UNIT - 5

Date ____/____/____
Page ____

① IP Security (IPsec) -

It is a capability that can be added to either current version of the Internet Protocol (IPv4 or IPv6) by means of additional headers.

IPSec encompasses three functional area i.e. Authentication, Confidentiality and Key management

→ **Application of IPSec -**

(1) Secure branch office connectivity over the Internet.
(2) Secure remote access over the Internet.
(3) Establishing extranet and intranet connectivity with partners.
(4) Enhancing electronic commerce security

→ **Benefits of IPSec -**

(1) Provide strong security if implimented in a firewall or router.
(2) Transparent to applications
(3) Transparent to end users
(4) Provide security to end users if needed.

→ **IPsec Documents** - It categorized in following groups -

(1) Architecture
(2) Authentication Header (AH)
(3) Encapsulating Security Payload (ESP)
(4) Internet Key Exchange (IKE)
(5) Cryptographic algorithms.

→ **IPSec Services -**

(1) Access Control
(2) Connectionless Integrity
(3) Data origin authentication
(4) Rejection of replayed packets (a form of partial sequence integrity)
(5) Confidentiality (encryption)
(6) limited traffic flow confidentiality.

→ **IP Security Policy -**

It is determined primarily by the interaction of two databases, the security association database (SAD) and the security policy database (SPD).

→ Tunnel mode and Transport mode functionality -

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers	Authenticates entire inner IP packet (inner header + IP payload) + selected portions of outer IP header and outer IPv6 extension header
ESP	Encrypts IP payload & any IPv6 extension headers following the ESP header.	Encrypts entire inner IP packet
ESP with authentication	Encrypts IP payload & any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header	Encrypts entire inner IP packet. Authenticates inner IP packet.

→ Security Association (SA) -

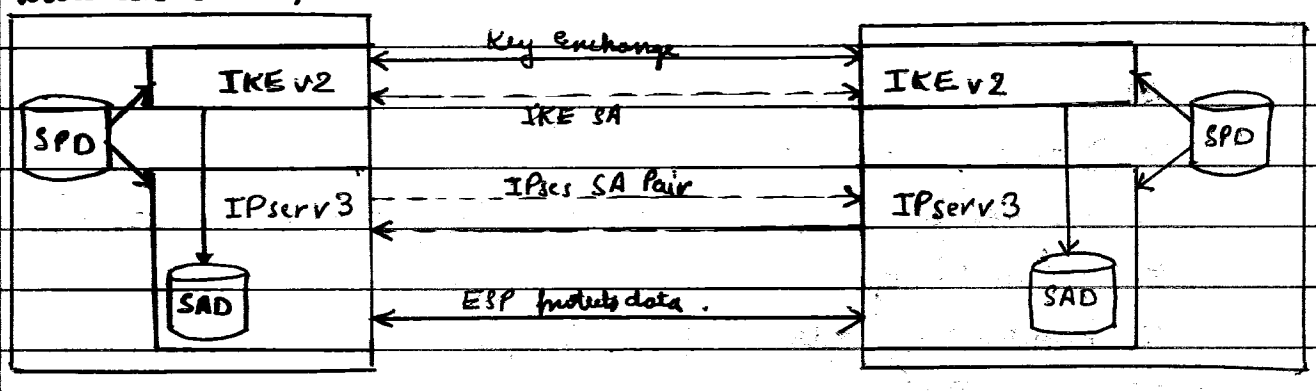
It is a one-way logical connection between a sender and a receiver that affords security services to the traffic carried out. It is identified by 3 parameters

(1) Security Parameter Index (SPI)

(2) IP destination address

(3) Security Protocol Identifier

→ IPsec architecture -



Date ____/____/____
Page ____

(2) Web Security -

Web based security protocols are used to provide for secure transactions between Internet users and Web site.

There are four types of threats on the web, they are integrity threats, confidentiality threats, Denial of service threats and authentication threats.

(3) Firewalls -

It forms a barrier through which the traffic going in each directions must pass. A firewall security policy dictates which traffic is authorized to pass in each direction.

A firewall may be designed to operate as a filter at the level of IP packets, or may operate at a higher protocol layer.

(4) Design Principles / Goals Of Firewall -

(1) All traffic from inside to outside, and vice versa, must pass through the firewall.

(2) Only authorized traffic, as defined by the local security policy, will be allowed to pass.

(3) The firewall itself immune to penetration.

(5) Types of Firewalls -

(1) Packet filtering firewall - It applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.

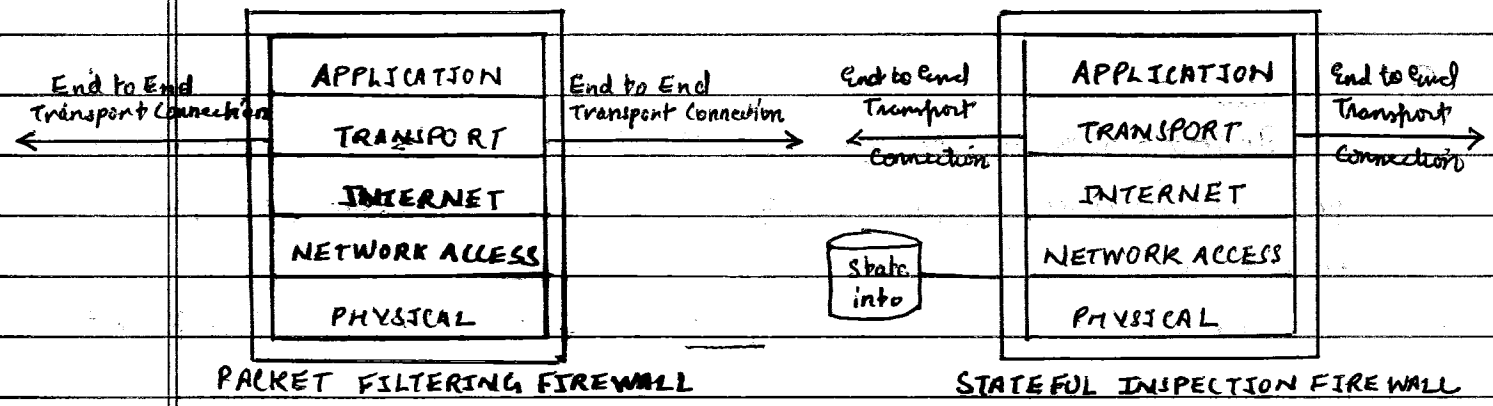
Filter rules are based on information contained in a network packet - i.e. Source IP address, Destination IP address, Source & destination transport-level address, IP protocol field and Interface.

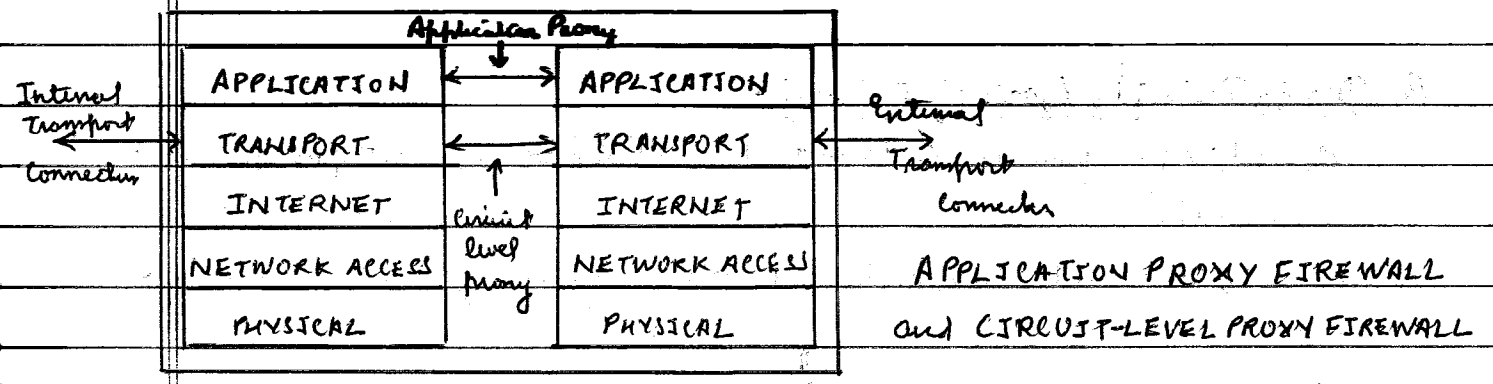
Packet filtering firewall attacks are IP address spoofing, source routing attacks and tiny fragment attacks.

(2) Stateful Inspection Firewalls - A traditional packet filter makes filtering decisions on an individual packet basis and does not take into consideration any higher layer context.

(3) Application level Gateway (Application Proxy) - It acts as a relay of application level traffic. More secure than packet filters.

(4) Circuit level Gateway (Circuit level proxy) - It can be a stand-alone system or it can be a specialized functions performed by an application-level gateway for certain applications.





(6) Trusted Systems -

A system believed to enforce a given set of attributes to a stated degree of assurance.

Initial work on trusted computer and trusted OS was based on the reference monitor concept.

The reference monitor enforces the security rules (no read up, no write down) and has the following properties -

(1) Complete Mediation → enforced on every access

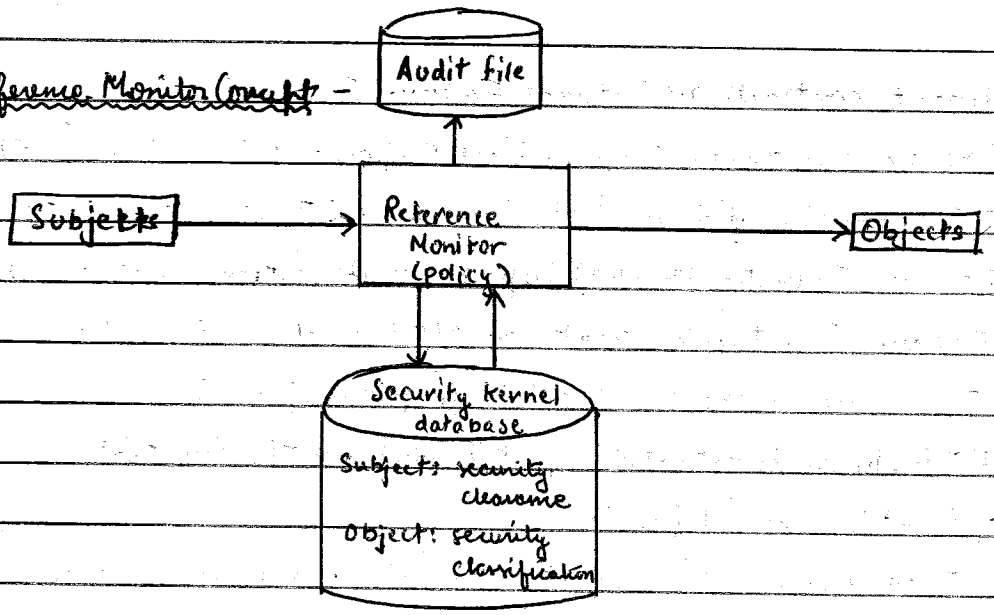
(2) Isolation

(3) Verifiability.

One way to secure against Trojan horse attacks is the use of a secure, trusted operating system.

Date ___/___/___
Page ___

→ Reference Monitor (concept) –



⑤ Computer Forensics –

It is the practice of collecting, analyzing and reporting on digital data in a way that is legally admissible. It can be used in detection and prevention of crime and in any dispute where evidence is stored digitally.

⑥ Need for computer forensics –

(1) Presence of a majority of electronic documents
(2) Search and identify data in a computer
(3) Digital evidence can be easily destroyed, if not handled properly.
(4) For recovering deleted, encrypted & corrupted files from a system.

Objectives

⑦ Objective of Computer forensics –

(1) To recover, analyze and present computer-based material in such a way that it can be presented as evidence in a court of law.
(2) To identify the evidence in short time, estimate potential impact of the malicious activity on the victim, and assess the intent and identity of the perpetrator.

Steps

⑧ Stages of Forensic Investigation in tracking cyber criminals –

(1) An incident occurs in which, the company's server is compromised.
(2) The client contacts the company's advocate for legal advice.

(3) The Advocate contracts an External Forensic Investigator.
(4) The Forensic Investigator prepares First Response of Procedures (FRP).
(5) The FI seizes the evidences in the crime scene & transports them to the Forensic lab
(6) The Forensic Investigator (FI) prepares the Bit-stream images of the files
(7) The Forensic Investigator creates an MD5 number of the files.
(8) The FI examines the evidence files for proof of a crime.
(9) The FI prepares investigation reports & concludes the investigation, enables the advocate identify required proofs.
(10) The FI handles sensitive report to the client in a secure manner
(11) The Advocate studies the report and might press charges against the offensive in the Court of law.
(12) The FI usually destroys all the evidences

~~(9) Key steps in Forensic Investigation -~~

(9) Incident Handling -

It helps to find out trends and patterns regarding intruder activity by analyzing it. It involves three basic functions -

(1) Incident reporting
(2) Incident analysis
(3) Incident response

The incident handling process is divided into six stages -

(1) Preparation → Create a policy, develop preventive measures
(2) Identification → It involves validating, identifying and reporting the incident
(3) Containment → limit the extent and intensity of an incident
(4) Eradication → Investigate further to uncover the cause of the incident
(5) Recovery → Determine course of actions, ~~monitor~~ validate systems, integrity of the backup
(6) Follow-up → Post-mortem analysis, Revise policies, cost analysis

(10) Hacking -

It is the gaining of access (wanted or unwanted) to a computer and viewing, ~~editing~~ copying, or erasing data (leaving a trace) without the intention of destroying

data or maliciously harming the computer.

(11) Classes of Hackers -

(1) Black Hats - Individuals with extraordinary computing skills, resorting to malicious or destructive activities. Also known as crackers.

(2) White Hats - Individuals professing hackers skills and using them for defensive purposes. Also known as security analysts.

(3) Grey Hats - Individuals who work both offensively and defensively at various times.

(4) Suicide Hackers - Individuals who aim to bring down critical infrastructure for a "cause" and do not worry about going 30 years in jail for their actions.

(12) Footprinting -

It is the blueprint of the security profile of an organization, undertaken in methodological manner with respect to networks (Internet/Intranet/Extranet/wireless) and systems involved.

An attacker spends 90% of the time in profiling an organization and another 10% in launching the attack.

Footprinting is necessary because -

(1) It is necessary to systematically and methodically ensure that all pieces of information related to the aforementioned technologies are identified.

(2) It is often the most difficult task to determine the security posture of an entity.

(13) Scanning -

It is one of the three components of intelligence gathering for an attacks. It mainly scans for ports, networks and vulnerabilities.

The attacker finds information about the -

(1) Specific IP addresses

(2) Operating systems

(3) System architecture

(4) Services running on each computer.

→ Types of scanning are -

(1) Port scanning - A series of messages sent by someone attempting to break into a computer to learn about the computer's network services.

Each associated with a "well-known" port number.

(2) Network Scanning - A procedure for identifying active hosts on a network either for the purpose of attacking them or for network security assessment.

(3) Vulnerability Scanning - The automated process of proactively identifying vulnerabilities of computing systems present in a network.

→ Objectives of scanning are -

(1) To detect the live systems running on the network.

(2) To discover which ports are active/running.

(3) To discover the OS running on the target system (Footprinting)

(4) To discover the services running/listening on the target system.

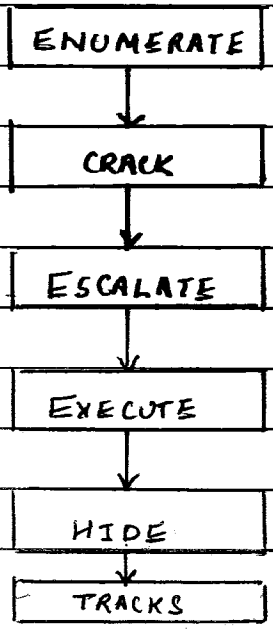
(5) To discover the IP address of the target system.

(14) E-mail Spiders -

It crawl web pages on the Internet and extract emails, that are later stored into a document or database.

Tools - 1st Email Address Spider, Web data Extractor

(15) Overview of System Hacking Cycle -



Date ___/___/___
Page _____

Step 1 - Enumerate users - Extract user names using Win 2K enumeration and SNMP probing.

Step 2 - Crack the password - of the user and gain access to the system

Step 3 - Escalate Privileges - Escalate to the level of the administrator

Step 4 - Execute applications - Plant keyloggers, spywares, & rootkits on the machine

Step 5 - Hide files - Use steganography to hide hacking tools and source code

Step 6 - Cover your tracks - Erase tracks so that you will not be caught