IDS Shortcomings: What’s wrong with the current generation?

Robert Graham
Internet Security Systems
interop-01@robertgraham.com

"Knowledge without wisdom is a load of books on the back of an ass"
-- *Japanese proverb*

"Without wisdom, knowledge is nothing"
-- *Islamic proverb*

Background Radiation

- Cable-modems
  - 40 scans per day from all over Internet
- Worms
  - Incessant probes against port 111, 515, 53
  - LPRng, rpc.statd, DNS (Iquery, version.bind, TSIG), IIS bugs (UTF8, decoding, …)
- So what?

Forensics

- /cgi-bin/phf
  - Was the target vulnerable?
    - Server: Apache/1.0.1
  - Did it succeed?
    - HTTP/1.0 200 OK
  - What else did the attacker do?
    - Other scans?
    - Compromises?

Evasion

- Beyond whisker/fragrouter
- E.g. Snort/1.8
  - BackOrifice plugin
  - Telnet normalization for FTP
  - RPC normalization
- Subtle evasion
  - <img src=“http://victim.com/..%c0%af../system32/cmd.exe?...”>

Education

- Installation != Comprehension
  - Installing IDS is the easy part
  - What do alerts mean?
  - Should I be worried?
  - Does this mean I have been hacked?
  - Where does this fit within my policies?

Why do you want IDS?

- Pages you when you've been hacked?
  - No, it doesn't do that
- Intelligence, visibility
  - Yes, it does that very well
- Logging, audit trail
- Policy enforcement

All products are tools

- Firewalls
  - Firewalls don’t stop hackers, people stop hackers (using firewalls)
- Crypto
  - Only works with strong keys/passwords
- Anti-virus: needs updating
- IDS
  - Tools to track hacker activity

Remedies

- Vendors
  - Make better products
- Customers
  - Make better people :-)

Remedies: workload reduction

- Removal of duplicates
  - E.g. SQL scripts
- State-based rather than stateless
  - E.g. HTTP return code
- Integration with scanner
- Integration with policy
  - E.g. attacks from DMZ against internal network very bad

Remedies: intelligence

- Include more data
  - More packets (e.g. sniffer)
  - More context (e.g. whois)
- Don’t wait for products
  - Set this up yourself
  - Have a network map handy
- Customer Scenario
  - Integrated database with everything

Remedies: education

- Training, training, training
  - Product, general
- Certification
  - E.g. CISSP, SANS
- On-line resources
  - E.g. BUGTRAQ

Conclusion

- IDS is *integrated*
  - It only works as part of overall security infrastructure
  - Infrastructure = products *and* people
- IDS is new
  - Still in its initial generations
- IDS is a tool
  - You use IDS
- IDS is fun