Network-Based IDSs

Network Based IDS

- A network based IDS monitors network traffic and analyses the network and application protocol activity to identify suspicious activity
- NIDS are suitable for medium to large scale organizations due to their volume of data and resources.

- Works on the principle of signature matching, i.e. comparing attack patterns to known signatures in their data base
- Ongoing network operations are not disrupted by deploying NIDS, since they are passive devices.

- There are two types of network-based intrusion detection technologies
  - Promiscuous-mode network intrusion detection
  - Network-node intrusion detection

- Promiscuous-mode network intrusion detection is the traditional technology that sniffs all the packets on a network segment for analysis.
- place a single sensor on each segment.
-

- Network-node intrusion detection systems sniff just the packets bound for a single destination computer.
- Are characterized by a set of distributed agents on mission critical machines.

Challenges of Network-based IDSs

- High-speed networks might increase the network throughput beyond the capabilities of sniffers.
- Switched networks make it more difficult to choose the location where the NIDSs should be placed.
- The adoption of encryption of the communications reduces or completely prevents NIDSs from accessing the contents of network connections.

Types of events detected

- **Application layer reconnaissance and attacks:** e.g. banner grabbing, buffer overflows, format string attacks, password guessing, malware transmission

- **Transport layer reconnaissance and attacks:** e.g. port scanning, unusual packet fragmentation, SYN floods.
- **Network layer reconnaissance and attacks:** e.g. spoofed IP addresses, illegal IP header values.

- **Unexpected application services:** e.g. tunnelled protocols, backdoors and hosts running unauthorized application services.
- **Policy violations:** e.g. use of inappropriate Web sites, use of forbidden application protocols.

Technology Limitations

- Network based IDS cannot detect attacks within encrypted network traffic, including Virtual Private Network (VPN) connections, HTTP over SSL (HTTPS) and SSH sessions.
- Network based IDS may be unable to perform appropriately under high loads. Attackers sometimes take advantage of this.

Information Sources of NIDS

- **SNMP information**
- **Network packets**

SNMP information

- Management Information Base (MIB) is a repository of information used for network management purposes
- It contains configuration information (routing tables,addresses, names) and performance/accounting data
- SNMP MIBs are a potentially candidate as an audit source for NIDS

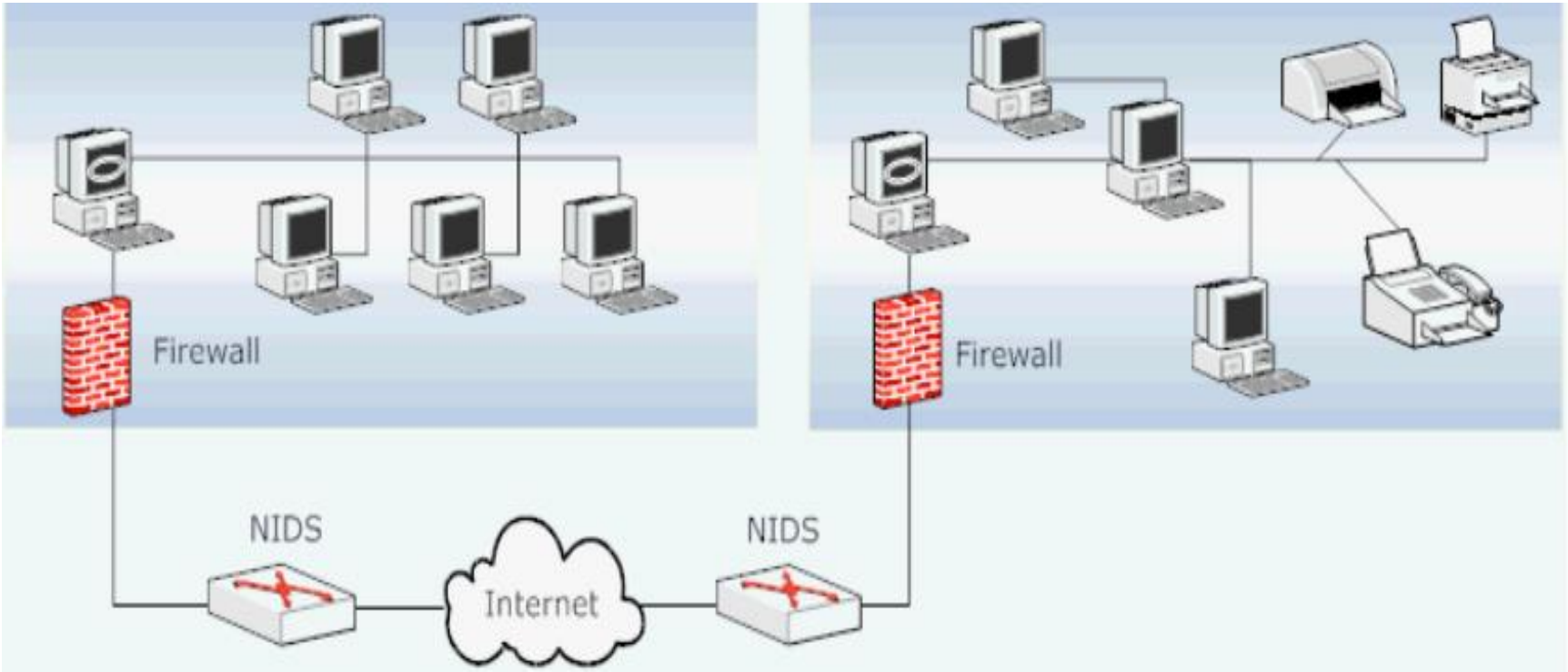
Network packets

- capturing the packets before they enter the server is probably the most efficient way to monitor this server.
- Network sniffers are used for analyzing network traffic.

Deploying Network-Based IDS sensors

- **Early Warning Mode**
- **Complete deployment mode**
- **NIDS within Every Host**

Early Warning Mode



Early Warning Mode

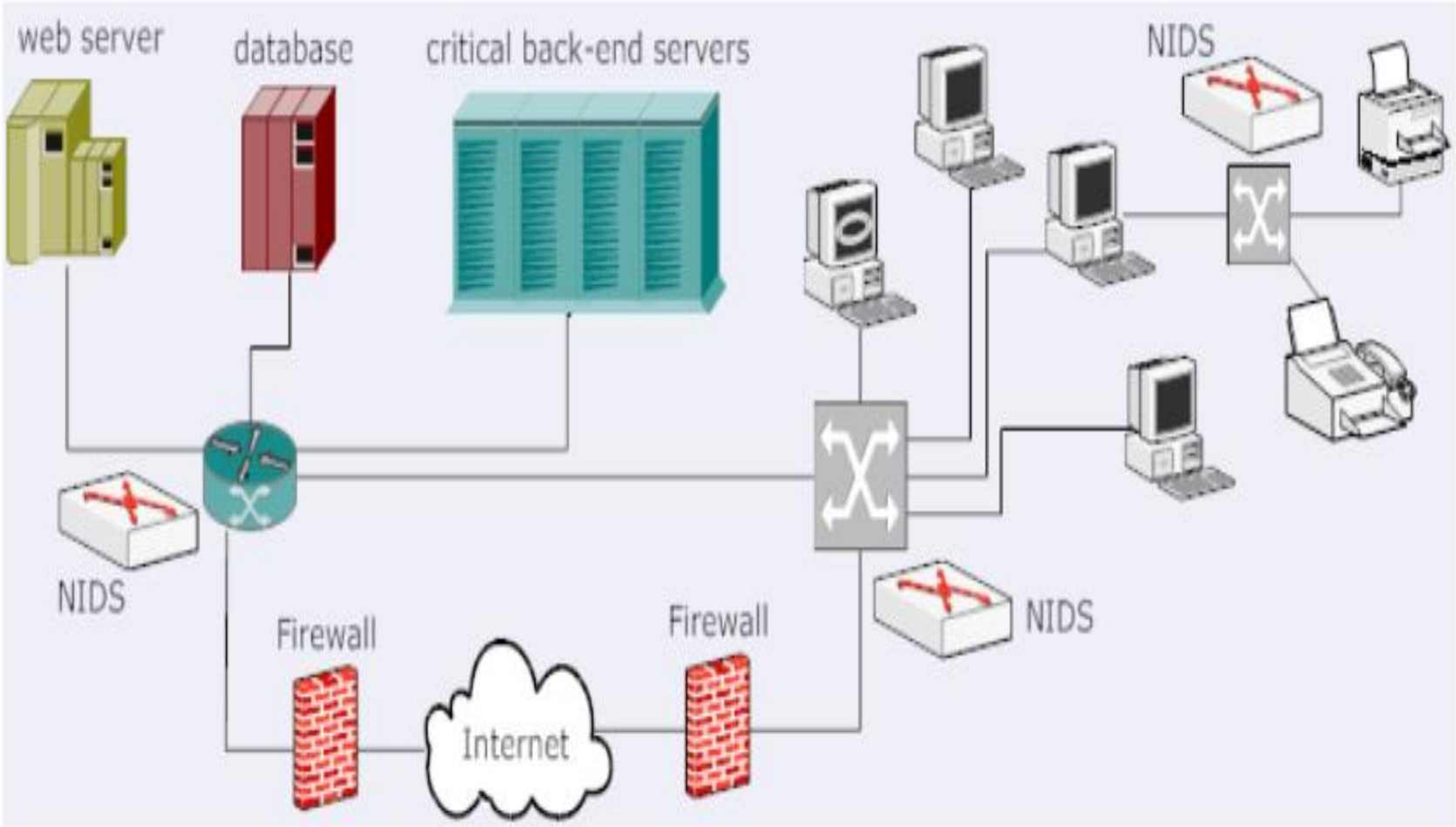
- Here, NIDS are employed outside the perimeter of the firewall
- All traffic entering the host and/or the local/enterprise network is scanned by the NIDS.

- Benefit
  - the NIDS remains at a single locating tapping at a high speed link and can potentially serve a large number of hosts.
  - management and update of the signatures is easier
  - keeping the configurations up-to-date are much easier.

Drawback

the attacks initiated by the hosts within the firewall perimeter will go undetected

NIDS in complete deployment



- NIDS is deployed near the switching nodes within the local network, and near the access routers at the network boundary.
- The NIDS will no longer monitor the traffic that has been blocked by the firewall, which will lead to a much reduced false alarm

- There will be multiple instances of NIDS, and it will become tedious to keep all of them up-to-date
- Such configurations are popular in ecommerce back end networks

NIDS within Every Host

- Every host has an inbuilt NIDS attached to all of its network interfaces
- The architecture is similar to an anti-virus running on the host
- Its key benefit is that the NIDS is decoupled from the host operating system, thus can be separately managed by the network administrator through a central location.

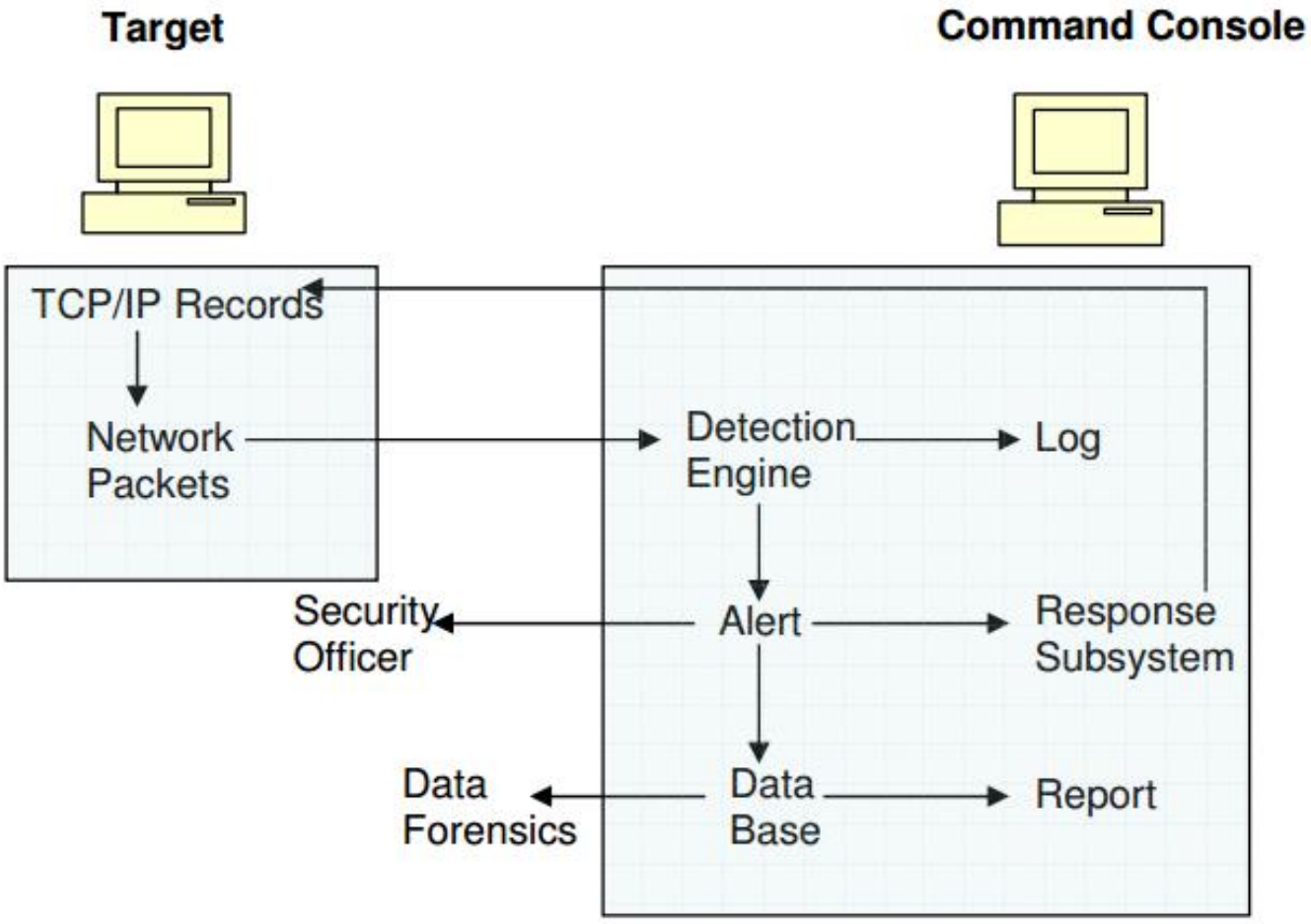
- NIDSs are vulnerable to a class of attacks (called insertion and evasion) that take advantage of the physical and logical separation of the NIDSs from their monitored hosts to undermine their detection capability.

- The management can become complex when the network is large containing several host computers

Network Intrusion Detection Architecture

- Two types:
  - **Traditional sensor-based architecture**
  - **Network node based architecture**

Network Intrusion Detection Architecture



Traditional sensor-based network intrusion detection architecture

- A sensor is used to “sniff” packets off of the network where they are fed into a detection engine
- The detection engine set off an alarm if any misuse is detected.
- These sensors are distributed to various mission-critical segments of the network.
- A central console is used to collect the alarms from multiple sensors.

Life cycle of a network packet

1. The network packet is created when one computer communicates with another.
2. The packet is read, in real time, off the network through a sensor that presides on a network segment located somewhere between the two communicating computers.
3. A sensor-resident detection engine is used to identify predefined patterns of misuse. If a pattern is detected, an alert is generated.

4. The security officer is notified about the misuse and a response to the misuse is generated
5. The alert is stored for correlation and review at a later time.
6. Reports are generated that summarize the alert activity
7. Data forensics is used to detect long-term trends.

Common NIDS tools

- *SNORT*
  - lightweight network intrusion detection and prevention system excels at traffic analysis and packet logging on IP networks
  - It detects threats, such as buffer overflows, stealth port scans, CGI attacks, SMB probes and NetBIOS queries, NMAP and other port scanners and DDoS clients, and alerts the user about them.

- It develops a new signature to find vulnerabilities.
- It records packets in their human-readable form from the IP address.

- Bro
- Network based IDS
- Currently developed for six Internet applications: FTP, Finger, Portmapper, Ident, Telnet and Rlogin.

Strengths of NIDS

- An anomaly based NIDS is capable of detecting high volume traffic flows, flash crowds, load imbalance in the network, sudden changes in demand of a port usage, sudden surge of traffic from/to a specific host, etc

- Signature based NIDS can detect known worms, viruses, and exploitation of a known security hole with fairly high degree of accuracy.
- Useful for Enforcement of the security policies and access control in a given network
- Anomaly based NIDS can also recognize new attacks and abnormal patterns in the network traffic, whose signatures are not yet generated.

Limitations of NIDS

- **False Positives**
  - A false positive is an event when a NIDS falsely raises a security threat alarm for harmless traffic.
- **Performance issues**
  - In order to reduce false positives long signatures are required which further reduces the performance.
  - The data throughput of current NIDS systems is limited to a few gigabit per second

- **Encryption**
  - Once the packet payloads are encrypted, the existing signatures will become completely useless in identifying the anomalous and harmful traffic
- **New and sophisticated attacks**
  - Commercial NIDS which are signature based are unable to detect new attacks whose signatures are not yet devised
  - Due to the limitations of the current anomaly detection algorithms, an intelligent attacker can always develop attacks that remain undetected

- **Human intervention**
  - Almost all NIDS systems require a constant human supervision, which slows down the detection and the associated actions.
- **Evasion of signatures**
  - polymorphic worms pose a critical threat to the current NIDS.

Attacks detected by a NIDS

- **Scanning Attack**
  - an attacker sends various kinds of packets to probe a system or network for vulnerability that can be exploited.
  - The target system's responses are analyzed to determine the characteristics of the target system and if there are vulnerabilities

- Network scanners, port scanners, vulnerability scanners, etc are used which yields information:
  - *The network topology*
  - *The type of firewall used by the system*
  - *The identification of hosts that are responding*
  - *The software, operating systems and server applications that are currently running*
  - *Vulnerabilities in the system.*
- Once the victim is identified, the attacker can penetrate them in a specific way.

- NIDS signatures can be devised to identify such malicious scanning activity from a legitimate scanning activity with fairly high degree of accuracy

Penetration Attacks

- An attacker gains an unauthorized control of a system, and can modify/alter system state, read files, etc.
- Generally such attacks exploit certain flaws in the software, which enables the attacker to install viruses, and malware in the system.

- The most common types of penetration attacks are:
  - **User to root:** A local user gets the full access to every component of the system.
  - **Remote to user:** A user across the network gains a user account and the associated controls.
  - **Remote to root:** A user across the network gains the complete control of the system

- **Remote disk read:** An attacker on the network gains access to the inaccessible files stored locally on the host.

- **Remote disk write:** An attacker on the network not only gains access to the inaccessible files stored locally on the host, but can also alter them.

Denial of Service (DoS) Attacks

- Slow down or completely shut down a target so as to disrupt the service and deny the legitimate and authorized users an access
- Very common in the Internet where a collection of hosts are often used to bombard web servers with dummy requests

- There are a number of different kinds of DoS attacks
  - Flaw Exploitation DoS Attacks
  - Flooding DoS Attacks
  - Distributed Denial of Service attack (DDoS)

Flaw Exploitation DoS Attacks

- An attacker exploits a flaw in the server software to either slow it down or exhaust it of certain resources.
- Ping of death attack is one such well known attack.
- NIDS needs to check the ping flag and packet size.

Flooding DoS Attacks

- An attacker simply sends more requests to a target that it can handle.
- It exhausts the processing capability of the target or exhaust the network bandwidth of the target, leading to a denial of service to other users.

Distributed Denial of Service attack (DDoS)

- It uses a large pool of hosts to target a given victim host.
- A hacker (Bot Master) can initiate a DDoS attack by exploiting vulnerability in some computer system, thereby taking control of it and making this the DDoS master
- Afterwards the intruder uses this master to communicate with the other systems (called bots) that can be compromised.

Role of NIDS in Combating Attacks

- NIDS can detect attacks, and anomalous conditions, additionally they can also provide a number of key information which can be used to identify the nature of attack, its origin and propagation characteristics.
- NIDS often reports the location of the attacker or hacker as an IP address
  - not a reliable information, as it can be changed by IP address spoofing.

- NIDS is to classify the attack and then determine if the attack requires the reply messages to be seen or not.
- Modern NIDS can also report the route that the attack packets have taken.
  - The route information contains key pieces that can be used to trace the hacker in spite of the source address spoofing.

Excessive Attack Reporting

- NIDS serving large enterprise network reports a significant number of attacks
- It often becomes impossible to manually examine each of these reports.
- Modern NIDS aggregate these reports into a smaller number of subsets that is much easier to examine
- They also classify the attacks into different levels of threats and present the most serious threats to the operator first.

- When the signatures of an attack are designed, a security level is attached to them.
- The security level depends not only upon the seriousness of attack, but also upon the accuracy of the signatures.

Reference

- The Practical Intrusion Detection Handbook, Paul E. Proctor, Prentice Hall