Intrusion Detection

Introdution

- Security is a big issue for all networks in today's enterprise environment. **Hackers** and **intruders** have made many successful attempts to bring down high-profile company networks and web services.
- Many methods have been developed to secure the network infrastructure and communication over the Internet, among them the use of **firewalls**, **encryption**, and **virtual private networks**.

(cont…)

- Intrusion detection is a relatively new addition to such techniques. Intrusion detection methods started appearing in the last few years.

Intrusion and Intrusion Detection

- Intrusion : Attempting to break into or misuse your system.
- An intrusion is a deliberate, unauthorized attempt to access or manipulate information or system and to render them unreliable or unusable.
- Intruders may be from outside the network or legitimate users of the network.
- Intrusion can be a physical, system or remote intrusion.

Classes of Intruder

- **Masquerader:** An individual who is not authorized to use the computer (outsider)
- **Misfeasor:** A legitimate user who accesses unauthorized data, programs, or resources (insider)
- **Clandestine user:** (either)

Intrusion Techniques

- aim to gain access and/or increase privileges on a system
- basic attack methodology
  - information gathering
  - initial access
  - privilege escalation
  - covering tracks
- key goal often is to acquire passwords
- so then exercise access rights of owner

Attacks

- Password guessing
- Password capture

Intrusion Detection Systems (IDS)

- Intrusion Detection Systems look for attack signatures, which are specific patterns that usually indicate malicious or suspicious intent.
- Software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer system, mainly through a network.

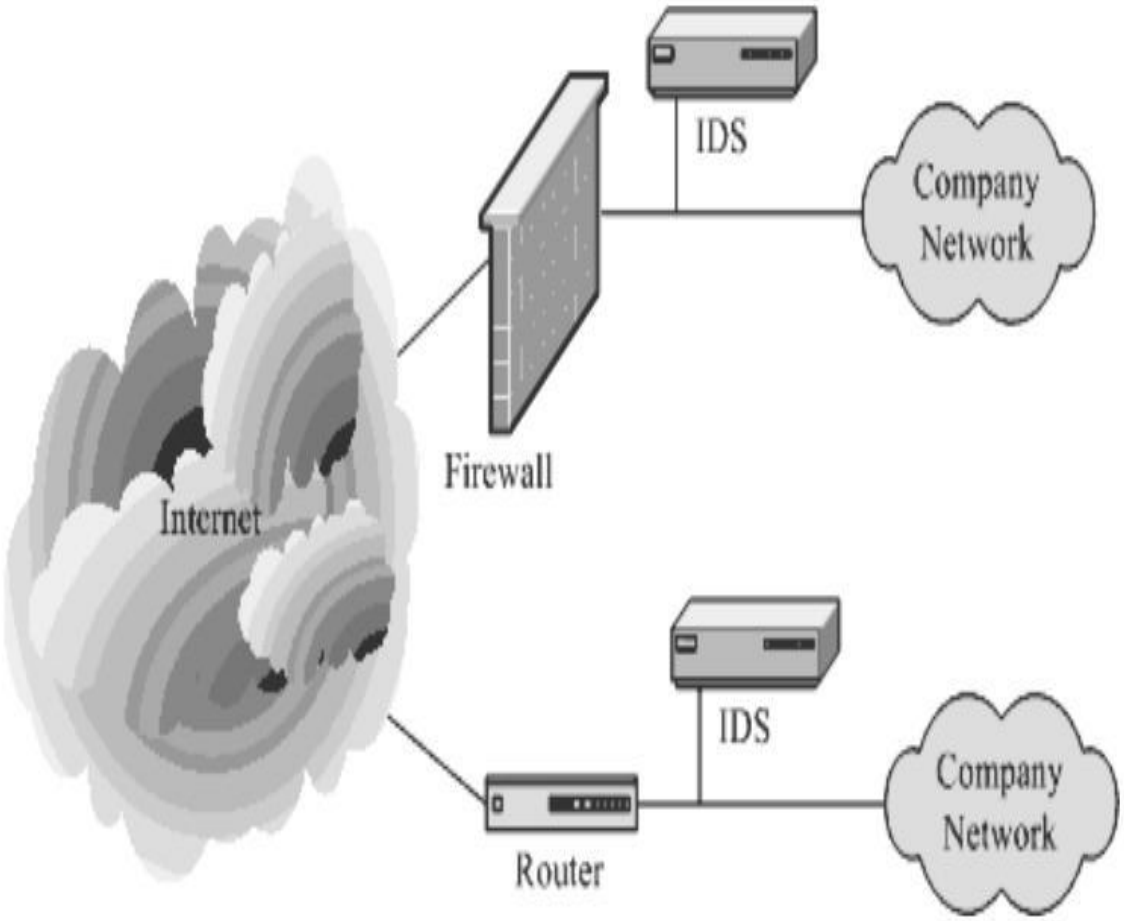

Figure 1-4 Typical locations for an intrusion detection system.

Intrusion Detection Systems (IDS)

- Different ways of classifying an IDS

  IDS based on
  - anomaly detection
  - signature based misuse
  - host based
  - network based

Anomaly based IDS

- This IDS models the normal usage of the network as a noise characterization.
- Anything distinct from the noise is assumed to be an intrusion activity.
  - E.g flooding a host with lots of packet.
- The primary strength is its ability to recognize novel attacks.

Drawbacks of Anomaly detection IDS

- Assumes that intrusions will be accompanied by manifestations that are sufficiently unusual so as to permit detection.
- These generate many false alarms and hence compromise the effectiveness of the IDS.

Signature based IDS

- Target intruders with known patterns
- ID system is programmed to interpret a certain series of packets, or a certain piece of data contained in those packets,as an attack.
- Most signature analysis systems are based on simple pattern matching algorithms. In most cases, the IDS simply looks for a sub string within a stream of data carried by network packets.

Drawbacks of Signature based IDS

- They are unable to detect novel attacks.
- Suffer from false alarms
- Have to programmed again for every new pattern to be detected.

Host/Applications based IDS

- The host operating system or the application logs in the audit information.
- These audit information includes events like the use of identification and authentication mechanisms (logins etc.) , file opens and program executions, admin activities etc.
- This audit is then analyzed to detect trails of intrusion.

Drawbacks of the host based IDS

- The kind of information needed to be logged in is a matter of experience.
- Unselective logging of messages may greatly increase the audit and analysis burdens.
- Selective logging runs the risk that attack manifestations could be missed.

Strengths of the host based IDS

- Attack verification
- System specific activity
- Encrypted environments
- Near Real-Time detection and response.
- No additional hardware

Network based IDS

- This IDS looks for attack signatures in network traffic via a promiscuous interface.
- A filter is usually applied to determine which traffic will be discarded or passed on to an attack recognition module. This helps to filter out known un-malicious traffic.

Strengths of Network based IDS

- Cost of ownership reduced
- Packet analysis
- Evidence removal
- Real time detection and response
- Malicious intent detection
- Complement and verification
- Operating system independence

Password Management

- front-line defense against intruders
- users supply both:
  - login – determines privileges of that user
  - password – to identify them
- passwords often stored encrypted
  - Unix uses multiple DES (variant with salt)
  - more recent systems use crypto hash function
- should protect password file on system

Password Studies

- many short passwords
- many guessable passwords
- conclusion is that users choose poor passwords too often
- need some approach to counter this

Future of IDS

- To integrate the network and host based IDS for better detection.
- Developing IDS schemes for detecting novel attacks rather than individual instantiations.