Ex/PG/CSE/T/1210C/2017

MCSE First Year Second Semester Examination, 2017

Network Security

Time – 3 Hours **Full Marks – 100**

Answer any five questions

Answer all parts of a question together

1.

a. Compare known plaintext and chosen plaintext attacks on encrypted messages.
b. Differentiate between block ciphers and stream ciphers.
c. What are the major requirements of Public-key cryptography?
d. What is a secure hash function? State some desirable properties of it.
e. Describe different ways in which message authentication codes can be generated?
f. What are digital envelops? How is it useful?

2+3+3+3+6+3=20

2.

a. What are the different entities in Kerberos authentication system? State the roles of each.
b. An enterprise network system uses Kerberos authentication system to authenticate users to different services (i.e. http, ftp, mail, print etc.). Identify different authentication messages exchanged between the Kerberos client in one of the users machine and other servers when the user
   i. First logs into the system
   ii. Uses http service
   iii. Uses mail service
   iv. Uses http service again

   Describe the content of each message.
c. In the above authentication scenario what will happen if the Ticket Granting Server is absent.
d. What are the drawbacks of Kerberos authentication system?

4+10+4+2=20

3.

a. Differentiate between the transport and tunnel mode of IPSec operation.
b. What is the utility of padding in ESP?
c. What is a security association? What are the different parameters of a security association?
d. Describe how security association database and security policy database is used for IPSec processing of outbound and inbound traffic.
e. How does IPSec differ from SSL? Mention some example scenarios where IPSec is useful.

2+2+4+8+4=20

4.

a. What is stateful packet filtering? Give one example where it is advantageous.
b. Describe two possible attacks against packet filtering firewalls. Also state appropriate countermeasures against those attacks.
c. How does PGP provide compatibility of e-mail messages?
d. How does PGP guarantee randomness between symmetric keys generated in two successive sessions?
e. How does PGP guarantee secrecy of private keys its user?
f. Explain how signature used in PGP message prevents replay attacks.

3+4+3+3+4+3=20

5.

a. What is a digital certificate? Briefly describe the X.509 digital certificate format.
b. Explain the role of a certification authority (CA) in X.509 authentication scheme. What is a root certification authority? How does a root certification authority get its own certificate?
c. What are the usages of personal certificates, server certificates, software publisher certificates and certificate authority certificates?
d. Identify cases when revocation of user certificates is necessary and briefly describe how it is done.

(2+4)+(2+2)+6+4=20

6.

a. Define "false positive" and "false negative". Explain why it is not possible to remove "false positive" and "false negative" completely.
b. What is profile based anomaly detection? Explain with suitable examples any three types of metrics that can be used to measure user behavior.
c. What is a protection domain? How modifications to the protection state are controlled in Discretionary Access Control mechanism?
d. What is role based access control? Describe three types of constraints in RBAC.
e. What is the difference between an access control list and a capability list?

4+4+4+4+4=20

7.

a. Explain how man-in-the-middle attack is possible against Diffie-Hellman Key Exchange Algorithm. State one way to prevent this kind of attack.
b. Explain how the pre master secret is established in SSL handshake protocol using (i) Ephemeral Diffie-Hellman and (ii) Anonymous Diffie-Hellman key exchange algorithms.
c. Name the different cryptographic parameters that are generated during SSL Handshake phase and also mention their intended usage.
d. What are the different functions of SSL Record Protocol?
e. Give some example scenario where SSL alert protocol is used.

6+4+4+4+2=20

--------|-------