# UNIVERSITY OF GHANA

## B.SC COMPUTER SCIENCE/INFORMATION TECHNOLOGY, SECOND SEMESTER EXAMINATIONS: 2015/2016

## CSIT 204: INTRODUCTION TO INFORMATION SECURITY (3 CREDITS)

**INSTRUCTION:**

*PLEASE READ THE INSTRUCTIONS AND QUESTIONS CAREFULLY*
*This exam comprises ofSECTION A and SECTION B. You will be graded for clarity and correctness. Write legibly and check answers before handing it in. Answer All Questions in SECTION A and any other THREE (3) Questions of your choice from SECTION B. Answer all questions in the answer booklet provided.*

**TIME ALLOWED:**
*TWO AND A HALF (2½) HOURS*

### SECTIONA(40 MARKS)

1. Which type of program can hide itself from normal inspection anddetection?
   a. Trojanhorse
   b. Stealth Trojan
   c. Spyware
   d. Rootkit

2. A______ occur(s) when a single security element failure defeats the overall security of a system.
   a. spot failure
   b. weakest link failure
   c. defense in depth departure
   d. critical failure

3. A______ isa random string of 40 to 4,000 bits (ones andzeros)usedto encrypt messages.
   a. key
   b.cipher
   c. plaintext
   d. code

4. Ifakeyis43bitslong,howmuchlongerwillittaketocrackitbyexhaustivesearchifitis extended to 50 bits?
   a. 7 times aslong
   b. 14 times aslong
   c. 128 times aslong
   d. 256 times aslong

5. In public key encryption for authentication, the supplicant uses______ toencrypt.
   a. the supplicant's private key
   b. the supplicant's public key
   c. the verifier's private key
   d. the verifier's public key

6. In public key encryption for authentication, the supplicant must prove that it knows______,which nobody else should be able toknow.
   a. the supplicant's public key
   b. the supplicant's private key
   c. the true party's private key
   d. the verifier's private key

7. Digital signatures provide______.
   a. message authentication
   b. message integrity
   c. Both A andB
   d. Neither A norB

8. Ensuring appropriate network,______ means preventing attackers from altering thecapabilities or operation of thenetwork.
   a. Confidentiality
   b. Integrity
   c. availability
   d. functionality

9. ______ is/are effective method(s) to preventing ARP poisoningattacks.
   a. Static tables
   b. Limiting local access
   c. Both A andB
   d. Neither A norB

10. WEP stands for ______.
    a. wireless equivalent privacy
    b. wireless equivalent policy
    c. wired equivalent privacy
    d. wired equivalent policy

11. In ______,usersauthenticatethemselvestotheaccesspointviatheuseofasingle,sharedinitialkey.
    a. WEP
    b. 802.11i pre-shared keymode
    c. WPA pre-shared keymode
    d. All of the above.

12. Which of the following is an example of a wirelessattack?
    a. Unauthorized network access
    b. Man-in-the-middle attack using an evil twin
    c. Wireless DOSattacks
    d. All of theabove

13. The strongest form of authentication is ______.
    a. biometrics
    b. cryptographic authentication
    c. reusablepasswords
    d. smart cards

14. In the context of PKI, ______is the process of accepting public keys and providing newdigital certificates to the users.
    a. provisioning
    b. reflection
    c. coordination
    d. certification

15. ______firewalls always examine application messages indepth.
    a. Static packet filtering
    b. SPI
    c. Application proxy
    d. All of theabove

16. WhichIntrusionPreventionSystemresponsetoanattackisthemosteffectiveinstoppingattacks?
    a. Dropping packets
    b. Limiting suspicious traffic to a certain percentage of the totalbandwidth
    c. Both A and B are equally effective
    d. Neither A norB

17. Any device with an IP address is a ______.
    a. server
    b. host
    c. client
    d. None of theabove

18. If an attacker takes over a firewall, he or she will be able to______.
    a. allow connection-opening requests that violate policy
    b. reroute internal data to alternate paths
    c. provide the false sense that the firewall is still workingcorrectly
    d. All of theabove

19. Assigningsecuritymeasurestogroupsisbetterthanassigningsecuritymeasurestoindividualswithin groups because______.
    a. applying security measures to groups takes less time than applyingthem individually
    b. applying security measures in groups reduces errors in assigning securitysettings
    c. Both A andB
    d. Neither A norB

20. Data Definition Language triggers are used to______.
    a. maliciously attack databases
    b. produce automatic responses if the structure of the database has beenaltered.
    c. Both A andB.
    d. Neither A norB.

21. An Intrusion Detection System is a______control.
    a. preventative
    b. detective
    c. Restorative
    d. All of theabove

22. A ______IDS sends data from many devices at a central managementconsole.
    a. centralized
    b. distributed
    c. fragmented
    d. decentralized

23. A(n) ______ attack requires a victim host to prepare for many connections, using up resources untilthecomputer can no longer serve legitimate users. (Choose the most specificchoice.)
    a. DoS
    b. directly-propagatingworm
    c. distributedmalwar
    d. SYNFlooding

24. A(n) ______attack attempts to make a server or network unavailable to serve legitimate usersbyflooding it with attack packets.
    a. virus
    b. directly-propagating worm
    c. DoS
    d. bot

25. Using botha firewall and host hardening to protecta hostis______.
    a. defense in depth
    b. risk acceptance
    c. an anti-weakest link strategy
    d. adding berms

26. In order to demonstrate support for security, top management must______.
    a. ensure that security has an adequate budget
    b. support security when there are conflicts between the needs of security andthe needs of other businessfunctions
    c. follow security procedures themselves
    d. All of theabove

27. ______ciphers move letters around within a message but characters are notsubstituted.
    a. Transposition
    b. Substitution
    c. BothAandB
    d. NeitherAnorB

28. ______ciphers leave letters in their original positions.
    a. Transposition
    b. Substitution
    c. BothAandB
    d. NeitherAnorB

29. When two parties communicate with each other using symmetric key encryption, how manykeys are used in total to encrypt and decrypt?
    a. 1
    b. 2
    c. 4
    d. 8

30. Strong RSA keys are at least bitslong.
a. 100
b. 256
c. 512
d. 1,024

31. The supplicant creates a digital signature by______.
a. adding the password to the challenge message and hashing thetwo
b. hashing the plain text message
c. encrypting the message digest with its own private key
d. encrypting the message digest with its own public key

32. Which of the following fields are contained on a digitalcertificate?
a. Public key
b. Digital signature
c. Serial number
d. All of theabove

33. WLAN DoS attacks are designed to affect the______ of thenetwork.
a. confidentiality
b. integrity
c. availability
d. authentication

34. A network administrator notices extensive damage to wireless packets. This might indicatea ______attack.
a. man-in-the-middle
b. SYN/ACK
c. DoS floodattack
d. None of theabove

35. Eavesdropping usually is more of a concern for ______LANs than for______LANs.
a. wired,wireless
b. wireless,wired
c. about an equal concern for wired and wirelessLANs
d. None of theabove

36. A______ firewall handling all traditional firewall functions (SPI, ACLs, etc.) as wellas additional security functions such as antivirus filtering, spam filtering, application proxyfiltering, and soforth.
a. unified threat management
b. stateful packet inspection
c. static packet inspection
d. None of theabove

37. Network Address Translation is able to stop______.
a. scanningprobes
b. sniffers from learning anything about the internal IP address of internalhosts
c. Both A andB
d. Neither A norB

38. If an Intrusion Prevention System identifies an attack, it can______.
a. drop the attack packet(s)
b. limit suspicious traffic to a certain percentage of the totalbandwidth
c. Both A andB
d. Neither A norB

39. ______is a password-cracking method wherein the attacker tries all possible passwords, startingwithsingle-characterpasswords.
a. A dictionary attack
b. A hybrid dictionary attack
c. A combinatorial attack
d. Brute-forceguessing

40. The three common core goals of security are______.
a. confidentiality, integrity, and availability
b. confidentiality, information, and availability
c. confidentiality, integrity, and authentication
d. confidentiality, information, and authorization

**SECTION B(60 MARKS)**

**Q1:**

a. State and briefly explain three common security threats to networks such as the University of Ghana network and the security measures necessary to defend against such threats. **[6 marks]**

b. Distinguish between intellectual property in general and trade secrets. **[4 marks]**

c. Briefly describe two (2) forms of security mechanisms that could be deployed in a network and give one example each. **[2 marks]**

d. As network security expert of University of Ghana, state three things you will consider essential in the development of network security analysis. **[2 marks]**

e. What is the difference between spam and phishing? **[2 marks]**

f. Explain IP address spoofing and why it is done? When can an attacker not use IP address spoofing? **[3 marks]**

**Q2:**

a. Describe Distributed Denial of Service. **[2 marks]**

b. Distinguish between credit card theft and identity theft. **[3 marks]**

c. Determine the outcomes of the following problems:

   i. If a key is 43 bits long, how much longer will it take to crack it by exhaustive search if it is extended to 45 bits? **[2 marks]**

   ii. If it is extended to 50 bits? **[1 mark]**

d. Describe the block encryption with Data Encryption Standard. **[3 marks]**

e. Julia encrypts a message to David using public key encryption for confidentiality. After encrypting the message, can Julia decrypt it? Explain your answer. **[2 marks]**

f. How does the verifier check the digital signature? **[4 marks]**

g. How are digital signatures and digital certificates used together in authentication? **[4 marks]**

**Q3:**

a. Distinguish between SSL and TLS. **[3 marks]**

b. Distinguish between transport and tunnel modes in IPsec in terms of packet protection. **[2 marks]**

c. Pretty Good Privacy (PGP) uses public key encryption and symmetric key encryption to encrypt long documents. How might this be possible? **[5 marks]**

d. What is meant by "death of the perimeter?" **[2 marks]**

e. What is Address Resolution spoofing? How could an attacker use ARP spoofing to manipulate host ARP tables? **[4 marks]**

f. What are Service Set Identifiers (SSIDs)? Does turning off SSID broadcasting offer real security? Explain. **[4 marks]**

**Q4:**

**a.** Three (3) main approaches, similar in services they provide, and to some extent, in the mechanisms that they use, have been considered but differ with respective to their scope of applicability and their relative location within the TCP/IP protocol stack. What are the advantages of each of these three (3) approaches? **[9 marks]**

**b.** What is the difference between an SSL connection and an SSL session? **[4 marks]**

**c.** What is the purpose of HTTPS? **[3 marks]**

**d.** Distinguish between Message Authentication Code (MAC) and Digital Signature. **[5 marks]**

**e.** What type of attacks are addressed by message authentication? **[4 marks]**

**Q5:**

**a.** What are the four authentication credentials? **[2 marks]**

**b.** What are one-time-password tokens. **[2 marks]**

**c.** Distinguish between verification and identification. Which requires more matches against templates? Explain [**3 marks]**

**d.** What are the functions of Public Key Infrastructures (PKIs)? **[3 marks]**

**e.** An asset has a value of $1,000,000. In an attack, it is expected to lose 60 percent of its value. An attack is expected to be successful once every ten years. Countermeasure X will cut the amount lost per incident by two-thirds. Counter measure Y will cut the frequency of successful attack in half. Countermeasure X will cost $30,000 per year, while Countermeasure Y will cost $5,000 per year. Do an analysis of these countermeasures and then give your recommendation for which to select. (if any) **[10 marks]**

**Q6:**

**a.** Distinguish between firewalls and Intrusion Detection Systems (IDSs). **[2 marks]**

**b.** Why can a firewall keep up with traffic in general but fail to do so during a major attack? **[2 marks]**

**c.** What are the two limitations of static packet filtering? Explain why each limitation is bad. **[3 marks]**

**d.** What is virtualization? **[2 marks]**

**e.** State the two main types of password guessing approaches and explain their differences. **[3 marks]**

**f.** University of Ghana does a full backup one night. Call this backup UGBKP. On three successive nights, the university does incremental backups, which it labels UGBKP1, UGBKP2, and UGBKP3. In restoration, what backups must be restored first and second? **[2 marks]**

**g.** Distinguish between file/directory data backup and image backup. **[2 marks]**

**h.** As security expert and a consultant, you have the privilege to advise a small company.

i. Would you recommend using a firewall? Explain. **[2 marks]**

ii. Would you recommend using antivirus filtering? Explain. **[2 marks]**