Cyber security

VB = flaw

flaw → whose → system → causes → data leak / breach / exploited

→ easy access to hackers.

Types of VB scanning:

① Internal : done → inside the network

Using → Privilege escalation.

eg. how well permissions are implemented ⟹ VB's that attacker can use to access servers.

② External : Scan → who → online assets.

eg. employee login pages, remote access ports.

→ this scan can tell how strong a company's front side is.

③ Application based :

↳ focuses on : specific segment of company

done on

↳ IoT devices or wireless networks.

helps — non technical staff to understand and correlate the VB's with risk to buisness op^n.

④ [redacted]

④ Continuous VB scans :

↳ used to scan networks regularly ..

↳ scanning inside & outside networks.

⑤ Authenticated scans

↳ allows scanner to directly access network based assets using SSH and organization provided credentials.

⑥ Non / Unauthenticated scans :

↳ can be performed remotely

↳ has few testing tools

↳ used for getting hackers perspective.

Banner Grabbing:

→ aka **OS fingerprinting**

A method to determine the **OS** or **software version** running on a remote target system.

2 types : Active & Passive.

Active BG:

1. **Specially crafted** packets are sent to the remote os and the responses are noted.
2. The responses are then compared with a database to **determine** the OS
3. Responses from different OSes varies **due to** differences in **TCP/IP implementation**.

Banner Grabbing is also used for retrieving that on the open port which services are up and running.

Passive Banner Grabbing:

(1) By error messages:

↳ they provide
- TYPE of OS
- TYPE of SERVER
- SSL TOOL USED By system.

(2) Sniffing the traffic:

→ Capturing and analyzing packets from the target enables an attacker to determine OS

(3) From page extensions:

→ looking at the URL extension may assists you in determining the application versions.

eg. .aspx = IIS server and window platform.

Command:

```
nc www.cyx.com 443
```

BCe via nmap :

In nmap we have a "script named "banner" foo BCe

To use it we just need to write

" --script = banner "

Command :

```
nmap -p22 --script=banner 192.168.0.1
```

Checks if port 22 is open?

if open : how many IP are up?
what type of connection?
what type of server:

In short all of the BCe stuff.

Overview of VB scans

(1) false negative:

⇓,

VB exists but scanner doesn't report it as vulnerable.

(2) false positive:

VB doesn't exists but scanner reports it as vulnerable.

VB scans steps:

(1) Network scan ⇒ identification of live hosts that responds to traffic

(2) Network probes ⇒ determine the host OS

(3) Enumerate services available on the host.

(4) Identify details about each service.

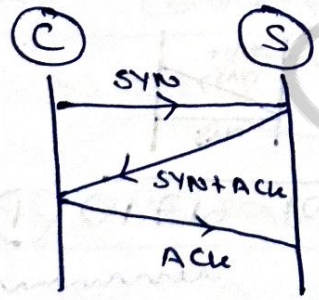
3-way handshaking:

When conn^xn is established,

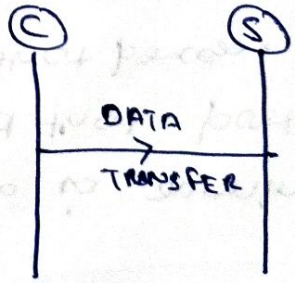
1. Client sends a request on server
2. server accepts it and send acknowledgement.
3. Client start sending data
4. Completion of data transfer make a conn^xn release request on server.
5. server accepts it and send acknowledgement.

3 main parts:

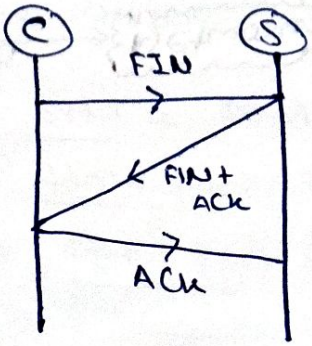
(1) conn^xn establishment:



(2) Data transfer:



(3) conn^xn release:

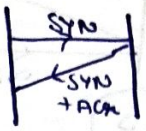


* Port scanning:

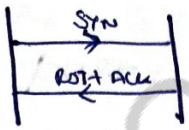
A port scanner.

3 responses:

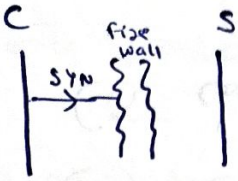
① OPEN PORT: if any process is running on a machine and that port is assigned to that process.



② Closed port: if you send a "SYN" packet & recieve "RST+ACK" packet that means port is closed



③ filtered port: filter ports has firewall embedded in it which makes the server secure if unknown requests are made.



Some services like "Telnet" is insecure
↳ can leak passwds less encryption.

→ services don't always run on default ports.
∴ scanner rely on banners and nudges.
↳ to elicit a response from a listening port.

Command: nmap <port number>

→ nmap -ST <port number> (TCP connect scan)

→ nmap -SS <port number> (Stealth scan)

3 types of TCP scans:

① TCP connect : 3 way handshake
↳ aka (full scan)

② TCP SYN scan: Half open scanning
① (SYN) is sent
② listener responds with (SYN + ACK)
③ non listener responds with (RST)

③ TCP FIN scan: (To find closed ports)
① SYN is sent
② Close port reply (RST)
③ Open port (ignores)

HTML injection:

↳ Some VB's are only suspected if we try the payload execution.

↳ and one of that type is (HTML injection)

in this, HTML form is given input in any form of payload

eg. in the search bar of some site we can search for xss vB by searching with keyword "<xss>" in search bar.

Port scanning techniques:

1. TCP connect scan
2. ARP scan: shows every IPv4 device on network.
3. SYN scan: SYN ⟶ SYN + ACK
4. FIN scan: FIN ⟶
5. ACK scan: filter ⟶ ICMP; unfilter ⟶ RST
6. FTP Bounce scan: Attacker hide behind FTP server.
7. TCP NULL scan: discard → open; RST → closed
8. TCP UDP scan

* Open VAS :

↳ Open **Vulnerability Assessment System**

- → managed by **Greenbone**.
- → classify 1st system resources.
- → innumerates values to the classified resources.

↳ detects VB in **each resources**.

↳ eliminates VB on priority base

It provides various service and tools for vulnerability assessment.

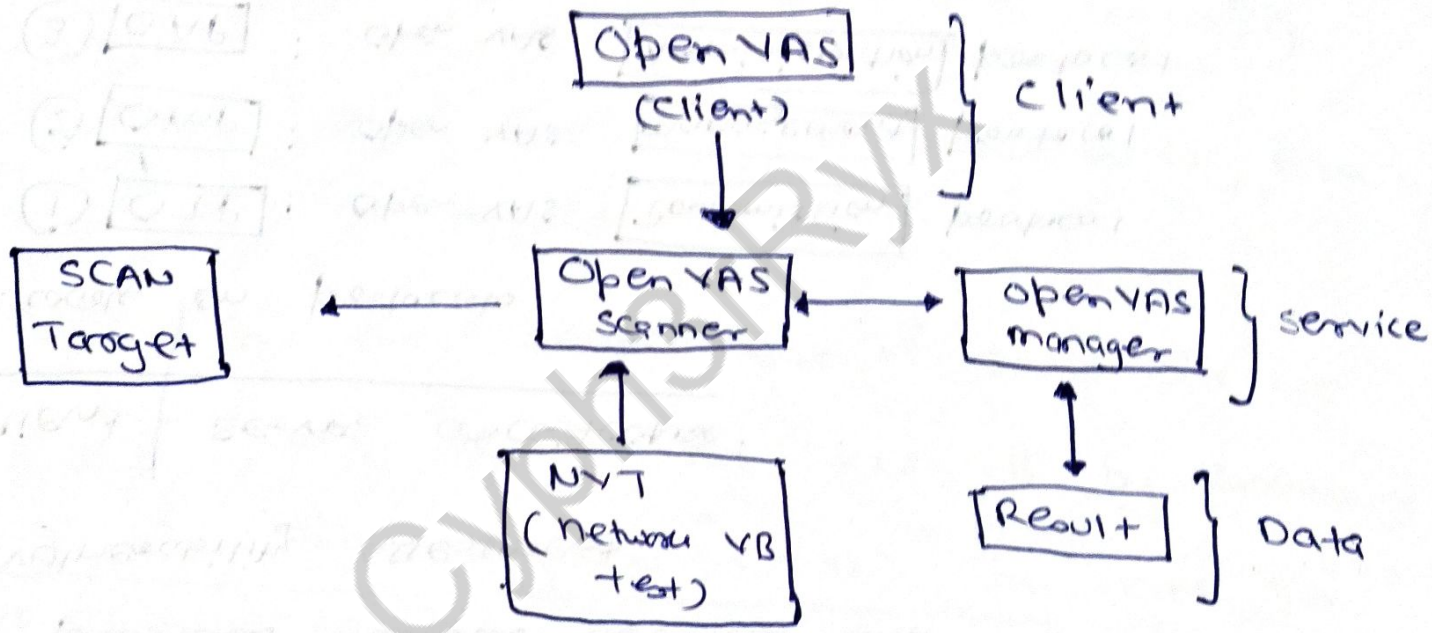
Client - Server architecture :

↳ works on protocols

1. **OTP** : Open VAS **Transmission** protocol
2. **Omp** : Open VAS **management** protocol
3. **OAP** : Open VAS **Administration** protocol

3 layer architecture:

1. Client layer
2. Service layer
3. Data layer

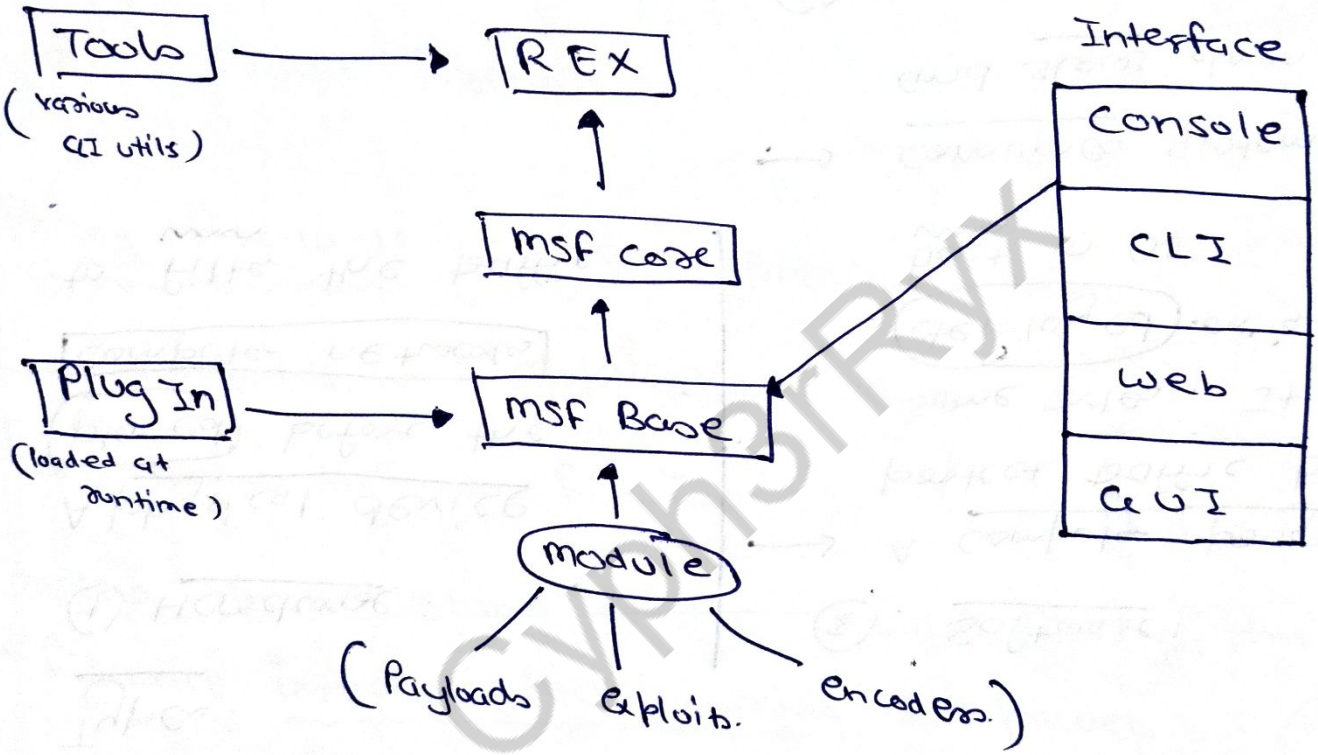


* **Metasploit** : (actively exploiting a vb to verify its existence)

↳ a complete framework rather than a single tool

↳ ruby based platform.

(fxn): enables users to write, test & execute exploits.



Rex: formatting and establishing a socket conxn.

msf core: defines the framework and provides basic API

msf Base : Provides simplified API

modules: The scary stuff / useful stuff.

① What is firewall?

⇒ A networking device to protect incoming & outgoing traffic from network. based on set of rules.

Types:

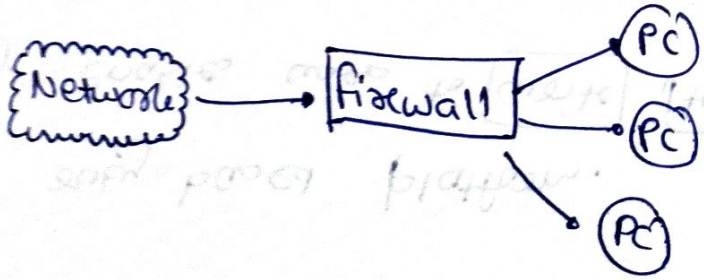
① Hardware:

A physical device placed before the Computer networks to filter the traffic

② Software:

→ A computer program to protect traffic based on some rules. It can be deployed on a particular host in OS.

∴ → Consumes system resources and slows down system



(2) Types of firewall based on deployment.

(i) ~~Proxy firewall~~

(ii) Software firewall

(iii) Hardware firewall

(iv) Cloud firewall

Proxy firewall : aka Application level

↳ operates on application layer

↳ same fxn as firewall

- rather than letting traffic connect directly, the proxy firewall inspects the incoming data packets.
- The inspection can go deep and it actually checks the (content) of the packet to ensure no malware
- once check is completed, packet is (forwarded).

Advantage : create additional anonymity & protection.

Software & Hardware firewalls are discussed earlier.

Cloud firewall: firewall as a Service (FaAS)

↳ Considered synonymous with proxy firewalls by many.

↳ easy to scale and additional capacity can be added.
↳ to filter larger traffic

↳ excels at perimeter security.

③ Types of firewall based on methods of operations:

(i) Packet filter

(ii) Circuit [redacted] firewal

(iii) Application [redacted] firewall

(iv) Stateful [redacted] firewall

(v) Next gen [redacted] firewall

Q.4 Stateful or stateless firewall

⇒ Stateful firewalls: (inspects everything inside data packet and than passes it through)

→ Combines both packet inspection technology and TCP hand shake

→ creates a level of protection that surpasses both packet filter and circuit level architecture

Main disadvantage:

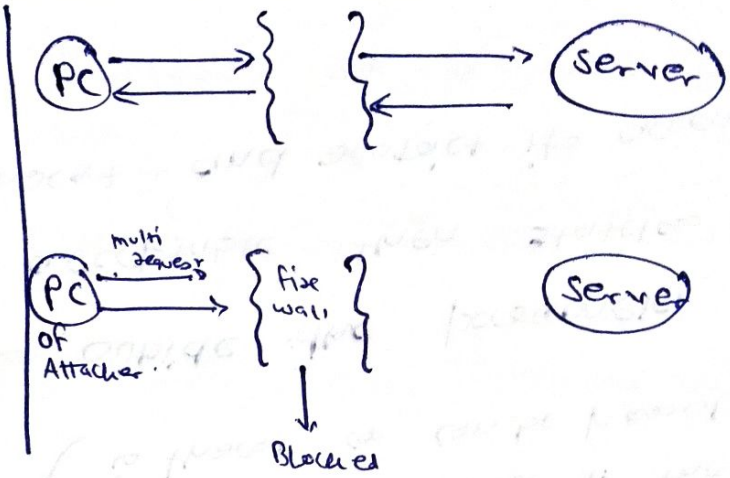
1. Uses more computer resource.
2. Slow down the transfer of packets.

Stateless firewall: (make use of data packet's source, destination to know if the data is threat or can be passed)

If data packet goes outside the parameter of what considered as acceptable then stateless firewall will identify it as threat and restrict its access.

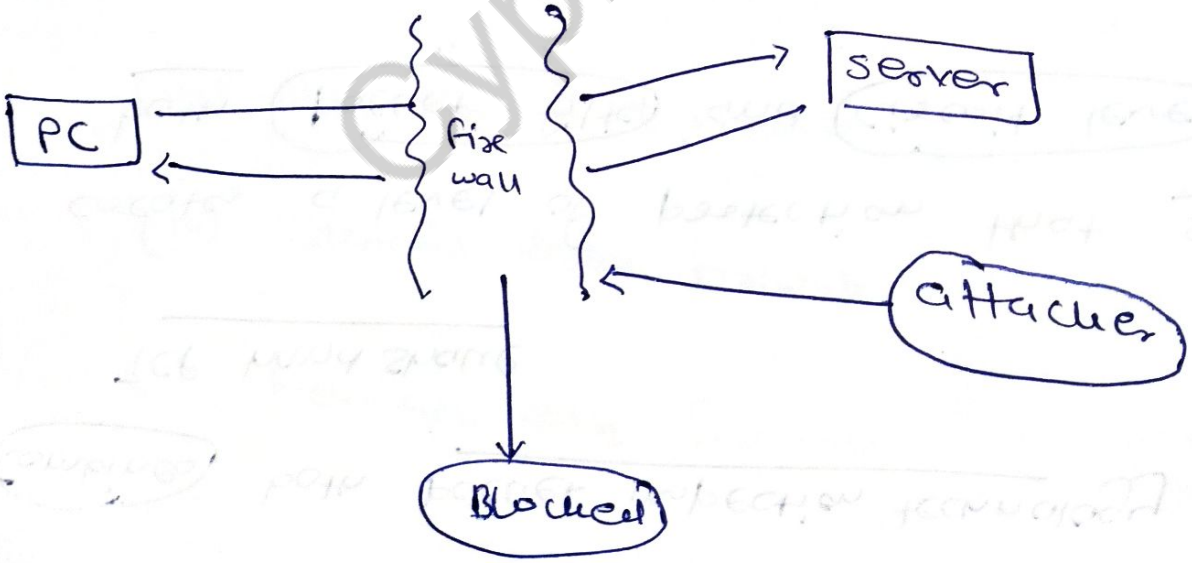
Advantages:

- ↳ fast
- ↳ Cheaper
- ↳ handle heavy traffic



Statefull firewalls have some advantage also:

- ↳ wider logging capacity
- ↳ lesser use of ports
- ↳ powerful memory to retain key aspects.



(Statefull firewall)

Q.5 Packet filter

⇒ oldest and most basic firewall

Creates a Checkpoint → Where? → at traffic router or switch

Simply checks the data packets w/o opening them.

Port no., type, source

if data packet passes inspection = allowed
" " doesn't " " = dropped

Benifit :
- less resource consuming
- simple to use
- good system performance

Disadvantage :
- easy to pass
- less protection than other architecture.

0.6 Circuit level

↳ another simple firewall

↳ passes / denies traffic w/o consuming too many resources

↳ works on TCP handshake verification.

⇓

designed in such a way that it make sure that packet is legitimate.

Benifit :
- less resource consuming
- fast
- light weight.

Disadvantage :
- doesn't check the whole packet
- if packet has malware and if it passes 3 way hand shake then it will allow packet to go forward.

Q.7 Application Layer :

↳ A type of firewall that search, monitor, control } network web & local services

→ Operates at application level

only filter traffic with regards to the application or a service for which they are intended.

eg. A firewall setup just for monitoring the traffic to all the web applications your network uses.

* Next Generation firewall :

↳ latest and most updated firewall architecture.

includes all the older functions & new fxns too

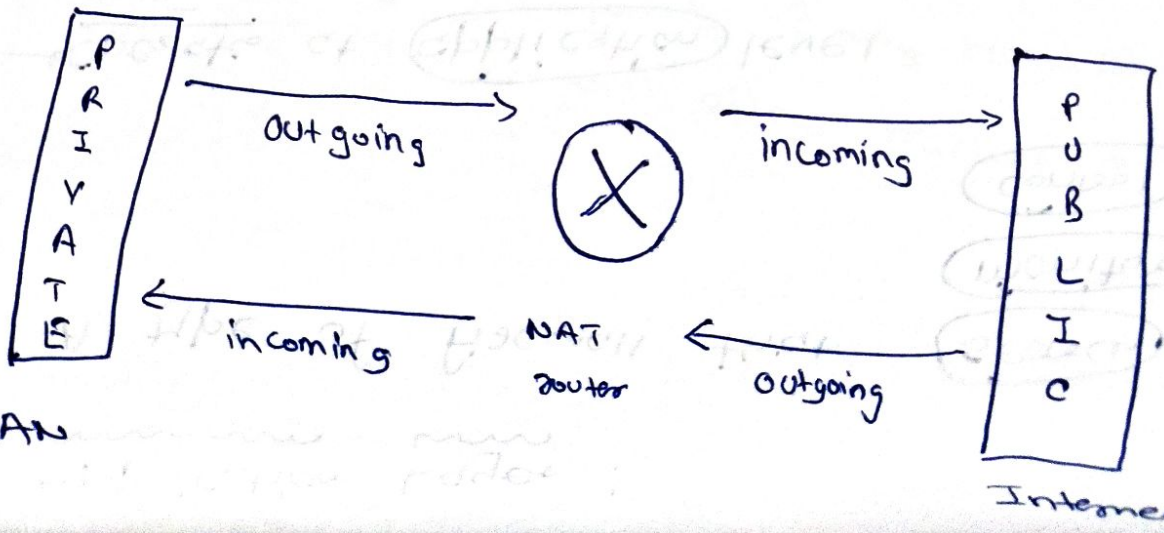
- older functions → TCP Hand shake, surface level inspection, deep level packet inspection
- new fxns → IPS, IDS & automatic stop attacks

10.8 NAT (Network Address Translation)

- designed for **IP address conservation**
- method to connect multiple PC to internet by using only one IP address
- enable **private IP networks** → that use unregistered IP address

Operations:

NAT operates on router & translates the private addresses to legal addresses before forwarding packet



Q.9 IDS & IPS

⟹ "A process of analyzing the flow of events in the networks and monitoring them until any event breaches the policies and pose itself as a threat to your networks."

Intrusion Detection System: (IDS)

↳ A system just to administor the flow of data traffic and events

↳ any unusual threat seen in the flow is then reported as a potential threat toward the networks.

The main disadvantage is that it can't do any further to stop the threat or eliminate it but it just only detects it.

Intrusion Prevention System (IPS):

- It does removes the disadvantage of IDS and makes it a advantage.
- IPS not only detects and administer the flow of data in the networks but also takes an action on that threat detected in the flow.
- IPS automatically rejects the traffic which donot meet the policies or is malicious by nature

Q.10 Port forwarding:

↳ A application of network address translation (NAT) that redirects a communication request from one address and port number combination to other, while the packets are crossing a network gateway.

↳ Ports are "open" and "close" in firewall, which says which type of traffic is allowed in/out.

↳ Port forwarding also allows computer of different network connects to a specific computer within LAN.

Assignment 4

Name: Rushi S. Padhiyar

Enrollment no.: 200303126026

Subject: CyberSecurity

Branch & Div.: CSE-CyberSecurity & 5B10

Q.1 Email Spoofing:

A spoofed email is one in which email header is forged so that mail appears to originate from one source but actually has been sent from another source.

- **Spamming:**

  Sending multiple copies of unsolicited mails.

- **Cyber Stalking:**

  Means following the moves of an individual activity over internet. It can be done with the help of many protocols available such as emails, chat rooms, etc.

- **Phishing:**

  A deception designed link to steal valuable personal data such as credit card nos., passwords, accountdata, etc.

- **Email bombing:**

  Sending large no. of emails to the individuals or company or mail servers to crash system

- **Salami attack:**

  A series of smaller attacks that together results into a larger attack. for eg. slicing fraction of dollars from each transaction.

- **Logic bombs:**

  A string of malicious code inserted intentionally into a program to harm a network when certain condn are not met.

- **Data diddling:**

  An attack that involves altering raw data just before it is processed by a computer and then changing it back after the processing.

Q.2

(I) Attack vector:

A path by which hacker gains access to a PC/server, in orders to deliever a payload or a malicious code.

Types:

(i) Email as an attack vector:

↳ Millions of messages can be sent out in hope that a large no. of people will be duped.

(ii) Attacks by deception:

↳ Aims at vulnerable entry point as a operator/user.

(iii) Attack by worms:

↳ Worms spread w/o the need for humans to open attachment

(iv) Heedless guest:

↳ Fake websites are used to dupe peoples.

(II) Classification of Cyber crimes:

(i) Cyber Crime against individual:

↳ Includes email spoofing, spamming, defamation, cyber harassment, etc

(ii) Against Property:

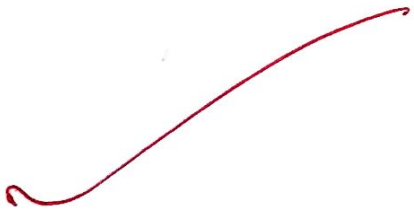
↳ Includes credit card frauds, internet time theft and intellectual property crimes.

(iii) Against organisations:

↳ Includes unauthorized access of PC, DOS, virus attack, etc.

(iv) Against Society:

↳ Includes forgery, cyber terrorism, web jacking, etc.



Q.3 (I) Data destruction & contaminants:

Data destruction:

↳ A process of destroying the data stored on tapes, hard disks and other forms of e-media so it is completely unreadable or unaccessable.

Data Contamination:

↳ The alteration of data in a PC system.

↳ Contamination of a computer can also occur when malware infiltrates it.

5 most commonly culprits of data loss:

1. Power outage
2. Virus, malware or attack
3. Natural disaster
4. Human Error
5. Malfxn.

(II) Indian Act IT 2000:

- Important law regarding to cyber laws of India.
- Aims at promoting E-commerce and e-governance.

Objectives:

- To get legal recognition to transactions by electronic ways or by internet.
- To provide the facility of filing document online
- To grant legal recognition to digital signature accepting any agreement via PC.
- To authorize any undertaking to store their data in e-storage
- Authorize banks and other financial institutions to execute transactions.
- Allowed to store web info in a central DB / hub.
- Approve lawful recognition through authorization codes to all the business deals via PC

07-09-22