CSE 127 Week 8 Discussion

Ariana Mirian

Zoom

Props to Deian Stefan for Slides

This is being recorded

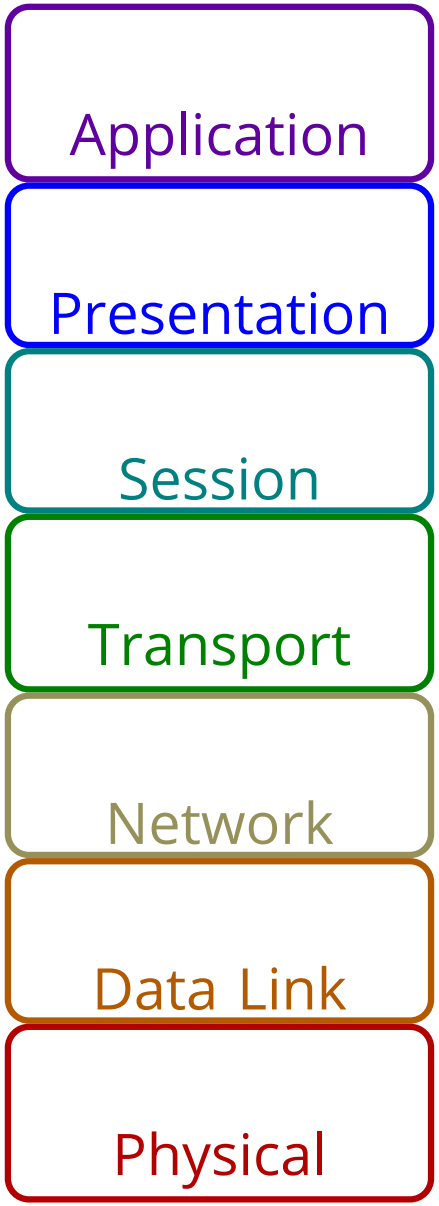
PA4 due tomorrow!

Overview of Today

- Overview of last two lectures
  - Some new information
- Brief overview of PA5
  - Tools that might be helpful during the PA
- Open office hours (if time)

OSI Layers

(Open Systems Interconnection)



- End user layer
- HTTP, FTP, Skype, SSH, SMTP, DNS

- Syntax, byte order, compression, encryption
- SSL, SSH, MPEG, JPEG

- Connection establishment and maintenance
- APIs, sockets

- End-to-end connections between processes
- TCP, UDP

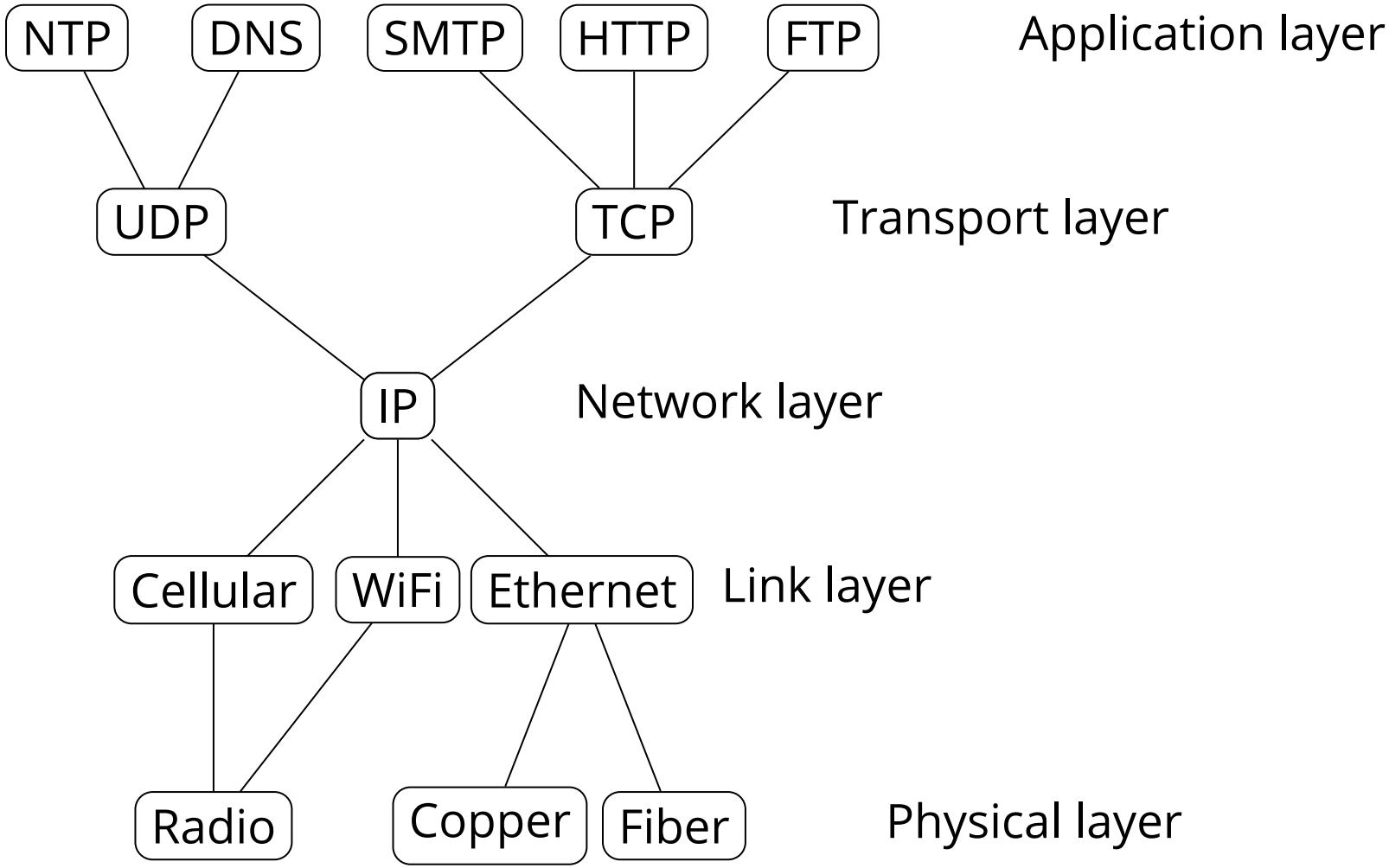
- Addressing, routing between nodes
- IP

- Link management, frames
- Ethernet, WiFi

- Physical wires
- Photons, RF modulation

Basic Internet Archictecture “Hourglass”

Narrow waist = interoperability



Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser’s URL bar. What happens?

Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser's URL bar. What happens?

1. Your laptop uses DHCP (Dynamic Host Configuration Protocol) to bootstrap itself on the local network.

Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser's URL bar. What happens?

1. Your laptop uses DHCP (Dynamic Host Configuration Protocol) to bootstrap itself on the local network.
   A. New host doesn't have an IP address, doesn't know who to ask

Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser's URL bar. What happens?

1. Your laptop uses DHCP (Dynamic Host Configuration Protocol) to bootstrap itself on the local network.
   A. New host doesn't have an IP address, doesn't know who to ask
   B. Broadcasts DHCPDISCOVER to 255.255.255.255 with its MAC address

Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser's URL bar. What happens?

1. Your laptop uses DHCP (Dynamic Host Configuration Protocol) to bootstrap itself on the local network.
   A. New host doesn't have an IP address, doesn't know who to ask
   B. Broadcasts DHCPDISCOVER to 255.255.255.255 with its MAC address
   C. DHCP server responds with config: lease on host IP address, gateway IP address, DNS server information

Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser’s URL bar. What happens?

2. Your laptop makes an ARP request to learn the MAC address of the local router.

Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser's URL bar. What happens?

2. Your laptop makes an ARP request to learn the MAC address of the local router.

A. Every connection outside the local network will be encapsulated in a link-layer frame with the local router's MAC address as the destination.

Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser's URL bar. What happens?

2. Your laptop makes an ARP request to learn the MAC address of the local router.

A. Every connection outside the local network will be encapsulated in a link-layer frame with the local router's MAC address as the destination.
B. Your laptop encapsulates each IP packet in an Ethernet frame addressed to the local router

Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser's URL bar. What happens?

2. Your laptop makes an ARP request to learn the MAC address of the local router.

A. Every connection outside the local network will be encapsulated in a link-layer frame with the local router's MAC address as the destination.
B. Your laptop encapsulates each IP packet in a WIFI Ethernet frame addressed to the local router
C. The local router de-capsulates these Ethernet frames and re-encodes them to forward them on its fiber connection to its upstream ISP, or to another part of the network.

Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser's URL bar. What happens?

2. Your laptop makes an ARP request to learn the MAC address of the local router.

A. Every connection outside the local network will be encapsulated in a link-layer frame with the local router's MAC address as the destination.
B. Your laptop encapsulates each IP packet in a WIFI Ethernet frame addressed to the local router
C. The local router de-capsulates these Ethernet frames and re-encodes them to forward them on its fiber connection to its upstream ISP, or to another part of the network.
D. Each hop re-encodes the link layer for its own network.

Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser's URL bar. What happens?

3. You laptop does a DNS lookup on ucsd.edu
    A. It learned the IP address of a DNS server from the router or was already hardcoded in (8.8.8.8)

Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser's URL bar. What happens?

3. You laptop does a DNS lookup on ucsd.edu
    A. It learned the IP address of a DNS server from the router or was already hardcoded in (8.8.8.8)
    B. Each request is a DNS query encapsulated in one or more UDP packets encapsulated in one or more IP packets

Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser's URL bar. What happens?

3. You laptop does a DNS lookup on ucsd.edu
    A. It learned the IP address of a DNS server from the router or was already hardcoded in (8.8.8.8)
    B. Each request is a DNS query encapsulated in one or more UDP packets encapsulated in one or more IP packets
    C. Each response tells the laptop what authority nameserver to query, until it learns the final IP Address (132.239.180.101) for ucsd.edu

Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser's URL bar. What happens?

3. You laptop does a DNS lookup on ucsd.edu
    A. It learned the IP address of a DNS server from the router or was already hardcoded in (8.8.8.8)
    B. Each request is a DNS query encapsulated in one or more UDP packets encapsulated in one or more IP packets
    C. Each response tells the laptop what authority nameserver to query, until it learns the final IP Address (132.239.180.101) for ucsd.edu
    D. This address is cached, along with the authorities for the hierarchy in the hostname

Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser’s URL bar. What happens?

4. You laptop opens a TCP connection to 132.239.180.101

Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser's URL bar. What happens?

4. You laptop opens a TCP connection to 132.239.180.101
    A. Each packet of the TCP handshake is encoded in an IP packet that is encoded as Ethernet frames that are decoded and re-encoded as they pass through the network

Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser's URL bar. What happens?

4. You laptop opens a TCP connection to 132.239.180.101
    A. Each packet of the TCP handshake is encoded in an IP packet that is encoded as Ethernet frames that are decoded and re-encoded as they pass through the network
    B. The local router has a routing table that contains IP prefixes that it matches against the IP address that tells it what address to forward the packets to

Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser's URL bar. What happens?

4. You laptop opens a TCP connection to 132.239.180.101
    A. Each packet of the TCP handshake is encoded in an IP packet that is encoded as Ethernet frames that are decoded and re-encoded as they pass through the network
    B. The local router has a routing table that contains IP prefixes that it matches against the IP address that tells it what address to forward the packets to
    C. The packet passes through a series of Autonomous Systems (AS)

Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser's URL bar. What happens?

4. You laptop opens a TCP connection to 132.239.180.101
    A. Each packet of the TCP handshake is encoded in an IP packet that is encoded as Ethernet frames that are decoded and re-encoded as they pass through the network
    B. The local router has a routing table that contains IP prefixes that it matches against the IP address that tells it what address to forward the packets to
    C. The packet passes through a series of Autonomous Systems (AS)
    D. E.g. sbcglobal.net -> att.net -> leve3.net -> cenic.net -> ucsd.edu

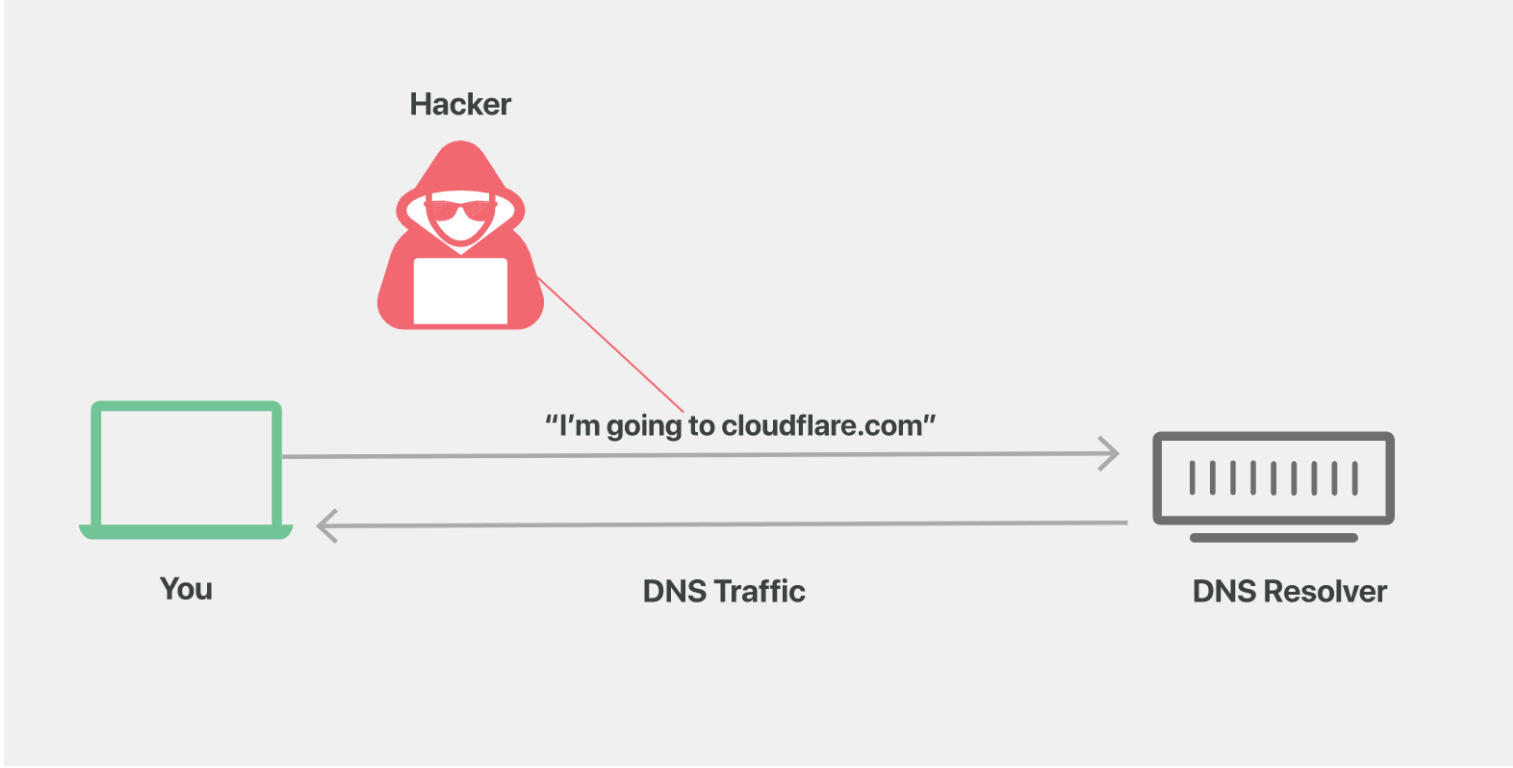
Working example

You connect your laptop to a café wifi network and type ucsd.edu into your browser's URL bar. What happens?

5. Your laptop sends a HTTP GET request inside the TCP connection
6. Based on the HTTP response, your laptop performs a new DNS lookup, TCP handshake, and HTTP GET for every resource in the HTML as it renders

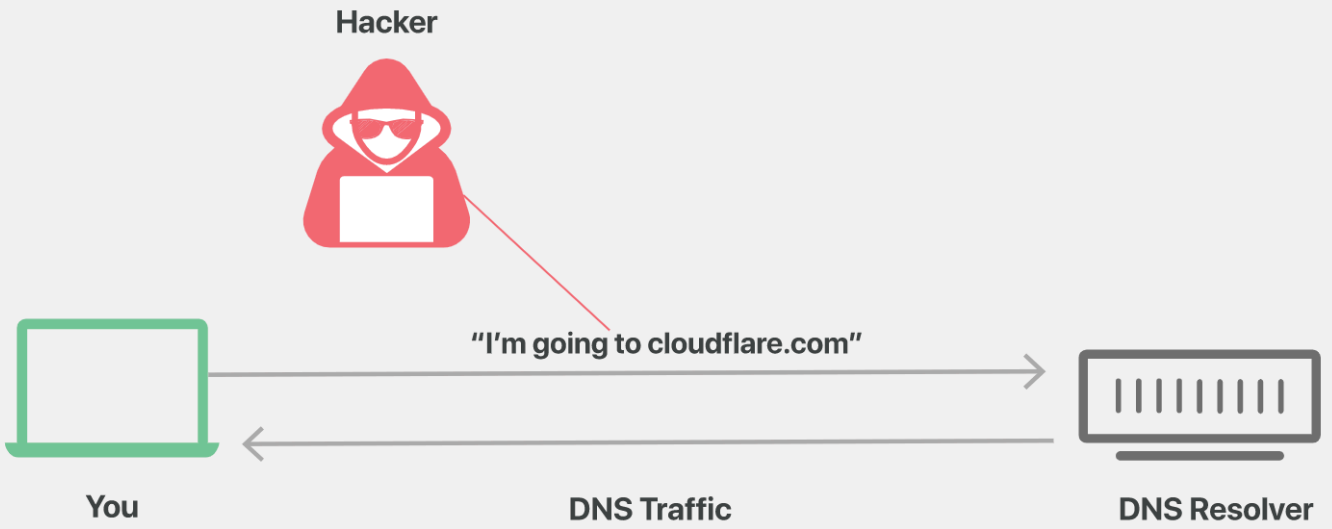
Network attacks overview

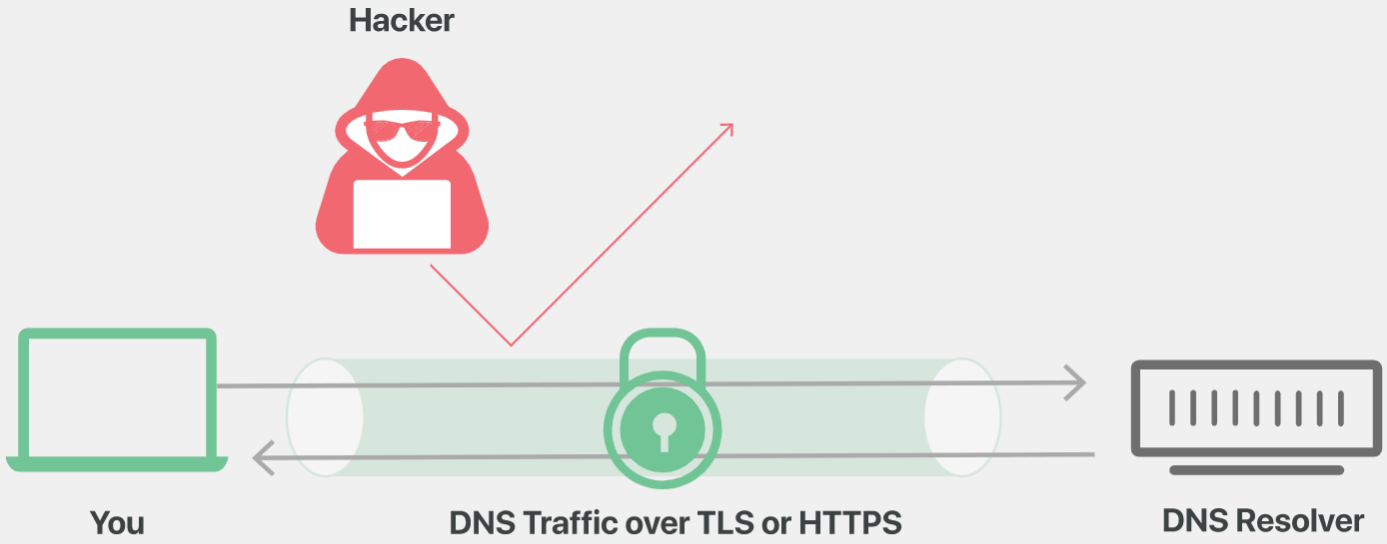
- DNS Cache poisoning



https://www.cloudflare.com/learning/dns/dns-over-tls/

https://www.cloudflare.com/learning/dns/dns-over-tls/

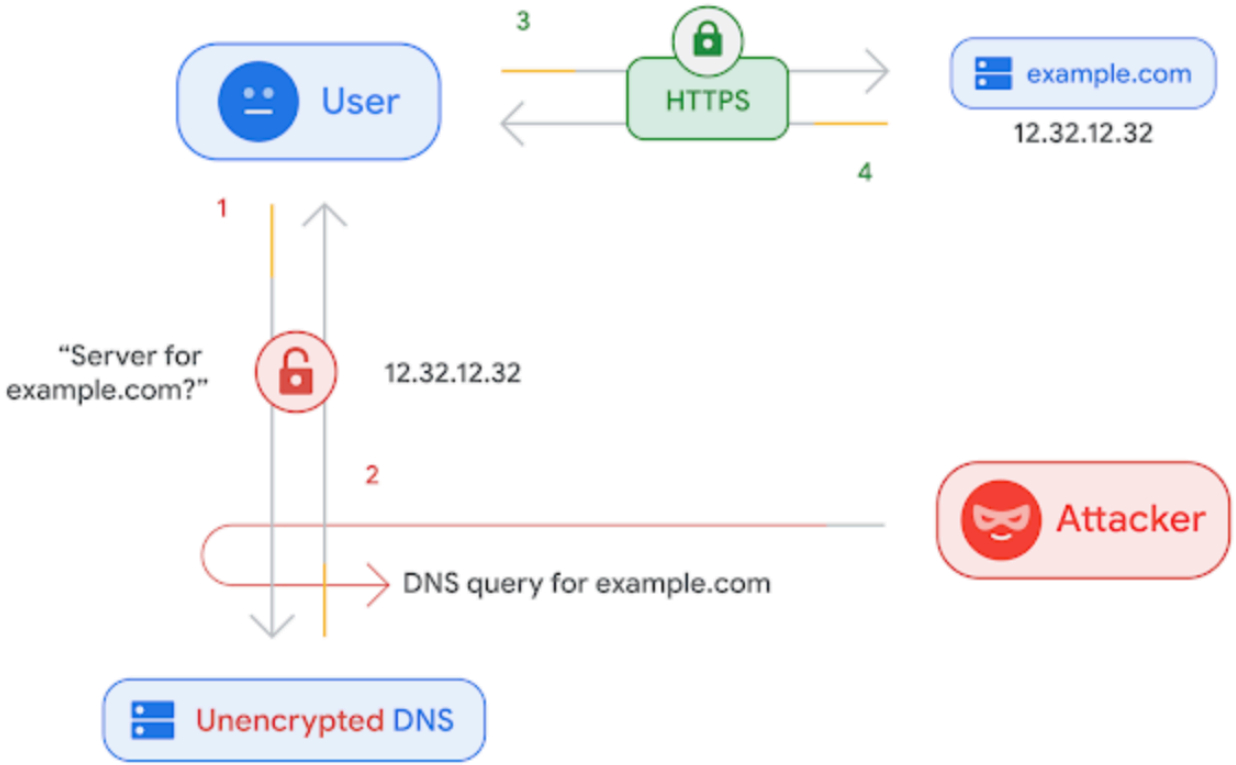




DNS over TLS and DNS over HTTPS

- DNS over TLS – uses TLS over UDP to protect DNS queries
  - Port 853
- DNS over HTTPS – uses HTTPS protocol/port to transfer DNS queries
  - Port 443
- Why two different solutions? Aren’t they the same?
  - Two different protocols/groups of people writing them
  - Pros and Cons of each

https://blog.chromium.org/2020/05/a-safer-and-more-private-browsing-DoH.html



With unencrypted DNS, an attacker connected to the same network can observe other users' browsing habits.

Network attacks overview

- DNS Cache poisoning
- Denial of Service
  - Resource consumption of service
  - TCP handshakes are expensive
- Network perimeter defenses
  - Hey you! Get off my firewall!

PA5 Overview!

PA5 overview

- Planned to be released Thursday or Friday, 2 weeks to finish it (hard deadline of June 11th because we need to turn in grades)
- Scavenger hunt! You need to find Stefan's "password"
  - Not his actual password…
- We'll send you an email with a tar file
  - From there, need to figure out how to get the password
  - Scavenger hunt so please be cautious of spoilers…come to office hours or utilize private posts on Piazza

Overview of tools you may need

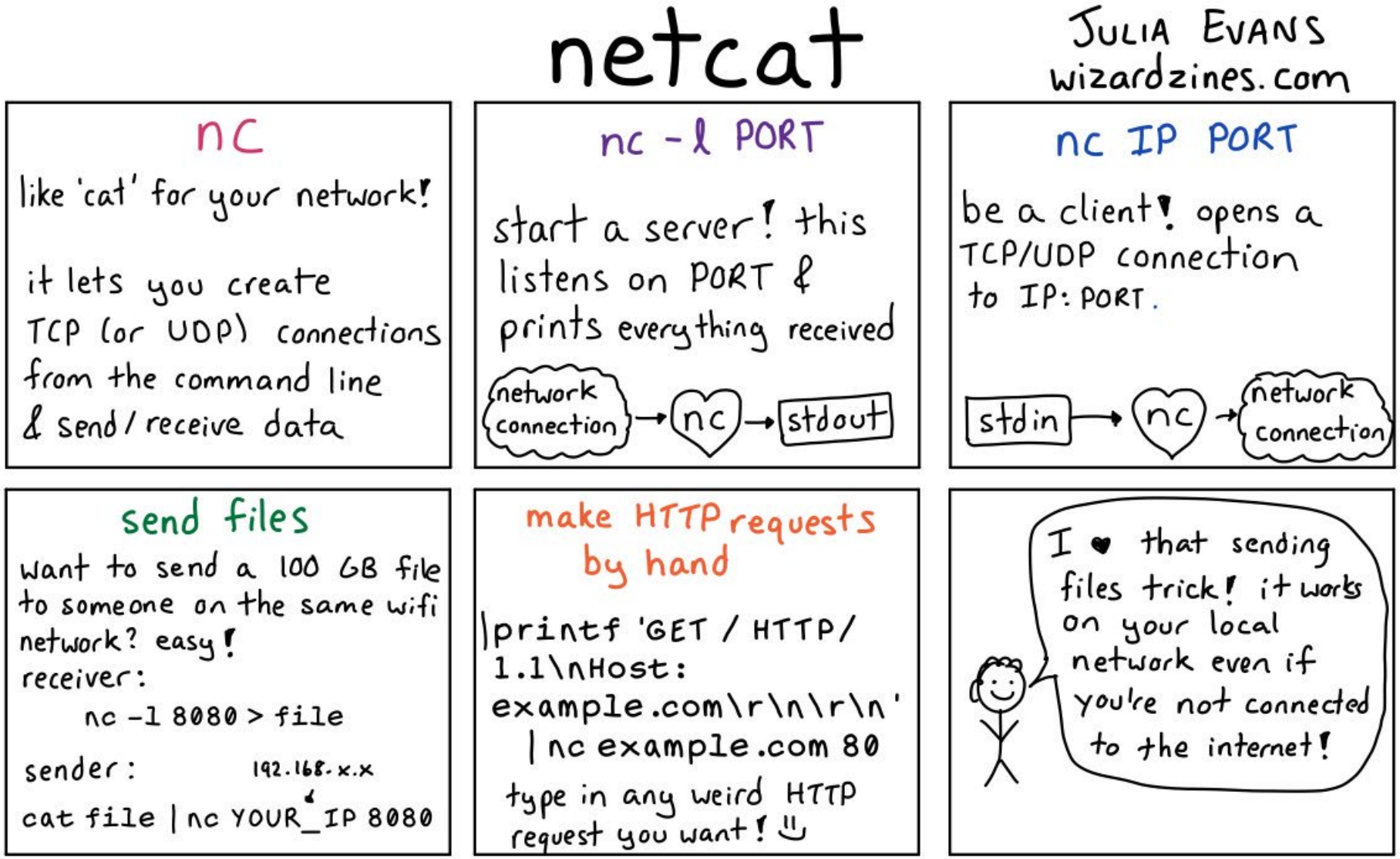
- nc
- nmap
- ssh
- tcpdump
- wget

Overview of tools you may need

- Nc – allows you to make connections locally
- Nmap – scan ports/IPs (locally and externally)
- Ssh – connect to servers
- Tcpdump – view traffic on machine
- Wget – download of files from internet

- All of these have “man” pages!

NetCat (shoutout to Julia Evans)



Happy hunting!