JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY
UNIVERSITY EXAMINATION 2012/2013

1ST YEAR ST SEMESTER EXAMINATION FOR THE DEGREE OF BSC COMPUTER SECURITY FORENSIC AND AUDIT

MAIN

COURSE CODE: IIT 3113

TITLE: PC SECURITY AND PRIVACY

DATE: 1/5/2013 TIME: 9.00-12.00NOON

DURATION: 3 HOURS

INSTRUCTIONS

1. **This paper contains FIVE (5) questions**
2. **Answer question 1 (Compulsory) and ANY other 2 Questions**
3. **Write all answers in the booklet provided**

SECTION A (20 MARKS)

Q1 True/False, Multiple choice and Explanation

1. Who finds vulnerabilities in systems and plugs the holes?
   A) White-hat hackers
   B) Black-hat hackers
   C) Hacktivists
   D) Script kiddies

2. Who breaks into other people's computer systems and steals and destroys information?
   A) White-hat hacker
   B) Black-hat hacker
   C) Hacktivists
   D) Script kiddies

3. What is a type of virus that spreads itself, not just from file to file, but from computer to computer via e-mail and other Internet traffic?
   A) Computer virus
   B) Worm
   C) Denial-of-service attack
   D) None of the above

4. What consists of the identification of risks or threats, the implementation of security measures, and the monitoring of those measures for effectiveness?
   A) Risk management
   B) Risk assessment
   C) Security
   D) None of the above

5. What is the process of evaluating IT assets, their importance to the organization, and their susceptibility to threats, to measure the risk exposure of these assets?
   A) Risk management
   B) Risk assessment
   C) Security
   D) None of the above

6. What is the process of making a copy of the information stored on a computer?
   A) Backup
   B) Anti-virus
   C) Firewall
   D) Biometrics

7. What is hardware and/or software that protects computers from intruders?
   A) Backup
   B) Anti-virus
   C) Firewall
   D) Biometrics

8. All of the following are considered biometrics, except:

A) Fingerprint
B) Retina
C) Password
D) Voice

9. What is an encryption system that uses two keys: a public key that everyone can have and a private key for only the recipient?
   A) Encryption
   B) Public key encryption
   C) Intrusion-detection software
   D) Security-auditing software

10. What checks out your computer or network for potential weaknesses?
   A) Encryption
   B) Public key encryption
   C) Security-auditing software
   D) None of the above

11. In simple terms, what does risk assessment ask?
   A) What can go wrong?
   B) How likely is it to go wrong?
   C) What are the possible consequences if it does go wrong?
   D) All of the above

12. Which of the following is a characteristic of a firewall?
   A) Examines each message as it seeks entrance to the network
   B) Blocks messages without the correct markings from entering the network
   C) Detects computers communicating with the Internet without approval
   D) All of the above

13. How do ethical people treat others?
   A) With respect
   B) With dignity
   C) With the same care for the rights of others as for their own rights
   D) All of the above

14. Which of the following examines information passing through switches, hubs, or routers?
   A) Key logger
   B) Packet sniffer
   C) Log analysis tools
   D) Screen captures

15. What might identity thieves do with your identity?
   A) Apply for and use credit cards
   B) Apply for a loan
   C) Change their identity
   D) All of the above

16. Cookies are used to do which of the following?
   A) Store your ID and password for subsequent logons to the site
   B) Store contents of electronic shopping carts

C) To track web activity
D) All of the above and more

17. A honey pot is an example of what type of software?
    A) Encryption
    B) Security-auditing
    C) Virus
    D) Intrusion-detection

18. Which type of software monitors a computer or network for potential weaknesses?
    A) Public key encryption
    B) Firewall
    C) Virus
    D) Intrusion-detection

19. What are the principles and standards that guide our behavior toward other people?
    A) Ethics
    B) Intellectual property
    C) Copyright
    D) Fair Use Doctrine

20. What is software that is manufactured to look like the real thing and sold as such?
    A) Fair Use Doctrine
    B) Pirated software
    C) Counterfeit software
    D) Privacy

21. It's illegal to copy copyrighted software, except if you are:
    A) Giving the copy to a relative
    B) Giving the copy to a Professor
    C) Making a single backup copy for yourself
    D) None of the above

22. What is software you don't want hidden inside software you do want?
    A) Adware
    B) Trojan-horse software
    C) Spyware
    D) All of the above

23. Which of the following is true regarding HIPAA?
    A) Gives businesses the right to access your medical records
    B) Limit the release and use of your health information without your consent
    C) Gives hospitals the right to put your medical records in an electronic format
    D) All of the above

24. Which act requires companies to implement policies to prevent illegal activity within the company and to respond in a timely manner to investigate illegal activity?
    A) Bork Bill
    B) Sarbanes-Oxley Act
    C) Cable Communications Act
    D) Fair and Accurate Credit Transactions Act

25. Despite the advantages of technology, which of the following is sacrificed in exchange for convenience?
    A) Money
    B) Privacy
    C) Technology
    D) Paper

26. What is a separate facility that does not have any computer equipment but is a place where the knowledge workers can move after the disaster?
    A) Disaster recovery plan
    B) Hot site
    C) Cold site
    D) Disaster recovery cost curve

27. Which factor determines when your IT system will be available for knowledge workers to access?
    A) Availability
    B) Accessibility
    C) Reliability
    D) None of the above

28. Your sister sends you an e-mail at school with a screen saver attachment. What should you do?
    A. Download it
    B. Forward the message
    C. Call a tech-savvy friend to help install it
    D. Delete the message

29. You receive an e-mail with an attachment from "IT Security" stating that you need to open the attachment. What should you do?
    A. Follow the instructions
    B. Open the e-mail attachment
    C. Reply and say "take me off this list"
    D. Delete the message
    E. Contact Customer Support Team

30. _____ software detects and removes or quarantines computer viruses.

SECTION B

Q2.

a) What is Information Security? **(Marks 2)**

b) Computer can be subject of an attack and/or the object of an attack. **(Marks 2)**

c) Define the following terms **(Marks 16)**

i) Vulnerability
ii) Threat
iii) Threat agent
iv) DDoS
v) Risk
vi) Exposure
vii) Vector
viii) Malware
ix) Disclosure
x) Authentication
xi) Authorization
xii) Incident

Q3.

a) It's well known that **Acts of Human Error or Failure** is one of the greatest threats to information security, why so? **(Marks 10)**

b) In the information security, define the following terms: **(Marks 10)**

i) Cultural mores
ii) Ethics
iii) Laws
iv) Policy
v) Standards, guidelines, & best practices
vi) Jurisdiction
vii) Long-arm jurisdiction
viii) Case law
ix) Liability
x) Due care
xi) Due diligence

Q4.

a) In IT security speak, its known that Good security practices follow the "90/10" rule, elaborate. **(Marks 2)**

b) Why is information Security Training important in any organization? **(Marks 2)**

c) It's important that as a security specialist, you should remain abreast with some of the key technology components, what do you understand with the following key terms: **(Marks 4)**

i) Firewall
ii) Demilitarized zone (DMZ)
iii) Intrusion Detection Systems (IDS)

d) What is Risk Management? **(Marks 2)**

e) Under risk management control, define the following terms: **(Marks 10)**

i) Avoidance
ii) Transference
iii) Mitigation
iv) Acceptance
v) Risk Appetite

Q5.

a) What is cybercrime? **(Marks 2)**

b) Explain on each of the following **(Marks 10)**

i) Hacking
ii) Virus Dissemination
iii) Computer Vandalism
iv) Cyber Terrorism
v) Software Piracy

c) List some of the advantages of cyber-security when using computer on the Internet. **(Marks 8)**