U-2 (CSDF)

DOMS | Page No.
Date / /

Q1 OS Security -

- process of ensuring OS integrity, confidentiality & availability.
- specific steps or measures used to protect OS from threats, viruses, worms, malware, etc.
- protecting system to computer system resources CPU, memory, disk, etc.
- encompasses all preventive control techniques.
- Ways to acheive OS security -
  - Authentication → username/password
    Usercard/key
    Uses attribute fingerprint.
  - 0 One time password
    - → Random numbers
    - → Secretkeys
    - → Network pass

Program threats → OS process & kernel do designated task as instructed
↓ If user program made these process do malicious tasks.

DOMS | Page No.
Date / /

Q2 Types of Virus & worms? How do they propagate?

* Virus – piece of self-replicating code embedded within another program (Host).
  - Hard disks, Floppy disks CD-ROMS & email attachments
  - slower than worm
  - deletes or modifies filed
  - can change location of file

* Type virus → File Infector
  Resident Program Infector
  Boot Sector Infector
  Multi-Partite Virus
  Dropper
  Stealth Virus
  Companion Virus
  Polymorphic Virus
  Mutation Engine
  Appln or Program Virus
  Macros Viruses
  Time bombs
  Active X & Java Control

* worms → code that replicate itself in order to consume resources to bring it down through computer network
  - exploits holes in computer network

- Instant message worm
- File sharing network worm
- IRC worms
- Internet worms

DOMS | Page No.
Date / /

Q3 Intellectual Property

- Rights → legal rights that cover privileges given to individuals who are owner and inventors of work & created intellectual creativity.
- Rights of creator → against any unauthorized use of exploitation of work

Types of IPR

- Patents
- Design Rights
- Performers Right
- Copyright
- Trademarks
- Database Rights.

Benefits →

- Grants author / inventor exclusive rights.
- promote sharing of info & data.
- offers artists reward for work & legal defence.
- Promotes economic & social growth.

DOMS | Page No.
Date / /

Q4: Internet Hacking & different approaches of hacking.

→ Internet hacking → cyber hacking or hacking
↳ gaining access of unauthorized computer systems, networks of data over internet with malicious intent

→ Hacker is an individual who is good in understanding of computers, networking programming & hardware but no malicious intentions.

Approaches
↳ Malware
↳ Password Attacks
↳ SQL Injection
↳ DDOS Attacks
↳ exploiting Vulnerabilites
↳ Brute Force Attacks
↳ Physical Attacks

Q5: Different ways to gain access to your computer/sys

Q7:
- Access your computer to view, change or delete info on your comp
- Crash or slow down your computer.
- Access private data by examining files on your system
- Use your computer to access other comp on internet

Significance

DOMS | Page No.
Date / /

Q6- Firewall- (control network traffic)

- Network security
- Access Control.
- Protection under Unauthorized access
- Appln layer filtering
- Logging & Monitoring.
- Compliance Requirements.

VPN- (Virtual Private Networks).
creating a secure network connection when utilising public networks.

- Secure Remote Access
- Data Encryption.
- Bypassing Censorship & Geo Restrictions
- Public Wifi Security
- Privacy & Anonymity.
- Secure Site-to-Site connections.
- Compliance.

DOMS | Page No.
Date / /

Q8. Computer Intrusions
↳ someone tries to access to any part of your computer system.

- used automated computer programs when they try to compromise computer's security.

* Intrusion Detection System—
- designed to detect automatically alert administrators when someone or something is comprimising informn system through malicious activities or through secrets

↳ 4 elements • events • Analysis • Counter Measure • storage

(Diagram dekh lo text mai)

functions →
- monitor user & system activities.
- audits system configuration for vulne-
- corrects system configuration errors.
- identifies known attack pattern in system.

Types → 1) Network Intrusion Detection System (NIDS)
- placed at strategic points throughout network to evaluate traffic
- monitors every passing traffic on subnet & compares to database of known threats.

2) Host Instrn Detecn System (HIDS)
- runs on specific hosts or devices.
- device's incoming & outgoing packets

Signature Based IDS
- signature software → identifies pattern.
- can't detect when no pattern exists

Anomaly based IDS
- identify & adapt to unknown assault.

DOMS | Page No.
Date / /

Q9

Virus	Worm
• malicious executable code attached to another executable file	• form of malware replic itself & can spread to diff computer via n
• modify info	• eats system resou
• host needed for spreading	• doesn't need a host
• more harmful	• less ~~com~~ harmful
• antivirus software for protection	• detected & remov ed Antivirus & firew
• Can't be controlled by remote	• controlled by remo
• executed via executable files	• executed via weakn in system
• Resident & non-resident are types	• Morris worm, Ster worm & SQL sla
• Needs human action to replicate	• no need of huma actio
• spreading speed is slower	• spreading speed is faster

DOMS | Page No.
Date / /

Q10 Short note.

1) Software Piracy – act of
- stealing software that is legally protected.
- theft when copied, distributed, altered or sold.
- deprives copyright holders of their pay.
- ensures software collects, stores & process data in way. respects user privacy & complies with data protection law.
- safeguarding user info from unauthorized access or misuse

2) Mail Bomb –
- Type of cyber attack
- attacker send massive volume of email message to overwhelm or disrupt recipient email server or inbox
- could lead to Denial of service (DOS) to use email service
- Disrupt operation or cause inconvinence

3) Exploitation –
- Taking adv of vulnerabilities or weakness in system.
- compromise system, launch attacks, steal data.
- Security patches; regular updates, robust security ↳ essential.

4) stalking & Obscenity
→ using digital means, social media, email or msg apps to repeatedly harass, threaten or intimate victim or person.
→ dissemination of explicit, sexually explicit or offensive content
- serious emotion & physiological consequences.

5) Cybercrime prevention method →
- strong password
- Install security software
- Regular updates
- Enable two factor authen
- Be cautious online.
- Educate Yourself
- Report cybercrime
- Regular Backups

Q1- Data Security Consideration backup, archival storage & disposal of data

safeguards of software & programs in computer & comm sys

- use of data concerning unwanted access

- preserving data integrity
- " " confidentiality
- prevent data from being lost or destroyed -

Backups → • creating extra copies of data & storing in different
• Avoid → • data damage • privacy & confidential ag
• theft of data • premature data relea
• real time data • before verified for

Archival storage → • preserving data for long term storage at safe locations.
• variety of shapes, cloud online or bot
• storage facility • usability of data
• space related issues.
• In contrast to offline storage

disposal of data
→ erasing data from cassets, hard drives, & other electronic devices.

- prevent wastful storage expenses.
- less info to look for

Q13 Appln Security -

- making apps & more secure by finding fixing & enhancing security

Appln Security tools -

- static testing
- dynamic testing
- Interactive Testing
- Mobile testing

Types → • Authentication
• Authorization
• Encryption
• Logging
• Appln security testing