

Intrusion Detection Systems (IDS)

John Kristoff

jtk@depaul.edu

+1 312 362-5878

DePaul University

Chicago, IL 60604

Why IDS?

- Interesting, but immature technology
- Provides lots of data/information
- Generally doesn't interfere with communications
- Anything that improves security...

What is IDS?

- Ideally, immediately identifies successful attacks
- Should have a immediate notification system
 - Out-of-band from the attack if possible
- Probably can also monitor attack *attempts* too
- Might have attack diagnosis, recommendation and/or automated attack mitigation response
- Lofty goals:
 - 0% false positive rate
 - 0% false negative rate

Privacy issues

- Does an IDS violate privacy?
 - Are packet headers (protocols) private?
 - Is identification (an address) private?
 - Are packet contents private (payload)?
 - Are communications (flows/sessions) private?
- Where is the IDS?
- Who manages the IDS?
- How is the IDS data handled and managed?

Storage, mining and presentation

- IDSs can collect LOTS of information
- What is useful data?
- What are you looking for?
- Data correlation within/outside of the IDS?
- What does the admin see?
- Where and for how long do you keep data?
- How do you secure access to IDS data?

Host IDS

- An integral part of an end–system
 - System log monitor
 - Kernel level packet monitor
 - Application specific
- A very good place to put security
- Distributed management issues
- Not all end systems will support an IDS
- Will be as useful as the end user is clueful

Network IDS

- An add-on to the communications system
- Generally passive and invisible to the ends
- May see things a host IDS cannot easily see
 - Fragmentation, other host attacks (correlation)
- May not understand network traffic
 - Unknown protocols/applications, encryption
- May miss things that don't cross its boundary

Anomaly detection

- A form of artificial intelligence
- Learn what is normal for a network/system
- If an event is not normal, generate alert
- May catch new attacks not seen before
- For a simple, but effective example see:
 - *Detecting Backdoors*, Y. Zhang and V. Paxson, 9th USENIX Security Symposium
- An area of active research

Signature matching

- Know what an attack looks like and look for it
- Very easy to implement
- Low false positive rate
- Most current IDSs are of this type
- Easy to fool
- Signatures must be added/updated regularly

Honeypots

- A system that welcomes attacks
 - Unbeknownst to the attacker generally
- The system is very closely monitored
- Can be used to test new technology/systems
- Generally educational in nature
- Helpful as trend monitor for that system type
- Be careful honeypot doesn't become liability

Possible IDS failure modes

- Fragmentation, state and high-speeds
- Requires lots of CPU, memory and bandwidth
- Inability to decode message/transaction
 - $t^{\wedge}Hr r^{\wedge}Hm56^{\wedge}H^{\wedge}H //^{\wedge}H -u^{\wedge}Hr f$
- Background noise
- Tunnelling/encryption
- IDS path evasion
- Stupid user tricks

The poor man's Network IDS

- Setup a router subnet and unix host
- Block all outgoing/incoming packets
 - `access-list 100 deny ip any any log`
- Log packets (filter matches) with `syslog`
- Use `perl/grep/uniq/...` to build simple reports
 - Total violations: 468
 - Top source host: badguy.org
 - Top dest. TCP port: 21 (ftp)

The poor man's host IDS

- Use snort (<http://www.snort.org>) or...
- Turn on all logging and do log reporting
- Install fake service and monitor
 - tcp_wrappers, back officer friendly
- Use *diff* (or equivalent), monitor file changes
 - Keep copies of data/configs elsewhere
- Use Tripwire or equivalent

References

- *Network Intrusion Detection, An Analyst's Handbook*, by Stephen Northcutt
- <http://www.cerias.purdue.edu>
- <http://www.usenix.org>
- `ids-request@uow.edu.au` in body put "help"
- <http://www.research.att.com/~smb/>
- <http://www.cert.org>
- <http://networks.depaul.edu>