UNIVERSITA' DEGLI STUDI DI PARMA
Dipartimento di Ingegneria dell'Informazione

Network Security: Intrusion Detection Systems

Luca Veltri

(mail.to: luca.veltri@unipr.it)

Corso di Sicurezza nelle reti, Reti di telecomunicazioni C, a.a. 2009/2010

http://www.tlc.unipr.it/veltri

Intrusion Detection Systems

- Intrusion detection systems (IDSs) are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of intrusions
  - **try to discover attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network**
  - **generate data as a consequence of normal or abnormal usage**
- They analize the "manifestation of the attack" (not the attack itself)
- Intrusions are caused by
  - **attackers accessing the systems from the Internet,**
  - **authorized users of the systems who attempt to gain additional privileges for which they are not authorized,**
  - **authorized users who misuse the privileges given them**

Challenges in Intrusion Detection

- Recognize malicious actions in the huge of stream of events provided by network monitors and host auditing facilities
  - **Problem: given the stream e1, e2, e3, …, e4 and the past system states S1, S2, S3, S4, can we conclude that e5 in S5 is the final evidence that an intrusion is occurring?**
- Detect intrusion in real-time
- Perform detection at different abstraction levels
- Correlate detection results with and across security domains
- Integrate different systems so that different analysis techniques and data source are covered
- Deploy IDSs in very different environments
- Take into the account the characteristics of the protected networks

Network based IDSs

- Majority of commercial IDSs
- They detect attacks by capturing and analyzing network packets
  - **monitoring a network segment or switch they can protect multiple host**
- Often consist of a set of single-purpose sensors or hosts placed at various points in a network
  - **sensor can run in "stealth" mode**
- Advantages:
  - **few placed IDSs can monitor a large network**
  - **little impact upon an existing network (Network-based IDSs are usually passive devices that listen on a network wire without interfering with the normal operation of a network)**
  - **Network-based IDSs can be made very secure against attack and even made invisible to many attackers**

Network based IDSs

- Disadvantages
  - **Network-based IDSs may have difficulty processing all packets in a large or busy network**
    - Some vendors are attempting to solve this problem by implementing IDSs completely in hardware, which is much faster
  - **Switches subdivide networks into many small segments (usually one wire per host)**
    - most switches do not provide universal monitoring ports
  - **Network-based IDSs cannot analyze encrypted information**
  - **Most network-based IDSs cannot tell whether or not an attack was successful**
    - administrators must manually investigate each attacked host to determine whether it was indeed penetrated
  - **problems dealing with attacks that fragment packets**
    - the IDSs may become unstable

Host based IDSs

- Operate on information collected from within an individual computer system (application-based IDSs are actually a subset)
  - **great reliability and precision, determining exactly which processes and users are involved in a particular attack on the operating system**
- They can "see" the outcome of an attempted attack, as they can directly access and monitor the data files and system processes usually targeted by attacks
- Host-based IDSs normally utilize information sources of two types
  - **operating system audit trails**
    - usually generated at the innermost (kernel) level of the OS
    - more detailed and better protected than system logs
  - **system logs**
    - much less obtuse and much smaller than audit trails, and are furthermore far easier to comprehend

Host based IDSs

- Advantages
  - **detection of attacks that cannot be seen by a network-based IDS**
  - **often operate in an environment in which network traffic is encrypted**
  - **Host-based IDSs are unaffected by switched networks**
  - **can help detect Trojan Horse or other attacks involving software integrity holes**
    - appear as inconsistencies in process execution
- Disadvantages
  - **harder to manage, as information must be configured and managed for every host monitored**
  - **the IDS may be attacked and disabled as part of the attack (hosted by the systems it is monitoring)**
  - **Host-based IDSs are not well suited for detecting surveillance that targets an entire network**
  - **Host-based IDSs can be disabled by certain denial-of-service attacks**
  - **in case of OS audit trails the amount of information can be immense**
  - **use of the computing resources of the hosts they are monitoring**

Tools that complement IDSs

- Vulnerability Analysis/Assessment Systems
  - **tools to determine whether a network or host is vulnerable to known attacks**
  - **host-based analysis**
  - **network-based (remote) analysis**
    - testing by exploit
    - inference method (looking for the artifacts that successful attacks would leave behind)
  - **e.g. SATAN (Security Analysis Tool for Auditing Network) or nessus**
- File integrity checkers
- Honeypot System
  - **system that look like a vulnerable system**