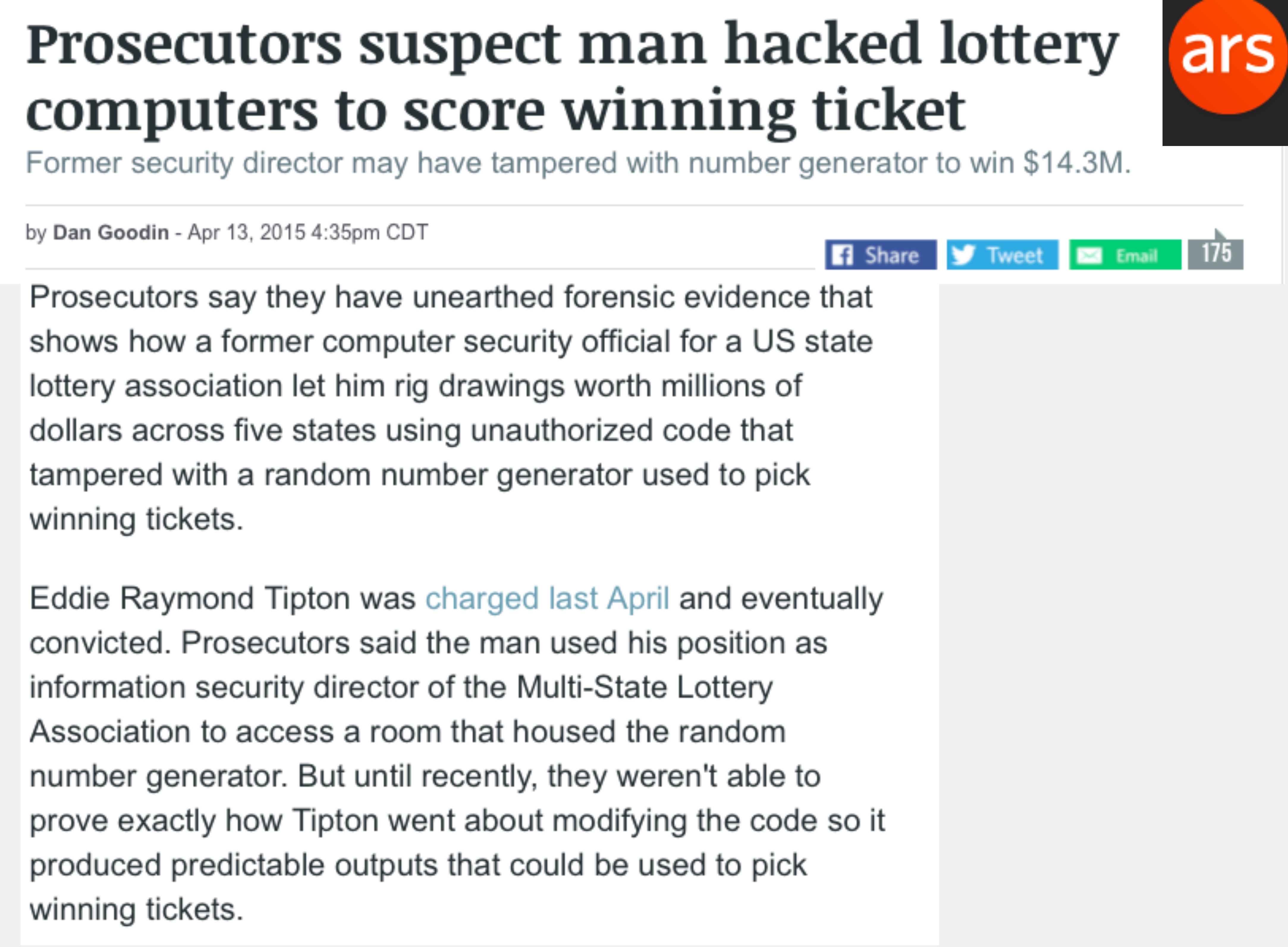


ars technica

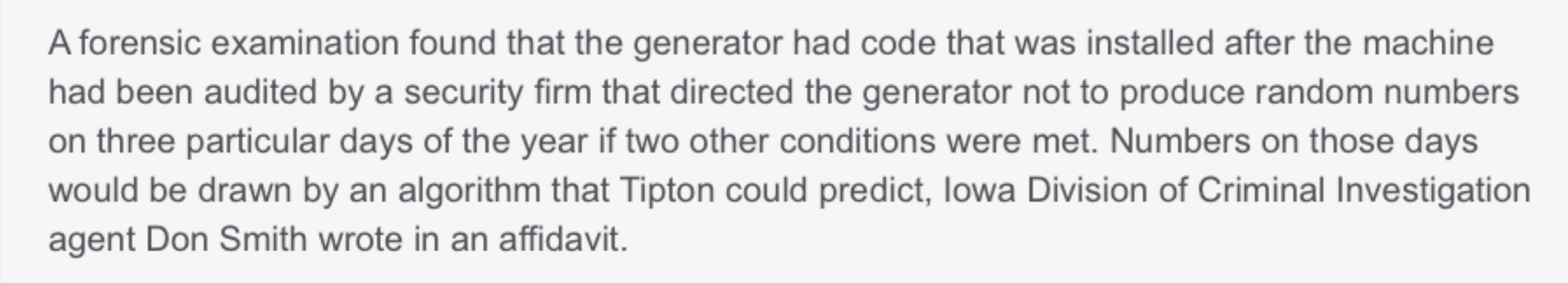
# Prosecutors suspect man hacked lottery computers to score winning ticket

Former security director may have tampered with number generator to win $14.3M.

by **Dan Goodin** - Apr 13, 2015 4:35pm CDT

Prosecutors say they have unearthed forensic evidence that shows how a former computer security official for a US state lottery association let him rig drawings worth millions of dollars across five states using unauthorized code that tampered with a random number generator used to pick winning tickets.

Eddie Raymond Tipton was charged last April and eventually convicted. Prosecutors said the man used his position as information security director of the Multi-State Lottery Association to access a room that housed the random number generator. But until recently, they weren't able to prove exactly how Tipton went about modifying the code so it produced predictable outputs that could be used to pick winning tickets.



> A forensic examination found that the generator had code that was installed after the machine had been audited by a security firm that directed the generator not to produce random numbers on three particular days of the year if two other conditions were met. Numbers on those days would be drawn by an algorithm that Tipton could predict, Iowa Division of Criminal Investigation agent Don Smith wrote in an affidavit.

# network security

cs642

computer security

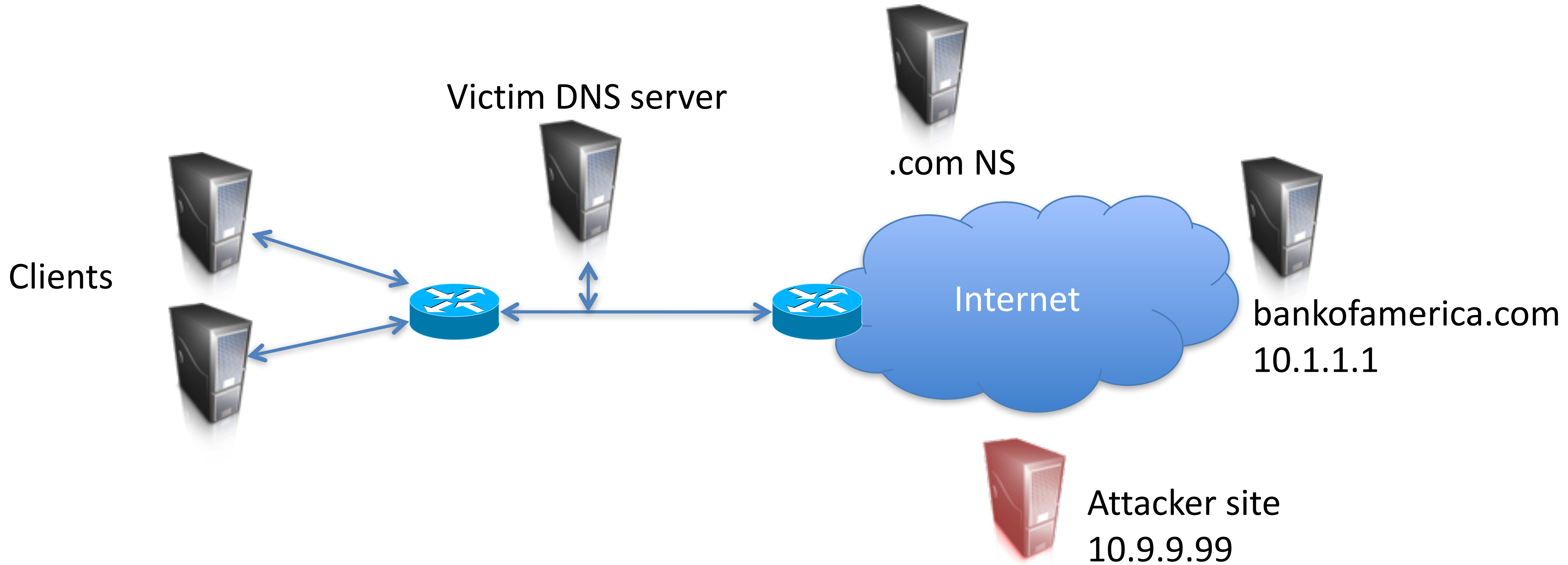
adam everspaugh

ace@cs.wisc.edu

# today

- **Reminder:** HW3 due in one week: April 18, 2016
- CIDR addressing
- Border Gateway Protocol
- Network reconnaissance via nmap
- Idle scans

# DNS cache poisoning



How might an attacker do this?

What security features must an attacker overcome?

- Packet spoofing ← Assume SRC port spoofing
- Guess UDP port ← Assume predictable UDP port
- Guess QID

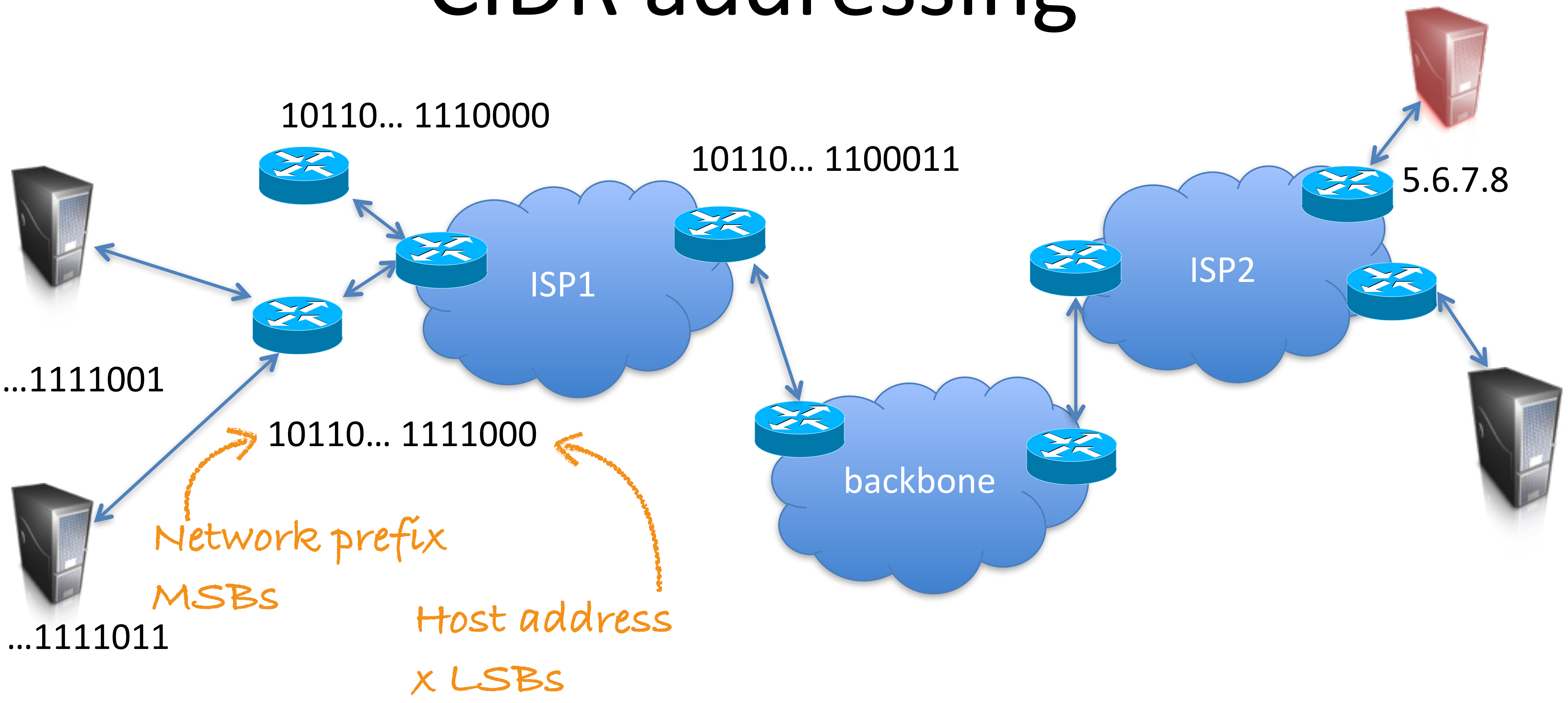
think-*pair*-share

# Phishing is common problem

- Typo squatting:
  - www.LansdEnd.com
  - www.goggle.com
  - secure.bank0fAmerica.com
  - wíkipedia.org
- Phishing attacks
  - Trick users into thinking a malicious domain name is the real one

# *ip routing*

# CIDR addressing

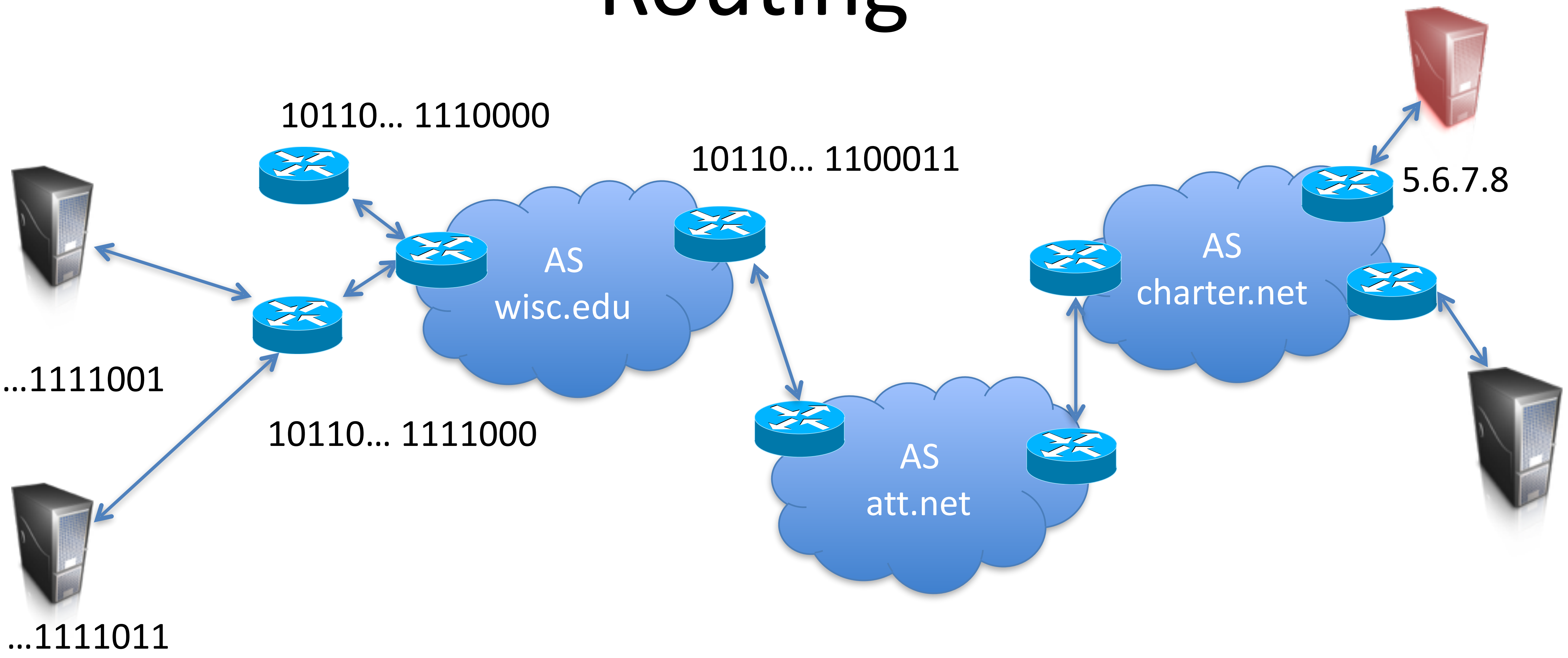


Classless inter-domain routing (CIDR)

Prefixes used to setup hierarchical routing:

- An organization assigned a.b.c.d/x
- It manages addresses prefixed by a.b.c.d/x

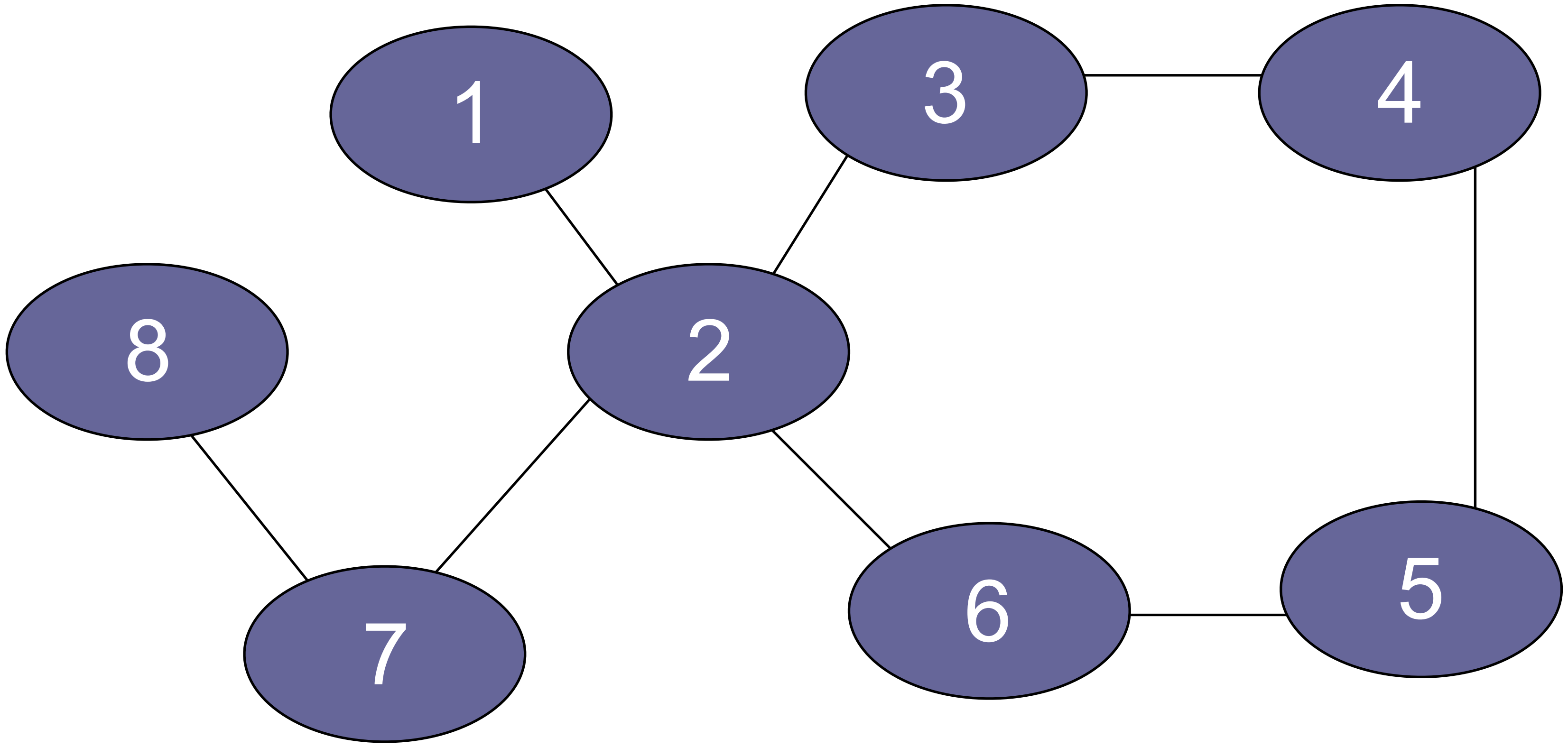
# Routing



**Autonomous systems** (AS) are organizational building blocks

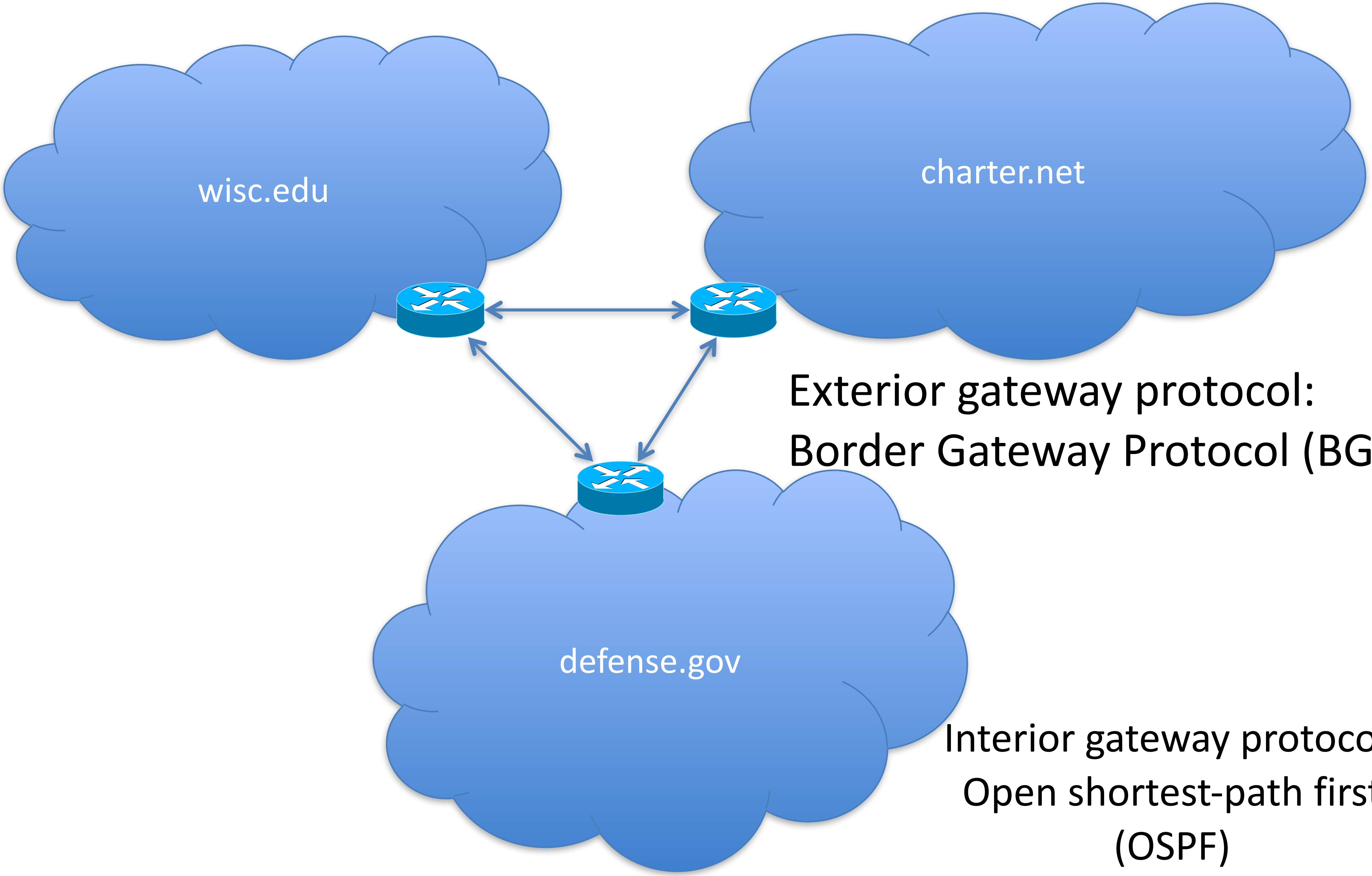
- Collection of IP prefixes under single routing policy
- wisc.edu

# AS Categories



- **Stub:** connected to only on other AS
- **Multi-homed:** connected to multiple other AS
- **Transit:** routes traffic through it's AS for other AS's

# BGP and routing



Exterior gateway protocol:
Border Gateway Protocol (BGP)

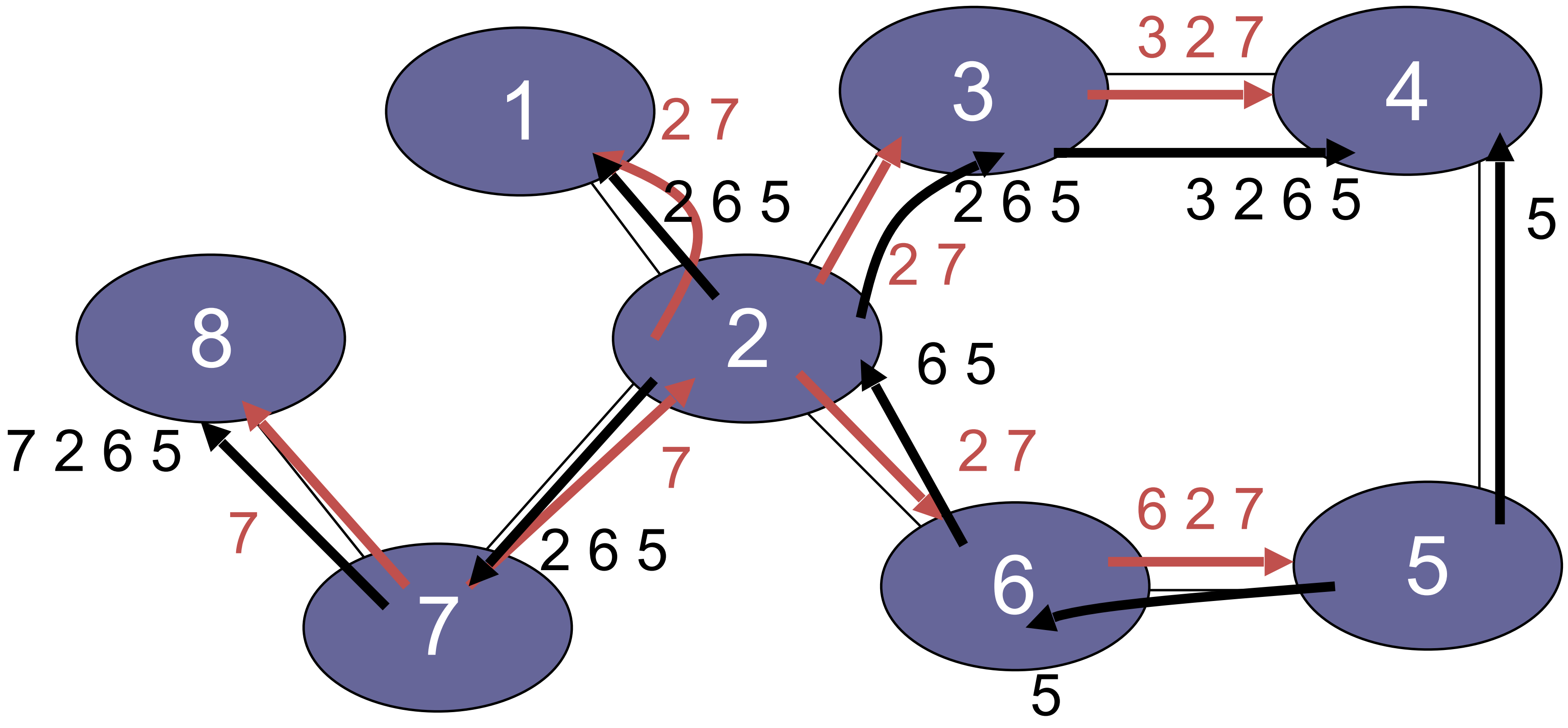
Interior gateway protocol:
Open shortest-path first
(OSPF)
used within an AS

# Border Gateway Protocol (BGP)

- Policy-based routing
  - AS can set policy about how to route
    - economic, security, political considerations
- BGP routers use TCP connections to transmit routing information
- Iterative announcement of routes

# BGP example

[D. Wetherall]



- 2, 7, 3, 6 are Transit AS
- 8, 1 are Stub AS
- 4,5 multihomed AS
- Algorithm seems to work OK in practice
  - BGP does not respond well to frequent node outages

# IP/Route Hijacking

- BGP unauthenticated
  - Anyone can advertise any routes
  - False routes will be propagated
- This allows IP/route hijacking
  - AS announces it originates a prefix it shouldn’t
  - AS announces it has shorter path to a prefix
  - AS announces more specific prefix

# YouTube

- 2008: Pakistan attempts to block YouTube
  - youtube is 208.65.152.0/22
  - youtube.com = 208.65.153.238
- Pakistan ISP advertises 208.65.153.0/24 via BGP
  - more specific, prefix hijacking
- Internet thinks youtube.com is in Pakistan
- Outage resolved in 2 hours…

*reconnaissance*

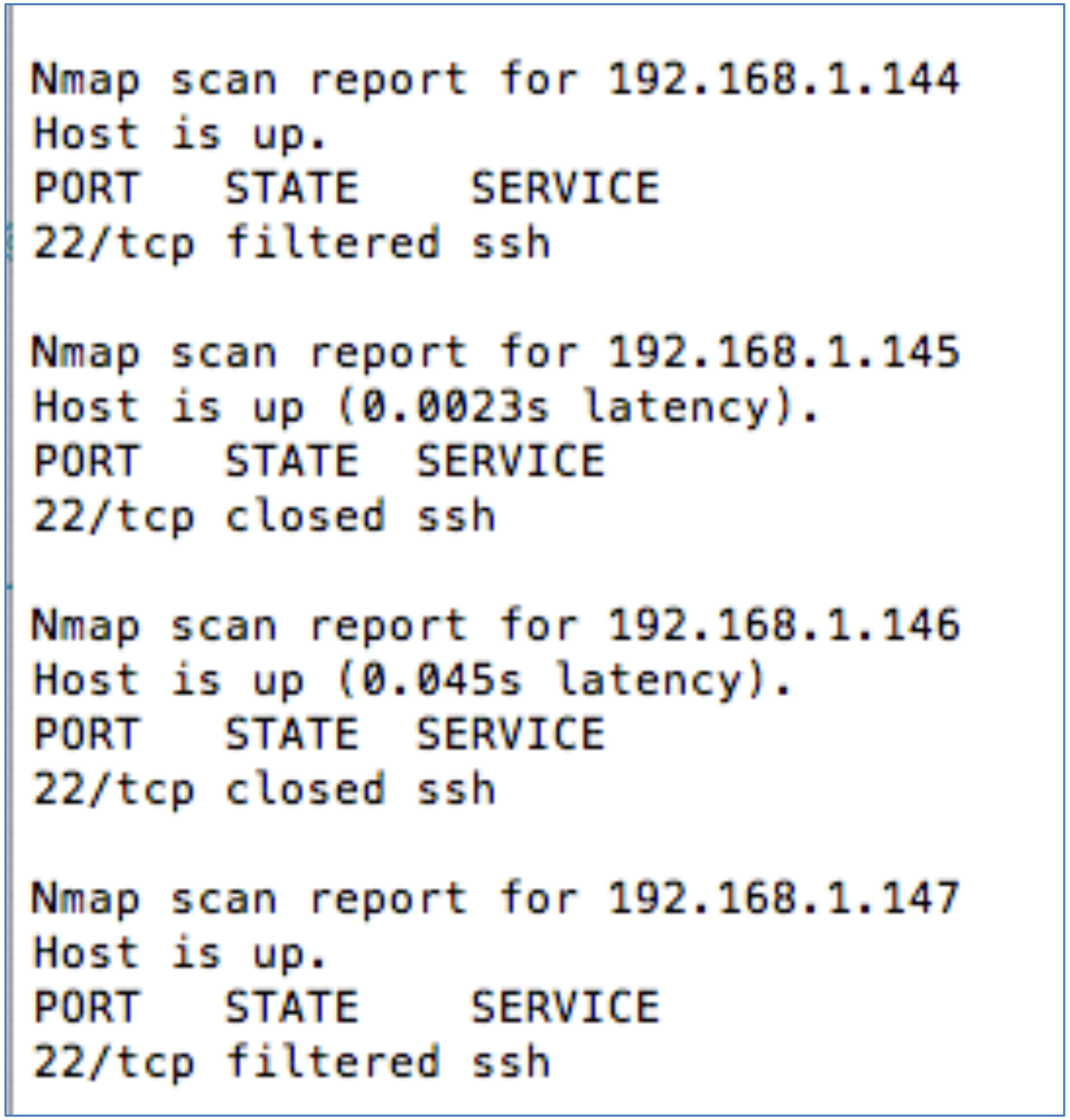
# Port scanning: legality

- United States’ Computer Fraud and Abuse Act (CFAA)
  - Computer system access must be authorized
- Moulton v VC3 (2000).
  - port scanning, by itself, does not create a damages claim (direct harm must be shown to establish damages under the CFAA).
- O. Kerr. “Cybercrime’s scope: Interpreting ’access’ and ’authorization’ in computer misuse statutes”. NYU Law Review, Vol. 78, No. 5, pp. 1596–1668, November 2003.

# NMAP

- Network map tool
- De-facto standard for network reconnaissance, testing
- Numerous built in scanning methods

# nmap –PN –sT –p 22  192.168.1.0/24

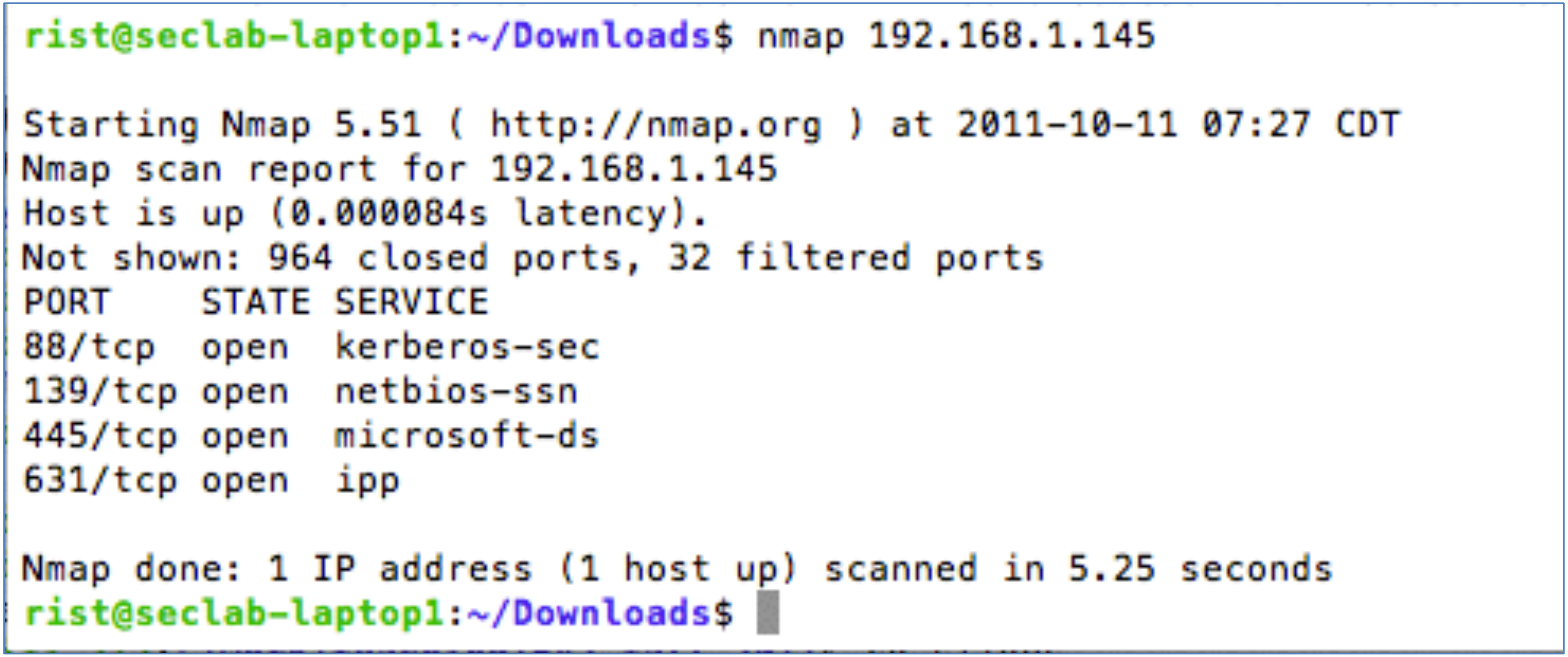


```
Nmap scan report for 192.168.1.144
Host is up.
PORT    STATE    SERVICE
22/tcp filtered ssh

Nmap scan report for 192.168.1.145
Host is up (0.0023s latency).
PORT    STATE  SERVICE
22/tcp closed ssh

Nmap scan report for 192.168.1.146
Host is up (0.045s latency).
PORT    STATE  SERVICE
22/tcp closed ssh

Nmap scan report for 192.168.1.147
Host is up.
PORT    STATE    SERVICE
22/tcp filtered ssh
```

# Some of the NMAP status messages

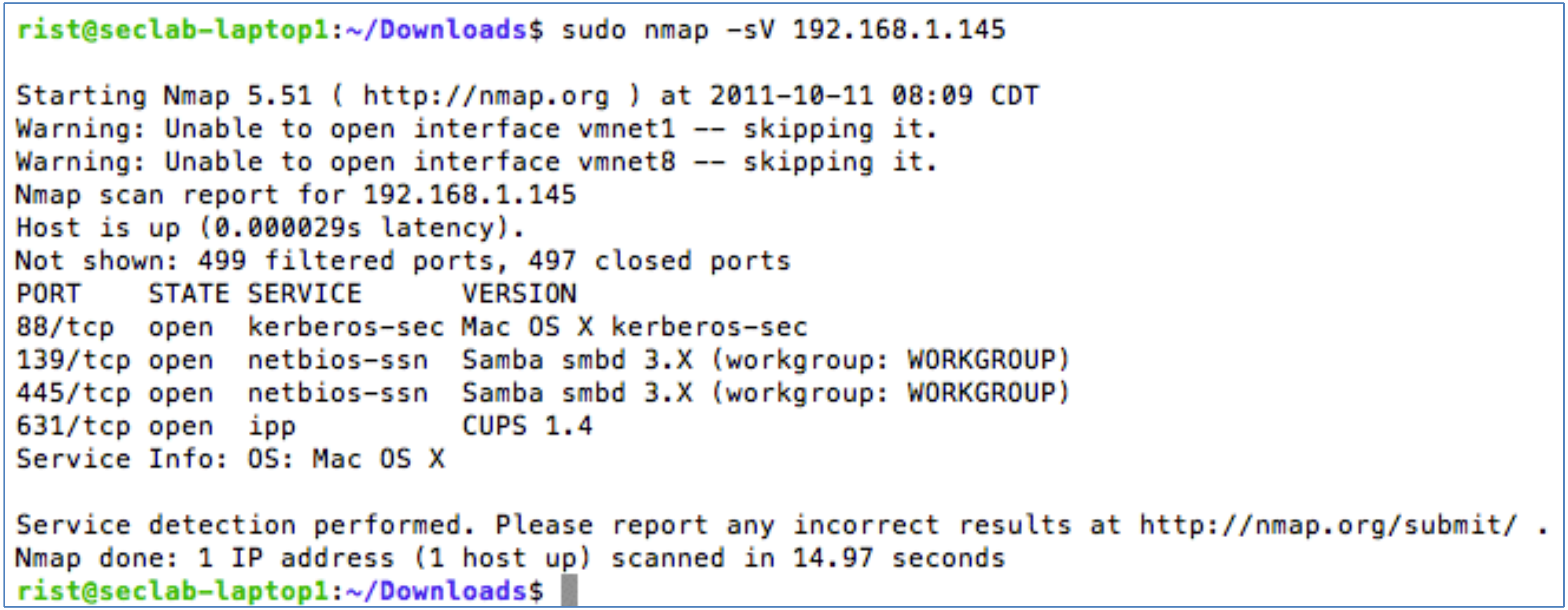
- open
  - host is accepting connections on that port
- closed
  - host responds to NMAP probes on port, but does not accept connections
- filtered
  - NMAP couldn’t get packets through to host on that port.
  - Firewall?

# Port scan of host



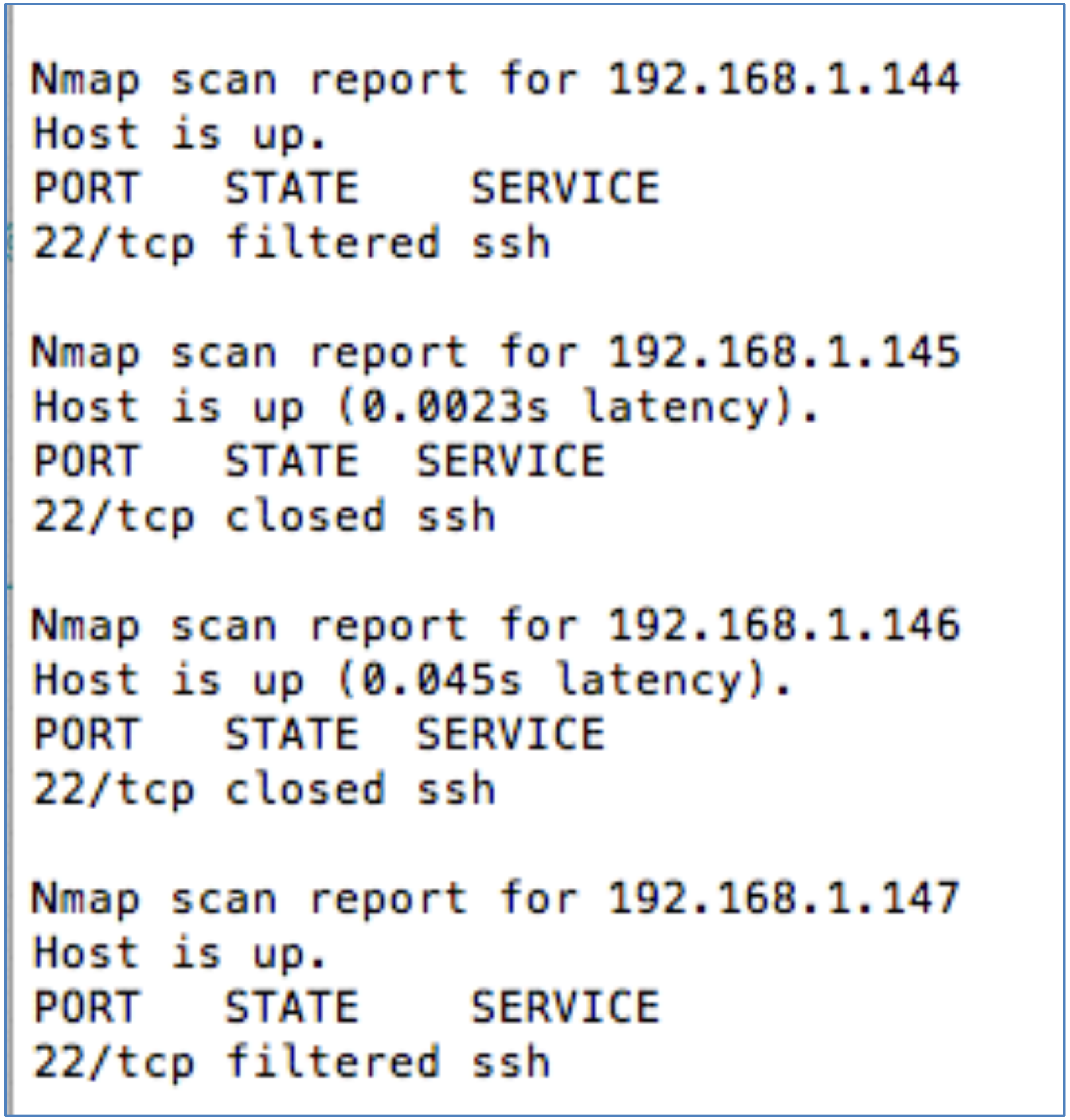
```
rist@seclab-laptop1:~/Downloads$ nmap 192.168.1.145

Starting Nmap 5.51 ( http://nmap.org ) at 2011-10-11 07:27 CDT
Nmap scan report for 192.168.1.145
Host is up (0.000084s latency).
Not shown: 964 closed ports, 32 filtered ports
PORT    STATE SERVICE
88/tcp  open  kerberos-sec
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
631/tcp open  ipp

Nmap done: 1 IP address (1 host up) scanned in 5.25 seconds
rist@seclab-laptop1:~/Downloads$
```

# Service detection



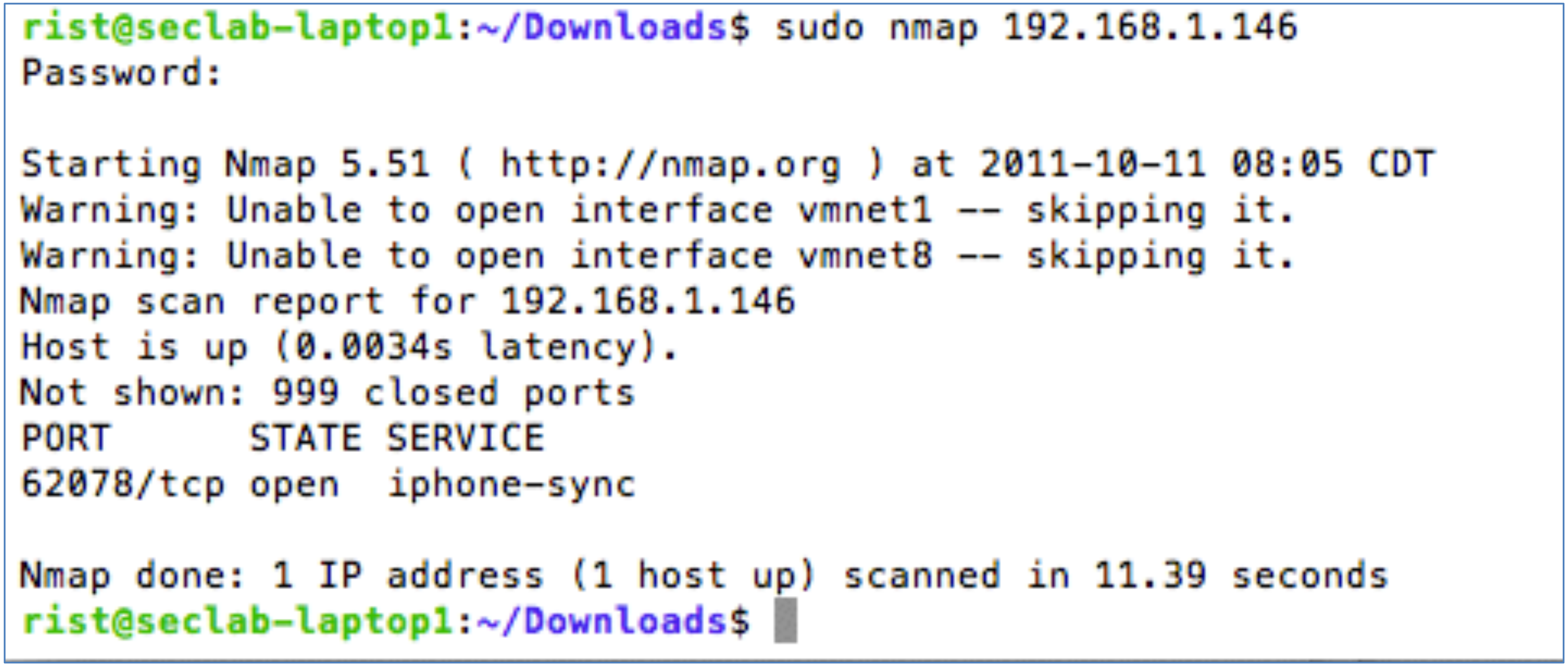
```
rist@seclab-laptop1:~/Downloads$ sudo nmap -sV 192.168.1.145

Starting Nmap 5.51 ( http://nmap.org ) at 2011-10-11 08:09 CDT
Warning: Unable to open interface vmnet1 -- skipping it.
Warning: Unable to open interface vmnet8 -- skipping it.
Nmap scan report for 192.168.1.145
Host is up (0.000029s latency).
Not shown: 499 filtered ports, 497 closed ports
PORT    STATE SERVICE      VERSION
88/tcp  open  kerberos-sec Mac OS X kerberos-sec
139/tcp open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
631/tcp open  ipp          CUPS 1.4
Service Info: OS: Mac OS X

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.97 seconds
rist@seclab-laptop1:~/Downloads$
```

# nmap –PN –sT –p 22  192.168.1.0/24



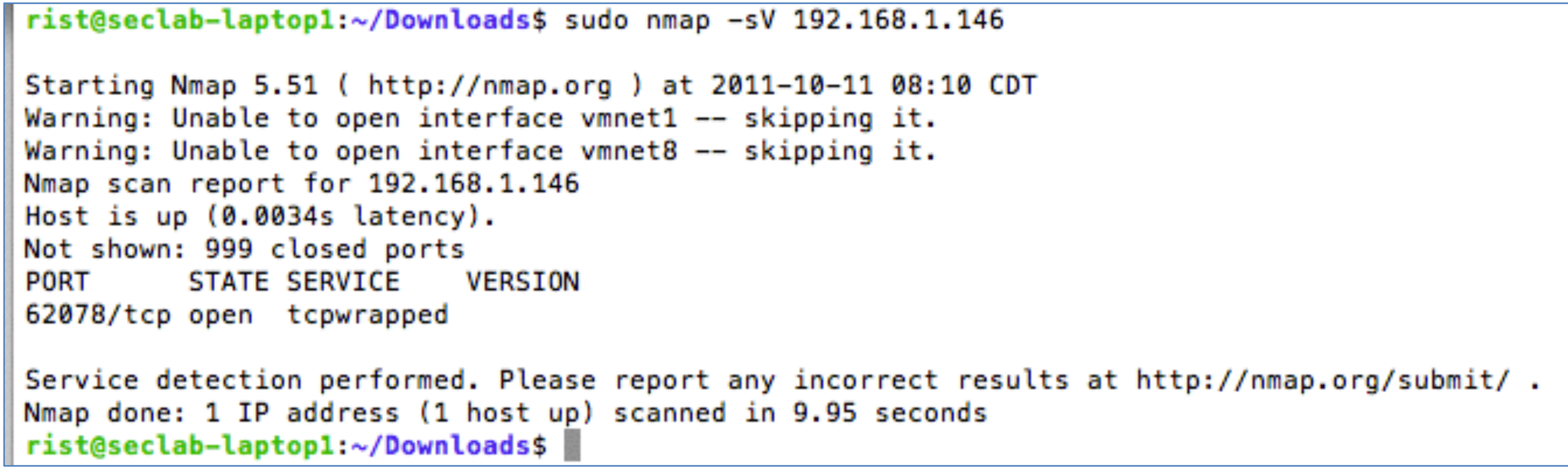
```
Nmap scan report for 192.168.1.144
Host is up.
PORT   STATE    SERVICE
22/tcp filtered ssh

Nmap scan report for 192.168.1.145
Host is up (0.0023s latency).
PORT   STATE  SERVICE
22/tcp closed ssh

Nmap scan report for 192.168.1.146
Host is up (0.045s latency).
PORT   STATE  SERVICE
22/tcp closed ssh

Nmap scan report for 192.168.1.147
Host is up.
PORT   STATE    SERVICE
22/tcp filtered ssh
```

# Port scan of host



```
rist@seclab-laptop1:~/Downloads$ sudo nmap 192.168.1.146
Password:

Starting Nmap 5.51 ( http://nmap.org ) at 2011-10-11 08:05 CDT
Warning: Unable to open interface vmnet1 -- skipping it.
Warning: Unable to open interface vmnet8 -- skipping it.
Nmap scan report for 192.168.1.146
Host is up (0.0034s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
62078/tcp open  iphone-sync

Nmap done: 1 IP address (1 host up) scanned in 11.39 seconds
rist@seclab-laptop1:~/Downloads$ 
```

# Service detection

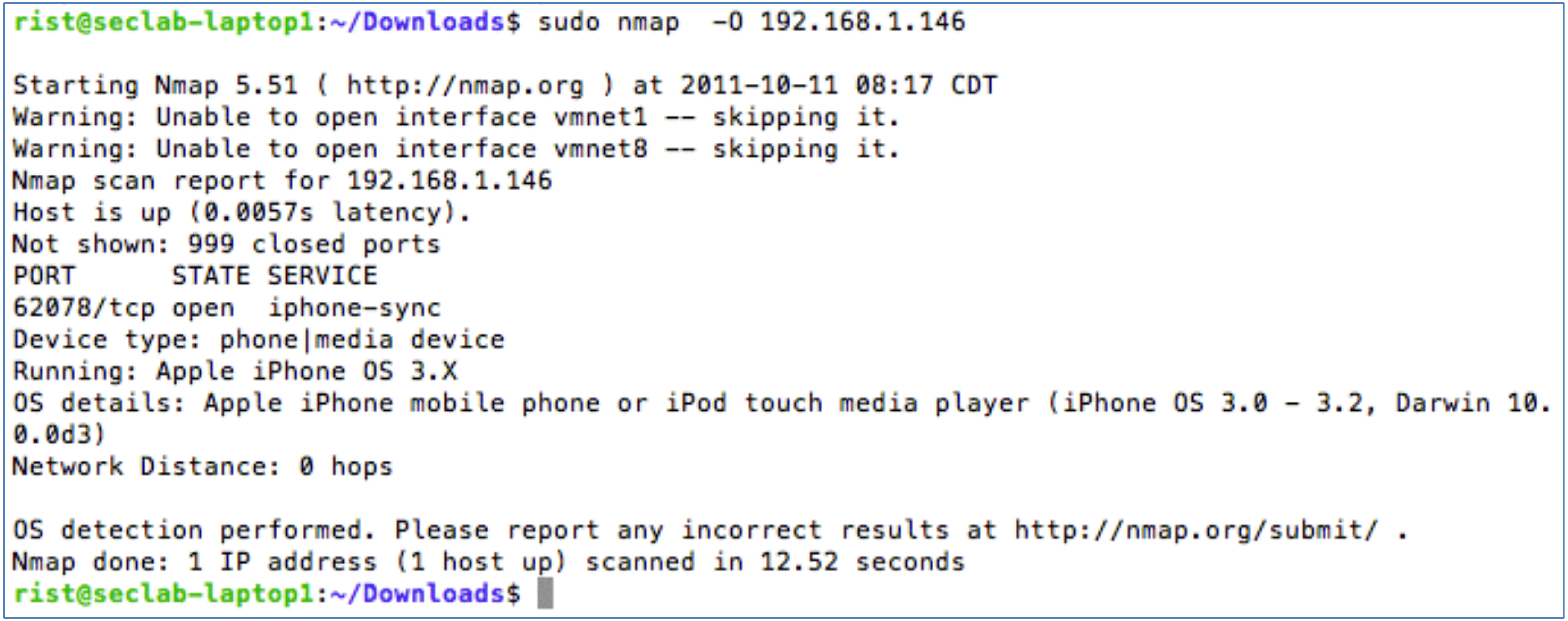


```
rist@seclab-laptop1:~/Downloads$ sudo nmap -sV 192.168.1.146

Starting Nmap 5.51 ( http://nmap.org ) at 2011-10-11 08:10 CDT
Warning: Unable to open interface vmnet1 -- skipping it.
Warning: Unable to open interface vmnet8 -- skipping it.
Nmap scan report for 192.168.1.146
Host is up (0.0034s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE    VERSION
62078/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.95 seconds
rist@seclab-laptop1:~/Downloads$
```

What is tcpwrapped ?

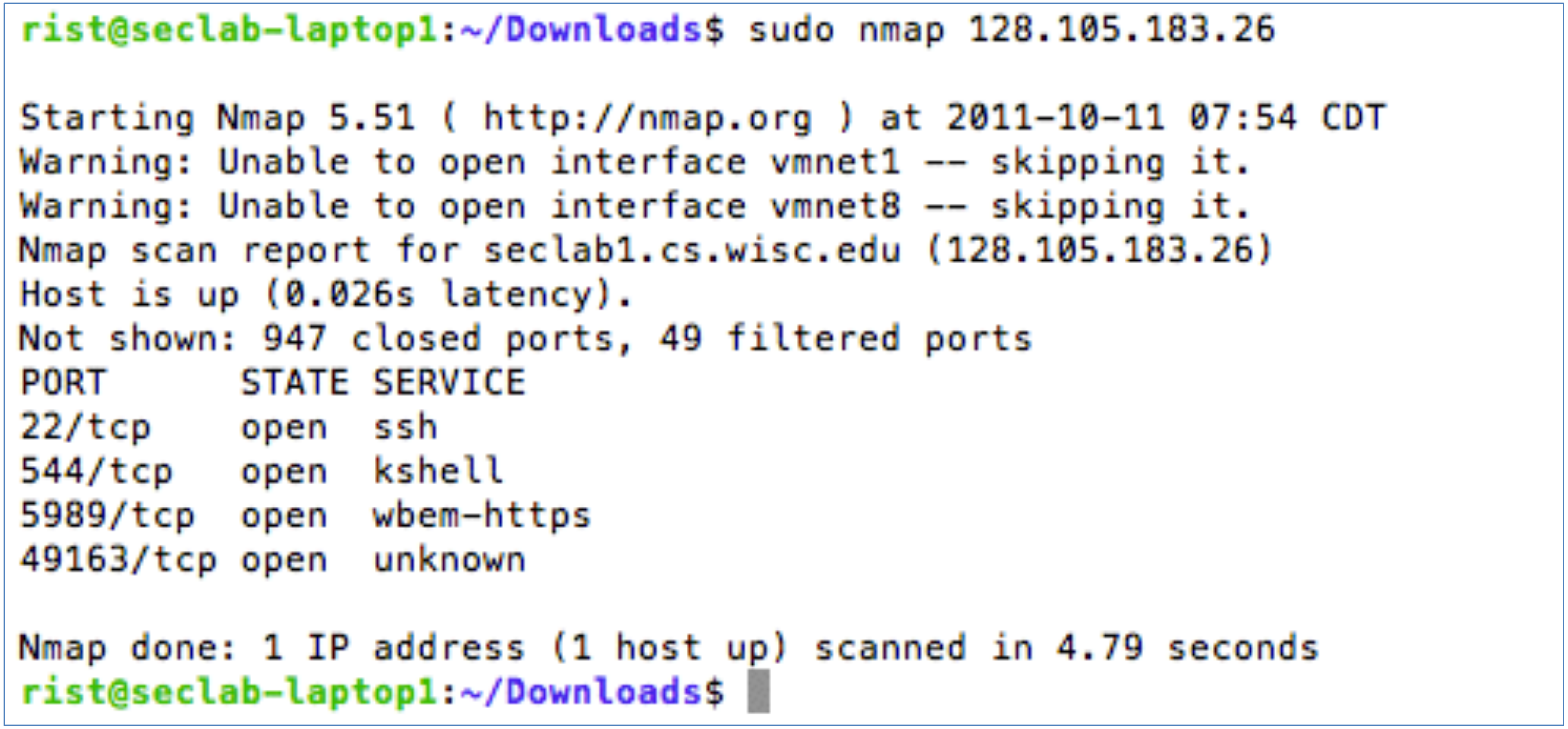
Firewall software
“man tcpd”

# OS fingerprinting



```
rist@seclab-laptop1:~/Downloads$ sudo nmap  -O 192.168.1.146

Starting Nmap 5.51 ( http://nmap.org ) at 2011-10-11 08:17 CDT
Warning: Unable to open interface vmnet1 -- skipping it.
Warning: Unable to open interface vmnet8 -- skipping it.
Nmap scan report for 192.168.1.146
Host is up (0.0057s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
62078/tcp open  iphone-sync
Device type: phone|media device
Running: Apple iPhone OS 3.X
OS details: Apple iPhone mobile phone or iPod touch media player (iPhone OS 3.0 - 3.2, Darwin 10.
0.0d3)
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.52 seconds
rist@seclab-laptop1:~/Downloads$ 
```

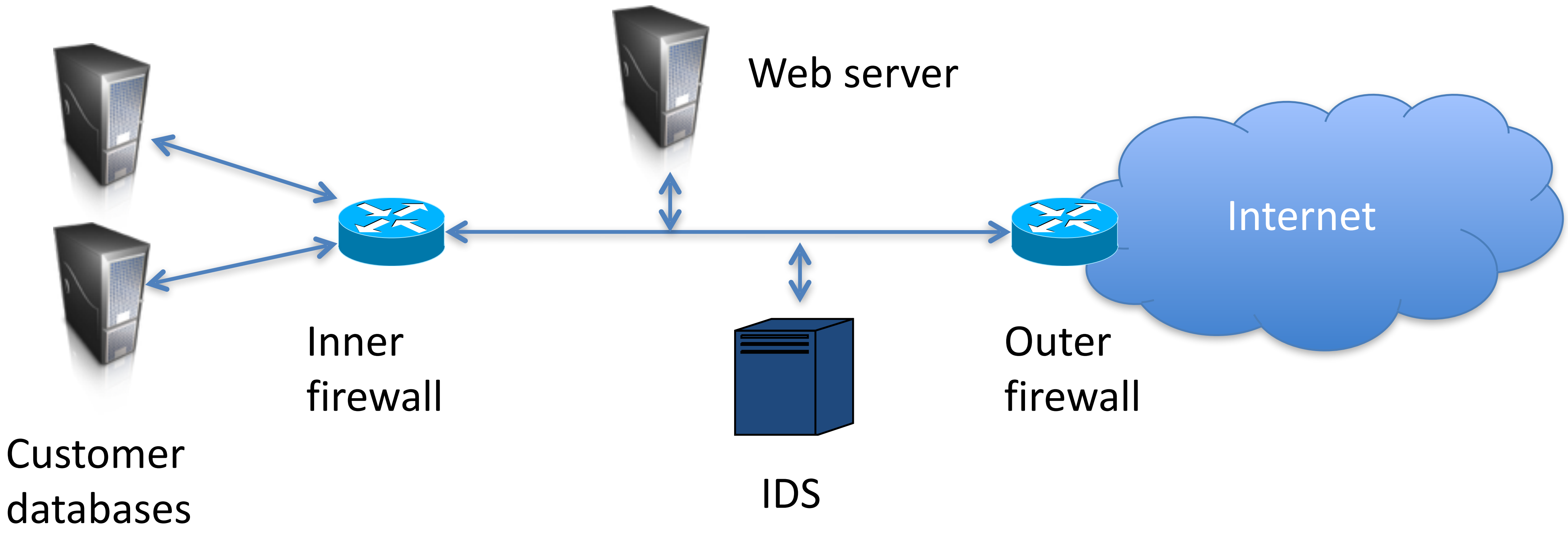
# Another example



```
rist@seclab-laptop1:~/Downloads$ sudo nmap 128.105.183.26

Starting Nmap 5.51 ( http://nmap.org ) at 2011-10-11 07:54 CDT
Warning: Unable to open interface vmnet1 -- skipping it.
Warning: Unable to open interface vmnet8 -- skipping it.
Nmap scan report for seclab1.cs.wisc.edu (128.105.183.26)
Host is up (0.026s latency).
Not shown: 947 closed ports, 49 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
544/tcp   open  kshell
5989/tcp  open  wbem-https
49163/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.79 seconds
rist@seclab-laptop1:~/Downloads$
```

# INTERMISSION

# Network DMZ

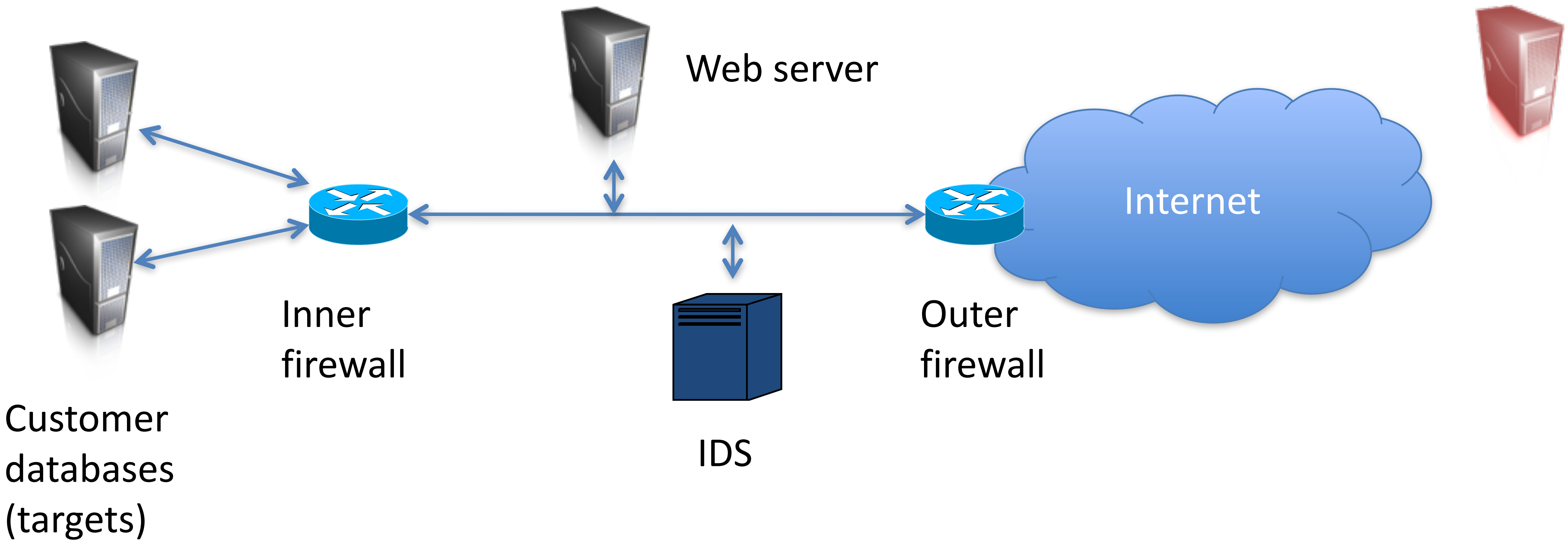


DMZ (demilitarized zone) helps isolate public network components from private network components

Firewall rules to disallow traffic from Internet to internal services

# Idle scans

- Adversary wants to port scan database machine

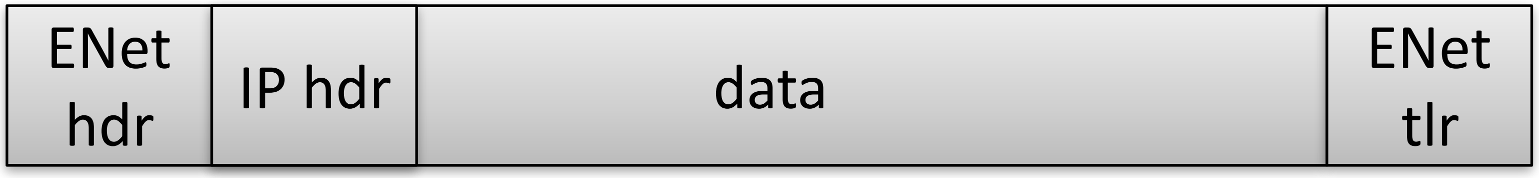


inet => web server OK
inet => databases X
WS => databases OK

# Idle scans

- Adversary wants to port scan database despite firewall/IDS rules
- Salvatore (Antirez) Sanfilippo 1998
- *Idle scan*
  1) Determine IPID of a zombie via SYN/ACK
  2) Send SYN spoofed from zombie
  3) Determine new IPID of zombie via SYN/ACK
- Old systems: IPID incremented with each IP packet sent

# IPv4



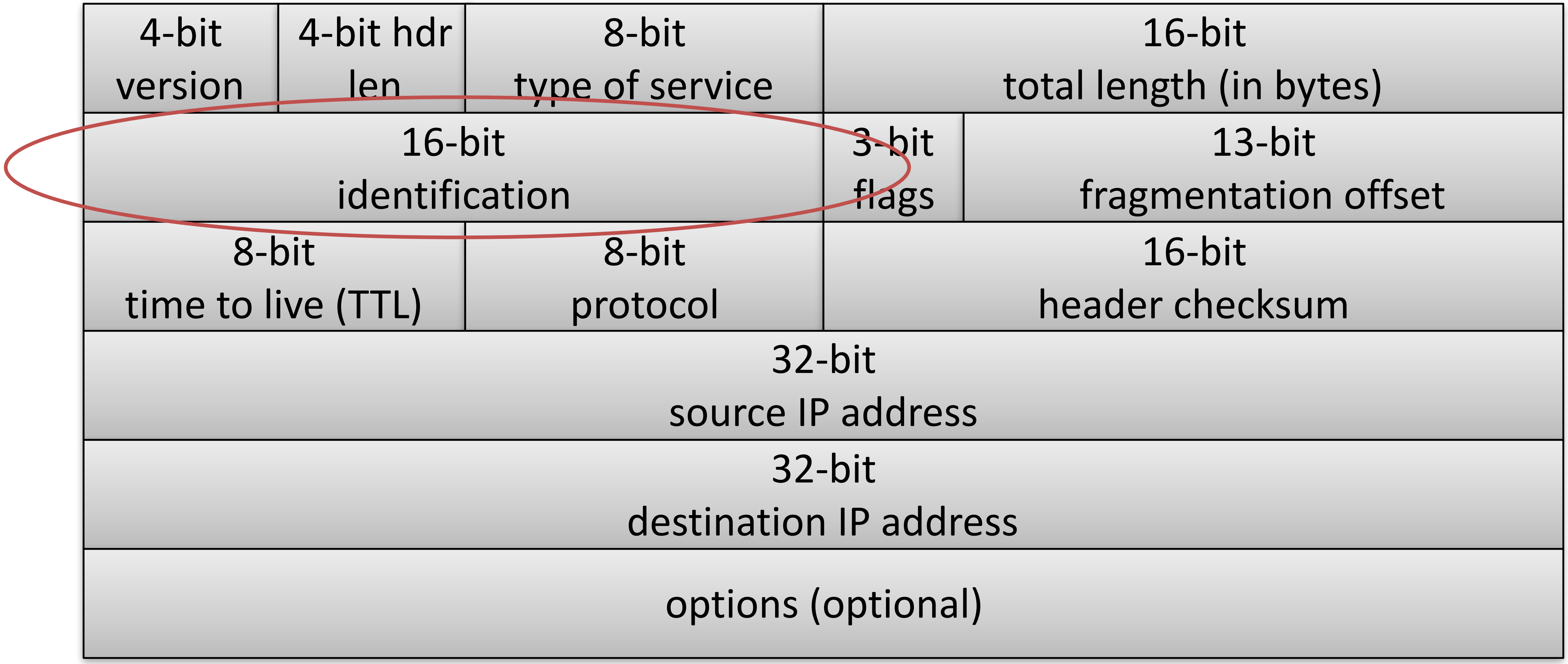
ENet hdr

IP hdr

data

ENet tlr

Ethernet frame
containing
IP datagram



4-bit version

4-bit hdr len

8-bit type of service

16-bit total length (in bytes)

16-bit identification

3-bit flags

13-bit fragmentation offset

8-bit time to live (TTL)

8-bit protocol

16-bit header checksum

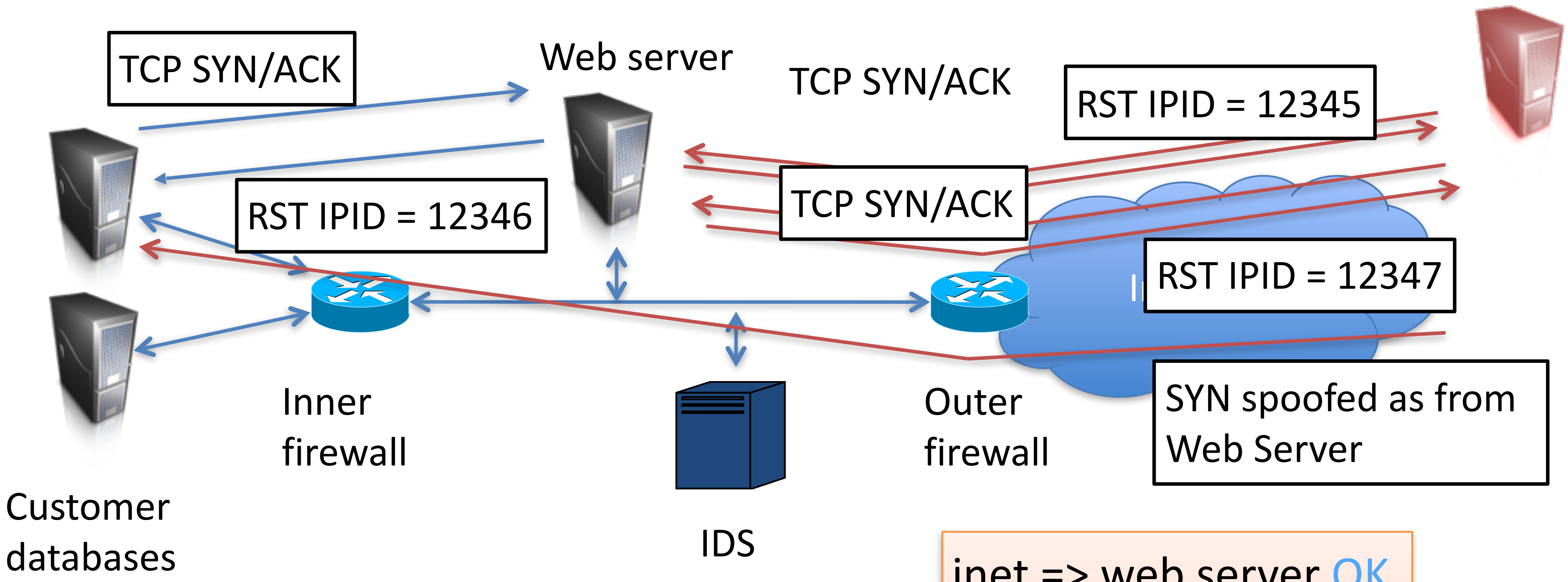
32-bit source IP address

32-bit destination IP address

options (optional)

# Idle scans

- We want to avoid sending any non-spoofed packets to the target, but still want to port scan it



inet => web server OK

inet => databases X

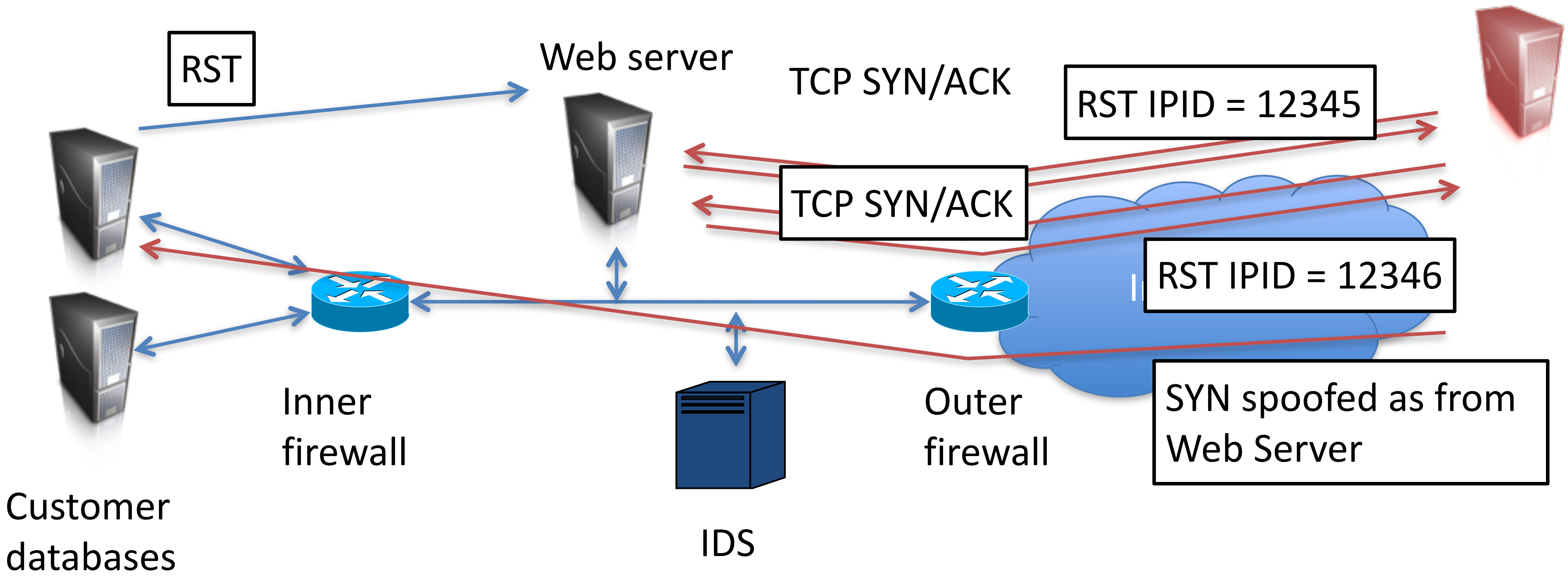
WS => databases OK

If port open final IPID = ??

If port closed final IPID = ??

# Idle scans

- We want to avoid sending any non-spoofed packets to the target, but still want to port scan it



RST

Web server

TCP SYN/ACK

RST IPID = 12345

TCP SYN/ACK

RST IPID = 12346

Inner firewall

Outer firewall

SYN spoofed as from Web Server

Customer databases

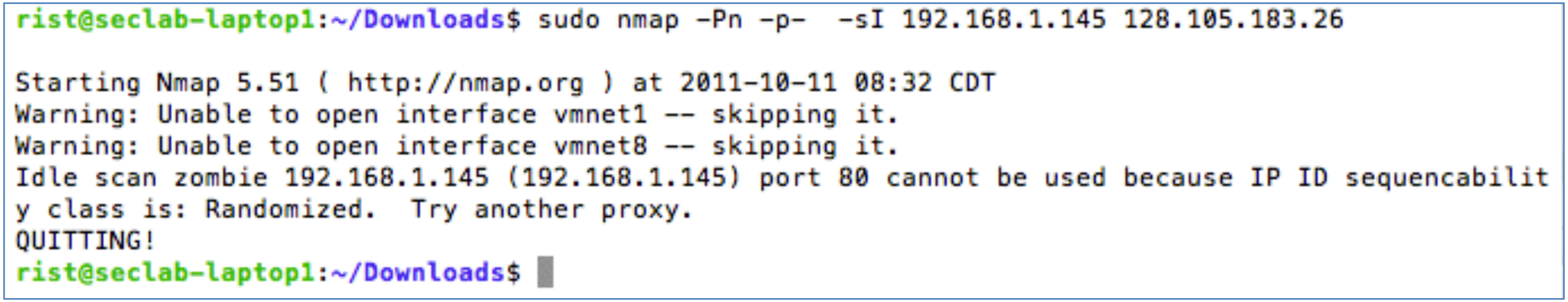
IDS

If port open final IPID = first + 2

If port closed final IPID = first + 1

# Preventing idle scans

- How can we prevent our system from being a zombie?



```
rist@seclab-laptop1:~/Downloads$ sudo nmap -Pn -p-  -sI 192.168.1.145 128.105.183.26

Starting Nmap 5.51 ( http://nmap.org ) at 2011-10-11 08:32 CDT
Warning: Unable to open interface vmnet1 -- skipping it.
Warning: Unable to open interface vmnet8 -- skipping it.
Idle scan zombie 192.168.1.145 (192.168.1.145) port 80 cannot be used because IP ID sequencabilit
y class is: Randomized.  Try another proxy.
QUITTING!
rist@seclab-laptop1:~/Downloads$
```

# recap

- CIDR, BGP
  / IP/route hijacking

- Network reconnaissance
  / scanning, nmap, fingerprinting

- Idle scans, zombie hosts

- Exit slips
  / 1 thing you learned
  / 1 thing you didn't understand