PA4 Discussion

PA4: Network Attacks

- Scavenger hunt! You need to find Stefan's “password” reset token
- You should be receiving a tar.gz file in your email
  - This will be the starting point
  - Subject: [CSE 127] PA5 Flash Drive Dump
  - From: ta_admin@bungle.sysnet.ucsd.edu
- Please be cautious of spoilers, utilize OH and private Piazza posts
- START EARLY! You could be stuck for a while if you don’t know what to do, and it can be hard to estimate how much further you still have to go

Logistics

- Deadline: Friday, Dec 2 at 11:59pm
- Submit to each of the Gradescope assignments:
  - Part A: Mystery
    - What to submit revealed in the middle of the PA
  - Part B: Token
    - Submit a single file named "token"
    - If you are in a group, you can submit any group member’s token
  - Part C: Writeup
    - Any file briefly describing what you did to achieve the end goal

Tools for PA4

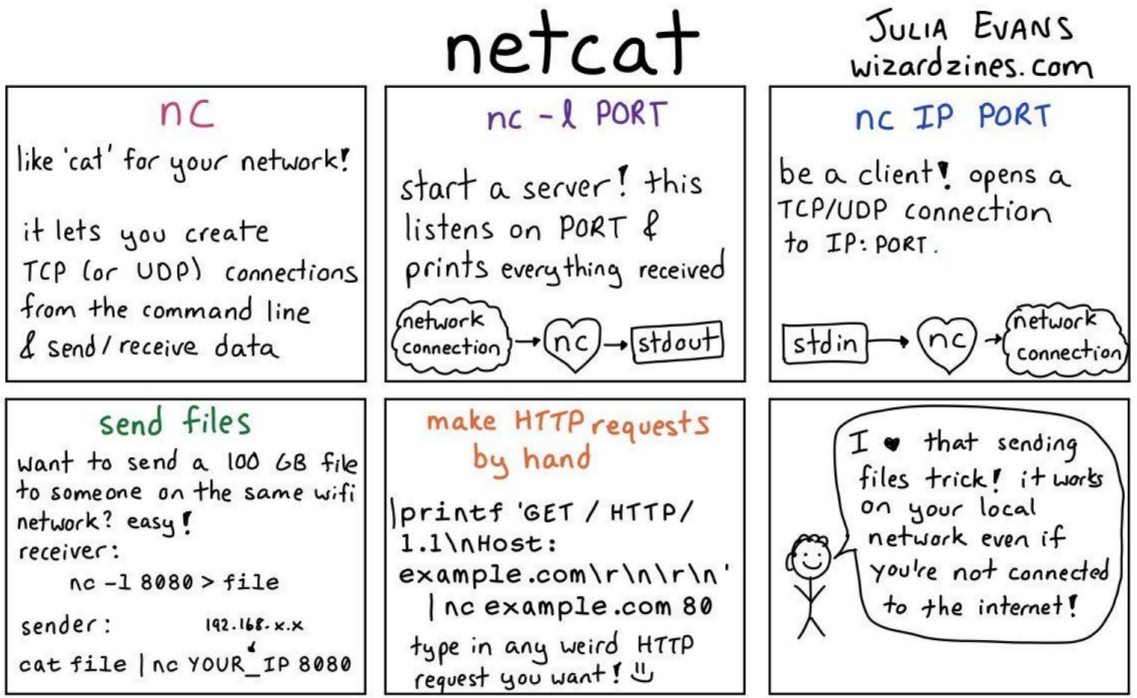
- nc - Allows you to make connections locally
- nmap - Scan ports/IPs (locally and externally)
- ssh - Connect to servers over shell
- tcpdump - View network traffic on machine
- wget - Download files from the internet

Check out all their "man" pages

Try to find the commands as well as the options that give you exactly what you need

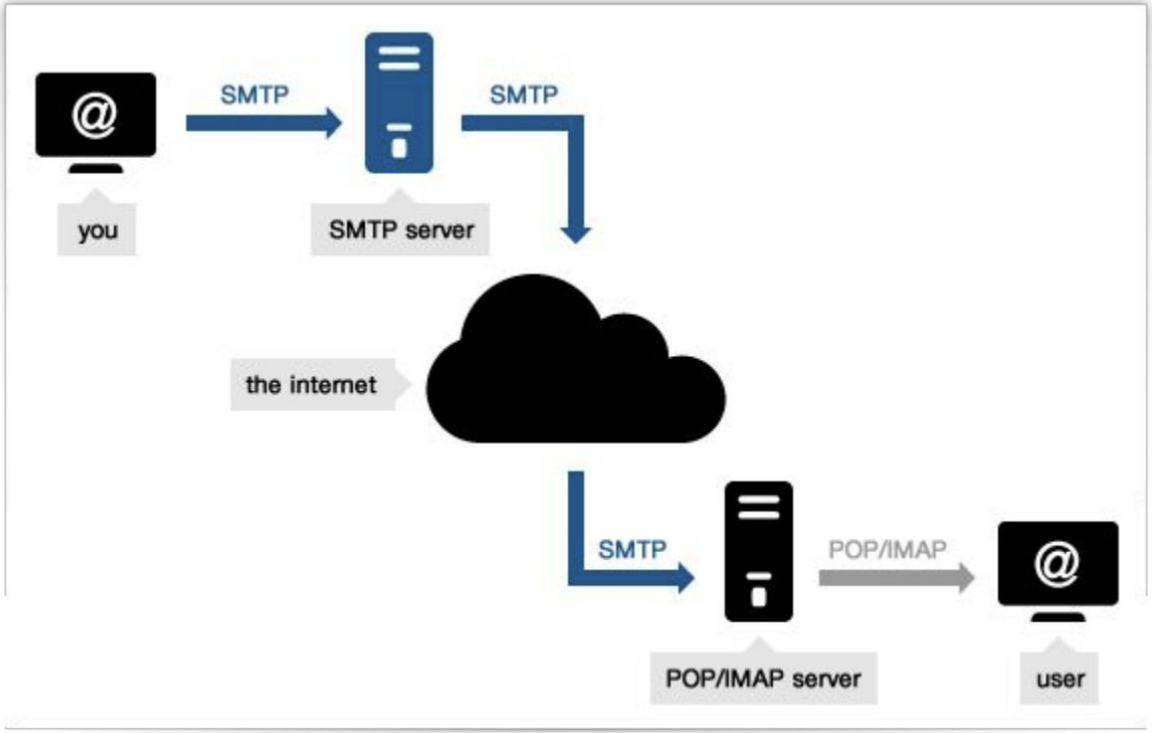
tcpdump

- Used to display TCP/IP and other packets that are transported over a network the machine is in
- Reading the tcpdump of a machine can be very noisy
  - Use "tcpdump -D" to see what interfaces are available
  - Specify an interface with the "-i" option
- By default, tcpdump only looks at packet header information
  - If you wish to view the packet contents, you must use the "-X" or "-A" options


netcat
Julia Evans
wizardzines.com
nc
like 'cat' for your network!
it lets you create TCP (or UDP) connections from the command line & send/receive data
nc -l PORT
start a server! this listens on PORT & prints everything received
network connection
nc
stdout
nc IP PORT
be a client! opens a TCP/UDP connection to IP:PORT.
stdin
nc
network connection
send files
Want to send a 100 GB file to someone on the same wifi network? easy!
receiver:
nc -l 8080 > file
sender: 192.168.x.x
cat file | nc YOUR_IP 8080
make HTTP requests by hand
printf 'GET / HTTP/1.1\nHost: example.com\r\n\r\n' | nc example.com 80
type in any weird HTTP request you want!
I ♥ that sending files trick! it works on your local network even if you're not connected to the internet!

SMTP

- Simple Mail Transfer Protocol
- A protocol for sending mail
- SMTP servers commonly use TCP on port 25
- SMTPS (S for secure) is often on port 465 as well
- The remote machine for this PA has a smtp server setup


SMTP
SMTP
you
SMTP server
the internet
SMTP
POP/IMAP
POP/IMAP server
user

SMTP Commands

- MAIL FROM
- RCPT TO
- DATA
  - From
  - To
  - Reply-To
  - Date
  - Subject
  - ...
  - The Message

SMTP Fields

- **FROM**: this is the field that indicates where the mail is from. This is our traditional notion of who the mail's sender is
- **REPLY-TO**: This is added by the sender to indicate where human replies should be addressed to. When you press the "Reply" button on, say, your Gmail client, the email in this field will show up as you compose your reply

SMTP Fields: MAIL FROM vs. FROM

- **MAIL FROM** and **RCPT TO** are both fields in the “envelope” of the email address whereas FROM and other fields are in the “letter” of the email
- **MAIL FROM** is the one used by SMTP servers to transport the mail
- But when it shows up in the client, typically the envelope is discarded and only the FROM is shown

SMTP Server

“Relay access denied”: you are using the wrong SMTP server

Don’t use meltdown.cse.127

Email Spoofing

- Pretend to be a legit sender
- Phishing and spam

“Hey, this is your TA Sumanth, something went wrong on Gradescope. Could you send your current PA back through email?”

Spoofing

- MAIL FROM is not checked :(
- FROM is not checked :(
- REPLY-TO is not checked :(

Helpful link: https://en.wikipedia.org/wiki/Email_spoofing

wget

- Need to use https://[some ip address]:[port number]
- Need to specify --no-check-certificate

Misc

- SSH permission too open on WSL: try to ssh from Windows directly
- If you are stuck staring at some chat log, re-read what Stefan says
- Don’t send email to anyone’s real email (e.g. xxx at ucsd.edu). The email addresses used in this PA are local and the format is for you to figure out.