Program: **Computer Engineering**
Curriculum Scheme: Rev 2016
Examination: BE Semester: VII
Course Code: CSDLO7031 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.	What is the main concern of the Bell-LaPadula security model?
Option A:	confidentiality
Option B:	integrity
Option C:	authentication
Option D:	Accountability
2.	Which of the following is a means of restricting access to objects based on the identity of the subject to which they belong?
Option A:	Mandatory access control
Option B:	Group access control
Option C:	Discretionary access control
Option D:	User access control
3.	Which of the following is a type of single sign-on system?
Option A:	Kerberos
Option B:	RBAC
Option C:	DAC
Option D:	SAML
4.	Which one of the following is not the type of malicious code.
Option A:	Trojan Horse
Option B:	Worm
Option C:	Buffer Overflow
Option D:	Trapdoor
5.	According to OWASP what is the most dangerous web vulnerability?
Option A:	Injections(SQL, LDAP,etc)
Option B:	Cross site scripting
Option C:	Security Misconfiguration
Option D:	Cross site request forgery
6.	What is the Necessity of Forensic Duplication?
Option A:	Performing analysis on duplicate copy is easy.
Option B:	Preserving the original digital evidences is important
Option C:	Performing analysis on original copy is time consuming.
Option D:	Performing analysis on original copy is easy.
7.	When examining the Windows registry key, the “Last Write Time” indicates
Option A:	The last time RegEdit was run
Option B:	When a value in that Registry key was altered or added
Option C:	The current system time

Option D:	The number of allowable changes has been exceeded
8.	____________ is another scam where a fraudster installs malicious code on a personal computer or server.
Option A:	Smishing
Option B:	Phishing
Option C:	Pharming
Option D:	Vishing
9.	Which act prohibits Unsolicited "junk" emails?
Option A:	CAN-SPAM Act
Option B:	CAN Act
Option C:	SPAM Act
Option D:	HIPAA
10.	For creating a true forensic duplicate image, ________ utility is the most efficient tool.
Option A:	DD
Option B:	openstego
Option C:	metasploit
Option D:	flawfinder
11.	A footballer sets up his own company to sell his own range of clothes. What type of IP can he use to show that the clothes are made by his company?
Option A:	copyright
Option B:	patents
Option C:	registered designs
Option D:	trademarks
12.	HTTPS uses Which Protocol for providing Secure link on internet
Option A:	Transmission Control Protocol
Option B:	Secure Socket Layer
Option C:	User Datagram Protocol
Option D:	Hyper Text Transfer Protocol
13.	SSO and FIM are related to
Option A:	Only User identification
Option B:	Only Authentication
Option C:	only Authorization
Option D:	Identity and access management
14.	Which key in Windows registry can reveal the software installed in the past
Option A:	HKEY_CLASSES_ROOT
Option B:	HKEY_CURRENT_USER
Option C:	HKEY_LOCAL_MACHINE
Option D:	HKEY_CURRENT_CONFIG
15.	Unauthorized copying of copyrighted software, music, movies, art, books is called___attack
Option A:	Copyright

Option B:	Piracy
Option C:	Identity Theft
Option D:	Denial of service
16.	To List the processes that are currently in running state, following command can be used
Option A:	hosts
Option B:	ps
Option C:	netstat
Option D:	arp
17.	In which step of Incident Response Methodology, Data Collection and Data Analysis happens
Option A:	Detection of Incident
Option B:	Formulate response strategy
Option C:	Investigate the Incident
Option D:	Reporting
18.	A system tool that enumerates all listening ports and all current connections to those ports
Option A:	PsLoggedOn
Option B:	netstat
Option C:	rasusers
Option D:	arp
19.	UMTS uses
Option A:	TDMA and FDMA
Option B:	WCDMA
Option C:	OFDMA and SC-FDMA.
Option D:	CDMA
20.	One of major flaws in WEP covered in 802.11 is
Option A:	Authentication
Option B:	Confidentiality
Option C:	Integrity
Option D:	Availability

Q2	**Solve any Four out of Six (5 marks each)**
A	Explain access control policies
B	Explain Cybercrime in detail
C	Describe Forensics Duplication
D	Describe Session Hijacking
E	Explain Biba model
F	Describe Intellectual Property in detail.

Q3.	**Solve any Two Questions out of Three. (10 marks each)**
A	Describe Incident Response Methodology
B	Describe GSM and UMTS security.

C	Explain the procedure for Volatile data collection.