T.Y.B.Sc. I.T. Semester V (2003-04) Internet Security
Final Chapterwise Question bank with possible allotment of marks:
(Compiled by: Prof. Rajesh M. Watve / S.I.W.S.)

(Important Disclaimer: Please note that this question bank is a compilation of questions suggested by various faculties teaching this subject. It may not be officially approved /recognized by the University. E&OE)

Chapter 1: Introduction

- What are different principles of security? Explain any four of them. (8 marks)
- How the attacks are classified? Give examples of each type of attack. (4 marks)
- What are the different strategies that can be used for securing the network? (6 marks)
- What are the different threats to the security? Explain. (8 marks)
- Recognize what type of threat is it when a particular situation is given. In case that threat can be put in two categories, then list both of them: (4 marks)
  a)Mr. Sharma is a typist in a C.A. firm. Unknowingly he has typed 25,000 instead of 2500.
  b)Mr. Sane is owner of a firm. His all important machinery was burned because of fire.
  c)Ms. Shah finds existence on Lehigh virus in her PC.
  d)Mr. Sampat is working in a small company. One day he tries to open a private mail sent by his boss to G.M.
- What do you mean by security policy &who should be involved when forming policy? (4 m)
- What are the components of a good security policy? (8m)
- What are the different types of services given by application layer. Explain with respect to attack and protection of individual services? Any three services. (6m)
- Write short notes on
  1 Risk assessment (8m)
  2 Security policy (8m)
  3 Incident handling(8)
- What do you mean by a 'security policy'? Also explain the characteristics of a good security policy. [5 mks]
- Explain the concept of 'Incident handling' in a security plan relating to website.[4 mks]
- Define 'security' and explain why it is required. [4 mks]
- What are the important factors to be considered in overall security plan ? [8 mks]
- What is 'Risk Assesment'? What procedure is required to be followed for it? [5 mks]

Chapter 2: Classes of Attacks

- What are the different types of services explain with respect to attack and protection of individual services? (8m)
- What are the different types of active attacks ? explain in detail? (8m)

- What is denial of service attack? (4m)
- What do you mean by packet sniffing and packet spoofing? (4m)
- What is the stealing password and what are the different ways to maintain the password?(6m)
- What is the problem associated with the clear text password how it is overcome
- A user can't access resources of computer system. Explain kind of attack comes under above scenario . (6)
- Explain Denial of service attack with example. (5)
- What are the exponential attacks? Explain any one in detail. (6)
- How fragemented packets and creation of processes used in denial of service attack by the attacker .Explain in Detail (8)
- What are 'Bugs' and 'backdoors'? what prevention mechanisms can be used for them ? [4 mks]
- Explain the various techniques used by hackers for 'stealing passwords'. Also mention the countermeasures for it. [6 mks]
- Explain the concept of 'social engineering'. what methods are used by the hackers for this purpose? Also mention the countermeasures.[6 mks]
- What are 'Bugs' and 'backdoors'? what prevention mechanisms can be used for them ? [4 mks]
- Differentiate between the 'active attacks' & 'passive attacks' giving examples in each. [4 mks]
- What is the commonly used method for 'Authentication' of users? How the authentication failure can be observed in this ? [5 mks]
- What are 'botnets' and how do they work? [4 mks]
- How the 'viruses' and 'worms' can be used by attackers for exponential attacks? [4 mks]
- Explain the concept of 'protocol failures'. How does it affect the security of a system? [4 mks]
- Explain the 'Denial of Service' attacks. In what ways the DoS attacks are made to a system? [5 mks]
- Explain the various requirements of a 'secure password'. [4 mks]
- Mention the differences between the 'inside' and 'outside' attacks.[4 mks]
- Discuss various situations for the 'information leakage' [4 mks]
- What is 'Distributed Denial of service' attack ? [4 mks]
- For the following statements, explain the exact 'class' of attack. Also mention whether it is passive or active in each case. [1 mk each]
  - An attacker explores a hole in 'internet explorer' program & uses it to compromise a system.
  - Attacker calls the company's staff and asks to create a new login id for him, posing as a newly appointed employee.
  - A hacker intercepts a TCP packet and finds valuable information in it.
  - An intruder sends a 'keylogger' to a system to receive all the keystrokes on that machine.
  - An attacker sends an anonymous mail to a person, posing as Email service provider staff member, asking him to send info such as login name, password date of birth, country & zip code.
  - An attacker makes a SYN attack on a host using nmap as the tool.
  - An intruder logs into a system remotely using login name/password which he has found already.
  - An attacker keeps a 'fake login screen' program running on a terminal.

Chapter 3: Computer Security

- How the viruses can be classified? How the process of infection takes place?
- Explain the functioning of any three viruses. (8 marks)
- Write a short note on Trojan horses with suitable examples. (4 marks)
- Write a short note on worms with suitable examples. (6 marks)
- What are the different types of virus? Explain any two in detail. (6)
- What do you mean by virus and how viruses spread (5)
- How to protect computer against virus ? (6)
- What is Trojan Horse attack ? (4)
- What is Internet worm ? (4)
- What symptoms are normally observed when virus infection is caused ? (4)
- Differentiate between the virus and trojan horse. (4)

Chapter 4: Firewalls and Proxy servers

- What is packet filtering? What are the different types of attack from which packet filtering protects your network? explain any one in detail. (8)
- How packets are handled by an ordinary router & How screening router is implemented to provide packet filtering? (8)
- Explain the concept of packet filtering in detail. State its advantages and disadvantages. (8)
- What do you mean by firewall? why it is needed and what firewalls can't do ? (4)
- Explain Dynamic Packet filtering. How it is implemented to achieve state tracking and Protocol checking. (6)
- How filtering can be used to prevent an attacker from injecting forged packet? (4)
- What is the Risk associated with this kind of filtering? (6)
- What are the possible attacks that rely on forgery explain in detail. (5)
- Explain the concept of filtering by service with respect to Telnet. (6)
- What are the kinds of firewalls configurations.Explain any one in detail (6)
- Explain Application gateway in detail. (8)
- What do you mean by firewalls? How it can be used to hide DNS information? (6)
- What is the difference between Application level versus circuit level proxies? (4)
- What do you mean by proxying? How proxy works as Transparent proxying? (5)
- "The default deny stance is much safer compare to default permit while implementing on proxy." But most users and managers prefer default permit stance Explain with reasons. (5)

Chapter 5: Cryptography

- Apply vernam cipher algorithm to plain text: best of luck using one time padding: -ncbt zq axyp ?(4m)
- Generate a symmetric key using D-H algorithm for n=11,g=7 (6m)
- Explain Diffie Hellman key exchange algorithm? (6m)
- Compare symmetric and asymmetric key cryptography ?(4m)
- What are the different transposition techniques explain in detail?(6m)
- What are the different substitution techniques explain in detail? (6m)

- Explain the role of trusted third party?(4m)
- How does simple columnar transposition technique work and assume the same plain text and generate the corresponding cipher text using this technique? (5m)
- What are the different algorithm modes explain in detail (8m)
- What are the basic steps in data encryption standard?(5m)
- What is the key wrapping ? how it is useful? (4m)
- Explain message digests algorithm in detail(8m)
- Explain hash based message authenticated code in detail(8m)
- Describe the general working of Digital Signatures (4m)
- Explain the general procedure of Encryption and Decryption. (4m)

E&OE.

(Compiled by: Prof. Rajesh M. Watve / S.I.W.S.)

(Important Disclaimer: Please note that this question bank is a compilation of questions suggested by various faculties teaching this subject. It may not be officially approved /recognized by the University. E&OE)