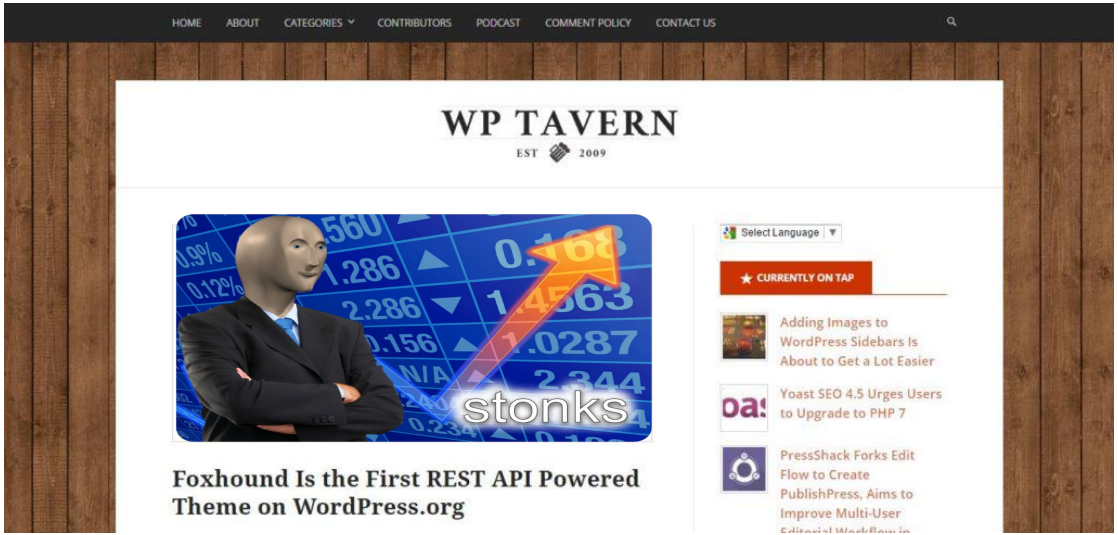
ISSS Beginner Talk Series: Networking 1

Matthew Pabst

If you want to follow along...

- Connect to “utexas” wifi
- Open a shell on your computer
  - SSH into a UTCS lab machine
  - On Linux/Mac, open “Terminal”
  - On Windows, open “Command Prompt” (cmd)

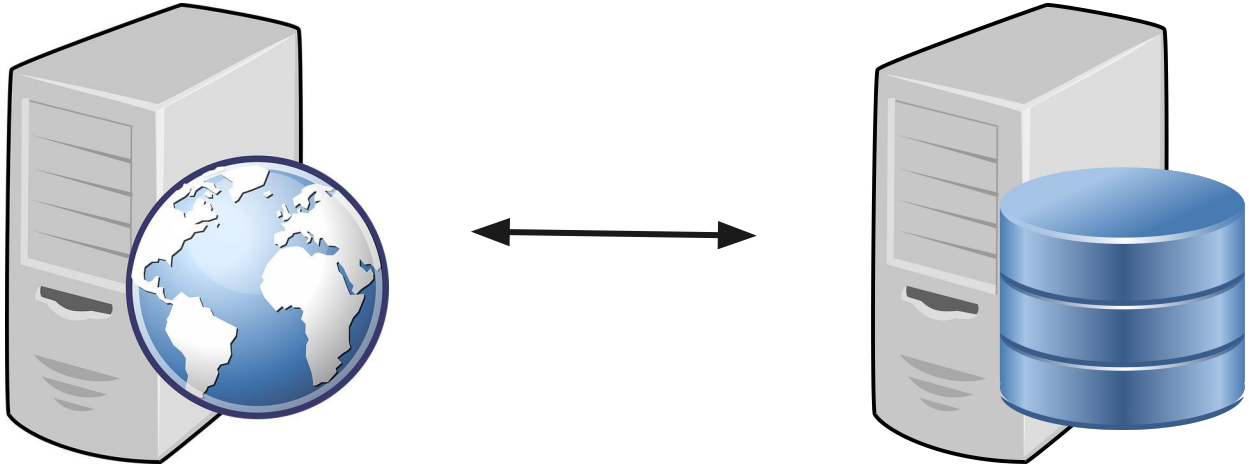
Picture this:



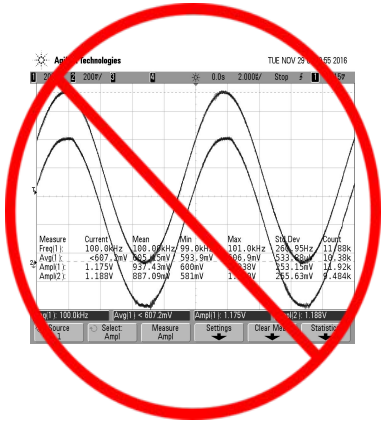
How the heck do you set this up?

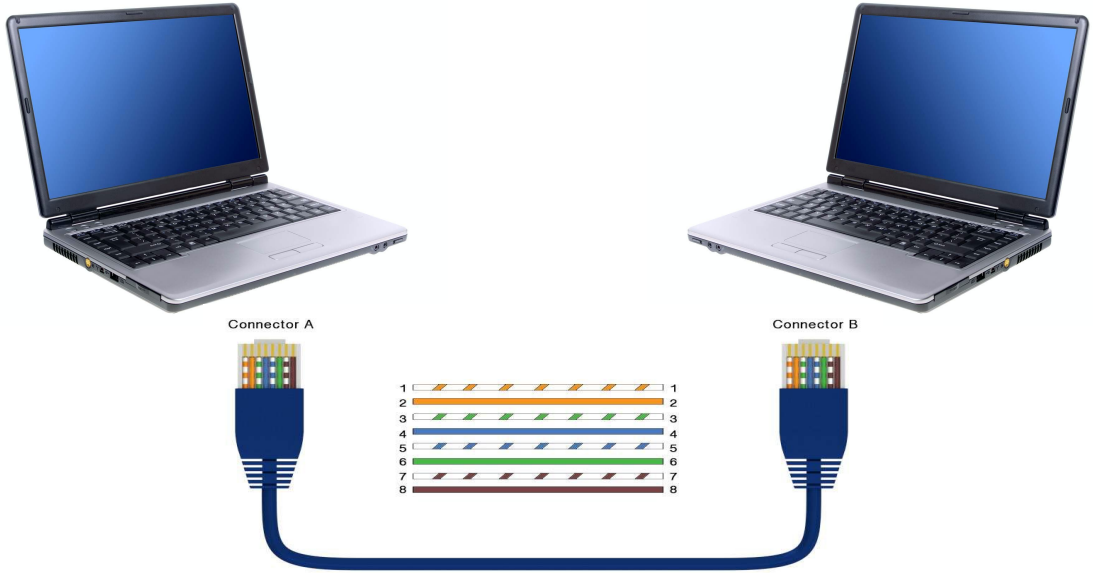
- Somewhere to store the posts, comments, etc.
  - You'll need a database server- one that's not publicly accessible!
- Web server to handle requests to the site
- Domain name (bitcoinisgoingup.com), so that people can find your amazing content

How to setup the database server?



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

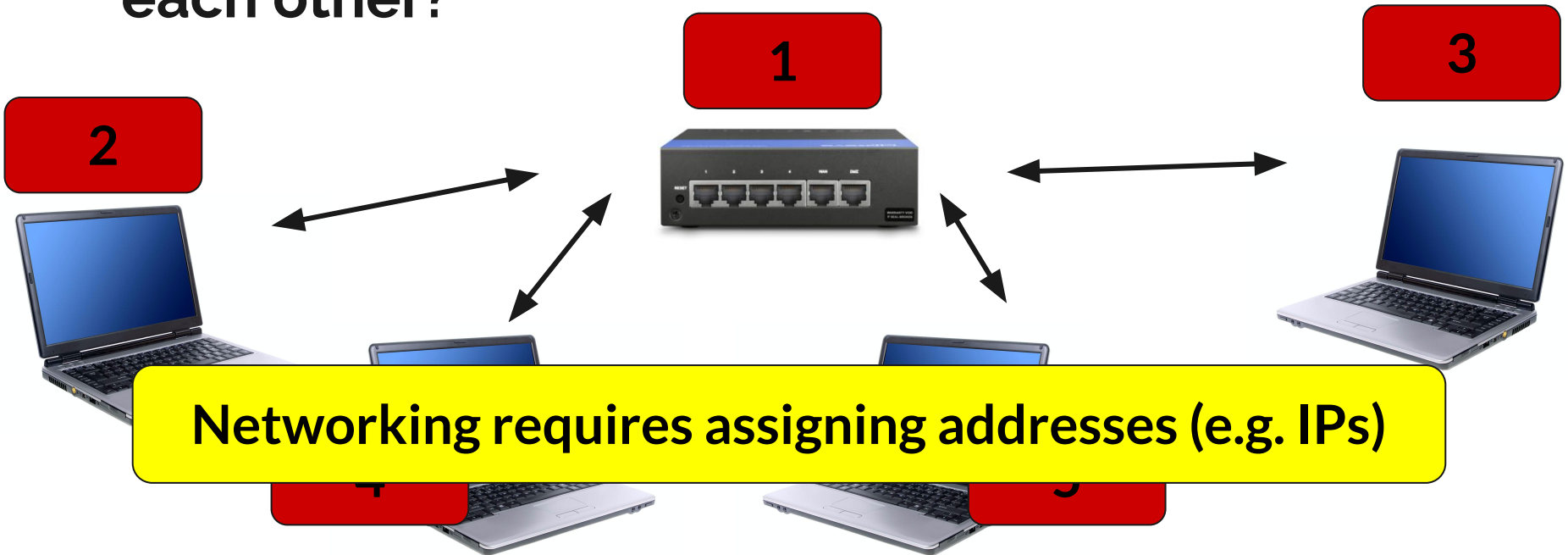




How to communicate between computers?

Communication requires common protocols

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



Networking requires assigning addresses (e.g. IPs)

Actually talking to each other

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

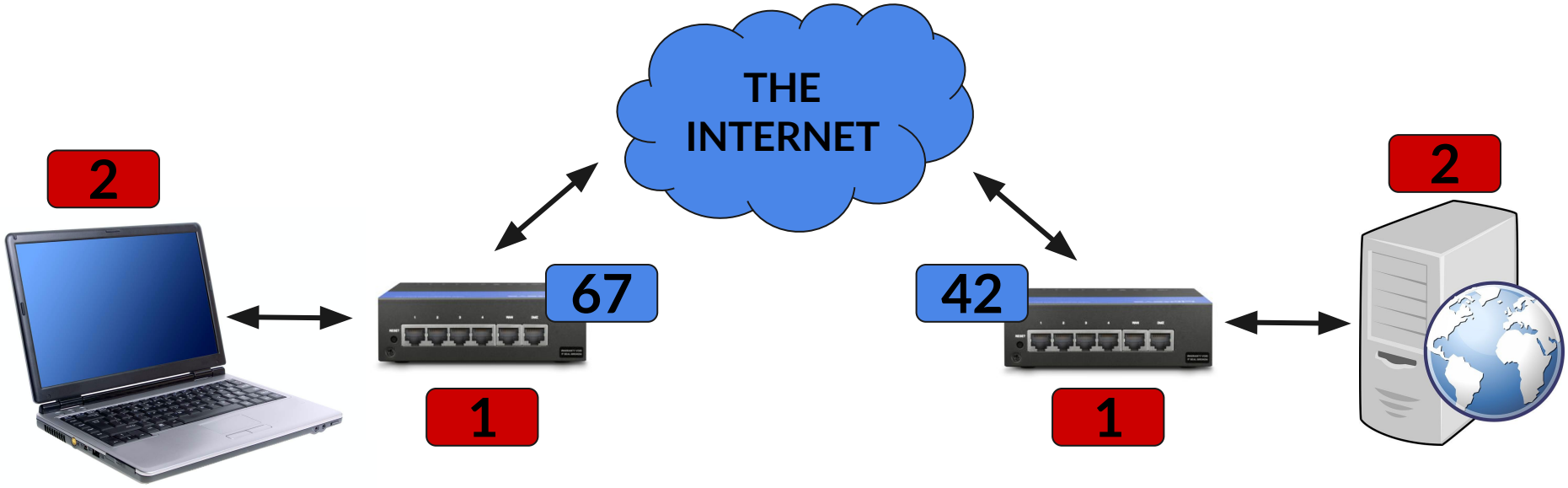
The sender and receiver's addresses → Source and destination IP

How long the message is → Size field

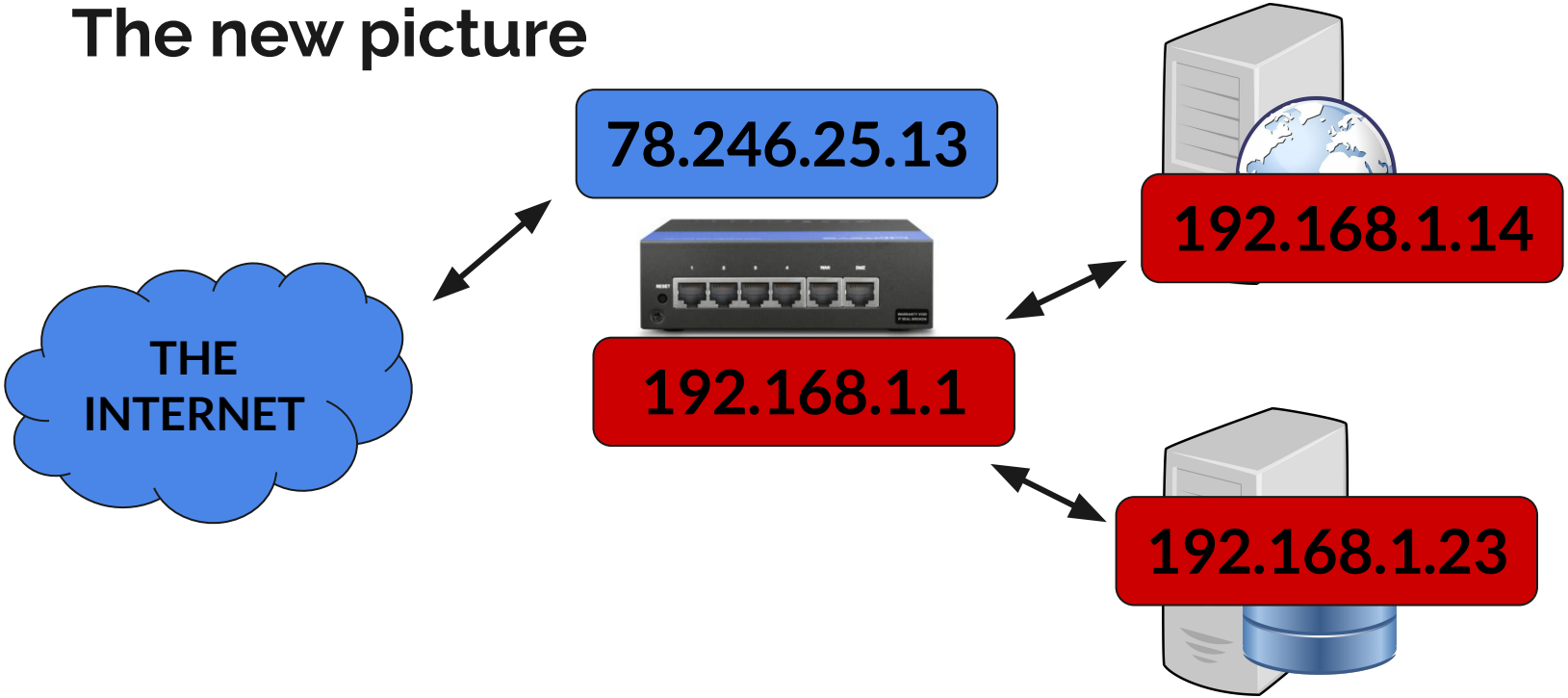
Which message is this in the sequence → Sequence number

Which program should get this message → Port number

How to address the server externally?



The new picture



Find your local IP address

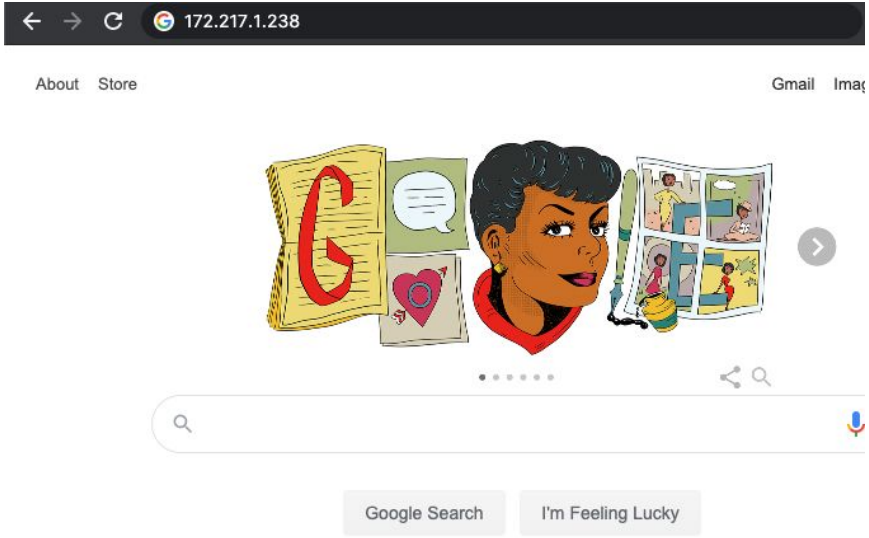
Mac: `ifconfig`

Most Linux distributions: `ip a`

Windows (cmd): `ipconfig`

Raise your hand when you’ve found your local IP to get a Starburst!

Domain names



172.217.1.238

google.com

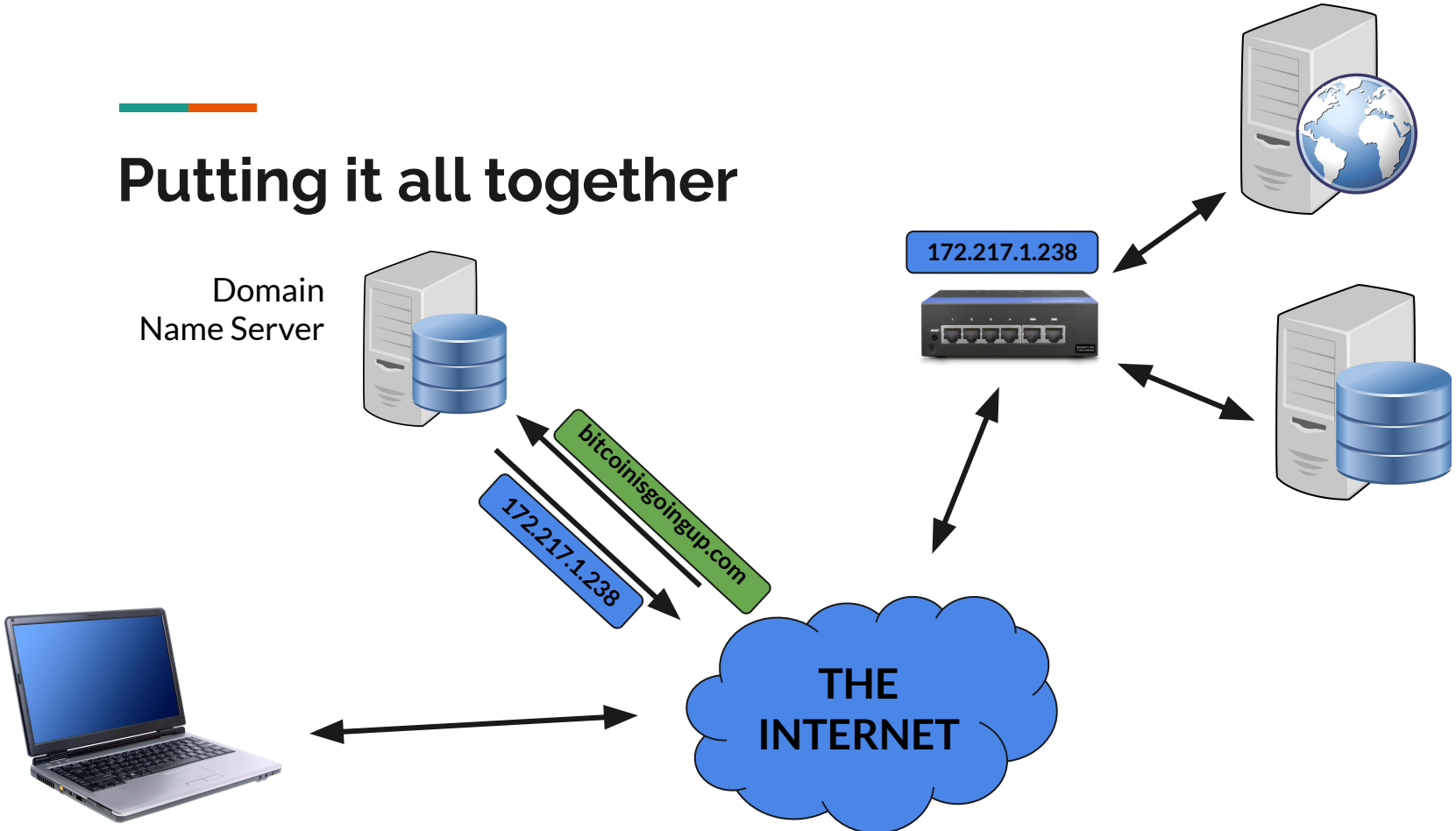
Domain
Name Server

Lookup up the IP for a domain

Mac/Linux/Windows: `nslookup domain.com`

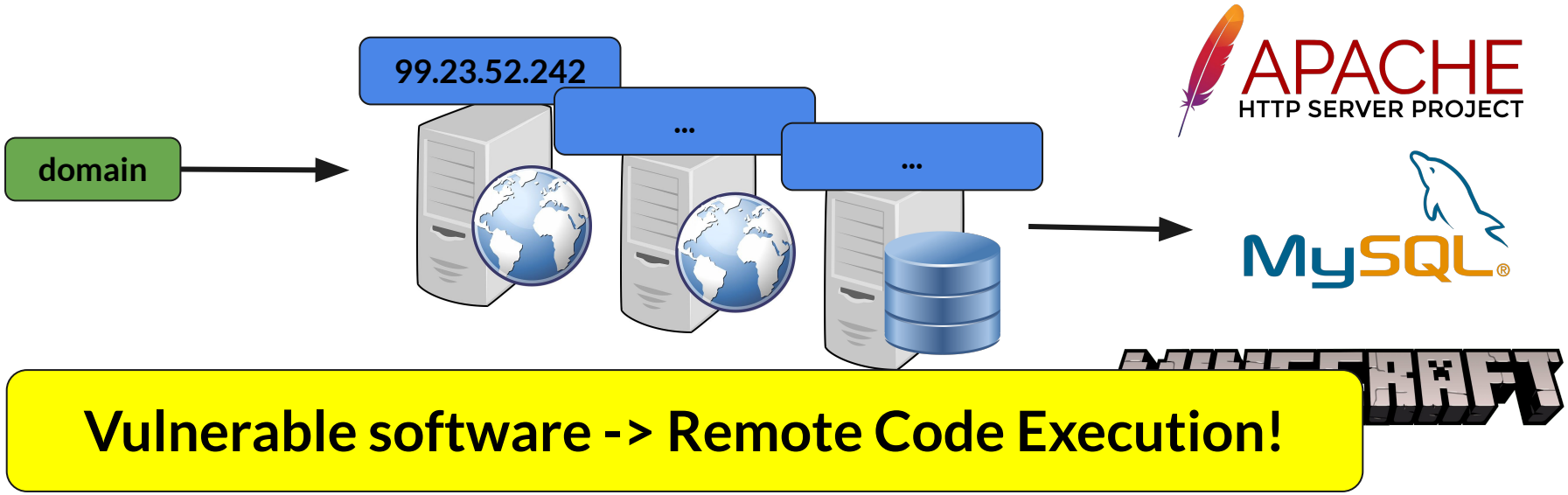
First person to find an IP address for *spotify.com* gets a Starburst!

Putting it all together



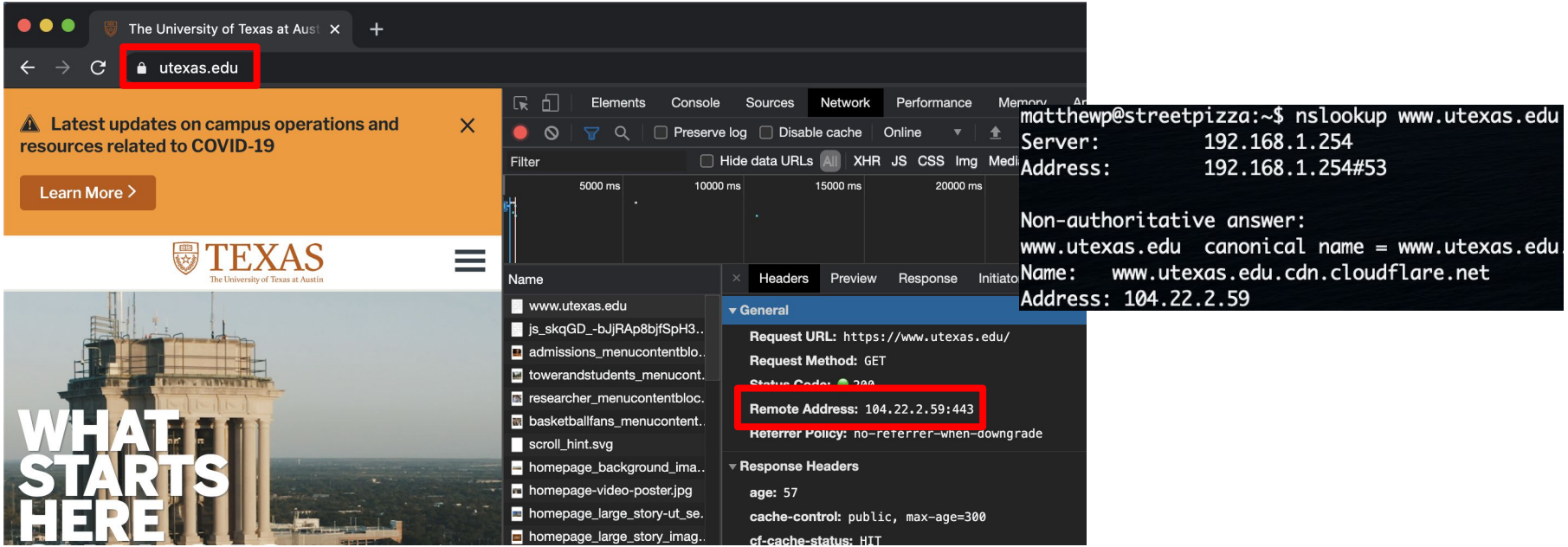
Attacking Networks

What's the goal?

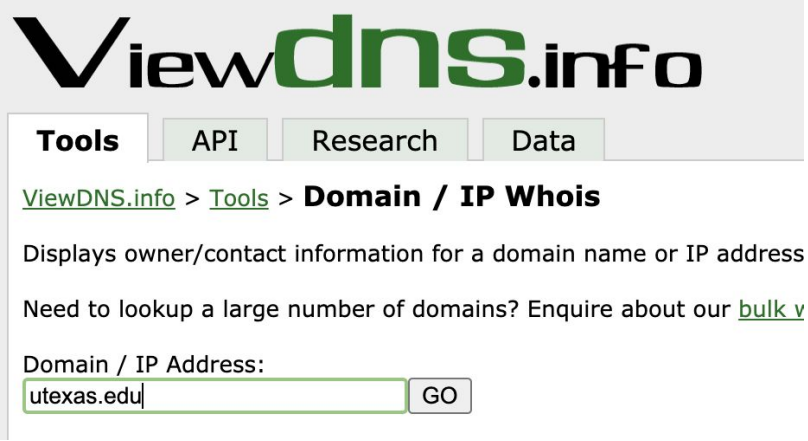


Vulnerable software -> Remote Code Execution!

Finding an organization's public servers



The WHOIS system:
Domain -> Contact info



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

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

https://viewdns.info/reversewhois/

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, administ
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.

university of texas | Go »

https://hackertarget.com/as-ip-lookup/

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
```

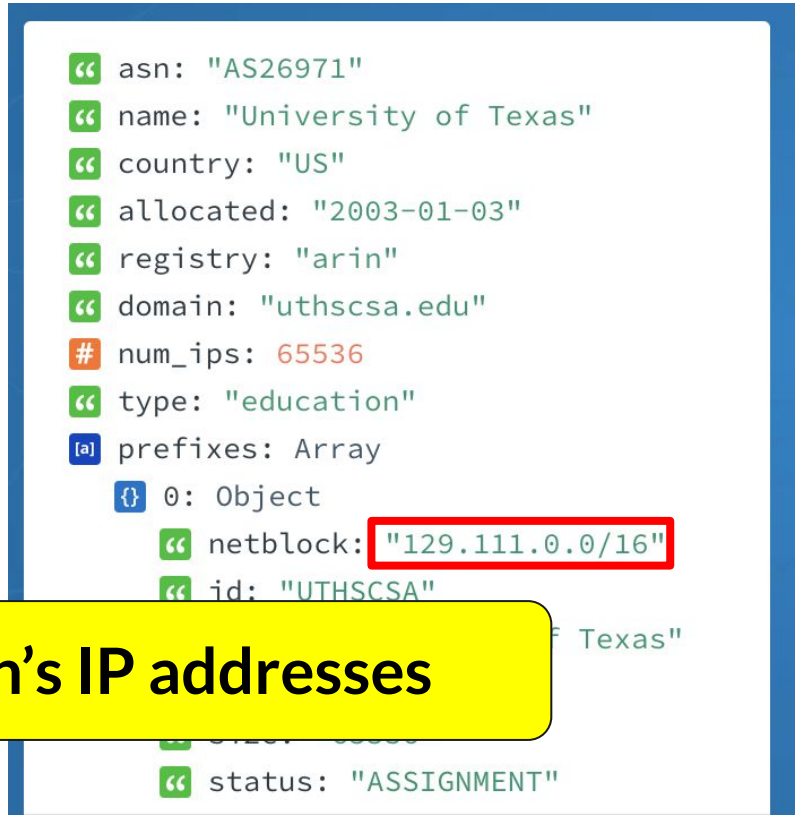
AS18515

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

AS11773

```
        Country: US
Registration Date: 1998-12-15
```

Autonomous Systems:
ASNs -> IPs



https://ipinfo.io

WHOIS/AS -> Find organization's IP addresses

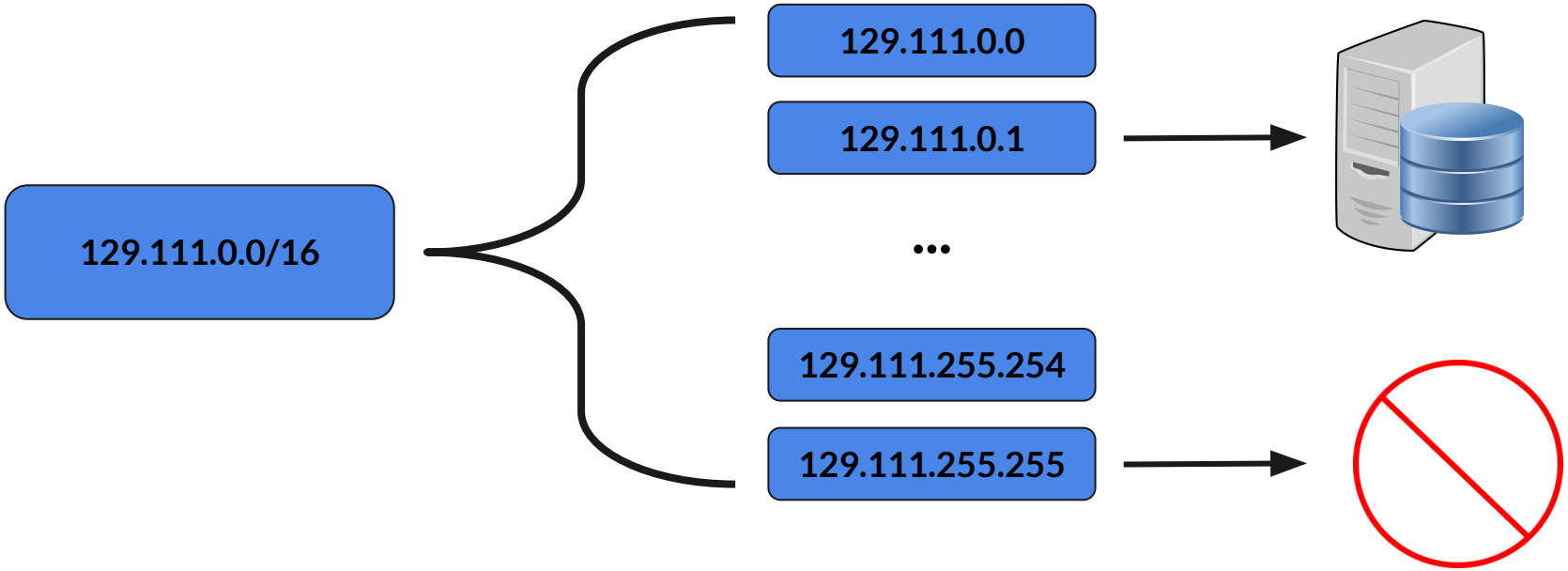
IP -> ASN

Find out the number of IPs belonging to the ASN that the “utexas” network belongs to.

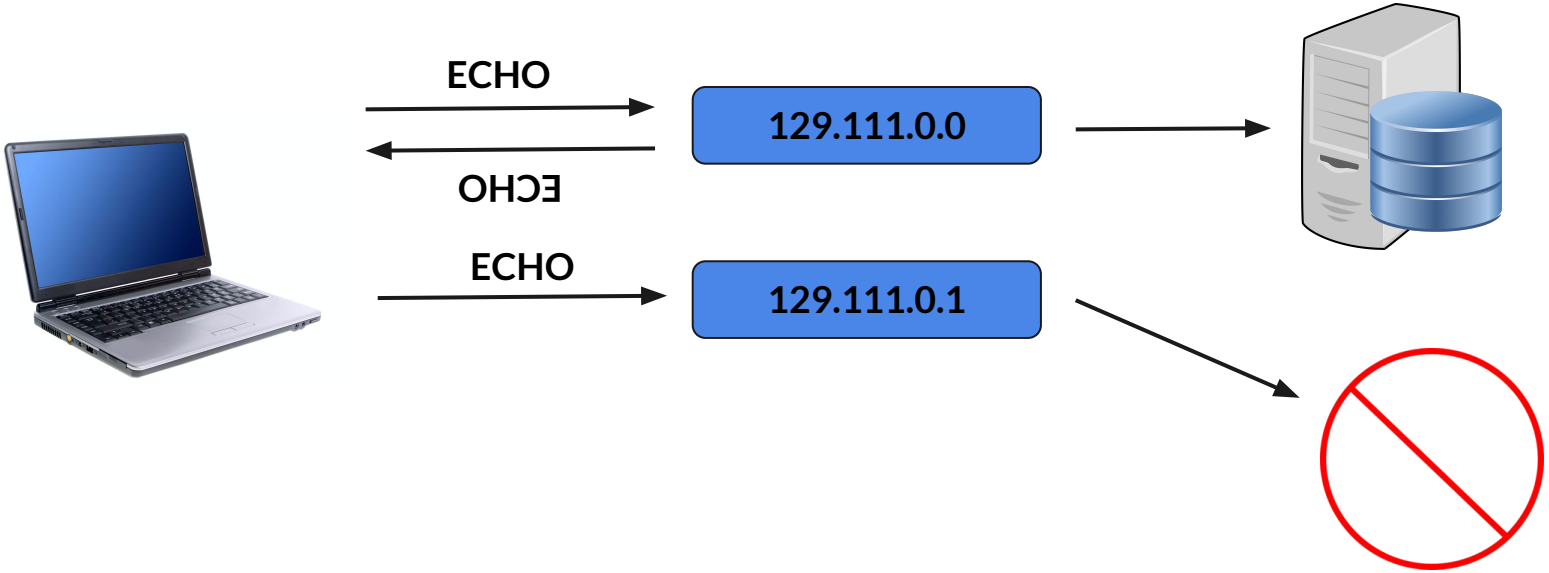
First one to find the answer gets a YubiKey!

Hint: You could use a website like “https://ipinfo.io” to do this.

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

211.32.53.23:80

211.32.53.23:25565

Port 80

Port 25565

Port # determines which service gets a message

Port scanning

211.32.53.23:1

211.32.53.23:2

...

211.32.53.23:80

Port 80

Scanning ports -> identifying services

Exploiting services

Windows
File Share

211.32.53.23:445

Exploiting services

EternalBlue exploit

Remote Code Execution

Exploiting services

About 200,000 computers impacted!

Estimated $4 billion extorted!

Run your own webserver!

If you have Python installed, you can run the following command to start a webserver, which will serve the files in the current directory:

Be careful which directory you run the server though- anyone on your network will be able to access the files in that directory!

```
python -m SimpleHTTPServer <port_number>
```

Try to access your server on the command-line using:

```
curl -m 1 http://localhost:<port_number>
```

CTF Challenge!

I'm running a webserver on a random port on my computer (10.146.23.77).

First to find the flag gets a Raspberry Pi 4B!

Hint 1: This command-line snippet might be useful:

```
for i in {0..65535}; do echo $i; done
```

Hint 2: The directory I ran the server in might have some hidden files that I accidentally included 👀

Extra credit: what version of Python am I running? I'll give you some candy!

My Solution

Bash:

```
for i in {0..65535}; do
    curl -m 1 localhost:$i 2> /dev/null
done
```

Nmap:

```
nmap -p 1-65535 localhost
```

Thanks!

Feel free to hang out and ask questions.

This Thursday: Daniel's talk on secure boot! More info on the ISSS Discord.