Day : Monday   Time : 10:00 AM TO 1:00 P.M.

Date : 19/12/2016   Max. Marks : 100

N.B.

1) Attempt any **THREE** questions from each section.
2) Figures to the right indicate **FULL** marks.
3) Answers to both the sections should be written in **SEPARATE** answer book.
4) Neat diagrams must be drawn **WHEREVER** necessary.

SECTION – I

Q.1 a) What is null session? Explain step to disable null session. (08)

    b) What is OS finger printing? Explain practical steps with tool. (08)

Q.2 a) Explain various counter measures for sniffing? (08)

    b) i) List out the terminology for following explanations: (04)

Pankaj, inspired by the hacking session. He came back home and started exploring few techniques demonstrated by the speaker. It can be said that Pankaj is a ....?

In computer security, ... means that computer system assets can be modified only by authorized parties.

Sending packets that, when reassembled, are too large for the system to understand.

A hacker wants to hack the password of one his friend who is the students of his college. Attack which is done by him is the fast way of cracking password but it's disadvantage is that the success rate is very poor. The attack is ......

ii) State True or False: (04)

1) Locking a server in a closet prevents malicious users from accessing it, but if not adequately ventilated, the computer will overheat and fail, rendering your security concerns pointless.

2) Cyber law means only applying the provisions of the Information Technology Act, 2000.

3) Hoaxes is a program or device that can monitor data traveling over a network.

4) If you wish to allow the external users access your web server you must block part number 110.

Q.3 a) What is e-mail header? How to trace an e-mail header? (08)

    b) Explain the flag sequence for following scan type: (08)
       i) Half open scan ii) Ideal scan iii) UDP scan iv) TCP connect scan.

Q.4 Write short note any **THREE**: (18)
    a) DHCP starvation attack
    b) Bot net
    c) Wireless threats
    d) Covering track

P.T.O.

SECTION – II

Q.5 **a)** Explain the most important steps recommended for security of web server? (08)

b) Explain Pen testing of SQL server. (08)

Q.6 **a)** What are the methods of session Hijacking? (08)

b) **i)** Identify Malware category for following explanations. (08)
Theses type of virus that attempts to attack both sector and the executable or program files at the same time.
These types of virus that attempts to modify directory table entries point to the virus code instead of the actual program.
Its type of Trojan, which gives remote control of a command shell on a victim's machine.
Its type of Trojan, which destroys the operating system on execution.
ii) State True or False:
1) IPsec is designed to provide the security at the Network layer.
2) When a DNS server accepts and uses incorrect information from a host that has no authority giving that information, then its called DNS Hijacking.
3) Digest authentication method is based on a challenge-response model and uses the MD5 algorithm.
4) A virus can infect the boot sector but a worm can not.

Q.7 **a)** What is Buffer overflow mutation technique? What are its counter measures? (08)

b) What are the Risks of Social Engineering to corporate network? (08)

Q.8 Write short note on any **THREE:** (18)
a) Spoofing vs Hijacking
b) Fragmentation time out attack
c) Transparent proxy
d) SLA

*   *   *

Day : Monday
Date : 19/12/2016

Time : 10:00 AM TO 1:00 P.M.
Max. Marks : 100

N.B.

1) Attempt any **THREE** questions from each section.
2) Figures to the right indicate **FULL** marks.
3) Answers to both the sections should be written in **SEPARATE** answer book.
4) Neat diagrams must be drawn **WHEREVER** necessary.

SECTION – I

Q.1 a) What is null session? Explain step to disable null session. (08)

b) What is OS finger printing? Explain practical steps with tool. (08)

Q.2 a) Explain various counter measures for sniffing? (08)

b) i) List out the terminology for following explanations: (04)
Pankaj, inspired by the hacking session. He came back home and started exploring few techniques demonstrated by the speaker. It can be said that Pankaj is a ....?
In computer security, ... means that computer system assets can be modified only by authorized parties.
Sending packets that, when reassembled, are too large for the system to understand.
A hacker wants to hack the password of one his friend who is the students of his college. Attack which is done by him is the fast way of cracking password but it's disadvantage is that the success rate is very poor. The attack is ......
ii) State True or False: (04)
1) Locking a server in a closet prevents malicious users from accessing it, but if not adequately ventilated, the computer will overheat and fail, rendering your security concerns pointless.
2) Cyber law means only applying the provisions of the Information Technology Act, 2000.
3) Hoaxes is a program or device that can monitor data traveling over a network.
4) If you wish to allow the external users access your web server you must block part number 110.

Q.3 a) What is e-mail header? How to trace an e-mail header? (08)

b) Explain the flag sequence for following scan type: (08)
i) Half open scan ii) Ideal scan iii) UDP scan iv) TCP connect scan.

Q.4 Write short note any **THREE**: (18)
a) DHCP starvation attack
b) Bot net
c) Wireless threats
d) Covering track

SECTION – II

Q.5 a) Explain the most important steps recommended for security of web server? (08)

b) Explain Pen testing of SQL server. (08)

Q.6 a) What are the methods of session Hijacking? (08)

b) i) Identify Malware category for following explanations. (08)
Theses type of virus that attempts to attack both sector and the executable or program files at the same time.
These types of virus that attempts to modify directory table entries point to the virus code instead of the actual program.
Its type of Trojan, which gives remote control of a command shell on a victim's machine.
Its type of Trojan, which destroys the operating system on execution.
ii) State True or False:
1) IPsec is designed to provide the security at the Network layer.
2) When a DNS server accepts and uses incorrect information from a host that has no authority giving that information, then its called DNS Hijacking.
3) Digest authentication method is based on a challenge-response model and uses the MD5 algorithm.
4) A virus can infect the boot sector but a worm can not.

Q.7 a) What is Buffer overflow mutation technique? What are its counter measures? (08)

b) What are the Risks of Social Engineering to corporate network? (08)

Q.8 Write short note on any THREE: (18)
a) Spoofing vs Hijacking
b) Fragmentation time out attack
c) Transparent proxy
d) SLA

* * *