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 areas: authentication, confidentiality, and key management.

   **Applications 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 implemented in a firewall or router.
   2. Transparent to applications.
   3. Transparent to end users.
   4. Provide security to end users if needed.

2. **IPsec Document** - 9 categories in following groups -
   1. Architecture.
   2. Authentication header (AH).
   3. Encapsulating security payload (ESP).
   4. Internet Key Exchange (IKE).
   5. Cryptographic algorithms.

3. **IPsec Session** -
   1. Access Control.
   2. Connectionless Integrity.
   3. Data origin authentication.
   4. Rejection of replayed packets (a form of partial sequence integrity).
   5. Confidentiality (encryption).

4. **IP Security Policy** -
   It is determined primarily by the interaction of two databases, the security announcement database (SAD) and the security policy database (SPD).
**Tunnel mode and Transport mode functionality**

<table>
<thead>
<tr>
<th>Transport Mode SA</th>
<th>Tunnel Node SA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AH</strong></td>
<td><strong>AH</strong></td>
</tr>
<tr>
<td>Authenticates IP payload and selects portion of IP headers and IPv6</td>
<td>Authenticates entire inner IP packet payload</td>
</tr>
<tr>
<td>extant IP headers</td>
<td>(without header + IP payload) + selected</td>
</tr>
<tr>
<td></td>
<td>portions of outer IP headers and outer</td>
</tr>
<tr>
<td></td>
<td>IPv6 extension headers</td>
</tr>
<tr>
<td><strong>ESP</strong></td>
<td><strong>ESP</strong></td>
</tr>
<tr>
<td>Encrypts IP payload &amp; any IPv6</td>
<td>Encrypts entire inner IP packet</td>
</tr>
<tr>
<td>extant IP headers following the</td>
<td></td>
</tr>
<tr>
<td>ESP header header</td>
<td></td>
</tr>
<tr>
<td><strong>ESP with authentication</strong></td>
<td><strong>ESP with authentication</strong></td>
</tr>
<tr>
<td>Encrypts IP payload &amp; any IPv6</td>
<td>Encrypts entire inner IP packet</td>
</tr>
<tr>
<td>extant IP headers following the</td>
<td></td>
</tr>
<tr>
<td>ESP header header, authenticates IP</td>
<td></td>
</tr>
<tr>
<td>payload but not IP headers</td>
<td></td>
</tr>
</tbody>
</table>

**Security Association (SA)**

- SA is a one-way logical connection between a sender and a receiver that affects security services to the traffic involved in it. It is identified by 3 parameters:
  1. Security Parameter Index (SPI)
  2. IP destination address
  3. Security protocol identifier

**IPsec architecture**

- IKE V2
- SPD
- IPServ3
- SAD
- Key exchange
- IKE SA
- IPServ3 SA pair
- ESP includes data
- SPD
- IKE V2
Web Security:
Web-based security protocols are used to provide for secure transactions between Internet users and Web sites.

Types of threats on the web: Integrity threats, confidentiality threats, denial of service threats, and authentication threats.

Firewalls:
A firewall is a device through which the traffic going in each direction 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.

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 is immune to manipulation.

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 and destination transport-layer address, IP protocol field, and interface.
   - Packet filtering firewalls protect against IP address spoofing, Denial of Service attacks, and trojan, fragment, attacks.
2. Stateful Inspection Firewalls — A traditional packet filter makes filtering decisions on the individual packet basis and does not take into consideration any higher-level context.

Companion
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 function performed by an application-level gateway for certain applications.

---

**Application Proxy**

```
<table>
<thead>
<tr>
<th>Application</th>
<th>Transport</th>
<th>Internet</th>
<th>Network Access</th>
<th>Physical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

---

6. Trusted systems - A system believed to enforce a given set of attributes to a stated degree of assurance.

```
<table>
<thead>
<tr>
<th>Trusted system</th>
<th>Trusted OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote from untrusted computer</td>
<td>Has the following properties:</td>
</tr>
<tr>
<td>(1) Secure</td>
<td>has the following properties:</td>
</tr>
<tr>
<td>(2) Isolation</td>
<td>(a) Secure against Targen horse attacks</td>
</tr>
</tbody>
</table>
```

---

Packet Filtering Firewalls

Stateful Inspection Firewalls

Circuit-Level Proxy Firewall
Computex 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.

Need for Computex 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 or corrupted files from a system

Objective

Objectives of Computex 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, victim, and assess the intent and identity of the perpetrator

Stages of Forensic Investigation in tracking cyber criminals -
(1) An incident occurs in which the company's server is compromised
(2) The client contact the company's advocate for legal advice
(3) The advocate contracts an external Forensic Investigator.
(4) The Forensic Investigator prepares First Response of Procedure (FRP).
(5) The FI seizes the evidence in the crime scene and 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 file.
(8) The FI examines the evidence file for proof of a crime.
(9) The FI prepares investigation reports & concludes the investigation enables the advocate to identify required proofs.
(10) The FI handles sensitive report to the client in secure manner.
(11) The Advocate1 examines the report and might file charges against the offender in the Court of law.
(12) The FI usually destroys all the evidence.

**Key Steps in Forensic Investigation**

**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 five stages:

1. Preparation - Create a policy, develop forensic procedures
2. Identification - It involves validating, identifying and reporting the incident
3. Containment - Limit the extent and intensity of the incident
4. Investigation - Investigate further to uncover the cause of the incident
5. Recovery - Determine course of action, restore systems, integrity of the source
6. Follow-up - Post-mortem analysis, forensic techniques, cost analysis

**Hacking**

It is the gaining of access (wanted or unwanted) to a computer and viewing, copying, or deleting data (leaving a trace) without the intention of destroying
data or maliciously harming the computer.

Class of Hackers -
(1) Black Hat - Individuals with extraordinary computing skills, venting to malicious or destructive activities, also known as crackers.
(2) White Hat - Individuals profiting hacking skills and using them for defensive purposes, also known as security analysts.
(3) Gray Hat - 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 facing 30 years in jail for their actions.

Footprinting -
It is the blueprint of the security profile of an organization, undertaken in methodological manners 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 fortune of an entity.

Scanning -
It is one of the three components of intelligence gathering for an attack. It mainly scans for hosts, networks, and vulnerabilities.

The attacker needs 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 stack. 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 services running/listening on the target system.
5. To discover the IP address of the target system.

**E-mail Spiders** -

Get useful web pages on the Internet and extract e-mails that are later stored into a document or database.

**Table - 1st E-mail Address Spiders, Web-data Extraction**

**Overview of System Hacking Cycle**

```
ENUMERATE

CRACK

ESCALATE

EXECUTE

HIDE

TRACKS
```
Step 1 - Enumerate Users - Extract user names using Win2K enumeration and SNMP tools.

Step 2 - Crack the passwords of the users and gain access to the system.

Step 3 - Escalate Privilege - Escalate to the level of the administrator.

Step 4 - Execute Malicious Code - Plant keystrokes, figure, and code on the machine.

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

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