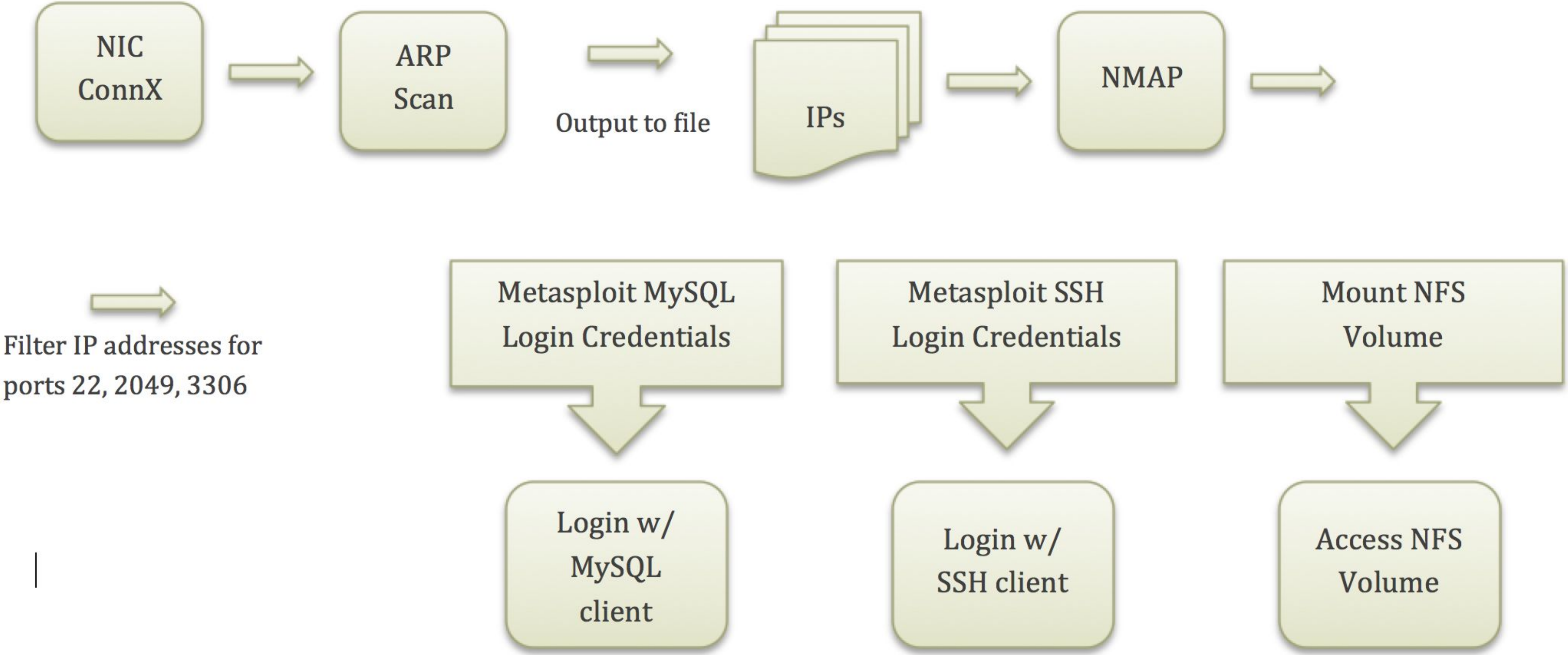
AUTOSCAN

Luke, Nima, Alfredo, Jesus

“Look mommy, here’s daddy’s private folder”

AUTOSCAN flowchart



Landscaping

- ARP-SCAN
  - arp-scan --localnet
  - To discover hosts efficiently

- NMAP
  - nmap -p22,3306 $ARPRESULT -oX nmap_outfile.xml
  - To discover services and open ports

NFS

- Take results of ARP scan, pipe to pingless nmap scan on port 2049
    - `nmap -Pn -p2049 $ARPRESULT --open`
        - `-Pn disables pinging of the host in the interest of speed`
        - `--open only displays open ports`
- Filter results into an iterable list of NFS hosts
    - grep with regular expression to filter for IPs, stored in iterable BASH array
- Search for mountable folders with showmount
    - showmount -e <host>
- Mount and launch new terminal window in target directory
    - Mount -t nfs <host>:<share> <mount point>
    - `Mount point is /tmp/automount/`

MySQL Script

- Evaluate scanned hosts for service mysql
    - services -S mysql -R
- Use auxiliary mysql_login scanner
    - Input Username File
    - Input Password File
- Spool console.log
    - Grep appropriate username and password from log file
- Exit Metasploit
    - Run mysql login from terminal using found host, username, and password

SSH

- Evaluate scanned hosts for open port 22
  - services -p 22 -R - u
  - -p filters out base on port 22
  - -u filters out base on open ports
  - -R sets as RHOSTS
- Use auxiliary SSH_LOGIN scanner
  - Sets rockyou.txt as passwords
  - Sets user as root
- Run any session that SSH brute force was able to open

Questions?