Intrusion Detection, Deception or Prevention?

David M. Piscitello
Core Competence, Inc.
mailto:dave@corecom.com

“An ounce of prevention is worth a pound of cure”
Benjamin Franklin, Poor Richard’s Almanac

“People are idiots”
Scott Adams, *The Dilbert Principle*

Reactive or Proactive?

If we exerted more effort to secure our systems, we wouldn’t have to rely on IDS or Honeynets

The sum of our bad habits

…is staggering!

- Shoddy Authentication
  - Limping along (still!) with passwords!
- Liberally defined Access Controls
  - Policies are outsider-focused (Who’s an outsider these days?)
  - Reactionary applications of policy to insiders (Orwellian filtering of content)
- Accounting vs. accountability

Policy?
Who has time for *Policy*?

- Policy and documentation do not match deployed systems and operating practices
- Pace of security technology change forces implementation without
  - due consideration to its impact,
  - adequate planning and testing, and
  - organizational awareness of its effects
- Policies deteriorate to “what the security technology provides”

But the Most Aggregious Offender Award goes to…

- Lame software (blame the vendor)
  - Features and time to market are more important than security
  - Little attention to (secure) code review
  - Consumers are beta (even alpha) testers
- Lame practices (blame yourself)
  - tolerate of poor software
  - don’t apply security patches
  - choose ease of use and availability over security (“Remember password”?)
- I.e., we *all* provide a fertile hunting ground for attackers

Remedies: Software

- Keep Software Current
  - Majority of successful attacks are perpetrated against commonly known vulnerabilities for which patches, hot fixes or upgrades are available
- Know what’s running in your shop
  - Investigate how new software “behaves” before you put it in production

Remedies: System level/OS

- Vulnerability assessment is proactive
- Scan, identify, then mitigate vulnerabilities
  - Run current software versions, images, builds
  - Apply hot fixes, service and security patches
  - Eliminate unnecessary services
  - Audit routinely
  - Consider system and file system integrity software

Remedies: Perimeter Enforcement

- Outbound is as important as inbound
  - Back-channels, from Adware to Zombies, are evil—block them
- Apply stringent access controls
  - Block all *outbound services*
  - Wait for the phone to ring
  - Require justification for all outgoing connections
  - Routinely check logs for (new) outbound connection attempts to blocked ports

Remedies: Identity and Access Controls

- Implement strong authentication
  - Two or all of:
    - Something you know
    - Something you possess
    - Something you are
  - Trash the Post-It Inventory in your supply closet (along with velcro strips)
- Implement authorization
  - at host and object level

Remedies: (D)DOS prevention

- Prevent source address spoofing
  - Features like Unicast Reverse Path Forwarding block forged packets
- Make it harder for DOS attackers
  - Apply ICMP and multicast flood filters
  - Rate limiting features (e.g., cisco CAR)
  - Selected Packet Discard (SPD) features
- Router neighbor authentication
- See also
  - http://www.sans.org/ddos_roadmap.htm
  - http://www.tisc2001.com/presentations.html (Savage, Hancock presentations, S01, S02)

Remedies: Predictive Analysis

- Maximize your logging and auditing information
- Look for trends that have historical precedence
- Stay abreast of news that affects your industry/sector
- Monitor mail lists that identify exploits and vulnerabilities
  - See *Predictive Analysis*, by Jeff Stutzman (http://tisc2001.com/insight.html)

Top Ten “Obvious but Often Ignored” Security Practices

1. Define a security policy
2. Implement what you define
3. Make the policy known and enforce it
4. Never put default installs into production
5. Never allow a new service through your perimeter without analyzing it
6. Review code & scripts before you use them
7. Log *everything*, and routinely review what you’ve logged
8. Learn how to gather evidence from audit/log data
9. Report incidents to law enforcement agencies
10. Prosecute attackers

Conclusion

- Detection and Deception are sexy
- Prevention is mundane and tedious
- Over time, prevention will cost you less and protect you more
  - Let someone else's network be "the low hanging fruit"