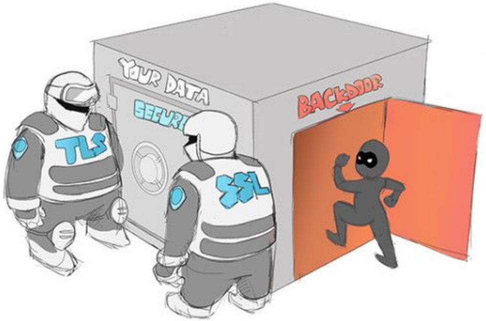
Backdoors

Week of 1o1/16/2020

Necessary Terminology

- port: network location in system to differentiate traffic from different applications/services
- host: the user system/computer
- localhost (or 127.0.0.1): YOUR computer

What are backdoors?



Backdoors: point of entry for users (authorized or not) to enter the system and gain remote access

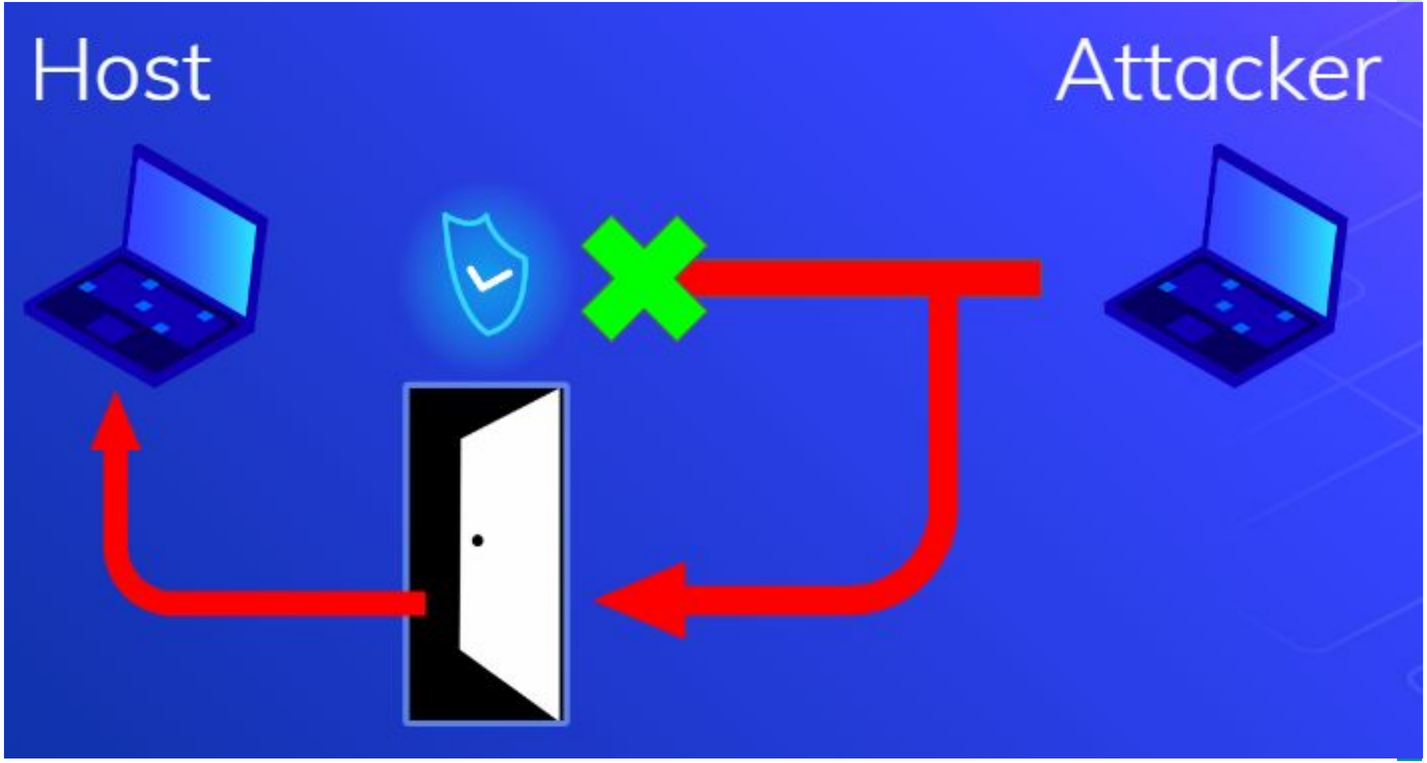
- bypasses normal authentication
- can be used for good or bad (companies, hackers, etc.)
- listen: state of being binded to an open port/process/IP address, establishing a connection
- **Persistence is key**

Threat level? Midnight

WarGames Scene :eyes:

https://www.youtube.com/watch?v=GfJJk7iONTk&ab_channel=sladehayes

A high school “hacker” decides to hack into a gaming company. In this scene he is asking for assistance from his friends…


Host
Attacker

Processes

- process: a running instance of a program
  - foreground: programs that require user interaction via terminal to run
  - background: programs that will run outside of the terminal (does not require user input)
- daemon: see prior definition
- How does this differ from services?

Commands for Processes

- ps [-]aux: lists out all current running processes
  - -a: lists info for all users
  - -u: additional info (can also use -f for full)
  - -x: info about processes w/o terminals
  - can be used w/ grep as well :)
- kill <pid>
  - kills the process w/ the associated process ID

nmap (network map)

- network mapping tool (helps to see ports used)
  - nmap -sV localhost: lists out (in detail) the ports that are open on your host machine
- is technically a hacking tool, so delete when you're done

netstat (network statistics)

- shows open ports and processes using the port
- different from nmap in that it can only be run on the host
  - nmap can work from any computer to any other (again, it’s a hacking tool)

netstat options

netstat -tulpen

- t- checks on tcp
- u- checks on udp
- l- looks at listening ports
- p- displays PID
- e- etc.
- n- shows address/port numbers instead of process names
    - (e.g. 0.0.0.0:22 instead of [::]:ssh)

lsof (list open files)

- lists currently opened files
  - includes executables, etc.
  - shows user running them, process ids, some other stuff
- what command to kill?

crontabs

- Sets up routine processes for users
  - Remember: users have to run processes for them to work
- crontab -e brings up your user’s crontab file
- crontab -u [user] brings up a specific user’s
- Look for any lines that seem harmful and remove them
  - I.e. * * * * * nc -lvp 1337

.rc files

- run when terminal opens
- in user’s home directory
- used to set default behavior and such
  - e.g. .bashrc, .zshrc
- not so much used for backdoors but can be used to screw with your image
- /etc/rc.local holds startup processes for computer (global)