Privacy

1) What is the acronym of the Canadian private sector privacy law?
   i) PIPA
   ii) PIPEDA
   iii) PEPODA
   iv) PIPADA

2) What type of OS uses a command line based interface?
   i) UNIX
   ii) Windows
   iii) MAC
   iv) AndroidOS

3) What is meant by 'authorization'?
   i) The act of indicating a person or a thing's identity.
   ii) The act of verifying/proving the claimed identity of the agent'
   iii) The act of specifying access rights/privileges to resources
   iv) The act of assigning a serial number to something

4) How many levels of assurance are there on identification and authentication based on NIST guidelines?
   i) 1
   ii) 2
   iii) 3
   iv) 4

5) How can someone best protect from having their passwords stolen?
   i) Create strong password based on NIST guidelines
   ii) Use multi factor authentication for all accounts
   iii) Not access unauthorized sites
   iv) All of the above

6) What is used to properly enforce authorization systems?
   i) Using access controls
   ii) Issuing ID cards
   iii) Using multifactor authentication
   iv) Using biometrics

7) Which of these ways can be used to identify a computer?
   i) Serial number
   ii) Cryptographic Keys
   iii) Network Address
   iv) All the above

Access Control

1) Which of these can be considered as ‘subjects’ in a university file system?
i) The student who logging in
ii) Student’s assignment files
iii) Password manager system
iv) Course homepage

2) Which of these can be considered as ‘objects’ in a university file system?
i) Student logging in
ii) Student’s assignment files
iii) Student’s profile page
iv) Teacher’s profile page

3) What kind of accesses does Jonathan have for file A?

Alice:	{<A,r/w>, <B,w>, <C,r>}
Jonas:	{<A,r/w/x>, <B,r/w>, <C,->}
Jonathan:	{<A,r/w/x>, <B,r>, <C,x>}
Ali:	{<A,x>, <B,r/w>, <C,r/w/x>}

i) Read only
ii) Write only
iii) Execute only
iv) All of the above

4) What kind of access policy allows users to pass on their privileges to other users?
i) Mandatory Access Policy
ii) Discretionary Access Policy
iii) Role Based Access Policy
iv) None of the above

5) Which one of these is a feature of Discretionary Access Control?
i) Information flow is easily controlled
ii) Information flow cannot be controlled
iii) Uses the Bell Lapuda model
iv) Has classes with partial order

6) What kind of access policy enforce access control based on regulations mandated by a central authority?
i) Mandatory Access Policy
ii) Discretionary Access Policy
iii) Role Based Access Policy
iv) None of the above

7) What is the main principle of the Bell Lapuda Model?
   i) No write up, no read up
   ii) No read up, no write down
   iii) No write down, no read down
   iv) No read down, no write up

8) Which numerical notation denotes unix permission of read and execute for all.
   i) 0000
   ii) 0700
   iii) 0555
   iv) 0666

9) What is the sixth field in the output of UNIX ls-l permission command?
   i) User that owns the file/directory
   ii) The group that owns the file/directory
   iii) The permissions of the owner
   iv) The number of links or directories inside this directory

10) What is the ‘Complete mediation’ principle from “The Protection of Information in Computer Systems” from Saltzer and Shroeder
   i) Base access decisions on permission rather than exclusion.
   ii) When things go wrong ensure system defaults to a safe state.
   iii) Every access to every asset must be checked for authority
   iv) Every program and user should operate while invoking as few privileges as possible.

Malware

1) What kind of malware spreads with little-to-no user involvement?
   i) Worms
   ii) Trojan
   iii) Virus
   iv) Logic Bomb

2) What does the 'dropper' malware do?
   i) Gathers information about users' and then uses it to display targeted advertisements to user
   ii) A program that has been designed to "install" malware on a target system
   iii) Surreptitiously gathers information about users' activities and transmits them to a third
   iv) Malware that are designed to runs with highest possible privileges, access software areas that are otherwise not allowed.

3) What was the name of the most widespread internet worm, that was released on September 18, 2001?
   i) NIMDA
   ii) PIMDA
   iii) SIMDA
   iv) KIMDA

4) What kind of malicious computer program can replicate itself by modifying other programs or files to insert a copy of itself?
   i) Virus
   ii) Trojan
   iii) Worm
   iv) Logic Bomb

5) How can a computer infect itself?
   a) Infect one or more programs that run at startup
   b) Add itself to list of startup programs
   c) Put itself in the boot sector ⇒ run before the OS boots
   d) All of the above

6) What kind of virus detection detects viruses by going over a list of known viruses and characteristics?
   i) Signature-based detection
   ii) Behaviour-based detection
   iii) File integrity checking with cryptographic key
   iv) None

7) What is the name of the malware program that appears to perform some useful task, but which also does something with negative consequences?

i) Virus

ii) Trojan

iii) Worm

iv) Logic Bomb

8) What is the name of threats that uses continuous sophisticated techniques to gain access to a system and remain inside for a prolonged period of time?

i) APT

ii) BPT

iii) PPT

iv) CPT