University of Mumbai

Program: Computer Engineering
Curriculum Scheme: Rev2016
Examination: BE Semester VII
Course Code: CSLDLO7031 and Course Name: Advanced System Security and Digital Forensics
Time: 2 hour Max. Marks: 80

==========

==========

Q1.	**Choose the correct option for following questions. All the Questions are compulsory and carry equal marks**
1.	The term Cyber attack means
Option A:	Attempt to steal, alter, or destroy a system
Option B:	Attempt to steal, alter, or destroy a system using only internet
Option C:	Attempt to steal, alter, or destroy a system using any network
Option D:	Attempt to steal, alter, or destroy a terminal
2.	Denial of performing any actions in order to escape responsibility is known as
Option A:	Denial of Service
Option B:	Tampering
Option C:	Repudiation
Option D:	Virus Attack
3.	Which of the following are examples of Vulnerabilities: 1. Denial of Service, 2. Programs with known flaws, 3. Weak firewall configurations
Option A:	1 and 2
Option B:	2 and 3
Option C:	1 and 3
Option D:	1, 2 and 3
4.	Cheat Codes are an example of:
Option A:	Buffer Overflow
Option B:	Undocumented Access Point
Option C:	Unsafe Utility Program
Option D:	Incomplete Mediation
5.	Worms are:
Option A:	Non-Malicious Codes
Option B:	Malicious Codes
Option C:	Targeted Malicious Code
Option D:	Selectively malicious
6.	Covert Channels are:

Option A:	Non-Malicious Codes
Option B:	Malicious Codes
Option C:	Targeted Malicious Code
Option D:	Selectively malicious
7.	If the data sent by the sender is not the same as the data received by the receiver then it is a loss of?
Option A:	Integrity
Option B:	Confidentiality
Option C:	Authentication
Option D:	Verification
8.	_____ Protocol under SSL indicated that the upcoming data is protected.
Option A:	Record Protocol
Option B:	Change Cipher Spec
Option C:	Alert
Option D:	Handshake
9.	HTTPS uses _____ port number.
Option A:	441
Option B:	442
Option C:	443
Option D:	444
10.	_____ is preferably used for connecting two computer terminals.
Option A:	SSL
Option B:	SSH
Option C:	VPN
Option D:	XSS

Q2 **20 Marks Total**	**Solve any four Questions out of six** **5 marks each**
A	Differentiate between Single Sign-On and Federated Identity Management
B	What are the various ways in which an Operating System Security can be ensured?
C	What is Session Hijacking? How can it be prevented?
D	What is WEP? What were its drawbacks which led to the development of WPA?
E	What is an Intellectual Property? What are its various types?
F	What are application logs? How can we retrieve evidences from log files?

Q3. **20 Marks Total**	**Solve any Two Questions out of Three** **10 marks each**

A	What is Discretionary and Mandatory Access Control. Explain and differentiate.
B	Explain GSM Security in detail
C	Explain and illustrate the Complete Digital Forensics Life Cycle.

Q4. **20 Marks Total**	**Solve any Two Questions out of Three** **10 marks each**
A	What is VPN Security in detail.
B	What is a Windows Registry? What are the various ways of obtaining evidences from windows registry?
C	What is chain of custody? Explain the Evidence Handling methodology.