Computer Security: Principles and Practice

Chapter 8 – Intrusion Detection

Intruders

- significant issue hostile/unwanted trespass
  - from benign to serious
- user trespass
  - unauthorized logon, privilege abuse
- software trespass
  - virus, worm, or trojan horse
- classes of intruders:
  - **Masquerader** : someone that penetrates the systems
  - **Misfeasor** : legitimate user that gain unauthorized privileges

Hacker Behavior Example

1. select target using IP lookup tools
2. map network for accessible services
3. identify potentially vulnerable services
4. brute force (guess) passwords
5. install remote administration tool
6. wait for admin to log on and capture password
7. use password to access remainder of network

Criminal Enterprise Behavior

1. act quickly and precisely to make their activities harder to detect
2. exploit perimeter via vulnerable ports
3. use trojan horses (hidden software) to leave back doors for re-entry
4. use sniffers to capture passwords
5. do not stick around until noticed
6. make few or no mistakes.

Insider Attacks

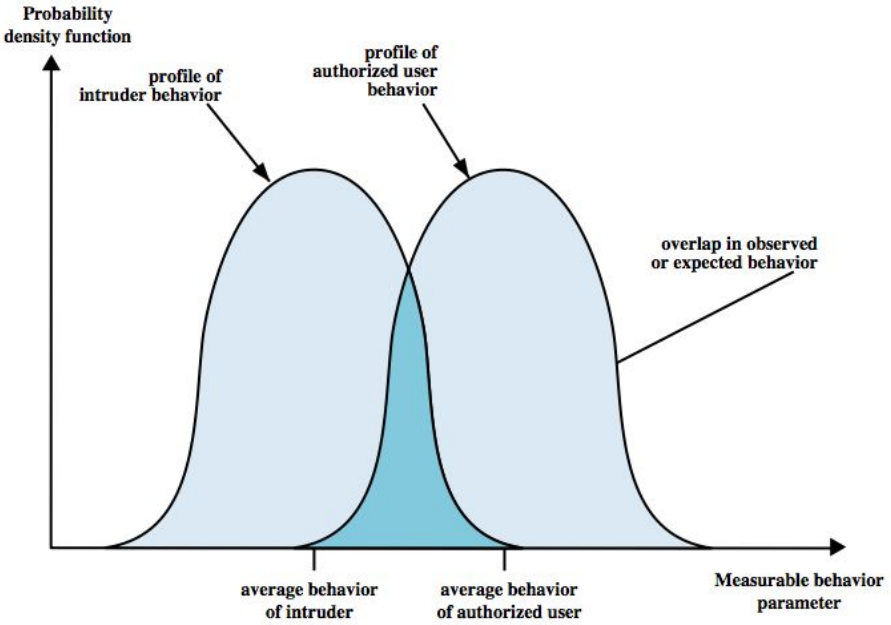
- among most difficult to detect and prevent
- employees have access & systems knowledge
- may be motivated by revenge / entitlement
  - when employment terminated
  - taking customer data when move to competitor
- IDS / IPS may help but also need:
  - least privilege, monitor logs, strong authentication, termination process to block access & mirror data

Intrusion Detection Systems

- classify intrusion detection systems (IDSs) as:
  - Host-based IDS: monitor single host activity
  - Network-based IDS: monitor network traffic
- logical components:
  - sensors - collect data
  - analyzers - determine if intrusion has occurred
  - user interface - manage / direct / view IDS

IDS Principles

- assume intruder behavior differs from legitimate users
  - expect overlap as shown
  - observe deviations from past history
  - problems of:
    - false positives
    - false negatives



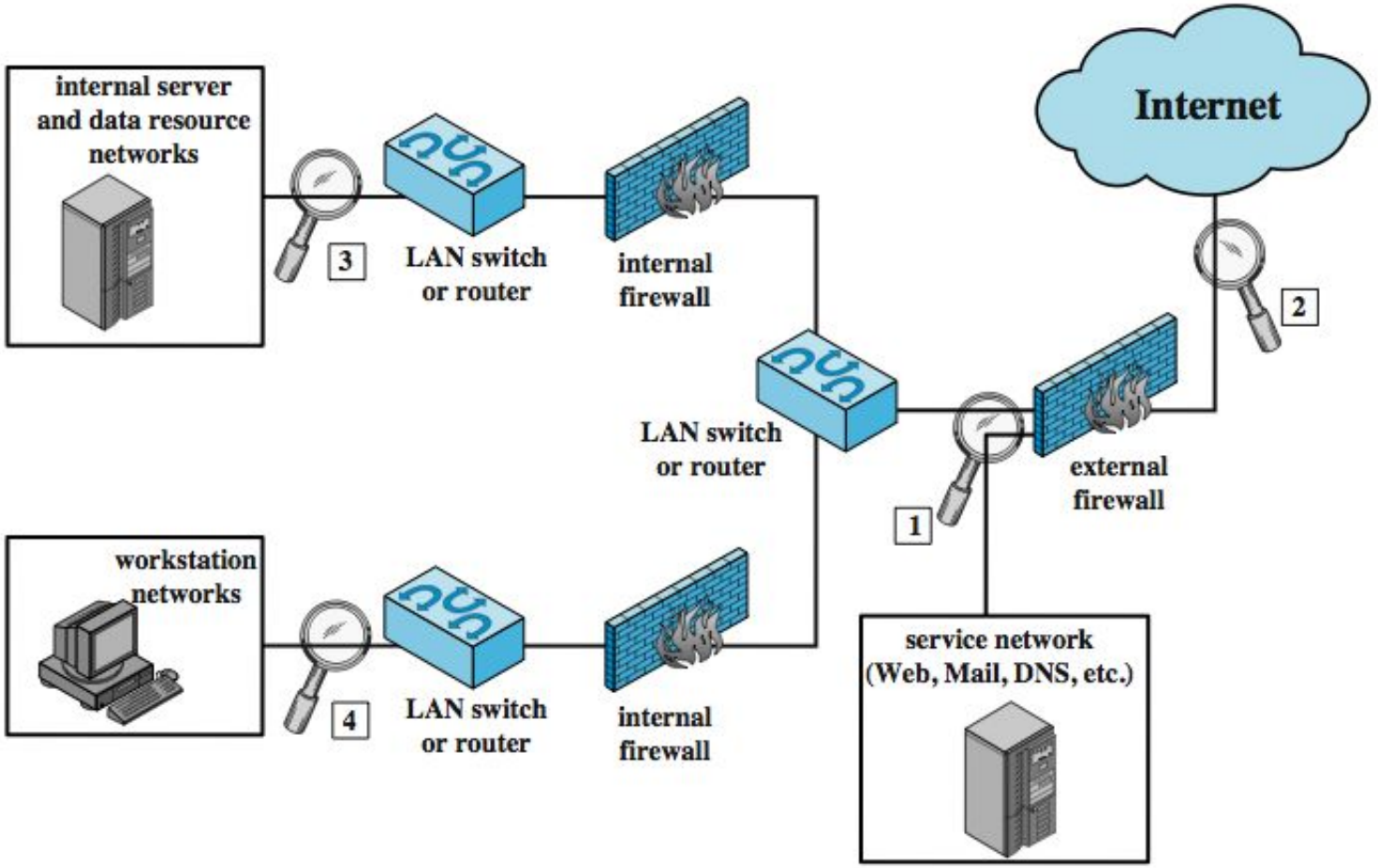
Host-Based IDS

- specialized software to monitor system activity to detect suspicious behavior
  - primary purpose is to detect intrusions, log suspicious events, and send alerts
  - can detect both *external* and *internal* intrusions
- two approaches, often used in combination:
  - anomaly detection - defines normal/expected behavior
  - signature detection - defines proper behavior
- *Audit record* fundamental in order to record the activities

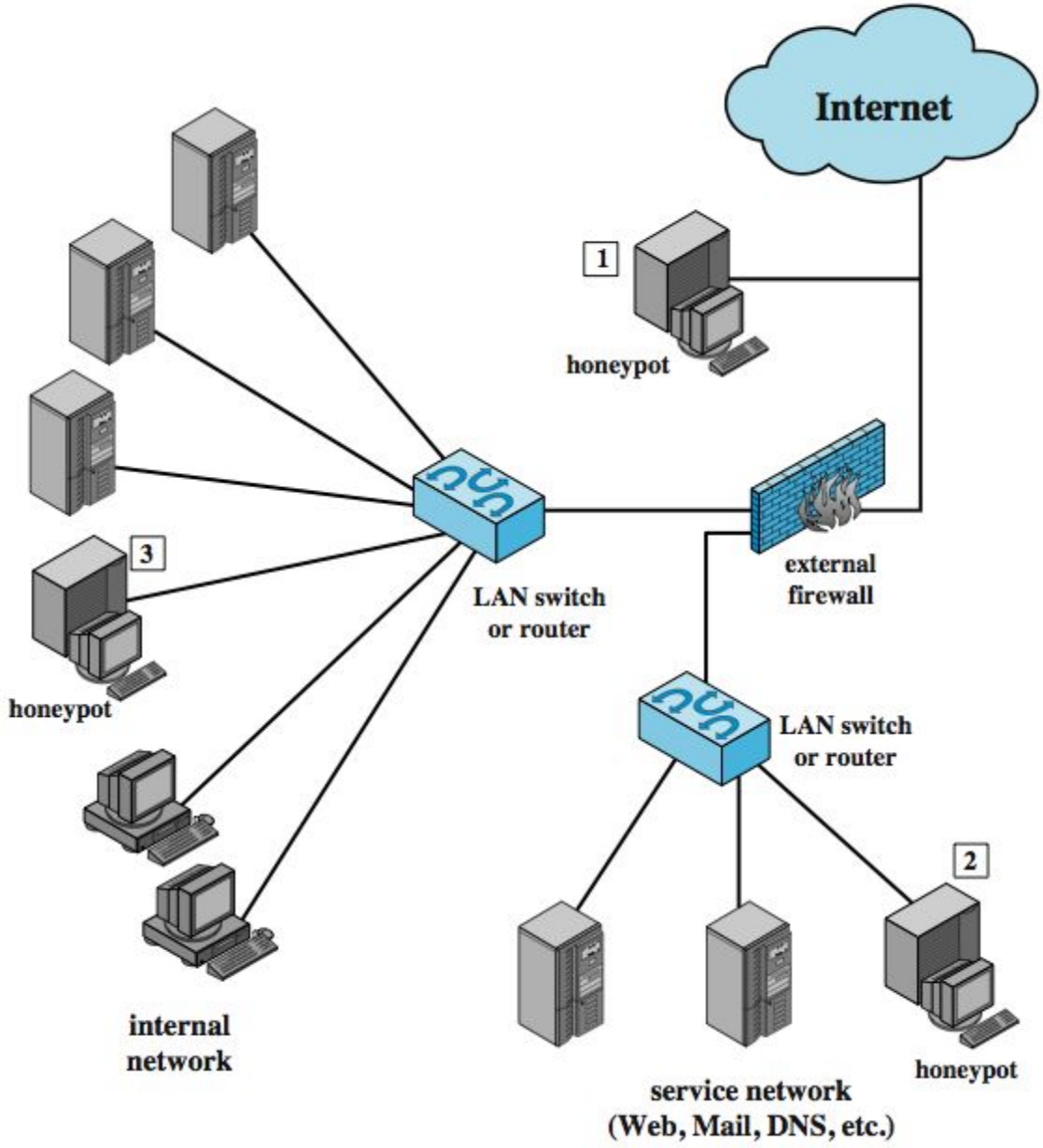
Network-Based IDS

- network-based IDS (NIDS)
  - monitor traffic at selected points on a network
  - in (near) real time to detect intrusion patterns
  - may examine network, transport and/or application level protocol activity directed toward systems
- comprises a number of sensors
  - inline (possibly as part of other net device)
  - passive (monitors copy of traffic)

NIDS Sensor Deployment



Honeypot Deployment



Summary

- introduced intruders & intrusion detection
  - hackers, criminals, insiders
- intrusion detection approaches
  - host-based (single and distributed)
  - network
  - distributed adaptive
- honeypots