CS Unit 1 :

Q1]. Basic network utilities :

⇒ 1> IPconfig.

- Info about network, ip address
- Network configurations
- ipconfig /all gives all info like name of computer, MAC, ip addr, etc

2> Ping.

- Sends a test / echo packet to find if machine is reachable
- Finds how long packet takes to reach the machine.
- Tells how packet was sent & returned.

// ping www.google.com ← Windows / Linux

3> ~~Tracert~~ Tracert.

- It is advance version of ping.
- Additional to all ping function, it also tells all intermediate hops to get there.

// tracert www.google.com ← Windows
// traceroute www.google.com ← Linux.

4> Netstat.

- Shortcut for network status.
- Tells the connections of computer.

5> NS Lookup.

- Shortcut for name server lookup.
- Used to connect your Network's DNS server.
- often used to verify whether DNS is running

6> ARP

- used to map ip address to MAC address. currently a device is aware of.

// arp -a.

7> Route.

- used to view IP routing table.
// route -print 4.

Q.2] Various Types of Threats.

⇒ ① Malware:

- Sw that has malicious purpose = Malware.
- Includes virus, worms, adware, Trojan Horse, Spyware.
- Most used type of attack & danger to system.

② Security Breaches.

- Breaches the security in attempt to gain access to unauthorized data.
- Cracking password, elevating privileges, breaking into server.

(3) DOS attack :

- The hacker blocks access of legitimate user.
- Floods the target server with false conn°.
- It is common & most easy.

(4) Web Attacks :

- Attacks the website.
- Locates interactive part of website & attempts to trick server to run commands.

- SQL injection
  - Websites that use relational db like SQL, communicates often with their db.
  - An SQL command through any website's input may risk the db like modify, delete etc.
  - It can also bypass login screens.

- Cross - Site Scripting.
  - It involves entering data other than what was intended.
  - The attacker finds some area of website that allows users to type text that others can see.
  - Then attacker injects client-side scripts. like fake link, redirecting, etc.

⑤ Session ~~Hic~~ Hijacking.

- Attacker monitors authenticated session.
- Can read authenticated data from packets header, gain userid, pass, other info, etc.
- Most complex type of attack.

⑥ Insider Threat.

- A person who has access to data, misuses & steals / compromise security.
- An employee of company, ...

⑦ DNS poisoning:

- The DNS www.google.com translates to an IP address 192.168.43.1 ....

- DNS poisoning makes translation wrong, & it redirects to illicit site to steal info of user.

- Phising is one example.

Unit 2.

Q.1] Trojan Horse.

→

// Explain the "fall of Troy". :=)) .

- It is a type of ~~xxxxx~~ malware.
- A term for program that looks good from outside but has malicious purpose.
- It can also be attached to a email as a script.
- Or it can be in a pirated game or any other contents.
- When we open the program or email attachment, the Trojan Horse might do the following -
  - ~~Downdo~~ Download harmful s/w.
  - Install spyware.
  - Delete files.
  - Open backdoor for hacker to use.
- If hacker wishes to spy on certain individual, a TH can be crafted especially for an individual.
- Creating TH doesn't require programming skill. Free tool can be used like 'EliteWrapper'.

Q2] How to protect yourself against cybercrime?
ff
protect against Investment fraud & Identity Theft.

=) • ① Protecting against Investment fraud.

- Only invest with well known brokers.
- If it is too good to be true, avoid it.
- Why would complete stranger share incredible investment opportunity to you?
- Never invest that you can't afford to lose.

② Protecting Against Identity Theft.

- Don't reveal anything about yourself
- Don't ~~Keep~~ keep transactional details's documents.
- Check your credit frequently.
- Check browsing history frequently.
-

③ Secure Browser settings.

- https.
- Trusted website
- delete history / saved passwords. / cookies.
- Avoid trackers
- Avoid pirates.

④ Protecting Against Auction Fraud:

- Use reputable auction sites eg: ebay.
- If sounds too good to be true, don't bid.
- Read feedback.
- Use different credit card with low limit.

⑤ Protecting Against Online Harassment.

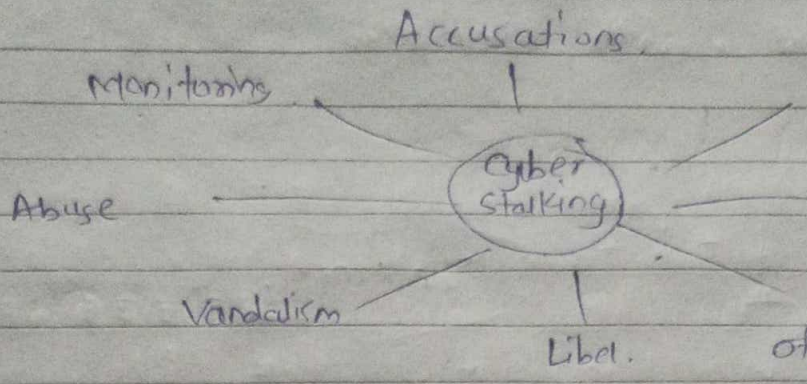
- If you use chat rooms, discussions, don't use real name.
- Set up different email / no.

- If you are victim of harassment, keep emails in both digital & printed format. Evidence too in printed format.

- Don't ignore cyber stalking.
  19% of cyber stalking escalated to stacking in real world.

Q 4] Concepts of cybet stalking.

- A type of crime that uses internet & technology to harass / stalk a person.
- Stalkers take advantage of anonymity afforded by internet.



1] Direct cyberstalking.

- Email flooding.
- Constant text.
- Attacker is ~~vulnerable too~~. not hidden.

2] Indirect & cyber stalking.

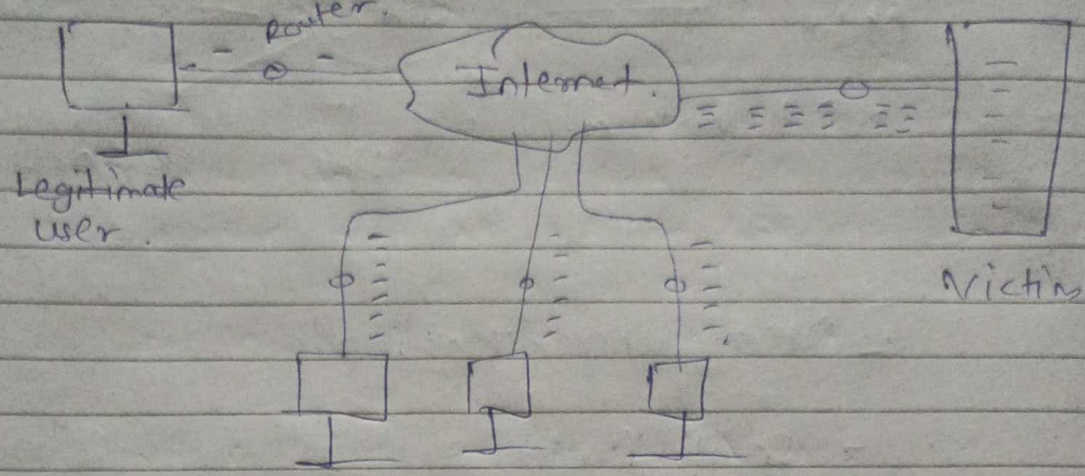
- Damage victim's device by inflicting ransomware
- Install virus to monitor behaviour & / or steal data.

Types of cyberstalking.

// Shortcut: CIMSHIT.

1. Catfishing // fake profiles.
2. Monitoring social media.
3. Spying via G. Maps & G. Street View.
4. Hijacking webcam.
5. Installing stalkerware.
6. Tracking location with geotags.

Q5. DDos with example.



// Explain.

- Signals of DOS attack:
  1> Degradation in n/w performance.
  2> Specific website unavailable.
  3> All websites are inaccessible on the n/w.
  4> High volume of email spam.

- Prevention of DOS attacks.

(1) Protect your IP address.
(2) Use a VPN.
(3) Beware of Phishing.
(4) Update apps & security softwares.
(5) Install antivirus s/w.

Q6] How to detect & eliminate virus, spyware.

⇒ (1) Antivirus s/w.

- Antivirus works in two ways:
  i) Looks for a sign. or pattern that matches a known virus.
  - Hence keep it updated to have most list of sign.

  ii) Scans behaviour of executable file for suspicious activities like:
  - Attempting to copy itself.
  - Attempting to access address book of system's email program.
  - Attempting to change Registry settings in Windows.

- famous antivirus s/w:
  - Norton,
  - McAfee
  - Avast
  - AVG
  - Malwarebytes
  - Windows Defender ← Most powerful.

(2) remediation steps.
- Run antimalware s/w. · Host based & n/w both.
- To avoid,
  - see if attachment is expected in email.
  - too good to be true emails should be avoided.
  - Generic sound like "Here is your doc" ↓
  - Ask technical supports beforehand.

Q7). What is Malware?

=).

- S/w intentionally designed to cause : damage to computer, server, client, or n/w.
- Delivered in form of link / file over email & requires user to click on link or open the file.
- Since early 1970s ... .
- First malware = Creeper Virus.

- Types of Malware.

(1) Computer Viruses.
- Replicate itself. (need human interaction)
- freq. pop ups, crashes, slow performance.
- eg: Melissa, 'I Love You'.

arrive through emails

(2) Worms
- Copies without human interaction.
- Takes free space of drive.
- Doesn't modify program like virus.
- eg: Code Red, Nimda.

(3) Trojan Horse.
- Greek.
- Must be executed by victim to work.
- Corrupts data / s/w / app^n^s.
- Doesn't replicate like above two.

④ Ransomeware.
⑤ Java scripts & Java applets.
⑥ Spyware, etc.