Processes and authentication
ssh b146-*
pstree -p | less -S
pstree -pu crandall
lsof -p31009
nc -l 20202 &
lsof -p31626
kill -9 31626
Authentication in general

• Bishop: “Authentication is the binding of an identity to a principal. Network-based authentication mechanisms require a principal to authenticate to a single system, either local or remote. The authentication is then propagated.”
Authentication in general (continued)

● Bishop: “Authentication consists of an entity, the user, trying to convince a different entity, the verifier, of the user's identity. The user does so by claiming to know some information, to possess something, to have some particular set of physical characteristics, or to be in a specific location.”

● Informally: something you know, something you have, something you are
2FA = 2-Factor Authentication

- Two of these:
  - Something you know
  - Something you have
  - Something you are
- *E.g.*, bank card plus PIN
- For Internet services, typically the first two
- Helps protect against phishing, for example
Basic Linux authentication

- Ties you (the identity) to your user ID (the principal), which is in turn tied to subjects (e.g., processes) and objects (e.g., files)
- Based on hashing
  - Also salting
  - Also shadowed password hashes
SHA-512

Hash

/etc/passwd

Salt

Username

/etc/shadow

Hash

Compare

Hash

Match? Yes or no.
Passwords

- Should be high entropy, algorithmic complexity
- Should be easy to remember

These requirements are in conflict with each other!
Password managers help.
Rainbow Table

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>aaaa</td>
<td>19330d1d</td>
</tr>
<tr>
<td>qwer</td>
<td>da09d7dc</td>
</tr>
</tbody>
</table>
Time-memory tradeoff

- Rainbow tables can store lots of hash results compactly (precomputation)
- Just check if a user's hash might be in a hash chain, only recalculate it if so
- As a fall-back, just try every possible password (brute force)

Salting helps against precomputation.

Good passwords, system-imposed delays, shadowing help against brute force.
Shadowing the password file

```
crandall@rubicon ~ $ sudo grep "hal" /etc/passwd
hal:x:1003:1003:Hal,,,:/home/hal:/bin/bash

 crandall@rubicon ~ $ sudo grep "hal" /etc/shadow
hal:$6$4asLz5vU$l5FDnfwLtlXQf/EEsxl3f3YbjM3fzTtw9EwKy8vsnEU4e8uKlvoy0ST99nquwh5QrHwt3SvGsciQk2D980Q9.17259:0:99999:7::

 crandall@rubicon ~ $ ls -l /etc/passwd
-rw-r--r-- 1 root root 2021 Apr 2 22:49 /etc/passwd

 crandall@rubicon ~ $ ls -l /etc/shadow
-rw-r----- 1 root shadow 1532 Apr 2 22:49 /etc/shadow

 crandall@rubicon ~ $ 
```
Phishing

From: "Dropbox Notification" <dropbox.noreplay@gmail.com>
Date: Dec 7, 2016
Subject: You have 1 new file in your inbox
To: [redacted]
Cc: [redacted]

Hi [redacted]

You have received a new document in your inbox, view the file "مذكرة القبض على عزة سليمان.pdf" on Dropbox.

[Button: View file]
Phishing

• Wide range of sophistication in terms of the social engineering aspect
  – One end of the spectrum: “Plez logg in and changer you password, maam!”
  – Other end of the spectrum: “The attached PDF is my notes from the meeting yesterday, it was nice to see you again!” (from someone you saw at a conference the day before)

  2FA helps protect against phishing (but state actors can easily spoof your cell phone and get SMS messages)
File permissions

```bash
# Search for the string "hal" in /etc/passwd
sudo grep "hal" /etc/passwd
hal:x:1003:1003:Hal,,,:/home/hal:/bin/bash

# Search for the string "hal" in /etc/shadow
sudo grep "hal" /etc/shadow
hal:$6$4asLz5vU$5FDnfwLtIXQf/EES sx3f3YbjM3fzTtw9EwKyr8vsnEU4e8uKIVoy0ST99nqwH5QrHwt3SvGsciqk2D980Q9.17259:0:99999:7::

# List files in /etc/passwd
ls -l /etc/passwd
-rw-r--r-- 1 root root 2021 Apr 2 22:49 /etc/passwd

# List files in /etc/shadow
ls -l /etc/shadow
-rw-r----- 1 root shadow 1532 Apr 2 22:49 /etc/shadow
```
-rwxr-x---

- First is special designations (symlink, directory)
- Next triplet is user (u)
- Triplet after is group (g)
- Last triplet is others (o)
- \( r = \text{read}, \ w = \text{write}, \ x = \text{execute} \)
- Sometimes you'll see other things, like s for Set UID
Processes (subjects) act on files (objects)
Processes are tied to principles (users)
File permissions are checked when the file is opened (and added to the file descriptor table of the process), not with every access!
man ...

- ls (ls -l is a useful flag), cd, pwd, chown, chgrp, chmod, stat, id, w, who, last, kill, ps, pstree, netstat, cat, less, sudo, watch, screen, fuser
Some more things to read up on

- FIFO pipes (can be unnamed or named)
- The /proc/ filesystem
- Character devices (e.g., PTY, PTS, TTY)
Resources

- http://www.cs.unm.edu/~crandall/linuxcommandcheatsheet.txt
- Matt Bishop's *Computer Security: Art and Practice*, Chapter 12
- https://citizenlab.org/