

C.U.SHAH UNIVERSITY

Summer Examination-2017

Subject Name : Computer Security

Subject Code : 2TE05CSE1

Branch: Diploma(CE)

Semester : 5

Date : 22/03/2017

Time : 02:30 To 05:30

Marks : 70

Instructions:

- (1) Use of Programmable calculator & any other electronic instrument is prohibited.
 - (2) Instructions written on main answer book are strictly to be obeyed.
 - (3) Draw neat diagrams and figures (if necessary) at right places.
 - (4) Assume suitable data if needed.
-

Q-1

Attempt the following questions:

(14)

- a) What is the full form of IDS?
 - a) Insider detection systems
 - b) Intrusion deciding systems
 - c) Intrusion detection systems
 - d) Intrusion detection setup
- b) _____ is a technique in which a system security mechanism is bypassed undetectably to access a computer or its data.
 - a) Backdoor
 - b) Bypass
 - c) Trojan Horse
 - d) Worm
- c) A _____ attempts to learn or make use of information from the system but does not affect system resources.
 - a) Massive Attack
 - b) Passive Attack
 - c) Positive Attack
 - d) Active Attack
- d) An _____ attempts to alter system resources or affect their operation.
 - a) Massive Attack
 - b) Passive Attack
 - c) Positive Attack
 - d) Active Attack
- e) _____ is a techniques to look over someone's shoulder, to get information.
 - a) Person Surfing
 - b) Shoulder See
 - c) Shoulder Surfing
 - d) Person See



- f) What is the full form of HIDS?
- Host Intrusion detection systems
 - Home Intrusion detection systems
 - Host Inside detection systems
 - Home Inside detection systems
- g) A _____ is a dedicated hardware, or software or a combination of both, which inspects network traffic passing through it, and denies or permits passage based on a set of rules.
- Domainwall
 - Hardwall
 - Softwall
 - Firewall
- h) What is the full form of PPTP?
- Person-to-Person Protocol
 - Point-to-Point Protocol
 - Point-to-Person Protocol
 - Person-to-Point Protocol
- i) Cryptanalysis is used
- to find some insecurity in a cryptographic scheme
 - to increase the speed
 - to encrypt the data
 - none of the mentioned
- j) A way of verifying both the sender of information and the integrity of a message is through the use of
- Public key encryption.
 - Digital signatures.
 - Private key encryption.
 - Digital certificates.
- k) Keys that are _____ bits long cannot be cracked by brute-force means within a reasonable period of time.
- 128
 - 28
 - 64
 - 56
- l) _____ is a software that collects information from a computer and transmits it to another system.
- Spyware
 - Hardware
 - Firmware
 - Software
- m) Which of the following is not a biometric device?
- Face Scanner
 - Finger Scanner
 - ID Scanner
 - Retina Scanner
- n) One security protocol for the email system is _____
- IPSec
 - SSL
 - PGP
 - None of the above



Attempt any four questions from Q-2 to Q-8

- Q-2** **Attempt all questions** (14)
a) Explain Dumpster diving in detail.
b) Explain Centralize and Decentralize Infrastructure.
- Q-3** **Attempt all questions** (14)
a) What is information security? Explain security attacks.
b) Explain model for network security.
- Q-4** **Attempt all questions** (14)
a) Draw and Explain Symmetric Encryption model.
b) List substitution techniques and explain any one.
- Q-5** **Attempt all questions** (14)
a) Explain man in the middle attack.
b) Explain Phishing Attack in detail
- Q-6** **Attempt all questions** (14)
a) Write a note on Virtual Private Network.
b) Explain Asymmetric encryption with Example.
- Q-7** **Attempt all questions** (14)
a) What is Virus? Explain Different Types of Virus.
b) Write a note on SQL Injection.
- Q-8** **Attempt all questions** (14)
a) Explain SSL.
b) Explain IP Security.

Q-1 **Attempt the following questions:** (14)

- a) IDS નું પૂરું નામ આપો
a) Insider detection systems b) Intrusion deciding systems
c) Intrusion detection systems d) Intrusion detection setup
- b) _____ તકનીક મા સિસ્ટમની સુરક્ષા પધ્ધતિ ને બાયપાસ કરી કંપ્યુટર અથવા તેના ડેટા ને મેળવવામા આવે છે.
a) Backdoor b) Bypass
c) Trojan Horse d) Worm
- c) _____ જાણવાનો પ્રયત્ન કરે છે અથવા સિસ્ટમ નો ઉપયોગ કરે છે પણ તેના સ્ત્રોતો ને અસર કરતુ નથી.
a) Massive Attack b) Passive Attack
c) Positive Attack d) Active Attack
- d) _____ સિસ્ટમ ના સ્ત્રોતો બદલી શકે અથવા તેમની કામગીરી પર અસર કરે છે.
a) Massive Attack b) Passive Attack
c) Positive Attack d) Active Attack
- e) _____ એક તકનીક કોઈની ખભા પરથી માહિતી મેળવવા માટે ઉપયોગ થાય છે.
a) Person Surfing b) Shoulder See



- f) HIDS નુ પૂરુ નામ આપો?
 a) Host Intrusion detection systems b) Home Intrusion detection systems
 c) Host Inside detection systems d) Home Inside detection systems
- g) _____ સમર્પિત હાર્ડવેર, સોફ્ટવેર કે બંને ભેગા છે કે જે તેના માથી પસાર થતા નેટવર્ક ના ટ્રાફિક પર નજર રાખે છે અને નીચમો ના આધાર પર તેને પરવાનગી આપે છે અથવા નકારી કાઢે છે.
 a) Domainwall b) Hardwall
 c) Softwall d) Firewall
- h) PPTP નુ પૂરુ નામ આપો?
 a) Person-to-Person Protocol b) Point-to-Point Protocol
 c) Point-to-Person Protocol d) Person-to-Point Protocol
- i) ક્રિપ્ટએનેલિસિસ શા માટે વપરાય છે?
 a) to find some insecurity in a cryptographic scheme
 b) to increase the speed
 c) to encrypt the data
 d) none of the mentioned
- j) સંદેશો મોકલનાર અને સંદેશા ની સમ્પૂર્ણતા ચકાસવા માટે શુ વપરાય છે?
 a) Public key encryption. b) Digital signatures.
 c) Private key encryption. d) Digital certificates.
- k) _____ બિટ કે તેનાથી લાંબી કી ને બ્રૂટ ફોર્સ અટેક થી નિશ્ચિત સમય ગાળામા તોડવી મુશ્કેલ છે.
 a) 128 b) 28
 c) 64 d) 56
- l) _____ એક સોફ્ટવેર છે કે જે એક કમ્પ્યુટર થી માહિતી ભેગી કરે છે અને અન્ય સિસ્ટમ ને પસાર કરે છે.
 a) Spyware b) Hardware
 c) Firmware d) Software
- m) નીચેનામાથી કયુ બાયોમેટ્રિક ઉપકરણ નથી?
 a) Face Scanner b) Finger Scanner
 c) ID Scanner d) Retina Scanner
- n) _____ ઈમેલ સિસ્ટમની સુરક્ષા માટેનો પ્રોટોકોલ છે.
 a) IPSec b) SSL
 c) PGP d) None of the above



