Intrusion Detection

Motivation

- We can't prevent all break-ins
- There will always be new holes, new attacks, and new attackers
- We need some way to cope

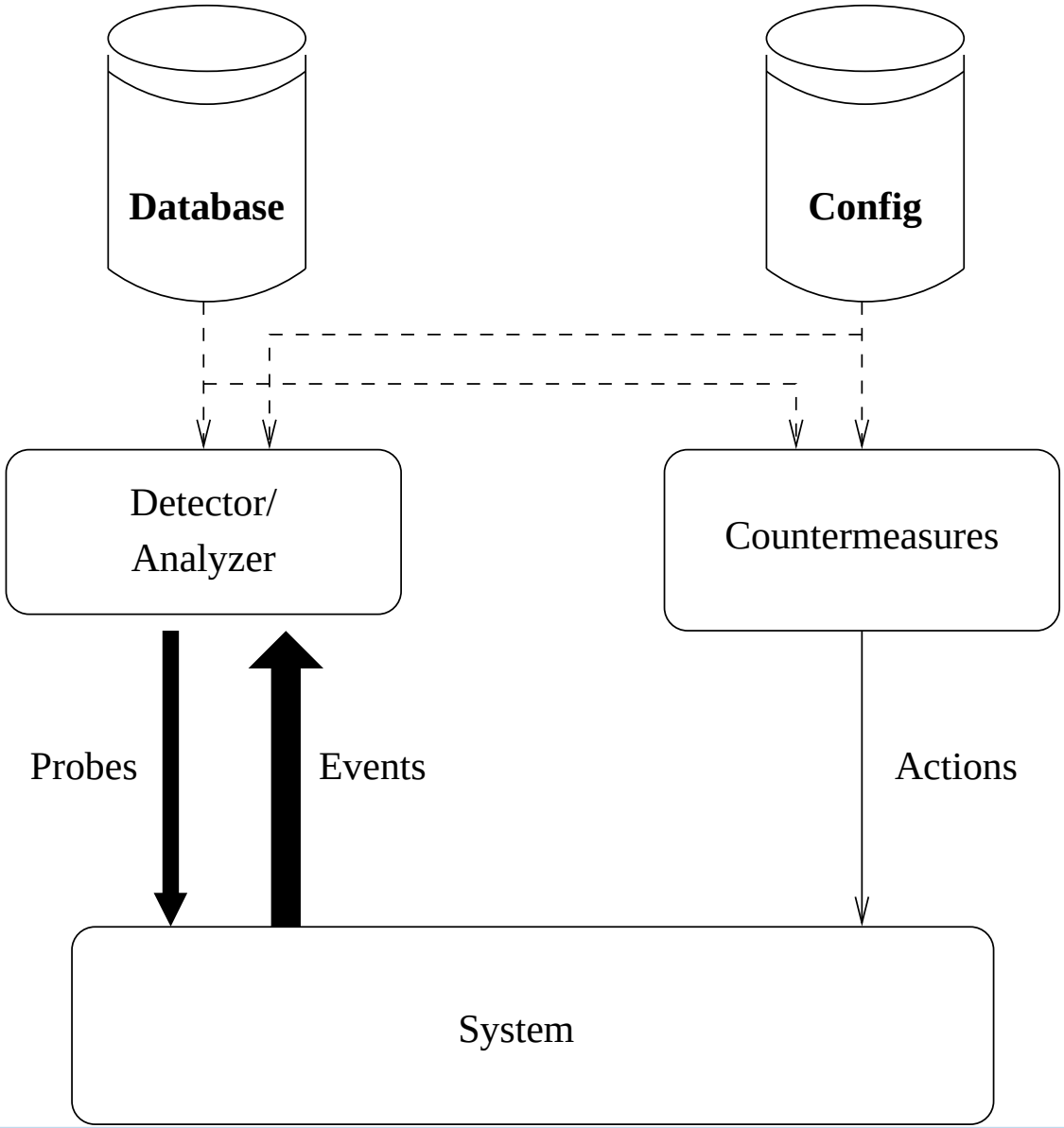
Defenses

- Harden the host
- Deploy a firewall
- Encrypt connections
- Use an *intrusion detection system* (IDS) to let us know that our other defenses have failed...

Just an Overview

- This lecture will just scratch the surface
- For more details, take COMS E6185

Generic Architecture



Fundamental Choices

- Location
- Type
- Actions

Location

- Host-resident
- Network-based
- Firewall-based

Type

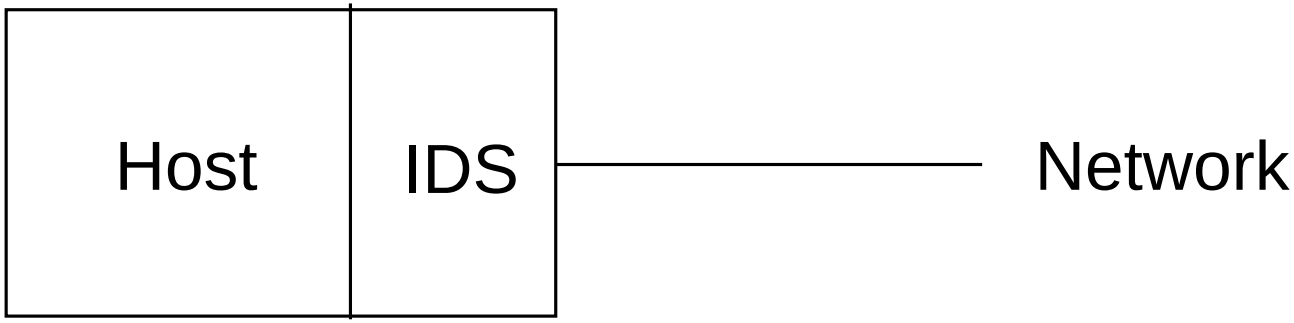
- Misuse detection (signature-based)
  - Specification-based
  - Hand-built
- Anomaly detection (statistical)
  - Hand-coded
  - Learning-based

Actions

- Alarms
- Shutdown

Location

Host-Based



- OS auditing mechanisms (log files, Solaris BSM, etc)
- Socket tap
- System call traces
- Shell command history
- Windows registry accesses
- Note: some of these also useful for forensics

Advantages and Disadvantage

- No confusion about what has happened
- Data is already decrypted
- But — may be expensive
- Subvertible
- Use a VM?
- Useful precaution: transmit data off-node immediately

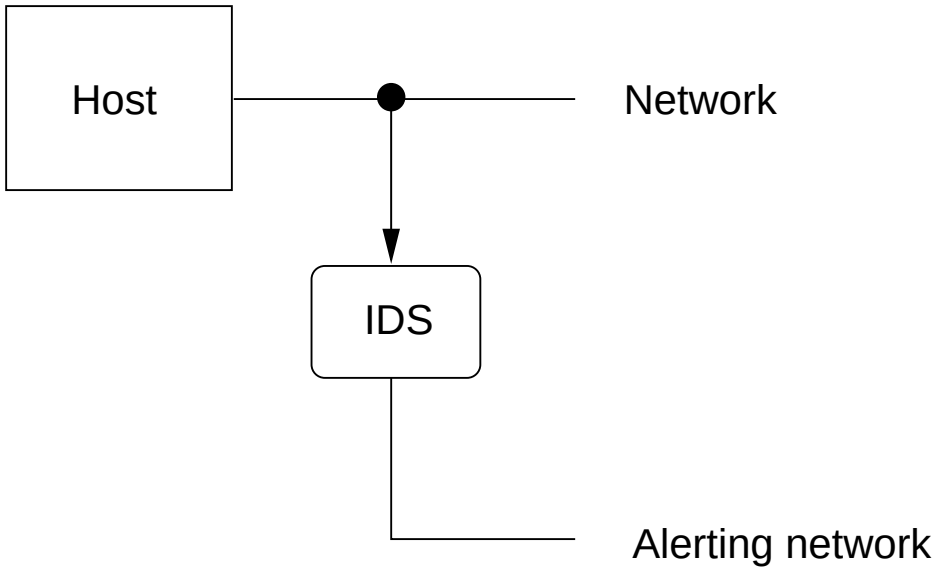
The Big Advantages of Host IDS

- More time
- More context
- Everything is reassembled
- Look at entire item, not streams
- Example: it's all but impossible to do email virus scanning in the network

Network-Based

- Packet-sniffing (via `tcpdump`?)
- In-line or in parallel?
- Can be confused
- Can't handle encrypted traffic

Net-Resident: Parallel

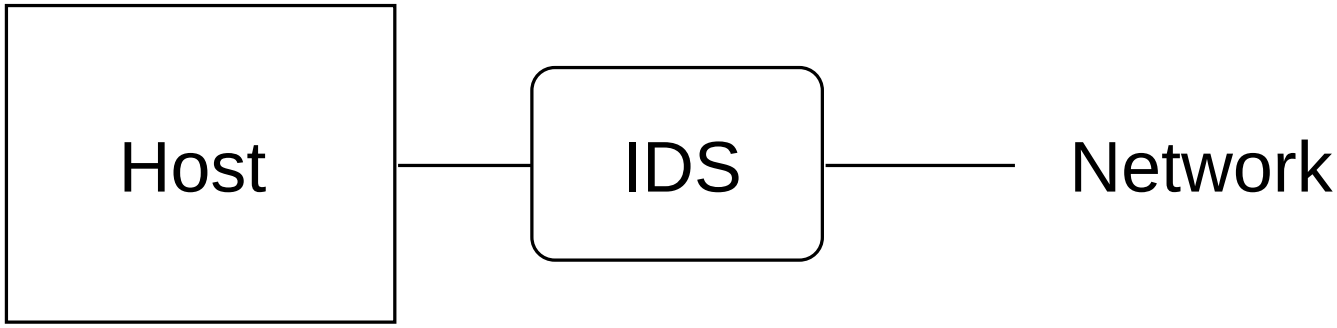


- Very unobtrusive
- But — need special hardware to tap an Ethernet
- Need some network connection to the IDS

Tapping an Ethernet

- Cannot simply wire IDS to jack
- Best solution: one-way tap gear
- Note: taps one traffic direction only; may need a pair of them
- Some switches have a monitoring port (AKA spanning port, mirroring port, etc) — can receive copies of data from any other port

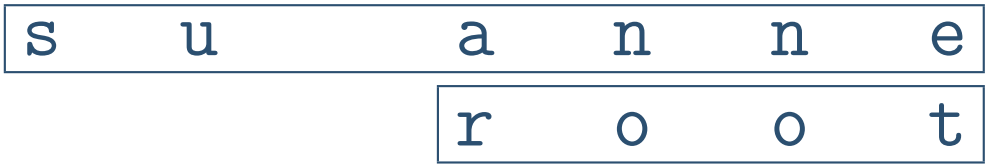
Net-Resident: Serial



- Can't miss packets
- But — if it crashes, the host is unreachable
- (Often part of firewalls)
- More detectable, via timing
- Can the IDS box be hacked?

TCP Normalization

- Attackers can play games with TCP/IP to confuse network-resident IDS
- Example: overlapping fragments:



Which fragment is honored? Varies!

- TTL games: give some packets a TTL just high enough to reach the IDS, but not high enough to reach the destination host
- Solution: *TCP normalizer*, to fix these

Locations

- Outside the firewall?
- We *know* there are bad guys there; what's the point?
- Just inside? What's the threat model?
- On sensitive internal nets?
- In front of each sensitive host?
- In "dark space"?

What's Dark Space?

- A block of address space not used by real machines and not pointed to by DNS entries
- There is no legitimate reason to send packets to such addresses
- Therefore, any host sending to such addresses is up to no good
- Commonly used to detect scanning worms

What's the Purpose of the IDS?

- Unless you're a researcher, all you care about is real threats to your own machines
- Inside edge of the firewall? Can detect data exfiltration, but misses insider attacks
- Sensitive internal nets: detect threats aimed at them
- Watching each host? Detect attacks on inside hosts from other hosts on the same LAN
- Dark space? Detect scanning worms (and attackers)

Auto-Quarantine

- Many organizations implement "auto-quarantine"
- This is especially common for university residence hall networks
- Machines that do too much scanning (and in particular attempt to probe dark space) are assumed to be virus-infected
- They're moved to a separate net; the only sites they can contact are Windows Update, the Mac equivlanet, anti-virus companies, and the like

CS@CU

Honeypots and Honeynets

- Special-purpose host or network designed to be attacked
- Equipped with copious monitoring
- Lure the attacker in deeper
- Waste the attacker's time; study the attacker's technique
- Note well: keeping honeypot (and dark space) addresses secret is vital

Extrusion Detection

- Detect bad things leaving your network
- Detect sensitive things leaving your network
- Finds theft of inside information, either by attacker or by rogue insider
- Can be done in the network or in application gateways

IDS Types

Signature-Based

- Enumerate known types of misbehavior
- Basis for most anti-virus software
- New attacks require new signatures
- Advantage: few false positives
- Disadvantage: can't detect new attacks

Specification-Based Signatures

- Define all possible legal behavior
- Note: not necessarily protocol-based — want to know what's legal in *your* environment
- Anything else is an attack
- But — very hard to build such a model

Anomaly-Based Detection

- Learn what "normal" is
- Train system in known-safe environment
- Any departure from this is presumed suspicious
- Can detect novel attacks
- But — frequent false positives

Actions

- Alarms — rely on a human to react

⇒ Good for after-the-fact clean-up

⇒ But — can't cope with high alarm rate

- Shutting it down — prevent further damage

⇒ But — can turn into a denial of service attack

Simple Monitoring

A Simple Approach

- I ran this command for a while, on two hosts:

```
tcpdump -p -l "tcp[13] == 0x2 and dst $us"
```

- What does it do?
- Logs all TCP SYN-only packets addressed to us (tcp[13] is the flags byte in the TCP header; 0x2 is SYN)

Some Results

- About 85 probes apiece, during a 30-hour run
- 63 different ports scanned
- Some obvious: http, ssh, Windows file-sharing, SMTP, web proxy
- Some strange: 49400–49402, 8081–8090, 81–86
- Some ominous: terabase, radmin-port
- Most probers looked at one port; one looked at 46 ports

The Most Probed Ports

Scans	*Port*
3	ms-wbt-server
3	ssh
5	8000
5	http-alt
6	ms-sql-s
6	radmin-port
7	BackupExec
8	smtp
9	WebProxy
9	http

What Did The Probers Want?

- WebProxy and SMTP are probably for spam email and connection-laundering
- The others look like probes for known vulnerabilities
- http could have been a "spider" or it could be looking for known holes

Dshield.org Data

Name	*Port*	
25	495300	SMTP
1433	128054	MS-SQL
445	127354	microsoft-ds (Conficker?)
34724	108615	
135	72758	MS name resolution
8906	52924	
139	52508	NetBIOS
1434	51798	Slammer worm (2003)
1211	48532	
23	36005	Telnet

Note that some ports are mysterious

Bad Neighborhoods

- I see more probes here than elsewhere. Why?
- There are different "neighborhoods" — ranges of IP addresses — in cyberspace
- University networks are good hunting — few firewalls, good bandwidth, many poorly-administered machines
- Newly-allocated network blocks have few hosts, and aren't scanned as much

Finding Compromised Hosts

Finding Attacking Hosts

- Suppose you've identified an attacking host. Now what?
- Get data: IP address and (when feasible) MAC address
- Find it

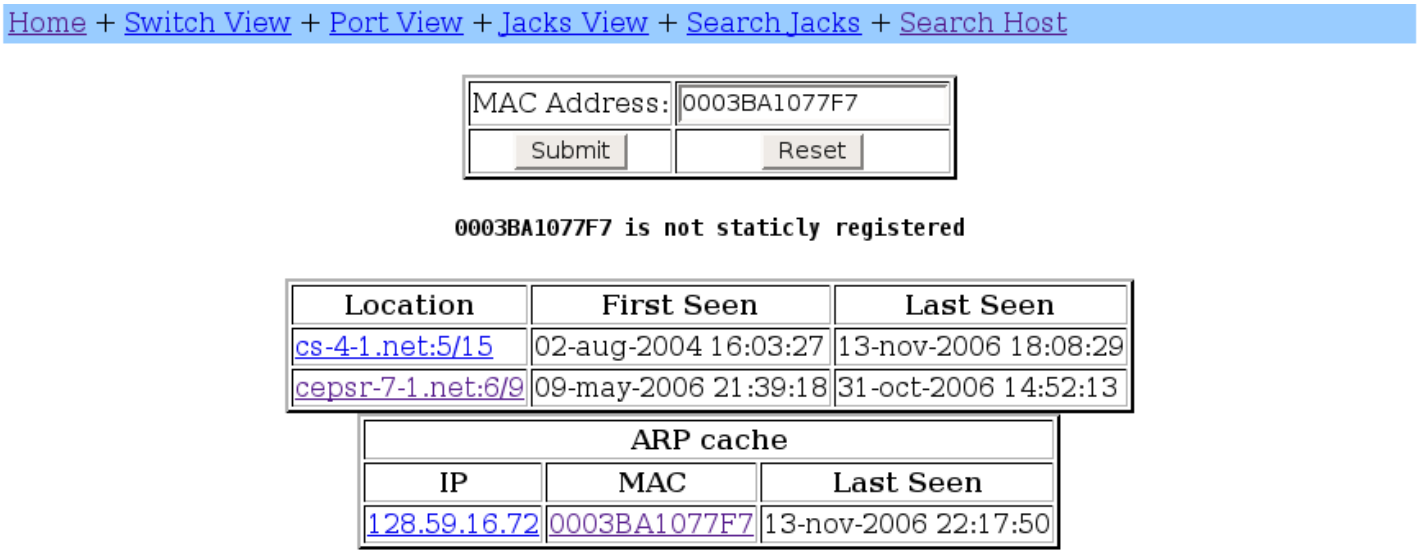
Databases

- Must be able to map IP address to location
- Must be able to map IP address to person
- Difficult on this campus — wide-open nets
- Primary reason for host registration in many places

Layer 2 Data

- Enterprise-grade switches are "managed"
- They can map an IP address or a MAC address to a physical port
- Especially useful if the attacker is forging addresses...

Switch Data



Home + Switch View + Port View + Jacks View + Search Jacks + Search Host

MAC Address:	0003BA1077F7
Submit	Reset

0003BA1077F7 is not staticly registered

Location	First Seen	Last Seen
cs-4-1.net:5/15	02-aug-2004 16:03:27	13-nov-2006 18:08:29
cepsr-7-1.net:6/9	09-may-2006 21:39:18	31-oct-2006 14:52:13

ARP cache		
IP	MAC	Last Seen
128.59.16.72	0003BA1077F7	13-nov-2006 22:17:50

Note that a single MAC address has shown up on two different switch ports, in different buildings. This is reasonable for a laptop, but not for the CS department's FTP server!

Locating an Evil WiFi Laptop

- Ask the switch what access point it's near
- Ping-flood the machine
- Wander around the room looking at the lights...

Cleaning Up a Host

- Suppose you find that one of your own machines is compromised
- Will you prosecute? Call the police *first*, to preserve evidence
- Will you (or can you) do forensics to learn how the attacker got in?
- At the least, figure out the patch level of all components and note the configuration
- Then — format the disk and reinstall; disinfecting a machine is often impossible

IDS in the Real World

Evaluating an IDS

- Accuracy — false positive and false negative rate
- Performance
- Ability to handle new attacks
- Fault tolerance
- Timeliness of alerts

Problems with Commercial IDS

- Constant (often costly) updates required
- False negatives — missed attacks generate false sense of security
- False positives — expensive to handle, especially if you shut things down
- Bad sensor positioning