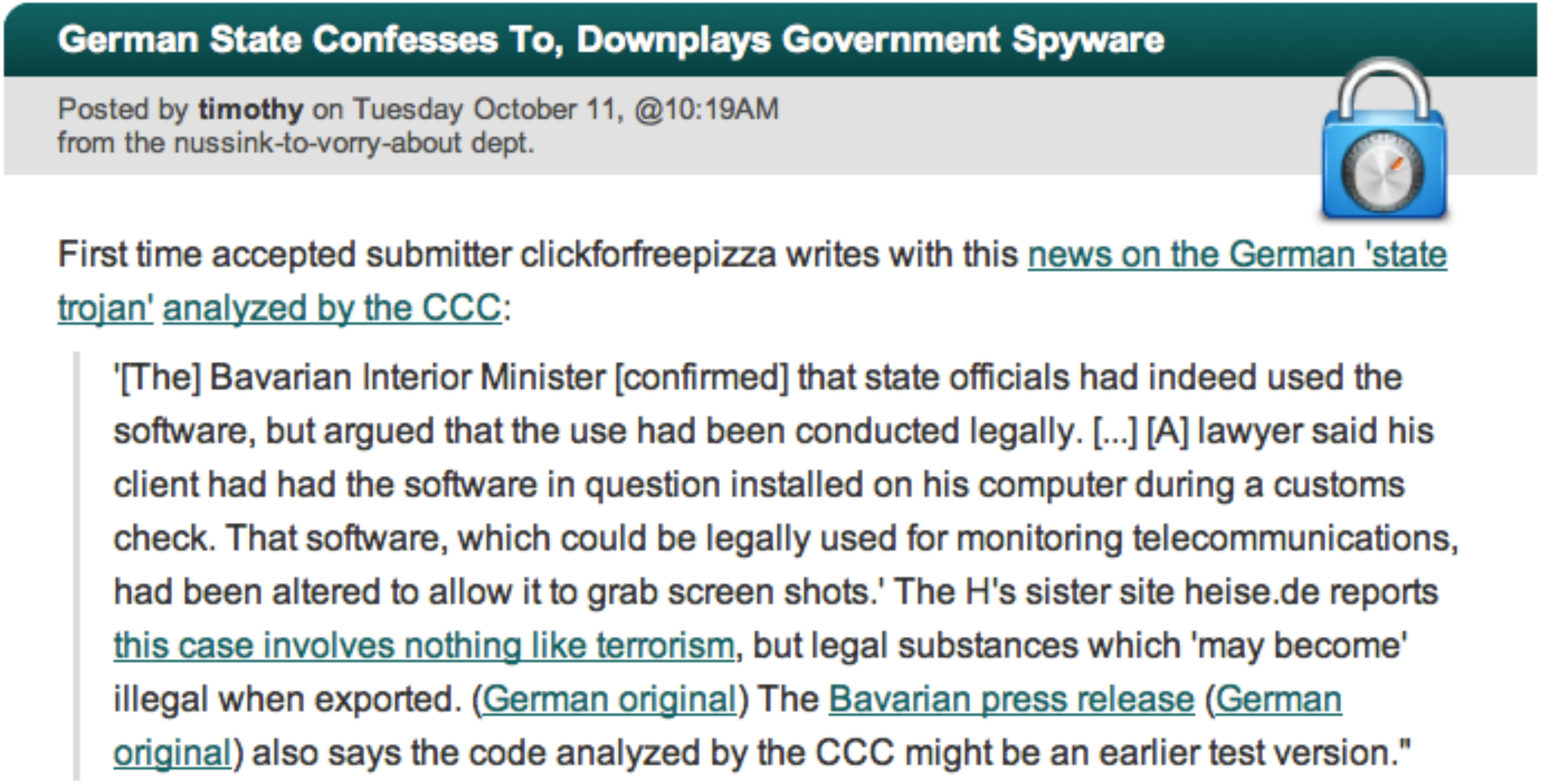
# Network reconnaissance and IDS

# CS642: Computer Security

Professor Ristenpart

http://www.cs.wisc.edu/~rist/

rist at cs dot wisc dot edu

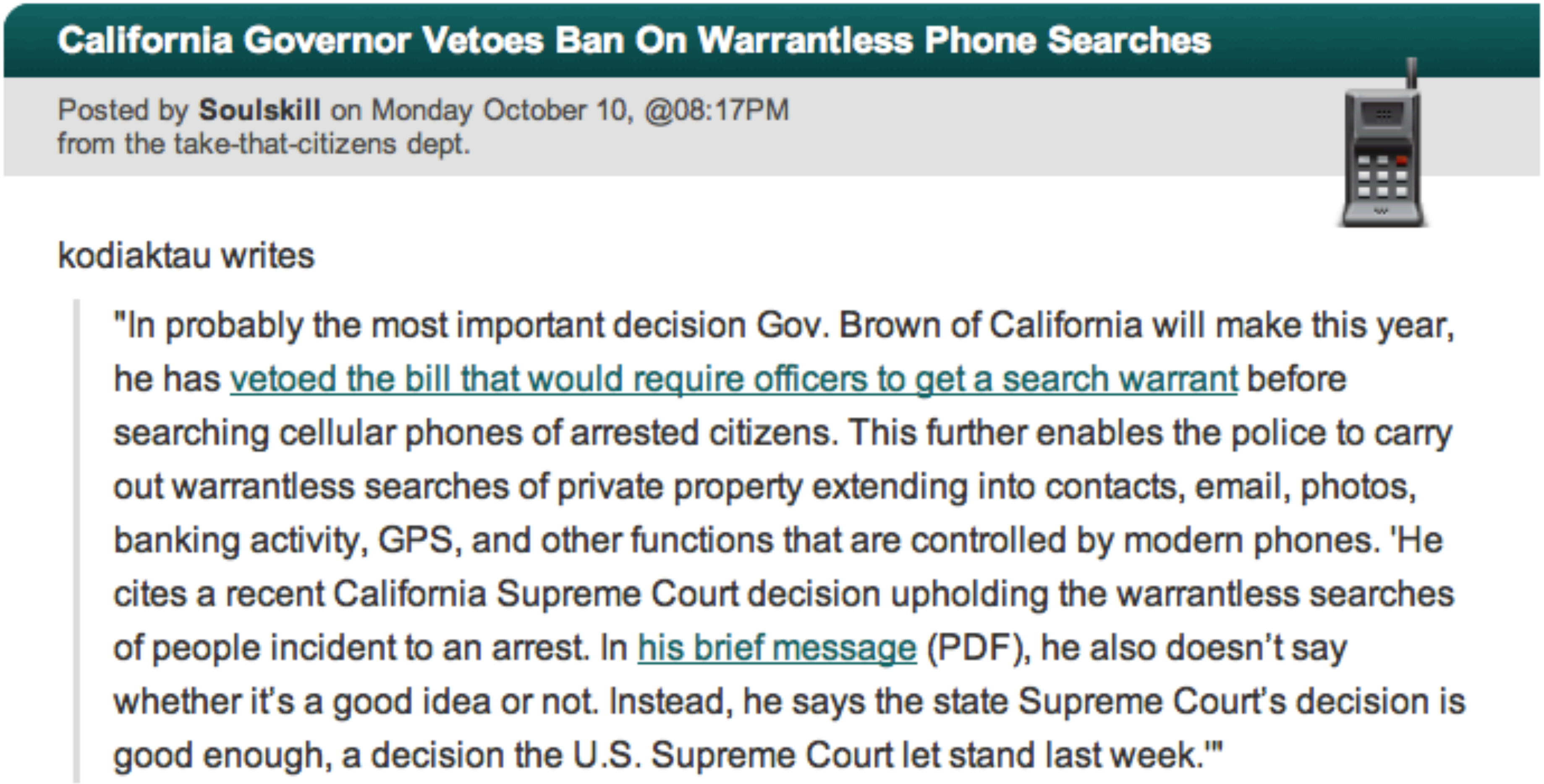


## German State Confesses To, Downplays Government Spyware

Posted by **timothy** on Tuesday October 11, @10:19AM
from the nussink-to-vorry-about dept.

First time accepted submitter clickforfreepizza writes with this news on the German 'state trojan' analyzed by the CCC:

> '[The] Bavarian Interior Minister [confirmed] that state officials had indeed used the software, but argued that the use had been conducted legally. [...] [A] lawyer said his client had had the software in question installed on his computer during a customs check. That software, which could be legally used for monitoring telecommunications, had been altered to allow it to grab screen shots.' The H's sister site heise.de reports this case involves nothing like terrorism, but legal substances which 'may become' illegal when exported. (German original) The Bavarian press release (German original) also says the code analyzed by the CCC might be an earlier test version."



## California Governor Vetoes Ban On Warrantless Phone Searches

Posted by **Soulskill** on Monday October 10, @08:17PM
from the take-that-citizens dept.

kodiaktau writes

> "In probably the most important decision Gov. Brown of California will make this year, he has vetoed the bill that would require officers to get a search warrant before searching cellular phones of arrested citizens. This further enables the police to carry out warrantless searches of private property extending into contacts, email, photos, banking activity, GPS, and other functions that are controlled by modern phones. 'He cites a recent California Supreme Court decision upholding the warrantless searches of people incident to an arrest. In his brief message (PDF), he also doesn't say whether it's a good idea or not. Instead, he says the state Supreme Court's decision is good enough, a decision the U.S. Supreme Court let stand last week.'"

# Let's play over the network …

Target acquisition

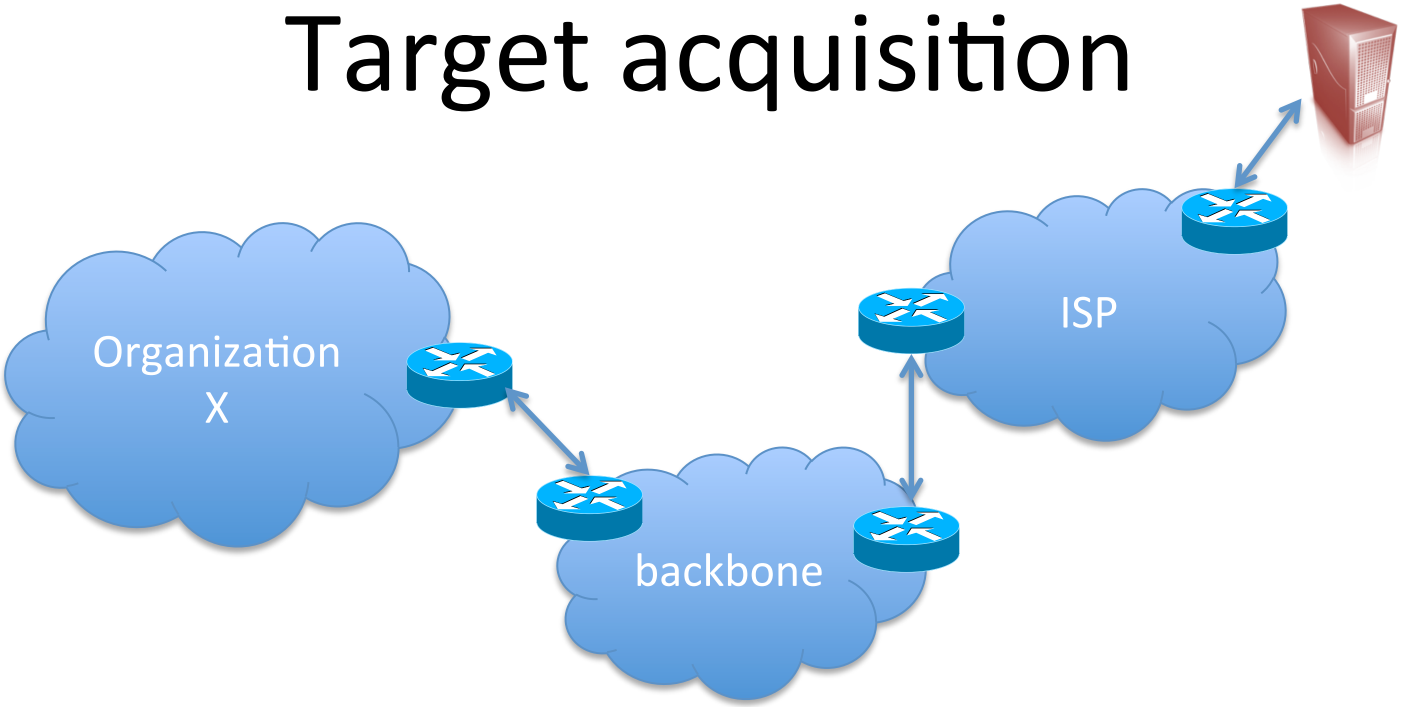
Port scanning

Host fingerprinting, NMAP

Network IDS basics

Avoiding IDS

# Target acquisition



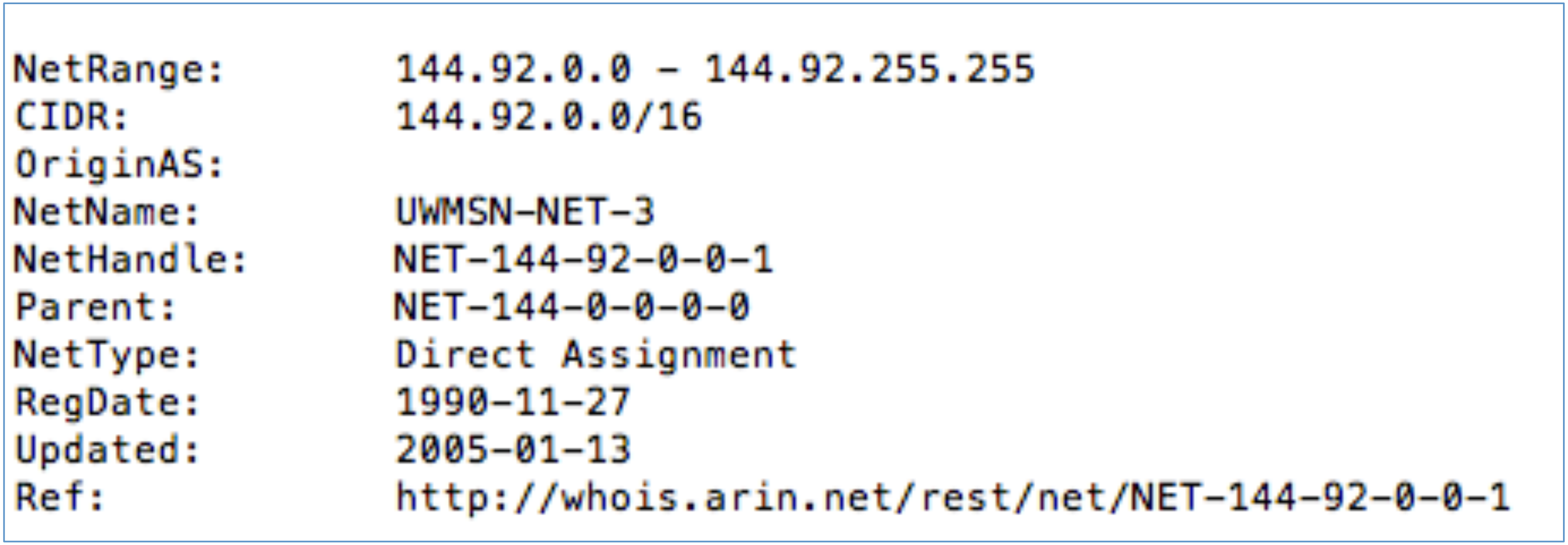
How do we find vulnerable server(s) within a target organization?

Starting point: one or more publicly routable IP addresses

- WHOIS queries are good way to find them

- Can be used to identify blocks of IP addresses owned

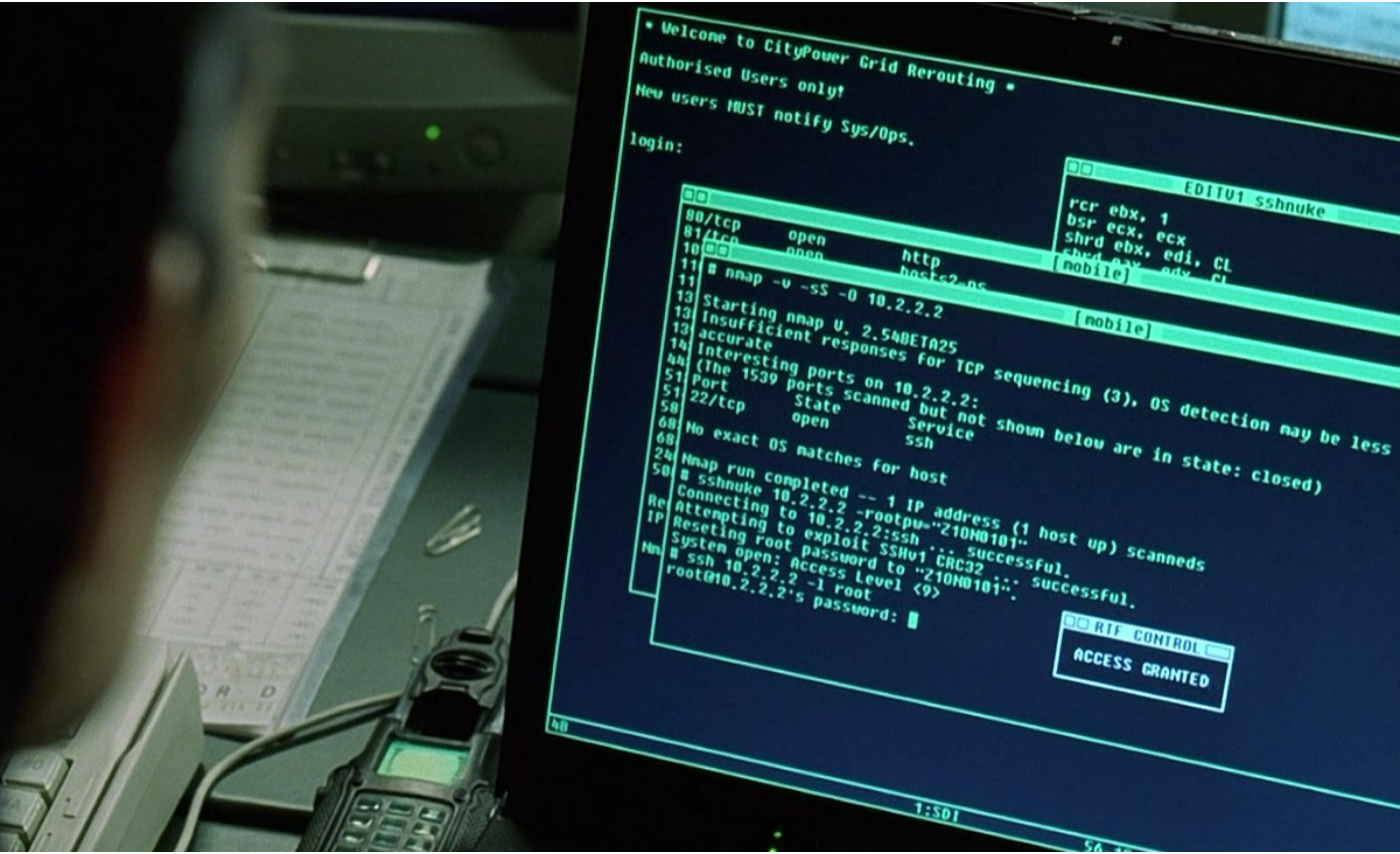
# WHOIS fun



```
NetRange:       144.92.0.0 - 144.92.255.255
CIDR:           144.92.0.0/16
OriginAS:
NetName:        UWMSN-NET-3
NetHandle:      NET-144-92-0-0-1
Parent:         NET-144-0-0-0-0
NetType:        Direct Assignment
RegDate:        1990-11-27
Updated:        2005-01-13
Ref:            http://whois.arin.net/rest/net/NET-144-92-0-0-1
```

# We’ve identified target (range of) IPs, now what?

- Host discovery
  - Narrow broad swath of potential IPs to ones that have hosts associated with them
- Service discovery
  - For a particular host, identify running services
  - E.g., is it accepting SSH connections (22) or HTTP (80)?
- OS fingerprinting
  - Identify the OS software version running
  - E.g., Windows vs Linux?
- Application fingerprinting
  - same at higher level
  - Apache version 1.3 or 2.0+?



```
* Welcome to CityPower Grid Rerouting *
Authorised Users only!
New users MUST notify Sys/Ops.

login:
```

```
rcr ebx, 1
bsr ecx, ecx
shrd ebx, edi, CL
```

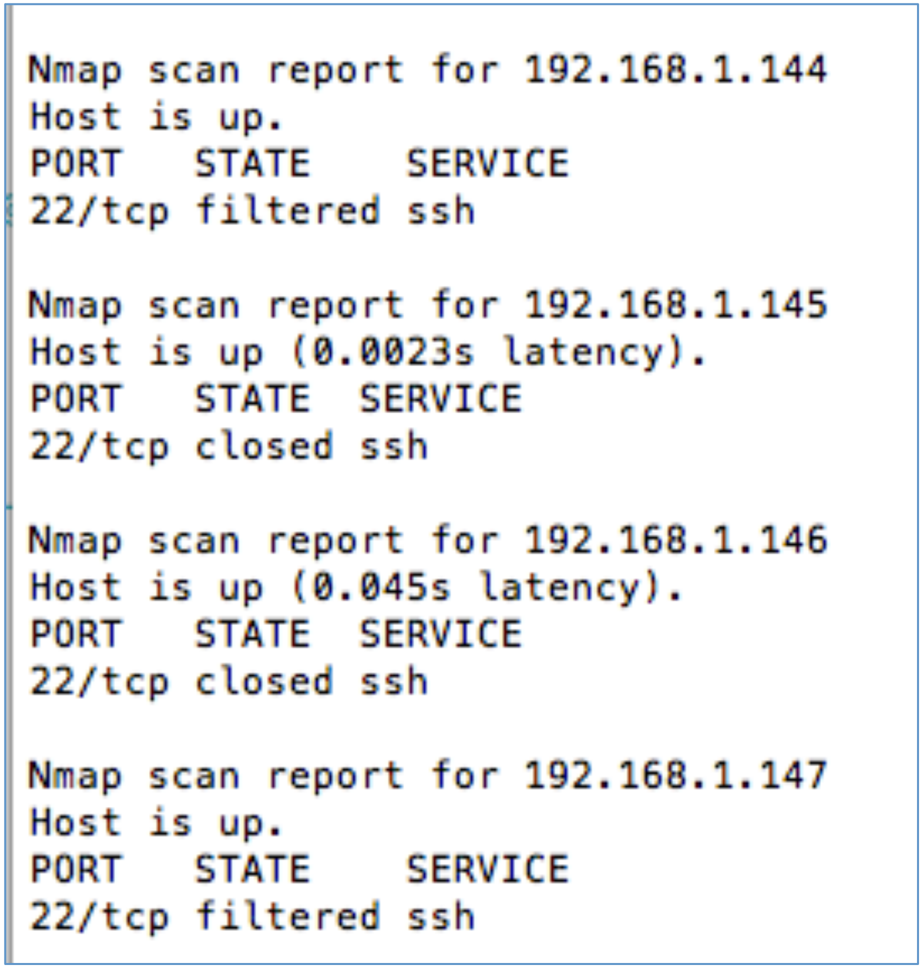
```
80/tcp
81/tcp      open       http
            open       hosts2-ns
```

```
# nmap -v -sS -O 10.2.2.2
Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS detection may be less
accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh

No exact OS matches for host

Nmap run completed -- 1 IP address (1 host up) scanneds
# sshnuke 10.2.2.2 -rootpw="Z10N0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z10N0101".
System open: Access Level <9>
# ssh 10.2.2.2 -l root
root@10.2.2.2's password:
```

# 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

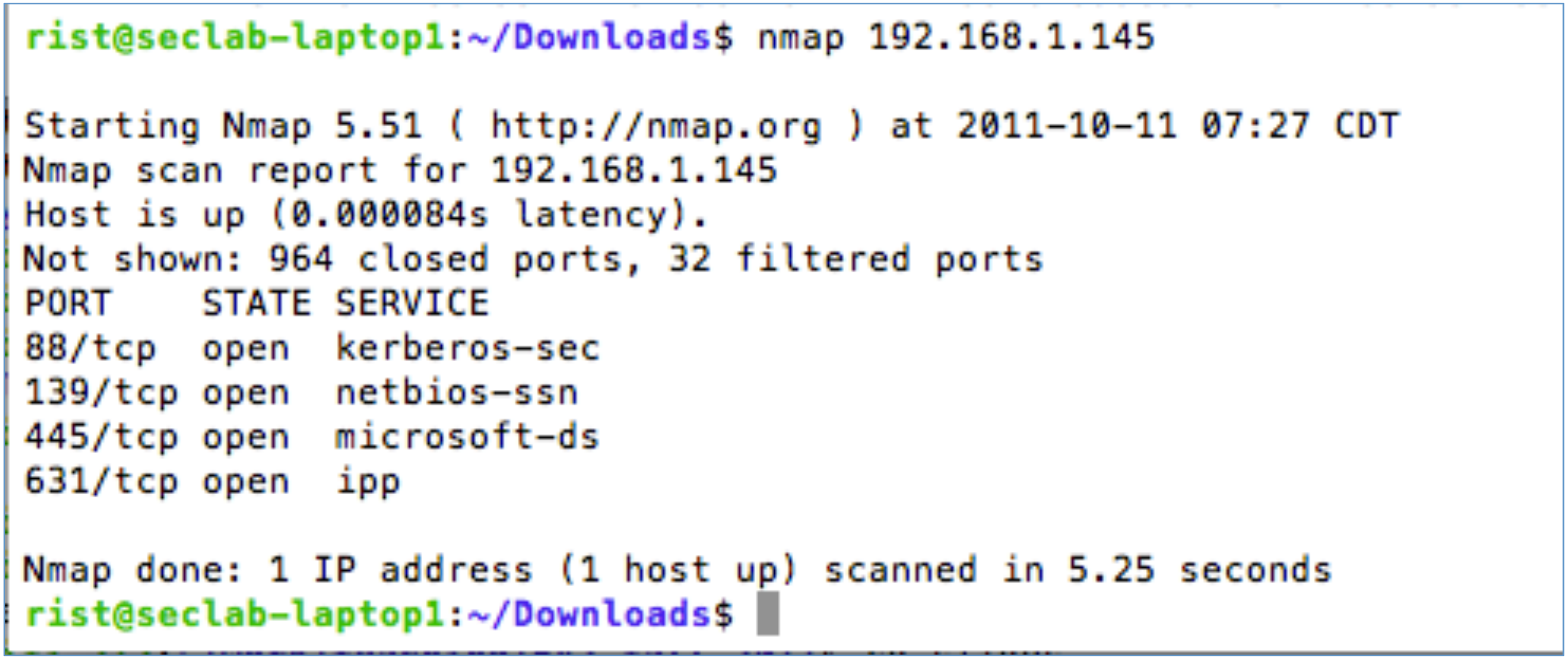


```
Nmap scan report for 192.168.1.144
Host is up.
PORT   STATE    SERVICE
22/tcp filtered ssh

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

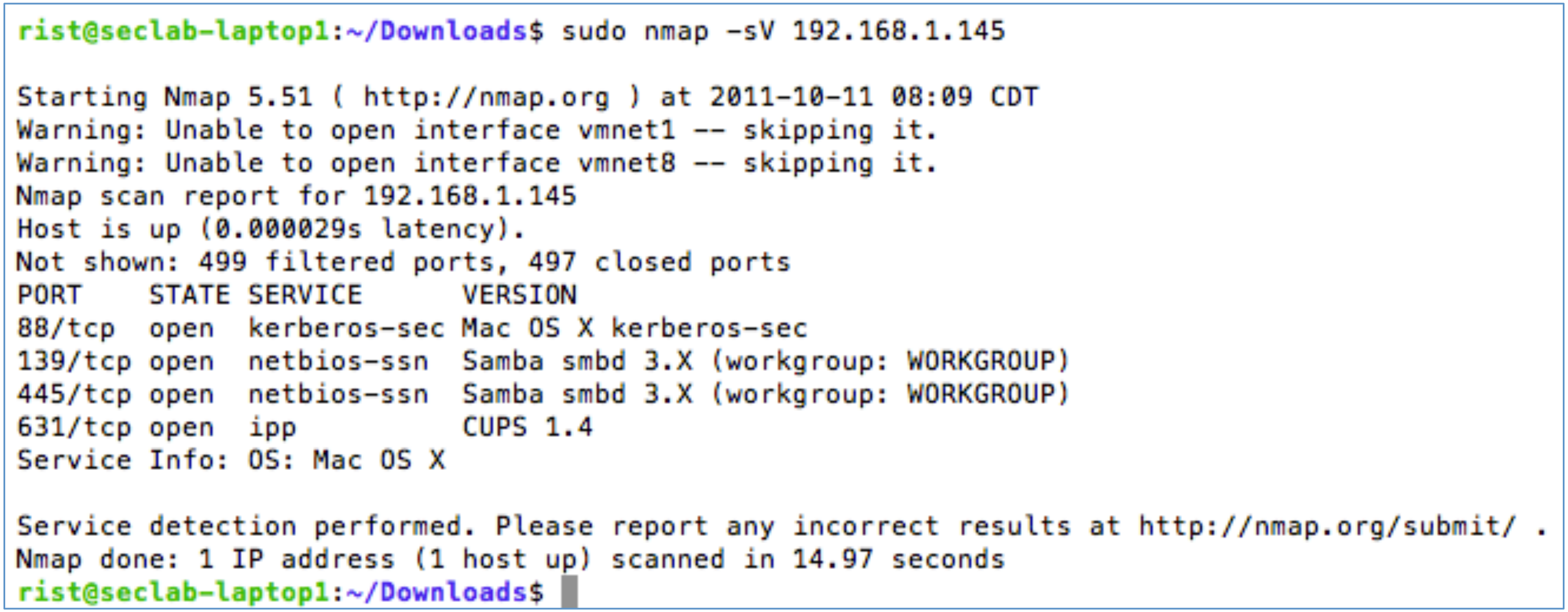
- open
  - host is accepting connections on that port
- closed
  - host responds to NMAP probes on port, but does not accept connections
- filtered
  - NMAP couldn't get packets through to host on that port.
  - Firewall?

# Port scan of host



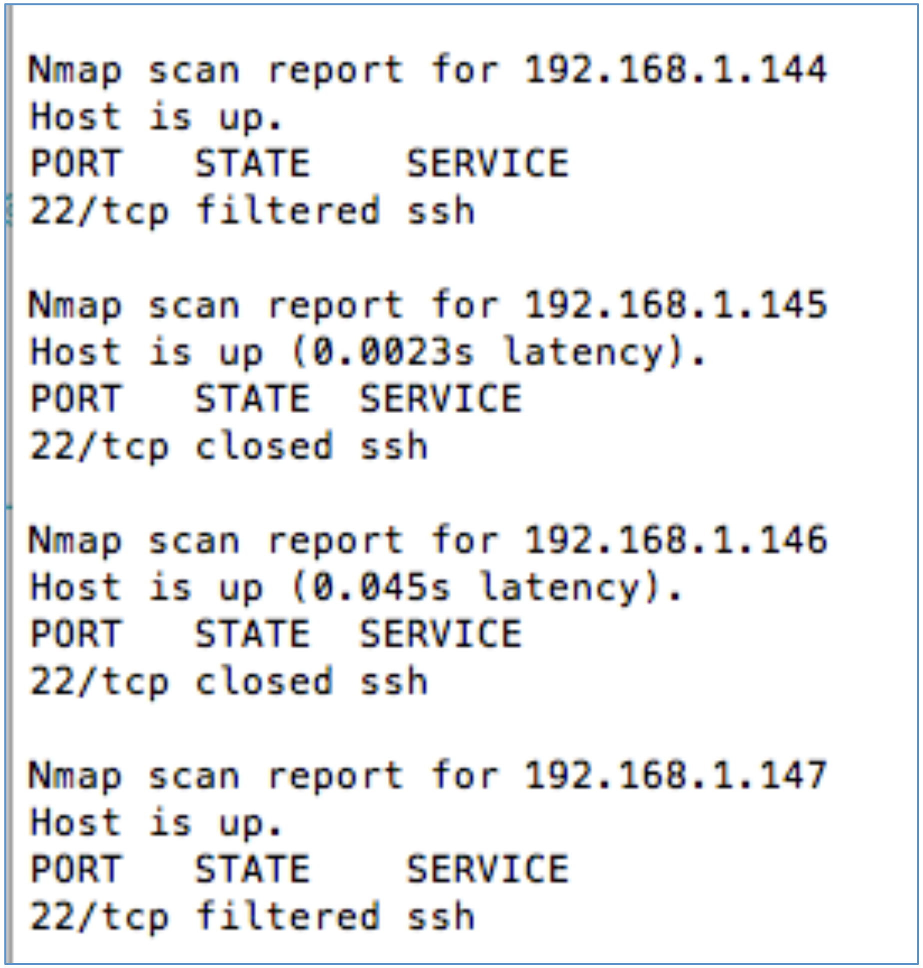
```
rist@seclab-laptop1:~/Downloads$ nmap 192.168.1.145

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 discovery



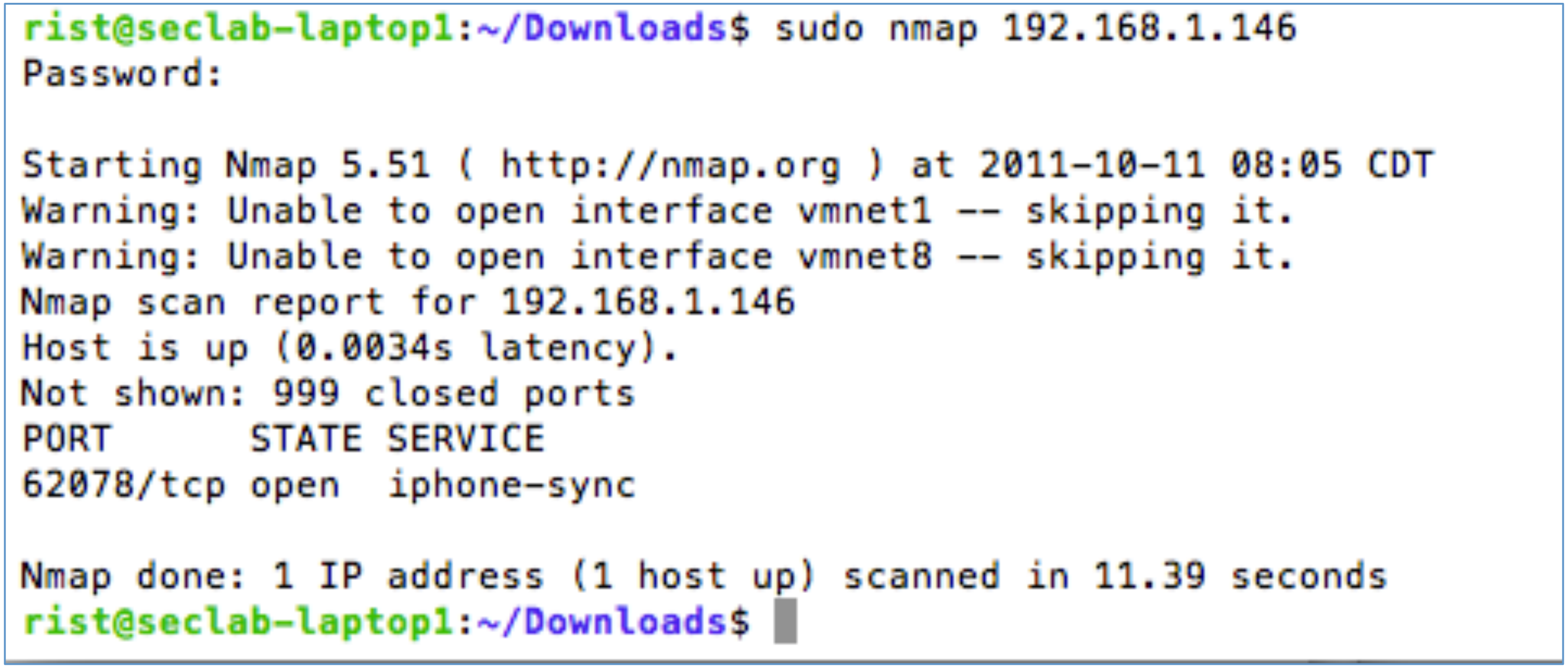
```
rist@seclab-laptop1:~/Downloads$ sudo nmap -sV 192.168.1.145

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



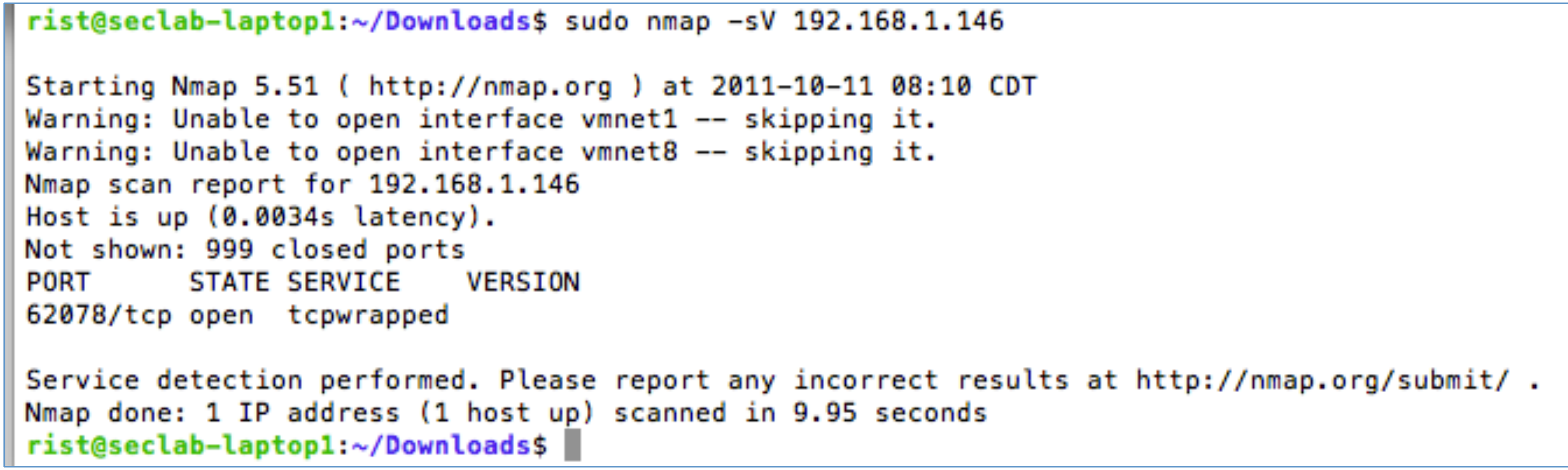
```
Nmap scan report for 192.168.1.144
Host is up.
PORT    STATE    SERVICE
22/tcp filtered ssh

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



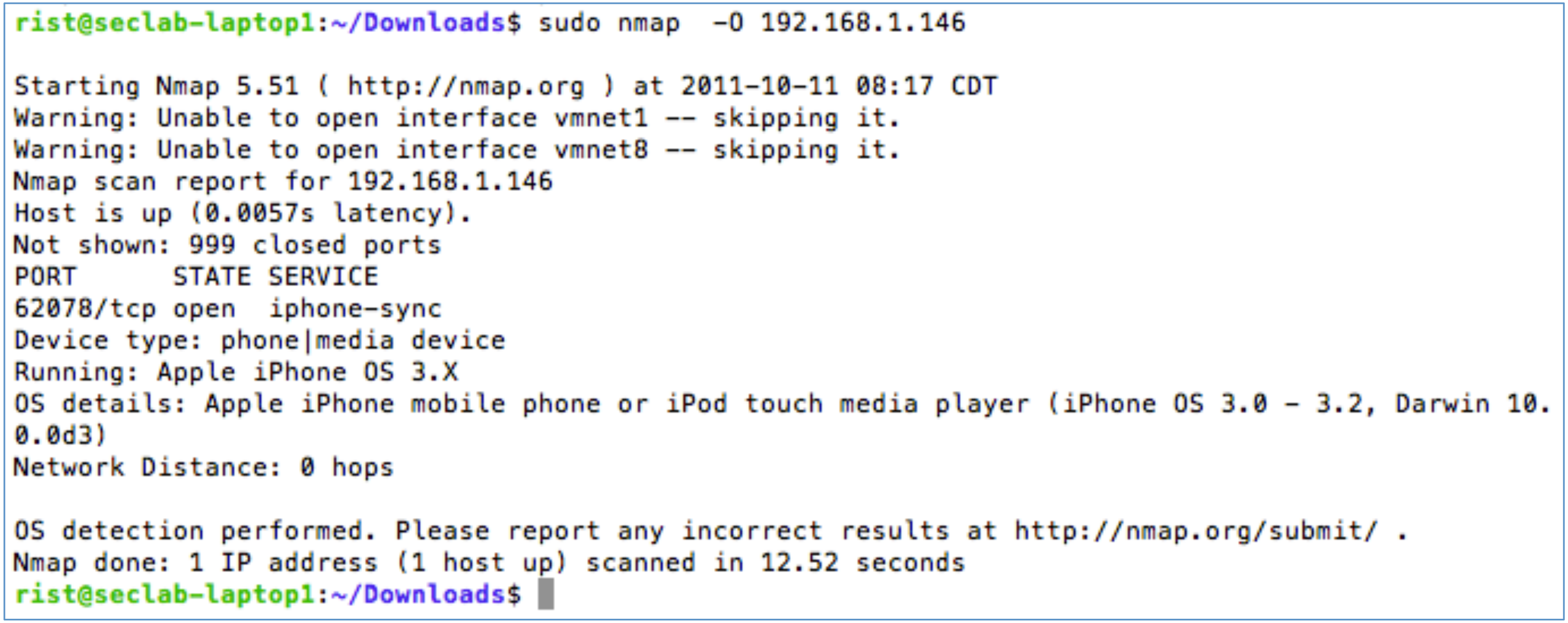
```
rist@seclab-laptop1:~/Downloads$ sudo nmap 192.168.1.146
Password:

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 discovery



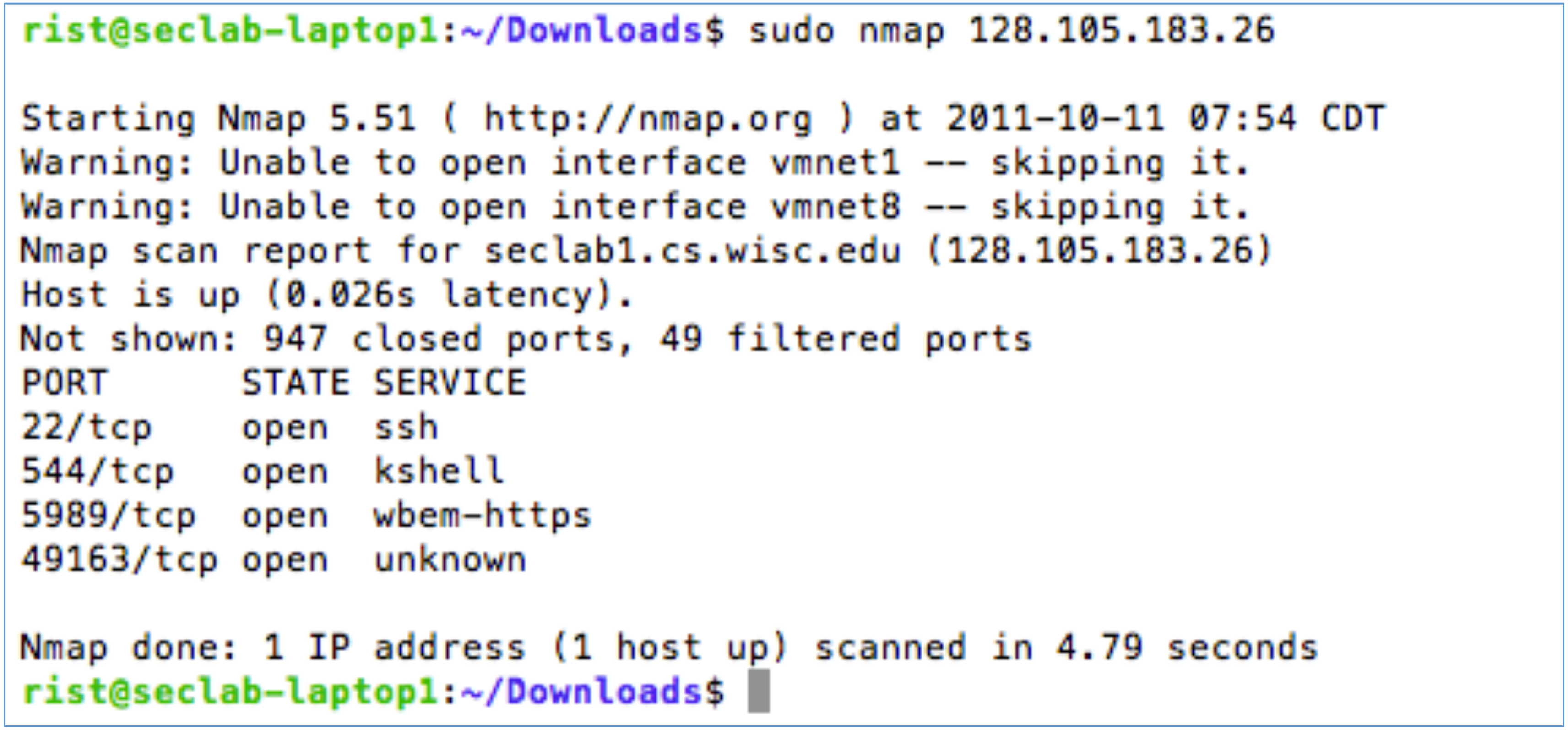
```
rist@seclab-laptop1:~/Downloads$ sudo nmap -sV 192.168.1.146

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$ 
```

# OS fingerprinting

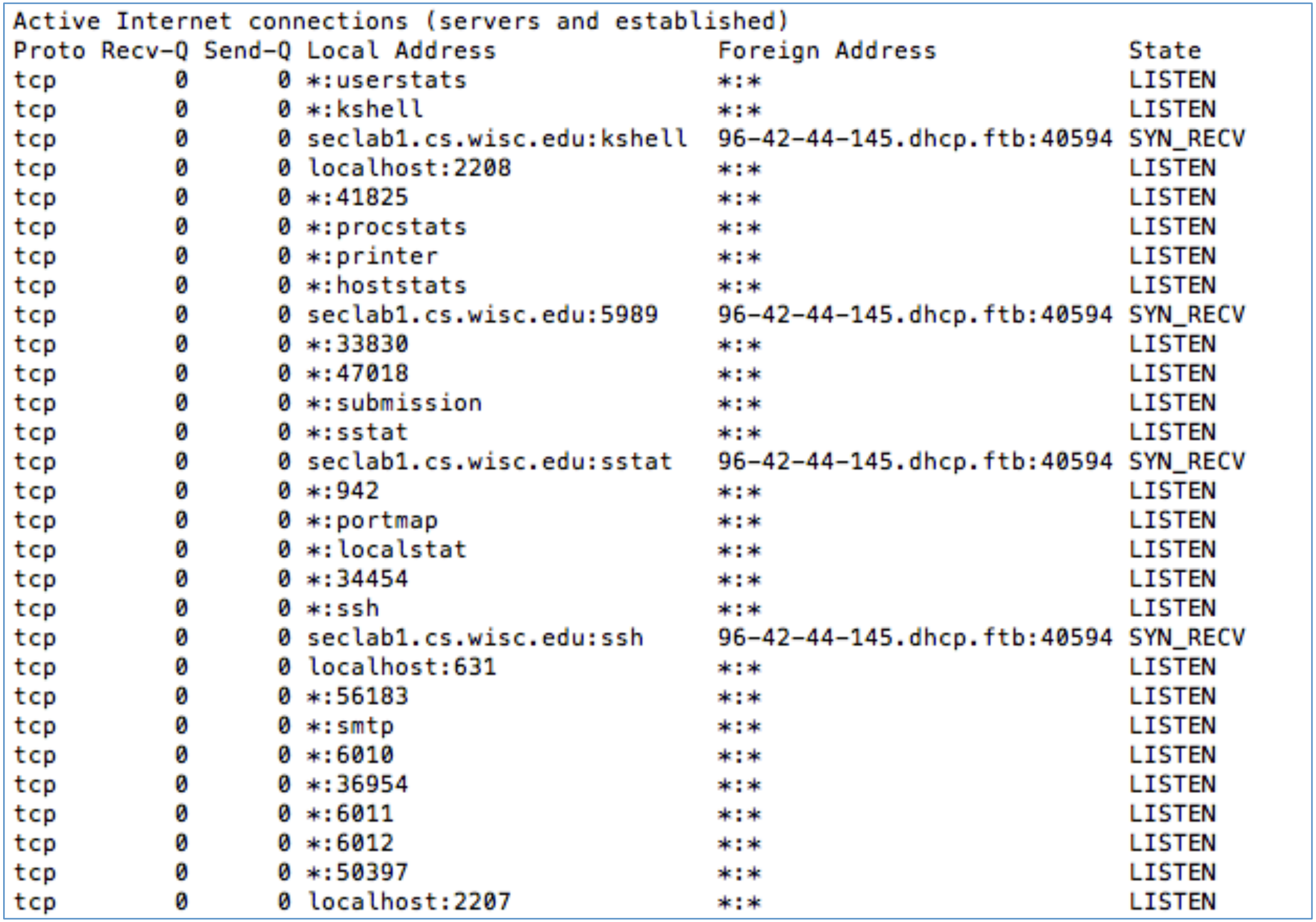


```
rist@seclab-laptop1:~/Downloads$ sudo nmap  -O 192.168.1.146

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

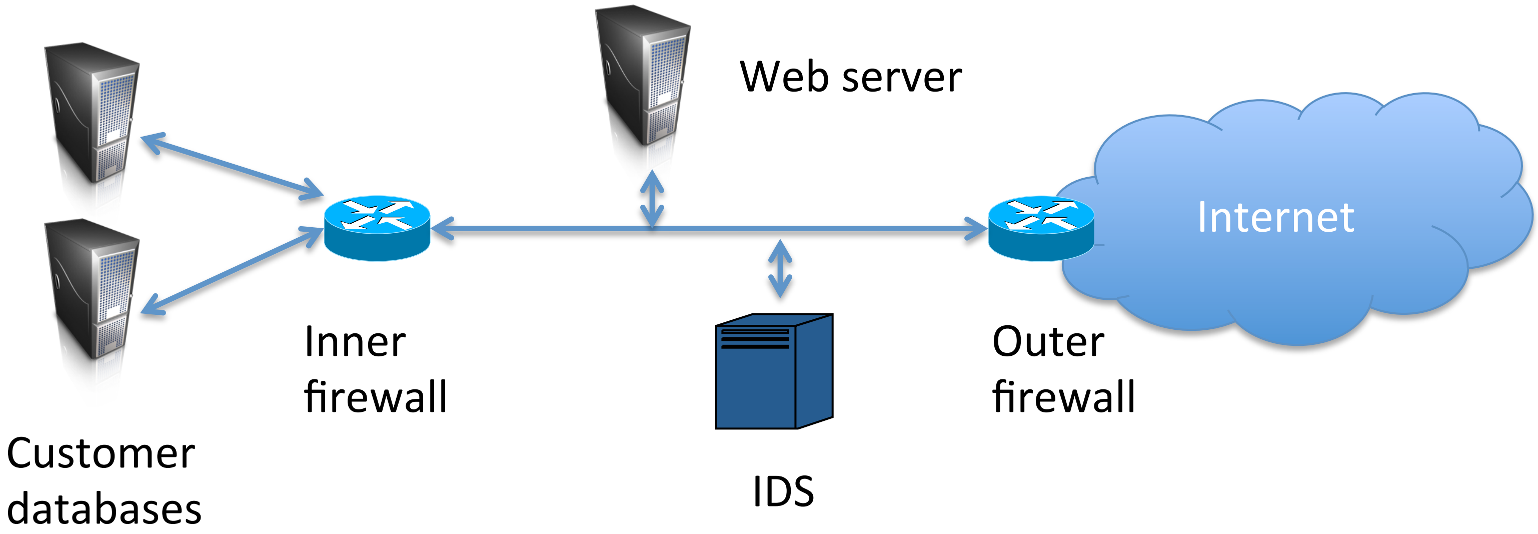


```
rist@seclab-laptop1:~/Downloads$ sudo nmap 128.105.183.26

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$ 
```



```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:userstats                 *:*                         LISTEN
tcp        0      0 *:kshell                    *:*                         LISTEN
tcp        0      0 seclab1.cs.wisc.edu:kshell  96-42-44-145.dhcp.ftb:40594 SYN_RECV
tcp        0      0 localhost:2208              *:*                         LISTEN
tcp        0      0 *:41825                     *:*                         LISTEN
tcp        0      0 *:procstats                 *:*                         LISTEN
tcp        0      0 *:printer                   *:*                         LISTEN
tcp        0      0 *:hoststats                 *:*                         LISTEN
tcp        0      0 seclab1.cs.wisc.edu:5989    96-42-44-145.dhcp.ftb:40594 SYN_RECV
tcp        0      0 *:33830                     *:*                         LISTEN
tcp        0      0 *:47018                     *:*                         LISTEN
tcp        0      0 *:submission                *:*                         LISTEN
tcp        0      0 *:sstat                     *:*                         LISTEN
tcp        0      0 seclab1.cs.wisc.edu:sstat   96-42-44-145.dhcp.ftb:40594 SYN_RECV
tcp        0      0 *:942                       *:*                         LISTEN
tcp        0      0 *:portmap                   *:*                         LISTEN
tcp        0      0 *:localstat                 *:*                         LISTEN
tcp        0      0 *:34454                     *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 seclab1.cs.wisc.edu:ssh     96-42-44-145.dhcp.ftb:40594 SYN_RECV
tcp        0      0 localhost:631               *:*                         LISTEN
tcp        0      0 *:56183                     *:*                         LISTEN
tcp        0      0 *:smtp                      *:*                         LISTEN
tcp        0      0 *:6010                      *:*                         LISTEN
tcp        0      0 *:36954                     *:*                         LISTEN
tcp        0      0 *:6011                      *:*                         LISTEN
tcp        0      0 *:6012                      *:*                         LISTEN
tcp        0      0 *:50397                     *:*                         LISTEN
tcp        0      0 localhost:2207              *:*                         LISTEN
```

# Network DMZ



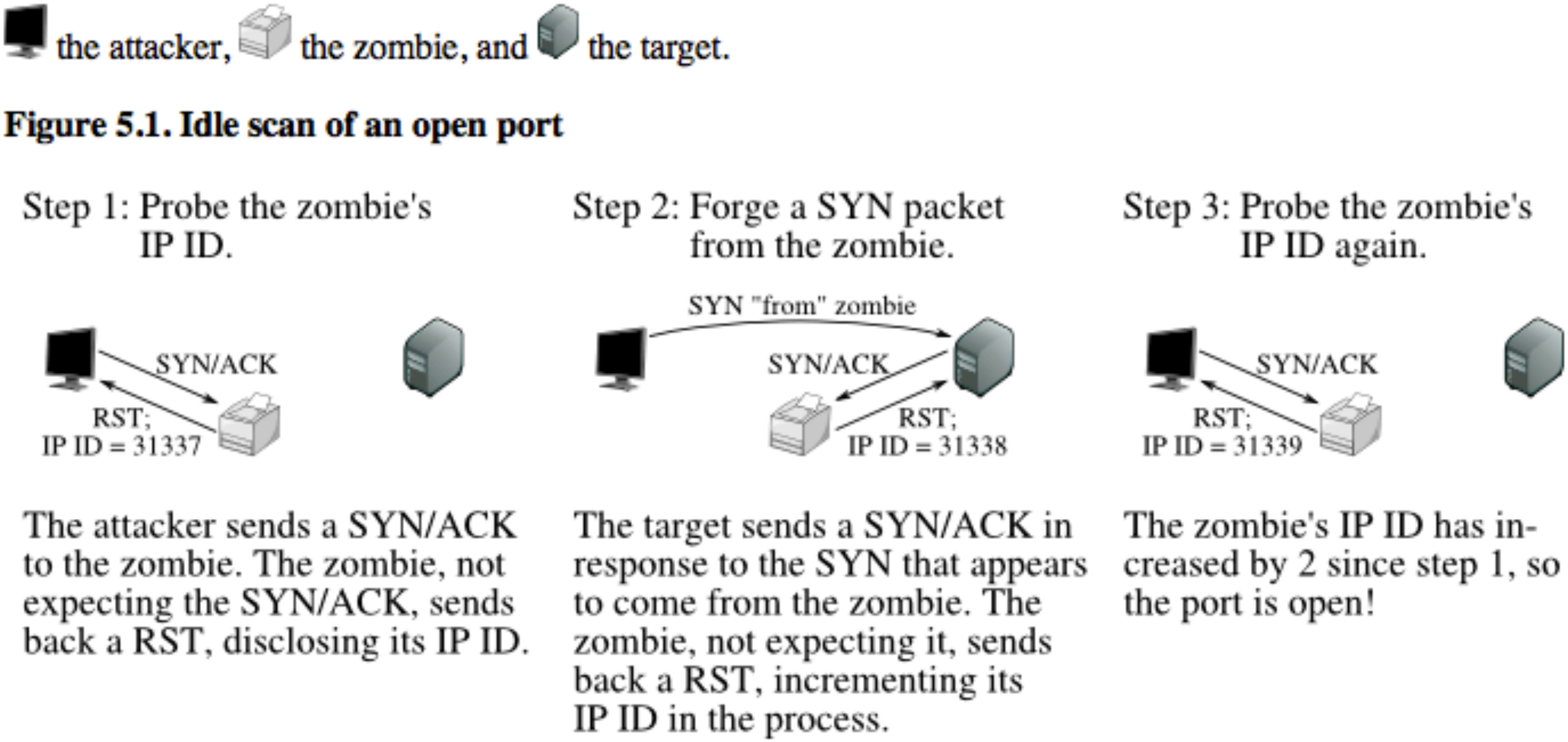
DMZ (demilitarized zone) helps isolate public network components from private network components

Firewall rules to disallow traffic from Internet to internal services

# Idle scans

- We want to avoid sending any non-spoofed packets to the target, but still want to port scan it
- Salvatore (Antirez) Sanfilippo 1998
- So-called idle scan can enable this
  1) Determine IPID of a zombie via SYN/ACK
  2) Send SYN spoofed from zombie
  3) Determine new IPID of zombie via SYN/ACK

# Idle scans



the attacker, the zombie, and the target.

**Figure 5.1. Idle scan of an open port**

Step 1: Probe the zombie's IP ID.

The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID.

Step 2: Forge a SYN packet from the zombie.

The target sends a SYN/ACK in response to the SYN that appears to come from the zombie. The zombie, not expecting it, sends back a RST, incrementing its IP ID in the process.

Step 3: Probe the zombie's IP ID again.

The zombie's IP ID has increased by 2 since step 1, so the port is open!

From http://nmap.org/book/idlescan.html

# Idle scan

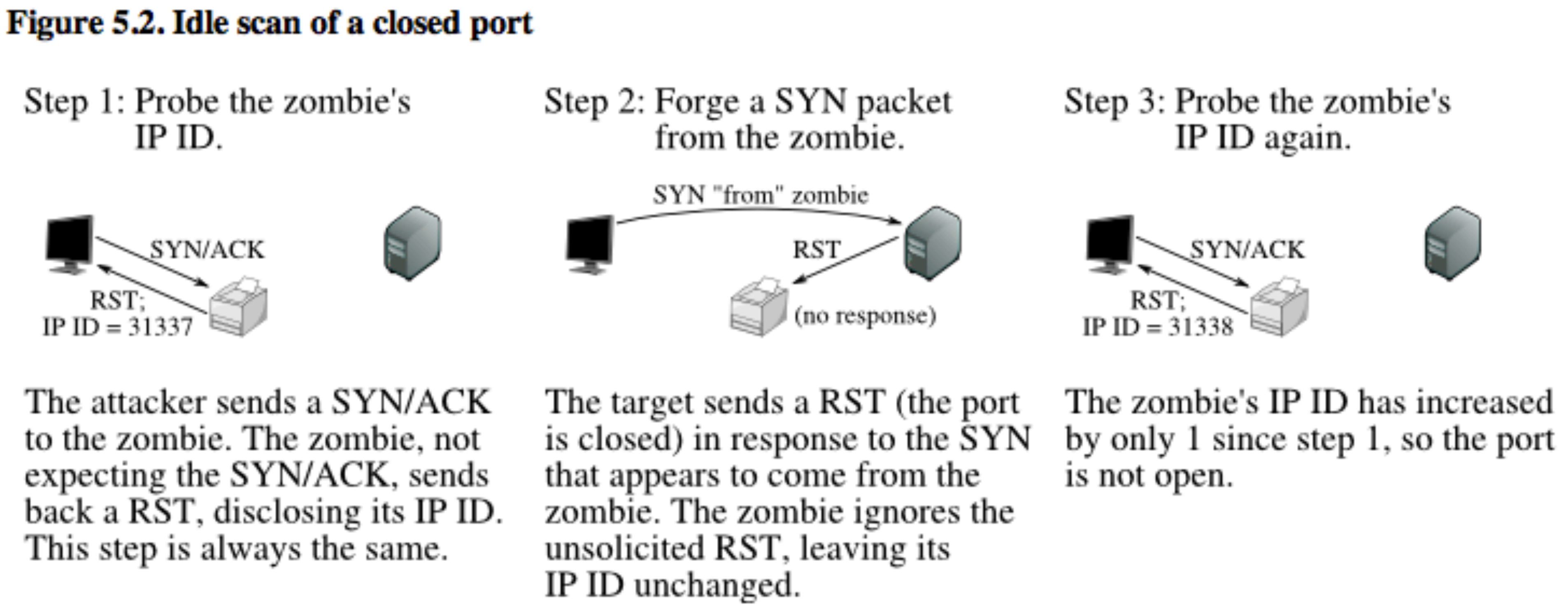


**Figure 5.2. Idle scan of a closed port**

Step 1: Probe the zombie's IP ID.

The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID. This step is always the same.

Step 2: Forge a SYN packet from the zombie.

The target sends a RST (the port is closed) in response to the SYN that appears to come from the zombie. The zombie ignores the unsolicited RST, leaving its IP ID unchanged.

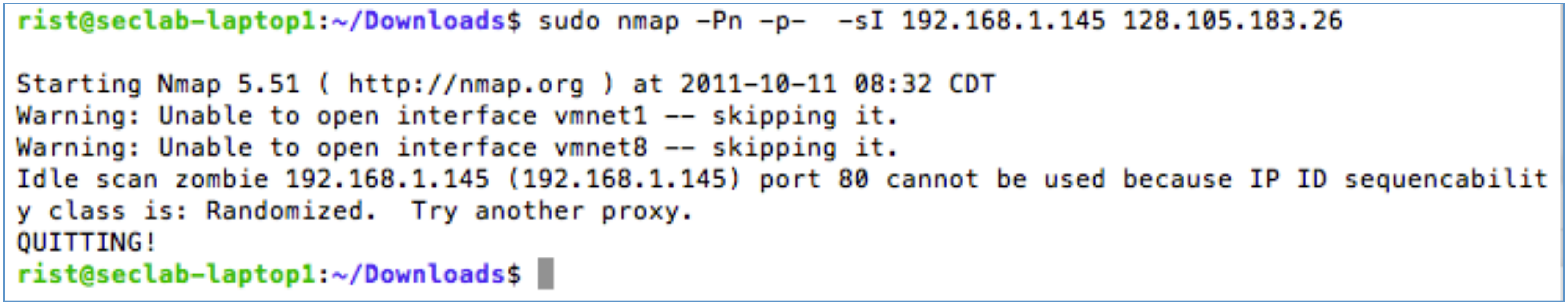
Step 3: Probe the zombie's IP ID again.

The zombie's IP ID has increased by only 1 since step 1, so the port is not open.

From http://nmap.org/book/idlescan.html

# 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$ 
```

# Other idle scan type methods?

- Ensafi et al. “Idle Port Scanning and Non-Interference Analysis of Network Protocol Stacks Using Model Checking”, USENIX Security 2010
- IPID is a side channel – maybe there are others?
  - RST rate
  - SYN cache size

# Idle scan: RST rate limit

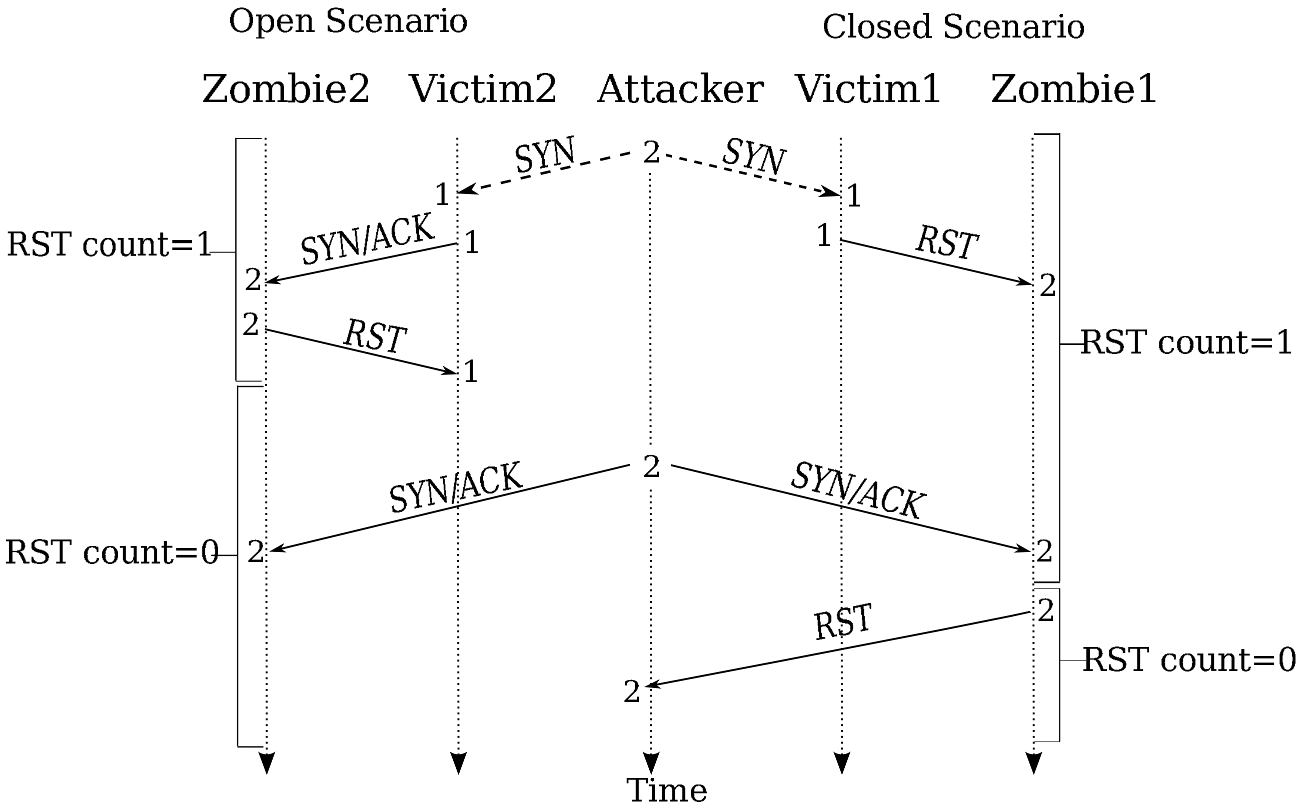


Figure 6: **RST rate limiting counterexample.**

From Ensafi et al. 2010

# SYN caches and SYN cookies

- SYN cache maintains state for outstanding TCP SYN requests received
  - Finite amount of memory
- SYN cookie is mechanism for dealing with DoS
  - When SYN cache is full, calculate response’s ISN

| | | |
|---|---|---|
| 5 bits<br>timestamp t<br>mod 32 | 3 bits<br>Max Seg<br>Size<br>encoding | 24 bits<br>MD5(serverIP,serverPort,clientIP,clientPort,t) |

# Idle scan: SYN cache

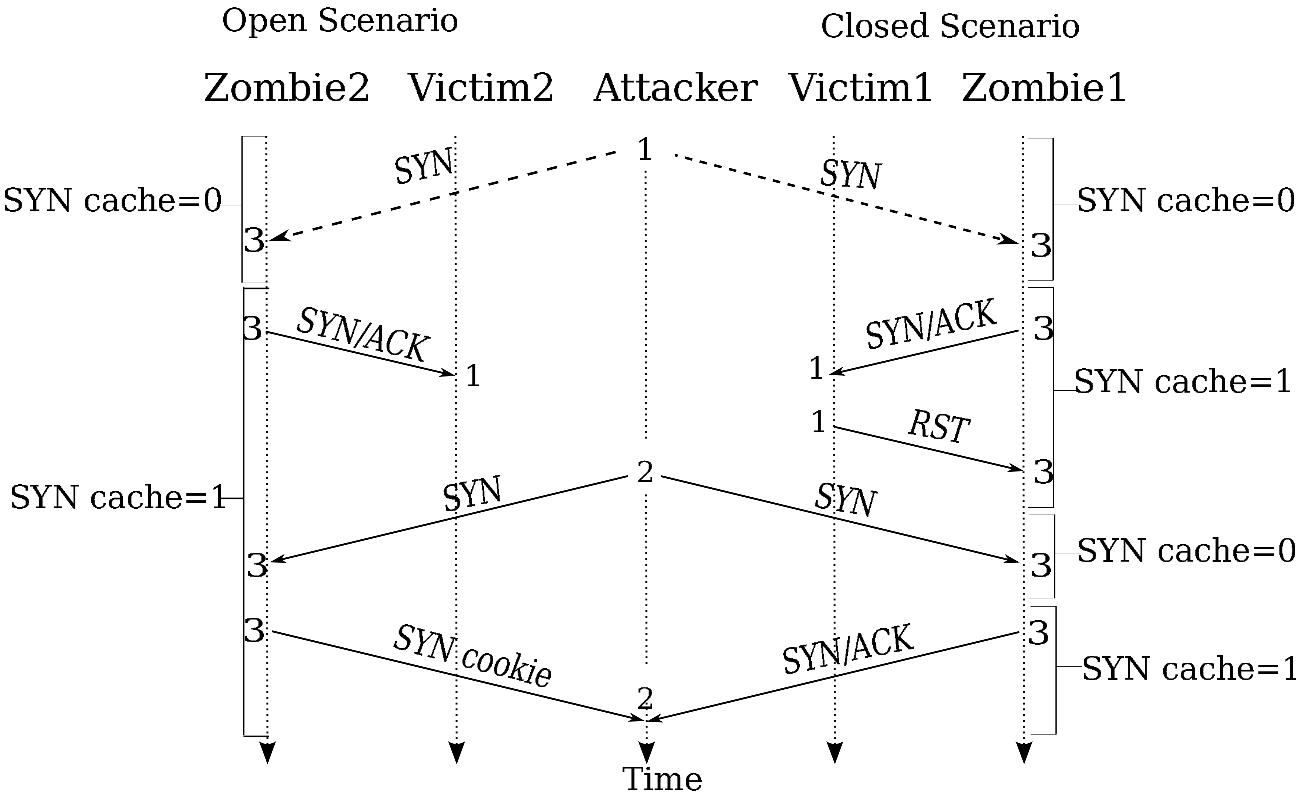


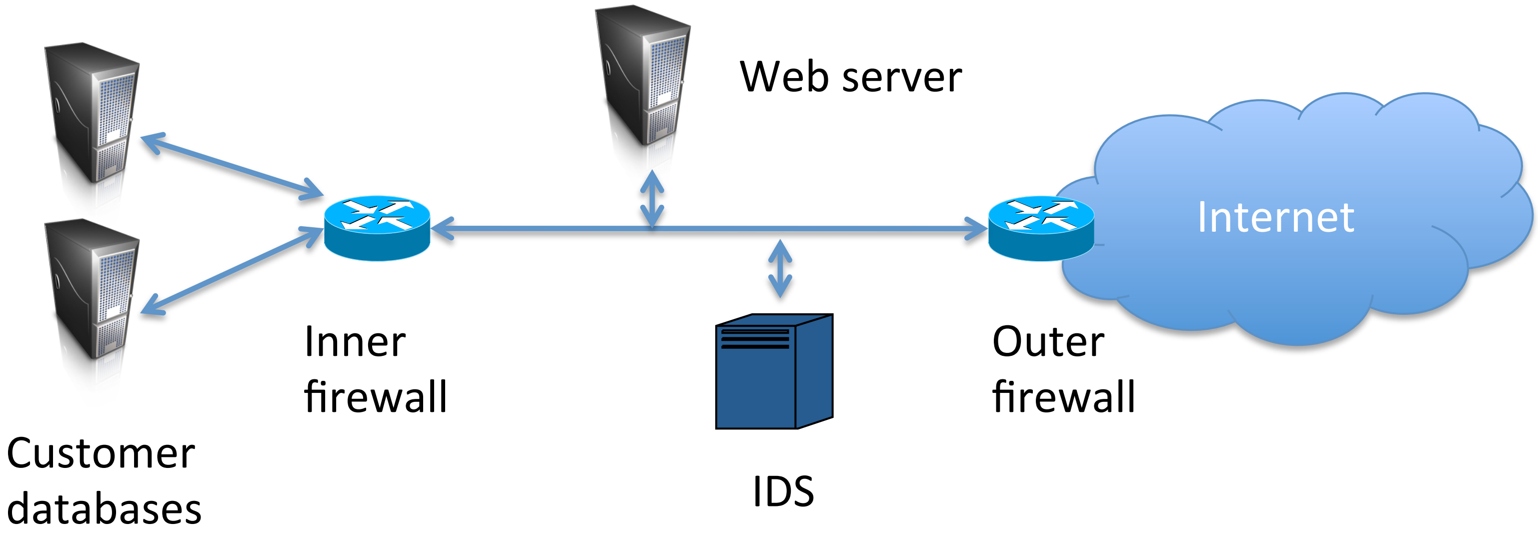
Figure 7: **SYN cache counterexample.**

From Ensafi et al. 2010

# 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.

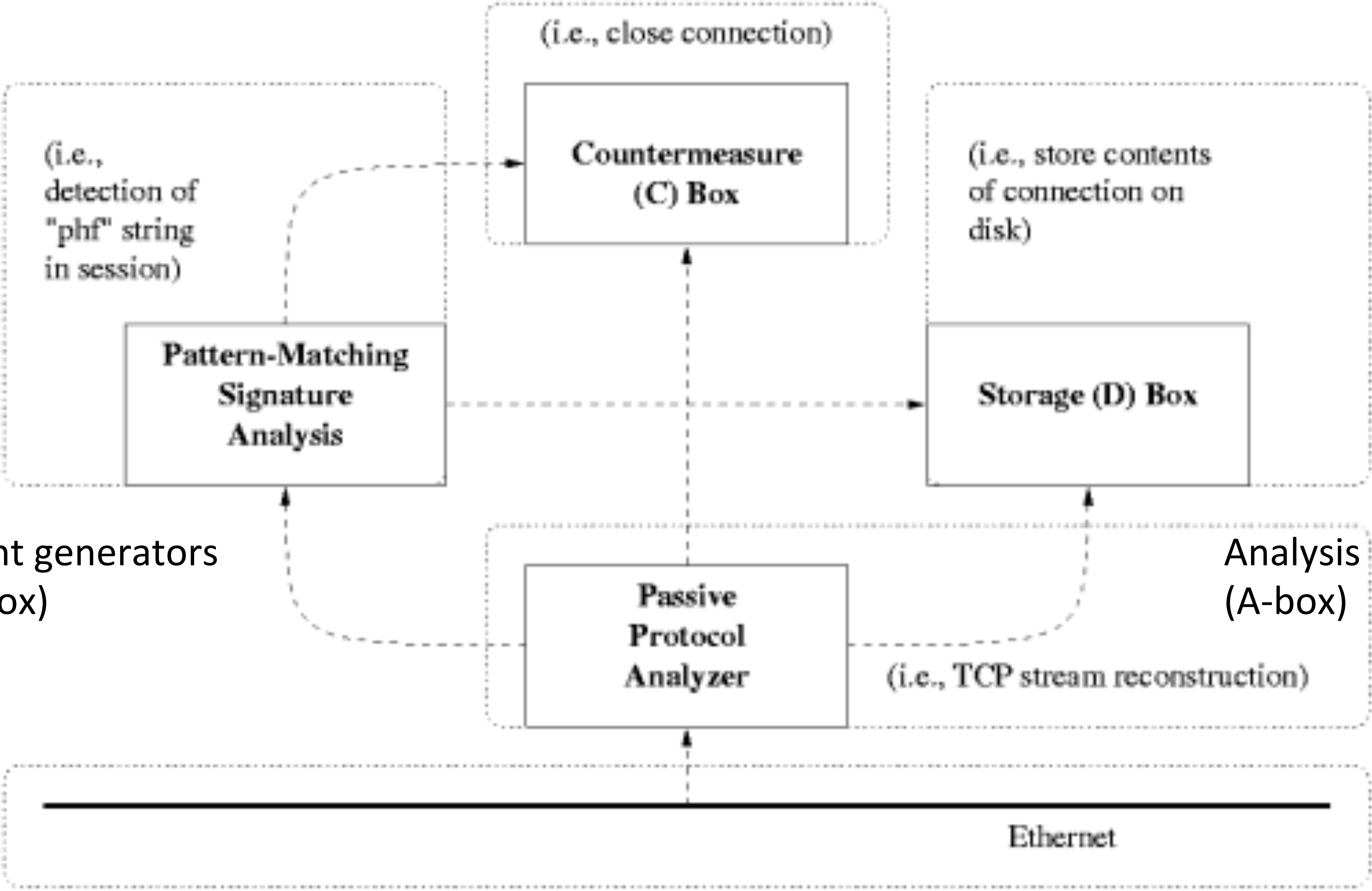
# Network DMZ



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

Firewall rules to disallow traffic from Internet to internal services

# CIDF
# (Common intrusion detection framework)


(i.e., close connection)
Countermeasure (C) Box
(i.e., detection of "phf" string in session)
Pattern-Matching Signature Analysis
(i.e., store contents of connection on disk)
Storage (D) Box
Passive Protocol Analyzer
(i.e., TCP stream reconstruction)
Ethernet

Event generators (E-box)

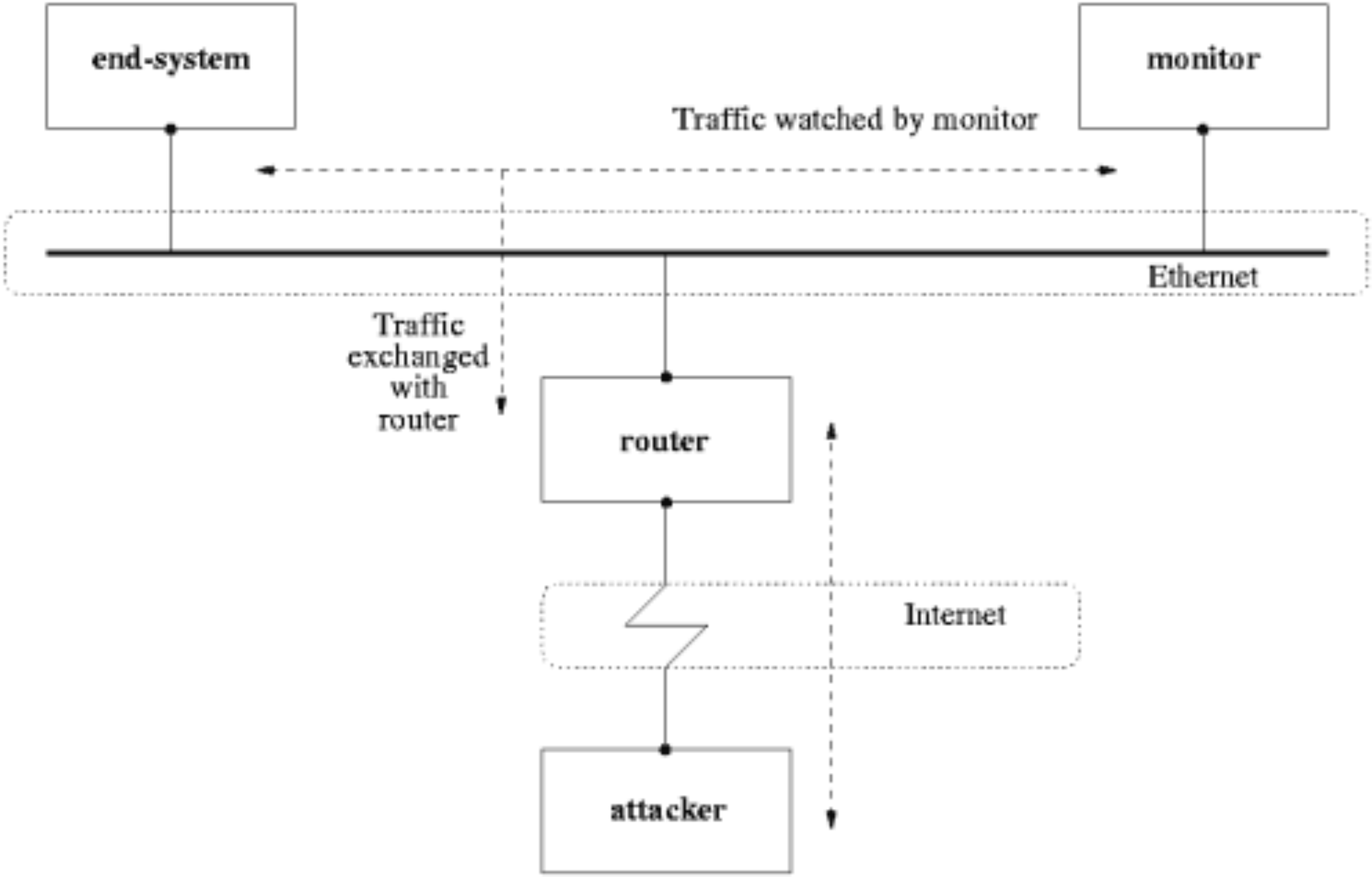
Analysis engine (A-box)

From http://insecure.org/stf/secnet_ids/secnet_ids.html

# Two broad classes

- Anomaly detection
  - What does "normal" traffic look like?
  - Flag abnormal traffic
- Signature based
  - Define some explicit traffic patterns as bad
  - Flag them
  - E.g., regular expressions

# Basic NIDS setup



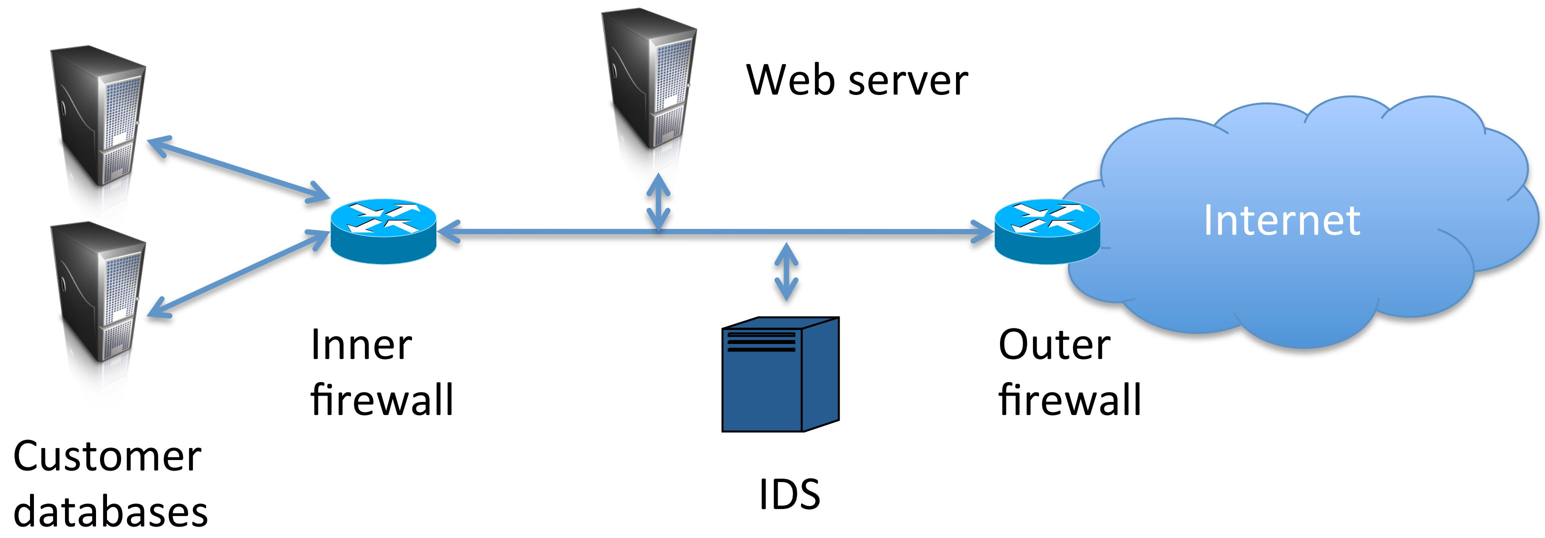
From http://insecure.org/stf/secnet_ids/secnet_ids.html

# Some examples

- Snort (Martin Roesch)
- Bro (Vern Paxson)
  - 1999: 27,000 lines of C++ code

# Attacking or bypassing NIDS

- How do we circumvent a NIDS?



Overload attacks, crash attacks, subterfuge attacks

# Subterfuge attack example

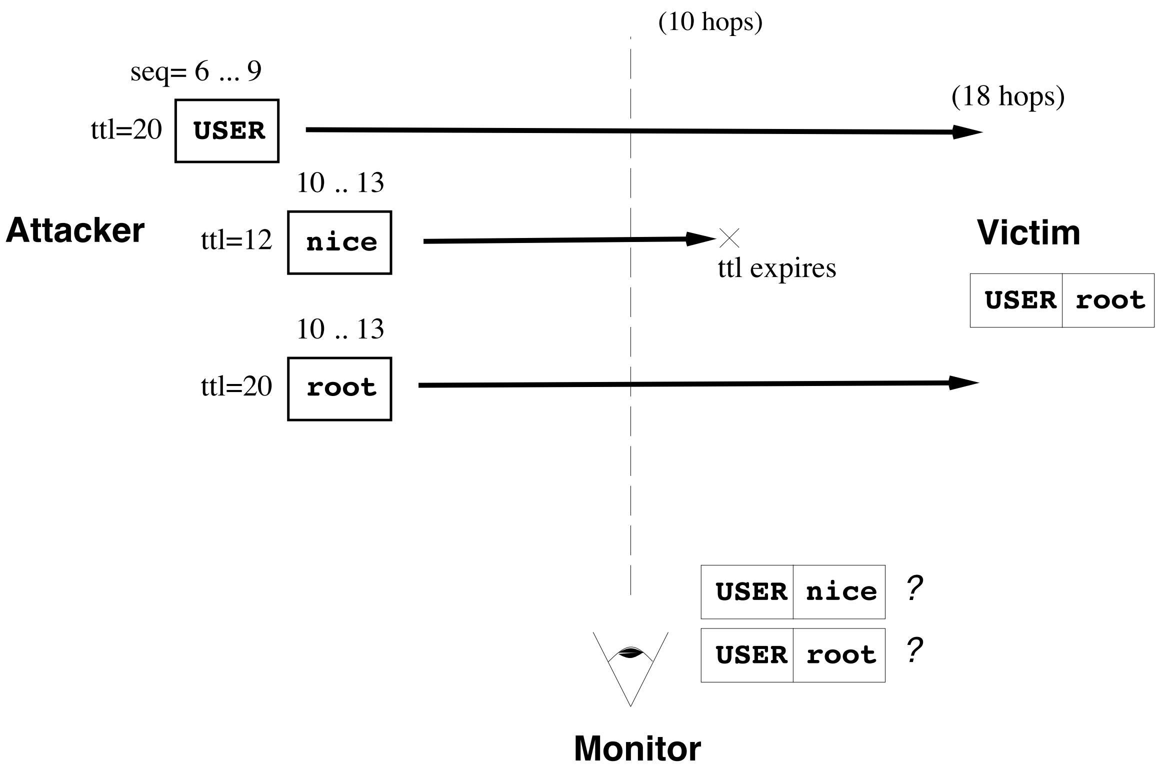


Figure 2: A TTL-based evasion attack on an intrusion detection system

From Paxson, "Bro: A System for Detecting Network Intruders in Real-Time", 1999

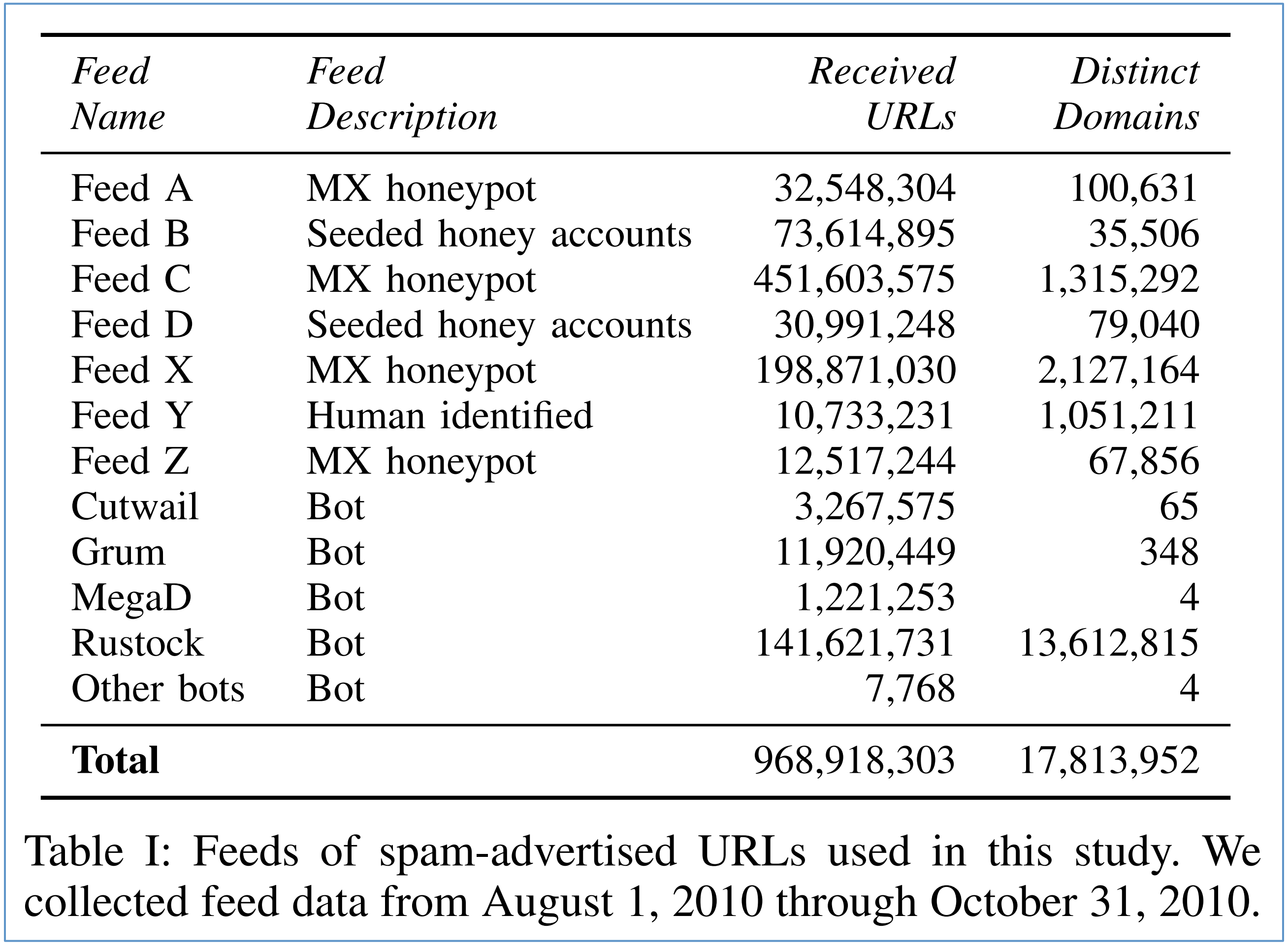
# Anomalous, non-attack traffic

- “Storms” of 10,000s of FIN or RST packets due to protocol implementation error
- “Storms” due to foggy days
  - Fog in SF bay area killed a connection, causing routing flaps and in turn routing loops
- SYN packet with URG flag set
  - Flags == SYN  fails

# Honeypots

- Systems that should have no legitimate traffic
  - Isolated and monitored
  - Any traffic routed to it is spurious
- High interaction (e.g., a full system)
- Low interaction (e.g., Honeyd)
- Honeynets, honeyfarms
  - lots of honeypots
- Honeytoken
  - email address
  - credit card number

# Honeypots and spam

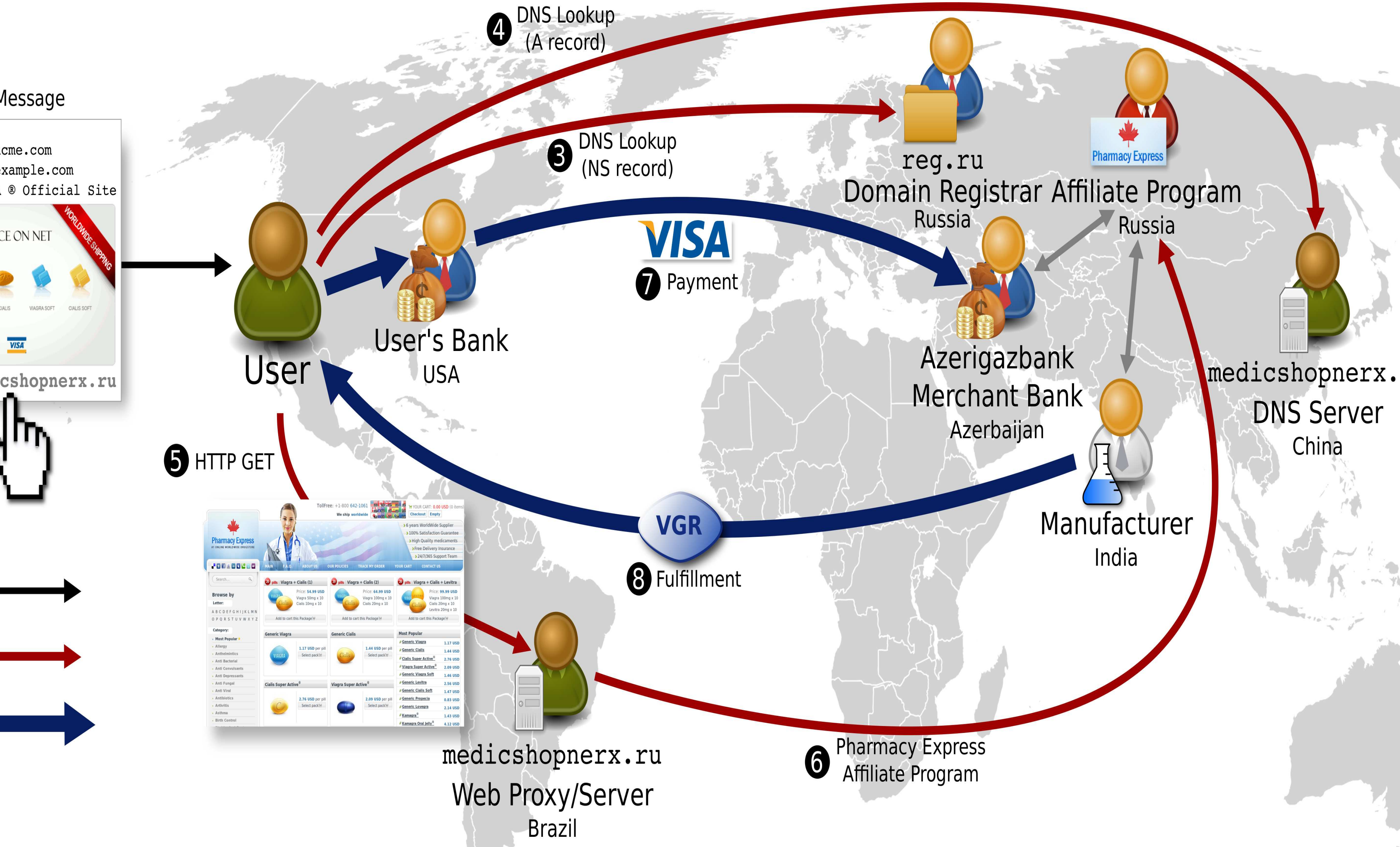


| *Feed Name* | *Feed Description* | *Received URLs* | *Distinct Domains* |
|---|---|---:|---:|
| Feed A | MX honeypot | 32,548,304 | 100,631 |
| Feed B | Seeded honey accounts | 73,614,895 | 35,506 |
| Feed C | MX honeypot | 451,603,575 | 1,315,292 |
| Feed D | Seeded honey accounts | 30,991,248 | 79,040 |
| Feed X | MX honeypot | 198,871,030 | 2,127,164 |
| Feed Y | Human identified | 10,733,231 | 1,051,211 |
| Feed Z | MX honeypot | 12,517,244 | 67,856 |
| Cutwail | Bot | 3,267,575 | 65 |
| Grum | Bot | 11,920,449 | 348 |
| MegaD | Bot | 1,221,253 | 4 |
| Rustock | Bot | 141,621,731 | 13,612,815 |
| Other bots | Bot | 7,768 | 4 |
| **Total** | | 968,918,303 | 17,813,952 |

Table I: Feeds of spam-advertised URLs used in this study. We collected feed data from August 1, 2010 through October 31, 2010.

From Levchenko et al., "Click Trajectories: End-to-End Analysis of the Spam Value Chain", IEEE Symposium on Security and Privacy, 2011

From Levchenko et al., “Click Trajectories: End-to-End Analysis of the Spam Value Chain”, IEEE Symposium on Security and Privacy, 2011


Message
cme.com
xample.com
® Official Site
CE ON NET
WORLDWIDE SHIPPING
VIAGRA SOFT
CIALIS SOFT
VISA
cshopnerx.ru
User
4 DNS Lookup (A record)
3 DNS Lookup (NS record)
reg.ru
Domain Registrar
Russia
Pharmacy Express
Affiliate Program
Russia
User's Bank
USA
VISA
7 Payment
Azerigazbank
Merchant Bank
Azerbaijan
medicshopnerx.
DNS Server
China
5 HTTP GET
Manufacturer
India
VGR
8 Fulfillment
Pharmacy Express
medicshopnerx.ru
Web Proxy/Server
Brazil
6 Pharmacy Express Affiliate Program