Cyber Security: Class-1

1). Cyber Kill chain Concept.
2). Information Security control.
3). Information loss and standed.

1). reconnesisms → Webpanization → Delivery → Expatation → Command and control → Target Achievent.

RECONNAISSANCE :- Research, Identification, Selection of targets.

WEAPONIZATION :- Pairing remote access with explot into a deliverable payload [Ex: MS Worle

DELIVERY :- Transmission of target eg:- Email, USB, attachment).

EXPLOITATION :- delivered the Weapon's code is triggered explating vulnerable applicatim or Systems.

INSTALLATION :- The Weapon's install backdoor on a target's System allowing axcess.

COMMAND AND CONTROL (C&C) :- The interpets Weapon's providing inside the target's network.

ACTIONS ON OBJECTIVES :- The attacker makes to achieve their objective (Ex: destruction of data, introduction into the target).

SECURITY CONTROLS :-
Compliance control, Techinacal control, Profedional control, Access control, Physical control

PHYSICAL CONTROL : Stoping other axcess.
ACCESS CONTROL :- Controling axcess.
PROCEDURE " :- Detail of all.
TECHINACAL " :- Web side → Strong.
COMPLIANCE " :- Process in all the ways.

PREVENTS ATTACKS :- Application → True or False pack updates in that apps, don't use unwanted ~~software~~ application want to be in hand, password change.
Admine prevalag don't give to all
OS update → OTP
Data Backup → Hacked means

CYBER AUDITS :- Tracking unwanted things like apps and etc...
① → Establish security standards
② → Determine the security postures
③ → Enforce Regulators and best practices.

INFORMATION SECURITY LAWS AND AUDIT STANDARDS :-

Class-2, PROFESSIONAL.

FOOT PRINTING, ENUMERATION, VULNERABILITY ANALYSIS
Step by step Addition table
Process information
collecting target DNS
and networks SNP, SIP
Social engineering, RTP
Foot Printing, Database
Informational track network
call, Business loss. bloss.
PASSIVE FOOTPRINTING ↔ Active FOOTPRINTING
Direct attack not Call attack, emai
but Indirect attack etc., OTP.
A, MX, RECORD.

SCOPE OF CYBER SECURITY EXPERT VULNERABILITY ANALYSIS :-
Vulnerabuity Identify, Risk accessment, analysis, solution.

Date
Page

class-3

System Hacking :- One virus to another virus attacks in computer. [Ex:- Hacking]
5 types :- computer axcess → Virus → active → all detail collecting.
GAINING axcess, ESCALATE ACCESS, EXECUTE APPS, HIDE YOUR APPS, COVER YOUR HACKS.
Keyloggers → password saved can as Hacks.
Rootkits → hardware Hacking.
Alternate data streams → one app to another app. → clean your path.
Malware → Distrub another computer.

class-4

An Application → Web server
APHOE → Micro soft
XSS → Cross Site Scripting.
IL → Information leakage
WA → Weak authentication
CSRF → Cross Site Request Forgery
NOT VALUDATING UNTRUSTED DATA.
SQL INJECTION.

Origin of Cyberspace:-

"Cyberspace" derived from the word Cybernetics. 1940, 1960 and 1984
Electronic Frontier Foundation (1990)
Mr. Benedict (1991)

Levels of Cyberspace:-
Core Cyberspace.
→ Electronic devices, Transmission or connecting medium
→ control codes, operation codes, Software, Data exchange.

The Extended Cyberspace.
→ It is an remote access.

COMPONENTS OF CYBERSPACE:-
6 major element
→ Physical infrastructure and Telecommunication devices
→ Computer System and related Software.
→ Networks connecting computer System and devices.

→ Network of Network or internet.
→ User and intermediaries accss .Nodes
→ constituent Data.

3 Layers
→ Physical layer
→ Logical layer
→ Cyber personal layer.

Cyber Domin Chooracteristics :-
→ interconnects a wide range of system. All these elements are not physically present in one place.
→ connected virtually diffient but they appear as a single.

Ambiguity :-
its virtual nature and lack of physical existence and absolutely no centralized mechanism.

Interactivity :-
All communication and data sharing occur seamlessly through this medium.

Factors influence Diving forces of cyberspace.
Time
Space
Anonymity.
Asymmetry.
Efficiency.

Advantages of cyberspace :-
→ Informational resources
→ Entertainment
→ Social network.

Disadvantages of cyberspace :-
→ HACKS.
→ Crimanal activities.

Internet is an interconnected network. WWW data exchange

Definition of cyber security.

Cyber security is a technology framework that consists of various procedures and operations intended to defind networks, computers, programs and data from outbreak damage or illegal access.

Application security → Information security → network security → IDS Intrusion Detection System and IPS Intrusion Prevention System → Disaster Recovery → Operational security → End - user - Edution (X)

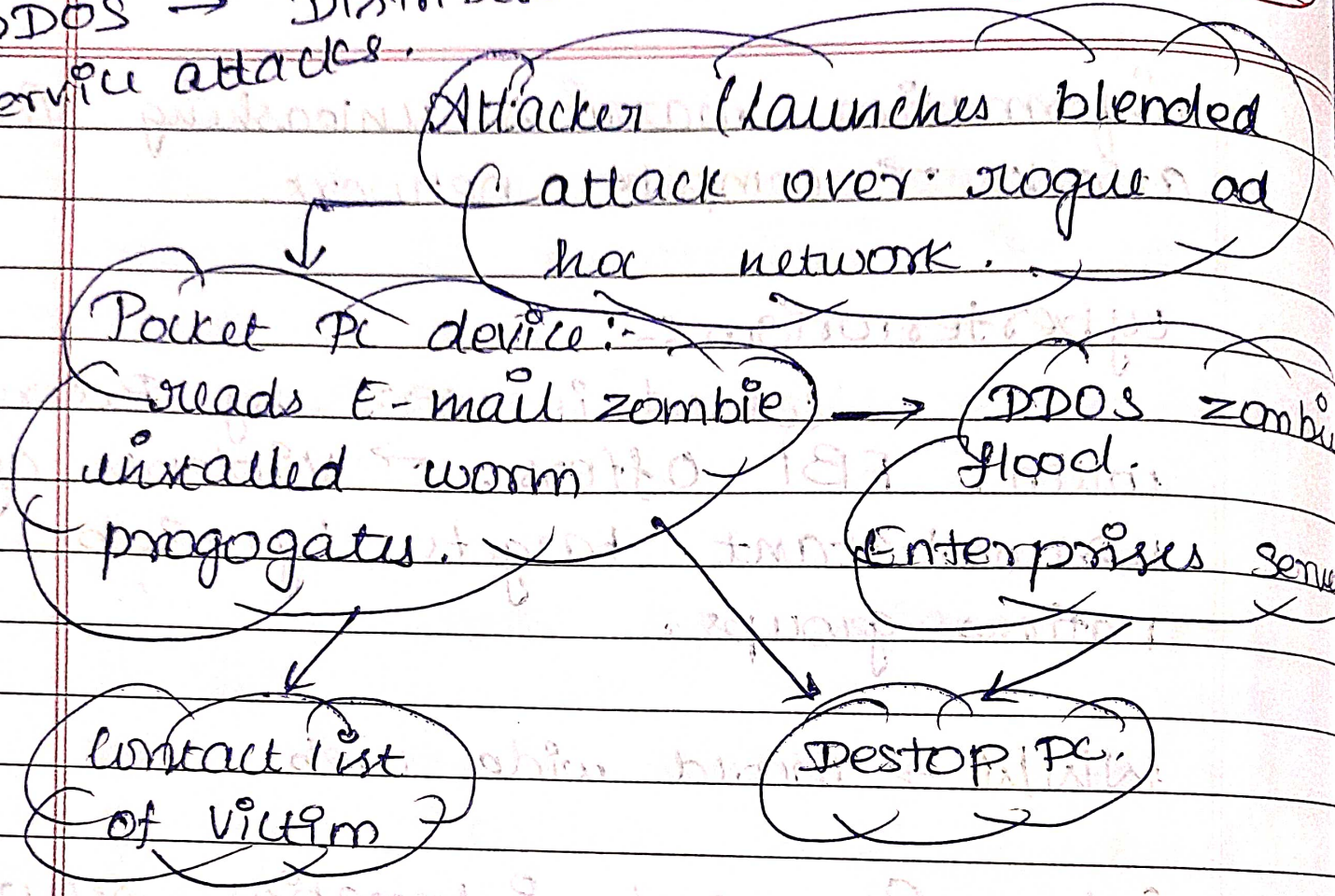
NIST → National Institude of Standards and Techology.

Types of cyber threats
→ IOT (Internet of Things).
→ Data Proliferation

1) ATTACKS ON CONFIDENTIALITY
* Stealing, or rather copying, the target's personal information

E-mail → Electronic mail.

DDOS → Distributed denial-of-service attacks.



IPC → Indian Penal code.

IPC section 499 → Email link. Froud.

EMP → excessive multiple posting.

Hacking person do for many purpose. Greed, power, revenge, destructive mindset.

Children's Online Privacy Protection Act or (COPPA) → Cybersitter.

Cybercrime Investigation Cell of India defines Software piracy.

E-Mail Bombing / Mail Bombs :-
→ It refers to sending a large number of E mail server crash.
→ Terrorism has hit the internet.

Usenet Newsgroup as the source of cybercrimes :- → distributing information. illegal or harmful content.

Computer network Intrusion :-
→ Mainly hackers are used Games for hacking the data. eg :- "War Game", login Id and password.

Password Sniffing :-
name, password, network and log in Id will be recorded.
password "cracking".

ITU → International Telecommunication Union.

Date
Page

Credit Card Frauds, Identity Theft Era. Data security:

Cybercrime is a way is the outcome of 'globalization'.

Cybercrimes:- An Indian perspective:-
India has the fourth highest number of Internet users in the world.

Indian Law: Hacking: implement in 2000
ITA Act in 2007, IPC 339

Sec - 43 → Damage to computer system → punishment: ₹1 Crore

Sec - 66 → Hacking computer system → ₹2 lakhs to 200,000 and 3 years jail

Sec - 67 → Publishing information obscene in electronic form → ₹1L to 100,000, 5 years jail.

→ (Council of Europe's)

COE's (Cyber Crime Treaty)

classmate Date Page

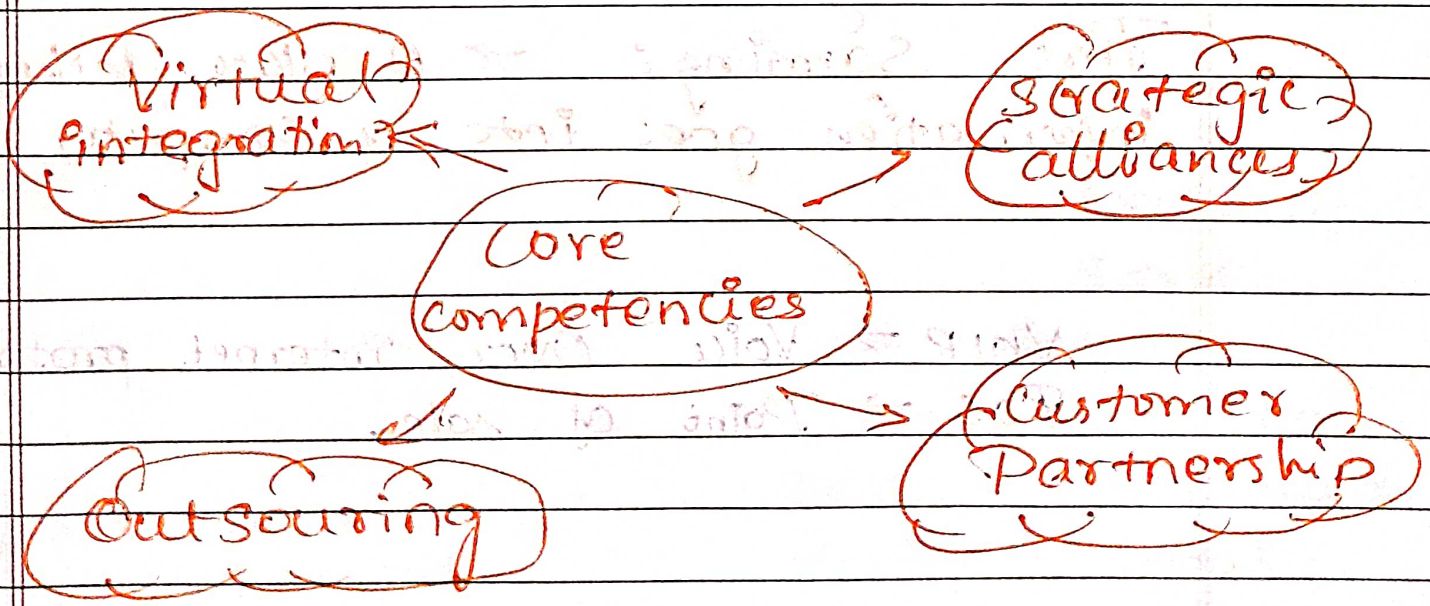
Sec - 68 → Not complying with directions of Controller → ₹ 2 lakhs → ₹200,000) → 3 years

Sec - 70 → Protected system → Imprisonment up to 10 years.

Sec - 73 → false certificate → ₹1L to 100,000 and 2 years. or both.

Sec - 72 → Confidentiality and Privacy → ₹1L to 100,000 up to 2 years.

Sec - 74 → fraudulent purpose → 2 years → ₹1L to 100,000.



Cyberoffenses:- Criminals plan them.

Ch-2

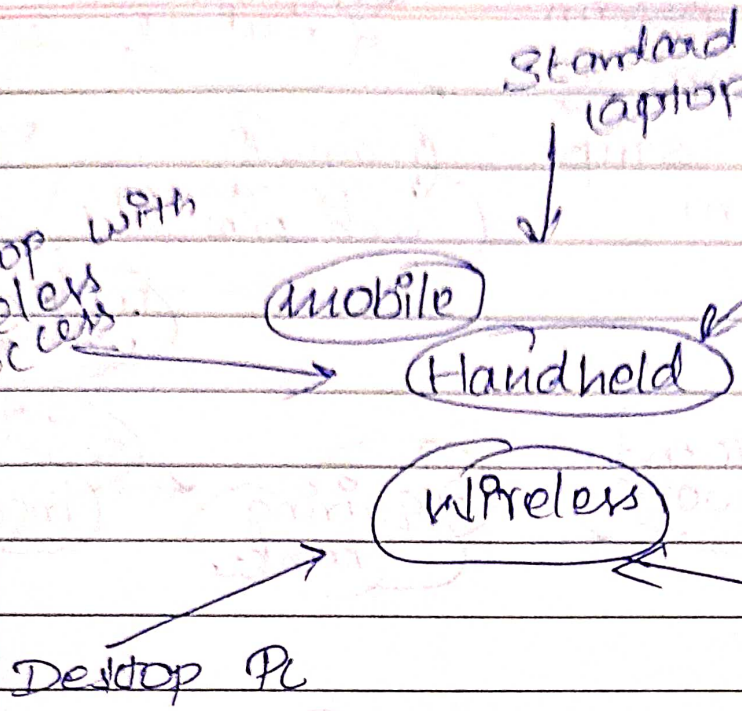
RAS → Remote access servers.
PDAS → Personal digital assistant
MAC → Media access control.
ARP → Address resolution protocol.
ICMP → Internet control message Protocol.
TTLS → Tunneled transport layer security.
IPS → Intrusion prevention system
NIDS → Network based intrustion detection system.
IANA → Internet Assigned number authority.
IABt → Internet Architecture Board.

Port Saming :- → A place where information goes into a computer.

VOIP → Voice Over Internet protocol.
POS → Point of sale.

Cybercrime: mobile and wireless devices.

Ch - 3



PDA → Personal digital assistant

□ → mobile device.

△ → Wireless device.

○ → Handheld device.

Mobility types.

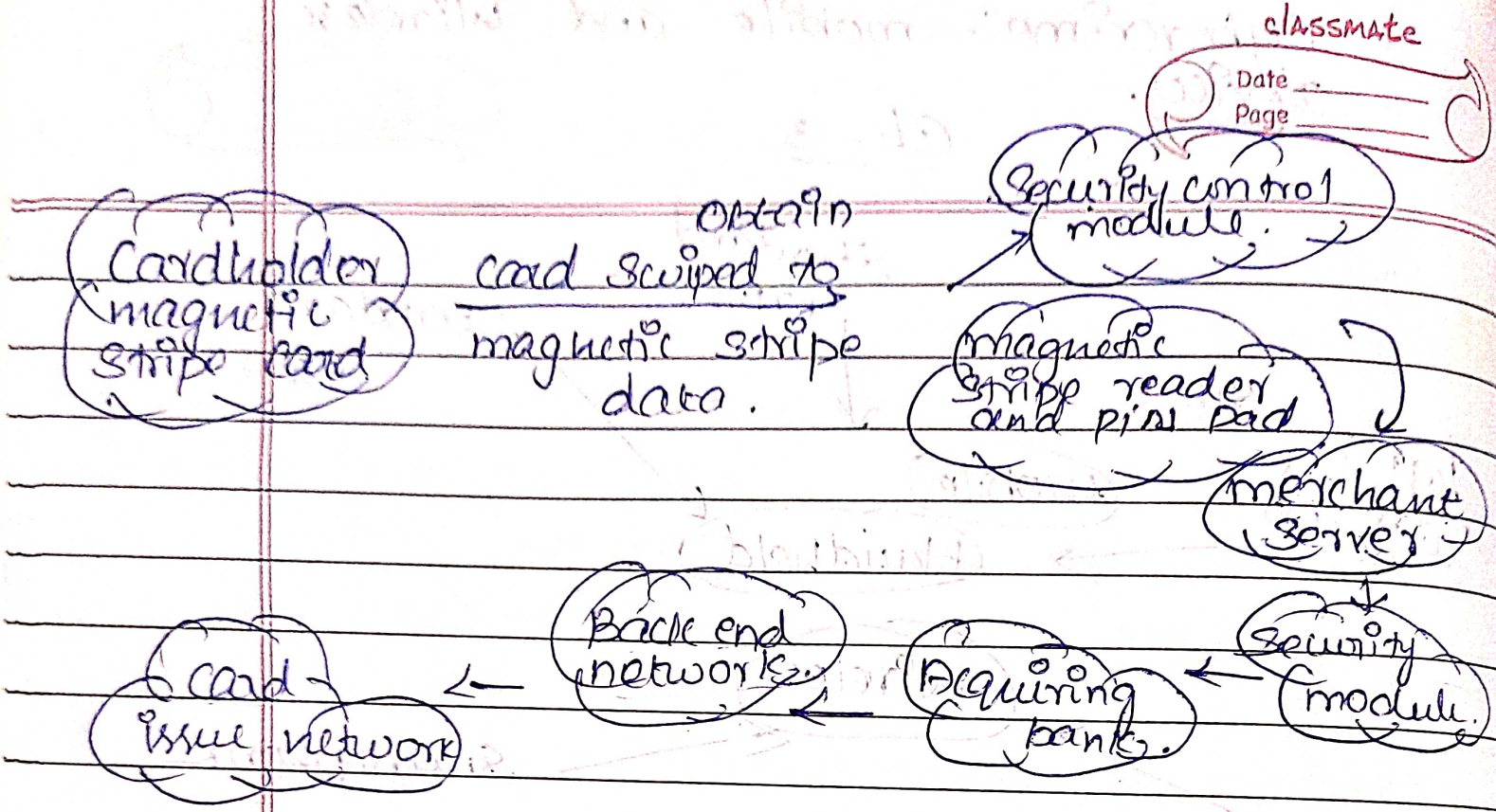
- User mobility
- Device mobility
- Session mobility
- Service mobility
- Code mobility

Virtual provite network. (VPN).

Dos → Denial of service.

ISP → Internet Service providers.

DDOS → Distributed denial of service.



PII → Personally Identifiable Information.

merchant → Bank. → Reject transaction.

↑

yes = Approve transaction.

Individual card holder. Using cell phone for credit card transaction.