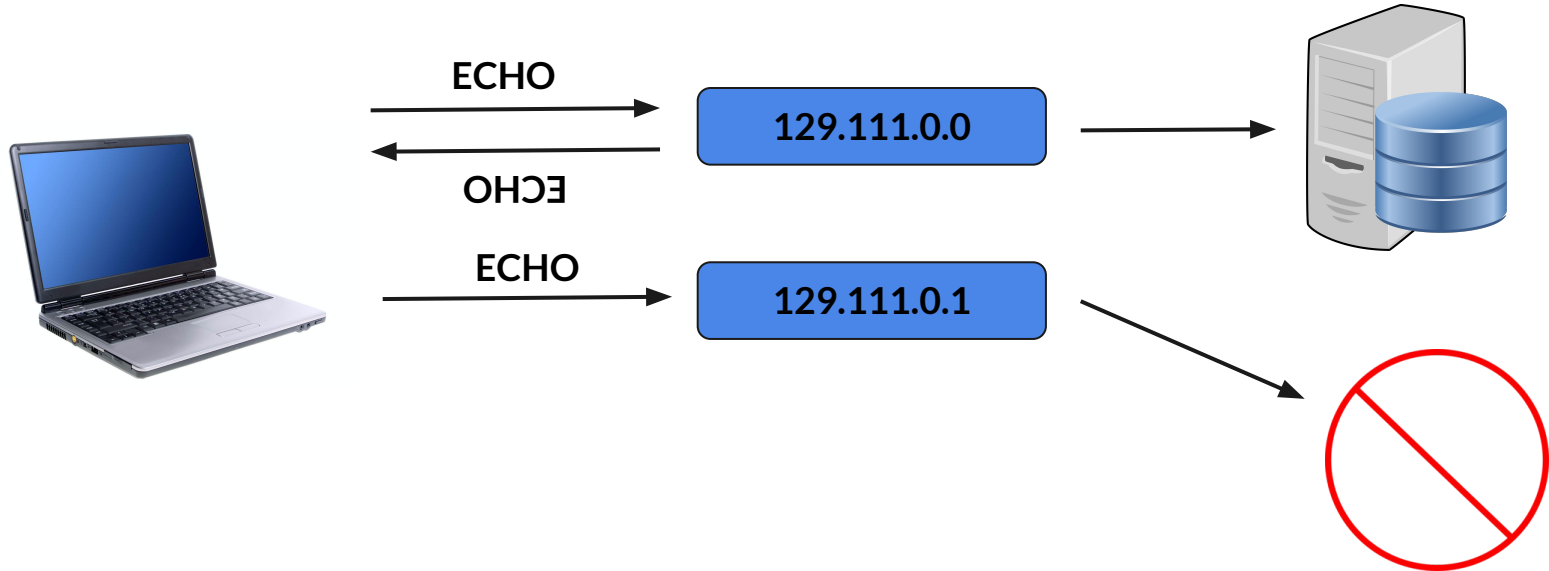
WHOIS/AS -> Find organization's IP addresses

```
“ asn: "AS26971"
“ name: "University of Texas"
“ country: "US"
“ allocated: "2003-01-03"
“ registry: "arin"
“ domain: "uthscsa.edu"
# num_ips: 65536
“ type: "education"
[a] prefixes: Array
  {} 0: Object
    “ netblock: "129.111.0.0/16"
    “ id: "UTHSCSA"
    “ status: "ASSIGNMENT"
```

IP Blocks (Subnets)



Host Discovery



WARNING!

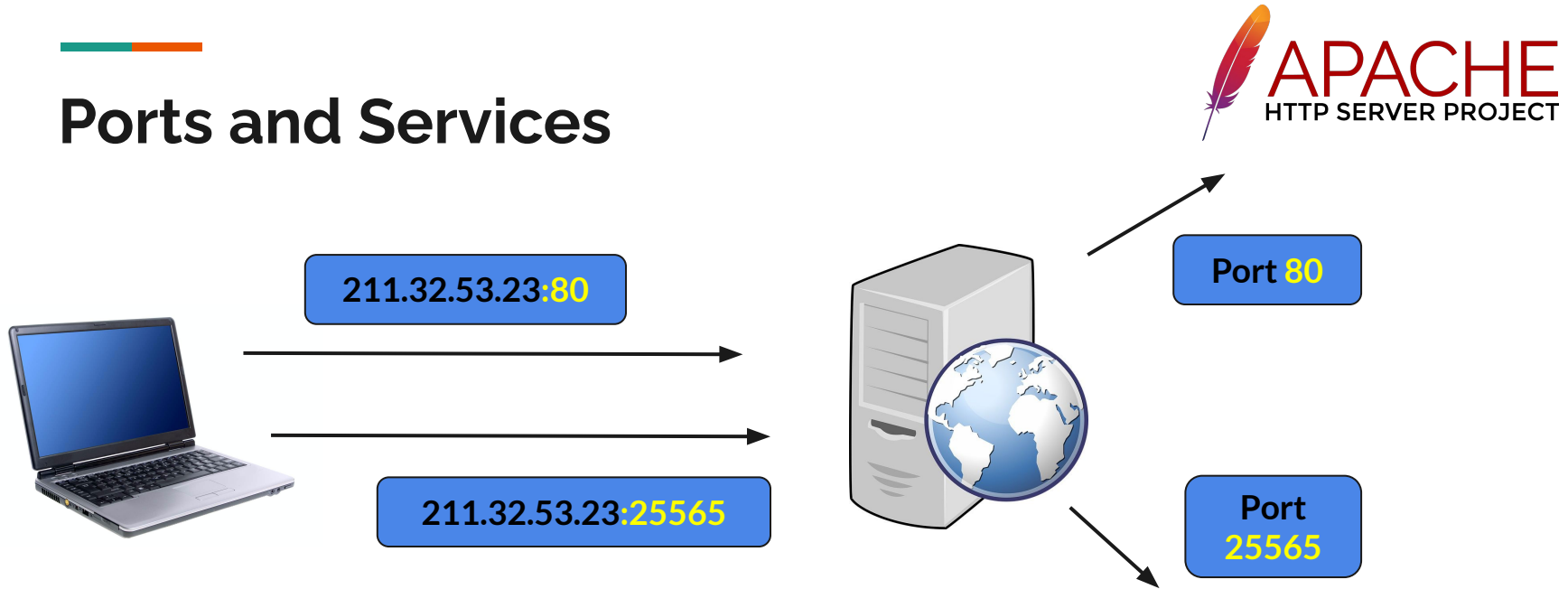
The techniques discussed after this point are very illegal!

Port scanning and/or service exploitation have led to felony sentences of many years in prison.

Only use these techniques in personal or educational settings in which you have express consent of the owner of the machines being attacked.



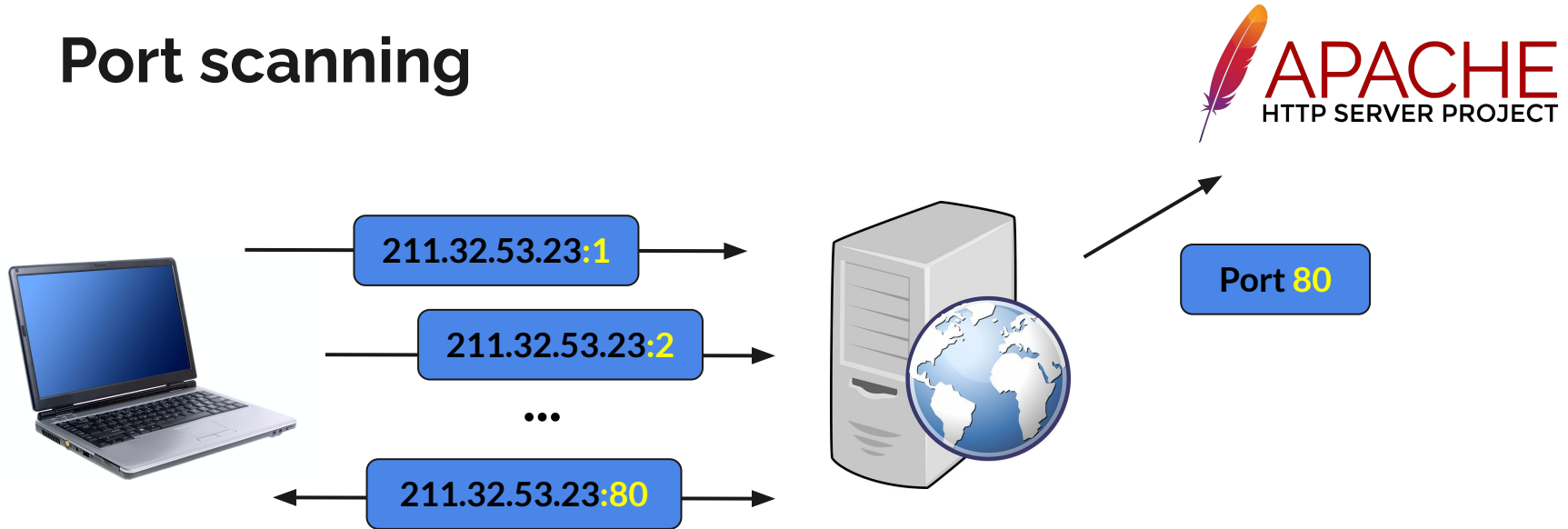
Ports and Services



Port # determines which service gets a message



Port scanning



Scanning ports -> identifying services



Exploiting services



Windows
File Share

211.32.53.23:445





Exploiting services



EternalBlue exploit



Remote Code Execution



Exploiting services

WannaCry
Ransomware Attack



About 200,000 computers
impacted!

Estimated \$4 billion
extorted!

Thanks!

Feel free to hang out and ask questions.

Event info goes here.

