

# Network reconnaissance and IDS

## CS642: Computer Security



Professor Ristenpart

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

rist at cs dot wisc dot edu



# Hackers Compromised Yahoo Servers Using Shellshock Bug

samzenpus posted 17 minutes ago | from the protect-ya-neck dept.

wiredmikey writes

Hackers were able to [break into some of Yahoo's servers](#) by exploiting the recently disclosed Shellshock bug over the past few weeks. This may be the first confirmed case of a major company being hit with attacks exploiting the vulnerability in bash. Contacted by SecurityWeek, a Yahoo spokesperson provided the following statement Monday afternoon: "A security flaw, called Shellshock, that could expose vulnerabilities in many web servers was identified on September 24. As soon as we became aware of the issue, we began patching our systems and have been closely monitoring our network. Last night, we isolated a handful of our impacted servers and at this time we have no evidence of a compromise to user data. We're focused on providing the most secure experience possible for our users worldwide and are continuously working to protect our users' data."



# Dubai Police To Use Google Glass For Facial Recognition

samzenpus posted 6 hours ago | from the watching-you-better dept.

cold fjord sends word about what the Dubai police plan on doing with their Google Glass.

Police officers in Dubai will soon be able to identify suspects wanted for crimes just by looking at them. Using Google Glass and a system developed facial recognition software, Dubai police

# Let's play over the network ...



Target acquisition

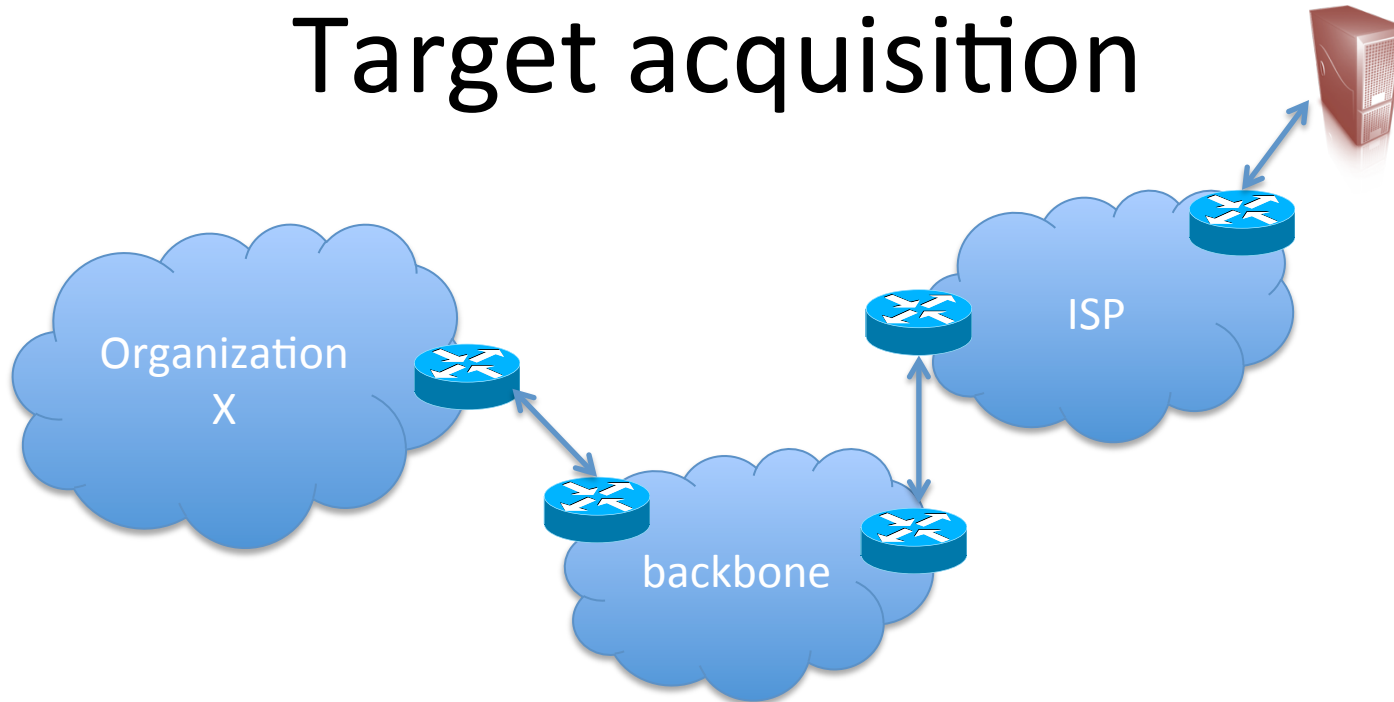
Port scanning

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+?

# Port scanners

- NMAP (network map tool)
  - De-facto standard for network reconnaissance, testing
  - Numerous built in scanning methods
- Increasingly common to perform scans of entire IPv4 address space
  - Zmap provides more efficient scanning of certain limited forms than NMAP
    - 1 machine => scan entire IPv4 range in ~45 minutes
- Active scanning now used frequently for research

• Welcome to CityPower Grid Rerouting •  
Authorized Users only!  
New users MUST notify Sys/Ops.  
login:

```
EDITV1 sshnuke  
rcr ebx, 1  
bsr ecx, ecx  
shrd ebx, edi, CL  
shrd eax, edx, CL  
[mobile]
```

```
80/tcp open http  
81/tcp open hosts2-ns  
10 [mobile]  
11 # nmap -v -sS -O 10.2.2.2  
11 Starting nmap V. 2.54BETA25  
13 Insufficient responses for TCP sequencing (3), OS detection may be less  
13 accurate  
14 Interesting ports on 10.2.2.2:  
44 (The 1539 ports scanned but not shown below are in state: closed)  
51 Port State Service  
51 22/tcp open ssh  
58 No exact OS matches for host  
68  
68  
24 Nmap run completed -- 1 IP address (1 host up) scanned  
50 # sshnuke 10.2.2.2 -rootpw="210N0101"  
Re Connecting to 10.2.2.2:ssh ... successful.  
IP Attempting to exploit SSHv1 CRC32 ... successful.  
System open: Access Level to "210N0101".  
New # ssh 10.2.2.2 -l root  
root@10.2.2.2's password: █
```

RTF CONTROL  
ACCESS GRANTED



`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$
```

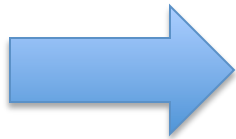
`nmap -PN -sT -p 22 192.168.1.0/24`

```
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

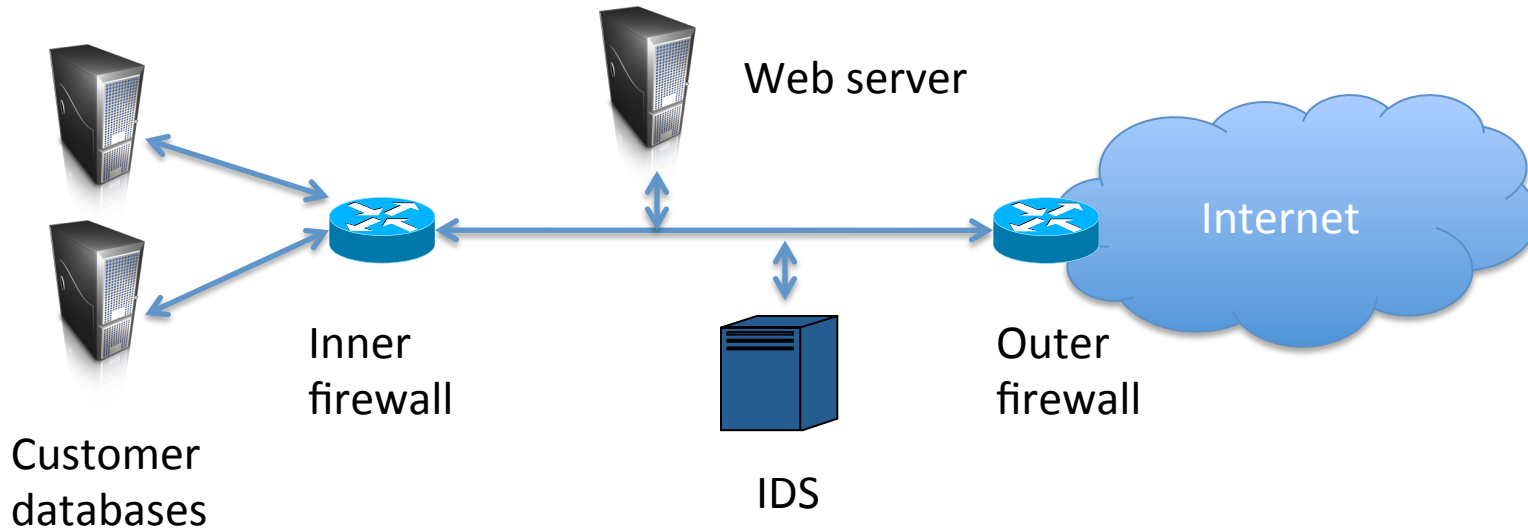
Starting Nmap 5.51 ( http://nmap.org ) at 2011-10-11 07:54 CDT
Warning: Unable to open interface vmnet1 -- skipping it.
Warning: Unable to open interface vmnet8 -- skipping it.
Nmap scan report for seclab1.cs.wisc.edu (128.105.183.26)
Host is up (0.026s latency).
Not shown: 947 closed ports, 49 filtered 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$ █
```

## 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

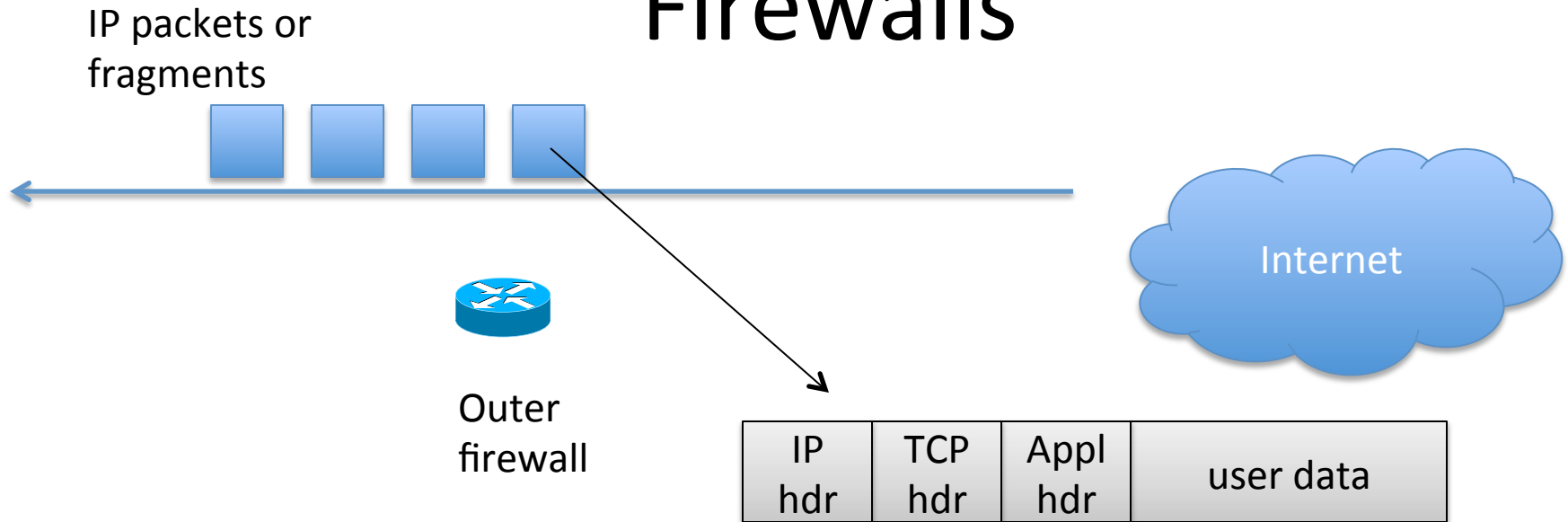
# Network DMZ



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

Firewall rules to disallow traffic from Internet to internal services

# Firewalls

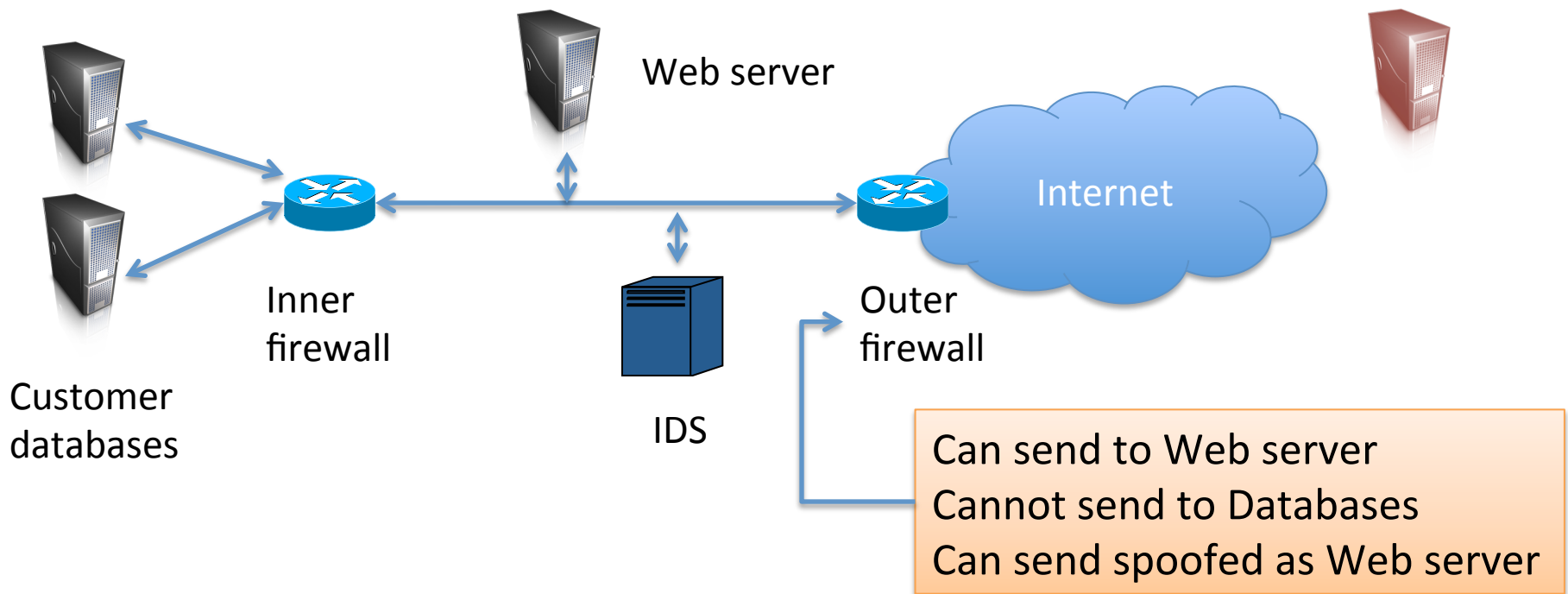


Firewalls apply rules to packets to determine routing actions

- Stateless: decision must be made looking at single packet (fragment)
- Stateful: reconstruct packets from fragments, maybe even TCP messages
- Host based or network based

# Port scanning behind firewalls: Idle scans

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



# 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
- Old systems: IPID incremented with each IP packet sent

# IPv4

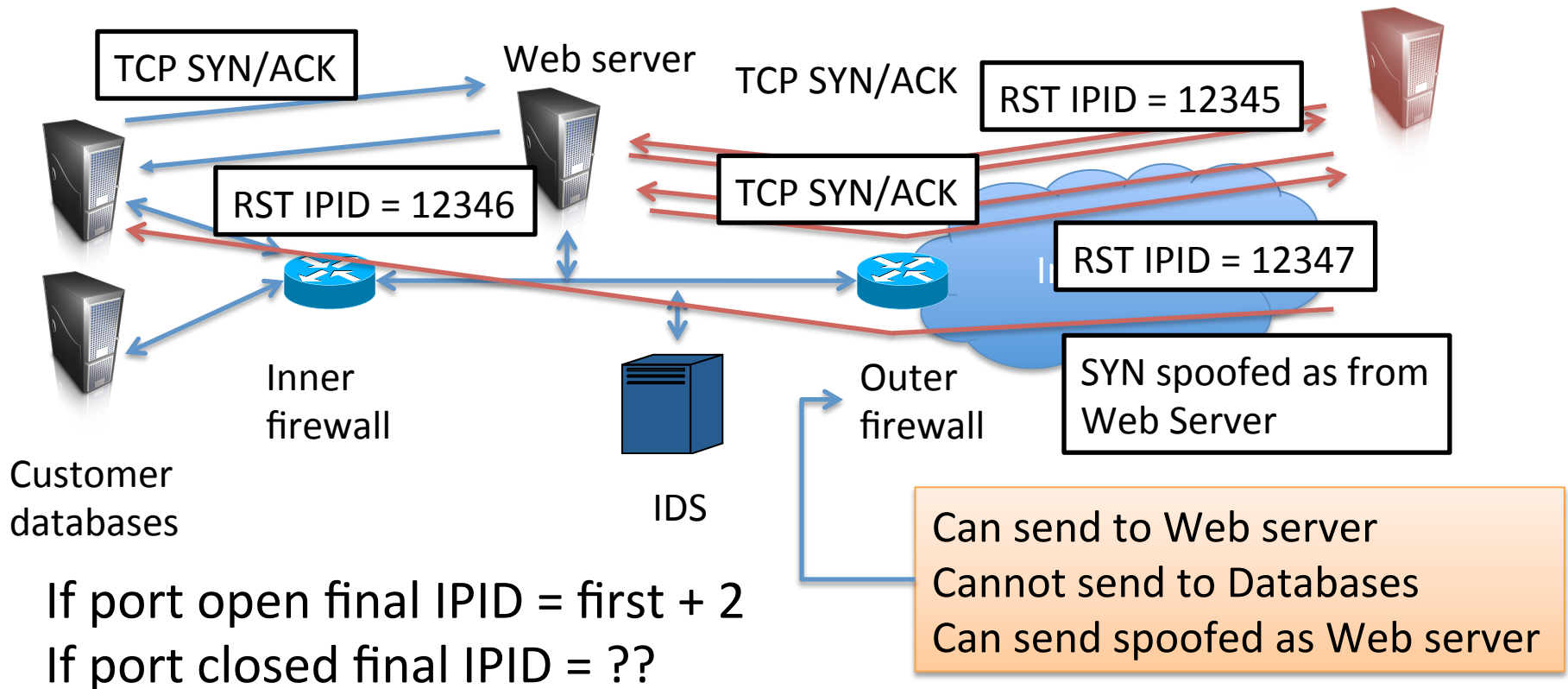


Ethernet frame  
containing  
IP datagram

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

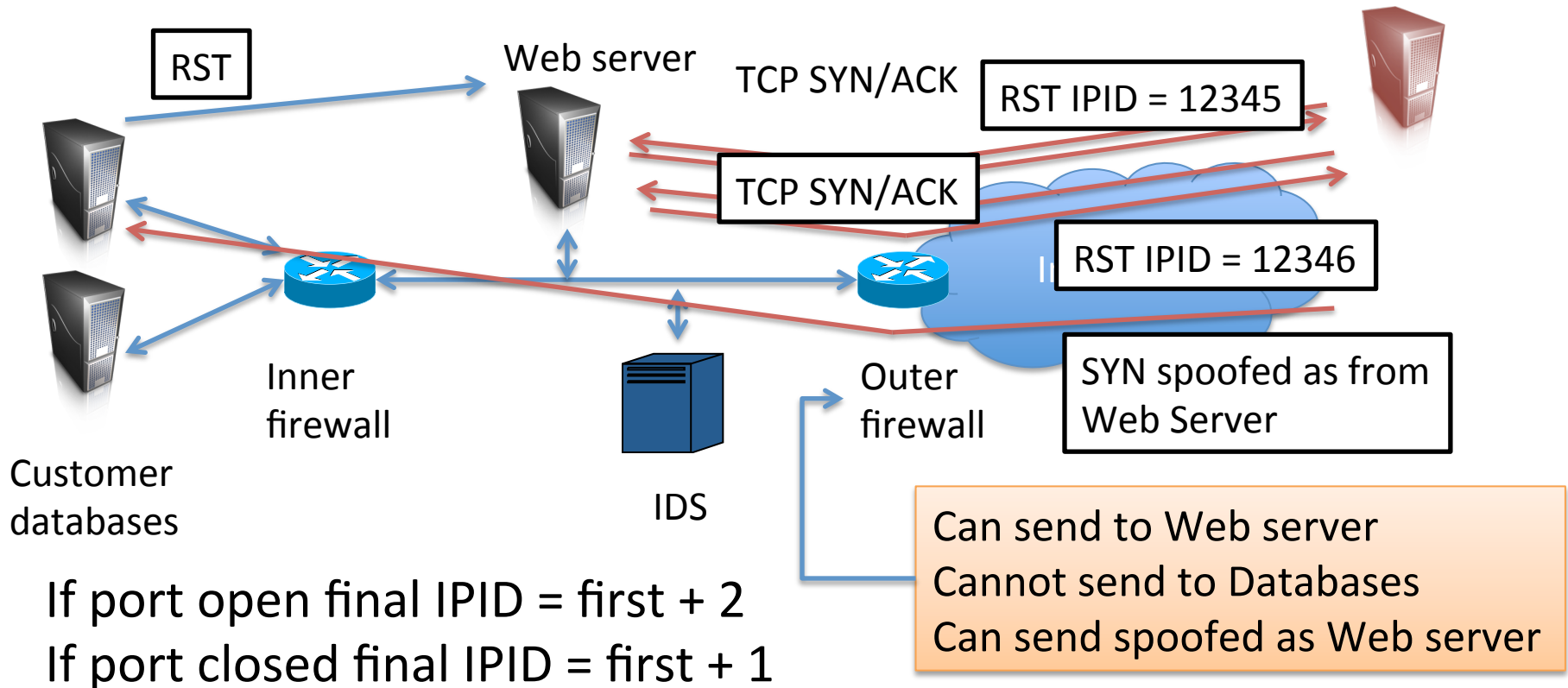
- We want to avoid sending any non-spoofed packets to the target, but still want to port scan it








# Idle scans

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



# Idle scans

 the attacker,  the zombie, and  the target.

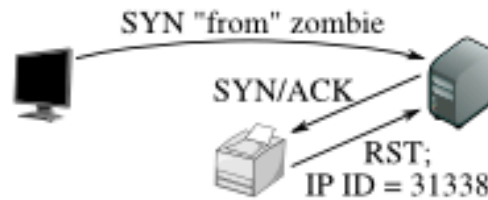
**Figure 5.1. Idle scan of an open port**

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!

# Idle scan

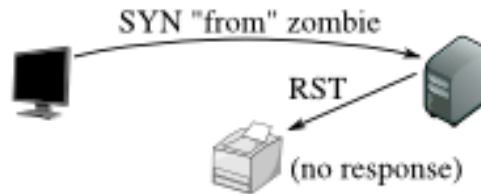
**Figure 5.2. Idle scan of a closed port**

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.

# 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 sequencability 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

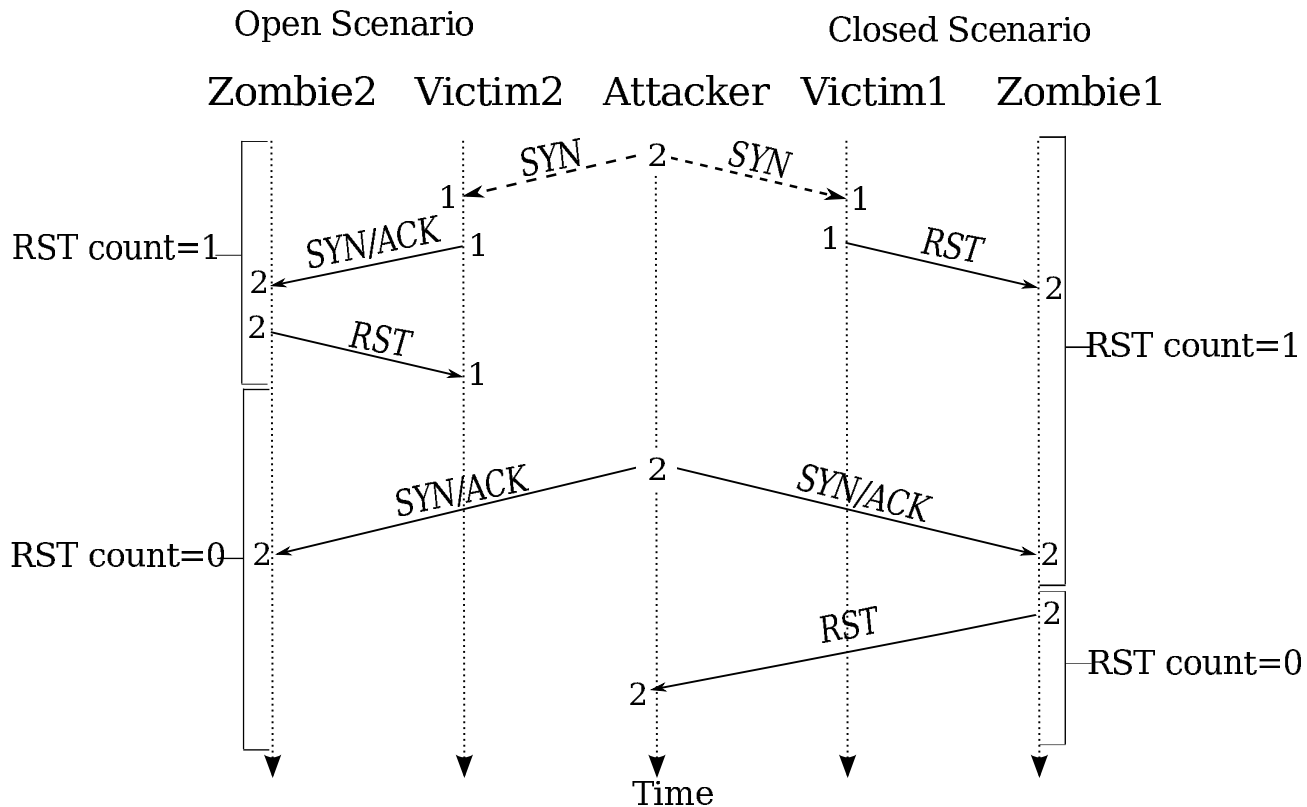


Figure 6: **RST rate limiting counterexample.**

# 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 (initial sequence number)

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

# Idle scan: SYN cache

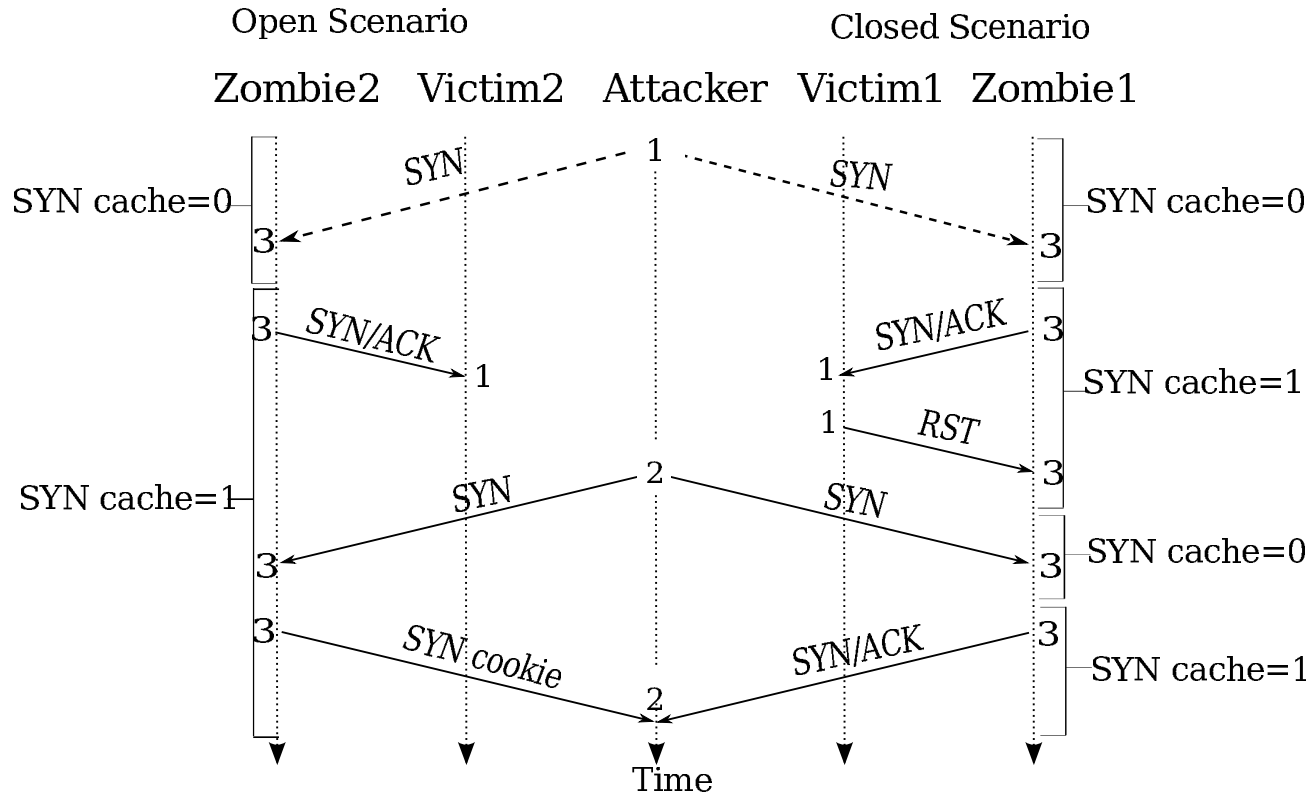


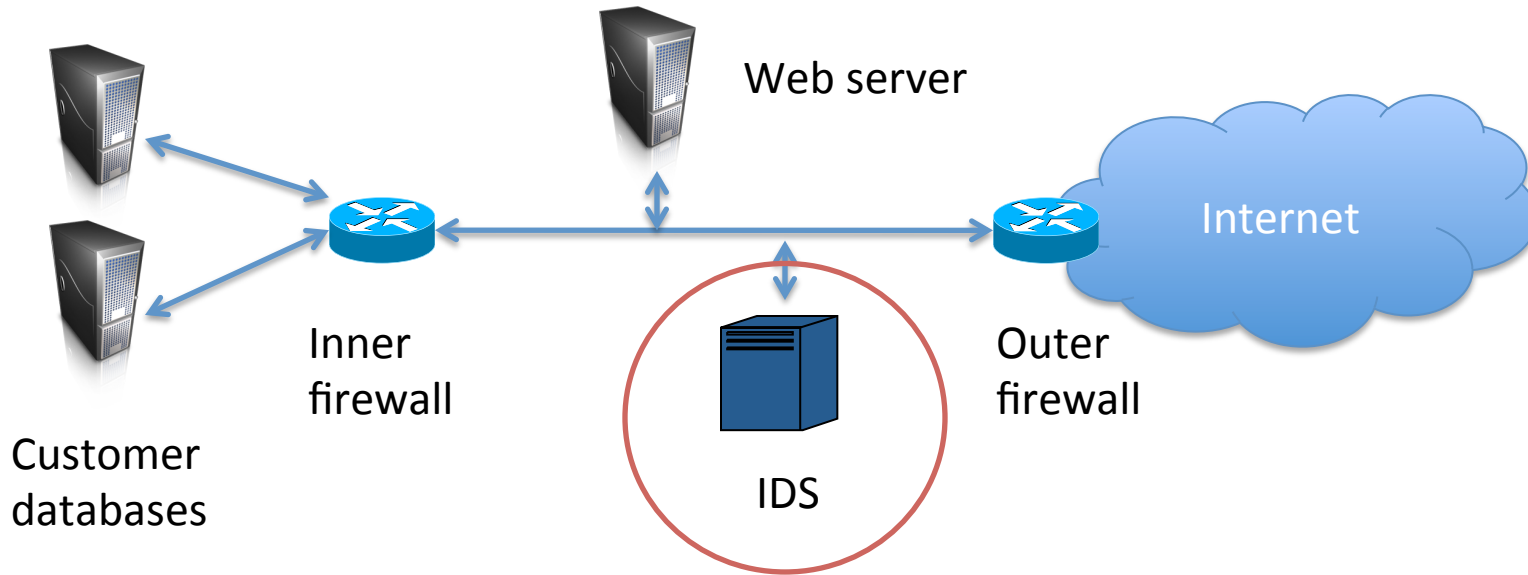
Figure 7: **SYN cache counterexample.**



# 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.
- <http://nmap.org/book/legal-issues.html>

# Network DMZ

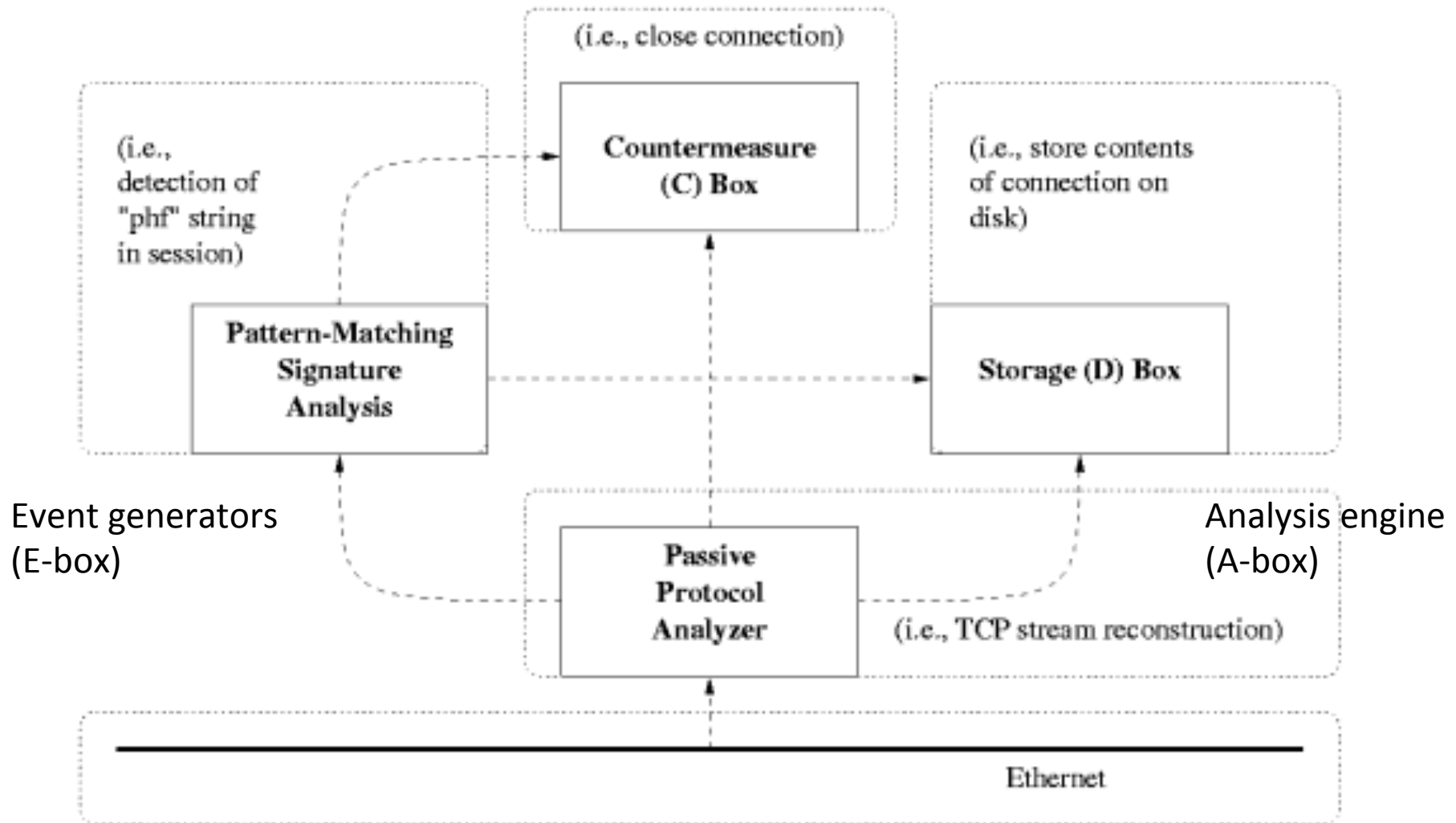


DMZ (demilitarized zone) helps isolate public network components from private network components

Firewall rules to disallow traffic from Internet to internal services

# CIDF

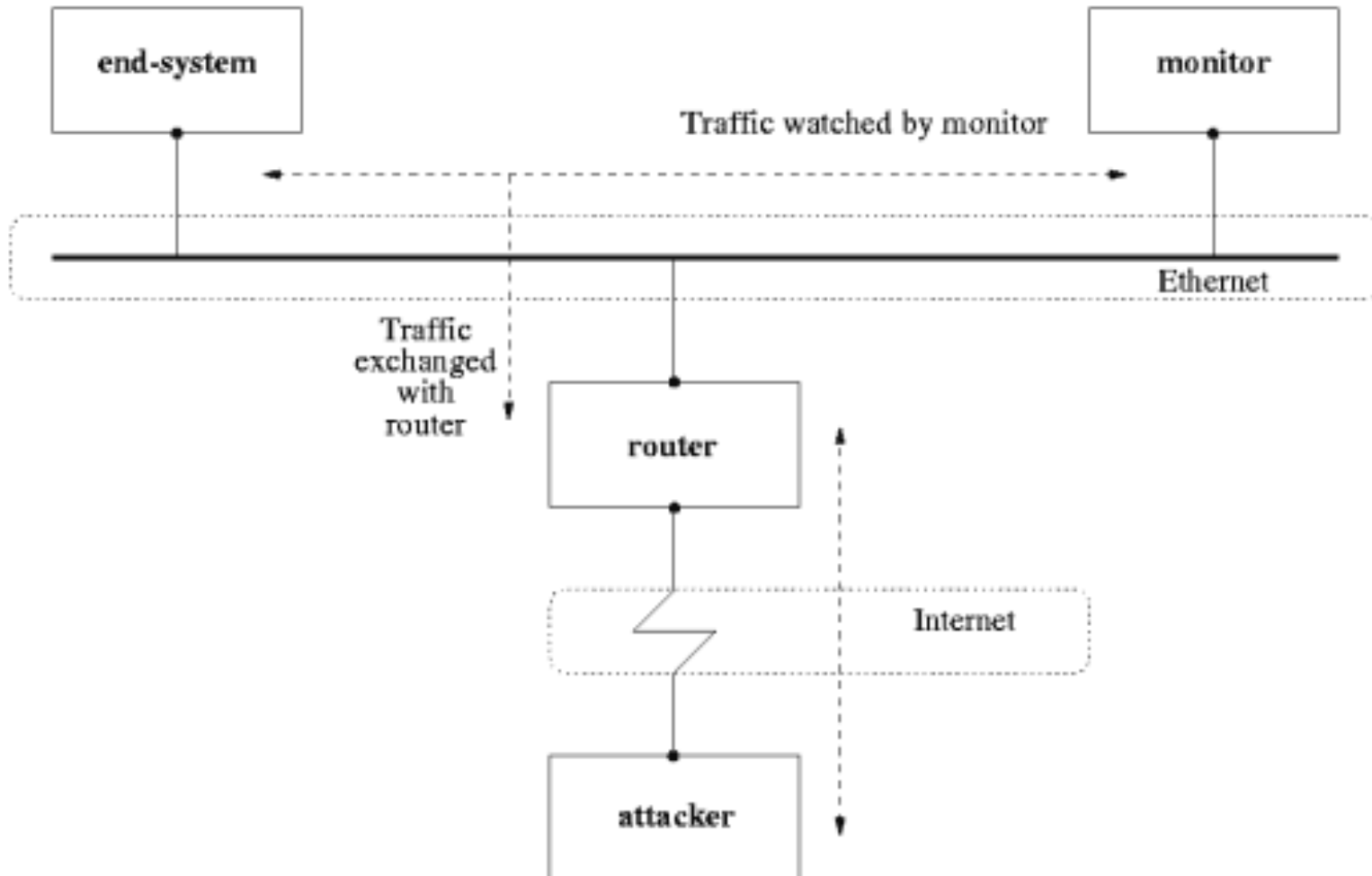
(Common intrusion detection framework)



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

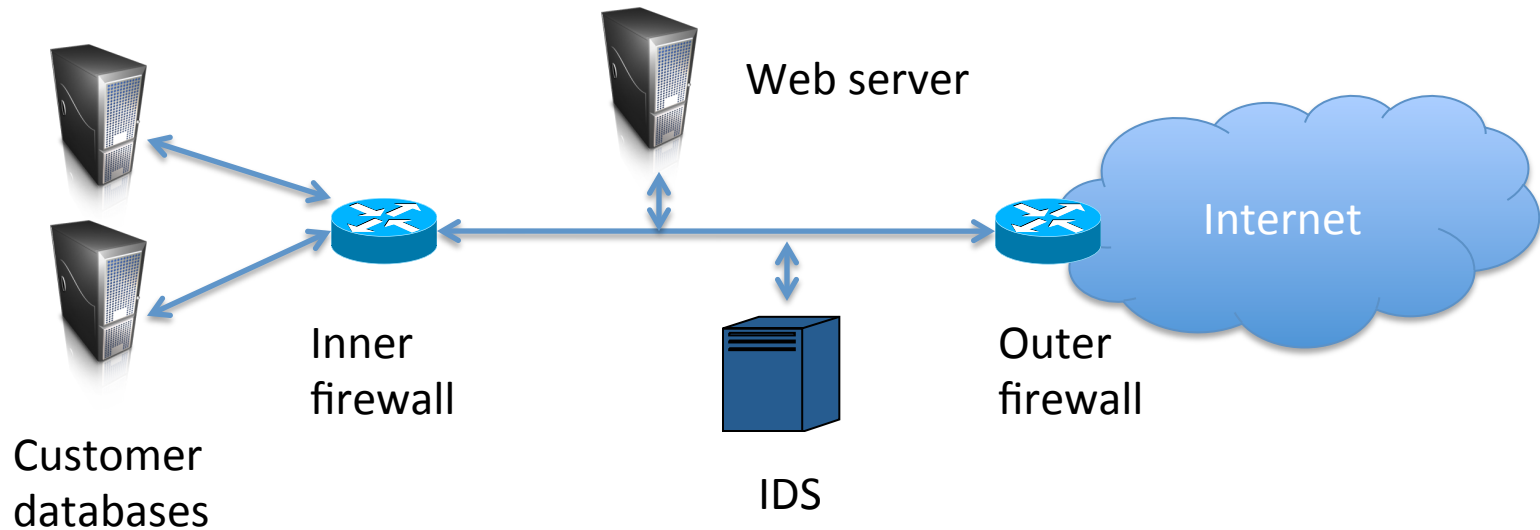
# Basic NIDS setup



From [http://insecure.org/stf/secnet\\_ids/secnet\\_ids.html](http://insecure.org/stf/secnet_ids/secnet_ids.html)

# Attacking or bypassing NIDS

- How do we circumvent a NIDS?



Overload attacks, crash attacks, subterfuge attacks

# Subterfuge attack example

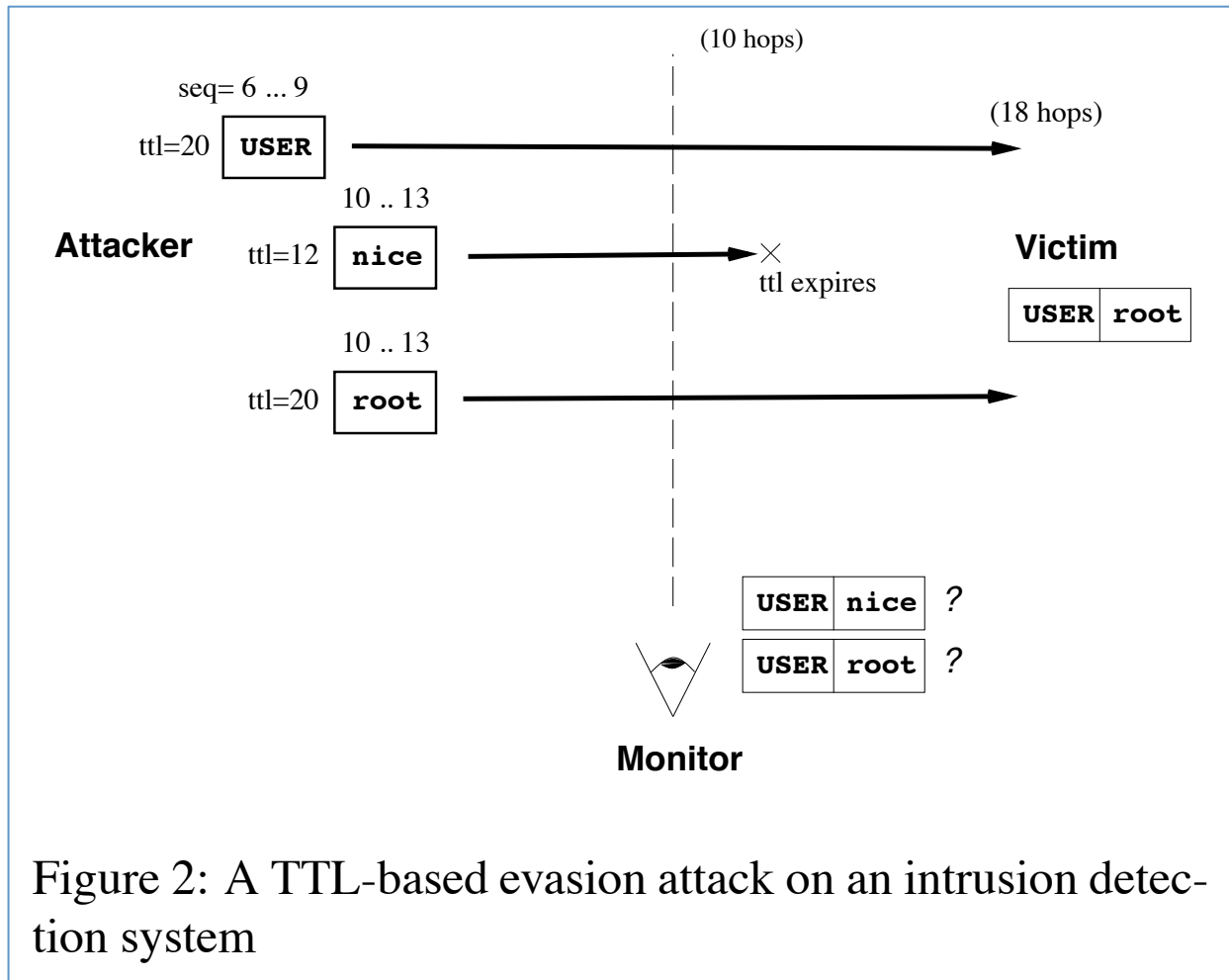


Figure 2: A TTL-based evasion attack on an intrusion detection system

# 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

<i>Feed Name</i>	<i>Feed Description</i>	<i>Received URLs</i>	<i>Distinct Domains</i>
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
<b>Total</b>		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

