CNS M6L1

Intrusion Detection Systems (IDS)

Content

- **What is IDS**
- **Intrusion Detection Systems (IDS)**
- **Anomaly detection**
- **Signature based misuse**
- **Host based**
- **Network based**
- **Benefits of IDS**
- **Future of IDS**

What is the Intrusion Detection

Intrusion detection is the act of detecting unwanted traffic on a network or a device. An IDS can be a piece of installed software or a physical appliance that monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates acceptable use policies.

- Intrusions are the activities that violate the security policy of system.
- Intrusion Detection is the process used to identify intrusions.

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

- This IDS possess an attacked description that can be matched to sensed attack manifestations.

- The question of what information is relevant to an IDS depends upon what it is trying to detect.
    - E.g DNS, FTP etc.

Signature based IDS (contd.)

- ID system is programmed to interpret a certain series of packets, or a certain piece of data contained in those packets,as an attack. For example, an IDS that watches web servers might be programmed to look for the string “phf” as an indicator of a CGI program attack.
- Most signature analysis systems are based off of simple pattern matching algorithms. In most cases, the IDS simply looks for a sub string within a stream of data carried by network packets. When it finds this sub string (for example, the ``phf'' in ``GET /cgi-bin/phf?''), it identifies those network packets as vehicles of an attack.

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.
- Host-based intrusion detection systems (HIDS)
- analyze network traffic and system-specific settings
- such as software calls, local security policy, local log
- audits, and more. A HIDS must be installed on each
- machine and requires configuration specific to that
- operating system and software.

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 and switch environments
- Monitoring key components
- Near Real-Time detection and response.
- No additional hardware

Stack based IDS

- They are integrated closely with the TCP/IP stack, allowing packets to be watched as they traverse their way up the OSI layers.
- This allows the IDS to pull the packets from the stack before the OS or the application have a chance to process the packets.

Network based IDS

- A Network Intrusion Detection System (NIDS) is one common type of IDS that analyzes network traffic at all layers of the Open Systems Interconnection (OSI) model and makes decisions about the purpose of the traffic, analyzing for suspicious activity.
- Most NIDSs are easy to deploy on a network and can often view traffic from many systems at once.
- A term becoming more widely used by vendors is “Wireless Intrusion Prevention System” (WIPS) to describe a network device that monitors and analyzes the wireless radio spectrum in a network for intrusions and performs countermeasures.

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

Benefits of IDS

- Monitors the operation of firewalls, routers, key management servers and files critical to other security mechanisms.
- Allows administrator to tune, organize and comprehend often incomprehensible operating system audit trails and other logs.
- Can make the security management of systems by non-expert staff possible by providing nice user friendly interface.
- Can recognize and report alterations to data files.

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.

Reference

- www.google.com
- www.wikipedia.com

Thanks