Roll No: ----------

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December, 2017

Program/course: B.Tech(CSE+SCF)	**Semester : VII**
Subject: IT Network Security	**Max. Marks : 100**
Code : CSIB442	**Duration : 3 Hrs**
No. of page/s: 03	

Section A (attempt all: 20 Marks)

1. **State True/False and give reason why:** [8]
   - **i.** In terms of Web Security Threats, "Impersonation of another user" is a Passive Attack.
     a) True
     b) False
   - **ii.** HTTPS stands for Hypertext Transfer Protocol over TLS.
     a) True
     b) False
   - **iii.** Wired networks are far more susceptible to eavesdropping and jamming than wireless networks.
     a) True
     b) False
   - **iv.** Assume there has been no change made to the default policy properties, to allow an FTP connection into your network you must write two rule:
     1) one to allow the initial ftp connection In, and
     2) one to allow the destination machine to send information back to the client machine.
     a) True
     b) False
2. **Choose the correct answer/answers:** [4]
   - **i.** WPA stands for –
     a) Wired Protected Access
     b) Wireless Protected Access
     c) Wireless Personal Access
     d) Wired Personal Access
   - **ii.** Reliable data delivery and Wireless access control protocols are functions of which layer?
     a) Physical Layer
     b) Logic Link Control Layer
     c) Medium Access Layer
     d) None of the mentioned
   - **iii.** Another name for the AAA key (Authentication, Authorization and Accounting Key) is –

a) pre-shared key
b) pairwise transient key
c) master session key
d) key conformation key

iv. _____ is a collection of protocols designed by the IETF (Internet Engineering Task Force to provide security for a packet at the network level.
a) IPSec
b) SSL
c) PGP
d) none of the above

3. Differentiate between TACACS and RADIUS with example. [4]

4. Explain with the help of diagram the difference between HIDS and NIDS. [4]

SECTION B (Attempt all Questions: 40 Marks)

5. What is VPN? Discuss the process for selecting the correct VPN technology for your needs. Distinguish between Transport and Tunnel Mode VPN. [2+4+4]

6. Write short notes on: [5+5]
i. Kerberos version 4
ii. Telnet vs SSH

7. Suppose you are working at an organization that has a small to medium sized network (~500 users) and about a dozen /24 subnets (and a handful of smaller ones behind NAT). Explain various types of monitoring soft wares that you would use to allow to keep tabs on remote parts of the network and respond to problems proactively. [10]

8. Wiring closets and operations centers are behind locked doors so that visitors can't insert themselves into the network. But consider the guy who cleans your office late at night – can he connect his PDA to your LAN? Can he leave a small access point somewhere, tricking stations into connecting with it instead of the real company LAN? Is that considered a rogue access point, or is there more to it? [3+3+4]

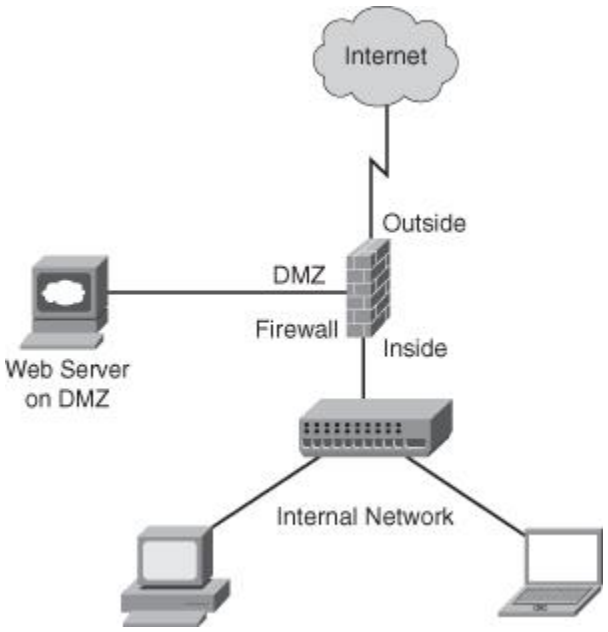
SECTION C (attempt either 9 and 10 or 11 and 12: 40 Marks)

9. **a**. Briefly explain the three classes of intruders. [6]
b. What are four basic techniques of choosing passwords? [6]
c. Explain the key management in IPSec. [8]

10. What is WEP? How secure is WEP? What is MAC filtering and how effective is it? I have heard that disabling the SSID beaconing functionality can stop war drivers from accessing my WLAN. Is this true? [4+4+6+6]

OR

11. The Organization IT staff is in the “If we self-host, we must use a DMZ” frame of mind. Is this frame of mind correct?



i. Explain the working of DMZ. [8]
ii. Can Internet traffic travel to servers on the private network, or is there another solution? [4]
iii. How can the IT staff ensure that inbound network traffic will stay? [4]
iii. What measures can be taken to hide the private network from the inbound network traffic? [4]

12. What Are The Phases Of Network Penetration? How Will You Protect The Data During And After Penetration Testing? What kind of penetration can be done with the Diffie Hellman exchange? [5+5+10]

…….……ALL THE BEST!!!!.....

Roll No: ----------

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December, 2017

Program/course: B.Tech(CSE+SCF)	**Semester : VII**
Subject: IT Network Security	**Max. Marks : 100**
Code : CSIB442	**Duration : 3 Hrs**
No. of page/s: 03	

Section A (Attempt all questions: 20 Marks)

1. **State True/False and give reason:** [8]
   - **i.** A sniffer program shows all the data on an uswitched network segment by including unencrypted passwords and the data inside files.
     a) True
     b) False
   - **ii.** A firewall is a device that keeps certain kinds of Network traffic out of a Private network.
     a) True
     b) False
   - **iii.** Network layer security protocol provides end-to-end security services for applications.
     a) True
     b) False
   - **iv.** SSL provides confidentiality
     a) True
     b) False
2. **Choose the correct answer/answers:** [4]
   - **i.** SHA-l has a message digest of
     a) 160 bits
     b) 512 bits
     c) 628 bits
     d) 820 bits
   - **ii.** Which topology has a central hub?
     a) Mesh
     b) Star c
     c) Bus
     d) Ring
   - **iii.** SSID stands for –
     a) Secure Service Identifier
     b) Secure Set Independent Device
     c) Secure Set Identifier c
     d) Service Set Independent Device

iv. Which one of the following is not a public key distribution means?

a) Public-Key Certificates
b) Hashing Certificates c
c) Publicly available directories
d) Public-Key authority

3. What is the difference between VPN and VLAN? Explain briefly. [4]

4. Explain authentication procedure used by x.509. [4]

SECTION B (Attempt all Questions: 40 Marks)

5. Describe how a man-in-the-middle attack may be performed on a Wi-Fi network and the consequences of such an attack with neat diagram. Explain how a man-in-the-middle attack on a Wi-Fi network can be defeated. [6+4]

6. What is IDS? Explain network-based IDS and Host based IDS and mention their advantages and disadvantages. [2+4+4]

7. What is an SSL Certificate? List out five SSL vulnerabilities. Explain one of SSL vulnerability with root cause along with mitigation and impact. [2+4+4]

8. Briefly explain the four types of security attacks that are normally encountered. Also distinguish between active and passive attacks. [6+4]

SECTION C (attempt either 9 and 10 or 11 and 12: 40 Marks)

9. Explain Below points:

a. Distinguish between penetration testing and vulnerability assessment with example.[6]
b. List out penetration testing stages, Explain penetration testing stages in proper order [2+4+4]
c. List out two open source and commercial penetration testing tool.[4]

10. If Alice digitally signed some data and then encrypted the data and the digital signature using Bob's public encryption key,
Bob could behave maliciously and...
1. decrypt and recover the data and the digital signature;
2. encrypt the data and the digital signature using Charlie's public encryption key;
3. send this ciphertext to Charlie, who decrypts it and verifies Alice's digital signature.
So Charlie can decrypt the message using his private key but how does he know what to do with the digital signature? How would he know what verification algorithm to use? How would he know who signed it? [20]

OR

11. Answer Below questions:

a. What is Kerberos?[4]
b. Where does the name "Kerberos" come from?[4]
c. What is a "Kerberos client", "Kerberos server", and "application server"?[4]
d. What is the role of Ticket Granting Server in inter realm operations of Kerberos?[4]
e. What are the advantages/disadvantages of Kerberos?[4]

12. Answer Below questions:

a. What Is The Difference Between a Vulnerability Scan, a Risk Analysis, and a Penetration Test? [6]
b. List out four Network vulnerabilities and Web application vulnerabilities.[4]
c. What is ransomware attack and root cause of this vulnerability?[3+3]
d. Differentiate between remote code injection, command injection and arbitrary code injection.[4]

…….……ALL THE BEST!!!!.....