

Information Security

CS3002

Lecture 22
13th November 2024

Dr. Rana Asif Rehman
Email: r.asif@lhr.nu.edu.pk



Intrusion Detection Systems (IDS)





**INTRUSION
DETECTION
SYSTEM**



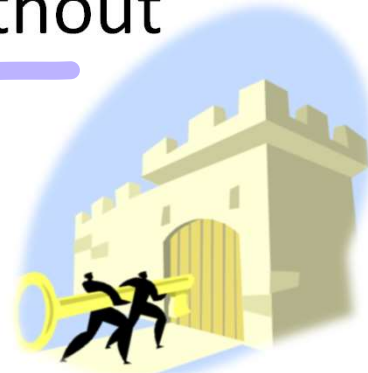
**INTRUSION
PREVENTION
SYSTEM**

Intrusion

- Attempt to break into or misuse a system
- Intruders may be from outside the network or legitimate users of the network
- Three classes of intruders:
 - 1 – **Masquerader**: an individual who is not authorized to use the computer and who penetrate a system's access controls to exploit a legitimate user's account. (usually outside)
 - 2 – **Misfeasor**: A legitimate user who access data, program, or resources for which such access is not authorized , or who is authorized for such access but misuses them. (usually inside)
 - 3 – **Clandestine user**: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection. (can be either inside or outside)

Types of Attacks using Intrusion

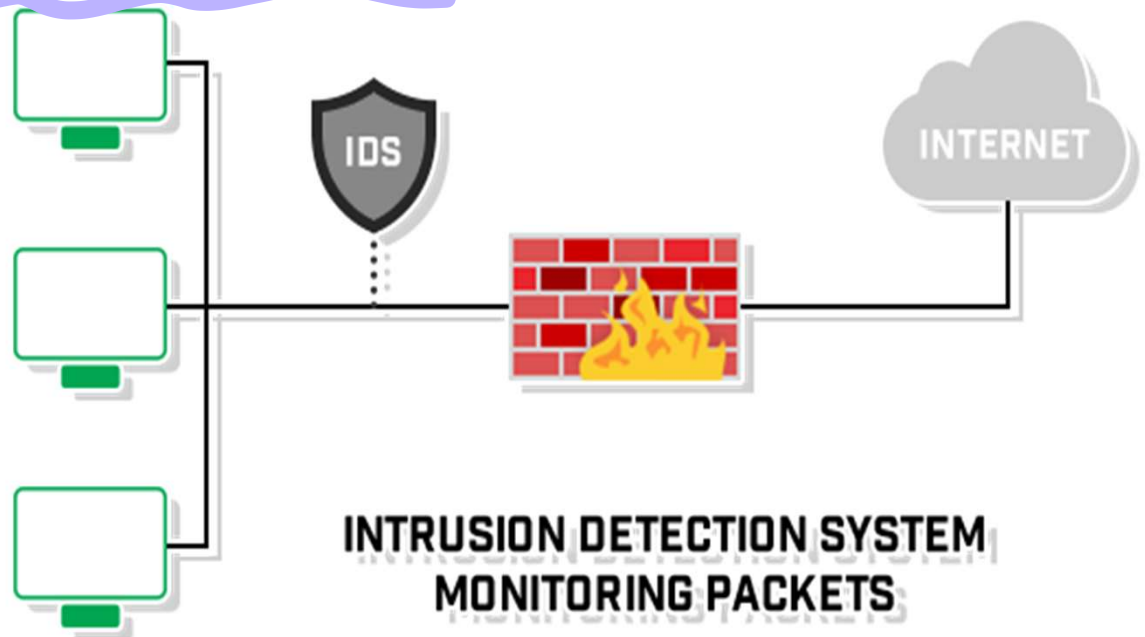
- Performing a remote root compromise of an e-mail server
- Defacing a Web server
- Guessing and Cracking passwords
- Copying a database containing credit card numbers
- Viewing sensitive data (i.e. Payroll records and media without authorizations)
- Running a packet sniffer on a workstation to capture usernames and passwords
- Using an unattended, logged-in workstation without permission



Intrusion Detection System (IDS)

A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.

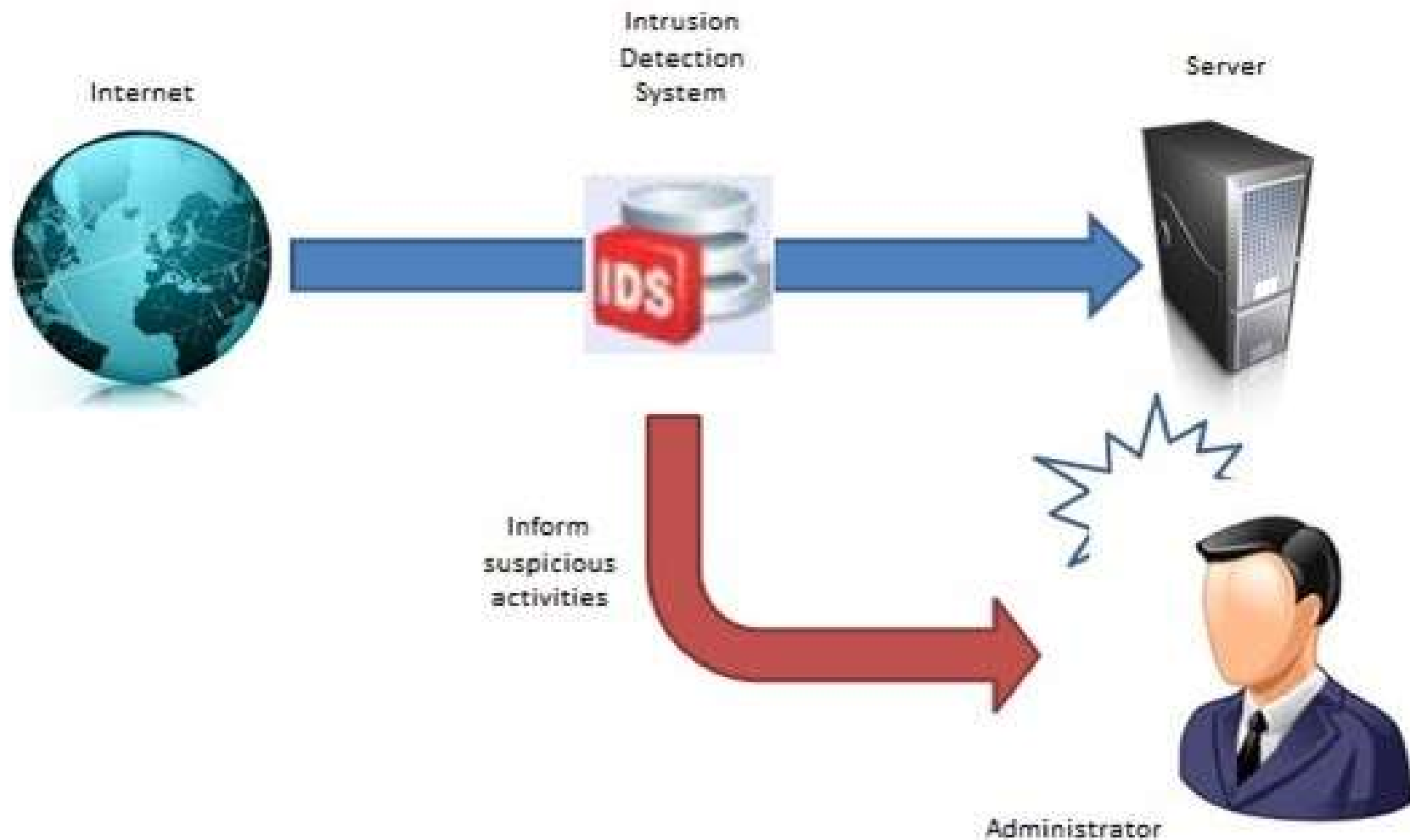
- Intrusion Detection Systems look for attack signatures (patterns that usually indicate malicious or suspicious intent)



IDS

Device or application that ...

- Monitors network activities
- Attempts to detect suspicious activities going through the network.



Components of an IDS

- An IDS comprises of three logical components:
 - **Sensors**: sensors are responsible for collecting data (i.e. network packets, log files, and system call traces)
 - **Analyzers**: analyzers receive inputs from one or more sensors or from other analyzers. The analyzer is responsible for determining if an intrusion has occurred.
 - **User Interface**: it enables a user to view output from the system or control behavior of the system. (i.e. UI may associate to a manager, director, or console component)

Sensors → Analyzers → UI

Basic Principles of IDSs

- 1) If an intruder is detected quickly enough, the intruder can be identified and ejected from the system before any damage. Even if the detection is not that quick, sooner the intrusion is detected, the less the amount of damage and more quickly the recovery can be achieved.
- 2) An effective IDS can serve as a deterrent, thus acting to prevent intrusion.
- 3) Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen intrusion prevention measures.

Intrusion Detection System

- Different ways of classifying an IDS

1

- Anomaly based detection

2

- Signature based detection

3

- Hybrid detection

- Specification based detection



1. Anomaly based Detection

- It involves a collection of information about legitimate user's behavior over a period of time. Then, statistical tests are applied to observe them.
- Anything distinct from the usual behavior is assumed to be an intrusion activity.
 - E.g flooding a host with lots of packet.
- The primary strength is its ability to recognize novel attacks.
- Such IDS generate many false alarms and hence compromise the effectiveness of the IDS.



2. Signature based Detection

- Involves an attempts to define a set of rules or attack patterns that can be used to decide that a given behavior is that of an intruder.
- The question of what information is relevant to an IDS depends upon what it is trying to detect.
 - E.g DNS, FTP etc.
- Most signature analysis systems are based simple pattern matching algorithms. For example, the IDS simply looks for a sub string within a stream of data carried by network packets. When it finds this sub string (for example, the "phf" in "GET /cgi-bin/phf?"), it identifies those network packets as vehicles of an attack.



Signature based detection

- Signature techniques detect intrusion by observing events on system & apply rules to decide if activity is suspicious or not.

Rule-based anomaly detection:

- analyze historical audit records to identify usage patterns & auto-generate rules for them
- then observe current behavior & match against rules to see if conforms
- like statistical anomaly detection does not require prior knowledge of security flaws
- It requires to have a large database of rules to be effective.



3. Specification-based Intrusion Detection

- The desirable behavior of a system is described through its functionalities and through the security policy. Any sequence of operations executed outside of the system's specifications is considered to be a security violation
- Use of manually specified program behavioral specifications is the basis to detect attacks
- It has been proposed as a promising alternative that combine the strengths of misuse detection (accurate detection of known attacks) and anomaly detection (ability to detect novel attacks)
- The development of the specifications is an expensive and tedious process and specifications are often very difficult to evaluate and verify.

Effectiveness of an IDS

- Practically an intrusion detection system needs to detect a substantial percentage of intrusions while keeping the false alarms rate at acceptable level.
 - if too few intrusions detected -> false security
 - if too many false alarms -> ignore / waste time while analyzing the false alarm
- Achieving this fate is very hard to achieve
- Existing systems seem not to have a good record

Types of IDS

- Intrusion Detection Systems (IDSs) can be classified into:

i) Host-based IDS (HIDS):

Monitors the characteristics of a single host and the events occurring within that host for suspicious activity.

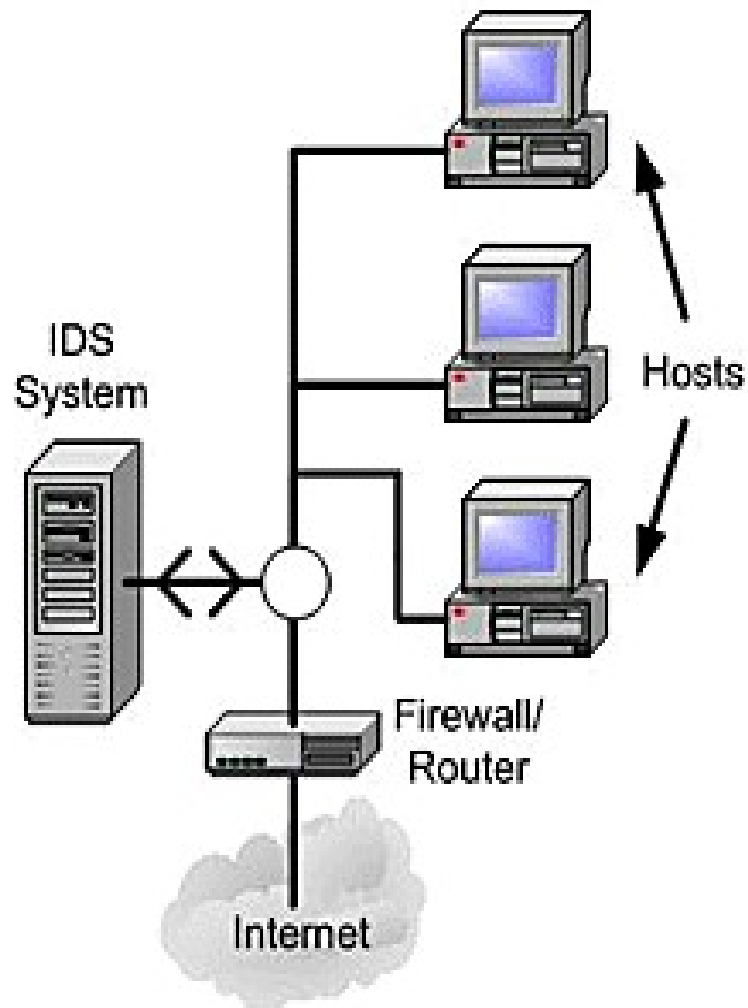
ii) Network-based IDS (NIDS):

Monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity.

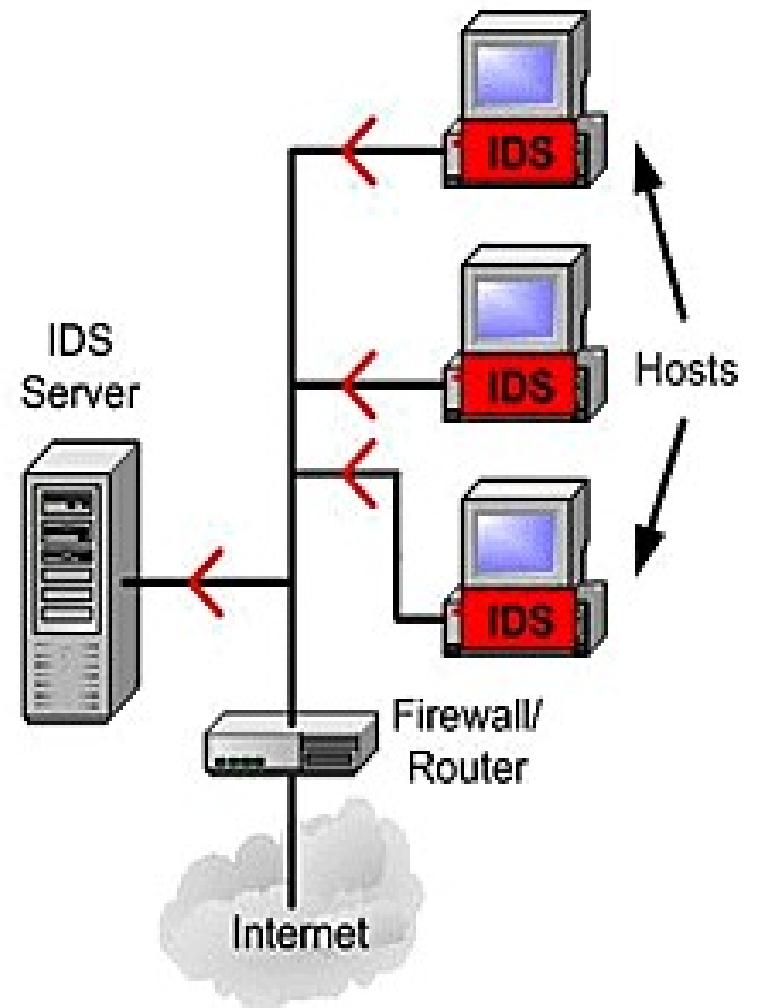


Types of IDS

Network Based IDS



Host Based IDS



1. Host/Applications based IDS (HIDS)

- The host operating system or the application logs in the audit information.
- These audit information includes events like the use of identification and authentication mechanisms (logins etc.) , file opens and program executions, admin activities etc.
- This audit is then analyzed to detect trails of intrusion.



Strengths of the HIDS



- Attack verification
- System specific activity
- Encrypted and switch environments
- Monitoring key components
- Near Real-Time detection and response
- No additional hardware

Drawbacks of the HIDS

- The kind of information needed to be logged in is a matter of experience.
- Unselective logging of messages may greatly increase the audit and analysis burdens.
- Selective logging runs the risk that attack manifestations could be missed.

2. Network based IDS (NIDS)

- A network-based IDS monitors traffic at selected points on a network or interconnected set of networks.
- It examines the traffic packet by packet in real time or close to real time in order to detect intrusion patterns.
- A filter is usually applied to determine which traffic will be discarded or passed on to an attack recognition module. This helps to filter out known un-malicious traffic.

Strengths of NIDS

- Cost of ownership reduced
- Packet analysis
- Real time detection and response
- Malicious intent detection
- Complement and verification
- Operating system independence

IDS Example: SNORT

- Lightweight IDS
 - real-time packet capture and rule analysis
 - easily deployed on nodes
 - uses small amount of memory and processor time
 - easily configured

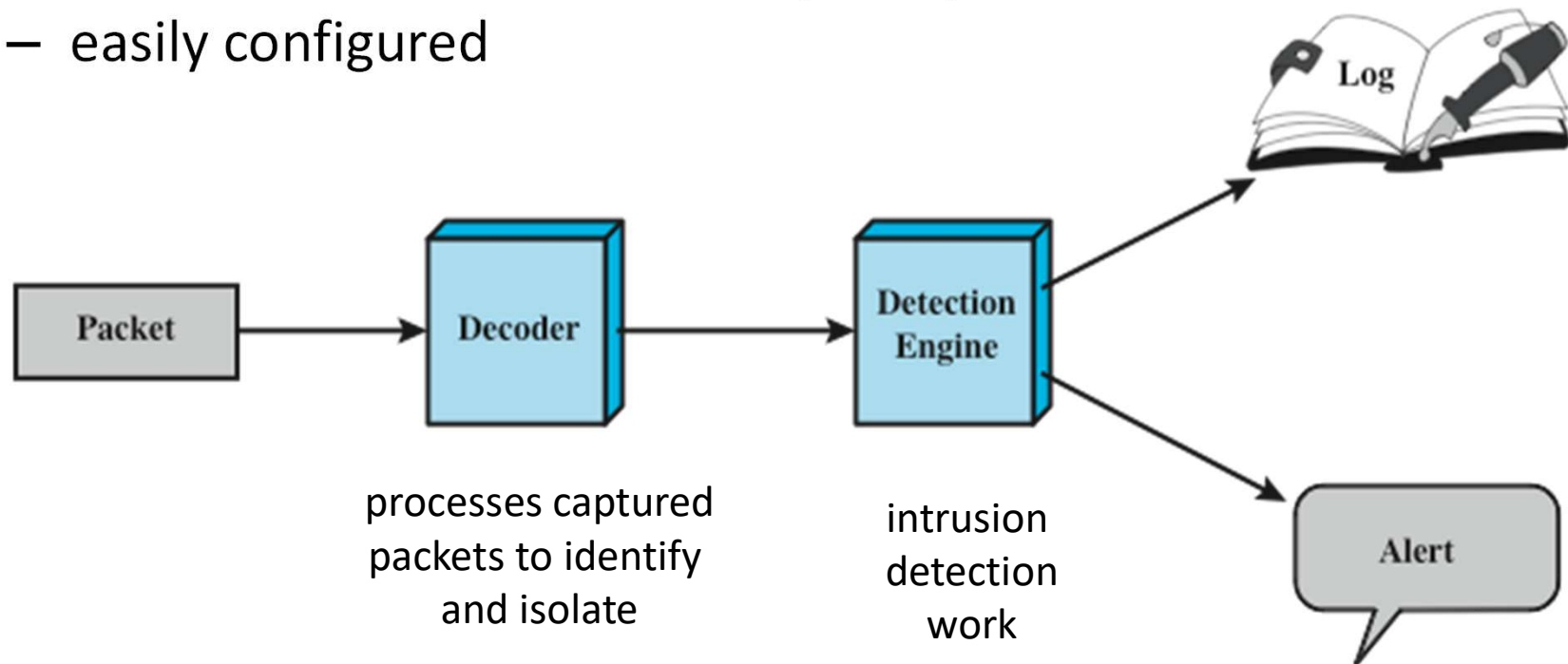


Figure 8.9 Snort Architecture

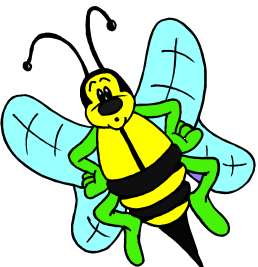
Honey Pots



- Decoy systems that designed to lure a potential attacker away from critical systems
- An asset that solely exists to be attacked
- It could be an individual item, a system or entire network
- It could be a real system or emulated.

Purpose

- Divert an attacker from accessing critical systems
- Collect information about the attacker's activity
- Good at detecting new or unknown threats
- Engage the attacker to stay on the system long enough for administration to respond



Honeypot Deployment

3. Full internal honeypot;
can detect internal attacks



2. In DMZ; must make sure the other
systems in the DMZ are secure; firewalls
may block traffic to the honeypot

1. Tracks attempts to connect
to an unused IP address; can't help
with inside attackers

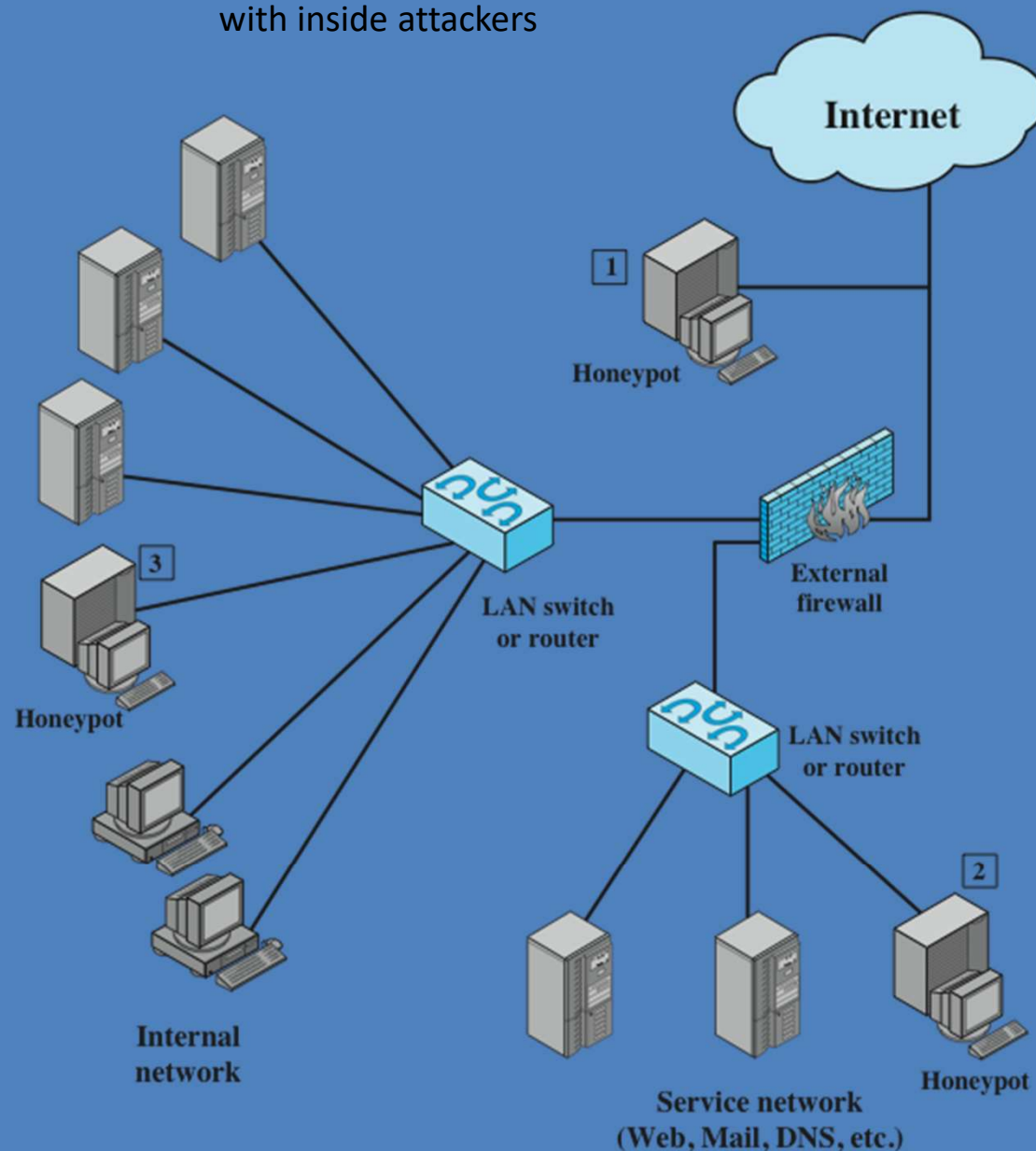



Figure 8.8 Example of Honeypot Deployment

Deception Technology

- Honeypots are limited in scope 
 - it uses static decoys due to which adversary starts to understand the decoys
 - requires expensive resources to implement and maintain

Deception technology is a proactive cyber defense system through the use of decoys to lure, detect and defend, without the issues of scalability, skilled and available resources.

- Uses automated dynamic traps generated by AI
- Immediate alerts with minimum false positive rates.
- Deploy traps according to the behavioral patterns of the hacker
- Provide detailed reports for post cyber defense investigation

Deception Technology

- **Decoy Files**
 - Used as a “marker”
 - In case of an access, read, copy, or deletion, it serves as an alert to monitors
 - It could be anything: file, database, picture, email, account, etc
 - Normally used to deliver bogus information to attackers
- **Honey net**
 - Collection of two or more honeypots/decoy devices
 - Could be at the same location or distributed
 - Managed by same entity

Interaction Level

It is the capability to mimic a real asset or object

- **High** – More Realistic that mimics real, legitimate computer or device with applications, activity, and changing content
 - Needed for more hacker interaction, intent, etc.
 - More involved setup and maintenance
- **Low** – Does very little to mimic real, legitimate device
 - Usually just TCP/IP port advertising or basic logon prompts
 - For early warning honeypots • Quicker setup, less ongoing maintenance, less risk
- If you can actually logon to a decoy, then you're at least at **Medium** interaction