0x03 - Firewalls, Port Scans, DoS

Slides:

http://gencyber.ialab.dsu.edu/2015/Networking/

Log Into (download plugins, etc.):

Learn.ialab.us

http://learn.ialab.us

Recap

- Physical connections send signals
  - What were some kinds of cables we used?
- Addresses let know who we talk to
  - What two types of addresses exist?
- How many “conversations” can you have at once?

The Problem: We talk a lot

- Firefox, Dropbox, Windows Update, Email…
- How can we have multiple conversations and keep them straight??

- Answer: Ports
  - When you communicate, you use a port

Apartment Example

- Think of your computer's network or your firewall like two apartments
  - Each holds 65,535 residents
  - Most units are empty
  - Building names: **TCP** and **UDP**
- The only way we communicate with the residents is through mail
- Each resident has a different job

TCP Building

- Only accepts certified mail, and they will always reply to you in some way
  - **Certified mail**: the sending and receipt of a letter or package are recorded
- Once you've started a conversation, they will always see it through to the end

UDP

- These fellas are a little more unreliable
- They only reply if they are available to be bothered
  - Usually they will get back to you, but no guarantees

Resident Jobs

- Remember, every single resident has a different job
- If you send a letter to the resident in unit 80, they may respond with a webpage
- Resident in unit 53 will likely give you a DNS conversation

Two main categories of packets

- **TCP**
- Have to handshake first
- Has overhead, slower
- Knows if a packet failed
- Referred to as:
  - "Connection Oriented"
  - Stateful
- Great for: browsing websites, email, downloading files

- **UDP**
- Just start talking
- Faster
- Doesn't care if it fails
- Referred to as:
  - "Connectionless"
  - Stateless
- Great for: phone calls, music, streaming video

I would tell you a joke about UDP, but I’m not sure if you’d get it.

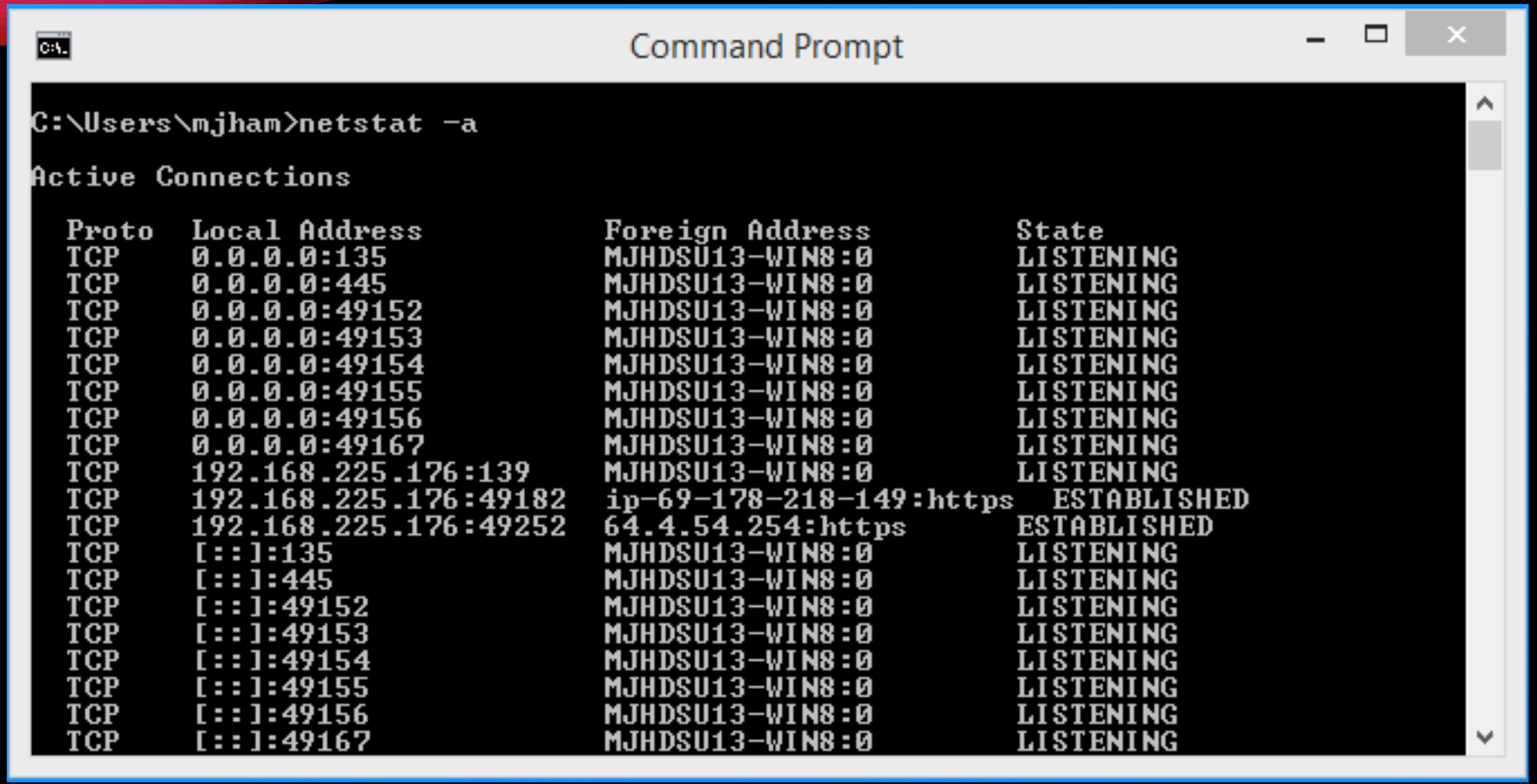
Ports

- You send traffic to www.google.com

- Firefox gets a port
- Google is probably using port 443

- You:57231 -----> Google: 443

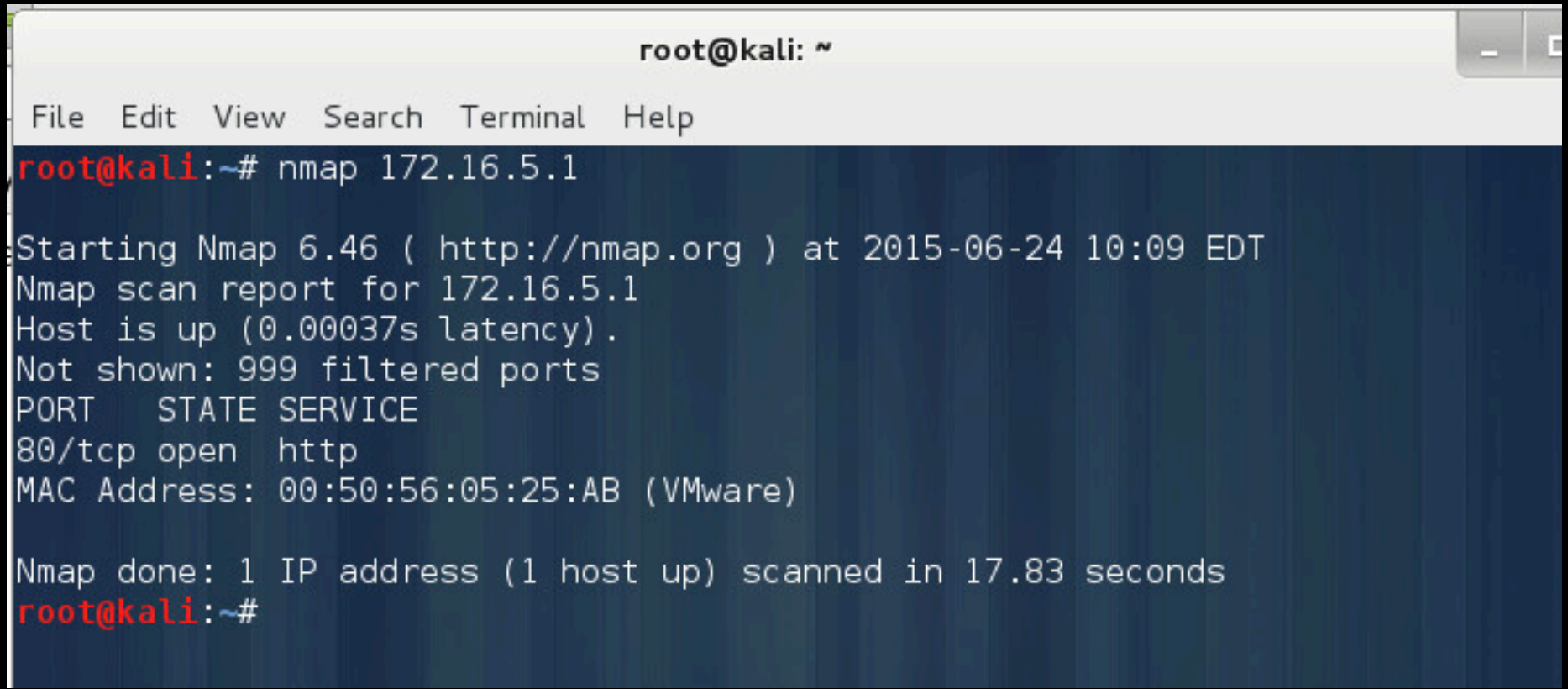
- Check your connections with ‘netstat’


Command Prompt
C:\Users\mjham>netstat -a
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 MJHDSU13-WIN8:0 LISTENING
TCP 0.0.0.0:445 MJHDSU13-WIN8:0 LISTENING
TCP 0.0.0.0:49152 MJHDSU13-WIN8:0 LISTENING
TCP 0.0.0.0:49153 MJHDSU13-WIN8:0 LISTENING
TCP 0.0.0.0:49154 MJHDSU13-WIN8:0 LISTENING
TCP 0.0.0.0:49155 MJHDSU13-WIN8:0 LISTENING
TCP 0.0.0.0:49156 MJHDSU13-WIN8:0 LISTENING
TCP 0.0.0.0:49167 MJHDSU13-WIN8:0 LISTENING
TCP 192.168.225.176:139 MJHDSU13-WIN8:0 LISTENING
TCP 192.168.225.176:49182 ip-69-178-218-149:https ESTABLISHED
TCP 192.168.225.176:49252 64.4.54.254:https ESTABLISHED
TCP [::]:135 MJHDSU13-WIN8:0 LISTENING
TCP [::]:445 MJHDSU13-WIN8:0 LISTENING
TCP [::]:49152 MJHDSU13-WIN8:0 LISTENING
TCP [::]:49153 MJHDSU13-WIN8:0 LISTENING
TCP [::]:49154 MJHDSU13-WIN8:0 LISTENING
TCP [::]:49155 MJHDSU13-WIN8:0 LISTENING
TCP [::]:49156 MJHDSU13-WIN8:0 LISTENING
TCP [::]:49167 MJHDSU13-WIN8:0 LISTENING

How we use ports?

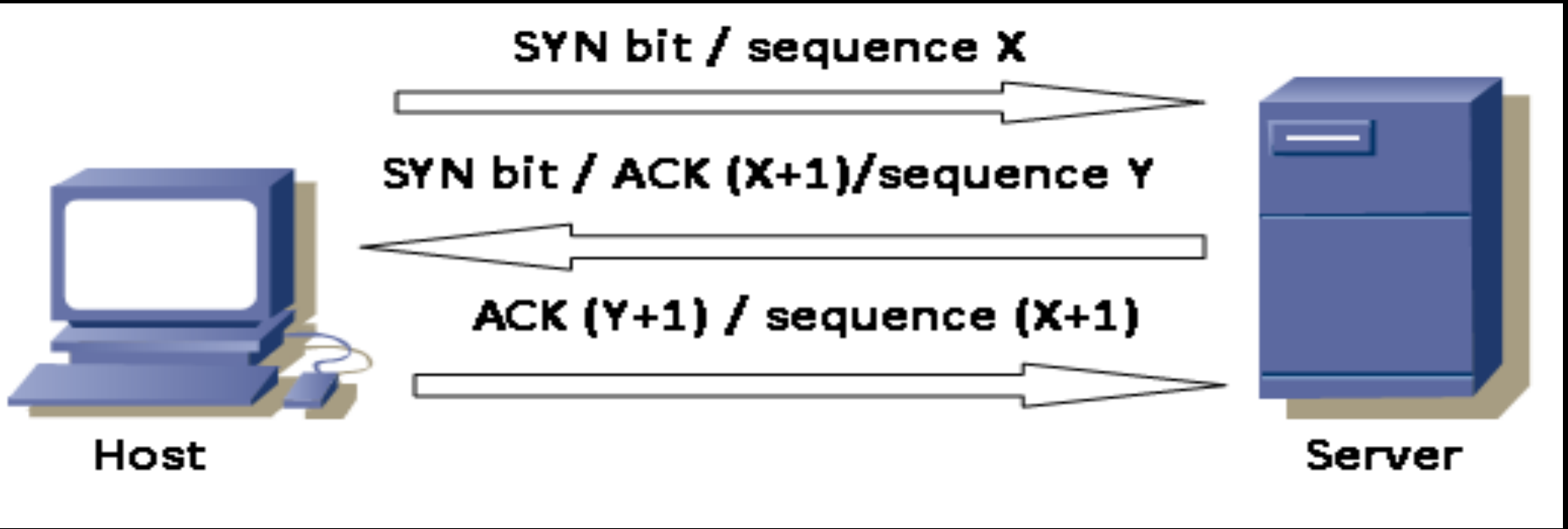
- What is a firewall for?
  - Checks the port numbers
  - If you're not running a web server, block packets to port 80/443
- Common Port Numbers
  - Email: 25
  - Websites: 80 & 443
  - DNS: 53
  - SSH: 25

Port Scan



scanme.nmap.org

Why is TCP Slower?



3 Way Handshake

- Three stages before we can talk:
  - SYN: Hello, I'd like to chat
  - SYN ACK: Ok, lets chat
  - ACK: Sounds good!
  - PSH: Now we're chatting
- Others
  - RST: Get lost, I don't want to talk to you
  - FIN: Thanks for chatting, have a good day

States

- TCP's 3 way handshake is called stateful
- Firewalls should make sure the conversation is going nicely
  - We don't like people that aren't nice
- Some firewalls don't do this though…

Stateful vs. Stateless

- Stateless firewalls don't track sessions
  - Each packet is a *new* packet
  - Much faster
  - Less hardware required
- What's bad about this?

Stateful Firewalls

- Keep a table of all 3-way handshakes
  - Tracks all TCP states
  - Knows who is talking to who
    - And for how long
- What's bad about this?

SYN Flood

- Flood a machine with SYN packets
  - Let it take itself down
- Most OSs have some pretty basic protections
  - Delete unanswered SYN-ACKs
- This is a type of denial of service (DoS) attack

hping3

- Network tool able to send custom TCP/IP packets and to display target replies like ping program does with ICMP replies
- Test firewall rules
- Advanced port scanning
- Test net performance using different protocols,
- packet size, TOS (type of service) and fragmentation.å

hping3

- hping3 <destination>
  - a <source>
    (spoofs the source)
  - S
    (sets the SYN flag)
  - -p 80
    (Port 80
  - -i u1
    (send every microsecond)

Activity: Syn Flood