NETWORK

SECURITY

09 Intrusion Detection System

Contents

Background

- The psychology and politics of ownership have historically dictated that individuals and groups tend to protect valuable resources.
- This grew out of the fact that once a resource has been judged to have value, no matter how much protection given to it, there is always a potential that the security provided for the resource will, at some point, fail.

- Computer network security is made up of three principles:
  - prevention,
  - detection, and
  - response.

Computer Network Security

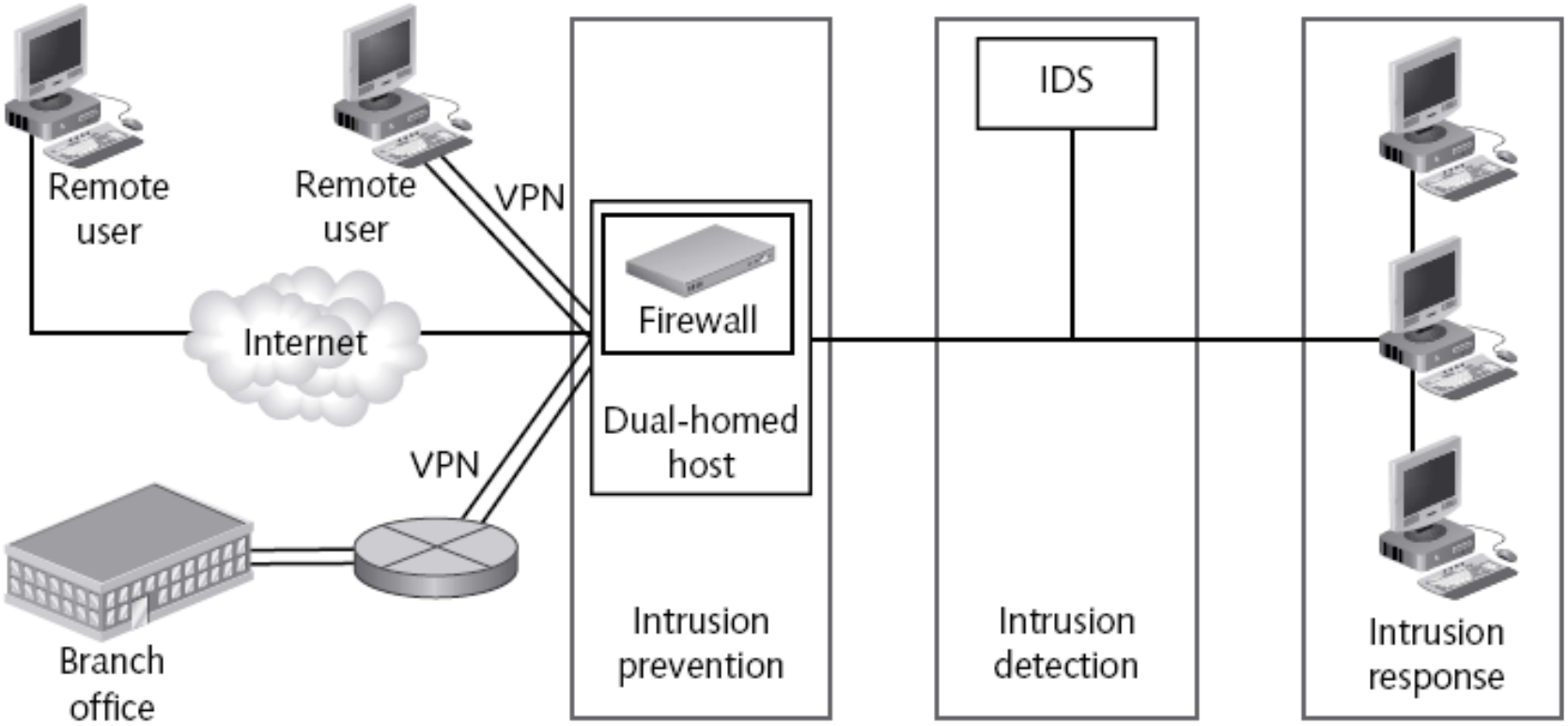


Figure 7-1 The role of intrusion detection in network defense

What is IDS?

- Intrusion detection is a technique of detecting unauthorized access to a computer system or a computer network
  - An intrusion into a system is an attempt by an outsider to the system to illegally gain access to the system
  - Intrusion prevention, on the other hand, is the art of preventing an unauthorized access of a system's resources

Intrusion Detection

- from a 1980 James Anderson's paper, "Computer Security Threat Monitoring and Surveillance."
- An intrusion is a deliberate unauthorized attempt, successful or not, to break into, access, manipulate, or misuse some valuable property and where the misuse may result into or render the property unreliable or unusable.
- The person who intrudes is an intruder.

Six types of intrusions

- Attempted break-ins,
  - which are detected by a typical behavior profiles or violations of security constraints.
- Masquerade attacks,
  - which are detected by a typical behavior profiles or violations of security constraints.
- Penetrations of the security control system,
  - which are detected by monitoring for specific patterns of activity.
- Leakage,
  - which is detected by a typical use of system resources.
- Denial of service,
  - which is detected by a typical use of system resources.
- Malicious use,
  - which is detected by a typical behavior profiles, violations of security constraints, or use of special privileges.

Intrusion Process

- Reconnaissance
- Physical Intrusion
- Denial of Service
  - Ping-of-Death
  - SYNFlood
  - Landnatierra
  - WinNuke

System Intrusions

- The dangers of system intrusion manifests are many including:
  - Loss of personal data that may be stored on a computer
  - Compromised privacy
    most of the information about an individual is stored online by companies and government organizations
  - Legal liability
    - If your organization network has customer personal information and it gets broken into, thus compromising personal information that you stored, you are potentially liable for damages caused by a hacker either breaking into your network or using your computers to break into other systems

Intrusion Detection Systems

- An intrusion detection system (IDS) is a system used to detect unauthorized intrusions into computer systems and networks
- In fact, according to the Greek legend of the Trojan Horse, the people of Crete were defeated by the Greeks because the Greeks managed to penetrate the heavily guarded gates of the city walls.
- intrusion detection has been used by individuals,
  - they have used dogs, flood lights , electronic fences, and closed circuit television and other watchful gadgets to be able to detect intrusions.

From 6 to 3

- Aurobindo Sundaram divides intrusions into six types, These six can now be put into three models of intrusion detection mechanisms
  - anomaly-based / behaviour
  - signature-based /misuse-based detection
    - unauthorized access
    - unauthorized modification and
    - denial of service.
  - hybrid detection

Anomaly Detection

- Anomaly based systems are "learning" systems in a sense that they work by continuously creating "norms" of activities
- these norms are then later used to detect anomalies that might indicate an intrusion
- In anomaly detection, it is assumed that all intrusive activities are necessarily anomalous
- Typical areas of interest are threshold monitoring, user work profiling, group work profiling, resource profiling, executable profiling, static work profiling, adaptive work profiling, and adaptive rule base profiling

Misuse/Signature detection

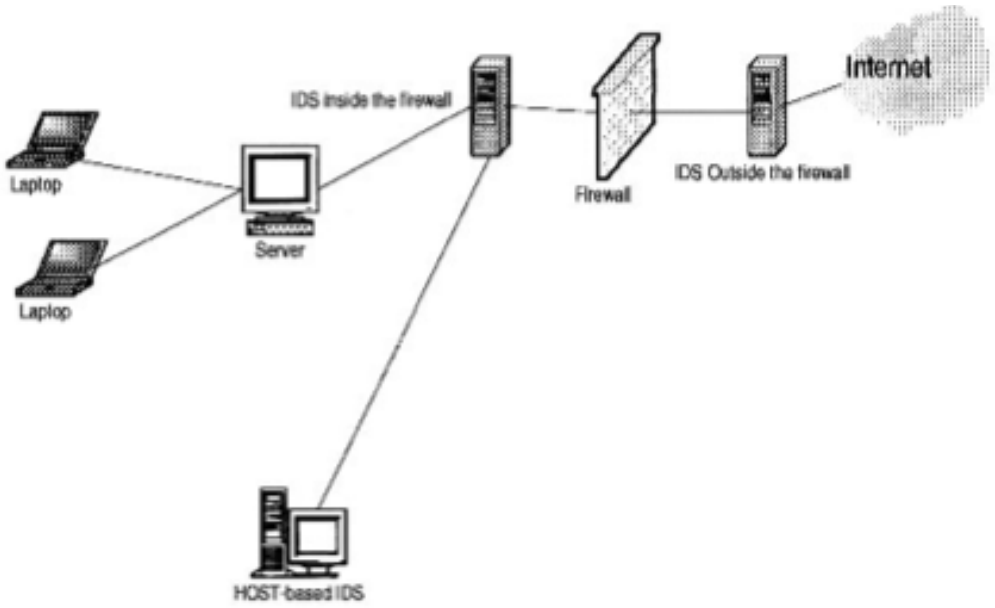
- each intrusive activity is representable by a unique pattern or a signature
  - a slight variations of the same activity produce a new signature and therefore can also be detected.
- work by looking for a specific signature on a system.
- Identification engines perform well by monitoring these patterns of known misuse of system resources.
- Two major problems arise out of this concept:
  - cannot detect unknown attacks with unmapped and un-archived signatures.
  - cannot detect new attacks.

Types of IDS

- Network-based Intrusion Detection Systems (NIDSs)
  - monitor the traffic on the network to detect intrusions.
  - can either run as an independent standalone machine where it promiscuously watches over all network traffic or it can just monitor itself as the target machine to watch over its own traffic.
    - example, it can watch itself to see if somebody is attempting a SYN-flood or a TCP port scan.

- is it possible that an attacker can evade this detection?

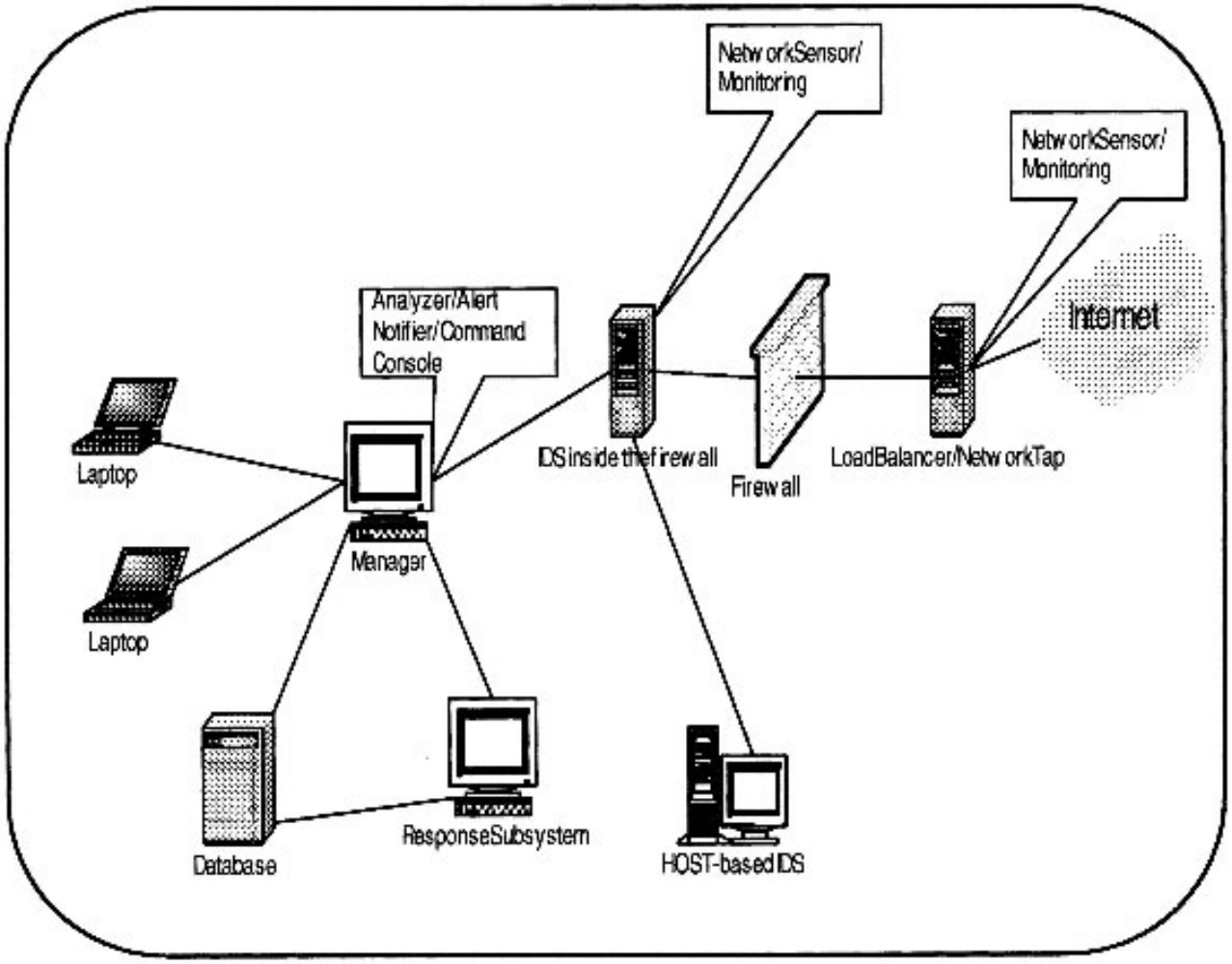
Architecture of NIDS



- Network Tap
- Network sensor
- analyzer
- alert notifier
- command console
- response subsystem
- database

Placement of IDS Sensors

- Inside DMZ
- between Firewall – Internet
- Behind Firewall
- Inside the network



Advantages NIDS

- able to detect attacks that a HIDS would miss, because NIDS monitors network traffic at a transport layer.
- Difficulty to remove evidence
- Real-time detection and response
- able to detect unsuccessful attacks and malicious intent.

Disadvantages of NIDS

- Blind Spots.
- Encrypted Data

Host-Based Intrusion Detection Systems (HIDS)

- Recent studies have shown that the problem of organization information misuse is not confirmed only to the "bad" outsiders but the problem is more rampart within organizations
- HIDS is the technique of detecting malicious activities on a single computer
- A HIDS
  - deployed on a single target computer
  - it uses software that monitors OS specific logs including system, event, and security logs

Advantages HIDS

- Ability to verify success or failure of an attack quickly
- Low-level monitoring.
- Near real-time detection and response
- Ability to deal with encrypted and switched environments
- Cost effectiveness

Disadvantages of HIDS

- Myopic Viewpoint. Since they are deployed at a host, they have a very limited view of the network.
- Since they are close to users, they are more susceptible to illegal tampering.

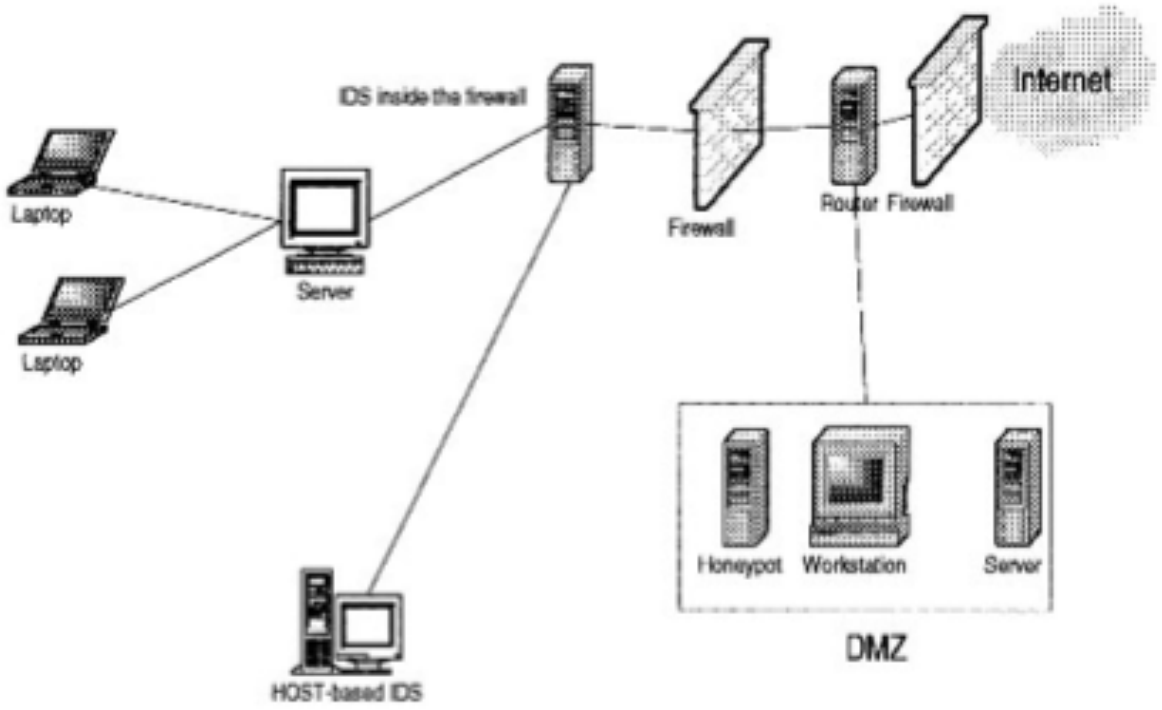
Hybrid IDS

- NIDS have been historically unable to work successfully in switched and encrypted networks
- HIDS have not been successful in high-speed networks – whose speed exceed 100 Mbps
- This raises the question of a hybrid system that contains all the things that each system has and those that each system misses, a system with both components
- Hybrids are new and need a great deal of support to gain on their two cousins.

Other Types of IDS

- System Integrity Verifiers
  - System integrity verifiers (SIVs) monitor critical files in a system, such as system files
- Log File Monitor
  - first create a record of log files generated by network services.
  - looking for system trends, tendencies, and patterns in the log files that would suggest an intruder is attacking

- Honeypot
  - is a system designed to look like something that an intruder can hack.



Response to System Intrusion

- Incident Response Team
  - keeping up-to-date with the latest threats and incidents,
  - being the main point of contact for incident reporting,
  - notifying others whenever an incident occurs,
  - assessing the damage and impact of every incident,
  - finding out how to avoid exploitation of the same vulnerability, and
  - recovering from the incident.

IDS Logs as Evidence

- First and foremost, IDS logs can be kept as a way to protect the organization in case of legal proceedings. Some people tend to view IDSasaformofwiretap.If sensorstomonitortheinternalnetworkare to be deployed, verify that there is a published policy explicitly stating that use of the network is consent to monitoring.

Challenges to IDS

- Deploying IDS in Switched Environments

Intrusion Prevention Systems

- NIPS
  - Traffic Normalizer
  - The Detection Engine
  - Traffic Shaper
- Host-Based Intrusion Prevention Systems (HIPSs)

Intrusion Detection Tools

Name	Source
Realsecure v.3.0	ISS
Net Perver 3.1	Axent Technologies
Net Ranger v2.2	CISCO
FlightRemohe v2.2	NFR Network
Sessi-Wall-3, v4.0	Computer Associates
Kane Security Monitor	Security Dynamics

- Monitoring tools give information on:
  - hundreds of thousands of network connections
  - external break-in attempts
  - internal scans
  - misuse patterns of confidential data
  - unencrypted remote logins or a Web sessions unusual or potentially troublesome observed network traffic.

Non-Commercial IDS Tools

- flow-tools
- tripwire
- tcpdump
- snort
- portsentry
- dragon IDS
- TCP Wrapper
- RealSecure
- Shadow
- NetProwler
- Network Auditor

Exercise

- Download and install honeypot and start using it.
- Discuss how exploits can be used to penetrate a network. Research and list 10 different common exploits