Network Architecture

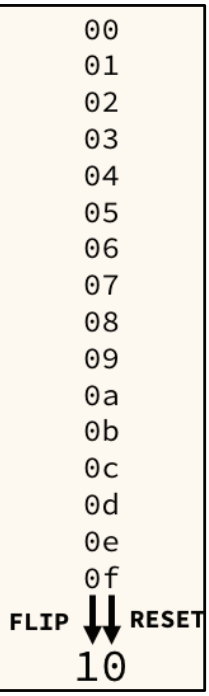
and Passive Gathering

Pre-Network Brain Warmer

Introducing Hex

Hexadecimal

- Base**16**
- We get **16** numbers before we “flip & reset”
  - 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f
  - 00,01,02,03,04,05,06,07,08,09,0a,0b,0c,0d,0e,0f
  - Leading zeros are *still* ignored



Manageable Binary

```
11010101001110111110101011111100
1101 0101 0011 1011 1110 1010 1111 1100
 13   05   03   11   14   10   15   12
 D    5    3    B    E    A    F    C
```

commonly as octets

```
11010101 00111011 11101010 11111100
   D5       3B       EA       FC
```

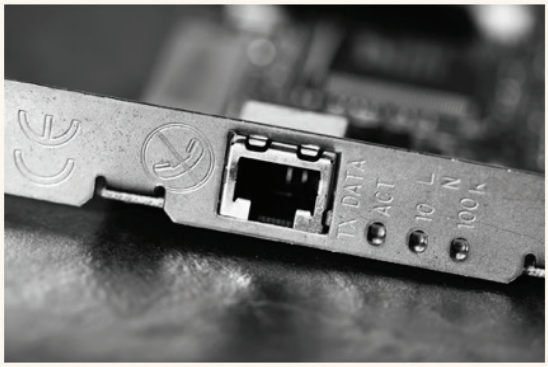
Networks

- Technologies which connect computers
  - And laptops, tablets, printers, IoT, etc...
- Local Area Networks (LANs)
  - Basic unit of networks
  - The network in your home for example
- Wide Area Networks (WANs)
  - Many LANs connected together
  - The internet for example

Network Hardware

Network Interface Cards

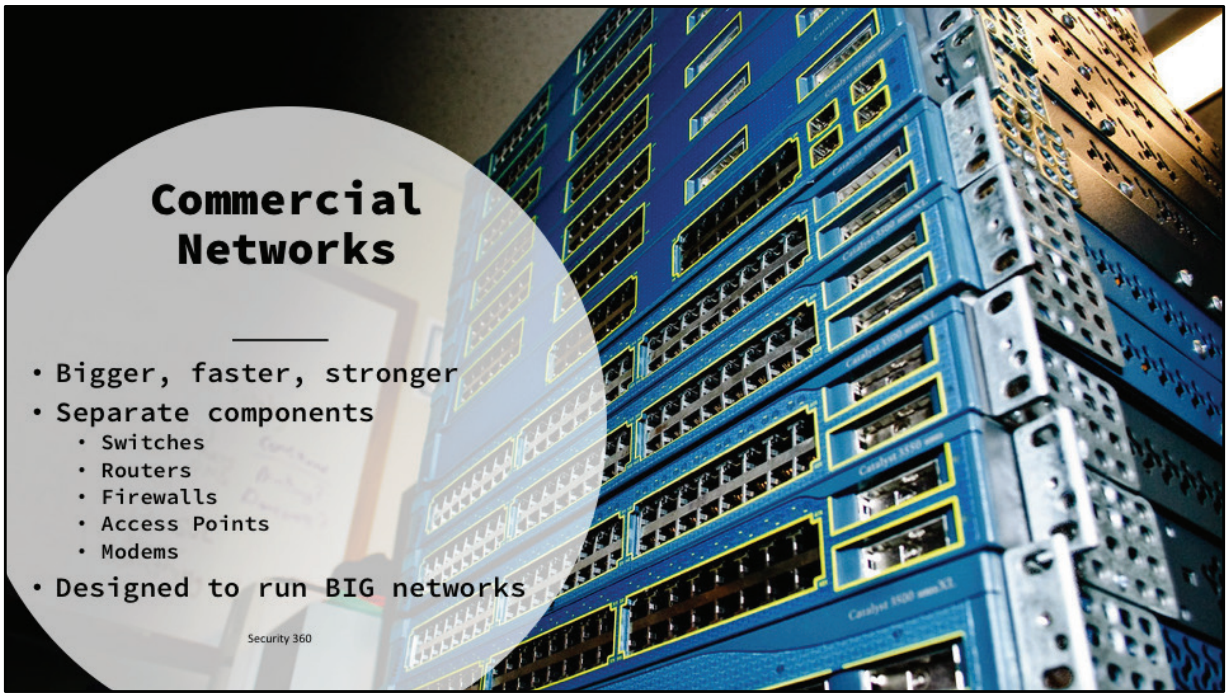
- Convert computer signals to networking signals
- Ethernet
  - For wired connections
  - Cables
- WiFi
  - For wireless connections



Home Networks

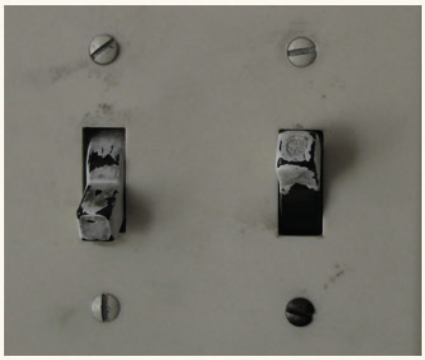
- All-in-one router/switch
- Usually with an access point
- Usually with a firewall
- Oftentimes with a modem
- Designed to run small networks

Security 360



Switches

- Predecessor: Hubs
  - Provided no addressing
  - Packets sent to everyone
- Connects devices on a LAN
  - Uses MAC addressing
    - Media Access Control
    - Hardware address (Ethernet/WiFi card)
    - 00:0d:83:b1:c0:8e
  - Packets sent to intended receiver



Routers

When a switch is not enough

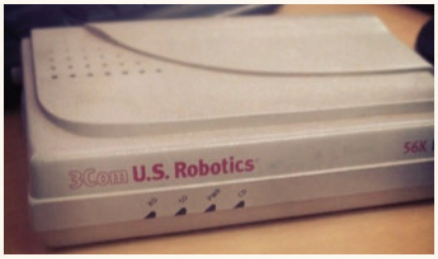
- Connect networks together
  - Provides the connection to the outside
- "Routes" traffic
  - More than a MAC address
  - Gives IP addresses to LAN devices
- Internet access!
- Or multiple company LANs

Modulator-Demodulator

- Signal converter

  DSL/Cable signals ↔ Computer signals

- Brings the Internet to the router

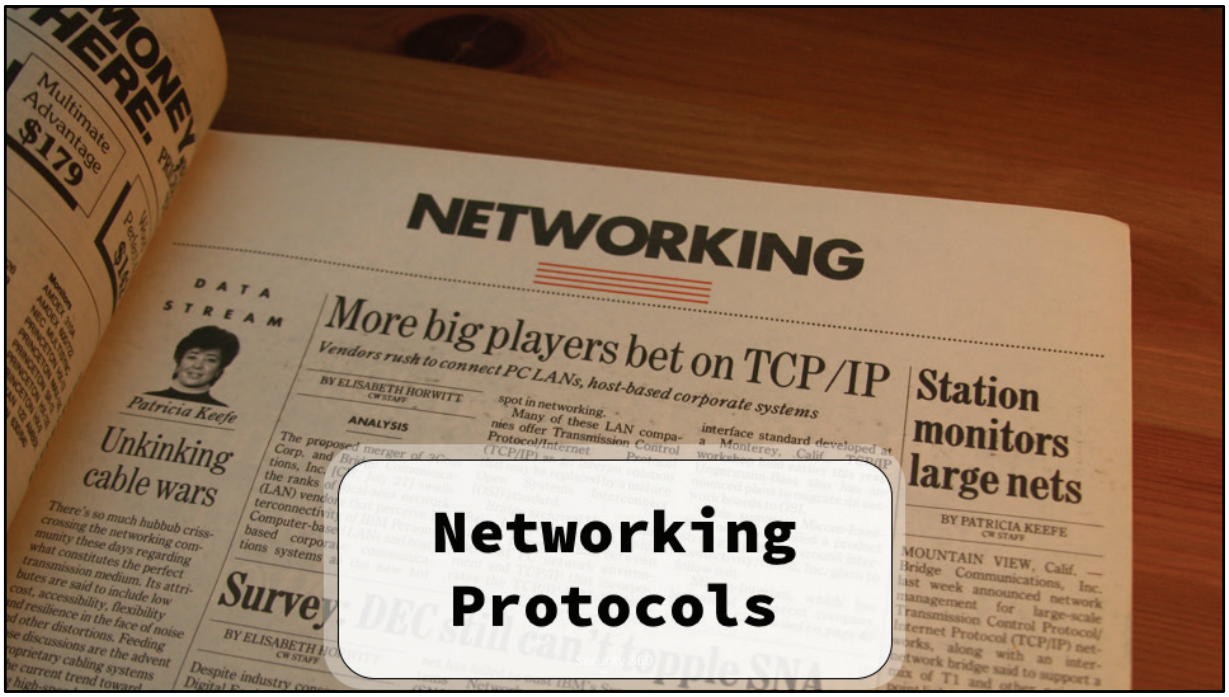


Security 360

Access Points

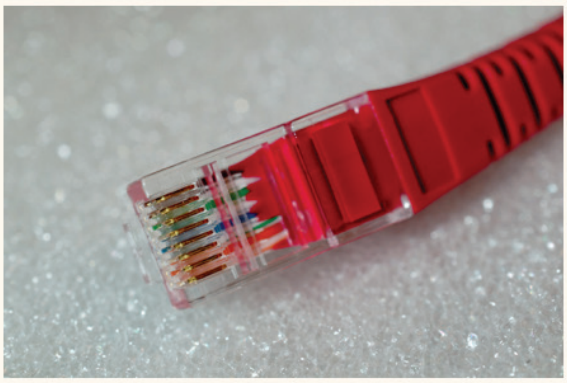
- Provide WiFi access to the network
- Wired connection to the switch/router

Security 360



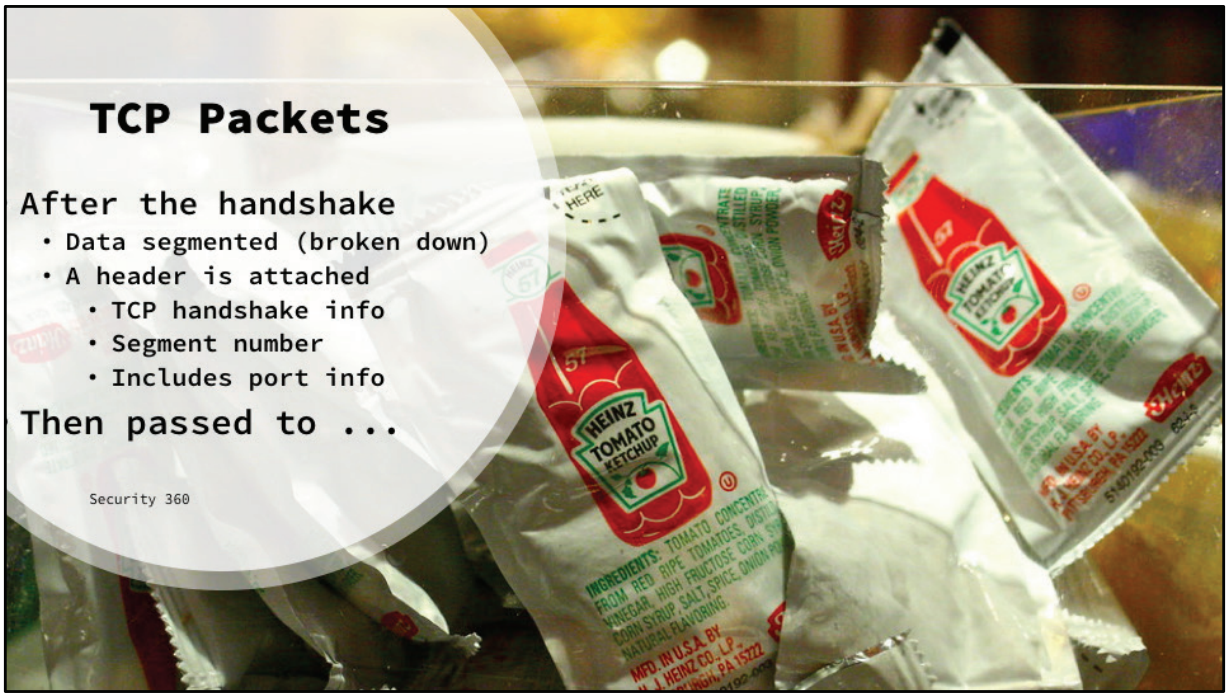
Ethernet

- Lowest-level protocol
- First to start encapsulating data
  - Data -> packets
- Actually called frames
  (But sometimes packets)
- Includes MAC Addressing



Transmission Control Protocol

- First **establishes** connection
- The three-way handshake
- Two parties
  - Alice sends
    - **SYN**(chronize) packet
  - Bob receives SYN, sends
    - **SYN-ACK**(nowledgement) packet
  - Alice receives SYN-ACK, sends
    - **ACK** packet



Internet Protocol

- Used to **send** the message/data
- IP takes over from TCP
  - Further “fragments” data
  - Encapsulates TCP segment
  - Includes IP addressing
  - Voila – IP datagram (packet)
- As/after packets are sent
  - TCP stays busy doing...

TCP/IP (and introducing UDP/IP)

TCP: re-transmits any bad/failed packets due to

- Incomplete transfers
- Failed transfers
- Out-of-order segments

IP re-assembles fragments on receiving end

TCP re-assembles segments on receiving end

UDP (User Datagram Protocol): send blindly, doesn't care

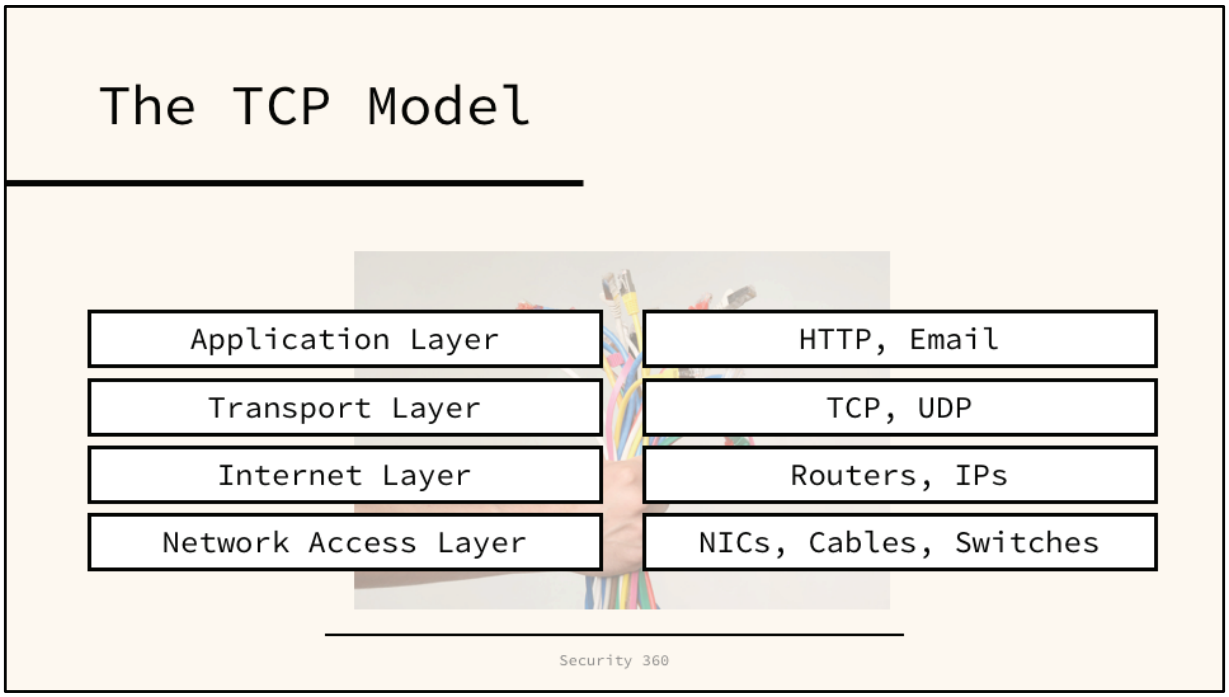
IP re-assembles fragments on receiving end

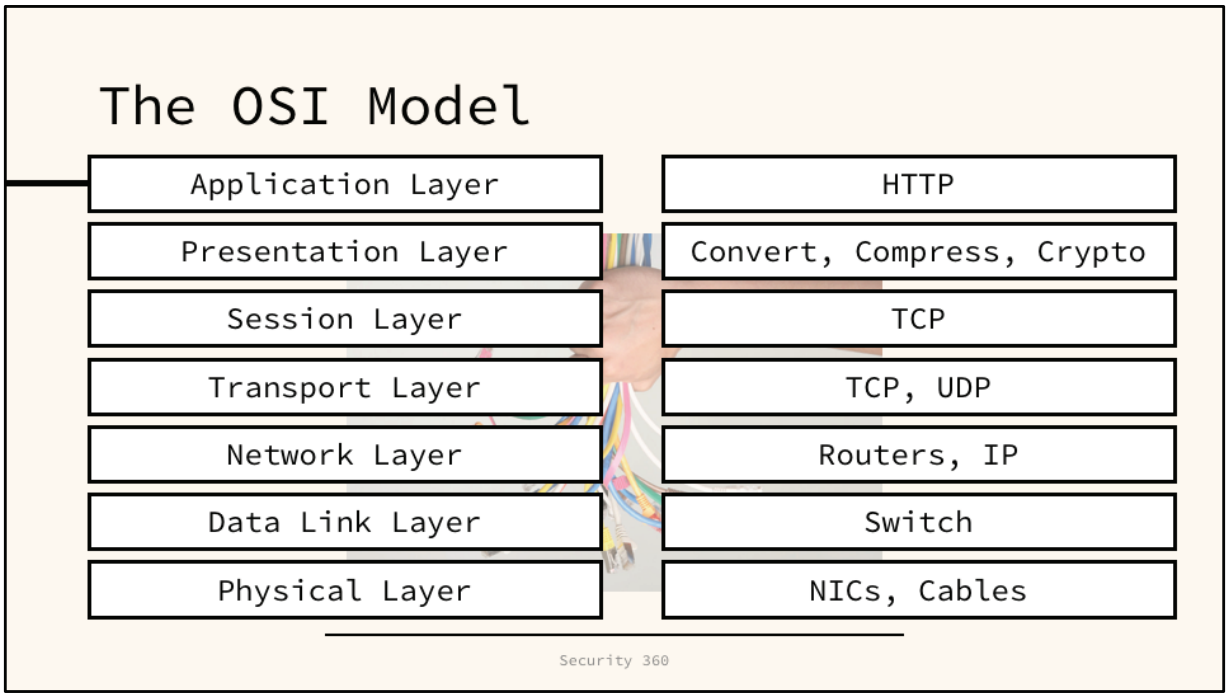
UDP doesn't do anything - doesn't care

Ending a TCP connection

- Graceful termination
  - Alice sends
    - **FIN**(al) packet
  - Bob receives FIN, sends
    - **ACK** packet, **FIN** packet
  - Alice receives ACK & FIN, sends
    - **ACK** packet
- Not-so-graceful termination (or to reject the handshake)
  - **RST** (reset) packet

Networking Models





Network Addresses

Especially IP Addresses

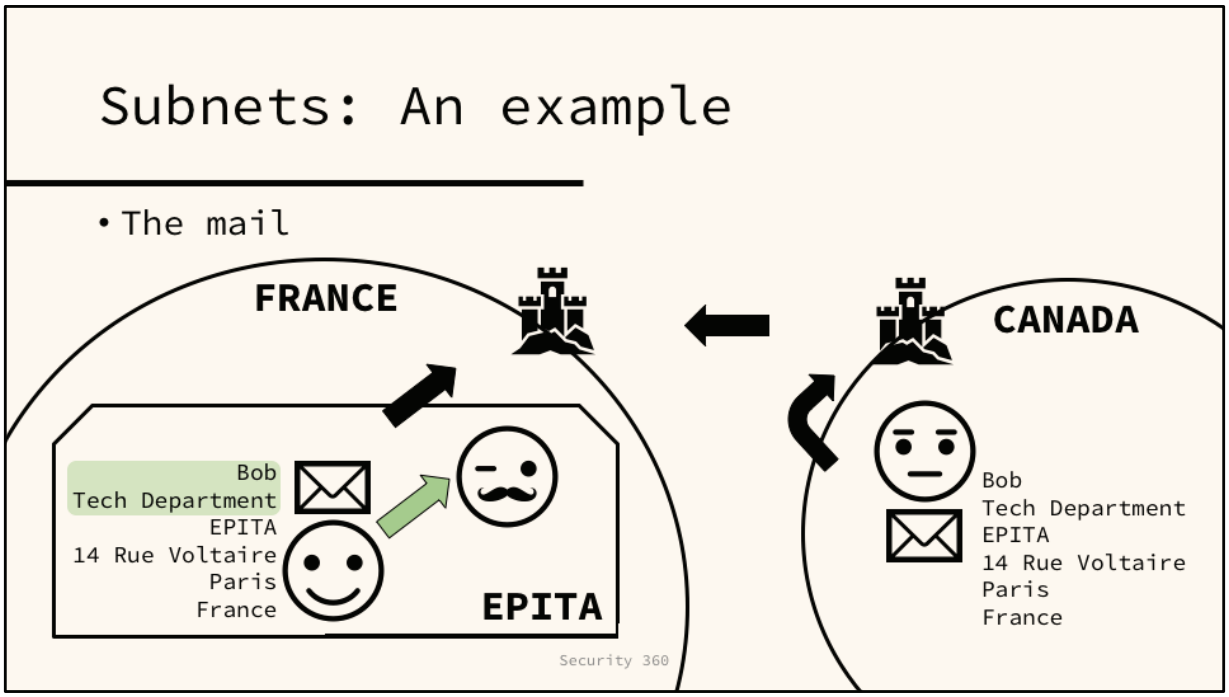
IP Addresses **192.168.1.1**

- Your **public** address on the internet (from your ISP)
  - Or, on your **private** address on your local **subnet**
- It's what a router "routes" to
  - The router gets an IP too! The *Default Gateway*

- Currently IPv4
  - **255.255.255.255** (2^{32} addresses - 4.29 billion)
- IPv6 is ready
  - 80a0:2000:08fb:1050:b0f0:0230 (2^{128} - 340 billion billion b

Subnets

- **Sub**divides **net**works into smaller networks
- Smaller networks are more manageable

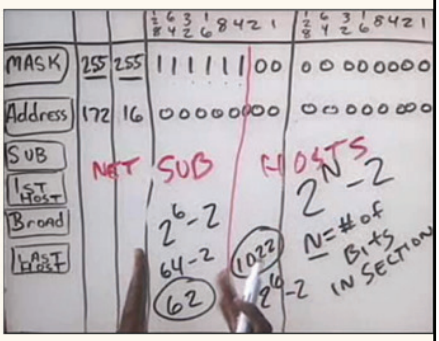

Subnets: An example
• The mail
FRANCE
CANADA
Bob
Tech Department
EPITA
14 Rue Voltaire
Paris
France
EPITA
Bob
Tech Department
EPITA
14 Rue Voltaire
Paris
France
Security 360

Subnetting IPs

- The size of a subnet depends on a **subnet mask**

```
       ip: 192.168.1.0
     mask: 255.255.255.0
my subnet: 192.168.1.0-255

       ip: 192.168.1.0
     mask: 255.255.0.0
my subnet: 192.168.0-255.0-255
```



Security 360

Masks aren't that simple

(they aren't this simple either)

decimal: 255.255.255.0
binary: 11111111.11111111.11111111.00000000
Easy enough, for the last field, use any number

What about this

binary: 11111111.11111111.11111111.10000000
decimal: 255.255.255.128
subnet: 192.168.1.0-128

Famous Subnets (IP Classes)

- Class A
  - assigned(0-127).**any.any.any**
  - Multi-national companies
- Class B
  - assigned(128-191).assigned(0-255).**any.any**
  - ISPs, schools
- Class C
  - assigned(192-223).assigned(0-255).assigned(0-255).**any**
  - Small/medium-businesses

Public/Private IP
at home

- ISP assigns you a single **public** IP
- You (your router) creates a subnet
- Your LAN can have many devices on it
- Each device gets its own **private** IP

Security 360

Domain Names

- Can you imagine typing in an IP each time you wanted to visit Google?
- The DNS (Domain Name System)

Domain name

microsoft

Top-level domain

com

Host name

www

Security 360

FQDN & Subdomains

- Fully Qualified Domain Name
  www.microsoft.com

- Subdomains
  - Other host name possibilities
    support
    store
    office

  support.microsoft.com
  store.microsoft.com
  office.microsoft.com

also FQDNs!

DNS Servers

- Translate an IP address to a FQDN, and back
- A kind of phonebook for the internet
  - You type the name, it finds the IP address
- Some famous/public ones
  - 8.8.8.8 & 8.8.4.4 (Google)
  - 1.1.1.1 & 1.0.0.1 (Cloudflare)

Ports

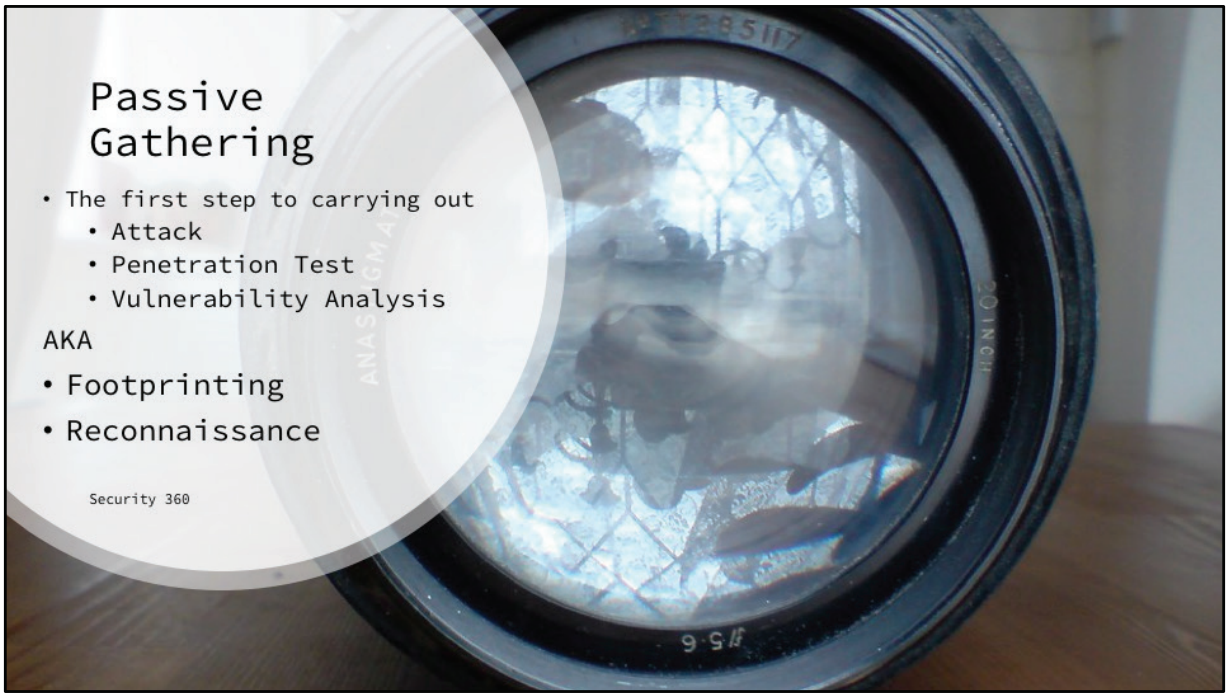
- When network traffic leaves, arr
  where does it go?
- Ports offer a connection
  to a specific application
- A sort of software address
- Sit on the end of an IP
  - 192.168.1.1:80 (HTTP)
- Other famous ports
  :20 :22 :443 (FTP / SSH / HTTPS)

Security 360

That was a lot of addresses

- Hardware address (Ethernet)
  - MAC address
- Network address (IP)
  - Private IP
- Router address (IP)
  - Default Gateway
- ISP assigned IP (IP)
  - Public IP
- Software address (TCP)
  - Port

So what?



Things we'd like to know

- IP address/domain names (across a network)
- Open ports
- Running software, versions
- Packets (if we're on a network)
- Email addresses
- Site info

It's all there, ready to be gathered!

How do we gather it??

- Some websites
  - Netcraft
  - Archive.org
  - Google-Fu/Dorking
  - pastebin
- Some tools
  - WHOIS
  - traceroute
  - nslookup
  - nmap
  - tcpdump / Wireshark

Google Dorks DB:
https://www.exploit-db.com/google-hacking-database

WHOIS, nslookup & traceroute

- Simple Linux tools, included in many distros

- WHOIS
  - Returns the Domain registration info
  - Owner, email, creation, etc...
- nslookup
  - Queries the DNS server for the matching IP/FQDN
- traceroute
  - Traces the route from your IP to the end IP
  - Where the connection passes through

nmap (Network Mapper)

- Scans networks (IPs / IP ranges / subnets)
- Finds hosts (devices)
- Finds services (software)
- Sends packet, waits for response
  - This is passive, but still invasive

BE CAREFUL WITH THIS ONE

https://nmap.org/movies/

Sites that don't mind being scanned:
http://scanme.nmap.org/
https://www.hackthissite.org/

tcpdump / Wireshark (GUI)

- The Packet Sniffer
- Observes packets on a connected network
  - This is passive, and not as explicitly invasive
- Wait, you think!
  - Since we're all using switches, how can I see all the packets on the network? Shouldn't I just see ones addressed to my MAC address?
- Promiscuous/Monitor, Port Mirror

Security 360

HTTP (unencrypted login) for sniffing:
http://testing-ground.scraping.pro/login