Network Security and Resilience

Intrusion Detection Systems (IDS)

Lecture eighteen

Outline and learning goals of Lecture

- Outline
  - IDS overview
  - IDS systems
- Learning goals
  - You should be able to explain the components and goals of IDS as well as some of the systems

IDS goals

- Detects attacks or abuse
- Collects data on system behaviour so as to prevent future intrusions or attacks
- Identify normal and damaging actions
- Scalable
- Able to monitor different kinds of network systems and architectures
- Adapt to new attacks
- Report and respond to attacks as they happen
- Be able to cooperate with other security mechanisms
- Not necessarily Intrusion Prevention Systems (IPS) although may be integrated with a Firewall

IDS goals

- Greater monitoring at sensitive points in the network such as firewalls
- Be able to protect itself
  - IDS is a likely target for hackers
- Be able to work even if the network is partially disabled
- Have minimum effects on the rest of the network
- Capture audit data
- Implement part of the security policy

IDS Terminology

- Alert/Alarm- A signal suggesting a system has been or is being attacked
- True attack stimulus- An event that triggers an IDS to produce an alarm and react as though a real attack were in progress
- False positive stimulus- The event signaling an IDS to produce an alarm when no attack has taken place
- False negative- A failure of an IDS to detect an actual attack
- Noise- Data or interference that can trigger a false positive
- Site policy- Guidelines within an organization that control the rules and configurations of an IDS

IDS Terminology

- Site policy awareness- The ability an IDS has to dynamically change its rules and configurations in response to changing environmental activity
- Confidence value- A value an organization places on an IDS based on past performance and analysis to help determine its ability to effectively identify an attack
- Alarm filtering- The process of categorizing attack alerts produced from an IDS in order to distinguish false positives from actual attacks
  - (From Wikipedia)

IDS operation

- Intent is that when an IDS identifies some suspicious event it takes some action or actions
  - Actions do not need to be identified as any particular kind of intrusion
  - Generally IDSs look for any anomalous behaviour
    - A huge spike in the number of new IP addresses
    - A dramatic change in the traffic profile such as lots of new UDP packets
- The action(s) are typically
  - Notifying a system administrator through some Instant Messaging system or email
  - Reconfiguring the Access Control List in a firewall to stop the attack
    - Intrusion Prevention Systems (IPS)

Types of IDS

- Network based IDS (NIDS)
  - Monitor network communications
  - Makes use of sensors to monitor traffic
  - Sensors might be hosts necessary software and with NICs operating in promiscuous mode, or dedicated appliances
  - Problem of monitoring traffic in a switched environment. Need to make use of SPANed ports
- Host based IDS (HIDS)
  - Installed on individual workstations
  - Watch for inappropriate or anomalous activity
  - Usually installed only on critical servers

IDS components

- Sensors
  - data gathering
- Monitors
  - process data
- Resolver
  - decides on appropriate response to events
- Controller
  - configuration of other components

Capabilities of IDS

- IDS aims to provide an accurate and timely view of an intrusion
- Needs to be able to identify the nature of the abuse and log information in the case of legal actions
- Can identify security holes
- Can determine which network resources are likely to be attacked

Limitations of IDS

- May itself be attacked
- Needs to be able to see all traffic
- Uses models of behaviour
  - Lots of implementation work
  - Many different systems
- May find it difficult to detect distributed attacks such as DDOS
- Depending on the attack may react too slowly

IDS approaches

- Knowledge or Signature based
- Statistical anomaly based
  - Protocol anomaly based
  - Traffic anomaly based
- Rule based
  - Stateful matching
  - Model based

Knowledge or signature based

- Based on the characteristics of specific attacks being known
- System contains a database of attack profiles
- Signature based systems the most commonly deployed IDSs
- Main weakness is requirement to keep signature database up to date
  - Useless against new attacks

Statistical anomaly based

- A behavioural system
  - Looks for changes in ‘normal’ activity
- Capture statistical characteristics of normal behaviour for that system
  - Any sudden change in ‘normal’ behaviour causes an alarm
- Builds profiles of user activity, traffic rates, new IP addresses etc.
  - Able to respond to new attacks
- Some of our work in this area has been on Recurrence Quantification Analysis (RQA) for routing protocol attacks
  - D. Klimovski, C. Fox and P. Branch, "Detection of Insider Attacks Against Interior Routing Protocols," *2019 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, Korea (South), 2019, pp. 549-554, doi: 10.1109/ICTC46691.2019.8939795.

Statistical anomaly based

- Main weakness is that ‘normal’ can change rapidly
  - Website becomes suddenly popular
  - New applications cause rapid changes in traffic profiles
- Require fine tuning to reduce the number of false-positives
- Another weakness is that an intruder can attempt to hide their activities within a ‘normal’ traffic profile
- A third weakness is that they are unable to tell the administrator what is wrong, only that something might be wrong
  - Require sophisticated traffic and protocol analysis by network engineers to decide whether or not this is a real attack

Example statistical anomaly based IDSs

- Protocol anomaly based
  - IDS builds a statistical model of each protocol's normal behaviour
- Traffic anomaly based
  - Keeps track of traffic behaviour
    - New IP addresses
    - Overall traffic loads

Rule based IDSs

- Make use of Expert Systems to identify attacks
  - Knowledge base
  - Inference engine
  - Rule based programming
- Knowledge represented as rules
  - IF situation THEN action
- Rules applied to data obtained from IDS sensors
- Two types of rule based system
  - State-based: tracks state changes of system that might indicate an attack is underway
  - Model-based: contains scenarios that represent the steps taken by an attacker during specific attacks

IDS Systems and products

- Manual review techniques
  - eg connect dummy service to ports
  - trigger script when attacked
  - use log and audit files to identify nature, frequency and source of attacks
- Shadow/Step/CIDER
  - Toolkit of public domain tools
  - Perl and shell scripts
    - tcpdump, ssh, apache
  - uses distributed sensors for traffic analysis
  - low level analysis

IDS Systems and products

- Check Point IPS-1 (originally Network flight recorder)
  - Good commercial system
  - Realtime detection of intrusions
  - content based monitoring
  - decision engine
- Distributed Intrusion Detection System (DIDS)
  - Global monitor receives reports from other components
  - System wide inspection of users
- Cisco
  - IOS router based, AIM and ASA appliance based
  - Uses a database of intrusion ‘signatures’ to identify and optionally block attacks

IDS Systems and products

- SNORT
  - Very popular open source network intrusion prevention and detection system using a rule-driven language
  - Snort widely deployed
  - Combines signature, protocol and anomaly based inspection methods
  - Able to do realtime analysis
  - Can be used to detect a variety of attacks
    - buffer overflow
    - port scans
    - CGI script attacks
    - OS fingerprinting
  - https://www.snort.org/

SNORT

- Uses libpcap (same as Wireshark and tcpdump)
- Runs in 4 modes
  - Sniffer
  - Packet logger
  - Intrusion Detection
  - Intrusion Prevention
    - Snort-Inline
- Snort-Inline
  - Integrated with Netfilter firewall
  - Receives packets from Netfilter
  - Analyses them and tags packets that match an attack
  - Sends them back to Netfilter
  - Tagged packets dropped

IDS Systems and products

- System integrity checkers
  - Stores hashed snapshot of file systems and compares to current system state and reports discrepancies
    - Tripwire
      - Supports hashing algorithms MD5, SHA
- Honeypot systems
  - System (simulated or real) whose sole purpose is to be attacked
  - Enables the administrator to see what attacks are happening

IDS Systems and products

- Darknets
  - A Darknet is a portion of routed, allocated IP space in which no active services or servers reside
    - These are "dark" because there seems to be nothing in them.
  - However, a Darknet includes at least one server that gathers any packets that enter it for analysis
  - Any packet that enters a Darknet is by its presence aberrant
    - No legitimate packets should be sent to a Darknet
    - Such packets have probably arrived because of portscans or similar

IDS Systems and products

- L3DGEWORLD
  - Developed here at Swinburne (Centre for Advanced Internet Architectures)
  - One of the limitations of IDS is that the data they produce can be difficult or slow to interpret
  - L3DGEWORLD uses game engine to visualise attacks hopefully making the attack quicker to diagnose
  - An object in the game world represents an IP address which spins, jumps up and down and varies in size and colour
  - Each of these indicates different types of activity
  - Can also use game engine to implement an ACL

http://www.youtube.com/watch?v=8ssg0Kklq2c

http://www.youtube.com/watch?v=-JRHQ4EW3e0

Conclusion

- Function of IDS systems
- Structure of IDS systems
- Different IDS systems and tools