Intrusion Detection Systems

Dr. Manas Khatua
Assistant Professor
Dept. of Computer Science & Engineering
Indian Institute of Technology Guwahati
URL: http://manaskhatua.github.io/
Email: manaskhatua@iitg.ac.in

Content

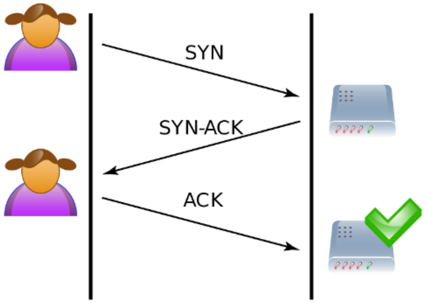
- ✓ Common Attacks on Networks and Systems
- ✓ Traditional Solution
- ✓ IDS (Intrusion Detection System)
  - Goals
  - Classifications
- ✓Anomaly vs Rule-based Detection
- ✓ Network v/s Host-based Detection
- ✓ Pros & Cons of IDS
- ✓ Snort NIDS Demo

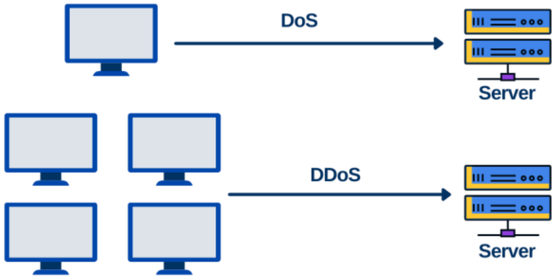
Common Attacks

- IP Spoofing: Hides the identity of the sender or impersonates another computer system

- SYN Flood: Makes a server unavailable to legitimate traffic by consuming all available server resources
- Denial of Service (DoS): Shut down a machine or network, making it inaccessible to its intended users
- Smurf Attack: Causes a ping flood on the victims computer resulting in DDoS attack

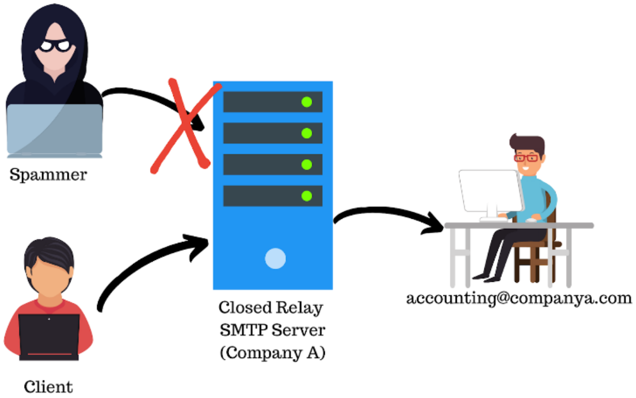
- CGI scripts: Uses Common Gateway Interface (CGI) program security holes
- Web Server attacks: Uses security holes (e.g. session hijacking, http response splitting, html injection)



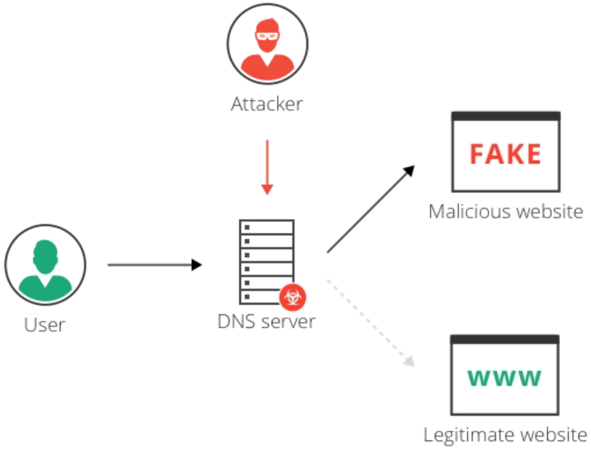


Common Attacks

- SMTP attacks: Uses security holes in DEBUG commands and SMTP protocol
- DNS attacks: Targets the availability or stability of a network's DNS service
- Access attacks: Failed login attempts, failed file access attempts, password cracking, administrative powers abuse.
- IMAP attacks: Uses security holes in IMAP protocol
- Buffer overflows: Hackers push too much data. The excess data corrupts nearby space in memory.



SMTP attacks



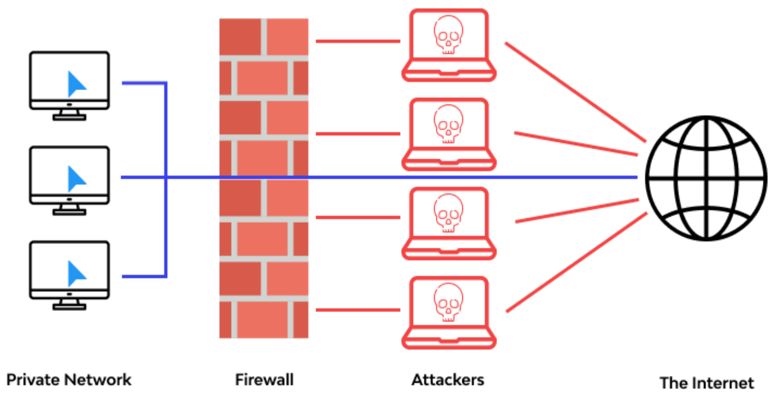
DNS attacks

The Traditional Solution

- Install a **firewall** to protect the internal network from the outside world.
  - Assume that the firewall will protect against all current security threats

- Usually the following are not done:
  - Do not install additional security measures to complement the firewall.
  - Do not individually secure internal networks and systems.
  - Do not regularly review the organizational security policy.
  - Do not regularly update the firewall.
  - Ignore the firewall logs because they are to voluminous and too difficult to process.

What is a Firewall



Shortcomings

- Firewalls are mandatory security component, but are not enough on their own
- Even a properly configured firewall is not absolutely secure
  - Because it is possible to exploit the services the firewall allows
  - Or to cause the firewall or network itself become unusable.
- Network security is similar to physical security
  - A multi-layered approach is best
- Also need
  - A solid understanding of network security issues
  - And a good security policy are essential to any successful network security deployment.
- Some of the most common security techniques are:
  - **Intrusion Detection System (IDS)**, Security Scanners

Intrusion Detection System

IDS definition

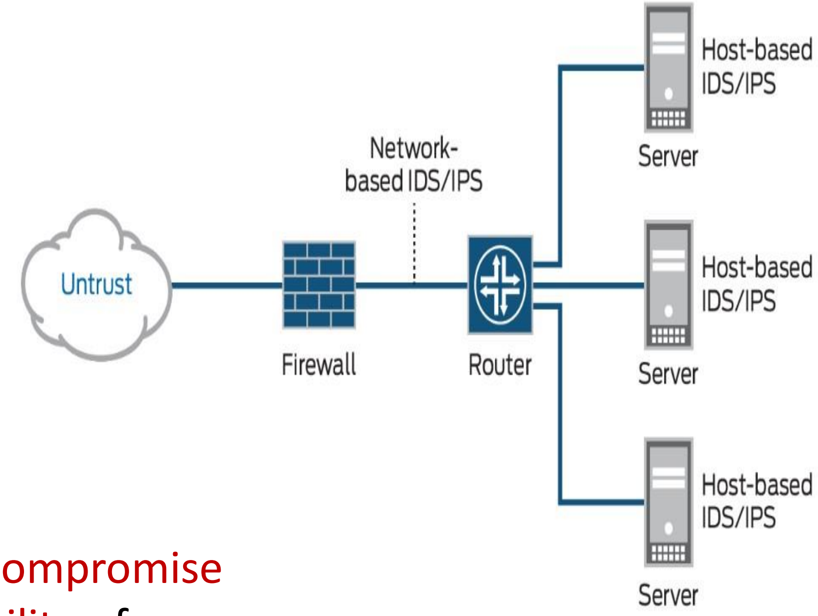
- An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

Intrusion Detection is the process of

- Discovering
- Identifying
- Analyzing

Unauthorized malicious activities

- Targeted at computing and networking resources



What is Intrusion?

- It is any set of actions that attempt to compromise Confidentiality, Integrity and/or Availability of a system resource.

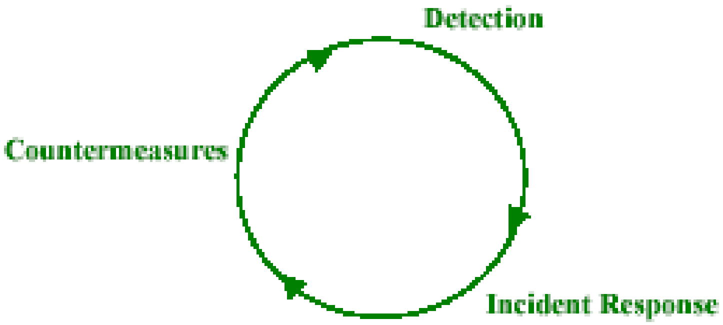
IDS (cont…)

- Detection is the act of discovering or ascertaining the
  - Existence
  - Presence
  - Or fact of something

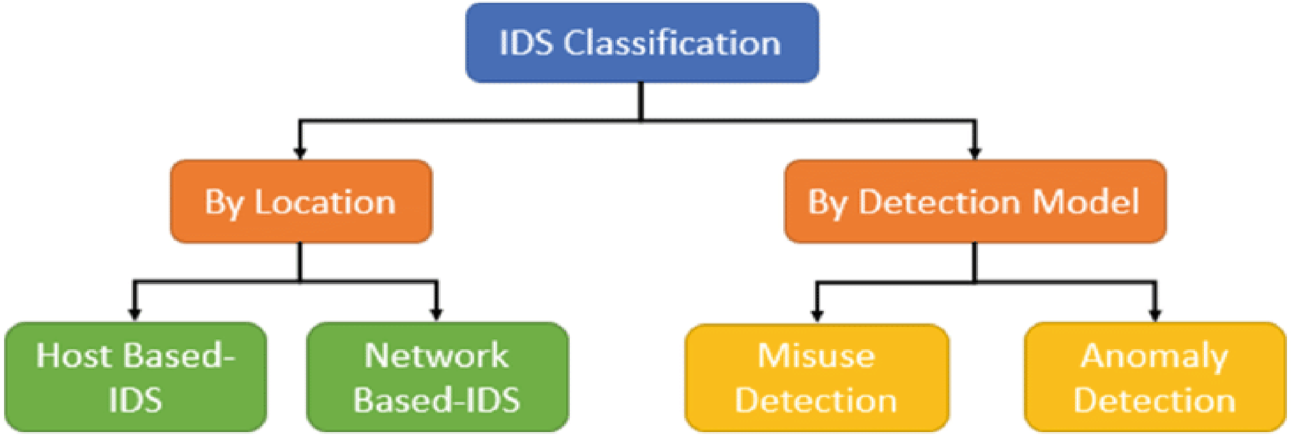
- A system is a group of interacting, interrelated, or independent elements forming a complex whole.
- Thus, IDS is a group of interacting elements that together are used to ascertain the existence of a set of actions that attempt to compromise confidentiality, integrity or availability of a resource.

Goal of Intrusion Detection

- It is best to prevent access
- As a second line of defense: Intrusion detection
  - Based on the assumption that the behaviour of intruder differs from legitimate users
- The intruder can be identified and ejected from the system
- Instruction detection enables
  - The collection of information about intrusion techniques
  - That can be used to strengthen the intrusion prevention facility
- A complete IDS consists of the following sequence of events



IDS Classification



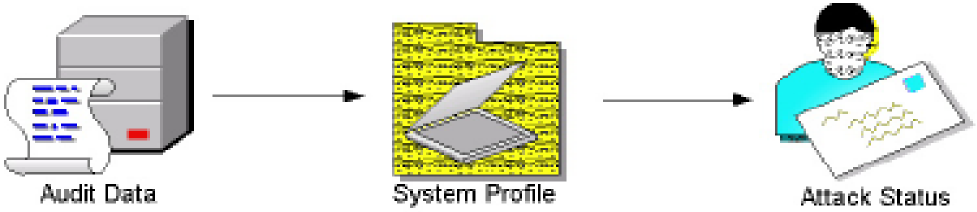
- Categorize IDS into the following:
  - Anomaly detection v/s Rule-based detection
  - Network-based v/s Host-based systems

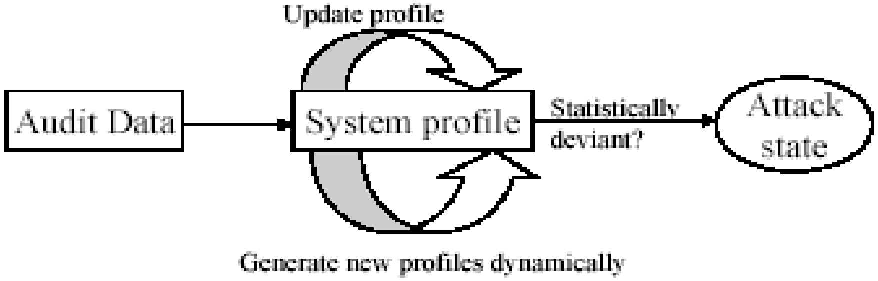
- Anomaly detection
  - Deviations from normal system operations

- Rule-based detection
  - Known patterns

Anomaly Detection

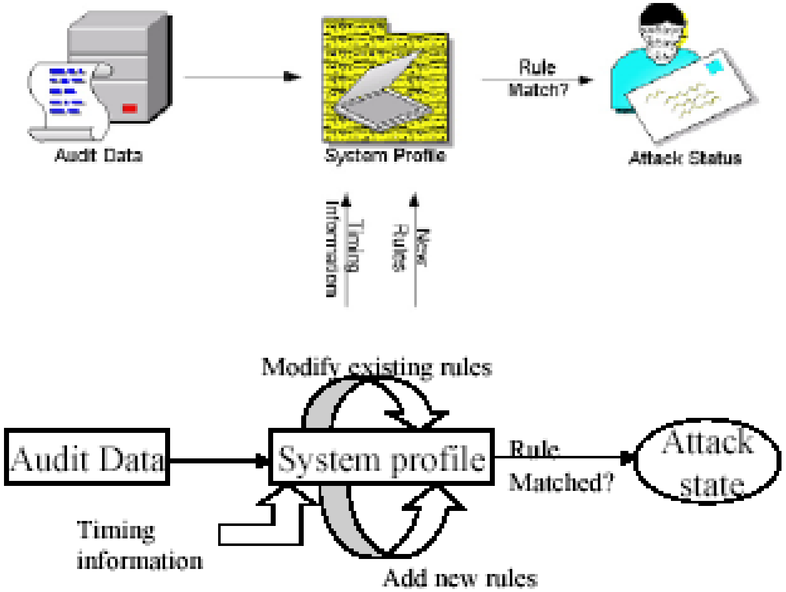
- Looks at behavior that deviates from normal system use
- Collect data and determine the pattern of legitimate user
- Threshold detection
  - Define thresholds for frequency of occurrence of events
- Profile based detection
  - Develop profile of activity for each user.





Rule-based Detection

- Looks for behavior that matches a known attack scenario
- Define a set of rules to evaluate a user’s behavior
- Deviation detection
  - Detect deviation from previous behavior
- Penetration identification
  - Use an expert system, based on a set of rules to evaluate user behavior



Example: Rules for Penetration Detection

- Users should not **read files** in other users' personal directories.
- Users must not **write** other users' files.
- Users who log in after hours often **access** the same files they used earlier.
- Users do not generally **open disk** devices directly but rely on highest level OS utilities.
- Users should not be **logged in** more than once to the same system.
- Users do not **make copies** of system programs.

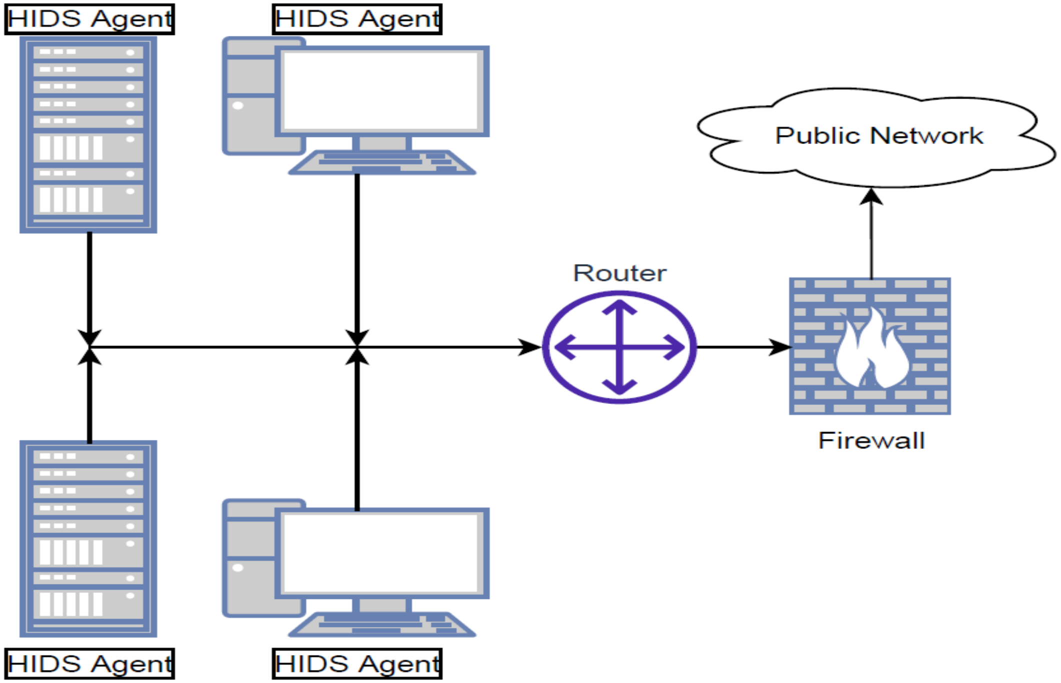
Host-based IDS

- Host-Based intrusion detection uses the following.
  - Monitor OS events and logs
  - Listens to the port activities
  - Monitors systems files by using checksums
  - Uses regular-expressions for signatures

- Checks
  - Unauthorized activity;
  - privilege violations;
  - failed login attempts

- Typically
  - Signature based for log monitors
  - cryptographic for change detection

- Aims to Detect
  - Signs of intrusion on hosts;
  - malicious system activities



Examples: Host-based IDS

OSSEC

- An open source HIDS produced by Trend Micro. Also supports NIDS.
- Can be used on a wide range of operating systems (OS)
- It monitors event logs and also the registry.

Source: https://www.ossec.net/

Splunk

- Offers both HIDS and NIDS features
- Follows anomaly-based detection method
- Can detect threats that aren’t discovered through logs
- Provides workflow automation features
- Splunk dashboard has multiple data visualization options
- Supports Linux and Windows

Source: https://www.splunk.com/

Examples: Host-based IDS

Sagan

- Uses both anomaly and signature-based detection methods.
- Multi-threaded architectural approach
- Offers IP geolocation facility
- Allows to set time-related rules to trigger alerts
- Supports Unix, Linux, and Mac OS, but not Windows.

Source: https://quadrantsec.com/sagan_log_analysis_engine/

Wazuh

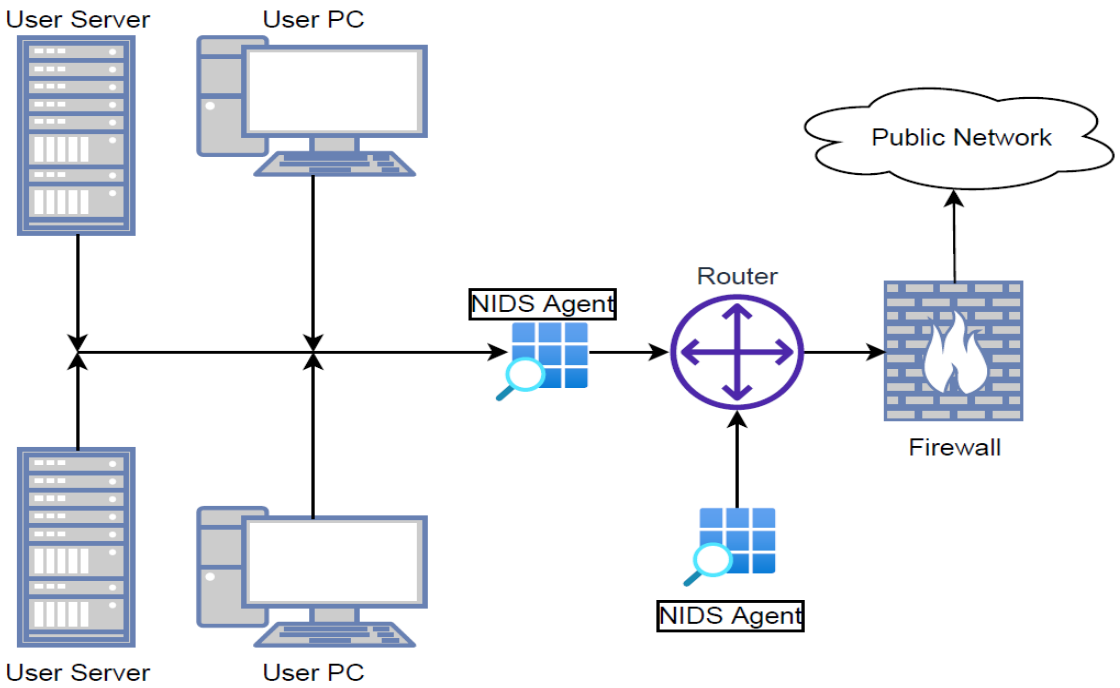
- Provides monitoring, detection, and alerting of security events and incidents
- Continuous managing and responses to advanced threats
- Provides users with navigation authority through security alerts
- Perform file integrity monitoring and log data analysis

Source: https://wazuh.com/

Network-based IDS

- Uses the following procedure to detect intrusion
  - Traffic sniffing on network
    - Sniffing (passive listening)
  - Uses signature database

- Detects unauthorized activities
  - Signs of intrusion on networks
  - Malicious network traffic
- Check
  - External attacks
  - Internal misuse



Examples: Network-based IDS

Snort

- Offers anomaly and signature-based solutions
- Identifies attacks such as buffer overflows, stealth port scans, CGI attacks;
- Works with platforms like Linux, Windows, Fedora, Centos, and FreeBSD;
- High-level customizable solutions

Source: https://www.snort.org/

Suricata

- Real-time intrusion detection and prevention
- Multi-Threaded architecture and scalable code base
- Application-layer logging and analysis, including TLS/SSL certs, HTTP requests, DNS requests, and more
- Cross-platform support - Linux, Windows, macOS, OpenBSD, etc.
- Built-in hardware acceleration (GPU for network sniffing)

Source: https://suricata.readthedocs.io/en/latest/#

Examples: Network-based IDS

Bro (renamed Zeek)

- Comprehensive traffic logging and analysis
- DNS/FTP/HTTP/IRC/SMTP/SSH/SSL/other protocol support
- Fully passive traffic analysis with network tap or monitoring port
- Real-time and offline analysis
- Cluster-support for large-scale deployments
- Powerful and flexible event-driven scripting language (Bro scripts)

Source: https://zeek.org/

IBM QRadar

- AI-driven anomaly-based detection
- Provides visibility and applies context to on premise and cloud-based resources
- Analyzes network, endpoint, asset, user, risk and threat data to uncover known and unknown threats
- Automatically makes sense of data from disparate sources
- Highly scalable, self-managing security database

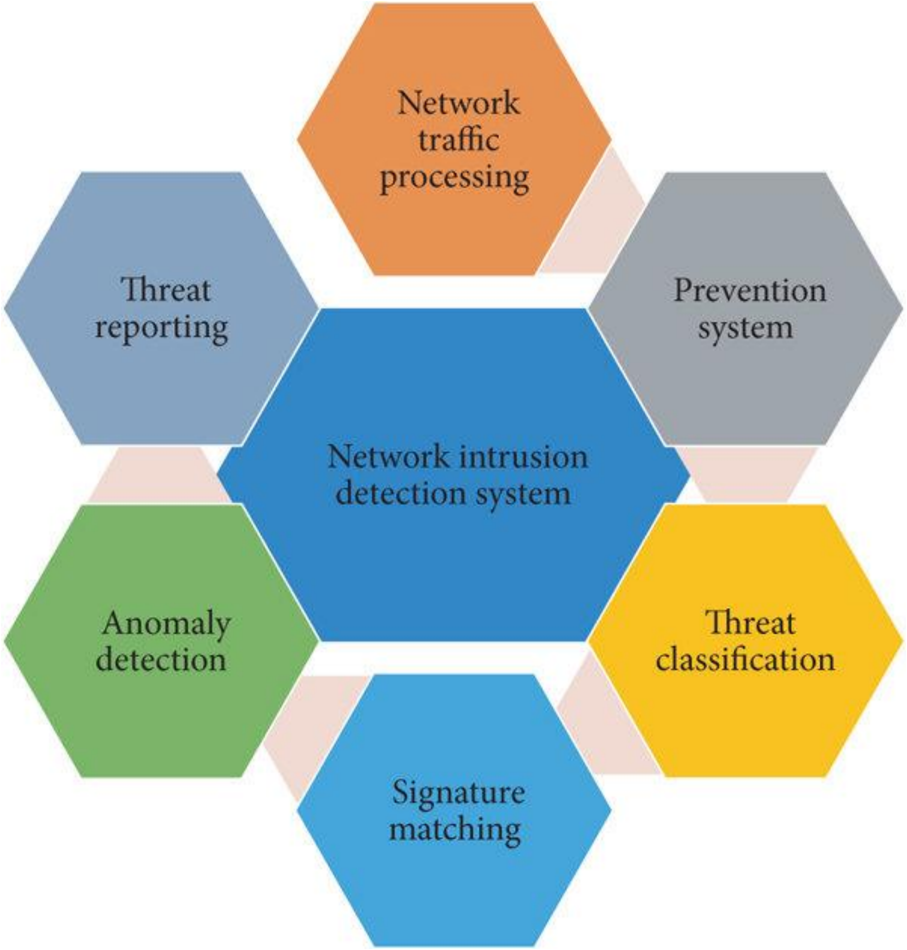
Source: https://www.ibm.com/in-en/products/qradar-siem/features

Why utilize IDS?

- Greater proficiency
  - (as opposed to humans) in detecting intrusions
- Reduction of manpower (needed to discover incidents)
- Technical expertise (not otherwise available)
- Wealth of information (useful in dealing with an attack)
- Ability to quickly shut off attacks (through “isolation”)
- Handle large amount of data
- Warning value

Why utilize IDS? (Cont...)

- Detecting external attacks
- Detecting internal attacks
- Detecting policy violations
  - Accessing non-work related web sites
- Detecting unauthorized changes to configurations
  - Bypassing change control procedures
- Detecting viruses and other malicious software



Data used by IDSs

- Firewall data (`best source')
- Log data from systems
- Data from passive devices (e.g. sniffers)
- Data from packet filters (e.g. TCP wrappers, Nuke Nabber)
- Data from integrity checking tools (e.g. Tripwire)
- Output of intrusion detection systems (other IDSs)
- Other types

Disadvantages

- Immaturity; False alarms; Performance decrements; Initial cost;
- Vulnerability to attacks; Applicability to the full range of attacks that occur;
- Vulnerability to tampering; Changing technology; May yield superfluous data

Vulnerabilities of IDS

- Insertion attacks
  - IDS accept host rejected packets
- Evasion attacks
  - Packets with same sequence numbers
  - Packet overlay
- Denial-of-service attacks
  - Especially from the inside
  - Unlike a firewall, an IDS does not block packets
  - An IDS discards packets if resources are exhausted

Snort NIDS

- Free and open source signature/rule based IDS currently developed by Cisco
- Network intrusion detection system (IDS) and intrusion prevention system (IPS)
- Ability to perform real-time traffic analysis and packet logging on IP networks
- Performs protocol analysis,

  content searching and matching
- Can also be used to detect attacks like:
  - operating system fingerprinting attempts
  - semantic URL attacks, buffer overflows
  - server message block probes, and stealth port scans

Snort NIDS

- Configured in **three main modes**:
  - Packet sniffer: Read network packets and display them on the console.
  - Packet logger: The program will log packets to the disk.
  - Network intrusion detection
- Network intrusion detection mode:
  - monitor network traffic and analyze it against a rule set defined by the user
  - Then perform a specific action based on what has been identified
- **Snort rules**:
  - Alert Rules: This uses the alert technique to produce notifications.
  - Logging Rules: It logs each individual alert as soon as it is generated.
  - Pass Rules: If the packet is deemed malicious, it is ignored and dropped.

Thank you

Questions and Discussion