ASSIGNMENT QUESTIONS

IMT CENTRE FOR DISTANCE LEARNING
GHAZIABAD Distance Learning
Programme

IMT-91
BASICS OF SECURITY

Notes:

a. All set of assignments would be made in a single MS. Word file and would be sent together through e-mail to imt.ankitfadia@gmail.com with a cc to nidhimathur@imtcdl.ac.in & richa@imtcdl.ac.in

b. Subject of the e-mail of assignment submission should be '**UNIT-1**'.

c. Students are required to clearly mention their name, roll no, and subject code in the first page of the word file.

d. Write answers in your own words as far as possible and refrain from copying from the textbooks/handouts.

FIRST SET OF ASSIG NMENTS (Subjective)	Assignment (I) = 10 Marks

ASSIGNMENT-I

1. What is an IP address? What are the various forms of an IP address? What are the various ways in which you can trace an IP address on the Internet?

2. Imagine that you are a cyber terrorist and you are planning a major cyber attack. Of course you don't want to get caught! What are the various strategies you will employ to protect your identity and prevent the police from tracing you?

3. How can you find out the IP address of a system hiding behind a proxy server?

4. Write down the IP address 163.114.24.14 in the following notation formats:

   • Decimal

   • Hexadecimal

   • Octal

   • Binary

   • DWORD

5. What are the differences and similarities between ping and tracert?

6. From a system administrator's perspective, which ICMP utility is more dangerous: ping or tracert? Give reasons to support your answer. Which counter-measures can a system administrator employ to counter it?

7. Describe three port scanning techniques. Give their pros and cons.

8. How can you carry out stealth port scanning on a target system?

9. How can you use ICMP scanning to carry out OS detection? Which counter-measures can a system administrator implement to prevent ICMP OS detection?

10. What are the advantages of carrying out ping sweeping? How can a system administrator detect that ping sweeping is taking place? How can it be countered?

SECOND SET OF ASSIGNMENTS (Subjective)	Assignment (II) = 5 Marks

ASSIGNMENT-II

1. What are the differences and similarities between active fingerprinting and passive fingerprinting?

2. How can an attacker perform passive fingerprinting? Describe in detail.

3. What counter-measures can be taken to prevent fingerprinting probes?

4. What is the regedit file? Describe its structure, format and uses.

5. Describe any three windows registry tweaks of your choice.

6. What are sniffers? How can you use a sniffer to record data packets being sent/received on a network?

7. How can a system administrator make it more difficult for an attacker to carry out information gathering?

8. Which information gathering technique is the most important from the attacker's perspective?

9. How can a system administrator mislead an attacker during the process of information gathering?

10. How can an attacker modify the registry on a remote system?

ASSIGNMENT-III

1. Find out if the following systems are alive. If they are alive, then find out their exact geographical information (Kindly submit actual logs as your answer):

   203.94.11.12
   203.94.12.11
   www.hackingmobilephones.com
   www.imt.edu

2. UsE all information gathering techniques taught in this course to find out as much information as possible about the following systems (Kindly submit actual logs as your answer):

   www.hackingmobilephones.com
   www.imt.edu