

**Government Polytechnic
Ahmedabad
Program: Diploma in Computer
Engg
Computer and Network Security
(3350704-C304)**

**UNIT_5
Web Security**

Intrusion and Intruders



- ❖ An intrusion is defined as the unauthorized use, misuse, or abuse of a computer system by either authorized user or external perpetrator.

Intruder:

- ❖ An intruder is a person who attempts to gain unauthorized access to a system or to damage that system.
- ❖ The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system.

Types of Intruders




Masquerader:

- ❖ An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.

Misfeasor:


- ❖ A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.

Clandestine user:

- ❖ An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection
- 

Intrusion Detection Systems (IDS)



- ❖ An intrusion detection system is a system that monitors network traffic for suspicious activity and alerts when such activity is discovered.
 - ❖ Intrusion detection is a type of security management system for computers and system and networks.
 - ❖ It includes functions like:
 - Monitoring and analyzing both user and system activities.
 - Analyzing system configurations and vulnerabilities.
 - Assessing system and file integrity.
 - Ability to recognize patterns typical of attacks.
 - Analysis of abnormal activity patterns.
 - Tracking user policy violations .
- 

Classification of IDS



❖ There are various types of Intrusion Detection System:-

- I. Network Based Intrusion Detection System(NIDS)
- II. Host Based Intrusion Detection Systems(HIDS)
- III. Protocol based Intrusion Detection Systems(PIDS)
- IV. Application protocol based Intrusion Detection Systems(APIDS)
- V. Hybrid Intrusion Detection Systems

Network based Intrusion detection



- ❖ NIDS are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network.
- ❖ It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks.
- ❖ Once the attack is identified or abnormal behaviour is sensed, the alert can be sent to the administrator.
- ❖ An example of an NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall.

Network based Intrusion detection



- ❖ Ideally one would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network.
- ❖ OPNET and NetSim are commonly used tools for simulation network intrusion detection systems.
- ❖ NID Systems are also capable of comparing signatures for similar packets to link and drop harmful detected packets which have a signature matching the records in the NIDS.

Host based Intrusion detection



- ❖ Host-based intrusion detection system is an intrusion detection system that monitors and analyses the internals of a computing system as well as the network packets on its network.
- ❖ HIDS run on individual hosts or devices on the network.
- ❖ A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected.
- ❖ It takes a snapshot of existing system files and matches it to the previous snapshot.
- ❖ If the critical system files were modified or deleted, an alert is sent to the administrator to investigate.

Host based Intrusion detection



- ❖ A host-based IDS monitors all parts of dynamic behaviour and the state of a computer system.
- ❖ HIDS might detect which program accesses what resources and discover and discover that, for example, a word-processor has started modifying the system password database
- ❖ Similarly HIDS might look at the state of the system, its stored information, whether in ram, in the file system, log files or elsewhere; and check that content of these appear as expected.
- ❖ One can think of HIDS as an agent that monitors whether anything or anyone, whether internal or external, has circumvented the system's security policy.

Protocol-based Intrusion Detection



- ❖ Protocol-based intrusion detection system (PIDS) comprises of a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server.
- ❖ It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol.
- ❖ As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

Application Protocol-based Intrusion Detection



- ❖ Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers.
- ❖ It identifies the intrusions by monitoring and interpreting the communication on application specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

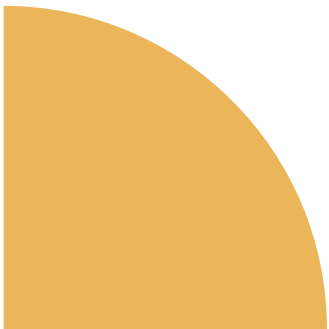
Hybrid Intrusion Detection System :

- ❖ Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system.
- ❖ In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system.
- ❖ Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

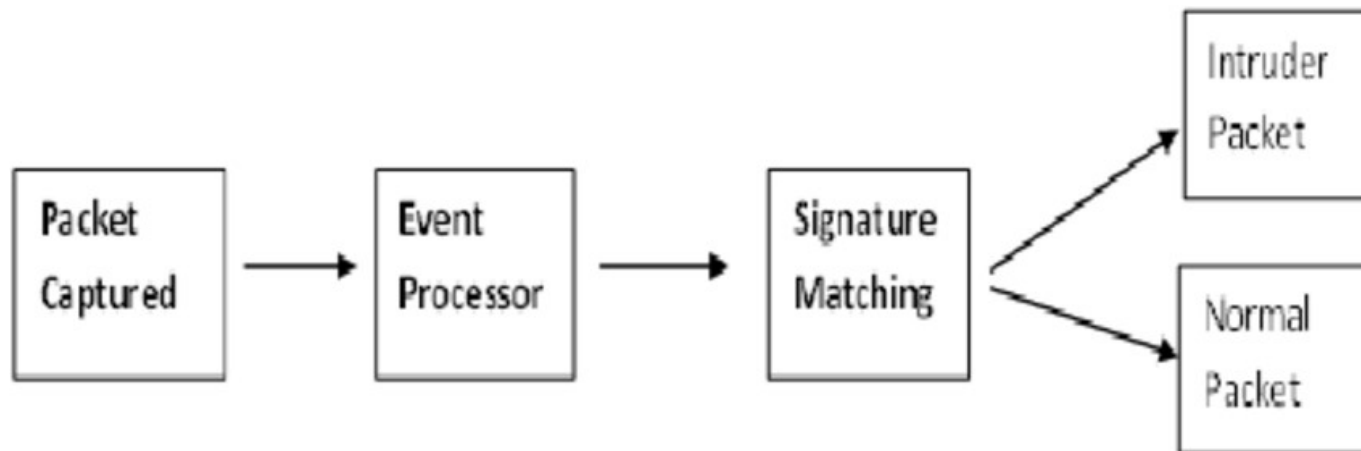
Detection Methods of IDS



- ❖ There are mainly two types of detection methods used by Intrusion Detection systems.
 1. Signature Based Intrusion detection system.
 2. Anomaly Based Intrusion detection system.



Signature Based IDS

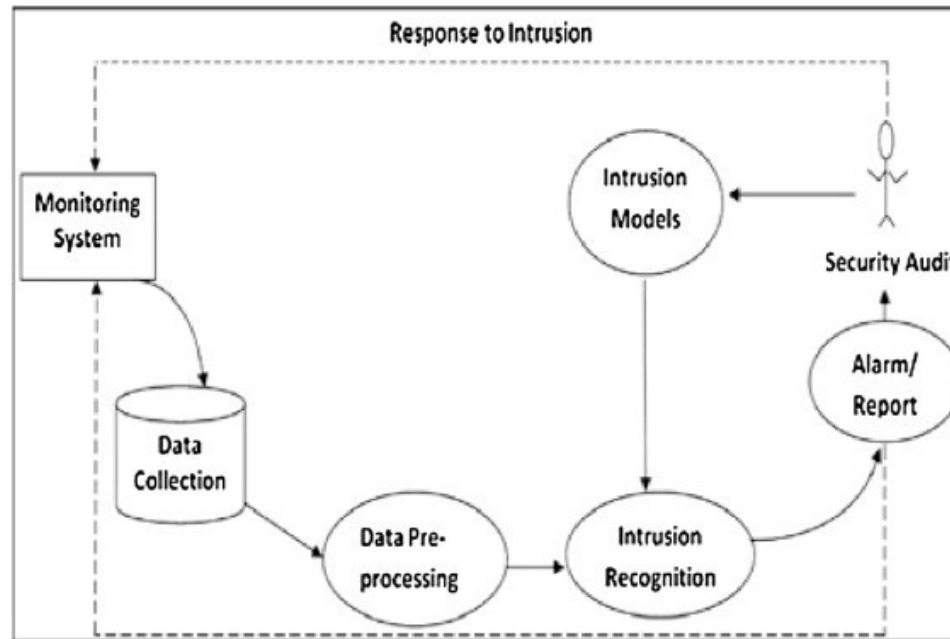


Signature Based Detection



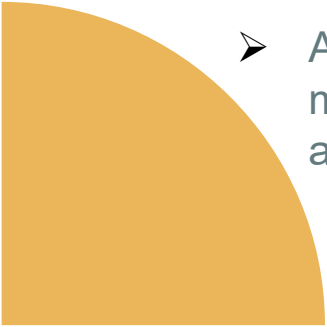
- ❖ A signature based IDS will monitor packets on the network and compare the against a database of signatures or attributes from known malicious threats. This is similar to the way most antivirus software detects malware.
- ❖ The issue is that there will be a lag between a new threat being discovered in the world and the signature for detecting that threat being applied to the IDS. During that lag time the IDS would be unable to detect the new threat.
- ❖ You Might use a signature that looks for particular Strings Within an payload to detect attacks that are attempting to a particular buffer-overflow vulnerability.
- ❖ Also, Pattern matching can be performed very quickly on modern systems so the amount of power needed to perform these checks is minimal for a confined rule set.

Anomaly based Detection




Anomaly based Detection



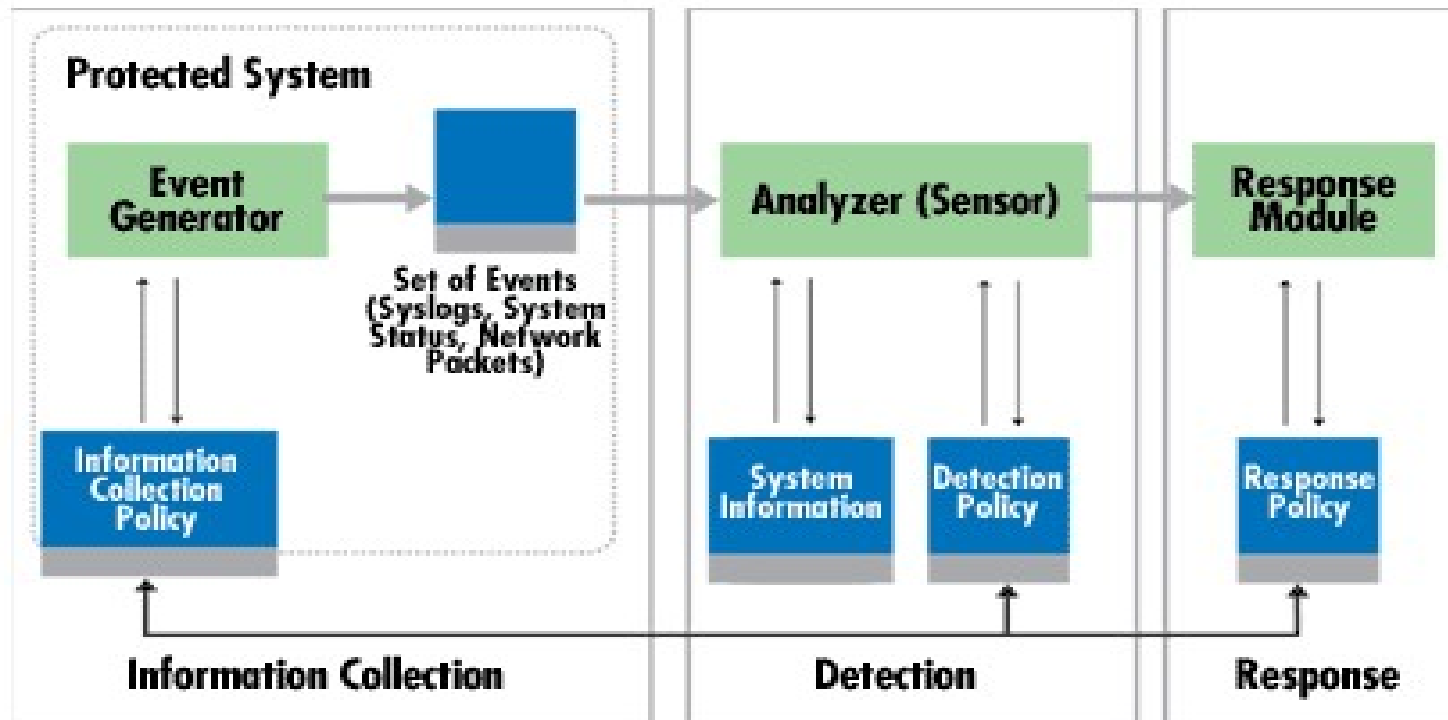
- ❖ An IDS which is anomaly based will monitor network traffic and compare it against an established baseline.
 - ❖ The baseline will identify what is “normal” for that network- what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other and alert the administrator or user when traffic is detected which is anomalous, or significantly different, than the baseline.
 - An Anomaly-Based ids, is a system for detecting computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous.
- 

Anomaly based Detection



- ❖ The Classification is based on heuristics or rules, rather than patterns or signatures, and attempts to detect any type of misuse that falls out of normal system operation. This is as opposed to signature based systems which can only detect attacks for which a signature has previously been created.
 - ❖ In order to determine what is attack traffic, the system must be taught to recognize normal system activity. This can be accomplished in several ways, most often with artificial intelligence type techniques.
 - ❖ The issue is that it may raise a False Positive alarm for a legitimate use of bandwidth if the baselines are not intelligently configured.
- 

LOGICAL COMPONENTS OF IDS





COMPONENTS OF IDS

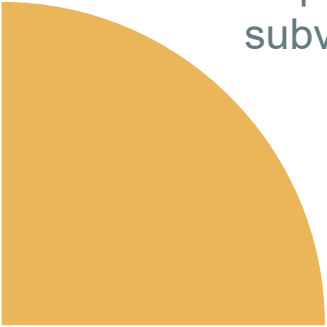
- It consists three parts:
 - 1) Event Generator
 - 2) Analyzer
 - 3) Response Module
- The event generator (operating system, network, application) produces a policy-consistent set of events that may be a log (or audit) of system events, or network packets.
- The role of the sensor is to filter information and discard any irrelevant data obtained from the event set associated with the protected system.
- Response module will fire the alarm if any intrusion of policy is detected by sensor.

5.2 WEB SECURITY THREATS

- A web threat is any threat that uses the World Wide Web to facilitate cybercrime.
- Web threats use multiple types of malware and fraud, all of which utilize HTTP or HTTPS protocols, but may also employ other protocols and components, such as links in email or IM, or malware attachments or on servers that access the Web.
- They benefit cybercriminals by stealing information for subsequent sale and help absorb infected PCs into botnets.
- It can divide into 2 primary category:
 - 1) Pull based threat
 - 2) Push based threat



Web Security Consideration

- The world wide web is fundamentally a client/server application running over the internet and TCP/IP intranets.
 - The Web is vulnerable to attacks on the web servers over the internet.
 - The Web is increasingly serving as a highly visible outlet for corporate and product information and as the platform for business transaction.
 - Reputations can be damaged and money can be lost if the web servers are subverted.
- 

Web Security Consideration



- Although Web browsers are very easy to use, Web server relatively easy to configure and manage and Web content is increasingly easy to develop the underlying software is extraordinarily complex.
- This complex software may hide many potential security flaws.
- A Web server can be exploited as a launching pad into the corporation's or agency's entire computer complex.
- Once the web server is subverted ,an attacker may be able to gain access to data and system not part of the web itself but connected to the server at the local site.

Web security threats



- One way to group these threats is in terms of passive attack and active attacks.
- Another way to classify Web security is in terms of the location of threat: Web server, Web browser and network traffic between browser and server.
- Issues of server and browser security fall into category of computer system security.



Web security threats


PARAMETERS	THREATS	CONSEQUENCES	COUNTERMEASURES
INTEGRITY	<ul style="list-style-type: none">•Modification of user data•Trojan horse browser•Modification of memory•Modification of message traffic in transit	<ul style="list-style-type: none">•Loss of information•Compromise of machine•Vulnerability to all other Threats	<ul style="list-style-type: none">•Cryptography•checksums
CONFIDENTIALITY	<ul style="list-style-type: none">•Eavesdropping on the net•Theft of info from server•Theft of data from client•Info about network configuration•Info about which client talks to server	<ul style="list-style-type: none">•Loss of information•Loss of privacy	<ul style="list-style-type: none">•Encryption•Web proxies

Web security threats

PARAMETERS	THREATS	CONSEQUENCES	COUNTERMEASURES
AVAILABILITY or DENIAL OF SERVICE	<ul style="list-style-type: none">•Killing of user threads•Flooding machine with bogus request•Filling up disk or memory•Isolating machine by DNS Attacks	<ul style="list-style-type: none">•Disruptive•Annoying•Prevent user from getting work done	<ul style="list-style-type: none">•Difficult to prevent
AUTHENTICATION	<ul style="list-style-type: none">•Impersonation of legitimate users•Data forgery	<ul style="list-style-type: none">•Misrepresentation of user•Belief that false information is valid	<ul style="list-style-type: none">•Cryptographic Techniques

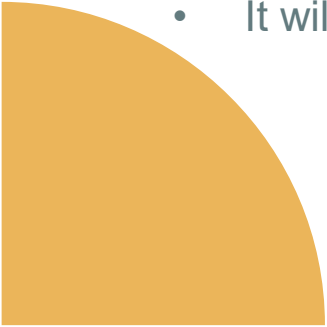


WEB TRAFFIC SECURITY APPROACHES

- Number of approaches to providing Web security are possible.
 - The various approaches that have been considered are similar in the services they provide and to some extent, in the mechanisms that they use.
 - But they differ with respect to their scope of applicability and their relative location within the TCP/IP protocol stack.
- 

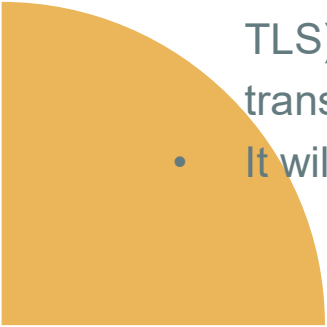


WEB TRAFFIC SECURITY APPROACHES

- One way to provide Web security is to use IP Security.
 - The advantage of using IPSec is that it is transparent to end users and applications and provides a general-purpose solution.
 - IPSec includes a filtering capability so that only selected traffic need incur the overhead of IPSec processing.
 - It will work on Network layer.
- 




WEB TRAFFIC SECURITY APPROACHES

- Another relatively general-purpose solution is to implement security just above TCP .
 - The foremost example of this approach is the Secure Sockets Layer (SSL) and the follow-on Internet standard of SSL known as Transport Layer Security (TLS).
 - At this level, there are two implementation choices. For full generality, SSL (or TLS) could be provided as part of the underlying protocol suite and therefore be transparent to applications.
 - It will work on Transport layer.
- 



WEB TRAFFIC SECURITY APPROACHES

- Application-specific security services are embedded within the particular application.
 - The advantage of this approach is that the service can be tailored to the specific needs of a given application.
 - It will work on Application layer.
- 

SECURE SOCKET LAYER(SSL)

- SSL is in fact not a single protocol but rather a set of protocols that can additionally be further divided in two layers:
- the protocol to ensure data security and integrity: this layer is composed of the SSL Record Protocol

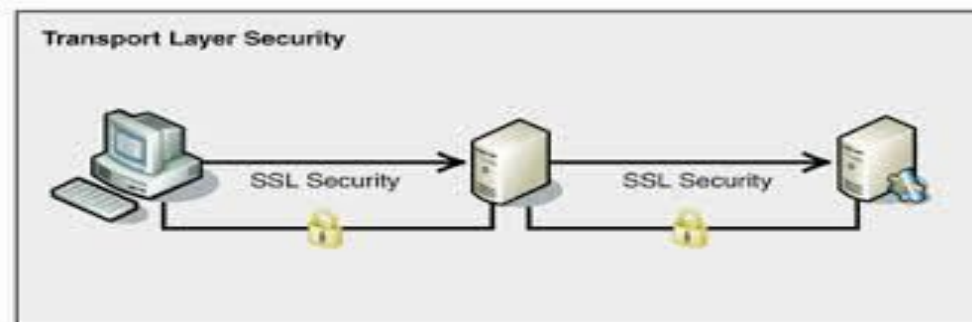
SSL handshake protocol	SSL cipher change protocol	SSL alert protocol	Application Protocol (eg. HTTP)
SSL Record Protocol			
TCP			
IP			

SECURE SOCKET LAYER(SSL)

- the protocols that are designed to establish an SSL connection: three protocols are used in this layer: the SSL Handshake Protocol, the SSL Change Cipher Spec protocol and the SSL Alert Protocol.
- Two important concept of SSL are: SSL session and connection
- connection: this is a logical client/server link, associated with the provision of a suitable type of service. In SSL terms, it must be a peer-to-peer connection with two network nodes.
- session: this is an association between a client and a server that defines a set of parameters such as algorithms used, session number etc. An SSL session is created by the Handshake Protocol

TRANSPORT LAYER SECURITY(TLS)

- A protocol that provides communications privacy and security between two applications communicating over a network.
- It composed of 2 layer
 - 1) TLS Record Protocol
 - 2) TLS Handshake Protocol



TRANSPORT LAYER SECURITY(TLS)

1) TLS Record Protocol

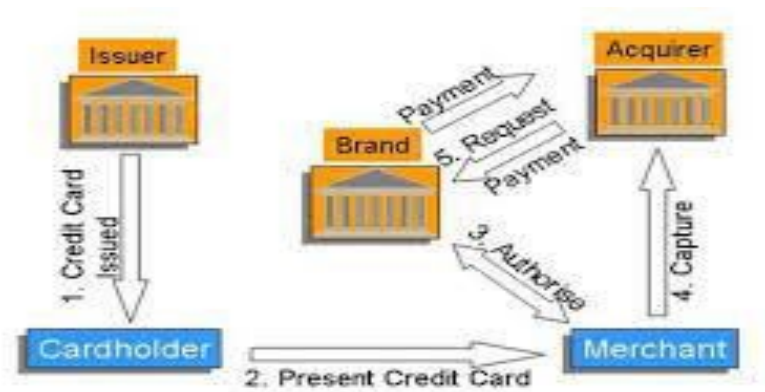
- The TLS Record protocol secures application data using the keys created during the Handshake.
- The Record Protocol is responsible for securing application data and verifying its integrity and origin.

2) TLS Handshake Protocol

- TLS Handshake Protocol is responsible for the authentication and key exchange necessary to establish or resume secure sessions. When establishing a secure session, the Handshake Protocol manages the following:
 1. Cipher suite negotiation
 2. Authentication of the server and optionally, the client Session key information exchange.

SECURE ELECTRONIC TRANSACTION

- Secure Electronic Transaction (SET) is a suit of protocol that has been developed and promoted by a consortium of Visa and MasterCard to ensure security of online financial transactions.



SECURE ELECTRONIC TRANSACTION

- Issuer (could be consumer's High street bank) issues consumer with the credit card
- Cardholder (consumer) presents the merchant with his credit card for payment along with the order
- Merchant requests and receives authorization of payment from the credit card brand (could be Visa, MasterCard, American Express, etc) before processing the order.
- Having received authorization from the brand, merchant initiates the process of capture of monetary funds through the acquirer (could be Merchant's High street bank)

SECURE ELECTRONIC TRANSACTION

5. Acquirer forwards authorization details to the brand and requests settlement from the brand
6. Having received payment from the brand, acquirer credits Merchant's account with the funds
7. Brand bills the consumer for the funds