University of BRISTOL

Computer System- B Security

Introduction to Network Security

Intrusion Detection Systems

Sanjay Rawat

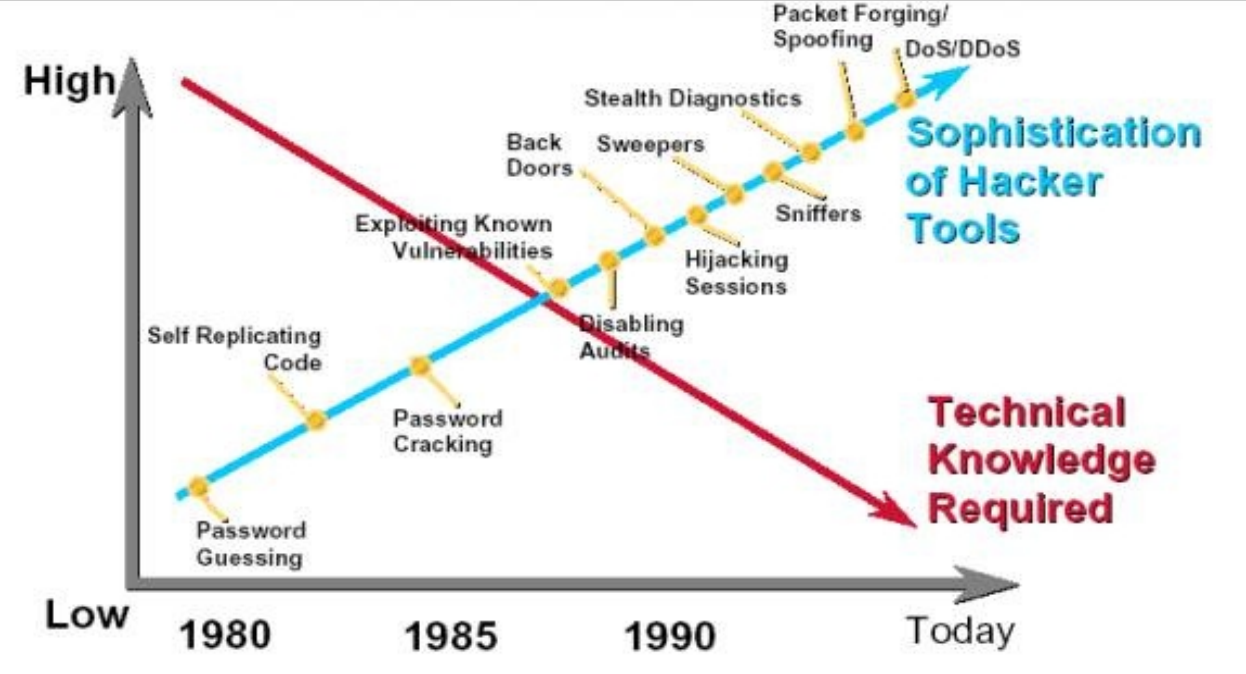
bristol.ac.uk

Intrusions

- DARPA IDS Evaluation Project 1998 attack categories[1]:
  - Probes (e.g. port scanning, fingerprinting)
  - Denial of Service (DoS) (e.g. packet flooding, crash)
  - Remote to Local (R2L)
  - User to Root (U2R)

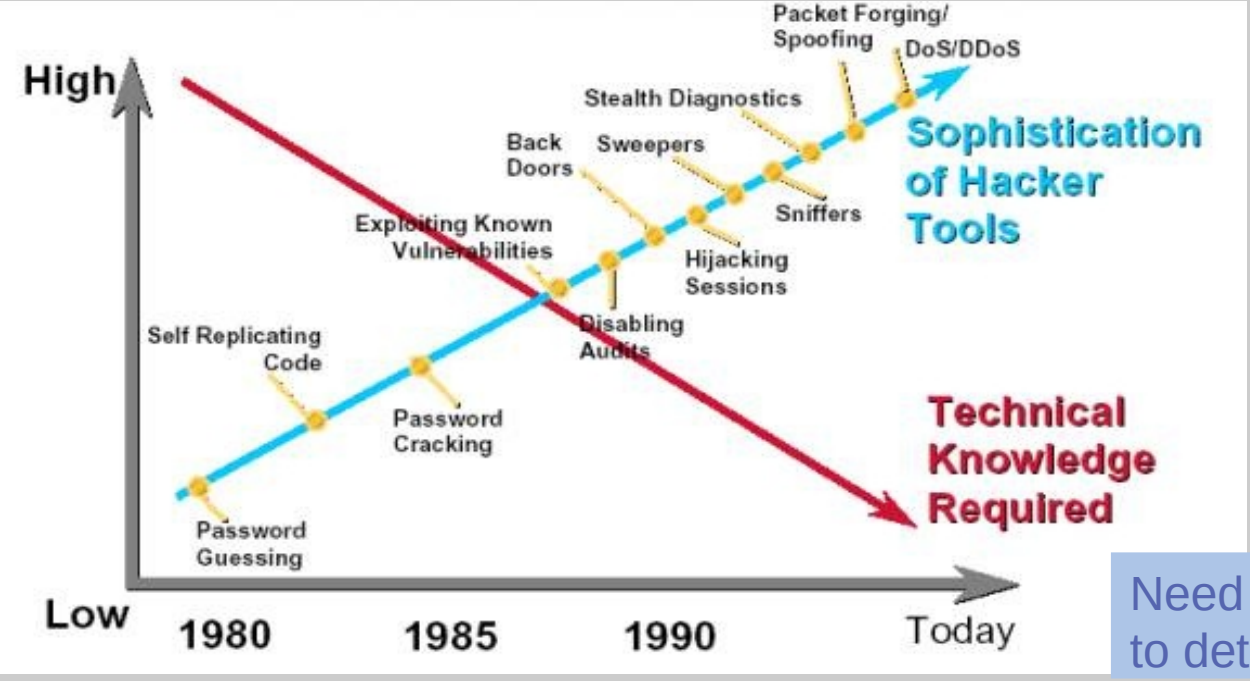
1. http://www.ll.mit.edu/mission/communications/cyber/CSTcorpora/ideval/docs/attackDB.html

Attacker's Picture



Curtsey: Internet source

Attacker's Picture



Need of automatic ways to detect them!

Curtsey: Internet source

Intrusion Detection Systems

What is intrusion detection?

Intrusion Detection Systems

What is intrusion detection?

- Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of *intrusions,* defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network.

Some (intended) General characteristics

Some (intended) General characteristics

- The ability to react in a timely fashion to prevent substantive damage – by automatic or manual intervention.

Some (intended) General characteristics

- The ability to react in a timely fashion to prevent substantive damage – by automatic or manual intervention.
- The ability to identify which is the precursor of more serious attacks.

Some (intended) General characteristics

- The ability to react in a timely fashion to prevent substantive damage – by automatic or manual intervention.
- The ability to identify which is the precursor of more serious attacks.
- The ability to identify a perpetrator.

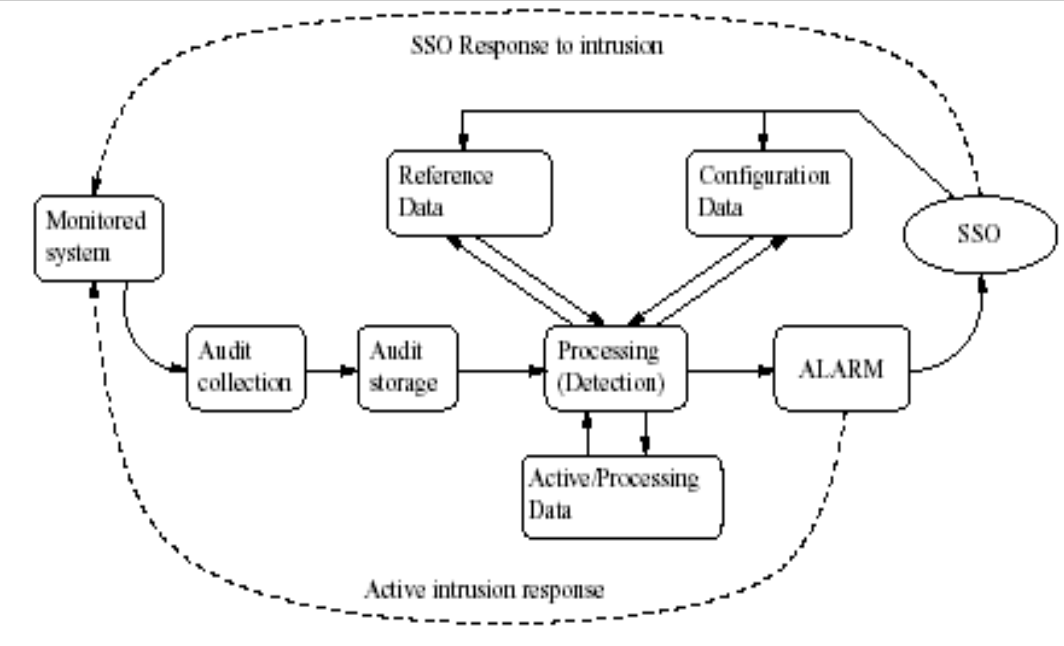
Some (intended) General characteristics

- The ability to react in a timely fashion to prevent substantive damage – by automatic or manual intervention.
- The ability to identify which is the precursor of more serious attacks.
- The ability to identify a perpetrator.
- The ability to discover new attack patterns.

Some (intended) General characteristics

- The ability to react in a timely fashion to prevent substantive damage – by automatic or manual intervention.
- The ability to identify which is the precursor of more serious attacks.
- The ability to identify a perpetrator.
- The ability to discover new attack patterns.
- The ability to produce evidence.

Generic IDS Architecture



From Wenke Lee et. el

Type of IDS

Type of IDS

- **Based on Data Collection**
  - **Network based :**
    - detects attacks by capturing and analyzing network packets
  - **Host based:**
    - utilizes information sources, available on the system- operating system audit trails and system logs, for example.

Type of IDS

- **Based on Data Collection**
  - **Network based :**
    - detects attacks by capturing and analyzing network packets
  - **Host based:**
    - utilizes information sources, available on the system- operating system audit trails and system logs, for example.
- **Advantages and Disadvantages**

Network based IDS (NIDS)

Network based IDS (NIDS)

- NIDS uses a passive interface to capture network packets for analyzing.

Network based IDS (NIDS)

- NIDS uses a passive interface to capture network packets for analyzing.
- NIDS sensors placed around the globe can be configured to report back to a central site, enabling a small team of security experts to support a large enterprise.

Network based IDS (NIDS)

- NIDS uses a passive interface to capture network packets for analyzing.
- NIDS sensors placed around the globe can be configured to report back to a central site, enabling a small team of security experts to support a large enterprise.
- Most network-based IDSs are OS-Independent (in the sense that they can protect systems, running on different OSs.

Network based IDS (NIDS)

- NIDS uses a passive interface to capture network packets for analyzing.
- NIDS sensors placed around the globe can be configured to report back to a central site, enabling a small team of security experts to support a large enterprise.
- Most network-based IDSs are OS-Independent (in the sense that they can protect systems, running on different OSs.
- Provide better security against DOS attacks(?)

NIDS disadvantages

NIDS disadvantages

- Cannot scan protocols or content if network traffic is encrypted

NIDS disadvantages

- Cannot scan protocols or content if network traffic is encrypted
- Intrusion detection becomes more difficult on modern switched networks (difficult to get all the packets to monitor, but getting better!)

NIDS disadvantages

- Cannot scan protocols or content if network traffic is encrypted
- Intrusion detection becomes more difficult on modern switched networks (difficult to get all the packets to monitor, but getting better!)
- Current network-based monitoring approaches may not efficiently handle high-speed networks.

NIDS disadvantages

- Cannot scan protocols or content if network traffic is encrypted
- Intrusion detection becomes more difficult on modern switched networks (difficult to get all the packets to monitor, but getting better!)
- Current network-based monitoring approaches may not efficiently handle high-speed networks.
- Most of Network-based systems are based on predefined attack signatures--signatures that will always be a step behind the latest underground exploits (zero-days)

Host based IDS (HIDS)

- HIDS runs on the system, it is protecting.
- It has better information about the health of the system- more sources of information.
- HIDS are better at detecting more sophisticated attacks.
- OS dependent.
- *For HIDS, reverse the points for advantage/disadvantages of NIDS*
- *Example: Anti-virus software*

Measuring the effectiveness

- Obviously, not every attack can be detected by an IDS and not every alert by an IDS is an attack!

Actual ↓ / Reported →	Attack	Not-attack
Attack	True positive (TP)	False negative (FN)
Not- attack (benign)	False positive (FP)	True negative (TN)

Measuring the effectiveness

- Obviously, not every attack can be detected by an IDS and not every alert by an IDS is an attack!

Actual ↓ / Reported →	Attack	Not-attack
Attack	True positive (TP)	False negative (FN)
Not- attack (benign)	False positive (FP)	True negative (TN)

$$DR = \frac{TP}{TP + FN}$$

DR: detection rate (*aka* ***Recall***).
Precision: What proportion of positive identifications was actually correct?

$$Precision = \frac{TP}{TP + FP}$$

Measuring the effectiveness

- Obviously, not every attack can be detected by an IDS and not every alert by an IDS is an attack!

Actual ↓ / Reported →	Attack	Not-attack
Attack	True positive (TP)	False negative (FN)
Not- attack (benign)	False positive (FP)	True negative (TN)

$$DR = \frac{TP}{TP + FN}$$

DR: detection rate (*aka* ***Recall***).
Precision: What proportion of positive identifications was actually correct?

$$Precision = \frac{TP}{TP + FP}$$

Ideally, one would like to have 0 FP and 0 FN

Types of IDS conti...

- Based on Processing

Types of IDS conti...

- Based on Processing
  - Misuse detection (a.k.a. signature/rule based IDS) :
    - analyzes system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack
    - Very effective in detecting known attacks
    - Not good at detection new attacks

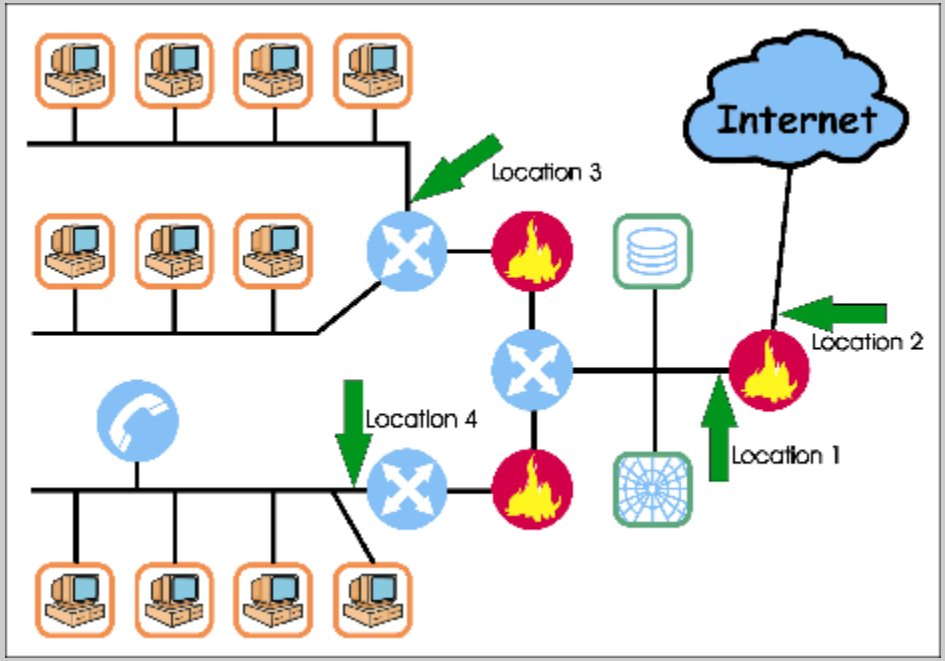
Types of IDS conti...

- Based on Processing
  - Misuse detection (a.k.a. signature/rule based IDS) :
    - analyzes system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack
    - Very effective in detecting known attacks
    - Not good at detection new attacks
  - Anomaly Detection:
    - identifies abnormal unusual behavior (anomalies) on a host or network
    - Good at detecting new attacks
    - High rate of false positive
    - Often use statistical properties to learn profile

Current Trend in IDS

- Future research trends seem to be converging towards a model that is hybrid of the anomaly and misuse detection models.
- It is slowly acknowledged that neither of the models can detect all intrusion attempts on their own.

Deploying NIDS



Intrusion Prevention System

Intrusion Prevention System

- IPS = IDS + Firewall

Intrusion Prevention System

- IPS = IDS + Firewall
- An IPS offers the ability to identify an intrusion, relevance, impact and proper analysis of an event, and then pass the appropriate information and commands to the firewalls, switches and other network devices to mitigate the event's risk.

Intrusion Prevention System

- IPS = IDS + Firewall
- An IPS offers the ability to identify an intrusion, relevance, impact and proper analysis of an event, and then pass the appropriate information and commands to the firewalls, switches and other network devices to mitigate the event's risk.
- An IPS is the next security layer to be introduced in the system that combines the protection of firewalls with the monitoring ability of an IDS to protect our networks with the analysis necessary to make the proper decisions on the fly.