R.M.K GROUP OF ENGINEERING INSTITUTIONS

R.M.K
GROUP OF INSTITUTIONS

R.M.K
GROUP OF
INSTITUTIONS

Please read this disclaimer before proceeding:

22CY701
INTRUSION DETECTION AND INTERNET SECURITY
(Lab Integrated)

UNIT II
INTRUSION DETECTION AND PREVENTION TECHNIQUES

Department : **CSE(CS)**

Batch/Year : **2022 - 2026 /IV**

Created by :**Dr. Dharini N**

Date : **10.06.2025**

R.M.K GROUP OF INSTITUTIONS

Table of Contents

R.M.K GROUP OF INSTITUTIONS

Course Objectives

22CY701 INTRUSION DETECTION AND INTERNET SECURITY

(Lab Integrated)

COURSE OBJECTIVES

- To Understand when, where, how, and why to apply Intrusion Detection tools and techniques in order to improve the security posture of an enterprise.
- To Apply knowledge of the fundamentals and history of Intrusion Detection in order to avoid common pitfalls in the creation and evaluation of new Intrusion Detection Systems
- To Analyze intrusion detection alerts and logs to distinguish attack types from false alarms
- To Understand the fundamentals of network security, including the MAC layer, Internet Protocol, and common attacks targeting these layers.
- To Gain an understanding of key internet security mechanisms, including firewalls, virtual private networks (VPNs), and TLS/SSL VPNs.

Prerequisite

22CY701 INTRUSION DETECTION AND INTERNET SECURITY

PREREQUISITE

1. 22CY401-CYBER SECURITY ESSENTIALS
2. 22CS501 – COMPUTER NETWORKS
3. 22CS901 – ETHICAL HACKING

Syllabus

22CY701 – INTRUSION DETECTION AND INTERNET SECURITY (Lab Integrated)

SYLLABUS **3 0 2 4**

UNIT I INTRODUCTION TO INTRUSION DETECTION

History of Intrusion detection, Audit, Concept and definition, Internal and external threats to data, attacks, Need and types of IDS, Information sources Host based information sources, Network based information sources.

List of Exercise/Experiments

1. Install Snort and configure it to monitor network traffic.

2. Deploy Snort as a Network Intrusion Detection System (NIDS).

UNIT II INTRUSION DETECTION AND PREVENTION TECHNIQUES

Intrusion Prevention Systems, Network IDs protocol based IDs , Hybrid IDs, Analysis schemes, thinking about intrusion. A model for intrusion analysis, techniques Responses requirement of responses, types of responses mapping responses to policy Vulnerability analysis, credential analysis non credential analysis

List of Exercise/Experiments

1. Write and implement custom Snort rules to detect specific traffic patterns.

2. Integrate Snort with MySQL to log alerts to a database.

UNIT III SNORT

Introduction to Snort, Snort Installation Scenarios, Installing Snort, Running Snort on Multiple Network Interfaces, Snort Command Line Options. Step-By-Step Procedure to Compile and Install Snort Location of Snort Files, Snort Modes Snort Alert Modes- Working with Snort Rules, Rule Headers, Rule Options, The Snort Configuration File etc. Plugins, Preprocessors and Output Modules, Using Snort with MySQL

List of Exercise/Experiments

1.Enhance Snort's functionality using preprocessors and plugins.

2.Set up advanced alerting and logging mechanisms.

UNIT IV ESSENTIALS OF INTERNET SECURITY

Network Security basics-The MAC Layer and Attacks- The Internet Protocol and Attacks- Packet Sniffing and Spoofing-Attacks on TCP Protocol- DNS Attacks Overview - Local DNS Cache Poisoning Attack- Remote DNS Cache Poisoning attack- Replay forgery attacks-DNS Rebinding attack- DoS on DNS Servers- DNSSEC-Securing DNS

List of Exercise/Experiments

1.Conducting TCP SYN Flood Attack

2.Sniffing Packets on Network Interfaces

3.Spoofing Source IP Address in Packets

4.Investigating DNSSEC Implementation and Validation

UNIT V INTERNET SECURITY MECHANISMS

Firewall-Virtual Private Network-Overview of How TLC/SSL VPN Works- Creating and using the TUN Interface- Implementing the IP Tunnel- Testing VPN- Tunneling and Firewall Evasion- -BGP and Attacks- The Heartbleed bug and attack- Reverse Shell

List of Exercise/Experiments

1. Configuring Linux Firewall using IP tables
2. Setting Up VPN Tunnels
3. Exploring BGP Session Hijacking
4. Simulating Heartbleed Attack Scenario

Course Outcomes

R.M.K GROUP OF INSTITUTIONS

COURSE OUTCOMES

- CO1: Understand fundamental concepts and demonstrate skills in capturing and analyzing network packets.
- CO2: Utilize various protocol analyzers and Network Intrusion Detection Systems (NIDS) to detect network attacks and troubleshoot network problems.
- CO3: Develop the ability to proficiently use the Snort tool for detecting and mitigating network attacks
- CO4: Demonstrate knowledge of network security basics, including MAC layer vulnerabilities and attacks, as well as common attacks targeting the Internet Protocol.
- CO5: Demonstrate understanding of firewall, VPN, and TLS/SSL VPN principles and functionalities in network security.
- CO6: Apply the concepts of Intrusion Detection and internet security protocols to develop cyber security mechanisms.

CO – PO/ PSO Mapping

R.M.K GROUP OF INSTITUTIONS

CO-PO MAPPING

COs	PO's/PSO's														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	3	3	1	2	2	–	–	–	–	1	–	2	2	3	1
CO2	3	3	1	2	2	–	–	–	–	1	–	2	2	3	2
CO3	2	2	2	1	3	–	–	1	1	2	1	2	1	3	3
CO4	3	2	1	1	1	–	–	2	–	1	–	3	1	3	1
CO5	3	2	1	1	2	1	–	2	1	2	1	2	1	3	2
CO6	2	2	3	2	3	1	–	2	2	2	2	3	3	3	3

1 – Low, 2 – Medium, 3 – Strong

Lecture Plan

R.M.K
GROUP OF
INSTITUTIONS

LECTURE PLAN

S No	Topics	No of periods	Proposed date	Actual Lecture Date	Pert aining CO	Taxo nomy level	Mode of delivery
1	Intrusion Prevention Systems	1	03.08.2025		CO2	K1	ICT Tools
2	Network IDS	1	04.08.2025		CO2	K2	ICT Tools
3	Protocol based IDS	1	06.08.2025		CO2	K3	ICT Tools
4	Hybrid IDS	1	08.08.2025		CO2	K2	ICT Tools
5	Analysis schemes, thinking about intrusion	1	09.08.2025		CO2	K2	ICT Tools
6	A model for intrusion analysis techniques	1	10.08.2025		CO2	K2	ICT Tools
7	Responses requirement of responses	1	11.08.2025		CO2	K2	ICT Tools
8	Types of responses mapping responses to policy	1	12.08.2025		CO2	K2	ICT Tools
9	Vulnerability analysis	1	13.08.2025		CO2	K3	ICT Tools
10	Credential analysis non credential analysis	1	13.08.2025		CO2	K3	Lecture and Practical
11	Write and implement custom Snort rules to detect specific traffic patterns.	1	29.08.2025		CO2	K3	Lecture and Practical
12	Write and implement custom Snort rules to detect specific traffic patterns.	1	30.08.2025		CO2	K3	Lecture and Practical

13	Integrate Snort with MySQL to log alerts to a database.	1	29.08.2025		CO2	K3	Lecture and Practical
14	Integrate Snort with MySQL to log alerts to a database.	1	30.08.2025		CO2	K3	Lecture and Practical
15	Integrate Snort with MySQL to log alerts to a database.	1	30.08.2025		CO2	K3	Lecture and Practical

Activity Based Learning

RIDDLES

S.No.	Riddle	Answer
1	I'm your silent guard, watching the gate, I block bad traffic before it's too late. I work in real-time, not just detection— Guess my name, I'm your protection.	Intrusion Prevention System (IPS)
2	I'm a silent observer, nothing I block. Just log and alert around the clock. I sniff your traffic like a cyber sleuth— Tell me now, what is this truth?	Intrusion Detection System (IDS)
3	I'm a blend of two, a hybrid design, Signature and anomaly—both align. I raise alerts when threats unfold— My nature is both new and old.	Hybrid IDS
4	I use patterns from past attacks, To catch new threats that leave no tracks. Though false positives I may bring, My signature still means everything.	Signature-based IDS
5	No known pattern do I need, I look for things that mislead. Baseline behavior is my friend, When it changes, I defend.	Anomaly-based IDS
6	Run on servers, deep and wide, Watching files and ports inside. On one machine, I hold my post— Which IDS am I the most?	Host-based IDS (HIDS)
7	From the network I draw my clue, Packets passing, old and new. I sniff the stream and raise my hand— To detect threats across the land.	Network-based IDS (NIDS)
8	I'm not a threat, but show you one. Simulating attacks just for fun. Pen-testers love me when I act— What am I, the red team's tact?	Vulnerability Scanner
9	I'm a list of what could go wrong, A catalog that's large and long. I help you patch before attacks begin— Guess what I am and you will win.	Vulnerability Database
10	If you want to know what users know, This kind of analysis will help you so. It checks for passwords and access keys— To see how safe your network be.	Credential Analysis
11	No login needed, yet I scan, Your open ports, from a van. I don't ask nicely, just explore— To see what services you ignore.	Non-Credentialed Analysis
12	I am the step that comes right after, An alert, a log, a cyber disaster. Shut it down, contain the spread— What is this action before we're dead?	Response
13	I can be automatic or manual too, Reactive or proactive, it's up to you. My types are many, my timing tight— I aim to fix what isn't right.	Response Type
14	In policies written clear and deep, I'm the rule you vow to keep. Your actions must map back to me, For governance and security.	Security Policy
15	I'm the model you use to think, When threats arise and systems sink. Analyze steps of a hacker's plan— Guess who I am, if you can.	Intrusion Analysis Model

Lecture Notes

R.M.K GROUP OF INSTITUTIONS

UNIT II

1. INTRUSION PREVENTION SYSTEMS

An Intrusion Prevention System (IPS) is a network security technology that monitors network traffic for malicious activity and automatically blocks or prevents it. It acts as a proactive defense, sitting inline with network traffic to detect and respond to threats in real-time. Unlike Intrusion Detection Systems (IDS) which only detect and alert, IPS can actively block or drop malicious traffic, preventing attacks from reaching their target.

Key Features and Functions:

- **Real-time Monitoring:**
  IPS continuously monitors network traffic for suspicious activity, looking for patterns and signatures that match known attacks.
- **Malicious Activity Blocking:**
  When a threat is detected, the IPS can automatically block the malicious traffic, preventing it from entering the network.
- **Alerting and Logging:**
  IPS can also generate alerts to notify security teams of detected threats and log relevant information for analysis and incident response.
- **Customizable Rules:**
  IPS systems can be configured with rules and policies to define what constitutes malicious activity and how the system should respond.
- **Integration with other security tools:**
  IPS can be integrated with other security solutions like firewalls and antivirus software to create a comprehensive security posture.

Common Actions Taken by IPS:

- **Blocking malicious traffic:** Dropping packets, resetting connections, or blocking traffic from specific IP addresses.
- **Alerting security personnel:** Sending notifications about detected threats.
- **Terminating dangerous connections:** Stopping malicious connections that are actively being used.
- **Modifying security policies:** Adjusting firewall rules or other security settings to prevent future attacks.

An IPS will typically consist of four main components:

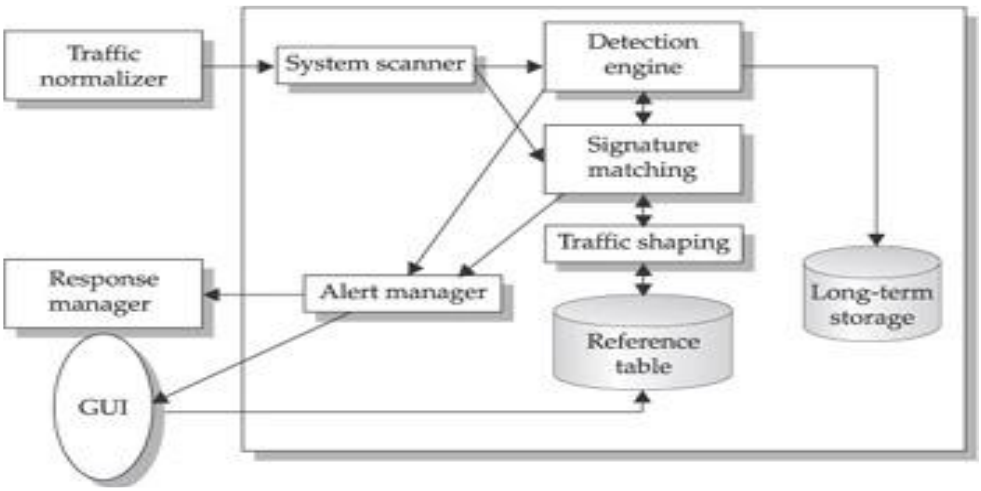
· Traffic normalizer

· Service scanner

· Detection engine

· Traffic shaper

The traffic normalizer will interpret the network traffic and do packet analysis and packet reassembly, as well as performing basic blocking functions. The traffic is then fed into the detection engine and the service scanner. The service scanner builds a reference table that classifies the information and helps the traffic shaper manage the flow of the information. The detection engine does pattern matching against the reference table, and the appropriate response is determined. Figure below outlines this process.



Standard IPS system

IDS	IPS
Installed on network segments (NIDS) and on hosts (HIDS)	Installed on network segments (NIPS) and on hosts (HIPS)
Sits on network passively	Sits inline (not passive)
Cannot parse encrypted traffic	Better at protecting applications
Central management control	Central management control
Better at detecting hacking attacks	Ideal for blocking web defacement
Alerting product (reactive)	Blocking product (proactive)

Benefits of using an IPS:

- **Enhanced security:**

  IPS provides a proactive layer of defense against a wide range of cyber threats, including malware, ransomware, and vulnerability exploits.

- **Reduced risk of attacks:**

  By automatically blocking malicious traffic, IPS helps to minimize the potential damage caused by successful attacks.

- **Improved security posture:**

  IPS complements other security tools and technologies to create a more robust and comprehensive security strategy.

- **Reduced workload for security teams:**

  By automating threat detection and response, IPS can free up security personnel to focus on more complex tasks.

  There are two complementary ways of looking at an IPS:

  1. An IPS is an inline network-based IDS (NIDS) that has the capability to block traffic by discarding packets as well as simply detecting suspicious traffic. Alternatively, the IPS can monitor ports on a switch that receives all traffic and then send the appropriate commands to a router or firewall to block traffic. For host-based systems, an IPS is a host-based IDS that can discard incoming traffic.

  2. An IPS is a functional addition to a firewall that adds IDS types of algorithms to the repertoire of the firewall.

  Thus, an IPS blocks traffic, as a firewall does, but makes use of the types of algorithms developed for IDSs. It is a matter of terminology whether an IPS is considered a separate, new type of product or simply another form of firewall.

  Host-Based IPS

  As with an IDS, an IPS can be either host based or network based. A host-based IPS (HIPS) makes use of both signature and anomaly detection techniques to identify attacks. In the former case, the focus is on the specific content of application payloads in packets, looking for patterns that have been identified as malicious. In the case of anomaly detection, the IPS is looking for behavior patterns that indicate malware. Examples of the types of malicious behavior addressed by a HIPS include the following:

  · **Modification of system resources:** Rootkits, Trojan horses, and backdoors

operate by changing system resources, such as libraries, directories, registry settings, and user accounts.

· **Privilege-escalation exploits:** These attacks attempt to give ordinary users root access.

· **Buffer-overflow exploits**: A buffer overflow occurs when a program writes more data to a fixed-length block of memory (a buffer) than it can hold. This extra data can overwrite adjacent memory, potentially allowing an attacker to:

- Execute arbitrary code,
- Crash the application,
- Escalate privileges.

This is commonly exploited when input is not properly validated.

· **Access to e-mail contact list:** Many worms spread by mailing a copy of themselves to addresses in the local system's e-mail address book.

· **Directory traversal:** A directory traversal vulnerability in a Web server allows the hacker to access files outside the range of what a server application user would normally need to access.

Attacks such as these result in behaviors that can be analyzed by a HIPS. The HIPS capability can be tailored to the specific platform. A set of general-purpose tools may be used for a desktop or server system. Some HIPS packages are designed to protect specific types of servers, such as Web servers and database servers. In this case, the HIPS looks for particular application attacks.

In addition to signature and anomaly-detection techniques, a HIPS can use a sandbox approach. Sandboxes are especially suited to mobile code, such as Java applets and scripting languages. The HIPS quarantines such code in an isolated system area, then runs the code and monitors its behavior. If the code violates predefined policies or matches predefined behavior signatures, it is halted and prevented from executing in the normal system environment.

The following are areas for which a HIPS typically offers desktop protection:

· **System calls:** The kernel controls access to system resources such as memory, I/O devices, and processor. To use these resources, user applications invoke system calls to the kernel. Any exploit code will execute at least one system call. The HIPS can be configured to examine each system call for malicious characteristics.

· **File system access:** The HIPS can ensure that file access system calls are not malicious and meet established policy.

System registry settings: The registry maintains persistent configuration information about programs and is often maliciously modified to extend the life of an exploit. The HIPS can ensure that the system registry maintains its integrity.

· **Host input/output:** I/O communications, whether local or network based can propagate exploit code and malware. The HIPS can examine and enforce proper client interaction with the network and its interaction with other devices.

THE ROLE OF HIPS Many industry observers see the enterprise endpoint, including desktop and laptop systems, as now the main target for hackers and criminals, more so than network devices. Thus, security vendors are focusing more on developing endpoint security products. Traditionally, endpoint security has been provided by a collection of distinct products, such as antivirus, antispyware, antispam, and personal firewalls. The HIPS approach is an effort to provide an integrated, single-product suite of functions. The advantages of the integrated HIPS approach are that the various tools work closely together, threat prevention is more comprehensive, and management is easier. It may be tempting to think that endpoint security products such as HIPS, if sophisticated enough, eliminate or at least reduce the need for network-level devices. For example, the San Diego Supercomputer Center reports that over a four-year period, there were no intrusions on any of its managed machines, in a configuration with no firewalls and just endpoint security protection. Nevertheless, a more prudent approach is to use HIPS as one element in a strategy that involves network-level devices, such as either firewalls or network-based IPSs.

2. NETWORK-BASED IPS

A network-based IPS (NIPS) is in essence an inline NIDS with the authority to discard packets and tear down TCP connections. As with a NIDS, a NIPS makes use of techniques such as signature detection and anomaly detection. Among the techniques used in a NIPS but not commonly found in a firewall is flow data protection. This requires that the application payload in a sequence of packets be reassembled. The IPS device applies filters to the full content of the flow every

time a new packet for the flow arrives. When a flow is determined to be malicious, the latest and all subsequent packets belonging to the suspect flow are dropped.

In terms of the general methods used by a NIPS device to identify malicious packets, the following are typical:

· **Pattern matching:** Scans incoming packets for specific byte sequences (the signature) stored in a database of known attacks

· **Stateful matching:** Scans for attack signatures in the context of a traffic stream rather than individual packets

· **Protocol anomaly:** Looks for deviation from standards set forth in RFCs

Traffic anomaly: Watches for unusual traffic activities, such as a flood of UDP packets or a new service appearing on the network

· **Statistical anomaly:** Develops baselines of normal traffic activity and throughput, and alerts on deviations from those baselines

Network IDS

A **Network Intrusion Detection System (NIDS)** is a security solution that monitors and analyzes network traffic for malicious activities or policy violations. Unlike host-based IDS, which is installed on individual devices, NIDS is deployed at strategic locations within the network to examine traffic from all devices.

The purpose of Network IDS is to

- Detect network-based threats like DoS attacks, port scans, malware transmissions.
- Analyze packet-level data for suspicious patterns.
- Generate alerts for system administrators.

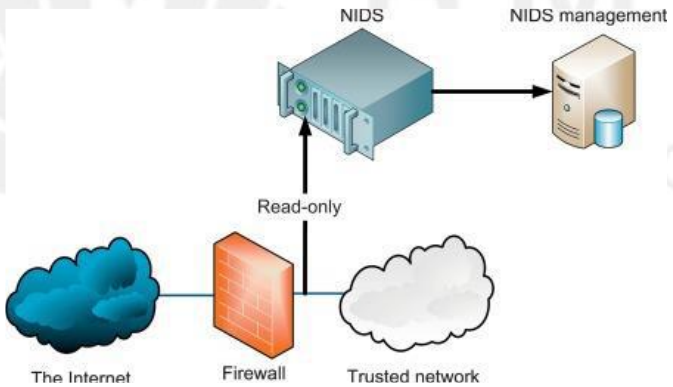
Components of NIDS

- Sensors: Capture network packets.
- Analyzers: Analyze the packets to detect attacks.
- Management Console: View alerts, logs, and reports.
- Signature/Anomaly Database: Contains known attack patterns or behavioral baselines.

Working of NIDS

1. **Traffic Capture**: Network packets are captured using port mirroring or taps.
2. **Preprocessing**: Packets are normalized and reassembled.
3. **Detection Engine**: Uses:
   - **Signature-based Detection**: Matches packets with known attack signatures.
   - **Anomaly-based Detection**: Detects deviations from normal behavior.
4. **Alerting/Logging**: Logs and alerts are generated for suspected attacks.

A network-based intrusion detection system (NIDS) detects malicious traffic on a network. NIDS usually require promiscuous network access in order to analyze all traffic, including all uncast traffic. NIDS are passive devices that do not interfere with the traffic they monitor; Fig below shows a typical NIDS architecture. The NIDS sniffs the internal interface of the firewall in read-only mode and sends alerts to a NIDS Management server via a different (ie, read/write) network interface.



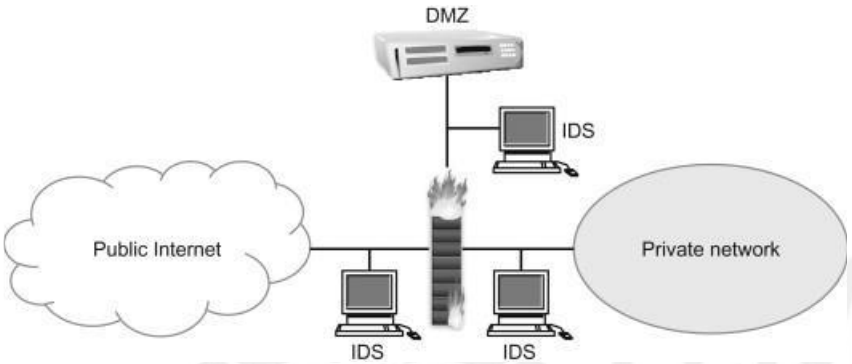
Network-based intrusion detection systems (NIDS)

Network-based intrusion detection systems (NIDS) are devices intelligently distributed within networks that passively inspect traffic traversing the devices on which they sit. NIDS can be hardware or software-based systems and, depending on the manufacturer of the system, can attach to various network mediums such as Ethernet, FDDI, and others. Oftentimes, NIDS have two network interfaces. One is used for listening to network conversations in promiscuous mode and the other is used for control and reporting.

With the advent of switching, which isolates uncast conversations to ingress and egress switch ports, network infrastructure vendors have devised port mirroring techniques to replicate all network traffic to the NIDS. There are other means of

supplying traffic to the IDS such as network taps. Cisco uses Switched Port Analyzer (SPAN) functionality to facilitate this capability on their network devices and, in some network equipment, includes NIDS components directly within the switch.

While there are many NIDS vendors, all systems tend to function in one of two ways; NIDS are either signature-based or anomaly-based systems. Both are mechanisms that separate benign traffic from its malicious brethren. Potential issues with NIDS include high-speed network data overload, tuning difficulties, encryption, and signature development lag time.



DMZ

Network Intrusion Detection Systems use one or more technologies to analyze for threats on your network. These can include:

Packet headers

Packet headers contain specific information about the packet being transmitted across your network. Information in the header can include source and destination IP addresses, ports, protocol types, etc. The NIDS will analyze this information for suspicious activity or malicious behavior.

Packets/transmissions

The total packets per second are a common technology used by a NIDS to monitor for threats on your network. This may be a configuration option that you specify when installing a traffic monitoring system on your network. IDS can compare normal traffic rates, with those being transmitted at any one time across the network, to detect anything out of the ordinary. For example, if there is no heavy traffic on the network, but packets are still being transmitted at a high rate of speed, this could indicate suspicious activity.

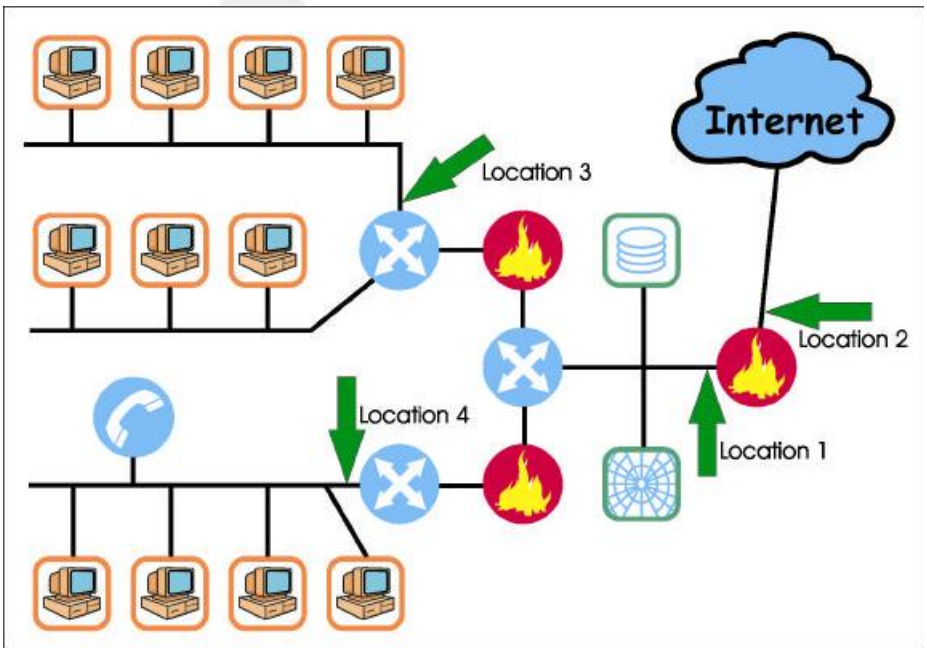
Protocols and applications

Network Intrusion Detection Systems use various types of protocols to monitor for

threats on your network. These can include:

- **Packet protocols**. TCP/IP, UDP/IP, ICMP etc.
- **Anomaly-based protocols**. This is where an IDS has been programmed to detect anomalies in protocols that are otherwise benign when working normally. For example, if you had a specific protocol that was known to have 50% packet loss during normal operation and a packet loss percentage significantly different from the norm is detected, this would trigger an alarm or alert enabling you to investigate the problem further.
- **Data flow analysis**. NIDS can analyze data flow throughout the network to determine where a problem may be taking place. For example, if a user suddenly begins transmitting a large amount of data, an IDS will recognize this and alert you to possible security breaches occurring on your network.

Deployment Locations



Locations of Network-based IDS sensors

a. Location: Behind each external firewall, in the network DMZ

(See above Figure – Location 1)

Advantages:

- Sees attacks, originating from the outside world, that penetrate the network's perimeter defenses.
- Highlights problems with the network firewall policy or performance
- Sees attacks that might target the web server or ftp server, which commonly reside in this DMZ

· Even if the incoming attack is not recognized, the IDS can sometimes recognize the outgoing traffic that results from the compromised server

b. Location: Outside an external firewall

(See above Figure – Location 2)

Advantages:

· Documents number of attacks originating on the Internet that target the network.

· Documents types of attacks originating on the Internet that target the network

c. Location: On major network backbones

(See above Figure – Location 3)

Advantages:

· Monitors a large amount of a network's traffic, thus increasing the possibility of spotting attacks.

· Detects unauthorized activity by authorized users within the organization's security perimeter.

d. Location: On critical subnets

(See above Figure – Location 4)

Advantages:

· Detects attacks targeting critical systems and resources.

· Allows focusing of limited resources to the network assets considered of greatest value.

Common types of network intrusion detection systems

There are five common types of NIDS that can be used to monitor traffic on your network. Each has its own benefits and drawbacks depending on your business needs:

- **Signature-based system**

This type of NIDS uses signatures from previously analyzed attacks. It learns which patterns indicate malicious activity so future events with similar characteristics will be detected immediately. Signature-based systems do not need any knowledge about the normal behavior of users or applications to operate.

- **Stateful protocol analysis system**

This type of NIDS is similar to a signature-based system in that it learns which patterns indicate malicious activity. Stateful protocol analysis systems differ because

they do not need to know what specific attacks look like before they are detected. Instead, it can maintain temporary information about how your network normally operates and will compare new events against the normal traffic rate of existing connections.

- **Behavioral-based system**

This type of NIDS uses behavioral analysis to determine whether any suspicious activity has occurred. If the behavior being analyzed meets certain conditions set by the administrator, an alert will be triggered so appropriate action can be taken in response to malicious activity.

- **Anomaly-based system**

This type of NIDS is similar to the behavior-based system, except that it learns what typical network behavior looks like by analyzing how real connections are established and used over time. The administrator may also need to provide information about which events should trigger alerts if anomalies are detected. This type of system is configured to learn what the normal traffic on your network looks like, which can reduce false-positive rates, however, changes in user computer activity or changes made by new software installations could also trigger false alarms.

- **Heuristic-based system**

This type of NIDS uses heuristics to look beyond attacks with known signatures and analyze them against a set of rules to determine whether any suspicious activity has occurred. The heuristic-based system is capable of detecting advanced attacks without previously knowing what those attacks look like by looking for a combination of characteristics that indicate a possible security issue.

Advantages and disadvantages of network intrusion detection system

There are several benefits and drawbacks associated with deploying a Network Intrusion Detection System on your organization's network. Some advantages include:

Detects known and unknown malware. A NIDS can be configured to detect common types of malware, as well as new or unknown threats, so you will quickly know when hackers have compromised your systems.

Reduces downtime. Once an intrusion is detected, NIDS immediately shuts down the process and alerts you so you can react quickly to stop further damage.

Prevents attacks. The NIDS constantly monitors network traffic to identify

suspicious activity and block it before hackers are able to gain access to your system.

Detects compromised devices. A NIDS can detect when a user's computer has been compromised so, the attacker cannot gain access to other machines on the network or use the compromised machine as an attack vector into other parts of your business's information technology infrastructure.

Disadvantages associated with deploying the Network Intrusion Detection System include:

- **Requires frequent updating**. It is important to update your NIDS regularly so it will continue to recognize known threats and keep up with new ones. There are several ways to perform this update; updates are essential to the success of your NIDS.
- **Requires extensive configuration**. To be most effective, a NIDS must be configured with information about how your network normally operates and what types of activities should trigger an alert. This can require some effort on your part but will ensure that you receive alerts for suspicious behavior or malware only after it has been detected.
- **Requires maintenance**. Many systems require manual updating and configuration and therefore need constant management by IT staff to be most effective. If you do not have dedicated IT resources available to maintain the system, it may need to be removed from your network until these resources become available.

Network intrusion detection system vs. network intrusion prevention system (NIPS)

A NIDS is a passive system that compares the current network traffic against known malware signatures. In contrast, a NIPS actively analyzes the network traffic in real-time and blocks any suspicious activities. It can be configured to prevent an intruder from gaining access to your private information even if it doesn't have a complete understanding of all possible security threats.

Network intrusion detection system vs. firewall

A firewall is a network security system that controls the incoming and outgoing network traffic by monitoring which computer or IP address is allowed to access other computers on your network. A NIDS analyzes the data packets that are transmitted over your business's network to identify possible cyber-attacks or

malicious activities.

While both systems monitor your private information networks looking for suspicious activity, they do it in different ways. A NIDS performs continuous analysis of all traffic passing through your business's network looking for known malware signatures, whereas a firewall denies access to specific users and/or IP addresses trying to access your network.

Network intrusion detection system vs. host-based intrusion prevention systems

A host-based intrusion prevention system monitors and blocks suspicious activity that is taking place on a single computer, whereas a NIDS looks for unusual or suspicious activity across all your business's computers, servers, and other devices in real-time to identify potential attacks against the entire network. In addition, a NIDS can be configured to automatically react to an attack by shutting down processes, blocking access from compromised machines, and alerting IT staff to the possible presence of malware.

Network intrusion detection system vs. virus protection

Virus protection software identifies and eliminates computer viruses after they have been downloaded onto your system, whereas NIDS monitor and analyze data packets as they pass through the network to identify suspicious activities that may indicate a security breach.

Network intrusion detection system vs. anti-virus software

Both anti-virus software and NIDS work together to automatically scan all incoming and outgoing data and compare it against known malware signatures. At first glance, you might think that these two products do the same thing, but there are subtle differences between them:

Anti-virus software is designed to protect single host computers from attack by locating specific types of malware on those computers; it scans binaries for known malware signatures and flags them as either safe or infected with malware. A NIDS analyzes all the data packets passing through your business's network to identify signs of an attack; it monitors the network traffic looking for patterns that may indicate suspicious activities such as port scanning or brute force attacks against common services like FTP or Telnet using default usernames and passwords.

A major difference between anti-virus software and NIDS is how they work in

practice. Anti-virus software relies on you to update it regularly so it can detect new viruses, whereas most NIDS products are updated automatically overnight without requiring intervention from the user.

Network intrusion detection system vs. anomaly-based intrusion detection system (ABIDS)

An anomaly-based intrusion detection system (ABIDS) works in much the same way that a NIDS does, but it uses statistical analysis to identify unusual activity instead of using signatures to flag suspicious traffic. This form of IDS is most effective against zero-day attacks because it looks for data patterns rather than known malware signatures. ABIDS analyzes all activity taking place on your network and identifies anomalous behavior, whereas NIDS analyzes only network traffic looking for signs of known malicious activities.

ABIDS must process all network data before any activity is flagged as anomalous or suspicious, whereas NIDS only processes the packets that are potentially malicious. Since this form of IDS is more proactive in its monitoring of your network traffic, it can sometimes be more of a drain on your business's resources than a NIDS.

Network intrusion detection system vs. anomaly-based intrusion prevention system

This form of IDS works in the same way that ABIDS do, but instead of generating alerts they automatically react to anomalies by blocking suspicious activities and shutting down compromised processes on your computers much like a host-based intrusion prevention system would. Since it does not rely on signatures to identify malware it is typically more effective at preventing zero-day attacks because it can react to any suspicious activities detected on your network.

The disadvantage of this form of IDS is that if a false positive occurs, legitimate traffic could be blocked, or processes shut down unnecessarily. This means that its accuracy should be carefully monitored and configured by an experienced security specialist so as not to result in too many false positives which would impact the performance of your business's computer systems.

3. PROTOCOL BASED IDS

A **Protocol-Based Intrusion Detection System (PIDS)** is a type of IDS that monitors and analyzes the **application-layer protocol traffic** to ensure it follows predefined standards and behavior. Unlike a traditional network IDS that checks all

network packets, a PIDS focuses on specific protocols like HTTP, FTP, SMTP, or DNS and verifies whether the communication aligns with the protocol specifications. PIDS operates by decoding protocol commands and inspecting them deeply to detect attacks that may be embedded within legitimate-looking requests. It acts as a filter or gatekeeper that sits **between the external client and the application server**, analyzing protocol-specific interactions in real time. If an anomaly or known attack pattern is found, it can either log the event, alert administrators, or block the malicious request.

HTTP Protocol-Based IDS

Let's consider a **web server** running an e-commerce website. A user interacts with this website using the **HTTP protocol** (via browsers or mobile apps). The attacker might try to inject a **malicious SQL query** in a form field to extract sensitive information from the backend database.

Example Attack Attempt:

http

CopyEdit

GET /search.php?query=shoes'+OR+1=1-- HTTP/1.1

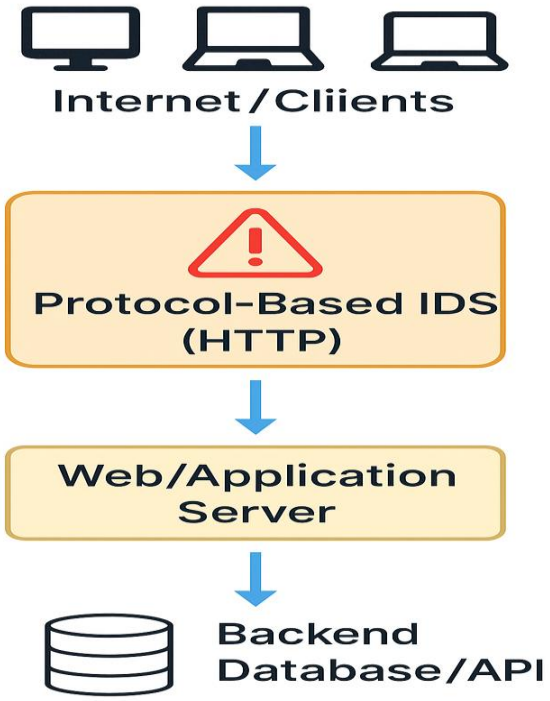
Host: example.com

This request contains a **SQL Injection attempt**: shoes' OR 1=1-- is an SQL condition that always evaluates to true and could potentially expose the entire product database or user information.

How PIDS Detects This:

- A **Protocol-Based IDS for HTTP** inspects the query string.
- It **parses the HTTP GET request**, identifies abnormal use of characters (like ', --, or OR 1=1), and flags it as **malicious behavior** based on:
    - Known signature patterns
    - Deviation from normal query behavior
- An alert is triggered, and the request is blocked **before it reaches the web server**.

This proactive detection helps prevent database leaks, unauthorized access, and application crashes caused by malformed protocol commands.



Architecture of Protocol based IDS

Components in the Architecture:

- Clients/Users: Initiate communication using application protocols.
- PIDS: Acts as a protocol-aware security layer, inspecting requests/responses.
- Web/Application Server: Executes requests if verified safe by PIDS.
- Backend Systems: Handle final data processing or business logic.

Key Functions of PIDS

- **Protocol Parsing:** Understands and analyzes the structure of HTTP, FTP, DNS, etc.
- **Signature Matching:** Compares request patterns against known attack signatures.
- **Anomaly Detection:** Flags deviations from normal usage, even if unknown attacks.
- **Real-Time Protection:** Acts before the request reaches the application.
- **Logging & Alerting:** Records suspicious activity for review and response.

4. HYBRID IDS

A Hybrid Intrusion Detection System (Hybrid IDS) combines two or more different types of intrusion detection approaches—primarily signature-based and anomaly-based detection systems, and may also integrate host-based and network-based detection components. This integration leverages the strengths of each type to create a more comprehensive and accurate detection system, mitigating the weaknesses of individual systems.

IDS Type	Strengths	Weaknesses
Signature-based	Accurate for known attacks	Can't detect new/unknown threats
Anomaly-based	Can detect unknown attacks	High false positive rate
Host-based IDS (HIDS)	Monitors system-level activities	Limited to specific host
Network-based IDS (NIDS)	Monitors entire network	May miss host-specific anomalies

A **Hybrid IDS** combines these to:

- Improve detection accuracy
- Reduce false positives
- Provide both breadth (network) and depth (host-level) monitoring

A generic architecture of a Hybrid IDS contains the following components:

◇ **Data Collection Module**

- Captures logs and traffic data from hosts and network.
- Examples: System calls, packet captures, logs

◇ **Preprocessing Module**

- Filters and normalizes data
- Extracts relevant features

◇ **Detection Engine**

- Uses **Signature Matching** (for known attacks)
- Uses **Anomaly Detection** (for unknown attacks)
- Often integrates **machine learning models** or **statistical methods**

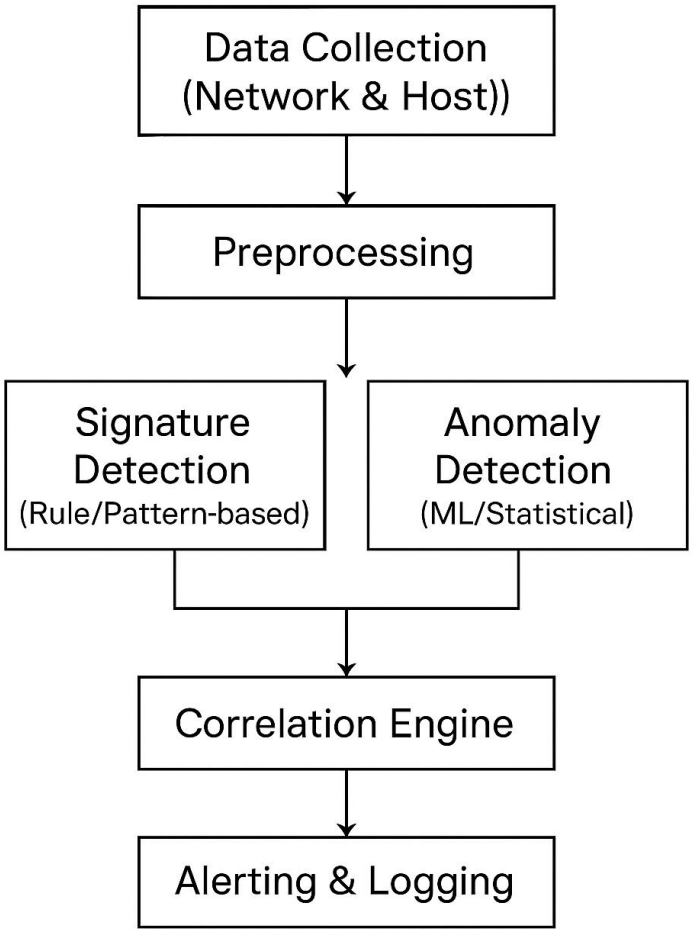
◇ **Correlation Engine**

- Combines outputs from HIDS and NIDS
- Correlates alerts across multiple sources

◇ **Alerting and Reporting**

- Generates alerts for administrators
- Provides dashboards, logs, or real-time notifications

Hybrid IDS Architecture



Hybrid IDS Architecture

Imagine a **hybrid IDS** deployed in a bank:

- **Signature-based engine** detects a known SQL Injection attack.
- **Anomaly-based engine** detects an unusual login time and large data exfiltration from a user account (a possible insider threat).
- **Correlation engine** links both events and flags it as a **high-severity incident**.

This synergy between components helps detect **complex attacks** that may otherwise go unnoticed.

Advantages of Hybrid IDS

- Detects **both known and unknown** threats
- Reduces **false positives** by validating anomalies with signatures
- Combines **host and network level** insights
- Supports **adaptive learning** using machine learning algorithms

5. ANALYSIS SCHEMES

Analysis, in the context of intrusion detection and prevention, is the organization of the constituent parts of data and their interrelationships to identify any anomalous activity of interest. *Real-time analysis* is analysis done on the fly as the data travels the path to the network or host. This is a bit of a misnomer, however, as analysis can only be performed after the fact in near-real-time.

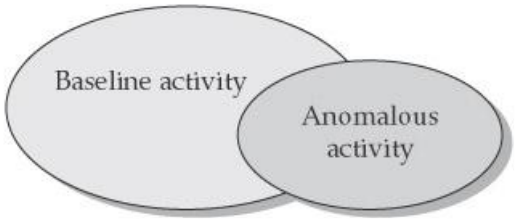
The fundamental goal of intrusion-detection and intrusion-prevention analysis is to improve an information

system's security. This goal can be further broken down:

- Create records of relevant activity for follow-up
- Determine flaws in the network by detecting specific activities
- Record unauthorized activity for use in forensics or criminal prosecution of intrusion attacks
- Act as a deterrent to malicious activity
- Increase accountability by linking activities of one individual across systems

Figure below illustrates the general idea of analysis. An IDS or IPS system will help identify-those anomalous activities that fall outside the realm of what is considered normal baseline activity for the environment. This is considered the general goal, but there is still much debate over how much anomalous data falls outside the realm of normal baseline activity. Some believe the gap is

large, while others see very little difference between the two.



The relationship between baseline and anomalous network activity

The Anatomy of Intrusion Analysis

There are many possible data-analysis schemes for an analysis engine, and in order to understand them, the

intrusion-analysis process can be broken down into four phases:

1. Preprocessing
2. Analysis
3. Response
4. Refinement

Preprocessing is a key function once data are collected from an IDS or IPS sensor. In this step, the data are organized in some fashion for classification. The preprocessing will help determine the format the data are put into, which is usually some canonical format or could be a structured database. Once the data are formatted, they are broken down further into classifications. These classifications can depend on the analysis schemes being used. For example, if rule-based detection is being used, the classification will involve rules and pattern descriptors. If anomaly detection is used, you will usually have a statistical profile based on different algorithms in which the user behavior is baselined over time and any behavior that falls outside of that classification is flagged as an anomaly. Upon completion of the classification process, the data is concatenated and put into a defined version or detection template of some object by replacing variables with values. These detection templates populate the knowledgebase which are stored in the core analysis engine:

- Detection of the modification of system log files
- Detection of unexpected privilege escalation
- Detection of Backdoor Netbus
- Detection of Backdoor SubSeven

· ORACLE grant attempt

· RPC mountd UDP export request

Once the prepossessing is completed, the *analysis* stage begins. The data record is compared to the knowledge base, and the data record will either be logged as an intrusion event or it will be dropped. Then the next data record is analyzed. The next phase, *response*, is one of the differentiating factors between IDS and IPS. With IDS, you typically have limited prevention abilities—you are getting the information passively after the fact, so you will have an alert after the fact. Once information has been logged as an intrusion, a response can be initiated. With IPS, the sensor is inline and it can provide real-time prevention through an automated response. This is the essential difference between reactive security and proactive security. Either way, the response is specific to the nature of the intrusion or the different analysis schemes used. The response can be set to be automatically performed, or it can be done manually after someone has manually analyzed the situation. For example, Network Flight Recorder (a commercial IDS) offers a feature that can send aTCPRST packet and kill a session. The final phase is the *refinement* stage. This is where the fine-tuning of the IDS or IPS system can be done, based on previous usage and detected intrusions. This gives the security professional a chance to reduce false-positive levels and to have a more accurate security tool. This is a very critical stage for getting the most from your IDS or IPS system. The system must be fine-tuned for your environment to get any real value from it. There are tools, like Cisco Threat Response (CTR), that will help with the refining stage by actually making sure that an alert is valid by checking whether you are vulnerable to that attack or not.

Analysis Process By Different Detection Methods

The intrusion analysis process is solely depends on the detection method being used. Following is the information regarding the four phases of intrusion analysis by different detection methods:

Analysis Process By Rule-Based Detection

Rule-based detection, also known as *signature detection, pattern matching and misuse detection*. Rule-based detection uses pattern matching to detect known attack patterns. The four phases of intrusion analysis process applied in rule-

based detection system are as under:

- Preprocessing: The data is collected about the intrusions, vulnerabilities and attacks and then it is putted down into classification scheme or pattern descriptors. From the classification scheme a behavior model is built and then into a common format;
- Signature Name: The given name of the signature
- Signature ID: The unique ID for the signature
- Signature Description: The description of the signature & what it does
- Possible False Positive Description: An explanation of any "false positives" that may appear to be an exploit but are actually normal network activity.
- Related Vulnerability Information: This field has any related vulnerability information

The pattern descriptors are typically either content-based signatures, which examine the payload and header of packet, or context-based signatures that evaluate only the packet headers to identify an alert. The pattern descriptors can be atomic (single) or composite (multiple) descriptors. Atomic descriptor requires only one packet to be inspected to identify an alert, while composite descriptor requires multiple packets to be inspected to identify an alert. The pattern descriptors are then put into a knowledge base that contains the criteria for analysis.

- Analysis: The event data are formatted and compared against the knowledge base by using pattern-matching analysis engine. The analysis engine looks for defined patterns that are known as attacks.
- Response: If the event matches the pattern of an attack, the analysis engine sends an alert. If the event is partial match, the next event is examined. Partial matches can only be analyzed with a stateful detector, which has the ability to maintain state, as many IDS systems do. Different responses can be returned depending on the specific event records.
- Refinement: Refinement of pattern-matching analysis comes down to updating signatures, because an IDS is only as good as its signature update.

Analysis Process By Profile-Based Detection (Anomaly Detection)

An anomaly is something that is different from the norm or that cannot be easily

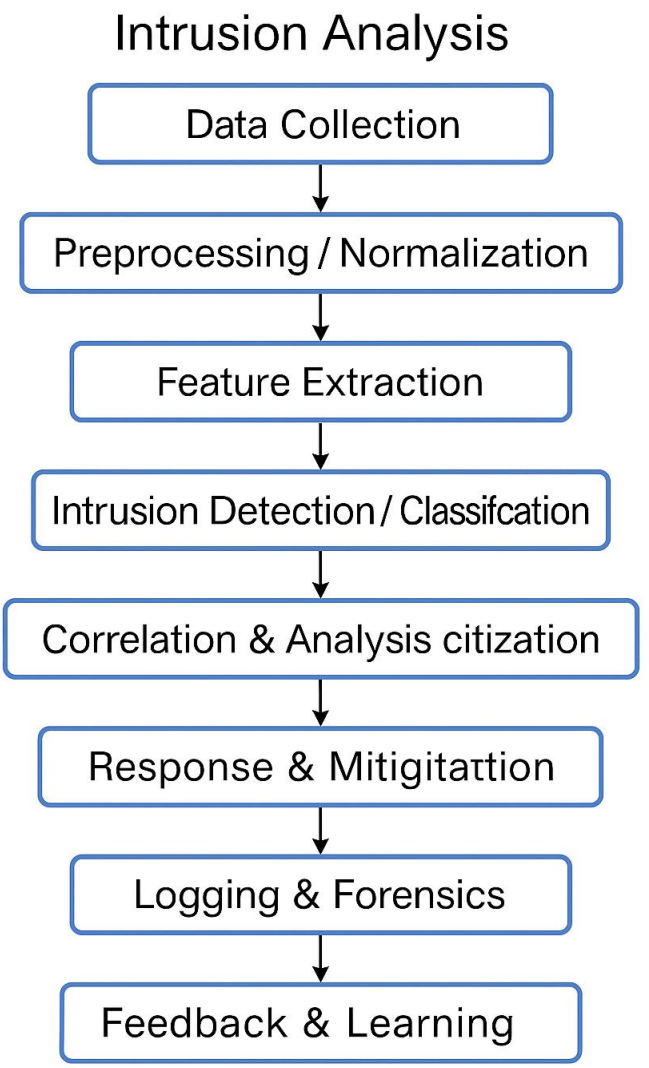
classified. Anomaly detection, also referred to as Profile-based detection, creates a profile system that flags any events that strays from a normal pattern and passes this information on to output routines.

One key distinction between anomaly detection and other analysis schemes is that anomaly-based schemes not only define activities that are *not allowed*, but also activities that are *allowed*. In addition, anomaly detection is typically used for its ability to collect statistical behavior and characteristic behavior. Statistics are quantitative and characteristics are more qualitative. For example, "This server's UDP traffic never exceeds 25 percent of capacity" describes a statistical behavior, and "User Stan321 does not normally FTP files outside of the company" describes a characteristic behavior. Anomaly-based schemes fall into three main categories: behavioral, traffic pattern, and protocol. *Behavioral analysis* looks for anomalies in the types of behavior that have been statistically baselined, such as relationships in packets and what is being sent over a network. *Traffic-pattern analysis* looks for specific patterns in network traffic. *Protocol analysis* looks for network protocol violations or misuse based on RFC-based behavior. Protocol analysis has the benefit of identifying possible attacks that are not yet publicized or that there is no known signature or remedy for. The analysis process by profile-based detection is as following:

Preprocessing: The first step in the analysis process is collecting the data in which behavior considered normal on the network is baseline over a period of time. The data are put into a numeric form and then formatted. Then the information is classified into a statistical profile that is based on different algorithms is the knowledge base.

- Analysis: The event data are typically reduced to a profile vector, which is then compared to the knowledge base. The contents of the profile vector are compared to a historical record for that particular user, and any data that fall outside of the baseline of normal activity is labeled as deviation.
- Response: At this point, a response can be triggered either automatically or manually.
- Refinement: The profile vector history is typically deleted after a specific time. In addition, different weighting systems can be used to add more weight to recent behavior than past behaviors.

6. A MODEL FOR INTRUSION ANALYSIS



1. Data Collection

The intrusion analysis process begins with data collection from various sources within the IT environment. These sources may include network traffic, system logs, application logs, user activity records, or protocol-specific communication. The aim is to gather comprehensive information that may contain evidence of malicious behavior. Tools like packet sniffers, system monitors, and log aggregators are commonly used in this phase.

2. Preprocessing / Normalization

After collecting raw data, preprocessing is performed to clean, standardize, and transform the data into a uniform format. This may include tasks such as removing

duplicates, handling missing values, converting timestamps, and filtering irrelevant fields. Normalization ensures consistency, which is essential for accurate analysis and feature extraction in the later stages.

3. Feature Extraction

This stage involves identifying and extracting important characteristics or patterns from the data that can indicate intrusion. These features might include source/destination IP addresses, protocol types, request rates, command sequences, or authentication failures. The quality of features greatly influences the effectiveness of intrusion detection algorithms.

4. Intrusion Detection / Classification

Once the data has been transformed into a feature-rich format, it is analyzed to detect intrusions. Detection can be:

Signature-Based: Matches data against known attack patterns.

Anomaly-Based: Flags behaviors that deviate from normal usage.

Machine Learning-Based: Uses classification algorithms (e.g., Decision Tree, Random Forest, SVM) to predict intrusions based on historical data.

The goal here is to label each event or activity as either normal or malicious.

5. Correlation & Analysis

In complex environments, attacks may occur in multiple stages. This phase correlates various related events over time to identify coordinated or multi-step attacks. It enhances the detection of sophisticated intrusion patterns that cannot be identified by analyzing isolated events alone. Threat intelligence feeds may also be used for enrichment.

6. Response & Mitigation

Once an intrusion is detected and analyzed, the IDS triggers a response. The response can be:

Passive (alert only): Notify administrators through logs, email, or dashboards.

Active (automatic action): Block IP, disconnect sessions, or isolate infected devices.

These responses are often mapped to predefined security policies, ensuring that each type of threat is handled according to the organization's acceptable risk level.

7. Logging & Forensics

All detected intrusions, response actions, and analysis results are logged for future reference. This data is crucial for forensic investigations, legal evidence, compliance

audits, and incident reviews. It also helps in identifying patterns in recurring attacks.

8. Feedback & Learning

In the final phase, the IDS uses past experience to improve its future detection capability. False positives and false negatives are reviewed, and detection models or rule sets are updated accordingly. In machine learning-based systems, feedback is used to retrain models and refine thresholds, making the IDS adaptive to evolving threats.

7. RESPONSE OPTIONS FOR IDSS

Once IDSs have obtained event information and analyzed it to find symptoms of attacks, they generate responses. Some of these responses involve reporting results and findings to a pre-specified location. Others involve more active automated responses. Though researchers are tempted to underrate the importance of good response functions in IDSs, they are actually very important. Commercial IDSs support a wide range of response options, often categorized as active responses, passive responses, or some mixture of the two.

Active Responses

Active IDS responses are automated actions taken when certain types of intrusions are detected. There are three categories of active responses.

Collect additional information

The most innocuous, but at times most productive, active response is to collect additional information about a suspected attack. Each of us have probably done the equivalent of this when awakened by a strange noise at night. The first thing one does in such a situation is to listen more closely, searching for additional information that allows you to decide whether you should take action. In the IDS case, this might involve increasing the level of sensitivity of information sources (for instance, turning up the number of events logged by an operating system audit trail, or increasing the sensitivity of a network monitor to capture all packets, not just those targeting a particular port or target system.) Collecting additional information is helpful for several reasons. The additional information collected can help resolve the detection of the attack (assisting the system in diagnosing whether an attack did or did not take place). This option also allows the

organization to gather information that can be used to support investigation and apprehension of the attacker, and to support criminal and civil legal remedies.

Change the Environment

Another active response is to halt an attack in progress and then block subsequent access by the attacker. Typically, IDSs do not have the ability to block a specific person's access, but instead block Internet Protocol (IP) addresses from which the attacker appears to be coming. It is very difficult to block a determined and knowledgeable attacker, but IDSs can often deter expert attackers or stop novice attackers by taking the following actions:

· Injecting TCP reset packets into the attacker's connection to the victim system, thereby terminating the connection

· Reconfiguring routers and firewalls to block packets from the attacker's apparent location (IP address or site),

· Reconfiguring routers and firewalls to block the network ports, protocols, or services being used by an attacker, and

· In extreme situations, reconfiguring routers and firewalls to sever all connections that use certain network interfaces.

Take Action Against the Intruder

Some who follow intrusion detection discussions, especially in information warfare circles, believe that the first option in active response is to take action against the intruder. The most aggressive form of this response involves launching attacks against or attempting to actively gain information about the attacker's host or site. However tempting it might be, this response is ill advised. Due to legal ambiguities about civil liability, this option can represent a greater risk than the attack it is intended to block. The first reason for approaching this option with a great deal of caution is that it may be illegal. Furthermore, as many attackers use false network addresses when attacking systems, it carries with it a high risk of causing damage to innocent Internet sites and users. Finally, strike back can escalate the attack, provoking an attacker who originally intended only to browse a site to take more aggressive action. Should an active intervention and traceback of this sort be warranted (as in the case of a critical system) human control and supervision of

the process is advisable. We strongly recommend that you obtain legal advice before pursuing any of these "strike-back" options.

Passive Responses

Passive IDS responses provide information to system users, relying on humans to take subsequent action based on that information. Many commercial IDSs rely solely on passive responses.

Alarms and Notifications

Alarms and notifications are generated by IDSs to inform users when attacks are detected. Most commercial IDSs allow users a great deal of latitude in determining how and when alarms are generated and to whom they are displayed. The most common form of alarm is an onscreen alert or popup window. This is displayed on the IDS console or on other systems as specified by the user during the configuration of the IDS. The information provided in the alarm message varies widely, ranging from a notification that an intrusion has taken place to extremely detailed messages outlining the IP addresses of the source and target of the attack, the specific attack tool used to gain access, and the outcome of the attack. Another set of options that are of utility to large or distributed organizations are those involving remote notification of alarms or alerts. These allow organizations to configure the IDS so that it sends alerts to cellular phones and pagers carried by incident response teams or system security personnel. Some products also offer email as another notification channel. This is ill advised, as attackers often routinely monitor email and might even block the message.

SNMP Traps and Plug-ins

Some commercial IDSs are designed to generate alarms and alerts, reporting them to a network management system. These use SNMP traps and messages to post alarms and alerts to central network management consoles, where they can be serviced by network operations personnel. Several benefits are associated with this reporting scheme, including the ability to adapt the entire network infrastructure to respond to a detected attack, the ability to shift the processing load associated with an active response to a system other than the one being targeted by the attack, and the ability to use common communications channels.

Reporting and Archiving Capabilities

Many, if not all, commercial IDSs provide capabilities to generate routine reports

and other detailed information documents. Some of these can output reports of system events and intrusions detected over a particular reporting period (for example, a week or a month.) Some provide statistics or logs generated by the IDS in formats suitable for inclusion in database systems or for use in report generating packages (An example of such a commonly-supported package is Crystal Reports.)

Failsafe considerations for IDS responses

When identifying candidate IDSs for your organization, it is important to consider the failsafe features included by the IDS vendor. Failsafe features are those design features meant to protect the IDS from being circumvented or defeated by an attacker. These represent a necessary difference between standard system management tools and security management tools. There are several areas in the response function that require failsafe measures. For instance, IDSs need to provide silent, reliable monitoring of attackers. Should the response function of an IDS break this silence by broadcasting alarms and alerts in plaintext over the monitored network, it would allow attackers to detect the presence of the IDS. Worse yet, the attackers can directly target the IDS as part of the attack on the victim system. Encrypted tunnels or other cryptographic measures used to hide and authenticate IDS communications are excellent ways to secure and ensure the reliability of the IDS.

Granular Types of IDS Responses

Type of Response	Nature	Description
Alert	Passive	Sends notification to administrator
Log Event	Passive	Stores the data in logs for later investigation
Connection Termination	Active	Cuts the TCP/UDP connection with the attacker
IP Address Blocking	Active	Prevents further access from attacker's IP
Session	Active	Disconnects only the session

Type of Response	Nature	Description
Isolation		involved in intrusion
Rate Limiting	Active	Reduces bandwidth for malicious traffic source
Quarantine	Active	Moves the infected host to a separate VLAN or subnet
Honeypot Redirection	Active	Redirects intruder to a trap system

Mapping IDS Responses to Policy

Mapping responses to security policies ensures that the IDS actions are aligned with organizational risk posture and compliance standards.

A. What is a Security Policy?

- A formal set of rules that governs how systems respond to threats.
- Defines acceptable use, incident handling, escalation procedures, and compliance mandates.

Policy Mapping Example

Policy Rule	TriggerCondition	IDSRespone
Deny access to unauthorized IP ranges	Access attempt from blacklisted IP	IP Block, Alert
Monitor all failed login attempts > 3	>3 failed SSH logins in 2 mins	Alert + Log Event
Stop data exfiltration attempts	Large data upload from user to unknown host	Connection Termination
Isolate infected systems	Malware signature detected	Host Quarantine
Inform admin about all suspicious	Any anomaly detection	Alert (Email, Dashboard)

Policy Rule	TriggerCondition	IDSRespone
activities		

Benefits of Mapping

- Enables **automated and consistent** responses.
- Supports **compliance** with standards (ISO 27001, NIST, GDPR).
- Reduces human error and ensures **timely mitigation**.
- Enhances **incident response planning**.

IDS response strategies must be tailored to the organization's security policy to maintain a balance between system availability, performance, and protection. Proper mapping ensures that each detected threat is met with a predefined, effective, and policy-compliant response.

8. VULNERABILITY ANALYSIS OR ASSESSMENT SYSTEMS

Vulnerability analysis (also known as vulnerability assessment) tools test to determine whether a network or host is vulnerable to known attacks. Vulnerability assessment represents a special case of the intrusion detection process. The information sources used are system state attributes and outcomes of attempted attacks. The information sources are collected by a part of the assessment engine. The timing of analysis is interval-based or batch-mode, and the type of analysis is misuse detection. This means that vulnerability assessment systems are essentially batch mode misuse detectors that operate on system state information and results of specified test routines.

Vulnerability analysis is a very powerful security management technique, but is suitable as a complement to using an IDS, not as a replacement. Should an organization rely solely on vulnerability analysis tools to monitor systems, a knowledgeable attacker may monitor the vulnerability analysis system, note when the information source is collected, and time the attack to fit between collection times.

However, vulnerability analysis systems can reliably generate a "snapshot" of the security state of a system at a particular time. Furthermore, as they exhaustively test systems for vulnerability to large numbers of known attacks, vulnerability

analysis systems can allow a security manager to check for problems due to human error or to audit the system for compliance with a particular system security policy.

Vulnerability Analysis System Process

The general process for vulnerability assessment is as follows:

· A specified set of system attributes is sampled

· The results of the sampling are stored in a secure data repository

· The results are organized and compared to at least one reference set of data (this set can be a manually specified "ideal configuration" template or a snapshot of the system state generated earlier)

· Any differences between the two sets are identified and reported. Commercial vulnerability assessment products often optimize this process by:

· splitting processing loads, running multiple assessment engines in parallel.

· using cryptographic mechanisms to do very sensitive and reliable tests of whether particular files or objects have changed unexpectedly.

Vulnerability Analysis Types

There are two major ways of classifying vulnerability analysis systems, first, by the location from which assessment information is gathered, and second, by the assumptions regarding the level of trust invested in the assessment tool. Those who use the first classification scheme for vulnerability assessment classify systems as either *network-based* or *host-based.* Those who use the second classification scheme, classify systems as *credentialed* or *non-credentialed*. These terms refer to whether the analysis is done with or without system credentials (such as passwords or other identification and authentication that grant access to the system internals.)

Host-based Vulnerability Analysis

Host-based vulnerability analysis systems determine vulnerability by assessing system data sources such as file contents, configuration settings, and other status information. This information is usually accessible using standard system queries and inspection of system attributes. As the information is gathered under the assumption that the vulnerability analyzer is granted access to the host, it is also sometimes known as *credential-based* vulnerability assessment. This class of assessment is also labeled *passive* assessment. The vulnerabilities best revealed by host-based vulnerability assessment are those involving privilege escalation attacks. (Such attacks might seek *superuser* or *root* privilege on a UNIX system, or

administrator access on an NT system.)

Network-Based Vulnerability Analysis

Network-based vulnerability analysis systems have gained acceptance in recent years. These vulnerability analysis systems require a remote connection to the target system. They may actually reenact system attacks, noting and recording responses to these attacks or simply probe different targets to infer weaknesses from their responses. This reenactment of attacks or probing can occur regardless of whether one has permission to access the target system; hence this is considered *noncredentialled* assessment. Furthermore, as network-based vulnerability analysis is defined as actively attacking or scanning the targeted system, it is also sometimes labeled *active* vulnerability assessment. Network-based vulnerability analysis tools are sometimes marketed as intrusion detection tools. Although, as discussed earlier in this document, this is correct by some definitions of intrusion detection, a vulnerability analysis product is not a complete intrusion detection solution for most environments. There are two methods typically used in network-based vulnerability assessment:

· *Testing by exploit* – in this method, the system reenacts an actual attack. A status flag is returned indicating whether the attack was successful.

· *Inference Methods* – in this method, the system doesn't actually exploit vulnerabilities, but looks for the artifacts that successful attacks would leave behind. Examples of inference techniques involve checking version numbers provided by systems as results of queries, checking ports to determine which are open, and checking protocol compliance by making simple requests for status or information.

Advantages and Disadvantages of Vulnerability Analysis

Advantages

· Vulnerability Analysis is of significant value as a part of a security monitoring system, allowing the detection of problems on systems that cannot support an IDS.

· Vulnerability Analysis Systems provide security-specific testing capabilities for documenting the security state of systems at the start of a security program and for reestablishing the security baseline whenever major changes occur.

· When Vulnerability Analysis Systems are used on a regular schedule, they can

reliably spot changes in the security state of a system, alerting security managers to problems that require correction.

· Vulnerability Analysis Systems offer a way for security managers and system administrators to double-check any changes they make to systems, assuring that in mitigating one set of security problems, they do not create another set of problems.

Disadvantages and Issues

· Host-based vulnerability analyzers are tightly bound to specific operating systems and applications; they are therefore often more costly to build, maintain, and manage.

· Network-based vulnerability analyzers are platform-independent, but less accurate and subject to more false alarms.

· Some network-based checks, especially those for denial-ofservice attacks, can crash the systems they're testing.

· When conducting vulnerability assessment of networks on which intrusion detection systems are running, the IDSs can block subsequent assessments. Worse yet, repeated network-based assessments can "train" certain anomaly-detection based IDSs to ignore real attacks.

· Organizations that use vulnerability assessment systems must take care to assure that their testing is limited to systems within their political or management control boundaries. Privacy issues must be taken into account, especially when employee or customer personal data is included in information sources.

9. CREDENTIAL AND NON CREDENTIAL VULNERABILITY ANALYSIS

Credential vulnerability analysis is performed **using valid user credentials** (such as admin or standard user logins) to **log into systems and perform in-depth internal scans.** This allows the scanner to access configuration settings, registry values, installed patches, and file systems, which are not visible from the outside.

🔍 Key Characteristics:

- Requires authorized access to systems.
- Provides **deep insights** into system vulnerabilities.
- Can identify issues like:
  - Missing patches
  - Weak password policies

- Misconfigured access rights
- Outdated software versions

- More accurate, with fewer false positives.

🔧 **Tools That Support It:**

- **Nessus** (with credentials)
- **Qualys** authenticated scans
- **OpenVAS** with login integration

🔐 **Example:**

Scanning a Linux server using SSH credentials to identify:

- That the root login is allowed (a security risk)
- That outdated packages like openssl are present
- That firewall rules are misconfigured

2. Non-Credential Vulnerability Analysis

Non-credential vulnerability analysis (or unauthenticated scanning) is performed **without logging into the system**. It simulates the perspective of an external attacker attempting to find weaknesses through open ports, banner grabbing, and fingerprinting.

🔍 **Key Characteristics:**

- No login or access to internal system settings.
- Relies on network scans and open service responses.
- Can detect:
  - Open ports
  - Default credentials (based on banners)
  - Publicly known vulnerabilities (based on version info)
- Produces **more false positives**, but useful for external threat analysis.

🛠️ **Tools That Support It:**

- **Nmap**
- **Nikto**
- **Nessus** unauthenticated scans
- **Shodan** (Internet-facing vulnerability data)

🔧 **Example:**

Scanning a web server externally without login access:

- Detects that HTTP port 80 is open

- Identifies that it's running Apache 2.2.3 (which has known vulnerabilities)
- Flags possible directory listing or outdated SSL protocols

Comparison Table

Feature	Credential Vulnerability Analysis	Non-Credential Vulnerability Analysis
Access Required	Yes – valid system credentials	No – works from outside without login
Depth of Analysis	Deep (internal configs, registry, files, patches)	Surface-level (network, open ports, services)
Accuracy	High – fewer false positives	Lower – may produce false alarms
Perspective	Internal (trusted user or admin)	External (attacker's point of view)
Detects	Misconfigurations, missing patches, policy flaws	Exposed ports, known vulnerabilities weak services
Use Case	Internal audits, compliance	Perimeter defense, external exposur assessment

Lab Exercises

1. Write and implement custom Snort rules to detect specific traffic patterns.

2. Integrate Snort with MySQL to log alerts to a database.

Lecture Slides

Lecture Slides
https://drive.google.com/drive/folders/1MdIU8YLJpG_n3byErvlaSDCn4JTDGb23?usp=drive_link

Assignment

Assignment

1. Write and test three Snort rules to detect: (a) ICMP traffic, (b) HTTP access on a specific port, and (c) traffic from a specific IP address. Show the alerts generated.

2. Use a network scanning tool (like Nmap) to simulate a port scan. Capture and analyze the alerts generated by Snort or any IDS tool. What signature did the IDS use to identify the scan?

3. Simulate a SQL injection attack on a sample vulnerable web application. Observe how a protocol-based IDS (PIDS) or HTTP log analysis detects the attack. Provide screenshots and explanation.

4. Demonstrate and compare the behavior of an IDS with passive response (logging only) and active response (blocking traffic). What are the advantages of each?

5. Perform a credentialed and non-credentialed vulnerability scan on a test system using OpenVAS or similar tools. Compare the results and explain which vulnerabilities were missed in the unauthenticated scan.

Part A Q & A

PART -A

1. What is the primary function of an Intrusion Prevention System (IPS)? *(CO2, K1)*
   Ans: An IPS is a network security solution that proactively monitors, detects, and blocks malicious traffic in real-time.
   It inspects network packets, identifies known threats using signatures or anomaly detection, and stops them before damage occurs.
   Unlike IDS, which only alerts, IPS takes immediate action like dropping packets or terminating sessions.
   It is usually deployed inline between source and destination for active prevention.

2. Differentiate between IDS and IPS. *(CO2, K2)*
   Ans: IDS is a passive system that detects intrusions and generates alerts without taking direct action.
   IPS is an active system that not only detects but also blocks or prevents suspicious activity.
   IDS is mainly used for monitoring, whereas IPS acts as a defense mechanism.
   IPS typically sits inline with the traffic, while IDS may be off to the side.

3. List the four components of a typical IPS architecture. *(CO2, K1)*
   Ans: The four components are: Traffic Normalizer, Service Scanner, Detection Engine, and Traffic Shaper.
   The Traffic Normalizer parses and analyzes packets.
   The Service Scanner identifies services and builds reference data.
   The Detection Engine applies rules, and the Traffic Shaper manages flow based on findings.

4. State two key benefits of using IPS in enterprise security. *(CO2, K2)*
   Ans: IPS enhances security by detecting and blocking threats before they cause harm.
   It reduces the risk of attacks like malware, DoS, and unauthorized access.
   It integrates with firewalls and antivirus systems for a layered defense.
   IPS also lowers security team workload by automating responses.

5. What is Host-Based IPS (HIPS)? *(CO2, K1)*
   Ans: HIPS is installed on individual hosts or endpoints to detect and prevent attacks locally.
   It uses signature and anomaly detection to identify suspicious behavior on the host system.
   It monitors system calls, registry changes, and file access to detect malware or exploits.
   HIPS adds a layer of defense, especially useful when the network perimeter is breached.

6. Mention two malicious behaviors that HIPS can detect. *(CO2, K2)*
   Ans: HIPS can detect buffer overflow attacks where malicious input overflows memory buffers.

It also detects privilege escalation where normal users try to gain admin access. Other behaviors include access to contact lists and directory traversal. HIPS watches internal system activities for early threat detection.

7. Define Network-Based IPS (NIPS). *(CO2, K1)*
Ans: NIPS is a type of IPS deployed at network points to inspect traffic flows and block malicious packets.
It uses both signature-based and anomaly-based techniques.
NIPS reassembles packet flows and applies policies in real-time.
It can terminate TCP sessions or drop suspicious packets.

8. What is flow data protection in NIPS? *(CO2, K2)*
Ans: Flow data protection refers to inspecting complete data flows rather than individual packets.
NIPS reassembles payloads of multiple packets for context-aware detection.
This helps in identifying attacks spread across multiple packets.
Once malicious flow is detected, subsequent packets are dropped.

9. List any two techniques used in NIPS for detection. *(CO2, K1)*
Ans: One is Pattern Matching, which compares packet content with known attack signatures.
Another is Stateful Matching, which considers the state of ongoing sessions.
Protocol Anomaly and Statistical Anomaly are other techniques.
These methods enable accurate real-time threat detection.

10. Mention two components of NIDS. *(CO2, K1)*
Ans: The Sensor captures live traffic from the network using mirroring or taps.
The Analyzer processes and detects anomalies or signatures.
NIDS also has a Management Console for alerts and reports.
Signature/Anomaly Database stores known attack patterns.

11. What is the role of the detection engine in NIDS? *(CO2, K2)*
Ans: The Detection Engine is the core that analyzes incoming packets for threats.
It matches traffic against signature rules or statistical models.
If an anomaly or match is found, it triggers alerts.
It plays a critical role in threat identification and classification.

12. What is the function of the management console in NIDS? *(CO2, K2)*
Ans: The management console provides a user interface to monitor and control the NIDS.
It shows alerts, logs, and detailed packet inspection data.
Admins can use it to update rules and analyze past events.
It is also useful for reporting and compliance documentation.

13. What is a Hybrid IDS? *(CO2, K1)*
Ans: A Hybrid IDS combines multiple detection methods like signature-based and anomaly-based techniques.
It also integrates both host-based and network-based components.
This enhances accuracy by covering a wider range of threats.

It reduces false positives while also detecting unknown attacks.

14. List two advantages of Hybrid IDS. *(CO2, K2)*
Ans: First, it detects both known and unknown attacks by combining multiple detection strategies.
Second, it offers comprehensive coverage by monitoring both hosts and networks.
It also improves reliability through correlation of alerts from multiple sources.
False positives are minimized using rule validation.

15. Where is NIDS usually deployed for monitoring DMZ traffic? *(CO2, K1)*
Ans: NIDS is typically deployed behind the external firewall in the DMZ (Demilitarized Zone).
This allows it to detect any attack that bypasses firewall rules.
It monitors incoming and outgoing traffic to critical servers like web or mail servers.
This placement helps identify both intrusion attempts and data exfiltration.

16. What is the advantage of placing NIDS outside the firewall? *(CO2, K2)*
Ans: When placed outside the firewall, NIDS can track and log all external attacks.
This helps in understanding the nature and frequency of threats targeting the network.
It also helps in firewall performance analysis and tuning.
However, it cannot detect internal traffic or post-breach behavior.

17. What is Signature-Based Detection? *(CO2, K1)*
Ans: Signature-based detection involves comparing network traffic to predefined attack patterns.
It is effective for identifying known threats based on historical data.
The system uses a database of signatures and alerts if a match is found.
However, it cannot detect new or unknown threats.

18. What is Anomaly-Based Detection? *(CO2, K1)*
Ans: Anomaly-based detection establishes a baseline of normal network behavior.
Any deviation from this baseline is flagged as suspicious.
It is useful for detecting zero-day or previously unknown attacks.
But it may generate more false positives than signature-based systems.

19. Differentiate between Atomic and Composite pattern descriptors. *(CO2, K2)*
Ans: Atomic descriptors detect attacks based on a single packet.
Composite descriptors require analyzing multiple packets to identify complex patterns.
Atomic descriptors are faster but may miss multi-step intrusions.
Composite descriptors offer deeper context but consume more resources.

20. What is Stateful Protocol Analysis? *(CO2, K1)*
Ans: Stateful Protocol Analysis monitors ongoing communication sessions over time.
It checks whether protocol behavior matches expected states and sequences.

It identifies attacks that occur during multi-step transactions. This technique is useful for protocols like HTTP, FTP, or TCP.

21. What is the first step in intrusion analysis? *(CO2, K1)*
Ans: The first step is data collection from sources like logs, network traffic, and user activity.
Tools like packet sniffers or log aggregators are used.
Collected data form the basis for further analysis and detection.
Accurate data collection is essential for detecting true intrusions.

22. Name the four phases of intrusion analysis. *(CO2, K2)*
Ans: The four phases are: Preprocessing, Analysis, Response, and Refinement.
Preprocessing organizes data; Analysis compares it with known patterns.
Response involves alerts or actions, and Refinement improves accuracy over time.
These phases help create an efficient and adaptive detection system.

23. What is the role of feature extraction in intrusion analysis? *(CO2, K2)*
Ans: Feature extraction identifies useful attributes like IP addresses, ports, login attempts, etc.
These features help differentiate between normal and abnormal activities.
They improve the performance of detection algorithms.
Good feature selection enhances accuracy and reduces false alarms.

24. State two types of IDS responses. *(CO2, K1)*
Ans: The two main response types are Passive and Active responses.
Passive responses include alerting administrators or logging events.
Active responses involve blocking traffic or terminating sessions.
The response type is selected based on the severity of the intrusion.

25. What is meant by rate limiting in IDS response? *(CO2, K2)*
Ans: Rate limiting is an active response that controls bandwidth usage from a suspicious source.
It helps in reducing the impact of DoS or brute-force attacks.
Instead of blocking completely, it slows down malicious traffic.
It is useful in maintaining availability while managing threats.

26. What is vulnerability analysis? *(CO2, K1)*
Ans: Vulnerability analysis is the process of identifying weaknesses in systems or networks that could be exploited.
It involves scanning and assessing systems for known vulnerabilities.
Tools are used to simulate attacks or infer potential risks.
It helps in securing systems proactively before real attacks occur.

27. List the two classifications of vulnerability analysis tools. *(CO2, K1)*
Ans: Vulnerability analysis tools are classified by:
(1) Location: Host-based or Network-based,
(2) Access level: Credentialed or Non-Credentialed.
These determine whether the tools assess system internals or external surfaces.
Each type has specific use cases and limitations.

28. What is credential vulnerability analysis? *(CO2, K2)*
Ans: Credential vulnerability analysis uses valid system credentials (like admin login) to scan deeper.
It checks for misconfigurations, weak passwords, outdated software, and patch status.
This method is accurate and generates fewer false positives.
Tools like Nessus or Qualys are often used for such scans.

29. Mention one advantage and one disadvantage of network-based vulnerability analysis. *(CO2, K2)*
Ans: Advantage: It is platform-independent and can scan remotely without needing system credentials.
Disadvantage: It may produce more false positives due to limited internal access.
It also risks missing internal vulnerabilities not visible externally.
Still, it's useful for external exposure analysis.

30. Which tools can be used for credentialed scans? *(CO2, K1)*
Ans: Common tools that support credentialed scans include:
(1) Nessus – popular for in-depth scanning using SSH or Windows login.
(2) Qualys – offers authenticated vulnerability scanning.
(3) OpenVAS – supports login-based scanning with integration options.

31. What does a Protocol-Based IDS (PIDS) monitor? *(CO2, K1)*
Ans: A PIDS monitors and analyzes application-layer protocols like HTTP, FTP, or SMTP.
It checks if protocol usage aligns with expected behavior or standards.
PIDS detects anomalies or attacks embedded in legitimate-looking protocol traffic.
It's typically placed between the client and the application server

32. Give an example of attack detected by HTTP PIDS. *(CO2, K2)*
Ans: A common example is SQL Injection, where malicious code is embedded in an HTTP query.
For instance: GET /search?query='OR 1=1-- may bypass authentication or expose data.
PIDS detects unusual patterns or characters like ', --, and blocks the request.
It prevents backend database compromise.

33. What is the purpose of mapping IDS responses to policy? *(CO2, K2)*
Ans: Mapping ensures that IDS responses align with the organization's security policies.
It defines what action to take for specific threat types—like alerts, blocks, or isolations.
It maintains consistency, supports compliance, and avoids arbitrary decisions.
This helps balance security with availability.

34. What are the common outputs of an IDS alert? *(CO2, K1)*
Ans: IDS alerts can be delivered through pop-up notifications, emails, dashboards, logs, or SNMP traps.

Some systems also forward alerts to incident response tools. These outputs contain information like source IP, attack type, and time. Alerts enable administrators to respond quickly to threats.

35. Why is refinement important in IDS analysis? *(CO2, K2)*

Ans: Refinement involves tuning the IDS rules and thresholds based on past results.

It helps reduce false positives and improve detection accuracy. Security teams analyze feedback and update signatures or anomaly profiles. This continuous improvement makes IDS more effective over time.

Part B Q

PART -B

1. Explain in detail the architecture and working of an Intrusion Prevention System (IPS). Highlight its components and response mechanisms. *(CO2, K3)*

2. Compare and contrast Host-Based Intrusion Prevention Systems (HIPS) and Network-Based Intrusion Prevention Systems (NIPS) with examples. *(CO2, K4)*

3. Describe the various types of Network Intrusion Detection Systems (NIDS) and explain their deployment locations with advantages. *(CO2, K3)*

4. Illustrate the working of a Hybrid IDS with a neat architecture diagram. How does it reduce false positives? *(CO2, K4)*

5. Write in detail about protocol-based IDS. Use an HTTP-based SQL injection example to explain how it detects protocol-layer threats. *(CO2, K4)*

6. Discuss the phases involved in the intrusion analysis process. How does this model help in threat classification and response? *(CO2, K4)*

7. What are the different types of IDS responses? Explain each with suitable examples and map them to appropriate policy actions. *(CO2, K3)*

8. Explain credentialed and non-credentialed vulnerability analysis. Provide a comparative table listing their strengths and weaknesses. *(CO2, K3)*

9. Analyze the benefits and limitations of anomaly-based detection methods. How does refinement improve their performance? *(CO2, K4)*

10. What is vulnerability analysis? Explain its types, tools used, and how it complements IDS in a modern cybersecurity framework. *(CO2, K4)*

Supportive Online Certification courses

R.M.K GROUP OF INSTITUTIONS

SUPPORTIVE ONLINE COURSES

S No	Course provider	Course title	Link
1	Udemy	The Complete Cyber Security Course : Network Security	https://www.udemy.com/course/network-security-course/?couponCode=ST12MT90625AI
2	Udemy	Snort Intrusion Detection, Rule Writing, and PCAP Analysis	https://www.udemy.com/course/snort-intrusion-detection-rule-writing-and-pcap-analysis/?couponCode=ST12MT90625AI
3	NPTEL	Network Security	https://onlinecourses.nptel.ac.in/noc25_ee54/preview

Real life Applications in day to day life and to Industry

REAL TIME APPLICATIONS IN DAY TO DAY LIFE AND TO INDUSTRY

1. Home Network Security (Wi-Fi Routers)
    - IDS tools embedded in routers (like ASUS AiProtection or Firewalla) monitor traffic.
    - Alerts users of unauthorized access or abnormal activity on home devices.
2. Mobile Security Apps
    - Apps like Avast and Norton use IDS techniques to detect suspicious app or network behavior.
    - Alerts users about data leakage, fake Wi-Fi, or background malware communication.

Content beyond Syllabus

Contents beyond the Syllabus

1. AI-Powered Intrusion Detection Systems (AI-IDS)

Reference: Datasets used to train/test AI-based IDS (NSL-KDD Dataset)

Assessment Schedule

FIAT: 14.08.2025

SIAT: 23.09.2025

Model Exam: 28.10.20

Prescribed Text books & Reference books

PRESCRIBED TEXT BOOKS AND REFERENCE BOOKS

TEXT BOOKS

1. Rafeeq Rehman : “Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID,” 1st Edition, Prentice Hall , 2003.

2. Internet Security: A Hands-on Approach, by Wenliang Du, Third Edition, 2019

REFERENCE BOOKS

1. Christopher Kruegel, Fredrik Valeur, Giovanni Vigna: “Intrusion Detection and Correlation Challenges and Solutions”, 1st Edition, Springer, 2005.

2. Carl Endorf, Eugene Schultz and Jim Mellander “Intrusion Detection & Prevention”, 1st Edition, Tata McGraw-Hill, 2004.

3. Stephen Northcutt, Judy Novak : “Network Intrusion Detection”, 3rd Edition, New Riders Publishing, 2002.

4. T. Fahringer, R. Prodan, “A Text book on Grid Application Development and Computing Environment”. 6th Edition, Khanna Publishers, 2012.

Mini Project Suggestions

R.M.K GROUP OF INSTITUTIONS

MINI PROJECT SUGGESTIONS

1. Real-Time Intrusion Detection with Snort
   Create custom Snort rules and send alerts via email for detected intrusions.
   K Level: K4 – Analyzing
2. Credentialed vs Non-Credentialed Scan Comparison
   Use Nmap and OpenVAS to compare vulnerability scans with and without login.
   K Level: K5 – Evaluating
3. Web Attack Detection Using Apache Logs
   Simulate SQL injection/XSS and detect them by analyzing HTTP server logs.
   K Level: K4 – Analyzing
4. Snort Log Visualization Dashboard
   Build a dashboard to visualize Snort alerts using charts and graphs.
   K Level: K6 – Creating
5. Simulate IDS Passive vs Active Responses
   Configure IDS to log or block based on policy and compare both actions.
   K Level: K5 – Evaluating

Thank you

R.M.K GROUP OF INSTITUTIONS