Defending Computer Networks
Lecture 11: Firewalls and DDOS

Stuart Staniford

Adjunct Professor of Computer Science

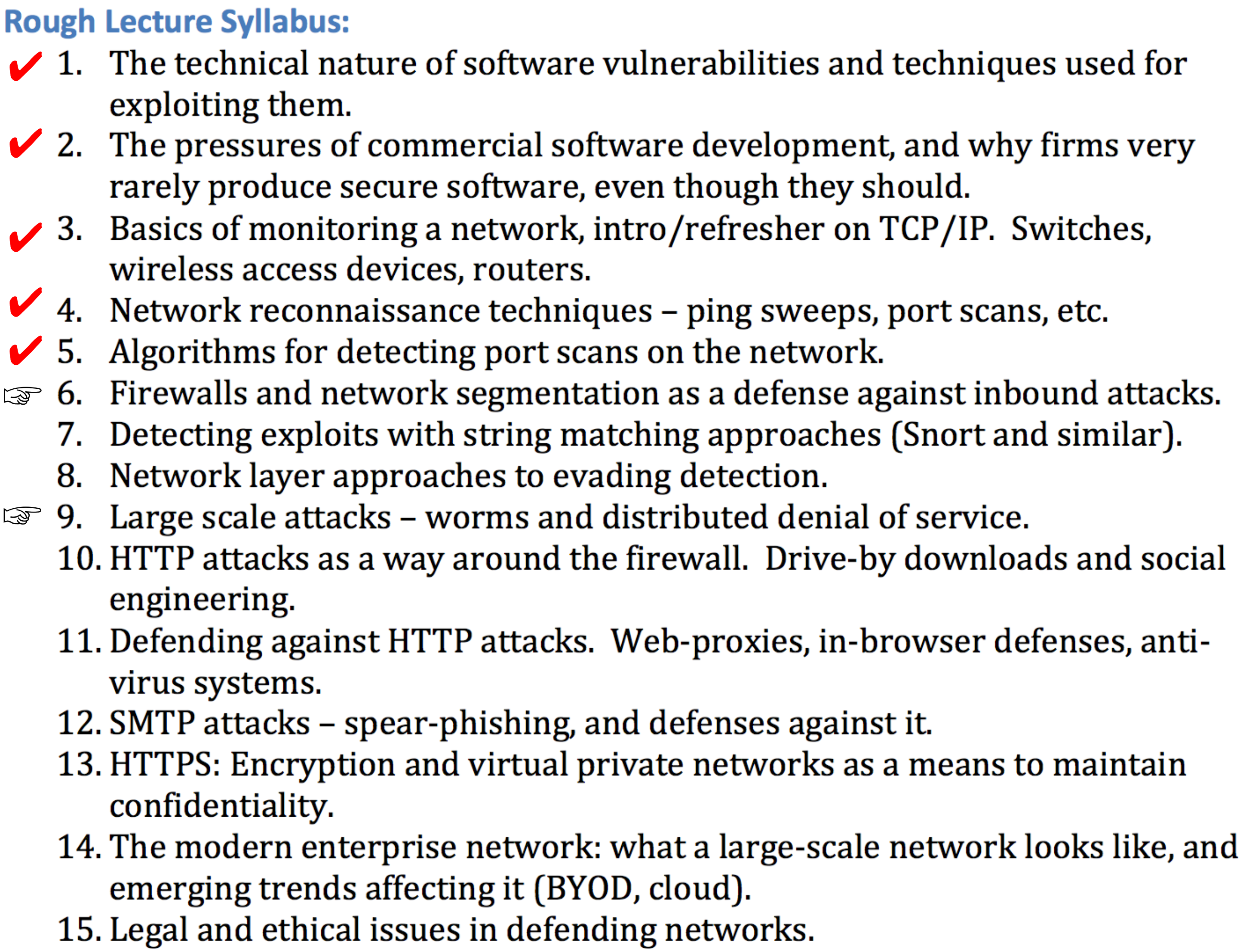
Logistics

- October 8th: Cornell ITSO office guest lecture
  - Wyman Miles/Glenn Larratt/Dan Valenti
  - Plan to formalize class project options that day also
- HW2 Due Tomorrow

Assigned Reading

- Paxson, *An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks*
  - http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.20.7882&rep=rep1&type=pdf

Where We Are in Syllabus



Rough Lecture Syllabus:

✓ 1. The technical nature of software vulnerabilities and techniques used for exploiting them.

✓ 2. The pressures of commercial software development, and why firms very rarely produce secure software, even though they should.

✓ 3. Basics of monitoring a network, intro/refresher on TCP/IP. Switches, wireless access devices, routers.

✓ 4. Network reconnaissance techniques – ping sweeps, port scans, etc.

✓ 5. Algorithms for detecting port scans on the network.

☞ 6. Firewalls and network segmentation as a defense against inbound attacks.

7. Detecting exploits with string matching approaches (Snort and similar).

8. Network layer approaches to evading detection.

☞ 9. Large scale attacks – worms and distributed denial of service.

10. HTTP attacks as a way around the firewall. Drive-by downloads and social engineering.

11. Defending against HTTP attacks. Web-proxies, in-browser defenses, anti-virus systems.

12. SMTP attacks – spear-phishing, and defenses against it.

13. HTTPS: Encryption and virtual private networks as a means to maintain confidentiality.

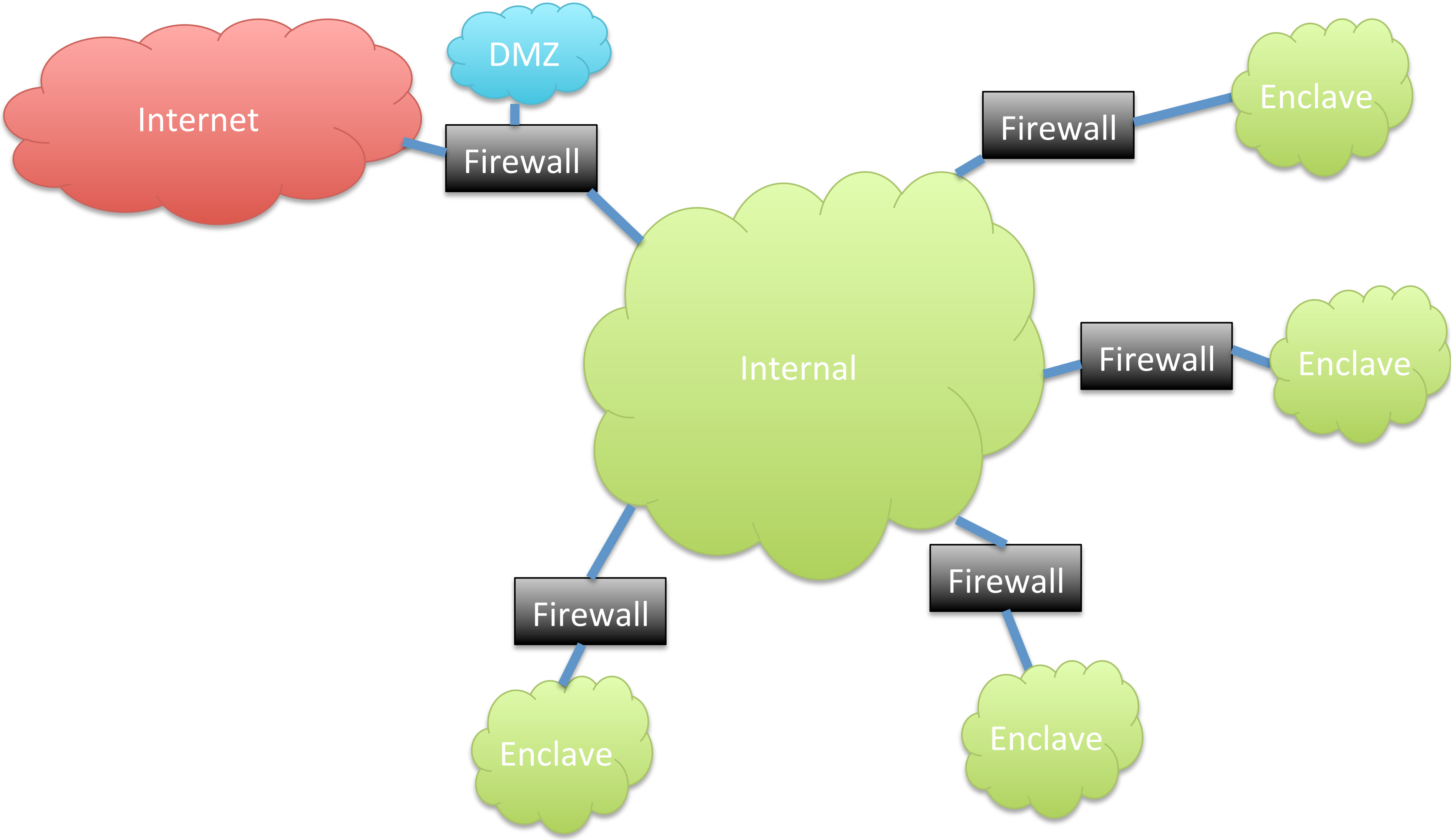
14. The modern enterprise network: what a large-scale network looks like, and emerging trends affecting it (BYOD, cloud).

15. Legal and ethical issues in defending networks.

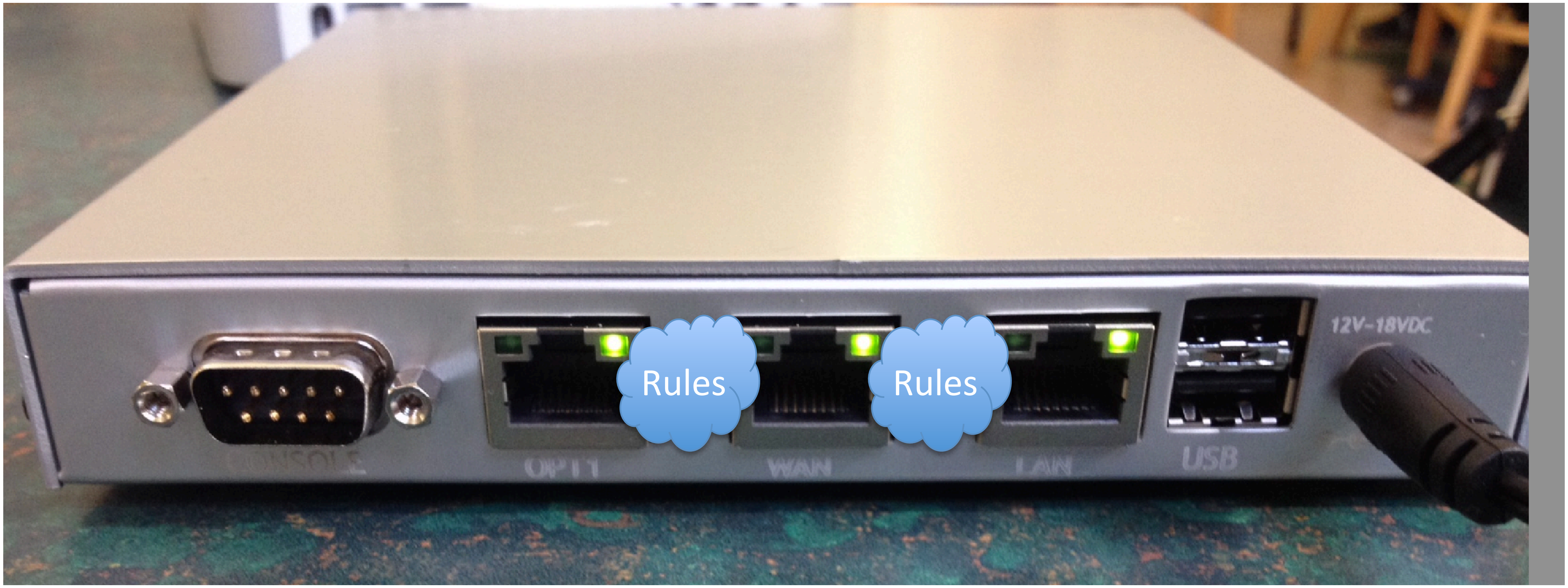
Main Goals for Today

- Finish up firewalls.
- DDOS

Firewall Setup



Firewall Basic Concept

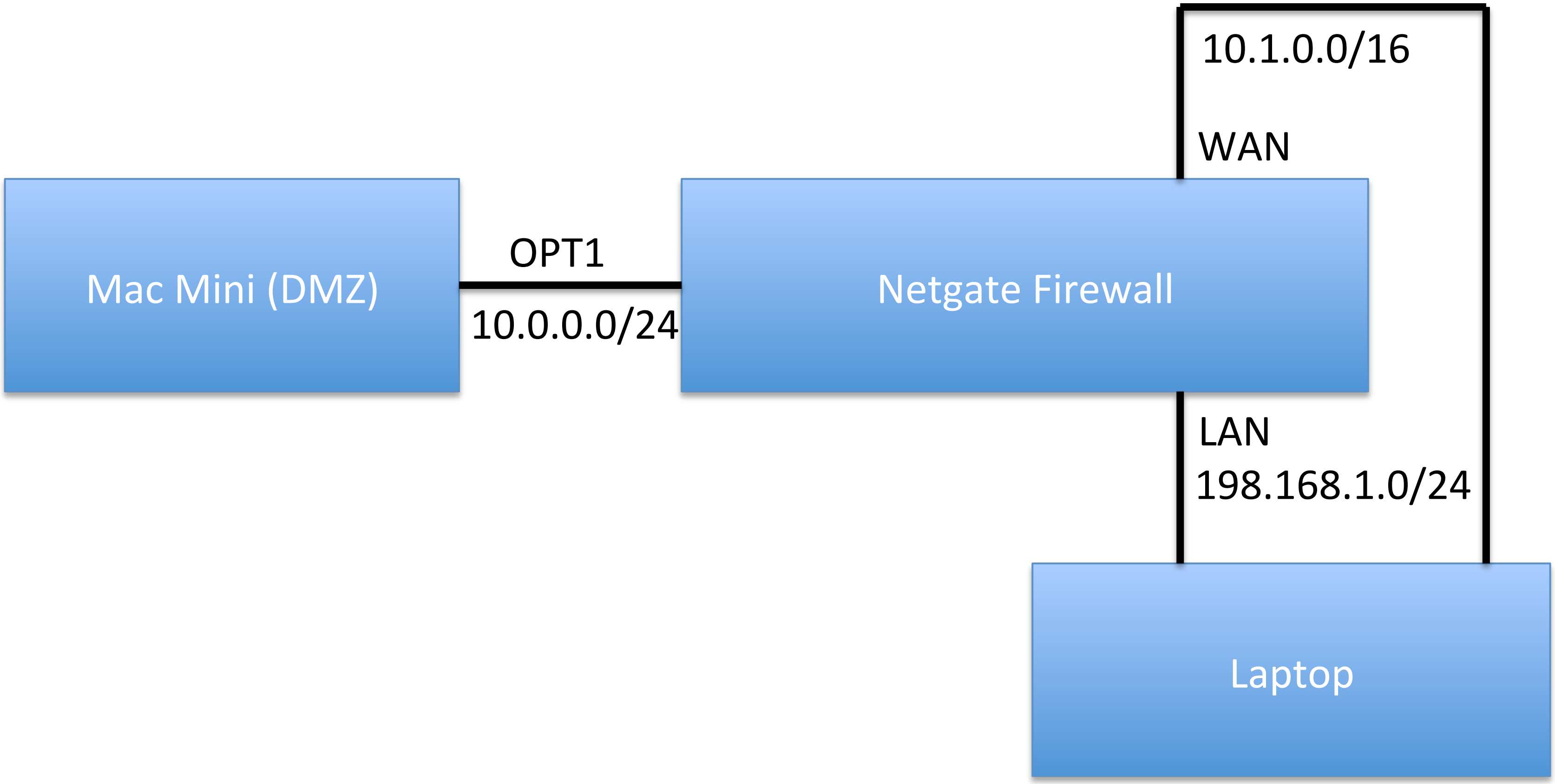


(This is Netgate M1N1Wall – low-cost, low-power open source firewall using FreeBSD/pfSense. Runs on AMD Geode cpu.)

Typical Firewall Rule

- Block in on LAN from 192.168.1.0/24 port any to 0.0.0.0/0 port 53
  - Any packets coming from LAN to port 53 will be dropped.
    - Effect of rule in isolation
    - Could be part of strategy to force clients to use only officially sanctioned DNS servers

Firewall Demo Wiring Diagram



Tour of a Firewall GUI

- Dashboard
  - Let’s check basic setup
    - Check IP addresses on laptop match
    - Dashboard
    - Routes correct
    - Make sure we can ping Mac Mini from firewall
    - Check arp table
    - Make sure we can ping Mac Mini from LAN network.
    - Have a quick look at state table

Firewall Rules

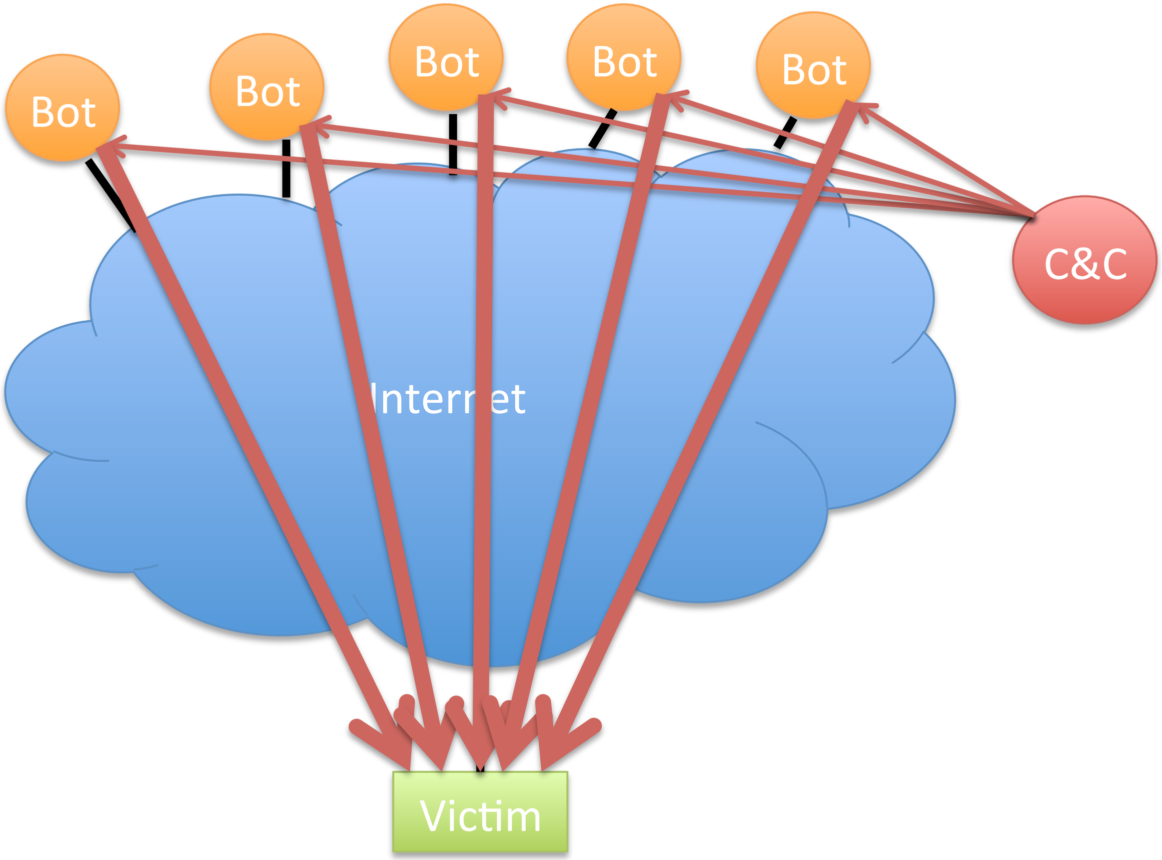
- Inspect the Rules
- Nmap through the firewall from WAN
  - Unplug LAN wire
  - sudo nmap -Pn -n -sS –T5 10.0.0.2
  - Replug LAN wire
- Change a rule
- Nmap through the firewall and see we can no longer see ports
- Inspect the state table in the fw
- Add a rule to reject (reset) connections
  - See how the nmap result changes

5 Minute Break

DDOS – Distributed Denial-Of-Service

- Main goal
  - take out an Internet site ("denial of service")
  - By flooding with bad traffic
  - From many source ("distributed")
- Could also be used on internal network,
  - Not seen much so far, if at all.
  - Obvious cyber-war/cyber-terrorism tactic

Basic Setup of a DDOS Botnet



Illustrative only: practical attacks will have many more bots

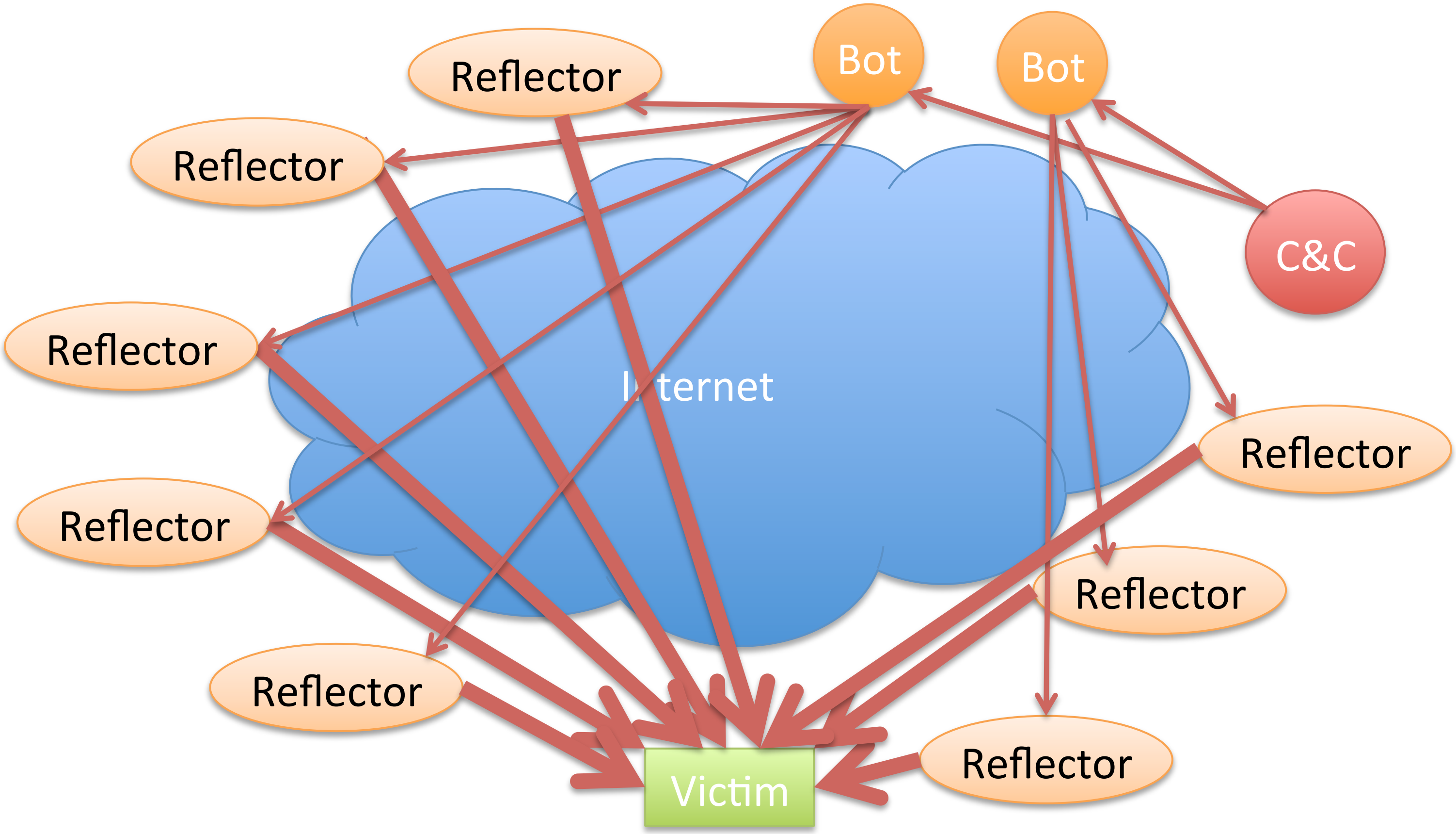
What Packets Should We Send?

- Ping flood
  - ICMP echo request
- Syn flood
  - Exploit limitations in handling of half-open connections in older stacks
- Genuine looking requests
  - The more genuine and randomized, the harder to block
- Application layer exploits
  - ASLR etc will prevent exploitation, but not crash

Reflectors

- A Reflector is anything that
  - If you send it a packet, will respond with pkts
  - Preferably lots of big packets
  - Then send it a packet with src spoofed as the victim
  - Get it to send lots of packets back to the victim
  - Can amplify a DDOS greatly
  - Also makes it harder to trace

Reflection Attacks



Illustrative only: practical attacks will have many more bots/reflectors

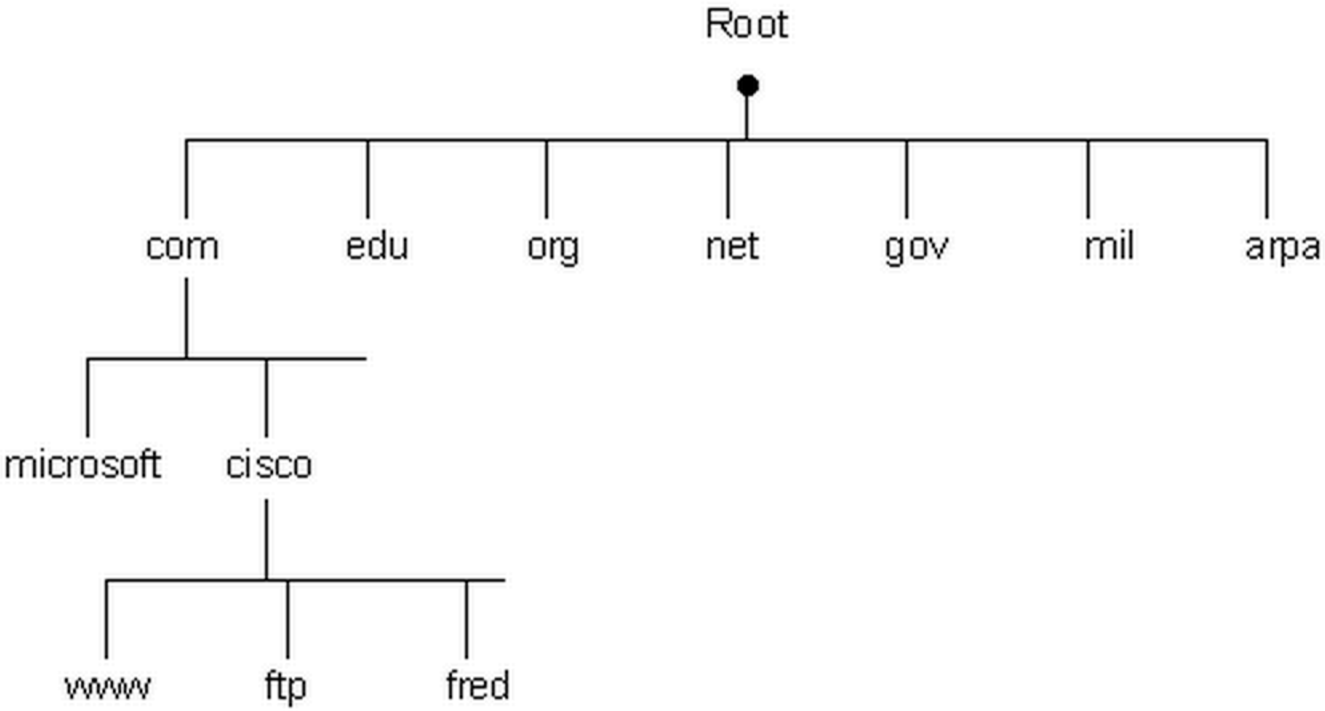
What Will Work as a Reflector?

- Any TCP host (send SA or R in response to S)
- ICMP (eg echo response to echo request)
- DNS – especially with recursion
  - – Issue on campus recently
  - – Let’s look at this in more detail

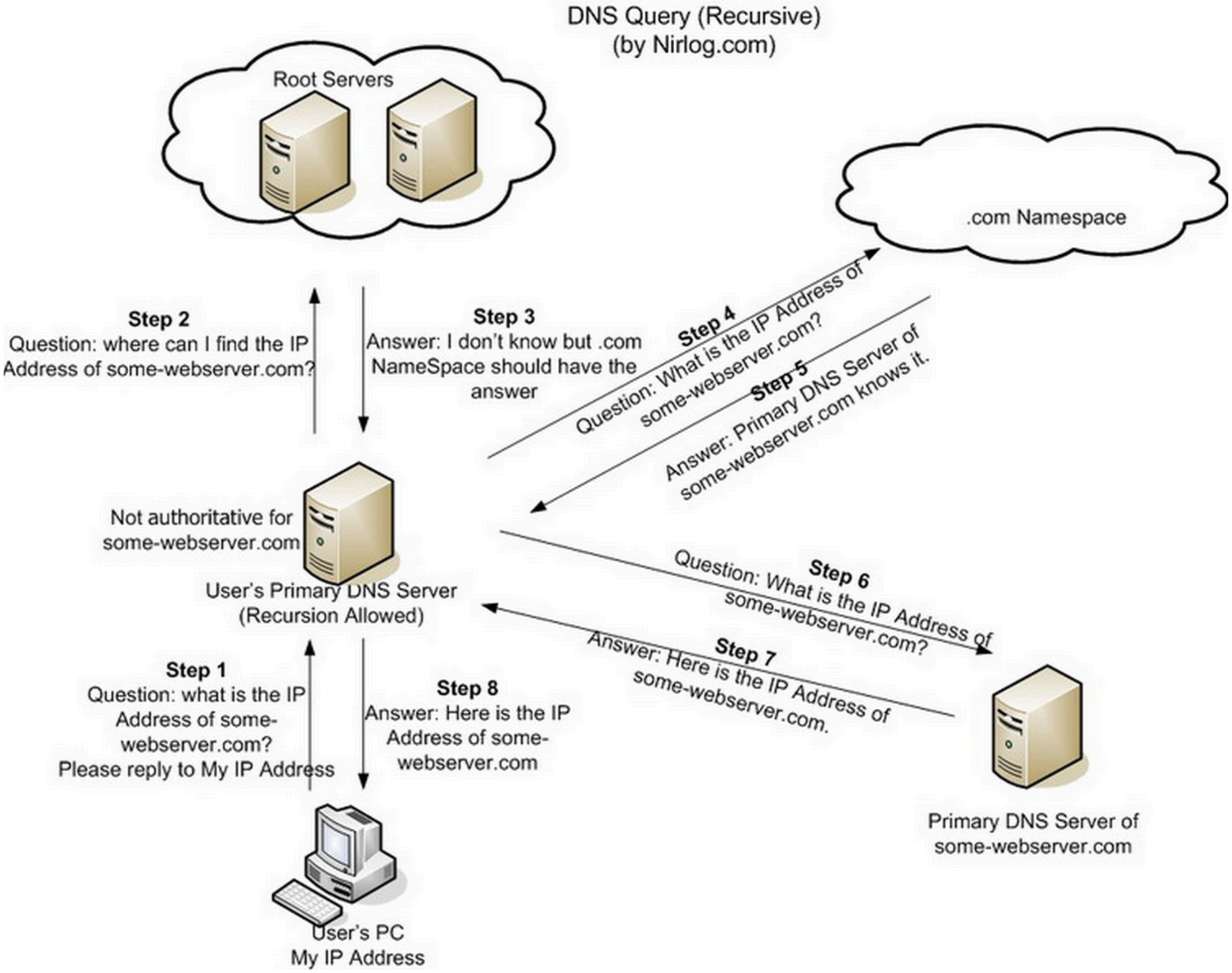
Domain Name Service

- Global Internet service to map names to IP addresses.
- Part of core TCP/IP suite of protocols
  - RFC 882 (1983) updated by RFC 1034 (1987)
  - Replaced manually maintained “hosts.txt” of all Internet connected computer’s IP addresses.
- Let’s do it
  - unplug from fw demo
  - dig www.nytimes.com

The DNS Hierarchical Name Tree



How a DNS Query Works


DNS Query (Recursive)
(by Nirlog.com)
Root Servers
.com Namespace
Step 2
Question: where can I find the IP Address of some-webserver.com?
Step 3
Answer: I don't know but .com NameSpace should have the answer
Step 4
Question: What is the IP Address of some-webserver.com?
Step 5
Answer: Primary DNS Server of some-webserver.com knows it.
Not authoritative for some-webserver.com
User's Primary DNS Server
(Recursion Allowed)
Step 6
Question: What is the IP Address of some-webserver.com?
Step 7
Answer: Here is the IP Address of some-webserver.com.
Step 1
Question: what is the IP Address of some-webserver.com?
Please reply to My IP Address
Step 8
Answer: Here is the IP Address of some-webserver.com
Primary DNS Server of some-webserver.com
User's PC
My IP Address

Credit: http://securitytnt.com/dns-amplification-attack/